

ARTIFICIAL INTELLIGENCE

Law and Regulation

SECOND EDITION

CHARLES KERRIGAN



© The Editors and Contributors Severally 2025

Every effort has been made to trace all the copyright holders but if any have been inadvertently overlooked please notify the publisher.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or photocopying, recording, or otherwise without the prior permission of the publisher.

Published by

Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

Authorised representative in the EU for GPSR queries only: Easy Access System Europe – Mustamäe tee 50, 10621 Tallinn, Estonia, gpsr.requests@easproject.com

A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2025946966

This book is available electronically in the **Elgaronline**
Law subject collection
<https://doi.org/10.4337/9781035334353>



ISBN 978 1 0353 3434 6 (cased)
ISBN 978 1 0353 3435 3 (eBook)
ISBN 978 1 0353 8024 4 (ePub)

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

CONTENTS

<i>Extended contents</i>	viii
<i>List of contributors</i>	xxx
<i>Foreword</i>	xlili
<i>Preface to the second edition</i>	xliv
<i>Preface</i>	xlvi
<i>Table of cases</i>	xliv
<i>Table of legislation</i>	liii
PART I INTRODUCTION	
1 Introductory essay <i>Charles Kerrigan</i>	2
2 Themes of the chapters <i>Charles Kerrigan</i>	38
3 Introduction to AI <i>Charles Kerrigan</i>	47
4 Understanding AI <i>Tirath Virdee</i>	67
5 Generative AI <i>Nik Yeo</i>	93
PART II LAW AND REGULATION	
6 Corporate governance <i>Martin Petrin</i>	115
7 Regulatory compliance <i>Hannah Yee-Fen Lim</i>	149
8 The EU AI Act <i>Charles Kerrigan, Sean Musch and Michael Borrelli</i>	178
9 Artificial intelligence and standards <i>Sam De Silva and Barbara Zapisetskaya</i>	240
10 Commercial contracts <i>Iain Sheridan</i>	257
11 Commercial trade <i>Minesh Tanna and William Dunning</i>	288

CONTENTS

12	Liability and agency <i>Jason G. Allen and Florian Gamper</i>	305
13	Data and data protection <i>Peter Church and Richard Cumbley</i>	330
14	Competition law <i>Jerome Dickinson</i>	373
15	Intellectual property <i>Rachel Free</i>	388
16	Employment <i>Dana Denis-Smith</i>	422
17	Disputes and litigation <i>Kushal Gandhi and Vanessa Whitman</i>	440
18	Investing in AI <i>Charles Kerrigan and insights4vc</i>	458
PART III INDUSTRY SECTORS		
19	Financial regulation <i>Richard Hay and Sophia Le Vesconte</i>	483
20	Insurance <i>Stephen Kenny KC and Charlotte Payne</i>	532
21	Retail and consumer <i>Matthew Bennett</i>	566
22	Healthcare <i>Roland Wiring</i>	585
23	Telecoms <i>Anne Chitan</i>	604
24	Real estate <i>Alastair Moore, Claudia Giannoni, Nick Kirby, Nick Doffman and Edmond Boulle</i>	635
25	Taxation <i>Xavier Oberson</i>	661
PART IV HUMAN AI		
26	Cybersecurity <i>Craig Kennedy</i>	675
27	Misinformation and disinformation <i>Erica Stanford</i>	702
28	Ethics <i>Patricia Shaw</i>	725

CONTENTS

29	Bias and discrimination <i>Minesh Tanna and William Dunning</i>	758
30	AI and human rights <i>Mando Rachovitsa</i>	784
31	Public policy and government <i>Charles Kerrigan and Erica Stanford</i>	802
PART V TECHNICAL AND CONSULTING		
32	Education <i>Charles Kerrigan</i>	825
33	AI taxonomies and emergent issues in intelligence <i>Tirath Virdee and Alex Flom</i>	834
34	Federated learning <i>Tom Marshall and Nicolas D. Lane</i>	897
35	Autonomy and fairness <i>Emre Kazim, Adriano Koshiyama, Airlie Hilliard, Anisha Chadha, Charles Kerrigan and Jeremy Barnett</i>	908
36	Risk management <i>Stephen Ashurst</i>	923
37	Business models and procurement <i>Petko Karamotchev</i>	936
38	Explainable AI and responsible AI <i>Charles Kerrigan</i>	952
39	Legaltech and law firms <i>Erica Stanford and Charles Kerrigan</i>	965
	Index	982

