PROTECTING SOUTH AFRICAN COMPANIES' AGAINST CYBERCRIME: A CRITICAL ANALYSIS OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF ARTIFICIAL INTELLIGENCE TO PROTECT COMPANIES' ONLINE MEETINGS

by

Dr Julian Kritzinger

D.E.L.F., BA (Stel.) LLB (UNISA)
LLM (Stel.) LLM (Stel.)
PhD (UCT)

Thesis presented for the Degree of
DOCTOR OF PHILOSOPHY
in the
FACULTY OF LAW
DEPARTMENT OF COMMERCIAL LAW
UNIVERSITY OF CAPE TOWN

Supervisor: Dr Kathy Idensohn
November 2020

University of Cape Town

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

DECLARATION

I, Julian Kritzinger, hereby declare that the work on which this thesis is based is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree in this or any other university.

I authorise the University to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

Signature: Signed by candidate

Date: 4 November 2022

PLAGIARISM DECLARATION

1. I know that plagiarism is a serious form of academic dishonesty.

2. I have read the document about avoiding plagiarism, am familiar with its contents and have avoided all forms of plagiarism mentioned there.

3. Where I have used the words of others, I have indicated this by use of quotation marks.

4. I have referenced all quotations and properly acknowledged other ideas borrowed from others.

5. I have not and shall not allow others to plagiarise my work.

6. I declare that this is my own work.

7. I am attaching the summary of the Turnitin match overview.

Signature: **Julian Kritzinger**

Date: 4 November 2022

ACKNOWLEDGEMENT

Introduction

Since I started studying fulltime in 2002, I did so with the full encouragement of my family. Although most of them are no longer with me today, they really believed in me. I know that they would have been immensely proud that I have obtained a double Masters and a double Doctorate in Commercial Law.

Synopsis of Life Lessons

Such an achievement can never be attained without the full support and encouragement of one's closest family members. Each of the respective life lessons that my family instilled in me were necessary to reach this success:

- My paternal grandmother, Melvonie (Botha) Kritzinger (1919 – 2004) taught me the power of daily routine – in order to sustain momentum;
- My maternal grandmother, Una (Rabie) Kloppers (1917 – 1995) taught me he importance of discipline and work ethic - how to work hard, the importance of detail and to never stand back from any challenge;
- My father, Pieter Kritzinger (1940 – 2018) taught me how books are the key to truly unlock and appreciate the world's wonders around me – some of my earliest memories are of me and my father reading books in the local library; and
- My mother, Jean (Kloppers) Kritzinger (1950 -) taught me the importance of daily administration and logistics – and how this back-up supports success.

Previous PhD Thesis Dedicated to Father

My previous PhD, *'Commercial Arbitration in Cyberspace: The Legal and Technical Requirements Towards a More Effective Lex Electronica Arbitralis'*, was dedicated to my father, Pieter Kritzinger. Fortunately he was still able to attend my graduation ceremony at the University of Cape Town on 21 December 2017, eight months before his unexpected death on 7 August 2018.

This PhD Thesis Dedicated to Mother

Since my previous thesis was dedicated to my father, this thesis is dedicated to my mother, Jean Kritzinger. At the time of completion, I have been a professional student for 22 years. I want to thank her for all of the love and support during this period. All of my accomplishments would never have been possible if it was not for your support, so thank you from the bottom my heart.

Expression of Gratitude to God

Lastly, I want to thank God for the gift of life and for making all of this possible. I want to thank Him for all of my blessings and for my family who helped me so much along the way. I want to also thank Him for all of my opportunities and for the strength to make the most of them. I want to also thank Him for His guidance through difficult times and for giving me the courage to face whatever came my way.

ABSTRACT

South Africa (SA) has one of the highest rates of cybercrime in the world and SA companies' cyberassets are vulnerable to cyberattacks. Since SA companies' online meetings (OMs) are conducted on an online platform and use online databases that contain sensitive Personally Identifiable Information (PII), they are particularly prone to cyberattacks. Artificial Intelligence (AI) could however be used to resist cyberattacks on a company's cyberassets, such as its online platform and its online databases. Contrariwise, AI could be used by cybercriminals to instigate cyberattacks.

This thesis will critically analyse how a more detailed treatment of the directors' duty of care in relation to cybersecurity can help to make SA companies more cyberresilient, with the specific focus on their OMs, as well as the role that the use of AI can play in this regard, and how it should be regulated?

Where other researchers looked at OMs as a means to enhance corporate governance and corporate social responsibility (CSR), they have failed to look at the dangers that cybercrime present to OMs and that directors may be held personally liable in the event that a company's cybersecurity was inadequate to thwart a cyberattack and the company's cyberassets were compromised.

By means of legal comparison, this thesis critically analyses how directors need to exercise their duty of care in relation to cybersecurity in order to help make SA companies more cyberresilient, and will argue for directors' use of AI as a tool to help resist cybercrime, and its regulation.

This thesis mounts the challenge of SA cybercrime by firstly looking at how OMs and the duty of care in relation to cybersecurity are regulated in different jurisdictions, and how corporate governance and CSR should include AI, while it also looks at directors' exposure to liability in terms of the use and regulation of AI.

It is submitted that the SA Cybercrimes Act 19 of 2020 and the King Code should be updated to include the use of AI, since it is an important tool for directors in the fight against cybercrime.

LIST OF KEYWORDS

Annual General Meeting (AGM); Artificial Intelligence (AI); Blockchain; Companies Act 71 of 2008 (‘the Act’); Consultative AI; Corporate Governance; Corporate Social Responsibility (CSR); Critically Conscious Computing (CCC); Cyberattack; Cyberbreach; Cybercrimes Act 19 of 2020; Cyberrisks; Cybersecurity; Cybersecurity ‘Red Flags;’ Data Analyis; Duty of Care; Environmental, Social and Governance (ESG) Investment Considerations; Information Regulator (IR); Internet; Liability; Online Meeting (OM); Online Platform; Personal Information; Protection of Personal Information (POPI) Act 4 of 2013; Right on Privacy; Self-Aware AI; Shareholders’ Meeting; Supportive AI.

TABLE OF CONTENTS

DECLARATION i

PLAGIARISM DECLARATION ii

ACKNOWLEDGEMENT iii

ABSTRACT iv

LIST OF KEYWORDS USED v

TABLE OF CONTENTS vi

CHAPTER 1: INTRODUCTION

1. INTRODUCTION 1

2. THE PROBLEM OF CYBERCRIME AND ITS CONSEQUENCES FOR COMPANIES 1

2.1. The Use of AI to Commit Cybercrime 3

2.2. Consequences of Cyberbreaches for Shareholders/ Stakeholders 4

3. A SHORT HISTORICAL OVERVIEW OF THE LARGEST CYBERATTACKS ON COMPANIES 4

3.1. US Cyberattacks and Cyberbreaches 4

3.2. SA Cyberattacks and Cyberbreaches 6

4. ONLINE MEETINGS (OMs) AS A VULNERABLE ASPECT OF A COMPANY'S OPERATIONS ……. 10

4.1. The Act's Regulation of Company Meetings and OMs …. 10

4.2. Online Platform …….. 11

4.3. Online Databases with Personally Identifiable Information (PII) ……... 12

5. THE CAUSAL LINK BETWEEN OMs AND IMPROVED CORPORATE GOVERNANCE ……..13

6. THE FURTHER CHALLENGES OF OMs IN TERMS OF CYBERSECURITY …….. 17

6.1. OMs as High Risk Events for Cyberbreaches, Worsened by the Covid 19-Pandemic …… 18

6.2. The Haphazard Regulation of OMs …… 19

6.3. A Lack of Guidance for SA Directors on Cybersecurity-Related AI …….. 20

6.4. Companies' and Directors' Further Exposure to Liability for the Improper Exercise of their Duty of Care In Relation to Cybersecurity and the Use of AI …… 22

7. THE USE OF ARTIFICIAL INTELLIGENCE (AI) TO HELP PROTECT A COMPANY'S CYBERASSETS AND ITS OMs …… 24

8. THE ROLE OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY TO HELP MAKE SA COMPANIES MORE CYBERRESILIENT …… 29

9. RESEARCH OBJECTIVE …….. 31

10. OUTLINE OF RESEARCH TOPIC 33

11. REASONS FOR SELECTING THE TOPIC 34

11.1. Primary Research Issues 34

11.2. Lack of Existing Literature in SA 35

11.3. Issues Have Far-Reaching Implications for Corporate Governance, Cybersecurity and the Protection of Shareholders'/Stakeholders' Privacy and PII 36

11.4. No Cross-Reference in Existing Legal Sources 37

11.5. Industry Custom on the Use of AI Inconclusive 38

12. RESEARCH QUESTION 38

13. STRUCTURE 39

14. RESEARCH METHODOLOGY 41

14.1. Legal Comparison 41

14.2. Literature Review 43

15. CONCLUSION 43

CHAPTER 2: THE REGULATION OF OMs IN OTHER JURISDICTIONS

1. INTRODUCTION 45

2. SHORT HISTORICAL OVERVIEW OF OMs 45

2.1. Advent of OMs in SA …….. 47

3. US ……..…… 49

3.1. US Federal Law …… 49
3.1.1. US Securities Exchange Commission (SEC) …….. 51

3.2. US State Law ……52
3.2.1. The Delawarean Example: OMs With Specific Procedures …… 53
3.2.2. The Colorado Example: OMs Without Specific Procedures …… 54
3.2.3. The Massachusetts and Montana Example: Limitations on Public Companies ……. 55
3.2.4. The New York (NY) Example: Obligatory Shareholder Input ……..…….. 56
3.2.5. The California and Maryland Example: Shareholder Participation ……..……57
3.2.6. The Illinois Example: No OMs ……..…… 59

3.3. Stock Exchange Rules ……...60

4. UK ……...60

4.1. European Union (EU) 'Directive on the Encouragement of Long Term Shareholder Engagement of 2017' ……..…..60

4.2. UK Companies Act of 2006 (Ch.46), section 360A ……. 61

4.3. UK Corporate Insolvency and Governance Act (CIGA) of 2020 ……. 64

4.4. UK Department for Business, Energy and Industrial - Strategy's Memorandum of 2020 …… 66

4.5. UK Chartered Governance Institute's Guidelines of 2020.67

4.6. Stock Exchange Rules ……...67

4.7. Case Law ……67

5. SA ……68

5.1. The Act ……68

5.2. King Reports I – IV …….. 71

5.3. Johannesburg Stock Exchange (JSE) '*Listing Requirements*' ……..……... 71

5.4. SA Companies Amendment Bill of 2021 ……72

6. LESSONS FOR SA ON THE REGULATION OF OMs IN OTHER LEGAL JURISDICTIONS ……..…. 75

6.1. US ……75

6.2. UK …… 78

6.3. SA ……81

7. CONCLUSION …… 83

CHAPTER 3: THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY

1. INTRODUCTION …….. 86

2. THE DIRECTORS' DUTY OF CARE IN SA …… 86

2.1. Common Law ……86
2.1.1. Common Law Negligence and the Duty of Care ……. 88

2.2. SA Constitution of 1996 ……91

2.3. The Act ……92

2.4. SA POPI 4 of 2013 ……. 97

2.5. Case Law ……98

2.6. King Reports I – IV …….. 99
2.6.1. King Report I on Corporate Governance of 1994 ……100
2.6.2. King Report II on Corporate Governance of 2002 …….. 101
2.6.3. King Report III on Corporate Governance of 2009 ……. 104
2.6.4. King Report IV on Corporate Governance of 2016 …….106

3. THE DIRECTORS' DUTY OF CARE IN THE UNITED KINGDOM (UK) ……..….. 107

3.1. Common Law ……108

3.2. UK Companies Act of 2006 …….. 109

3.3. GDPR ……..…. 110

3.4. UK Data Protection Act (DPA) of 2018 ……...112

3.5. Case Law ……112

4. THE DIRECTORS' DUTY OF CARE IN THE UNITED STATES (US) ……... 114

4.1. Common Law ……115

4.2. Federal Law …….. 116

4.3. States' Law …… 118

4.4. Case Law ……119
4.4.1. Federal Level ……119
4.4.2. US States' Case Law …….. 120
4.4.2.1. California ……120
4.4.2.2 Delaware …… 121
4.4.2.3. Georgia …….. 124
4.4.2.4. Pennsylvania …… 124
4.4.2.5. Minnesota …… 125

4.4.2.6. New Jersey …… 125

5. REMEDIES FOR DIRECTORS WHO BREACHED THEIR DUTY OF CARE IN RELATION TO CYBERSECURITY .. 127

5.1. The Act, section 71(5): Taking the Removal of a Director on Review …….. 127

5.2. The Act, section 76(4): Business Judgment Rule (BJR) ...127

5.3. The Act, section 77(9): The Court's Relief of a Director …131

5.4. The Act, section 78: Indemnity Insurance …… 131

5.5. The Act, section 165(3): Application to Set Derivative Action Aside ……..132

5.6. Contract Breach …….. 132

5.7. Unfair Dismissal …….. 132

6. NO DIFFERENTIATION BETWEEN EXECUTIVE AND NON-EXECUTIVE DIRECTORS ……132

7. LESSONS FROM A LEGAL COMPARISON OF THE SA, UK AND US DUTY OF CARE IN RELATION TO CYBERSECURITY …….. 133

8. CONCLUSION ……..137

CHAPTER 4 : THE INDIRECT IMPACT OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY ON CORPORATE GOVERNANCE AND CORPORATE SOCIAL RESPONSIBILITY (CSR)

AND ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG) INVESTMENT CONSIDERATIONS

1. INTRODUCTION …….. 139

2. THE EVOLUTION OF THE EMPHASIS ON CSR TO SUSTAINABILITY TO ESG INVESTMENT CONSIDERATIONS ……140

2.1. The Origins and Development of CSR and ESG Investing 141

2.2. The Characteristics of CSR and ESG Investing …….. 143

3. THE EXERCISE OF SA DIRECTORS' DUTY OF CARE IN TERMS OF CORPORATE GOVERNANCE AND CSR 144

3.1. King Report I on Corporate Governance of 1994 ……148

3.2. King Report II on Corporate Governance of 2002 …….. 148
3.2.1. Stakeholder Inclusive Approach ……. 150
3.2.2. African Approach ……151

3.3. King Report III on Corporate Governance of 2009 ……. 152

3.4. King Report IV on Corporate Governance of 2016 …….153

4. THE EXERCISE OF SA DIRECTORS' DUTY OF CARE IN TERMS OF ESG INVESTMENT CONSIDERATIONS . 154

4.1. Relevant International ESG Sources ……. 158
4.1.1. EU 'Taxonomy Regulation of 2020' and the EU 'Sustainable Governance Initiative' ……..…… 159
4.1.2. UK Financial Reporting Council (FRC)'s Stewardship Code of 2020 ……. 160

4.2. Relevant SA ESG Sources …… 161
4.2.1. SA Code for Responsible Investing in SA (CRISA) of

2011 161
4.2.2. JSE's Responsible Investment Index Series (RIIS) 163
4.2.3. The Protection of Stakeholders' Interests 163
4.2.4. Shareholder and Stakeholder Activism 164
4.2.5. Disclosure 165

5. THE EXERCISE OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI AND BLOCKCHAIN TECHNOLOGY 166

5.1. The Use of AI at OMs 167
5.1.1. Challenges of AI 169

5.2. The Use of Blockchain Technology at OMs 170
5.2.1. Challenges of Blockchain Technology 172

6. LESSONS ON HOW THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI COULD HELP TO IMPROVE CORPORATE GOVERNANCE, CSR AND ESG INVESTMENT CONSIDERATIONS AT SA OMs 174

7. CONCLUSION 176

CHAPTER 5: THE FURTHER ACCOUNTABILITY MECHANISMS TO HOLD DIRECTORS ACCOUNTABLE FOR THE WAY IN WHICH THEY EXERCISE THEIR DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI

1. INTRODUCTION 178

2. AN OVERVIEW OF THE INTERNATIONAL PRIVACY LAW AND CYBERSECURITY REGIMES 179

2.1. The International Privacy Law Regime …….. 179
2.1.1. UN Universal Declaration on Human Rights of 1948 ……. 179
2.1.2. UN International Covenant on Civil and Political Rights of 1966 ……..…….. 180
2.1.3. The Organisation for Economic Co-operation and Development (OECD)'s Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data of 1981 ……. 180

2.2. The International Cybersecurity Regime …….. 180
2.2.1. The Council of Europe (CoE)'s Budapest Convention of 2001 …… 181

3. AN OVERVIEW OF THE SA CYBERSECURITY AND PRIVACY LAW REGIMES …… 181

3.1. The SA Common Law Position on Cybersecurity ..……. 182

3.2. The Legislative Regulation of Cybersecurity in SA …….. 182
3.2.1. The SA Electronic Communications and Transactions Act (ECTA) 25 of 2002 ……182
3.2.2. The SA Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 70 of 2002 ……..183
3.2.3. The SA Protection of Personal Information (POPI) Act 4 of 2013 …… 184
3.2.4. The SA Cybercrimes Act 19 of 2020 …….. 185

4. THE FURTHER ACCOUNTABILITY MECHANISMS TO HOLD DIRECTORS ACCOUNTABLE FOR THE WAY IN WHICH THEY EXERCISE THEIR DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI ……. 186

4.1. Constitutional Right to Privacy ……..……. 188

4.2. The Act ……..…….. 188
4.2.1. Section 20: The Validity of Company Actions

4.2.1.1. Section 20(4): Restraining the Company from Contravening the Act ……..188
4.2.1.2. Section 20(5): Restraining the Company from Contravening the Memorandum of Incorporation (MOI) …… 189
4.2.1.3. Section 20(6): Each Shareholder Has a Claim Against Anyone Who Intentionally, Fraudulently or Due to Gross Negligence Causes Anything Inconsistent with the Act …….. 189
4.2.2. Section 71: The Removal of Directors…… 191
4.2.3. Section 77: Liability of Directors ……192
4.2.4. Section 78(6): Directors Cannot be Indemnified Against Liability for Not Exercising Their Duty of Care ……193
4.2.5. Section 165: Legislative Derivative Action …….. 193
4.2.6. Section 218(2): Claim for Damages …… 195
4.2.6.1. The 'No Reflective Loss' Principle ……..197

4.3. SA POPI 4 of 2013 ……199

4.4. SA Criminal Procedure Act 51 of 1977 …….. 199

4.5. Common Law …… 200
4.5.1. Common Law Duty of Care …….. 200
4.5.2. Common Law Personal Action …… 201

4.6. Contract …….. 202

4.7. *Concursus Actionem* …….. 203

4.8. Regulatory Action ……203
4.8.1. King Reports on Corporate Governance …….. 203
4.8.2. Stock Exchange Listing Requirements …….. 204
4.8.3. SA Companies and Intellectual Property Commission (CIPC) ……..204

5. LESSONS ON HOW DIRECTORS' USE OF AI SHOULD BE REGULATED IN THE SA CYBERCRIMES ACT 19 OF 2020 AND THE KING CODE …… 205

6. CONCLUSION ……..212

CHAPTER 6: CONCLUSION

1. INTRODUCTION …….. 213

2. RECOMMENDATIONS FOR SA ON THE REGULATION OF OMs IN OTHER LEGAL JURISDICTIONS ……..……213

2.1. US …… 214

2.2. UK …… 218

2.3. SA …… 221

3. RECOMMENDATIONS FROM A LEGAL COMPARISON OF THE SA, UK AND US DUTY OF CARE IN RELATION TO CYBERSECURITY …..……..223

4. RECOMMENDATIONS ON HOW THE DUTY OF CARE IN RELATION TO CYBERSECURITY COULD HELP TO IMPROVE CORPORATE GOVERNANCE AND CSR, ESG INVESTMENT CONSIDERATIONS AT SA OMs ……....227

5. RECOMMENDATIONS ON DIRECTORS' EXPOSURE TO LIABILITY IN TERMS OF THE USE AND REGULATION OF AI …… 230

5.1. Recommendations on the Adequacy of the SA Privacy Law and Cybersecurity Regimes and the Ways in Which They Are Enforced …….. 230

5.2. Recommendations on the Further Accountability Mechanisms to Hold Directors Accountable for the Way in Which They Exercise Their Duty of Care in Relation

to Cybersecurity and the Use of AI ……232

5.3. Recommendations on How Directors' Use of AI Should Be Regulated in the SA Cybercrimes Act 19 of 2020 and the King Code ……...236

6. THE DISTINCTION BETWEEN THE PROPOSED LEGAL REGULATION OF AI IN THE SA CYBERCRIMES ACT 19 OF 2020 AND ITS REGULATION BY MEANS OF CORPORATE GOVERNANCE GUIDANCE IN THE KING CODE ……..… 241

7. SUMMARY OF RECOMMENDATIONS……... 243

8. FINAL REMARKS …… 245

BIBLIOGRAPHY

I. BOOKS …… 249
II. RESEARCH DISSERTATIONS ……251
III. JOURNAL ARTICLES …… 252
IV. CASE LAW ……..…… 258
V. LAWS AND REGULATIONS ……..….. 263
VI. INTERNATIONAL CONVENTIONS AND RELATED DOCUMENTS ……..…… 267
VII. BILLS, DIRECTIVES, OFFICIAL PUBLICATIONS AND POLICIES ……..... 268
VIII. ENFORCEMENT AGENCY SOURCES …….. 271
IX. REPORTS ……...…… 272
X. GUIDELINES, RULES AND STANDARDS ……273
XI. LISTING REQUIREMENTS AND STOCK EXCHANGE SOURCES……..…… 276
XII. ONLINE SOURCES ……..……..…… 277
XIII. NEWSPAPERS AND MAGAZINES …… 287
XIV. SOURCES RELATED TO SERVICE PROVIDERS AND

THEIR WEBSITES …….. 291
XV. WEBSITES OF COMPANIES' OMs AND RELATED INFORMATION ……294
XVI. BLOGS …….. 295

APPENDIX

I. LIST OF DEFINITIONS …….. 297

CHAPTER 1:

INTRODUCTION

1. INTRODUCTION

According to Surfshark's '*Global Data Breach Heat Map 2022*,' South Africa (SA) has the sixth highest rate of cybercrime in the world, because every 52 Internet users in a million fell prey to cybercrime in 2021.[1] SA Internet users and companies are as a result vulnerable to cyberattacks.[2] Since SA companies' online meetings (OMs) are conducted on an online platform and use online databases that contain sensitive personal information and Personally Identifiable Information (PII) of the company's shareholders/stakeholders, they are particularly prone to cyberattacks.

Artificial Intelligence (AI) could be used to resist the cyberattacks of a company's cyberassets, such as its online platform and its online databases. Contrariwise, AI could also be used by cybercriminals to instigate cyberattacks.

AI is the imitation of natural intelligence by computer algorithms that follow a certain reasoning and which then apply such reasoning to reach conclusions, and that is also able to correct itself in the process.[3] It also refers to intelligent machines that use algorithms to function like humans.[4] AI consists of different sub-types that are available to either cause cybercrime – or to help improve cybersecurity.[5]

This Chapter will explain that this thesis will critically analyse how a more detailed treatment of the directors' duty of care in relation to cybersecurity can help to make SA companies more cyberresilient, with the specific focus on their OMs, as well as the role that the use of AI can play in this regard, and how it should be regulated.

2. THE PROBLEM OF CYBERCRIME AND ITS CONSEQUENCES FOR COMPANIES

---

[1] Surfshark '*Global Databreach Heat Map 2022*,' *s.p.*, available online at <https://surfshark.com/research/data-breach-impact/statistics>, last accessed on 13 January 2023.

[2] *Ibid.*

[3] Sarker 'AI-Based Modelling: Techniques, Applications, and Research Issues Towards Automation, Intelligence and Smart Systems' in *SN Computer Science* 3(2021) 1 - 2.

[4] *Ibid.*

[5] Shani 'AI Automation: What You Need to Know' by the *Marketing AI Institute*, *s.p.*, available online at <https://www.marketingaiinstitute.com/blog/automation-and-ai-what-you-need-to-know#:~:text=AI%20is%20not%20the%20same,its%20own%20pathways%20to%20success.>, last accessed on 2 July 2022.

Cybercrime is performed online on computers and the Internet.[6] It is criminal activities that are committed on a computer system, with the use of software and the Internet.[7] There are different types of cybercrimes, such as cyberterrorism, cyberuttering (the presentation of false information), cyberwarfare, hacking, identity theft, the misuse of websites, phishing, (the sending of sham emails to obtain personal information in response), ransomware (online extortion) and other forms.[8] Advancements in the development of AI software help cybercrime to proliferate, especially if it used in cyberattacks that are directed on companies.[9]

The SA Cybercrimes Act 19 of 2020, Part I, identifies nine such cybercrime offences, and sets these Type 1 offences out in sections 2 to 10.[10] These offences are unlawful access to a computer system; the unlawful interception of data; unlawful acts pertaining to the use of software or hardware; the unlawful interference with data or a software programme; the unlawful interference with a database or a computer system; the unlawful use of passwords or codes; cyberfraud; cyberforgery and cyberuttering; and cyberextortion, or ransomware.[11] The use of AI for the intent to commit of cybercrime is not listed.

Cybercrime is not mentioned in the SA Electronic Communications and Transactions Act (ECTA) 25 of 2002, the SA Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 70 of 2002, the SA Protection of Personal Information (POPI) Act 4 of 2013, nor the SA Cybercrimes Act 19 of 2020, and as a result it does not prohibit the use of AI to commit cybercrime.[12]

Cybercriminals conduct their cybercrime activity and then direct their cyberattack on an individual or an entity, such as a company. Such a cyberattack can be described as an illegal attempt by means of the Internet to harm an individual or an entity, such as a company's computer system or information on it.[13]

Such a cyberattack then causes a cyberbreach, which can be described as an incident where information is either stolen, copied, transmitted, viewed or used by an unauthorised party.[14] This information is usually either of a confidential or a personal

---

[6] Mabunda *SA Legislative Responses to Cybercrime*, PhD Thesis submitted at the University of the Western Cape, 2021, 9 – 14.
[7] *Ibid.*
[8] *Ibid.*
[9] Velasco 'Cybercrime and AI: An Overview of the Work of International Organisations on Criminal Justice and the Applicable International Instruments' in *ERA Forum* 23(2022) 111 – 114.
[10] SA Cybercrimes Act 19 of 2020, Part I.
[11] SA Cybercrimes Act 19 of 2020, sections 2 to 10.
[12] SA Electronic Communications and Transactions (ECTA) 25 of 2002; SA Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) 70 of 2002; SA Protection of Personal Information (POPI) 4 of 2013; SA Cybercrimes Act 19 of 2020.
[13] Cambridge Dictionary, *s.v.* '*cyberattack*,' available online at <https://dictionary.cambridge.org/dictionary/english/cyberattack>, last accessed on 12 January 2023.
[14] Sutherland '*What is a Directors Liability Following a Cyberbreach?*' *op cit s.p.*

nature.[15] This information could belong to the company itself (intellectual property) or it could be shareholders' or stakeholders' personal information that is in possession of the company, and which is then compromised.[16] Stakeholders are groups or an individual who have a legal or moral interest or a share in a company.[17]

A cyberbreach is in other words an online security violation of confidential information where confidential or personal information is copied, edited, sent, stolen or used by a cybercriminal.[18] A cyberbreach can also be described as a data spill.[19] Cyberbreaches range from intensive attacks by so called, 'black hat' cybercriminals who hack for personal gain or malice, to organised cybercrime syndicates, political activists and even national governments.[20] The target is usually entities with poorly configured cybersecurity systems or clouds and computer equipment whose cybersecurity measures have a weak spot.[21] Information that is leaked can vary from national security matters, to the trade secrets of a company, to the personal information of the shareholders and stakeholders of a company.[22]

A cyberbreach that was caused deliberately by a person who worked with such information, such as an employee, is referred to as a data leak.[23]

Some countries, such as SA, have passed legislation, such as the SA POPI Act 4 of 2023, to protect privacy in the format of personal information, and this requires a company, which has been subject to a cyberbreach, to inform shareholders and stakeholders when a cyberbreach occurred, and to take remedial action.[24]

2.1. The Use of AI to Commit Cybercrime

The problem is that cyberattacks are getting much more frequent and more sophisticated, since cybercriminals have now started to use AI to bypass ordinary cybersecurity systems and measures that use AI themselves.[25]

AI is a powerful tool that cybercriminals uses to commit cybercrime and to help gain access to a company's cyberassets, such as its online platform and its online

---

[15] Sutherland '*What is a Directors Liability Following a Cyberbreach?*' *op cit s.p.*
[16] *Ibid.*
[17] Keay *The Enlightened Shareholder Value and Corporate Governance* 12.
[18] Li *et al.* 'A Comprehensive Review Study of Cyberattacks and Cybersecurity: Emerging Trends and Recent Developments' in *Energy Reports* 7 (November 2021) 8177 – 8181.
[19] *Ibid*.
[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*
[23] *Ibid.*
[24] SA POPI 4 of 2013.
[25] United Nations (UN) Interregional Crime and Justice Research Institute (UNICRI) *et al.* '*Malicious Uses and Abuses of AI*,' 6 – 27, available online at <https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf>, last accessed on 25 January 2023.

databases. AI could be used to not only detect weakspots, but also to instigate and increase cyberattacks on a company's cyberassets and to also encrypt or destroy them.

In 2020, the United Nations' (UN) Interregional Crime and Justice Research Institute (UNICRI), collaborated with Europol and Trend Micro to do research on the ways and trends in which AI is used for cybercrime, entitled; '*Malicious Uses and Abuses of Artificial Intelligence*.'[26] This comprehensive study explains in great detail the ways in which AI is used to launch cyberattacks on cybersecurity systems and online platforms by means of AI malware, the abuse of AI Clouds, the abuse of smart assistants, AI-supported password guessing, AI-supported CAPTCHA breaking, AI-aided encryption, AI-aided human impersonation, AI-supported hacking, and social engineering.[27]

Research still needs to be done on how many SA companies use AI in their cybersecurity systems, but according to the latest research by Dataprot, only 37% of entities worldwide use AI in their operations.[28]

2.2. Consequences of Cyberbreaches for Shareholders/Stakeholders

When a cybercriminal hacks an online platform to improperly access the PII in its online databases, the consequences can be devastating for the companies' shareholders and stakeholders. Identity thieves could get hold of their personal information and they could suffer from a range of losses, ranging from mere inconvenience and out-of-pocket expenses to credit, emotional and reputational losses or even lost opportunities.[29] Johnson explains that in more extreme cases, affected persons could be blackmailed, stalked by an assailant, or even physically harmed.[30]

3. A SHORT HISTORICAL OVERVIEW OF THE LARGEST CYBERATTACKS ON COMPANIES

This section will give a short overview of some of the largest cyberbreaches that were caused by cybercrime, and that occurred at United States' (US) and SA companies in the last ten years to show what kinds of damage were caused.

3.1. US Cyberattacks and Cyberbreaches

---

[26] UNICRI *et al. op cit* 6 – 27.
[27] *Ibid.*
[28] Dataprot *'55 Fascinating AI Statistics and Trends,' s.p.*, available online at <https://dataprot.net/statistics/ai-statistics/#:~:text=Key%20AI%20statistics,billion%20a%20year%20by%202025.>, last accessed on 25 January 2023.
[29] Johnson 'Cybersecurity, Identity Theft and the Limits of Tort Liability' in *South Carolina Law Review* 57(2005) 257.
[30] *Ibid.*

Some of the largest cyberbreaches in history occurred in the mid-2010's in the US.[31]

In October 2013, a cyberbreach at Adobe Systems took the personal information of 2.9 million of its customers.[32]

In November 2013, a cyberbreach at Target Corporation compromised the personal information of more than 70 million customers.[33] This event was followed by declines in revenue, declining share prices, retrenchments, the dismissal of the Chief Executive Officer (CEO) and court cases that dragged on years afterwards.[34] In addition, many banks had to limit the further personal debts of those affected, monitor any withdrawals on their accounts and provide them with new credit and debit cards.[35]

In September 2014, Home Depot suffered a cyberbreach and it had cost the company US$62 Million to conduct the subsequent investigation, and to recover personal information and to pay legal expenses.[36]

In October 2014, JPMorgan Chase had a cyberbreach that compromised the personal information of 76 million households.[37]

In 2020 and 2021, at the hight of the Covid-19 Pandemic (the Pandemic), a big crisis occurred when it was discovered that millions of the online platform provider, Zoom's, users' privacy and personal information were compromised, because Zoom's online platforms were not properly end-to-end encrypted and allowed cybercriminals to 'Zoombomb' in on OMs.[38] This type of cybercrime that is specifically directed towards OMs have since been referred to as 'Zoombombing' and it occurs when a cybercriminal manages to find a cybersecurity loophole in an online platform and then hijacks it to

---

[31] Johnson *op cit* 257.

[32] *S.n.* 'Adobe Warns 2.9 Million Customers of Data Breach After Cyberattack' in *The Guardian* of 3 October 2013, *s.p.*, available online at <http://www.theguardian.com/technology/2013/oct/03/adobe-hacking-databreach-cyber-attack>, last visited on 8 July 2021.

[33] McKoy 'Target to Pay $18.5 Million for 2013 Data Breach that Affected 41 Million Consumers' in *USA Today* of 23 May 2017, *s.p.*, available online at <https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/>, last accessed on 8 July 2021.

[34] Clark 'Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer' in *International Business Times* of 5 May 2014, *s.p.*, available online at <https://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056>, last accessed on 8 July 2021.

[35] McGrath '*Target Profit Falls 46% on Credit Card Breach and the Hits Keep on Coming,*' *s.p.,* available online at <https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/?sh=57f7cb937326>, last accessed on 11 May 2021.

[36] Home Depot '*The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in all US Stores,*' Press Release of 18 September 2014, *s.p.*, available online at <https://ir.homedepot.com/news-releases/2014/09-18-2014-014517752>, last accessed on 8 July 2021.

[37] CNBC Staff Report '*JP Morgan Attack Hits 76 Million Households,*' *s.p.*, available online at <https://www.cnbc.com/2014/10/02/jpmorgan-details-breadth-of-march-cyberattack.html>, last accessed on 8 July 2021.

[38] Spadafora '*Zoom Security Issues: What's Gone Wrong and What's Been Fixed*,' *s.p.*, available online at <https://www.tomsguide.com/news/zoom-security-privacy-woes>, last accessed on 5 October 2022.

either disrupt it or to commit cybercrime.[39] Reseach by Spadafora, sets out a detailed timeline of cyberbreaches at OMs that were held on Zoom and details how this crisis unfolded and contains numerous case studies where participants' privacy and/or personal information were compromised.[40]

In the aftermath of the Zoom crisis, the problem with cyberbreaches at OMs become so grave that on 16 February 2022, the US Federal Bureau of Investigation (FBI) had to issue a Public Service Announcement, entitled; '*Business E-Mail Compromise (BEC): Virtual Meeting Platforms;*' to warn the participants at OMs of BEC scams.[41] This warning explains that this is a type of scam that is performed by hackers who gain access to online platforms via personal e-mail accounts through social engineering and online intrusion.[42] The FBI warned that hackers then compromise a participant's e-mail account, use their picture, together with deepfake audio that sounds like that victim's voice and then gain access to the online platform, which then compromise the privacy of the other participants, while they steal their personal information from the online databases.[43]

3.2. SA Cyberattacks and Cyberbreaches

There were also numerous cyberattacks and cyberbreaches in SA over the years.

In 2013, malware was inserted in payment terminals at various SA fast food restaurants to obtain credit card information of an undisclosed number of customers, and this cyberbreach had cost SA banks an undisclosed amount to contain.[44]

In 2016, hackers of a group, called 'Anonymous,' breached Armscor's cybersecurity and targeted their supply chain database and leaked the personal information of 20 000 of its suppliers.[45]

---

[39] Lorenz 'Zoombombing: When Videoconferences Goes Wrong' in the *NY Times* of 20 March 2020, *s.p.*, available online at <https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html>, last accessed on 24 January 2023.

[40] Spadafora *op cit s.p*.

[41] US Federal Bureau of Investigation (FBI) '*Public Service Announcement: Business E-Mail Compromise: Virtual Meeting Platforms*,' *s.p.*, available online at <https://www.ic3.gov/Media/Y2022/PSA220216>, last accessed on 5 October 2022.

[42] *Ibid.*

[43] FBI *op cit s.p.*

[44] Kelion '*Dexter Payment Card Malware Strike SA,' s.p.*, available online at <https://www.bbc.com/news/technology-24550505>, last accessed on 8 July 2021.

[45] Hosken 'Military Secrets Stolen' in *Times Live SA* of 13 July 2021, *s.p.*, available online at <https://www.timeslive.co.za/news/south-africa/2016-07-13-military-secrets-stolen/>, last accessed on 19 June 2021.

In March 2017, a cyberbreach compromised the personal information of 7 million customers of the local cinema chain, Ster-Kinekor.[46] In October 2017, the largest cyberbreach in SA history occurred when Jigsaw Holdings was hacked and the personal information of 60 million customers were compromised because of their unsecured server.[47] In addition, in 2017, the phishing rate in SA was found to be the highest in world, and it was found that every one out of 785 e-mails was a phishing attack.[48]

In May 2018, ViewFines had a cyberbreach were the personal information of 943 000 SA drivers were compromised.[49] In June 2018, Liberty reported that their cybersecurity system was hacked and that the personal information of an unknown number of its clients was compromised.[50]

In April 2020, an OM of Taragin was targeted by hackers who made anti-Semitic remarks.[51] On 15 April 2020, an OM of the SA National Assembly, which was chaired by the Minister of Women, Youth and Persons with Disabilities, Maite Nkoana-Mashabane, was Zoombombed, when the hackers gained access to the online platform and shared explicit images.[52] In a follow-up, highly-publicised incident that occurred on 10 May 2020, an OM of the SA National Assembly was Zoombombed when hackers gained access to its online platform and again shared explicit images.[53] In May 2020, an OM of cars.co.za was Zoombombed by American hackers who shared explicit images.[54]

On 22 July 2021, Transnet fell victim to a DeathKitty ransomware cyberattack, which sabotaged its entire software system, when hackers encrypted it and made it

---

[46] Shapshak 'Cinema Chain Ster-Kinekor Hacked in SA's Biggest Data Breach' Data at Risk' in *Forbes* of 17 March 2017, *s.p.*, available online at <https://www.forbes.com/sites/tobyshapshak/2017/03/17/cinema-chain-ster-kinekor-hacked-in-south-africas-biggest-data-breach/?sh=5e84f3b95fa1>, last accessed on 19 June 2021.

[47] Fihlani 'Millions Caught in SA's 'Worst Data Breach' on *BBC News* of 20 October 2017, *s.p.*, available online at <https://www.bbc.com/news/world-africa-41696703>, last accessed on 8 July 2021.

[48] Staff Writer 'Internet Fraud and Phishing Costs SA R2.2 Billion' in *BusinessTech* of 14 September 2014, *s.p.*, available online at <https://businesstech.co.za/news/trending/68212/sa-internet-fraud-and-phishing-costs-r2-2-billion/>, last accessed on 8 July 2021.

[49] Nieselow 'Five Massive Data Breaches Affecting South Africans' in *Mail and Guardian* of 19 June 2018, *s.p.*, available online at <https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/>, last accessed on 19 June 2021.

[50] *Ibid.*

[51] Moshe 'Zoombombing Takes Anti-Semitic Twist' in the *SA Jewish Report* of 2 June 2020, *s.p.*, available online at <https://www.sajr.co.za/zoombombing-takes-on-an-anti-semitic-twist/>, last accessed on 11 June 2023.

[52] Shapshak 'SA's Parliamentarians Zoombombed with Porn Images' in *Forbes* of 11 May 2020, *s.p.*, available online at <https://www.forbes.com/sites/tobyshapshak/2020/05/11/south-africas-parliamentarians-zoombombed-with-porn-images/>, last accessed on 11 June 2023.

[53] *Ibid.*

[54] Knowler 'Zoombombing on its Way Out, Plus Tips on How to Ace Video Conferencing and Save Data' in *Times Live* of 18 June 2020, *s.p.*, available online at <https://www.timeslive.co.za/news/consumer-live/2020-06-18-zoombombing-on-its-way-out-plus-tips-on-how-to-ace-video-conferencing-and-save-data/>, last accessed on 11 June 2023.

inaccessible.[55] This forced the company to declare *force majeure* at its depots at Cape Town, Durban, Port Elizabeth and elsewhere and this caused backlogs and hampered exports and imports for months afterwards.[56] In August 2021, the SA credit bureau, Experian, suffered a cyberbreach, which exposed the PII of 24 million South Africans and more than 790 000 businesses.[57] In September 2021, the PII of a million clients were stolen after a ransomware attack on the SA debt recovery company, Debt-IN Consultants.[58] Most SA banks make use of Debt-IN Consultants' services.[59] In September 2021, the SA Department of Justice and Constitutional Development (DoJ & CD)'s website was hacked and ransomware was used to prevent officials from accessing the system, and this caused backlogs at all SA courts that carried on for months.[60] Afterwards it was realised that the DoJ & CD's cybersecurity software had expired in 2020 and the Information Regulator (IR) found that they did not properly secure their IT systems.[61]

In May 2022, a hacking syndicate called SpiderLog$, got hold of the personal information of President Cyril Ramaphosa, when they stole a database that contained personal information on bank loans.[62] SpiderLog$ said that they got this information from another group, N4ugtysecTU from Brazil, who launched a cyberattack on the credit bureau, TransUnion, earlier that year.[63] The personal information that they obtained included President Ramaphosa's home address, ID number and cellphone number.[64] TransUnion refuted the claim that additional personal information from the SA Department of Home Affairs was stolen from their databases, and claimed that the attackers had obtained it from another cyberattack.[65] SpiderLog$ also said that they were able to identify the private Internet Protocol (IP) addresses on the government's servers, which indicates that the proxy servers that the SA government use to hide IP addresses are inadequate and that the locations from where citizens and government

---

[55] Reuters 'SA's Transnet Restores Operations at Ports After Cyberattacks' in *Reuters* of 29 July 2021, *s.p.*, available online at <https://www.reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ>, last accessed on 12 June 2023.
[56] Shapshak 'Note to Transnet: Cyberattacks Only Works When There Are Vulnerabilities to Exploit' in the *Daily Maverick* of 4 August 2021, *s.p.*, available online at <https://www.dailymaverick.co.za/opinionista/2021-08-04-transnet-ports-closed-and-were-in-the-dark/>, last accessed on 12 June 2023.
[57] *Ibid.*
[58] Moyo 'Over 3.6 Million Records Exposed in Dis-Chem Cyberattack' in *ITWeb* of 11 May 2022, *s.p.*, available online at <https://www.itweb.co.za/content/PmxVE7KEABOqQY85>, last accessed on 18 January 2023.
[59] *Ibid.*
[60] Goba 'DoJ Found Guilty of Being Negligent in Its Actions to Prevent a Data Breach' in *Eyewitness News* of 10 May 2023, *s.p.*, available online at <https://ewn.co.za/2023/05/10/doj-found-guilty-of-being-negligent-in-its-actions-to-prevent-a-data-breach>, last accessed on 12 June 2023.
[61] Staff Writer 'Cyril Ramaphosa's Private Data Hacked' in *MyBroadband* of 29 May 2022, *s.p.*, available online at <https://mybroadband.co.za/news/security/446282-cyril-ramaphosas-private-data-hacked.html>, last accessed on 12 June 2023.
[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid.*
[65] *Ibid.*

officials access the Internet have been revealed.[66] Also in May 2022, more than 3,6 million records of personal information of the clients of Dis-Chem were exposed, following a cyberattack on a third-party service provider.[67] In 2022, IBM's Ponemon Institute's '*2022 Cost of Cyber Breach Study*' showed that a cyberbreach, on average, costs a SA company R49 million and that the average cost to retrieve a stolen or compromised record of personal information amounts to R2650.[68] It showed that, on average, it takes more or less 250 days for SA companies to contain the damage that was caused by a cyberbreach.[69] It also showed that the main causes of cyberbreaches in SA are the security immaturity of databases in Clouds, the misconfiguration of Clouds and stolen credentials and that financial institutions are the main targets for a cyberattack.[70]

The prevalence of these incidents compelled the cybersecurity company, Kaspersky, to issue a warning to SA companies in December 2022 on the prevalence of fake business correspondence from partners and fake links for OMs and their related documents.[71] Kaspersky explained that access to PII during an OM is gained by infecting users' devices with a data stealer.[72] The PII then gets stolen while users continue to work on their devices.[73] The malware then sends the stolen PII back to the cybercriminal's command-and-control (C&C) server, which then breaks it down in databases that contains different types of information that cybercriminals require, and then it is advertised on fora on the dark web and put up for sale.[74]

Between 15 and 18 March 2023, Nedbank fell victim to a cyberattack when cybercriminals tried to create false online profiles with valid SA identity numbers on its online platform, the Nedbank MoneyApp.[75] The attackers obtained more than 40 000 cellphone numbers of the bank's clients, which are connected to these ID numbers, through this attack.[76] As soon as the bank became aware of the incident, the enrolment

---

[66] Staff Writer 'Cyril Ramaphosa's Private Data Hacked' *op cit s.p.*
[67] Moyo 'Over 3.6 Million Records Exposed in Dis-Chem Cyberattack' *op cit s.p.*
[68] Ponemon Institute '*2022 Cost of Cyberbreach Study,*' *s.p.*, available online at <https://www.ibm.com/reports/data-breach>, last accessed on 13 October 2022.
[69] *Ibid.*
[70] *Ibid.*
[71] Smith 'From Fake Links to OMs to Drones: SA Companies Warned of Cyberattacks' in *News24* of 4 December 2022, *s.p.*, available online at <https://www.news24.com/fin24/companies/sa-businesses-warned-of-cyber-attacks-involving-fake-links-for-online-meetings-and-drones-20221204>, last accessed on 11 June 2023.
[72] *Ibid.*
[73] *Ibid.*
[74] *Ibid.*
[75] *S.n.* '41 000 Nedbank Clients' Cellphone Numbers Retrieved in Cyberattack' in *TimesLive* of 23 March 2023, s.p., available online at <https://www.businesslive.co.za/bd/national/2023-03-24-41000-nedbank-clients-cellphone-numbers-retrieved-in-cyberattack/>, last accessed on 12 June 2023.
[76] *Ibid.*

functionality on the MoneyApp channel was immediately disabled, thereby preventing the attackers to gain access to other online functions.[77]

Now that the SA POPI 4 of 2013 has come into effect on 1 July 2021, it can be expected that reported incidents will increase as boards are now legally mandated by section 22(1) to report cyberbreaches to the IR.[78]

4. OMs AS A VULNERABLE ASPECT OF A COMPANY'S OPERATIONS

This section will look at how the Act regulates company meetings and OMs and why OMs are a vulnerable aspect of a company's operations.

4.1. The Act's Regulation of Company Meetings and OMs

The Act states in section 61(7)(a) that SA public companies must conduct an annual general meeting (AGM) within eighteen months after a company was incorporated.[79] Thereafter, section 61(7)(b) requires that an AGM must be conducted once in a calendar year, and within fifteen months after the previous one.[80]

Section 61(10) requires every shareholders' meeting of a public company to be reasonably accessible within SA for online participation and subjects it to section 63(2), irrespective of whether the OM is conducted in SA or elsewhere.[81]

Section 62(3)(a) sets out a shareholders' meeting notice's requirements and states that it must be in written format, and must state the date, time and place where the meeting will be held.[82]

Section 63(2) however makes provision for instances where a shareholders' meeting is not held at a physical place.[83] Section 63(2) is the enabling provision that allows OMs and states that if a company's MOI does not prohibit an OM, it may conduct (a) a shareholders' meeting completely online; or that (b) participants may take part online in the physical shareholders' meeting, as long as the online communication allows everyone to communicate effectively and simultaneously with one another without an intermediary.[84]

---

[77] *S.n.* '41 000 Nedbank Clients' Cellphone Numbers Retrieved in Cyberattack' *op cit s.p.*

[78] SA POPI 4 of 2013, section 22(1); Privacy International '*The State of Privacy in SA,' s.p.*, available online at <https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa>, last accessed on 14 May 2021.

[79] The Act, section 61(7)(a).

[80] The Act, section 61(7)(b); See Chapter 2, section 5.1.

[81] The Act, sections 61(10); 63(2); See Chapter 2, section 5.1.

[82] The Act, section 62(3)(a); See Chapter 2, section 5.1.

[83] The Act, section 62(3).

[84] The Act, section 63(2)(a)-(b); See Chapter 2, section 5.1.

Section 63(3) regulates online participation and states that if a company makes provision for online participation, then (a) the notice must inform shareholders of the availability of online communication for remote participation, and must state the required access information; and explain that (b) the cost of using the online communication is a cost to be borne by the participant, unless the company decides something else.[85]

Section 63(4) regulates voting rights on a poll of hands and states that any participant who is present and who may vote, only has one vote, regardless of how many shares they own.[86] Section 63(5) further regulates voting rights and states that on a poll at any meeting, any participant may use all the voting rights of their shares.[87]

Since SA companies' OMs are conducted on an online platform and use online databases that contain the sensitive personal information and the PII of the shareholders/stakeholders, they are particularly prone to cyberattacks. There are two main reasons why a company's OM is so particularly vulnerable when compared to an ordinary face-to-face meeting, and both are attributed to the nature of the OM. The first reason is that the online platform, which the company uses to facilitate the meeting, could contain a potential weakspot whereby a cyberattacker could gain access to a company's IT system; and secondly, it is because the online platform uses online databases, which could be targeted by cyberattackers, since they contain the PII of the shareholders/stakeholders who participate in the OM.

4.2. Online Platform

An online platform makes use of a software programme to facilitate the OM and examples include Bluejeans, Google Meet, Microsoft Teams, Skype, Yahoo Video Conferences or Zoom, an app such as FaceTime, a conference call dial-in, live streaming or through a web browser, a custom-made online platform, such as the Johannesburg Stock Exchange (JSE)'s online platform, or a combination of these.

If such an online platform was not configured correctly, and if there is a software coding error, a weak spot in the firewall, or if it lags, or if it is not properly end-to-end encrypted due to the company's insufficient hardware or software, it creates a cybersecurity loophole where a cybercriminal can access the company's online platform and 'zoombomb' an OM. Once a cybercriminal finds that loophole, they can hack the online platform, gain access to the OM and 'Zoombomb' it and commit numerous types of cybercrimes with either the online platform itself, or its online databases, which contains the sensitive personal information and PII of the shareholders/stakeholders. Once that PII is obtained, cybercrimes, such as cyberuttering, cyberwarfare, hacking,

[85] The Act, section 63(3)(a)-(b); See Chapter 2, section 5.1.
[86] The Act, section 63(4); See Chapter 2, section 5.1.
[87] The Act, section 63(5); See Chapter 2, section 5.1.

identity theft, the misuse of websites and computer networks, phishing, ransomware and other forms of cybercrime could be committed.

4.3. Online Databases with Personally Identifiable Information (PII)

OMs work with very sensitive personal information of especially shareholders that contains details that go way beyond the ordinary personal information that is recorded in companies' shareholders' registers that the SA Companies Act 71 of 2008 (the Act), section 26(3) requires to be open for inspection.[88] Besides the usual personal information in the shareholder register that the Act, section 50(2)(b) prescribes for shareholders' meetings, such as the names of shareholders, their addresses and nature of shares they hold, OMs require much more detailed additional personal information of shareholders.[89]

OMs make use of much more sensitive personal information, called PII, which could include contact information (such as phone numbers, online and physical addresses), financial information (such as broker information, investment account numbers and tax numbers), official identification information (such as ID numbers, passport numbers, social security numbers (SSNs)), personal histories (such as birth dates, medical information on Covid statuts (of employees participating online from work), physical information (that is gender-related) or relationship information (such as information on employers and family trusts).[90] It could also include PII on algorithms, biometric information, IP addresses, locations, online communications and online voting records based on Blockchain technology and PII that was acquired for credit or anti-money laundering checks.[91] A Blockchain is a public ledger that records information across various computer systems, so that the information cannot be altered on just one computer system.[92]

In addition, in the event that a SA shareholder requires Internet access from a company's branch or agent office to attend an OM, a company will usually require such a shareholder to present their ID smartcard to identify themself, and by doing so, the company gains access to the microchip embedded in the card that contains additional

---

[88] SA Companies Act 71 of 2008 (The Act), section 26(3).
[89] The Act, section 50(2)(b); Delport *et al. Henochsberg on the Companies Act* 135.
[90] Johnson *op cit* 256.
[91] McCarrick '*FI Observer: Data Protection Law Implications for Directors and Officers of Real Estate Investment Trusts' (REITs),' s.p.*, available online at <https://www.willistowerswatson.com/en-AU/Insights/2019/07/fi-observer-data-protection-law-implications-for-directors-of-real-estate-investment-trusts>, last accessed on 13 May 2021.
[92] Synopsis '*Blockchain*,' *s.p.*, available online at <https://www.synopsys.com/glossary/what-is-blockchain.html>, last accessed on 23 January 2023.

PII that is stored on the SA Home Affairs National Identification System (HANIS), such as the fingerprints of the holder and their signature.[93]

Personal information of this nature is beyond the scope of access that a shareholder register requires, and in terms of SA POPI 4 of 2013, Part B, sensitive personal information can only be collected and processed in certain circumstances, such as when it is needed for compliance with a legal obligation.[94]

The fact that OMs use PII, make them one of the most vulnerable aspects of a company's operations, because all participants participate from their respective online locations by means of their own online security protocols, which are not necessarily all secure, up to standard or end-to-end encrypted, and once a cybercriminal can get access to such a device, they can get access to the online platform and its online databases.[95]

5. THE CAUSAL LINK BETWEEN OMs AND IMPROVED CORPORATE GOVERNANCE

No generally accepted definition for the concept of corporate governance exists.[96] A well-known definition for corporate governance was however provided by the United Kingdom (UK)'s Committee on the Financial Aspects of Corporate Governance's 'Final Report and Code of Best Practice of 1992' ('Cadbury Report') that explains that corporate governance aims to harmonise a company's economic and social goals as well as shareholders' goals with other stakeholders' goals in an attempt to unite the interests of the company, shareholders, stakeholders, its community and environment in the way in which a company is governed.[97] Hence, Keay summarises the concept and explains it as the system that directs and controls companies.[98]

This thesis starts from the premise that OMs are beneficial, as they facilitate shareholder engagement, which in turn helps to improve corporate governance and corporate social responsibility (CSR).[99] OMs have many advantages: they could possibly lessen the chances for internal corruption and fraud since they help companies to conduct their affairs with more transparency through improved oversight due to

---

[93] SA Department of Home Affairs '*Verify Identity Online,' s.p.*, available online at <https://www.gov.za/services/verify-identity-online>, last accessed on 8 July 2021.
[94] SA POPI 4 of 2013, Part B; Delport *et al. Henochsberg on the Companies Act op cit* 135.
[95] Brandenburg *et al*. 'Cybersecurity for a Remote Workforce' in *MIT Sloane Management Review* of 23 July 2020, *s.p.*
[96] Keay *Board Accountability on Corporate Governance* 15.
[97] UK Committee on the Financial Aspects of Corporate Governance '*Final Report and Code of Best Practice of 1992*' ('Cadbury Report') 'Introduction,' paragraph 2.5.
[98] *Ibid.*
[99] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *International Journal of Computer Theory and Engineering* 5(2) (April 2013) 284.

greater shareholder attendance and participation.[100] Improved oversight could possibly help to add value and a higher performance will likely lead to wealth creation.[101] If the company's interests are better taken into account by improved oversight, profit maximisation will likely occur.[102]

Since OMs facilitate contact with all other stakeholders who are part of the company, namely the community, consumers, creditors, employees, shareholders and the suppliers, they facilitate CSR through the participation of more role players.[103]

OMs also put pressure on the board to be more caring as more participation and inputs encourage the board to invest in the company's environment, social (community) and governance (ESG), and this helps to create a value-added circle of CSR that may benefit the company.[104]

Once the board can show that it has implemented a proper cybersecurity policy and system, it will help to make the company's operations more transparent, and it will also be easier for financial institutions to finance the company.[105]

OMs also have other advantages, such as saving time on travelling and saving the expenses on accommodation, subsistence, travelling and venue hire. The savings on travelling will also lead to less carbon emissions when a board, employees, shareholders and stakeholders do not all need to travel across the globe or a country to attend a meeting.

The phenomenon of OMs is important because the research of Ali *et al.*, Gao *et al*., Grzybkowski *et al.* and Lafarre *et al*., indicates a causal relationship between OMs and improved corporate governance due to increased shareholder attendance and participation.[106]

Ali *et al.* explains that the law that regulates shareholders' meetings plays an important part in corporate governance, but that it does not always get the attention that it deserves.[107] Since OMs offer a cheap and international means of communication, they offer a solution to resolve shareholder passivism by enhancing shareholders' rights to attend and participate at shareholders' meetings.[108] They argue that corporate

---

[100] Flores-Araoz 'CSR in SA: More Than a Nice Intention' in *Polity* of 12 September 2011, *s.p.*, available online at <https://www.polity.org.za/article/corporate-social-responsibility-in-south-africa-more-than-a-nice-intention-2011-09-12>, last accessed on 9 July 2021.

[101] *Ibid.*

[102] *Ibid*.

[103] Kondlo *The Importance of Corporate Governance in SA Family-Owned Companies* 21.

[104] *Ibid*.

[105] Claessens *et al. Corporate Governance & Development: An Update* 20.

[106] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *op cit* 284; Grzybkowski *et al.* '*Internet and Corporate Governance,*' 2, available online at <file:///C:/Users/Julian/Downloads/SSRN-id914520.pdf>, last accessed on 3 February 2022; Lafarre *et al.* '*Blockchain Technology for Corporate Governance and Shareholder Activism*,' European Corporate Governance Institute's Law Working Paper 390/2018, 1, available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135209>, last accessed on 3 February 2022.

[107] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *op cit* 284.

[108] *Ibid*.

governance can mainly be improved through the greater involvement of shareholders in shareholders' meetings.[109] They explain that when more shareholders attend and participate in corporate decision-making, it leads to more well-informed decisions, and also improves oversight by enhancing the 'checks and balances' system against the boards' power.[110] They make the important point that bad planning of OMs will obstruct any increase in shareholder attendance and participation, once OMs fall prey to IT glitches.[111] In addition, they say that since Globalisation has led to a change in the corporate society's structure, and since the owners of a company's shares has become more widespread from different countries, many shareholders find it too difficult to travel to attend ordinary meetings, but that OMs present a bridge to overcome this problem.[112]

Ali *et al.*'s research corresponds with the research of Gao *et al.* who found that shareholders' attendance and participation in ordinary shareholders' meetings are especially low with public companies due to their scattered shareholdership and the need for shareholders to travel to attend meetings in person.[113] Gao *et al.* researched empirically whether, when shareholders are allowed to attend OMs, OMs can enhance the participation in shareholders' meetings?[114] The results show that OMs can indeed help to increase the online attendance and participation of shareholders.[115] They find that this is especially the case when it costs too much for the shareholders to travel to attend an ordinary meeting and when the shareholders live too far to travel to attend.[116] They even found more positive share returns once companies started to switch to OMs.[117] In addition, they provide evidence that minority shareholders indeed voice their opinions at OMs.[118] Overall, their research found that OMs are a less expensive, but nevertheless an effective, manner to allow more shareholders a say in a company's affairs.[119]

In their research, Grzybkowski *et al.* explains that the development of effective and efficient Information Technology (IT) to bring shareholders closer to companies is an overlooked, but important factor that can help corporate governance reform.[120] Specifically, their research explores the role that the Internet can play to help improve oversight in corporate governance and find that it enables the proper functioning of scattered shareholdership.[121]

---

[109] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *op cit* 284.
[110] *Ibid*.
[111] *Ibid*.
[112] *Ibid*.
[113] Goa *et al. op cit* 1.
[114] Goa *et al. op cit* 18.
[115] *Ibid*.
[116] *Ibid*.
[117] *Ibid*.
[118] Goa *et al. op cit* 1; 18.
[119] Goa *et al. op cit* 18.
[120] Grzybkowski *et al. op cit* 2.
[121] *Ibid.*

Lafarre *et al.* again points out that Blockchain technology is also a means to enhance the relationship between the company and shareholders.[122] They found that it helps to lower expenses for both shareholders' and companies.[123] They also found that it helps to make decisions faster and also facilitates the involvement of shareholders.[124] It also eases the identification and verification of shareholders who vote and thereby facilitates the transparency of shareholders' meetings.[125] It also addresses many of the problems associated with chains of intermediaries and remote voting systems of normal proxy solicitors.[126] As a result, it shows that Blockchain technology can help to improve the participation of shareholders when it is properly integrated with OMs.[127]

Bebchuk looked at how power is distributed between boards and shareholders in public companies and went as far as saying that, shareholders must be given the power to intervene in corporate decision-making in an attempt to increase the say that they have in a company's affairs.[128] According to this way of thinking, it should be the shareholders and not the board who needs to decide whether OMs need to be held – and as such it would disempower stakeholders and their input in this regard. In a critique of Bebchuk, Mervis *et al.* writes that the time of the shareholder dominance theory has passed and that in this modern day era, boards need to be responsive to all shareholders and stakeholders and that a mediatory approach between these groupings should be followed.[129] In this regard, OMs are ideal, as they will help to dismantle the shareholder dominance theory and help corporate governance to move away from a board dominated approach at company meetings, and help to give shareholders a bigger voice, help to include more stakeholders and help company meetings to have a more mediatory approach to problems that face the company in its physical and online environment, and the way in which it interacts with its physical and online community.

The problem is however that all of these positive consequences that result from OMs that these researchers researched, could all be wiped out in a split-second once a cyberbreach ocurrs and a cybercriminal gains access to a company's online platform, 'zoombombs' an OM, and hijacks the online platform and compromises or steals its online databases. Not only will the company be faced with external investigations on the cause of the cyberbreach, but directors could also be held personally liable if shareholders/stakeholders can prove that the company's cybersecurity measures were inadequate for the cyberrisks that the company faced at that point in time.

---

[122] Lafarre *et al. op cit* 1.
[123] *Ibid.*
[124] *Ibid.*
[125] *Ibid.*
[126] *Ibid.*
[127] *Ibid.*
[128] Bebchuk 'The Case for Increasing Shareholder Power' in *Harvard Law Review* 118(2005) 833.
[129] Mervis *et al*. 'Bebchuk's 'The Case for Increasing Shareholder Power:' An Opposition' in *Harvard Law Review* 121(2007) 53.

Where these researchers looked at OMs as a means to enhance corporate governance and CSR, they have failed to look at the dangers that cybercrime present to companies' OMs. The potential of a cyberattack is an omnipresent reality and threat that affects an OM of any company, at any time.

In addition, they failed to recognise that directors may be held personally liable in the event that a company's cybersecurity was inadequate to thwart a cyberattack and the company's cyberassets, such as its online platform and its online databases were compromised, and if the OM was 'zoombombed' and hijacked.

In addition, they have also failed to acknowledge the role that the duty of care in relation to cybersecurity and the use of AI can play to help secure a company's cyberassets, such as its online platform and its online databases. So, in other words, where other researchers only looked at OMs as a tool to improve corporate governance and CSR, this thesis will explain that a more detailed treatment of the directors' duty of care in relation to cybersecurity and the use of AI will improve companies' cyberresilience and will especially help to make their OMs more cyberresilient.

Only once a company's cyberassets, such as its online platform and its online databases, are properly secured, can the real advantages of an OM be reaped, and in order to properly secure an OM, directors need to properly exercise their duty of care in relation to cybersecurity and use AI responsibly. If SA directors could be provided with more detailed treatment on the use of AI in order to help them exercise their duty of care in relation to cybersecurity more effectively, this thesis proposes that it will help make SA companies more cyberresilient.

6. THE FURTHER CHALLENGES OF OMs IN TERMS OF CYBERSECURITY

Although OMs have numerous advantages pertaining to the improvement of corporate governance and CSR of companies, they also have a dark side that can instantaneously eclipse all of their advantages. If OMs are not properly constituted and if their online platforms are not properly configured and if they are hacked; and if their online databases are not properly secured, and if the PII that they contain are compromised, the financial, legal and reputational consequences can ruin such a company overnight. These consequences will particularly be dire for such a company's directors, since they were the ones who had to properly exercise their duty of care in relation to cybersecurity and who had to oversee that the online platform was properly configured and end-to-end encrypted, and that the online databases were properly secured in Clouds that are properly configured. If it is found that the directors omitted to exercise their duty of care in relation to cybersecurity in this regard, or that they were negligent, the IR or court may hold the directors criminally liable, while the company or

the shareholders/stakeholders may hold them personally liable.[130] Since directors can incur liability when they do not exercise their duty of care in relation to cybersecurity properly, it is important that this thesis looks at lessons how SA directors could exercise their duty of care in relation to cybersecurity and the responsible use of AI to help make SA companies more cyberresilient so that it limits the possibility that SA directors could be held liable for not exercising their duty of care in relation to cybersecurity properly.

Unfortunately, OMs are faced with numerous challenges, which enhances the chances for cybercrime, and which means that directors are more exposed to liability when OMs are conducted, than with physical meetings.

6.1. OMs as High Risk Events for Cyberbreaches, Worsened by the Covid 19-Pandemic

Even though no academic research has yet been done on the way in which a more detailed treatment of the duty of care in relation to cybersecurity and the use of AI could help to fight cybercrime that is directed towards companies, and especially towards their OMs, Chigada *et al*. has researched the worrying state of cybersecurity and the protection of PII in SA during the Pandemic.[131] Since OMs process PII, it can be accepted against the background of Chigada *et al.*'s research that OMs are at risk in terms of cybersecurity and susceptible to cyberbreaches.[132]

According to the SA shareholder activist body, Just Share, OMs are high risk events in terms of not only cyberbreaches, but also in the way in which they conform to the Act's requirements.[133]

The Pandemic has proven to be a hotbed for cybercriminals who started to take advantage of the loopholes that arose from companies who had to very quickly restructure their operations with a home-based workforce.[134] Cyberrisks are becoming more sophisticated, more durable and more expensive, in terms of the expenses of remediation and associated random demands.[135] The reality is that no company or director is immune to the risks and consequences of a cyberattack – and they may become leading targets

---

[130] SA POPI 4 of 2013, section 40.

[131] Chigada *et al.* 'Cyberattacks and Threats During Covid-19' in *SA Journal of Information Management* 23(1)(2021), *s.p*.

[132] Astfalck *et al*. '*Cybersecurity and Adequate Data Protection Have Become Key Focus Areas for Company Boards Across the World,' s.p*., available online at <https://www.clydeco.com/en/insights/2021/04/directors-beware-of-obligations-and-liabilities-un>, last accessed on 14 May 2021; Chigada *et al. op cit s.p*.

[133] Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act,' s.p.*, available online at <https://justshare.org.za/media/news/sa-companies-virtual-agm-arrangements-risk-non-compliance-with-companies-act>, last accessed on 8 July 2021; Just Share '*Best Practices for SA Virtual AGMs,' s.p.*, available online at <https://justshare.org.za/wp-content/uploads/2020/05/Just-Share-Virtual-AGM-Guide.pdf>, last accessed on 8 July 2021.

[134] Brandenburg *et al. op cit s.p.*

[135] Astfalck *et al*. *op cit s.p*.

of legal action by shareholders and/or stakeholders after a cyberbreach when their privacy and/or personal information were compromised.[136]

The Pandemic and subsequent Lockdown regulations on self-isolation and work from home created the perfect loopholes for cybercriminals to exploit.[137] These regulations continue to change working environments and how people work and interact.[138] Employees who work from home usually do so with weaker cybersecurity measures and security protocols (that are not always end-to-end encrypted) on their home networks than at work.[139] Working from home also results in skeleton staff who must help to do the work of others and this also creates loopholes for cybercriminals.[140] Working from home also leads to more people than ever before who works on companies' networks with remote access.[141]

This creates the ideal circumstances for cybercriminals and one can only expect that more companies will be subject to increased cyberattacks ranging from cyberwarfare, doxware, espionage, hacking, phishing, ransomware, spyware, theft of personal information, Trojan horses, virus implants and worms, and that this may in future be directed more and more towards OMs in order to get hold of the PII that are contained in the online databases.[142]

Cyberbreaches are also occurring more frequently and the Institute of Directors of SA (IoDSA), who is the custodian of the King Code, warns directors that they are inevitable and can happen at any time.[143]

6.2. The Haphazard Regulation of OMs

At the moment, the cybersecurity aspects of OMs are regulated in a haphazard manner and no guidance on the use of AI exist that can help directors on how they need to exercise their duty of care in relation to cybersecurity so that it can help to make the company more cyberresilient.[144]

---

[136] Astfalck *et al. op cit s.p.*
[137] Brandenburg *et al. op cit s.p.*
[138] *Ibid.*
[139] *Ibid.*
[140] *Ibid.*
[141] *Ibid.*
[142] Bowmans '*Covid-19: Impact on Businesses and Investments in SA,' s.p.*, available online at <https://www.bowmanslaw.com/insights/mergers-and-acquisitions/covid-19-impact-on-businesses-and-investments-in-south-africa/#Dataprotection>, last accessed on 15 May 2021.
[143] Institute of Directors of SA (IoDSA) '*Governing Body's Role in Cyber Resilience,*' 3, available online at <https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/05E93ACB-10BE-4507-9601-307A66F34BD8/CGN_Position_paper_13_Cyber_Resilience_April_2018.pdf>, last accessed on 15 May 2021.
[144] Peterson '*Sarbanes-Oxley: Ten Years After - Are We Having Fun Yet?,' s.p., available online at* <https://finance.toolbox.com/blogs/jimpeterson/sarbanes-oxley-ten-years-after-are-we-having-fun-yet-080712>, last accessed on 9 July 2021.

Since many companies assembled their own online platforms, which are regulated by their own rules, there is no consistency across the spectrum and examples will be shown that were not always the best-suited to SA legislation.[145]

The JSE adopted an online platform so quickly, that there was no time to include guidance on the use of AI, which could help directors with how they need to exercise their duty of care in relation to cybersecurity in the King Code. As a result, the precise differentiation between important AI concepts, such as 'Consultative AI,' 'Blockchain encrypted ledger,' 'Data Analysis,' 'Self-Aware AI,' 'Supportive AI' and other terms, are open to interpretation.[146]

OMs also need to be overseen and guided and this requires financial and human resources, which are free of corruption.[147] Just like other emerging economies, SA has resource constraints and challenges when it comes to the independence of regulators.[148]

The enforcement of corporate legal duties in SA is also hampered by a lack of specialised divisions in the high courts.[149] In SA, the High Court has fourteen divisions, situated in nine provinces.[150] Under these divisions there are specialised courts, such as the Commercial Court, Divorce Court, Equity Court, Income Tax Court, Labour Court and the Land Claims Court.[151] Since the King Committee's '*Report on Corporate Governance I*' (King Report I) was accepted in 1994, corporate governance in SA had to be enforced without a dedicated sub-division on corporate governance matters in the Commercial Court division of the High Court.[152]

6.3. A Lack of Guidance for SA Directors on Cybersecurity-Related AI

Based on case studies of cyberbreaches, which were caused by directors' ineffective oversight on cybersecurity, Lunn finds in his research that board oversight on

---

[145] Moyo 'Virtual AGMs May Infringe SA Companies' Act' in *ITWeb* of 13 May 2020, *s.p.*, available online at <https://www.itweb.co.za/content/KPNG878K2brv4mwD>, last accessed on 8 July 2021; Organisation for Economic Cooperation and Development (OECD) '*Corporate Governance in Asia: Progress and Challenges,*' 11, available online at <http://www.oecd.org/daf/ca/corporategovernanceprinciples/corporategovernanceinasia-progressandchallenges.htm>, last accessed on 18 May 2019; See Chapter 2, section 2.1.

[146] Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p.*; OECD '*Corporate Governance in Asia: Progress and Challenges*' *op cit* 11.

[147] *Ibid*.

[148] Gillwald '*Review of Chapter 9 Institutions,' s.p.*, available online at <https://static.pmg.org.za/docs/2007/070612gillwald2.htm>, last accessed on 30 May 2021.

[149] Chakanika *Corporate Governance in SA: Progress and Challenges*, LLM Thesis submitted at the University of Cape Town, 2013, 53; OECD '*Corporate Governance in Asia: Progress and Challenges*' 12.

[150] SA Department of Justice and Constitutional Development (SA DoJ & CD) '*Courts in SA,' s.p.*, available online at <http://www.justice.gov.za/about/sa-courts.html>, last accessed on 18 May 2019.

[151] *Ibid.*

[152] Chakanika *op cit* 53.

cybersecurity has not always been adequate.[153] He attributed this to what he calls, directors' "IT confidence gap," and indicated that up until recently, many directors who are in the age range of 60 to 65 have spent the most of their working careers in an era before the Internet was widely used in commerce.[154] This finding provides a background to the findings of the US National Association of Corporate Directors (NACD) (who is the largest representative body of US directors) in their annual survey, '*Trends and Priorities of the American Boardroom 2020 – 2021*,' which found that 50 percent of US directors acknowledged that they do not properly oversee cybersecurity and that there are gaps in their oversight on cybersecurity, and that 40 percent reported that their boards do not spend enough time on cybersecurity matters.[155] 49 Percent of directors ranked their cybersecurity concerns among their top five concerns for their companies and 70 percent of directors viewed cybersecurity as a strategic risk enterprise on which they will need to focus more.[156] Alarmingly, the NACD's '*Public Companies' Governance Survey 2019 - 2020*' found that 61 percent of directors said that they would cut down on cybersecurity to rather focus on the other goals of their company.[157] It also found that less than one percent of the directors of Fortune 500 companies have ever been a chief information officer (CIO) and this shows that there is not always proper representation of persons with IT backgrounds to talk about cybersecurity-related matters within the boardrooms of the world's largest companies.[158]

Based on his research, Lunn explains that although directors may know that cyberbreaches occur regularly, they will still find it difficult to oversee cybersecurity, since it is such an extremely difficult subject to grasp, unless one is an IT expert or has an IT background.[159] He says that difficulty does however not mean that proper oversight is not required and draws a comparison with financial controls, which were not universally understood by directors before the Enron scandal occurred in 2001 (and before the US Sarbanes Oxley (SOX) Act of 2002 was promulgated afterwards to tighten up oversight on financial controls), and says that an improper understanding of financial controls did not mean that proper oversight on financial matters was not required, but rather that the proper oversight on financial matters lacked in the early 2000's.[160]

---

[153] Lunn 'Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine' in *Journal of Law and Cyber Warfare* (2014) 1.

[154] US National Association of Corporate Directors (NACD) '*NACD Trends and Priorities of the American Boardroom 2020 – 2021*,' 15 – 20, available online at <https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71668>, last accessed on 5 October 2022.

[155] *Ibid.*

[156] *Ibid.*

[157] *Ibid.*

[158] US NACD '*Public Companies' Governance Survey 2019 – 2020*,' *s.p.*, available online at <https://www.nacdonline.org/analytics/survey.cfm?ItemNumber=66753>, last accessed on 5 October 2022.

[159] Lunn *op cit* 4 - 6.

[160] *Ibid*.

In the SA context, it is a particular problem that neither the SA Cybercrimes Act 19 of 2020, nor the King Code on Corporate Governance prescribes the use of AI as a tool for directors to use in the fight against cybercrime. This thesis consequently submits that the SA Cybercrimes Act 19 of 2020 and the King Code should be updated to include the use of AI, since it is an important tool for directors in the fight against cybercrime.

SA directors need to anticipate that new cyberrisks and cybersecurity measures will continue to pressure the courts to require directors to oversee cybersecurity with an increased duty of care in relation to cybersecurity and the use of AI, which will in turn lead to increased director liability.

6.4. Companies' and Directors' Exposure to Liability for the Improper Exercise of their Duty of Care in Relation to Cybersecurity and the Use of AI

Directors can also be held both criminally and personally liable for cyberbreaches when cyberassets are lost and when shareholders/stakeholders' privacy and/or personal information is compromised.[161]

Although directors owe their duty of care to the company, and not to the shareholders, boards need to protect the OM and the company's cyberassets, such as its online platform and its online databases, against cyberbreaches.[162] This duty of care in relation to cybersecurity stems from the Act, section 76(3)(c), which needs to be read together with King Report IV, principle 12, on IT governance.[163] Since the responsibility to implement and oversee an effective cybersecurity system, which will protect the company and its cyberassets, is part of risk management, directors need to exercise due care in relation to cybersecurity and the use of AI in this regard.[164]

Although the duty of care is owed to the company, and not the shareholders, boards need to ensure that the company complies with their obligations to protect the PII of shareholders and stakeholders, as required by the SA POPI Act 4 of 2013, otherwise they may be held directly accountable for the violation of their privacy and/or personal information.[165]

As a result, the board needs to proactively manage cybersecurity and ensure that the company's cyberassets are cyberresilient and that they are able to thwart any cyberrisks.[166] Although it is very difficult and almost impossible for any director who

---

[161] Financial Intermediaries Association (FIA) of Southern Africa '*What is a Directors' Liability Following a Cyber Breach?,' s.p.*, available online at <https://www.fia.org.za/blog/what-is-a-directors-liability-following-a-cyber-breach/#:~:text=Right%20to%20privacy%3A%20Directors%20and,3%20of%202013%20(POPI)>, last accessed on 27 April 2022.

[162] The Act, section 76(3)(c); IoDSA 'King Report IV' *op cit* principle 12.

[163] *Ibid.*

[164] *Ibid.*

[165] SA POPI 4 of 2013,

[166] FIA *op cit s.p.*

does not have IT training to stray abreast with cyberrisks, a statement or claim that such a director has an insufficient understanding of cyberrisks will not be a reasonable defence during litigation after a cyberbreach.[167]

Liability for cyberbreaches attaches to directors in various ways and SA directors could be held liable for cyberbreaches on various legal bases, as explained below.[168]

Shareholders can hold directors liable when their constitutional right to privacy is breached in terms of the SA Constitution of 1996 (SA Constitution), section 14.[169]

The Act enacted the common law and codified directors' duties.[170] The Act, section 76 regulates the standard with which directors need to exercise their duty of care and not only codified their common law duty of care, but also increased it by requiring them to act honestly, in good faith and in a way that they reasonably deem to be in the company's best interests.[171] Section 76(3) requires a director to act (a) in good faith and with a proper purpose; (b) in the company's best interests; (c) and with the degree of care, skill and diligence that can reasonably be expected from someone who performs the same functions and who has similar experience and skills.[172]

There is also a legislative derivative action in the Act, section 165, which allows anyone to institute an action on behalf of a company in an attempt to protect the company's interests.[173] This means that if a director breaches their duty of care in relation to cybersecurity and the company refuses to hold the directors liable for that breach, then a shareholder/stakeholder may, subject to compliance with the Act's requirements, institute a derivative action on behalf of a company.[174] If the action succeeds, any relief obtained will go to the company, which may indirectly benefit its shareholders and/or stakeholders.

The SA POPI 4 of 2013 determines that the IR may criminally prosecute a responsible party, such as the director, who did not properly oversee the management of personal information.[175]

It is also possible that regulatory action may be taken against directors. Although it depends on the regulatory framework and industry of an affected company, interested and affected parties can lay complaints at the SA Companies and Intellectual Property

---

[167] Sutherland 'What is a Director's Liability Following a Cyber Breach?' in *ITWeb* of 14 June 2018, *s.p.*, available online at <https://www.itweb.co.za/content/nWJadvb8ARmMbjO1>, last accessed on 27 April 2022.
[168] See Chapter 5, section 5.4.
[169] SA Constitution, section 14.
[170] The Act, section 76.
[171] *Ibid.*
[172] The Act, section 76(3)(a)-(c)
[173] The Act, section 165; Blackman *et al. op cit* 9-178.
[174] Blackman *et al. op cit* 9-178; Hayath '*Delving Deeper into the Territory of Derivative Actions,' s.p.*, available online at <https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/corporate/corporate-and-commercial-alert-7-october-delving-deeper-into-the-territory-of-derivative-actions-.html#:~:text=A%20derivative%20action%20is%20an,action%20to%20redress%20such%20wrong>, last accessed on 3 February 2022.
[175] SA POPI 4 of 2013, section 40.

Commission (CIPC) who will then investigate and take action against a company or its directors.[176]

The King Committee's '*Reports on Corporate Governance I- IV*,' on which IoDSA owns the copyright, are not enforced by means of legislation, but the courts will take their recommendations into account.[177] Voluntary corporate governance guidelines, such as King Report IV, only recommend best practices on corporate governance, but they do influence and affect what practices boards should look at and implement and how the courts will evaluate such conduct.[178] In this regard, King Report IV explains that if the recommendations on good corporate governance are more regularly used by directors in practice, the court will be more likely to consider those recommendations, since it sets a standard on the nature of care that is required on a certain aspect pertaining to corporate governance.[179] Consequently, the recommendations of voluntary corporate governance guidelines could be used in case law and could in such a way become part of the common law over time.[180] As a result, directors could then be held liable when they do not comply with an established corporate governance practice, even if such practice is not codified.[181]

In addition, the JSE '*Listing Requirements*' ensures the further enforcement of good corporate governance practices.[182]

7. THE USE OF AI TO HELP PROTECT A COMPANY'S CYBERASSETS AND ITS OMs

---

[176] SA Companies and Intellectual Property Commission (CIPC) '*Home Page*,' *s.p.*, available online at <http://www.cipc.co.za/za/>, last accessed on 27 April 2022.

[177] IoDSA '*King I: Report on Corporate Governance for SA of 1994*' (*'King Report I'*), *s.p.*, available online at <https://www.saica.co.za/Technical/LegalandGovernance/King/tabid/2938/language/en-ZA/Default.aspx>, last accessed on 27 April 2018; IoDSA '*King II: Report on Corporate Governance for SA of 2002*' ('*King Report II'*), *s.p.*, available online at <http://library.ufs.ac.za/dl/userfiles/documents/Information_Resources/KingII%20Final%20doc.pdf>, last accessed on 27 April 2018; IoDSA '*King III: Report on Corporate Governance for SA of 2009'* (*'King Report III'*), *s.p.*, available online at <https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iii/King_Report_on_Governance_fo.pdf>, last accessed on 27 April 2019; IoDSA '*King IV: Report on Corporate Governance for SA of 2016'* ('*King Report IV*'), *s.p.*, available online at <http://www.iodsa.co.za/?page=about_main>, last accessed on 27 April 2018; Visser '*The Application and Enforcement of King IV,' s.p.*, available online at <https://www.adams.africa/wp-content/uploads/2020/04/King-IV_APPLICATION_ENFORCEMENT.pdf>, last accessed on 27 April 2022; See Chapter 3, section 2.6.2.

[178] IoDSA '*King Report IV' op cit* 35.

[179] *Ibid*.

[180] *Ibid.*

[181] *Ibid.*

[182] JSE '*Listing Requirements,' s.p.*, available online at <https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/JSE%20Listings%20Requirements.pdf>, last accessed on 21 May 2019.

AI is a powerful tool that companies and their directors can use in the fight against cybercrime and to help make a company more cyberresilient and to help protect the company's cyberassets, such as its online platform and its online databases. AI could be used to not only detect, but also to prevent and resist cyberattacks on a company's cyberassets, and to secure them.

AI is now being used by some SA companies to not only help facilitate their functions, but also to secure such functions, which includes OMs.[183] The general types of AI that are used, include Consultative AI, Supportive AI and Self-Aware AI, but there are various sub-types of AI, such as Blockchain technology, Data Analysis and Machine Learning, which could all use Analytic AI, Functional AI, Graphic AI, Interactive AI and Text AI to a greater or lesser extent.[184] Other examples of AI include automation, language processing, robotics and self-execution functions, which could include the automatic counting of votes at an OM.[185] The key components of AI include advanced data analysis, deep learning, fast Internet speed, machine learning and neural networks, which can process data in a similar way as the human brain.[186]

It is important to have an understanding of the unique attributes of the most important types of AI, in order to understand how they can be used to help combat cybercrime that affects OMs.

Consultative AI uses unique algorithms and machine learning tools so that companies can create AI-driven solutions.[187] The algorithms of Consultative AI is in other words used to improve company operations and could be used to help make proposals and give advice on how to best encrypt an online platform with security codes that can prevent unauthorised access.[188]

Supportive AI uses machine learning to generate algorithms automatically.[189] Such an algorithm tool allows the developer to explain what the algorithm needs to do, and then it starts to generate the algorithm automatically.[190] Over time, the algorithm

---

[183] Staff Writer 'How AI Is Being Used in SA' in *BusinessTech* of 10 June 2019, *s.p.*, available online at <https://businesstech.co.za/news/enterprise/322505/how-ai-is-being-used-in-south-africa/#:~:text=Nearly%20half%20(46%25)%20of,Process%20Automation%20and%20Advanced%20Analytics>, last accessed on 13 January 2023.

[184] Sarker *op cit* 1.

[185] *Ibid*.

[186] *Ibid.*

[187] StarTechUp '*AI Consulting: Everything You Need to Know*,' *s.p.*, available online at <https://www.startechup.com/blog/ai-consulting-everything-you-need-to-know/#:~:text=AI%20consulting%20is%20the%20practice,intelligence%20to%20improve%20company%20operations.>, last accessed on 24 January 2023.

[188] *Ibid.*

[189] Tozzi 'What is AI-Assisted Coding and Should You Use It?' in *ITPro Today* of 16 December 2022, *s.p.*, available online at <https://www.itprotoday.com/development-techniques-and-management/what-ai-assisted-coding-and-should-you-use-it>, last accessed on 24 January 2023.

[190] *Ibid.*

can learn how to make the online platform more cyberresilient to new cyberthreats that emerge.[191]

Self-Aware AI uses an algorithm that acts independently from humans, and which cannot be directly overseen by humans since it is self-aware, for example the algorithm that is used by self-driving cars.[192] In this regard, the AI algorithm can be programmed to tell the online platform how to learn to operate on its own and to withstand any interference and oversight, even from the company's IT officials or the directors themselves.[193]

Machine Learning uses an AI algorithm that replicates the way in which humans learn, and which, through its own continuous learning, improve its own accuracy over time.[194] This type of AI in other words leverage data to improve its own performance when it does the tasks that it is given, such as the continuous improvement of the end-to-end encryption of the communications on an online platform.[195]

Since Blockchain uses a public ledger that records information across various computer systems, information that is altered on one computer system, is automatically altered on various computer systems due to the decentralised nature of the public ledger that helps to store AI.[196] This means that even if a cyberbreach on an ordinary online platform does occur, the PII of shareholders/stakeholders that was saved on Blockchain could still be retrieved, because it is not stored on just one ledger, but in a chain of ledgers.

A key component of AI is the need for fast Internet connectivity.[197] The IT Revolution recently accelerated in SA with the introduction of the fifth generation (5G) cellular network technology that follows on the 2G, 3G and 4G networks.[198] It performs faster and connects more efficient than the previous networks, and can reach speeds of up to 20 Gbps.[199] It also has a higher capacity than previous networks and can accommodate more devices on a single network.[200] This means that companies will be able to connect more devices on the online platform, without a drop in performance.[201]

---

[191] Tozzi *op cit s.p*.
[192] Alechina 'Autonomous Intelligence Systems' in the *Human-Centered AI Interest Group* site of Utrecht University, *s.p.*, available online at <https://www.uu.nl/en/research/human-centered-artificial-intelligence/special-interest-groups/autonomous-intelligent-systems>, last accessed on 24 January 2023.
[193] *Ibid.*
[194] IBM '*Machine Learning*,' *s.p.*, available online at <https://www.ibm.com/za-en/cloud/learn/machine-learning>, last accessed on 24 January 2023.
[195] *Ibid.*
[196] Synopsis *op cit s.p.*
[197] Sarker *op cit* 1.
[198] Vermeulen 'This Article Was Written by an AI: What is 5G and How Will it Benefit SA' in *MyBroadband* of 3 December 2022, *s.p.*, available online at <https://mybroadband.co.za/news/software/472475-this-article-was-written-by-an-artificial-intelligence.html>, last accessed on 6 January 2023.
[199] *Ibid.*
[200] *Ibid.*
[201] *Ibid.*

The introduction of 5G in SA is expected to bring a range of benefits to companies' cybersecurity measures, especially at their OMs.[202] It will allow for much faster downloading and uploading speeds than previous networks, and will allow for faster streaming.[203] This will be especially beneficial for OMs, which rely on fast internet speeds to transfer data and support the connections of remote participants.[204] It will be more reliable than previous networks, with lower latency and reduced network congestion.[205] This means that participants at OMs will experience less buffering, fewer dropped calls and slower connection speeds, even during peak times.[206] It will also have a higher capacity and allow for more connected devices to be supported on a single network.[207] This means that the company will be able to connect more devices on an online platform, without experiencing a drop in the quality of the OM. It will also provide the high-speed connectivity that other technologies beside, AI, requires, such as the Internet of Things (IoT), self-distribution of information and virtual reality.[208] This will open up new opportunities for innovation and growth of SA companies, and especially their OMs.[209]

In addition, 5G helps to facilitate and support the use of the various AI components.[210] This is possible, because 5G uses ultrabroadband Internet access.[211] As a result, AI and 5G are now used by some companies to help perform their cybersecurity functions, which support the cyberresilience of the online platform, and the way in which OMs is conducted.[212] The combination of AI and 5G may in other words be used to resist cyberbreaches at companies, especially at their OMs.[213]

When used with 5G, AI may also be used to act in response to certain functions of companies when they hold their OMs in order to resist cybercrimes and to enhance cybersecurity.[214] In this regard, AI could also be used to search for cybersecurity data, interpret that knowledge, and to solve cybersecurity problems, while Blockchain technology could be used to facilitate online communication and voting during OMs.[215]

---

[202] Vermeulen *op cit s.p.*
[203] *Ibid.*
[204] *Ibid.*
[205] *Ibid.*
[206] *Ibid.*
[207] *Ibid.*
[208] *Ibid.*
[209] *Ibid.*
[210] Drenik 'Cybercrime is Evolving: AI Can Help Improve Consumer Safety Online,' in *Forbes* of 17 May 2022, *s.p.*, available online at <https://www.forbes.com/sites/garydrenik/2022/05/17/cybercrime-is-evolving-artificial-intelligence-can-help-improve-consumer-safety-online/?sh=195648f615d0>, last accessed on 6 January 2023.
[211] *Ibid.*
[212] Malinga 'Telkom's 5G Network Goes Live in Various Parts of SA' in *ITWeb* of 27 January 2022, *s.p.*, available online at <https://www.itweb.co.za/content/WnxpEv4YYxy7V8XL>, last accessed on 6 January 2023.
[213] Drenik *op cit s.p*.
[214] Adi *et al.* 'Harnassing AI Capabilities to Improve Cybersecrity' in *Journal of the Institute of Electrical and Electronic Engineers* 8(2020) 23817 – 23818.
[215] *Ibid.*

Contrariwise, AI could also be used by cybercriminals to instigate cyberattacks.[216] To further worsen the problem, the high speeds of 5G will help to facilitate the speed with which cybercriminals can commit cybercrime.[217]

It is against this background that this thesis also needs to determine the adequacy of the legislative and corporate governance measures – or the lack thereof - in SA to determine how the SA cybersecurity regime assists directors to help keep their companies cyberresilient. This is required since the Fourth Industrial Revolution has led to the largescale use of new technology such as AI, and the SA legislature and the King Committee should respectively ensure that legislation and corporate governance guidance stay abreast with these developments and cyberrisks.[218]

This thesis submits that a more detailed treatment of the directors' duty of care in relation to cybersecurity and the use of AI can help to make SA companies more cyberresilient. Therefore, the SA Cybercrimes Act 19 of 2020 should be updated to prohibit the use of AI to commit cybercrime, and the King Code should be updated to encourage directors to use AI responsibly to help fight cybercrime in SA.[219] In this regard, an aspect of AI, such as pattern recognition will especially help to prevent cybercrime that is directed towards SA companies, and especially their OMs, since it can help to detect patterns of cyberattacks.[220] Since the SA Cybercrimes Act 19 of 2020 does not prohibit the use of AI to commit cybercrime, and since the King Code does not encourage directors to use AI to enhance cybersecurity, the SA legislature and the King Committee should seriously start to look at the way in which AI is used and regulated not only to commit cybercrime, but also to fight cybercrime, in SA.[221] As can be witnessed with the continuous occurrence of cyberattacks in SA, the current legislative and corporate governance frameworks and the use of ordinary firewalls and anti-virus software by companies is not enough to deter and thwart cyberattacks.[222] If the King Code could start to encourage directors to use AI, such as Data Analysis, it could help to prevent cybercrime and thereby help to improve the state of cybersecurity in SA.[223]

As a result, this thesis submits that the SA legislature should update the SA Cybercrimes Act 19 of 2020 and that the King Commission should update the King Code to regulate the use of AI to resist cybercrimes towards SA companies and their OMs.[224]

---

[216] Drenik *op cit s.p*.
[217] Von Solms in 'Kubermisdaad Gaan Groei' in *Die Burger* of 2 November 2022, 14.
[218] Adi *et al. op cit* 23819 – 23820.
[219] SA Cybercrimes Act 19 of 2020; SA ECTA 25 of 2002.
[220] Adi *et al. op cit* 23817 – 23818.
[221] SA Cybercrimes Act 19 of 2020; IoDSA '*King Reports I - IV' op cit s.p*.
[222] See Chapter 1, section 3.2.
[223] Adi *et al. op cit* 23817 – 23818.
[224] SA Cybercrimes Act 19 of 2020; IoDSA '*King Reports I - IV' op cit s.p*.