EXTENDED CONTENTS

List of contributors xxi
 Foreword xlii
 Preface to the second edition xlv
 Preface xlvii
 Table of cases xlix
 Table of legislation li

PART I INTRODUCTION

1 Introductory essay
Charles Kerrigan
 A. INTRODUCTION TO THE BOOK 1.001
 B. HOW TO READ THIS BOOK 1.011
 C. WHAT IS AI? 1.027
 D. HOW IS AI DEFINED? 1.041
 E. IS AI DIFFERENT? 1.056
 F. AI AND ECONOMICS 1.058
 G. THE PHILOSOPHY OF TECHNOLOGY 1.065
 H. REGULATION 1.071
 I. INTERNATIONAL ASPECTS 1.087
 J. SOCIAL PURPOSE 1.094
 K. COGNITIVE BIASES 1.100
 1. Trust 1.101
 2. Bias from incentives 1.102
 3. Tendency to distort due to liking/loving or disliking/hating 1.103
 4. Availability heuristic 1.104
 5. Tendency to overgeneralize from small samples 1.105
 6. Hindsight bias 1.106
 7. Sensitivity to fairness 1.107
 L. AI AND THE FUTURE OF WORK 1.109
 M. PRESUPPOSITION 1.116
 N. COMMERCIAL LAW TEXTBOOKS 1.121
 O. COMMERCIAL LAW PRACTICE 1.129
 P. YOU LOOK LIKE A STEALTH ASSASSIN FROM THE CLOUDS 1.137
 Q. GENERATIVE AI 1.139
 R. AI FOR GOOD 1.147
 S. LEGISLATIVE AND REGULATORY ATTENTION SINCE THE FIRST EDITION 1.150
 T. DEFINITIONS OF AI AT THE TIME OF WRITING THE SECOND EDITION 1.157

2 Themes of the chapters
Charles Kerrigan
 A. INTRODUCTION 2.001
 B. THE CHAPTERS 2.003

3 Introduction to AI
Charles Kerrigan
 A. INTRODUCTION 3.001
 B. AI IN PRINCIPLE 3.002
 C. AI IN PRACTICE: CAPABILITIES OF AI 3.008
 D. AI IN PRACTICE: OPERATIONS OF AI 3.018
 E. BIG DATA 3.033
 F. TECHNOLOGIES USED TO DEVELOP AI SYSTEMS 3.038
 1. Machine learning (ML) 3.038
 2. Deep learning (DL) 3.056
 3. Federated learning 3.063
 4. Natural language processing (NLP) 3.068
 5. Computer vision 3.074
 6. Expert systems 3.079
 (a) AI planning 3.082
 G. THE AI STACK 3.086
 H. WHAT HOLDS BACK AI ADOPTION 3.087
 I. EMERGING TRENDS AND FUTURE DIRECTIONS 3.089
 J. LEGAL AND REGULATORY POLICY: PAST AND PRESENT 3.090
 K. LEGAL AND REGULATORY POLICY: FUTURE 3.098
 L. CONCLUSION 3.100

4 Understanding AI
Tirath Virdee
 A. INTRODUCTION 4.001
 B. INTRODUCTION TO AI 4.002
 C. LARGE LANGUAGE MODELS AND GENERATIVE AI 4.013
 D. MACHINE LEARNING 4.017
 E. DEEP LEARNING NEURAL NETWORKS 4.018
 F. AI USE CASES 4.035
 1. Law enforcement and justice 4.036
 2. Science 4.037
 3. Health and medicine 4.038
 4. Marketing and advertising 4.039
 5. Security 4.040
 6. Defence and warfare 4.041
 7. Agriculture 4.042
 8. Education 4.043
 9. Transportation and autonomous vehicles 4.044
 10. Environment 4.045
 11. Autonomous electric vehicles 4.046
 12. Smart agriculture 4.047
 13. Smart disaster response 4.048
 14. Connected cities 4.049
 15. Transparent digital earth 4.050
 16. Financial services 4.051
 17. Virtualization 4.052
 G. TRUST IN AI 4.054
 1. Fairness 4.060
 2. Explainability 4.061
 3. Robustness adversaries 4.062
 4. Lineage 4.063
 (a) Sensitivity analysis 4.066
 (b) Local Interpretable Model-Agnostic Explanations (LIME) 4.067
 (c) Shapley Additive Explanations (SHAP) 4.068

	(d) Tree and neural network interpreters	4.069
H.	ETHICAL IMPLICATIONS, EXPLAINABILITY AND THE RISK OF MISINFORMATION	4.072
I.	AI ETHICS, SECURITY AND GOVERNANCE	4.075
	1. Anti-classification	4.082
	2. Calibration	4.083
	3. Classification	4.084
J.	CONCLUSION	4.086
5	Generative AI	
	<i>Nik Yeo</i>	
A.	INTRODUCTION	5.001
B.	GenAI CHALLENGES	5.010
	1. How GenAI models are built	5.011
	(a) GenAI is not transparent	5.012
	(b) Tension between efficacy and the environment	5.017
	(c) GenAI is a product not a platform; an author not an agent	5.021
	2. How GenAI models are used	5.023
	(a) Control over use of GenAI models	5.024
	(b) Appropriateness of use of GenAI models: style vs substance; accuracy vs artistry	5.026
C.	REGULATION OF GenAI	5.035
	1. An existential threat?	5.035
	(a) Sentience	5.036
	(b) Sentiment – anthropomorphising Alexa	5.039
	2. ‘Right-sized regulation’	5.041
	(a) Existing consumer, competition and copyright legislation	5.043
	(b) Data regulation	5.046
	(c) Human rights	5.058
	(d) EU Artificial Intelligence Act (EU AIA)	5.059
	(e) International conventions, recommendations and principles	5.066
	(f) UK’s approach	5.073
	(g) Professionalism of developers of GenAI?	5.074
D.	CONCLUSION	5.076

PART II LAW AND REGULATION

6	Corporate governance	
	<i>Martin Petrin</i>	
A.	INTRODUCTION	6.001
B.	CAN AI TAKE OVER?	6.009
	1. Corporate leadership tasks	6.010
	(a) Directors	6.010
	(b) Managers	6.015
	2. AI and corporate leadership	6.020
	(a) Potential roles for AI	6.021
	(b) Administrative work versus judgment work	6.027
C.	ASSESSMENT	6.047
D.	CONSEQUENCES OF AI MANAGEMENT	6.053
	1. Corporate boards	6.054
	(a) Boards today	6.054
	(b) Boards tomorrow	6.062
	2. Corporate management	6.068
	3. Directors’ and officers’ liability	6.071
	(a) Liability today	6.071
	(b) Liability tomorrow	6.077
E.	CONCLUSION	6.085

7	Regulatory compliance	
	<i>Hannah Yee-Fen Lim</i>	
A.	INTRODUCTION	7.001
B.	TECHNOLOGICAL CONSIDERATIONS	7.003
	1. Traditional software	7.003
	2. AI algorithms	7.004
	3. AI and data	7.008
	(a) Size of the datasets	7.009
	(b) Quality of the datasets	7.013
C.	LEGAL RESPONSES	7.019
	1. Challenges for regulators	7.019
	2. Governmental and inter-governmental responses – ethics codes and principles	7.024
	(a) Ethics frameworks: Australia	7.025
	(b) Ethics principles: United States	7.028
	(c) Ethics frameworks: European Union	7.032
	(d) Ethics frameworks: OECD	7.040
	(e) Ethics principles in general	7.054
	3. Creating laws and regulations	7.057
	4. Concrete general laws	7.062
	(a) Substantive areas of law	7.067
	(b) Personal data protection laws	7.069
	(c) Civil liability laws	7.087
	(d) Ethics laws	7.094
	(e) Intellectual property laws	7.096
	5. Highly regulated industries	7.105
	6. Compliance with regulation using AI	7.109
D.	CONCLUSION	7.117
8	The EU AI Act	
	<i>Charles Kerrigan, Sean Musch and Michael Borrelli</i>	
A.	INTRODUCTION	8.001
B.	CHAPTER OVERVIEW	8.002
C.	SCOPE AND GLOBAL INFLUENCE	8.012
D.	RISK-BASED FRAMEWORK	8.015
E.	ETHICS	8.022
	1. Protection for vulnerable groups	8.024
	2. Prevention of bias and discrimination	8.025
	3. Transparency obligations	8.027
	4. Human oversight	8.028
	5. Trust	8.031
F.	SCOPE OF THE EU AI ACT	8.037
	1. Scope of application	8.037
	2. Definition of AI systems	8.040
	(a) Territorial scope of the Act	8.054
	(b) Entities established in the EU	8.055
	(c) AI systems used in the EU by non-EU entities	8.056
	(d) Products and services exported into the EU	8.057
	(e) Applicability across EU member states	8.058
	(f) Making available	8.060
	(g) Placing on the market	8.062
	(h) Putting into service	8.064
	3. Exemptions	8.067
	(a) Public authorities in third countries	8.068
	(b) Military, defence and national security applications	8.070
	(c) Exclusions from the Act’s scope	8.073