8. THE ROLE OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY TO HELP MAKE SA COMPANIES MORE CYBERRESILIENT

In Company Law, the duty of care is the moral or legal obligation of directors to ensure the safety and well-being of others.[225] Company law places a duty on a director to take a specific degree of care when they exercise their role – and this duty applies, among other things to the care that they take when they make a decision or when they oversee management, and to gain insight into the company's internal workings and their external consequences – in order to make effective decisions, or to pro-actively identify red flags that the company face.[226] Although Kershaw also refers to the duty of care as the quality of a business decision, this standard requires directors to exercise their duty of care honestly, in good faith and in the interests of the company.[227]

Originally, directors' duty of care was regulated by the common law.[228] Today, the approach to the duty of care in SA, the US and the UK clearly indicates different corporate legal philosophies.[229] In a US state such as Delaware, the courts apply a gross negligence standard to the decision-making process and a good faith standard to the oversight of care, while in the UK and SA, company law requires a more demanding standard of reasonable care.[230]

Directors' duty of care is stands apart from their fiduciary relationship towards the company, which is created when they agree to perform a representative function on behalf of the company, to act in the best interests of the company, and when they are empowered with the legal authority to do so.[231]

The Act enacted the common law position and partially codified directors' duties.[232] The Act, section 76 regulates the standard with which directors need to exercise their duties, and this section not only codified the common law duty of care, but also increased it by requiring directors to act honestly, in good faith and in a way that they reasonably deem to be in the company's best interests.[233] Section 76(3) specifically regulates the duty of care and states that it is subject to subsection 76(4) (which sets out the Business Judgment Rule (BJR); and subsection 76(5), which allows

---

[225] Deloitte '*Duty of Care,*' 3, available online at <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-customer-breach-support-duty-of-care-white-paper.pdf>, last accessed on 19 June 2022.
[226] Kershaw *The Foundations of Anglo-American Fiduciary Law* 137.
[227] Ibid.
[228] Delport *Henochsberg on the Companies Act et al. op cit* 288.
[229] Ibid.
[230] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 137; See Chapter 3, section 4.4.2.2.
[231] Kershaw 'Corporate Law's Fiduciary Personas' in *Law Quarterly Review* (October 2019) 1.
[232] The Act, section 76.
[233] *Ibid.*

a director to rely on the advice of an employee.[234] Section 76(3) then goes on to explain that a director must exercise their powers and perform their functions (a) in good faith and for a proper purpose; (b) in the best interests of the company; and (c) with the degree of care, skill and diligence that may reasonably be expected of someone (i) who carries out the same functions; and (ii) who has the general knowledge, skill and experience of that director.[235]

In short, the duty of care in relation to cybersecurity and the use of AI thus requires a director to act (a) in good faith and with a proper purpose; (b) in the company's best interests; (c) and with the degree of care, skill and diligence that can reasonably be expected from someone who also exercises oversight on cybersecurity-related aspects and who has similar experience and skills as the relevant director.[236]

This in other words means that directors have a duty to ensure that the company's assets, such as its online platform and its online databases, which contain the personal information of shareholders/stakeholders that was entrusted to the company, must not be compromised by a cyberbreach, as well as its OMs, must all be properly protected by a cyberresilient cybersecurity system.

Although directors owe their duty of care in terms of cybersecurity to the company and not to the shareholders, a proper application of the directors' duty of care in relation cybersecurity will indirectly benefit shareholders as it will help to secure online platforms and their online databases.[237] Properly secured OMs will therefore enable OMs to occur safely, while shareholders and stakeholders exercise their rights to attend and participate.[238] Such OMs will secure the input from shareholders, and also help to improve oversight by enhancing the 'checks and balances' system against the boards' power.[239] They will also help to make it more convenient for many shareholders and stakeholders to attend meetings, and not cause them inconvenience in the aftermath of a cyberbreach when their PII is spilled.[240] They will also help to save company resources, because otherwise the company will have a lot of expenses to retrieve stolen PII.[241] In addition, they will help to enhance the transparency of corporate governance and will help to enable the proper functioning of widespread, international shareholdership.[242] Lastly, they will help companies and shareholders to reach decisions faster, and help shareholders and stakeholders to participate more effectively.[243]

---

[234] The Act, sections 76(3); 76(4).
[235] The Act, section 76(3).
[236] The Act, section 76(3)(a)-(c)
[237] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *op cit* 284.
[238] *Ibid*.
[239] *Ibid*.
[240] *Ibid*.
[241] Goa *et al. op cit* 18.
[242] Grzybkowski *et al. op cit* 2.
[243] Blackman *et al. Commentary on the Companies Act* 8-328, note 15; Lafarre *et al. op cit* 1.

AI could be used to resist cyberattacks on a company's cyberassets, such as its online platform and its online databases.[244] Contrariwise, AI could also be used by cybercriminals to instigate cyberattacks.[245] It is therefore of utmost importance that SA directors start to use AI, because otherwise cybercriminals will always have the upper hand in the fight against cybercrime, since cybercriminals already use it to commit cybercrime, while the SA Cybercrimes Act 19 of 2020 does not prohibit them from doing it.[246]

9. RESEARCH OBJECTIVE

Cybercrime, the directors' duty of care in relation to cybersecurity, OMs and the protection of personal information of shareholders and/or stakeholders are all regulated in SA by a regime of different legislation.[247]

To make this situation even more difficult, there is no prohibition in the SA Cybercrimes Act 19 of 2020 on the use of AI to commit cybercrime, nor does the King Code encourage directors to use AI when they exercise their duty of care in relation to cybersecurity.

Due to this lack of guidance on how directors need to responsibly use AI when they exercise their duty of care in relation to cybersecurity, it is difficult for them to exercise due care on the use of AI in their company's cybersecurity policy and system before a cyberbreach occurs. It is only *ex post* after a cyberbreach has occurred, when the court will determine whether directors exercised due care in relation to cybersecurity, without providing *ex ante* guidance to directors on how they need to exercise due care in relation to cybersecurity and the use of AI. This lack of guidance and cross-reference between the different legal sources on what constitutes due care in relation to cybersecurity and the use of AI, consequently leaves companies susceptible to cyberbreaches and directors susceptible to be held personally liable for a breach of their duty of care in relation to cybersecurity and financially responsible for the subsequent violations of shareholders/stakeholders' privacy and/or personal information.

Since there are aspects of the duty on care in relation to cybersecurity and the use of AI that are very intricate and unclear and because directors are in need of guidance on what types of AI is permissible in terms of the Act and corporate

---

[244] Australian National University's Cybercrime Observatory *et al. AI and Crime*, 43 – 45, available online at <https://regnet.anu.edu.au/sites/default/files/news/related-documents/2019-07/KIC_2019_final_word_08July.pdf>, last accessed on 13 January 2023.

[245] Durbin 'How Cybercriminals Use AI to Fuel Cyberattacks' in *Forbes* of 13 October 2020, *s.p.*, available online at <https://www.forbes.com/sites/forbesbusinesscouncil/2020/10/13/how-criminals-use-artificial-intelligence-to-fuel-cyber-attacks/>, last accessed on 13 January 2023.

[246] Baker *et al. AI and the Law: Cybercrime and Criminal Liability* 201 – 202.

[247] JSE '*Listing Requirements' op cit s.p*.

governance guidelines, the SA Cybercrimes Act 19 of 2020 and the King Code will have to regulate the use of AI.[248]

This thesis will therefore critically analyse the duty of care in relation to cybersecurity and argue for the use of AI in order to help guide directors on how they need to exercise their duty of care in this regard, in an attempt to make SA companies more cyberresilient and will evaluate how directors can apply AI to lessen the potential for cyberbreaches at SA companies, with specific reference to their OMs.

In doing so, this thesis will identify trends in the Company Law and Privacy Law of various jurisdictions and use those lessons for the SA legislature and the King Committee in order to draw lessons for the prohibition on the use of AI to commit cybercrimes in the SA Cybercrimes Act 19 of 2020; and to encourage directors in the King Code to use AI responsibly when they exercise their duty of care in relation to cybersecurity. This is needed in order to help directors prepare for, and respond to, cyberattacks on their companies, and specifically their OMs, and to help protect SA companies and their directors from being held liable for cyberbreaches that were caused by inadequate cybersecurity and which caused damage or loss to the company's cyberassets, or led to the violation of shareholders/stakeholders' privacy and/or personal information.

This thesis makes the argument that the duty of care has a potentially significant role to play to help reduce the likelihood of cyberbreaches if directors knew more clearly how they should exercise their duty of care in relation to cybersecurity and the use of AI. A prohibition in the SA Cybercrimes Act 19 of 2020 on the use of AI to commit cybercrime and the inclusion of a detailed treatment in the King Code on how directors should oversee the responsible use of AI when they exercise their duty of care in relation to cybersecurity, will help directors to oversee more effective cybersecurity policies and systems, and indirectly ensure that their companies become more cyberresilient.

As the compilers of the King Code, the King Committee is in an ideal position to provide corporate governance guidance on the duty of care in relation to cybersecurity and the use of AI, since they have already published the King Reports I – IV, which sets out many recommendations on good corporate governance.

Unlike legislation that is rigid, corporate guidance is non-legislative and based on corporate governance principles and recommendations.[249] As such, the inclusion of a detailed treatment how directors should exercise their duty of care in relation to cybersecurity and the use of AI in the King Code will fit in with the King Code's philosophy of the three key elements of good corporate governance, namely ethical leadership, sustainability and good corporate citizenship.[250] The King Code regards

[248] See Chapter 5, section 5.
[249] See Chapter 5, section 6.
[250] IoDSA '*King Report III' op cit* 10 – 11; Du Plessis *et al. Principles of Contemporary Corpoarte Governance* 292.

ethical leadership as the cornerstone of good corporate governance and that directors should take the lead to help improve companies' economic, environmental and social impact.[251] It regards sustainability as a company's most important economic and ethical goal and views corporate citizenship in terms of the Constitution.[252]

10. OUTLINE OF RESEARCH TOPIC

This thesis will critically analyse how a more detailed treatment of the directors' duty of care in relation to cybersecurity can help to make SA companies more cyberresilient, with the specific focus on their OMs, as well as the role that the use of AI, and its regulation, can play in this regard.

This thesis will therefore start by looking at how OMs function in other jurisdictions in order to draw lessons on how OMs in SA should ideally be conducted and regulated and to identify best practices in terms of the directors' duty of care in relation to cybersecurity.[253] It will then dissect the directors' duty of care and its application on cybersecurity by looking at the ways in which directors in the UK, US and SA apply their duty of care in relation to cybersecurity in order to help limit the possibility that SA directors could be held liable for not exercising their duty of care in relation to cybersecurity properly.[254] It will also determine how AI can be incorporated with OMs so that OMs can be a tool to improve corporate governance and CSR even more.[255] It will also explain how directors should exercise their duty of care in relation to cybersecurity and the use of AI in order to look for lessons on how the duty of care in relation to cybersecurity could help to improve corporate governance and CSR at OMs.[256] It will also look at directors' further exposure to liability in terms of the use and regulation of AI, and set out the lessons on how directors' use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code in order to help lessen directors' exposure to the improper use of AI when they exercise their duty of care in relation to cybersecurity.[257]

In conclusion, the thesis will summarise all of the lessons that were looked at on how directors should apply their duty of care in relation to cybersecurity and the use of AI, to help make SA companies more cyberresilient, by especially lessening the potential for cyberbreaches at SA OMs, as well as directors' further exposure to liability

---

[251] IoDSA '*King Report III' op cit* 10 – 11; Du Plessis *et al. Principles of Contemporary Corpoarte Governance* 292.
[252] SA Constitution; IoDSA '*King Report III' op cit* 11.
[253] See Chapter 2.
[254] See Chapter 3.
[255] See Chapter 4.
[256] See Chapter 5.
[257] *Ibid.*

for not exercising their duty of care in relation to cybersecurity and the use of AI properly.[258]

11. REASONS FOR SELECTING THE TOPIC

There are five main reasons why this topic was selected.

11.1. Primary Research Issues

SA has one of the highest rates of cybercrime in the world and SA companies' cyberassets are vulnerable to cyberattacks. Since SA companies' OMs are conducted on an online platform and use online databases that contain sensitive personal information and PII of the shareholders/stakeholders, they are particularly prone to cyberattacks. AI could be used by directors to resist cyberattacks on a company's cyberassets, such as its online platform and its online databases. Contrariwise, AI could be used by cybercriminals to instigate cyberattacks in an attempt to obtain PII. A shortcoming in the SA cybersecurity regime is that neither the SA Cybercrimes Act 19 of 2020, nor the King Code regulate the use of AI in the fight against cybercrime. As a result, this creates the situation where cybercriminals are using AI to conduct cybercrime, and are not prohibited from doing it, while directors are not encouraged, by means corporate governance guidance, to also use AI to resist such cybercrime that are committed by AI. As a result, cybercriminals are currently still a step ahead of directors as the latter is already using AI to instigate cyberattacks.

When a company creates an online platform, it facilitates the dissemination of information and participation at a company's meeting, but, at the same time the different online security protocols that the company and participants use, pose enormous risks to the company's cybersecurity, especially to the shareholders/stakeholders' privacy and/or personal information, especially if such means of online communication are not end-to-end encrypted.[259] AI advances also create greater opportunities for hackers and crackers to access personal information by means of circumvertor technology that circumvent the interception of online records.[260] Once a cybersecurity system is hacked by a cybercriminal, a comprehensive personal dossier can quickly be obtained from the company's databases.[261]

---

[258] See Chapter 6.
[259] Burchell 'The Legal Protection of Privacy in SA: A Transplantable Hybrid' in *Electronic Journal of Comparative Law* 13(1) March 2009 1.
[260] Bellasio *et al. The Future of Cybercrime in Light of Technology Developments*, 2 – 3, available online at <https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf>, last accessed online at 18 July 2021.
[261] Burchell *op cit* 1.

Since the SA corporate governance regime is not that conducive to help directors understand what their duty of care requires of them in the AI context, there is no *ex ante* legal clarity for directors on how they need to properly exercise their duty of care in relation to cybersecurity and the use of AI before a cyberbreach occurs, and likewise limited guidance for shareholders/stakeholders on what to expect from directors in terms of the protection of their privacy and/or personal information by means of AI.[262] As part of this process, the considerations that the court should look at when they need to determine whether the duty of care in relation to cybersecurity has been breached when it comes to the use of AI, need to be treated in more detail.

This thesis consequently helps with understanding how the directors' duty of care should apply in relation to cybersecurity and the use of AI, and devise guidance to not only protect the company's assets, such as its online platform and its online databases, but also the company, and helps prevent the board and directors from being held liable after a cyberbreach. The focus falls on OMs specifically, as they are a particularly vulnerable aspect of a company's online operations. The updating of the SA Cybercrimes Act 19 of 2020 and the King Code to regulate the use of AI will encourage directors to do their very best and guide those who are uncertain. Simultaneously, it should not entrap directors who tried their best to prevent cyberbreaches from occurring, but they nevertheless occurred. Without the inclusion of a detailed treatment on the duty of care in relation to cybersecurity and the use of AI, directors are exposing themselves and the company to litigation from shareholders/stakeholders every time that a cyberbreach occurs. Once the prohibition on the use of AI is included in the SA Cybercrimes Act 19 of 2020, directors will require a more detailed treatment in the King Code on how they need to exercise their duty of care in relation to cybersecurity, pertaining to the use of AI.[263] Directors cannot benefit from uncertainty, and especially not in the aftermath of the Pandemic when there are many competing interests.[264]

11.2. Lack of Existing Literature in SA

Currently, very little academic research has been done on the way in which a more detailed treatment of the duty of care in relation to cybersecurity and the use of AI could help to fight cybercrime that is directed towards companies and their OMs. All that seems to be known in this field of SA Company Law is reserved to secluded legal provisions, and there is no comprehensive guidance on the duty of care in relation to

---

[262] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *op cit* 284; Deloitte SA '*Post Covid-19: The Benefits and Challenges of Virtual AGMs,*' 2, available online at <https://www2.deloitte.com/content/dam/Deloitte/za/Documents/za-Post-Covid-19-Publication-Virtual-AGMs-Final.pdf>, last accessed on 8 July 2021; Gao *et al*. *op cit* 1; Moyo 'Virtual AGMs May Infringe SA Companies' Act'*op cit s.p.*

[263] Harner 'A More Realistic Approach to Directors' Duties' in *Tennessee Journal of Business Law* (2013) 16.

[264] Harner *op cit* 16 – 18.

cybersecurity and the use of AI that directors can refer to. No standard body of work exists on AI, nor the cybersecurity of OMs in SA.

11.3. Issues Have Far-Reaching Implications for Corporate Governance, Cybersecurity and the Protection of Shareholders'/Stakeholders' Privacy and/or PII

OMs help shareholders and stakeholders to exercise oversight over the board and help to direct the corporate decision-making process.[265] If more shareholders and stakeholders could be involved in this process, oversight on the company's affairs could be improved - and as a result also the good corporate governance and CSR practices that a company follows.[266] OMs also offer shareholders and stakeholders the chance to participate more actively in the governance of a company.[267] This is because Gao *et al*. state that the most affordable and easiest option to increase shareholders/stakeholders' attendance and participation is via the Internet and to hold an OM, since it does not require any travel and subsistence costs to attend a company's meeting.[268]

OMs proliferated in part because ordinary shareholders' meetings had to adapt to meet Lockdown regulations.[269] The problem is however that since many participants work from home, companies worldwide are more susceptible to cyberbreaches, especially when they have improper cybersecurity policies and systems that are not properly overseen by directors.[270]

In addition, an OM increases the possibility for cybercrime because participants will all access the online platform from their phone or laptop from various locations and all of these devices may have different online security protocols.[271] The various online security protocols create a nightmare when it comes to protecting the company against a cyberbreach, since not all of them may be end-to-end encrypted, and just one such a device with insufficient encryption could create a loophole that AI will find, and which a cybercriminal that uses AI could then exploit.[272] Although the use of the JSE online platform helps to put access control measures in place that help to diminish the

---

[265] Ali *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' *op cit* 284; Gao *et al*. *op cit* 1.
[266] *Ibid.*
[267] *Ibid.*
[268] Gao *et al*. *op cit* 1.
[269] Jubb *et al.* 'The Future of the AGM' on *Oxford Business Law Blog* (*OBLB*), *s.p.*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/future-agm>, last accessed on 8 August 2021.
[270] Hiscox Insurance 'Cyberattacks on the Rise for Businesses, Pushing Many to the Brink' in *Insurance Journal* (April 2021) *s.p.*
[271] UK Data and Marketing Association '*The Board Member Checklist: Non-Executive Directors,*' 4, available online at <https://dma.org.uk/uploads/misc/checklist-v3-(1).pdf>, last accessed on 13 May 2021.
[272] Askounis *et al.* '*Working from Home During Covid-19: A Cybersecurity Culture Assessment Survey,*' *s.p.*, available online at <https://link.springer.com/article/10.1057/s41284-021-00286-2>, last accessed on 8 July 2021.

possibility for a cyberbreach, not all SA companies are making use of it, and no information exists on whether it uses AI to improve its cyberresilience or not.[273]

The Lockdown has shown that regulations pertaining to a ban on public meetings, restrictions on travel, self-isolation and social distancing can be instituted on very short notice.[274] With the potential of future outbreaks of Covid-19 and the reinstitution of Lockdown regulations and self-isolation and work from home requirements, SA directors will have to reconsider the way in which they protect their companies assets, especially their online platforms and their online databases and how they conduct their OMs.[275]

It is important to get a grasp of this dynamic, substantive and growing body of Company, Criminal and Privacy Law now, so that it can be adapted, improved and applied meaningfully to the SA corporate governance regime so that SA law can stay abreast with not only cyberrisks and IT advances in the context of AI, but also with international developments in this regard.[276]

11.4. No Cross-Reference in Existing Legal Sources

OMs, the directors' duty of care and the protection of personal information of shareholders and stakeholders are regulated by a regime of different legal sources, which regulate different aspects without cross-referencing each other, ranging from the Constitution, which regulates privacy, to the common law, which still helps to regulate the duty of care of directors, as well as the Act, which regulates OMs and the directors' duty of care.[277] There is also SA POPI Act 4 of 2013, which regulates the protection of shareholders' and stakeholders' personal information, as well as the SA Cybercrimes Act 19 of 2020, which regulates cybercrimes.[278] Then there is the King Committee's '*Reports on Corporate Governance I- IV,*' which regulates corporate governance and CSR.[279] Then there is also the JSE '*Listing Requirements,*' which set out requirements that any listed company has to comply with in order to have their shares publicly traded.[280] Since none of these sources explicitly cross-reference each other on the duty of care in relation to cybersecurity, it is difficult for directors to determine *ex ante* what is required of them when they use AI.

---

[273] Deloitte SA '*Post Covid-19: The Benefits and Challenges of Virtual AGMs' op cit* 2.
[274] Chalwin-Milton '*Electronic AGMs in SA: Reacting to a Pandemic,' s.p.*, available online at <https://www.financialinstitutionslegalsnapshot.com/2020/03/electronic-agms-in-south-africa-reacting-to-a-pandemic/>, last accessed on 15 May 2021.
[275] *Ibid.*
[276] Papadopoulos *et al. Cyberlaw @SA III: The Law of the Internet in SA* 2.
[277] See Chapter 3, section 2; Chapter 5, section 4.
[278] SA POPI 4 of 2013; SA Cybercrimes Act 19 of 2020.
[279] See Chapter 3, section 2.
[280] See Chapter 2, section 5.3.

11.5. Industry Custom on the Use of AI Inconclusive

SA case law shows that a defendant's adherence to, or departure from an industry custom or standard can prove either due care or negligence, but this is not conclusive.[281]

In 1921, Solomon AJ of the Appellate Division in Bloemfontein explained in *Van Breda and Others v Jacobs and Others* that industry custom is a widely accepted and feasible practical measure that is used in an industry, which the defendant was supposed to have been aware of and used.[282] When it needs to be determined whether a defendant complied with industry custom, the court will be cautious as any decision on a defendant's negligence will have implications for the entire industry.[283] At the same time, the court will also be cautious to accept industry custom, as the industry may have pursued self-interest to the detriment of reasonable precaution.[284]

Solomon AJ explained that in order for an industry custom to be conclusive, it will need to be proven that it is reasonable, that it has existed for a long time, that it is generally accepted and followed by the community and that its content is clear and established.[285]

This finding presents many challenges to directors, as there is no certainty on what will constitute the responsible use of AI in terms of cybersecurity, the inclusion of AI in companies' cybersecurity policies and systems have not existed for a long time, there are no uses of AI in companies' cybersecurity policies and systems that are generally accepted and followed by other companies, and the content of companies' cybersecurity policies and systems on the use of AI is not clear and established.[286] As a result, SA industry custom on the use of AI is still inconclusive to help establish industry customs on how directors should exercise their duty of care in relation to cybersecurity.[287]

12. RESEARCH QUESTION

SA has one of the highest rates of cybercrime in the world and SA companies' cyberassets are vulnerable to cyberattacks. Since SA companies' OMs are conducted on an online platform and use online databases that contain sensitive PII, they are particularly prone to cyberattacks. AI could be used to resist cyberattacks on a company's cyberassets, such as its online platform and its online databases.

---

[281] *Van Breda and Others v Jacobs and Others* 1921 AD 330.
[282] *Ibid.*
[283] *Ibid.*
[284] *Ibid.*
[285] *Ibid.*
[286] *Ibid.*
[287] *Ibid.*

Contrariwise, AI could be used by cybercriminals to instigate cyberattacks in an attempt to obtain PII.

This thesis will critically analyse how a more detailed treatment of the directors' duty of care in relation to cybersecurity can help to make SA companies more cyberresilient, with the specific focus on their OMs, as well as what role the use of AI can play in this regard?

Where other researchers looked at OMs as a means to enhance corporate governance and CSR, they have failed to look at the dangers that cybercrime present to OMs and that directors may be held personally liable in the event that a company's cybersecurity was inadequate to thwart a cyberattack and the company's cyberassets were compromised.

By means of legal comparison, this thesis critically analyses how directors need to exercise their duty of care in relation to cybersecurity in order to help make SA companies more cyberresilient, and will argue for directors' use of AI as a tool to help resist cybercrime, and its regulation.

This thesis mounts the challenge of SA cybercrime by firstly looking at how OMs and the duty of care in relation to cybersecurity are regulated in different jurisdictions, and how corporate governance and CSR should include AI, while it also looks at directors' exposure to liability in terms of the use and regulation of AI.

It is submitted that the SA Cybercrimes Act 19 of 2020 and the King Code should be updated to include the use and regulation of AI, since it is an important tool for directors in the fight against cybercrime. The SA Cybercrimes Act 19 of 2020 should be updated to prohibit the use of AI to commit cybercrime, and the King Code should be updated to encourage directors to use AI responsibly to help fight cybercrime in SA

13. STRUCTURE

This thesis is divided into six parts, and starts with the introduction in this chapter.

Chapter 2 will evaluate the regulation of OMs in other jurisdictions. It will start with a short historical overview of OMs and will look at the advent of OMs in SA. It will then look at how OMs themselves are regulated in the US, with its federal and state law, the UK and what the SA legal position on OMs is. This Chapter is needed in order to draw lessons for SA on how OMs are regulated in other jurisdictions, and to determine what the best practices on the regulation of OMs are, in order to understand how to best protect the integrity of the OM, as well as the cybersecurity of the online platform and its online databases.

Chapter 3 will outline the directors' duty of care in relation to cybersecurity. A specific focus will once again be placed on the UK and US positions on the duty of care in relation to cybersecurity in order to contrast it to the SA position by means of a legal comparison. Attention will also be given to the remedies for directors who breached

their duty of care in relation to cybersecurity. The position of non-executive directors will also be looked at in order to make it representative of the legal position of all directors. Lastly, lessons from the legal comparison of the SA, UK and US duty of care in relation to cybersecurity will be looked at in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted.

Chapter 4 will look at the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG investment considerations. It will start by looking at the evolution of the emphasis on CSR to sustainability to ESG considerations. Then it will look at the exercise of SA directors' duty of care in terms of corporate governance and CSR. Then it will look at how SA directors should exercise their duty of care in terms of ESG considerations. Specific attention will then be given to the exercise of the directors' duty of care in relation to cybersecurity and the use of AI and Blockchain technology since this is a new field that is developing fast and directors will need to address the challenges that they present. Lastly, lessons will be drawn on how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.

Chapter 5 will build on the analysis offered in Chapters 2, 3 and 4 and will look at the further accountability mechanisms to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI. It is important that directors have a proper understanding of these various accountability mechanisms in order to limit the possibility that they could be held liable for not exercising their duty of care in relation to cybersecurity properly. It will begin by also giving an overview of both the international and SA privacy law and cybersecurity regimes. It will then focus on directors' liability in terms of the duty of care in relation to cybersecurity and the use of AI. Lastly, it will look at the lessons how the use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code.

Chapter 6 is the Conclusion and will summarise the lessons for SA that were drawn from the various chapters. It will start by summarising the lessons from Chapter 2 for SA on the regulation of OMs in other jurisdictions in order to highlight the various ways how OMs are regulated and the different examples and best practices that exist. Thereafter it will summarise the lessons from Chapter 3 from the legal comparison of the SA, UK and US duty of care in relation to cybersecurity in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted. Then, it will summarise the lesssons from Chapter 4 on the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG considerations in order to look how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs. Lastly, it will summarise the lessons from Chapter 5 that looks at the further accountability mechanisms to hold directors accountable for

how they exercise their duty of care in relation to cybersecurity and the use of AI, and will look for lessons on how directors' use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code.

The Chapter will then end with recommendations on the duty of care in relation to cybersecurity and the use of AI in SA, and then the Chapter will then finally conclude with final remarks that will summarise the contribution of this thesis to SA Law.

14. RESEARCH METHODOLOGY

The research methodology consists of a legal comparison and literature review.

14.1. Legal Comparison

Throughout the thesis, legal comparisons will be drawn on how directors exercise their duty of care in relation to cybersecurity and the use of AI in other jurisdictions, specifically with regards to OMs. Most notably, the legislation of the UK and US, will be looked at, and this will then be contrasted with the SA position. These different approaches will provide insight for the SA legislature and the King Commitee on how these problems are tackled in first world countries, who are right at the forefront of the Fourth Industrial Revolution.

More specifically, Chapter 2 will look at the regulation of OMs in the US and UK, and then compare these two positions with the SA position.[288] Chapter 3 will also look at the ways in which directors exercise their duty of care in relation to cybersecurity in those two jurisdictions and then also compare it to the SA position.[289]

This is the best approach for this thesis, as this will help the SA legislature and the King Committee to determine what the main advantages and disadvantages of the legislation, regulations and corporate governance guidelines of other important jurisdictions are, and will help them with lessons on how to strengthen cybersecurity in SA pertaining to the use of AI, by means of best examples and recommendations on how directors should exercise their oversight in this regard.[290]

Although SA has a hybrid legal system, which was influenced by Roman Dutch civil law and English common law, this research required that the SA position should be contrasted against the law of jurisdictions who are pro-active on the role that the duty of care in relation to cybersecurity could play to help improve cyberresilience, even though the US and UK are examples of common law jurisdictions.

Although the US and UK are developed countries, and SA is a developing country, all three are members of the Group of Twenty (G20), which is an

[288] See Chapter 2, sections 3 - 5.
[289] See Chapter 3, sections 2 – 4.
[290] See Chapter 6, section 5.

intergovernmental forum that works to address matters pertaining to the global economy, such as climate change mitigation, the promotion of financial sustainability and sustainable development.[291] The G20 'Principles of Corporate Governance of 2015,' principle 7 requires member countries to implement a corporate governance framework that gives strategic guidance to companies, and that such a framework must ensure that the board effectively oversees management, and that the board is accountable to the company and the shareholders.[292] In addition, SA is a BRICS (Brazil, Russia, India, China and SA) member country, which means that it is a leader in the developing world, and the lessons that are learned could as a result mean a lot for these other emerging economies.[293] Since the US, UK and SA are all members of the G20 and because SA is also a member of BRICS, the states that were chosen help to be representative of the world-wide state of affairs on countries that strive towards inclusive economic growth and allows a comparison to be drawn between common law jurisdictions in developed countries and a hybrid legal system in an emerging economy.

Next to SA, the US was chosen as it developed the Internet, and because it is at the forefront of developing the cybersecurity software and hardware, which are used around the world, and research would not be complete without covering the rich body of law of the US. Since the US consists of 50 states, which each have their own legal system, complementary to federal law, the evaluation of the US law is necessarily intricate, but rewarding as especially the US states' law presents a rich body of examples and best practices for the King Committee.

Besides the UK's influence on SA common law, the UK was chosen not only because of the shared common law tradition with SA, but also to see how its law regulates AI and Blockchain technology.[294]

Chapter 4 will look at the important international CSR and ESG developments that indirectly influences the way in which SA directors exercise their duty of care in terms of cybersecurity.[295] Since SA is a country which tries to attract foreign direct investment (FDI), it is important that SA directors take cognisance of what investors from these two important trading partners of SA look at, when they decide to invest in a company.

The SA legal position is thus compared with the US and UK, since both are important trading partners of SA. UK, US and SA multinational corporations (MNCs)

---

[291] G20 '*About the G20*,' *s.p.*, available online at <https://www.g20.org/about-the-g20/>, last accessed on 5 October 2022.

[292] G20 'Principles of Corporate Governance of 2015,' principle 7.

[293] Brazil, Russia, India, China, SA (BRICS) '*Information Portal*,' *s.p.*, available online at <https://infobrics.org/>, last accessed on 5 October 2022.

[294] See Chapter 2, section 4.1

[295] See Chapter 4.

need to comply with the law in each country where they do business and these countries are longstanding trading partners of SA with deep-reaching ties *vice versa*.[296]

A legal comparison will also be useful to dual-listed SA companies who have their shares traded on different national stock exchanges, as well as SA companies seeking to relocate their headquarters across jurisdictions, and also UK and US companies who have to comply with SA law.[297]

In addition, as in the US and UK, SA directors have a familiar duty of care in relation to cybersecurity and Chapter 5 will explain that they face certain familiar liability risks for a company's cybersecurity and privacy failures.[298]

Lastly, like the US and the UK, SA is in the midst of rethinking how it looks at cybersecurity.[299] All of these jurisdictions have to date favoured, to a greater or lesser degree, a more voluntary approach to enhance the cybersecurity of companies, especially with regards to their OMs.[300]

Consequently, a legal comparative study of how directors exercise their duty of care in relation to cybersecurity and the use of AI, to protect companies' OMs, is undertaken. A comparative approach is allowed since the Act, section 5(2) provides that may consider foreign company law when it interprets the Act and it is appropriate to do so.[301] This section complements the Act, section 5(1), which directs that the Act must be interpreted in terms of the purpose of section 7, which states that the Act must allow companies the opportunity to grow in a way that will enhance the economic welfare of SA in the world's economy.[302]

14.2. Literature Review

Literature, online sources from companies themselves, expert opinions and journal articles that exist on this topic will be looked at. The way how large companies conduct OMs will also be looked at as examples. Viewpoints of writers at the forefront will be incorporated to find best-practices for the King Committee.

15. CONCLUSION

This chapter introduced the concept of cybercrimes and the consequences of cyberbreaches for companies. It also gave a short historical overview of the largest

---

[296] Horrigan *et al.* 'Directors Duties and Liabilities: Where Are We Now and Where Are We Going in the UK, Broader Commonwealth and Internationally?' in *International Journal of Business and Social Science* 3(2)(2012) 2.
[297] *Ibid*.
[298] See Chapter 2, sections 3 – 5; Chapter 5.
[299] Craig *et al.* 'Toward a Global Cybersecurity Standard of Care?' in *Texas International Law Journal* (2015) 6.
[300] *Ibid.*
[301] The Act, section 5(2).
[302] The Act, sections 5(1); 7.

cyberattacks on US and SA companies. It also explained that OMs are a particularly vulnerable aspect of a company's operations. Thereafter, it explained the causal link between OMs and improved corporate governance and explained the shortcomings in others researchers' research that fails to look at the consequences that cybercrime holds for companies' cybersecurity, especially with regards to their OMs. In this regard, it explained the challenges of OMs in terms of cybersecurity and how AI could be used to help protect a company's cyberassets, such as its online platform and its online databases. Thereafter the role that the directors' duty of care in relation to cybersecurity and the use of AI could play to help make SA companies more secure, was highlighted.

With the research objective it was explained that cybercrime, the directors' duty of care in relation to cybersecurity, OMs and the protection of personal information are all regulated by a regime of different legislation, and to make this situation even more difficult, no mention is made on the use of AI in neither the SA Cybercrimes Act 19 of 2020, nor the King Reports I – IV, which can help directors in the fight against cybercrime. As a result, this Act will have to updated so that it can prohibit the use of AI to commit cybercrime, while the King Code will have to be updated to regulate the use of the different types of AI, so that directors can properly know how to oversee the use of AI when they exercise their duty of care in relation to cybersecurity.

As its research question, it was explained that this thesis will critically analyse how a more detailed treatment of the directors' duty of care in relation to cybersecurity can help to make SA companies more cyberresilient, with the specific focus on their OMs, as well as the role that the use of AI, and its regulation, can play in this regard?

Lastly, the thesis structure and research methodology were explained.

The next chapter will evaluate the regulation of OMs in other jurisdictions, such as the US with its federal and state law, the UK and the SA legal position. This will help the King Committee to draw lessons for SA on how OMs are regulated in other jurisdictions, and to determine what the best practices on the regulation of OMs are, in order to understand what role cybersecurity should play to preserve the integrity of the OM itself, as well as the cybersecurity of the online platform and its online databases.

CHAPTER 2:

THE REGULATION OF OMs IN OTHER JURISDICTIONS

1. INTRODUCTION

This Chapter will look at how OMs are regulated by law, and how these regulatory frameworks and legislative requirements that other jurisdictions have in place help to ensure the cybersecurity of OMs, and the online platforms on which they are held, as well as their online databases that they use that contain the sensitive personal information and PII of shareholders/stakeholders. Once there is a better understanding on how OMs function and how they are regulated, it is possible to look in the following chapters how directors should exercise their duty of care in relation to cybersecurity in order to best protect the integrity of the OM, as well as its online platform and its online databases.

As such, this Chapter is needed to draw lessons for SA on how OMs are regulated in other jurisdictions, and to determine what the best practices on the regulation of OMs are, in order to understand what role cybersecurity and the use of AI should play to preserve the integrity of the OM.

In order for the King Committee to regulate the use of the different types of AI, so that directors can properly know how to oversee the use of AI when they exercise their duty of care in relation to cybersecurity, they need to firstly know how SA and other jurisdictions regulate OMs. They need to identify existing gaps, look for mutual traits, determine how other jurisdictions bridge those gaps, and then use the lessons learned from best practices for the SA corporate governance regime, in order for directors in SA to stay up to date with the latest developments and to exercise their duty of care in relation to cybersecurity in the best way.

2. SHORT HISTORICAL OVERVIEW OF OMs

There has been increasing recognition in other jurisdictions that physical presence is not, or should not, be required for a legally valid shareholders' meeting. Over time, the traditional concept of a shareholders' meeting has changed with advances in the IT Revolution.[303]

In 1990, a UK court decided that being physically present was no longer an indispensable element to constitute a valid shareholders' meeting.[304] The judgment of Browne-Wilkinson VC of the English Court of Appeal in 1990 in *Byng v London Life*

[303] Boros 'Virtual Shareholder Meetings' in *Duke Law and Technological Review* (8)(2004) 6.
[304] *Ibid*.

Association Ltd was the first to mark the court's willingness to accept the concept of a virtual shareholders' meeting – and this consequently opened the door to OMs.[305] Here, an AGM was conducted across different rooms that were connected as each had a live video recording.[306] Browne-Wilkinson VC held that it did constitute a valid meeting, because even though the meeting was held at different places, it was linked by both audio and visual communication, and it allowed shareholders to both see and hear what happen in the other rooms.[307] This judgment thus allowed a meeting to be held in separate places, as long as all of the shareholders were electronically linked.[308]

In 1995 Knecht J of the Appellate Court of Illinois, Fourth District, made a landmark decision in *Freedom Oil Co. v Illinois Pollution Control Board* when he held that administrative agencies may hold a board meeting by tele-conference and that it did not violate Illinois law.[309]

The way in which US companies held their shareholders' meetings changed forever when the Delaware General Corporations Law (DGCL) (Title 8, Chapter 1 of the Delaware Code) was reviewed in 2000 to allow companies incorporated in Delaware – which comprise most US public companies, and two-thirds of the Fortune 500 – to conduct OMs.[310] In this regard, the DGCL of 2000, section 211(a)(1) validates a shareholders' meeting that is held at no venue.[311] This change eventually inspired many other US states, and influenced other jurisdictions of the world, to also make provision for OMs.[312]

In 2001 and 2002, the first two Delawarean companies which held OMs were respectively Inforte Corporation and Ciber Incorporated.[313] At Inforte Corporation's Online Annual General Meeting (OAGM), voting was not required because shareholders already voted on 97% of the shares by facsimile before the OAGM.[314] No report could be found on Ciber Incorporated's OAGM, but in a circular that was issued prior to it, the

---

[305] *Byng v London Life Association Ltd* (1990) Ch 170.
[306] *Ibid*.
[307] *Byng supra* 182.
[308] Delport *et al. Henochsberg on the Companies Act op cit* 231.
[309] *Freedom Oil Co. v Illinois Pollution Control Board* 655 N.E.2d 1184 (Ill. App. Ct. 1995).
[310] Delaware General Corporations Law (DGCL) (Title 8, Chapter 1 of the Delaware Code) of 2000; The Corporate Governance Review '*US: Delaware,' s.p.*, available online at <https://thelawreviews.co.uk/edition/the-corporate-governance-review-edition-7/1140934/united-states-delaware>, last accessed on 12 February 2018.
[311] DGCL of 2000, section 211(a)(2).
[312] Matera 'Delaware's Dominance and Wyoming's Dare: Blockchain Companies and the Market for Corporate Chraters' on *Oxford Business Law Blog* (OBLB), *s.p.*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/delawares-dominance-wyomings-dare-blockchain-companies-and-market>, last accessed on 8 August 2021; Morgenson 'Meet the Shareholders? Not at These Shareholder Meetings' in the *New York (NY) Times* of 31 March 2017, *s.p.*, available online at <https://www.nytimes.com/2017/03/31/business/corporate-virtual-shareholder-meetings.html>, last accessed on 12 February 2018.
[313] Boros *op cit* 7.
[314] *Ibid*.

company stated that it had to resort to an OAGM, as on average only 10 out of its more than 28 000 shareholders attended an AGM.[315]

From this start, OMs spread through Globalisation across the world and continue to grow as the Fourth Industrial Revolution unfolds and the Pandemic continues.

According to Morgenson, the status of OMs in other jurisdictions can be drawn on a spectrum, from making unrestricted legal provision for OMs (such as Delaware); to jurisdictions that will allow OMs if certain restrictions are adhered to (such as California, Illinois and SA); to jurisdictions that prohibit OMs and hybrid meetings (such as New York (NY) and Massachusetts) – although these states did temporarily allow them under state executive order, as part of Pandemic measures.[316]

Many of the world's largest companies, such Hewlett-Packard, PayPal and others have already switched to OMs before the Lockdown; while some companies such as Berkshire Hathaway, Johnson & Johnson and Microsoft, and others, already switched to hybrid meetings before the Lockdown.[317]

In 2020, another landmark decision was made in the midst of the Pandemic, when Trower, J of the England and Wales High Court (Chancery Division) evaluated the visibility requirement and held in *Re Castle Trust Direct Plc & Others* that shareholders do not have to see the proceedings of shareholders' meetings, and that it will suffice if companies only adhere to the audibility requirement.[318]

The dawning of the Pandemic thus compelled companies to hold OMs in some form or other due to social distancing measures and restrictions on travelling.[319]

2.1. Advent of OMs in SA

---

[315] Boros *op cit* 7.

[316] Morgenson *op cit s.p.*; Lexology.com '*NY Governor Issues Executive Order Allowing Virtual AGMs,' s.p.*, available online at <https://www.lexology.com/library/detail.aspx?g=c96e05de-803a-4ca6-9e03-2701186fa70b>, last accessed on 19 June 2021; Mass.gov '*Governor Baker Files Legislation to Extend Certain Covid-19 Emergency Measures,' s.p.*, available online at <https://www.mass.gov/news/governor-baker-files-legislation-to-extend-certain-covid-19-emergency-measures>, last accessed on 19 June 2021.

[317] Cao 'Warren Buffet Hosts First Online Shareholders Meeting' in *Observer* of 1 May 2011, *s.p.*, available online at <https://observer.com/2020/05/warren-buffett-online-berkshire-hathaway-shareholder-meeting-2020-coronavirus/>, last accessed on 6 August 2021; Microsoft '*Microsoft Annual Shareholders' Meeting 2019,' s.p.*, available online at <https://www.microsoft.com/en-us/Investor/events/FY-2020/2019-Annual-Shareholder-Meeting>, last accessed on 6 August 2021; Roman '*What HP's Virtual Annual Shareholder Meeting Means for Remote Meetings,' s.p.*, available online at <https://www.azeusconvene.com/articles/virtual-annual-shareholder-meeting-means-means-remote-meetings>, last accessed on 6 August 2021; PayPal '*Questions for PayPal Holdings Inc, 2017 Annual Meeting of Stockholders,' s.p.*, available online at <https://materials.proxyvote.com/default.aspx?dochostid=325761>, last accessed on 6 August 2021.

[318] *Re Castle Trust Direct Plc & Others* (2020) EWHC 969 (Ch).

[319] UN Principles of Responsible Investment '*The New Normal: Company AGMs in a Covid-19 World,' s.p.*, available online at <https://www.unpri.org/pri-blog/the-new-normal-company-agms-in-a-covid-19-world/5859.article>, last accessed on 8 July 2021.

OMs were virtually unheard of in SA until the Pandemic struck and a Lockdown was declared on Tuesday, 26 March 2020 by President Cyril Ramaphosa, in terms of the SA Disaster Management Act 57 of 2002.[320] Until then, SA companies generally held physical meetings and OMs were unusual.[321]

When Lockdown struck, SA companies were challenged on how to meet legislative obligations and how to comply with their memorandums of incorporation (MOIs) when it comes to the holding of shareholders' meetings.[322] Lockdown regulations initially prevented any in-person meetings and even as SA has moved to lower Lockdown levels it remained difficult for most companies to hold in-person meetings.

Fortunately, the Act, section 63(2) does make legal provision for OMs, and enabled SA companies to hold them, so this allowed the JSE to step in and devise an online platform as a practical means for this purpose.[323] The JSE solicited the services of a company called, 'The Meeting Specialist' (TMS), to devise SA's first online platform for shareholders' OMs.[324] The JSE announced that this online platform could be used for all shareholders' meetings, as well as OAGMs, and that it makes provision for online voting.[325] The weblink of this online platform is proxy@tmsmeetings.co.za.[326]

History was made on 27 March 2020 when Alexander Forbes hosted SA's first OAGM by a listed company when they used this online platform.[327] Afterwards, Alexander Forbes reported that almost 91% of their shares were represented at this OAGM.[328] Many of SA's most prominent companies, such as Old Mutual and Standard Bank and others, followed suit.[329]

On 9 May 2020, Strate was the first SA company to hold its OAGM by using an e-Voting platform.[330] The Strate e-Voting platform uses AI in the form of the Blockchain

---

[320] SA Disaster Management Act 57 of 2002; Coenraad *et al*. '*Virtual AGMs in the Wake of Covid-19,' s.p.*, available online at <https://www.werksmans.com/legal-updates-and-opinions/virtual-agms-in-the-wake-of-covid-19/>, last accessed on 16 May 2021.

[321] Coenraad *et al. op cit s.p*.

[322] *Ibid*.

[323] The Act, section 63(2); Johannesburg Stock Exchange (JSE) '*JSE and TMS Launch First Virtual AGMs Enabling Clients to Engage with Shareholders,' s.p.*, available online at <https://www.jse.co.za/articles/jse-and-tms-launch-first-virtual-agms-enabling-clients-to-engage-with-shareholders>, last accessed on 2 June 2021.

[324] JSE '*JSE and TMS Launch First Virtual AGMs Enabling Clients to Engage with Shareholder' op cit s.p*.

[325] *Ibid*.

[326] JSE '*AGMs,' s.p.*, available online at <https://www.jse.co.za/services/company-services/annual-general-meetings>, last accessed on 8 July 2021.

[327] Coenraad *et al*. *op cit s.p*.

[328] *Ibid*.

[329] Old Mutual '*AGM, 21 May 2021,' s.p.*, available online at <https://www.oldmutual.com/about/governance/annual-general-meeting/>, last accessed on 9 July 2021; Standard Bank '*AGM, 27 May 2021,' s.p.*, available online at <https://reporting.standardbank.com/agm/>, last accessed on 9 July 2021.

[330] Strate '*Strate Holds First Remote AGM,' s.p.*, available online at <https://www.strate.co.za/2020/05/>, last accessed on 4 August 2021.

technology of Nasdaq to allow online voting and administer proxy administration.[331] Strate is the central securities depository and is responsible for the safekeeping of the legal, online record of share ownership.[332] It secures ownership rights of different types of securities, such as bonds, equities, money market funds and participatory notes in collective investment schemes and shares.[333]

Another important event happened on 1 July 2021, when the SA POPI Act 4 of 2013 came into effect and started to regulate how companies should process the personal information of data subjects, such as shareholders and stakeholders, and hold boards directly accountable for any violations pertaining to the protection of personal information and PII.[334]

3. US

OMs are not allowed in all US states, but where they are allowed, they are regulated by requirements that differ between states.[335]

In the US, state law generally governs the legality of OMs and, if permitted, the ways in which they should be conducted.[336] At the federal level, the US Model Business Corporations Act (MBCA) of 2016 regulates remote shareholder participation in a shareholders' meeting and the US Securities Exchange Commission (SEC) regulates proxy documentation.[337]

Since the US law on OMs and the accompanying corporate governance aspects that have an impact on cybersecurity and the use of AI are complex, this sub-section will be broken down into US federal law, with a sub-section on securities exchange regulations; followed by the legislation of the six different models of US states' law on OMs, as well as the relevant US stock exchange listing regulations.

3.1. US Federal Law

---

[331] Strate '*Strate Holds First Remote AGM' op cit s.p*.

[332] Strate '*Annual Integrated Report 2020,'* 5, available online at <https://www.strate.co.za/wp-content/uploads/2021/06/Strate-INTEGRATED-REPORT-2020.pdf>, last accessed on 4 August 2021.

[333] Strate '*Annual Integrated Report 2020' op cit* 10; 15.

[334] SA POPI Act 4 of 2013.

[335] Albano *et al.* '*Update: Coronavirus and Virtual Annual Meetings,' s.p.*, available online at <https://www.clearymawatch.com/2020/03/coronavirus-virtual-annual-meetings/>, last accessed on 22 June 2021.

[336] *Ibid.*

[337] Albano *et al. op cit s.p.*; US Model Business Corporations Act (MBCA) as amended in 2016, Chapter 7, Subchapter A, section 7.09; US Securities Exchange Commission (SEC) '*SEC Adopts Rule Amendments to Provide Investors Using Proxy Voting Advice More Transparent, Accurate and Complete Information,' s.p.*, available online at <https://www.sec.gov/news/press-release/2020-161>, last accessed on 7 July 2021.

In the US, Federal Law emanates from the US Constitution of 1788, which allows the US Congress to promulgate legislation for certain fields, such as Company Law.[338] Federal legislation allows executive agencies to promulgate regulations, which are compiled in the US Code of Federal Regulations.[339]

In 1950, the US MBCA was compiled by the American Bar Association (ABA)'s Committee on Corporate Laws of the Section of Business Law.[340] The MBCA was later updated and the MBCA of 2002 is followed by 24 states.[341]

The MBCA of 2002 was amended in 2016 and Chapter 7: 'Shareholders,' Subchapter A: 'Meetings,' section 7.09 specifically regulates remote shareholder participation in a meeting.[342] It states that (a) shareholders of any class or series of shares may participate in any shareholders' meeting by online communication if the board authorises it.[343] In addition, it states that participation by online communication is bound by the guidelines and procedures that a board decides, thereby allowing the board to set a standard on the duty of care in relation to cybersecurity that needs to be exercised that is above and beyond existing legal requirements.[344] Section 7.09(b) says that shareholders who participate online is regarded as being present and may vote if reasonable measures exist to verify their identity; and if they are given a reasonable opportunity to participate and to vote and communicate and to follow the proceedings as they occur.[345] Although the important requirement that participants must be able to follow the proceedings as they occur has the purpose to prevent the exclusion of shareholders from the proceedings, it indirectly requires that buffering, freezing or lagging must be mitigated, which could potentially create a loophole for a cyberattack.[346] Buffering (which is a constant break down in the loading of the live feed) causes the livestream to lag (which is the slowing down of the online live feed) and prevents participants from following the proceedings as they occur.[347] Buffering and lagging are caused by software coding errors, while freezing is caused by either too many online processes happening at once, a shortage of Random Access Memory (RAM) or malware that causes the central processing unit (CPU) to stop working – and all of this

---

[338] US Constitution of 1788; Garner *et al. Black's Law Dictionary s.v.* 'federal law'.
[339] US Code of Federal Regulations; Pennsylvania State University Library '*US Government: Executive Branch,' s.p.*, available online at <http://guides.libraries.psu.edu/executive/regulations>, last accessed on 7 December 2018.
[340] American Bar Association (ABA) '*Committee on Corporate Laws,' s.p.*, available online at <https://www.americanbar.org/groups/business_law/committees/corplaws/>, last accessed on 24 February 2022.
[341] *Ibid.*
[342] US MBCA of 2016, Chapter 7, Subchapter A, section 7.09.
[343] US MBCA of 2016, section 7.09(a).
[344] *Ibid.*
[345] US MBCA of 2016, section 7.09(b)(1)-(2).
[346] *Ibid.*
[347] Din '*What is Buffer Overflow?,' s.p.,* available online at <https://heimdalsecurity.com/blog/what-is-buffer-overflow/#:~:text=In%20information%20security%20and%20programming,access%20to%20a%20company's%20system.>, last accessed on 14 May 2022.

creates loopholes that cybercriminals can use to launch a cyberattack on the online platform.[348]

When it comes to proxy solicitations and shareholder proposals made in terms of the US Securities Exchange Act of 1934, section 78(a), federal US Securities Law generally do not prescribe how companies should conduct shareholders' meetings.[349] This Act consequently leaves it to the board to determine the logistics of OMs.[350]

3.1.1. US SEC

At a federal level, the US SEC regulates the administration of proxy documentation, while state law regulates the legality and the requirements of OMs.[351]

Recently, the US SEC's Division of Corporation Finance and the Division of Investment Management released a statement in April 2020, entitled; '*Staff Guidance for Conducting Shareholder Meetings in Light of COVID-19 Concerns*' ('Staff Statement').[352] This Staff Statement is today virtually the blueprint that provides guidance from US federal level on US OMs, not only to the US SEC's staff, but also to directors on the way in which they need to exercise their duty of care in relation to cybersecurity.[353] Since the Staff Statement constitutes a form of 'soft law' in non-binding norms that provides guidance on the corporate governance aspects pertaining to US OMs, its format is of importance to the King Committee.[354]

The Staff Statement only contains the views of this division of the staff of the SEC, and not even of the US SEC itself.[355] It therefore has no legal force, but it does provide guidance to directors on important corporate governance matters that pertain to the duty of care in relation to cybersecurity in the light of the Pandemic.[356]

The Staff Statement encourages all role players to consider a company's circumstances when they need to conduct a shareholders' meeting and allows the board to adopt any additional measures, which may include cybersecurity, in order to allow the company to continue to function under the circumstances.[357] It also

---

[348] Din *op cit s.p.*; Quora 'What's the Difference Between Buffering, Freezing and Lagging?,' *s.p.*, available online at <https://www.quora.com/What-is-the-difference-between-lagging-freezing-and-buffering-on-a-computer-or-other-device>, last accessed on 28 October 2022.
[349] US Securities Exchange Act of 1934, section 78(a).
[350] US Securities Exchange Act of 1934.
[351] Albano *et al. op cit s.p*.
[352] US SEC Division of Corporate Finance and the Division of Investment Management '*Staff Guidance for Conducting Shareholder Meetings in Light of Covid-19 Concerns,*' *s.p.*, available online at <https://www.sec.gov/ocr/staff-guidance-conducting-annual-meetings-light-covid-19-concerns>, last accessed on 10 July 2021.
[353] *Ibid.*
[354] *Ibid.*
[355] *Ibid.*
[356] *Ibid.*
[357] *Ibid.*

encourages all parties to be flexible and to collaborate to facilitate companies' obligations when it comes to holding secure and successful shareholders' meetings and to allow shareholders to continue to vote, despite the Pandemic.[358]

With regards to OMs, the Staff Statement points out that the ability to conduct OMs is determined by state law, and companies' MOIs.[359] It also accentuates that directors need to make robust disclosures, for example on cybersecurity and the use of AI to protect the online platform and its online databases, in order to facilitate informed shareholder attendance and participation.[360]

Further on OMs, the Staff Statement requested companies to set out clear steps on the logistics of their OMs, such as how to access, participate and vote securely online, and that directors need to ensure that this is the case.[361] No mention was however made of how directors could oversee the use of Blockchain technology to secure the online voting process.

In addition, the Staff Statement accentuates the important role of disclosure, and requires that directors must provide shareholders with the necessary information to inform them on cybersecurity matters that affect them.[362]

3.2. US State Law

The 50 states of the US are distinct jurisdictions, each with their own constitution and government.[363] Each state's legislature enacts their legislation and their judiciary applies their state law.[364] The states have plenary power, not subject to review, to promulgate legislation on any matter not regulated by the federal constitution or federal law.[365] The states' supreme courts are the highest courts of law to interpret state constitutions and legislation promulgated in terms thereof, but in cases where federal issues come into play, decisions are appealed to the US Supreme Court.[366] States' laws have developed in different directions since the US was founded in 1776, and their laws differ so significantly that the US federal legal system is basically 50 different systems of Company Law.[367]

---

[358] US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*
[359] *Ibid.*
[360] *Ibid.*
[361] *Ibid.*
[362] *Ibid.*
[363] US Constitution of 1788, Amendment X.
[364] Cooper '*Essay on the Tenth Amendment: Reserved Power for the States,*' *s.p.*, available online at <https://www.heritage.org/constitution/#!/amendments/10/essays/163/reserved-powers-of-the-states>, last accessed on 10 December 2018.
[365] *Ibid.*
[366] US Code of Federal Regulations, Title 28, 'Judiciary and Judicial Procedure,' section 1257.
[367] Cooper *op cit s.p.*

As stated, US states' law determines the legality of OMs' format and a board should begin by looking at the law of the state where a company is incorporated to determine the legality of OMs and their specific requirements in order to know how they should exercise their duty of care in relation to cybersecurity within a certain state.[368]

The last comprehensive survey that was conducted in the US to determine which states' allow and prohibit OMs and what the different requirements to conduct legally valid OMs are, was when the Best Practices Working Group for Online Shareholder Participation in AGMs compiled their survey, '*Guidelines for Protecting and Enhancing Online Shareholder Participation in OMs,*' in June 2012.[369] Some states, such as Virginia, have since amended their state law to make provision for OMs.[370]

In states where OMs are allowed, directors should still study the relevant regulations, since some states have further requirements on OMs.[371] In addition, some states have their own requirements on cybersecurity and the way in which directors should exercise their duty of care in relation to cybersecurity.

Albano *et al.* states that their research did not detect direct guidance from state legislatures on OMs in the context of the Pandemic, and that most companies had to rely on the guidance from the Staff Statement.[372]

Until the Pandemic, not all of the various US states' law allowed companies to conduct OMs, but special state executive orders allowed OMs until such time when the Pandemic subsides.[373]

The following section sets out the different legislative examples by means of models on how the various US states regulate OMs, ranging from those that require specific procedures for OMs to those that do not make provision for it. The different requirements of each of these models determine the way in which directors need to exercise their duty of care in relation to cybersecurity in each of the states of these models.

3.2.1. The Delawarean Example: OMs With Specific Procedures

The DGCL of 2000, section 211 has two sections that regulate OMs.[374]

---

[368] Albano *et al. op cit s.p.*

[369] Best Practices Working Group for Online Shareholder Participation in AGMs '*Guidelines for Protecting and Enhancing Online Shareholder Participation in OMs,*' 9 – 10, available online at <https://www.broadridge.com/_assets/pdf/broadridge-guidelines-for-protecting-and-enhancing-online-shareholder-participation-in-annual-meetings.pdf>, last accessed on 21 June 2021.

[370] *Ibid.*

[371] *Ibid.*

[372] Albano *et al. op cit s.p.*; US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*

[373] *Ibid.*

[374] DGCL of 2000, section 211.

Section 211(a)(1) states that shareholders' meetings may be held anywhere, inside or outside Delaware, as determined by the MOI, or in the absence thereof, as resolved by the board.[375] Section 211(a)(2) allows the board to decide that a shareholders' meeting will not be held at a physical place, but solely online.[376]

Section 211(a)(2) says that if a board has so decided, and if a MOI allows it, participants may (a) participate online; and (b) be deemed physically present and vote at a physical meeting or OM, as long as: (i) their identity is reasonably verified; and (ii) everyone present is afforded a reasonable opportunity to participate, vote and to follow the proceedings as they occur; and (iii) any decisions and votes are recorded.[377]

The first part of this section indicates that Delaware makes provision for both OMs and hybrid meetings and that it is up to the board to decide which option they choose.[378] The second part requires boards to follow three general and flexible measures when they hold an OM or a hybrid meeting.[379] The first requirement demands that the identity of all participants should be known in order for the board to practice access control.[380] The second requirement indirectly has the effect that it helps to mitigate buffering, freezing and lagging, which could cause a loophole for a cyberattack.[381] The third requirement on the recording of the decisions and votes could easily be done by AI by means of Blockchain technology, but such records should be kept confidential and should be held safely with strict access control to the Blockchain central securities depository.[382] The third requirement makes no mention whether only the name of the participant or also the weblink which the participant used to access the online platform, should also be recorded.[383]

3.2.2. The Colorado Example: OMs Without Specific Procedures

The Colorado Revised Statutes Annotated of 2017, section 7-107-108 regulates OMs and stipulates that unless a MOI precludes it, shareholders may take part in a shareholders' meeting, and that it may be conducted by any means of communication that will enable all participants to hear each other.[384] A shareholder who participates in such a way is then legally regarded as being present at the shareholders' meeting.[385] In terms of this section, a MOI is also a tool that can be used to set requirements on how

[375] DGCL of 2000, section 211(a)(1).
[376] DGCL of 2000, section 211(a)(2)
[377] DGCL of 2000, section 211(a)(2)(b)(i)-(iii).
[378] DGCL of 2000, section 211(a)(1).
[379] DGCL of 2000, section 211(a)(2)(b)(i)-(iii).
[380] DGCL of 2000, section 211(a)(2)(b)(i).
[381] DGCL of 2000, section 211(a)(2)(b)(ii).
[382] DGCL of 2000, section 211(a)(2)(b)(iii).
[383] *Ibid.*
[384] Colorado Revised Statutes Annotated of 2017, section 7-107-108.
[385] Colorado Revised Statutes Annotated of 2017, section 7-108.

OMs are held, on cybersecurity requirements, as well as the way in which directors should exercise their duty of care in relation to cybersecurity. 'Online presence' at an OM is an important aspect of the duty of care in relation to cybersecurity and this concept should be well-defined, so that directors can ensure that strict access control measures to the online platform are in place, and remain in place, and that they may be held liable if they are not in place.

Ambiguity exists in the Colorado example, because although section 7-107-108 evidently makes provision for hybrid meetings, legal uncertainty exists when it comes to OMs.[386] This is due to section 7-107-101 that states that meetings should be held at the place that a company's MOI prescribes.[387] This section seems to denote a physical place for a meeting and is ambiguous when read together with the section that makes provision for OMs.[388] Since section 7-107-108 makes room for 'remote-shareholder participation' as well as any means of communication, Colorado does seem to allow OMs, as any other interpretation would be contradictory.[389] In the case of hybrid meetings, directors should also ensure that there are proper physical access control measures in place, besides the online access control measures, and as a result this then place a higher requirement on the duty of care in relation to cybersecurity that they need to exercise.

It should however be pointed out that in contrast to the DGCL of 2000, section 211(2)(b)(i)-(iii), Colorado's section 7-107-108 does not prescribe any procedures that companies need to follow for an OM, except that the participants should be able to hear each other during the meeting.[390] If interpreted strictly, this section would mean that only teleconference-OMs (where participants use a telephone and are able to hear each other simultaneously and to follow the proceedings in real-time) are permitted in Colorado.[391] The requirement of audibility is good, as this safeguards shareholders against exclusion, but the Delawarean requirement on the ability to follow the proceedings as they occur is stricter, and more conducive to cybersecurity, as it also requires the software coding errors of buffering, freezing and lagging to be mitigated, or otherwise backed-up, since it could otherwise cause a loophole for a cyberattack.[392]

3.2.3. The Massachusetts and Montana Example: Limitations on Public Companies

---

[386] Colorado Revised Statutes Annotated of 2017, section 7-107-108; Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1373.
[387] *Ibid*.
[388] *Ibid.*
[389] *Ibid*.
[390] Colorado Revised Statutes Annotated of 2017, section 7-107-108; DGCL of 2000, section 211(2)(b)(i)-(iii).
[391] Colorado Revised Statutes Annotated of 2017, section 7-107-108.
[392] Colorado Revised Statutes Annotated of 2017, section 7-107-108; DGCL of 2000, section 211(a)(2)(b)(ii).

When it comes to holding shareholders' meetings, the Massachusetts General Laws Annotated 156D of 2004, section 7.08 differentiates between private and public companies.[393] Provision is made for hybrid meetings at companies which have a class of public shares, but they are not allowed to hold an OM.[394] On the contrary, private companies may have hybrid meetings, but may also hold OMs.[395]

Massachusetts's section 7.08 follows the example of the DGCL of 2000, section 211(a)(1), but differentiates between public and private companies.[396] In this regard, section 7.08 stipulates that unless a MOI states something else, and as long as the board authorises it, a shareholders' meeting does not have to be held at a physical place, and that it can be held entirely online, unless it is a public company.[397]

The Montana Code Annotated of 2010 also differentiates between the sizes of companies.[398] As such, section 35-1-516 stipulates that if a company has less than 50 shareholders and if its MOI allows it, the shareholders at a hybrid meeting may use a tele-conference or similar communication to hear each other and follow the proceedings as they occur.[399] The fact that Montana requires the audibility requirement as well as the ability to follow the proceedings as they occur, indirectly acts as a double mitigation measure against buffering, freezing and lagging, and requires, as a result, a higher duty of care in relation to cybersecurity to be exercised.[400]

It would seem that Montana's section 35-1-516 was influenced by Colorado's section 7-107-108, but it limits remote-shareholder participation to companies with less than 50 shareholders and precludes larger companies from allowing such participation.[401] Also, Montana's section 35-1-516 does not allow any company to hold an OM.[402] Although both Massachusetts's section 7.08 and Montana's section 35-1-516 differentiate between the sizes of companies, Montana's provision is more limited.[403]

No other US state restricts OMs to particular types of companies.[404]

3.2.4. The New York (NY) Example: Obligatory Shareholder Input

[393] Massachusetts General Laws Annotated 156D of 2004, section 7.08.
[394] *Ibid.*
[395] Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1375.
[396] DGCL of 2000, section 211(a)(1); Massachusetts General Laws Annotated 156D of 2004, section 7.08.
[397] Massachusetts General Laws Annotated 156D of 2004, section 7.08.
[398] Montana Code Annotated of 2010, section 35-1-516.
[399] *Ibid.*
[400] *Ibid.*
[401] Colorado Revised Statutes Annotated of 2017, section 7-107-108; Montana Code Annotated of 2010, section 35-1-516.
[402] Montana Code Annotated of 2010, section 35-1-516.
[403] Massachusetts General Laws Annotated 156D of 2004, section 7.08; Montana Code Annotated of 2010, section 35-1-516.
[404] Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1376.

The NY 'Bill to Authorise Shareholders to Attend Meetings via Remote Communication and Be Deemed Present for Voting Purposes of 2019' was passed in January 2019 and amends the NY Business Corporation Law of 2010, section 602 to allow OMs.[405]

New York's section 602(1) determines that (b)(i) a board may, after they first obtained shareholders' input, hold OMs, but then the board must, (1) allow shareholders a reasonable opportunity to participate; and must (2) provide reasonable measures for online voting, as long as the company (A) reasonably identifies each participant; and (B) keeps a record of any vote or resolution.[406] It also states that a shareholder who participates online is regarded as being present in person.[407] Section 602(1)(b)(ii) states that no requirement in the previous paragraph, (i), may be interpreted in a manner that limits or restricts voting and participation.[408] In terms of section 602(1)(b)(iii), "reasonable measures," pertaining to shareholder participation, will mean webcast or other broadcasts and for voting it will mean online and telephone voting.[409]

In terms of these requirements AI could play an important part to help secure the online voting process and to keep record of any vote or resolution by means of Blockchain technology on the central securities depository.[410] Telephone voting is also a unique type of voting that differs from online voting, and no requirements are laid down that require directors to ensure that one-time-pin (OTP) numbers, voice recognition or other access control measures, which specifically pertains to access control for telephone voting, are in place.[411]

3.2.5. The California and Maryland Example: Shareholder Participation

The California Corporations Code of 2009, section 600 and the Maryland Code Annotated on Corporations and Associations of 2017, section 2-503 make provision for shareholders' input when a company has to decide whether to hold an OM or not, as well as its logistics.[412] This presents an opportunity for shareholders to give their feedback and input to the board on the cybersecurity measures that they require and how they want the board to exercise their duty of care in relation to cybersecurity, and it

[405] NY Business Corporation Law (NY BCL) of 2010 (amended 2019), section 602; NY State Assembly Bill 'Bill to Authorise Shareholders to Attend Meetings via Remote Communication and be Deemed Present for Voting Purposes, Bill A434 of 2019,' 1.
[406] NY BCL of 2010 (amended 2019), section 602(1)(b)(i)(1)-(2)(B).
[407] NY BCL of 2010 (amended 2019), section 602(1)(b)(i)(2)(B).
[408] NY BCL of 2010 (amended 2019), section 602(1)(b)(i)-(ii).
[409] NY BCL of 2010 (amended 2019), section 602(1)(b)(iii).
[410] NY BCL of 2010 (amended 2019), section 602(1)(b)(i)(2)(A)-(B).
[411] NY BCL of 2010 (amended 2019), section 602(1)(b)(iii).
[412] California Corporations Code of 2009, section 600; Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503; Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1377.

also presents an opportunity for the board to ensure that the cybersecurity measures that the company use are in line with the IT tools that the shareholders require and use.

In this regard, Maryland's section 2-503(b)(1) stipulates that if the board is authorised to decide on the place where a meeting should be held, it can decide that it should not be held physically, but entirely online in terms of section 2-503(c).[413] Also, Maryland's section 2-503(b)(2) states that if a shareholder so requests, the board must determine the place where a shareholders' meeting must be held.[414]

Although Maryland's section 2-503(b)(1) allows the board to decide whether the company will hold an OM, section 2-503(b)(2) contains a limitation in the sense that an OM cannot be held if any shareholder objects.[415] A valid objection may include an objection based on a cybersecurity-related aspect or if the board does not exercise due care in relation to cybersecurity.[416] Besides this provision, section 2503 closely follows the example of the DGCL of 2000, section 211(a)(2).[417] Section 2503(a)-(b) thus also makes provision for OMs and hybrid meetings.[418]

Both Maryland's section 2-503 and the California Corporations Code of 2009, section 600 were influenced by the DGCL of 2000, section 211, with the exception that instead of just requiring authorisation from the board, California's section 600 also requires companies to obtain shareholders' consent before an OM can be held.[419] This presents an opportunity for shareholders to acquaint themselves with an OM's cybersecurity logistics beforehand and to ensure that it is suited to their expectations. Should shareholders feel that the board exercises an insufficient duty of care in terms of cybersecurity, they are at liberty to withhold their consent.[420]

In this regard, California's section 600(a) states that shareholders' meetings may be held anywhere inside or outside California, as determined by the MOI.[421] If no place is determined, then the shareholders' meeting will be held at the company's main headquarters.[422] Unless precluded by a MOI, but authorised by the board and subject to the consent required by California's section 20(b) and the procedures determined by the board, hybrid meetings are allowed, and shareholders' meetings may be held either

---

[413] Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(b)(1)-(2); section 2-503(c).
[414] Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(b)(2).
[415] Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(b)(1)-(2).
[416] *Ibid.*
[417] DGCL of 2000, section 211(a)(2); Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503.
[418] Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(a)-(b).
[419] California Corporations Code of 2009, section 600; DGCL of 2000, section 211; Maryland Code Annotated on Corporations and Associationsof 2017, sections 2-503; Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1377.
[420] California Corporations Code of 2009, section 600; DGCL of 2000, section 211; Maryland Code Annotated on Corporations and Associationsof 2017, sections 2-503; Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1377.
[421] California Corporations Code of 2009, section 600.
[422] *Ibid.*

physically, entirely or partly online, in terms of section 600(e).[423] Directors need to remember that if a shareholders' meeting is conducted partly online, then not only are both online and physical access control measures required, but also different measures to protect personal information that is stored online and physically.[424]

California's section 600(e) states that a shareholders' meeting may be conducted entirely or partly online, if (1) the company reasonably allows participants to participate and vote, and also to follow the proceedings in real-time and (2) to take minutes of the votes and resolutions.[425] Any request by a company to shareholders in terms of section 20(b) for consent to hold an OM shall include a notice that will inform them that without their consent, the meeting will have to be held at a physical place, as is required by section 600(a).[426] This provision is problematic in the unlikely event that shareholders do not give their consent for an OM during a time of crisis, such as the Pandemic, but Californian directors will nevertheless have to inform shareholders about this provision, as part of their duty of care in relation to cybersecurity.[427]

No other US state requires shareholders' consent to hold an OM, except the Minnesota Statutes Annotated of 2017, section 302A, which only requires shareholders to be informed of the company's intention to conduct an OM.[428]

3.2.6. The Illinois Example: No OMs

The Illinois Compiled Statutes Annotated 805, section 5/7.05 only makes provision for hybrid meetings.[429] As such, no provision is made for companies to hold an OM, as a physical meeting will have to be held at a physical place.[430] There are other US states that follow this example and also only allow companies to make provision for hybrid meetings.[431] The laws of these states just differ with regards to the specific procedures that are required for hybrid meetings.[432] Despite a prohibition on OMs, a hybrid meeting still requires directors to oversee the same strict online access control measures that an OM require, as well as a proper cybersecurity system, in order to protect the meeting and the participants' personal information.

---

[423] California Corporations Code of 2009, sections 20; 600(e).
[424] *Ibid.*
[425] California Corporations Code of 2009, section 600(e)(1)-(2).
[426] California Corporations Code of 2009, sections 20(b); 600(a).
[427] *Ibid.*
[428] California Corporations Code of 2009, section 20(b); Minnesota Statutes Annotated of 2017, section 302A; Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1378.
[429] Illinois Compiled Statutes Annotated 805 of 1983, section 5/7.05.
[430] Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1379.
[431] For example, Indiana, Montana, Nevada, North Carolina, Oregon, Virginia and Washington; Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1379.
[432] Fairfax '*Virtual Shareholder Meetings Reconsidered*' *op cit* 1379.

3.3. Stock Exchange Rules

The NY Stock Exchange (NYSE)'s 'Listed Company Manual,' section 302.00 merely states that listed companies must hold an AGM for each fiscal year.[433]

In January 2021, the NYSE issued a '*Listed Company Compliance Guidance,*' that explained that in response to the Pandemic, the NYSE filed temporary rules with the SEC, to provide relief from certain rules, which require shareholder approval in the NYSE '*Listed Company Manual,*' and which were to remain in force until 1 July 2020.[434] The temporary relief was later extended until 31 March 2021.[435] The guidance makes no mention of OMs *per se*, but lay down specific requirements when it come to regular AGMs and shareholder approval and voting rights requirements.[436] No mention was made of how Blockchain should be used to store online votings and resolutions on the central securities depository.

Nasdaq's 'Listing Rule' 5620(a) similarly only states that a listed company must hold an AGM within a year after its fiscal year-end and specifies that it must permit shareholders to address company affairs, which may include the duty of care in relation to cybersecurity, with management.[437] It however makes no mention whether shareholders may do so online.

4. UK

OMs are also regulated by various legal sources in the UK, which impacts on how directors need to exercise their duty of care in relation to cybersecurity.[438]

4.1. European Union (EU) 'Directive on the Encouragement of Long-Term Shareholder Engagement of 2017'

The European Union (EU) 'Directive on the Encouragement of Long-Term Shareholder Engagement of 2017' (EU 'Shareholder Engagement Directive') is applicable to the UK (from before Brexit) and regulates how certain shareholder rights of voting shares should be exercised at shareholders' meetings of companies who are

---

[433] NY Stock Exchange (NYSE) '*Listed Company Manual,*' rule 302.00, available online at <http://wallstreet.cch.com/LCMTools/PlatformViewer.asp?selectednode=chp_1_4&manual=%2Flcm%2Fsections%2Flcm-sections%2F>, last accessed on 9 February 2018.

[434] NYSE '*Listed Company Compliance Guidance,*' 1, available online at <https://www.nyse.com/publicdocs/nyse/regulation/nyse/NYSE_2021_Annual_Guidance_Letter.pdf>, last accessed on 22 June 2021.

[435] *Ibid.*

[436] NYSE '*Listed Company Compliance Guidance' op cit* 4, 8.

[437] Nasdaq *'Listing Rules*' 5620(a).

[438] UK Companies Act of 2006 (Ch. 46), section 360A.

registered in an EU member state and whose shares are listed in an EU member state.[439]

Shares of listed companies are sometimes held by intermediaries on a central securities depository that uses encrypted Blockchain technology, and which makes shareholder engagement difficult, because companies are not always able to identify their shareholders.[440] It goes without saying that a company cannot engage with its shareholders if it is not able to identify them.[441] Likewise, shareholders will have difficulty to exercise their rights if they have to work through an intermediary to make contact with the company.[442] This is especially problematic in cross-border situations where different privacy and/or personal information protection legislation applies.[443] Section 4 therefore dictates that intermediaries may provide listed companies with the personal information of their shareholders, so that the listed companies can directly communicate with them.[444] This means that when companies ask intermediaries for the personal information of their shareholders that are stored by means of Blockchain technology on a central securities depository, they must decrypt it and provide it.[445]

Although it does not mention the use of AI for cybersecurity purposes by name, section 3(c)(3) says that the EU Commission may adopt implementing acts, for example on cybersecurity and the protection of shareholders/stakeholders' privacy and/or personal information, with minimum requirements to help with the further exercise of shareholders' rights.[446]

4.2. UK Companies Act of 2006 (Ch.46), section 360A

UK companies have been allowed to hold OMs since 2009 after the UK Companies Act of 2006 (Ch. 46), section 360A was amended by the UK Companies (Shareholder Rights) Regulations of 2009.[447] Although the EU 'Shareholder Engagement Directive of

---

[439] EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017,' section 1, available online at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017L0828>, last accessed on 11 February 2018.

[440] EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017' *op cit* section 4.

[441] *Ibid.*

[442] *Ibid.*

[443] *Ibid*.

[444] *Ibid.*

[445] *Ibid.*

[446] EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017' *op cit* section 3(c)(3).

[447] UK Companies Act of 2006 (Ch. 46), section 360A; UK 'The Companies' (Shareholders Rights) Regulations of 2009,' *s.p.*, available online at <https://www.legislation.gov.uk/uksi/2009/1632/contents/made>, last accessed on 11 February 2018; Younghusband '*Electronic Meetings: Holding a Virtual AGM,*' *s.p.*, available online at <https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/corporate/2017/electronic-meetings--holding-a-virtual-agm/>, last accessed on 11 February 2018.

2017' is only applicable to listed companies, the UK Companies Act of 2006 (Ch. 46), section 360A ("Electronic Meetings and Voting") applies to all UK public or private companies.[448]

The provisions that regulate shareholder meetings are set out in the relevant sections of the UK Companies Act of 2006, Part 13.[449] Here, section 311(1) requires a notice to state the date, time and place of the meeting.[450]

In June 2016 the first OAGM in the UK was held by Jimmy Choo Ltd.[451] This OAGM was followed by a lot of debate on whether the "place of meeting" only refers to a physical place.[452] As a result of the legal uncertainty, many companies decided until recently to stick with either ordinary shareholders' meetings or hybrid meetings.[453]

Critics are of the opinion that the UK Companies Act of 2006, section 311 does not allow for a shareholders' meeting to be held completely online, because a meeting notice is required to state the "place of meeting," and they reckon that this requirement cannot be interpreted as to refer to anything else other than a physical place.[454]

Contrariwise, the more liberal interpretation of the word "place of meeting" in section 311 could just as well include an online location and section 360A could be interpreted in a way that overrides section 311; while the EU 'Shareholder Engagement Directive of 2017,' section 8 could be seen as the enabling provision that allows OMs, and which does not limit companies to only hybrid meetings.[455]

In an attempt to clarify the meaning of section 311, a company could amend its MOI to give a definition of the "place of meeting."[456] Such a definition would however still have to be interpreted according to its ordinary meaning in the UK Companies Act of 2006, section 311 and cannot simply be overridden in the MOI.[457] If clarity could be provided on the true meaning of section 311, companies who wish to conduct OMs

---

[448] EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017' *op cit s.p.*; UK Companies Act of 2006 (Ch. 46), section 360A.

[449] UK Companies Act of 2006 (Ch. 46), Part 13.

[450] UK Companies Act of 2006 (Ch. 46), section 311.

[451] Coen '*Virtual AGMs: A Global Update,' s.p.*, available online at <https://webcache.googleusercontent.com/search?q=cache:oD_0jGbtcJsJ:https://www.eqs.com/ir-blog/virtual-annual-general-meetings-update/+&cd=7&hl=en&ct=clnk&gl=za>, last accessed on 11 July 2020.

[452] Thomson Reuters Practical Law Corporate '*Virtual and Hybrid General Meetings: Practical Considerations and Best Practice*,' *s.p.*, available online at <https://uk.practicallaw.thomsonreuters.com/w-029-6286?transitionType=Default&contextData=(sc.Default)>, last accessed on 17 June 2023.

[453] Coen *op cit s.p.*

[454] UK Companies Act of 2006 (Ch. 46), section 311; Birkett's Solicitors '*Are All General Meetings Virtually the Same?,' s.p.*, available online at <https://webcache.googleusercontent.com/search?q=cache:JunDRF7q_9cJ:https://www.birketts.co.uk/insights/legal-updates/are-all-general-meetings-virtually-the-same+&cd=15&hl=en&ct=clnk&gl=za>,last accessed on 12 December 2018.

[455] EU 'Directive on the Exercise of Certain Rights of Shareholders in Certain Companies (2007/36/EC) of 2007,' section 8; UK Companies Act of 2006 (Ch. 46), section 311; section 360A; Younghusband *op cit s.p.*

[456] UK Companies Act of 2006 (Ch. 46), section 311; Younghusband *op cit s.p.*

[457] *Ibid.*

should ensure that their MOIs include enabling provisions that allow OMs.[458] The directors should ensure that the MOI does not prohibit online participation at shareholders' meetings and that the definition of 'being present' does not only prohibit online presence.[459]

There has been much debate whether the MOIs of companies who wish to hold hybrid meetings should especially make provision for them.[460] The UK Institute of Chartered Secretaries and Administrators (ICSA) explained in its guidelines entitled, '*2021 General Meetings and the Impact of Covid-19*' that, due to the legal uncertainties that were caused by Lockdown restrictions, companies were allowed to hold valid hybrid meetings even when their MOIs did not make provision for them.[461] It says that it would however be best if directors could ensure that their companies' MOIs especially make provision for hybrid meetings.[462] It also explains that directors need to add provisions in the MOI of what needs to happen if the OM or hybrid meeting experiences IT challenges, such as the ability of the chairperson to adjourn or postpone the OM without the approval of the participants, and how this will affect the validity of the OM.[463]

Section 360A regulates OMs and voting and can be regarded as a more general provision on the holding of OMs, but then it has to be interpreted together with the EU 'Directive on the Exercise of Certain Rights of Shareholders in Certain Companies of 2007,' section 8 and has to be seen as supporting hybrid meetings instead of OMs.[464] This conclusion may be deduced if section 360A is interpreted carefully.[465]

In this regard, section 360A(1) states that nothing in the UK Companies Act of 20016 may be interpreted in a manner that will cause participants of a shareholders' meeting who are not present, to not attend, speak or vote online.[466]

Section 360(A)(2) subjects this right, set out above, by stating that the use of IT during a shareholders' meeting may only be subject to requirements which are (a) needed to identify the participants; and that (b) the cybersecurity measures for online communications must be reasonable.[467] Although no definition or examples are provided on what would constitute reasonable cybersecurity measures, it is expected that the use of AI for cybersecurity will conform to this requirement.[468]

---

[458] UK Companies Act of 2006 (Ch. 46), section 311; Thomson Reuters *op cit s.p.*
[459] *Ibid.*
[460] Thomson Reuters *op cit s.p.*
[461] UK Institute of Chartered Secretaries and Administrators (ICSA) '*2021 General Meetings and the Impact of Covid-19,' s.p.*, available online at <https://www.cgi.org.uk/knowledge/resources/2021-general-meetings-and-the-impact-of-covid-19>, last accessed on 17 June 2023.
[462] *Ibid.*
[463] Thomson Reuters *op cit s.p.*
[464] EU 'Directive on the Exercise of Certain Rights of Shareholders in Certain Companies (2007/36/EC) of 2007' *op cit* section 8; UK Companies Act of 2006 (Ch. 46), section 360A; Younghusband *op cit s.p.*
[465] UK Companies Act of 2006 (Ch. 46), section 360A; Younghusband *op cit s.p.*
[466] UK Companies Act of 2006 (Ch. 46), section 360A(1).
[467] UK Companies Act of 2006 (Ch. 46), section 360A(2)(a)-(b).
[468] UK Companies Act of 2006 (Ch. 46), section 360A(2)(b).

Section 360A(3) again relates to the physical access control measures of proxies and allows a company to require proof of identity of a proxy, but does not mention online access control requirements.[469]

Directors also need to adhere to the requirements of section 360AA(1), which states that when a poll is used for online voting, a company needs to ensure that a confirmation of receipt of the vote is given to such a voter.[470]

OMs may make provision for split voting and allow shareholders to change their vote after it was cast, before voting closes.[471] Once the vote was cast, the participant need to receive confirmation, as explained in terms of section 360AA(1), that their vote was received.[472]

The UK Financial Reporting Council (FRC) explained in '*Corporate Governance AGMs: An Opportunity for Change*' of October 2020 that it is liaising with the UK government to get clarity on how sections 311 and 360A should be interpreted.[473] In addition, the General Counsel from the Financial Times Stock Exchange (FTSE) 100 Index of Companies (GC100), has also requested the UK government to give clarity on whether section 311 allows companies to hold OMs.[474]

4.3. UK Corporate Insolvency and Governance Act (CIGA) of 2020

The temporary UK Companies Act dispensation, which was instituted via the UK Corporate Insolvency and Governance Act (CIGA) in June 2020, allowed companies to hold OMs and was extended by the UK's 'CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021' until 30 March 2021.[475]

CIGA was intended to provide companies with temporary relief to continue to trade and to avoid insolvency due to the financial pressures that were caused by the Pandemic.[476] It especially helped companies by relaxing corporate governance provisions for those companies who grappled with the legal requirements of shareholders' meetings.[477]

---

[469] UK Companies Act of 2006 (Ch. 46), section 360A(3).
[470] UK Companies Act of 2006 (Ch. 46), section 360AA(1).
[471] Thomson Reuters *op cit s.p.*
[472] UK Companies Act of 2006 (Ch. 46), section 360AA(1).
[473] UK Financial Reporting Council (FRC) '*Corporate Governance AGMs: An Opportunity for Change – October 2020*,' *s.p.*, available online at <https://www.frc.org.uk/getattachment/48c4ee08-b7be-4b7c-8f19-bcaf3d44e441/Corporate-Governance-AGM.pdf>, last accessed on 17 June 2023.
[474] *Ibid.*
[475] UK Companies Act of 2006 (Ch. 46); UK Corporate Insolvency and Governance Act (CIGA) of 2020; UK CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021, section 2.
[476] Steeden *et al.* '*CIGA,*' *s.p.*, available online at <https://bateswells.co.uk/2020/07/corporate-insolvency-and-governance-act-2020/?hub=coronavirus>, last accessed on 22 June 2021.
[477] Coen *op cit s.p.*

As such, it introduced a more flexible framework to conduct shareholders' meetings, such as granting the ability in Schedule 14, rule 3(4) to hold them online, even if they were not authorised in terms of an MOI.[478] Not only were these measures helpful for companies who had upcoming shareholders' meetings, but it also allowed companies to amend their MOIs in order to enable OMs to be held in future - particularly since the flexibility that it offered on OMs only lasted until 30 March 2021.[479]

The first flexibility was an extended period to hold shareholders' meetings.[480] If a company had to hold a shareholders' meeting on a date that fell between 26 March 2020 and 30 March 2021, it could validly hold it at any point then.[481]

The second flexibility was its provision for OMs.[482] If a shareholders' meeting had to be held in the relevant period, companies were afforded additional flexibilities by Schedule 14, rule 3, even if their MOI did not make provision for it.[483] In this regard, subsection 3 said that the shareholders' meeting did not need to be held in a particular place, even if the MOI required it.[484] In addition, subsection 4 said that any votes were permitted to be cast online or by any other means.[485] Subsection 5 went on to say that the shareholders' meeting could be held without a quorum that is gathered at a physical place.[486] Lastly, subsection 6 said a shareholder did not have a right to (a) physically attend the shareholders' meeting, (b) participate in a specific manner, or to (c) vote by any particular means.[487] As a result, directors were essentially given the opportunity to decide how to best conduct and secure their OM, in terms of the prescribed measures above.[488]

These measures did not prevent shareholders to vote or to resolve matters and directors had to make reasonable efforts to gain the usual degree of shareholder engagement.[489] The measures did however require shareholders to cast their votes in a particular way, for example, by allowing shareholders to nominate the chairperson as a proxy, to cast their votes beforehand and to vote online.[490]

The new flexibilities of CIGA had three different implications for OMs and the duty of care in relation to cybersecurity: in the first instance, once a company had already held

---

[478] UK CIGA of 2020, Schedule 14, rule 3(4).
[479] UK CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021, section 2.
[480] UK CIGA of 2020, Schedule 14, rule 2(1).
[481] UK CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021, section 2.
[482] UK CIGA of 2020, Schedule 14, rule 3(3).
[483] UK CIGA of 2020, Schedule 14, rule 3.
[484] UK CIGA of 2020, Schedule 14, rule 3(3).
[485] UK CIGA of 2020, Schedule 14, rule 3(4).
[486] UK CIGA of 2020, Schedule 14, rule 3(5).
[487] UK CIGA of 2020, Schedule 14, rule 36(a)-(c).
[488] Simmons & Simmons '*Extension of Rules that Temporarily Ease Company Meeting Flexibility,' s.p.*, available online at <https://www.simmons-simmons.com/en/publications/ckaifpkvmkkhu0900lf31ftdf/proposals-to-temporarily-ease-company-meetings-and-filing-requirements>, last accessed on 23 June 2021.
[489] *Ibid.*
[490] *Ibid.*

an OM during Lockdown, Schedule 14, rule 3 validated it, even if it was not in line with the MOI and also validated any resolutions that were taken in this period during an OM.[491] However, in terms Schedule 14, of rule 3(8) the company still had to comply with the rules of shareholders' meetings that were not superseded by CIGA.[492]

In the second instance, when a company had to hold a shareholders' meeting during the relevant period, it was then possible in terms of Schedule 14, rule 3(5) to make use of the flexibilities, such as the postponement of the shareholders' meeting or to hold an OM.[493]

CIGA in other words provided temporary relief from parts of the UK insolvency regime to help directors steer through the Pandemic without the risk of personal liability and to temporarily ease requirements that relate to shareholders' meetings.[494] It thereby provided relief to directors who were faced with difficult decisions on how to conduct shareholders' meetings safely and to get the necessary cybersecurity policies and systems in place, while it also sought to preserve the rights of their companies' shareholders to participate in meetings.[495] Although the flexibilities made provision for OMs, it did not actively encourage directors to use AI to safeguard the online platform and its online databases, nor to use Blockchain technology to secure online voting and to secure resolutions on the central securities depositry.