EXTENDED CONTENTS

	(d) National security and defence	8.074
	(e) Scientific research, testing and development	8.074
	(f) Personal use	8.077
4.	Prohibited AI practices	8.082
	(a) Subliminal, manipulative or deceptive techniques	8.084
	(b) Exploitation of vulnerabilities	8.089
	(c) Social scoring	8.089
	(d) Profiling for criminal risk assessment	8.089
	(e) Facial recognition databases from untargeted scraping	8.099
	(f) Inference of emotions in workplaces and educational institutions	8.101
	(g) Biometric categorisation based on sensitive data	8.104
	(h) Real-Time Remote Biometric Identification (RBI) in public spaces for law enforcement	8.101
5.	Enforcement and scope of prohibited practices	8.110
	(a) High-risk AI systems	8.110
6.	Classification of persons under the AI Act	8.110
	(a) Providers	8.110
	(b) Requirements for high-risk AI systems	8.110
	(c) Deployers	8.112
	(d) Importers	8.113
	(e) Distributors	8.115
7.	Responsibilities Along the AI Value Chain	8.116
8.	Commercial terms	8.116
	(a) General-purpose AI models – background to regulation	8.117
	(b) General-purpose AI models – definition and applications	8.117
	(c) Providers of general-purpose AI models	8.118
9.	Transparency	8.119
	(a) Transparency obligations for providers	8.120
	(b) Transparency obligations for deployers	8.121
	(c) Deepfakes	8.121
	(d) AI literacy	8.123
10.	AI regulatory sandboxes	8.123
	(a) Definition	8.123
11.	Governance and enforcement	8.125
	(a) Post-market obligations for high-risk AI systems	8.125
	(b) Reporting of serious incidents	8.126
12.	Non-high-risk AI systems	8.126
	(a) Procedures for enforcement under the AI Act	8.126
13.	Identification of authorities	8.127
	(a) General-purpose AI models	8.128
	(b) Penalties under the Act	8.128
	(c) Remedies for third parties	8.129
14.	Governance framework for the AI Act	8.130
	(a) Governance at Union level	8.130
	(b) Governance at national level	8.133
15.	Timeline of implementation	8.134
	(a) Key dates	8.135
16.	Expected updates to guidelines, codes of practice and technical standards	8.135
G.	CONCLUSION	8.140
9	Artificial intelligence and standards	9.000
	<i>Sam De Silva and Barbara Zapisetskaya</i>	9.000
	A. INTRODUCTION	9.000
	B. HOW STANDARDS ARE DEVELOPED AND THE ROLE OF NATIONAL STANDARDS' BODIES	9.000
	1. Relationship between European and international standards	9.000