4.4. UK Department for Business, Energy and Industrial Strategy's Memorandum of 2020

In addition, in June 2020, the UK Department for Business, Energy and Industrial Strategy issued a memorandum, '*Measures in Respect of Company Filings, AGMs and Other General Meetings During Covid-19*,' which offered guidance on best practices on OMs.[496] These measures allowed a quorum to be formed online; allowed shareholders to ask questions and to get answers on matters (which may include the way in which directors exercise their duty of care in relation to cybersecurity and the use of AI) before voting commences; and required the disclosure of answers on any questions raised; as

---

[491] UK CIGA of 2020, Schedule 14, rule 3.
[492] UK CIGA of 2020, Schedule 14, rule 3(8).
[493] UK CIGA of 2020, Schedule 14, rule 3(5).
[494] Chiu *et al.* 'Relief and Rescue Policies in Financial Regulation at the Time of the Pandemic' on *OBLB*, *s.p.*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/relief-and-rescue-policies-financial-regulation-time-pandemic>, last accessed on 8 August 2021; Simmons & Simmons *op cit s.p.*
[495] Goldthorp *et al*. '*The UK CIGA 2020: A Move to a More Debtor-Friendly Restructuring Regime?,' s.p.*, available online at <https://www.nortonrosefulbright.com/en/knowledge/publications/5ac21a15/the-uk-corporate-insolvency-and-governance-act-2020>, last accessed on 23 June 2021.
[496] UK Department for Business, Energy and Industrial Strategy '*Measures in Respect of Company Filings, AGMs and Other General Meetings During Covid-19,' s.p.*, available online at <https://www.frc.org.uk/getattachment/e3224310-c39c-4b48-b56b-cc703936beeb/Updated-QA-AGMs-Best-Practice-Final.pdf>, last accessed on 23 June 2021.

well as the offering of a physical meeting to all shareholders once the Lockdown restrictions were eased.[497]

4.5. UK Chartered Governance Institute's Guidelines of 2020

In 2020, the UK Chartered Governance Institute released the '*New Guidance Issued about Shareholder Meetings under CIGA 2020*,' which guides shareholders' meetings in terms of CIGA.[498] This elaborated on the previous guidelines from March 2020 on how shareholders' meetings had to be held during the Pandemic and contained more detailed information on logistical aspects that includes cybersecurity-related aspects that directors need to oversee and the way in which shareholders could vote more securely online.[499]

4.6. Stock Exchange Rules

Although the London Stock Exchange (LSE)'s '*Rules of the LSE,*' contain no provisions on OMs, the LSE took a pro-active stance and went as far as lobbied the UK government to allow OMs as soon as the Pandemic struck.[500] The LSE did however not make use of the opportunity to lobby for regulations to increase cybersecurity at OMs, and neither did it help to devise an online platform, like the JSE did.

4.7. Case Law

It was explained earlier that in 1990, Browne-Wilkinson VC of the English Court of Appeal in 1990 in *Byng supra* held that being physically present was no longer an essential element to constitute a valid shareholders' meeting.[501] He held that in order to satisfy the legal requirements for an OM, shareholders must be able to participate as if they were attending the meeting in person.[502] He explained that shareholders must be

---

[497] UK Department for Business, Energy and Industrial Strategy *op cit* 7 – 8.

[498] UK Corporate Governance Institute '*New Guidance Issued about Shareholder Meetings under CIGA 2020,' s.p.*, available online at <https://www.cgi.org.uk/about-us/press-office/news-releases/new-guidance-issued-about-shareholder-meetings-under-the-corporate-insolvency-and-governance-act-2020>, last accessed on 23 June 2021.

[499] *Ibid.*

[500] London Stock Exchange (LSE) '*Rules of the LSE,' s.p.*, available online at <https://docs.londonstockexchange.com/sites/default/files/documents/rules-lse.pdf>, last accessed on 19 July 2021; Clark 'LSE Pushes for Virtual AGMs due to Corona Virus' in *City AM* of 22 March 2020, *s.p.*, available online at <https://www.cityam.com/london-stock-exchange-pushes-for-virtual-agms-due-to-coronavirus/>, last accessed on 29 July 2021.

[501] See Chapter 2, section 2; *Byng supra.*

[502] *Byng supra* 182.

able to firstly, hear the proceedings; and secondly, to speak and be heard at the meeting.[503]

In 2020, Trower, J of the England and Wales High Court (Chancery Division) added another requirement to these two above-mentioned requirements.[504] Trower, J held in *Re Castle Trust Direct Plc & Others supra* that although it is no longer required that shareholders must be able to see the proceedings of the meeting, shareholders need to vote in real time when they use an online platform.[505]

In addition to being able to vote in real time and to ask questions during the meeting, shareholders must be able to hear each other and to be heard by the other participants.[506] Trower, J consequently explained that if there is no specific provisions in the MOI which makes provision for participation in a certain manner, some form of audio functionality (such as a dedicated phone line) must be provided to ensure that the legal requirements for a meeting are satisfied.[507] If a company's MOI makes provision for other methods of communication to be used, the directors should seek advice on whether it is in line with the legal requirements for a valid OM or hybrid meeting.[508]

5. SA

OMs in SA are also regulated by a regime of different legislation which impacts on how directors need to exercise their duty of care in relation to cybersecurity.

5.1. The Act

When it comes to AGMs, the Act is specific and states in section 61(7)(a) that SA public companies must conduct an AGM within eighteen months after a company was incorporated.[509] Thereafter, section 61(7)(b) requires that an AGM must be conducted once in a calendar year, and within fifteen months after the previous one.[510]

Section 61(10) requires every shareholders' meeting of a public company to be reasonably accessible within SA for online participation and subject to section 63(2), irrespective of whether the OM is conducted in SA or elsewhere.[511] This then places another requirement on directors as part of their duty of care in relation to cybersecurity,

---

[503] *Byng supra* 182.
[504] *Re Castle Trust Direct Plc & Others supra*.
[505] *Ibid.*
[506] Thomson Reuters *op cit s.p*.
[507] *Re Castle Trust Direct Plc & Others supra*, par. 42.
[508] *Re Castle Trust Direct Plc & Others supra*, par. 42; Thomson Reuters *op cit s.p*.
[509] The Act, section 61(7)(a).
[510] The Act, section 61(7)(b).
[511] The Act, sections 61(10); 63(2).

namely that they need to ensure that a company's OM is also reasonably accessible for online participation.[512]

Section 62(3)(a) sets out a shareholders' meeting notice's requirements and states that it must be in written format, and must state the date, place and time where it will be held.[513] A notice will usually state a physical place as the 'place of meeting'.[514] This provision can also be interpreted liberally so as to include a meeting which is held online.[515] No mention is however made in the accompanying SA Company Regulations of 2011 of the need to provide a secured weblink to access the OM, or that each participant needs to get a unique username and pin number to access the OM, or the need to provide a helpline for participants who struggle to get online access, nor that provision should be made for computer illerate participants to get assistance to access an OM at a company or agency office somewhere in SA.[516]

Section 63(2) however makes provision for instances where a shareholders' meeting is not held at a physical place.[517] Section 63(2) is the enabling provision that allows OMs and states that if a company's MOI does not prohibit an OM, it may conduct (a) a shareholders' meeting completely online; or that (b) participants may take part online in the physical shareholders' meeting, as long as the online communication allows everyone to communicate effectively and simultaneously with one another without an intermediary.[518] The requirement that directors needs to ensure that all participants need to communicate simultaneously with one another and also reasonably effectively, places a big responsibility on their duty of care in relation to cybersecurity and indirectly presents a double mitigation measure against buffering, freezing and lagging that cybercriminals could exploit, and is similar to the Montana example that also presents a double precautionary measure with both the audibility requirement as well as the requirement on the ability to follow the proceedings as they occur.[519]

The prohibition of section 63(2)(b) on the use of intermediaries in the online communication between shareholders and the company is a unique provision when compared with other legislation, and the King Code should set out examples of what it entails and should explain why this is a forbidden practice.[520]

When it comes to the requirement to communicate without intermediaries, research by Just Share shows that some of SA's blue-chip companies use forms of AI, such as chatbots that moderate questions before they reach the board.[521] Particularly

---

[512] The Act, sections 61(10); 63(2).
[513] The Act, section 62(3)(a).
[514] *Ibid.*
[515] The Act, section 62(3)(a); Coenraad *et al*. *op cit s.p*.; Delport *et al*. *Henochsberg on the Companies Act op cit* 240.
[516] SA Company Regulations of 2011.
[517] The Act, section 62(3).
[518] The Act, section 63(2)(a)-(b).
[519] Montana Code Annotated of 2010, section 35-1-516; The Act, section 63(2)(a)-(b).
[520] The Act, section 63(2)(b); See Chapter 2, section 2.3.1.
[521] Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act' op cit s.p*.

worrisome in this regard is the description of the JSE's partner in the online platform, TMS, where it states on its website under "Mobile Meeting Services," that it allows questions that are sent to the board, to be moderated.[522] Some large SA companies, such as Exxaro SA and Old Mutual, have held their OMs via TMS.[523] If any of the questions that were sent to the board were moderated, it would be in conflict with section 63(2), which requires shareholders to pose their questions to the board without them being moderated.[524]

The JSE online platform is not the only OM service provider who allows this to happen.[525] Remgro's '*OM Shareholders' Guide 2020*' clearly states that "Questions sent via the Lumi online platform will be moderated before being sent to the chairperson. This is to avoid repetition and to remove any inappropriate language".[526] This conflicts with section 63(2) and creates the potential to avoid accountability and infringes the shareholders' right to speak freely.[527] It also creates external interference in the OM that could lead to a cybersecurity loophole. Section 63(2) requires shareholders to send their questions directly to the board, and they must then answer it without any moderation, so shareholders must not be forced to submit their questions in writing before a meeting starts.[528] If an OM does not allow shareholders to interact directly with the board it serves no purpose, because nothing prevents shareholders from sending their written questions to the board whenever they want to.[529] The King Code will need to lay down guidance on how directors need to exercise their duty of care in relation to cybersecurity when it comes to the use of AI intermediaries and the use of AI to moderate questions, as the Act basically sees this as external inference with the online proceedings.[530]

Section 63(3) regulates online participation and states that if a company makes provision for online participation, then (a) the notice must inform shareholders of the availability of online communication for remote participation, and must state the required access information; and must explain that (b) the cost of using the online communication is a cost to be borne by the participant, unless the company decides

---

[522] TMS '*The Meeting Specialist (Pty) Ltd,' s.v.* 'mobile meeting services,' available online at <https://www.tmsmeetings.co.za/>, last accessed on 20 June 2021.
[523] Old Mutual '*Notice of AGM for the Year Ended 31 December 2020,*' 1, available online at <https://www.oldmutual.com/v3/assets/blt566c98aeecc1c18b/bltcaf2ee861b069f47/607d6facb290e724ab00aad0/2021-04-14_-_OM_Notice_of_AGM.PDF>, last accessed on 20 June 2021; Exxaro '*Summarised Group Annual Financial Statements for the Year Ended 31 December 2019 and Notice of AGM,*' 50, available online at <https://www.exxaro.com/assets/files/Exxaro-Notice-to-AGM-2019.pdf>, last accessed on 20 June 2021.
[524] Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p*.
[525] Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act' op cit s.p*.
[526] Remgro Ltd '*OM Shareholders' Guide 2020,*' 2, available online at <https://www.remgro.com/wp-content/uploads/2020/11/Remgro-Virtual-Meeting-Instructions.pdf>, last accessed on 20 June 2021.
[527] The Act, section 63(2); Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act' op cit s.p*.
[528] The Act, section 63(2); Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p*.
[529] *Ibid*.
[530] The Act, section 63(2)(b); See Chapter 2, section 2.3.1.

something else.[531] The cost provision of section 63(3)(b) only relates to the cost of online communication and makes no mention of any cybersecurity responsibilities that a shareholder may have (there is for example no requirement that their online device needs to be encrypted), and this effectively places all of the responsibility for the cybersecurity of the entire OM on the board.[532] The cost provision in SA's Act is a unique provision, when compared to other legislation and was probably intended to act as an equalising measure in the SA society, which is a society that is characterised by income inequality.[533]

Section 63(4) regulates voting rights on a poll of hands and states that any participant who is present and who may vote, only has one vote, regardless of how many shares they own.[534] Section 63(5) further regulates voting rights and states that on a poll at any meeting, any participant may use all the voting rights of their shares.[535] No requirement is however made that Blockchain technology could be used to secure the online voting or that resolutions should stored in a central securities depositry.[536]

5.2. King Reports I–IV

Additionally, King Report IV, principle 12 recommends that boards exercise ongoing oversight over IT management, so that there is an ethical and responsible usage of IT.[537] The King Committee still has to provide recommendations for directors on how they need to exercise their duty of care in relation to cybersecurity in terms of the ethical and responsible usage of AI, because otherwise this principle will remain hollow.[538]

5.3. Johannesburg Stock Exchange (JSE) '*Listing Requirements*'

The JSE '*Listing Requirements*' is a list of all the rules and procedures that any listed company will, in terms of section 1.28, need to comply with if they want to be listed on the JSE and have their shares traded publicly.[539] In terms of the Requirements, section 3.84, any listed company will also have to conform with the King Reports I - IV if they want to be listed on the JSE, and have their shares traded there.[540] This effectively means that directors will have to exercise their duty of care in relation to cybersecurity

[531] The Act, section 63(3)(a)-(b).
[532] The Act, section 63(3)(b).
[533] *Ibid.*
[534] The Act, section 63(4).
[535] The Act, section 63(5).
[536] The Act, sections 63(4) - (5).
[537] IoDSA '*King Report IV' op cit* principle 12.
[538] *Ibid.*
[539] JSE '*Listing Requirements,'* section 1.28.
[540] JSE '*Listing Requirements,'* section 3.84.

responsibly when they oversee the use of Blockchain technology to store shareholders' personal information on the central securities depository, if they want their company's shares to be listed on the JSE.[541]

5.4. SA Companies Amendment Bill of 2021

The SA Companies Amendment Bill (the Bill) of 2021 contains some provisions that will also influence the way in which companies will need to administer PII, and the way in which directors will need to exercise their duty of care in relation to cybersecurity.[542] This Bill will amend the Act, and it will give a new definition for securities; define a true owner of a security; provide clarity on the right to access companies' records; and will also help companies to identify beneficial interest holders in their securities.[543]

With regards to the change in the definition of 'securities,' the Bill of 2021, section 1(b) wants to amend it, so that it can refer to any shares or debentures, despite their form or title, which are issued by a profit company.[544] 'Securities' will therefore no longer include other instruments in its definition and will be limited to shares and debentures.[545]

The Act does not require that the identity of the true owners of companies must be revealed.[546] The Bill of 2021 will correct this and will require directors to establish and report on the true nature of their company's shareholder ownership.[547] In order to help determine who really owns such a security, the Bill of 2021, section 4.3 contains a definition to help determine the 'true owner' of a security.[548] In short, it defines a 'true owner' of a security as a natural person who is able to direct its registered holder to act in a certain way or someone who ultimately benefits from the shareholding.[549] It states that it is just a natural person who can be the true owner of a security.[550] Directors will find the identification of a true owner as necesarrily complex, but that it will help to identify beneficial interest holders in the company.[551] The Bill wants to make other amendments to the Act, section 56 to help identify the true owner of a security.[552]

The implication of having to determine who a "true owner" is, is that directors will not only have to exercise their duty of care in terms of cybersecurity on the privacy and

---

[541] JSE '*Listing Requirements,'* section 3.84.
[542] SA Companies Amendment Bill of 2021.
[543] SA Bill of 2021, *s.v.* 'General Explanatory Note.'
[544] SA Bill of 2021, section 1(b).
[545] *Ibid.*
[546] SA Bill of 2021, section 4.2.
[547] *Ibid.*
[548] SA Bill of 2021, section 4.3.
[549] *Ibid.*
[550] *Ibid.*
[551] *Ibid.*
[552] The Act, section 56; SA Bill of 2021, section 4.3.

personal information of the current holder of a security, but that the personal information of the entire chain of intermediaries right up until the "true owner" needs to be established and reported, and that it also has to be administered and safeguarded, whenever the true ownership of a security is determined.[553] This provision will necessarily complicate directors' oversight on the the administration and safeguarding of personal information even further, since the volume of PII will effectively double in the case of securities which are held by juristic persons, and because it means that companies will have to unravel the complex and intricate chain of ownership for each security.[554]

The Bill of 2021, section 2.1 will also provide clarity on the right to access companies' records.[555] It wants to amend the Act, section 26, which regulates access to company records, in order to promote transparency.[556] It will allow the public to see and copy a company's shareholder register and the register of disclosed beneficial interests of the company.[557] In this regard, it will also provide more clarity on aspects related to the register of disclosed beneficial interests, as well as beneficial holders.[558]

In terms of the Act, section 56, directors may ask the registered shareholders to reveal the identity of those for whom they hold them.[559] The proposed amendments to this section will require directors to request registered shareholders to provide the identity of the beneficial interest holders in its securities.[560] In addition, it will require directors to establish and maintain a register with the personal information of the beneficial interest holders in a company's securities.[561] It will require directors to audit the details of all beneficial interest holders in excess of 5% of the total number of shares of that class, and to then publish those names in the audited statements.[562] It will also strengthen the provisions for registered shareholders to give their personal information to companies once they hold beneficial interests in a company's shares.[563]

The Bill of 2021, section 4.13 relates to instances where directors are not able to identify the beneficial interest holders and will compel directors to disclose their accurate holdings.[564]

---

[553] SA Bill of 2021, section 4.2.
[554] *Ibid.*
[555] SA Bill of 2021, section 2.1.
[556] The Act, section 26; SA Bill of 2021, section 2.2.
[557] SA Bill of 2021, section 2.2.
[558] *Ibid.*
[559] The Act, section 56; SA Bill of 2021, section 4.4.
[560] The Act, section 56; SA Bill of 2021, section 4.4.1.
[561] SA Bill of 2021, section 4.4.2.
[562] SA Bill of 2021, section 4.4.3.
[563] SA Bill of 2021, section 4.4.4.
[564] SA Bill of 2021, section 2.3.

The Act, section 56 does not compel directors to verify the identity and to obtain the personal information of the holders of any beneficial interests.[565] This section simply states that the directors "may" request the registered or suspected beneficial interest holders to state the situation.[566] The Bill of 2021 wants to change the "may" to "must," and to thereby require the directors to collect this personal information.[567]

There are various reasons why legislative measures are required to help determine who has beneficial interests in a company.[568] Not only does the uncertainty of corporate ownership encourage fraud and tax evasion, it can also be misused for crimes such as the financing of terrorism and money laundering.[569] The board consequently need to know who the company's registered shareholders and beneficial interest holders are, in if they are juristic persons, they need to know who the beneficial interest holder is.[570]

EU countries have taken the lead in this regard, and they have already made progress with the institution of legal requirements that requires companies to disclose the names of beneficial interest holders.[571] The EU 'Fourth Anti-Money Laundering Directive of June 2017,' article 32(a), compels all EU member states to get central registers where holders can declare beneficial ownership.[572] In terms of the EU 'Fifth Anti-Money Laundering Directive of April 2018,' section 42, this information should have been reported on since 2020.[573]

The G20 'Global Framework for Tracing Beneficial Ownership' also requires members to encourage the disclosure of beneficial ownership in their legislation.[574] As a result, SA implemented the G20 'High-Level Principles on Beneficial Ownership Transparency' in 2015 to help stop the abuse of juristic persons in these regards.[575]

It is possible that ultimate beneficial ownership could be held by only one nominee or various nominees who hold smaller amounts of securities.[576] As a result, the Bill of 2021, section 4.15 distinguishes between firstly, the company who requests personal information from shareholders; and secondly, the company who reports or

---

[565] The Act, section 56; SA Bill of 2021, section 4.13.
[566] *Ibid.*
[567] SA Bill of 2021, section 4.13.
[568] SA Bill of 2021, section 4.8.
[569] *Ibid.*
[570] SA Bill of 2021, section 4.9.
[571] SA Bill of 2021, section 4.10.
[572] EU 'Directive on Anti-Money Laundering and Terrorist Financing (AMLDIV) 2015/849 of 2017,' section 32(a); SA Bill of 2021, section 4.10.
[573] EU 'Directive on Anti-Money Laundering and Terrorist Financing (AMLDV) 2018/843 of 2018,' section 42; SA Bill of 2021, section 4.10.
[574] G20 'Global Framework for Tracing Beneficial Ownership,' *s.p.*, available online at <https://www.global-solutions-initiative.org/policy_brief/a-global-framework-for-tracing-beneficial-ownership/>, last accessed on 15 June 2023; SA Bill of 2021, section 4.11.
[575] *Ibid.*
[576] SA Bill of 2021, section 4.15.

publishes the beneficial ownership information.[577] Section 4.15 requires that the information pertaining to beneficial ownership should be obtained by a company, and that the directors should only report on it in instances where single persons or together with others, are the beneficial interest holders of 5% of the shares in a class.[578]

6. LESSONS FOR SA ON THE REGULATION OF OMs IN OTHER JURISDICTIONS

There are important lessons that SA directors can learn from the other jurisdictions that were evaluated in this Chapter and that they can use. Since these lessons are influenced by established legal principles and best practices, they can help fill the gaps on how directors need to exercise their duty of care in relation to cybersecurity in order to best protect online platforms and their online databases.

6.1. US

In US Federal Law, the MBCA of 2016 states that participation by online communication is bound by the guidelines and procedures that a board decides.[579] This is an important provision, because it allows the board to set its own standard on the duty of care in relation to cybersecurity and the use of AI in its company-specific cybersecurity policy, above and beyond what legislation requires.[580]

The MBCA, section 7.09 gives the board the liberty to adopt additional guidelines and procedures on cybersecurity and the duty of care that needs to be exercised thereon.[581] Section 7.09(a) allows the board to ask shareholders their opinion when they need to choose the most efficient means of online communication.[582] This consequently presents an opportunity for the board to ensure that the cybersecurity measures that they use are in line with the IT tools that the shareholders use and require.[583]

The two parts of section 7.09(b), which set out the minimum requirements to safeguard the integrity of shareholders' meetings, are especially important, because the one part firstly requires the board to use reasonable measures to determine the identity of participants.[584] Cybersecurity demands that the identity of all participants who are

[577] SA Bill of 2021, section 4.15.
[578] *Ibid.*
[579] US MBCA of 2016, section 7.08; See Chapter 2, section 3.1.
[580] *Ibid.*
[581] US MBCA of 2016, section 7.09; See Chapter 2, section 3.1.
[582] US MBCA of 2016, section 7.09(a); See Chapter 2, section 3.1.
[583] *Ibid.*
[584] US MBCA of 2016, section 7.09(b); See Chapter 2, section 3.1.

logged in should at all times be known to the chairperson, the IT section and the auditors in order to practice access control.[585]

Although the second requirement that participants must be able to follow the proceedings as they occur, has the purpose to prevent the exclusion of shareholders from the proceedings, it indirectly also requires that directors must try to mitigate software coding errors, which cause buffering, freezing and lagging during the OM.[586]

When it comes to the US SEC, its Division of Corporation Finance and the Division of Investment Management's '*Staff Guidance for Conducting Shareholder Meetings in Light of Covid-19 Concerns*' shows what a powerful source of law, 'soft law' can be, and how even a staff statement can guide directors to fulfil their duty of care in relation to cybersecurity and the use of AI.[587] SA directors can also learn a lesson on the importance of robust disclosures, (for example on cybersecurity measures and the use of AI), and to facilitate informed shareholder attendance and participation on cybersecurity matters that affect them.[588]

Various lessons for the King Code can also be learned from US state law.

The Delawarean Example on OMs With Specific Procedures focuses mostly on the legal requirements for online participation and shows with DGCL, section 211(a)(2)(b) that the three main requirements for online participation are that (i) everyone's identity must be reasonably verified; (ii) everyone present must get a reasonable opportunity to participate, vote and to follow the proceedings as they occur; and that (iii) any decisions and votes must be recorded.[589] In this regard, the King Code should provide guidance on how the decision to hold an OM, and its cybersecurity requirements, should be taken, and whether this ability rests solely with the board, or whether shareholders/stakeholders should also be provided with an opportunity to provide their input when it comes to how they would like their PII to be protected in the online databases.[590]

The Colorado Example on OMs Without Specific Procedures focuses mostly on definitions and processes and shows that without specific definitions and prescribed procedures, attempts to guide the directors' duty of care are open to ambiguity and that it will lead to legal uncertainty.[591] This is because although section 7-107-108 makes provision for hybrid meetings, legal uncertainty still exists when it comes to OMs.[592] This section also shows that a company's MOI is a powerful tool, which can help guide the directors' duty of care in relation to cybersecurity and the use of AI, and that it can hold

---

[585] US MBCA of 2016, section 7.09(b); See Chapter 2, section 3.1.
[586] *Ibid.*
[587] US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*
[588] US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*; See Chapter 2, section 3.1.1.
[589] DGCL, section 211(a)(2)(b)(i)-(iii); See Chapter 2, section 3.2.1.
[590] *Ibid.*
[591] See Chapter 2, section 3.2.2.
[592] Colorado Revised Statutes Annotated of 2017, section 7-107-108; See Chapter 2, section 3.2.2.

directors responsible to uphold a certain standard on cybersecurity, because once a MOI sets requirements on how OMs need to be held and how the online platform and its online databases need to be secured by AI, directors then need to reasonably ensure that such requirements are adhered to.[593] It also shows that the King Code should not prescribe too strict legal provisions for the way in which OMs need to be held, but rather focus more on strict cybersecurity measures to protect online platforms and their online databases.[594] Most importantly, it shows that the requirement of audibility is good, as this safeguards shareholders against exclusion, but that it does not safeguard the online platform and its online databases.[595] In this regard, Delaware's section 211(a)(2) on the requirement to follow the proceedings as they occur is stricter as it indirectly helps to safeguard participants in terms of cybersecurity, because if participants need to follow the proceedings as they occur, it requires that additional hardware should be installed to augment the RAM in order to overcome freezing and that coding errors should be overcome by additional software, which will help to mitigate buffering, freezing and lagging.[596]

The Massachusetts and Montana Example on Limitations on Public Companies differentiates between companies and shows that Massachusetts's differentiation in its section 7.08 between public and private companies and Montana's differentiation on company size in its section 35-1-516 only unnecessarily complicates the duty of care in relation to cybersecurity, and it is not advised that the King Code differentiates along the same lines.[597] Although compliance with the King Code is compulsory to listed companies, there is no reason why public and private companies, as well as companies of all sizes, may not voluntarily use it, because cyberrisks is a challenge to all companies.[598]

The NY Example on Obligatory Shareholder Input focuses on the identification of participants and accentuates in section 602(1)(b)(i)(A) the importance that all participants must be identified.[599] Section 602(1)(b)(i)(B) again only requires decisions and votes to be recorded, but says nothing on how such decisions and votes then need to be stored securely by AI and Blockchain technology and this is an aspect that the King Code will have to address.[600] It also shows how important it is for legal clarity that the King Code should define 'online presence.'[601]

---

[593] Colorado Revised Statutes Annotated of 2017, section 7-107-108; See Chapter 2, section 3.2.2.
[594] See Chapter 2, section 3.2.2.
[595] Colorado Revised Statutes Annotated of 2017, section 7-107-108; See Chapter 2, section 3.2.2.
[596] Colorado Revised Statutes Annotated of 2017, section 7-107-108; DGCL of 2000, section 211(a)(2)(b)(i)-(iii); See Chapter 2, section 3.2.1.
[597] Massachusetts General Laws Annotated 156D of 2004, section 7.08; Montana Code Annotated of 2010, section 35-1-516; See Chapter 2, section 3.2.3.
[598] See Chapter 2, section 3.2.3.
[599] *Ibid.*
[600] NY BCL of 2010 (amended 2019), section 602(1)(b)(i)(2)(B); See Chapter 2, section 3.2.4.
[601] *Ibid.*

The California and Maryland Example on Shareholder Participation makes provision for shareholder input in how OMs are held and this shows how important shareholder input is in corporate governance processes and that provision for the input and objections on cybersecurity-related aspects should be made.[602] California's section 600 and Maryland's section 2-503(b)(2) acknowledge the importance of shareholder input in the decision to hold OMs and how the duty of care in relation to cybersecurity must be exercised and make provision for such input and objections.[603] This provides the board with the opportunity to correlate that its cybersecurity measures are synchronised and end-to-end encrypted with the IT tools that shareholders use, and to ensure that the shareholders and stakeholders are content with the way in which cybersecurity is managed.[604]

The lesson that can be learned from the Illinois Example on No OMs is that the King Code should be applicable to hybrid meetings as well, so that it can accommodate instances where companies' MOIs have not been changed to accommodate OMs.[605]

From the NYSE, the King Committee should learn that additional measures on the duty of care in relation to cybersecurity, which are of a temporary nature, could be issued in future to supplement the King Code, should the need ever arise.[606] In addition, should SA Lockdown levels ever increase again in future, the King Committee could approach the JSE with a request to provide temporary relief for OMs, similar to the NYSE's '*Listed Company Compliance Guide,*' or to provide guidance on matters pertaining to the use of Blockchain technology to record online votes and resolutions.[607] The King Committee should also keep in mind that Blockchain technology requires specific cybersecurity measures and that it should include guidance on how directors need to exercise their duty of care in relation to cybersecurity on this complex field of AI.

6.2. UK

Various lessons for the King Code can also be drawn from the UK's legal sources.

The lesson from the EU 'Directive on the Encouragement of Long-Term Shareholder Engagement of 2017' again confirms that the King Code will have to provide guidance to directors on how they need to oversee AI in instances where

---

[602] See Chapter 2, section 2.2.5.
[603] California Corporations Code of 2009, section 600; Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(b)(2); See Chapter 2, section 3.2.5.
[604] *Ibid.*
[605] Illinois Compiled Statutes Annotated 805 of 1983, section 5/7.05; See Chapter 2, section 3.2.6.
[606] See Chapter 2, section 3.3.
[607] NYSE '*Listed Company Compliance Guidance' op cit s.p.*

companies require or send shareholders' personal information by means of Blockchain technology to a central securities depository.[608]

The UK Companies Act of 2006 (Ch.46) shows that the King Code should not make the same mistake as the UK Companies Act of 2006, section 311, which does not clearly define 'place of meeting.'[609] It should clearly define the "place of meeting" so as to include cyberspace in order to accomodate OMs, because otherwise the "place of meeting" is left open to interpretation, and this could lead to uncertainty on whether the duty of care in relation to cybersecurity is also required on the physical aspects pertaining to a hybrid meeting.[610] The interpretation of aspects related to the duty of care in relation to cybersecurity will not be facilitated if instances of amibiguity or legal uncertainty exist in the King Code.[611] In addition, section 311 shows that the King Code should also encourage companies to use their MOIs to help set requirements on the duty of care in relation to cybersecurity and the use of AI to protect online platforms and their online databases.[612] The King Code should follow the lesson of section 360A(1), which states that nothing in the Act may be interpreted in a way that will cause participants of a shareholders' meeting who are not present, to not attend, speak or vote online, but that this right should not be unqualified, and should be made subject to the requirement that a participant must first properly identify themself as a registered shareholder/stakeholder.[613] The requirements of section 360(A)(2) is important because it determines that OMs may be subject only to such requirements that are (a) needed to identify the participants; and that (b) the cybersecurity measures for online communications must be reasonable.[614] As a result, this places only the requirement to identify themselves on shareholders.[615] This effectively places the entire responsibility to protect the integrity of the OM, the online platform and its online databases on the board, as no requirement is placed on shareholders to adhere to, or implement, any online security protocol, such as end-to-end encryption.[616] The other requirement is that the cybersecurity measures must be reasonable.[617] No guidance is however given on what would constitute reasonable cybersecurity measures in terms of the responsible

[608] EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017' *op cit* section 4; See Chapter 2, section 4.1.
[609] UK Companies Act of 2006 (Ch. 46), section 311.
[610] *Ibid.*
[611] UK Companies Act of 2006 (Ch. 46), section 311; Coen *op cit s.p.*; See Chapter 2, section 4.2.
[612] *Ibid.*
[613] UK Companies Act of 2006 (Ch. 46), section 360A(1); See Chapter 2, section 4.2.
[614] UK Companies Act of 2006 (Ch. 46), section 360A(2)(a)-(b); See Chapter 2, section 4.2.
[615] UK Companies Act of 2006 (Ch. 46), section 360A(2)(a); See Chapter 2, section 4.2.
[616] *Ibid.*
[617] UK Companies Act of 2006 (Ch. 46), section 360A(2)(b); See Chapter 2, section 4.2.

use of AI.[618] In addition, the King Code should follow section 360A(3) and advise a company to reasonably require proof of identity of a proxy.[619]

The UK CIGA of 2020 shows that it is a pity that the SA government was not as pro-active and did not promulgate similar relief in nature to CIGA to provide companies with an extended period to hold shareholders' meetings during the Pandemic.[620] Such an extended period to hold shareholders' meetings would have been of great assistance to SA directors to get the necessary cybersecurity policies and systems in place, as UK directors were essentially given the opportunity to decide how to best conduct and secure their OM, in terms of the prescribed measures.[621] Not only were these measures helpful for companies with upcoming shareholders' meetings, but it also allowed companies to amend their MOIs to allow the use of AI for cybersecurity and to get the necessary cybersecurity policy and system in place to ensure that they were able to conduct secure OMs in future.[622] These measures in other words provided the opportunity for directors to switch to OMs, and as a result, also served as a catalyst for directors to start exercising their duty of care in relation to cybersecurity. The SA government should take cognisance of this pro-active drive to help proliferate OMs and their cybersecurity.[623] At the same time, the King Committee should take note that CIGA contained an oversight due to its omission to not actively encourage directors to use AI to safeguard the online platform and its online databases, nor to use Blockchain technology to secure online voting and to secure resolutions on the central securities depositry.

The UK Department for Business, Energy and Industrial Strategy's '*Memorandum of 2020*' shows that the King Code should encourage the board to reply on questions before voting, as this would allow shareholders to raise concerns beforehand on cybersecurity and it is important that answers on any questions in this regard must be provided to all participants, before, during and after an OM.[624]

The UK Chartered Governance Institute's '*Guidelines of 2020*' show what an important role corporate governance institutes can play to provide guidance on cybersecurity matters.[625] The King Committee should have issued similar detailed guidance to help guide SA directors on how they should exercise their duty of care in relation to cybersecurity and the use of AI, especially to accompany the JSE online platform after it was unveiled.[626]

---

[618] UK Companies Act of 2006 (Ch. 46), section 360A(2)(b); See Chapter 2, section 4.2.
[619] UK Companies Act of 2006 (Ch. 46), section 360A(3); See Chapter 2, section 4.2.
[620] UK CIGA of 2020; Steeden *et al. op cit s.p.*; See Chapter 2, section 4.3.
[621] Simmons & Simmons *op cit s.p*.
[622] UK CIGA of 2020, Schedule 14, rule 2(1); UK CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021, section 2; Steeden *et al. op cit s.p.*; See Chapter 2, section 4.3.
[623] See Chapter 2, section 4.3.
[624] UK Department for Business, Energy and Industrial Strategy *op cit* 7-8; See Chapter 2, section 4.4.
[625] UK Chartered Governance Institute's '*Guidelines of 2020*' *op cit s.p.*; See Chapter 2, section 4.5.
[626] *Ibid.*

Lastly, is it interesting to note that both the LSE and the JSE took pro-active approaches in this regard, but the JSE can be commended that it went even further when it devised its own online platform.[627]

6.3. SA

The focus on SA's legal sources, helped to show how OMs are currently regulated and helped to show how directors should exercise their duty of care in relation to the cybersecurity of OMs in order to best protect the online platform and its online databases.

The requirements of the Act have certain consequences that directors need to abide by, and which the King Code wil have to highlight: they firstly need to adhere to the Act, section 61(10)'s provision on accessibility, which requires shareholders' meetings to be reasonably accessible for online participation by shareholders, regardless of whether they are held in SA or elsewhere.[628] This provision has dual consequences for how SA directors need to exercise their duty of care in relation to cybersecurity: firstly, it compels companies to have at least hybrid meetings, and that companies also need to have the necessary cybersecurity and physical access control measures in place for hybrid meetings.[629] The requirement that OMs must be reasonably accessible for online participation, regardless of whether they are held in SA or elsewhere, effectively places another requirement on directors.[630] As a result, this means that directors will also need to ensure that their companies improve their cybersecurity systems' cyberresilience to thwart cyberrisks that originate from outside the borders of SA.[631] In this regard, the King Code should provide a definition for "reasonably accessible" and examples of it.[632] This is required because different access points and portals to OMs all require different security protocols, which require their own cybersecurity measures.[633]

In the second instance, the enabling provision of section 63(2) states that if a company's MOI does not prevent OMs, it may conduct (a) a shareholders' meeting entirely online; or (b) one or more participants, may participate online in the physical shareholder's meeting, as long as the online communication allows everyone to communicate effectively and simultaneously with one another without an intermediary.[634] It was explained that the requirement to communicate simultaneously

---

[627] Clark op cit s.p.; See Chapter 2, section 3.6.
[628] The Act, section 61(10); See Chapter 2, section 5.1.
[629] *Ibid.*
[630] *Ibid.*
[631] *Ibid.*
[632] *Ibid.*
[633] *Ibid.*
[634] The Act, section 63(2)(a)-(b); See Chapter 2, section 5.1.

indirectly helps to mitigate the software coding errors, which causes buffering, freezing and lagging, and that the King Code should highlight its importance.[635]

The prohibition of section 63(2)(b) on the use of intermediaries in the online communication between shareholders/stakeholders and the company is a unique provision when compared to other legislation, and the King Code should thirdly set out examples of what it entails, and that the use of AI in the form of chatbots as intermediaries during the OM is a forbidden practice.[636]

When it comes to the requirement to communicate without intermediaries, research by Just Share shows that some of SA's blue-chip companies use AI to moderate questions before they reach the board.[637] Particularly worrisome in this regard is the description of the JSE's partner in the online platform, TMS, where it states on its website under 'mobile meeting services' that it allows questions, which are sent to the board, to be moderated.[638] Some large SA companies, such as Exxaro SA and Old Mutual, have held their OMs via TMS.[639] If any of the questions that were sent to the board were moderated, it would be in conflict with section 63(2), which requires shareholders to pose their questions to the board without moderation.[640]

The JSE online platform is not the only OM service provider who allows this to happen.[641] Remgro's '*OM Shareholders' Guide 2020*' clearly states that "Questions sent via the Lumi online platform will be moderated before being sent to the chairperson. This is to avoid repetition and remove any inappropriate language".[642] This conflicts with section 63(2) and creates the potential to avoid accountability and infringes the shareholders' right to speak freely.[643] In addition it creates external interference in the OM that could lead to a cybersecurity loophole. Section 63(2) allows shareholders to send their questions directly to the board, and that they must then answer it without any moderation, and that shareholders must not be forced to submit their questions in writing before a meeting starts.[644] If an OM does not allow shareholders to interact directly with the board it serves no purpose, because nothing prevents shareholders from sending their written questions to the board whenever they want to.[645] The King Code will need to explain to directors that AI intermediaries cannot be used to interpret

---

[635] The Act, section 63(2)(b); See Chapter 2, section 3.1.
[636] The Act, section 63(2)(b); See Chapter 2, section 5.1.
[637] Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act' op cit s.p*.
[638] TMS '*The Meeting Specialist (Pty) Ltd' op cit s.v.* 'mobile meeting services.'
[639] Old Mutual *op cit* 1; Exxaro *op cit* 50.
[640] Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p*.
[641] Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act' op cit s.p*.
[642] Remgro Ltd *op cit* 2.
[643] The Act, section 63(2); Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act' op cit s.p*.
[644] The Act, section 63(2); Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p*.
[645] *Ibid*.

and reply on shareholders' questions, since the Act basically sees this as external inference with the online proceedings.[646]

With regards to the notice requirements of section 63(3)(a), the OM notice will have to fourthly, provide the necessary online access information upfront to enable participants to access the OM.[647] It is submitted that the online access information should explain that the necessary security protocols and encryption is in place to secure the OM. Should browser, dial-in or weblink details be recorded incorrectly on the notice or if the web-link on a notice does not lead to the online platform, or if it has unsecured online security protocols, and if it is not properly encrypted, it could render the entire OM null and void, and provide an opportunity for cybercriminals to exploit. Besides the need to provide a secured weblink, which is properly end-to-end encrypted to access the OM, the company must also provide a unique username and pin number for each participant to access the OM.

Lastly, with regards to the expense requirement of section 63(3)(b), it is required that the notice mentions that the costs of the online communication is to be borne by the participant, unless the board decides something else.[648] This section only relates to the cost of online communication and makes no mention of any cybersecurity responsibilities that a shareholder may have (for example, that their access device needs to be encrypted), and effectively places all of the responsibility for the cybersecurity of the entire OM on the board.

In addition, since King Report IV, principle 12 recommends that boards exercise ongoing oversight over IT management, to a point that it results in the ethical and responsible usage of IT, so the King Code will need to detail this with examples and recommendations on best practices on what is deemed the ethical and responsible usage of AI, otherwise it will remain a hollow principle, which is open to interpretation.[649]

Also, in accordance with the JSE '*Listing Requirements*,' section 1.28, which sets out the rules that any listed company will need to comply with if they want to be be listed on the JSE and have their shares traded publicly, directors will have to exercise their duty of care in relation to cybersecurity responsibly when they oversee the use of Blockchain to store shareholders' personal information on the central securities depository, if they want their company's shares to be listed on the JSE.[650]

7. CONCLUSION

[646] The Act, section 63(2)(b); See Chapter 2, section 5.1.
[647] The Act, section 63(3)(a).
[648] The Act, section 63(3)(b).
[649] IoDSA '*King Report IV' op cit* principle 12; See Chapter 2, section 5.2.
[650] JSE '*Listing Requirements,'* section 1.28; See Chapter 2, section 5.3.

Chapter 2 evaluated how OMs are regulated by law, and how these regulatory frameworks and legislative requirements, which other jurisdictions have in place, helps to protect the integrity of the OM, as well as the cybersecurity of its online platform and its online databases, in order to infer lessons for how SA directors need to exercise their duty of care in relation to cybersecurity and the use of AI.

It started with OMs in the US and it was explained that federal US Securities Law do not prescribe how companies should conduct shareholders' meetings and that the US has no uniform model and that its states' law follows six different examples on OMs, ranging from the Delawarean Example, where OMs are regulated with specific procedures, to the Illinois Example, which does not make provision for OMs.

An important development was the US SEC's Division of Corporation Finance and the Division of Investment Management's '*Staff Guidance for Conducting Shareholder Meetings in Light of COVID-19 Concerns*' of April 2020.[651] It was explained that this unofficial statement is virtually the guideline on US OMs to directors and this shows the King Committee how advantageous corporate governance guidance on matters such as the way in which the duty of care in relation to cybersecurity and the use of AI can be.[652]

Thereafter the UK position was looked at and it was explained that OMs have been allowed since the UK Companies Act of 2006 (Ch.46), section 360A was amended by the UK Companies (Shareholder Rights) Regulations of 2009.[653] The temporary UK Companies Act dispensation that was introduced by UK CIGA in June 2020 allowed companies to hold OMs and it was extended by the UK's 'CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021' until 30 March 2021.[654] It was pointed out that unfortunately the SA government did not take such a pro-active stance to provide temporary relief in this regard, but that it needs to take cognisance of it for future reference in order to present an opportunity for OMs to proliferate in SA.

The regulation of OMs in SA was also looked at and the aspects related to the duty of care in relation to cybersecurity and the protection of the integrity of an OM, as well as the cybersecurity of its online platform and its online databases, were outlined. The impact of especially the Act, section 63(2)(b), which compels companies to allow participants to communicate simultaneously and reasonably effectively with one another without an AI intermediary, was highlighted.[655]

Lastly, the lessons that the King Committee can infer from the different legal jurisdictions on how OMs are regulated and how the duty of care in relation to cybersecurity needs to be exercised, were explained.

Now that there is a better understanding on how OMs function and how they are regulated, and how their integrity should be preserved, it is possible to look in the

---

[651] US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*
[652] *Ibid.*
[653] UK Companies Act of 2006, section 306A; Coen *op cit s.p*.
[654] UK CIGA of 2020; UK CIGA Coronavirus Extensions of Relevant Periods Regulations of 2021, section 2.
[655] The Act, section 63(2)(b).

following chapters how directors should exercise their duty of care in relation to cybersecurity on OMs in order to best protect the online platform and its online databases.

While the focus in Chapter 2 fell on the lessons for directors on the regulation of OMs in other jurisdictions, Chapter 3 will look at the duty of care in relation to cybersecurity in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted.

CHAPTER 3:

THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY

1. INTRODUCTION

While the focus in Chapter 2 fell on the lessons on the regulation of OMs in other jurisdictions in order to best protect the integrity of OMs, as well as the cybersecurity of their online platform and their online databases, Chapter 3 will look at the duty of care in relation to cybersecurity. In Company Law, the duty of care is the moral or legal obligation of directors to ensure the safety and well-being of others.[656] This means that directors have a duty to ensure the cybersecurtity of the OM and the online platform and its online databases, in order to protect the privacy and/or personal information of the shareholders and stakeholders that were entrusted to them. This chapter will consequently place a specific focus on the UK and US positions on the duty of care in relation to cybersecurity in order to contrast it to the SA position by means of a legal comparison. The remedies for directors who breached their duty of care in relation to cybersecurity will be evaluated; and the position of non-executive directors will also be looked at.

This Chapter will therefore evaluate the SA, UK and US legal positions in order to identify existing gaps, look for mutual traits, and determine how these jurisdictions bridge those gaps, in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted.

2. THE DIRECTORS' DUTY OF CARE IN SA

Six SA legal sources constitute the SA legal regime on the duty of care in relation to cybersecurity, namely common law, the Constitution, the Act, SA POPI 4 of 2013, the King Reports I – IV and case law.

2.1. Common Law

SA Company Law on the directors' duty of care was shaped by English law.[657] As in the UK, SA company law requires a standard of reasonable care.[658] As such, the duty of care initially espoused a conservative approach by using a subjective test when

---

[656] Deloitte '*Duty of Care*' *op cit* 3.

[657] Blackman *et al. op cit* 8-29; Delport *Henochsberg on the Companies Act et al. op cit* 288; Maharaj *A Discussion on the Duty of Care, Skill and Diligence to be Exercised by a Director in Light of the Companies Act 71 of 2008, as well as the Common Law and an Overview of the BJR: A Company Law Perspective* 20.

[658] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 137.

directors' fault had to be determined.[659] British common law and SA common law traditionally set a low standard of care on directors due to the *laissez-faire* principle.[660] As a result, directors were allowed to oversee companies ineffectually, simply because the courts followed a 'hands-off' approach on the way in which directors oversaw their companies.[661]

Over time, the common law developed to require directors to perform their duties with the standard of care that could be expected from someone with similar experience and skills and started to include the need to exercise care, skill and diligence.[662] This means that as soon as directors do not perform their duties with care, they could be held liable for the damage or loss that the company has suffered due to such in/action.[663]

The liability of directors is delictual and sometimes it also derives from contractual breach.[664] In 1995, Friedman JP of the Cape Provincial Division of the SA High Court held in *Du Plessis NO v Phelps* that when a director did not oversee a company with due care, the *Lex Aquilian* principles will determine liability.[665] The *Lex Aquilian* principles base liability on fault, which either derives from *dolus* or *culpa*, and that caused loss or damage to a plaintiff.[666]

In order for an affected party to prove negligence in terms of delictual law, the five elements of a delict need to be proven, namely harm caused to the plaintiff, conduct by the defendant that was wrongful, together with a causal link between the conduct of the defendant and the harm caused to the plaintiff and lastly, fault on the side of the defendant.[667]

Although directors owe their duty of care to the company, and not to the shareholders, boards need to protect the company's cyberassets, such as its online platform and its online databases, against cyberbreaches in terms of its common law duty of care, otherwise the shareholders/stakeholders will hold them directly liable for any violations of their privacy and/or personal information, if a cyberbreach occurs which could have been prevented.[668]

---

[659] Delport *Henochsberg on the Companies Act et al. op cit* 296, note 16; Stevens 'The Legal Nature of the Duty of Care and Skill: Contract or Delict?' in *Potchefstroomse Elektroniese Regsblad* 2017 (20) 17; Maharaj *op cit* 20.
[660] Maharaj *op cit* 20.
[661] *Ibid*.
[662] Cassim *et al. Contemporary Company Law op cit* 747 - 751; Werksmans '*Duties and Liabilities of Directors,*' 3, available online at <https://www.werksmans.com/wp-content/uploads/2013/04/Director-duties-and-liabilities-FINAL-updated-electronic.pdf>, last accessed on 3 February 2022.
[663] Kanamugire *et al. op cit* 71.
[664] *Ibid*.
[665] *Du Plessis NO v Phelps* 1995 (4) SA 165 (C).
[666] *Ibid*.
[667] Neethling *et al. Deliktereg* 25
[668] The Act, section 76(3)(c); IoDSA 'King Report IV' *op cit* principle 12.

The duty to perform care and skill requires a director to perform all of their functions with due care and skill.[669] This duty therefore has two aspects, namely to act with a degree of skill and to act with a degree of care.[670] The degree of skill does not require that a director needs to perform a level of skill which they do not possess.[671] The degree of skill that is needed is subjective.[672] A director's performance will in other words be evaluated by the manner in which they performed their care.[673] In the case of cybersecurity, a director will be held personally liable – even if they know nothing of cybersecurity, but did not seek expert advice.[674]

The fact that directors could be held personally liable – even if they know nothing of cybersecurity, but did not seek advice on it – is quite problematic, because without any industry standards or recommendations on what constitutes proper cybersecurity and the use of AI, any advice that was sought, even if it does not conform to industry standards, will suffice to fulfil this requirement.

2.1.1. Common Law Negligence and the Duty of Care

In the Roman Dutch law, which serves as the basis for the SA law of delict, negligence is determined by means of the reasonable person test that evaluates whether a reasonable person in similar circumstances would have foreseen the harm that was caused by a cyberbreach and could have prevented it.[675]

Instead of determining negligence simply by means of this reasonable person test, some SA courts, due to the influence of English law, have over time, started to use the duty of care principle to determine negligence.[676] An example of this approach that is followed by the English courts will follow later in this Chapter in the section under UK case law, where it will be explained how Lord Bridge of the House of Lords applied this test in 1990 in *Capraro Industries PLC supra.*[677]

In terms of this approach, which is followed in English law, and that has influenced SA law, it has happened in the past that SA courts sometimes used the foreseeability test (which in terms of the Roman Dutch law is used to determine neligence) to determine whether the duty of care was breached.[678]

---

[669] The Act 71 of 2008, section 76(3)(a)-(c); Norton Rose Fulbright SA '*Duties and Responsibilities of Company Directors,' s.p.,* available online at <https://www.mondaq.com/southafrica/contracts-and-commercial-law/35736/duties-and-responsibilities-of-company-directors>, last accessed on 25 May 2020.
[670] *Ibid.*
[671] *Ibid.*
[672] *Ibid.*
[673] The Act 71 of 2008, section 76(3)(a)-(c); Norton Rose Fulbright SA *op cit s.p.*
[674] *Ibid.*
[675] Midgley *et al. Principles of Delict* 80.
[676] *Ibid.*
[677] *Capraro Industries PLC v Dickman* (1990) ALL ER 568; See Chapter 3, section 3.5.
[678] Neethling *et al. Deliktereg op cit* 144.

An example of this occurred in 1923, when Innes J of the Cape High Court in *Cape Town Municipality v Paine* used the foreseeability criteria to determine whether someone, who was in the position of the defendant, and who a had a duty to exercise care, could have foreseen that his action would cause harm to the plaintiff.[679]

In terms of the Roman Dutch law, the correct approach is to determine whether a legal duty of care was breached in terms of wrongfulness as an element of delictual liability, and not that of negligence.[680]

In 1979, Mostert, J of the Natal Provincial Division made it clear in *Administrateur, Natal v Trust Bank van Afrika, Bpk* that when due care needs to be determined, foreseeability plays no role, and that the focus should be placed on the protection of interests against a negligent act.[681] Mostert J explained that the duty of care has nothing to do with reasonable foresight, and that it is instead focused on interests which the law wants to protect against negligence.[682]

This approach that was influenced by the English law, where the duty of care was sometimes used by SA courts to determine negligence, instead of the reasonable person test, is novel to the Roman Dutch law, which forms the basis of the SA law on delict.[683] Objection can thus be made against the application of the duty of care to determine negligence in SA law.[684] A more important objection is that it is an unnecessary and more complicated method to determine what should instead directly be determined by the reasonable person test for negligence.[685] In addition, the use of the duty of care to determine negligence can lead to confusion between the test for wrongfulness (to determine the breach of a legal duty) and that of negligence.[686]

In 1966 Holmes JA of the Appeal Court explained in *Kruger v Coetzee* that there exists no reason why the duty of care needs to be used in SA to determine negligence, and that courts should simply use the reasonable person test.[687] In 1995, Botha JA of the Transvaal Supreme Court also explained in *Knop v Johannesburg City Council* that the duty of care should only be used to determine whether a legal duty was breached, and not to determine negligence.[688] He also explained that the breach of the duty of care needs to be determined in accordance with the requirement of wrongfulness as an element of delictual liability, and not that of negligence.[689] Likewise, in 2005 Brand, JA of the SA Supreme Court of Appeal (SCA) explained in *Local Transitional Council of*

---

[679] *Cape Town Municipality v Paine* 1923 AD 207.
[680] *Knop v Johannesburg City Council* 1995 2 SA 1 (A).
[681] *Administrateur, Natal v Trust Bank van Afrika, Bpk* 1979 3 SA 824 (A).
[682] *Ibid.*
[683] Neethling *et al. Deliktereg op cit* 145.
[684] *Ibid.*
[685] *Ibid.*
[686] *Ibid.*
[687] *Kruger v Coetzee* 1966 2 SA 428 (A).
[688] *Knop supra*.
[689] *Ibid*.

Delmas v Boshoff that the legal duty of care has nothing to do with fault (negligence).[690] He warned that it must not be confused with the duty of care in English law, which is used to determine negligence.[691]

In other words, in an attempt to prevent confusion, SA courts need to determine separately whether the legal duty of care was breached; and if that is the case, only thereafter apply the negligence test.[692]

Unfortunately, some important findings, such as those made in 1995 by Hefer, J of the SA SCA in *Government of the RSA v Basdeo*, and in 1997 by Joubert JA of the Witwatersrand Division of the Transvaal High Court in *Faiga v Body Corporate of Dumbarton Oaks*, and by Lewis JA of the SA SCA in 2003 in *Premier, Western Cape v Faircape Property Developers (Pty) Ltd* were opportunities for the court to end the legal uncertainity, but instead only further contributed to the confusion, when the court again mixed up the two different approaches to wrongfulness and negligence to the duty of care principle.[693]

In 1992, Corbett, CJ of the Appeal Court explained in *Simon's Town Municipality v Dews* that when this happens, the modern distinction in the law of delict between fault and wrongfulness gets clouded.[694] He said that in such instances the theoretical underpinnings of the law of delict in SA is undermined and that this contributes to legal uncertainty.[695]

Hopefully, the uncertainty will be cleared up in future.[696] Unless this happens the two different approaches to the duty of care principle – the right one and the wrong one – will continue to reflect in SA case law.[697]

The court should thus explain that the directors' duty of care in relation to cybersecurity should, in terms of Roman Dutch law, be more properly referred to as a 'legal duty' and not as a means to determine negligence.[698] In addition, it should explain that the breach of the duty of care in relation to cybersecurity needs to be determined in accordance with the requirement of wrongfulness as an element of delictual liability, and not that of negligence.[699] It should also state that the breach of the duty of care in

---

[690] *Local Transitional Council of Delmas v Boshoff* (2005) 5 SA 515 (SCA).
[691] *Ibid.*
[692] Neethling *et al. Deliktereg op cit* 145.
[693] *Faiga v Body Corporate of Dumbarton Oaks* 1997 2 SA 651 (W); *Government of the RSA v Basdeo* 1996 1 SA 355 (A); *Premier, Western Cape v Faircape Property Developers (Pty) Ltd* 2003 6 SA 13 (SCA); Neethling *et al.* 'Statutêre Bevoegdheid: Die Rol van Redelike Voorsienbaarheid by Onregmatigheid en Nalatigheid' in *Obiter* (2004) 483 – 485.
[694] *Simon's Town Municipality v Dews* 1993 1 SA 191 (A).
[695] Neethling *et al. Deliktereg op cit* 146.
[696] *Ibid.*
[697] *Ibid.*
[698] *Knop supra.*
[699] *Ibid*.

relation to cybersecurity must not to be confused with the duty of care in English law, which is used to determine negligence.[700]

The court should thus explain that the correct approach to determine whether the duty of care was breached in the event of a cyberbreach, would be to do so in terms of the requirement of wrongfulness as an element of delictual liability.[701] Only thereafter can the court apply the negligence test and determine whether a reasonable person in similar circumstances as the relevant director would have foreseen the harm that a cyberbreach of the online platform and its online databases could cause to shareholders/stakeholders' privacy and/or personal information and whether they would have prevented it by exercising their duty of care in relation to cybersecurity properly.[702]

2.2. SA Constitution of 1996

In terms of section 2 of the Constitution, it is the supreme law, and section 7(2) requires the state to fulfil, promote, protect and respect the Bill of Rights.[703] Section 8 binds the Constitution on state and non-state actors.[704] Section 10 also guarantees the right to human dignity and requires everyone's dignity to be protected.[705]

The right to privacy is guaranteed in section 14, which says that each person has a right to privacy.[706] Section 14(d) specifically states that it consists of the right not to have one's communications violated.[707]

In 1996, both Harms, JA of the SCA in *National Media v Jooste*, and Ackermann, J of the CC in *Bernstein v Bester* accepted Neethling's definition of privacy, which explains it as a condition where humans are allowed to seclude themselves from the public and the public gaze.[708] The concept embraces all those personal facts which such a person wishes to exclude from others and that they want to keep private.[709]

Ackermann, J explained in *Bernstein supra* that in terms of a legitimate expectation, the right to privacy can reasonably be assumed in a person's inner sanctum.[710] In 2000, Langa, DP of the CC explained in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* that a legitimate expectation of privacy will fade as a person interacts more and more with the world; and

---

[700] *Local Transitional Council of Delmas supra*.
[701] *Knop supra.*
[702] Midgley *et al. op cit* 80.
[703] SA Constitution, sections 2; 7(2).
[704] SA Constitution, section 8.
[705] SA Constitution, section 10.
[706] SA Constitution, section 14.
[707] SA Constitution, section 14(a)-(d).
[708] *Bernstein v Bester* 1996 2 SA 751 (CC); *National Media Ltd v Jooste* 1996 3 SA 262 (A); Neethling *et al. Neethling on Personality Rights* 45.
[709] *Ibid.*
[710] *Bernstein supra* par. 67.

this was confirmed in 2019 by Mogoeng, CJ of the CC in *Centre for Child Law v Media 24 Limited*.[711] In this regard, Mogoeng CJ explained that the right to privacy is based on a reasonable expectation of what a person can subjectively expect of privacy to be objectively reasonable.[712]

As it was influenced by the SA Constitution of 1996, the preamble of the SA POPI 4 of 2013 makes it clear that the right to privacy requires that data subjects need to be protected against the misuse of their personal information; and as such, the processing of personal information could threaten the right to privacy.[713] As a result, the legislature promulgated the SA POPI 4 of 2013 to set out principles in relation to the collection, processing, used, store and destroying of personal information.[714]

The SA Constitution of 1996, section 36 determines that the application of the Bill of Rights can be limited by a law that is generally applicable, if it is justifiable and reasonable in a democratic and open society.[715]

2.3. The Act

The Act enacted the common law and codified directors' duties.[716] The Act, section 76 regulates the standard with which directors need to exercise their duty of care and not only codified their common law duty of care, but also increased it by requiring them to act honestly, in good faith and in a way that they reasonably deem to be in the company's best interests.[717]

The Act took the common law subjective approach, and qualified it with an objective approach, when it codified the directors' duty of care, together with the duties of diligence and skill.[718] The duty to practice care and skill thus originates from the common law, and although it is now codified by the Act, section 76(3), the common law is still applicable.[719]

Not only did the Act codify the common law duties of directors and added a few aspects, it also increased the accountability of directors to the shareholders.[720] Section 76(3)(a)-(c) extends the standard of conduct further than the common law duty of

---

[711] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) par. 15; *Centre for Child Law v Media 24 Limited* 2020 4 SA 319 (CC) par. 45.
[712] *Centre for Child Law supra* par. 45.
[713] SA POPI 4 of 2013, preamble; Neethling 'The Concept of Privacy in South African Law' in *SA Law Journal* (2005) 20; Swales 'The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock' in *Potchefstroomse Elektroniese Regsblad* 25(1) 2002 5.
[714] Swales *op cit* 5.
[715] SA Constitution, section 36.
[716] The Act, section 76.
[717] *Ibid.*
[718] Delport *et al. Henochsberg on the Companies Act op cit* 298; Kanamugire *et al. op cit* 73.
[719] The Act, section 76(3); Blackman *et al. op cit* 8-29; Delport *et al. Henochsberg on the Companies Act op cit* 298; Kanamugire *et al. op cit* 71.
[720] Blackman *et al. op cit* 8-29.

directors by requiring them to act in good faith, honestly and in a way which they reasonably believe is in the best interests of their company.[721] Section 76(3) determines that directors need to perform their functions (a) in good faith and for a proper purpose; (b) in the company's best interests; (c) and with the degree of care, skill and diligence that one can reasonably expect from (i) someone in a similar position; and who (ii) has similar experience and skills.[722]

The requirement of diligence in section 76(3)(c) is a new addition to the common law duties of care and skill.[723] Diligence requires directors to perform their duty of care with attention and caution.[724] A diligent director will regularly attend meetings, pay attention to agendas, minutes and reports and gain insight into a company's cybersecurity situation.[725] Directors could use AI to improve their duty of care in relation to cybersecurity and it could help to improve their diligence, when it helps to make notes during OMs, schedule and prepare report for follow-up OMs.

Section 76(3)(c) codified in part the common law duty of care, together with the Act's objective approach, and as a result the duty of care consists of both objective and subjective parts.[726] Section 76(3)(c)(i) contains the objective part, which directors need to adhere to in order to meet the threshold so as to not be held liable for a breach of due care.[727] Section 76(3)(c)(ii) again contains the subjective part, which relates to the experience of the relevant director.[728] By including the objective part in section 76(3)(c)(i), this sub-section lessened the common law subjective test, which was characterised by the hands-off approach.[729]

The Act enhanced the common law position on the duty of care and skill and sets a stricter standard of care that is not as subjective.[730] The enactment of the common law and its upgrade to a stricter approach is a reflection of the international trend to improve corporate governance and to hold directors more accountable – also when it comes to oversight on cybersecurity.[731]

Since the common law duty of care is partially codified, there is a need for a clear explantion of the nature of the interaction between the legislative and common law

---

[721] The Act, section 76.
[722] The Act, section 76(3)(a)-(c)(ii).
[723] Blackman *et al. op cit* 8-29.
[724] *Ibid*.
[725] *Ibid.*
[726] The Act, section 76(3)(c)(i)-(ii); Delport *et al. Henochsberg on the Companies Act op cit* 298.
[727] *Ibid*.
[728] *Ibid*.
[729] The Act, section 76(3)(c); Cassim *et al. Contemporary Company Law op cit* 750 - 753; Delport *et al. Henochsberg on the Companies Act op cit* 298.
[730] The Act; Delport *et al. Henochsberg on the Companies Act op cit* 296, note 16; Kanamugire *et al. op cit* 73.
[731] Cassim *et al. Contemporary Company Law op cit* 750 - 753; Delport *et al. Henochsberg on the Companies Act op cit* 298; Sutherland 'The State of Company Law in SA' in *University of Stellenbosch Law Review* 2012(1) 172.

duties of care when they need to be interpreted.[732] Otherwise, it will remain open to interpretation whether the legislative duty of care is superior to the common law duty of care.[733] This is the result of an oversight by the SA legislature, who was supposed to have provided guidance on the matter beforehand either in the Act itself or in explanatory notes, which could have been issued with the Act, like in the case of the UK Companies Act of 2006.[734]

In contrast to the UK Companies Act of 2006, the Act does not provide guidance on the exact nature of the interaction between the legislative and common law duties of care.[735] The Act, section 76(3)(c) followed the example of the UK to codify the common law duty of care, as it is contained in the UK Companies Act of 2006, section 174.[736] The standards of the legislative duty of care of the UK Companies Act of 2006, section 174 is explained clearly, while the similar standards of the Act, section 76(3)(c) are not as clearly explained.[737] There is still ongoing debate whether the standards in the Act, section 76(3)(c) are both objective and subjective as is the case with the UK Companies Act of 2006, section 174, or whether it is either objective or subjective.[738]

As a result, there is still uncertainty on whether the Act, section 76(3)(c) contains a reasonable person test or not.[739] Although the Act, section 76(3)(c)(i) contains an objective standard, section 76(3)(c)(ii) seems to subject this standard by saying that the director only needs to act according to the skill and experience of that specific director.[740] This could potentially subject the objective standard of care to the subjective standard of the common law.[741] In '*Company Directors,*' the UK Law Commission pointed out that the standard of care also requires greater clarity in UK law in this regard.[742] It also explained that the approaches are both objective and subjective and that the common law should be used to interpret the wording of the UK Companies Act of 2006, section 174.[743] This explanation facilitates the notion that the wording of the UK Companies Act of 2006, section 174(2) does not undermine the objective standard in section 174(1).[744]

---

[732] The Act, section 76(3)(c); legislation.gov.uk '*Companies Act of 2006: Explanatory Notes,*' available online at <https://www.legislation.gov.uk/ukpga/2006/46/notes/division/6/4>, last accessed on 11 October 2022
[733] *Ibid.*
[734] The Act; UK Companies Act of 2006; legislation.gov.uk *op cit* section 174.
[735] legislation.gov.uk *op cit* section 174.
[736] The Act, section 76(3)(c); UK Companies Act of 2006, section 174.
[737] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; Cassidy 'Models for Reform: The Directors' Duty of Care in a Modern Commercial World' 3(2009) *Stellenbosch Law Review* 385.
[738] *Ibid*.
[739] The Act, section 76(3)(c); Cassidy *op cit* 385.
[740] The Act, sections 76(3)(c)(i)-(ii); Cassidy *op cit* 385.
[741] *Ibid*
[742] UK Law Commission *'Company Directors*,' section 5.19.
[743] UK Companies Act of 2006, section 174; UK Law Commission *op cit* section 5.19.
[744] UK Companies Act of 2006, section 174(1)-(2); UK Law Commission *op cit* section 5.19.

The UK Companies Act, section 170(3) helps to explain the interaction between the common law and legislative duties of care.[745] This section explains that the general duties of directors are based on certain common law rules and have effect in the place of those principles and rules.[746] In addition, section 170(4) explains that the general duties shall be interpreted and applied in the same way as common law rules, and that the court must look at the common law rules when they interpret and apply the general duties.[747] This means that the common law duty of care will apply simultaneously with the legislative duty of care and that the role of the former is to help interpret the latter.[748]

SA courts can learn from the UK Companies Act of 2006's explanatory notes and the UK Law Commission's explanation in order to clearly explain the way in which the Act, section 76(3)(c) formulates the duty of care.[749] Due to the unclear wording of the Act, section 76(3)(c), the standard of the duty of care can be interpreted as either subjective or objective.[750] In order to determine the Act's true meaning, SA courts will need to look at the *travaux preparatoires* of the SA Companies Bill of 2007 on which the Act was based, as it was drafted at the same time as the UK Companies Act of 2006.[751] Since the standards in the UK Companies Act of 2006, section 174 are objective and subjective, and because the Act, section 76(3)(c) was compiled at the same time as it, it is thought that section 76(3)(c)'s true meaning is to introduce both objective and subjective as opposed to either subjective or objective standards.[752]

The SA court needs to provide guidance on what the SA legislature's intent was in this regard when it promulgated the Act, in order to bring the interpretation of the Act, section 76(3)(c), in line with it.[753] It also needs to provide guidance which has a similar effect as the UK Companies Act of 2006, section 170(3) to explain the interaction between the legislative and common law duties of care.[754] Such guidance should explain whether the legislative duty of care in the Act complements, overrides or substitutes the common law duty of care.[755] Such guidance will help to determine if the common law is still applicable and what exactly its role is now that it has been enacted in part in the Act.[756]

---

[745] UK Companies Act of 2006, section 170(3).
[746] Ibid.
[747] UK Companies Act of 2006, section 170(4).
[748] UK Companies Act of 2006, sections 170(3) – 170(4).
[749] The Act, section 76(3)(c); legislation.gov.uk *op cit s.p.*; UK Law Commission *op cit* section 5.19.
[750] *Ibid.*
[751] SA Companies Bill B612D of 2007; UK Companies Act of 2006.
[752] The Act, section 76(3)(c); UK Companies Act of 2006, section 174.
[753] The Act, section 76(3)(c).
[754] UK Companies Act of 2006, section 170(3).
[755] The Act, section 76(3).
[756] The Act, section 76(3)(c).

Guidance on this matter is also important for the application of the Act, section 76(4)(a), which contains the BJR.[757] This is because it is uncertain whether the BJR, which applies to the legislative duty of care, will also apply to the common law duty of care.[758]

In each instance where a breach of the duty of care in relation to cybersecurity is alleged, the court will first have to determine what standard of care is expected from a director in a similar position, and then secondly it has to determine the standard of care in relation to cybersecurity that could be expected from such a director.[759]

Although the Act stipulates varying thresholds for directors with different skillsets, it is evident that all directors must maintain a standard of oversight over their companies' cybersecurity.[760] Since the importance of e-commerce is increasing and because of the continuing digitalisation of business operations, directors can no longer plead a lack of knowledge on cybersecurity and the protection of privacy and/or personal information.[761]

In the past, if a company had a cyberbreach and personal information was stolen, a director would have been judged according to the common law subjective test according to only their skill level.[762] Previously, a director could plead a lack of knowledge or inexperience on cybersecurity and be judged more forgiving; but the Act, section 76(3)(c) read together with the King Report IV of 2016 on corporate governance changed that.[763] King Report IV led to a new approach to corporate governance and its principle 12, which regulates IT governance, urges companies to improve processes that are to their advantage, to predict change and to make the best of new opportunities and to manage new risks.[764]

When the Act, section 76(3)(c) is read with King Report IV, principle 12 on IT governance, it does increase the expectation of a director's duties in relation to cybersecurity.[765] A court would therefore also need to consider the recommendations that the King Code prescribes when it determine a director's liability.[766]

Since section 24(1)(a) already allows the company to store information online, a director should be allowed to use aspects of AI, such as Consultative AI and Data

---

[757] The Act, sections 76(3)(c); 76(4)(a).
[758] *Ibid.*
[759] Cassim *et al. Contemporary Company Law op cit* 747.
[760] The Act, section 76(3)(c); Burger '*The Liability of Directors in Cyberspace,' s.p.*, available online at <https://www.golegal.co.za/cyberspace-risks-director-liability/>, last accessed on 25 May 2020.
[761] Burger *op cit s.p.*
[762] *Ibid*.
[763] The Act, section 76(3)(c); IoDSA '*King Report IV*' *op cit* principle 12; Burger *op cit s.p.*
[764] IoDSA '*King Report IV*' *op cit* principle 12; Burger *op cit s.p.*
[765] The Act, section 76(3)(c); IoDSA '*King Report IV*' *op cit* principle 12; Burger *op cit s.p.*
[766] *Ibid.*

Analysis to exercise their duty of care in relation to cybersecurity properly.[767] The duty of care and diligence requires an objective test, while the duty of skill uses a subjective test, because each one's skillset differs.[768] When one thinks about the information-overload that confronts a director, it is possible for the courts to allow a reasonable director to use Consultative AI and Data Analysis when they properly exercise their duty of care in relation to cybersecurity, whenever the court needs to apply the objective test of section 76(3)(c).[769] The wording of section 76(3)(c) could thus be interpreted in a way that will allow directors to integrate and rely on AI in the way in which they exercise their duty of care in relation to cybersecurity.[770]

2.4. SA POPI 4 of 2013

The SA POPI 4 of 2013 was promulgated to ensure that the right on privacy enshrined in the Constitution, section 14 is protected.[771]

In terms of SA POPI 4 of 2013, section 1, *s.v.* 'responsible party,' read together with section 8, which explains that the lawful processing of personal information is the duty of the responsible party, it is the duty of the board to make sure that all of the relevant requirements are met when shareholders/stakeholders' privacy and/or personal information is processed.[772]

SA POPI 4 of 2013 lays down many requirements on the collection and processing of personal information.[773] Section 19 requires companies to only process personal information if they have implemented proper safeguards; and in terms of section 13(1) when the processing is done for legitimate purposes.[774]

SA POPI 4 of 2013 sets out eight conditions for the lawful processing of personal information, of which the most important one when it comes to the duty of care in relation to cybersecurity is Condition 7 (which contains sections 19 to 22), which regulates security safeguards.[775] Section 19(1) determines that a board must make sure that its databases remain confidential by taking reasonable measures to prevent (a) its damage, loss or unauthorised discarding; or (b) its unlawful access or processing.[776]

---

[767] The Act, section 24(1)(a); Andrade *et al.* 'Application of Big Data Analytics in Cybersecurity' from the *International Conference on Applied Cognitive Computing* (2019), 26, available online at <https://www.researchgate.net/profile/Roberto-Andrade-7/publication/338582915_Application_of_Big_Data_Analytic_in_Cybersecurity/links/5e1dedc745851536bfe621bb/Application-of-Big-Data-Analytic-in-Cybersecurity.pdf>, last accessed on 10 January 2023.

[768] The Act, section 76(3).

[769] The Act, section 76(3)(c); Andrade *et al. op* 26.

[770] *Ibid.*

[771] SA Constitution, section 14.

[772] SA POPI 4 of 2013, sections 1, *s.v.* 'responsible party;' 8.

[773] Bowmans *op cit s.p.*

[774] SA POPI 4 of 2013, sections 13(1); 19.

[775] SA POPI 4 of 2013, sections 19 - 22.

[776] SA POPI 4 of 2013, section 19(1)(a)-(b).

Section 19(2) says that the board needs to (a) identify internal and external risks; (b) devise proper safeguards, and ensure that it is (c) implemented; and (d) updated.[777] Section 21(1) requires the board to reach a written agreement with third party service providers to ensure that they implement and maintain reasonable security measures.[778] Section 22(1) says that any cyberbreach must be notified to the IR and affected parties.[779]

SA POPI 4 of 2013, section 74(1) states that anyone may submit a complaint to the IR once the personal information of a data subject was compromised.[780] This means that anyone - not just the shareholders/stakeholders who were affected by a cyberbreach - may submit a complaint to the IR.[781]

SA POPI 4 of 2013, Chapter 11 has rights to recourse to hold companies and by extension, directors, liable for damages in instances where they did not exercise their duty of care sufficiently.[782] Section 107(1) determines that in certain instances, the penalty can be a fine or a period of imprisonment of not more than ten years.[783] Section 108 says that penalties can be issued by a magistrate's court and section 109 says that the IR can impose a fine, and that the amount can be determined at the court or IR's discretion depending on the facts and seriousness of the matter.[784]

2.5. Case Law

In 1983, Margo J of the Witwatersrand Local Division of the Transvaal High Court, set out the SA legal position on the duty of care in three parts in *Fisheries Development Corporation of SA Ltd v Jorgensen & Another; Fisheries Development Corporation of SA Ltd v AWJ Investments (Pty) Ltd & Others.*[785]

He firstly affirmed the finding of 1925 that Romer J of the British Court of Appeal of England and Wales made in *Re City Equitable Fire Insurance Co Ltd* where the latter said that the standard of care is determined by the nature of a company's business and also the specific obligation a specific director has.[786] This implies that, due to the nature of their business, certain boards will have a greater responsibility to keep personal

[777] SA POPI 4 of 2013, section 19(2)(a)-(d).
[778] SA POPI 4 of 2013, section 21(1).
[779] *Ibid.*
[780] SA POPI 4 of 2013, Chapter 10, section 74(1).
[781] *Ibid.*
[782] SA POPI 4 of 2013, Chapter 11.
[783] SA POPI 4 of 2013, section 107(1).
[784] SA POPI 4 of 2013, sections 108 - 109.
[785] *Fisheries Development Corporation of SA Ltd v Jorgensen & Another; Fisheries Development of SA Ltd v AWJ Investments (Pty) Ltd & Others* 1980 (4) SA 156 (W).
[786] *Fisheries Development Corporation of SA Ltd supra* 156; *Re City Equitable Fire Insurance Co Ltd* 1925 Ch 407.

information private.[787] For example, a greater standard of care will be required from the directors of a bank, than the directors of a construction company.[788]

Margo J, then explained that a director does not need to have any experience, qualification or skills in the company's affairs.[789] A director just has to exercise the care that could reasonably be expected from someone with their experience and skills.[790] This effectively means that a director is not required to be a cybersecurity expert, but that they are required to seek expert advice on cybersecurity matters.[791]

Lastly, he held that directors may delegate tasks to employees, as long as it is permissible and there is no suspicion that it would not be done with care.[792] He said that a director may trust an employee who performs their duty sincerely if there is no hint of unfaithfulness.[793] He also said that a reasonably prudent director would however not just accept reports and statements, but would apply their mind to it, reasonably consider it and exercise their own discretion.[794] The implication of this is that the King Code also needs to give guidance on how to properly delegate decisions, what tasks can be delegated to AI to perform virtually and what not, and how to implement a proper system of delegations in terms of the use of AI.

In 1998, Chaskalson, P of the SA CC listed some general guidelines on information protection in *Mistry v Interim Medical and Dental Council of SA* and provided some guidance on the type of questions which the court will ask in instances where a breach of privacy occurred in order to determine liability, such as how the personal information was obtained?[795] Was the personal information about intimate aspects?[796] What was the purpose for which it was provided?[797] Lastly, were there any reasonable expectations that such information should have been kept private?[798]

2.6. King Reports I – IV

The King Reports I – IV were first published in 1994, with the last one published in 2016. These Reports set out codes of good practice to serve as guidelines on good corporate governance for directors and to set the corporate governance framework in SA. Although it is a voluntary set of corporate governance principles and guidelines,

---

[787] *Fisheries Development Corporation of SA Ltd supra* 156; *Re City Equitable Fire Insurance Co Ltd* 1925 Ch 407.
[788] *Ibid.*
[789] *Fisheries Development Corporation of SA Ltd supra*.
[790] *Ibid*.
[791] *Ibid.*
[792] *Ibid*.
[793] *Ibid.*
[794] *Ibid*.
[795] *Mistry v Interim Medical and Dental Council of SA* 73 1998 (4) SA 1127 (CC).
[796] *Ibid.*
[797] *Ibid.*
[798] *Ibid.*

compliance is compulsory in terms of the JSE '*Listing Requirements*,' section 3.84 once a company is listed on the JSE.[799]

In 1996, Hussain J of the Witwatersrand Local Division held in *Minister of Water Affairs and Forestry v Stilfontein Gold Mining Company Limited* that the courts will take the King Reports into account when they interpret and apply directors' common law and legislative duties, and if they did not comply with the King Reports, they will be in breach of their duty of care, or even their fiduciary duty.[800] Directors consequently need to take reasonable measures to try and implement and follow the King Reports' good corporate governance principles and practices.[801]

Although the King Reports I – IV make no mention of OMs by name, their regulation of IT governance is of significance as it helps to set the corporate governance framework in which OMs are conducted. The following subsections will look at the recommendations of the King Reports I - IV on IT governance that impacts on the duty of care in relation to cybersecurity.

2.6.1. King Report I on Corporate Governance of 1994

The 'King Report I on Corporate Governance for SA' was published in 1994 by the IoDSA.[802] It was influenced by the Cadbury Report, but the King Committee also had to look at SA's unique challenges.[803]

King Report I introduced new concepts of corporate governance, and also made recommendations in its Code of Corporate Practices and Conduct ('the Code').[804] This Report only applied to certain companies (such as banks, large public entities, large unlisted companies, listed companies and parastatals) and did not apply to non-affected companies.[805] It required such affected companies to explain in their statements if they complied with the recommendations in the Code and if not, to explain why not.[806]

King Report I of 1994 regulated five areas of corporate governance, namely the responsibilities of directors, the role of auditors, stakeholder links, ethical practices and compliance with the recommendations.[807]

---

[799] JSE '*Listing Requirements' op cit* section 3.84; Du Plessis *et al. op cit* 294.

[800] *Minister of Water Affairs v Stilfontein Gold Mining Company Limited* 2006 5 SA 333 (W); Delport *et al.* 'The Duty of Care, Skill and Diligence: The King Report and the 2008 Companies Act' in *Tydskrif vir Hedendaagse Romeinse Reg* 2011(74) 450; Du Plessis *et al. op cit* 298.

[801] IoDSA '*King Report III*' *op cit* 12; Du Plessis *et al. op cit* 298.

[802] IoDSA '*King Report I*'*op cit* 4.

[803] UK Committee on the Financial Aspects of Corporate Governance *op cit* Chapter 3, paragraph 3.3.1.1; IoDSA '*King Report I*'*op cit* Appendix I: 'Code of Ethics for Enterprises;' Oost *A Safe Harbour for Directors in SA? A Comparative Study of the BJR*, LLD Thesis submitted at the University of SA (2020) 248.

[804] IoDSA '*King Report I*'*op cit* Chapter 20: 'Code of Corporate Practices and Conduct;' Oost *op cit* 248.

[805] IoDSA '*King Report I*'*op cit* 5.

[806] *Ibid*.

[807] IoDSA '*King Report I*'*op cit* 4 – 11; 13 – 14; 12; 18; 21 – 22.

In order to prevent that any of these new corporate governance standards restrained directors, the King Committee sought to introduce principles that could strike a balance between the *laissez-faire* approach to business, but which could keep companies accountable, while at the same time making sure that the interests of stakeholders are taken into account.[808] Directors therefore needed to make sure that they acted with the required care and skill when they exercise their duties.[809] In this regard, this Report recommended that the duty of care should be codified.[810] It also explained that a director should not be held liable for a breach of their duty of care if their decision was informed and rational and based on all the facts in a certain instance, and made without self-interest.[811] One can see that these requirements are related to the BJR, which was later included in the Act, section 76(4).[812]

This Report also recommended that the previous SA Companies Act 61 of 1973 should legislatively limitat the directors' duty of care.[813] Chapter 5 of this Report motivated this recommendation and explained that it is required to encourage the appointment of skilled persons and to promote higher standards of corporate governance.[814] It also explained that it was needed because of the burdensome standard of care that was required from non-executive directors.[815]

Oost critiques the King Report I's reason of the burdensome standard of the common law duty of care, and that it caused directors to be caught up in litigation.[816] She explains that the common law duty of care is low and that, contrary to the recommendations in this Report, the duty was made more burdensome in the Act, section 76(3)(c).[817]

Understandably, King Report I made no mention at the time of OMs, not only because the Internet was so new at the time, but also because SA just emerged from decades of international isolation.

2.6.2. King Report II on Corporate Governance of 2002

IoDSA reviewed King Report I, and introduced King Report II in 2002.[818] King Report II identified areas of good corporate governance practice which directors had to

---

[808] Bekink 'An Historical Overview of the Director's Duty of Care and Skill: From the 19th Century to the Companies Bill of 2007' in the *SA Mercantile Law Journal* 20(2008) 108.
[809] Oost *op cit* 248.
[810] *Ibid*.
[811] IoDSA '*King Report I*'*op cit* Chapter 5, sections 3.4; 3.4.1. – 3.4.3; Oost *op cit* 248 – 249.
[812] The Act, section 76(4); Oost *op cit* 249.
[813] SA Companies Act 61 of 1973; IoDSA '*King Report I*'*op cit* Chapter 5.
[814] IoDSA '*King Report I*'*op cit* Chapter 5, section 3.2.
[815] IoDSA '*King Report I*'*op cit* Chapter 5, sections 3.3; 3.5.
[816] IoDSA '*King Report I*'*op cit* Chapter 5, sections 3.3; 3.5; Oost *op cit* 249.
[817] The Act, section 76(3)(c); Oost *op cit* 249.
[818] IoDSA '*King Report II*'*op cit s.p.*

apply voluntarily, namely accountability, discipline, fairness, independence, responsibility, social responsibility and transparency.[819]

This Report also distinguished between executive and non-executive directors and their responsibilities.[820] It explained that although both need to exercise the duty of care, the latter needs to exercise their duty less frequently as they do not have similar access to the administrative records as executive directors.[821] It also advised non-executive directors to be prudent about the amount of boards on which they serve, as they need to pay full attention to the burdensome responsibilities of each board.[822]

This Report said that in the common law, directors are liable to the company for negligence when they have a duty of care, but that they cannot be held liable for judgment errors.[823] It also explained that the BJR does not mean that shareholders are entitled to damages that were caused by the judgement errors of directors, unless they were irrational and uninformed with a conflict of interest.[824] In terms of non-executive directors, it stated that their task is burdensome due to the common law test for a breach of the duty of care.[825] This Report consequently made the recommendation that a legislative BJR should be introduced in SA.[826]

Although companies were not compelled to comply with this Report, Hussain, J used this Report in *Minister of Water Affairs and Forestry supra* to evaluate if the directors had breached both their fiduciary duties and their duty of care.[827] In addition, non-compliance could lead to secondary liability in terms of the JSE '*Listing Requirements*.'[828]

In *Minister of Water Affairs and Forestry supra*, the Minister of Water Affairs and Forestry issued notices to the board of the Stilfontein Gold Mining Company Ltd.[829] This company's mining activities caused underground water to siphon into mine shafts, and this acidic water had to be pumped to the surface to be treated, otherwise it would pollute underground water sources.[830] The Minister's notices required the board to supply him with progress reports and to contribute to the treatment of the water.[831] The board disregarded the notices and the Minister got a court order, and this caused the

---

[819] IoDSA '*King Report II*'*op cit* 'Introduction,' paragraphs 18.1 – 18.7; Oost *op cit* 250.
[820] IoDSA '*King Report II*'*op cit* Section 1, Chapter 4; Oost *op cit* 250 – 251.
[821] *Ibid.*
[822] *Ibid.*
[823] IoDSA '*King Report II*' *op cit* Chapter 9, paragraph 3.
[824] IoDSA '*King Report II*' *op cit* Chapter 9, paragraph 4.
[825] IoDSA '*King Report II*' *op cit* Chapter 6, paragraph 10.
[826] IoDSA '*King Report II*' *op cit* Chapter 9, page 70.
[827] IoDSA '*King Report II*' *op cit* page 22, paragraph 2.1.1; *Minister of Water Affairs and Forestry supra*, paragraph 16.7.
[828] IoDSA '*King Report II*'*op cit* Section 6; JSE '*Listing Requirements*,' paragraphs 1.20 - 1.22.
[829] *Minister of Water Affairs and Forestry supra*, paragraph 13.2.
[830] *Ibid*.
[831] *Minister of Water Affairs and Forestry supra*, paragraph 13.2.3.

entire board to resign.[832] As a result, Hussain J had to determine if the directors breached their duties by resigning at the same time and to whom they owed their duties.[833]

On the first matter, Hussain J said that he was unable to locate case law of an instance where the entire board resigned at the same time.[834] He however criticised their timing and said that a company needs a board to function and that directors always have a duty to act in the interests of the company.[835]

On the second matter, Hussain, J looked at the breach of their fiduciary duties by all resigning at the same time, and said that they should have acted in terms of the King Report II's recommendations and are liable for non-corformance.[836] He found that these directors had acted against this Report's recommendations and that they had acted irresponsible to abandon the company.[837] He quoted the Report when he explained that a board should be aware of social issues and respond to them, and should focus on ethical standards and should act responsibly on environmental and human rights issues.[838] He consequently found that they did not act in good faith and on reasonable grounds when they resigned at the same time and abandoned the company.[839]

King Report II also sets out guidelines how directors should practice the duty of care.[840] Chapter 4 states that directors should not just practice the standard of care that is reasonably expected from someone with their experience and skills, but that they should also practice the standard of care that could be expected from someone who administers their own affairs with their relevant experience and skills.[841] This effectually means that directors should oversee a company's cybersecurity in the same way they would oversee the cybersecurity of their personal computer (PC).[842] In addition, it says that directors should continually try and gain greater insight into a company's affairs.[843]

Chapter 4 introduced the concept of IT governance and required directors to protect the confidentiality of information and to encourage the use of a well-functioning

---

[832] *Minister of Water Affairs and Forestry supra*, paragraph 13.2.6.
[833] *Minister of Water Affairs and Forestry supra*, paragraph 16; Esser & Delport 'The Duty of Care, Skill and Diligence: The King Report and the 2008 Companies Act' in *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 74 (2011) 451; Oost *op cit* 253.
[834] *Minister of Water Affairs and Forestry supra*, paragraph 16.1.
[835] Oost *op cit* 253 - 254; *Minister of Water Affairs and Forestry supra*, paragraphs 16.5; 16.6.
[836] *Minister of Water Affairs and Forestry supra*, paragraphs 16.5; 16.6; IoDSA '*King Report II*' *op cit* page 12, paragraph 18.7; page 22, paragraph 2.1.1.
[837] Oost *op cit* 254.
[838] *Minister of Water Affairs and Forestry supra*, paragraph 16.9; IoDSA '*King Report II*' *op cit* page 12, paragraph 18.7.
[839] *Minister of Water Affairs and Forestry supra*, paragraph 16.6.
[840] IoDSA '*King Report II' op cit* Chapter 4.
[841] *Ibid*.
[842] *Ibid*.
[843] *Ibid.*

information mangagement system.[844] It determines that IT systems are part of the business strategy of a company, and warns that such systems are susceptible to cyberrisks that the board needs to manage.[845]

2.6.3. King Report III on Corporate Governance of 2009

IoDSA reviewed King Report II, and introduced King Report III in 2009.[846]

King Report III heralded further corporate governance reform, because unlike the previous Reports, it applied to companies of all forms.[847]

Another difference was that this Report prescribed an "apply or explain" approach, unlike the "comply and explain" approach that was prescribed by the previous Reports.[848] The King Committee motivated this change and explained that the initial "comply and explain" approach only required a checklist exercise, whereas the "apply and explain" approach instead compels the directors to apply the recommendations.[849] After they have applied the recommendations they need to explain how they were applied, and if they were not applied, they need to explain why.[850] This still gives a board the freedom to say that the application of a certain recommendation is not in their best interests and that they instead apply a different practice, but then they need to explain the reasons for such non-compliance.[851]

Keay explains that the 'comply or explain' approach is the basic approach of a voluntary corporate governance code.[852] He however points out that no provision is made in the UK, as is the case in SA, for any regulatory body to evaluate the reports in which the directors explain how they applied the 'apply and explain' approach.[853] In such instances, it is left to the market and the shareholders to determine whether the company's compliance and explanation is sufficient, and for them to take action if it is not.[854] Keay evaluated this voluntary scheme, which is overseen by the market and the shareholders to determine whether a regulatory body is needed to help evaluate if companies are complying with corporate governance codes, and came to the

---

[844] IoDSA '*King Report II' op cit* Chapter 4.
[845] IoDSA '*King Report II*' *op cit* 140.
[846] IoDSA '*King Report II*'*op cit s.p.*; IoDSA '*King Report III*' *op cit s.p.*
[847] IoDSA '*King Report I*'*op cit s.p.*; IoDSA '*King Report II*' *op cit s.p.*; IoDSA '*King Report III*' *op cit* 'Introduction,' section 13; Oost *op cit* 255; The Act of 2008.
[848] IoDSA '*King Report I*' *op cit* Chapter 3; IoDSA '*King Report II*' *op cit* page 21; IoDSA '*King Report III*' *op cit* 'Introduction,' page 6.
[849] IoDSA '*King Report III*' *op cit* 'Introduction,' page 6.
[850] *Ibid.*
[851] *Ibid.*
[852] Keay 'Comply or Explain in Corporate Governance Codes: In Need for Greater Regulatory Oversight?' in *Legal Studies* 34(2) 2014 279.
[853] Keay 'Comply or Explain in Corporate Governance Codes: In Need for Greater Regulatory Oversight?' *op cit* 279.
[854] *Ibid*.

conclusion that there is a need for such a regulatory body in the UK, as is the case in SA, which also follow this model.[855]

The introduction of the King Report III also contains a reference to the common law duties of directors, as it is explained in the Act, section 77(2)(a), and this could mean that directors' duties should be interpreted by reference to the common law.[856] The Report explains in its introduction, paragraph 4 that its recommendations could be used to test if a director exercised the required care.[857] It explains that when corporate governance practices are widely used and becomes a custom, a court will be more likely to take them into consideration when it needs to decide whether due care was followed in a certain situation.[858] It explains that corporate governance guidelines consequently help to raise the standards of conduct.[859] It also says that whenever a board or a director does not meet a recognised standard of corporate governance, they may be held liable for their non-conformity, even if such a standard was not enacted in legislation.[860]

The introduction of this Report gives further guidance on how directors should exercise their duty of care and explains that directors should seek to settle disputes effectively.[861] Principle 2.14 again sets out guidelines on how directors should act in the company's best interests.[862] It explains that directors need to exercise the degree of care, skill and diligence that would be expected from a reasonable person who has (1) the general knowledge, skills and experience that may reasonably be expected from someone who performs similar functions; and who has (2) the general knowledge, skills and experience of that director.[863]

The introduction of this Report also requires directors to ensure that reasonable steps are followed in terms of IT governance matters.[864] Chapter 5 sets out the following seven principles in terms of IT governance: Principle 5.1 tasks the board with IT governance and requires it to be a standing point on a board meeting agenda.[865] Principle 5.2 determines that IT should support the sustainability of the company.[866] Principle 5.3 compels the board to implement an IT governance framework.[867] Principle

---

[855] Keay 'Comply or Explain in Corporate Governance Codes: In Need for Greater Regulatory Oversight?' *op cit* 279.
[856] The Act, section 77(2)(a); IoDSA '*King Report III*' *op cit* 'Introduction,' paragraph 4; Oost *op cit* 256.
[857] IoDSA '*King Report III*' *op cit* 'Introduction,' paragraph 4.
[858] *Ibid.*
[859] *Ibid.*
[860] *Ibid*.
[861] IoDSA '*King Report III*' *op cit* 'Introduction,' paragraph 4; Bouwman 'An Appraisal of the Modification of the Director's Duty of Care and Skill' in *SA Mercantile Law Journal* 21(2009) 520; Oost *op cit* 256.
[862] IoDSA '*King Report III*,' *op cit* principle 2.14.
[863] IoDSA '*King Report III*,' *op cit* principle 2.14, section 17.1.1 – 17.1.2.
[864] IoDSA '*King Report III*' *op cit* 'Introduction,' paragraph 4; Bouwman *op cit* 520.
[865] IoDSA '*King Report III*' *op cit* Chapter 5, sections 1; 9.
[866] IoDSA '*King Report III*' *op cit* Chapter 5, sections 10; 14.
[867] IoDSA '*King Report III*' *op cit* Chapter 5, sections 22.1; 22.2.