EXTENDED CONTENTS

	2. International AI standards development	9.009
C.	HOW STANDARDS WORK	9.011
	1. Overview	9.011
	2. How do standards work for AI?	9.014
D.	THE ROLE THAT THE AI ACT GIVES TO STANDARDISATION	9.016
E.	THE COMMISSION'S STANDARDISATION REQUEST	9.018
	1. Alignment with the AI Act	9.022
F.	RISK MANAGEMENT – ARTICLE 9 AND AI RISK MANAGEMENT STANDARD (ISO/IEC 23894)	9.024
	1. Gaps with Article 9	9.030
G.	QUALITY MANAGEMENT – ARTICLE 17 AND AI MANAGEMENT SYSTEM STANDARD (ISO/IEC 42001)	9.033
	1. AI Management System Standard (ISO/IEC 42001)	9.038
	2. Gaps with Article 17	9.042
H.	INTERNATIONAL STANDARDS AND AI GOVERNANCE	9.045
	1. AI Governance Standard: scope	9.046
	2. Accountability of governing bodies	9.048
	3. Appropriate level of oversight of AI	9.051
	4. Practical steps organisations can take to alleviate constraints on the use of AI	9.053
	(a) Increase oversight of compliance	9.054
	(b) Address the scope of AI use	9.055
	(c) Assess and address the impact on stakeholders	9.056
	(d) Determine legal requirements or obligations of using the technology	9.057
	(e) Align the use of AI to the organisation's objectives, culture and values	9.058
	(f) Ensure that problem solving takes due account of context	9.059
	(g) Examine the additional risk that the use of AI can bring to an organisation	9.060
I.	CONCLUSION	9.061
10	Commercial contracts	
	<i>Iain Sheridan</i>	
A.	INTRODUCTION	10.001
B.	PRINCIPLES OF ENGLISH CONTRACT LAW	10.004
	1. Intention to create legal relations	10.006
	2. Offer and acceptance	10.007
	3. Consideration	10.008
	4. Certainty of the subject matter	10.009
	5. Compliance	10.010
C.	MACHINE LEARNING	10.012
	1. Definitions	10.012
	2. Three key types of machine learning methods	10.013
	3. Clause drafting for machine learning methods	10.016
	4. Machine learning concepts relevant to contract management	10.018
D.	AI AUGMENTING HEDGING AND INVESTMENT DECISIONS	10.019
	1. Example of a company using unsupervised classification	10.020
	2. Example of a company providing products relying on IBM Watson	10.023
	3. Example of a company supplying an investment scoring system	10.025
	4. Example of a company providing trading strategies	10.026
E.	AI STANDARDS IN TERMS AND CONDITIONS	10.027
	1. Leading AI standards	10.027
	2. Common principles in AI standards	10.030
	(a) Technical transparency	10.031
	(b) Explainability	10.036
	(c) Robustness	10.038
	3. AI allocation of liability chart	10.040
	4. Drafting AI standards in contracts	10.041
	5. Miscellaneous AI risks to cover in contracts	10.043

EXTENDED CONTENTS

(a)	Trade secret risk exposure	10.043
(b)	Key partner risk	10.044
(c)	Data risk	10.045
F.	AI AUGMENTING CONTRACT CLAUSES AND PROCESSES	10.046
1.	AI image recognition of authorised contract signatures	10.046
2.	AI prediction of <i>force majeure</i> events	10.047
(a)	Backpropagation of errors	10.052
3.	AI calculation of termination payments	10.056
4.	Key questions to answer on any AI augmentation	10.075
G.	CONCLUSION	10.086
11	Commercial trade	10.087
	<i>Minesh Tanna and William Dunning</i>	
A.	INTRODUCTION	11.001
B.	USE OF AI IN COMMERCE AND TRADE	11.003
C.	RESEARCH AND DEVELOPMENT	11.005
1.	Manufacturing	11.007
2.	Logistics and transport	11.009
3.	Retail	11.011
4.	Financial services	11.015
5.	Commercial contracts	11.017
6.	AI and agency	11.020
(a)	Legal concept of 'agency'	11.021
(b)	Difficulties of agency in AI context	11.022
(c)	Scenario 1: AI system unforeseeably creates legal relations	11.027
(d)	Scenario 2: AI system unforeseeably causes loss to a third party	11.030
(e)	Scenario 3: AI system used by multiple 'principals' acts in an unforeseeable manner	11.033
7.	Marketing and AI 'washing'	11.036
(a)	The attractiveness of the 'AI' label in marketing	11.036
(b)	AI washing	11.038
(c)	Advertising Standards Agency	11.046
(d)	Misrepresentation	11.052
(e)	Future of AI marketing	11.056
8.	Conflict of laws	11.059
D.	CONCLUSION	11.066
12	Liability and agency	12.001
	<i>Jason G. Allen and Florian Gamper</i>	
A.	INTRODUCTION	12.011
B.	CONCEPTUAL FRAMEWORK	12.020
C.	PRINCIPLES OF ATTRIBUTION AND LIABILITY	12.028
D.	AUTONOMY, OPACITY AND UNPREDICTABILITY IN FAULT-BASED LIABILITY SYSTEMS	12.039
E.	SPECIAL CONSIDERATIONS IN THE PUBLIC LAW CONTEXT	12.051
F.	CONCLUSION	
13	Data and data protection	13.001
	<i>Peter Church and Richard Cumbley</i>	
A.	INTRODUCTION	13.001
1.	The General Data Protection Regulation	13.006
2.	Overview	13.010
B.	KEY CONCEPTS	13.011
1.	What is personal data?	13.014
(a)	Examples of personal data	13.018
2.	Does data have to be structured?	13.018
3.	What about inferences?	13.021