5.4 requires the board to oversee IT investments.[868] Principle 5.5 determines that IT governance is part of risk management.[869] Principle 5.6 requires the board to ensure that personal information databases are properly managed.[870] Lastly, Principle 5.7 determines that the risk and audit committees need to support the board to fulfill any IT responsibilities.[871]

This Report also required directors to properly inform themselves on any relevant laws and codes when they need to exercise their fiduciary duties and duty of care.[872]

This Report however contained an omission since it made no mention of the legislative BJR and its impact on how directors should exercise their duty of care, since this important provision was at that time just recently included in the Act, section 76(4).[873]

2.6.4. King Report IV on Corporate Governance of 2016

IoDSA reviewed King Report III, and introduced King Report IV in 2016.[874]

Like the previous Reports, it also contains voluntary principles and good corporate governance practices.[875] It explains that good corporate governance practices is a part of the law and that a court will take coginsance of them when it needs to determine what is an accepted practice in a certain situation.[876] It states that if anything in the King Reports conflicts with legislation, the latter will take precedence.[877]

The introduction does explain that corporate governance requires directors to exercise their duty of care and to exercise their duty to act in good faith in the best interests of the company.[878]

Hussain, J determined in *Minister of Water Affairs and Forestry supra* that the directors of a listed company had to comply with King Report II, and that those who did not adhere will be held liable for not exercising the required care.[879] Oost points out that the finding in this case referred only to King Report II, which was only applicable to listed companies.[880] She explains that should Hussain, J's argument be extrapolated to the directors of an unlisted company, which did not exercise the required care, it means

---

[868] IoDSA '*King Report III*' *op cit* Chapter 5, sections 23; 29.
[869] IoDSA '*King Report III*' *op cit* Chapter 5, sections 30; 34.
[870] IoDSA '*King Report III*' *op cit* Chapter 5, principle 5.6; section 35.
[871] IoDSA '*King Report III*' *op cit* Chapter 5, principle 5.7; sections 43; 48.
[872] IoDSA '*King Report III*' *op cit* principle 6.2; Bouwman op cit 520; Oost *op cit* 256 – 257.
[873] The Act, section 76(4); Oost *op cit* 257.
[874] IoDSA '*King Report III*' *op cit s.p.*; IoDSA '*King Report IV*' *op cit s.p.*
[875] IoDSA '*King Report IV*' *op cit* 'Introduction,' section 3.
[876] IoDSA '*King Report IV*' *op cit* 'Introduction,' section 4.
[877] *Ibid.*
[878] *Ibid*.
[879] *Minister of Water Affairs and Forestry supra*, paragraphs 16.7; 16.9.
[880] IoDSA '*King Report II*' *op cit* page 21; Oost *op cit* 257 – 258.

by implication that they too can be held liable in terms King Report IV, since it is applicable to all companies.[881]

Principle 12 of this Report puts an obligation on a director to oversee cybersecurity and to manage cyberrisks.[882] Principle 12 states that the board should govern IT to support its goals and it requires boards to formulate a vision for the way in which it governs the company's IT.[883] It also requires companies to disclose IT governance-related aspects to the shareholders and stakeholders in order for them to ascertain whether the company is following recommendations.[884] Although Principle 12 does not establish a direct link with directors' liability, it does increase directors' duties, which in turn increases directors' liability.[885]

The Act, section 76(3)(b) specifically says that directors owe their duty of care to the company and not to shareholders.[886] The board does however have a duty of care to ensure that the company and its cyberassets are cyberresilient and protected against cyberattacks.[887] This duty of care in relation to cybersecurity derives from the Act, section 76(3)(c) that needs to be read together with King Report IV, principle 12, on IT governance.[888] Directors' duty to protect privacy and/or personal information is therefore a consequence of their duty of care to oversee an effective risk management system, which includes an effective cybersecurity system.[889]

If a cyberbreach occured, a court will weigh King Report IV, principle 12 against a director's in/action and then decide if they acted with the due care that the Act requires.[890] Principle 12 will in other words help the court with the interpretation of the Act, section 76(3)(a)-(c) when the standard of conduct of directors needs to be determined when it comes to cybersecurity.[891]

3. THE DIRECTORS' DUTY OF CARE IN THE UNITED KINGDOM (UK)

The common law duty of care as stood before the UK Companies Act of 2006 was promulgated and the legislative duty of care as it is now codified in this Act in

---

[881] IoDSA '*King Report II*' *op cit* page 21; Oost *op cit* 257 – 258.
[882] IoDSA '*King Report IV*' *op cit* principle 12.
[883] *Ibid*.
[884] Burger *op cit s.p*.
[885] *Ibid*.
[886] The Act, section 76(3)(b); Delport *et al. Henochsberg on the Companies Act op cit* 298.
[887] The Act, section 73(3)(c); IoDSA '*King Report IV*' *op cit* 62.
[888] *Ibid*.
[889] *Ibid.*
[890] IoDSA '*King Report IV*' *op cit* principle 12; Burger *op cit s.p*.
[891] *Ibid*.

section 174 is very similar.[892] Loughrey explains that recent UK case law on the common law duty of care are especially relevant to help interpret the codified duty of care and warns that older case law must be approached with caution due to the relaxed attitude to the duty of care and the application of only a subjective standard in many of the early decisions.[893]

Six UK legal sources are relevant to the UK's duty of care in relation to cybersecurity, namely the common law, the UK Companies Act of 2006, the GDPR, the UK Data Protection Act (DPA) of 2018, case law and other sources.

3.1. Common Law

The earliest case where the nature of a duty of care in relation to directors was considered, appeared in the judgment by Lord Hardwicke in 1742 in *The Charitable Corporation* v *Sutton*, which was a monitoring care case in relation to a chartered company.[894] Here, Lord Hardwicke held that a director of a company owes the same duties to a company as a trustee does to a trust.[895] He also said that the court should be careful when they evaluate the business decisions which directors made, when they evaluate such business decisions with hindsight, outside of its business context.[896]

In 1747, Lord Hardwicke also gave an early objective form to the duty of care of a trustee, namely the ordinary businessman, in *Knight* v *The Earl of Plymouth* and in 1754 in *Ex Parte Belchier.*[897]

The common law places a duty on UK directors to promote the success of the company as well as a duty to exercise due care, skill and diligence in their role.[898]

A board's failure to reasonably protect a company against cyberrisks, for example when they do not reasonably oversee the implementation of a cybersecurity policy and system, or do not actively monitor it, will therefore constitute a breach of the duty to promote the success of the company and the duty of care.[899] The duty to exercise due care, skill and diligence needs to exercised by a reasonably diligent person with the experience and skills of a relevant director.[900] Directors who do not

---

[892] UK Companies Act of 2006, section 174; Loughrey *Directors' Duties and Shareholder Litigation in the Wake of the Financial Crisis* 14.
[893] Loughrey *Directors' Duties and Shareholder Litigation in the Wake of the Financial Crisis op cit* 15
[894] The *Charitable Corporation v Sutton* 2 ATK 400 (1754); Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* Par 8, section B(1).
[895] *Ibid.*
[896] *Ibid.*
[897] *Knight v The Earl of Plymouth* (1747) Dickens 120; *Ex Parte Belchier* (1754) Ambler 218.
[898] Hadwin *et al*. '*Cyber Risk and Directors' Liabilities: An International Perspective,' s.p.*, available online at <https://www.nortonrosefulbright.com/en-za/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective>, last accessed on 14 May 2021.
[899] UK Companies Act of 2006, sections 172; 174; Hadwin *et al*. *op cit s.p*.
[900] UK Companies Act of 2006, section 174; Hadwin *et al*. *op cit s.p*.

manage and reasonably oversee the cybersecurity policies and systems of their companies will not act in accordance with this standard.[901]

3.2. UK Companies Act of 2006

The UK Companies Act of 2006, sections 172 and 174 respectively codified the duties of directors.[902]

Section 172 states that a director has to act in a manner which they consider, in good faith, to be the best to promote the success of the company for the benefit of all of its members and, while they do this, pay close attention to some stipulated factors, which include (a) the long-term consequences of any decision; (b) the employees' interests, (c) the need to promote the company's relationships with customers, suppliers and other stakeholders; (d) the consequences of its business on the community and the environment; (e) the need to uphold high standards; and (f) the need to treat all of its members fairly.[903] If sub-section (d) is interpreted liberally it could also include the company's impact on its online community and online environment.[904]

Keay explains that there has been a lot of debate in the UK for many years on the determining the objective of public companies, since there was no definitive legislative guidance on the matter.[905] This was until the UK Companies Act of 2006 was promulgated, where section 172(1) explains in its statement on directors' duties, what the objective of companies should be.[906] In his research, Keay discusses the shareholder value concept, which represents the corporate objective in the UK.[907] He evaluates this concept and argues that although the enlightened shareholder value approach, which is set out in section 172(1), is an important new milestone in UK law, it is very similar to the shareholder value concept.[908] Keay explains that shareholder value refers to the benefits that the shareholders of a company get, while enlightened shareholder value, which is the concept that emanates from section 172(1), refers to the benefits that all the stakeholders of a company, including its shareholders, get.[909]

---

[901] UK Companies Act of 2006, section 174; Hadwin *et al*. *op cit s.p*.
[902] UK Companies Act of 2006, sections 172; 174.
[903] UK Companies Act of 2006, sections 172(a)-(f).
[904] UK Companies Act of 2006, section 172(d).
[905] Keay 'Ascertaining the Corporate Objective: An Entity Maximisation and Sustainability Model' in *The Modern Law Review* 71(5) 2008 663 – 665.
[906] Keay 'Tackling the Issue of the Corporate Objective: An Analysis of the UK's Enlightened Shareholder Value Approach' in *Sydney Law Review* 29(4) (2007) 577.
[907] Keay '*Shareholder Primacy in Corporate Law: Can It Survive? Should It Survive*,' 1, available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1498065>, ladst accessed on 27 June 2023.
[908] Keay 'Tackling the Issue of the Corporate Objective: An Analysis of the UK's Enlightened Shareholder Value Approach' *op cit* 577.
[909] UK Companies Act of 2006, sections 172; Keay 'Tackling the Issue of the Corporate Objective: An Analysis of the UK's Enlightened Shareholder Value Approach' *op cit* 577.

In follow-up research, Keay and Loughrey explain that due to a lack of guidance from the court on how section 172 should be interpreted, and because of the potential of derivative litigation, legal practitioners' interpretation of this section is important to help guide directors on how they should exercise their duty of care.[910]

In terms of section 174, directors must exercise the care, skill, and diligence of a reasonably diligent person in the director's position.[911] Section 174(1) determines that a director must exercise due care, skill and diligence.[912] Section 174(2) explains that this means the standard of care, skill and diligence that one could expect from a reasonable person with (a) the experience and skills who performs the same functions; and has (b) the experience and skills of that director.[913] Since section 174 states that directors must exercise due care, skill and diligence in their oversight, it extends the application of their duty of care to risk management.[914] The implication of this is that directors will have to exercise due care and implement and oversee cybersecurity policies and systems to mitigate cyberbreaches and that they need to exercise diligence and ensure that it functions properly and that they cannot simply accept management's assurances that it does.[915]

It should be pointed out that these duties are subject to private enforcement only.[916] Directors of financial institutions however also have a regulatory duty to exercise due care, skill and diligence when they manage the affairs of their company, which is enforceable by the UK Financial Conduct Authority (FCA) and Prudential Regulation Authority.[917]

3.3. GDPR

---

[910] Keay, Loughrey *et al.* 'Legal Practitioners, Enlightened Shareholder Value and the Shaping of Corporate Governance' in *Journal of Corporate Law Studies* (April 2008) 79.
[911] UK Companies Act of 2006, section 174.
[912] UK Companies Act of 2006, section 174(1).
[913] UK Companies Act of 2006, section 174(2).
[914] UK Companies Act of 2006, section 174; Rathod '*Board of Directors' Fiduciary Duties in Terms of Cybersecurity,*' *s.p.*, available online at <https://diligent.com/au/board-directors-fiduciary-duties-terms-cybersecurity/>, last accessed on 26 May 2021.
[915] *Ibid.*
[916] Loughrey 'Breaching the Accountability Firewall: Market Norms and the Reasonable Director' in *Seattle University Law Review* 37(3) 2014 990.
[917] UK Financial Conduct Authority (FCA) *Handbook, Statements of Principle and Code of Practice for Approved Persons* (PRA), section 2.1A.3.

The EU 'General Data Protection Regulation' (GDPR) helps to protect individuals by ensuring that their personal information, when held by a third party, is secure.[918] The GDPR was implemented in all EU member states on 25 May 2018, including the UK.[919]

The GDPR, article 5(2) introduced the accountability principle, which requires boards to both comply with personal information protection requirements, and to also show that they adhere to the GDPR.[920] Since cyberbreaches are also caused by internal human errors, the GDPR, article 32(1) requires boards to implement both proper IT and internal organisational measures in order to prevent both external and internal risks.[921] This requires directors to implement and oversee secure cybersecurity policies and systems, to train employees on matters such as how personal information must be managed and stored.[922]

The duty of care features prominently in the GDPR where EU regulators are specifically tasked to consider it when they determine fines after a cyberbreach occured.[923] The EU 'Data Protection Working Party 253 (WP253)' sets out guidelines on the determination of administrative fines and the third criteria relates directly to the duty of care and states that "any action," which the board took to mitigate the consequences of a cyberbreach, may be taken into account.[924] The EU 'Data Protection Working Party (WP253)' then explains that the board has an obligation to implement the proper cybersecurity measures for its cyberrisks, and that the board needs to carry out impact evaluations on personal information in order to help mitigate cyberrisks that arise from the processing of personal information.[925] Importantly, it states that when a cyberbreach occurs, the board should do "whatever they can" to reduce its consequences.[926] This is an important provision that makes room for the use of AI to help make companies cyberresilient.[927]

Since the determination of the amount of a fine will be influenced by the rigour with which the board exercised their duty of care before the cyberbreach occurred, it will

---

[918] EU 'General Data Protection Regulation' (GDPR).
[919] UK Information Commissioner's Office (ICO) '*Guide to the GDPR,*' i, available online at <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>, last accessed on 11 July 2021.
[920] EU GDPR *op cit* article 5(2).
[921] EU GDPR *op cit* article 32(1).
[922] Carter '*Directors' Liabilities: How Much Risk Are You Prepared to Take?,' s.p.*, available online at <https://www.kingsleynapley.co.uk/insights/blogs/data-protection-blog/data-protection-a-new-board-room-priority>, last accessed on 13 May 2021.
[923] EU Data Protection Working Party '*Guidelines on the Setting of Administrative Fines,*' 4, available online at <file:///C:/Users/Julian/Downloads/20171020_wp253_en_43FBAE3D-B195-7648-AD40DD676CB8416E_47889.pdf>, last accessed on 19 June 2022.
[924] EU Data Protection Working Party *op cit* 12.
[925] *Ibid*.
[926] *Ibid.*
[927] *Ibid.*

encourage a board to exercise effective oversight in order to help to tip the balance in its favour whenever a cyberbreach occurred and liability needs to be determined.[928]

3.4. UK Data Protection Act (DPA) of 2018

The UK Data Protection Act (DPA) of 2018, section 56 relates to the general obligations of the controller of personal information, such as a board, and states that (1) each board must not only implement the proper measures to process personal information, but must also be able to demonstrate that it complies with the UK DPA.[929] It specifically states that such measures include proper policies on the protection of personal information.[930] It also requires such measures to be updated regularly.[931] This means that the UK DPA places additional burdens on a board, and besides the duty to implement a proper cybersecurity policy and system, a board also needs to demonstrate that their measures comply with the UK DPA, and that it is regularly updated.[932]

3.5. Case Law

In 1911, Neville J of the English Court of Appeal made the first attempt to instill a basis in the duty of care, when he held in *Re Brazilian Rubber Plantations & Estates Ltd* that the duty of care expects that a director should practice their duties with the standard of care that could reasonably be expected from someone with their experience and skills.[933]

With regards to liability for not exercising their duty of care properly, Neville J said that as long as it can be proven that a director performed their duty sincerely, they cannot be held liable for a loss, as such liability only sets in once they acted with gross negligence.[934] He acknowledged that the test for liability, in instances were the duty of care was breached was vague, and that it is difficult to determine negligence if there is not certainty on what standard of care was required.[935] He also explained that a director, who manages a company that works with rubber, even though they know nothing of the trade, will not be held liable for any losses due to their lack of skills.[936] However, as soon as they do know something of rubber, the company must gain from

---

[928] EU Data Protection Working Party *op cit* 13.
[929] UK Data Protection Act (DPA) of 2018, section 56(1).
[930] UK DPA of 2018, section 56(1)-(2).
[931] UK DPA of 2018, sections 56(1); 56(3).
[932] UK DPA of 2018, sections 56(1)-(3).
[933] *Re Brazilian Rubber Plantations & Estates Ltd* (1911) Ch 425.
[934] *Ibid*.
[935] *Ibid*.
[936] *Ibid*.

their experience and skills.[937] This finding is of importance for directors when they need to exercise their duty of care in relation to cybersecurity, because if they know nothing about cybersecurity, they need to obtain expert advice.[938] In addition, it is important because Neville J said that as long as it can be proven that a director performed their duty sincerely, they cannot be held liable for a loss, as such liability only sets in once they acted with gross negligence.[939]

Another turning point was Romer J's finding in 1925 in *Re City Equitable Fire Insurance Co Ltd supra* when he held that directors should employ the standard of care that is expected from an ordinary person in a similar position.[940] In addition, he reaffirmed that a director only has to practice the standard of care of someone with their experience and skills.[941] This means that directors of companies who work with personal information should employ the standard of care that is expected from an ordinary person in a similar position.[942] Importantly, this case reaffirms that a director only has to practice the standard of care of someone with their experience and skills.[943]

In 1990, Lord Bridge of the House of Lords explained the test for the duty of care in *Capraro supra* and set out a three-part test to prove negligence in terms of the duty of care: firstly, harm has to be a reasonably foreseeable consequence of the defendant's in/action.[944] Secondly, there must be proximity in the relationship of the parties, and lastly, it must be fair to hold the defendant liable.[945]

In 2015, Nugee J of the High Court of England and Wales reaffirmed in *Sharp and Others v Blank and Others* the common law position that a director has a duty of care towards the company, but not a fiduciary duty towards the shareholders.[946] As a result, courts will only hold a director liable when there is evidence that shows that they had acted *mala fide* in an attempt to jeopardise the interests of shareholders, or if no sensible board would have reached the decision which the board has reached.[947]

In 2015, Lord Dyson MR of the England and Wales Court of Appeal, Queen's Bench Division held in *Google Inc. v Vidal-Hall and Others*, that a tort claim may be instituted for the unlawful use of private information and that third parties may institute it when the UK DPA of 1998 is transgressed, even if the claimant did not suffer any

---

[937] *Re Brazilian Rubber Plantations & Estates Ltd supra*.
[938] *Ibid*.
[939] *Ibid*.
[940] *Re City Equitable Fire Insurance Co Ltd supra* 407.
[941] *Ibid.*
[942] *Ibid*.
[943] *Ibid*.
[944] *Capraro Industries PLC supra* 568.
[945] *Ibid.*
[946] *Sharp and Others v Blank and Others* [2015] EWHC 3220; Institute of Chartered Accountants of England and Wales '*Case Law: Court Clarifies Directors' Duties to Shareholders,' s.p.*, available online at <https://www.icaew.com/archive/library/subject-gateways/law/legal-alert/2016-03/case-law-court-clarifies-directors-duties-to-shareholders>, last accessed on 25 May 2020.
[947] *Ibid.*

pecuniary loss or damage.[948] Although this case was instituted against the company instead of an individual director, the court will necessarily try and determine if the directors complied with their duty of care to oversee a cybersecurity policy and system that protects online databases that contain such personal information.[949]

In 2020, Lady Hale P of the UK Supreme Court held in *Various Claimants v Wm Morrisons Supermarket PLC* that a board of directors is not liable for a cyberbreach that was caused by an employee who deliberately wanted to harm the company and the board itself did not breach any information protection legislation.[950]

Keay and Loughrey explain in their research that because the UK does not have a legislative BJR provision, some may think that the UK courts are cautious to review directors' business decisions, and that there is a lack of director accountability.[951] Their research evaluated this assumption and looked at English case law over time to determine how the courts review and impose liability for directors' judgments.[952] They found that such actions have been successful since the 1950's, and that there was a rise since 2007.[953] They explain that this was not caused by any legislative changes, but because of an increase in insolvencies and because the claimants of insolvent companies were more willing to institute actions based on business decisions.[954]

Loughrey goes on to explain that the UK courts do review the substance of directors' decisions, but that they however rarely impose liability in the absence of some failure in the decision-making process, and she then lists examples of such aspects which the courts do take into account, such as the failure to exercise any or independent judgment, the failure to take advice or the failure to take the relevant considerations into account.[955]

Keay and Loughrey however acknowledge that there are not many instances where directors are held liabile, and that such instances mostly relate to private companies.[956] Their research shows that the directors of large public companies are not regularly held liable for their business decisions, but makes it clear that this is not because such decisions cannot be reviewed by court, as it can and does happen.[957]

4. THE DIRECTORS' DUTY OF CARE IN THE UNITED STATES (US)

[948] UK Data Protection Act of 1998, c.29; *Google Inc. v Vidal-Hall and Others* (2014) EXHC (Civ) 113; Norton Rose Fulbright SA *op cit s.p*.
[949] *Ibid*.
[950] *Various Claimants v Wm Morrisons Supermarkets* PLC UKSC 2018/0213.
[951] Keay, Loughrey, 'Business Judgment and Director Accountability: A Study of Case Law Over Time' in *Journal of Corporate Law Studies* 20(2) 2020 386 – 387.
[952] *Ibid.*
[953] *Ibid.*
[954] *Ibid.*
[955] Loughrey *Business Judgment and Director Accountability op cit* 2.
[956] Keay, Loughrey, 'Business Judgment and Director Accountability: A Study of Case Law Over Time' *op cit* 387.
[957] *Ibid.*

There are four US legal sources which are relevant to the duty of care in relation to cybersecurity, namely the common law, federal law, states' law and case law, and each of these will now in turn be looked at.

4.1. Common Law

The directors' duty of care in the US is based on UK common law.[958]

There are conflicting case law on the origin of the duty of care in the US, and Kershaw explains that the duty of care for directors in NY, and in several other jurisdictions, can be traced to two cases that served before the NY Court of Chancery in 1832.[959] The first is *Scott* v *Depeyster*, where McCoun, VC held that the standard of care for directors was one of ordinary care.[960] The second case is *Robinson* v *Smith* in which Walworth, C held that a gross negligence standard applies to directors.[961] Interestingly enough, the two cases made no reference to each other.[962]

Kershaw explains that NY law basically adopted a 'gross negligence as a label' approach to the duty of care in an attempt to overcome the divide between these two cases.[963] In terms of this bridging approach, gross negligence only explains the low expectations that the 'situation demands' standard requires.[964]

The 'situation demands' understanding of gross negligence, comes from a judgment that Lord Loughborough of the High Court of England and Wales made in 1789 in *Shiells* v *Blackburne* – and this approach was used by Bradley, J of the Circuit Court of the Southern District of New York in 1873 in *Railroad Company* v *Lockwood.*[965] Here Bradley, J explained that negligence, or whatever name the court gives it, is the failure to exercise the care that is required in a given situation.[966] Kershaw explains that when this approach is used, ordinary care can be exercised according to the nature of the directorship – which in the case of non-executive directors might be limited or no reward or a limited understanding of the company's business – and that such a situation could require a lower standard.[967]

Following the approach in *Robinson supra*, the courts in Delaware apply a gross negligence standard to the decision-making process and a good faith standard to the

---

[958] Harner *op cit* 22.
[959] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 174.
[960] *Scott v Depeyster* 6 NY Ch. Ann 229 (1832).
[961] *Robinson v Smith* 3 Paige Ch. 222 (1832).
[962] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 174.
[963] *Ibid.*
[964] *Ibid*.
[965] *Railroad Company v Lockwood* 84 US 357 (1873); *Shiells v Blackburne* (1789) 1 HB1 158, 126 ER 94.
[966] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* Part 6, section 1.
[967] *Ibid.*

oversight of care, while other jurisdictions mostly followed the outcome of *Scott supra* and requires an ordinary standard of care.[968]

With the passing of time, the move to codify directors' duties in the UK informed a similar move in the US.[969] The US Third Restatement of Torts of 2005 is a treatise issued by the American Law Institute (ALI), which sets out the general principles of the US common law on torts.[970] It notes that the main features to look at when it needs to be determined whether a person's conduct falls short of due care are the anticipated probability that the in/action will cause damage or loss, the anticipated severity of the damage or loss, as well as the burden of precautions which is needed to reduce the risk of the damage or loss.[971]

4.2. Federal Law

The MBCA of 2016, which has been adopted by many US states in some version, sets out the general standards of conduct for directors in section 8.30.[972] Section 8.30 states that directors shall perform their duties (a)(1) in good faith; (2) with the care that an ordinary prudent person would reasonably believe to be appropriate under similar circumstances; and (3) in a way that the director reasonably believes will be in the company's best interests.[973] It also states that (b) a director who does not have knowledge of a certain aspect may rely on information that was presented by: (1) employees who the director reasonably believes are competent and reliable; and/or (2) accountants or legal advisors if it falls within such a person's competence; and/or (3) a board committee of which the director is not a member and in whose work the director has confidence.[974] It is submitted that directors would also be able to rely on the advice of cybersecurity experts when it comes to cybersecurity matters.[975] The section ends by saying that (c) a director is not liable for any action or inaction if they performed their duties in compliance with this section.[976]

Importantly, the Official Comment of section 8.30 says that Company Law looks at whether processes were followed with due care and not outcomes as such.[977] What is "reasonable" is thus a question that the board needs to determine by evaluating the

---

[968] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 137; See Chapter 3, section 4.4.2.2.
[969] Harner *op cit* 22.
[970] American Law Institute (ALI) US Third Restatement of Torts of 2005; Cornell Law School Legal Information Institute '*Negligence,' s.p.*, available online at <https://www.law.cornell.edu/wex/negligence>, last accessed on 11 July 2021.
[971] Cornell Law School Legal Information Institute *op cit s.p.*
[972] US MBCA of 2016, section 8.30.
[973] US MBCA of 2016, section 8.30(a)(1)-(3).
[974] *Ibid.*
[975] US MBCA of 2016, section 8.30(a)(2).
[976] US MBCA of 2016, section 8.30(c).
[977] US MBCA of 2016, Official Comment on section 8.30.

cyberrisks that the company face by following a process with due care to mitigate such cyberrisks.[978]

The MBCA of 2016's Official Notes on section 8.30 explain that the concept, 'reasonably believes,' is both subjective and objective.[979] Subjectively it analyses what a particular director, who acted in good faith, actually believed.[980] Objectively it analyses whether a director's belief is reasonable – and whether a reasonable director in a similar position could have reached the same conclusion.[981]

Directors consequently do not have to make perfect decisions on cybersecurity, but they instead need to act reasonably by following a reasonable process under the circumstances in terms of the cyberrisks that the company face.[982]

It is worth noting that a few other federal laws and regulations also have bearing to a lesser extent on cybersecurity, and that directors whose companies form part of the health or international commerce sectors need to pay special attention to the requirements that are set out in this regard in the US Federal Trade Commission (FTC) Act of 1938, US Health Insurance Portability and Accountability Act (HIPPA) of 1996, US Gramm-Leach-Bliley Act of 1999, US Electronic Signatures in Global and National Commerce Act of 2000 and the US Homeland Security Act of 2002.[983]

In addition, public companies are required to disclose certain mandatory requirements in terms of the US Securities Act of 1933 and the US Securities Exchange Act of 1934.[984] In this regard, the US SEC already issued a bulletin in 2013 that provides guidance on the duty of care when it comes to cyberbreaches.[985] In terms of its disclosure regulations, the US SEC requires a Form 8-K to be completed and submitted two business days after a cyberbreach.[986] This requirement puts a clear responsibility on boards to act immediately after a cyberbreach occurred and disclose it quickly.[987] The US SEC rules also place a burden on companies to develop and adopt proper

---

[978] US MBCA of 2016, Official Comment on section 8.30.
[979] *Ibid.*
[980] *Ibid.*
[981] *Ibid.*
[982] Lunn *op cit* 9.
[983] US Federal Trade Commission (FTC) Act of 1938, US Health Insurance Portability and Accountability Act (HIPPA) of 1996, US Gramm-Leach-Bliley Act of 1999, US Electronic Signatures in Global and National Commerce Act of 2000, US Homeland Security Act of 2002; Litt *et al. op cit* 202 - 205.
[984] US Securities Act of 1933; US Securities Exchange Act of 1934; 17 US Code of Federal Regulations, section 240. 10b-5.
[985] US SEC *'Regulation Systems Compliance and Integrity,' s.p.*, available online at <https://www.sec.gov/rules/proposed/2013/34-69077.pdf>, last accessed on 12 July 2021; 17 US CFR parts 242 and 249.
[986] US SEC '*Form 8-K,' s.p.*, available online at <https://www.sec.gov/files/form8-k.pdf>, last accessed on 12 July 2021.
[987] *Ibid.*

disclosure procedures.[988] The US SEC's '*Regulation System's Compliance and Integrity*' states that it expects each company to develop a disclosure process.[989]

In 2018, the US SEC issued further obligations for listed companies to disclose cyberbreaches in its '*Commission Statement and Guidance on Public Company Cybersecurity Disclosures.*'[990]

In 2018, the US SEC also issued an '*Investigative Report on Cyberfrauds*' that emphasised that boards should ensure that internal auditing measures look at cyberrisks and that they should audit the potential of the cybersecurity measures to withstand manipulated and spoofed e-mails.[991]

The US SEC has also emphasised in its '*Commission Statement*' that it is the board's duty to understand cyberrisks, to make sure that they are addressed, and to exercise oversight on the company's cybersecurity.[992] The US SEC also wants the board to disclose its involvement in cybersecurity and risk management as part of its proxy statement.[993]

4.3. States' Law

Since each of the 50 US states have their own tort laws in terms of the US Constitution, Tenth Amendment, there are numerous different tests to determine a breach of the duty of care in US tort law.[994]

In this regard, states such as Florida and Massachusetts merely look at whether the defendant foresaw that their actions would cause the ensuing harm to the plaintiff.[995] On the other side, the California Civil Code, section 1714 sets a duty of general care and requires that reasonable measures need to be implemented to prevent that harm is caused to others.[996] Most US states have however adopted a multi-element test to determine negligence on the duty of care, or use a modified version of the tests named above.[997]

A large company that operates in various US states faces many legal considerations when they oversee their cybersecurity. The American Business Association (ABA) notes numerous US state laws and regulations on cybersecurity and

---

[988] US SEC *'Regulation Systems Compliance and Integrity' op cit s.p.*
[989] *Ibid.*
[990] US SEC '*Commission Statement and Guidance on Public Company Cybersecurity Disclosures,' s.p.*, available online at <https://www.sec.gov/rules/interp/2018/33-10459.pdf>, last accessed on 12 July 2021.
[991] US SEC '*Investigative Report on Cyberfrauds,' s.p.*, available online at <https://www.sec.gov/litigation/investreport/34-84429.pdf> ,last accessed on 12 July 2021.
[992] US SEC '*Commission Statement and Guidance on Public Company Cybersecurity Disclosures' op cit* 4 - 6.
[993] *Ibid*.
[994] US Constitution, Tenth Amendment.
[995] *McCain v Florida Power Corporation* 593 So. 2d 500 (Florida 1992); *Jupin v Kask* 849 N.E 2d 829 (Massachusetts).
[996] California Civil Code, section 1714.
[997] *Adams v City of Fremont* 68 Cal. App. 4th 243 (1998).

a study on the topic by Lunn identified 140 rules that place obligations on US companies to implement proper cybersecurity measures for the processing of credit card information and the encryption and discarding of personal information and SSNs.[998]

US states' legislation is however starting to move in a direction that outlines specific standards for directors when they exercise their duty of care, like the Colorado Privacy Act, which took effect on 1 July 2023.[999] The Colorado Privacy Act, section 1-1-1308(5) regulates the duty of care of directors and requires the board to implement reasonable cybesecurity measures to secure personal information against unauthorised acquisition.[1000] It requires such measures to be sufficient for the nature, scope and volume of the personal information that is processed as well as the nature of the company.[1001] The New York Privacy Act (NYPA) of 2021, section 5642 also proposes that directors undertake cyberrisk evaluations when it comes to how they exercise their duty of care in terms of personal information.[1002]

4.4. Case Law

No case law could be found on due care in relation to cybersecurity at OMs specifically, but relevant US case law exists on due care in relation to cybersecurity, and these will be evaluated below.[1003]

4.4.1. Federal Level

An interesting federal case of negiligence theory that derives from Maritime Law has bearing and a comparison can be drawn with cybersecurity.[1004] *The TJ Hooper* involved the sinking of a coal ship at sea off the New Jersey coast in 1928.[1005] The ship was not fitted with a radio that would have allowed it to know of an approaching storm and to then manoeuvre to safe waters.[1006] The equipment was available and relatively inexpensive, yet was not deemed as standard equipment back then.[1007] The ship's

---

[998] Litt *et al. op cit* 202 – 205; Lunn *op cit* 9.
[999] Usercentrics '*The Colorado Privacy Act: An Overview,' s.p.*, available online at <https://usercentrics.com/knowledge-hub/colorado-privacy-act/#:~:text=What%20is%20the%20Colorado%20Privacy,doing%20business%20in%20the%20state.>, last accessed on 16 June 2022.
[1000] Colorado Privacy Act of 2021, section 1-1-1308(5).
[1001] *Ibid.*
[1002] New York Privacy Act of 2021, section 6542.
[1003] *The TJ Hooper* 60 F.2d 737, 1932 US App. Lexis 2592 (2d Cir. NY 1932).
[1004] Litt *et al. op cit* 202 – 205.
[1005] *The TJ Hooper supra*.
[1006] *Ibid*.
[1007] *Ibid*.

operator argued that there was no industry standard, which required its use, and that there was no common practice to do so.[1008] Learned Hand J of the US Court of Appeals, Second Circuit, said that eventually it is up to the court to say what is required and held that there are certain measures that are so vital that even if their use is not common practice it will not excuse their omission.[1009] Although the case did not involve cybersecurity, the reasoning of Learned Hand J can be extrapolated to the duty of care in relation to cybersecurity, since AI measures are available to mitigate cyberattacks, even though there is no standard measure according to AI industry standards.[1010] Although there is no industry standard and no common practice to implement for example a firewall of a certain strength, or to use a certain type of AI, directors have a duty of care to protect the company against cyberbreaches as best they can.[1011] One can only agree with Learned Hand J when he said that there are certain measures that are so vital that even if their use is not common practice it will not excuse their omission, when one thinks of the potential of AI to help combat cyberattacks.[1012]

4.4.2. US States' Case Law

There are relevant case law on the duty of care that has bearing on cybersecurity from California, Delaware, Georgia, Pennsylvania, Minnesota and New Jersey.

4.4.2.1. California

In 2019, Koh, J of the Northern District Court of California settled three derivative suits of shareholders in *In re Yahoo! Inc. Securities Litigation* against Yahoo!'s former directors.[1013] This case alleged that the former directors did not disclose cyberattacks that occurred between 2013 and 2016.[1014] Besides other cyberbreaches, the non-disclosure included a cyberattack, which occurred in 2014 were hackers stole personal information databases, but the directors failed to disclose the incident.[1015] It was found that the board and mangement of Yahoo! actively concealed this information.[1016] Due to the seriousness of the allegations and the US SEC's settlement, Yahoo! agreed to settle the consolidated cases.[1017] Since this was such a prominent case, it will likely influence

[1008] *The TJ Hooper supra*.
[1009] *Ibid*.
[1010] Litt *et al. op cit* 202 – 205.
[1011] *The TJ Hooper supra*.
[1012] *Ibid*.
[1013] *In Re Yahoo! Inc. Securities Litigation* 17-CV-307054 (4 January 2019).
[1014] *Ibid.*
[1015] *Ibid*.
[1016] *Ibid*.
[1017] *Ibid*.

future shareholder cases against directors and managers in cases were the disclosure of a cyberattack was concealed.[1018]

4.4.2.2 Delaware

In his research on the hdevelopment of the duty of care in Delaware, Kershaw could find no case law on the duty of care of a Delawarean director prior to 1960.[1019] Yet, Delaware is today well known for its 'gross negligence' care jurisprudence that were formulated in 1984 in *Aronson* v *Lewis* and in 1985 in *Smith* v *Van Gorkom*.[1020]

Kershaw explains that the absence of case law on the link of the duty of care with the standard of gross negligence, indicates that Delaware's standards are homespun, and that they were influenced by Delaware's view of the company as a tool for wealth-generation, and the pressures of corporate legal federalism.[1021] He explains further that the exact origin of the courts' of Delaware's unique interpretation of the duty of care is difficult to determine and can only be deduced from borrowed concepts.[1022] As a result, Delaware's courts today apply a gross negligence standard to the decision-making process and a good faith standard to the monitoring or oversight of care.[1023]

In 1963, Southerland, CJ of the Supreme Court of Delaware still held in *Graham v Allis-Chalmers Mfg Co* that the duty of care compels a director to act with the degree of care of an ordinary person in a similar position.[1024] The courts will as a result look at whether a director acted with the degree of care of an ordinary person who faced a similar cyberrisk.[1025]

In 1984, Moore J of the Delaware Supreme Court applied a gross negligence standard to the decision-making process and held in *Aronson supra* that the BJR can only be used in instances of director action and not when directors have failed to act.[1026] The implication of this finding is that directors who did nothing to comply with cybersecurity and personal information management responsibilities will not be protected by the BJR.[1027]

In 1985, Herrmann, CJ of the Supreme Court of Delaware held in *Smith v Van Gorkom*, that in terms of the standard that was laid down in *Graham supra*, a director

---

[1018] *In Re Yahoo! Inc. Securities Litigation supra*.
[1019] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 198.
[1020] *Aronson v Lewis* 473 A. 2D 805 (Del. 1984); *Smith v Van Gorkom* 488 A 2d 858 (Del 1985); Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 198.
[1021] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 198.
[1022] *Ibid.*
[1023] Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* 137.
[1024] *Graham v Allis-Chalmers Mfg Co* 188 A 2d 130 (Del 1963).
[1025] *Ibid.*
[1026] *Aronson supra*.
[1027] Kohne *et al.* Fiduciary Duties of Directors are Key to Minimise Cybersecurity Risks in *NACD Directorship* (May/June 2015), 42.

must be informed, act in good faith and must truly believe that their actions were in the company's best interests.[1028] Herrmann CJ also said that a party who claims damages against a board's decision will have to rebut the presumption that the board's decision was made on an informed basis.[1029] He said that the determination whether a decision was made on an informed basis or not, is determined looking at whether the directors have acquainted themselves, before they made their decision, of all information that were known to them at the time.[1030] This finding therefore shows that directors have a duty to become informed.[1031] In addition, he said that the BJR does not afford protection for directors who have made a reckless decision.[1032] Herrmann CJ's decision shows the importance that a board must make an informed decision on cybersecurity, and that the determination whether a board's business decision was made on an informed basis or not, is decided by looking at whether they have acquainted themselves, before they made their decision, with all information that were known to them at the time.[1033] This finding therefore places a duty on directors to become informed of the cyberrisks that a company face and the cybersecurity measures that could be used to prevent them.[1034]

In 1996, Allen C of the Delaware Court of Chancery held in *In Re Caremark International Derivative Litigation* that directors must make an attempt in good faith to oversee a company's business and that only a continuous or a systemic failure of oversight will fulfil the *mala fide* requirement to hold directors liable.[1035] *In Re Caremark supra* shows that directors must make an attempt in good faith to oversee a company's cybersecurity and that only a continuous or a systemic oversight on cybersecurity will establish the *bona fide* requirement, which shows that directors exercised their duty of care reasonably.[1036]

In Re Caremark supra also introduced two important concepts that relate to cybersecurity, namely 'red flags' and the 'director passive model'.[1037] Cybersecurity 'red flags' indicate any pattern of cyberincidents that led to a cyberbreach, which should have been detected, and that should have indicated the existence of cyberrisks to the board.[1038] The 'director passive model' again asks whether directors were proactive or reactive when cybersecurity 'red flags' appeared.[1039]

[1028] *Smith supra*.
[1029] *Ibid*.
[1030] *Ibid*.
[1031] *Ibid*.
[1032] *Ibid*.
[1033] *Ibid*.
[1034] *Ibid*.
[1035] *In Re Caremark International Inc. Derivative Litigation* 698 A.2d 959 (Del. Ch. 1996).
[1036] *Ibid*.
[1037] US FTC '*Fighting Identity Theft with the 'Red Flag' Rule,' s.p.*, available online at <https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business>, last accessed on 12 July 2021.
[1038] US FTC *op cit s.p*.
[1039] *Ibid.*

In 2006, Holland J of the Supreme Court of Delaware held in *Stone v Ritter* that if directors do not act when they know they had a duty to act, they ignore their responsibilities, and in doing so, they breach their duty of care by not acting in good faith.[1040] With the continuous occurrence of cyberrisks, directors should know that they have a duty to act to prevent cyberbreaches and that the duty of care requires directors to exercise due care in their oversight, and that it is breached if directors do not implement a cybersecurity policy, or if it is implemented, and they fail to oversee it.[1041]

In 2009, Chandler C of the Delaware Court of Chancery held in *In Re Citigroup Inc. Shareholder Derivative Litigation* that directors should implement and oversee a proper cybersecurity policy with a reporting function to disclose any fraudulent or criminal conduct.[1042] This means that the duty of care requires the building of cyberresilience through the proactive discovering and prevention of cyberrisks.[1043]

In 2013, Laster, CJ of Delaware's Court of Chancery held in *In Re Trados Inc. Shareholder Litigation* that the BJR is Delaware's default review standard.[1044] He explained that the BJR presumes that when directors make a business decision, that they acquainted themselves with all of the relevant facts and circumstances, that they did so in good faith and in the honest belief that it would be in the company's best interests.[1045] Except when one of the BJR's elements is disproven, the court will only look at whether the business decision was rational, meaning that it was a logical way to advance the company's objectives.[1046] It is thus only in instances were a decision is void of a rationally conceivable basis that a court will find that it was made in bad faith and that it constitutes a breach of the duty of care.[1047]

In 2019, Strine CJ of the Delaware Supreme Court extended on *In Re Caremark supra* in *Marchand v Barnhill* when he held that directors must prove that they have made an effort in good faith to prevent important risks.[1048] As a result, directors will not be liable for a breach of their duty of care if they can prove that they have made an effort in good faith to oversee a company's cybersecurity in order to prevent cyberrisks.[1049]

[1040] *Stone v. Ritter* 911 A 2d 362 (Del. 2006).
[1041] *Ibid*.
[1042] *In Re Citigroup Inc. Shareholder Derivative Litigation* 964 A 2d 106 (Del. Ch. 2009).
[1043] Iaquinto *et al.* 'Cybersecurity and Privacy: Fiduciary Considerations and Dodd-Frank's Enterprise Risk Management' in the *Financier Worldwide* of April 2019, *s.p.*, available online at <https://www.hklaw.com/en/insights/publications/2019/04/cyber-security-and-privacy-fiduciary-considerations-and-doddfranks-ent>, last accessed on 11 July 2021.
[1044] *In Re Trados Inc. Shareholder Litigation*, Ct. of Ch. Del. 73A.3d 17.
[1045] *Ibid.*
[1046] *Ibid*.
[1047] *Ibid.*
[1048] *Marchand v. Barnhill* 212 A.3d 805 (Del. 2019
[1049] *Marchand supra* 805; LaCroix '*Recent Delaware Caremark Duty Decision Underscores Board Cybersecurity and Privacy Liability Risks,' s.p.*, available online at <https://www.dandodiary.com/2019/08/articles/director-and-

4.4.2.3. Georgia

In 2016, Thrash JR of the Northern District Court of Georgia, set aside a claim for damages in *In Re Home Depot Shareholder Derivative Litigation*, when he said that the plaintiffs did not prove that the board consciously failed to act in an instance where they knew they had a duty to act.[1050] He also explained that directors just need to make decisions that are reasonable, and that it does not have to be perfect decisions.[1051] This shows how important it is for directors to be able to prove that they consciously acted in an instance of a known duty to act, and that they have made decisions that are reasonable, even though they were not perfect decisions.[1052]

In 2019, in the Georgian Northern District Court, Thrash, J allowed a part of a motion and set aside the other part of a motion that was brought to dismiss in *In Re Equifax Inc. Securities Litigation*.[1053] This was a cyberbreach class action against Equifax Inc. and some of its directors due to a cyberbreach where hackers stole the personal information of customers.[1054] The leading plaintiff represented certain shareholders, and claimed that securities laws were violated and that the directors made false statements about a cyberbreach and the company's compliance with information protection law.[1055] The court set aside the claims against the directors, but denied the motion of the former CEO and chairperson, who had personal knowledge that the cybersecurity system was completely improper, but nevertheless made false statements on its inadequacy, while it was within their power to ensure that the company's cybersecurity policy was properly implemented.[1056] This shows that the court will not look kindly at directors who had personal knowledge that a cybersecurity system was completely improper, and who then made false statements on its inadequacy, while it was within their power to see to it that the company's cybersecurity policies could have been properly implemented.[1057]

4.4.2.4. Pennsylvania

A more subjective evaluation of the duty of care was done in 2015 by Schwab, DJ of the Pennsylvania Third Circuit Court of Appeals in *In Re Lemington Home for the*

---

officer-liability/recent-delaware-caremark-duty-decision-underscores-board-cyber-and-privacy-liability-risks/>, last accessed on 21 October 2020.

[1050] *In Re Home Depot Shareholder Derivative Litigation* 223 F. Supp. 3d 1317 (N.D. Ga. Nov. 30, 2016).

[1051] *Ibid.*

[1052] *Ibid.*

[1053] *In Re Equifax Inc. Securities Litigation* 357 F. Supp. 3d 1189 (N.D. Ga. Jan. 28, 2019).

[1054] *Ibid*.

[1055] *Ibid.*

[1056] *Ibid*.

[1057] *Ibid*.

Aged, even though it is not a cyberbreach case.[1058] In this case, Schwab DJ upheld a finding that directors must be held personally liable for a breach of their duty of care when they tolerated employees who underperformed and allowed employees who were unqualified to remain in their posts and failed to remove them after the consequences of their mismanagement of an old-age home became evident.[1059] Schwab DJ said that directors may rely on information and reports, but that these directors had actual knowledge of the mismanagement, yet looked the other way despite repeated signs that residents were given insufficient care.[1060] This case is completely consistent with the analysis in *In Re Caremark supra*, which noted that a continuous failure of the board to exercise due care in their oversight will constitute the lack of good faith that is needed to determine liability.[1061] Since *In Re Lemington Home supra* was about operational matters that later-on resulted in risks, its lessons are equally applicable to the failure to proactively implement and monitor a cybersecurity policy and system, and for not reacting reasonably after a cyberrisk occured.[1062]

4.4.2.5. Minnesota

In 2017, Benton DJ of the US Court of Appeal, District of Minnesota, Eighth District, held in *In Re Target Corp. Data Security Breach Litigation* that proper oversight over IT governance requires directors to ensure that proper cybersecurity policies and systems are implemented to respond to cyberbreaches.[1063] This finding confirms the importance of the implementation and continuous monitoring of a cybersecurity policy and system.[1064]

4.4.2.6. New Jersey

Although New Jersey codified the duty of care in its Administrative Code of 1969, it only has limited case law with no sustained clear position on the duty of care.[1065]

[1058] *In Re Lemington Home for the Aged* 13-2707 (3d Cir. 2015).
[1059] *Ibid*.
[1060] *In Re Lemington Home for the Aged supra*; Sarkar '*Director and Officer Liability and Cyber-Security: Four Questions Every Officer and Director Must Answer (Part 2 of 3),' s.p.*, available online at <https://www.linkedin.com/pulse/director-officer-liability-cyber-security-4-questions-richik-sarkar-2e>, last accessed on 14 May 2021.
[1061] *In Re Caremark supra*; Sarkar *op cit s.p.*
[1062] *In Re Lemington Home for the Aged supra*; Sarkar *op cit s.p.*
[1063] *In Re Target Corp. Data Security Breach Litigation* US District Court, D Minnesota 66F. Supp. 3d 1154 (D. Minn. 2014).
[1064] *Ibid.*
[1065] New Jersey Administrative Code of 1969; Kershaw *The Foundations of Anglo-American Fiduciary Law op cit* Part 11, section 6(c).

In 2014 in *Palkon v. Holmes*, Chesler, J of District Court of New Jersey set aside a shareholder class action in the case against the chairperson, CEO and board of Wyndam Worldwide Corporation.[1066] In this instance, the action claimed that directors breached their duty of care after cyberbreaches took place from 2008 until 2010 and that this led to the loss of the personal information of more than 600,000 customers.[1067] The BJR was critical to Chesler J's decision making, and he found that the rule protected the directors because they held fourteen quarterly board meetings to discuss cyberrisks, and the company's cybersecurity policy and system.[1068] They appointed the audit committee, which met at least sixteen times to review the cybersecurity policy and system and to investigate the cyberbreaches.[1069] They also hired an IT company to recommend cybersecurity improvements, which the company had begun to implement, and had discussed the ways to enhance their cybersecurity numerous times prior to the cyberbreaches.[1070] This case sets an objective standard of the safeguards that will protect directors.[1071] It shows that when it comes to cybersecurity issues, the court will use strict standards and will specifically evaluate how boards went about to implement and monitor their cybersecurity policies and systems.[1072] This finding also indicates that when directors follow a process with due care by proactively implementing and monitoring a cybersecurity policy and system – even if it is not successful – it will help to protect them from being held liable for a cyberbreach.[1073]

In 2015, Ambro CJ of the US Court of Appeal, District of New Jersey, Third Circuit held in *US FTC v Wyndham Worldwide Corp. et al.* that when it needs to be determined whether directors have performed their duty with care, the court will seek evidence whether the board acted in a deliberate and informed manner and identified and explored alternative avenues.[1074] The court will also determine whether the company conducted a proper investigation and whether the board acted when they became aware of cyberrisks.[1075] This case shows that the court will seek evidence whether the board acted in a deliberate and informed manner and identified and explored alternative avenues, and as such, directors need to ideally minute all of their decisions on cybersecurity by means of a decision manifesto to serve as proof that they conducted a proper investigation and acted when they became aware of cyberrisks.[1076]

[1066] *Palkon v Holmes* 2014 WL 5341880, D.N.J.
[1067] *Ibid.*
[1068] *Ibid*.
[1069] *Ibid*.
[1070] *Ibid.*
[1071] Sarkar *op cit s.p.*
[1072] *Ibid.*
[1073] *Ibid.*
[1074] *US FTC v Wyndham Worldwide Corp. et al.* US District Court, District of New Jersey 13 – 01887.
[1075] *Ibid*.
[1076] *Ibid.*

5. REMEDIES FOR DIRECTORS WHO BREACHED THEIR DUTY OF CARE IN RELATION TO CYBERSECURITY

This section will explain the remedies that are available to SA directors who breached their duty of care in relation to cybersecurity.

5.1. The Act, section 71(5): Taking the Removal of a Director on Review

A director who is removed from office in terms of the Act, section 71(5), by a board or the Companies Tribunal, or by a person who had directly appointed them, has 20 business days to go to court on review.[1077] This section also states that any director who voted in favour of the resolution to remove a director, or any shareholder who has voting rights to elect that director, can also take such a matter to court for review.[1078]

5.2. The Act, section 76(4): Business Judgment Rule (BJR)

The BJR is the default review standard of directors' conduct in Delaware and this provision has since been codified in the Act.[1079] The Act, section 76(4) contains the legislative BJR provision and states that a director or employee is not liable for acts of mere negligence because the court will not interfere with the business judgement of directors where no bad faith, fraud or lack of care occurred.[1080] The BJR in other words protects a decision which directors made, even if it afterwards turns out to have been the wrong decision in the circumstances, as long as it was made in terms of the prescribed set of criteria of section 76(4).[1081] This means that directors may exercise their discretion *bona fide* in a manner that they deem to be in the best interests of the company, and not in a manner that the court deems to be in the best interests of the company.[1082] In 2011, Makgoba, J of the North Gauteng High Court explained in *Swart v Beagles Run Investments 25 (Pty) Ltd and Others* (2011) (5) SA 422 (GNP) that the directors' decision must be in the company's best interests, even if it is disadvantageous to the shareholders.[1083]

This provision determines that a director would be in line with section 76(3)(b) and (c) if they took reasonably diligent steps to inform themselves on the content of a

---

[1077] The Act, section 71(5).
[1078] *Ibid.*
[1079] The Act, section 76(4)(a)-(b).
[1080] The Act, section 76(4); Naidoo *op cit* 213.
[1081] Naidoo *op cit* 212.
[1082] Mupangavanhu *Directors Standards of Care, Skill, Diligence and the BJR in View of SA's Companies Act 71 of 2008: Future Implications for Corporate Governance*, PhD Thesis submitted at the University of Cape Town, 2016, 58.
[1083] *Swart v Beagles Run Investments 25 (Pty) Ltd and Others* (2011) (5) SA 422 (GNP); Du Plessis *et al. op cit* 297.

business decision.[1084] Section 76(4)(a) requires that directors should have had all the information available before they made a decision.[1085] The BJR determines that directors will not be held liable for any damage, which the company has suffered, if it was caused by their judgment errors when they acted in good faith and in the best interests of the company, and as such, it protects directors who acted honestly from hindsight bias.[1086]

When directors make a business decision, they have to consider various interests from their own personal value position on what they deem to be in the company's best interests.[1087] Should directors make poor decisions they could be held personally liable for any losses that the company incurred.[1088] The BJR is thus a 'safe harbour' provision for directors against personal liability because it limits the court's scrutiny of their business decisions.[1089]

In this regard, section 76(4) states that a director (a) would have acted in the company's best interests and with the degree of care that is expected from someone who has (i) the same function; and (ii) the same experience and skills, if - (i) the director made a reasonable attempt to acquaint him/herself on a matter; and (ii) either (aa) had no personal material interest in it; or (bb) had no personal financial interest in it, and had a rational basis to believe that it was in the company's best interests; and if they were (b) entitled to base their business decision on - (i) the performance by anyone - (aa) to whom the board have delegated a duty; and (ii) any information presented by such an employee.[1090]

The duty of care does not require boards and individual directors to make perfect decisions, but only to act with the required duty of care in the circumstances.[1091] As a result, the BJR serves as a presumption that protects directors against liability when they make a business decision in good faith, but it later turns out to be unsuccessful.[1092]

When an alleged breach of the duty of care in relation to cybersecurity occurred, the BJR will provide the court with a test to review a director's conduct.[1093] So the duty of care in relation to cybersecurity is the standard for directors' conduct, while the BJR is the standard to review directors' conduct.[1094]

[1084] The Act, sections 76(3)(b) - (c); 76(4)(a)(i); Naidoo *op cit* 212.
[1085] The Act, section 76(4)(a).
[1086] The Act, section 76(4); Cassim *et al. Contemporary Company Law op cit* 759.
[1087] Ramnath *Interpreting Directors' Fiduciary Duty to Act in the Company's Best Interests Through the Prism of the Bill of Rights: Taking Other Stakeholders Into Consideration* 112.
[1088] *Ibid*.
[1089] The Act, section 76(4).
[1090] The Act, sections 76(4)(a)(i)-(iii).
[1091] Lunn *op cit* 9.
[1092] *Potter v. Pohlad*, 560 NW2d 389 (Minnesota Court of Appeals 1997); Naidoo *op cit* 212.
[1093] The Act, section 76(4); Naidoo *op cit* 212.
[1094] The Act, section 76(4); Naidoo *op cit* 212.

The requirement of a rational basis for the decision has an objective test and requires that the decision should be one that anyone else in a similar position as the director would have reached.[1095]

In 2004, Moseneke J, of the SA Constitutional Court (CC) explained in *Minister of Finance v Van Heerden* that a decision with a rational basis must have a reasonable likelihood of meeting its desired outcome.[1096] He explained that a director is not required to make an exact prediction of a decision's outcome, because this will set the standard too high and thereby make the BJR ineffectual.[1097]

The Act, section 76(4)(a)-(b) presumes that when a director made a business decision, that it was made on an informed basis and in the honest belief that it was made in the company's best interests.[1098] Except when one of the BJR's requirements is refuted, the court will only look at whether the business decision was rational and helped to promote the company's goals.[1099]

The Act, section 1, does not explain what a company's 'best interests' are and the concept is thus open to interpretation.[1100] If it is interpreted liberally, its meaning is far broader than the profit maximisation of shareholders and includes board decisions on cybersecurity that will also benefit stakeholders.[1101]

It is difficult to apply the BJR when directors have to base their decisions on a matter on which they do not have guidance and on which there is legal uncertainty.[1102] One needs to remember that directors just have to conduct the business of the company in terms of the applicable law.[1103] The legal obligations of directors in terms of their duty of care in relation to cybersecurity and the use of AI are not always clear and some of these aspects must often be interpreted reasonably.[1104] This is because certain aspects of the duty of care in relation to cybersecurity has not yet been decided on in case law, and because industry custom is inconclusive.[1105] As a result, directors have to take decisions that are based on uncertain legal aspects on which they have very limited guidance.[1106]

Since the BJR only became part of SA law in 2008 when the Act was promulgated, SA courts still have to provide case law on how it will be applied to the

---

[1095] Cassim *et al. Contemporary Company Law op cit* 750 - 753.
[1096] *Minister of Finance and Other v Van Heerden* (2004) 12 BLLR 1181 (CC).
[1097] The Act, section 76(4); *Minister of Finance supra.*
[1098] The Act, section 76(4)(a)-(b).
[1099] Lunn *op cit* 9; Naidoo *op cit* 213.
[1100] The Act, section 1.
[1101] The Act, section 76(3)(b); Ramnath *op cit* 113.
[1102] Eisele *Codification of the BJR in the SA Companies Act 2008, Section 76(4)*, LLM thesis submitted at the University of Stellenbosch in 2017 49.
[1103] *Ibid*.
[1104] See Chapter 1, section 11.5.
[1105] *Ibid.*
[1106] *Ibid.*

duty of care in relation to cybersecurity.[1107] As a result, US case law on the duty of care in relation to cybersecurity will need to provide guidance on how the BJR should be interpreted in SA law.[1108]

It will be difficult for the court to apply the BJR when there is limited legal guidance on an aspect, such as the duty of care in relation to cybersecurity and the responsible use of AI.[1109] The BJR should avoid hindsight bias.[1110] Since there is limited guidance on the responsible use of AI, and because judges are not cybersecurity experts, it will be difficult for them to apply the BJR in instances which involve the use of AI for cybersecurity after a cyberbreaches occurred.[1111]

In 1998, Horsey, J of the Delaware Supreme Court said in *Grobow v Perot* that US case law places a big focus on the important role that good faith plays when the courts apply the BJR.[1112] The Act, section 76(4) not only makes no mention of this requirement, but it also does not explain why it was excluded in the Act.[1113] Good faith is a so-called 'catch-all' requirement that could have been used to determine what formed the heart of a certain business decision.[1114] Fortunately, the Act, section 5(2) allows SA courts to interpret or apply foreign law, if it is appropriate, and as a result, SA courts may turn to US case law to help explain that good faith plays an important part when it comes to the interpretation of the requirements of the BJR.[1115]

In addition, the Act, section 76(4) does not specifically call the BJR with this name, as it is called in the US.[1116] This then begs the question whether the decisions that relate to the duty of care in relation to cybersecurity will be deemed to constitute 'business decisions' for the intents of section 76(4)?[1117] It is thought that since section 76(4) does not refer to the BJR itself as a 'business judgment rule' in so many words, that this section may be interpreted to protect directors who took decisions that lay beyond the protection of only business (in other words, financial) decisions and that the decisions that a director took when they exercised their duty of care in relation to cybersecurity will also be covered.[1118]

[1107] The Act, section 76(4)(a).
[1108] See Chapter 3, section 4.4.
[1109] Leach *The Correct Understanding of the BJR in the Companies Act 71 of 2008, Section 76(4): Avoiding the American Mistakes*, LLM Thesis submitted at the University of Cape Town in 2017 36.
[1110] Osode *et al.* 'The Nature and Evolution of the BJR and Its Transplantation to SA under the Companies Act of 2008' in *Speculum Iuris* 33(1) 2019 27-28.
[1111] *Ibid.*
[1112] *Grobow v Perot* 539 a.2d 180 (Del. 1988).
[1113] The Act, section 76(4)(a).
[1114] *Grobow supra.*
[1115] The Act, section 5(2).
[1116] The Act, section 76(4).
[1117] *Ibid.*
[1118] *Ibid.*

Keay and Loughrey explain that the labelling of a decision as a business decision can prevent that directors are held accountable for their decisions.[1119] In their research they evaluated the nature of business decisions and why they are protected.[1120] Their research shows that the courts in the UK and US use this concept either as an ability or as a decision.[1121] They explain further that although both interpretations link with directors' role to help create wealth, their research shows that decisions which relate to corporate governance matters are not of a business nature and are therefore less likely to be regarded as business decisions.[1122]

Keay and Loughrey *et al.* also evaluated the sentiments of directors worldwide on how they feel about the notion of judicial review of their business judgements.[1123] Interestingly enough they found that most directors were receptive of the idea of some form of review and that they were not necessarily negatively inclined towards the judicial review of their business decisions.[1124] They consequently propose that the debate about whether the courts should review directors' business judgements should cease and should instead start to support it.[1125]

5.3. The Act, section 77(9): The Court's Relief of a Director

Section 77(9) explains that in any proceedings against a director, besides matters that are related to wilful breach of trust or wilful conduct, the court may relieve the director, either totally or in part, from any liability, if the court is of the opinion that such a director has acted honestly and reasonably.[1126]

This means that when the court applies the BJR and determines that the decision, which directors reached, were not made in a company's best interests, the court may in terms of section 77(9)(b) still not hold a director liable if it would be fair in the circumstances to excuse them.[1127]

5.4. The Act, section 78: Indemnity Insurance

[1119] Keay, Loughrey 'The Concept of Business Judgment' in *Legal Studies* 39(1) March 2019 36.
[1120] Keay, Loughrey 'The Concept of Business Judgment' *op cit* 36; See Chapter 3, section 3.5.
[1121] Keay, Loughrey 'The Concept of Business Judgment' *op cit* 36.
[1122] *Ibid.*
[1123] Keay, Loughrey *et al.* 'Reviewing Directors' Business Judgments: Views from the Field' in *Journal of Law and Society* 47(4) (November 2020) 639 - 640.
[1124] *Ibid.*
[1125] *Ibid.*
[1126] The Act, section 77(9).
[1127] The Act, sections 77(9)(b).

In terms of section 78, a company may take out indemnity insurance to protect a director.[1128] Section 78(1) allows the company to also indemnify former directors.[1129] Section 78(6) however states that a company is not allowed to indemnify a director against (a) any liability that arose (i) in terms of section 77(3)(a)-(c).[1130]

5.5. The Act, section 165(3): Application to Set Derivative Action Aside

In the event of a derivative action, section 165(3) explains that when a demand is served on the company, the company has 15 business days to ask the court to set it aside if it has no merit.[1131]

5.6. Contract Breach

A director who was appointed with a fixed-term contract, but who is then removed from that position without any cause by means of an ordinary resolution of the shareholders, before the contract has expired, may institute a claim for contract breach against the company.[1132] In 2008, Davis, AJ of the SA Labour Appeal Court (LAC) held in *Amazwi Power Products (Pty) Ltd v Turnbull* that in the event that an executive directors resigns as a director, but still works as an employee of the company, the ending of such employment will be deemed as a dismissal.[1133] In 2009 this was also the opinion of Ngalwana, AJ of the SA Labour Court in *SA Post Office Ltd v Mampeule*.[1134]

5.7. Unfair Dismissal

In 2004, Revelas, J, of the Johannesburg Labour Court explained in *PG Group (Pty) Ltd v Mbambo NO and Others* that in the event of an unfair dismissal, the best remedy will most likely be monetary compensation since reinstatement would seem impossible.[1135]

6. NO DIFFERENTIATION BETWEEN EXECUTIVE AND NON-EXECUTIVE DIRECTORS

[1128] Camillo *op cit s.p.*
[1129] The Act, section 78(1).
[1130] The Act, sections 77(3(a) – (c); 78(6)(a)(i).
[1131] The Act, section 165(3).
[1132] Ncube 'You're Fired! The Removal of Directors under the SA Companies Act 71 of 2008' in the *SA Law Journal* (2011) 128 47.
[1133] *Amazwi Power Products (Pty) Ltd v Turnbull* (2008) 9 BLLR 817 (LAC); Ncube *op cit* 48.
[1134] *SA Post Office Ltd v Mampeule* (2009) 8 BLLR 792 (LC); Ncube *op cit* 48.
[1135] *PG Group (Pty) Ltd v Mbambo NO and Others* (JR215/2004) 92004) ZALCJHB 8 (26 October 2004); Ncube *op cit* 49.

For some time there was legal uncertainty about the exact standard of care that was required from non-executive directors.

In an attempt to clarify this matter, Chitty J of the British High Court held in 1884 in *Re Denham & Co* that non-executive directors do not need to pay constant attention to a company's affairs, and that they only have to perform the duty of care at board meetings and related meetings.[1136] In addition, he said that such directors do not have to attend all meetings, but that they should try when it is reasonably possible.[1137]

The matter re-surfaced in 1925 in *Re City Equitable Fire Insurance Co Ltd supra* when Romer J of the British Court of Appeal of England and Wales differentiated between the duty of care that is required from an executive director, who oversees the company full-time, and a non-executive director, who only oversees the affairs on an irregular basis.[1138]

In 1983 Margo J of the Witwatersrand Local Division reaffirmed in *Fisheries Development Corporation of SA Ltd supra* these findings of Chitty J and Romer J and affirmed them as being part of SA Company Law.[1139]

In 1991, Goldstone, J of the SA SCA however held in *Howard v Herrigel NO and Another* that the common law determines that as soon as someone is appointed as a director, they need to exercise the highest good faith to the company in their endeavours.[1140] He said that in principle, no difference exists between executive and non-executive directors when it comes to their duties, but when a director's conduct needs to be judged, it is a factor that may be looked at.[1141]

In 2008 the Act was promulgated, and section 1 says a director is a board member and includes an alternate director (a synonym for a non-executive director) in this definition.[1142] As such, the Act does not differentiate between an executive, or a non-executive or an independent non-executive director and the duty of care in relation to cybersecurity is thus equally applicable to all the different designations of directors.[1143]

7. LESSONS FROM A LEGAL COMPARISON OF THE SA, UK AND US DUTY OF CARE IN RELATION TO CYBERSECURITY

[1136] *Re Denham & Co* (1884) LR 25 Ch D 752.
[1137] Kanamugire *et al. op cit* 71.
[1138] *Re City Equitable Fire Insurance Co Ltd supra* 407.
[1139] *Fisheries Development Corporation of SA Ltd supra* 156.
[1140] *Howard v Herrigel NO and Another* (130/89) (1991) 2 AII SA 113 (A).
[1141] *Ibid.*
[1142] The Act, sections 1, *s.v.* 'director'; 66; Deloitte '*Duties of Directors,*' 5, available online at <https://www.google.com/search?q=deloitte+duties+of+directors&rlz=1C1AOHY_enZA708ZA708&oq=Deloitte+Duties+&aqs=chrome.1.69i57j0l4j69i61.5172j0j8&sourceid=chrome&ie=UTF-8>, last accessed on 13 December 2019.
[1143] The Act, sections 1, *s.v.* 'director'; 66; Blackman *et al. op cit* 8-12; Deloitte '*Duties of Directors' op cit* 5.

The SA Constitution, section 39(1) says that when a court interprets the Bill of Rights, it (b) must consider international law; and (c) that it may consider foreign law.[1144]

In addition, the Act, section 5(2) states with regards to its general interpretation that a court may interpret or apply foreign company law when it applies the Act, if it is appropriate to do so.[1145]

The further interpretation of the duty of care in relation to cybersecurity in SA through international and foreign law, especially UK case law on the duty of care and US case law on how the BJR is applied in cybersecurity cases will help SA courts to interpret the legislative duty of care in relation to cybersecurity.[1146] Since the SA Constitution of 1996 and the Act both allow SA courts to look at foreign law when they interpret the Act, SA courts may draw on the examples and best practices from UK case law on the duty of care and US case law on the BJR that were highlighted.[1147]

Both the Act, section 76(3)(c) and the UK Companies Act of 2006, section 174 espouse an objective and subjective standard in the duty of care, skill and diligence.[1148] In the US, the MBCA of 2016, section 8.30 again sets out the duty of care and states that directors shall perform their duties (a)(1) in good faith; (2) with the care that an ordinary prudent person would reasonably believe to be appropriate in similar circumstances; and (3) in a way that the director reasonably believes will be in the company's best interests.[1149]

According to Cassidy, the Act, section 76(3)(c) could be interpreted to mean that both the objective and subjective standards, as is the case with the UK Companies Act of 2006, section 174, apply to each element of care, skill and diligence.[1150]

The Act has been criticised on the nature of the interaction between sections 76(3)(c)(i) and 76(3)(c)(ii).[1151] Bekink explains that the wording of the Act, section 76(3)(c) creates the potential for the court to subject the legislative duty of care to the subjective common law standard.[1152] He compares the wording, "that director," of the Act, section 76(3)(c)(i) with the wording, "the general knowledge, skill and experience of that director," of section 76(3)(c)(ii), and comes to the conclusion that the words of the subjective considerations in section 76(3)(c)(ii) seems to subject the objective standard in section 76(3)(c)(i).[1153] Cassidy points out that the wording of the duty of care in the

---

[1144] SA Constitution of 1996, section 39(1)(a)-(c).
[1145] The Act, section 5(2).
[1146] The Act, section 76(3)(c).
[1147] *Ibid.*
[1148] The Act, section 76(3)(c); UK Companies Act of 2006, section 174.
[1149] US MBCA of 2016, section 8.30(a)(1)-(3).
[1150] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; Cassidy *op cit* 385.
[1151] The Act, section 76(3)(c); Cassidy *op cit* 385.
[1152] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; Bekink *op cit* 110.
[1153] The Act, section 76(3)(c)(i)-(ii); Cassidy *op cit* 385.

UK Companies Act of 2006, section 174 does not seem to subject the objective standard to subjective considerations.[1154]

The US MBCA of 2016, section 8.30 does not look in similar detail at the different requirements of the duty of care when it is compared with the Act and the UK Companies Act of 2006.[1155] The wording of the MBCA of 2016, section 8.30 only looks at the standards of care and diligence.[1156] Cassidy makes an interesting observation when she points out that the test in the MBCA of 2016, section 8.30 contains both elements of subjectivity and objectivity.[1157] In this regard, the reference to an "ordinary prudent person" objectifies the standard.[1158] She elaborates that the test's objectivity is strenghtened by the requirement that the director's conduct must conform to the conduct of an "ordinary prudent person" who is "in a like position and under similar circumstances."[1159] This then means that the MBCA of 2016, section 8.30's duty of care takes the circumstances into account within which a director performs their power and functions, as is the case with the objectivity standard in the Act, section 76(3)(c)(i).[1160]

As is the case with the UK Companies Act of 2006, section 174(2)(a), the Act section 76(3)(c)(i) sets a minimum objective standard to evaluate the conduct of directors.[1161] The standard is the nature of the conduct which can reasonably be expected from someone who performs "the same functions in relation to the company as those carried out by that director."[1162] Bekink points out that the word "having" in the Act, section 76(3)(c)(ii) in terms of someone "having the general knowledge, skill and knowledge of that director," serves to subject the minimum objective standards to the subjective ability of that director.[1163]

In SA, the duty of care originates from the common law, and although it is now enacted by the Act, section 76(3), the common law still applies.[1164] The Act does not have a provision like the UK Companies Act of 2006, section 170(3)-(4), which provides guidance on the interaction between the common law and legislative duties of care.[1165] The Act consequently leaves it open to interpretation whether legislation supersedes the common law, whether they co-exist, or whether the common law should be used to help

---

[1154] The Act, section 76(3)(c); UK Companies Act of 2006, section 174.
[1155] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; US MBCA of 2016, section 8.30.
[1156] US MBCA of 2016, section 8.30(a)(1)-(3); The Act, section 76(3)(c); Cassidy *op cit* 385.
[1157] Cassidy *op cit* 385.
[1158] *Ibid*.
[1159] *Ibid*.
[1160] *Ibid*.
[1161] The Act, section 76(3)(c)(ii); UK Companies Act of 2006, section 174(2)(a).
[1162] The Act, section 76(3)(c)(i).
[1163] The Act, section 76(3)(c)(ii).
[1164] The Act, section 76(3); Blackman *et al. op cit* 8-29; Delport *et al. Henochsberg on the Companies Act op cit* 298; Kanamugire *et al. op cit* 71.
[1165] The Act; UK Companies Act of 2006, sections 170(3)-(4).

interpret the Act, section 76(3)(c).[1166] Hopefully a SA court will provide guidance on the interpretation of the Act, section 76 in this regard in future.[1167]

Unlike the UK Companies Act of 2006, the Act, section 76(4)(a)-(b) incorporated a 'safe harbour' provision to a breach of the duty of care, in the form of the BJR.[1168] In this regard, the Act, section 76(4)(b)(i) allows directors to state that they delegated a certain task or that they relied on certain information to reach their business decision.[1169] The Act, section 76(5) even provides a list of people on whose information directors may rely when they exercise their duty of care.[1170] The UK Companies Act of 2006 does not have a BJR, nor the defences of delegation and reliance.[1171] Since the BJR in the Act, section 76(4) is an import from US legislation, it is anticipated that US law can play a big role to provide guidance to the SA courts with its application.[1172]

It needs to highlighted that the duty of care in the US differs from the same duty as it is applied in the UK and SA, and although it has elements that could prove beneficial to these two jurisdictions, it cannot be extrapolated and applied without challenges.[1173] An example in this regard is that gross negligence is sometimes used as a standard of review, as was the case when Herrmann, CJ of the Supreme Court of Delaware used it in 1985 in *Smith supra* instead of mere negligence.[1174] It is submitted that the usage of a standard of gross negligence is not the most appropriate solution to serve as a general review standard for the duty of care when it is compared to the legislation of other jurisdictions.[1175]

It was explained that when the Act, section 76(3)(c) is read with King Report IV, principle 12 on IT governance, it does increase the expectation of a director's duties in relation to cybersecurity.[1176] A court would therefore also need to consider the recommendations that the King Code prescribes when it determine a director's liability.[1177]

Since the Act, section 24(1)(a) already allows the company to store information online, a director should be allowed to use aspects of AI, such as Consultative AI and Data Analysis to help analyse such information in order to gain greater insights from the information, especially if it can help to improve cybersecurity.[1178] The duty of care and

---

[1166] The Act; UK Companies Act of 2006, section 170(4).
[1167] The Act, section 76.
[1168] The Act, section 76(a)-(b); UK Companies Act of 2006.
[1169] The Act, section 76(4)(b).
[1170] The Act, section 76(5).
[1171] The Act, section 76(4).
[1172] *Ibid.*
[1173] *In Re Caremark supra*; US FTC '*Fighting Identity Theft with the 'Red Flag' Rule' op cit s.p.*
[1174] *Smith supra.*
[1175] *In Re Caremark supra*; US FTC '*Fighting Identity Theft with the 'Red Flag' Rule' op cit s.p.*
[1176] The Act, section 76(3)(c); IoDSA '*King Report IV*' *op cit* principle 12; Burger *op cit s.p.*
[1177] *Ibid.*
[1178] The Act, section 24(1)(a); Andrade *et al. op cit* 26.

diligence requires an objective test, while the duty of skill uses a subjective test, since each person's skillset differs.[1179] When one thinks about the information-overload that confronts a director, it is possible for the courts to allow a reasonable director to use Consultative AI and Data Analysis when they properly exercise their duty of care in relation to cybersecurity, whenever the court needs to apply the objective test of section 76(3)(c).[1180] The wording of section 76(3)(c) could be interpreted to allow directors to integrate and rely on AI when they analyse information in order to gain greater insights from it.[1181]

In summary, with increased cyberattacks and cyberbreaches, UK and US law are starting to establish responsibility in the event of a cyberbreach.[1182] Legislation is starting to cite specific requirements that boards need to conform with when they exercise their duty of care in relation to cybersecurity and in some instances boards are even required to demonstrate that they have implemented a cybersecurity strategy in the form of a policy and system, which is based on their company's cyberrisk profile.[1183] US state law is also starting to outline how directors need to exercise their duty of care in relation to cybersecurity, such as the Colorado Privacy Act, section 1-1-1308(5) and the NYPA of 2021, section 5642.[1184]

It seems that the most important components that directors need to include when they exercise their duty of care in relation to cybersecurity is the evaluation of the potential cyberrisks that faces their company, determining the likelihood that these cyberrisks may occur, and what losses or damage may result, and to then put the adequate precautionary measures in place to prevent such a cyberattack.[1185] The important thing is that SA directors need to follow a process in this regard and that they need to keep evidence of how they applied their minds and reached decisions and implemented and oversaw proper cybersecurity measures to help make their company cyberresilient.

8. CONCLUSION

Chapter 3 looked at the directors' duty of care and how directors in other jurisdictions exercise their duty of care in relation to cybersecurity.

A focus was placed on the UK and US positions on the duty of care in relation to cybersecurity in order to contrast it to the SA position by means of a legal comparison.

[1179] The Act, section 76(3).

[1180] The Act, section 76(3)(c); Andrade *et al. op* 26.

[1181] *Ibid.*

[1182] Johnson *op cit* 255.

[1183] *Ibid*.

[1184] Colorado Privacy Act of 2021, section 1-1-1308(5); New York Privacy Act of 2021, section 6542.

[1185] Duty of Care Risk Analysis Standard (DoCRA) Council '*The Duty of Care Risk Analysis Standard,' s.p.*, available online at <https://www.docra.org/>, last accessed on 16 June 2022.

The remedies for directors who breached their duty of care in relation to cybersecurity were evaluated; and the position of non-executive directors was also looked at in order to represent the position of all directors.

Lastly, lessons were drawn how directors should exercise their duty of care in relation to cybersecurity in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted. It was explained that UK case law on the duty of care and US case law on how the BJR is applied in cybersecurity cases will help SA courts to interpret the legislative duty of care in relation to cybersecurity.[1186]

Carrying on, the next chapter will look at the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG considerations.

[1186] The Act, sections 76(3)(c); 76(4).

CHAPTER 4:

THE INDIRECT IMPACT OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY ON CORPORATE GOVERNANCE AND CORPORATE SOCIAL RESPONSIBILITY (CSR) AND ECONOMIC, SOCIAL AND GOVERNANCE (ESG) INVESTMENT CONSIDERATIONS

1. INTRODUCTION

Where the previous Chapter focused on the duty of care and its application on cybersecurity, this Chapter will look at the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG investment considerations in order to look how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.[1187]

It was previously explained that other researchers only looked at OMs as a tool to improve corporate governance and CSR, so this chapter will explain that directors' oversight on good corporate governance practices and their integration of CSR and ESG considerations with the use of AI and Blockchain technology, will improve companies' cyberresilience and will especially help to make their OMs more cyberresilient in order to help attract investors. Since SA is a country which tries to attract FDI, it is important that SA directors take cognisance of what investors from these two important trading partners of SA look at, when they decide to invest in a company.

This Chapter will consequently start by looking at the evolution of the focus that the international corporate governance regime initially placed on CSR considerations, thereafter on the concept of sustainability, and how the gradual focus on ESG considerations came about. Then it will look at the exercise of SA directors' duty of care in terms of corporate governance and CSR. Then it will look at the exercise of SA directors' duty of care in terms of ESG considerations. Specific attention will then be given to how corporate governance should regulate the directors' duty of care in relation to cybersecurity and the use of AI and Blockchain technology since this is a new field that is developing fast and directors will need to address the challenges that they present.

Lastly, lessons will be drawn on how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.

[1187] Amodu 'Stakeholder Protection and CSR from a Comparative Company Law Perspective' in *Journal of African Law* March 2020, 2.

2. THE EVOLUTION OF THE EMPHASIS ON CSR TO SUSTAINABILITY TO ESG INVESTMENT CONSIDERATIONS

The gradual change in the focus of the international corporate governance regime from CSR to ESG investing, changed the focus from the external consequences of companies' activities to investors' risk and return consequences when they make their investment decisions.[1188] The change in the focus of investors was caused when the concept of sustainability was introduced in the 1980s, because it required investors to think about the long term consequences of their investment decisions.[1189] The ESG model of investing has since become the universally accepted investment approach and it is regulated by various codes and requirements in each country, which are then rated in terms of prescribed criteria.[1190] This model in other words requires investors to take ESG considerations into account when they make their investment decisions in an attempt to minimise a company's environmental risks (such as climate change), social risks (such as any infrigements on human rights) and governance risks (such as ineffective corporate oversight), which could harm their investment.[1191] This model in other words focuses on the role that investors and their investments should play to help promote sustainable corporate practices instead of the traditional sole focus on the role of directors' decisions and their duties.[1192]

Due to their basic characteristics, CSR, sustainability and ESG have different meanings.[1193] Sustainability is the main goal of a company, while CSR and ESG are sub-models which are located within a company's respective corporate and financial domains.[1194] The ethical focus of CSR means that the company should exercise sufficient care in its physical context.[1195] The ethical choice of a company is not prescribed in any instrument, and acting according to it may not necessarily improve financial performance, although the upholding of ethical standards may yield such results over time.[1196] On its turn, sustainability is only focused on the protection of the company and the shareholders' investments and interests in the long term.[1197] On the

---

[1188] Esser *et al.* 'From a Financial to an Entity Model of ESG' in *European Organisation Business Law Review* (26 April 2021) 1.
[1189] *Ibid*.
[1190] *Ibid*.
[1191] Esser *et al. op cit* 2.
[1192] *Ibid*.
[1193] *Ibid.*
[1194] Ellis '*ESG vs Sustainability: What is the Difference?,' s.p.*, available online at <https://www.measurabl.com/esg-vs-sustainability-whats-the-difference/>, last accessed on 19 June 2023.
[1195] Esser *et al. op cit* 2.
[1196] Esser *et al. op cit* 2 – 3; Kershaw *et al.* 'Toward a More Ethical Culture in Finance: Regulatory and Governance Strategies' in Morris *et al. Capital Failure: Rebuilding Trust in Financial Services* 278 – 283.
[1197] Agudelo *et al.* in 'A Literature Review of the History and Evolution of CSR' in *International Journal of CSR* 1(2019) 18.

other hand, ESG looks at the financial risk and return consequences of investors and requires investors to integrate ESG considerations in their investment decisions as it will improve returns on their investment and will help to minimise the risks that are associated with such ESG factors.[1198]

2.1. The Origins and Development of CSR and ESG Investing

It is important to understand the origins and development of CSR and ESG investing and how the shift in the focus of the corporate governance regime came about.

Initially, in the 1930s, CSR began to evolve as corporate ownership started to gain traction and a clear differentiation between ownership and management started to develop.[1199] At the same time, policy makers started to focus on how companies should ideally be managed to help optimise growth.[1200]

After the end of the Second World War in 1945, the profit that some companies made from the War, sparked a debate about the social responsibilities of companies, as many thought that they should not just focus on profits, but should also consider the consequences of their actions.[1201]

In the Post-War era of the 1950s, CSR started to gain momentum and the debate started to focus on the obligations of companies to help rebuild wartorn countries and to pursue policies that ascribe to the values of the societies in which they find themselves.[1202]

In 1987, the World Commission on Environment and Development (WCED) published a report called, '*Our Common Future*,' also known as '*the Brundtland Report*,' which sets out guiding principles for sustainable development.[1203] This led to a clearer focus on sustainable development and a focus was the first time placed on the role that stakeholders need to play to enable sustainable development.[1204] This Report introduced the 'triple bottom line approach' to help balance a company's environmental, social and economic sustainability.[1205]

In the 1990s, a focus started to emerge on ESG considerations as the debate started to shift towards warning investors of the need to manage the sustainability risks

---

[1198] Esser *et al. op cit* 3.
[1199] Agudelo *et al. op cit* 3.
[1200] *Ibid*.
[1201] *Ibid*.
[1202] Hazen 'Social Issues in the Spotlight: The Increasing Need to Improve Publicly Held Companies' CSR and ESG Disclosures' in the *University of Pennsylvania Journal of Business Law* (2021) 745.
[1203] World Commission on Environment and Development (WCED) '*Our Common Future: The Brundtland Report of 1987,*' Part 2, available online at <https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf>, last accessed on 19 June 2023; Esser *et al. op cit* 5 - 6.
[1204] *Ibid*.
[1205] *Ibid*.

in their investment portfolios.[1206] ESG investing requires investors to integrate basic ESG considerations into their risk and return profile when they make a sustainable investment.[1207] Sustainable investment consequently requires investors to not invest in companies with poor ESG track records.[1208] It was also during this time that investors started to request investment managers to integrate ESG considerations into the investment decisions which they make on their behalf.[1209] Other related aspects, such as shareholder activism or engagement, as well as the measuring of positive environmental or social outcomes were also introduced and started to gain prominence.[1210]

In 2000, companies started to increasingly implement voluntary CSR initiatives after the UN Global Compact was launched.[1211] Five years later the International Finance Corporation (IFC)'s Conference Report of 2005, '*Who Cares Wins: Investing for Long-Term Value*' was published.[1212] This Report made recommendations to investors and portfolio managers how they should integrate ESG considerations in asset management.[1213] It was during this time that ESG reporting started to be measured by metrics according to prescribed criteria.[1214] The financial reformations that came after the Global Financial Crisis of 2008 gave further impetus to sustainability and ESG, while companies continued to report on their CSR activities.[1215]

In 2015, the UN launched its Sustainable Development Goals (SDGs), which helped to link the ethical dimension of CSR with the economy.[1216] In 2015, the G20 also established the Task Force on Climate-Related Financial Disclosures (TFCRFD), who compiled a framework for climate-related disclosures in an attempt to reduce the financial system's exposure to climate-related risks.[1217] In 2018, the International

---

[1206] WCED *op cit*, Part 2; Esser *et al. op cit* 5 - 6.
[1207] *Ibid.*
[1208] *Ibid.*
[1209] *Ibid.*
[1210] *Ibid.*
[1211] Agudelo *et al. op cit* 9; UN Global Compact '*About*,' *s.p.*, available online at <https://unglobalcompact.org/about>, last accessed on 19 June 2023.
[1212] Agudelo *et al. op cit* 9; International Finance Corporation (IFC) 'Who Cares Wins: Investing for Long Term-Value,' Conference Report, for *IFC Conference* which was held in Zurich on 25 August 2005, 1 – 4, available online at <https://www.scribd.com/fullscreen/16876744?access_key=key-mfg3d0usaiuaob4taki>, last accessed on 19 June 2023.
[1213] IFC *op cit* 4 – 5.
[1214] Hazen *op cit* 745.
[1215] Esser *et al. op cit* 8.
[1216] UN '*Sustainable Development Goals*,' *s.p.*, available online at <https://www.un.org/en/footballforthegoals?gclid=EAIaIQobChMI0qDjjsrP_wIVWRwGAB15kQAqEAAYASAAEgL8b_D_BwE>, last accessed on 19 June 2023; Bekaert *et al.* 'Sustainable Investment: Exploring the Linkage Between Alpha, ESG, and SDG's,' *Social Science Research Network (SSRN) Working Paper*, published on 23 May 2023, *s.p.*, available online at <file:///C:/Users/Julian/Downloads/SSRN-id3623459.pdf>, last accessed on 19 June 2023.
[1217] Task Force on Climate-Related Financial Disclosures (TFCRF) '*About*,' *s.p.*, available online at <https://www.fsb-tcfd.org/about/>, last accessed on 19 June 2023.

Capital Market Association (ICMA) published the '*Green Bond Principles*,' which are voluntary principles for the issuing of green bonds, for projects that will positively impact the environment.[1218] The EU 'Renewed Sustainable Finance Strategy and Implementation of the Action Plan on Financing Sustainable Growth of 2018' also helped to develop the ESG model further.[1219] This was followed further by the EU 'Regulation on Sustainability-Related Disclosures in the Financial Services Sector of 2019,' which requires financial companies to advise investors about their products' sustainability characteristics.[1220] This was further strengthened by the EU 'Regulation on the Establishment of a Framework to Facilitate Sustainable Investment of 2020,' which evaluates the sustainable investments.[1221]

2.2. The Characteristics of CSR and ESG Investing

The following characteristics highlight the differences between CSR and ESG investing further.

In terms of their focus, the CSR approach has a clear focus on the company's accountability and ethical responsibility towards the community within which it finds itself, while the ESG approach focuses on investors' concerns over the risk and return consequences of their investment's ESG considerations.[1222]

The transmission channel is also different because CSR is applied on the basis that boards will take the lead and compile and implement their companies' CSR policies, while ESG considerations require investors to take the lead when they make their investment decisions and to only invest in companies with a positive risk and return profile.[1223]

The board also plays a different role with each, because with CSR, the board is the implementing agent, while investors are the implementing agents in the case of ESG.[1224] Esser *et al.* says that ESG investing also require investors to engage with the board, but explains that this then happens in a context where existing shareholders'

[1218] International Capital Market Association (ICMA) '*Green Bond Principles (GBP): Voluntary Process Principles for Issuing Green Bonds*' of July 2021, 3 - 4, available online at <https://www.icmagroup.org/assets/documents/Sustainable-finance/2022-updates/Green-Bond-Principles-June-2022-060623.pdf>, last accessed on 19 June 2023.

[1219] *EU 'Renewed Sustainable Finance Strategy and Implementation of the Action Plan on Financing Sustainable Growth of 2018,' s.p.*, available online at <https://finance.ec.europa.eu/publications/renewed-sustainable-finance-strategy-and-implementation-action-plan-financing-sustainable-growth_en>, last accessed on 19 June 2023.

[1220] EU 'Regulation on Sustainability-Related Disclosures in the Financial Services Sector (2019/2088)' *s.p*.

[1221] EU 'Regulation on the Establishment of a Framework to Facilitate Sustainable Investment (2020/852)' *s.p.*

[1222] Esser *et al. op cit* 9.

[1223] *Ibid*.

[1224] Esser *et al. op cit* 10.

interests are considered first, to the detriment of the interests of a potential stakeholder, such an investor who wishes to invest in a company.[1225]

The measurement of the concepts is another important difference, because although CSR could be measured, ESG is measured far more regularly in practice, when investors base their investment decisions on metrics and the ratings which a company received in terms of prescribed criteria.[1226]

The introduction of ESG reporting frameworks were also an important contributor in the evolution from CSR to ESG.[1227]

Important recent events at the global level (such as the establishment of the TFCRD in 2015) and sectoral levels (such as ICMA's introduction of the '*Green Bond Principles*' in 2018) were more in accordance with the ESG model.[1228] In addition, important actions where the EU took the lead with their 'Renewed Sustainable Finance Strategy and Implementation of the Action Plan on Financing Sustainable Growth of 2018' and the 'Regulation on Sustainability-Related Disclosures in the Financial Services Sector of 2019' and the 'Regulation on Sustainability-Related Disclosures in the Financial Services Sector of 2019' and the 'Regulation on the Establishment of a Framework to Facilitate Sustainable Investment of 2020' helped to develop the ESG model further.[1229]

3. THE EXERCISE OF SA DIRECTORS' DUTY OF CARE IN TERMS OF CORPORATE GOVERNANCE AND CSR

SA has a corporate governance regime where different legal sources regulate corporate governance, and the regime draws from various sources, such as the SA Constitution of 1996, various acts, case law, regulations, King Reports I – IV, the SA Code for Responsible Investing in SA (CRISA Code) of 2011, JSE '*Listing*

[1225] Esser *et al. op cit* 10.

[1226] Gillan *et al.* 'Firms and Social Responsibility: A Review of ESG and CSR Research in Corporate Finance' in the *Journal of Corporate Finance* 66(February 2021) 18 – 21.

[1227] Green Finance Platform 'Non-Financial Reporting Directive (NFRD): Directive 2014/95/EU and the Proposal for a Corporate Sustainability Reporting Directive (CSRD),' *s.p.*, available online at <https://www.greenfinanceplatform.org/policies-and-regulations/non-financial-reporting-directive-nfrd-directive-201495eu-and-proposal>, last accessed on 19 June 2023; Esser *et al. op cit* 10.

[1228] ICMA *op cit s.p.*

[1229] EU 'Renewed Sustainable Finance Strategy and Implementation of the Action Plan on Financing Sustainable Growth of 2018' *op cit s.p.*; EU 'Regulation on Sustainability-Related Disclosures in the Financial Services Sector (2019/2088)' *s.p.*; EU 'Regulation on the Establishment of a Framework to Facilitate Sustainable Investment (2020/852)' *s.p.*

Requirements' and the JSE RIIS.[1230] The interdependence of these regulatory sources constitutes a 'mixed system' of corporate governance in SA.[1231]

Companies are held responsible for human rights violations, such as the violation of privacy, due to the SA Constitution of 1996, sections 8(2) and 39(2), which impose human rights obligations on them.[1232]

In addition, the Act, section 7(a) recognises the Bill of Rights as the basis of democracy in SA.[1233] Section 7(b) obliges the state to encourage compliance with the Bill of Rights and this means that the state needs to ensure compliance with the right on privacy when it comes to the directors' duty of care in relation to cybersecurity.[1234] Similarly, the Act, section 5(1) requires the Act to be interpreted so that it will promote compliance with the Bill of Rights.[1235] These provisions mean that the duty of care in relation to cybersecurity cannot be viewed in isolation, but that it must be interpreted with the human right on privacy and the subsequent protection of personal information.[1236]

Since the Constitution is the supreme law and because the Bill of Rights binds everyone, it also binds companies.[1237]

It was said earlier that in 1996, Hussain J of the Witwatersrand Local Division held in *Minister of Water Affairs and Forestry supra* that the courts will take the King Reports into account when they interpret and apply directors' common law and legislative duties.[1238] Directors consequently need to take reasonable measures to try and implement and follow the King Reports' good corporate governance principles and practices.[1239]

Corporate governance regulates the internal operations of a company in an ethical manner, while sustainability encourages the sustainable growth of the company in its environment.[1240] CSR in other words provides the nexus between corporate governance and the protection of the company's stakeholders.[1241]

A standard definition for corporate governance was given by the Cadbury Report, which explains that corporate governance aims to harmonise companies' economic and

---

[1230] SA Constitution of 1996; IoDSA '*King Reports I - V*' *op cit*; SA CRISA Code of 2011; JSE Listings Requirements *op cit s.p.*; Du Plessis *et al. op cit* 292.
[1231] *Ibid.*
[1232] SA Constitution, sections 8(2); 39(2).
[1233] SA Constitution, Chapter 2; The Act, sections 7(a)-(b).
[1234] *Ibid.*
[1235] The Act, section 5(1).
[1236] SA Constitution, Chapter 2; The Act, sections 5(1); 7(1)(a); Delport *et al. Henochsberg on the Companies Act op cit* 36.
[1237] SA Constitution, Chapter 2.
[1238] *Minister of Water Affairs supra*; Delport *et al.* 'The Duty of Care, Skill and Diligence: The King Report and the 2008 Companies Act' *op cit* 450; See Chapter 3, section 2.6.
[1239] IoDSA '*King Report III*' *op cit* 12.
[1240] SA CIPC *op cit s.v.* 'About,' *s.v.* 'Function'.
[1241] Amodu *op cit* 2.

social goals with companies' stakeholders' goals in an attempt to unite the interests of the company, the community, environment, shareholders and stakeholders.[1242] This is also the definition that the King Report II explained in its introduction.[1243] King Report IV elaborated on this by tasking the board with effective governance, and to practice ethical values, and to seek optimal performance and legitimacy within the company's community.[1244]

The Act provides no definition for corporate governance nor CSR. This is unfortunate, because CSR provides the nexus between corporate governance and stakeholder protection.[1245] King Report IV defines CSR in terms of good corporate citizenship and places the company as a role player in its community and environment – and defines it as an entity that has certain rights and responsibilities within that community and environment.[1246] Amodu explains that CSR is about acknowledging that the broader society is the company's licensor and that it should therefore invest in its community and environment and help to protect the community and environment.[1247]

The King Reports led to a change in thinking when it came to the traditional shareholder dominance theory and started to espouse stakeholder theory, which is a theory of organisational management and ethics.[1248] Of particular relevance is King Report I, section 10's explanation that a company is the nexus that binds the mutual interests of a company's various stakeholders.[1249] The company's stakeholders include different stakeholder groups, such as consumers, employees, managers, shareholders, society and suppliers and others who should all cooperate to further the well-being of the company to which they are all tied.[1250] This view consequently differs from the shareholder dominance theory, as it means that directors have a duty of care to look after the interests of all the stakeholders of a company, and not just the interests of the shareholders.[1251]

It is against this background important that directors must realise that corporate governance and CSR are not just legal principles, but that they are instead business concerns.[1252] Gwanyanya draws the link that the protection of the interests of a company's stakeholders is in its best interests as well as those of its shareholders.[1253]

[1242] UK Committee on Financial Aspects of Corporate Governance *op cit* 'Introduction,' paragraph 2.5.
[1243] IoDSA '*King Report II' op cit* 7.
[1244] IoDSA '*King Report IV' op cit* 11.
[1245] Amodu *op cit* 2.
[1246] *Ibid*.
[1247] *Ibid.*
[1248] Keay 'Stakeholder Theory in Corporate Law: Has It Got What It Takes?' in the *Richmond Journal of Global Law & Business* 9(3) 2010 254.
[1249] IoDSA '*King Report I*'*op cit* section 10.
[1250] *Ibid.*
[1251] *Ibid.*
[1252] Gwanyanya 'The SA Companies Act and the Realisation of Corporate Human Rights' in *Potchefstroomse Elektroniese Regsblad* of 18(1)(2015) *op cit s.p*.
[1253] *Ibid*.

He explains that when directors exercise due care over all stakeholders' interests and take it into account in their decision-making, it helps to create stability in the company's activities and environment from which all of the stakeholders, including the shareholders, stand to benefit.[1254] This means that the probability of community activism, consumer boycotts, employee strikes and supplier disagreements and other disrupting endeavours may be minimised if stakeholders feel that their fundamental rights, such as the right on their privacy or the protection of their personal information, are reasonably protected.[1255] In other words, the protection of stakeholders' interests amounts to a corporate strategy that is in companies' best interests, all of their stakeholders' best interests, as well as their shareholders' best interests, because it helps to create business certainty, sustainable growth and a stable physical and online environment for the company.[1256]

The directors' duty of care in relation to cybersecurity needs to play a more pro-active role to protect the online platform and its online databases, because it was shown that cyberbreaches could have negative consequences for companies, shareholders and stakeholders themselves and even the company's entire financial environment.[1257] Once cybercriminals obtain personal information, they could transfer funds out of shareholders/stakeholders' bank accounts, access and steal corporate intellectual property, access confidential shareholder records, alter corporate accounting records, access and adjust files, change grades or use trade secrets. For the company, it could lead to enormous fines, financial losses and court cases and thus requires a high degree of care from directors.

If the board do not exercise their duty of care in relation to cybersecurity properly, it could compromise the company's OM, online platform or its online databases and should a large scale cyberbreach occur, its repercussions can have continuing national and international consequences.[1258] For example, it was pointed out earlier that after the cyberbreach at Target Corporation in 2013, many banks had to limit the further personal debts of those affected, monitor any withdrawals on their accounts and provide them with new credit and debit cards.[1259] In other words, the compromised personal information of both shareholders and stakeholders could easily be used for financial gain, and as a result, disrupt the normal way in which they, as well as capital markets and the financial system functions.[1260]

[1254] Gwanyanya *op cit s.p.*
[1255] *Ibid.*
[1256] Lunn *op cit* 4.
[1257] See Chapter 1, section 2.
[1258] Slaughter and May '*Cybersecurity: Corporate Insights for Companies and Their Directors,*' 3, available online at <https://prodstoragesam.blob.core.windows.net/highq/2536333/cyber-security-corporate-insights-for-companies-and-their-directors.pdf>, last accessed on 11 May 2021.
[1259] McGrath *op cit s.p.*; See Chapter 1, section 3.1.
[1260] McGrath *op cit s.p.*

To understand how the King Code is relevant to the directors' duty of care in relation to cybersecurity and the use of AI, a grasp is needed on how the King Code regulates the corporate governance and CSR aspects related to privacy and the protection of shareholders' and stakeholders' privacy and/or personal information.

Although the King Reports I – IV make no mention of OMs by name, their regulation of shareholders' and stakeholders' interests and IT governance are of significance as they help to set the corporate governance and CSR framework in which directors need to exercise their duty of care in relation to cybersecurity. The following subsections will look at the recommendations of the King Reports I - IV on shareholders' and stakeholders' interests that impact on the duty of care in relation to cybersecurity.

3.1. King Report I on Corporate Governance of 1994

King Report I of 1994 regulated five areas of corporate governance, namely the responsibilities of directors, the role of auditors, the integration of stakeholder links, as well as ethical practices and lastly, compliance with recommendations.[1261]

Of particular relevance was its explanation that modern companies are the nexus that binds the mutual interests of a company's various stakeholders.[1262] It explained that it is in stakeholders' own interests that they should cooperate by means of the integrated approach to further the well-being of the company to which they are tied.[1263]

An OM is a helpful forum to facilitate such cooperation. Although King Report I made no mention at the time of OMs, it is still very relevant because it allows the courts to determine whether directors exercised their duty of care in relation to cybersecurity in terms of the interests of the stakeholders and it also requires the auditors to audit the cyberrisks and the company's cybersecurity policy and system.[1264] In addition, it allows the courts to look at whether the directors followed a stakeholder integrated approach and helped to build stakeholder links and to look whether they secured those links and also whether directors implemented and oversaw ethical practices in terms of shareholder and stakeholder relations.[1265] Lastly, it allows the courts to look at whether the directors complied with corporate governance and CSR regulations.[1266]

3.2. King Report II on Corporate Governance of 2002

[1261] IoDSA '*King Report I*'*op cit* Chapters 4 – 11; 13 – 14; 12; 18; 21 – 22.
[1262] IoDSA '*King Report I*'*op cit* section 10.
[1263] *Ibid.*
[1264] IoDSA '*King Report I*'*op cit* Chapters 4 – 11; 13 – 14; 12; 18; 21 – 22.
[1265] *Ibid*.
[1266] *Ibid.*

IoDSA updated King Report I in 2002 with King Report II.[1267] King Report II sets out the principles for corporate governance, it reviews the 'stakeholder inclusive approach' and it also addresses non-financial matters, (such as CSR and environmental concerns), while it also ensures that compliance with the King Reports is measured.[1268]

King Report II's corporate governance principles determined that the most important principles that directors need to adhere to are accountability, CSR, discipline, fairness, independence and transparency.[1269]

In *Minister of Water Affairs and Forestry supra*, Hussain, J referred twice to aspects in this Report that explains good corporate governance practices and their characteristics.[1270] He said that one of these characteristics is social responsibility, and quoted paragraph 18.7 of this Report, which explains that directors should be aware of, and respond to social issues, and should focus on ethical standards.[1271] This paragraph also explains that a good corporate citizen does not discriminate, does not exploit and helps to protect environmental and human rights.[1272] This paragraph further states that it could likely yield indirect economic benefits for a company, such as higher productivity and a good reputation, when it pays attention to these factors.[1273]

What is of importance here is that the courts will look at whether directors exercised their duty of care in terms of the prescribed corporate governance principles, in other words, and will in other words try to determine whether they exercised their duty of care in an accountable manner (by looking at the board's corporate disclosures on cybersecurity and compliance with reporting obligations).[1274] It will also look at whether they exercised their duty in a disciplined manner (by looking at whether the board voluntarily exercised a high standard of the duty of care in relation to cybersecurity).[1275] It will also look at whether the board exercised their duty in a fair manner (by ensuring that the board should not afford special treatment to shareholders' interests in the company's cybersecurity policy and system, to the detriment of stakeholders' interests).[1276] It will also look at whether the board exercised their duty in an independent manner (by looking at whether the board sought the official sanctioning of a standard-setting authority on the way in which the company practices cybersecurity).[1277] Then it will look at whether the board exercised their duty in a

---

[1267] IoDSA '*King Report II*' *op cit* Introduction.
[1268] IoDSA '*King Report II*' *op cit* 16; Du Plessis *et al. op cit* 297.
[1269] IoDSA '*King Report II*' *op cit* sections 18.1 – 18.7.
[1270] IoDSA '*King Report II*' *op cit* page 22, paragraph 2.1.1; *Minister of Water Affairs and Forestry supra*, paragraphs 16.7; 16.9.
[1271] IoDSA '*King Report II*' *op cit* page 12, paragraph 18.7.
[1272] *Ibid.*
[1273] *Ibid.*
[1274] Horrigan *et al. op cit* 26.
[1275] *Ibid.*
[1276] *Ibid.*
[1277] *Ibid*.

manner that incorporates CSR (by looking at whether the board integrated CSR issues with cybersecurity requirements at the board level)[1278] Lastly, it will look at whether the board exercised their duty in a transparent manner (by integrating cybersecurity requirements in the company's audit process).[1279]

These are important principles that the King Code need to nurture in order to help directors with practical examples on how they need to integrate the principles mentioned above when they exercise their duty of care in relation to cybersecurity.

Besides the principles mentioned above, the courts will in terms of this Report, also look at whether directors exercised their duty of care in terms of the prescribed stakeholder inclusive approach, which is explained below.[1280] The court will also look at whether they addressed non-financial matters, (such as CSR and online environmental concerns) and whether they ensured that compliance with the King Reports is measured.[1281]

King Report II made no mention of how cybersecurity might affect shareholders and stakeholders, but regulated IT governance for the first time, and also introduced the inclusive approach to stakeholder relationships and emphasised the need for an African approach to stakeholder relationships.

3.2.1. Stakeholder Inclusive Approach

A prominent feature of King Report II was its 'stakeholder inclusive approach' when compared with King Report I's 'integrated approach' to corporate governance.[1282]

This new approach explains that the aim of the company should be to bring economics and ethics together, and to ensure that directors take the interests of all stakeholders into account when they make their business decisions.[1283] Keay explains that with this approach, stakeholders should not be seen as actors whose sole purpose is to enlarge the wealth of shareholders; and that the consideration of stakeholder interests should be a goal in itself.[1284]

In this regard, section 6 explains that the board needs to identify all of the relevant stakeholders who are part of the company and its operations and environment.[1285] The board then needs to determine the company's vision and values in consultation with these stakeholders and ensure that it is explained to all of them.[1286]

[1278] Horrigan *et al. op cit* 26.
[1279] *Ibid*.
[1280] IoDSA '*King Report II*' *op cit* 16; Du Plessis *et al. op cit* 297.
[1281] *Ibid.*
[1282] IoDSA '*King Report II*' *op cit* 8.
[1283] Keay 'Stakeholder Theory in Corporate Law: Has It Got What It Takes?' in the *Richmond Journal of Global Law & Business* 9(3) 2010 298.
[1284] *Ibid.*
[1285] IoDSA '*King Report II*' *op cit* section 6.
[1286] *Ibid*.

These factors must then be integrated in a company strategy to help it reach its goals.[1287] The company and its stakeholders should then strive towards a mutually beneficial relationship while they pursue these goals.[1288] In addition, the section explains how the inclusive approach creates sustainable growth for the company as well as long-term growth in share capital for the shareholders as a stakeholder group.[1289]

When the inclusive approach is integrated with the company's cybersecurity requirements, section 6 means that the vision and values of the company must also include the company's cybersecurity requirements, and that its cybersecurity policy should be communicated to all stakeholders.[1290] The cybersecurity policy must be mutually beneficial to both the company as well as its stakeholders, which includes the shareholders.[1291] As a result, when the inclusive approach is used to integrate the company's cybersecurity strategy with the stakeholders' interests, it will help to create sustainable growth for the company and help to protect the stakeholders' privacy and/or personal information and also create long-term growth in share capital for the shareholders if it helps to prevent cyberbreaches.[1292]

The section also explained that boards need to make sure that the required skilled employees are appointed to manage the company's internal control systems.[1293] In addition, the board should provide feedback on IT management in order to improve transparency.[1294] This means that boards need to ensure that IT personnel with the required skills are appointed and that they perform their duties in terms of cybersecurity properly and that they use AI responsibly.[1295] In addition, the board should be pro-active and start to use AI to improve reporting and transparency (such as corporate disclosure and adherence to reporting obligations and by including AI measures in the cybersecurity audit process).[1296]

3.2.2. African Approach

King Report II also emphasised that a corporate governance system is needed that recognises the African value system.[1297]

[1287] IoDSA '*King Report II*' *op cit* section 6.
[1288] *Ibid*.
[1289] *Ibid*.
[1290] *Ibid*.
[1291] *Ibid*.
[1292] *Ibid*.
[1293] IoDSA '*King Report II*' *op cit* 140.
[1294] *Ibid*.
[1295] *Ibid*.
[1296] *Ibid*.
[1297] Magang *Culture and Corporate Governance in SA*, PhD thesis submitted at the University of Bradford in 2012, 87.

OMs provide an excellent means to recognise the African philosophy of *Ubuntu* ('I am because we are') within a company, because it provides an opportunity for debate and for more shareholders and stakeholders to attend and participate in a meeting and to only reach a decision once everyone's opinion has been heard.[1298] OMs should strive towards *Ubuntu's* goals of consensus decision-making and the peaceful and harmonious resolution of conflict within the society or company.[1299] The chairperson and the board could be equated to the chief and his elders in African society, who then needs to be responsive to the needs of the rest of the community or shareholders and stakeholders and their environment, or in this instance, the online environment.[1300] OMs should also strive towards *Ubuntu's* characteristics of social justice and redress of inequalities, as both emphasise communal rights within the company, where a minority shareholder should never be treated as being of lesser importance than a majority shareholder.[1301] When the lessons of *Ubuntu* are applied to the duty of care in relation to cybersecurity, it means that directors should strive towards its characteristics of social justice in the aftermath of a cyberbreach and redress any inequalities that may exist between shareholders' interests and stakeholders' interests.[1302]

3.3. King Report III on Corporate Governance of 2009

King Report III, principle 1.2, sections 16 and 17 follow the Pluralist Theory and requires that directors follow a 'triple bottom line' approach when they interact with stakeholders and that directors also base their decisions on economic, environmental and social (EES) considerations.[1303] This means that directors must not just focus on profit maximisation, but that they must also look after the interests of other stakeholders within society.[1304] In terms of the Pluralist Theory, directors do not have to favour shareholders' interests above those of the stakeholders when they need to determine what will be in a company's best interests.[1305]

The 'triple bottom line' approach requires directors to base their decisions on EES considerations, which is of particular relevance to OMs since they are so much more environmentally friendly than AGMs (in terms of savings on paper and carbon-emissions, which are virtually zero due to the non-requirement of travel).[1306] It also means that directors should also look at the interests of other stakeholders within the online environment in which a company finds itself and also think of their cybersecurity

---

[1298] West 'Theorising SA's Corporate Governance' in *Journal of Business Ethics* (2002) 68(4) 442.
[1299] *Ibid*.
[1300] *Ibid*.
[1301] *Ibid*.
[1302] West *op cit* 442.
[1303] IoDSA '*King Report IV*' *op cit* principle 1.2, sections 16 – 17.
[1304] IoDSA '*King Report IV*' *op cit* principle 1.2, section 16.
[1305] IoDSA '*King Report IV*' *op cit* principle 1.2, section 17.
[1306] IoDSA '*King Report IV*' *op cit* principle 1.2, sections 16 – 17.

requirements.[1307] This means that directors do not have to favour shareholders' interests, but that they may afford special treatment to non-shareholders' interests, such as the protection of the privacy and/or personal information of consumers or suppliers as a certain stakeholder interest group, in the event that such an online database, which contains their personal information, is particulary vulnerable and requires extra added protection.[1308]

What is of importance for the King Code is that the courts will look at whether directors exercised their duty of care in terms of the prescribed EES considerations, in other words whether the board looked at economic considerations (such as savings on subsistence costs that are usually required for physical meetings), environmental considerations (such as a preference to OMs as it helps to cut the need for paper and cut carbon emissions to virtually zero) and social considerations (such as whether the impact of cyberbreaches on stakeholders and the online environment and financial system were considered).[1309]

3.4. King Report IV on Corporate Governance of 2016

King Report IV builds upon King Report III, Chapter 5, with principle 16, which recommends practices for shareholder relationships.[1310]

There are two recommendations for stakeholder relationships under principle 16 of King Report IV that are of particular relevance to the duty of care in relation to cybersecurity.[1311] The first one is recommendation 6, which specifies the need for the board to ensure that the company proactively engages with stakeholders, and especially talks about how shareholders' meetings should be conducted.[1312] The second one is recommendation 9, which requires the board to make sure that stakeholders are treated equally and that the interests of minority shareholders are properly protected.[1313] These two principles are important as they allow the courts to look at whether directors exercised their duty of care by proactively engaging with stakeholders on cybersecurity and whether the board ensured that stakeholders are treated equally and whether they ensured that the online databases with the personal information of especially minority shareholders are cyberresilient.[1314]

[1307] IoDSA '*King Report IV*' *op cit* principle 1.2, section 16.
[1308] IoDSA '*King Report IV*' *op cit* principle 1.2, section 17.
[1309] IoDSA '*King Report IV*' *op cit* principle 1.2, sections 16 – 17.
[1310] IoDSA '*King Report III*' *op cit* Chapter 5; IoDSA '*King Report IV*' *op cit* principle 16.
[1311] IoDSA '*King Report IV*' *op cit* principles 9; 16.
[1312] IoDSA '*King Report IV*' *op cit* principle 16.
[1313] *Ibid*.
[1314] *Ibid*.

4. THE EXERCISE OF SA DIRECTORS' DUTY OF CARE IN TERMS OF ESG INVESTMENT CONSIDERATIONS

Although there is a lot of debate about sustainable corporate practices worldwide, not much research on ESG investment considerations has so far been done in SA.[1315] Erasmus *et al.* explains that local research have so far mostly focused on SA's corporate governance framework that was introduced by the King reports and that more research of ESG considerations is required.[1316] They explain that the implementation of ESG considerations follows a phased approach, which starts when companies' first start to implement good corporate governance practices in order to become sustainable.[1317] In order to ensure corporate sustainability, directors will have to integrate all three ESG considerations in their business decisions in order to attract investors.[1318]

The Act, section 76(3) places an obligation on directors to exercise all of their functions in the best interests of the company and with the necessary degree of care, skill and diligence.[1319] This section will consequently also need to look at the other functions of directors, besides their duty of care in terms of cybersecurity, when they need to act in the best interests of the company and with the necessary degree of care, skill and diligence.[1320]

Although the obligations that are imposed by section 76(3) can be deemed to constitute the general duties of a director, different acts, together with the King Code also place specific duties on directors with which they need to comply with.[1321] As a result, Tolmay, J of the High Court, North Gauteng Division, held in 2019 in *OUTA NPC v Myeni* that the courts will refer to such acts and the King Reports when they to need to determine the compliance of directors with these specific duties, and if a director did not ensure that a company complied with these specific obligations, such a director may be held liable for a breach of not only these specific duties, but also of their general director duties.[1322]

Directors have a specific duty to exercise their duty of care in relation to environmental concerns since SA is a resource scarce country and SA companies are confronted with climate change, the destruction of natural habitats, a lack of water,

---

[1315] Erasmus *et al.* 'Assessing the Business for Environmental, Social and Corporate Governance Practices in SA' in *SA Journal of Economic and Management Sciences* 22 (2019) 3.
[1316] *Ibid.*
[1317] *Ibid.*
[1318] *Ibid.*
[1319] The Act, section 76(3).
[1320] *Ibid.*
[1321] The Act, section 76(3); *OUTA NPC v Myeni* (2019) ZAGPPHC 957.
[1322] *Ibid*.

mining pollution, ocean pollution, overfishing and various other concerns.[1323] Directors therefore have a specific duty of care in relation to physical environmental duties, and the SA National Environment Management Act (NEMA) 107 of 1998 sets out general environmental governance and decision-making principles, which applies to various types of activities that may affect a company's physical environment.[1324] Section 34(7) states that someone who was a director of a company at the time when it committed environmental pollution, will be guilty of that offence and will be liable to a fine or to imprisonment, if it was caused due to the director's failure to take all reasonable steps into consideration which were required under the circumstances to prevent such pollution.[1325]

It is submitted that an online environmental aspect, such as the state of cybersecurity in SA and the potential of a cyberattack on a company, could be added to these environmental considerations, because besides finding itself in a physical environmental eco-system, a company also finds itself within an online environment or eco-system. The potential of an online environmental concern such as a cyberattack could in some instances even have a greater effect on certain types of SA companies' expenses, operations and revenues (such as banks and financial institutions who work with very sensitive PII) than a physical environmental concern. It is also submitted that an improved understanding of these aspects would enable SA companies to address their consequences more efficiently.[1326] Local investors should also pay attention to these considerations when they evaluate environmental considerations.[1327]

Directors also have a specific duty to exercise their duty of care in relation to social aspects, since SA still struggles with a legacy of social injustices, which have adversely impacted on the country's socio-economic development.[1328] Legislation such as the SA Employment Equity Act 55 of 1998 and the SA Broad-Based Black Economic Empowerment (BBBEE) Act 53 of 2003 were promulgated to address the inequalities that were created by Apartheid and directors need to ensure that their companies comply with their requirements.[1329] The Act, section 72, read together with the SA Companies Regulations of 2011, regulation 43(1) also requires that the directors of (a) state-owned companies; (b) listed companies; and (c) every other company which has had a public interest score of at least 500 points in the past two years to appoint a social and ethics

[1323] Hebb *et al. The Routledge Handbook of Responsible Investment* 5 - 10.
[1324] SA National Environmental Management Act (NEMA) 107 of 1998.
[1325] NEMA 107 of 1998, section 34(7).
[1326] Hebb *et al. op cit* 5- 10.
[1327] *Ibid.*
[1328] Herringer *et al.* 'Key Challenges Facing the SRI Sector in SA' in *Investment Analysts Journal* 70(2) (2009) 12 - 15.
[1329] SA Broad-Based Black Economic Empowerment (BBBEE) Act 53 of 2003; SA Employment Equity Act 55 of 1998; Herringer *et al. op cit* 12 – 15.

committee.[1330] In terms of regulation 26(2) a social interest score is calculated based on a company's number of employees, its revenues, its third party liabilities, and its number of shareholders.[1331] In terms of regulation 43(4), the social and ethics committee cannot consist out of less than three members who may be directors or employees of that company.[1332] Regulation 43(5) states that such a committee should monitor a company's activities that pertain to consumer relations, environment, good corporate citizenship, health and public safety, labour matters and social and economic development.[1333] When this committee oversees social and economic development, regulation 43(5)(a) requires them to monitor compliance with (i) social and economic development in terms of the goals of the (aa) UN Global Compact Principles; (bb) the OECD Recommendations Regarding Corruption; (cc) the SA Employment Equity Act 55 of 1998; and (dd) the SA Broad-Based Black Economic Empowerment (BBBEE) Act 53 of 2003.[1334]

In addition, directors also have a specific duty to exercise their duty of care in relation to corporate governance and in this regard the corporate governance practices, which are expected of directors, are set out in the Act, King Reports I - IV and the common law.[1335] Good corporate governance requires directors to act in good faith and in the best interests of their companies, and also to exercise care, skill and diligence in the way in which they perform their duties.[1336] The King Code prescribes general standards of corporate governance, which SA courts often look at when they need to interpret this duty of directors.[1337] In terms of corporate governance issues, IoDSA's King Reports I – IV helps to constitute a well-developed corporate governance framework that focuses on sustainability.[1338]

The latest report, King Report IV, sets out 16 principles, which a company should apply in order to ensure that it is practising good corporate governance.[1339] As its objective, King Report IV requires a board to ensure responsible corporate citizenship, to govern ethics and to establish an ethical culture, to lead ethically and effectively and serve as the custodian of corporate governance.[1340] This Report also focuses on value creation in a sustainable manner and highlights the importance of corporate citizenship, ethical

---

[1330] The Act, section 72; SA Companies Regulations of 2011, regulation 43(1)(a)-(c); Delport *et al.* 'The Protection of Stakeholders: The SA Social and Ethics Committee and the UK's Enlightened Shareholder Approach, Part 1' in *De Iure* 50(1)(2017) 97.

[1331] SA Companies Regulations of 2011, regulation 26(2).

[1332] SA Companies Regulations of 2011, regulation 43(4).

[1333] SA Companies Regulations of 2011, regulation 43(5).

[1334] SA Companies Regulations of 2011, regulation 43(5)(a)(i)(aa)-(cc); Du Plessis *et al. op cit* 295.

[1335] Bertram *et al. Legal Guide for Company Directors and CEO's in SA*, *s.v.* 'ESG Obligations for Directors and CEO,' available online at <https://cms.law/en/int/expert-guides/cms-expert-guide-for-directors-of-companies/south-africa>, last accessed on 9 January 2023.

[1336] *Ibid.*

[1337] IoDSA '*King Report IV*' *op cit* principle 3.14 42.

[1338] Erasmus *et al. op cit* 3.

[1339] IoDSA '*King Report IV*' *op cit* principles 1 - 16.

[1340] IoDSA '*King Report IV*' *op cit* principles 1 – 16; Naidoo *op cit* 48.

leadership, integrated reporting and thinking, stakeholder inclusivity and sustainable development.[1341] King Report IV, principle 3.14 states in this regard that a board should continually oversee whether the consequences of their activities conform to those of a responsible corporate citizen.[1342] It requires that directors should perform continuous oversight over four main areas: firstly, in terms of sub-section (a), in the workplace (for example, since OMs do not require physical interaction, they help to prevent the spreading of Covid-19, and this in turn helps to uphold employees' health and safety).[1343] Secondly, in terms of (b) the economy, (for example, OMs help to promote economic transformation by means of digitisation; and if directors exercise their duty of care in relation to cybersecurity properly, it could help to prevent, detect and respond to cyberfraud).[1344] Thirdly, in terms of (c), the society (for example, since OMs do not require physical interaction, they help to prevent the spreading of Covid-19 since participants only interact online; and in addition, they can also help to improve CSR and help to facilitate interaction with minority shareholders and stakeholders).[1345] Fourthly, in terms of (d), the environment (for example, since OMs do not require paper agendas, travelling, catering or subsistence, they help the company to save on paper usage, catering and subsistence costs, as well as travel costs and as a result, carbon emmissions).[1346]

Integrated reporting is promoted by the Integrated Reporting Committee (IRCSA), which sets out standardised integrated reporting guidelines and who explains that an efficient integrated report should reflect the economic, environmental and social dimensions of a company.[1347] IRCSA also encourages companies to disclose details that relate to their financial, human, intellectual, manufacturing, natural and social capital.[1348]

It will be explained below that in 2011, CRISA was released by the CRISA Committee to guide institutional SA investors on what they should look at when they make their investment decisions.[1349] This Code clearly states that institutional investors should no longer just focus on financial gains to the detriment of ESG considerations which also contribute to long-term sustainability and value creation.[1350]

[1341] IoDSA '*King Report IV*' *op cit* Part 5.
[1342] *Ibid.*
[1343] IoDSA '*King Report IV*' *op cit* principle 3.14(a).
[1344] IoDSA '*King Report IV*' *op cit* principle 3.14(b).
[1345] IoDSA '*King Report IV*' *op cit* principle 3.14(c).
[1346] IoDSA '*King Report IV*' *op cit* principle 3.14(d).
[1347] Integrated Reporting Committee of SA (IRCSA) '*Preparing an Integrated Report: A Starter's Guide*,' 6, available online at <http://integratedreportingsa.org/ircsa/wp-content/uploads/2017/05/IRCSA_StartersGuide.pdf>, last accessed on 19 June 2023.
[1348] *Ibid.*
[1349] IoDSA '*King Report Iii*' *op cit s.p.*; IoDSA '*CRISA Home Page,' s.p.*, available online at <https://www.iodsa.co.za/page/CRISACode>, last accessed on 14 July 2021.
[1350] *Ibid*.

There are also other obligations of directors that relate to ESG considerations, such as climate-related risks, gender pay inequality, health and safety and stakeholder management, and directors should also keep these in mind, since AI could also be used to gain insight into how some of these aspects should be addressed, such as making a prediction on the change of weather patterns, evaluating whether gender pay inequality exists in a company, and to look for potential health and safety concerns in the company.[1351] Although AI is a neutral medium, it affects traditional corporate governance systems, since it not only facilitates business operations and helps to create business opportunities, but it can also be used to commit cybercrime or to launch a cyberattack.[1352]

The duty of care requires directors to protect the assets of the company, which includes the online platform and its online databases.[1353] The duty to promote the success of the company requires directors to look after the long term sustainability of the company, and to pay attention to the protection of personal information as an economic asset (which has financial worth) of the company.[1354]

If directors do no exercise their duty of care in relation to cybersecurity properly, it will compromise shareholders/stakeholders' privacy and/or personal information to the detriment of these groups' interests.[1355] This is because cyberbreaches often lead to other crimes, such as fraud and theft.[1356] Should a large scale cyberbreach occur, its repercussions can have continuing national and international downstream consequences in the company's online environment.[1357]

Besides the sources mentioned above, there are also other measures that deserve specific mention as they have bearing on how the directors' duty of care in relation to cybersecurity could help to improve aspects of corporate governance and ESG considerations.

4.1. Relevant International ESG Sources

SA directors will be well-advised if they look at the EU 'Taxonomy Regulation of 2020' and the EU 'Sustainable Governance Initiative,' as well as the UK FRC's

---

[1351] Bertram *et al op cit s.p.*

[1352] *Ibid.*

[1353] The Act, section 76(3)(c); Lyons 'Governance Bodies Endorse Value Preservation as Primary Purpose and Fiduciary Duty' on *OBLB*, *s.p.*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/governance-bodies-endorse-value-preservation-primary-purpose-and>, last accessed on 8 August 2021; Slaughter and May *op cit* 2.

[1354] The Act, section 76(3)(b); Slaughter and May *op cit* 3; Lyons *op cit s.p.*

[1355] Slaughter and May *op cit* 3.

[1356] *Ibid*.

[1357] *Ibid*.

Stewardship Code of 2020, since there are many lessons in good practices that can be learned from these sources and applied at home.[1358]

4.1.1. EU 'Taxonomy Regulation of 2020' and the EU 'Sustainable Governance Initiative'

Loughrey warns that there is a increasing trend in climate-related litigation, and that there is a growing number of claims worldwide which are brought against directors personally.[1359] Since OMs help to promote environmental sustainability, the King Committee can also look for lessons in the EU 'Taxonomy Regulation of 2020,' which classifies environmentally sustainable economic activities.[1360] This Regulation helps directors in the EU to increase sustainable investment and sets out environmental requirements that an economic activity has to conform with before it can be regarded as being environmentally sustainable, such as climate change conversion, climate change reduction, pollution reduction, the preservation of ecosystems, and the encouragement of a circular economy.[1361] Since OMs do not require travel, they minimise travel pollution, they also do not require paper-based agendas and minutes and because they save on catering and subsistence, they will qualify as an environmentally sustainable activity that directors can implement.

In addition, the EU 'Sustainable Governance Initiative' will soon be adopted in the EU and will guide directors to pursue sustainable growth instead of just quick gains.[1362] It aims to bring the interests of companies, their consumers, employees, managers, shareholders, society and stakeholders in line.[1363] In addition, it will also help directors to advance the sustainability of their companies' operations when it comes to climate change, the environment, human rights and social rights.[1364] Since OMs help to integrate the interests of companies, shareholders and stakeholders, they will also qualify as a sustainable governance initiative that directors can implement.

Although the UK government has not adopted the EU 'Taxonomy Regulation of 2020' nothing prevents the King Code from using its lessons and its best practices, as well as the lessons of the EU 'Sustainable Governance Initiative' to help guide SA

[1358] EU 'Taxonomy and Regulation of 2020,' *s.p.*, available online at <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/eu-taxonomy-sustainable-activities_en>, last accessed on 8 August 2021; EU 'Sustainable Governance Initiative,' *s.p.*, available online at <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12548-Sustainable-corporate-governance_en>, last accessed on 8 August 2021; UK FRC Stewardship Code of 2020 *op cit* 4.

[1359] Loughrey *Business Judgment and Director Accountability op cit* 1.

[1360] EU 'Taxonomy and Regulation of 2020' *op cit s.p*.

[1361] *Ibid*.

[1362] EU 'Sustainable Governance Initiative' *op cit s.p*.

[1363] *Ibid.*

[1364] *Ibid.*

directors to improve the corporate governance and CSR and ESG considerations of OMs.[1365]

4.1.2. UK Financial Reporting Council (FRC)'s Stewardship Code of 2020

In addition, the UK FRC's Stewardship Code of 2020 is another important corporate governance and ESG instrument that sets ethical standards for investors and investment managers who want to invest in the UK.[1366] It explains that investment institutions, who are voluntary signatories, must manage investments responsibly so that they will help generate continuing value for consumers and beneficiaries, so that investments can lead to sustainable economic growth and be advantageous to the environment and society.[1367] It also allows companies to align their own business model and strategy in terms of the requirements of effective stewardship and does not follow a prescriptive approach.[1368] It explains that environmental and social factors are important considerations on which investors need to base their investment decisions and undertake stewardship.[1369] Although it does not mention online environmental factors as such, it is submitted that besides physical environmental factors, online environmental factors, such as cybersecurity, will also be important ESG considerations for investors.

The Stewardship Code sets out twelve principles that is applied on an 'apply and explain' basis for investors and investment managers, and another six principles for service providers, such as personal information management service providers and proxy administrators.[1370] Of particular relevance is principle 5 that requires signatories to review their policies, enhance their systems and monitor the effeciency of their activities.[1371] This principle requires signatories to provide feedback on how they have reviewed their policies to maximise effective stewardship, the assurance that they have obtained on the effectiveness of their approach, and how they ensure that their stewardship reporting is balanced and easy to understand.[1372] In this way, investment institutions are supposed to review the cybersecurity policies and sytems of the companies in which they would like to invest.[1373] In addition, they need to obtain

---

[1365] Grant Thornton '*Sustainable Finance: A Guide to the UK Taxonomy,' s.p.*, available online at <https://www.grantthornton.co.uk/insights/sustainable-finance-a-guide-to-the-eu-taxonomy/>, last accessed on 8 August 2021.

[1366] UK FRC Stewardship Code of 2020 *op cit* 4; Reddy 'The Emperor's New Code? Time to Re-Evaluate the Nature of Stewardship Engagement Under the UK's Stewardship Code' on *Oxford Business Law Blog (OBLB), s.p.,* available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/emperors-new-code-time-re-evaluate-nature-stewardship-engagement>, last accessed on 8 August 2021.

[1367] UK FRC Stewardship Code of 2020 *op cit* 4.

[1368] *Ibid*.

[1369] *Ibid*.

[1370] *Ibid.*

[1371] UK FRC Stewardship Code of 2020 *op cit* 12.

[1372] *Ibid*.

[1373] *Ibid.*

assurance from an information officer (IO) that a company's cybersecurity policy and system are cyberresilient.[1374] Lastly, they need to ensure that they include stewardship reporting on a company's cybersecurity policy and system that is balanced and easy to understand for investors.[1375] In short, such investment institutions need to inform investors whenever a company's cybersecurity policy and system are cyberresilient or not, and whether it uses AI to help increase cyberresilience or not, and if it does, whether it uses it responsibly.

4.2. Relevant International ESG Sources

SA directors need to pay particular attention to the following ESG sources.[1376]

4.2.1. SA Code for Responsible Investing in SA (CRISA) of 2011

In SA, CRISA sets out guidelines for institutional investors' activities and decisions.[1377] It states that the King Reports I - IV only sees the board as the main role player in terms of corporate governance, but that investors also have an important role to play.[1378] It consequently requires that the King Code should be read and interpreted together with CRISA, in order to provide a framework for boards, investors and beneficiaries on how to invest responsibly.[1379] This framework then guides companies to not only focus on economic value, but also on value within its broader meaning.[1380] This means that the definition of 'value' has evolved from its traditional understanding in pure financial terms to value in terms of the sustainability of the company, its operations and its impact on the environment, which will include the company's online environment if it is interpreted liberally.[1381] Investors should consequently not only focus on shareholder supremacy and profit maximisation to the detriment of other factors that enable long-term sustainability, such as cybersecurity policies and systems and the use of AI.[1382] CRISA consequently guides investors to also look at factors that influence the

---

[1374] UK FRC Stewardship Code of 2020 *op cit* 12.
[1375] *Ibid.*
[1376] EU 'Taxonomy and Regulation of 2020,' *s.p.*, available online at <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/eu-taxonomy-sustainable-activities_en>, last accessed on 8 August 2021; EU 'Sustainable Governance Initiative,' *s.p.*, available online at <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12548-Sustainable-corporate-governance_en>, last accessed on 8 August 2021; UK FRC Stewardship Code of 2020 *op cit* 4.
[1377] IoDSA '*Code for Responsible Investing in SA (CRISA) of 2011,*' 4, available online at <https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/crisa/crisa_19_july_2011.pdf>, last accessed on 14 July 2021.
[1378] IoDSA '*CRISA' op cit* 7.
[1379] *Ibid*.
[1380] *Ibid.*
[1381] *Ibid.*
[1382] *Ibid.*

long-term growth potential of companies, for example companies' communities' cybersecurity needs, the protection of the physical and online environment and stakeholders' privacy and the protection of their personal information.[1383] It explains that this approach will in the long-term be advantageous to investors as it will yield risk-adjusted returns on investment and will simultaneously speak to community needs and help with the protection of the environment – be it the physical or online environment.[1384]

CRISA was needed because investors usually follow a conservative approach to corporate governance when they make their investment decisions and look at financial yields on their investments and not at corporate governance structures, processes and systems and their outcomes.[1385] CRISA also says that it was needed because it was never the intention that the King Code should be interpreted conservatively.[1386]

CRISA has the following five key principles, which investors need to follow when they make their investment decisions: they should firstly include sustainability considerations (such as ESG factors and the need for a company to have a cyberresilient cybersecurity policy and system).[1387] They should exercise their ownership responsibilities responsibly (such as obtaining assurance from the board that the necessary cybersecurity insurance is in place, should a cyberbreach occur).[1388] Investors should also follow an integrated approach and apply CRISA as well as any other relevant codes and standards (such as requesting the board to obtain the official sanctioning of a standard-setting authority on cybersecurity).[1389] They should also recognise conflicts of interest and avoid them (such as ensuring that non-shareholder interests, such as stakeholders' interests, who may also be affected by cyberbreaches, are also taken into account).[1390] Lastly, they should disclose how they have applied CRISA in their investment strategies so that it can help stakeholders to make informed decisions (and in this regard they can request cybersecurity audit reports on a company's cybersecurity situation).[1391]

SA corporate governance guidelines are for the most part voluntary in nature for boards and CRISA sets counterbalancing influences that apply to investors to make this framework more effective.[1392] When interpreted together with the King Code, whose principles are applied on an 'apply and explain' basis, CRISA contains examples of best

---

[1383] IoDSA '*CRISA' op cit* 7.
[1384] *Ibid*.
[1385] *Ibid*.
[1386] *Ibid.*
[1387] *Ibid*.
[1388] *Ibid.*
[1389] *Ibid*.
[1390] *Ibid*.
[1391] IoDSA '*CRISA' op cit* 10 - 11.
[1392] IoDSA '*CRISA Home Page' op cit s.p*.

practices that investors can use to base their investment decisions on.[1393] Although CRISA also informs investors how they can improve their oversight on their investments, it unfortunately does not mention cybersecurity itself, nor the responsible use of AI for cybersecurity purposes, and this is an important oversight that will have to be rectified in future.[1394]

4.2.2. JSE's Responsible Investment Index Series (RIIS)

The JSE launched the Responsible Investment Index Series (JSE RIIS) in 2015 and it has three goals. It is firstly a means to inform investors on listed companies' responsible investment and CSR and ESG policies and practices.[1395] It also encourages investors to invest in those companies who have a proven CSR and ESG record.[1396] Lastly, it also encourages companies in which they have invested to improve their responsible investment, social and environmental, and ultimately corporate governance initiatives, so as to be featured on the JSE RIIS.[1397]

This shows that responsible investment is an important concept of corporate governance that attempts to foster CSR, ESG, good corporate citizenship and sustainable development.[1398]

Although the JSE RIIS also helps to inform investors on how they can improve their oversight over their investments, it unfortunately does not mention cybersecurity itself, nor the responsible use of AI for cybersecurity purposes, and this is something that will have to be looked at in future.[1399]

4.2.3. The Protection of Stakeholders' Interests

In terms of the common law, the duty of care is not a general duty; it is not a duty towards each person, but only towards (a) certain person(s) or classes of persons.[1400]

It was against this background that it was held in 1949 in the Cape High Court in *Workmen's Compensation Commissioner v De Villiers* that if a plaintiff cannot prove that

---

[1393] IoDSA '*King Reports I - IV*' *op cit s.p.*; IoDSA '*CRISA Home Page' op cit s.p.*
[1394] *Ibid.*
[1395] *Ibid.*
[1396] *Ibid.*
[1397] JSE '*We Make it Easier to Invest in Companies that Invest in the Future,' s.p.*, available online at <https://www.jse.co.za/services/market-data/indices/ftse-jse-africa-index-series/responsible-investment-index>, last accessed on 19 May 2019.
[1398] *Ibid.*
[1399] *Ibid.*
[1400] Neethling *et al. Deliktereg op cit* 145.

he is someone to whom a duty of care was owed, he has no action.[1401] In addition, there is only a duty of care owed towards a foreseeable plaintiff.[1402]

In terms of the finding in *Workmen's Compensation Commissioner supra* it will be easy for shareholders to prove that directors owe them a duty of care, because they own shares in the company and have a share certificate as proof.[1403] For stakeholders, the finding however means that unless they can prove that they are someone to whom a duty of care was owed, they will have no action.[1404] This is because directors do not have a general duty of care to a group of unlimited stakeholders, but only to stakeholders who are able to prove that directors owed them a duty of care.[1405]

The gradual change over time from the conservative common law approach to the liberal constitutional approach also manifests itself in the Act, section 165, which allows stakeholders such as employees' representatives and trade unions' representatives to serve on a company's board.[1406] In addition, other legislation besides the Act protects stakeholder interests when it comes to the rights of consumers, employees and the environment.[1407] As a result, directors must take stakeholder rights into account when they make their decisions.[1408]

Initially, stakeholders, unlike shareholders, could not make decisions at shareholders' meetings, until the Act changed that in two ways: in the first instance, section 165(2) affords certain stakeholders the right to demand that a company protects their rights by for example taking legal action against its directors for a breach of their duty of care on a matter that affects them.[1409] Section 165(2) says that this action may be instituted by a (a) shareholder; (b) director or prescribed employee; (c) trade union; or (d) anyone else with leave of the court.[1410] This section thus allows stakeholders to have *locus standi* and to also bring derivative actions.[1411]

In the second instance, the Act, section 72(4) also makes provision for certain types of companies to have an ethics and social committee as part of their boards, which is then tasked to consider CSR and ESG considerations.[1412]

4.2.4. Shareholder and Stakeholder Activism

[1401] *Workmen's Compensation Commissioner v De Villiers* 1949 1 SA 474 (C).
[1402] *Ibid.*
[1403] *Ibid.*
[1404] *Ibid*.
[1405] Neethling *et al. Deliktereg op cit* 145.
[1406] The Act, section 165.
[1407] SA Consumer Protection Act 68 of 2008; SA Environmental Law Rationalisation Act 51 of 1997; SA Labour Relations Act 66 of 1995; Ramnath *op cit* 108.
[1408] Ramnath *op cit* 108.
[1409] The Act, section 165(2).
[1410] The Act, sections 165(2)(a) – (d).
[1411] The Act, section 165; Blackman *et al. op cit* 9-178.
[1412] The Act, section 72(4).

Shareholders and stakeholders could use their voting power or opportunities to make presentations to put pressure on the board to exercise due care in relation to cybersecurity.

Shareholder and stakeholder activists are usually focused on financial and ESG considerations and try to influence the company to accommodate such considerations in its growth strategy.[1413] More investors are however starting to look at ESG considerations and according to research by Deloitte UK, the percentage of shareholders that invest in ESG compliant companies grew from 48% to 75% between 2017 and 2019.[1414]

Although SA has various responsible investment initiatives, Kemp *et al.* found that only a few SA shareholders base their investment decisions on the responsible investment philosophy, but they say that there is always room for growth.[1415] Since cyberrisks and cyberbreaches will no doubt increase in future, it can be anticipated that shareholder and stakeholder activists will in future play a more active role in SA in terms of the protection of not only the company against cyberattacks, but also their privacy and/or personal information.

4.2.5. Disclosure

Some companies do not disclose any information on their cyberattacks and cyberbreaches to the shareholders.[1416] Some companies do not want to acknowledge that a cyberbreach occurred out of fear for a drop in their share price, bad public relations (PR) publicity, to prevent litigation with affected parties, and to not scare potential investors.[1417] Some boards are also hesitant to disclose any information on the company's cyberattacks and cyberbreaches as they might fear that it could expose the company's cybersecurity weak spots.[1418] Although one can understand why companies' want to keep this information private, it is in conflict with the SA POPI 4 of 2013, section 22(1), which requires that any cyberbreach must be notified to the IR and affected

---

[1413] Kemp *et al.* 'Reflecting on the Changing Landscape of Shareholder Activism in SA' in *SA Journal of Economic and Management Sciences* of 25 January 2021, 3.

[1414] Deloitte '*Advancing Environmental, Social and Governance Investing,*' 3, available online at <https://www2.deloitte.com/content/dam/insights/us/articles/5073_Advancing-ESG-investing/DI_Advancing-ESG-investing_UK.pdf>, last accessed on 8 August 2021.

[1415] Kemp *et al. op cit* 3.

[1416] Riley 'The Cybersecurity 202: Companies Are Doing a Terrible Job at Reporting Cybersecurity Risks to Investors, New Report Says' in *Washington Post* of 5 March 2021, *s.p.*, available online at <https://www.washingtonpost.com/politics/2021/03/05/cybersecurity-202-companies-are-doing-terrible-job-reporting-cybersecurity-risks-investors-new-study-says/>, last accessed on 12 May 2021.

[1417] *Ibid.*

[1418] *Ibid.*

parties.[1419] Section 22(1) thus requires that companies should share any information on cyberattacks and cyberbreaches with the IR, so that they can warn other companies and help to strategise to resist the cyberattacks.[1420]

A notable example is the EU 'Directive on Corporate Sustainability Reporting of 2014' that compels certain companies to disclose how they conduct their business and manage CSR.[1421] It encourages stakeholders to also look at non-financial performance and to formulate a responsible approach on matters that affect them, such as cybersecurity.[1422]

Similarly, the King Code should require directors to disclose how they exercise their duty of care in relation to cybersecurity and the responsible use of AI.

The directors of SA listed companies could also disclose how they exercise due care in relation to cybersecurity in prospectuses and annual reports.[1423]

Under the JSE '*Listing Requirements,*' section 19(13)(h), a listed company must explain in its prospectus all of the risks that the company face and how it curtails those risks.[1424] It would be expected that a board should disclose its cyberrisks, and also disclose that it has an appropriate cybersecurity policy and system in place, and that it uses AI responsibly, to prevent those cyberrisks.[1425]

5. THE EXERCISE OF THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI AND BLOCKCHAIN TECHNOLOGY

The responsible use of AI is also relevant to the way in which directors should exercise their duty of care in relation to cybersecurity because AI, and more specifically Blockchain technology, addresses many cybersecurity and privacy issues of OMs and is especially useful when it comes to online voting and resolutions.[1426]

Companies receive numerous cybersecurity alerts daily from the various cybersecurity measures which they employ to look for online intruders, malware and

---

[1419] SA POPI 4 of 2013, section 22(1).
[1420] *Ibid*.
[1421] EU 'Directive on Corporate Sustainability Reporting (2014/95/EU) of 2014,' *s.p.*, available online at <https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en>, last accessed on 8 August 2021.
[1422] *Ibid.*
[1423] UK FCA '*Disclosure Guidance and Fiscal Disparity Guideline,*' *s.p.*, available online at <https://www.handbook.fca.org.uk/handbook/DTR.pdf>, last accessed on 12 May 2021.
[1424] JSE Listing Requirements *op cit* section 19(13)(h)
[1425] Slaughter and May *op cit* 6 - 7.
[1426] Chiu *et al.* 'Technology vs Ideology: How Far Will AI and Distributed Ledger Technology Transform Corporate Governance and Business' on *OBLB, s.p.*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/technology-vs-ideology-how-far-will-artificial-intelligence-and>, last accessed on 8 August 2021; Strate '*Strate Holds First Remote AGM' op cit s.p*.

other cyberrisks.[1427] The IO and IT employees often find themselves flooded with cybersecurity alerts and warnings that they need to prioritise and manage.[1428]

These challenges accentuate the need for the King Code to help prevent cyberbreaches. This is because AI is especially useful to detect patterns in large quantities of data, and as a result, AI is starting to become an indispensable aid for directors, when it comes to cybersecurity.[1429]

Since AI and Blockchain technology also hold risks for companies, and because cyberbreaches are increasing and affecting more and more companies, shareholders and stakeholders, directors need to know how they should effectively exercise their duty of care in relation to cybersecurity in terms of the use of AI and Blockchain technology.[1430]

5.1. The Use of AI at OMs

AI consists of different sub-types that are available to companies and which could be used to help improve company's cybersecurity, especially at their OMs.[1431]

Analytic AI makes use of a machine learning technique, which is called deep learning.[1432] It scans data in order to discern patterns which are then used to give cybersecurity recommendations and to help with data-driven decisionmaking on aspects related to the cybersecurity of an online platform and its online databases.[1433] Examples include the evaluation of shareholders' sentiments and firewall risk evaluation.[1434]

Functional AI scans data and looks for patterns, analyses the data derived from the patterns and then makes suggestions to the directors in order for them to decide on proper actions.[1435] It may consequently identify a pattern in the data that it receives from the sensors of the online platform's firewall and then, as a result, send an instruction to the IT department to upgrade the firewall.[1436] Examples include machine learning, robotics and supplier risk evaluation.[1437]

Graphic AI uses computer vision to classify, identify and sort information, and convert an image into insight.[1438] Examples include usage to help companies grade

---

[1427] Fortinet '*Overcoming the Challenges of Rapid and Effective Incident Responses,' s.p.,* available online at <https://www.fortinet.com/blog/industry-trends/overcoming-the-challenges-of-rapid-and-effective-incident-response>, last accessed on 2 July 2022.
[1428] *Ibid.*
[1429] Adi *et al. op cit* 23817 – 23818.
[1430] *Ibid.*
[1431] Shani *op cit s.p*.
[1432] Sarker *op cit* 3.
[1433] *Ibid.*
[1434] *Ibid.*
[1435] Sarker *op cit* 3 - 4.
[1436] *Ibid.*
[1437] *Ibid.*
[1438] *Ibid.*

certain cybersecurity functions during the OM and to evaluate the cyberresilience of the company's cyberassets with the latest trends.[1439]

Interactive AI enables companies to automatically send interactive communications to shareholders and stakeholders.[1440] An examples in this regard is a chatbot, which can immediately answer questions during an OM - but it is very important that directors must understand that this will not conform to the requirements of the Act, section 63(2), which requires shareholders to pose their questions to the board without moderation by an AI intermediary.[1441]

Text AI includes content generation capabilities, machine translation, speech-to-text conversion and text recognition.[1442] It could be used to do research and to send information to shareholders/stakeholders before/during/after an OM.[1443]

In addition, AI can help automate many tasks related to the administration of personal information that an employee otherwise would have to conduct manually before, during or after an OM.[1444] The tasks it does include are the automatic distribution of ballots, as well as the automatic detection of unknown code repositories, intruders, servers or hardware or software on an online platform or in an online database.[1445] It can also help to determine how security defences could be employed optimally.[1446]

AI has the potential to filter large quantities of data much faster and more precise than employees.[1447] It can detect patterns that employees would not be able to find.[1448] AI would be able to decipher the workings of attackers and hackers who are busy preparing a cyberattack in the dark web and warn the IO.[1449] An example that AI-programmes picked up is the term, 'Mirai,' (which refers to a botnet that distributes Distributed Denial of Service (DDoS) attacks), which is a secret word that hackers made up in an attempt to circumvent certain cybersecurity systems and measures.[1450]

[1439] Sarker *op cit* 3 - 4.
[1440] Sarker *op cit* 4.
[1441] The Act, section 63(2); Sarker *op cit* 4.
[1442] *Ibid.*
[1443] *Ibid.*
[1444] Shani *et al. op cit s.p.*
[1445] ComputerScience.org '*Understanding Automation and AI*,' *s.p.*, available online at <https://www.computerscience.org/resources/learn-ai/>, last accessed on 2 July 2022.
[1446] *Ibid.*
[1447] Knight 'AI Is Coming for Your Most Mind-Numbing Office Tasks' in *Wired* of 14 March 2020, *s.p.*, available online at <https://www.wired.com/story/ai-coming-most-mind-numbing-office-tasks/>, last accessed on 2 July 2022.
[1448] Gehl 'Illuminating the Dark Web' in *The Conversation* of 30 October 2018, *s.p.*, available online at <https://theconversation.com/illuminating-the-dark-web-105542>, last accessed on 2 July 2022.
[1449] Penta Security '*Top 5 AI-Powered Cyberthreats and How to Avoid Them*,' *s.p.*, available online at <https://www.pentasecurity.com/blog/top-5-ai-powered-cyber-threats-how-to-prevent-them/>, last accessed on 2 July 2022.
[1450] Cloudflare '*What is The Mirai Botnet?*,' *s.p.*, available online at <https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>, last accessed on 2 July 2022.

Companies who are focused on cybersecurity are continuously busy developing AI programmes that combat disinformation, malware and phishing.[1451] Directors should especially take note of Microsoft's CyberSignals program since it deciphers cybersecurity algorithms, the data that hails from certain countries and numerous hacker sindicates to produce cyberthreat alerts and notifications for companies.[1452]

The US Department of Defense and its partners have also developed an advanced AI programme, Github, to extract data from the Dark Web in an attempt to look for patterns and identify hackers and how they operate.[1453]

Directors will be well-advised if they were to exercise their duty of care in relation to cybersecurity in a manner that will incorporate all of these five sub-types in their cybersecurity strategy, but then they will have to use it responsibly in terms of the provsions that the Act stipulates.

5.1.1. Challenges of AI

Although AI holds numerous advantages for cybersecurity, the King Committee should also have their concerns and questions about it when it is not used responsibly.[1454] Directors might be contemplating the replacement of their IT employees with AI systems, even though they might be unsure to which extent they can rely on data that is produced by AI systems.[1455] In addition, it is also still unclear how the problems of bias, ethics, fairness and transparency, which manifests itself in, for example country-biased, gender or racially biased-algorithms, will be overcome in AI-based cybersecurity systems.[1456]

The problem with AI is however that it is used not only by directors in the fight against cyberattacks, but also by attackers and hackers.[1457] They employ generative adversarial networks (GANs) to develop cyberattacks that can circumvent cybersecurity systems.[1458]

[1451] Fireeye '*AI in the Cyber Domain*,' *s.p.*, available online at <https://www.fireeye.com/blog/products-and-services/2018/03/artificial-intelligence-in-the-cyber-domain.html>, last accessed on 2 July 2022; Google.com '*Advancing AI for Everyone*,' *s.p.*, available online at <https://ai.google/>, last accessed on 2 July 2022; Microsoft '*CyberSignals*,' *s.p.*, available online at <https://news.microsoft.com/cyber-signals/>, last accessed on 2 July 2022.

[1452] Microsoft *op cit s.p*.

[1453] Github.com '*Where the World Builds Software*,' *s.p.*, available online at <https://github.com/>, last accessed on 2 July 2022.

[1454] Shani *op cit s.p.*

[1455] *Ibid.*

[1456] Calo 'FTC Warns the AI Industry: Don't Discriminate or Else' in *Th e Conversation* of 27 April 2021, *s.p.*, available online at <https://theconversation.com/ftc-warns-the-ai-industry-dont-discriminate-or-else-159622>, last accessed on 2 July 2022.

[1457] Brownlee 'A Gentle Introduction to Generative Adversarial Networks (GANs)' at *Machine Learning Mastery*, of 17 June 2019, *s.p.*, available online at <https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/>, last accessed on 2 July 2022.

[1458] *Ibid.*

Although lots of research still needs to be done on the ways in which attackers and hackers use AI, the King Committee should already start to include the basic principles on how directors should exercise their duty of care in relation to cybersecurity on the use of AI in the King Code. The SA corporate governance regime should start to nurture the use of AI in cybersecurity while it is still in its infant shoes.[1459] The insight that AI programmes extract from data from the Internet and the Dark Web will especially help directors to prevent potential cyberattacks.[1460] When directors are guided to exercise their duty of care in relation to cybersecurity properly in terms of the responsible use of AI, AI could become one of the most important tools that there is to prevent cyberbreaches.[1461]

5.2. The Use of Blockchain Technology at OMs

For a long time, companies have had to contend with paper agendas and minutes, circulars, proxy solicitation documentation and physical voting.[1462] According to the SA share depositry, Strate, most SA shareholders do not attend shareholders' meetings but submit their physical proxy form in which they nominate someone to vote on their behalf.[1463] This is in many instances still done by courier, e-mail or post.[1464]

The problem with this manual, paper-based administration is that it complicates communication between companies and their shareholders, it increases the potential for human error, votes can go missing in the post or in a spam folder and because the administration and vote counting process is not opened to viewing, there is a lack of transparency.[1465]

OMs allow participants to ask questions online, but some do not allow them to cast their votes in real time.[1466] Many shareholders still have to submit their votes before the OM without the opportunity to make real-time amendments after they have spoken to directors about their concerns.[1467]

[1459] Belani 'The Use of AI in Cybersecurity: A Review' in *IEEE Computer Society*, *s.p.*, available online at <https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity>, last accessed on 2 July 2022.
[1460] *Ibid.*
[1461] Olzak 'Adverserial AI: What It Is and How to Defend Against It?' in *Spiceworks*, *s.p.*, available online at <https://www.spiceworks.com/tech/artificial-intelligence/articles/adversarial-ai-attack-tools-techniques/>, last accessed on 2 July 2022.
[1462] Strate '*Adoption of Digital Solutions for AGMs is Long Overdue,*' *s.p.*, available online at <https://www.strate.co.za/2020/07/03/adoption-of-digital-solutions-for-agms-is-long-overdue/>, last accessed on 15 May 2021.
[1463] *Ibid.*
[1464] Strate '*Annual Integrated Report 2020*' *op cit* 4.
[1465] Strate '*Adoption of Digital Solutions for AGMs is Long Overdue' op cit s.p.*
[1466] *Ibid.*
[1467] *Ibid.*

It was explained that Strate is the central securities depository and that it is responsible for the safekeeping of the legal, online record of share ownership.[1468] It safeguards ownership rights of different types of securities, such as bonds, equities, money market funds and participatory notes in collective investment schemes and shares.[1469] Strate has partnered with Nasdaq to develop an innovative, groundbreaking IT solution to enable OMs.[1470] It is called the Strate e-Voting platform and it allows shareholders to vote and also communicate directly with directors online.[1471]

The advantage of the Strate e-Voting platform is that it ensures that shareholders can participate in an OM, vote in real time, and change their votes at any time before the OM closes, from anywhere in the world.[1472] This allows for greater shareholder participation, as well as a more efficient and transparent voting process.[1473] It also saves time and expenses as participants do not have to incur travel and subsistence expenses, nor do they need to physically deliver a written proxy.[1474]

The Strate e-Voting platform basically gives shareholders, and not intermediaries, greater control over the voting process when it comes to their shares.[1475] Normally shareholder and proxy votes follow a complex process that is performed by numerous intermediaries, before it reaches a company.[1476] A manual voting process takes time, increases the risk of human error, and does not give shareholders a direct communication line to the board where they can add a comment to their vote.[1477]

The Strate e-Voting platform also sends out reminders to shareholders to remind them that they must register for an OM, remind them to attend the OM once they RSVP'd, and reminds them to vote before the OM closes.[1478] Shareholders can see that their votes were cast, change their votes in real-time and send questions to the chairperson during the OM.[1479] The chairperson is notified of the votes of individual shareholders and not just the aggregated vote of financial institutions – and this helps a shareholder to have their voice heard as it allows the shareholder to insert their

---

[1468] Strate '*Annual Integrated Report 2020*' *op cit* 5; See Chapter 2, section 2.1.
[1469] Strate '*Annual Integrated Report 2020*' *op cit* 10; 15.
[1470] Strate '*Strate Holds First Remote AGM*' *op cit s.p*.
[1471] *Ibid.*
[1472] Strate '*Adoption of Digital Solutions for AGMs is Long Overdue*' *op cit s.p.*
[1473] *Ibid.*
[1474] *Ibid.*
[1475] Nasdaq '*Nasdaq to Deliver Blockchain E-Voting to Strate,*' *s.p.*, available online at <https://ir.nasdaq.com/news-releases/news-release-details/nasdaq-deliver-blockchain-e-voting-solution-strate>, last accessed on 4 August 2021.
[1476] *Ibid.*
[1477] *Ibid.*
[1478] Strate '*Adoption of Digital Solutions for AGMs is Long Overdue*' *op cit s.p.*
[1479] *Ibid.*

commentary with the vote.[1480] The platform also provides auditable results immediately after the OM.[1481]

By making use of the Strate e-Voting platform, companies get an online voting solution from the registrar of the online securities ownership register, while service providers, such as the JSE online platform, can easily integrate it.[1482]

By helping to make online voting more efficient and transparent, the Strate e-Voting platform improves communication by allowing shareholders to add their comments to their votes and thereby helps to build stronger relations between companies and shareholders.[1483] Communication on the platform occurs in real-time, and because the system is an extension of a binding ledger, the vote of each participant can easily be tracked and audited.[1484] It also helps to uphold a company's ethical integrity, as antagonistic shareholder activists can verify resolutions or voting outcomes for themselves.[1485]

The Strate e-Voting platform uses Nasdaq's Blockchain technology to constitute the proxy chain, to compile voting records and to deliver real-time voting outcomes.[1486] The underlying Blockchain technology helps to ensure the integrity and security of personal information, and all personal information that is gathered is kept in a tamper-proof ledger, which in turn reduces cyberrisks.[1487]

Strate was the first SA company to hold its OAGM by using the e-Voting platform on 9 May 2020.[1488] The results were submitted to the chairperson to audit after the OAGM, as is usually the case with unlisted companies, and everything was found to be in order.[1489] With listed companies, auditing is done by external auditors who use the immutable ledger to underpin accuracy and security.[1490]

5.2.1. Challenges of Blockchain Technology

Blockchain technology also has many challenges that the King Committee will have to look at.

[1480] Strate '*Strate Holds First Remote AGM' op cit s.p*.
[1481] *Ibid.*
[1482] Strate '*Annual Integrated Report 2020' op cit* 15.
[1483] *Ibid*.
[1484] *Ibid.*
[1485] Strate '*Strate e-Voting Continues to Serve Market Amidst Covid-19,' s.p.*, available online at <https://www.strate.co.za/2020/03/25/strate-e-voting-continues-to-serve-the-financial-markets-amidst-covid-19/>, last accessed on 4 August 2021.
[1486] Strate '*Strate Holds First Remote AGM' op cit s.p*.
[1487] Strate '*Strate e-Voting Continues to Serve Market Amidst Covid-19' op cit s.p.*
[1488] Strate '*Strate Holds First Remote AGM' op cit s.p*.
[1489] Strate '*Adoption of Digital Solutions for AGMs is Long Overdue' op cit s.p.*
[1490] *Ibid.*

Blockchain still has many technological shortcomings and a coding flaw or coding loophole could easily lead to a cyberbreach.[1491] The decentralised nature of Blockchain technology is a breeding ground for attackers and hackers, because it presents anonymity.[1492]

Blockchain technology also slows down drastically when it needs to process lots of personal information, since the encryption function is time-consuming, and when it slows down, it is especially vulnerable to a cyberattack.[1493] Blockchain also has a high energy consumption and it mostly uses the Proof of Work (PoW) algorithm, which means that when a user initiates a transaction, 'miners' or supercomputers, which use a lot of energy, has to try and solve it.[1494]

Besides having to acquire Blockchain hardware and software, a company will also have to recruit qualified employees to manage it.[1495]

Another problem that stands in the way of its large scale adoption is a lack of knowledge on how Blockchain works.[1496] There is still not any specific regulations on it in SA.[1497] According to Weston, many directors are also still not aware of its potential, or even its existence.[1498] Also, if Blockchain technology is to succeed, it has to be accepted and used more widely.[1499]

The most serious challenge of Blockchain technology is however privacy, because the public ledger system is the driving force of the entire Blockchain system, so the total privacy of personal information is not a characteristic of this technology.[1500] This is why it is necessary to change its registers to limit access to the personal information.[1501] Making access available for only the individual relevant shareholder or stakeholder will be a solution.[1502] The public ledger system is however an essential characteristic of media

---

[1491] Anwar 'Blockchain Implementation Guide: Empower Your Business' in *101 Blockchains* of 25 September 2018, *s.p.*, available online at <https://101blockchains.com/blockchain-implementation-guide/>, last accessed on 3 July 2022.

[1492] *S.n.* 'Decentralised vs Centralised: A Detailed Comparison' in *101 Blockchains* of 29 May 2021, *s.p.*, available online at <https://101blockchains.com/decentralized-vs-centralized/>, last accessed on 3 July 2022.

[1493] Geroni 'Blockchain Scalability Problem: Why is it Difficult to Scale Blockchain?' in *101 Blockchains* of 30 September 2021, *s.p.*, available online at <https://101blockchains.com/blockchain-scalability-challenges/>, last accessed on 3 July 2022.

[1494] *S.n.* 'Know Everything About Blockchain Proof of Work (PoW)' in *101 Blockchains* of 29 March 2019, *s.p.*, available online at <https://101blockchains.com/blockchain-proof-of-work/>, last accessed on 3 July 2022.

[1495] Anwar 'Blockchain Technology Explained: A Decentralised Ecosystem' in *101 Blockchains* of 30 July 2021, *s.p.*, available online at <https://101blockchains.com/blockchain-technology-explained/>, last accessed on 3 July 2022.

[1496] Weston 'A Definitive Guide on Cryptocurrencies' in *101 Blockchains* of 10 April 2022, *s.p.*, available online at <https://101blockchains.com/what-is-cryptocurrency/>, last accessed on 3 July 2022.

[1497] *S.n.* 'Decentralised vs Centralised: A Detailed Comparison' *op cit s.p*.

[1498] Weston *op cit s.p.*

[1499] *Ibid.*

[1500] Geroni 'What is a Public Blockchain: A Beginner's Guide' in *101 Blockchains* of 10 November 2020, *s.p.*, available online at <https://101blockchains.com/public-blockchain/>, last accessed on 3 July 2022.

[1501] *Ibid*.

[1502] *Ibid.*-

such as Bitcoin and other cryptocurrencies.[1503] Private Blockchain (as in the case of Strate) can however still work if all personal information is encrypted.[1504] An individual relevant shareholder or stakeholder could then get limited access to their own PII, and all their sensitive information would stay private.[1505]

Since the merger of the JSE online platform and the Strate e-Voting platform is a complex and novel matter that includes Blockchain technology, the King Code will have to provide guidance to directors on how this affects their duty of care in relation to cybersecurity and the use of AI. The King Committee would have to lay down principles for directors on how to use it and require directors to ensure that there is limited access to the ledgers, that personal information is encrypted and that only individual relevant shareholders/stakeholders can access their own personal information.[1506]

6. LESSONS ON HOW THE DIRECTORS' DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI COULD HELP TO IMPROVE CORPORATE GOVERNANCE, CSR AND ESG CONSIDERATIONS AT SA OMs

This Chapter examined the indirect impact of the duty of care in relation to cybersecurity to look how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs, and it is explained below that this could happen in various ways.

The duty of care in relation to cybersecurity could help to improve cybersecurity issues on shareholder and stakeholder protection at board level through deliberation.[1507]

The protection of the online platform and its online databases could be made a requirement in the official sanctioning of a standard-setting authority, (such as cybersecurity-sensitive auditing) or cybersecurity standard-setting or inclusion on the JSE RIIS.[1508]

The duty to exercise a pre-determined standard of care in relation to cybersecurity could also be inserted as part of directors' duties or executive remuneration.[1509]

[1503] Geroni *op cit s.p*.

[1504] Anwar 'What is Private Blockchain: A Beginner's Guide' in *101 Blockchains* of 2 June 2020, *s.p.*, available online at <https://101blockchains.com/what-is-a-private-blockchain/>, last accessed on 3 July 2022.

[1505] *Ibid.*

[1506] *Ibid.*

[1507] Vigeo '*Integration of CSR into Corporate Governance System,*' 8 – 9, available online at <https://vigeo-eiris.com/wp-content/uploads/2013/06/2013_12_Vigeo_Governance_Study_GB.pdf>, last accessed on 12 July 2021.

[1508] Horrigan *et al. op cit* 26.

[1509] Vigeo op cit 15.

Corporate disclosure and reporting obligations on the standard of the duty of care in relation to cybersecurity, should be done as this will help safeguard the interests of the community, consumers, employees and the online environment by promoting transparency.[1510]

The duty of care in relation to cybersecurity could be included in the standard-setting for good corporate governance, such as stakeholder engagement mechanisms.[1511]

Greater shareholder and stakeholder participation on cybersecurity matters could be promoted.[1512] Otherwise a shareholder vote on the appropriate cybersecurity policy and system could be held or shareholder proposals on cybersecurity issues, such as the use of AI, could be asked.[1513]

Special treatment could be afforded to important non-shareholder interests in the company's cybersecurity strategy, such as employees' interests or creditors' interests whenever it is required.[1514]

Incentives could be created and disincentives could be removed at the policy level for social and online environmental responsible corporate behaviour, such as procurement and licensing requirements of cybersecurity systems.[1515]

Awareness could be raised on the accommodation of cybersecurity criteria in decision-making on investments in cybersecurity systems and measures, in the SA CRISA of 2011.[1516]

Directors could voluntarily adopt self-regulatory measures on cybersecurity and the use of AI, such as the voluntary adoption of recommendations, which are contained in cybersecurity reports or industry cybersecurity best practices.[1517]

Directors will need to adhere to other important laws, regulations and corporate governance guidance that regulate aspects of cybersecurity, such as the Act, section 63(2), which requires shareholders to pose their questions to the board without any moderation by an AI intermediary.[1518]

Directors could also integrate cybersecurity issues on stakeholder protection in the audit process by allowing the audit committee to review cybersecurity risks.[1519] They

---

[1510] Libit '*The CSR Report and Effective Stakeholder Engagement,*' *s.p.*, available online at <https://corpgov.law.harvard.edu/2013/12/28/the-corporate-social-responsibility-report-and-effective-stakeholder-engagement/>, last accessed on 12 July 2021.

[1511] Jutterström *CSR Standards and Organisations Setting Them* Score Working Paper Series, 11, available online at <https://www.diva-portal.org/smash/get/diva2:649943/FULLTEXT01.pdf>, last accessed on 19 July 2021.

[1512] Gao *et al. op cit* 1.

[1513] *Ibid.*

[1514] Horrigan *et al. op cit* 26.

[1515] Derchi *et al.* '*CSR Performance, Incentives and Learning Effects,*' *s.p.*, available online at <https://link.springer.com/article/10.1007/s10551-020-04556-8>, last accessed on 12 July 2021.

[1516] Horrigan *et al. op cit* 26.

[1517] *Ibid*.

[1518] The Act, section 63(2); Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p*.

[1519] Viego *op cit* 11 – 15.

could also obtain the independent accreditation of their cybersecurity practices and their responsible use of AI.[1520]

7. CONCLUSION

Chapter 4 looked at the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG investment considerations in order to look how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.[1521]

This Chapter consequently looked at the evolution of the emphasis on CSR to sustainability to ESG considerations. It was explained that the evolution of ESG shows clear differences between CSR, sustainability and ESG considerations.[1522] The development of CSR focused on accountability and ethics, sustainability emerged in the 1980's and focused on the role that stakeholders need to play to ensure sustainable development, while the introduction of ESG considerations places a focus on changing the behaviour of investors when they make their investment decisions.[1523] Although the three concepts overlap in terms of their goal to ensure that the company survives and flourishes, they have many differences.[1524] In this regard, it was highlighted that the umbrella concept of sustainability cannot be implemented without tension with CSR and ESG.[1525] It was explained by means of a timeline how the model of ESG considerations became the universal standard approach.[1526]

The Chapter then looked at the way in which SA directors should exercise their duty of care in terms of corporate governance, CSR and ESG considerations. It was explained that since SA is a resource-scarce country, sustainability-related challenges will continue to threaten the growth and survival of SA companies as the competition for resources will increase.[1527] It consequently becomes more important that SA companies need to adapt to their corporate sustainability challenges and to manage their ESG risks.[1528] In addition, stakeholders, such as customers, investors, shareholders and suppliers should acknowledge that ESG considerations should be included in the long run to create value in a sustainable manner.[1529]

[1520] Viego *op cit* 11 – 15.
[1521] Amodu 'Stakeholder Protection and CSR from a Comparative Company Law Perspective' in *Journal of African Law* March 2020, 2.
[1522] Esser *et al. op cit* 34.
[1523] *Ibid*.
[1524] *Ibid*.
[1525] *Ibid*.
[1526] *Ibid*.
[1527] Erasmus *et al. op cit* 3 – 4.
[1528] *Ibid*.
[1529] *Ibid*.

Specific attention was also given to the exercise of the directors' duty of care in relation to cybersecurity and the use of AI and Blockchain technology since this is a new field that is developing fast and directors will need to address the challenges that they present. It was said that the King Code should start to regulate AI and Blockchain technology in the SA corporate governance regime at a time when these technologies are still in their infant shoes.

Lastly, lessons were drawn on how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.

Following on this, Chapter 5 will look at the further accountability mechanisms to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI.

CHAPTER 5:

THE FURTHER ACCOUNTABILITY MECHANISMS TO HOLD DIRECTORS ACCOUNTABLE FOR THE WAY IN WHICH THEY EXERCISE THEIR DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI

1. INTRODUCTION

The previous Chapter explained the indirect impact of the directors' duty of care in relation to cybersecurity in order for the King Code to maximise this indirect impact on corporate governance and CSR and ESG investment considerations.

It has been explained in Chapters 2, 3 and 4 that keeping directors accountable in terms of their duty of care in relation to cybersecurity is an important way to help prevent prevent cyberbreaches at a company.[1530] One of the most important issues in the Cadbury Report was to look at how the accountability of directors could be strengthened to the shareholders.[1531] Keay explains that good corporate governance should focus on the accountability of directors, and he argues that it is the basis for the successful implementation of all other corporate governance principles.[1532]

At the same time, there is a lot of debate under researchers on the accountability of boards and many researchers evaluated if boards are held accountable enough.[1533] In response, Loughrey went as far as saying that the lack of keeping them accountable has created an "accountability firewall."[1534] Keay and Loughrey also explain that researchers in the field of corporate governance have not done enough research on the concept of directors' accountability and what it means or demands.[1535] They also say that this lack of research and debate creates a problem, because if shareholders and stakeholders don't have a clearer idea on how to keep directors accountable, it will create an "accountability deficit" if they are not held sufficiently accountable.[1536] This Chapter addresses this problem by explaining why accountability is important and then

---

[1530] See Chapters 2, 3, 4.

[1531] UK Committee on Financial Aspects of Corporate Governance *op cit* paragraph 6.1; Keay 'Stewardship Theory: Is Board Accountability Necessary' in *International Journal of Law and Management* 59(6) 2017 1292.

[1532] Keay 'Accountability and the Corporate Governance Framework: From Cadbury to the UK Corporate Governance Code,' *Social Science Research Network Working Paper* (August 2012), 42, available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143171>, last accessed on 27 June 2023; Keay *Board Accountability in Corporate Governance op cit* 21; Keay 'Stewardship Theory: Is Board Accountability Necessary' *op cit* 1292.

[1533] Keay, Loughrey 'The Framework for Board Accountability in Corporate Governance' in *Legal Studies* 35(2) 2015 252.

[1534] Loughrey 'Breaching the Accountability Firewall: Market Norms and the Reasonable Director' *op cit* 990.

[1535] Keay, Loughrey 'The Framework for Board Accountability in Corporate Governance' *op cit* 252.

[1536] *Ibid*.

explains how directors should be held accountable when they exercise their duty of care in relation to cybersecurity.

Chapter 5 will consequently build on the analysis offered in Chapters 2, 3 and 4 and will look at the various other accountability mechanisms, besides the common law and legislative duties of care, which shareholders/stakeholder may use to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the responsible use of AI. It is important that directors have a proper understanding of these various accountability mechanisms in order to limit the possibility that they could be held liable for not exercising their duty of care in relation to cybersecurity properly.

The Chapter will also look at lessons on how directors' use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code. It will begin by giving an overview of the international privacy law and cybersecurity regimes. Thereafter it will analyse the SA privacy law and cybersecurity regimes and look at their shortcomings. Thereafter, it will look at the further accountability mechanisms and the lessons on how the responsible use of AI should be regulated within this regime.

2. AN OVERVIEW OF THE INTERNATIONAL PRIVACY LAW AND CYBERSECURITY REGIMES

Many of the world's largest international organisations (IOs) have long ago started to realise the importance of privacy and cybersecurity and have promulgated regulations in this regard.[1537] These regulations are also applicable to SA, since SA is a member of these IO's and a signatory of their international instruments.

2.1. The International Privacy Law Regime

Companies are incorporated in jurisdictions that are signatories to a number of international instruments that contain privacy regulations. As soon as a country has ratified such a treaty, its law has to comply with the provisions thereof. Since SA, the UK and the US are signatories to the following treaties that regulates aspects of privacy or the protection of personal information, a glance of the relevant provisions of these international instruments is required.

2.1.1. UN Universal Declaration on Human Rights of 1948

[1537] Kirby '*Privacy Protection, A New Beginning: OECD Principles 20 Years On,' s.p.*, available online at <http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/41.html>, last accessed on 27 December 2019.

The UN Universal Declaration on Human Rights of 1948, article 12 has bearing since it states that no one may arbitrarily interfere with someone's privacy, correspondence, family or home or attack their honour or reputation.[1538] This implies that a director has a duty to see to it that no one interferes with the online databases.[1539]

2.1.2. UN International Covenant on Civil and Political Rights of 1966

The UN International Covenant on Civil and Political Rights of 1966, article 17 also has bearing.[1540] Although, section 17(1) is similar to the provision in the UN Universal Declaration on Human Rights of 1948, article 12, its subsection (2) states that everyone's privacy is protected by law.[1541] This further implies that directors have a duty to protect the online databases.

2.1.3. The Organisation for Economic Co-operation and Development (OECD)'s Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data of 1981

In 1981, the Organisation for Economic Co-Operation (OECD) issued the Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (the 'OECD Guidelines') and this has served as the basis for many jurisdictions' legislation and guidelines on the protection of personal information.[1542] The security safeguards principle contained in the 'OECD Guidelines,' section 11 states that personal information should be protected by reasonable security measures.[1543] Additionally, the accountability principle contained in section 14 states that a data controller, such as a board, is responsible to comply with all of the measures that are set out in the 'OECD Guidelines.'[1544]

The 'OECD Guidelines' should however be updated to specifically prohibit the use of AI to commit cybercrime to obtain personal information, and it should also be updated to encourage the responsible use of AI to protect personal information.[1545]

2.2. The International Cybersecurity Regime

[1538] UN Universal Declaration of Human Rights of 1948, article 12.
[1539] *Ibid.*
[1540] UN International Covenant on Civil and Political Rights of 1996, article 17.
[1541] UN International Covenant on Civil and Political Rights of 1996, article 17(2).
[1542] OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data ('OECD Guidelines') of 1980.
[1543] OECD Guidelines of 1980 *op cit* section 11.
[1544] OECD Guidelines of 1980 *op cit* section 14.
[1545] OECD Guidelines of 1980 *op cit* section 11.

The international cybercrime landscape is dominated by one treaty that is of particular importance to SA.