EXTENDED CONTENTS

4.	What does processing mean?	13.026
5.	Who is responsible for processing?	13.028
(a)	Controller or processor?	13.033
6.	Can I just anonymise the personal data?	13.034
(a)	Has Netflix told the world what you are watching?	13.037
7.	Who regulates and enforces the law?	13.040
8.	How does the GDPR apply internationally?	13.048
C.	SUBSTANTIVE OBLIGATIONS	13.051
1.	Principle-based regulation	13.052
2.	The data processing principles	13.056
3.	Processing conditions and consent	13.059
4.	Sensitive data and discrimination	13.066
5.	International transfers	13.073
D.	SPECIFIC COMPLIANCE OBLIGATIONS	13.075
1.	Data protection impact assessment and privacy by design	13.076
2.	Transparency and a 'right to an explanation'	13.085
3.	Automated decisions - 'The computer says no'	13.091
(a)	Example: shortlisting employment applicants	13.096
4.	Other rights for individuals	13.099
5.	Repurposing personal data	13.102
E.	FRESH CHALLENGES FOR GENERATIVE AI	13.107
1.	Can you use web scraped data?	13.108
2.	What about the strict rules on special category personal data?	13.112
3.	Are 'hallucinations' illegal?	13.115
4.	How do you comply with individual rights in practice?	13.118
5.	Enforcement	13.121
F.	OTHER CHALLENGES RECONCILING AI AND GDPR	13.125
1.	The black box	13.126
(a)	Example: a military weather detector	13.128
2.	Accuracy	13.130
(a)	Example: understanding accuracy	13.137
3.	Bias and fairness	13.142
(a)	Example: unfair exam moderation algorithms?	13.149
4.	Security and the ghosts of training data	13.157
G.	SAFEGUARDS AND COMPLIANCE MEASURES	13.166
1.	Human in the loop	13.167
2.	Peering into the black box	13.172
3.	Privacy-enhancing techniques	13.177
4.	General safeguards	13.180
H.	ALGORITHMIC FAIRNESS AND FUTURE REGULATION	13.183
1.	Should we think more about algorithms and less about AI?	13.184
2.	How do you understand an algorithm?	13.189
3.	Do we need new regulatory remedies?	13.191
4.	Do we need an algorithmic 'super regulator' in the UK?	13.194
I.	CONCLUSION	13.200
14	Competition law	14.001
	<i>Jerome Dickinson</i>	
A.	INTRODUCTION	14.001
B.	HOW DO COMPETITION LAW AND AI IMPACT EACH OTHER?	14.003
1.	Mapping out the subject-matter	14.003
(a)	Artificial intelligence	14.003
(b)	Machine learning	14.005
(c)	Big data	14.007
2.	Does use of AI lead to anti-competitive outcomes?	14.012

(a) Will AI facilitate collusion?	14.012
(b) Will AI lead to other outcomes which present concerns for consumer welfare?	14.017
(c) Other potentially anti-competitive outcomes	14.022
(d) Other potentially anti-competitive outcomes	14.027
3. Is there a policy or enforcement gap?	14.028
(a) Parallel pricing	14.028
(b) Personalised pricing	14.032
4. Different approaches to AI from the various regulators	14.037
(a) EU Commission	14.037
(b) UK Competition and Markets Authority	14.043
(c) United States (Department of Justice and Federal Trade Commission)	14.047
(d) France	14.051
(e) Other jurisdictions	14.052
C. CONCLUSION	14.055
15 Intellectual property	
<i>Rachel Free</i>	
A. INTRODUCTION	15.001
B. HOW DOES THE INTELLECTUAL PROPERTY SYSTEM INCENTIVISE KNOWLEDGE SHARING?	15.003
1. Copyright	15.005
2. Designs	15.006
3. Trade marks	15.007
4. Patents	15.008
5. Trade secrets	15.009
C. KNOWLEDGE SHARING IS PARTICULARLY IMPORTANT IN THE CASE OF AI TECHNOLOGY	15.011
1. AI technology has a significant impact on our lives	15.012
2. AI technology today has some degree of independence and uncontrollability	15.014
3. AI technology is likely to advance in the future	15.017
4. Drawbacks of knowledge sharing	15.018
D. MECHANISMS TO PROMOTE KNOWLEDGE SHARING	15.021
1. Market pressure due to scarcity of AI experts leads to knowledge sharing	15.022
2. Regulation and standards are also mechanisms to promote or, in the case of regulation, mandate knowledge sharing of AI algorithms	15.023
3. Intellectual property system as a mechanism to promote knowledge sharing	15.025
4. International language of patents and multi-national nature of patents	15.026
5. Patent documents are freely available	15.028
6. Patents are not source code	15.029
7. Comments about mechanisms to promote knowledge sharing	15.030
E. THE INTELLECTUAL PROPERTY SYSTEM MAY NEED BROADENING AND STRENGTHENING IN ORDER TO PROMOTE KNOWLEDGE SHARING	15.035
1. The balance between trade secrets and knowledge-sharing forms of intellectual property	15.036
2. Paraphrased claim 1 of EP 3 055 813 B1	15.046
3. New problems of AI	15.051
4. Fundamental technical problems for CII	15.056
5. New technical problems	15.060
6. Generating a rationale for an AI decision	15.061
7. Paraphrased claim 1 of EP3291146A1	15.062
8. Implementing the right to be forgotten	15.063
9. Determining accountability where an autonomous agent is involved	15.064
10. Driving 'acceptable' behaviour	15.065
11. The 'problem' of ethics using AI	15.066
12. Do AI ethics-related problems have anything in common?	15.068
13. What is the relevance of a 'new' fundamental technical problem to patent drafting and patent prosecution of CII inventions?	15.073