2.2.1. The Council of Europe (CoE)'s Budapest Convention of 2001

The Council of Europe (CoE)'s 'Convention on Cybercrime' or 'Budapest Convention,' was the world's first multilateral treaty on the prevention of cybercrime, and it came into effect on 1 July 2004.[1546] This Convention is the only binding multilateral treaty that regulates cybercrime.[1547]

This Convention sets out a framework on the combatting of cybercrime, as well as guidelines that member states can use when they compile their own national legislation in this regard.[1548] It also enables international cooperation between member states to help combat cybercrime and also recommends cooperation on cross-border investigations on cybercrime.[1549]

It specifically prohibits any illegal access to a computer system, any illegal interception of online communications, any interference with data or software programmes, any misuse of hardware or software devices, any computer-related forgery and fraud, as well as any attempt to assist the committing of a cybercrime.[1550]

It also encourages all member states to adopt national legislation against cybercrime that could then be enforced globally by means of this Convention.[1551] Sixty seven member states have so far ratified this Convention.[1552]

Although SA adopted this Convention on 23 November 2001, it has not yet ratified the treaty.[1553] SA is consequently not obliged to comply with this Convention's provisions.[1554] It is as a result important that SA must ratify this treaty as soon as possible.

3. AN OVERVIEW OF THE SA PRIVACY LAW AND CYBERSECURITY REGIMES

[1546] Council of Europe (CoE) '*Convention on Cybercrime of 2001*' (ETS 185), *s.p.*

[1547] *Ibid.*

[1548] CoE '*Details of Treaty No. 185*,' *s.p.*, available online at <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>, last accessed on 7 January 2023.

[1549] *Ibid.*

[1550] CoE '*Convention on Cybercrime of 2001*' (ETS 185) *op cit*, articles 2 – 12.

[1551] *Ibid.*

[1552] CoE '*Chart of Signatures and Ratifications of Treaty No. 185*,' *s.p.*, available online at <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, last accessed on 7 January 2022.

[1553] CoE *'Chart of Signatures and Ratifications of Treaty No. 185' op cit s.p.*

[1554] *Ibid.*

The following section will give an overview of the SA privacy law and cybersecurity regimes.

3.1. The SA Common Law Position on Cybersecurity

The concept of cybersecurity only really started to become known in the 1990's as SA was starting to emerge from decades of international isolation due to sanctions, which the international community imposed on the country's Apartheid regime.[1555] Initially, the common law was used during this transitional period to combat cybercrime in SA and to enforce cybersecurity.[1556] As a result, only cybercrimes such as cyberfraud and online defamation were initially prohibited in terms of the SA common law.[1557] Since the concepts of cyberforgery, cyberuttering and the interception of online information were at that point in time so new, they were initially not prohibited in terms of the SA common law.[1558] As a result, SA companies were for a long time left exposed to cybercrimes, such as cyberattacks, identity theft, online information theft, online scams and phishing before legislation was adopted to regulate these crimes.[1559] In addition, the enforcement of the SA common law on cybercrime was hampered by physical court jurisdictional challenges due to the fact that cybercrime is committed online.[1560]

3.2. The Legislative Regulation of Cybersecurity in SA

The following section will explain the legislative regulation of cybersecurity in SA.

3.2.1. The SA Electronic Communications and Transactions Act (ECTA) 25 of 2002

After a few years without regulations on cybersecurity, the SA Electronic Communications and Transactions Act (ECTA) 25 of 2002 was promulgated to, amongst other things, also help fight cybercrime in SA.[1561] The SA ECTA 25 of 2002, sections 85 – 89 were the first legal provisions to directly prohibit cybercrime in SA.[1562] It omitted to define the concepts of 'cybercrime' and 'cybersecurity,' but section 85 did

---

[1555] Thornton *et al. Telecommunications Law in SA* 332.
[1556] Cassim 'Addressing the Challenges Posed by Cybercrime: A SA Perspective' in *Journal of International Commercial Law and Technology* (2010) 119; Thornton *et al. op cit* 332.
[1557] *Ibid.*
[1558] Chitimira 'The Regulation and Use of AI and 5G Technology to Combat Cybercrime and Financial Crime in SA Banks' in *Potchefstroomse Elektroniese Regsblad* (24) 2021 6.
[1559] Cassim 'Addressing the Challenges Posed by Cybercrime: A SA Perspective' *op cit* 119.
[1560] Snail 'Cybercrime in SA: Hacking, Cracking, and Other Unlawful Online Activities' in *Journal of International Logistics and Trade* (2009) 3.
[1561] *Ibid*.
[1562] SA ECTA 25 of 2002, sections 85 - 89.

define that 'unlawful online access' is when a cybercriminal intentionally accesses prohibited online information.[1563] Section 86 outlaws any unauthorised access to online communications, as well as the unuathorised interception of, or interference with, online communications.[1564] In this regard, section 86(1) explains that anyone who intentionally accesses or intercepts any online information without the authorisation of its owners is liable for an offence.[1565] Section 86(2) also explains that anyone who intentionally interferes with online information and destroys, modifies or tries to make it useless is liable for an offence.[1566] Section 86(3) again prohibits anyone from unlawfully using hardware or software that can overcome cybersecurity measures.[1567] These provisions are clearly focused to help fight cybercrime that involves the unlawful interference with online information.[1568] In addition, section 87 prohibits all cyberforgery, cyberfraud and online extortion.[1569] In this regard, section 87(1) explains that anyone who performs a cybercrime or who interferes with any online information may be fined.[1570] Section 88(1) states that anyone who tries to commit any of the listed cybercrimes may also be held liable.[1571] Section 88(2) states that anyone who assists someone else to commit cybercrime may be fined.[1572]

Although this Act helps to resist hacking and the use of anti-cybersecurity and circumventer IT that are used to create cyberbreaches at SA companies, it does have its shortcomings.[1573] The first shortcoming is found in section 89, since the unspecified amount of the fine and the prison term does not help to deter cybercrimes.[1574] In addition, this Act does not prohibit the use of AI to commit cybercrime, nor does it make provision for the use of AI to improve the cyberresilience of SA companies, and it also does not especially prohibit a cybercrime such as cyberwarfare.[1575]

3.2.2. The SA Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 70 of 2002

[1563] SA ECTA 25 of 2002, section 85.
[1564] SA ECTA 25 of 2002, section 86.
[1565] SA ECTA 25 of 2002, section 86(1).
[1566] SA ECTA 25 of 2002, section 86(2).
[1567] SA ECTA 25 of 2002, section 86(3).
[1568] *Ibid.*
[1569] SA ECTA 25 of 2002, section 87.
[1570] SA ECTA 25 of 2002, section 87(1).
[1571] SA ECTA 25 of 2002, section 88(1).
[1572] SA ECTA 25 of 2002, section 88(2).
[1573] SA ECTA 25 of 2002, section 86; Pitts *Cybercrimes: A History of the World's Worst Cyberattacks* 53.
[1574] SA ECTA 25 of 2002, section 89 of the ECTA; Cassim 'Addressing the Challenges Posed by Cybercrime: A SA Perspective' *op cit* 119.
[1575] Van Der Merwe *et al. Information and Communications Technology Law* 71.

Hereafter, the SA RICA 70 of 2002 was promulgated in an attempt to further improve cybersecurity in SA.[1576] According to its preamble, it, amongst other things, regulates applications to intercept communications.[1577] It contains some sections which are relevant to the hosting of OMs and the protection of the online databases, such as section 10, which enables law enforcement agencies to identify illegal cellphone users.[1578] Section 11 allows these entities to track and locate such cybercriminals.[1579] Section 43 does however not prevent the disclosure of information by an authorised person for the performance of official duties, as long as it does not violate this Act.[1580] Section 49 prohibits the unlawful interception of communications by any unauthorised persons.[1581] Section 50 prohibits the unlawful provision of online or stored information to someone else.[1582]

A shortcoming is that the SA RICA 70 of 2002 does not specifically prohibit cybercrime towards SA companies.[1583] It also does not prohibit the use of AI, and specifically GANs, which can circumvent cybersecurity systems in order to circumvent the interception of communications, nor does it make provision for the responsible use of AI to fight cybercrime that are committed towards SA companies and their online databases.[1584]

3.2.3. The SA Protection of Personal Information (POPI) Act 4 of 2013

The SA POPI Act 4 of 2013, sections 5 - 35 aims to protect the personal and private information of all data subjects.[1585]

Chapter 3 explains the conditions for the lawful processing of personal information.[1586] Condition 1 is accountability and it determines that the board is accountable for all of the personal information in its possession, even if it is passed on to a third party.[1587] Condition 2 is processing limitation and it requires that personal information must be processed lawfully and not comprise a data subject's privacy.[1588] Condition 3 is purpose specification and it determines that personal information can only be collected for a lawful and specific purpose.[1589] Condition 4 is further processing

[1576] SA RICA 70 of 2002.
[1577] SA RICA 70 of 2002, Preamble.
[1578] SA RICA 70 of 2002, section 10.
[1579] SA RICA 70 of 2002, section 11.
[1580] SA RICA 70 of 2002, section 43.
[1581] SA RICA 70 of 2002, sections 49; 2-15.
[1582] SA RICA 70 of 2002, sections 50; 2-15.
[1583] Chitimira *op cit* 15.
[1584] *Ibid.*
[1585] SA POPI 4 of 2013, sections 5 - 35.
[1586] SA POPI 4 of 2013, Chapter 3.
[1587] SA POPI 4 of 2013, section 8.
[1588] SA POPI 4 of 2013, sections 9 - 12.
[1589] SA POPI 4 of 2013, sections 13 - 14.

limitation and it determines that personal information can only be processed for the reason why it was collected.[1590] Condition 5 is information quality and it requires the board to ensure that the personal information, which was collected, is accurate and updated.[1591] Condition 6 is openness and this requires the board to be open on why they require the personal information and how they will process it.[1592] Condition 7 is security safeguards and this require the board to implement the proper organisational and technical measures to safeguard the processing of the personal information.[1593] Condition 8 is data subject participation and this allows data subjects such as the shareholders/stakeholders to enquire whether boards are in possession of any of their personal information and for them to obtain a copy thereof, should they require it.[1594]

Chapter 5, Part A, sections 39 to 53 establishes the IR and sets out its duties, where it is amongst other things tasked to monitor and enforce compliance with the SA POPI's provisions.[1595]

Chapter 9, section 72 regulates the transfer of personal information outside SA.[1596]

Chapter 10, sections 71 – 96 again regulate the enforcement of this Act.[1597] Chapter 10, sections 80 – 86 regulate amongst other things the issuing, requirements and execution of warrants that are needed to fight cybercrime.[1598]

Despite these provisions, cybercrime that comprises the integrity of personal information is still widespread in SA.[1599] It is a shortcoming that the SA POPI 4 of 2013 does not prohibit the use of AI to commit cybercrime that involves personal information, nor that it encourages the responsible use of AI to help combat cybercrime that involves personal information.

3.2.4. The SA Cybercrimes Act 19 of 2020

In an attempt to fill some of the remaining legislative gaps, the SA Cybercrimes Act 19 of 2020 was promulgated and came into effect on 1 December 2021.[1600] Amongst other things, this Act aims to protect all persons, including companies, from cybercriminals who use online means to commit cybercrimes.[1601] Section 2 states that

[1590] SA POPI 4 of 2013, section 15.
[1591] SA POPI 4 of 2013, section 16.
[1592] SA POPI 4 of 2013, sections 17 - 18.
[1593] SA POPI 4 of 2013, sections 19 - 22.
[1594] SA POPI 4 of 2013, sections 23 - 25.
[1595] SA POPI 4 of 2013, Chapter 5, Part A, sections 39 - 53.
[1596] SA POPI 4 of 2013, Chapter 9, section 72.
[1597] SA POPI 4 of 2013, Chapter 10, sections 71 - 96.
[1598] SA POPI 4 of 2013, Chapter 10, sections 80 - 86.
[1599] See Chapter 1, section 3.2.
[1600] SA Cybercrimes Act 19 of 2020.
[1601] SA Cybercrimes Act 19 of 2020, Preamble.

any unlawful access to online information is prohibited.[1602] Section 3 states that any unlawful acquisition of online information is prohibited.[1603] Section 4 determines that any unlawful acts pertaining to the use of software or hardware are illegal.[1604] Section 5 states that any unauthorised interference with online information or a computer programme is illegal.[1605] Section 6 explains that any unlawful interference with an online information storage medium or online system is illegal.[1606] Section 7 says that any illegal acquisition or use of access codes or passwords is prohibited.[1607] Sections 8, 9 and 10 prohibits cyberfraud, cyberuttering and online extortion.[1608] Section 11 also prohibits cyber-related aggravated offences.[1609] Section 12 explains that the theft of an incorporeal thing is also considered to be a cybercrime.[1610]

Section 52 establishes the SA Cybercrime Point of Contact (PoC) in an attempt to help combat cybercrime.[1611] Section 54(1)(a) obliges persons and companies to report a cybercrime and; (b) to preserve any evidence which could be used to prove that a cybercrime was committed and to hand it over to the PoC.[1612]

In instances were a cybercrime was committed, directors also need to remember that if they do not report it, and if they do not preserve any evidence related to it, that they will be liable for criminal penalties.[1613] It is a shortcoming that this Act does not especially prohibit the use of AI to commit cybercrimes, and also that it does not make provision for the responsible use of AI to fight cybercrime towards SA companies.[1614]

4. THE FURTHER ACCOUNTABILITY MECHANISMS TO HOLD DIRECTORS ACCOUNTABLE FOR THE WAY IN WHICH THEY EXERCISE THEIR DUTY OF CARE IN RELATION TO CYBERSECURITY AND THE USE OF AI

Besides the common law and legislative duties of care, which was already looked at in Chapter 3, directors may in the event of cyberbreach or even a potential cyberbreach, also be exposed to various other types of liability due to the improper exercise of their duty of care in relation to cybersecurity, and this could lead to various

[1602] SA Cybercrimes Act 19 of 2020, section 2.
[1603] SA Cybercrimes Act 19 of 2020, section 3.
[1604] SA Cybercrimes Act 19 of 2020, section 4.
[1605] SA Cybercrimes Act 19 of 2020, section 5.
[1606] SA Cybercrimes Act 19 of 2020, section 6.
[1607] SA Cybercrimes Act 19 of 2020, section 7.
[1608] SA Cybercrimes Act 19 of 2020, sections 8 – 10.
[1609] SA Cybercrimes Act 19 of 2020, section 11.
[1610] SA Cybercrimes Act 19 of 2020, section 12.
[1611] SA Cybercrimes Act 19 of 2020, section 52.
[1612] SA Cybercrimes Act 19 of 2020, section 54(1)(a) – (b).
[1613] *Ibid.*
[1614] SA Cybercrimes Act 19 of 2020.

costs that could be recovered from them and also their removal. Amongst other things, they may be held liable by the company for the losses it sustained.[1615] The company may as a result hold them liable for the data recovery or the recovery or the replacing of the computer system.[1616] A company may also not remain operational after a cyberbreach occurred, as their computer system will remain offline while it is being fixed, and this means that if their system is inaccessible, it will lead to additional revenue loss.[1617]

In addition, they may be held liable for breach notification expenses since they need to immediately notify data subjects of a cyberbreach, even if there was a suspected cyberbreach.[1618]

Added to this, they may be held liable for the payment of regulatory fines, which are not only imposed by the IR, but in some instances also by industry sector regulators.[1619] Certain industry regulators may also impose substantial fines on a board in the event that a cyberbreach occurred, and this was caused because a board failed to meet compliance requirements.[1620]

The board could also be held liable for a class action lawsuit that is filed on behalf of shareholders/stakeholders whose privacy and personal information were compromised.[1621] They may hold them liable for the costs which they had to incur as a result of a cyberbreach and the compromisation of the integrity of their personal information.[1622] They may also hold them liable because they did not properly disclose a cyberrisk or a cyberattack.[1623]

They may also be held liable for the reimbursement and/or reissuance of the monetary value of fraudulent transactions that resulted for shareholders/stakeholders after a cyberbeach occurred when their personal information was compromised.[1624]

In addition, companies could also suffer additional financial losses, which may be caused by cyberextortion, reputational harm to their brand promise, or the theft of their intellectual property and hold directors liable for these losses.[1625]

[1615] Cohen *et al.* 'Understanding Cyberrisk and Cyberinsurance' in the *Social Science Research Network's Electronic Law Journal* (January 2017) 5 – 6.
[1616] D'Cruze *et al.* 'Economic Costs and Impacts of Business Data Breaches' in *Issues in Information Systems* (2019) 20(2) 165.
[1617] *Ibid.*
[1618] Insurance Information Institute (III) 'Cyberliability Risks,' *s.p.*, available online at <https://www.iii.org/article/cyber-liability-risks#What%20are%20your%20cyber%20liability%20risks?>, last accessed on 10 January 2023.
[1619] D'Cruze *et al. op cit* 166.
[1620] *Ibid.*
[1621] *Ibid.*
[1622] Cohen *et al. op cit* 5 – 6.
[1623] III *op cit s.p.*
[1624] *Ibid.*
[1625] *Ibid.*

Although directors owe their duty of care to the company, and not to the shareholders, boards still need to make sure that companies comply with their obligations to protect their online databases, otherwise they will be held directly accountable by the shareholders/stakeholders for the violation of their privacy.

The rest of this section will look at all of the various internal and external accountability mechanisms, besides the common law and legislative duties of care, which could be used to hold directors accountable to the company itself, or which could be used by the shareholders/stakeholders, when the board did not properly exercise their duty of care in relation to cybersecurity.

4.1. Constitutional Right to Privacy

Directors could be held personally liable when shareholders/stakeholders' right to privacy is breached in SA, because this right is protected in terms of the Constitution, section 14, which guarantees the right to privacy.[1626]

4.2. The Act

It will be explained below that in terms of the Act, directors may be held liable in various ways when they do not exercise their duty of care in relation to cybersecuity properly.

4.2.1. Section 20: The Validity of Company Actions

The Act, section 20 provides shareholders with a legislative right to prevent the board or the company from violating any of the Act's provisions.[1627] This section also provides shareholders with a legislative right to prevent the company from conducting any *ultra vires* actions.[1628]

4.2.1.1. Section 20(4): Restraining the Company from Contravening the Act

The Act, section 20(4) states that one or more directors, employees, shareholders or a representative of a trade union that represents the employees, may ask the High Court for an order to prevent the company from doing an action that is not in accordance with the Act.[1629] This section is therefore limited to contraventions of the Act only, and does not cover contraventions of the MOI.[1630]

[1626] SA Constitution, section 14.
[1627] The Act, section 20(4).
[1628] The Act, section 20(5).
[1629] The Act, section 20(4).
[1630] *Ibid*.

This section in other words allows shareholders to act when directors do not, amongst other things, properly exercise their duty of care properly as required in terms of section 24, which pertains to the form and standards for company records; section 25, which pertains to the location of company records; or section 26, which relates to access to company records.[1631]

4.2.1.2. Section 20(5): Restraining the Company from Contravening the MOI

Section 20(4) is strenghtened by section 20(5), which enables directors, employees or shareholders to approach the High Court to obtain an order to prevent the company from performing any action that is not in accordance with any limitation, qualification or restriction of the capacity of a company or the authority of the directors in terms of its MOI, as contemplated in section 20(2).[1632]

This means that if a MOI requires certain actions in terms of cybersecurity, and the directors do not ensure that it happens, then shareholders have an action to enforce such provisions of the MOI.[1633]

4.2.1.3. Section 20(6): Each Shareholder Has a Claim Against Anyone Who Intentionally, Fraudulently or Due to Gross Negligence Causes Anything Inconsistent with the Act

The Act, section 20(6) determines that each shareholder may claim damages from anyone who due to fraud, gross negligence or intentionally caused the company to do anything that is not in line with (a) the Act; or (b) with a limitation of the company's capacity or its directors' authority, and which has not been ratified by a special resolution, as required by section 20(2).[1634] Section 20(3) states that an action that is prohibited by the Act may not be ratified.[1635]

It needs to be pointed out that this provision specifically refers only to shareholders, and thus excludes stakeholders.[1636]

Cassim *et al.* explains that a rare opportunity to clarify the ambit and scope of section 20(6) was sadly missed in 2020 by Unterhalter, J, of the South Gauteng High Court in *De Bruyn v Steinhoff International Holdings NV*.[1637] Here, the conduct of the Steinhoff directors was alleged to have contravened the Act and to have given rise to

---

[1631] The Act, sections 20(4); 24 – 26.
[1632] The Act, sections 20(2); 20(4); 20(5).
[1633] The Act, section 20(5).
[1634] The Act, sections 20(2); 20(6)(a) – (b).
[1635] The Act, section 20(3).
[1636] The Act, section 20(6)(a)-(b).
[1637] The Act, section 20(6); *De Bruyn v Steinhoff International Holdings NV* (29290/2018) (2020) ZAGPHJC 145 (26 June 2020); Cassim *et al. Contemporary Company Law op cit* 223.

liability in terms of section 20(6) or 218(2) for the damages of the shareholders.[1638] Alternatively, it was argued that the Steinhoff directors deliberately or negligently breached their duties of care and thereby became delictually liable to the class shareholders for the damages which they suffered.[1639]

The shareholders alleged that Steinhoff, through the actions of its directors, made unlawful transactions.[1640] These transactions misrepresented the company's assets, income and profits in the financial statements and understated its expenses and liabilities.[1641] It was argued that the directors of Steinhoff were required to disclose the true nature of the fraudulent transactions and statements, but failed to do so.[1642]

The argument of the shareholders however had a challenge.[1643] An argument could be made out that the directors' conduct was in breach of their fiduciary duties, but the challenge was that those duties were owed to the company.[1644] The harm that the company suffered due to the breach of their fiduciary duties was only actionable by the company to whom the duties were owed.[1645] The breach may also have caused harm to the shareholders, and also possibly to the stakeholders, but the fact that harm was caused does not mean that the duty was owed to everyone who suffered harm.[1646]

It was held in *De Bruyn supra* that section 20(6) does not give shareholders a personal right to claim damages for personal loss which they suffered due to such misconduct.[1647] If the company suffered a loss, damages can be claimed by the shareholders on behalf of the company, in terms of section 20(6), but not on their own personal behalf.[1648] If the shareholders were able to prove that they had suffered a loss that is apart from the company's loss, it would however be a different scenario.[1649]

Section 20(6) however, unlike section 218(2), gives this right to each shareholder of a company.[1650] This section also sets out the different types of fault for which the defendant should be held liable; and this also helps to distinguish section 20(6) from section 218(2).[1651]

Cassim *et al.* explains that despite the clear meaning of section 20(6), Unterhalter, J strangely decided that the section allowed shareholders the right to claim

---

[1638] The Act, sections 20(6); 218(2); *De Bruyn supra*.
[1639] The Act, section 76(3)(c); *De Bruyn supra*.
[1640] *De Bruyn supra*.
[1641] *Ibid*.
[1642] *Ibid*.
[1643] *De Bruyn supra*; Cassim *et al. Contemporary Company Law op cit* 868.
[1644] *Ibid*.
[1645] *Ibid*.
[1646] *Ibid*.
[1647] The Act, section 20(6); *De Bruyn supra* paras. 220 - 237; Cassim *et al. Contemporary Company Law op cit* 373.
[1648] *Ibid*.
[1649] *Ibid*.
[1650] The Act, sections 20(6); 218(2); Cassim *et al. Contemporary Company Law op cit* 872.
[1651] *Ibid*.

damages for the loss that the company suffered.[1652] In this regard, Unterhalter J, said that the shareholders could not claim damages suffered by them, as the shareholders themselves.[1653] Unterhalter, J did not explain why his understanding of the purpose of section 20(6) could not be reached by section 165.[1654] In this regard, Cassim *et al.* says correctly that since section 165 makes provision for a derivative claim by shareholders for the loss that the company suffered, the SA legislature surely did not intend section 20(6) to also serve the same purpose as the derivative action.[1655] It needs to be pointed out that Unterhalter, J did not cite any authority for his view.[1656]

4.2.2. Section 71: The Removal of Directors

Section 71(1) determines that directors who breached their duty of care and skill, may be removed by the shareholders with an ordinary resolution at a general meeting.[1657] Directors who were appointed *ex officio* may only be removed by the board or the Companies Tribunal, after they were given notice of the meeting where such a matter was on the agenda and if they were given a chance to make representations.[1658] In terms of section 71(3), a director may also be removed if the directors insist thereon.[1659] The allegations against such a director must then satisfy the board.[1660]

If a director was appointed to a board by a specific person, such a director can only be removed by that person, the board or the Companies Tribunal.[1661] Directors who were appointed by the shareholders can be removed by the board, the Companies Tribunal or the shareholders.[1662] Section 71(3) states that a removal from the board is only possible where the board has more than two directors; while section 71(8) states that it is only possible for the Companies Tribunal to remove a director when a board has less than three directors.[1663] Section 71(8) states that any director or shareholder may apply to the Companies Tribunal for an order to remove a director in terms of the grounds listed in section 71(3).[1664]

Directors may be removed at the request of directors or shareholders who allege that they are disqualified or ineligible in terms of section 69, in the event that a court

---

[1652] The Act, section 20(6); *De Bruyn supra*; Cassim *et al. Contemporary Company Law op cit* 223.
[1653] *Ibid*.
[1654] The Act, sections 20(6); 165; *De Bruyn supra*; Cassim *et al. Contemporary Company Law op cit* 223 - 224.
[1655] *Ibid*.
[1656] *Ibid*.
[1657] The Act, section 71(1).
[1658] The Act, section 71(2).
[1659] The Act, section 71(3).
[1660] *Ibid.*
[1661] The Act, section 66(4)(a)(i).
[1662] Ncube *op cit* 37.
[1663] The Act, sections 71(3); 71(8).
[1664] The Act, section 71(8).

order has been made that prohibits such a person from being a director or which declares them as a delinquent in terms of section 162.[1665] In 2012, Kathree-Setiloane, J of the South Gauteng High Court confirmed in *Msimang NO and Another v Katuliiba and Others* the requirements to declare a director delinquent, in terms of section 162 (5)(c)(iv)(aa).[1666] In 2016, Yekiso, J of the Western Cape High Court also came to a similar conclusion in *Cape Empowerment Trust Limited v Druker and Others* and reconfirmed these requirements.[1667] In 2011, Tshabalala, J of the South Gauteng High Court explained in the *Kukama v Lobela and Others* that as soon as a director is declared a delinquent they have been removed automatically with that order and a separate order to this effect is not required.[1668]

The directors or shareholders may also insist on the removal of a director on other grounds, such as a dereliction of duties, an inability to perform their functions, or negligence (in terms of section 76) in terms of their oversight on cybersecurity.[1669]

4.2.3. Section 77: Liability of Directors

The Act, section 77 allows directors to be held liable for a breach of their duties, since they are accountable to the company.[1670] The Act, section 76(3) has enhanced the accountability of directors with the partial codification of their duties, and by holding them liable in the the event of a breach thereof.[1671] Directors need to perform these duties since they stand in a fiduciary relationship to the company and because they have a duty of care.[1672]

The Act, section 77(2)(a) determines that a director may be held liable (due to the common law principles on the breach of a fiduciary duty) for any damages that the company experienced, which were caused by any breach of the duties that are set out in sections 75, section 76(2) or 76(3)(a) or (b).[1673] Likewise, section 77(2)(b) states that a director may be held liable in terms of the common law delict for any damages which the company has suffered that were caused by a breach of the duty of care and skill in terms of section 76(3)(c); losses due to a breach of a provision of the Act that is not mentioned in section 77; and losses that were caused by a contravention of the MOI.[1674]

[1665] The Act, sections 69; 162.
[1666] *Msimang NO and Another v Katuliiba and Others* (2013) JOL 30522 (GSJ).
[1667] *Cape Empowerment Trust Limited v Druker and Others* (2016) JOL 36987 (WCC).
[1668] *Kukama v Lobelo and Others* (38587/2011) (2012) ZAGPJHC 60.
[1669] The Act, section 76; Ncube *op cit* 39.
[1670] The Act, section 77.
[1671] The Act, section 76(3).
[1672] *Hlumisa Investment Holdings (RF) Limited v Kirkinis (No. 1)* 2019 4 SA 569 (GP).
[1673] The Act, sections 77(2)(a); 75; 66(2); 76(3)(a) – (b).
[1674] The Act, sections 76(3)(c); 77; 77(2)(b).

Section 77(2) therefore includes the common law liability of directors, and states that it is the company which needs to enforce its interests against the directors.[1675]

In 2019, Molopa-Sethosa, J, of the North Gauteng High Court stated in *Hlumisa Investment Holdings (RF) Ltd v Kirkinis (No. 1)* that shareholders may not institute an action against directors for a breach of their fiduciary duties, as set out in section 76(3), in terms of section 218(2) since those duties are owed to the company.[1676] Section 77(2)(a) – (b) provides a special remedy for contraventions of section 76(3), on which plaintiffs must rely, and in terms of which subsection (a) allows liability in terms of the common law; and subsection (b) allows liability in terms of delict.[1677] Molopa-Sethosa, J used the principle that where a statute provides a special remedy, such a special remedy must be used instead of a general remedy.[1678]

In 2019, Navsa JA of the SA SCA highlighted in *Hlumisa Investment Holdings (RF) Limited (No. 2) supra* that the special remedy which the Act, section 77(2) provides with respect to the contravention of section 76(3), derives from directors' fiduciary duty to the company and not to the shareholders.[1679]

4.2.4. Section 78(6): Directors Cannot be Indeminfied Against Liability for Not Exercising Their Duty of Care

The Act, section 78(5) allows a company to indemnify its directors from being held liable in certain instances.[1680]

Section 78(6) however says that a company is not allowed to indemnify a director against (a) any of their liabilities that are imposed (i) in terms of section 77(3)(a) - (c).[1681]

4.2.5. Section 165: Legislative Derivative Action

The Act, section 165 contains a legislative derivative action, which allows anyone to institute an action on behalf of a company in an attempt to protect the company's interests.[1682]

This means that besides the company, shareholders and stakeholders also have legal standing to claim damages for losses.[1683] This inclusion of this legislative action in the Act ended the common law right that anyone could take action on behalf of the

---

[1675] The Act, sections 76(3)(c); 77; 77(2)(b).
[1676] The Act, sections 76(3); 218(2); *Hlumisa Investment Holdings (RF) Ltd (No. 1) supra*, paras. 29 – 30; Cassim *et al. Contemporary Company Law op cit* 1130.
[1677] The Act, sections 77(2)(a) – (b); 76(3); *Hlumisa Investment Holdings (RF) Ltd (No. 1) supra*, paras. 29 – 30.
[1678] *Ibid*.
[1679] The Act, sections 76(3); 77(2); *Hlumisa Investment Holdings (RF) Limited (No. 2)* 2020 (5) SA 419 (SCA).
[1680] The Act, section 78(5).
[1681] The Act, sections 77(3(a) – (c); 78(6)(a)(i).
[1682] The Act, section 165; Blackman *et al. op cit* 9-178.
[1683] The Act, sections 20(6)(a)-(b); 218(2).

company.[1684] Section 165 however makes provision for wide legal standing to force the company to take action, for example when a duty of care in relation to cybersecurity was not exercised properly, or to take action to protect the company's interests, for example when a company's online platform and its online databases need to be properly protected.[1685]

This is one of the ways in which a shareholder, or someone listed in section 165(2), can try to protect the company's interests against a potential cyberattack, when directors refuse to do so.[1686] It also means that if a director breached their duty of care in relation to cybersecurity and a cyberatatck occurred, and the company refuses to hold the directors liable for such a cyberbreach, then a shareholder/stakeholder may, subject to compliance with the Act's requirements, institute a derivative action on behalf of a company.[1687] If it succeeds, any relief obtained will go to the company, which may indirectly benefit its shareholders/stakeholders. This effectively allows shareholders/stakeholders to institute an action against the board before a cyberbreach whenever directors do not exercise due care in relation to cybersecurity.[1688] An action could also be instituted after a cyberbreach if directors were negligent and did not exercise due care in relation to cybersecurity with the required oversight.[1689]

This action requires shareholders/stakeholders to serve a demand on a company.[1690] In 2011, Ndlovu, J of the Kwazulu-Natal High Court held in *Mouritzen v Greystone Enterprises (Pty) Ltd and Another* that any way which is a legally recognised way to institute a legal process will constitute a proper way of serving a demand.[1691]

Section 165(4) explains that if the company does not challenge the demand, or if the court does not set it aside, the company must (a) appoint an independent person or committee to investigate it.[1692] Section 65(4)(b) states that the company must within 60 days after it was served, either adhere to the demand, continue with the investigation, or initiate legal proceedings, or serve a notice on the person who made the demand.[1693]

In terms of section 165(5), the court will thereafter consider whether the person who served the demand may be granted a right to institute or continue with legal proceedings.[1694]

[1684] The Act, section 165.
[1685] *Ibid.*
[1686] The Act, section 165(2); Subramanien ''Legal Standing' and 'the Demand' in the Companies Act 71 of 2008, section 165: A Comparative Discussion' in *Obite*r 43(2) (2022) 47.
[1687] Blackman *et al. op cit* 9-178; Hayath *et al. s.p*.
[1688] Blackman *et al. op cit* 9-178.
[1689] *Ibid*.
[1690] Subramanien *op cit* 49.
[1691] *Mouritzen v Greystone Enterprises (Pty) Ltd and Another* (10442/2011) (2012).
[1692] The Act, section 165(5); *Caxton and CTP Publishers and Printers Ltd v Novus Holdings Lid* (Case no. 219/2021) [2022] ZASCA 24 (09 March 2022).
[1693] The Act, section 65(4)(b).
[1694] The Act, section 65(5).

4.2.6. Section 218(2): Claim for Damages

In addition, a director may also be held liable for a civil action in terms of the Act.[1695] In this regard, section 218(2) determines that anyone who contravenes any section of the Act is liable to any other person for any damage which that person suffered as a result.[1696]

Since this provision uses the words, "liable . . . to any other person for any loss or damage suffered by that person," its ambit is wide enough to also allow stakeholders to take action against directors in the event of a cyberbreach.[1697]

In this regard, the basis of the claim is a loss that class members suffered that differs from the loss which the company suffered.[1698] This differs from section 20(6), which does not give shareholders the opportunity to claim for such losses.[1699]

The courts have explained in *De Bruyn supra* and *Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*, that the wording of section 218(2) can be interpreted widely in terms of the individuals who fall within its ambit.[1700] Its application is however restricted as it only applies to damage that such a person suffered due to such a contravention.[1701] If the contravention caused a loss to the company, section 218(1) does not give shareholders the right to claim damages for their personal reflective loss that results from a drop in the value of their shares.[1702] The company can claim damages for its loss and the rationale is that the shareholders therefore indirectly benefit from those damages as a result of their shareholding.[1703]

Cassim *et al.* explains that section 218(2) may be contrasted with section 20(6) in different ways.[1704]

The first difference is that section 218(2) makes provision for a claim for damages against "any person" who contravenes any provision of the Act, and which may include the company itself.[1705] In 2014, Fourie, J, of the Western Cape Division of the High Court held in *Grancy Property Ltd v Gihwala* that the reference to "any person" in section 218(2) would, of course, include a director.[1706] Section 20(6) only makes

---

[1695] The Act, section 218(2).
[1696] The Act, section 218(2); Cassim *et al. Contemporary Company Law op cit* 1129.
[1697] The Act, sections 20(6); 218(3); Cassim *et al. Contemporary Company Law op cit* 875.
[1698] The Act, section 218(3); Cassim *et al. Contemporary Company Law op cit* 874 - 875.
[1699] The Act, sections 20(6); 218(3); Cassim *et al. Contemporary Company Law op cit* 875.
[1700] The Act, section 218(2); *De Bruyn supra*, paras 188 - 190; *Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*, paras 9; 31 – 32; 38 – 39; Cassim *et al. Contemporary Company Law op cit* 373.
[1701] *Ibid*.
[1702] *Ibid.*
[1703] *Ibid*.
[1704] The Act, sections 20(6); 218(2); Cassim *et al. Contemporary Company Law op cit* 1129.
[1705] The Act, section 218(2); Cassim *et al. Contemporary Company Law op cit* 1129.
[1706] The Act, section 218(2); *Grancy Property v Gihwala* 2014 JDR 1292 (WCC), par. 104.

provision for a claim against the person who fraudulently, or intentionally or due to gross negligence caused the company to contravene the Act; and does not allow such a claim to be instituted against the company itself.[1707]

A second difference is that section 218(2), depending on the circumstances of the particular provision which was contravened, may apply if the defendant contravened the Act intentionally, negligently or even innocently, and this caused damage to the plaintiff suffered.[1708] In other words, as long as a causal link can be established, the action may be instituted.[1709] Contrariwise, section 20(6) only requires proof of intention, fraud or gross negligence.[1710]

A third difference is that, while shareholders may have standing to claim damages under both section 20(6) and section 218(2), the latter additionally provides wider standing to "any other person" who has suffered "any loss or damage" as a result of the contravention.[1711]

In terms of the application of section 218(2), it was emphasised in 2013 by Du Plessis, AJ of the South Gauteng High Court in *Rabinowitz v Van Graan* that a director can only be liable in terms of section 218(2) for loss or damage that was caused by a contravention of the Act itself.[1712] Du Plessis, AJ, in *Rabinowitz supra*, as well Makgoba, JP of the Limpopo High Court held in 2018 in *Maake v Chemfit Fine Chemicals (Pty) Ltd*, that in terms of section 218(2), the plaintiff must be able to state the particular provision of the Act, which was contravened by the defendant, as well as the exact damage that this caused to the plaintiff.[1713] In 2016, Thulare, AJ, of the North Gauteng High Court stated in *Burco Civils CC v Stolz and Another* that in order to succeed with an action in terms of section 218(2), a plaintiff must not only show that a person contravened the Act, and that the plaintiff suffered damage, but the causal link between the contravention and the damage also needs to be shown.[1714] There must in other words be a causal link between the contravention and the damage, such as the improper exercise of the duty of care in relation to cybersecurity that led to a cyberbreach and that the cyberbreach caused damage to a stakeholder, for example

---

[1707] The Act, section 20(6); Cassim *et al. Contemporary Company Law op cit* 1129.
[1708] The Act, sections 20(6); 218(2); Cassim *et al. Contemporary Company Law op cit* 1130.
[1709] *Ibid*.
[1710] The Act, section 20(6); Cassim *et al. Contemporary Company Law op cit* 1130.
[1711] The Act, sections 20(6); 218(2); Cassim *et al. Contemporary Company Law op cit* 1130.
[1712] The Act, section 218(2); *Rabinowitz v Van Graan* 2013 (5) SA 315 (GSJ), par. 9; Cassim *et al. Contemporary Company Law op cit* 1130.
[1713] The Act, section 218(2); *Maake v Chemfit Fine Chemicals (Pty) Ltd* (5772/2016/HCAA04/2018) (2018) ZALMPPHC 71 (22 November 2018); *Rabinowitz supra*; Cassim *et al. Contemporary Company Law op cit* 1130.
[1714] The Act, section 218(2); *Burco Civils CC v Stolz and Another* (2017) JOL 39331 (GP), par. 47; Cassim *et al. Contemporary Company Law op cit* 1130.

cyberfraud that was commited in their name after the cybercriminal obtained their PII.[1715]

When it comes to way in which section 218(2) needs to be interpreted in terms of the common law, Unterhalter, J, was in disagreement in *De Bruyn supra* with the view that was held in *Hlumisa Investment Holdings (RF) Ltd (No.2) supra* that section 218(2) imports common law concepts of liability.[1716] Unterhalter, J said that although legislation must be interpreted in terms of the common law, section 218(2) leads to a legislative liability.[1717] He said that this does not replace the common law liability, except for the common law-claim for a breach of the legislative duty.[1718] Instead, the legislative liability exists besides the common law liability, and he said that the latter may be enforced by a delict for a breach of the duty of care.[1719]

Cassim *et al.* agrees with this view and then provides the following reasons:[1720] first, if an Act makes provision for a claim after a legislative duty was contravened, this will usually exclude a common law-claim for a breach of a legislative duty.[1721] Secondly, in instances where an Act directly imports common law principles in order to impose liability for contraventions of that Act, as is the case with section 77(2), it will clearly state this.[1722] Thirdly, the common law may still inform how the legislative liability needs to be interpreted, but this does not mean that the legislative liability is similar to the common law liability or that the legislative liability has imported the common law liability, unless an Act specifically states that this is the case.[1723]

4.2.6.1. The 'No Reflective Loss' Principle

The 'no reflective loss' principle needs to be briefly touched on, since it comes into the picture whenever personal claims of shareholders and derivative actions or other corporate actions are instituted simultaneously.[1724] This principle is equally applicable to both section 218(2) and section 20(6).[1725]

[1715] The Act, section 218(2); *Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*, par. 51; *Motor Industry Bargaining Council v Botha* (34198/2013) 2016 ZAGPPHC 615 (10 June 2016), par. 61; Cassim *et al. Contemporary Company Law op cit* 1130.

[1716] The Act, section 218(2); *De Bruyn supra*; *Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*; Cassim *et al. Contemporary Company Law op cit* 871.

[1717] *Ibid*.

[1718] *Ibid*.

[1719] *Ibid*.

[1720] Cassim *et al. Contemporary Company Law op cit* 871.

[1721] *Ibid*.

[1722] *Ibid*.

[1723] *Ibid*.

[1724] Cassim *et al. The New Derivative Action under the Companies Act: Guidelines for Judicial Discretion* 85 – 88.

[1725] The Act, sections 20(6); 218(2); *De Bruyn supra; Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*; Cassim *et al. Contemporary Company Law op cit* 1133.

It comes into the picture when the company as well as the shareholders have a claim against the directors (or others), which are based on a similar set of facts, as may happen after a cyberbreach occurred.[1726] Consequently, the shareholder's loss, (when this is for example a reduction in their shares' value after a cyberbreach or a loss of dividends, since the money had to be used to instead implement mitigation measures after a cyberbreach), simply reflects the loss that the company also experienced.[1727]

In such instances, it was held in the UK in 2000 by Lord Bingham of the House of Lords in *Johnson v Gore Wood & Co* and also in 2020 by Lord Reed of the UK Supreme Court in *Sevilleja v Marex Financial Ltd*, as well as in SA in 2016 by Ponnan, JA in *Itzikowitz v ABSA Bank Ltd* and in 2016 by Maya ADP in *Off-Beat Holiday Club v Sanbonani Holiday Spa Shareblock Ltd*, that the shareholders cannot claim for a loss that the company also experienced.[1728]

This rule was also applied in 1982 in *Prudential Assurance Co Ltd v Newman Industries Ltd (No. 2)*, when Cumming-Bruce, LJJ of the UK Court of Appeal held that shareholders' personal claim for a loss in the value of their shares cannot be allowed, even in an instance where the loss was caused by a misleading circular, which the directors issued to seek the shareholders consent for a transcation where assets were bought for far more than their real value.[1729] He held that even in such an instance, the company experienced the same loss as the shareholders.[1730]

In 1983, Lawton, LJ of the UK Court of Appeal explained in *Heron International Ltd v Lord Grade* that this rule will not prevent an action when the losses that the shareholder and the company experienced arose from a different set of facts.[1731]

In 1995, Lord Hoffman of the House of Lords held in *Stein v Blake (No. 2)* that when a company suffers a loss due to the misuse of its assets, the shareholders also cannot claim for a loss in their shares' value, since that loss may only be recovered by the company, and not by a shareholder who does not have a separate loss, other than the same loss that the company also experienced.[1732]

This principle stops double-recovery, should the company also decide to take action.[1733] At the same time, it also prevents a shareholder from recovering their loss to the disadvantage of the company, the other shareholders as well as the creditors.[1734]

[1726] Cassim *et al. Contemporary Company Law op cit* 1133.
[1727] *Ibid*.
[1728] *Johnson v Gore Wood & Co* (2002) 2 AC 1 (HL) 62; *Sevilleja v Marex Financial Ltd* (2020) UKSC 31*; Itzikowitz v ABSA Bank Ltd* 2016 (4) SA 432 (SCA); *Off-Beat Holiday Club v Sanbonani Holiday Spa Shareblock Ltd* 2016 (6) SA 181 (SCA); Cassim *et al. Contemporary Company Law op cit* 1133.
[1729] *Prudential Assurance Co Ltd v Newman Industries Ltd (No.2)* (1981) Ch 257; 1982 (1) Ch 204 (CA); Cassim *et al. Contemporary Company Law op cit* 1134.
[1730] *Ibid*.
[1731] *Heron Interational Ltd v Lord Grade* (1983) BCLC 261; Cassim *et al. Contemporary Company Law op cit* 1133.
[1732] *Stein v Blake (No. 2)* (1998) 1 AII ER 724 (CA); Cassim *et al. Contemporary Company Law op cit* 1134.
[1733] Cassim *et al. Contemporary Company Law op cit* 1134.
[1734] *Ibid*.

In 2002, Tuckey, LJ of the England and Wales Court of Appeal (Civil Division) explained in *Day v Cook* that when a shareholder and the company both have a claim due to a loss that was caused by a breach of a duty of care that was owed to both of them, and this loss was caused by the same set of facts, this principle also prevents the shareholder from recovering their loss even if the company decides not to use this remedy, or even if the company accepts less for the damage than what it could get.[1735]

There is however an exception to this principle, and this is whenever it happens that the company is not allowed to pursue its claim due to a defendant's wrongful act.[1736] In 2004, Rimer, J, of the England and Wales Chancery Division explained in *Perry v Day* that in these circumstances, as long as a shareholder has a separate loss, such a shareholder should be able to take action.[1737]

4.4. SA POPI 4 of 2013

The SA POPI 4 of 2013 came into force on 1 July 2021 and, section 22(1) determines that any cyberbreach must be notified to the IR as well as affected parties, such as shareholders and stakeholders – so gone are the days that cyberbreaches could just be swept under the carpet.[1738]

In terms of this Act, section 40, the IR is mandated (d) to process complaints and (i) to investigate complaints on violations of the privacy of personal information; (ii) to gather information in order to investigate such violations; (iii) to try and resolve complaints through alternative dispute resolution (ADR) mechanisms; and (iv) to serve any notices in terms of this Act.[1739]

Chapter 11 of this Act allows affected parties to keep the directors liable for the loss of the privacy of their personal information.[1740] Section 107(1) determines that in certain instances, the penalty can be a fine or a period of imprisonment that does not exceed ten years.[1741] Section 108 says that matters may be refered to court and that penalties can be issued by a magistrate's court.[1742] Section 109 again says that the IR may impose a fine, and that the amount can be determined at the IR's discretion depending on the facts and seriousness of the matter.[1743]

4.4. The SA Criminal Procedure Act 51 of 1977

[1735] *Day v Cook* (2002) BCLC 1 CA; Cassim *et al. Contemporary Company Law op cit* 1134.
[1736] *Perry v Day* (2005) BCLC 405; Cassim *et al. Contemporary Company Law op cit* 1134.
[1737] *Ibid.*
[1738] SA POPI 4 of 2013, section 22(1).
[1739] SA POPI 4 of 2013, section 40(d)(i)-(iii).
[1740] SA POPI 4 of 2013, Chapter 11.
[1741] SA POPI 4 of 2013, section 107(1).
[1742] SA POPI 4 of 2013, sections 108.
[1743] SA POPI 4 of 2013, sections 109.

In terms of the SA Criminal Procedure Act 51 of 1977, section 332(1), criminal proceedings may also be taken against a company or its directors.[1744] Both may be prosecuted for any common law offence.[1745] This section makes provision for all types of criminal activities by companies, and includes those that require negligence, and it also includes the acts or inactions of a director.[1746] Such an act or inaction is then considered to have been committed by the company and intent does not need to be shown.[1747]

4.5. Common Law

Directors are also exposed to the common law duty of care, as well as a common law personal action.

4.5.1. Common Law Duty of Care

Although the Act partially codified directors' duty of care, the common law duty of care still applies.[1748] Before the Act was promulgated, directors' duties were regulated by the common law.[1749] The common law requires directors to exercise their duties in good faith and in their companies' best interests, together with the need to exercise care, skill and diligence in the way in which they exercise their oversight to all aspects in the performance of their functions.[1750] If they do not exercise their common law duties reasonably, it will expose them to personal liability for redress.[1751]

When a board fails to implement and oversee a proper cybersecurity policy and system, it could amount to a breach of their common law duties.[1752] The directors' fiduciary duty originated in the common law, and became part of the Act, section 76(3)(b) as the duty to look after a company's best interests.[1753] The directors' duty of care also originated in the common law and is now codified in the Act, section 76(3)(c), which requires them to act with the degree of care, skill and diligence that may

---

[1744] SA Criminal Procedure Act 51 of 1977, section 332(1).
[1745] Farisani 'The Regulation of Corporate Criminal Liability in SA: A Close Look' in *Obiter* (January 2006) 264.
[1746] *Ibid.*
[1747] *Ibid.*
[1748] Blackman *et al. op cit* 8-29; Faris *et al. The Law of SA* (LAWSA) (Companies) 4(2), par. 116; Delport *et al. Henochsberg on the Companies op cit* 288.
[1749] *Ibid.*
[1750] Werksmans *op cit* 3.
[1751] *Ibid.*
[1752] Flockhart *et al.* '*Cyber Risk and Directors' Liabilities: An International Perspective*,' *s.p.*, available online at <https://www.nortonrosefulbright.com/en/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective#section8>, last accessed on 27 April 2022.
[1753] The Act, section 76(3)(b); Naidoo *op cit* 203.

reasonably be expected from (i) someone in a similar position; and who (ii) has similar experience and skills.[1754]

Directors can consequently be held personally liable to the company as well as third parties once their common law duty of care in relation to cybersecurity is breached.[1755]

A breach of the directors' common law duty of care could lead to claims against directors in contract or tort.[1756] This is because the Act, section 128(2) determines that anyone who contravenes any section of the Act is liable to anyone else who have experienced a loss or damage as a consequence.[1757]

4.5.2. Common Law Personal Action

When a shareholder experienced a loss and they want to exercise their individual shareholder rights, they can institute a common law personal action in their own name.[1758] The Act preserves the personal action.[1759]

This means that shareholders/stakeholders can hold directors personally liable if they did not properly exercise their duty of care in relation to cybersecurity. The shareholders/stakeholders who were affected by a cyberbreach can hold the board accountable on the basis that they failed to address weaknesses in the company's cybersecurity policy and system and that this, for example resulted in their financial loss that was caused after a cybercriminal managed to obtain their PII and were able to commit fraud in their name.[1760] In such a way, shareholders/stakeholders can sue directors after a cyberattack for the recovery costs to retrieve their personal information as well as reputational damage that was inflicted on them due to a loss of their privacy, since the directors did not exercise their duty of care in relation to cybersecurity properly.[1761]

Section 77(2)(b) states that a director's liability for the breach of their common law duty of care is delictual in nature.[1762] In this regard, the most applicable form of delict will be the *Actio Legis Aquiliae*, since it be used to recover damages for the wrongful and culpable (irrespective of whether it was caused intentionally or negligently) causation of patrimonial loss.[1763] It was explained that five elements will need to be

---

[1754] The Act, section 76(3)(c)(i)-(ii).
[1755] Flockhart *et al. op cit s.p.*
[1756] *Ibid.*
[1757] The Act, section 128(2).
[1758] Cassim *et al. Contemporary Company Law op cit* 1131.
[1759] *Ibid*.
[1760] FIA *op cit s.p*.
[1761] *Ibid*.
[1762] The Act, section 77(2)(b).
[1763] *Du Plessis NO supra*; See Chapter 3, section 2.1.

proven in this regard, namely conduct, wrongfulness, fault, loss and causation.[1764] It was also explained earlier that it was held in *Du Plessis NO supra* that the liability of a director for a breach of their common law duty of care is delictual in nature.[1765]

Section 165 did not replace the common law personal action.[1766] Section 165(1) explains that any common law right of a person, besides a company, to institute any actions on behalf of it is replaced, and that section 165 replaces such a right.[1767] This provision consequently replaced the common law derivative action, which allowed a shareholder to institute an action on behalf of a company, but still allows a shareholder's common law right to institute an action in their own name to defend their own shareholder rights by means of a personal action.[1768]

It was confirmed in 2012 by Swain, AJA, of the SA SCA in *Communicare and Others v Kahn and Another* that section 165 does not replace the personal action, and that the common law personal action and the legislative derivative action both exist seperately.[1769] This case was about the difference between these two actions, or the difference between corporate rights and personal shareholder rights.[1770] In this regard, Swain, AJA explained that where damage was caused to the company, the company itself should take action.[1771] In contrast, a shareholder has a personal action against the company when the company harmed the shareholder.[1772]

With the new Act, common law personal action is now of lesser importance.[1773] This is due to the inclusion of section 20(4), which gives a legislative right to shareholders to prevent the company from contravening the Act; and section 20(5), which gives a legislative right to prevent the directors from *ultra vires* actions.[1774] In addition, section 218(2) allows a legislative right to damages for contraventions of the Act that caused damage to a shareholder (or someone else).[1775]

4.6. Contract

Whenever a company concluded a contract with a director, and that contract contains a provision that requires that director to exercise a certain standard of care in

---

[1764] *Du Plessis NO supra*; See Chapter 3, section 2.1.
[1765] *Ibid*.
[1766] The Act, section 165; Cassim *et al. Contemporary Company Law op cit* 1131.
[1767] *Ibid*.
[1768] *Ibid*.
[1769] The Act, section 165; *Communicare and Others v Kahn and Another* 2013 (4) SA 482 (SCA); Cassim *et al. Contemporary Company Law op cit* 1131 - 1132.
[1770] *Communicare and Others supra*.
[1771] *Ibid*.
[1772] *Ibid*.
[1773] Cassim *et al. Contemporary Company Law op cit* 1132.
[1774] The Act, sections 20(4); 20(5).
[1775] The Act, section 218(2).

relation to cybersecurity, the breach of such a duty will be contractual in nature.[1776] The company will then be able to claim damages either due the intentional or negligent way in which the director exercised their duty of care in relation to cybersecurity.[1777]

4.7. *Concursus Actionem*

In some instances the damage that a director caused a company, may constitute a breach of both a fiduciary duty as well as a duty of care, skill, and diligence.[1778]

SA law allows the same set of facts to be used for a delictual claim as well as a contractual claim and the plaintiff may decide which one of the two they will use.[1779] This is called a *concursus actionum* and is only present when the separate requirements of both a contractual action as well as a delictual action have been fulfilled.[1780] In 2014, Van Der Westhuizen, J of the SA CC upheld in *Loureiro v iMvula Quality Protection (Pty) Ltd* both a contractual claim and a delictual claim that a defendant had acted both negligently and wrongfully.[1781]

4.8. Regulatory Action

Liability in terms of the duty of care in relation to cybersecurity and the use of AI may also derive from corporate governance guidance, stock exchange listing requirements, and industry regulators.[1782] Where such guidance or regulations may not always have the force of law, the courts may use them to help determine the standard of reasonable care, skill and diligence that are required of directors when they exercise their duty of care in relation to cybersecurity.[1783]

4.8.1. King Reports on Corporate Governance

Voluntary corporate governance guidelines, such as King Report IV, only recommend best practices on corporate governance, but they do influence and affect what practices boards should look at and implement.[1784] In this regard, King Report IV explains that if the recommendations on good corporate governance are more regularly used by directors in practice, it will enhance the possibility that a court will consider such

---

[1776] Cassim *et al. Contemporary Company Law op cit* 1132.
[1777] Ca*lbid*.
[1778] The Act, section 77(3)(a)-(e).
[1779] Mabunda *op cit* 75; Mupangavanhu op cit 192; Price 'The Contract/Delict Interface in the Constitutional Court' in *Stellenbosch Law Review* 25(2014) 501.
[1780] *Ibid.*
[1781] *Loureiro v iMvula Quality Protection (Pty) Ltd* 2014 3 SA 394.
[1782] See Chapter 1, section 6.2.
[1783] *Ibid.*
[1784] IoDSA '*King Report IV' op cit* 35.

recommendations to set a standard on the nature of care that is required on a certain aspect pertaining to corporate governance.[1785] Consequently, the recommendations of voluntary corporate governance guidelines could be used in case law and could in such a way become part of the common law over time.[1786] As a result, directors could then be held liable when they do not comply with an established corporate governance practice, even if such practice is not codified.[1787]

Especially noteworthy is the King Report IV, which requires the board to govern risk so that it supports the company to achieve its objectives; and principle 12 requires the board to ensure that IT risks are integrated into the risk management of the entire company.[1788] Directors need to exercise their duty of care in relation to cybersecurity properly and oversee good corporate governance practices when they want to protect themselves and rely on the protection of the BJR in the Act, section 76(4), during litigation in the aftermath of a cyberbreach.[1789] If directors did not exercise due care in relation to cybersecurity by means of the implementation and oversight on a proper cybersecurity policy and system, it will be very difficult for such a director to use the BJR and to prove in terms of section 76(4) that (a)(i) they took reasonable steps to become informed; and (iii) that they had a real reason to believe that the decision was made in the company's best interests.[1790]

4.8.2. Stock Exchange Listing Requirements

In addition, the JSE '*Listing Requirements*' ensures the further enforcement of good corporate governance practices.[1791]

The JSE '*Listing Requirements*' is a list of all the rules and procedures that any listed company will, in terms of its section 1.28, have to comply with when they want to be listed on the JSE and have their shares traded publicly.[1792] In terms of these Requirements, section 3.84, any listed company will also have to conform with King Reports I - IV if they want to be listed on the JSE, and trade their shares there.[1793]

4.8.3. SA Companies and Intellectual Property Commission (CIPC)

[1785] IoDSA '*King Report IV*' *op cit* 35.
[1786] *Ibid.*
[1787] *Ibid.*
[1788] IoDSA '*King Report IV*' *op cit* principles 10; 12.
[1789] The Act, section 76(4); IoDSA '*King Report IV*' *op cit* 35.
[1790] The Act, section 76(4)(a)(i)-(iii); IoDSA '*King Report IV*' *op cit* 35; Naidoo *op cit* 212.
[1791] JSE '*Listing Requirements*,' *s.p.*, available online at <https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/JSE%20Listings%20Requirements.pdf>, last accessed on 21 May 2019.
[1792] JSE '*Listing Requirements*,' section 1.28.
[1793] JSE '*Listing Requirements*,' section 3.84.

Although it depends on the regulatory framework and industry of an affected company, interested and affected parties can lay complaints at the SA CIPC who will then investigate them and take action against a company or its directors.[1794]

5. LESSONS ON HOW DIRECTORS' USE OF AI SHOULD BE REGULATED IN THE SA CYBERCRIMES ACT 19 OF 2020 AND THE KING CODE

It was explained that the CoE's 'Convention on Cybercrime' was the world's first multilateral treaty on the prevention of cybercrime, and that it came into effect on 1 July 2004.[1795] This Convention is currently the only binding multilateral treaty that regulates and combats cybercrime.[1796] It was explained that although SA adopted it, it has not yet ratified it.[1797] This is still a shortcoming in the SA cybersecurity regime, because SA is consequently still not obliged to comply with this Convention's provisions.[1798]

It was also explained that the SA Cybercrimes Act 19 of 2020 was promulgated and came into effect on 1 December 2021.[1799] A shortcoming is that neither the SA ECTA 25 of 2002, the SA RICA 70 of 2002, the SA POPI 4 of 2013, nor the SA Cybercrimes Act 19 of 2020 provides a definition for the term, 'cybercrime'.[1800]

Amongst other things, the SA Cybercrimes Act 19 of 2020 aims to protect all persons, including companies, from cybercriminals who use online means to commit cybercrimes.[1801] Sections 2 to 12 list various cybercrimes and activities that it prohibits.[1802] Sections 19(1) – (2) states that anyone who commits any of its listed offences will be liable for a fine and/or imprisonment between five and ten years.[1803] In this regard, section 19(3) explains that aggravated offences could lead to fines and/or imprisonment for up to 15 years.[1804] Since the amount of the fine is not stated, the court may decide on the amount of the fine in terms of the SA Criminal Procedure Act 51 of 1977, section 276.[1805] This does not send a clear message to cybercriminals of the

---

[1794] SA CIPC *op cit s.p*.
[1795] Council of Europe (CoE) '*Convention on Cybercrime of 2001*' (ETS 185), *s.p.*
[1796] *Ibid.*
[1797] *Ibid.*
[1798] *Ibid.*
[1799] SA Cybercrimes Act 19 of 2020.
[1800] SA ECTA 25 of 2002; SA RICA 70 of 2002; SA POPI 4 of 2013; SA Cybercrimes Act 19 of 2020.
[1801] SA Cybercrimes Act 19 of 2020, Preamble.
[1802] SA Cybercrimes Act 19 of 2020, sections 2 - 12.
[1803] SA Cybercrimes Act 19 of 2020, sections 19(1) – (2).
[1804] SA Cybercrimes Act 19 of 2020, section 19(3).
[1805] SA Criminal Procedure Act 51 of 1977, section 276.

liability that they could incur when they commit a cybercrime.[1806] This Act also does not make provision for administrative sanctions, nor civil sanctions.[1807]

Section 52 establishes the SA Cybercrime PoC in an attempt to help combat cybercrime.[1808] Section 54(1)(a) obliges persons and companies to report a cybercrime and; (b) to preserve any evidence that could be used to investigate a cybercrime.[1809] Directors need to remember that any company who does not report a cybercrime, and who does not preserve any evidence related to a cybercrime act, will be liable for criminal penalties.[1810]

It was also said that it is a shortcoming that this Act does not especially prohibit the use of AI to commit cybercrimes, and also that it does not make provision for the responsible use of AI to fight cybercrime towards SA companies.[1811]

There are six ways in which SA directors can use AI and Blockchain technology to enhance the cyberresilience of their companies' OMs, but not all of them fulfil the requirements that the Act stipulate for the way in which directors need to exercise their duty of care. It is as a result important to pay careful attention to the advantages and disadvantages of each of these types of AI in order to determine what is permissible in terms of the Act and what not.

The first way in which directors can use AI to improve their company's cyberresilience is through Consultative AI.[1812] Consultative AI also uses algorithms to assist natural intelligence without substituting the director.[1813] As a result, the use of this type of AI would not release a director from their duty of care.[1814] It can assist directors with reaching decisions that require creative thinking, and it can ask questions that relate to various scenarios and then provide answers on those questions based on those and other scenarios.[1815] It can as a result help to increase the quality of the decisions that directors need to make on cybersecurity matters. It can assist directors by drawing insights and answers from patterns of data that would otherwise be hard for directors to determine.[1816] It can also help them to identify and examine intricate cybersecurity problems and then make recommendations on the best solutions.

[1806] Chitimira *op cit* 8.
[1807] SA Cybercrimes Act 19 of 2020, section 19.
[1808] SA Cybercrimes Act 19 of 2020, section 52.
[1809] SA Cybercrimes Act 19 of 2020, section 54(1)(a) – (b).
[1810] SA Cybercrimes Act 19 of 2020, section 54(1)(a) – (b).
[1811] SA Cybercrimes Act 19 of 2020.
[1812] Chitimira *et al.* 'The Integration and Reliance on Technology to Enhance the Independence and Accountability of Company Directors in SA' in *Potchefstroomse Elektroniese Regsblad* 24 (2021) 6 – 7; Hassani *et al.* 'Artificial Intelligence (AI) or Intelligence Augmentation (IA): What is the Future?' in *AI* 1(2) (2020) 147.
[1813] Chitimira *et al. op cit* 5 – 6; Petrin 'Corporate Management in the Age of AI' in *Columbia Business Law Review* (2020) 982 - 984.
[1814] *Ibid*.
[1815] *Ibid*.
[1816] *Ibid*.

The King Code should allow SA directors to use Consultative AI when they use algorithms to exercise their duty of care in relation to cybersecurity.[1817] The function of the algorithm that Consultative AI uses will help to give effect to the Act, section 7(b), which states that the Act aims to (i) promote the development of the SA economy by encouraging high standards of corporate governance; and to (ii) balance the rights and obligations of directors and shareholders.[1818] The use of Consultative AI could therefore help to balance the rights and obligations of directors and shareholders and help to minimise bias, since the algorithm can be programmed to objectively evaluate a certain scenario, and it wil then as a result not be susceptible to the subjective influence of a director in the recommendation that it provides.[1819] The use of Consultative AI is permissible, since it only provides recommendations, which are then subject to the directors' approval.[1820] Its use still allows directors to add their own insights to that recommendation, and to then maybe make another conclusion.[1821] Directors can also use it to make better-informed decisions that will help to bring a company more in line with the requirements of the Act and the King Code and in doing so, help to protect stakeholders' interests.[1822] Since the Act prescribes the enlightened shareholder value approach, Consultative AI can be programmed to take various stakeholders' interests into account and to prevent bias.[1823]

The second one is Supportive AI, where the algorithm helps to perform certain tasks, but does not substitute the director.[1824] The algorithm can do administrative tasks such as call an OM in terms of section 61(1); and deliver a notice of an OM in terms of section 62(1).[1825] Since it can also be used to determine whether the minutes of OMs are properly recorded, it could help to save time.[1826] Directors could however also use it to set up OMs, to compile reports for OMs or to give directors informed opinions on the cybersecurity aspects related to OMs.[1827]

A third possibility exists in the form of Self-Aware AI.[1828] The problem with this is however that its algorithm takes on human functions and then basically substitutes a

---

[1817] Can Kaya '*The Role of AI in Corporate Governance*,' paper delivered at the Istanbul Medeniyet University on 22 June 2022, 7 – 8, available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4143846>, last accessed on 14 January 2022.
[1818] The Act, sections 7(b)(i)-(ii).
[1819] Chitimira *et al. op cit* 5 – 6.
[1820] *Ibid.*
[1821] *Ibid.*
[1822] The Act, sections (7(a); (d); (i); IoDSA '*King Report IV*' *op cit* principle 8.3; Petrin *op cit* 970.
[1823] Can Kaya *op cit* 5 – 6; Delport *et al.* 'The Protection of Stakeholders: The SA Social and Ethics Committee and the UK's Enlightened Shareholder Approach, Part 1' *op cit* 97.
[1824] Chitimira *et al. op cit* 5 – 6; Petrin 'Corporate Management in the Age of AI' in *Columbia Business Law Review* (2020) 980.
[1825] The Act, sections 61(1); 62(1).
[1826] The Act, section 88(2).
[1827] The Act, section 76(4)(a).
[1828] Can Kaya *op cit* 7 – 8; Chitimira *et al. op cit* 7 - 8.

director with AI.[1829] It would however not be possible to use this type of AI to assume the role of a director or to replace them, since the Act, section 69(7) only allows natural persons to be directors.[1830] The King Code should thus explain that the use of Self-Aware AI is not permissible if it is used to substitute directors. Another reason why Self-Aware AI could not be used to take over the decision-making function of directors, is because the substitution of human directors with AI would lead to legal uncertainty whenever liability needs to be determined in events where the duty of care was not properly exercised.[1831] The court will be confronted with many questions when they need to determine the liability of AI, such as whether they should be held liable in terms of contract or delict? This would be difficult to answer, because in such instances, board decisions would not be made by independent, free-thinking directors, but by algorithms.[1832] In order to then determine whether the duty of care in relation to cybersecurity was performed properly, the court would then have to determine whether the directors' decision was in fact made by the designer of the algorithm, the programme developer, the machine itself or the supplier.[1833] The legislature will also have to determine what types of AI directors may use, before they are held liable for not exercising their duty of care properly.[1834] Should Self-Aware AI ever replace directors, it would undermine the diversity of the board, since human characteristics, which contribute to diversity, such as gender and race, would then be circumvented, and this would adversely affect the quality of the board's decisions.[1835]

The fourth way in which directors can integrate AI to improve their company's cyberresilience is through Data Analysis.[1836] Big Data is volumes of data which are too large to be processed by traditional methods.[1837] Data Analysis is a type of AI that quickly analyses and processes large volumes of data and helps to facilitate decisions that needs to be made quickly.[1838] It would especially be helpful to assist directors when they need to make decisions that pertain to cybersecurity-related matters, since it is able to analyse cybersecurity reports and look for weak spots in the cybersecurity system, but it can also be used at all other levels of a company to analyse logistical information.[1839] It could also help directors with real-time recommendations that can

---

[1829] Can Kaya *op cit* 7 – 8; Chitimira *et al. op cit* 7 - 8.
[1830] The Act, section 69(7); Chitimira *et al. op cit* 7 - 8.
[1831] Can Kaya *et al. op cit* 7 – 8; Chitimira *et al. op cit* 7 - 8.
[1832] *Ibid*.
[1833] *Ibid.*
[1834] *Ibid*.
[1835] *Ibid*.
[1836] Boura *et al.* 'Big Data Analytics and Firm Performance: Findings from a Mixed-Method Approach' in *Journal of Business Research* 98 (2019) 261 - 264; Chitimira *et al. op cit* 9 - 11.
[1837] *Ibid.*
[1838] *Ibid*.
[1839] *Ibid*.

help to improve the quality of their decisions.[1840] If the Act's provision on the written format in which company records should be kept is read liberally, section 24(1) will allow it to be used to facilitate the online storage of such records.[1841] Since cyberattacks will require directors to analyse lots of data in real-time, Consultative AI and Data Analysis could help them to make informed decisions.[1842] Studying numerous cyberreports in the aftermath of a cyberattack in an attempt to try and understand what is important and what is not, may overwhelm directors, and this may cause them to not make an informed decision.[1843]

Due to information-overload, directors may find it difficult to gain proper insights into all the relevant business reports and corporate governance principles when they need to make a business decision, usually within a specific time.[1844] In this regard, directors could fifthly use Critically Conscious Computing (CCC).[1845] CCC is already used by some companies for cybersecurity evaluations and advice.[1846] CCC is adaptable and a person can ordinarily communicate with it by speaking to it.[1847] A director can ask it any question in a certain field and get an instantaneous reply.[1848] It can also access agendas and minutes of any previous OM and answer questions related to it.[1849] Since CCC can comprehend spoken words, directors can interact with the algorithms, and this can help directors to make better-informed business decisions.[1850] CCC can also sort lots of data and it can learn itself new tasks related to the management thereof.[1851] It can also start its own database and create hypotheses in order to provide answers for questions which it is asked.[1852] When it is presented with new information, it sorts, manages and stores it, and could allow some information, such as cybersecurity reports to remain confidential.[1853] It is anticipated that easy access to company reports and industry reports in real-time, by means of Consultative AI, will help directors to exercise their duty of care in relation to cybersecurity more efficiently.[1854] As a cognitive system, CCC is able to understand highly-technical terms

---

[1840] Boura *et al. op cit* 261 - 264; Chitimira *et al. op cit* 9 - 11.
[1841] The Act, section 24(1).
[1842] Chitimira *et al. op cit* 9 - 11.
[1843] *Ibid.*
[1844] Bowles *et al. Cognitive Computing and Big Data Analytics* 2; Chitimira *et al. op cit* 20.
[1845] *Ibid.*
[1846] *Ibid.*
[1847] Bowles et al. op cit 4; Gudivada 'Cognitive Computing Systems: Their Potential and the Future' in *Computer* 52(5) 2019 6.
[1848] Bowles et al. op cit 6.
[1849] *Ibid.*
[1850] Hamm *et al. Smart Machines: IBM's Watson and the Era of Cognitive Computing* 43.
[1851] Noor 'Potential of Cognitive Computing and Cognitive Systems' in *Open Engineering* 5(1) (2015) 76 - 77.
[1852] *Ibid.*
[1853] Hamm *et al. op cit* 44 – 45; Noor *et al.* 76.
[1854] Hamm *et al. op cit* 44 – 45.

and industry jargon and is able to predict scenarios and to provide instant unbiased answers.[1855]

Sixthly, it was explained that although the public ledger system is an essential characteristic of Blockchain technology, Private Blockchain could be used (as in the case of Strate) to encrypt all personal information on the public ledgers.[1856] An individual relevant shareholder or stakeholder could then get limited access to their own PII, and all their sensitive information would stay private.[1857] It was explained that the King Code will have to provide guidance to directors on how to use Blockchain technology and require directors to ensure that there is limited access to the ledgers, that personal information is encrypted and that only individual relevant shareholders/stakeholders can access their own personal information.[1858]

As soon as directors will start to especially use Consultative AI and Data Analysis they will already start to switch the scales and start to gain the upper hand over the AI that cybercriminals use to instigate their cyberattacks.[1859] The volume of cybersecurity reports that a company's cybersecurity system produce cannot be analysed manually by directors, and such reports will in most cases be too large for ordinary databases.[1860] Data Analysis could be used to try and look for patterns and trends in the type and frequency of cyberattacks and from where such attacks originate, and it will help to determine how resilient the company's cybersecurity system is to thwart such attacks.[1861] The use of Data Analysis will also help to increase the return on assets of the company's cybersecurity system and will help with its optimum asset utilisation.[1862]

AI can however also be subject to bias, which is usually caused by either one or two factors: firstly, when the designer of the algorithm, or the programme developer programmes their own preferences into an algorithm it can lead to design bias.[1863] This is problematic, since it could lead to misleading recommendations.[1864] Directors will not exercise due care if they rely on AI recommendations that are biased.[1865] Another problem is that the designer of the algorithm or the programme developer may

---

[1855] Noor *et al.* 77.
[1856] Anwar *op cit s.p.*; Geroni *op cit s.p*.
[1857] Anwar *op cit s.p.*
[1858] *Ibid.*
[1859] Shabbir *et al.* 'Application of Big Data Analytics and Organisational Performance: The Mediating Role of Knowledgement Management Practices' in *Journal of Big Data* 7(47) 2020 2 – 3.
[1860] *Ibid.*
[1861] Shabbir *et al. op cit* 2 – 3.
[1862] *Ibid.*
[1863] Berendt *et al.* 'Bias in Data-Driven AI Systems: An Introductory Survey' in *Wires: Data Mining and Knowledge Discovery* of May/June 2020 10(3) 3; Chitimira *et al. op cit* 11 – 12; Weiss *et al.* 'Ethical Implications of Bias in Machine Learning,' in *Proceedings of the 51st Hawaii International Conference on System Sciences* (2018), 5366, available online at <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1649&context=hicss-51>, last accessed on 9 January 2023.
[1864] *Ibid.*
[1865] *Ibid.*

deliberately develop an algorithm that will work towards a certain pre-determined goal, which is not in line with the provisions of the SA Constitution of 1996, the Act or the King Code's recommendations.[1866] In this regard, the King Code should have a strict principle on the use of only objective algorithms that were sourced from industry leaders, and which does not contain design bias, because otherwise it would lead to misleading recommendations.

Secondly, when the system is fed biased information, it will provide biased results.[1867] Since the algorithm can only use the information with which it is provided, it is of utmost importance that it is fed with accurate data.[1868] In this regard, the King Code should have a strict principle on the accuracy of the data that is fed to the algorithm.

It is also important to look at how directors should exercise their duty of care in relation to cybersecurity and the use of AI in terms of the King Code's principles. King Report IV explains that the board must govern ethics to make sure that the ethical culture within a company is in line with the board's vision.[1869] This is done through the implementation of proper cybersecurity policies and systems.[1870] The board is therefore responsible to ensure that AI is used in an ethical manner and that the company's cybersecurity policy and system uses AI in an ethical manner, and that the use of AI aligns with the company's ethical culture, and that the algorithms do not suffer from design bias, and that the algorithms are not fed with inaccurate information.[1871]

King Report IV, principles 1 - 3 explains how directors should align cybersecurity advances with ethical principles: Principle 1 explains with reference to ethical leadership, that the board should set an ethical example.[1872] The board will thus have to determine the vision and provide leadership and guidance on how the company should use AI.[1873]

Principle 2 refers to organisational ethics, culture and values and explains that the board should oversee that the way in which they govern will help to nurture an ethical culture.[1874] The board will thus have to ensure that the company's codes of conduct and ethics regulate the responsible use of AI, including when to use it and when not to use AI.[1875]

[1866] Berendt *et al. op cit* 3; Chitimira *et al. op cit* 11 – 12; Weiss *et al. op cit* 5366.
[1867] Berendt *et al. op cit* 4.
[1868] *Ibid.*
[1869] IoDSA '*The Role of the Board in Organisational Ethics*,' *s.p.*, available online at <https://www.iodsa.co.za/news/607020/The-Role-of-the-Board-in-Artificial-Intelligence-Ethics.htm>, last accessed on 9 January 2023; Naidoo *op cit* 48.
[1870] IoDSA '*King Report IV*' *op cit* 44.
[1871] *Ibid*.
[1872] Du Plessis *et al. op cit* 292.
[1873] IoDSA '*King Report IV*' *op cit* principle 1, 43.
[1874] IoDSA '*King Report IV*' *op cit* principle 2, 44; Du Plessis *et al. op cit* 292; Naidoo *op cit* 48.
[1875] *Ibid.*

Principle 3 requires the board to practice governance that demonstrate the company's good corporate citizenship.[1876] It must ensure that AI complies with the SA Constitution of 1996 and the country's laws and standards as well as company policies and procedures, strategy, and the company's codes of conduct and ethics.[1877] The directors should thus also ensure that AI helps the company to improve the well-being of not only the physical environment and society in which the company finds itself, but also its online environment and online society in which it finds itself.[1878] This will ensure that data biases, privacy and racial discrimination, are addressed in all AI development stages and further provide buy-in from both shareholders and stakeholders.[1879]

Directors' use of AI to help make decisions will not be a quick solution to help improve cybersecurity, because of all of AI's ethical and moral issues.[1880] The ethical and moral issues are very complex and need to be addressed in the King Code while AI is still busy developing.[1881]

6. CONCLUSION

This Chapter looked at the various other accountability mechanisms that shareholders/stakeholder may use to hold directors accountable.

It began by giving an overview of the international privacy law and cybersecurity regimes and then looked at their shortcomings.

It then looked at the various other accountability mechanisms, besides the common law and legislative duties of care, which shareholders/stakeholder may use to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI.

Thereafter, it looked at lessons on how directors' use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code.

This Chapter showed that in an attempt to protect the company and themselves from liability, directors can take proactive steps by using Consultative AI, Supportive AI and Data Analysis in the way in which they exercise their duty of care in relation to cybersecurity, but that they should definitely not use Self-Aware AI when they need to exercise ther duty of care in relation to cybersecurity, as this would lead to 'AI directors' that will substitute the role of the director.

The next Chapter is the conclusion that will summarise the findings of this thesis.

[1876] IoDSA '*King Report IV' op cit* principle 3, 44; Du Plessis *et al. op cit* 292.
[1877] *Ibid.*
[1878] *Ibid.*
[1879] *Ibid.*
[1880] IoDSA '*The Role of the Board in Organisational Ethics' op cit s.p*.
[1881] *Ibid*.

CHAPTER 6:

CONCLUSION

1. INTRODUCTION

While the previous Chapter looked at directors' liability in terms of the use of AI, as well as lesons on the way in which AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code, this Chapter is the conclusion and will summarise the lessons for SA that was drawn from the various chapters on the role that a more detailed treatment of the directors' duty of care in relation to cybersecurity can play to improve companies' cyberresilience, with the specific focus of their OMs, and how the use of AI can facilitate this.

This Chapter will start by summarising the lessons from Chapter 2 for SA on the regulation of OMs in other jurisdictions in order to understand how to best protect the integrity of a SA OM, as well as the cybersecurity of its online platform and its online databases.

Thereafter it will summarise the lessons from Chapter 3, which were drawn from other jurisdictions, and more specifically the lessons that were drawn in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted.

Then, it will summarise the lesssons from Chapter 4 on the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG investment considerations in order to look how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.

Lastly, it will summarise the lessons from Chapter 5, which looked at the further accountability mechanisms to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI. More specifically, it will provide lessons on the adequacy of the SA privacy law and cybersecurity regimes, lessons on directors' further liability in terms of the duty of care in relation to cybersecurity and the use of AI. Lastly, it will look at the lessons how the use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code.

The Chapter will then begin to end off with recommendations for a more detailed treatment on the duty of care in relation to cybersecurity and the use of AI in the King Code, and then the Chapter will conclude with final remarks, which will summarise the contribution of this thesis to SA Law.

2. RECOMMENDATIONS FOR SA ON THE REGULATION OF OMs IN OTHER JURISDICTIONS

It was shown that there are important lessons, which directors can learn on how OMs are regulated in other jurisdictions, particularly with regard to the use of the online platform and its online databases, in order to understand how to best protect the integrity of the OM, as well as the cybersecurity of its online platform and its online databases.

2.1. US

This thesis has examined the US legal regime, and deduced various lessons on how US legal sources regulate OMs, particularly with regard to the online platform and its online databases, in order to best protect the integrity of the OM.

In terms of US Federal Law, the MBCA of 2016, section 7.09 was firstly looked at, and it was seen that it sets out the minimum requirements on procedures that directors need to follow, and that it allows the board to add additional precautionary measures in the MOI in order to improve the standard of the duty of care in relation to cybersecurity that could be expected of directors.[1882] It states in this regard that participation by online communication is bound by the guidelines and procedures that a board decides.[1883] This shows the King Committee that SA directors should also be encouraged to set their own standards on the duty of care in relation to cybersecurity and the use of AI in their company's MOI and that such self-imposed requirements may be stricter than those which legislation already requires of them, so that they can act as additional precautionary measures to cyberbreaches and the irresponsible use of AI.[1884]

It was explained that it is also possible to obtain the input from shareholders on how directors should exercise their duty of care in relation to cybersecurity, and the responsible use of AI. The MBCA of 2016, section 7.09(a) allows the board to ask shareholders their opinion when they need to choose the most efficient means of online communication.[1885] This consequently shows the King Committee that the board should determine what types of IT tools shareholders/stakeholders use and then ensure that the company's cybersecurity measures are in line with the threats that those IT tools pose.[1886]

It was said that the two parts of section 7.09(b), which set out the minimum requirements to safeguard the integrity of shareholders' meetings, are important, because the one part shows that the board must use reasonable measures to determine the identity of all participants, so that their identity can at all times be known

---

[1882] US MBCA of 2016.
[1883] US MBCA of 2016, section 7.08; See Chapter 2, section 3.1.
[1884] *Ibid.*
[1885] US MBCA of 2016, section 7.09(a); See Chapter 2, section 3.1.
[1886] *Ibid.*

to the chairperson, the IT section and the auditors in order to practice access control.[1887]

Although the main purpose of the second requirement, that participants must be able to follow the proceedings as they occur, is to prevent the exclusion of shareholders from an OM, it also indirectly requires directors to ensure that buffering, freezing or lagging are mitigated, since it creates a loophole for a cyberattack.[1888] The King Code will have to accentuate to directors the danger that buffering, freezing and lagging presents for a potential cyberbreach, and require them to oversee the installation of additional hardware to augment the RAM in order to overcome freezing and for helping them overcome software coding errors by encouraging them to oversee the installation of additional software that will help to mitigate buffering and lagging.[1889]

Attention was then given to the powerful role that corporate governance guidance in the format of non-binding norms can play to help guide directors on how they need to exercise their duty of care in relation to cybersecurity. In this regard, the US SEC's Division of Corporation Finance and the Division of Investment Management's '*Staff Guidance for Conducting Shareholder Meetings in Light of Covid-19 Concerns,*' shows how greatly non-binding normative guidance could also assist SA directors with the implementation of AI safeguards to protect their company's online platform and its online databases, and the importance of the disclosure of the responsible use of such measures, such as AI.[1890] Nothing prevents the King Committee from publishing similar guidance in non-binding normative format whenever Lockdown regulations are instituted again in future or when a new cyberthreat emerges, which the responsible use of AI can help to combat.

The King Committee can also infer lessons when it comes to the importance of robust disclosures, for example on the responsible use of AI as cybersecurity measures, and to facilitate informed shareholder attendance and participation on cybersecurity matters that affect them.[1891]

The thesis also examined US state law, and various lessons for the King Code were also drawn from these sources.

It was explained that the Delawarean Example on OMs With Specific Procedures focuses mostly on the legal requirements for online participation and the DGCL, section 211(a)(2)(b) shows that the three main requirements for online participation, which each also has their own cybersecurity requirements, are: (i) everyone's identity must be reasonably verified; (ii) everyone present must be given a reasonable opportunity to participate, vote and to follow the proceedings as they occur; and that (iii) any decisions

---

[1887] US MBCA of 2016, section 7.09(b); See Chapter 2, section 3.1.

[1888] *Ibid.*

[1889] *Ibid.*

[1890] US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*

[1891] US SEC Division of Corporate Finance and the Division of Investment Management *op cit s.p.*; See Chapter 2, section 3.1.1.

and votes must be recorded.[1892] The requirement that everyone needs to follow the proceedings as they occur is an important provision, because it was explained that this places a responsibility on directors to help mitigate buffering, freezing and lagging.[1893] It was also explained that online votes and decisions must be recorded and properly stored on the central securities depository by means of AI and Blockchain technology, but that public access thereto must be restricted, so encrypted ledgers will have to be used.[1894]

It was pointed out that the Colorado Example on OMs Without Specific Procedures shows that without specific definitions and prescribed procedures, important concepts that pertain to the directors' duty of care in relation to cybersecurity are open to ambiguity and that it will lead to legal uncertainty.[1895] In this regard, it was said that although section 7-107-108 makes provision for hybrid meetings, legal uncertainty still exists when it comes to OMs.[1896] This section also shows that a company's MOI is a powerful tool that can help guide the directors' duty of care in relation to cybersecurity and hold directors responsible to uphold a certain standard on cybersecurity and to use AI responsibly.[1897] It also shows that the King Code should not prescribe too strict legal provisions for OMs, but rather focus more on strict cybersecurity measures to protect the integrity of the OM, the online platform and its online databases.[1898] Most importantly, it shows that the requirement of audibility is less strict than Delaware's section 211(a)(2), which requires that shareholders should be allowed to follow the proceedings as they occur, because the latter indirectly helps to safeguard shareholders in terms of cybersecurity, because if participants need to follow the proceedings as they occur, it will require directors to implement mitigation measures that can help to mitigate buffering, freezing and lagging.[1899]

Thereafter the Massachusetts and Montana Example on Limitations on Public Companies was looked at and it was seen that it differentiates between companies and it was shown that Massachusetts's differentiation between public and private companies and Montana's differentiation on company size only unnecessarily complicates the duty of care in relation to cybersecurity, and it was explained that it is not advised that the King Code differentiates along the same lines.[1900] Although compliance with the King Code is compulsory to listed companies, there is no reason why public and private

---

[1892] DGCL, section 211(a)(2)(b)(i)-(iii); See Chapter 2, section 3.2.1.
[1893] DGCL, section 211(a)(2)(b)(ii)
[1894] DGCL, section 211(a)(2)(b)(iii).
[1895] See Chapter 2, section 3.2.2.
[1896] Colorado Revised Statutes Annotated of 2017, section 7-107-108; See Chapter 2, section 3.2.2.
[1897] *Ibid.*
[1898] See Chapter 2, section 3.2.2.
[1899] Colorado Revised Statutes Annotated of 2017, section 7-107-108; DGCL of 2000, section 211(a)(2)(b)(i)-(iii); See Chapter 2, sections 3.2.1; 3.2.2.
[1900] Massachusetts General Laws Annotated 156D of 2004, section 7.08; Montana Code Annotated of 2010, section 35-1-516; See Chapter 2, section 3.2.3.

companies, as well as companies of all sizes, may not voluntarily use it, because cyberrisks are a challenge to all companies.[1901]

Attention was then given to the NY Example on Obligatory Shareholder Input, which focuses on the identification of participants, and section 602(1)(b)(i)(A), was highlighted as it accentuates the importance that all participants must be identified.[1902] Section 602(1)(b)(i)(B) again only requires decisions and votes to be recorded, but says nothing on how such decisions and votes then need to be stored securely by Blockchain technology.[1903] Once again, this is an aspect that the King Code will have to address.[1904] It also shows how important it is for legal clarity that the King Code define 'online presence' and state that a shareholder who attends online, be it via BlueJeans, Facebook, Microsoft Teams, Zoom or even WhatsApp, is deemed to be present in person.[1905]

The California and Maryland Example on Shareholder Participation makes provision for shareholder input in how OMs are held and their cybersecurity requirements and it was explained how important shareholder input is in corporate governance processes and that provision for shareholders/stakeholders' input and objections on cybersecurity-related aspects and the responsible use of AI should be made.[1906] California's section 600 and Maryland's section 2-503(b)(2) acknowledge the importance of shareholder input in the decision to hold OMs and related aspects on cybersecurity and how the duty of care in relation to cybersecurity must be exercised and make provision for such input and objections.[1907] This provides the board with the ability to ensure that their cybersecurity measures are synchronised with the IT tools that shareholders use and require, and that they exercise their duty of care in relation to cybersecurity effectively in terms of what the shareholders require.[1908] It was explained that the King Code should however not go as far as Maryland's section 2-503(b)(2), which determines that an OM cannot be held if any shareholder objects, as this will leave room for frivolous and vexatious inputs from shareholder activists who may want to veto an OM and prevent it from being held.[1909] This is especially problematic during the time of a Pandemic when OMs are needed.

The lesson from the Illinois Example on No OMs is that the guidance on cybersecurity and the responsible use of AI to combat cybercrime in the King Code

---

[1901] See Chapter 2, section 3.2.3.
[1902] *Ibid.*
[1903] NY BCL of 2010 (amended 2019), section 602(1)(b)(i)(2)(B); See Chapter 2, section 3.2.4.
[1904] *Ibid.*
[1905] *Ibid.*
[1906] See Chapter 2, section 3.2.5.
[1907] California Corporations Code of 2009, section 600; Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(b)(2); See Chapter 2, section 3.2.5.
[1908] *Ibid.*
[1909] Maryland Code Annotated on Corporations and Associations of 2017, sections 2-503(b)(2); See Chapter 2, section 3.2.5.

should be applicable to hybrid meetings as well, so that it can accommodate instances where companies' MOIs have not been changed to accommodate OMs.[1910]

From the NYSE, the King Committee should see that additional measures on the duty of care in relation to cybersecurity and the responsible use of AI, which are of a temporary nature, could be issued in future to supplement the King Code, should the need ever arise.[1911] In addition, should SA Lockdown levels ever increase again, the King Committee could approach the JSE with a request to provide temporary relief to hold OMs and for companies to get their cybersecurity arrangements in order, similar to the NYSE's '*Listed Company Compliance Guide*'.[1912]

The lessons from US federal legislation show the King Committee that the duty of care in relation to cybersecurity and the use of AI in SA requires guidance on the minimum requirements to hold an OM, and also that provision should be made for the board to implement additional safeguards.

The lessons from the US states' legislation again show the King Committee how important it is that the legal requirements for online participation must be stipulated, the need for proper definitions and for best examples on processes to be followed, as well as not to differentiate between the types of companies and their size.[1913] In addition, it shows the need to properly identify participants, the need to make provision for shareholder input in the way in which OMs are held and their cybersecurity requirements, and for shareholders/stakeholders' input on the due care in relation to cybersecurity that they feel is required from directors.[1914] Lastly, it shows that the King Committee should issue additional measures of a temporary nature in future to supplement the King Code on new cyberrisks.[1915]

2.2. UK

This thesis has also examined the UK legal regime, and deduced various lessons for the King Code from UK legal sources.

The lesson from the EU 'Directive on the Encouragement of Long-Term Shareholder Engagement of 2017' focuses on the securing of personal information on a central securities depository and this shows that SA directors will need guidance on how they need to oversee instances where EU shareholders' personal information is sent or requested from a central securities depository that is domiciled in the EU.[1916]

[1910] Illinois Compiled Statutes Annotated 805 of 1983, section 5/7.05; See Chapter 2, section 3.2.6.
[1911] See Chapter 2, section 4.3.
[1912] NYSE '*Listed Company Compliance Guidance' op cit s.p.*
[1913] See Chapter 2, sections 3; 6.1.
[1914] *Ibid.*
[1915] *Ibid.*
[1916] EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017' *op cit* section 4; See Chapter 2, section 4.1.

When the focus fell on the UK Companies Act of 2006 (Ch.46), it was seen that it focuses mostly on setting out the responsibilities of the board on how they need to exercise their duty of care.[1917] It also showed that the King Code should not make the same mistake as the UK Companies Act of 2006, section 311, which does not clearly define "place of meeting" and that it must also clearly include cyberspace in the definition of an OM, because once it leaves this definition open to interpretation, it leads to uncertainty on whether the duty of care in relation to cybersecurity is also required on the physical aspects pertaining to a hybrid meeting.[1918] It was said that the duty of care in relation to cybersecurity will not be facilitated if there are instances of amibiguity or legal uncertainty in the King Code.[1919] It is submitted that it is against this background that the definitions, which are related to aspects of AI and Blockchain technology, such as a 'central securities depository,' 'encrypted ledgers' and 'restricted access' thereto, should also be properly defined. In addition, section 311 shows that the King Code should also encourage companies to use their MOIs to help set requirements on how OMs, online platforms and their online databases should be properly secured.[1920] The King Code should follow the example of the UK Companies Act of 2006, section 360A(1), which states that nothing in that Act may be interpreted in a way that will cause participants of a shareholders' meeting who are not present, to not attend, speak or vote online, but this right should not be unqualified, and should be made subject to the requirement that a participant must first identify themself as a registered shareholder/stakeholder.[1921] The requirements of section 360(A)(2) is important in this regard because it determines that OMs may be subject only to such requirements (a) needed to identify the participants; and that (b) the cybersecurity measures for online communications must be reasonable.[1922] As a result, this places only the requirement to identify themselves on shareholders, and no requirement is placed on them to ensure that their access devices are end-to-end encrypted.[1923] This effectively places the entire responsibility to protect the integrity of the OM, the online platform and its online databases on the board, as no requirement is placed on shareholders to adhere to, or implement, any online security protocol, such as end-to-end encryption.[1924] The other requirement is that the cybersecurity measures must be reasonable.[1925] No guidance is however given on what will constitute a reasonable and responsible use of AI.[1926]

[1917] UK Companies Act of 2006 (Ch. 46), section 311; See Chapter 2, section 4.2.
[1918] UK Companies Act of 2006 (Ch. 46), section 311.
[1919] UK Companies Act of 2006 (Ch. 46), section 311; Coen *op cit s.p.*; See Chapter 2, section 4.2.
[1920] *Ibid.*
[1921] UK Companies Act of 2006 (Ch. 46), section 360A(1); See Chapter 2, section 4.2.
[1922] UK Companies Act of 2006 (Ch. 46), section 360A(2)(a)-(b); See Chapter 2, section 4.2.
[1923] UK Companies Act of 2006 (Ch. 46), section 360A(2)(a); See Chapter 2, section 4.2.
[1924] *Ibid.*
[1925] UK Companies Act of 2006 (Ch. 46), section 360A(2)(b); See Chapter 2, section 4.2.
[1926] *Ibid.*

It was also seen how the UK CIGA of 2020 provided a window-period for companies to adapt to OMs, even if their MOIs did not allow it, and it was pointed out that it is a pity that the SA government was not as pro-active and did not promulgate similar relief in nature to CIGA to provide SA companies with an extended period to hold OMs and to get all of their cybersecurity arrangements in place during the Pandemic.[1927] The SA government should take cognisance of this pro-active drive to help proliferate OMs.[1928] At the same time, the King Committee should take note that CIGA contained an oversight due to its omission to stipulate any minimum requirements on cybersecurity and details on the duty of care in relation to cybersecurity and the responsible use of AI.

It was seen that the UK Department for Business, Energy and Industrial Strategy's '*Memorandum of 2020*' makes provision for shareholders to voice their concerns on cybersecurity matters in the beginning of a meeting and it was explained that the King Code should encourage the board to reply on such questions before voting.[1929] This would allow shareholders to raise concerns on the way in which directors exercise their duty of care in relation to cybersecurity and the use of AI and it is important that answers on any questions in this regard must be provided to all participants, both before, during and after the OM.[1930]

The UK Chartered Governance Institute's '*Guidelines of 2020*' provides additional guidance on cybersecurity-related matters and show what an important role corporate governance institutes, such as IoDSA, can play to provide guidance on cybersecurity matters and matters related to the duty of care in relation to cybersecurity and the use of AI.[1931] The King Committee should have issued similar detailed guidance to SA companies to help guide SA directors on how they should exercise their duty of care in relation to cybersecurity and the use of AI, especially to accompany the JSE online platform.[1932]

Lastly, it was interesting to note that both the LSE and the JSE took pro-active stances on OMs when the Lockdown struck, but that the JSE can be commended because it went even further and devised its own online platform.[1933]

The lessons from the UK legal regime show the King Committee that the duty of care in relation to cybersecurity and the use of AI requires guidance on the securing of personal information by means of Blockchain technology in a central securities depository on encrypted ledgers, the delineation of the responsibilities of the board and shareholders, as well as the need for the SA legislature to provide a window period for

---

[1927] UK CIGA of 2020; Steeden *et al. op cit s.p.*; See Chapter 2, section 4.3.
[1928] See Chapter 2, section 4.3.
[1929] UK Department for Business, Energy and Industrial Strategy *op cit* 7-8; See Chapter 2, section 4.4.
[1930] *Ibid*.
[1931] UK Chartered Governance Institute's '*Guidelines of 2020*' *op cit s.p.*; See Chapter 2, section 4.5.
[1932] *Ibid*.
[1933] Clark op cit s.p.; See Chapter 2, section 4.6.

companies to adapt to OMs, even if their MOIs do not allow OMs.[1934] In addition, it shows the need for the creation of an opportunity for shareholders to voice their concerns on cybersecurity matters and the way in which the duty of care in relation to cybersecurity is exercised in the beginning of an OM.[1935] Lastly, it shows the pro-active role that corporate governance institutions could play to provide additional guidance on cybersecurity-related matters and the duty of care in relation to cybersecurity and the use of AI.[1936]

2.3. SA

The focus on SA's legal sources helped to understand how OMs are regulated in SA and helped to understand how the duty of care in relation to cybersecurity should be exercised to best protect the integrity of the OM, as well as the cybersecurity of the online platform and its online databases.

It was explained that the requirements of the Act have certain consequences that the King Code will need to abide by: in the first instance, attention must be given to the Act, section 61(10)'s provision on accessibility that requires shareholders' meetings to be reasonably accessible for online participation by shareholders, regardless of whether they are held in SA or elsewhere.[1937] This provision has dual consequences for how SA directors need to exercise their duty of care in relation to cybersecurity: firstly, it compels companies to have at least hybrid meetings, and that companies also need to have the necessary cybersecurity measures in place for hybrid meetings.[1938] The requirement that OMs must be reasonably accessible for online participation by shareholders, regardless of whether they are held in SA or elsewhere, effectively requires directors to ensure that an OM is also reasonably accessible for online participation even for shareholders outside of SA's borders.[1939] As a result, this means that directors will also need to ensure that their companies improve their cyberresilience to thwart cyberrisks that originate from outside the borders of SA.[1940] In future, a court will have to determine the true meaning of "reasonably accessible" and examples of it.[1941] This is important, because different access points and portals to OMs all require different online security protocols that require their own cybersecurity measures.[1942]

In the second instance, the enabling provision of section 63(2) states that if a company's MOI does not prohibit an OM, it may conduct (a) a shareholders' meeting

---

[1934] See Chapter 2, sections 4; 6.2.
[1935] *Ibid.*
[1936] *Ibid.*
[1937] The Act, section 61(10); See Chapter 2, section 5.1.
[1938] *Ibid.*
[1939] *Ibid.*
[1940] *Ibid.*
[1941] *Ibid.*
[1942] *Ibid.*

entirely online; or (b) one or more participants, may participate online in the physical shareholders' meeting, as long as the online communication allows all participants to communicate reasonably effectively and simultaneously without an intermediary.[1943] In this regard, the King Code should look at all the different types of cyberrisks that could occur when online communication does not occur simultaneously, and it should also lay down a definition with examples of "reasonably effective" online communication.[1944] It was explained that the requirement to communicate simultaneously indirectly requires that buffering, freezing and lagging should be mitigated.[1945]

The prohibition of section 63(2)(b) on the use of AI intermediaries in the online communication between shareholders/stakeholders and the company is a unique provision when compared to other legislation, and the King Code should set out examples of what it entails and should underline that the use of chatbots to answer the questions of shareholders/stakeholders during an OM is a forbidden practice.[1946] The King Code will need to lay down guidance on how directors need to exercise their duty of care in relation to cybersecurity when it comes to the involvement of AI intermediaries and AI's moderation of questions, as this can basically be seen as external inference with the online proceedings.[1947]

Thirdly, with regards to the notice requirements of section 63(3)(a), the OM notice will have to provide the necessary online access information upfront to enable participants to access the online platform.[1948] It is submitted that the online access information should disclose that the necessary security protocols and encryption is in place to secure the OM. Should browser, dial-in or weblink details be recorded incorrectly on the notice or if the web-link on a notice does not lead to the online platform, or if its security protocols are unsecured, and if it is not properly encrypted, it could render the entire OM null and void, and provide an opportunity for cybercriminals to exploit.

Fourthly, with regards to the expense requirement of section 63(3)(b), it is required that the notice mentions that the costs of the online communication is a cost to be borne by the participant, unless the board decides something else.[1949] Although the notice needs to state that the cost of online communication is to be borne by the participant, no mention is made that the participant also needs to adhere to, or implement, any online security protocol, such as end-to-end encryption – and this effectively places the entire responsibility to protect the integrity of the OM, the online platform and its online databases on the board.

[1943] The Act, section 63(2)(a)-(b); See Chapter 2, section 5.1.
[1944] The Act, section 63(2)(b); See Chapter 2, section 5.1.
[1945] See Chapter 2, section 5.1.
[1946] The Act, section 63(2)(b); See Chapter 2, section 5.1.
[1947] *Ibid.*
[1948] The Act, section 63(3)(a).
[1949] The Act, section 63(3)(b).

It was said that the King Report IV, principle 12 recommends that boards exercise ongoing oversight over IT management to a point that it results in the ethical and responsible usage of IT.[1950] As a result, the King Code will need to detail this with examples and recommendations on best practices on what is deemed to constitute ethical and responsible usage of AI, (since there are certain types of AI which directors cannot use when they perform their functions), otherwise it will remain a hollow principle that is open to interpretation.[1951]

In accordance with the JSE '*Listing Requirements*,' section 1.28, which sets out the rules and procedures that any listed company will have to comply with when they want to be listed on the JSE and to have their shares traded publicly, it was said that the King Committee should clearly state the consequences of the irresponsible use of Blockchain to store shareholders' personal information on the central securities depository, when the ledgers are not encrypted.[1952]

3. RECOMMENDATIONS FROM A LEGAL COMPARISON OF THE SA, UK AND US DUTY OF CARE IN RELATION TO CYBERSECURITY

It was explained that although SA, the UK and the US each has their own requirements on the standards on the duty of care in relation to cybersecurity, there are also important lessons that SA directors can learn from these jurisdictions to provide context for how the SA duty of care in relation to cybersecurity should be interpreted.

The SA Constitution, section 39(1) says that when a court interprets the Bill of Rights, it (b) must consider international law; and (c) that it may consider foreign law.[1953]

In addition, the Act, section 5(2) states with regards to its general interpretation that a court may interpret or apply foreign company law when it applies the Act, if it is appropriate to do so.[1954]

The further interpretation of the duty of care in relation to cybersecurity in SA through international and foreign law, (especially UK case law on the duty of care and US case law on how the BJR was applied in cybersecurity cases), will help SA courts to interpret the legislative duty of care in relation to cybersecurity.[1955] Since the SA Constitution of 1996 and the Act both allow SA courts to look at foreign law when they interpret the Act, SA directors may draw on the examples and best practices from UK

[1950] IoDSA '*King Report IV' op cit* principle 12; See Chapter 2, section 5.2.
[1951] *Ibid.*
[1952] JSE '*Listing Requirements*,' section 1.28; See Chapter 2, section 5.3.
[1953] SA Constitution of 1996, section 39(1)(a)-(c).
[1954] The Act, section 5(2).
[1955] The Act, section 76(3)(c).

case law on the duty of care and US case law on the BJR that were highlighted to help guide them with the application of their duty of care in relation to cybersecurity.[1956]

Both the Act, section 76(3)(c) and the UK Companies Act of 2006, section 174 espouse an objective and subjective standard on the duty of care, skill and diligence.[1957] In the US, the MBCA of 2016, section 8.30 again sets out the duty of care and states that directors shall perform their duties (a)(1) in good faith; (2) with the care that an ordinary prudent person would reasonably believe to be appropriate in similar circumstances; and (3) in a way that the director reasonably believes will be in the company's best interests.[1958]

According to Cassidy, the Act, section 76(3)(c) could be interpreted to mean that both the objective and subjective standards, as is the case with the UK Companies Act of 2006, section 174, apply to each element of care, skill and diligence.[1959]

The Act has been criticised on the nature of the interaction between sections 76(3)(c)(i) and 76(3)(c)(ii).[1960] Bekink explains that the wording of section 76(3)(c) creates the potential for the court to subject the legislative duty of care to the subjective common law standard.[1961] He compares the wording, "that director," of section 76(3)(c)(i) with the wording, "the general knowledge, skill and experience of that director," of section 76(3)(c)(ii), and comes to the conclusion that the words of the subjective considerations in section 76(3)(c)(ii) seems to subject the objective standard in section 76(3)(c)(i).[1962] Cassidy points out that the wording of the duty of care in the UK Companies Act of 2006, section 174 does not seem to subject the objective standard to subjective considerations.[1963]

The US MBCA of 2016, section 8.30 does not look in similar detail at the different requirements of the duty of care when it is compared with the Act and the UK Companies Act of 2006.[1964] The wording of the MBCA of 2016, section 8.30 looks only at the standards of care and diligence.[1965] Cassidy makes an interesting observation when she points out that the test in the MBCA of 2016, section 8.30 contains both elements of subjectivity and objectivity.[1966] In this regard, the reference to an "ordinary prudent person" objectifies the standard.[1967] She elaborates and says that the test's objectivity is strenghtened by the requirement that the director's conduct must conform

---

[1956] The Act, section 76(3)(c).
[1957] The Act, section 76(3)(c); UK Companies Act of 2006, section 174.
[1958] US MBCA of 2016, section 8.30(a)(1)-(3).
[1959] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; Cassidy *op cit* 385.
[1960] The Act, section 76(3)(c); Cassidy *op cit* 385.
[1961] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; Bekink *op cit* 110.
[1962] The Act, section 76(3)(c)(i)-(ii); Cassidy *op cit* 385.
[1963] The Act, section 76(3)(c); UK Companies Act of 2006, section 174.
[1964] The Act, section 76(3)(c); UK Companies Act of 2006, section 174; US MBCA of 2016, section 8.30.
[1965] US MBCA of 2016, section 8.30(a)(1)-(3); The Act, section 76(3)(c); Cassidy *op cit* 385.
[1966] Cassidy *op cit* 385.
[1967] *Ibid*.

to the conduct of an "ordinary prudent person" who is "in a like position and under similar circumstances."[1968] This then means that the MBCA of 2016, section 8.30's duty of care takes the circumstances into account within which a director performs their power and functions, as is the case with the objectivity standard in the Act, section 76(3)(c)(i).[1969]

As is the case with the UK Companies Act of 2006, section 174(2)(a), the Act section 76(3)(c)(i) sets a minimum objective standard to evaluate the conduct of directors.[1970] The standard is the nature of the conduct that can reasonably be expected from someone who performs "the same functions in relation to the company as those carried out by that director."[1971] Bekink points out that the word "having" in the Act, section 76(3)(c)(ii) in terms of someone "having the general knowledge, skill and knowledge of that director," acts to subject the minimum objective standards to the subjective ability of that director.[1972]

In SA, the duty of care originates from the common law, and although it is now codified by the Act, section 76(3), the common law still applies.[1973] The Act does not have a provision like the UK Companies Act of 2006, section 170(3)-(4), which provides guidance on the interaction between the common law and legislative duties of care.[1974] The Act consequently leaves it open to interpretation whether legislation supersedes the common law, whether they co-exist, or whether the common law should be used to help interpret the Act, section 76(3)(c).[1975] Hopefully a SA court will provide guidance on the interpretation of the Act, section 76 in this regard in future.[1976]

Unlike the UK Companies Act of 2006, the Act, section 76(4)(a)-(b) incorporated a 'safe harbour' provision to a breach of the duty of care, in the form of the BJR.[1977] In this regard, the Act, section 76(4)(b)(i) allows directors to state that they delegated a certain task or that they relied on certain information on which they based their decision.[1978] The Act, section 76(5) even gives a list of people whose advice directors may use and rely on in order to exercise their duty of care.[1979] The UK Companies Act of 2006 does not have a BJR, nor the defences of delegation and reliance.[1980] Since the legislative BJR in the Act, section 76(4) is an import from US legislation, it is anticipated

---

[1968] Cassidy *op cit* 385.
[1969] *Ibid*.
[1970] The Act, section 76(3)(c)(ii); UK Companies Act of 2006, section 174(2)(a).
[1971] The Act, section 76(3)(c)(i).
[1972] The Act, section 76(3)(c)(ii).
[1973] The Act, section 76(3); Blackman *et al. op cit* 8-29; Delport *et al. Henochsberg on the Companies Act op cit* 298; Kanamugire *et al. op cit* 71.
[1974] The Act; UK Companies Act of 2006, sections 170(3)-(4).
[1975] The Act; UK Companies Act of 2006, section 170(4).
[1976] The Act, section 76.
[1977] The Act, section 76(a)-(b); UK Companies Act of 2006.
[1978] The Act, section 76(4)(b).
[1979] The Act, section 76(5).
[1980] The Act, section 76(4).

that US law can play a big role to provide guidance to the SA courts with its application.[1981]

It needs to highlighted that the duty of care in the US differs from the same duty as it is applied in the UK and SA, and although it has elements which could prove beneficial to these two jurisdictions, it cannot be applied without challenges.[1982] An example in this regard is that gross negligence is sometimes used as a standard of review, as was the case when Herrmann, CJ of the Supreme Court of Delaware used it in 1985 in *Smith supra* instead of mere negligence.[1983] It is submitted that the usage of a standard of gross negligence is not the most appropriate solution to serve as a general review standard for the duty of care when compared to the legislation of other jurisdictions.[1984]

It was also explained that when the Act, section 76(3)(c) is read with King Report IV, principle 12 on IT governance, it does increase the expectation of a director's duties in relation to cybersecurity.[1985] A court would therefore also need to consider the recommendations that the King Code prescribe when it determines a director's liability.[1986]

Since the Act, section 24(1)(a) already allows a company to store information online, a director should be allowed to use aspects of AI, such as Consultative AI and Data Analysis to exercise their duty of care in relation to cybersecurity properly.[1987] The duty of care and diligence requires an objective test, while the duty of skill uses a subjective test, because the skillsets of persons differ.[1988] When one thinks about the information-overload that confronts a director, it is possible for the courts to allow a reasonable director to use Consultative AI and Data Analysis when they properly exercise their duty of care in relation to cybersecurity, whenever the court needs to apply the objective test of section 76(3)(c).[1989] The wording of section 76(3)(c) could be interpreted in a way that will allow directors to integrate and rely on AI in the way in which they exercise their duty of care in relation to cybersecurity, just as long as the AI does not substitute the director or prescribe how the director should exercise his/her own free will.[1990]

In summary, with increased cyberattacks and cyberbreaches, UK and US law are starting to establish responsibility in the event of a cyberbreach.[1991] Legislation is also starting to cite specific requirements that boards need to conform with when they

---

[1981] The Act, section 76(4).
[1982] *In Re Caremark supra*; US FTC '*Fighting Identity Theft with the 'Red Flag' Rule' op cit s.p.*
[1983] *Smith supra.*
[1984] *In Re Caremark supra*; US FTC '*Fighting Identity Theft with the 'Red Flag' Rule' op cit s.p.*
[1985] The Act, section 76(3)(c); IoDSA '*King Report IV*' *op cit* principle 12; Burger *op cit s.p.*
[1986] *Ibid.*
[1987] The Act, section 24(1)(a); Andrade *et al. op cit* 26.
[1988] The Act, section 76(3).
[1989] The Act, section 76(3)(c); Andrade *et al. op* 26.
[1990] *Ibid.*
[1991] Johnson *op cit* 255.

exercise their duty of care in terms of cybersecurity and in some instances boards are even required to demonstrate that they have implemented a cybersecurity strategy in the form of a policy and system based on their cyberrisk profile.[1992] US state law is also starting to outline how directors need to exercise their duty of care in relation to cybersecurity, such as the Colorado Privacy Act, section 1-1-1308(5) and the NYPA of 2021, section 5642.[1993]

It seems that the most important components that directors need to include when they exercise their duty of care in relation to cybersecurity is the evaluation of the potential cyberrisks that faces their company, determining the likelihood that these cyberrisks may occur, and what losses or damage may result, and to then put the adequate precautionary measures in place to prevent such a cyberattack.[1994] The important thing is that SA directors need to follow a process in this regard and that they need to keep evidence of how they applied their minds and reached decisions and implemented and oversaw proper cybersecurity measures to help make their company cyberresilient.

4. RECOMMENDATIONS ON HOW THE DUTY OF CARE IN RELATION TO CYBERSECURITY COULD HELP TO IMPROVE CORPORATE GOVERNANCE, CSR AND ESG INVESTMENT CONSIDERATIONS AT SA OMs

Chapter 4 looked at the evolution of the emphasis on CSR to sustainability to ESG considerations. It was explained that the evolution of ESG shows clear differences between CSR, sustainability and ESG considerations.[1995] The early development of CSR is characterised by a focus on accountability and ethics, sustainability emerged in the 1980's and focused on the role that stakeholders need to play to ensure sustainable development, while the introduction of ESG considerations places a focus on changing the behaviour of investors when they make their investment decisions.[1996] Although the three concepts overlap in terms of their goal to ensure that the company survives and flourishes, they have many differences.[1997] In this regard, it was highlighted that the umbrella concept of sustainability cannot be implemented without tension with CSR and ESG.[1998] It was explained by means of a timeline how the model of ESG considerations became the universal standard approach.[1999]

[1992] Johnson *op cit* 255.
[1993] Colorado Privacy Act of 2021, section 1-1-1308(5); New York Privacy Act of 2021, section 6542.
[1994] DoCRA Council *op cit s.p*.
[1995] Esser *et al. op cit* 34.
[1996] *Ibid*.
[1997] *Ibid*.
[1998] *Ibid*.
[1999] *Ibid*.

The Chapter then looked at the way in which SA directors should exercise their duty of care in terms of corporate governance, CSR and ESG considerations. It was explained that since SA is a resource-scarce country, sustainability-related challenges will continue to threaten the growth and survival of SA companies as the competition for resources will increase.[2000] It consequently becomes more important that SA companies need to adapt to their corporate sustainability challenges and to manage their ESG risks.[2001] In addition, stakeholders, such as customers, investors, shareholders and suppliers should acknowledge that ESG considerations should be included in the long run to create value in a sustainable manner.[2002]

Specific attention was also given to the exercise of the directors' duty of care in relation to cybersecurity and the use of AI and Blockchain technology since this is a new field that is developing fast and directors will need to address the challenges that they present. It was said that the King Code should start to regulate AI and Blockchain technology in the SA corporate governance regime at a time when these technologies are still in their infant shoes. It explained that it could help to improve aspects of corporate governance and CSR and ESG considerations in the ways set out below, once directors use AI responsibly.

The duty of care in relation to cybersecurity could help to improve cybersecurity issues on shareholder and stakeholder protection at board level through deliberation.[2003]

The protection of the online platform and its online databases could be made a requirement in the official sanctioning of a standard-setting authority, (such as cybersecurity-sensitive auditing) or cybersecurity standard-setting or inclusion on the JSE RIIS.[2004]

The duty to exercise a pre-determined standard of care in relation to cybersecurity could also be inserted as part of directors' duties or executive remuneration.[2005]

Corporate disclosure and reporting obligations on the standard of the duty of care in relation to cybersecurity, should be done as this will help safeguard the interests of the community, consumers, employees and the online environment by promoting transparency.[2006]

[2000] Erasmus *et al. op cit* 3 – 4.
[2001] *Ibid*.
[2002] *Ibid*.
[2003] Vigeo *op cit* 8 – 9.
[2004] Horrigan *et al. op cit* 26.
[2005] Vigeo op cit 15.
[2006] Libit *op cit s.p*.

The duty of care in relation to cybersecurity could be included in the standard-setting for good corporate governance, such as stakeholder engagement mechanisms.[2007]

Greater shareholder and stakeholder participation on cybersecurity matters could be promoted.[2008] Otherwise a shareholder vote on the appropriate cybersecurity policy and system could be held or shareholder proposals on cybersecurity issues, such as the use of AI, could be asked.[2009]

Special treatment could be afforded to important non-shareholder interests in the company's cybersecurity strategy, such as employees' interests or creditors' interests whenever it is required.[2010]

Incentives could be created and disincentives could be removed at the policy level for social and online environmental responsible corporate behaviour, such as procurement and licensing requirements of cybersecurity systems.[2011]

Awareness could also be raised on the accommodation of cybersecurity criteria in decision-making on investments in cybersecurity systems and measures, in the SA CRISA of 2011.[2012]

Directors could voluntarily adopt self-regulatory measures on cybersecurity and the use of AI, such as the voluntary adoption of recommendations, which are contained in cybersecurity reports or industry cybersecurity best practices.[2013]

Directors will need to adhere to other important laws, regulations and corporate governance guidance that regulate aspects of cybersecurity, such as the Act, section 63(2), which requires shareholders to pose their questions to the board without moderation by an AI intermediary.[2014]

Directors could also integrate cybersecurity issues on stakeholder protection in the audit process by allowing the audit committee to review cybersecurity risks.[2015] They could also obtain the independent accreditation of their cybersecurity practices and their responsible use of AI.[2016]

So, in other words, where other researchers only looked at OMs as a tool to improve corporate governance and CSR, this chapter explained that directors' oversight on good corporate governance practices and their integration of CSR and ESG

[2007] Jutterström *op cit* 11.
[2008] Gao *et al. op cit* 1.
[2009] *Ibid.*
[2010] Horrigan *et al. op cit* 26.
[2011] Derchi *et al. op cit s.p.*
[2012] Horrigan *et al. op cit* 26.
[2013] *Ibid*.
[2014] The Act, section 63(2); Moyo 'Virtual AGMs May Infringe SA Companies' Act' *op cit s.p*.
[2015] Viego *op cit* 11 – 15.
[2016] *Ibid.*

considerations with the use of AI and Blockchain technology, will improve companies' cyberresilience and will especially help to make their OMs more cyberresilient.[2017]

5. RECOMMENDATIONS ON DIRECTORS' FURTHER EXPOSURE TO LIABILITY IN TERMS OF THE USE AND REGULATION OF AI

Chapter 5 looked at the various other accountability mechanisms that shareholders/stakeholder may use to hold directors accountable.

The first part of this Chapter gave an overview of the international privacy law and cybersecurity regimes in order to look for lessons on their adequacy and their shortcomings.

The second part of this Chapter looked at the various other accountability mechanisms, besides the common law and legislative duties of care, which shareholders/stakeholder may use to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI. This section was required in order to look for lessons on how shareholders/stakeholders could hold directors better accountable.

The last part of this Chapter looked at lessons on how directors' use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code.

5.1. Recommendations on the Adequacy of the SA Privacy Law and Cybersecurity Regimes and the Ways in Which They Are Enforced

It was explained that the CoE's 'Convention on Cybercrime' was the world's first multilateral treaty on the prevention of cybercrime, and that it came into effect on 1 July 2004.[2018] The 'Convention on Cybercrime' is currently the only binding multilateral treaty which regulates cybercrime.[2019] Sixty seven member states have so far ratified this Convention.[2020] SA has signed this Convention on 23 November 2001, but has not yet ratified it.[2021] SA is consequently not obliged to comply with this Convention's provisions.[2022] It is important that SA ratifies this convention as soon as possible in order to facilitate cross-border cybercrime investigations.

With regards to the SA common law position on cybersecurity it was explained that SA was isolated for so long by the international community that initially only cybercrimes such as cyberfraud and online defamation were initially prohibited in terms

---

[2017] See Chapter 1, section 5; See Chapter 4, section 5.
[2018] CoE '*Convention on Cybercrime of 2001*' (ETS 185), *s.p.*
[2019] *Ibid.*
[2020] CoE '*Chart of Signatures and Ratifications of Treaty No. 185' op cit s.p*.
[2021] *Ibid*.
[2022] *Ibid.*

of the SA common law.[2023] Since the concepts of cyberforgery, cyberuttering and the interception of online information were at that point in time so new, they were initially not prohibited by the SA common law.[2024] As a result, SA companies were for a long time left exposed to cybercrimes, such as cyberattacks, identity theft, online information theft, online scams and phishing.[2025]

After a few years without regulations on cybersecurity, the SA ECTA 25 of 2002 was promulgated to, amongst other things, also help fight cybercrime in SA.[2026] Although this Act helps to resist hacking and the use of anti-cybersecurity and circumventer IT, which are used to create cyberbreaches at SA companies, it does have its shortcomings.[2027] The first shortcoming is that it omitted to define the concepts of 'cybercrime' and 'cybersecurity.' Secondly, the unspecified amount of the fine and the prison term in section 89 does not help to deter cybercrimes.[2028] In addition, this Act does not prohibit the use of AI to commit cybercrime, nor does it make provision for the responsible use of AI to improve the cyberresilience of SA companies, and it also does not especially prohibit a cybercrime such as cyberwarfare.[2029]

Hereafter, the SA RICA 70 of 2002 was promulgated in an attempt to further improve cybersecurity in SA.[2030] It also has the shortcoming that it does not specifically prohibit cybercrime towards SA companies.[2031] It also does not prohibit the use of AI to circumvent the interception of online communications, nor does it make provision for the responsible use of AI to fight cybercrime that are committed towards SA companies and their personal information databases.[2032]

The SA POPI Act 4 of 2013 also has the shortcoming that it does not prohibit the use of AI to obtain personal information, and it also does not encourages the use of AI to help combat cybercrime towards SA companies.[2033]

The SA Cybercrimes Act 19 of 2020 recently came into effect on 1 December 2021.[2034] Section 54(1)(a) obliges persons and companies to report a cybercrime and; (b) to preserve any evidence that could be used to prove that a cybercrime was committed and directors need to remember that any company who does not report a cybercrime that was committed against it, and who does not preserve any evidence

---

[2023] Cassim 'Addressing the Challenges Posed by Cybercrime: A SA Perspective' *op cit* 119; Thornton *et al. op cit* 332.
[2024] Chitimira *op cit* 6.
[2025] Cassim 'Addressing the Challenges Posed by Cybercrime: A SA Perspective' *op cit* 119.
[2026] *Ibid.*
[2027] SA ECTA 25 of 2002, section 86; Pitts *op cit* 53.
[2028] SA ECTA 25 of 2002, section 89 of the ECTA; Cassim 'Addressing the Challenges Posed by Cybercrime: A SA Perspective' *op cit* 119.
[2029] Van Der Merwe *et al. op cit* 71.
[2030] SA RICA 70 of 2002.
[2031] Chitimira *op cit* 15.
[2032] SA RICA 70 OF 2002.
[2033] SA POPI 4 of 2013.
[2034] SA Cybercrimes Act 19 of 2020.

related to a cybercrime act, will be liable for criminal penalties.[2035] It is also a shortcoming of this Act that it does not especially prohibit the use of AI to commit cybercrimes, and also that it does not make provision for the use of AI to fight cybercrime towards SA companies.[2036]

5.2. Recommendations on the Further Accountability Mechanisms to Hold Directors Accountable for the Way in Which They Exercise Their Duty of Care in Relation to Cybersecurity and the Use of AI

Besides the common law and legislative duties of care that was already looked at in Chapter 3, directors may in the event of cyberbreach or even a potential cyberbreach, also be exposed to various other types of liability due to the improper exercise of their duty of care in relation to cybersecurity, and this could result in not only various costs that need to be recovered from them, but also their removal. Amongst other things, they may be held liable by the company for the losses it sustained, or by the shareholders/stakeholders for the costs that they had to incur as a result of a cyberbreach and the compromisation of the integrity of their personal information.[2037]

Although directors owe their duty of care to the company, and not to the shareholders, boards still need to make sure that companies comply with their obligations to protect the online databases, otherwise they will be held directly accountable by the shareholders/stakeholders for the violation of their privacy.

It is important that directors have a proper understanding of these various accountability mechanisms in order to limit the possibility that they could be held liable for not exercising their duty of care in relation to cybersecurity properly.

This section will look at the lessons from the various internal and external accountability mechanisms, besides the common law and legislative duties of care, which could be used to hold directors accountable to the company itself, or to the shareholders/stakeholders, when they did not properly exercise their duty of care in relation to cybersecurity.

In terms of the SA Constitution of 1996, directors could be held personally liable when shareholders/stakeholders' right to privacy is breached, because this right is protected in terms of the Constitution, section 14.[2038]

In terms of the Act, directors may be held liable in various ways when they do not exercise their duty of care in relation to cybersecuity properly, as can be seen below.

[2035] SA Cybercrimes Act 19 of 2020, section 54(1)(a) – (b).
[2036] SA Cybercrimes Act 19 of 2020.
[2037] Cohen *et al. op cit* 5 – 6.
[2038] SA Constitution, section 14.

Section 20(4) affords shareholders a legislative right to restrain the company from contravening any provision of the Act; while section 20(5) affords shareholders a legislative right to restrain the company from contravening its MOI.[2039]

Section 20(6) determines that each shareholder may claim damages from any person who due to gross negligence, fraudulently or intentionally caused the company to do anything that is not in line with (a) the Act; or (b) with a limitation of the company's capacity or its' directors authority, and which has not been ratified by a special resolution, as required by section 20(2).[2040] It needs to be pointed out that this provision specifically refers only to shareholders, and thus excludes stakeholders.[2041] It was held in *De Bruyn supra* that section 20(6) does not give shareholders a personal right to claim damages for personal loss that they suffered due to such a misconduct.[2042] If the company suffered a loss, damages can be claimed by the shareholders on behalf of the company, in terms of section 20(6), but not on their own personal behalf.[2043] If the shareholders were able to prove that they had suffered a loss, which is apart from the company's loss, it would however be a different scenario.[2044]

Section 71(1) determines that directors who were found to have breached their duty of care and skill, may be removed by the shareholders with an ordinary resolution at a general meeting.[2045] The directors or shareholders may also insist on the removal of a director on other grounds, such as a dereliction of duties, an inability to perform their functions, or negligence (in terms of section 76).[2046]

The Act, section 77 allows directors to be held liable for a breach of their duties, since they are accountable to the company.[2047] The Act, section 76(3) has enhanced directors' accountability by partially codifying their duties, and a breach thereof will lead to liability.[2048] Directors need to perform these duties since they stand in a fiduciary relationship to the company and because they have a duty of care.[2049]

The Act, section 77(2)(a) determines that a director may be held liable (due to the common law principles on the breach of a fiduciary duty) for any damages that the company experienced, which were caused by any breach of the duties that are set out in sections 75, section 76(2) or 76(3)(a) or (b).[2050] Likewise, section 77(2)(b) states that a director may be held liable in terms of the common law delict for any damages that the

---

[2039] The Act, sections 20(4) - (5).
[2040] The Act, sections 20(2); 20(6)(a) – (b).
[2041] The Act, section 20(6)(a)-(b).
[2042] The Act, section 20(6); *De Bruyn supra* paras. 220 - 237; Cassim *et al. Contemporary Company Law op cit* 373.
[2043] *Ibid*.
[2044] *Ibid*.
[2045] The Act, section 71(1).
[2046] The Act, section 76; Ncube *op cit* 39.
[2047] The Act, section 77.
[2048] The Act, section 76(3).
[2049] *Hlumisa Investment Holdings (RF) Limited v Kirkinis (No. 1)* 2019 4 SA 569 (GP).
[2050] The Act, sections 77(2)(a); 75; 66(2); 76(3)(a) – (b).

company has suffered, which were caused by a breach of the duty of care and skill in terms of section 76(3)(c); losses due to a breach of a provision of the Act that is not mentioned in section 77; and losses caused by a contravention of the MOI.[2051] Section 77(2) therefore includes the common law liability of directors, and states that it is the company that needs to enforce its interests against the directors.[2052]

The Act, section 165 contains a legislative derivative action, which allows anyone to institute an action on behalf of a company in an attempt to protect the company's interests.[2053] This means that besides the company, shareholders and stakeholders also have legal standing to claim damages for losses.[2054] The inclusion of this legislative action in the Act ended the common law right that anyone could take action on behalf of the company.[2055] Section 165 however makes provision for wide legal standing to force the company to institute an action, for example when a duty of care in relation to cybersecurity was not exercised properly, or to take action to protect the company's interests, for example when a company's online platform and its online databases need to be properly protected.[2056]

In addition, a director may also be held liable for a civil action in terms of the Act.[2057] In this regard, section 218(2) determines that anyone who contravenes any section of the Act is liable to any other person for any damage that such a person suffered as a result.[2058] In this regard, the basis of the claim is a loss that class members suffered, which differs from the loss that the company suffered.[2059] This differs from section 20(6), which does not give shareholders the opportunity to claim for such losses.[2060] The courts have explained in *De Bruyn supra* and *Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*, that the wording of section 218(2) can be interpreted widely in terms of the individuals who fall within its ambit.[2061]

In terms of the SA POPI 4 of 2013, section 40, the IR is mandated (d) to process complaints and (i) to investigate complaints on violations of privacy/and personal information; (ii) to gather information in order to investigate such violations; (iii) to try and resolve complaints through ADR mechanisms; and (iv) to serve any notices in

---

[2051] The Act, sections 76(3)(c); 77; 77(2)(b).
[2052] *Ibid.*
[2053] The Act, section 165; Blackman *et al. op cit* 9-178.
[2054] The Act, sections 20(6)(a)-(b); 218(2).
[2055] The Act, section 165.
[2056] *Ibid.*
[2057] The Act, section 218(2).
[2058] The Act, section 218(2); Cassim *et al. Contemporary Company Law op cit* 1129.
[2059] The Act, section 218(3); Cassim *et al. Contemporary Company Law op cit* 874 - 875.
[2060] The Act, sections 20(6); 218(3); Cassim *et al. Contemporary Company Law op cit* 875.
[2061] The Act, section 218(2); *De Bruyn supra*, paras 188 - 190; *Hlumisa Investment Holdings (RF) Ltd (No. 2) supra*, paras 9; 31 – 32; 38 – 39; Cassim *et al. Contemporary Company Law op cit* 373.

terms of this Act.[2062] Chapter 11 of this Act allows affected parties to keep the directors liable for the loss of their privacy and/or personal information.[2063]

In terms of the SA Criminal Procedure Act 51 of 1977, section 332(1), criminal proceedings may also be instituted against a company or its directors.[2064] Both may be prosecuted for any common law offence.[2065]

Directors are also still exposed to the common law duty of care, as well as a common law personal action.

Although the Act partially codified the directors' duty of care, the common law duty of care still applies.[2066] A breach of the directors' common law duty of care could lead to claims against directors in contract or tort.[2067] This is because the Act, section 128(2) determines that anyone who contravenes any section of the Act is liable to anyone else who have experienced a loss or damage as a consequence.[2068]

When a shareholder experienced a loss and they want to exercise their individual shareholder rights, they can also institute a common law personal action in their own name.[2069] The Act preserves the personal action.[2070] Section 77(2)(b) states that a director's liability for the breach of their common law duty of care is delictual in nature.[2071] In this regard, the most applicable delict will be the *Actio Legis Aquiliae*.[2072]

Whenever a company concluded a contract with a director, and that contract contains a provision that requires that director to exercise a certain standard of care in relation to cybersecurity, the breach of such a duty will be contractual in nature.[2073]

SA law allows the same set of facts to be used for a delictual claim as well as a contractual claim and the plaintiff may decide which one of the two they will use.[2074] This is called a *concursus actionum* and is only present when the separate requirements of both a contractual action as well as a delictual action have been fulfilled.[2075]

Liability in terms of the duty of care in relation to cybersecurity and the use of AI may also derive from corporate governance guidance, stock exchange listing

---

[2062] SA POPI 4 of 2013, section 40(d)(i)-(iii).
[2063] SA POPI 4 of 2013, Chapter 11.
[2064] SA Criminal Procedure Act 51 of 1977, section 332(1).
[2065] Farisani 'The Regulation of Corporate Criminal Liability in SA: A Close Look' in *Obiter* (January 2006) 264.
[2066] Blackman *et al. op cit* 8-29; Faris *et al. The Law of SA* (LAWSA) (Companies) 4(2), par. 116; Delport *et al. Henochsberg on the Companies op cit* 288.
[2067] *Ibid.*
[2068] The Act, section 128(2).
[2069] Cassim *et al. Contemporary Company Law op cit* 1131.
[2070] *Ibid*.
[2071] The Act, section 77(2)(b).
[2072] *Du Plessis NO supra*; See Chapter 3, section 2.1.
[2073] Cassim *et al. Contemporary Company Law op cit* 1132.
[2074] Mabunda *op cit* 75; Mupangavanhu op cit 192; Price *op cit* 501.
[2075] *Ibid.*

requirements, and industry regulators.[2076] Where such guidance or regulations may not always have the force of law, the courts may use them to help determine the standard of reasonable care, skill and diligence that are required of directors when they exercise their duty of care in relation to cybersecurity.[2077]

In this regard, King Report IV explains that if the recommendations on good corporate governance are more regularly used by directors in practice, it will enhance the possibility that a court will consider such recommendations to set a standard on the nature of care that is required on a certain aspect pertaining to corporate governance.[2078] Consequently, the recommendations of voluntary corporate governance guidelines could be used in case law and could in such a way become part of the common law over time.[2079] As a result, directors could then be held liable when they do not comply with an established corporate governance practice, even if such practice is not codified.[2080]

In addition, the JSE '*Listing Requirements*,' section 3.84 states that any listed company will also have to conform with the King Code if they want to be listed on the JSE, and trade their shares there.[2081]

Lastly, although it depends on the regulatory framework and industry of an affected company, interested and affected parties can also lay complaints at the SA CIPC who will then investigate and take action against a company or its directors.[2082]

5.3. Recommendations on How Directors' Use of AI Should Be Regulated in the SA Cybercrimes Act 19 of 2020 and the King Code

It is a shortcoming in the SA privacy law and cybersecurity regime that the SA Cybercrimes Act 19 of 2020 does not especially prohibit the use of AI to commit cybercrimes, and that the King Code does not encourage the responsible use of AI to fight cybercrime towards SA companies.[2083]

There are six ways in which SA directors can use AI and Blockchain technology to enhance cyberresilience, but not all of them fulfil the requirements that the Act requires for the way in which directors need to exercise their duty of care. It is as a result important to pay careful attention to the advantages and disadvantages of each of these types of AI.

[2076] See Chapter 1, section 6.4.
[2077] *Ibid.*
[2078] IoDSA '*King Report IV*' *op cit* 35.
[2079] *Ibid.*
[2080] *Ibid.*
[2081] JSE '*Listing Requirements*,' section 3.84.
[2082] SA CIPC *op cit s.p*.
[2083] SA Cybercrimes Act 19 of 2020.

The first way in which directors can integrate AI to improve their company's cyberresilience is through Consultative AI.[2084] Consultative AI also uses algorithms to assist natural intelligence without substituting the director.[2085] As a result, the use of this type of AI would not release a director from their duty of care.[2086] It can assist directors with reaching decisions that require creative thinking, and it can ask questions that relate to various scenarios and then provide answers on those questions based on those and other scenarios.[2087] It can assist directors by drawing insights and answers from patterns of data that would otherwise be hard for directors to determine.[2088]

The King Code should allow SA directors to use Consultative AI when they use algorithms to exercise their duty of care in relation to cybersecurity.[2089] The function of the algorithm that Consultative AI uses will help to give effect to the Act, section 7(b), which states that the Act aims to (i) promote the development of the SA economy by encouraging high standards of corporate governance; and to (ii) balance the rights and obligations of directors and shareholders.[2090] The use of Consultative AI could therefore help to balance the rights and obligations of directors and shareholders and help to minimise bias, since the algorithm can be programmed to objectively evaluate a certain scenario, and it wil then as a result not be susceptible to the subjective influence of a director in the recommendation that it provides.[2091] The use of Consultative AI is permissible, since it only provides recommendations, which are then subject to the directors' approval.[2092] Its use still allows directors to add their own insights to that recommendation, and to then maybe make another conclusion.[2093] Directors can also use it to make better-informed decisions that will help to bring a company more in accordance to the requirements of the Act and the King Code.[2094] Since the Act prescribes the enlightened shareholder value approach, Consultative AI can be programmed to take various stakeholders' interests into account and to prevent bias.[2095]

The second one is Supportive AI, where the AI helps to perform certain tasks, but where the machine does not substitute a director.[2096] It was explained that it can do

---

[2084] Chitimira *et al. op cit* 6 – 7; Hassani *et al. op cit* 147; Petrin *op cit* 981 - 984.
[2085] *Ibid*.
[2086] *Ibid*.
[2087] *Ibid*.
[2088] *Ibid*.
[2089] Can Kaya *op cit* 7 – 8.
[2090] The Act, sections 7(b)(i)-(ii).
[2091] Chitimira *et al. op cit* 6 – 7.
[2092] *Ibid.*
[2093] *Ibid*.
[2094] The Act, sections (7(a); (d); (i); IoDSA '*King Report IV' op cit* principle 8.3; Petrin *op cit* 970.
[2095] Can Kaya *op cit* 5 – 6; Delport *et al.* 'The Protection of Stakeholders: The SA Social and Ethics Committee and the UK's Enlightened Shareholder Approach, Part 1' *op cit* 97.
[2096] Chitimira *et al. op cit* 5 – 11; Petrin *op cit* 980.

administrative tasks and that it could also be used to do research on items for OMs and to give informed opinions.[2097]

The third possibility, Self-Aware AI, and the dangers that it presents, were especially accentuated.[2098] It was explained that the problem with this is that its algorithms takes on human functions and then basically substitute a director with AI.[2099] It would however not be possible to use this type of AI to assume the role of a director or to replace them, since the Act, section 69(7) only allows natural persons to be directors.[2100] The King Code should thus explain that the use of Self-Aware AI is not permissible if it is used to substitute directors. Another reason why Self-Aware AI should be prohibited is because the substitution of human directors with AI would lead to legal uncertainty whenever liability has to be determined when the duty of care was not properly exercised.[2101] The court will be confronted with many questions when they need to determine the liability of AI, such as whether they should be held liable in terms of contract or delict? This would be difficult to answer, because in such instances, board decisions would not be made by independent, free-thinking directors, but by algorithms.[2102] In order to then determine whether the duty of care in relation to cybersecurity was performed properly, the court would then have to determine whether the directors' decision was in fact made by the designer of the algorithm, the programme developer, the machine itself or the supplier.[2103] The legislature will also have to determine what types of AI directors may use, before they are held liable for not exercising their duty of care properly.[2104] Should Self-Aware AI ever replace directors, it could would undermine the diversity of the board, since human characteristics, which contributes to diversity, such as gender and race, would then be circumvented, and this would adversely affect the quality of the board's decisions.[2105]

The fourth way in which directors can integrate AI to enhance their company's cyberresilience is through Data Analysis.[2106] Big Data is volumes of data which are too large to be processed by traditional methods.[2107] Directors should however also be cautious when they use Data Analysis, because there are different versions that make use of descriptive AI, predictive AI and prescriptive AI.[2108] The King Code should

---

[2097] The Act, section 76(4)(a).
[2098] Chitimira *et al. op cit* 7; Can Kaya *op cit* 7 – 8.
[2099] *Ibid.*
[2100] The Act, section 69(7).
[2101] Can Kaya *et al. op cit* 7 – 8; Chitimira *et al. op cit* 7.
[2102] *Ibid.*
[2103] *Ibid*.
[2104] *Ibid.*
[2105] *Ibid*.
[2106] Boura *et al. op cit* 261; Chitimira *et al. op cit* 9 – 11.
[2107] *Ibid.*
[2108] Boura *et al. op cit* 262 – 263; Chitimira *et al. op cit* 9 – 11.

prohibit the use of prescriptive Data Analysis, because a situation cannot be allowed where Data Analysis prescribes the decisions that directors need to take.

It was explained, fifthly, that due to information-overload, directors may use CCC to make evaluations, to gain proper insights and to obtain advice of all the relevant business reports and corporate governance principles when they need to make a business decision, usually within a specific time.[2109] A director can ask it any question in a certain field, such as cybersecurity, and get an instantaneous reply.[2110] It can also access agendas and minutes of any previous OM and answer questions related to it.[2111] CCC can also sort lots of data and it can learn itself new tasks related to the management thereof.[2112] It can also start its own database and create hypotheses in order to provide answers for questions which it is asked.[2113] As a cognitive system, CCC is able to understand highly-technical terms and industry jargon and is able to predict scenarios and to provide instant unbiased answers to the questions of directors within a certain field, and thereby allow them to make better-informed business decisions in terms of cybersecurity.[2114]

Sixthly, it was explained that although the public ledger system is an essential characteristic of Blockchain technology, Private Blockchain could be used (as in the case of Strate) to encrypt all personal information on the public ledgers.[2115] An individual relevant shareholder or stakeholder could then get limited access to their own PII, and all their sensitive information would stay private.[2116] It was explained that the King Code will have to provide guidance to directors on how to use Blockchain technology and require directors to ensure that there is limited access to the ledgers, that personal information is encrypted and that only individual relevant shareholders/stakeholders can access their own personal information.[2117]

AI can however also be subject to bias, which could be caused by either design bias or biased information.[2118] This should be prohibited since it could lead to misleading recommendations.[2119] Directors will not exercise due care if they rely on AI recommendations that are biased.[2120] These problems should be addressed in the King

---

[2109] Bowles *et al. op cit* 2; Chitimira *et al. op cit* 20.
[2110] Bowles et al. op cit 6.
[2111] *Ibid.*
[2112] Noor *op cit* 76 - 77.
[2113] *Ibid.*
[2114] Noor *et al.* 77.
[2115] Anwar *op cit s.p.*; Geroni *op cit s.p*.
[2116] Anwar *op cit s.p.*
[2117] *Ibid.*
[2118] Berendt *et al. op cit* 3; Chitimira *et al. op cit* 11 – 12; Weiss *et al. op cit* 5366.
[2119] Weiss *et al. op cit* 5366.
[2120] *Ibid.*

Code since AI should not be used to substitute a director and perform their duties on their behalf, and it also should not be used to make misleading recommendations.[2121]

It is also important to look at how directors should exercise their duty of care in relation to cybersecurity and the use of AI in terms of the King Code's principles. King Report IV explains that the board must govern ethics to make sure that the ethical culture within a company is in line with the board's vision.[2122] This is done through the implementation of proper cybersecurity policies and systems.[2123] It is therefore the responsibility of the board to ensure that the use of AI aligns with the company's ethical culture.[2124]

King Report IV, principles 1 - 3 explains how directors should align cybersecurity advancement such as AI with ethical principles: in terms of Principle 1, which requires ethical leadership, the board will have to determine the vision and provide leadership and guidance on how the company should use AI.[2125]

In terms of Principle 2, which requires organisational ethics, culture and values, the board will have to ensure that the company's code of ethics and code of conduct guide the responsible development of cybersecurity measures and AI, including when to use and not to use AI.[2126]

Principle 3 requires the board to practice governance that demonstrate the company's good corporate citizenship.[2127] It must ensure that AI complies with the SA Constitution of 1996, laws and standards as well as company policies and procedures, strategy, and the company's codes of conduct and ethics.[2128] The board should thus also ensure that AI helps the company to improve the well-being of the environment and society in which the company finds itself.[2129] This will ensure that data biases, privacy and racial discrimination, are addressed in all cybersecurity development stages and further provide buy-in from both shareholders and stakeholders.[2130]

It was also said that directors' use of AI to help make decisions will not be a quick solution to help improve cybersecurity, because of all of AI's ethical and moral issues.[2131] The ethical and moral issues are very complex and need to be addressed by the SA Cybercrimes Act 19 of 2020 and the King Code while AI is still busy developing.[2132]

[2121] Weiss *et al. op cit* 5366.
[2122] IoDSA '*The Role of the Board in Organisational Ethics*' *op cit s.p*; Naidoo *op cit* 48.
[2123] IoDSA '*King Report IV*' *op cit* 44.
[2124] *Ibid.*
[2125] IoDSA '*King Report IV*' *op cit* principle 1, 43.
[2126] IoDSA '*King Report IV*' *op cit* principle 2, 44.
[2127] IoDSA '*King Report IV*' *op cit* principle 3, 44.
[2128] IoDSA '*King Report IV*' *op cit* principle 3, 44.
[2129] *Ibid.*
[2130] *Ibid.*
[2131] IoDSA '*The Role of the Board in Organisational Ethics*' *op cit s.p*.
[2132] *Ibid.*

6. THE DISTINCTION BETWEEN THE PROPOSED LEGAL REGULATION OF AI IN THE SA CYBERCRIMES ACT 19 OF 2020 AND ITS REGULATION BY MEANS OF CORPORATE GOVERNANCE GUIDANCE IN THE KING CODE

It is important to also explain the distinction between corporate governance and legal regulation and how these areas interact. The question is how can the use of AI best be regulated – by legislation or corporate governance guidelines?[2133]

Legislation is rigid, while cyberrisks and cybersecurity systems are always changing.[2134]

The SA legislature cannot compile legislation or regulations that enumerate all the relevant aspects of AI because business practices, IT, the types of cyberbreaches and anti-hacking software evolve way too fast for this approach.[2135] Policy on cybersecurity, and especially AI, must as a result remain nimble.[2136]

So what is then best in this context?[2137]

What is needed is for the SA Cybercrimes Act 19 of 2020 to be updated to clearly prohibit the use of AI to commit cybercrime.

At the same time, the King Code should be updated to encourage directors to use AI responsibly, and should make provision for the use of Consultative AI, Supportive AI, Data Analysis and Blockchain technology with encrypted ledgers, to be used to assist directors when they exercise their duty of care in relation to cybersecurity. The use of Self-Aware AI should however be strictly prohibited, as this will result in the replacement of human directors with AI. Prescriptive Data Analysis should also be prohibited because a situation cannot be allowed where AI prescribes the decisions that directors need to take.

A corporate governance guideline such as the King Code has many advantages: it takes a less rigid and a more dynamic approach than a pure rules-based framework.[2138] It is flexible, and it also provides legal clarity.[2139] It helps directors to oversee that compliance processes meet legislation, and it is also flexible enough to be extended in the future.[2140] It also helps to detail legislation and explain best practices.[2141] A further advantage is that it is not compiled by the legislative process or

---

[2133] Frankel *Fiduciary Law* 96.
[2134] Furlow 'Good Faith, Fiduciary Duties and the BJR in Delaware' in *Utah Law Review* (2009) 1067.
[2135] Harner *op cit* 21.
[2136] *Ibid.*
[2137] Harner *op cit* 22.
[2138] Amodu op cit 2; Harner *op cit* 22.
[2139] Harner *op cit* 22.
[2140] Privacy International *op cit s.p*.
[2141] Advanced National Network for Administrators (ANNA) '*On the Legal Status of Guidelines,*' *s.p.*, available online at <http://www.annamsw.eu/news/117-on-the-legal-status-of-guidelines.html>, last accessed on 5 July 2020.

rule-making procedure and can thus be drafted much faster.[2142] It is also possible to obtain public input during its compilation process, but this will not award it the force of law.[2143] Although a board cannot 'violate' corporate governance guidelines, they do serve as examples of best practices and provide guidance on the compliance with various laws and regulations.[2144]

The disadvantage of corporate governance guidelines such as the King Code is however that companies will not be subject to an enforcement action when they do not comply with it. However, it must be kept in mind that King Reports I - IV set the corporate governance framework in SA and although they contain a voluntary set of corporate governance principles, compliance for listed companies is compulsory in terms of the JSE '*Listing Requirements*,' section 3.84.[2145]

Examples of corporate governance guidelines include advisories, bulletins, circulars, frequently-asked-questions, guidelines in booklet form, interdepartmental statements, policy statements and staff guidance statements.[2146] Although the King Code is produced in report format, it can easily be supplemented by some of the above-mentioned sources in future when a new cyberthreat emerges.

The inclusion of the use and regulation of AI in the King Code should be based on the broad ideas that relate to the directors' duty of care in relation to cybersecurity as influenced by the Constitution, the Act, King Reports I - IV, case law, corporate governance codes, best practices and relevant international sources.[2147]

By being compiled in a corporate governance guideline format, the King Code allows companies to compile their own cybersecurity policy on how their board interprets the provisions that relate to the use and regulation of AI, and the King Code can as a result be used as a basis for company-specific 'AI Policies'.[2148]

Since each company's budget, cyberassets and cyberrisks differ from each other, the King Code should take this into account.[2149] Since there is no one-size-fits-all solution to cybersecurity, the King Code should be updated in a way that will guide the executive and non-executive directors of all types of companies, large and small, listed and unlisted, private companies and public companies to oversee the responsible use of AI in an easy-to-understand manner.[2150] In addition, since the violation of privacy

---

[2142] ANNA *op cit s.p.*
[2143] *Ibid.*
[2144] *Ibid.*
[2145] JSE '*Listing Requirements' op cit* section 3.84.
[2146] ANNA *op cit s.p.*
[2147] SA Constitution, The Act, IoDSA '*King Reports I – IV*' *op cit s.p.*
[2148] Education and Training Unit (ETU) for Democracy Development '*The Policy and Law-Making Process,' s.p.*, available online at <https://www.etu.org.za/toolbox/docs/govern/policy.html>, last accessed on 5 July 2020.
[2149] Asgarian *et al.* '*Cyber Security: The Evolving Nature of a Director's Duty,' s.p.*, available online at <https://www.mondaq.com/guernsey/offshore-financial-centres/633480/cyber-security-the-evolving-nature-of-a-director39s-duty>, last accessed on 26 May 2021.
[2150] *Ibid.*

and/or personal information presents different kinds of harm, the use and regulation of AI should also make provision for different levels of cybersecurity according to the sector in which a company finds itself.[2151]

7. SUMMARY OF RECOMMENDATIONS

In terms of the recommendations on the adequacy of the SA privacy law and cybercrimes regimes and the way in which they are enforced, it was explained that is a shortcoming of the SA Cybercrimes Act 19 of 2020 that it does not especially prohibit the use of AI to commit cybercrimes, and also that the King Code does not make provision for the responsible use of AI to fight cybercrime towards SA companies.[2152]

In terms of the recommendations on the further accountability mechanisms to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI, it was explained that liability in terms of the duty of care in relation to cybersecurity and the use of AI may also derive from corporate governance guidance, stock exchange listing requirements, and industry regulators.[2153]

In this regard, King Report IV explains that if the recommendations on good corporate governance are more regularly used by directors in practice, it will enhance the possibility that a court will consider such recommendations to set a standard on the nature of care that is required on a certain aspect pertaining to corporate governance.[2154] If the King Commission could consequently provide a more detailed treatment of directors' duty of care in relation to cybersecurity and the responsible use of AI, such recommendations of voluntary corporate governance guidelines could be used in case law and could in such a way become part of the common law over time.[2155] As a result, directors could then be held liable when they do not comply with an established corporate governance practice, even if such practice is not codified.[2156]

It was explained that there are six ways in which SA directors can use AI and Blockchain technology to enhance cyberresilience, but not all of them fulfil the requirements that the Act requires for the way in which directors need to exercise their duty of care. It is as a result important to pay careful attention to the advantages and disadvantages of each of these types of AI.

[2151] Working Group 11 on Data Security and Privacy Liability (WG11) '*The Sedona Conference, Commentary on a Reasonable Security Test,'* 27, available online at <https://thesedonaconference.org/node/9702>, last accessed on 1 March 2022.
[2152] SA Cybercrimes Act 19 of 2020.
[2153] See Chapter 1, section 6.4.
[2154] IoDSA '*King Report IV' op cit* 35.
[2155] *Ibid.*
[2156] *Ibid.*

The first way in which directors can integrate AI to improve their company's cyberresilience is through Consultative AI.[2157] Consultative AI also uses algorithms to assist natural intelligence without substituting the director.[2158] It was explained that this type of AI also conforms to the requirements of the Act.

The second one is Supportive AI, where the AI helps to perform certain tasks, but where the machine does not substitute a director.[2159] It was explained that this type of AI conforms to the requirements of the Act.

The third possibility, Self-Aware AI, and the dangers that it presents, were especially accentuated.[2160] It was explained that the problem with this is that its algorithms takes on human functions and then basically substitute a director with AI.[2161] It was explained that it would however not be possible to use this type of AI to assume the role of a director or to replace them, since the Act, section 69(7) only allows natural persons to be directors.[2162]

The fourth way in which directors can integrate AI to enhance their company's cyberresilience is through Data Analysis to analyse data that is too large to be processed by traditional methods.[2163] Directors should however also be cautious when they use Data Analysis, because there are different versions that make use of descriptive AI, predictive AI and prescriptive AI.[2164] The King Code should prohibit the use of prescriptive Data Analysis, because a situation cannot be allowed where Data Analysis prescribes the decisions that directors need to take.

It was explained, fifthly, that due to information-overload, directors may use CCC to make evaluations, to gain proper insights and to obtain advice of all the relevant business reports and corporate governance principles when they need to make a business decision, usually within a specific time.[2165] A director can ask it any question in a certain field, such as cybersecurity, and get an instantaneous reply.[2166] It can also access agendas and minutes of any previous OM and answer questions related to it.[2167] CCC can also sort lots of data and it can learn itself new tasks related to the management thereof.[2168] It can also start its own database and create hypotheses in order to provide answers for questions which it is asked.[2169] As a cognitive system, CCC

[2157] Chitimira *et al. op cit* 6 – 7; Hassani *et al. op cit* 147; Petrin *op cit* 982.
[2158] *Ibid.*
[2159] Chitimira *et al. op cit* 5 – 11; Petrin *op cit* 980.
[2160] Chitimira *et al. op cit* 7; Can Kaya *op cit* 7 – 8.
[2161] *Ibid.*
[2162] The Act, section 69(7).
[2163] Boura *et al. op cit* 261 - 263; Chitimira *et al. op cit* 9 – 11.
[2164] *Ibid*.
[2165] Bowles *et al. op cit* 2; Chitimira *et al. op cit* 20.
[2166] Bowles et al. op cit 6.
[2167] *Ibid.*
[2168] Noor *op cit* 76 - 77.
[2169] *Ibid.*

is able to understand highly-technical terms and industry jargon and is able to predict scenarios and to provide instant unbiased answers to the questions of directors within a certain field, and thereby allow them to make better-informed business decisions in terms of cybersecurity.[2170]

Sixthly, it was explained that although the public ledger system is an essential characteristic of Blockchain technology, Private Blockchain could be used (as in the case of Strate) to encrypt all personal information on the public ledgers.[2171] An individual relevant shareholder or stakeholder could then get limited access to their own PII, and all their sensitive information would stay private.[2172] It was explained that the King Code will have to provide guidance to directors on how to use Blockchain technology and require directors to ensure that there is limited access to the ledgers, that personal information is encrypted and that only individual relevant shareholders/stakeholders can access their own personal information.[2173]

AI can however also be subject to bias, which could be caused by either design bias or biased information.[2174] This should be prohibited since it could lead to misleading recommendations.[2175] Directors will not exercise due care if they rely on AI recommendations that are biased.[2176] These problems should be addressed in the King Code since AI should not be used to substitute a director and perform their duties on their behalf, and it also should not be used to make misleading recommendations.[2177]

Shareholders/stakeholders should not be complacent and they could also start to push internally and request directors to increase their safety protocols when it comes to cybersecurity.[2178] Holding the board to a higher standard of oversight on cybersecurity in a company could start when just one shareholder or stakeholder makes a proposal at a company meeting that the company must start to use AI responsibly and that directors need to integrate it when they exercise their duty of care in relation to cybersecurity.[2179]

8. FINAL REMARKS

SA has one of the highest rates of cybercrime in the world and SA companies' cyberassets are vulnerable to cyberattacks. Since SA companies' OMs are conducted on an online platform and use online databases that contain sensitive PII, they are

---

[2170] Noor *et al.* 77.
[2171] Anwar *op cit s.p.*; Geroni *op cit s.p*.
[2172] Anwar *op cit s.p.*
[2173] *Ibid.*
[2174] Berendt *et al. op cit* 3; Chitimira *et al. op cit* 11 – 12; Weiss *et al. op cit* 5366.
[2175] Weiss *et al. op cit* 5366.
[2176] *Ibid.*
[2177] *Ibid.*
[2178] Ali *et al.* 'A Legal Perspective of Shareholders' Meetings in the Globalised and Interconnected Business Environment' 764.
[2179] *Ibid*.

particularly prone to cyberattacks. AI could however be used to resist cyberattacks on a company's cyberassets, such as its online platform and its online databases. Contrariwise, AI could be used by cybercriminals to instigate cyberattacks in order to obtain intellectual property or PII.

It was explained against this background that especially the online platform and its online databases that contain personal information of shareholders and stakeholders need to be properly protected against cyberbreaches, since directors could be held liable on numerous counts in the event that they did not exercise due care in relation to cybersecurity, and a cyberbreach then occured that compromised the PII.

This thesis critically analysed how a more detailed treatment of the directors' duty of care in relation to cybersecurity can help to make SA companies more cyberresilient, with the specific focus on their OMs, as well as the role that the use of AI, and its regulation, can play in this regard.

This topic had to be undertaken in order to lessen the potential for cyberattacks on SA companies and to help them improve their cyberresilience.

Where other researchers looked at OMs as a means to enhance corporate governance CSR, they have failed to look at the dangers that cybercrime present to OMs and that directors may be held personally liable in the event that a company's cybersecurity was inadequate to thwart a cyberattack and the company's cyberassets were compromised.

In addition, where other researchers only looked at OMs as a tool to improve corporate governance and CSR, this thesis explained that a more detailed treatment of the directors' duty of care in relation to cybersecurity and the use of AI will improve companies' cyberresilience and will especially help to make their OMs more cyberresilient.

The problem of cybercrime in SA is further worsened by a lack of detailed treatment of cybersecurity in corporate governance guidance, and as a result, it was uncertain until now with this research how directors should properly integrate AI when they exercise their duty of care in relation to cybersecurity.

By means of legal comparison, this thesis critically analysed how directors need to exercise their duty of care in relation to cybersecurity in order to help make SA companies more cyberresilient.

Chapter 2 evaluated how OMs are regulated in other jurisdictions. It started with a short historical overview of OMs and looked at the advent of OMs in SA. It then looked at how OMs themselves are regulated in the US, with its federal and state law, the UK and what the SA legal position on OMs is. This Chapter drew lessons for SA on how OMs are regulated in other jurisdictions, and what the best practices on the regulation of OMs are, in order to understand how to best protect the integrity of the OM, as well as the cybersecurity of the online platform and its online databases.

Chapter 3 outlined the directors' duty of care in relation to cybersecurity. A specific focus was placed on the UK and US positions on the duty of care in relation to cybersecurity in order to contrast it to the SA position by means of a legal comparison. Attention was also given to the remedies for directors who breached their duty of care in relation to cybersecurity. The position of non-executive directors was also looked at in order to make it representative of the legal position of all directors. Lastly, lessons from the legal comparison of the SA, UK and US duty of care in relation to cybersecurity were looked at in order to understand how these different legal sources help to provide context for how the SA duty of care in relation to cybersecurity should be interpreted.

Chapter 4 looked at the indirect impact of the directors' duty of care in relation to cybersecurity on corporate governance and CSR and ESG investment considerations. It started by looking at the evolution of the emphasis on CSR to sustainability to ESG considerations. Then it looked at the exercise of SA directors' duty of care in terms of corporate governance and CSR. Then it looked at how SA directors should exercise their duty of care in terms of ESG considerations. Specific attention was given to the exercise of the directors' duty of care in relation to cybersecurity and the use of AI and Blockchain technology since this is a new field that is developing fast and directors will need to address the challenges that they present. Lastly, lessons were drawn on how the duty of care in relation to cybersecurity could help to improve corporate governance, CSR and ESG considerations at SA OMs.

Chapter 5 built on the analysis offered in Chapters 2, 3 and 4 and looked at the further accountability mechanisms to hold directors accountable for the way in which they exercise their duty of care in relation to cybersecurity and the use of AI. It is important that directors have a proper understanding of these various accountability mechanisms in order to limit the possibility that they could be held liable for not exercising their duty of care in relation to cybersecurity properly. It began by also giving an overview of both the international and SA privacy law and cybersecurity regimes. It then focused on directors' liability in terms of the duty of care in relation to cybersecurity and the use of AI. Lastly, it looked at the lessons how the use of AI should be regulated in the SA Cybercrimes Act 19 of 2020 and the King Code.

This thesis showed that fortunately boards can take proactive steps to improve their duty of care in relation to cybersecurity by the use of AI and thus reduce liabilities without imposing unreasonable burdens on themselves.[2180] The compilation and implementation of a company-specific cybersecurity policy and system that includes the use of AI, based on the lessons shown in this thesis, will be a good start.[2181] Although

---

[2180] Lunn *op cit* 20.

[2181] Organisation of American States (OAS) *Cyberrisk Oversight Handbook for Corporate Boards,* 12, available online at <https://webcache.googleusercontent.com/search?q=cache:zilNEoUGzVMJ:https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf+&cd=1&hl=en&ct=clnk&gl=za>, last accessed on 14 July 2021.

directors do not have to be cybersecurity experts, they are fully expected to seek help to implement and oversee a proper cybersecurity policy and system, and to seek advice on how to use AI to make their companies more cyberresilient.[2182] It was explained that for directors to avoid liability, a court will need to find that the board used a rational process to compile and implement its cybersecurity policy and system, that it exercised effective oversight thereon by staying well-informed on the company's cybersecurity challenges, and that their decisions on cybersecurity was an outcome of a process that was followed with due care. Directors need to remember that they have to be proactive in their oversight, and not idle and hope that a cyberbreach does not occur and in this regard the use of AI will be helpful.[2183]

With the potential of future outbreaks of Covid-19 and the reinstitution of Lockdown regulations, it can be expected that a ban on public meetings, restrictions on travel, self-isolation and social distancing can be re-instituted on very short notice.[2184] With continuing self-isolation and work from home, SA companies will have to adapt their approach to online solutions.[2185] The groundwork already laid by the JSE with its online platform in a short space of time will help more companies to hold their OMs, while the reinstitution of Lockdown regulations could mean that directors, management and employees will have to continue to work remotely and shareholders and stakeholders will not always be allowed to travel inter/nationally.[2186] All that is now needed is that the SA Cybercrimes Act 19 of 2020 should be updated to prohibit the use of AI to commit cybercrime, and that the King Code should be updated to encourage directors to use AI responsibly to combat cybercrime, since AI is an important tool for directors in the fight against cybercrime. By doing so, the SA legislature and the King Committee will also help to prevent that the company, the board and directors could be held liable in the event of a cyberbreach. In addition, it is submitted that these measures will contribute to help resist cyberbreaches in SA and to help build cyberresilience and increase cybersecurity at SA companies, and especially their OMs.

[2182] Lunn *op cit* 21.
[2183] US FTC '*Fighting Identity Theft with the 'Red Flag' Rule' op cit s.p.*
[2184] Chalwin-Milton *op cit s.p*.
[2185] *Ibid*.
[2186] JSE '*JSE and TMS Launch First Virtual AGMs Enabling Clients to Engage with Shareholder' op cit s.p*.

BIBLIOGRAPHY

I. BOOKS

Baker, D. *et al. AI and the Law: Cybercrime and Criminal Liability*, Routledge Publishers, Oxford, 2021.

Berkowitz, M. *AI, Machine Learning and Big Data 2021*, Global Legal Group, London, 2021.

Blackman, M. *et al. Commentary on the Companies Act*, Juta & Co, Cape Town, 2017.

Bowles, A. *et al. Cognitive Computing and Big Data Analytics*, Wiley Publishers, New York, 2015.

Cassim, F. *et al. Contemporary Company Law*, Juta Publishers, Cape Town, 2021.

Cassim, M. *et al. The New Derivative Action under the Companies Act: Guidelines for Judicial Discretion*, Juta Publishers, Cape Town, 2016.

Claessens, S. *et al. Corporate Governance & Development: An Update*, A Global Corporate Governance Forum Publication, International Finance Corporation, Washington, DC, 2012.

Delport, P (ed.) *Henochsberg on the Companies Act 71 of 2008*, LexisNexis Publishers, Johanesburg, 2021.

Du Plessis, J. *et al. Principles of Contemporary Corporate Governance* Cambridge University Press, Cambridge, 2018.

Faris, J. *et al. The Law of SA* (LAWSA) (Companies) LexisNexis Publishers, Johannesburg (updated).

Frankel, T. *Fiduciary Law* Oxford University Press, NY, 2011.

Garner, B. *et. al. Black's Law Dictionary* Thomson-West Publishers, St Paul, 2009.

Hamm, S. *et al. Smart Machines: IBM's Watson and the Era of Cognitive Computing*, Columbia Business School Publishing, New York, 2013.

Hebb, T. *et al. The Routledge Handbook of Responsible Investment*, Routledge Publishers, London, 2016.

Keay, A. *Board Accountability on Corporate Governance*, Routledge Publishers, Oxford, 2015.

Keay, A. *The Enlightened Shareholder Value and Corporate Governance*, Routledge Publisher, Oxford, 2013.

Kershaw, D. *The Foundations of Anglo-American Fiduciary Law*, Cambridge University Press, Cambridge, 2018.

Loughrey, J. *Business Judgment and Director Accountability*, Edgar Elgar Publishing, Cheltenham, 2022

Loughrey, J. *Directors' Duties and Shareholder Litigation in the Wake of the Financial Crisis*, Edgar Elgan Publishers, Cheltenham, 2013.

McIntosh, C. *et al. Cambridge Advanced Learner's Dictionary*, Cambridge University Press, Cambridge, 2008.

Midgley, J. *et al. Principles of Delict* LexisNexis Publishers, Durban, 2016.

Miles, L. *et al. Corporate Governance*, Cavendish Publishing, London, 2003.

Morris, N *et al. Capital Failure: Rebuilding Trust in Financial Services*, Oxford University Press, Oxford, 2014.

Naidoo, R. *Corporate Governance: An Essential Guide for Companies*, LexisNexis Publishers, Durban, 2016.

Neethling, J. *et al. Deliktereg*, LexisNexis Publishers, Johannesburg, 2015.

Neethling, J. *et al. Neethling on Personality Rights*, LexisNexis Publishers, Johannesburg, 2018.

Papadopoulos, S. *et al. Cyberlaw @SA III*, Van Schaik Publishers, Pretoria, 2012.

Pitts, V. *Cybercrimes: A History of the World's Worst Cyberattacks*, Alpha Editions, New Delhi, 2016.

Thornton, L. *et al. Telecommunications Law in SA*, STE Publishers, Johannesburg, 2006.

Vacca, J. *Guide to Wireless Network Security*, Springer Publishers, New York, 2006.

Van der Merwe, D. *et al. Information and Communications Technology Law*. LexisNexis Publishers, Johannesburg, 2022.

Wells, J. *Internet Fraud Casebook*, Wiley Publishers, New York, 2010\.

Wiese, T. *Corporate Governance in South Africa: With International Perspectives* Juta Publishers, Cape Town, 2017.

II. RESEARCH DISSERTATIONS

Chakanika, A. *Corporate Governance in SA: Progress and Challenges*, LLM submitted at the University of Cape Town, 2013.

Eisele, S. *Codification of the BJR in the SA Companies Act 2008, Section 76(4)*, LLM thesis submitted at the University of Stellenbosch, 2017.

Kondlo, N. *The Importance of Corporate Governance in SA Family-Owned Companies* University of the Western Cape, 2016.

Leach, J. *The Correct Understanding of the BJR in the Companies Act 71 of 2008, Section 76(4): Avoiding the American Mistakes*, LLM Thesis submitted at the University of Cape Town, 2017.

Mabunda, S. *SA Legislative Responses to Cybercrime*, PhD Thesis submitted at the University of the Western Cape, 2021

Magang, T. *Culture and Corporate Governance in SA*, PhD Thesis submitted at the University of Bradford, UK, 2012.

Maharaj, N. *A Discussion on the Duty of Care, Skill and Diligence to be Exercised by a Director in Light of the Companies Act 71 of 2008, as well as the Common Law and an Overview of the BJR: A Company Law Perspective*, LLM Thesis submitted at the University of KwaZulu-Natal, 2015.

Mupangavanhu, B. *Directors Standards of Care, Skill, Diligence and the BJR in View of SA's Companies Act 71 of 2008: Future Implications for Corporate Governance*, PhD Thesis submitted at the University of Cape Town, 2016.

Oost, A. *A Safe Harbour for Directors in SA? A Comparative Study of the BJR*, LLD Thesis submitted at the University of SA, 2020.

III. JOURNAL ARTICLES

Adi *et al.* 'Harnassing AI Capabilities to Improve Cybersecrity' in *Journal of the Institute of Electrical and Electronic Engineers* 8(2020) 23817.

Agudelo, M. *et al.* in 'A Literature Review of the History and Evolution of CSR' in *International Journal of CSR* 1(2019) 18.

Ali, H. *et al.* 'Some Legal Uncertainties in Electronic Corporate Meetings' in *International Journal of Computer Theory and Engineering* 5(2) (April 2013) 284.

Amodu, N. 'Stakeholder Protection and CSR from a Comparative Company Law Perspective' in *Journal of African Law* March 2020, 1.

Bebchuk, L. 'The Case for Increasing Shareholder Power' in *Harvard Law Review* 118(2005) 833.

Bekink, M. 'An Historical Overview of the Director's Duty of Care and Skill: From the 19th Century to the Companies Bill of 2007' in the *SA Mercantile Law Journal* 20(2008) 108.

Berendt, B. *et al.* 'Bias in Data-Driven AI Systems: An Introductory Survey' in *Wires: Data Mining and Knowledge Discovery* of May/June 2020 10(3) 3.

Boros, E. 'Virtual Shareholder Meetings' in *Duke Law and Technological Review* (8) 2004 *s.p.*

Bosch, J. *et al.* 'The Risk-Adjusted Performance of Responsible Investment Funds in SA' in *Investment Analysts Journal* 37(68) (2008) 40.

Boura, M. *et al.* 'Big Data Analytics and Firm Performance: Findings from a Mixed-Method Approach' in *Journal of Business Research* 98 (2019) 261.

Bouwman, N. ‘An Appraisal of the Modification of the Director’s Duty of Care and Skill’ in *SA Mercantile Law Journal* 21(2009) 520.

Brandenburg, R *et al*. ‘Cybersecurity for a Remote Workforce’ in *MIT Sloane Management Review* of 23 July 2020, *s.p.*

Burchell, J. ‘The Legal Protection of Privacy in SA: A Transplantable Hybrid’ in *Electronic Journal of Comparative Law* 13(1) March 2009 1.

Camillo, M. ‘Cyber Risk and the Changing Role of Insurance’ in *Journal of Cyber Policy* 2(1) (2017) *s.p.*

Cassidy J, ‘Models for Reform: The Directors’ Duty of Care in a Modern Commercial World’ 3(2009) in *Stellenbosch Law Review* 385.

Cassim, F. ‘Addressing the Challenges Posed by Cybercrime: A SA Perspective’ in *Journal of International Commercial Law and Technology* (2010) 119.

Chigada, J. *et al.* ‘Cyberattacks and Threats During Covid-19’ in *SA Journal of Information Management* 23(1)(2021) 1.

Chitimira, H. *et al.* ‘The Integration and Reliance on Technology to Enhance the Independence and Accountability of Company Directors in SA’ in *Potchefstroomse Elektroniese Regsblad* (24) 2021 2.

Chitimira, H. ‘The Regulation and Use of AI and 5G Technology to Combat Cybercrime and Financial Crime in SA Banks’ in *Potchefstroomse Elektroniese Regsblad* (24) 2021 1.

Cohen, R. *et al.* ‘Understanding Cyberrisk and Cyberinsurance’ in the *Social Science Research Network’s Electronic Law Journal* (January 2017) 5.

Cossin, D. *et al.* ‘Board Oversight of Cyberrisks and Cybersecurity’ in *Journal of the IMD Business School for Management and Leadership* (May 2021) 2.

Craig, A. *et al.* ‘Toward a Global Cybersecurity Standard of Care?’ in *Texas International Law Journal* (2015) 6.

D’Cruze, H. *et al.* ‘Economic Costs and Impacts of Business Data Breaches’ in *Issues in Information Systems* (2019) 20(2) 165.

Delport, P. *et al.* 'The Duty of Care, Skill and Diligence: The King Report and the 2008 Companies Act' in *Tydskrif vir Hedendaagse Romeinse Reg* 2011(74) 450.

Delport, P. *et al.* 'The Protection of Stakeholders: The SA Social and Ethics Committee and the UK's Enlightened Shareholder Approach, Part 1' in *De Iure* 50(1)(2017) 97.

Erasmus, P. *et al.* 'Assessing the Business for Environmental, Social and Corporate Governance Practices in SA' in *SA Journal of Economic and Management Sciences* 22 (2019) 3.

Esser, I. *et al.* 'From a Financial to an Entity Model of ESG' in *European Organisation Business Law Review* (26 April 2021) 1.

Esser, I. & Delport, P. 'The Duty of Care, Skill and Diligence: The King Report and the 2008 Companies Act' in *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 74 (2011) 451.

Farisani, D. 'The Regulation of Corporate Criminal Liability in SA: A Close Look' in *Obiter* (January 2006) 264.

Furlow, C. 'Good Faith, Fiduciary Duties and the BJR in Delaware' in *Utah Law Review* (2009) 1067.

Gillan, S. *et al.* 'Firms and Social Responsibility: A Review of ESG and CSR Research in Corporate Finance' in the *Journal of Corporate Finance* 66(February 2021) 18.

Gudivada, V. 'Cognitive Computing Systems: Their Potential and the Future' in *Computer* 52(5) 2019 6.

Gwanyanya, M. 'The SA Companies Act and the Realisation of Corporate Human Rights' in *Potchefstroomse Elektroniese Regsblad* of 18(1)(2015), *s.p.*

Harner, M. 'A More Realistic Approach to Directors' Duties' in *Tennessee Journal of Business Law* (2013) 16.

Hassani, H. *et al.* 'Artificial Intelligence (AI) or Intelligence Augmentation (IA): What is the Future?' in *AI* 1(2) (2020) 147.

Hazen, T. 'Social Issues in the Spotlight: The Increasing Need to Improve Publicly Held Companies' CSR and ESG Disclosures' in the *University of Pennsylvania Journal of Business Law* (2021) 745.

Herringer, A. *et al.* 'Key Challenges Facing the SRI Sector in SA' in *Investment Analysts Journal* 70(2) (2009) 12.

Hiscox Insurance ‘Cyberattacks on the Rise for Businesses, Pushing Many to the Brink’ in *Insurance Journal* (April 2021) *s.p.*

Horrigan, B. *et al.* ‘Directors Duties and Liabilities: Where Are We Now and Where Are We Going in the UK, Broader Commonwealth and Internationally?’ in *International Journal of Business and Social Science* 3(2) 2012 40.

James, N. ‘Separate Legal Personality: Legal Reality and Metaphor’ in *Bond Law Review* (1996) 5(2) 217.

Johnson, V. ‘Cybersecurity, Identity Theft and the Limits of Tort Liability’ in *South Carolina Law Review* (57) 255.

Kanamugire, J. *et al.* ‘The Directors’ Duty of Care to Exercise Care and Skill in Contemporary SA Company Law and the BJR’ in *Mediterranean Journal of Social Sciences* 5(20) (September 2014) 70.

Keay, A. ‘Ascertaining the Corporate Objective: An Entity Maximisation and Sustainability Model’ in *The Modern Law Review* 71(5) 2008 663.

Keay, A. ‘Comply or Explain in Corporate Governance Codes: In Need for Greater Regulatory Oversight?’ in *Legal Studies* 34(2) 2014 279.

Keay, A. ‘Stakeholder Theory in Corporate Law: Has It Got What It Takes?’ in the *Richmond Journal of Global Law & Business* 9(3) 2010 249.

Keay, A. ‘Stewardship Theory: Is Board Accountability Necessary’ in *International Journal of Law and Management* 59(6) 2017 1292.

Keay, A. ‘Tackling the Issue of the Corporate Objective: An Analysis of the UK’s Enlightened Shareholder Value Approach’ in *Sydney Law Review* 29(4) (2007) 577.

Keay, A., Loughrey, J. ‘Business Judgment and Director Accountability: A Study of Case Law Over Time’ in *Journal of Corporate Law Studies* 20(2) 2020 359.

Keay, A. Loughrey, J. *et al.* ‘Reviewing Directors’ Business Judgments: Views from the Field’ in *Journal of Law and Society* 47(4) (November 2020) 639.

Keay, A., Loughrey, J. 'The Concept of Business Judgment' in *Legal Studies* 39(1) March 2019 36.

Keay, A., Loughrey, J. 'The Framework for Board Accountability in Corporate Governance' in *Legal Studies* 35(2) 2015 252.

Keay, A. Loughrey, J. *et al.* 'Legal Practitioners, Enlightened Shareholder Value and the Shaping of Corporate Governance' in *Journal of Corporate Law Studies* (April 2008) 79.

Kemp, N. *et al.* 'Reflecting on the Changing Landscape of Shareholder Activism in SA' in *SA Journal of Economic and Management Sciences* of 25 January 2021, *s.p.*

Kershaw, D. 'Corporate Law's Fiduciary Personas' in *Law Quarterly Review* (October 2019) 1.

Kohne, N. *et al.* 'Fiduciary Duties of Directors are Key to Minimise Cybersecurity Risks' in *NACD Directorship* (May/June 2015), 42.

Li, Y. *et al.* 'A Comprehensive Review Study of Cyberattacks and Cybersecurity: Emerging Trends and Recent Developments' in *Energy Reports* 7 (November 2021) 8177.

Loughrey, J. 'Breaching the Accountability Firewall: Market Norms and the Reasonable Director' in *Seattle University Law Review* 37(3) 2014 990.

Lunn, B. 'Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine' in *Journal of Law and Cyber Warfare* (2014) 1.

Mervis, M. *et al*. '*Bebchuk's* 'The Case for Increasing Shareholder Power:' An Opposition' in *Harvard Law Review* 121(2007) 53.

Muswaka, L. 'Shielding Directors Against Liability Imputations: The BJR and Good Corporate Governance' in *Speculum Iuris* 2(2013) *s.p.*

Ncube, C. 'You're Fired! The Removal of Directors under the SA Companies Act 71 of 2008' in the *SA Law Journal* (2011) 128 34.

Neethling, J. 'The Concept of Privacy in South African Law' in *SA Law Journal* 122 (2005) 18.

Neethling, J., Potgieter, J. ‘Statutêre Bevoegdheid: Die Rol van Redelike Voorsienbaarheid by Onregmatigheid en Nalatigheid’ in *Obiter* (2004) 483.

Noor, A. ‘Potential of Cognitive Computing and Cognitive Systems’ in *Open Engineering* 5(1) (2015) 76.

Osode, P. *et al.* ‘The Nature and Evolution of the BJR and Its Transplantation to SA under the Companies Act of 2008’ in *Speculum Iuris* 33(1) 2019 *s.p.*

Petrin, M. ‘Corporate Management in the Age of AI’ in *Columbia Business Law Review* (2020) 980.

Price, A. ‘The Contract/Delict Interface in the Constitutional Court’ in *Stellenbosch Law Review* 25(2014) 501.

Sarker, I. ‘AI-Based Modelling: Techniques, Applications, and Research Issues Towards Automation, Intelligence and Smart Systems’ in *SN Computer Science* 3(2021) 1.

Shabbir, M. *et al.* ‘Application of Big Data Analytics and Organisational Performance: The Mediating Role of Knowledgement Management Practices’ in *Journal of Big Data* 7(47) 2020 2.

Sicard, K. ‘The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters vs Cyberattacks’ in *Kennesaw Journal* 6(2)(2019), 1.

Snail, S. ‘Cyber Crime in SA: Hacking, Cracking, and Other Unlawful Online Activities’ in *Journal of International Logistics and Trade* (2009) 3.

Stevens, R. ‘The Legal Nature of the Duty of Care and Skill: Contract or Delict?’ in *Potchefstroomse Elektroniese Regsblad* (2017) 10.

Subramanien, D. ‘’Legal Standing’ and ‘the Demand’ in the Companies Act 71 of 2008, section 165: A Comparative Discussion’ in *Obite*r 43(2) (2022) 47.

Sutherland, P. ‘The State of Company Law in SA’ in *University of Stellenbosch Law Review* 2012(1) 172.

Swales, L. ‘The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock’ in *Potchefstroomse Elektroniese Regsblad* 25(1) 2002 5.

Velasco, C. ‘Cybercrime and AI: An Overview of the Work of International Organisations on Criminal Justice and the Applicable International Instruments’ in *ERA Forum* 23(2022) 111.

West, A. ‘Theorising SA's Corporate Governance’ in *Journal of Business Ethics* (2002) 68(4).

IV. CASE LAW

UK

Byng v London Life Association (1990) 1Ch 170.

Capraro Industries PLC v Dickman (1990) ALL ER 568.

Day v Cook (2002) BCLC 1 CA.

Ex Parte Belchier (1754) Ambler 218.

Google Inc. v Vidal-Hall and Others (2014) EXHC (Civ) 113.

Heron International Ltd v Lord Grade (1983) BCLC 261.

Johnson v Gore Wood & Co (2002) 2 AC 1 (HL) 62.

Knight v The Earl of Plymouth (1747) Dickens 120.

Perry v Day (2005) BCLC 405.

Prudential Assurance Co Ltd v Newman Industries Ltd (No.2) (1981) Ch 257; 1982 (1) Ch 204 (CA).

Railroad Company v Lockwood 84 US 357 (1873).

Shiells v Blackburne (1789) 1 HB1 158, 126 ER 94.

Re Brazilian Rubber Plantations & Estates Ltd (1911) Ch 425.

Re Castle Trust Direct Plc & Others (2020) EWHC 969 (Ch).

Re City Equitable Fire Insurance Co Ltd 1925 Ch 407.

Re Denham & Co (1884) LR 25 Ch D 752.

Sevilleja v Marex Financial Ltd (2020) UKSC 31.

Sharp and Others v Blank and Others [2015] EWHC 3220.