(a) Methods designed based on specific technical considerations of the internal functioning of the computer	15.082
(b) Methods controlling the internal functioning or operation of a computer	15.083
(c) Programs for processing code at a low level, such as compilers	15.084
14. Inventions created by AI machines	15.085
15. Fictional case study 1: AI machine used to create drug candidates to treat a given disease	15.088
16. Fictional case study 2: AI machine used to create source code for an AI algorithm to label regions depicting cancer in medical images	15.092
17. Case law establishing that the class of inventions created by non-human inventors is excluded from patent protection in Europe and the US	15.093
18. Possibilities for changing the law regarding machine inventors in order to promote knowledge sharing	15.096
(a) Option 1: allow machines to be listed as inventors	15.096
(b) Option 2: follow the approach of the CDPA regarding the copyright of machine-generated works	15.097
(c) Option 3: allow patent protection for a wide range of AI-assisted inventions	15.098
(d) AI technologies outwith patent protection	15.099
(e) What was the patent application about?	15.101
(f) Why was there so much interest?	15.102
(g) What happened during the oral proceedings?	15.103
(h) Direct link with physical reality	15.104
(i) What was the outcome?	15.105
(j) How were the referred questions answered?	15.109
(k) AI tools to assist patent issuing authorities	15.110
F. EVIDENCE THAT THE INTELLECTUAL PROPERTY SYSTEM IS ALREADY INVOLVED WITH ETHICS	15.121
1. Trade marks	15.122
2. Designs	15.123
3. Patents	15.124
4. Copyright	15.125
G. CONCLUSION	15.126
16 Employment	
<i>Dana Denis-Smith</i>	
A. INTRODUCTION	16.001
B. REGULATORY FRAMEWORKS PROGRESS	16.009
C. AI AND RECRUITMENT	16.018
D. POST-EMPLOYMENT	16.041
E. REGULATORY TRENDS	16.047
F. CONCLUSION	16.051
17 Disputes and litigation	
<i>Kushal Gandhi and Vanessa Whitman</i>	
A. INTRODUCTION	17.001
B. AI IN RESOLVING DISPUTES	17.004
C. DISPUTES RELATING TO AI	17.012
D. DAY 1 CONSIDERATIONS	17.015
1. Root cause analysis, investigations and privilege	17.015
2. Parties to the dispute	17.020
3. Governing law and jurisdiction	17.023
4. Limitation period	17.025
5. Pre-action conduct	17.026
6. Preserving documentary and data evidence	17.030
E. LEGAL TOOLS UNDER ENGLISH LAW	17.033
1. Procedure in a nutshell	17.036