Stein v Blake (No. 2) (1998) 1 AII ER 724 (CA).

The Charitable Corporation v Sutton 2 ATK 400 (1754).

Various Claimants v Wm Morrisons Supermarkets PLC UKSC 2018/0213.

US

Federal

US FTC v Wyndham Worldwide Corporation 799 F.3d 236 (3 Circuit 2015).

California

Adams v City of Fremont 68 Cal. App. 4th 243 (1998).

In Re Yahoo! Inc. Securities Litigation 17-CV-307054 (Cal. Sup. Ct., Santa Clara County, 4 January 2019).

Delaware

Aronson v Lewis 473 A. 2D 805 (Del. 1984).

Graham v Allis-Chalmers Mfg Co 188 A 2d 125 (Del 1963).

Grobow v Perot 539 a.2d 180 (Del. 1988).

In Re Caremark International Inc. Deriv Litig., 698 A 2d (Del. Ch. 1996).

In Re Citigroup Inc. Shareholder Derivative Litigation 964 A 2d 106 (Del. Ch. 2009).

In Re Trados Inc. Shareholder Litigation, Ct. of Ch. Del. 73A.3d 17.

Marchand v Barnhill 212 A. 3D (Del. 2019) 805.

Smith v Van Gorkom 488 A 2d (Del 1985) 858.

Stone v Ritter 911 A 2d (Del 2006) 362.

Florida
McCain v Florida Power Corporation 593 So. 2d 500 (Florida 1992).

Georgia
In Re Home Depot Shareholder Derivative Litigation 223 F. Supp. 3d 1317 (N.D. Ga. Nov. 30, 2016).

In Re Equifax Inc. Securities Litigation 357 F. Supp. 3d 1189 (N.D. Ga. Jan. 28, 2019).

Illinois
Freedom Oil Co. v Ill. Pollution Control Board 655 N.E.2d 1184 (Ill. App. Ct. 1995).

Massachusetts
Jupin v Kask 849 N.E 2d 829.

Minnesota
In Re Target Corp. Data Security Breach Litigation US District Court, D Minnesota 66F. Supp. 3d 1154 (D. Minn. 2014).

Potter v. Pohlad, 560 NW2d 389 (Minnesota Court of Appeals 1997).

New Jersey
Palkon v Holmes 2014 WL 5341880, D.N.J.

US FTC v Wyndham Worldwide Corp. et al. US District Court, District of New Jersey 13 – 01887.

New York
Robinson v Smith 3 Paige Ch. 222 (1832).

Scott v Depeyster 6 NY Ch. Ann 229 (1832).

The TJ Hooper 60 F.2d 737, 1932 US App. LEXIS 2592 (2d Cir. NY 1932).

Pennsylvania

In Re Lemington Home for the Aged 13-2707 (3d Cir. 2015).

SA

Administrateur, Natal v Trust Bank van Afrika, Bpk 1979 3 SA 824 (A).

Amazwi Power Products (Pty) Ltd v Turnbull (2008) 9 BLLR 817 (LAC).

Bernstein v Bester 1996 2 SA 751 (CC).

Burco Civils CC v Stolz and Another (2017) JOL 39331 (GP).

Cape Empowerment Trust Limited v Druker and Others (2016) JOL 36987 (WCC).

Cape Town Municipality v Paine 1923 AD 207.

Caxton and CTP Publishers and Printers Ltd v Novus Holdings Lid (Case no. 219/2021) [2022] ZASCA 24 (09 March 2022).

Centre for Child Law v Media 24 Limited 2020 4 SA 319 (CC).

Communicare and Others v Kahn and Another 2013 (4) SA 482 (SCA).

De Bruyn v Steinhoff International Holdings NV (29290/2018) (2020) ZAGPHJC 145 (26 June 2020).

Du Plessis NO v Phelps 1995 (4) SA 165 (C).

Faiga v Body Corporate of Dumbarton Oaks 1997 2 SA 651 (W).

Fisheries Development Corporation of SA Ltd v Jorgensen & Another; Fisheries Development of SA Ltd v AWJ Investments (Pty) Ltd & Others 1980 (4) SA 156 (W).

Government of the RSA v Basdeo 1996 1 SA 355 (A).

Grancy Property v Gihwala 2014 JDR 1292 (WCC).

Hlumisa Investment Holdings (RF) Ltd v Kirkinis 2019 (4) SA 569 (GP); 2020 (5) SA 419 (SCA).

Howard v Herrigel NO and Another (130/89) (1991) 2 AII SA 113 (A).

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

Itzikowitz v ABSA Bank Ltd 2016 (4) SA 432 (SCA).

Knop v Johannesburg City Council 1995 2 SA 1 (A).

Kruger v Coetzee 1966 2 SA 428 (A).

Kukama v Lobelo and Others (38587/2011) (2012) ZAGPJHC 60.

Local Transitional Council of Delmas v Boshoff (2005) 5 SA 515 (SCA).

Loureiro v iMvula Quality Protection (Pty) Ltd 2014 3 SA 394.

Maake v Chemfit Fine Chemicals (Pty) Ltd (5772/2016/HCAA04/2018) (2018) ZALMPPHC 71 (22 November 2018).

Minister of Finance and Other v Van Heerden (2004) 12 BLLR 1181 (CC).

Minister of Water Affairs v Stilfontein Gold Mining Co Ltd 2006 5 SA 333 (W).

Mistry v Interim Medical and Dental Council of SA 73 1998 (4) SA 1127 (CC).

Motor Industry Bargaining Council v Botha (34198/2013) 2016 ZAGPPHC 615 (10 June 2016).

Mouritzen v Greystone Enterprises (Pty) Ltd and Another (10442/2011) (2012).

Msimang NO and Another v Katuliiba and Others (2013) JOL 30522 (GSJ).

Narlis v SA Bank of Athens 1976 2 SA 573 (A).

National Media Ltd v Jooste 1996 3 SA 262 (A).

Off-Beat Holiday Club v Sanbonani Holiday Spa Shareblock Ltd 2016 (6) SA 181 (SCA).

OUTA NPC v Myeni (2019) ZAGPPHC 957.

PG Group (Pty) Ltd v Mbambo NO and Others (JR215/2004) 92004) ZALCJHB 8 (26 October 2004).

Premier, Western Cape v Faircape Property Developers (Pty) Ltd 2003 6 SA 13 (SCA).

Rabinowitz v Van Graan 2013 (5) SA 315 (GSJ).

S v Mashiyi 2002 2 SACR 387 (Tk).

SA Post Office Ltd v Mampeule (2009) 8 BLLR 792 (LC).

Simon's Town Municipality v Dews 1993 1 SA 191 (A).

Swart v Beagles Run Investments 25 (Pty) Ltd and Others (2011) (5) SA 422 (GNP).

Van Breda and Others v Jacobs and Others 1921 AD 330.

Workmen's Compensation Commissioner v De Villiers 1949 1 SA 474 (C).

V. LAWS AND REGULATIONS

EU
EU 'General Data Protection Regulation (GDPR) of 2018'

UK
UK Corporate Insolvency and Governance Act (CIGA) Coronavirus Extensions of Relevant Periods Regulations of 2021.

UK Corporate Insolvency and Governance Act (CIGA) of 2020.

UK Data Protection Act (DPA) of 1998, (Ch. 29).

UK DPA of 2018.

UK Financial Reporting Council (FRC) Corporate Governance Code of 2018.

UK FRC Stewardship Code of 2020.

UK Companies Act of 2006 (Ch. 46).

UK Companies' (Shareholders' Rights) Regulations of 2009.

US

American Law Institute (ALI), US Third Restatement of Torts of 2005.

US Code of Federal Regulations (CFR).

US Constitution of 1788.

US Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

US Electronic Signatures in Global and National Commerce Act of 2000.

US Federal Trade Commission (FTC) Act of 1938.

US Gramm-Leach-Bliley Act of 1999.

US Health Insurance Portability and Accountability Act (HIPPA) of 1996.

US Homeland Security Act of 2002.

US Model Business Corporations Act (MBCA) of 2016.

US Sarbanes-Oxley (SOX) Act of 2002.

US Securities Act of 1933.

US Securities Exchange Act of 1934.

US Third Restatement of 2005.

Legislation of the States of the US:

Arizona

Arizona Revised Statutes Annotated of 2010.

California

California Civil Code.

California Corporations Code of 2009.

Colorado
Colorado Privacy Act of 2021.

Colorado Revised Statutes Annotated of 2017.

Delaware
Delaware General Corporations Law (DGCL) (Title 8, Chapter 1 of the Delaware Code) of 1995.

Delaware General Corporations Law (DGCL) (Title 8, Chapter 1 of the Delaware Code) of 2000.

Delaware General Corporations Law (DGCL) (Title 8, Chapter 1 of the Delaware Code) of 2016.

Illinois
Illinois Compiled Statutes Annotated 805 of 1983.

Maryland
Maryland Code Annotated on Corporations and Associations of 2017.

Massachusetts
Massachusetts General Laws Annotated 156D of 2004.

Minnesota
Minnesota Statutes Annotated of 2017.

Montana
Montana Code Annotated of 2010.

New Jersey
New Jersey Administrative Code of 1969.

NY
NY Business Corporation Law (NY BCL) of 2010.

New York Privacy Act of 2021.

Ohio
Ohio Data Protection Act (DPA) of 2018's Revised Code 1354.

Virginia
Virginia Code (Title 13.1) of 2014.

SA
SA Broad-Based Black Economic Empowerment (BBBEE) Act 53 of 2003.

SA Companies Act 71 of 2008.

SA Companies Regulations of 2011.

SA Constitution of 1996.

SA Consumer Protection Act 68 of 2008.

SA Criminal Procedure Act 51 of 1977.

SA Cybercrimes Act 19 of 2020.

SA Electronic Communications and Transactions Act (ECTA) 25 of 2002.

SA Employment Equity Act 55 of 1998.

SA Environmental Law Rationalisation Act 51 of 1997.

SA Financial Markets Act 19 of 2012.

SA Independent Communications Authority of SA (ICASA) Act 13 of 2000.

SA Labour Relations Act 66 of 1995.

SA National Environmental Management Act (NEMA) 107 of 1998.

SA Protection of Personal Information (POPI) Act 4 of 2013.

SA Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) 70 of 2002.

SA Reserve Bank Act 90 of 1989.

SA Share Blocks Control Act 59 of 1980.

VI. INTERNATIONAL CONVENTIONS AND RELATED DOCUMENTS

Brazil, Russia, India, China, SA (BRICS)
BRICS '*Information Portal*,' available online at <https://infobrics.org/>, last accessed on 5 October 2022.

Council of Europe (CoE)
Council of Europe (CoE) 'Convention on Cybercrime of 2001' (ETS 185).

CoE '*Chart of Signatures and Ratifications of Treaty No. 185*,' available online at <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, last accessed on 7 January 2022.

CoE '*Details of Treaty No. 185*,' available online at <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>, last accessed on 7 January 2023.

Group of 20 (G20)
G20 '*About the G20*,' available online at <https://www.g20.org/about-the-g20/>, last accessed on 5 October 2022.

G20 'Global Framework for Tracing Beneficial Ownership,' available online at <https://www.global-solutions-initiative.org/policy_brief/a-global-framework-for-tracing-beneficial-ownership/>, last accessed on 15 June 2023.

G20 'Principles of Corporate Governance of 2015.'

Organisation for Economic Cooperation and Development (OECD)
OECD '*Corporate Governance in Asia: Progress and Challenges*,' available online at <http://www.oecd.org/daf/ca/corporategovernanceprinciples/corporategovernanceinasia-progressandchallenges.htm>, last accessed on 18 May 2019.

Task Force on Climate-Related Financial Disclosures (TFCRF)

Task Force on Climate-Related Financial Disclosures (TFCRF) '*About*,' available online at <https://www.fsb-tcfd.org/about/>, last accessed on 19 June 2023.

United Nations (UN)

UN International Covenant on Civil and Political Rights of 1996.

UN Universal Declaration on Human Rights of 1948.

UN Global Compact '*About*,' available online at <https://unglobalcompact.org/about>, last accessed on 19 June 2023.

UN '*Sustainable Development Goals*,' available online at <https://www.un.org/en/footballforthegoals?gclid=EAIaIQobChMI0qDjjsrP_wIVWRwGAB15kQAqEAAYASAAEgL8b_D_BwE>, last accessed on 19 June 2023.

VII. BILLS, DIRECTIVES, OFFICIAL PUBLICATIONS AND POLICIES

European Union (EU)

EU 'Directive on Anti-Money Laundering and Terrorist Financing (AMLDIV) 2015/849 of 2017.'

EU 'Directive on Anti-Money Laundering and Terrorist Financing (AMLDV) 2018/843 of 2018.'

EU 'Directive on Corporate Sustainability Reporting 2014/95/EU of 2014'.

EU 'Directive on the Encouragement of Long-Term Shareholder Engagement (2017/828) of 2017'.

EU 'Directive on the Exercise of Certain Rights by Shareholders (2007/36/EC) of 2007'.

EU 'Regulation on Sustainability-Related Disclosures in the Financial Services Sector (2019/2088).'

EU 'Regulation on the Establishment of a Framework to Facilitate Sustainable Investment (2020/852).'

EU 'Renewed Sustainable Finance Strategy and Implementation of the Action Plan on Financing Sustainable Growth of 2018,' available online at <https://finance.ec.europa.eu/publications/renewed-sustainable-finance-strategy-and-implementation-action-plan-financing-sustainable-growth_en>, last accessed on 19 June 2023.

EU ‘Sustainable Governance Initiative,’ available online at <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12548-Sustainable-corporate-governance_en>, last accessed on 8 August 2021.

EU ‘Taxonomy and Regulation of 2020’.

UK

legislation.gov.uk ‘*Companies Act of 2006: Explanatory Notes,*’ available online at <https://www.legislation.gov.uk/ukpga/2006/46/notes/division/6/4>, last accessed on 11 October 2022.

UK Department for Business, Energy and Industrial Strategy ‘*Measures in Respect of Company Filings, AGMs and Other General Meetings During Covid-19,*’ available online at <https://www.frc.org.uk/getattachment/e3224310-c39c-4b48-b56b-cc703936beeb/Updated-QA-AGMs-Best-Practice-Final.pdf>, last accessed on 23 June 2021.

UK Department of Trade and Industry (UK DTI) ‘*Modern Company Law for a Competitive Economy: Company General Meetings and Shareholder Communication (URN 99/1144),*’ available online at <http://webarchive.nationalarchives.gov.uk/20121101192029/http://www.bis.gov.uk/files/file23274.pdf>, last accessed on 20 March 2018.

UK Law Commission ‘*Company Directors*’ (1998) Consultation Paper Number 153.

UN

UN Interregional Crime and Justice Research Institute (UNICRI) *et al.* ‘*Malicious Uses and Abuses of AI*,’ available online at <https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf>, last accessed on 25 January 2023.

US

Federal

US Securities Exchange Commission (SEC) ‘*Commission Statement and Guidance on Public Company Cybersecurity Disclosures,*’ available online at <https://www.sec.gov/rules/interp/2018/33-10459.pdf>, last accessed on 12 July 2021.

US SEC ‘*Form 8-K,*’ available online at <https://www.sec.gov/files/form8-k.pdf>, last accessed on 12 July 2021.

US SEC '*Investigative Report on Cyberfrauds,*' available online at <https://www.sec.gov/litigation/investreport/34-84429.pdf> , last accessed on 12 July 2021.

US SEC *'Regulation Systems Compliance and Integrity,'* available online at <https://www.sec.gov/rules/proposed/2013/34-69077.pdf>, last accessed on 12 July 2021.

US SEC '*SEC Adopts Rule Amendments to Provide Investors Using Proxy Voting Advice More Transparent, Accurate and Complete Information,*' available online at <https://www.sec.gov/news/press-release/2020-161>, last accessed on 7 July 2021.

US SEC Division of Corporate Finance and the Division of Investment Management '*Staff Guidance for Conducting Shareholder Meetings in Light of Covid-19 Concerns,*' available online at <https://www.sec.gov/ocr/staff-guidance-conducting-annual-meetings-light-covid-19-concerns>, last accessed on 10 July 2021.

US States

Massachusetts

Mass.gov '*Governor Baker Files Legislation to Extend Certain Covid-19 Emergency Measures,*' available online at <https://www.mass.gov/news/governor-baker-files-legislation-to-extend-certain-covid-19-emergency-measures>, last accessed on 19 June 2021.

NY

Lexology.com '*NY Governor Issues Executive Order Allowing Virtual AGMs,*' available online at <https://www.lexology.com/library/detail.aspx?g=c96e05de-803a-4ca6-9e03-2701186fa70b>, last accessed on 19 June 2021.

NY State Assembly Bill 'Bill to Authorise Shareholders to Attend Meetings via Remote Communication and be Deemed Present for Voting Purposes, Bill A434 of 2019'.

SA

SA Companies Bill B612D of 2007.

SA Companies Amendment Bill of 2021 (SA Bill of 2021).

SA Cybercrimes Bill B6 of 2017.

SA Department of Home Affairs '*Verify Identity Online,*' available online at <https://www.gov.za/services/verify-identity-online>, last accessed on 8 July 2021.

SA Department of Justice and Constitutional Development (SA DoJ & CD) '*Courts in SA,*' available online at <http://www.justice.gov.za/about/sa-courts.html>, last accessed on 18 May 2019.

VIII. ENFORCEMENT AGENCY SOURCES

UK

UK Financial Conduct Authority (FCA) *Handbook, Statements of Principle and Code of Practice for Approved Persons* (PRA) (May 2023).

UK Information Commissioner's Office (ICO) '*Guide to the GDPR,*' available online at <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>, last accessed on 11 July 2021.

UK Institute of Chartered Secretaries and Administrators (ICSA) '*2021 General Meetings and the Impact of Covid-19*,' available online at <https://www.cgi.org.uk/knowledge/resources/2021-general-meetings-and-the-impact-of-covid-19>, last accessed on 17 June 2023.

US

American Bar Association (ABA) '*Committee on Corporate Laws,*' available online at <https://www.americanbar.org/groups/business_law/committees/corplaws/>, last accessed on 24 February 2022.

Duty of Care Risk Analysis Standard (DoCRA) Council '*The Duty of Care Risk Analysis Standard,'* available online at <https://www.docra.org/>, last accessed on 16 June 2022.

US Cybersecurity and Infrastructure Security Agency, '*Cybersecurity,*' available online at <https://www.cisa.gov/uscert/ncas/tips/ST04-001>, last accessed on 5 March 2022.

US Federal Bureau of Investigation '*Public Service Announcement: Business E-Mail Compromise: Virtual Meeting Platforms*,' available online at <https://www.ic3.gov/Media/Y2022/PSA220216>, last accessed on 5 October 2022.

SA

SA Companies and Intellectual Property Commission (CIPC), '*Home Page,*' available online at <http://www.cipc.co.za/index.php/about/our-functions/>, last accessed on 10 July 2021.

IX. REPORTS

General

Andrade, R. *et al.* 'Application of Big Data Analytics in Cybersecurity' from the *International Conference on Applied Cognitive Computing* (2019), available online at <https://www.researchgate.net/profile/Roberto-Andrade-7/publication/338582915_Application_of_Big_Data_Analytic_in_Cybersecurity/links/5e1dedc745851536bfe621bb/Application-of-Big-Data-Analytic-in-Cybersecurity.pdf>, last accessed on 10 January 2023.

Ponemon Institute '*2022 Cost of Cyberbreach Study,*' available online at <https://www.ibm.com/reports/data-breach>, last accessed on 13 October 2022.

Weiss, J. *et al.* 'Ethical Implications of Bias in Machine Learning,' in *Proceedings of the 51st Hawaii International Conference on System Sciences* (2018), available online at <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1649&context=hicss-51>, last accessed on 9 January 2023.

IOs (International Organisations)

International Finance Corporation (IFC) 'Who Cares Wins: Investing for Long Term-Value,' Conference Report, for *IFC Conference* which was held in Zurich on 25 August 2005, available online at <https://www.scribd.com/fullscreen/16876744?access_key=key-mfg3d0usaiuaob4taki>, last accessed on 19 June 2023.

World Commission on Environment and Development (WCED) '*Our Common Future: The Brundtland Report of 1987,*' available online at <https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf>, last accessed on 19 June 2023.

SA

Institute of Directors of South Africa (IoDSA) 'King I: Report on Corporate Governance for SA of 1994,' available online at <https://www.saica.co.za/Technical/LegalandGovernance/King/tabid/2938/language/en-ZA/Default.aspx>, last accessed on 27 April 2018.

IoDSA 'King II: Report on Corporate Governance for SA of 2002,' available online at <http://library.ufs.ac.za/dl/userfiles/documents/Information_Resources/KingII%20Final%20doc.pdf>, last accessed on 27 April 2018.

IoDSA 'King III: Report on Corporate Governance for SA of 2009,' available online at <https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iii/King_Report_on_Governance_fo.pdf>, last accessed on 27 April 2018.

IoDSA 'King IV: Report on Corporate Governance for SA of 2016,' available online at <http://www.iodsa.co.za/?page=about_main>, last accessed on 27 April 2018.

Privacy International '*The State of Privacy in SA,*' available online at <https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa>, last accessed on 14 May 2021.

UK

UK Committee on the Financial Aspects of Corporate Governance 'Report from the Committee on the Financial Aspects of Corporate Governance of 1992' ('Cadbury Report'), available online at <https://ecgi.global/sites/default/files//codes/documents/cadbury.pdf>, last accessed on 19 May 2019.

US

Working Group 11 on Data Security and Privacy Liability (WG11) '*The Sedona Conference, Commentary on a Reasonable Security Test,'* available online at <https://thesedonaconference.org/node/9702>, last accessed on 1 March 2022.

National Association of Corporate Directors (NACD) '*Public Companies' Governance Survey 2019 – 2020*,' available online at <https://www.nacdonline.org/analytics/survey.cfm?ItemNumber=66753>, last accessed on 5 October 2022.

NACD *'Trends and Priorities of the American Boardroom 2020 – 2021*,' available online at <https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71668>, last accessed on 5 October 2022.

X. GUIDELINES, RULES AND STANDARDS

EU

EU Data Protection Working Party '*Guidelines on the Setting of Administrative Fines,*' available online at <file:///C:/Users/Julian/Downloads/20171020_wp253_en_43FBAE3D-B195-7648-AD40DD676CB8416E_47889.pdf>, last accessed on 19 June 2022.

International Organisations (IOs)

International Capital Market Association (ICMA) '*Green Bond Principles (GBP): Voluntary Process Principles for Issuing Green Bonds*' of July 2021, available online at <https://www.icmagroup.org/assets/documents/Sustainable-finance/2022-updates/Green-Bond-Principles-June-2022-060623.pdf>, last accessed on 19 June 2023.

Organisation of American States (OAS) *Cyberrisk Oversight Handbook for Corporate Boards*, available online at <https://webcache.googleusercontent.com/search?q=cache:zilNEoUGzVMJ:https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf+&cd=1&hl=en&ct=clnk&gl=za>, last accessed on 14 July 2021.

OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data of 1980.

UN Principles of Responsible Investment (PRI) '*The New Normal: Company AGMs in a Covid-19 World,*' available online at <https://www.unpri.org/pri-blog/the-new-normal-company-agms-in-a-covid-19-world/5859.article>, last accessed on 8 July 2021.

UK

UK Chartered Governance Institute's '*Guidelines of 2020,*' available online at <https://www.cgi.org.uk/assets/files/pdfs/guidance/agms-and-impact-of-covid-19-web.pdf>, last accessed on 10 July 2021.

UK Corporate Governance Institute '*New Guidance Issued about Shareholder Meetings under CIGA 2020,*' available online at <https://www.cgi.org.uk/about-us/press-office/news-releases/new-guidance-issued-about-shareholder-meetings-under-the-corporate-insolvency-and-governance-act-2020>, last accessed on 23 June 2021.

UK Data and Marketing Association '*The Board Member Checklist: Non-Executive Directors,*' available online at <https://dma.org.uk/uploads/misc/checklist-v3-(1).pdf>, last accessed on 13 May 2021.

UK Financial Conduct Authority (FCA) '*Disclosure Guidance and Fiscal Disparity Guideline,*' available online at <https://www.handbook.fca.org.uk/handbook/DTR.pdf>, last accessed on 12 May 2021.

UK FRC '*Corporate Governance AGMs: An Opportunity for Change – October 2020*,' available online at <https://www.frc.org.uk/getattachment/48c4ee08-b7be-4b7c-8f19-bcaf3d44e441/Corporate-Governance-AGM.pdf>, last accessed on 17 June 2023.

US

Best Practices Working Group for Online Shareholder Participation in AGMs '*Guidelines for Protecting and Enhancing Online Shareholder Participation in OMs,*' available online at <https://www.broadridge.com/_assets/pdf/broadridge-guidelines-for-protecting-and-enhancing-online-shareholder-participation-in-annual-meetings.pdf>, last accessed on 21 June 2021.

US Federal Trade Commission (FTC) '*Fighting Identity Theft with the 'Red Flag' Rule,*' available online at <https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business>, last accessed on 12 July 2021.

SA

Integrated Reporting Committee of SA (IRCSA) '*Preparing an Integrated Report: A Starter's Guide*,' available online at <http://integratedreportingsa.org/ircsa/wp-content/uploads/2017/05/IRCSA_StartersGuide.pdf>, last accessed on 19 June 2023.

IoDSA '*Code for Responsible Investing in SA (CRISA) of 2011,*' available online at <https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/crisa/crisa_19_july_2011.pdf>, last accessed on 14 July 2021.

IoDSA '*CRISA Home Page,*' available online at <https://www.iodsa.co.za/page/CRISACode>, last accessed on 14 July 2021.

IoDSA '*Governing Body's Role in Cyber Resilience,*' available online at <https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/05E93ACB-10BE-4507-9601-307A66F34BD8/CGN_Position_paper_13_Cyber_Resilience_April_2018.pdf>, last accessed on 15 May 2021.

IoDSA '*The Role of the Board in Organisational Ethics*,' available online at <https://www.iodsa.co.za/news/607020/The-Role-of-the-Board-in-Artificial-Intelligence-Ethics.htm>, last accessed on 9 January 2023.

Just Share '*Best Practices for SA Virtual AGMs,*' available online at <https://justshare.org.za/wp-content/uploads/2020/05/Just-Share-Virtual-AGM-Guide.pdf>, last accessed on 8 July 2021.

XI. LISTING REQUIREMENTS AND STOCK EXCHANGE SOURCES

UK

LSE '*Rules of the LSE,*' available online at <https://docs.londonstockexchange.com/sites/default/files/documents/rules-lse.pdf>, last accessed on 19 July 2021.

US

Nasdaq '*Listing Rule,*' available online at <http://business.nasdaq.com/list/rules-and-regulations/index.html>, last accessed on 9 February 2018.

NYSE '*Listed Company Compliance Guidance,*' available online at <https://www.nyse.com/publicdocs/nyse/regulation/nyse/NYSE_2021_Annual_Guidance_Letter.pdf>, last accessed on 22 June 2021.

NYSE '*Listed Company Manual,*' available online at <http://wallstreet.cch.com/LCM/>, last accessed on 9 February 2018.

SA

Johannesburg Stock Exchange (JSE) '*AGMs,*' available online at <https://www.jse.co.za/services/company-services/annual-general-meetings>, last accessed on 8 July 2021.

JSE '*JSE and TMS Launch First Virtual AGMs Enabling Clients to Engage with Shareholders,*' available online at <https://www.jse.co.za/articles/jse-and-tms-launch-first-virtual-agms-enabling-clients-to-engage-with-shareholders>, last accessed on 2 June 2021.

JSE '*Listing Requirements,*' available online at <https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/JSE%20Listings%20Requirements.pdf>, last
2019.

JSE '*We Make it Easier to Invest in Companies that Invest in the Future,*' available online at <https://www.jse.co.za/services/market-data/indices/ftse-jse-africa-index-series/responsible-investment-index>, last accessed on 19 May 2019.

XII. ONLINE SOURCES

Advanced National Network for Administrators (ANNA) '*On the Legal Status of Guidelines,*' available online at <http://www.annamsw.eu/news/117-on-the-legal-status-of-guidelines.html>, last accessed on 15 January 2023.

Albano, M. *et al.* 'Úpdate: Coronavirus and Virtual Annual Meetings,' available online at <https://www.clearymawatch.com/2020/03/coronavirus-virtual-annual-meetings/>, last accessed on 22 June 2021.

Ali, H. *et al.* '*A Legal Perspective of Shareholders' Meetings in the Globalised and Interconnected Business Environment,*' available online at <https://www.sciencedirect.com/science/article/pii/S187704281500467X>, last accessed on 2 February 2018.

Anwar H. 'Blockchain Implementation Guide: Empower Your Business' in *101 Blockchains* of 25 September 2018, available online at <https://101blockchains.com/blockchain-implementation-guide/>, last accessed on 3 July 2022.

Anwar H. 'Blockchain Technology Explained: A Decentralised Ecosystem' in *101 Blockchains* of 30 July 2021, available online at <https://101blockchains.com/blockchain-technology-explained/>, last accessed on 3 July 2022.

Anwar H. 'What is Private Blockchain: A Beginner's Guide' in *101 Blockchains* of 2 June 2020, available online at <https://101blockchains.com/what-is-a-private-blockchain/>, last accessed on 3 July 2022.

Asgarian, T. *et al.* '*Cyber Security: The Evolving Nature of a Director's Duty,*' available online at <https://www.mondaq.com/guernsey/offshore-financial-centres/633480/cyber-security-the-evolving-nature-of-a-director39s-duty>, last accessed on 15 January 2023.

Askounis, D. *et al.* '*Working from Home During Covid-19: A Cybersecurity Culture Assessment Survey,*' available online at <https://link.springer.com/article/10.1057/s41284-021-00286-2>, last accessed on 8 July 2021.

Astfalck, L. *et al*. '*Cybersecurity and Adequate Data Protection Have Become Key Focus Areas for Company Boards Across the World,*' available online at <https://www.clydeco.com/en/insights/2021/04/directors-beware-of-obligations-and-liabilities-un>, last accessed on 14 May 2021.

Australian National University's Cybercrime Observatory *et al. AI and Crime*, available online at <https://regnet.anu.edu.au/sites/default/files/news/related-documents/2019-07/KIC_2019_final_word_08July.pdf>, last accessed on 13 January 2023.

Bekaert, G. *et al.* 'Sustainable Investment: Exploring the Linkage Between Alpha, ESG, and SDG's,' *Social Science Research Network (SSRN) Working Paper*, published on 23 May 2023, available online at <file:///C:/Users/Julian/Downloads/SSRN-id3623459.pdf>, last accessed on 19 June 2023.

Belani G. 'The Use of AI in Cybersecurity: A Review' in *IEEE Computer Society*, available online at <https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity>, last accessed on 2 July 2022.

Bellasio, J. *et al. The Future of Cybercrime in Light of Technology Developments*, available online at <https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf>, last accessed online at 18 July 2021.

Berman, M. '*Laws vs Regulations vs Guidance: New Interstate Agency Provides Clarity,*' available online at <https://ncontracts.com/media-type/articles/laws-vs-regulations-vs-guidance-new-interagency-statement-provides-clarification/>, last accessed on 5 July 2020.

Bertram, M. *et al. Legal Guide for Company Directors and CEO's in SA*, available online at <https://cms.law/en/int/expert-guides/cms-expert-guide-for-directors-of-companies/south-africa>, last accessed on 9 January 2023.

Birkett's Solicitors '*Are All General Meetings Virtually the Same?,*' available online at <https://webcache.googleusercontent.com/search?q=cache:JunDRF7q_9cJ:https://www.birketts.co.uk/insights/legal-updates/are-all-general-meetings-virtually-the-same+&cd=15&hl=en&ct=clnk&gl=za>,last accessed on 12 December 2018.

Bowmans '*Covid-19: Impact on Businesses and Investments in SA,*' available online at <https://www.bowmanslaw.com/insights/mergers-and-acquisitions/covid-19-impact-on-businesses-and-investments-in-south-africa/#Dataprotection>, last accessed on 15 May 2021.

Brownlee J. 'A Gentle Introduction to Generative Adversarial Networks (GANs)' at *Machine Learning Mastery*, of 17 June 2019, available online at <https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/>, last accessed on 2 July 2022.

Burger, B. '*The Liability of Directors in Cyberspace,*' available online at <https://www.golegal.co.za/cyberspace-risks-director-liability/>, last accessed on 25 May 2020.

Calo R. 'FTC Warns the AI Industry: Don't Discriminate Or Else' in *The Conversation* of 27 April 2021, available online at <https://theconversation.com/ftc-warns-the-ai-industry-dont-discriminate-or-else-159622>, last accessed on 2 July 2022.

Cambridge Dictionary, available online at <https://dictionary.cambridge.org/dictionary/english/cyberattack>, last accessed on 12 January 2023.

Can Kaya, B. '*The Role of AI in Corporate Governance*,' paper delivered at the Istanbul Medeniyet University on 22 June 2022, available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4143846>, last accessed on 14 January 2022.

Carter, E. '*Directors' Liabilities: How Much Risk Are You Prepared to Take?,*' available online at <https://www.kingsleynapley.co.uk/insights/blogs/data-protection-blog/data-protection-a-new-board-room-priority>, last accessed on 13 May 2021.

Chalwin-Milton, A. '*Electronic AGMs in SA: Reacting to a Pandemic,*' available online at <https://www.financialinstitutionslegalsnapshot.com/2020/03/electronic-agms-in-south-africa-reacting-to-a-pandemic/>, last accessed on 15 May 2021.

Clark, J. 'LSE Pushes for Virtual AGMs due to Corona Virus' in *City AM* of 22 March 2020, available online at <https://www.cityam.com/london-stock-exchange-pushes-for-virtual-agms-due-to-coronavirus/>, last accessed on 29 July 2021.

Coenraad, S. *et al*. '*Virtual AGMs in the Wake of Covid-19,*' available online at <https://www.werksmans.com/legal-updates-and-opinions/virtual-agms-in-the-wake-of-covid-19/>, last accessed on 16 May 2021.

ComputerScience.org '*Understanding Automation and AI*,' available online at <https://www.computerscience.org/resources/learn-ai/>, last accessed on 2 July 2022.

Cooper C '*Essay on the Tenth Amendment: Reserved Power for the States,*' available online at <https://www.heritage.org/constitution/#!/amendments/10/essays/163/reserved-powers-of-the-states>, last accessed on 10 December 2018.

Cornell Law School Legal Information Institute '*Negligence,*' available online at <https://www.law.cornell.edu/wex/negligence>, last accessed on 11 July 2021.

Deloitte '*Advancing Environmental, Social and Governance Investing,*' available online at <https://www2.deloitte.com/content/dam/insights/us/articles/5073_Advancing-ESG-investing/DI_Advancing-ESG-investing_UK.pdf>, last accessed on 8 August 2021.

Derchi, G. *et al.* '*CSR Performance, Incentives and Learning Effects,*' available online at <https://link.springer.com/article/10.1007/s10551-020-04556-8>, last accessed on 12 July 2021.

Diamond, C. *et al.* 'Certain Considerations Relating to Virtual Shareholder Meetings,' available online at <https://www.whitecase.com/publications/alert/certain-considerations-relating-virtual-shareholder-meetings>, last accessed on 9 August 2017.

Din, A. '*What is Buffer Overflow?,*' available online at <https://heimdalsecurity.com/blog/what-is-buffer-overflow/#:~:text=In%20information%20security%20and%20programming,access%20to%20a%20company's%20system.>, last accessed on 14 May 2022.

Education and Training Unit (ETU) for Democracy Development '*The Policy and Law-Making Process,*' available online at <https://www.etu.org.za/toolbox/docs/govern/policy.html>, last accessed on 15 January 2023.

Ellis, M. '*ESG vs Sustainability: What is the Difference?*,' available online at <https://www.measurabl.com/esg-vs-sustainability-whats-the-difference/>, last accessed on 19 June 2023.

Encyclopedia Britannica '*Cybercrime,*' available online at <https://www.britannica.com/topic/cybercrime>, last accessed on 5 March 2022.

Fairfax, L. '*Virtual Shareholder Meetings Reconsidered,*' available online at <https://scholarship.law.gwu.edu/faculty_publications/747/>, last accessed on 11 December 2018.

Featherstone, T. '*The AGM Evolution: We Need a Better Format for AGMs,*' available online at <http://aicd.companydirectors.com.au/advocacy/governance-leadership-centre/practice-of-governance/the-agm-evolution-we-need-a-better-format-for-annual-general-meetings>, last accessed on 12 February 2018.

Financial Intermediaries Association (FIA) of Southern Africa '*What is a Directors' Liability Following a Cyber Breach?,*' available online at <https://www.fia.org.za/blog/what-is-a-directors-liability-following-a-cyber-breach/#:~:text=Right%20to%20privacy%3A%20Directors%20and,3%20of%202013%20(POPI)>, last accessed on 27 April 2022.

Gao, H. *et al*. '*Can OAGMs Increase Shareholders' Participation in Corporate Governance?,*' available online at <https://onlinelibrary.wiley.com/doi/abs/10.1111/fima.12301>, last accessed on 19 June 2021.

Gehl R. 'Illuminating the Dark Web' in *The Conversation* of 30 October 2018, available online at <https://theconversation.com/illuminating-the-dark-web-105542>, last accessed on 2 July 2022.

Geroni D. 'Blockchain Scalability Problem: Why is it Difficult to Scale Blockchain?' in *101 Blockchains* of 30 September 2021, available online at <https://101blockchains.com/blockchain-scalability-challenges/>, last accessed on 3 July 2022.

Geroni D. 'What is a Public Blockchain: A Beginner's Guide' in *101 Blockchains* of 10 November 2020, available online at <https://101blockchains.com/public-blockchain/>, last accessed on 3 July 2022.

Gillwald, A. '*Review of Chapter 9 Institutions,*' available online at <https://static.pmg.org.za/docs/2007/070612gillwald2.htm>, last accessed on 30 May 2021.

Goldthorp, A. *et al*. '*The UK CIGA 2020: A Move to a More Debtor-Friendly Restructuring Regime?,*' available online at

<https://www.nortonrosefulbright.com/en/knowledge/publications/5ac21a15/the-uk-corporate-insolvency-and-governance-act-2020>, last accessed on 23 June 2021.

Grant Thornton '*Sustainable Finance: A Guide to the UK Taxonomy,'* available online at <https://www.grantthornton.co.uk/insights/sustainable-finance-a-guide-to-the-eu-taxonomy/>, last accessed on 8 August 2021.

Green Finance Platform 'Non-Financial Reporting Directive (NFRD): Directive 2014/95/EU and the Proposal for a Corporate Sustainability Reporting Directive (CSRD),' available online at <https://www.greenfinanceplatform.org/policies-and-regulations/non-financial-reporting-directive-nfrd-directive-201495eu-and-proposal>, last accessed on 19 June 2023.

Grzybkowski, M. *et al.* '*Internet and Corporate Governance,*' available online at <file:///C:/Users/Julian/Downloads/SSRN-id914520.pdf>, last accessed on 3 February 2022.

Hadwin, S. *et al*. '*Cyber Risk and Directors' Liabilities: An International Perspective,*' available online at <https://www.nortonrosefulbright.com/en-za/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective>, last accessed on 14 May 2021.

Hampton Alexander Review '*FTSE Women Leaders: Improving Gender Imbalance in FTSE Leadership,*' available online at <https://30percentclub.org/assets/uploads/UK/Third_Party_Reports/Hampton_Alexander_Review_Paper_Nov_2016.pdf>, last accessed on 18 February 2018.

Hayath, B. '*Delving Deeper into the Territory of Derivative Actions,*' available online at <https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/corporate/corporate-and-commercial-alert-7-october-delving-deeper-into-the-territory-of-derivative-actions-.html#:~:text=A%20derivative%20action%20is%20an,action%20to%20redress%20such%20wrong>, last accessed on 3 February 2022.

Institute of Chartered Accountants of England and Wales '*Case Law: Court Clarifies Directors' Duties to Shareholders,*' available online at <https://www.icaew.com/archive/library/subject-gateways/law/legal-alert/2016-03/case-law-court-clarifies-directors-duties-to-shareholders>, last accessed on 25 May 2020.

Insurance Information Institute (III) 'Cyberliability Risks,' available online at <https://www.iii.org/article/cyber-liability-

risks#What%20are%20your%20cyber%20liability%20risks?>, last accessed on 10 January 2023.

Jutterström, M. *CSR Standards and Organisations Setting Them* Score Working Paper Series, available online at <https://www.diva-portal.org/smash/get/diva2:649943/FULLTEXT01.pdf>, last accessed on 19 July 2021.

Just Share '*SA Companies' Virtual AGM Arrangements Risk Non-Compliance with Companies Act,*' available online at <https://justshare.org.za/media/news/sa-companies-virtual-agm-arrangements-risk-non-compliance-with-companies-act>, last accessed on 8 July 2021.

Keay, A. 'Accountability and the Corporate Governance Framework: From Cadbury to the UK Corporate Governance Code,' *Social Science Research Network Working Paper* (August 2012), available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143171>, last accessed on 27 June 2023

Keay, A. '*Shareholder Primacy in Corporate Law: Can It Survive? Should It Survive*,' available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1498065>, ladst accessed on 27 June 2023.

Kelion, L. '*Dexter Payment Card Malware Strike SA,'* available online at <https://www.bbc.com/news/technology-24550505>, last accessed on 8 July 2021.

Kirby, H. '*Privacy Protection, A New Beginning: OECD Principles 20 Years On,*' available online at <http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/41.html>, last accessed on 27 December 2019.

Knight W. 'AI Is Coming for Your Most Mind-Numbing Office Tasks' in *Wired* of 14 March 2020, available online at <https://www.wired.com/story/ai-coming-most-mind-numbing-office-tasks/>, last accessed on 2 July 2022.

LaCroix K '*Recent Delaware Caremark Duty Decision Underscores Board Cybersecurity and Privacy Liability Risks,*' available online at <https://www.dandodiary.com/2019/08/articles/director-and-officer-liability/recent-delaware-caremark-duty-decision-underscores-board-cyber-and-privacy-liability-risks/>, last accessed on 21 October 2020.

Lafarre, A. *et al.* '*Blockchain Technology for Corporate Governance and Shareholder Activism*,' European Corporate Governance Institute's Law Working Paper 390/2018, available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135209>, last accessed on 3 February 2022.

Libit, B. '*The CSR Report and Effective Stakeholder Engagement,*' available online at <https://corpgov.law.harvard.edu/2013/12/28/the-corporate-social-responsibility-report-and-effective-stakeholder-engagement/>, last accessed on 12 July 2021.

Litt, R. *et al. The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*, available online at <https://www.americanbar.org/products/inv/book/309654847/>, last accessed on 11 July 2021.

McCarrick, C. '*FI Observer: Data Protection Law Implications for Directors and Officers of Real Estate Investment Trusts' (REITs),*' available online at <https://www.willistowerswatson.com/en-AU/Insights/2019/07/fi-observer-data-protection-law-implications-for-directors-of-real-estate-investment-trusts>, last accessed on 13 May 2021.

McGrath, M. '*Target Profit Falls 46% on Credit Card Breach and the Hits Keep on Coming,*' available online at <https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/?sh=57f7cb937326>, last accessed on 11 May 2021.

Muir, J. '*Five Common Issues that Arise in Corporate Governance,*' available online at <https://jmuirandassociates.com/corporate-governance-issues/>, last accessed on 30 May 2021.

Norton Rose Fulbright SA '*Duties and Responsibilities of Company Directors,*' available online at <https://www.mondaq.com/southafrica/contracts-and-commercial-law/35736/duties-and-responsibilities-of-company-directors>, last accessed on 25 May 2020.

Olzak T. 'Adverserial AI: What It Is and How to Defend Against It?' in *Spiceworks*, available online at <https://www.spiceworks.com/tech/artificial-intelligence/articles/adversarial-ai-attack-tools-techniques/>, last accessed on 2 July 2022.

Pennsylvania State University Library '*US Government: Executive Branch,*' available online at <http://guides.libraries.psu.edu/executive/regulations>, last accessed on 7 December 2018.

Peterson, J. '*Sarbanes-Oxley: Ten Years After - Are We Having Fun Yet?,' available online at* <https://finance.toolbox.com/blogs/jimpeterson/sarbanes-oxley-ten-years-after-are-we-having-fun-yet-080712>, last accessed on 9 July 2021.

Poole, J. *et al.* '*SA: The Role of Directors in the Age of Cybercrime,*' available online at <https://www.mondaq.com/southafrica/directors-and-officers/868876/the-role-of-directors-in-the-age-of-cybercrime>, last accessed on 16 May 2021.

Quora '*What's the Difference Between Buffering, Freezing and Lagging?,*' available online at <https://www.quora.com/What-is-the-difference-between-lagging-freezing-and-buffering-on-a-computer-or-other-device>, last accessed on 28 October 2022.

Ramnath, M. '*Interpreting Directors' Fiduciary Duty to Act in the Company's Best Interests Through the Prism of the Bill of Rights: Taking Other Stakeholders into Consideration,*' available online at <https://webcache.googleusercontent.com/search?q=cache:q1hEDF0peScJ:https://www.dentons.com/en/~/media/c9bf2ed981454d558b598a5c01de5e73.ashx+&cd=1&hl=en&ct=clnk&gl=za>, last accessed on 13 May 2021.

Rathod, L. '*Board of Directors' Fiduciary Duties in Terms of Cybersecurity,*' available online at <https://diligent.com/au/board-directors-fiduciary-duties-terms-cybersecurity/>, last accessed on 26 May 2021.

Sarkar, R. '*Director and Officer Liability and Cyber-Security: Four Questions Every Officer and Director Must Answer (Part 2 of 3),*' available online at <https://www.linkedin.com/pulse/director-officer-liability-cyber-security-4-questions-richik-sarkar-2e>, last accessed on 14 May 2021.

Shani O. 'AI Automation: What You Need to Know' by the *Marketing AI Institute*, available online at <https://www.marketingaiinstitute.com/blog/automation-and-ai-what-you-need-to-know#:~:text=AI%20is%20not%20the%20same,its%20own%20pathways%20to%20success.>, last accessed on 2 July 2022.

Simmons & Simmons '*Extension of Rules that Temporarily Ease Company Meeting Flexibility,*' available online at <https://www.simmons-

simmons.com/en/publications/ckaifpkvmkkhu0900lf31ftdf/proposals-to-temporarily-ease-company-meetings-and-filing-requirements>, last accessed on 23 June 2021.

Slaughter and May '*Cybersecurity: Corporate Insights for Companies and Their Directors,*' available online at <https://prodstoragesam.blob.core.windows.net/highq/2536333/cyber-security-corporate-insights-for-companies-and-their-directors.pdf>, last accessed on 11 May 2021.

S.n. 'Decentralised vs Centralised: A Detailed Comparison' in *101 Blockchains* of 29 May 2021, available online at <https://101blockchains.com/decentralized-vs-centralized/>, last accessed on 3 July 2022.

S.n. 'Know Everything About Blockchain Proof of Work (PoW)' in *101 Blockchains* of 29 March 2019, available online at <https://101blockchains.com/blockchain-proof-of-work/>, last accessed on 3 July 2022.

Spadafora, A. '*Zoom Security Issues: What's Gone Wrong and What's Been Fixed*,' available online at <https://www.tomsguide.com/news/zoom-security-privacy-woes>, last accessed on 5 October 2022.

StarTechUp '*AI Consulting: Everything You Need to Know*,' available online at <https://www.startechup.com/blog/ai-consulting-everything-you-need-to-know/#:~:text=AI%20consulting%20is%20the%20practice,intelligence%20to%20improve%20company%20operations.>, last accessed on 24 January 2023.

Steeden, S. *et al.* '*CIGA,*' available online at <https://bateswells.co.uk/2020/07/corporate-insolvency-and-governance-act-2020/?hub=coronavirus>, last accessed on 22 June 2021.

The Corporate Governance Review '*US: Delaware,*' available online at <https://thelawreviews.co.uk/edition/the-corporate-governance-review-edition-7/1140934/united-states-delaware>, last accessed on 12 February 2018.

Thomson Reuters Practical Law Corporate '*Virtual and Hybrid General Meetings: Practical Considerations and Best Practice*,' *s.p.*, available online at <https://uk.practicallaw.thomsonreuters.com/w-029-6286?transitionType=Default&contextData=(sc.Default)>, last accessed on 17 June 2023.

Tozzi, C. 'What is AI-Assisted Coding and Should You Use It?' in *ITPro Today* of 16 December 2022, *s.p.*, available online at <https://www.itprotoday.com/development-techniques-and-management/what-ai-assisted-coding-and-should-you-use-it>, last accessed on 24 January 2023.

Usercentrics '*The Colorado Privacy Act: An Overview,*' available online at <https://usercentrics.com/knowledge-hub/colorado-privacy-act/#:~:text=What%20is%20the%20Colorado%20Privacy,doing%20business%20in%20the%20state.>, last accessed on 16 June 2022.

Visser, A. '*The Application and Enforcement of King IV,*' available online at <https://www.adams.africa/wp-content/uploads/2020/04/King-IV_APPLICATION_ENFORCEMENT.pdf>, last accessed on 27 April 2022.

Werksmans '*Duties and Liabilities of Directors,*' available online at <https://www.werksmans.com/wp-content/uploads/2013/04/Director-duties-and-liabilities-FINAL-updated-electronic.pdf>, last accessed on 3 February 2022.

Weston G. 'A Definitive Guide on Cryptocurrencies' in *101 Blockchains* of 10 April 2022, available online at <https://101blockchains.com/what-is-cryptocurrency/>, last accessed on 3 July 2022.

Younghusband, V. '*Electronic Meetings: Holding a Virtual AGM,*' available online at <https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/corporate/2017/electronic-meetings--holding-a-virtual-agm/>, last accessed on 11 February 2018.

XIII. NEWSPAPERS AND MAGAZINES

Cao, S. 'Warren Buffet Hosts His First Online Shareholders Meeting' in *Observer* of 1 May 2011, available online at <https://observer.com/2020/05/warren-buffett-online-berkshire-hathaway-shareholder-meeting-2020-coronavirus/>, last accessed on 6 August 2021.

Clark, M. 'Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer' in *International Business Times* of 5 May 2014, available online at <https://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056>, last accessed on 8 July 2021.

CNBC Staff Report '*JP Morgan Attack Hits 76 Million Households,*' available online at <https://www.cnbc.com/2014/10/02/jpmorgan-details-breadth-of-march-cyberattack.html>, last accessed on 8 July 2021.

Drenik, G. 'Cybercrime is Evolving: AI Can Help Improve Consumer Safety Online,' in *Forbes* of 17 May 2022, *s.p.*, available online at <https://www.forbes.com/sites/garydrenik/2022/05/17/cybercrime-is-evolving-artificial-intelligence-can-help-improve-consumer-safety-online/?sh=195648f615d0>, last accessed on 6 January 2023.

Durbin, S. 'How Cybercriminals Use AI to Fuel Cyberattacks' in *Forbes* of 13 October 2020, *s.p.*, available online at <https://www.forbes.com/sites/forbesbusinesscouncil/2020/10/13/how-criminals-use-artificial-intelligence-to-fuel-cyber-attacks/>, last accessed on 13 January 2023.

Fihlani, P. 'Millions Caught in SA's 'Worst Data Breach' on *BBC News* of 20 October 2017, *s.p.*, available online at <https://www.bbc.com/news/world-africa-41696703>, last accessed on 8 July 2021.

Flores-Araoz, M. 'CSR in SA: More Than a Nice Intention' in *Polity* of 12 September 2011, *s.p.*, available online at <https://www.polity.org.za/article/corporate-social-responsibility-in-south-africa-more-than-a-nice-intention-2011-09-12>, last accessed on 18 May 2019.

Goba, T. 'DoJ Found Guilty of Being Negligent in Its Actions to Prevent a Data Breach' in *Eyewitness News* of 10 May 2023, *s.p.*, available online at <https://ewn.co.za/2023/05/10/doj-found-guilty-of-being-negligent-in-its-actions-to-prevent-a-data-breach>, last accessed on 12 June 2023.

Home Depot '*The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in all US Stores,*' Press Release of 18 September 2014, available online at <https://ir.homedepot.com/news-releases/2014/09-18-2014-014517752>, last accessed on 8 July 2021.

Hosken, G. 'Military Secrets Stolen' in *Times Live SA* of 13 July 2016, s.p., available online at <https://www.timeslive.co.za/news/south-africa/2016-07-13-military-secrets-stolen/>, last accessed on 19 June 2021.

Iaquinto, C. *et al.* 'Cybersecurity and Privacy: Fiduciary Considerations and Dodd-Frank's Enterprise Risk Management' in the *Financier Worldwide* of April 2019,

available online at <https://www.hklaw.com/en/insights/publications/2019/04/cyber-security-and-privacy-fiduciary-considerations-and-doddfranks-ent>, last accessed on 11 July 2021.

Knowler, W. 'Zoombombing on its Way Out, Plus Tips on How to Ace Video Conferencing and Save Data' in *Times Live* of 18 June 2020, *s.p.*, available online at <https://www.timeslive.co.za/news/consumer-live/2020-06-18-zoombombing-on-its-way-out-plus-tips-on-how-to-ace-video-conferencing-and-save-data/>, last accessed on 11 June 2023.

Lorenz, T. 'Zoombombing: When Videoconferences Goes Wrong' in the *NY Times* of 20 March 2020, available online at <https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html>, last accessed on 24 January 2023.

Malinga, S. 'Telkom's 5G Network Goes Live in Various Parts of SA' in *ITWeb* of 27 January 2022, *s.p.*, available online at <https://www.itweb.co.za/content/WnxpEv4YYxy7V8XL>, last accessed on 6 January 2023.

McKoy, K. 'Target to Pay $18.5 Million for 2013 Data Breach that Affected 41 Million Consumers' in *USA Today* of 23 May 2017, available online at <https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/>, last accessed on 8 July 2021.

Morgenson, G. 'Meet the Shareholders? Not at These Shareholder Meetings' Business Day Supplement of the *NY Times* of 31 March 2017, available online at <https://www.nytimes.com/2017/03/31/business/corporate-virtual-shareholder-meetings.html>, last accessed on 9 August 2017.

Moshe, J. 'Zoombombing Takes Anti-Semitic Twist' in the *SA Jewish Report* of 2 June 2020, *s.p.*, available online at <https://www.sajr.co.za/zoombombing-takes-on-an-anti-semitic-twist/>, last accessed on 11 June 2023.

Moyo, A. 'Over 3.6 Million Records Exposed in Dis-Chem Cyberattack' in *ITWeb* of 11 May 2022, available online at <https://www.itweb.co.za/content/PmxVE7KEABOqQY85>, last accessed on 18 January 2023.

Moyo, A. 'Virtual AGM's May Infringe SA Companies Act' in *ITWeb* of 13 May 2020, *s.p.* available online at <https://www.itweb.co.za/content/KPNG878K2brv4mwD>, last accessed on 15 May 2021.

Nieselow, T. 'Five Massive Data Breaches Affecting South Africans' in *Mail and Guardian* of 19 June 2018, available online at <https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/>, last accessed on 19 June 2021.

Reuters 'SA's Transnet Restores Operations at Ports After Cyberattacks' in *Reuters* of 29 July 2021, *s.p.*, available online at <https://www.reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ>, last accessed on 12 June 2023.

Riley, T. 'The Cybersecurity 202: Companies Are Doing a Terrible Job at Reporting Cybersecurity Risks to Investors, New Report Says' in *Washington Post* of 5 March 2021, *s.p.*, available online at <https://www.washingtonpost.com/politics/2021/03/05/cybersecurity-202-companies-are-doing-terrible-job-reporting-cybersecurity-risks-investors-new-study-says/>, last accessed on 12 May 2021.

Shapshak, T. 'Cinema Chain Ster-Kinekor Hacked in SA's Biggest Data Breach' Data at Risk' in *Forbes* of 17 March 2017, *s.p.*, available online at <https://www.forbes.com/sites/tobyshapshak/2017/03/17/cinema-chain-ster-kinekor-hacked-in-south-africas-biggest-data-breach/?sh=5e84f3b95fa1>, last accessed on 19 June 2021.

Shapshak, T. 'Note to Transnet: Cyberattacks Only Works When There Are Vulnerabilities to Exploit' in the *Daily Maverick* of 4 August 2021, *s.p.*, available online at <https://www.dailymaverick.co.za/opinionista/2021-08-04-transnet-ports-closed-and-were-in-the-dark/>, last accessed on 12 June 2023.

Shapshak, T. 'SA's Parliamentarians Zoombombed with Porn Images' in *Forbes* of 11 May 2020, *s.p.*, available online at <https://www.forbes.com/sites/tobyshapshak/2020/05/11/south-africas-parliamentarians-zoombombed-with-porn-images/>, last accessed on 11 June 2023.

Smith, C. 'From Fake Links to OMs to Drones: SA Companies Warned of Cyberattacks' in *News24* of 4 December 2022, *s.p.*, available online at <https://www.news24.com/fin24/companies/sa-businesses-warned-of-cyber-attacks-involving-fake-links-for-online-meetings-and-drones-20221204>, last accessed on 11 June 2023.

S.n. 'Adobe Warns 2.9 Million Customers of Data Breach After Cyberattack' in *The Guardian* of 3 October 2013, available online at <http://www.theguardian.com/technology/2013/oct/03/adobe-hacking-databreach-cyber-attack>, last visited on 8 July 2021.

S.n. '41 000 Nedbank Clients' Cellphone Numbers Retrieved in Cyberattack' in *TimesLive* of 23 March 2023, *s.p.*, available online at <https://www.businesslive.co.za/bd/national/2023-03-24-41000-nedbank-clients-cellphone-numbers-retrieved-in-cyberattack/>, last accessed on 12 June 2023.

Staff Writer 'Cyril Ramaphosa's Private Data Hacked' in *MyBroadband* of 29 May 2022, *s.p.*, available online at <https://mybroadband.co.za/news/security/446282-cyril-ramaphosas-private-data-hacked.html>, last accessed on 12 June 2023.

Staff Writer 'How AI Is Being Used in SA' in *BusinessTech* of 10 June 2019, *s.p.*, available online at <https://businesstech.co.za/news/enterprise/322505/how-ai-is-being-used-in-south-africa/#:~:text=Nearly%20half%20(46%25)%20of,Process%20Automation%20and%20Advanced%20Analytics>, last accessed on 13 January 2023.

Staff Writer 'Internet Fraud and Phishing Costs SA R2.2 Billion' in *BusinessTech* of 14 September 2014, available online at <https://businesstech.co.za/news/trending/68212/sa-internet-fraud-and-phishing-costs-r2-2-billion/>, last accessed on 8 July 2021.

Sutherland, C. 'History of SA Cyberlegislation' in *ITWeb* of 7 February 2019, available online at <https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o>, last accessed on 14 January 2023.

Vermeulen, J. 'This Article Was Written by an AI: What is 5G and How Will it Benefit SA' in *MyBroadband* of 3 December 2022, *s.p.*, available online at <https://mybroadband.co.za/news/software/472475-this-article-was-written-by-an-artificial-intelligence.html>, last accessed on 6 January 2023.

Von Solms, B. in 'Kubermisdaad Gaan Groei' in *Die Burger* of 2 November 2022, 14.

XIV. SOURCES RELATED TO SERVICE PROVIDERS AND THEIR WEBSITES

Cloudflare '*What is The Mirai Botnet?*,' available online at <https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>, last accessed on 2 July 2022.

Computershare Ltd '*The Future of Shareholder Meetings is Virtually Here,*' available online at <http://www.computershare.com/News/Virtual-Meetings.pdf>, last accessed on 12 January 2018.

Dataprot *'55 Fascinating AI Statistics and Trends*,' available online at <https://dataprot.net/statistics/ai-statistics/#:~:text=Key%20AI%20statistics,billion%20a%20year%20by%202025.>, last accessed on 25 January 2023.

Deloitte '*Duties of Directors,*' available online at <https://www.google.com/search?q=deloitte+duties+of+directors&rlz=1C1AOHY_enZA708ZA708&oq=Deloitte+Duties+&aqs=chrome.1.69i57j0l4j69i61.5172j0j8&sourceid=chrome&ie=UTF-8>, last accessed on 13 December 2019.

Deloitte '*Duty of Care,*' available online at <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-customer-breach-support-duty-of-care-white-paper.pdf>, last accessed on 19 June 2022.

Deloitte SA '*Post Covid-19: The Benefits and Challenges of Virtual AGMs,*' available online at <https://www2.deloitte.com/content/dam/Deloitte/za/Documents/za-Post-Covid-19-Publication-Virtual-AGMs-Final.pdf>, last accessed on 8 July 2021.

Equiniti '*AGM Trends 2017,*' available online at <https://equiniti.com/media/3492/8056eqb_agm_brochure-v5-310817.pdf>, last accessed on 8 February 2018.

Fireeye '*AI in the Cyber Domain*,' available online at <https://www.fireeye.com/blog/products-and-services/2018/03/artificial-intelligence-in-the-cyber-domain.html>, last accessed on 2 July 2022.

Fortinet '*Overcoming the Challenges of Rapid and Effective Incident Responses*,' available online at <https://www.fortinet.com/blog/industry-trends/overcoming-the-challenges-of-rapid-and-effective-incident-response>, last accessed on 2 July 2022.

Github.com '*Where the World Builds Software*,' available online at <https://github.com/>, last accessed on 2 July 2022.

Google '*Advancing AI for Everyone*,' available online at <https://ai.google/>, last accessed on 2 July 2022.

IBM '*Machine Learning*,' available online at <https://www.ibm.com/za-en/cloud/learn/machine-learning>, last accessed on 24 January 2023.

Lumi '*What is a Hybrid AGM?,*' available online at <https://go.lumiglobal.com/what-is-a-hybrid-agm#:~:text=Hybrid%20AGM%20Meaning,traditional%20AGM%20and%20virtual%20AGM>, last accessed on 8 July 2021.

Microsoft '*CyberSignals*,' available online at <https://news.microsoft.com/cyber-signals/>, last accessed on 2 July 2022.

Nasdaq '*Nasdaq to Deliver Blockchain E-Voting to Strate,*' available online at <https://ir.nasdaq.com/news-releases/news-release-details/nasdaq-deliver-blockchain-e-voting-solution-strate>, last accessed on 4 August 2021.

Penta Security '*Top 5 AI-Powered Cyberthreats and How to Avoid Them*,' available online at <https://www.pentasecurity.com/blog/top-5-ai-powered-cyber-threats-how-to-prevent-them/>, last accessed on 2 July 2022.

Strate '*Adoption of Digital Solutions for AGMs is Long Overdue,*' available online at <https://www.strate.co.za/2020/07/03/adoption-of-digital-solutions-for-agms-is-long-overdue/>, last accessed on 15 May 2021.

Strate '*Strate Holds First Remote AGM,*' available online at <https://www.strate.co.za/2020/05/>, last accessed on 4 August 2021.

Strate '*Strate e-Voting Continues to Serve Market Amidst Covid-19,*' available online at <https://www.strate.co.za/2020/03/25/strate-e-voting-continues-to-serve-the-financial-markets-amidst-covid-19/>, last accessed on 4 August 2021.

Surfshark '*Global Data Breach Heat Map 2021*,' available online at <https://surfshark.com/research/data-breach-impact/statistics>, last accessed on 5 October 2022.

Vigeo '*Integration of CSR into Corporate Governance System,*' available online at <https://vigeo-eiris.com/wp-content/uploads/2013/06/2013_12_Vigeo_Governance_Study_GB.pdf>, last accessed on 12 July 2021.

XV. WEBSITES OF COMPANIES' OMs AND RELATED INFORMATION

Exxaro '*Summarised Group Annual Financial Statements for the Year Ended 31 December 2019 and Notice of AGM,*' available online at <https://www.exxaro.com/assets/files/Exxaro-Notice-to-AGM-2019.pdf>, last accessed on 20 June 2021.

Johnson & Johnson 'Investor Information,' available online at <http://www.investor.jnj.com/>, last accessed on 9 August 2017.

Microsoft '*Microsoft Annual Shareholders' Meeting 2019,*' available online at <https://www.microsoft.com/en-us/Investor/events/FY-2020/2019-Annual-Shareholder-Meeting>, last accessed on 6 August 2021

Old Mutual '*AGM, 21 May 2021,*' available online at <https://www.oldmutual.com/about/governance/annual-general-meeting/>, last accessed on 9 July 2021.

Old Mutual '*Notice of AGM for the Year Ended 31 December 2020,*' available online at <https://www.oldmutual.com/v3/assets/blt566c98aeecc1c18b/bltcaf2ee861b069f47/607d6facb290e724ab00aad0/2021-04-14_-_OM_Notice_of_AGM.PDF>, last accessed on 20 June 2021.

PayPal '*Questions for PayPal Holdings Inc, 2017 Annual Meeting of Stockholders,*' available online at <https://materials.proxyvote.com/default.aspx?dochostid=325761>, last accessed on 6 August 2021.

Remgro Ltd '*OM Shareholders' Guide 2020,*' available online at <https://www.remgro.com/wp-content/uploads/2020/11/Remgro-Virtual-Meeting-Instructions.pdf>, last accessed on 20 June 2021.

Roman, A. '*What HP's Virtual Annual Shareholder Meeting Means for Remote Meetings,*' available online at <https://www.azeusconvene.com/articles/virtual-annual-shareholder-meeting-means-means-remote-meetings>, last accessed on 6 August 2021.

Standard Bank '*AGM, 27 May 2021,*' available online at <https://reporting.standardbank.com/agm/>, last accessed on 9 July 2021.

Strate '*Annual Integrated Report 2020,'* available online at <https://www.strate.co.za/wp-content/uploads/2021/06/Strate-INTEGRATED-REPORT-2020.pdf>, last accessed on 4 August 2021.

XVI. BLOGS

Alechina, N. 'Autonomous Intelligence Systems' in the *Human-Centered AI Interest Group* site of Utrecht University, available online at <https://www.uu.nl/en/research/human-centered-artificial-intelligence/special-interest-groups/autonomous-intelligent-systems>, last accessed on 24 January 2023.

Chiu, I. *et al.* 'Relief and Rescue Policies in Financial Regulation at the Time of the Pandemic' on *OBLB*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/relief-and-rescue-policies-financial-regulation-time-pandemic>, last accessed on 8 August 2021.

Chiu, I. *et al.* 'Technology vs Ideology: How Far Will AI and Distributed Ledger Technology Transform Corporate Governance and Business' on *OBLB*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/technology-vs-ideology-how-far-will-artificial-intelligence-and>, last accessed on 8 August 2021.

Jubb, G. *et al.* 'The Future of the AGM' on *Oxford Business Law Blog* (*OBLB*), available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/future-agm>, last accessed on 8 August 2021.

Lyons, S. 'Governance Bodies Endorse Value Preservation as Primary Purpose and Fiduciary Duty' on *OBLB*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/governance-bodies-endorse-value-preservation-primary-purpose-and>, last accessed on 8 August 2021.

Matera, P. 'Delaware's Dominance and Wyoming's Dare: Blockchain Companies and the Market for Corporate Chraters' on *Oxford Business Law Blog* (OBLB), available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/delawares-dominance-wyomings-dare-blockchain-companies-and-market>, last accessed on 8 August 2021.

Reddy, B. ‘The Emperor’s New Code? Time to Re-Evaluate the Nature of Stewardship Engagement Under the UK’s Stewardship Code’ on *OBLB*, available online at <https://www.law.ox.ac.uk/business-law-blog/blog/2021/03/emperors-new-code-time-re-evaluate-nature-stewardship-engagement>, last accessed on 8 August 2021.

Sutherland, C. ‘What Is a Director’s Liability Following a Cyber Breach?’ in *ITWeb* of 14 June 2018, available online at <https://www.itweb.co.za/content/nWJadvb8ARmMbjO1>, last accessed on 27 April 2022.

APPENDIX

I. LIST OF DEFINITIONS (in alphabetic order)

AGM

The Act, section 1 *s.v.* states that an 'AGM' is the meeting held by a public company as required by section 61(7).[2187]

Section 61(7) requires a public company to have an AGM (a) within eighteen months after being set up; and (b) then annually. [2188]

The oversight over the board vests with shareholders at the AGM, the governing power vests with the board and the power to manage the company vests with the management.[2189]

Artificial Intelligence (AI)

AI refers to a computer's artificial replication of natural intelligence, in order to reason.[2190] Such a computer applies self-correcting algorhythms that can generate hypotheses with likely answers.[2191] AI also refers to intelligent devices that replicates human activities.[2192] AI consists of different sub-types that are available to companies and that could be used to help improve company's cybersecurity, especially at their OMs.[2193]

Blockchain

A Blockchain is a public ledger that records information across various computer systems, so that the information cannot be altered on just one computer system.[2194] When information is altered on one computer system it is automatically altered on various computer systems due to the decentralised nature of the public ledger that helps to store AI.[2195]

Board

The Act, (1) states that the board has oversight over a company, and that the MOI prescribes their governing powers and functions they need to perform.[2196]

[2187] The Act, sections 1 *s.v.* 'annual general meeting'; 61(7).
[2188] The Act, section 61(7).
[2189] Miles *et al. op cit* 111.
[2190] Sarker *op cit* 1 - 2.
[2191] *Ibid*.
[2192] *Ibid.*
[2193] Shani *op cit s.p.*
[2194] Synopsis *op cit s.p.*
[2195] *Ibid.*
[2196] The Act, section 66(1).

Buffering

A constant breakdown in the loading of the live feed due to a software coding error.[2197]

Business E-Mail Compromise (BEC)

Business E-Mail Compromise (BEC) is a type of scam performed by hackers who gain access to OMs via personal e-mail accounts through social engineering and online intrusion.[2198]

Consultative AI

Consultative AI uses unique algorithms and machine learning tools so that companies can create AI-driven solutions.[2199] The algorithms of Consultative AI is in other words used to improve company operations.[2200]

Corporate Governance

No generally accepted definition for the concept of corporate governance exists.[2201] A definition for corporate governance was provided by the Cadbury Report, which explains that corporate governance aims to harmonise a company's economic and social goals as well as shareholders' goals with other stakeholders' goals in an attempt to unite the interests of the company, shareholders, stakeholders, its community and environment in the way in which a company is governed.[2202]

This was also the definition that King Report II stated in its introduction.[2203] King Report IV elaborated on this by tasking the board with effective governance, and to practice ethical values, to seek optimal performance and legitimacy.[2204]

The Act provides no definition for corporate governance.

Corporate Social Responsibility (CSR)

King Report IV defined CSR in terms of corporate citizenship that places the company as a role player in the community and environment in which it operates – and defines it as an entity that has certain rights and responsibilities within that community

---

[2197] Quora *op cit s.p*.
[2198] US FBI *op cit s.p.*
[2199] StarTechUp *op cit s.p.*
[2200] *Ibid.*
[2201] Keay *Board Accountability on Corporate Governance op cit* 15.
[2202] UK Committee on Financial Aspects of Corporate Governance *op cit* 'Introduction,' paragraph 2.5.
[2203] IoDSA '*King Report II*' *op cit* 7.
[2204] IoDSA '*King Report IV*' *op cit* 11.

and environment.[2205] CSR is about acknowledging that the broader society is the company's licensor and that it should therefore invest therein.[2206]

The Act provides no definition for CSR.

Critically Conscious Computing (CCC)

Critically conscious computing (CCC) uses a platform that incorporates AI with signal processing that allows a computer and a human to interact.[2207] CCC can process an array of signals, such as language processing, machine learning, narrative generation, reasoning and speech recognition, while it replicates human intelligence.[2208]

Cyberbreach

A cyberbreach is an incident where confidential, protected, sensitive information is either stolen, copied, transmitted, viewed or used by an unauthorised party.[2209] This information is usually of a personal nature.[2210] This information could belong to the company itself (intellectual property) or it could be shareholders' or stakeholders' personal information that is compromised.[2211]

Cybercrime

Cybercrime is performed online on computers and the Internet.[2212] It refers to criminal activities that are committed on a computer system, with the use of software and the Internet.[2213] Cybercrime is caused by cybercriminals who engage in online criminal behaviour ranging from nuisance or political hacking to the spreading of computer viruses to criminal extortion to government-sponsored espionage and all out cyberwar.[2214] The term is not expressly defined in the SA ECTA 25 of 2002, the SA RICA 70 of 2002, the SA POPI 4 of 2013, nor the SA Cybercrimes Act 19 of 2020.[2215]

For the purposes of this thesis, cybercrimes include bribery, corporate scams, embezzlement, forgery, fraud, money laundering and tax evasion.

Cyberforgery

[2205] IoDSA '*King Report IV*' *op cit* 11.
[2206] Amodu *op cit* 2.
[2207] Gudivada *et al. op cit* 13.
[2208] *Ibid.*
[2209] Sutherland '*What is a Directors Liability Following a Cyberbreach?*'*op cit s.p.*
[2210] *Ibid.*
[2211] *Ibid.*
[2212] Mabunda *op cit* 9 – 14.
[2213] *Ibid.*
[2214] Encyclopedia Britannica '*Cybercrime,*' *s.p.*, available online at <https://www.britannica.com/topic/cybercrime>, last accessed on 5 March 2022.
[2215] SA ECTA 25 of 2002; SA RICA 70 of 2002; SA POPI 4 of 2013; SA Cybercrimes Act 19 of 2020.

Cyberforgery is where one party creates false information with the intention to commit fraud with someone else.[2216]

Cyberfraud

Cyberfraud is where a cybercriminal unlawfully and intentionally makes misrepresentations online that causes someone to suffer actual or potential harm.[2217]

Cyberuttering

Cyberuttering is the online presentation of false information with the intention to cause actual or potential harm to someone else.[2218] An example is when someone pass off a false ID as an authentic ID in order to obtain an advantage.[2219]

Cyberresilience

Cyberresilience is the ability of a company to successfully resist a cyberbreach and to continue improving its ability in this regard.[2220] As part of their duty of care, directors need to ensure that their activities and decisions result in a continuous and up-to-date cyberresilience strategy.[2221]

Cybersecurity

Cybersecurity is security measures to safeguard virtual assets and has the aim to safeguard corporate and personal information and prevent online fraudulent transactions, online identity theft, online intellectual property loss, damage caused online to infrastructure and the compromise or loss of classified or personal information.[2222]

Cybersecurity 'Red Flags'

Cybersecurity 'red flags' indicate any pattern of cyberincidents that led to a cyberbreach and that should have been detected and indicated security risks to the board.[2223]

The term was introduced in 1996 by Allen C of the Delaware Court of Chancery held in *In Re Caremark International Derivative Litigation*.[2224]

[2216] SA Cybercrimes Act 19 of 2020, section 9(1).
[2217] SA Cybercrimes Act 19 of 2020, section 8.
[2218] SA Cybercrimes Act 19 of 2020, section 9(2).
[2219] Ibid.
[2220] IoDSA '*Governing Body's Role in Cyber Resilience' op cit* 3.
[2221] *Ibid*.
[2222] US Cybersecurity and Infrastructure Security Agency, '*Cybersecurity,' s.p.*, available online at <https://www.cisa.gov/uscert/ncas/tips/ST04-001>, last accessed on 5 March 2022.
[2223] US FTC '*Fighting Identity Theft with the 'Red Flag' Rule' op cit s.p.*
[2224] *In Re Caremark supra*.

Data Analysis

Data Analysis uses AI and machine learning to manage, process and store large volumes of data that cannot be processed manually.[2225] The insights which it produces from such information are then used to improve the quality of decisions that humans need to make.[2226]

Director

In terms of the Act, section 1, director refers to a board member of a company, as set out in section 66, as well as a non-executive director (or alternate director) and also refers to anyone who occupies such a position, even it is designated by another name.[2227]

Duty of Care

In Company Law, the duty of care is the moral or legal obligation of directors to ensure the safety and well-being of others.[2228]

The Act, section 76(3)(c) states that a director, when they act in their capacity, must do so in good faith and with the standard of care, skill and diligence that may be reasonably expected of someone in their position acting with the same experience and skills.[2229]

This means that directors should have an objective evaluation of their work based on the subjective criteria of someone who acts with the same level of skill and intellect.[2230] When a director fails to exercise the required due care, they could be held personally liable in terms of section 77(2) for any damages that follow.[2231]

Environmental, Social and Governance (ESG) Investment Considerations

Environmental, Social and Corporate Governance (ESG) investing focuses on the risk and return consequences when investors incorporate ESG considerations in their investment decisions.[2232] The ESG model of investing has since become the universally accepted investment approach and is regulated by various codes and requirements in each country.[2233] It requires investors to also take ESG considerations

---

[2225] Boura *et al op cit* 261.
[2226] *Ibid*.
[2227] The Act, section 1 *s.v.* 'director;' section 66.
[2228] Deloitte '*Duty of Care' op cit* 3.
[2229] The Act, section 76(3)(c).
[2230] Poole *et al. 'SA: The Role of Directors in the Age of Cybercrime,' s.p.*, available online at <https://www.mondaq.com/southafrica/directors-and-officers/868876/the-role-of-directors-in-the-age-of-cybercrime>, last accessed on 16 May 2021.
[2231] The Act, section 77(2).
[2232] Esser *et al.* 'From a Financial to an Entity Model of ESG' in *European Organisation Business Law Review* (26 April 2021) 1.
[2233] *Ibid*.

into account when they make their investment decisions in order to minimise environmental risks (such as climate change), social risks (such as any infrigements on human rights) and governance risks (such as ineffective corporate oversight), which could harm their investment.[2234] This model in other words focuses on the role that investors and their investments should play to help promote sustainable corporate practices instead of the role of directors' decisions and their duties can play in this regard.[2235]

Fifth Generation (5G) Technology

Fifth generation (5G) cellular network technology follows on 2G, 3G and 4G networks.[2236] It performs faster and connects more efficient than the previous networks, and can reach speeds of up to 20 Gbps.[2237] It also has a higher capacity than previous networks and can accommodate more devices on a single network.[2238]

Freezing

Freezing is caused by either too many online processes happening at once on a computer, a shortage of Random Access Memory (RAM) or malware, and causes the central processing unit (CPU) of a computer to stop working (IT term).[2239]

Hacking

Hacking is the crime of unlawful online access, and is committed when a cybercriminal intentionally and unlawfully accesses computers, online systems or smart phones.[2240]

Hybrid Meeting

A hybrid meeting is an ordinary meeting that is held at a physical place, but that also allows online participation from participants situated at other locations.[2241] Such remote-shareholder participation is usually facilitated by telephone or webcast.[2242]

[2234] Esser *et al. op cit* 2.
[2235] *Ibid*.
[2236] Vermeulen *op cit s.p.*
[2237] *Ibid.*
[2238] *Ibid.*
[2239] Quora *op cit s.p.*
[2240] SA Cybercrimes Act 19 of 2020, section 2.
[2241] Lumi '*What is a Hybrid AGM?,' s.p.*, available online at <https://go.lumiglobal.com/what-is-a-hybrid-agm#:~:text=Hybrid%20AGM%20Meaning,traditional%20AGM%20and%20virtual%20AGM>, last accessed on 8 July 2021.
[2242] *Ibid.*

Hybrid meetings differ from OMs, because a hybrid meeting occurs at a physical place but allows for online access, while an OM occurs entirely online.[2243]

Neither the Act nor King Reports I - IV give a definition for such a meeting.

Information Officer (IO)

IoDSA's 'King III: Report on Corporate Governance for SA of 2009,' section 20 compels the CEO to appoint an IO to manage IT.[2244]

Section 22 states that the IO is responsible for: IT;[2245] should compile the IT policy of the company and implement it;[2246] should integrate IT strategically into the company;[2247] and develop IT solutions to help achieve the company's goals.[2248]

Lagging

A slowing down of the online live feed on a computer due to a software coding error (IT term).[2249]

Machine Learning

Machine Learning uses an algorithm that replicates the way in which humans learn, and which, through its own continuous learning, improve its own accuracy over time.[2250] This type of AI in other words leverage data to improve its own performance when it does the tasks that it is given.[2251]

Mangement

Management is the administration in the company, who is responsible to implement the decisions of shareholders' meetings and the board.

MOI

The Act, section 1 states that a MOI prescribes the roles and responsibilities of the directors and shareholders towards each other, towards the company and in terms of the section 15.[2252]

[2243] Equiniti '*AGM Trends 2017,*' 8, available online at <https://equiniti.com/media/3492/8056eqb_agm_brochure-v5-310817.pdf>, last accessed on 8 February 2018.
[2244] IoDSA '*King Report III*'*op cit* Chapter 5, section 20.
[2245] IoDSA '*King Report III*' *op cit* Chapter 5, sections 22.1; 22.2; 22.3; 22.4.
[2246] *Ibid.*
[2247] *Ibid.*
[2248] *Ibid.*
[2249] Quora *op cit s.p.*
[2250] IBM *op cit s.p.*
[2251] *Ibid.*
[2252] The Act, sections 1 *s.v.* 'memorandum of incorporation'; 15.

Section 15(2)-(3) allows a company to determine the limits and boundaries in which it operates.[2253] Section 15(2) states that a MOI may (*a*) add a provision that will (iii) require a higher standard of the company.[2254]

OM

Although the Act, section 1 does not define an OM, its most common definition is that it is a shareholders' meeting, which is held entirely in cyberspace through online communication, in real-time, without a physical meeting place.[2255]

In terms of section 61(10) "every shareholders' meeting of a public company must be reasonably accessible within SA for online participation by shareholders, subject to section 63(2), regardless of whether the meeting is held in SA or elsewhere".[2256]

Section 63(2) says that "unless prohibited by its MOI, a company may provide for (a) a shareholders meeting to be conducted entirely by online communication; or (b) one or more shareholders, or proxies, to participate by online communication in all or part of a shareholders' meeting that is being held in person, as long as the online communication ordinarily enables all participants to communicate concurrently with each other without an intermediary, and to participate reasonably effectively."[2257]

An OM is facilitated by software programmes, such as Microsoft Teams or Zoom, an app such as FaceTime, a conference call dial-in, live streaming, Skype or through a web browser, a custom-made online platform, such as the JSE online platform, or a combination of these.

Neither the Act nor King Reports I - IV gives a definition for such a meeting.

Ordinary Shareholders' Meeting

The Act, section 1, *s.v.* defines an 'ordinary shareholders' meeting' as a meeting of the shareholders of a company's issued shares who may vote because of the voting rights that attach to their shares.[2258]

The Act affords shareholders at an ordinary meeting considerable rights, namely: section 16(1)(c)'s right to amend the MOI; section 15(4) and (5)'s right to vote on and approve rules on the governance of the company; section 71(1)'s right to dismiss directors; section 70(3)(b)'s right to appoint directors; and section 112(2)(a)'s right to dispose of company assets.[2259]

[2253] The Act, section 15(2)-(3).
[2254] The Act, section 15(2)(a)(iii).
[2255] Equiniti '*AGM Trends 2017'op cit* 8.
[2256] The Act, sections 61(10); 63(2).
[2257] The Act, section 63(2)(a)–(b).
[2258] The Act, section 1 *s.v.* 'shareholders' meeting'.
[2259] The Act, sections 15(4); 15(5); 16(1)(c); 70(3)(b); 71(1); 112(2)(a).

Personally Identifiable Information (PII)

OMs make use of personally identifiable information (PII), which is of a sensitive nature and that could lead to the direct or indirect identification of an individual.[2260] This could include contact information, financial information, official identification information, personal histories, physical information or relationship information.[2261] It could also include PII on algorithms, biometric information, IP addresses, locations, online communications and online voting records, which are based on Blockchain technology, and sometimes it can also include PII that was acquired for credit or anti-money laundering checks.[2262]

Personal Information

The processing of personal information is regulated by the SA POPI 4 of 2013.[2263] The SA POPI 4 of 2013 was signed into law on 19 November 2013. On 1 December 2016, the IR opened its doors and SA POPI 4 of 2013 came into effect on 1 July 2021.

In terms of SA POPI 4 of 2013, section 1, *s.v.* "personal information" is information about the personal aspects of a person's life.[2264] Section 1 also creates a sub-category of personal information, *s.v.* "special personal information," which includes private information that is of a sensitive nature and that relates to the intimate aspects of a person's life.[2265]

Due to their inherent online nature, OMs require and work with very sensitive personal information of shareholders, which go way beyond the details recorded in the shareholder register that the Act, section 26(3) requires.[2266]

Proxy

In terms of the Act, section 58(1) a shareholder may nominate anyone, also a non-shareholder, as proxy to (a) participate and vote on their behalf.[2267]

Ransomware

Ransomware can be described as cyberextortion, and occurs when a cybercriminal uses software to prevent someone to access their online system until a ransom has been paid.[2268]

[2260] Johnson *op cit* 256.
[2261] *Ibid*.
[2262] McCarrick *op cit s.p*.
[2263] SA POPI 4 of 2013, preamble.
[2264] SA POPI 4 of 2013, section 1, *s.v.* "personal information."
[2265] SA POPI 4 of 2013, section 1, *s.v.* "special personal information."
[2266] The Act, section 26(3).
[2267] The Act, section 58(1)(a)-(b).
[2268] SA Cybercrimes Act 19 of 2020, section 10.

Right to Privacy

The right to privacy in SA is protected under the Constitution, section 14.[2269] Latching on to this right is section 10, which contains the right to human dignity and that states that everyone's dignity is protected by law.[2270]

Cyberbreaches mainly compromise these two express, justiciable and invaluable rights through either unlawfully obtaining, processing, retaining, recording or sharing someone's personal information.[2271]

Securities

The SA Financial Markets Act 19 of 2012, section 1, *s.v.* 'securities' explains that 'securities' refer to "(a) listed and unlisted- (i) shares, depository receipts and other equivalent equities in public companies, other than shares in a share block company as defined in the SA Share Blocks Control Act 59 of 1980; (ii) debentures, and bonds issued by public companies, public state-owned enterprises, the SA Reserve Bank and the Government of SA; (iii) derivative instruments; (iv) notes; (v) participatory interests in a collective investment scheme as defined in the SA Collective Investment Schemes Control Act 45 of 2002, and units or any other form of participation in a foreign collective investment scheme; (vi) instruments based on an index; (b) units or any other form of participation in a collective investment scheme outside SA; (c) the securities contemplated in paragraphs (a)(i) to (vi) and (b) that are listed on an external exchange; (d) an instrument similar to one or more of the securities contemplated in paragraphs (a) to (c) prescribed by the registrar to be a security for the purposes of this Act; (e) rights in the securities referred to in paragraphs (a) to (d), but excludes (i) money market securities; or if prescribed by the registrar as contemplated in paragraph (d); (ii) the share capital of the SA Reserve Bank referred to in the SA Reserve Bank Act 90 of 1989, section 21; and (iii) any security contemplated in paragraph (a) prescribed by the registrar."[2272]

The SA Companies Amendment Bill of 2021, section 1(b) contains a proposed amendment for term, 'securities,' in the Act, so that it will refer to; "any shares or debentures, irrespective of their form or title, issued or authorised to be issued by a profit company."[2273] The definition will therefore no longer include other instruments and will be limited to shares and debentures.[2274]

Self-Aware AI

[2269] SA Constitution, section 14(a)-(d).
[2270] SA Constitution, section 10.
[2271] Poole *et al. op cit s.p*.
[2272] SA Financial Markets Act 19 of 2012, section 1 s.v. 'securities;' SA Reserve Bank Act 90 of 1989; SA Share Blocks Control Act 59 of 1980.
[2273] SA Companies Amendment Bill of 2021, section 1(b).
[2274] *Ibid.*

Self-Aware AI uses an algorithm that acts independently from humans and that is self-aware, and which cannot be directly overseen by humans, for example the algorithm that is used by self-driving cars.[2275]

Shareholder

The Act, section 1, *s.v.* states that 'shareholder' means the holder of a company's shares and whose name is behind the number of that share in the company's shares register.[2276]

Section 57(1) says that a 'shareholder' is "a person who is entitled to exercise any voting rights in relation to a company, irrespective of the form, title or nature of the shares to which those voting rights are attached."[2277]

The Act, section 43(3) states that "except to the extent that a MOI provides otherwise, a debt instrument issued by the company may grant special privileges on (a) attending and voting at shareholders' meetings."[2278]

Stakeholder

Stakeholders are groups or an individual who have a legal or moral interest or a share in a company.[2279]

A stakeholder is a person such as a community member, creditor, customer, employee, supplier or the wider community who is involved with a company and therefore has responsibilities towards it and an interest in its success.[2280]

The Act provides no definition for a stakeholder.

Supportive AI

Supportive AI uses machine learning to generate algorithms automatically.[2281] Such an algorithm tool allows the developer to explain what the algorithm needs to do, and then it generates the algorithm automatically.[2282]

Sustainable Development

In 1987, the World Commission on Environment and Development (WCED) published a report called, '*Our Common Future*,' also known as '*the Brundtland Report*,' which sets out guiding principles for sustainable development.[2283] It highlighted the need for sustainable development and a focus was the first time placed on the role that

---

[2275] Alechina *op cit s.p*.
[2276] The Act, section 1 *s.v.* 'shareholder'.
[2277] The Act, section 57(1).
[2278] The Act, section 43(3)
[2279] Keay *The Enlightened Shareholder Value and Corporate Governance op cit* 12.
[2280] McIntosh *et al. Cambridge Advanced Learner's Dictionary s.v.* 'stakeholder'.
[2281] Tozzi *op cit s.p.*
[2282] *Ibid.*
[2283] WCED *op cit*, Part 2; Esser *et al. op cit* 5 - 6.

stakeholders need to play to enable sustainable development.[2284] This Report introduced the 'triple bottom line approach' to help balance a company's environmental, social and economic sustainability.[2285]

True Owner

The SA Companies Amendment Bill of 2021 defines a 'true owner' of a security as a natural person who is able to direct its registered holder to act in a certain way or someone who ultimately benefits from the shareholding.[2286] It states that only a natural person can be a true owner.[2287] The Bill wants to make other amendments to the Act, section 56 to help identify the true owner of a security.[2288]

The Bill, section 4.3. defines a 'true owner' of a security as; "a natural person, who would in all the circumstances be considered to be the ultimate and true owner of the relevant securities, whether by reason of being capable either directly or indirectly (via the intermediation of others in the chain of holders of beneficial interest in the relevant securities) of directing the registered holder with regard to the securities or because of being a person for whose benefit the securities enure or for any other reason, not limited *ejusdem generis*, which could be the registered holder itself, or if the registered holder is not the true owner or the only true owner, would be the last person in the chain of any holders of beneficial interest in the relevant securities."[2289]

Unlawful Interception of Data

This is a cybercrime that prohibits a cybercriminal to unlawfully intercept or prevent any online communications to reach its intended recipient.[2290]

Zoombomb

Zoombombing occurs when a cybercriminal manages to find a cybersecurity loophole in an online platform and then hijacks it to either disrupt the meeting or to commit cybercrime.[2291]

[2284] WCED *op cit*, Part 2; Esser *et al. op cit* 5 - 6.
[2285] *Ibid*.
[2286] SA Bill of 2021, section 4.3.
[2287] *Ibid.*
[2288] The Act, section 56; SA Bill of 2021, section 4.3.
[2289] SA Companies Amendment Bill of 2021, section 1.
[2290] SA Cybercrimes Act 19 of 2020, section 3.
[2291] Lorenz *op cit s.p.*