2.	Key requirements for obtaining SSOs and freezing orders	17.038
3.	Timing of the application	17.040
4.	Supporting evidence	17.041
5.	Undertakings to Court	17.044
6.	Undertaking in damages	17.045
7.	Search orders in AI disputes: practicalities	17.048
8.	Other remedies where an SSO is not appropriate	17.057
F.	CONCLUSION	17.058
18	Investing in AI <i>Charles Kerrigan and insights4vc</i>	
A.	INTRODUCTION	18.001
B.	EARLY FOUNDATIONS: GOVERNMENT AS THE PRIMARY INVESTOR	18.003
1.	Challenges in early AI funding	18.006
2.	Growth in the 1960s and beyond	18.010
C.	THE AI WINTERS	18.013
1.	The first AI winter (1974–1980)	18.014
2.	The second AI winter (1987–1993)	18.016
D.	EVOLUTION OF ARTIFICIAL INTELLIGENCE FROM THE LATE 1990S TO 2024	18.018
1.	Venture capital investments in artificial intelligence (2012–2020)	18.023
2.	Current state of venture capital investments in artificial intelligence	18.028
E.	DIFFERENCES BETWEEN FUNDING AI AND OTHER VENTURES	18.033
1.	Funding stages in AI ventures	18.035
(a)	Seed stage	18.035
(b)	Early-stage funding	18.036
(c)	Growth stage	18.037
2.	Types of AI ventures attracting investment	18.038
(a)	Infrastructure providers	18.038
(b)	Model developers	18.039
(c)	Developer tools and infrastructure software	18.040
(d)	Application layer startups	18.041
(e)	Investment characteristics of AI startups	18.042
(f)	Comparison with other startups	18.045
(g)	Sector breakdowns and emerging trends	18.047
(h)	Healthcare and biotechnology	18.048
(i)	Autonomous systems	18.049
3.	Infrastructure and AI platforms	18.050
(a)	Natural language processing (NLP) and computer vision	18.051
(b)	Financial services	18.052
(c)	Manufacturing and supply chains	18.053
(d)	Concepts and trends influencing AI investment shift from System 1 to System 2 thinking in AI models	18.055
(e)	Emergence of inference-time computation	18.056
(f)	Service-as-a-software model	18.057
(g)	Custom cognitive architectures	18.058
(h)	Investment strategies and considerations investment process and due diligence in AI ventures	18.059
(i)	Strategic investment approaches	18.059
F.	LEGAL ISSUES IN DILIGENCE AND INVESTMENT TERMS	18.060
1.	Investment committee	18.068
2.	Diligence	18.069
3.	Term sheet	18.071
4.	Issues for founders	18.072
5.	Documents	18.073
6.	AI-specific terms	18.074

G.	CONCLUSION	18.075
PART III	INDUSTRY SECTORS	
19	Financial regulation <i>Richard Hay and Sophia Le Vesconte</i>	
A.	INTRODUCTION	19.001
B.	MARKET ACTIVITY	19.005
1.	Nature of AI in financial services	19.006
2.	Areas of deployment	19.013
3.	Use of third parties	19.016
C.	LEGAL AND REGULATORY LANDSCAPE	19.020
1.	Existing law and regulation	19.021
2.	Existing soft law, guidance and commentary	19.025
D.	GENERAL OBLIGATIONS AND BEST PRACTICE CONSIDERATIONS	19.028
1.	Regulatory perimeter	19.030
2.	Governance and regulatory responsibility	19.040
3.	Explainability, transparency and fairness	19.054
4.	Control and risk-management	19.068
5.	Outsourcing, third party service provision and operational resilience	19.082
E.	SPECIFIC CONSIDERATIONS IN RELATION TO ANTI-MONEY LAUNDERING AND ALGORITHMIC TRADING	19.089
1.	Anti-money laundering	19.090
2.	Algorithmic trading	19.101
(a)	Application of algorithmic trading rules	19.101
(b)	Market abuse concerns	19.117
(c)	Legal validity of contracts	19.120
F.	POTENTIAL FUTURE DEVELOPMENTS	19.125
20	Insurance <i>Stephen Kenny KC and Charlotte Payne</i>	
A.	INTRODUCTION	20.001
B.	AN OVERVIEW OF THE IMPLICATIONS OF AI FOR THE BUSINESS OF INSURANCE	20.007
C.	RISK ASSESSMENT AND UNDERWRITING	20.011
D.	INITIAL REGULATORY AND LEGISLATIVE RESPONSES TO THE IMPLEMENTATION OF AI SYSTEMS IN SO FAR AS AFFECTING RISK ASSESSMENT AND UNDERWRITING	20.020
1.	The UK position	20.020
2.	The EU position	20.028
(a)	Prohibited AI practices	20.031
(b)	High-risk AI systems	20.033
(c)	General purpose AI systems	20.038
(d)	Minimal-risk AI systems	20.040
E.	UNLAWFUL DISCRIMINATION AND THE USE OF ILLEGITIMATE FACTORS IN THE ASSESSMENT OF RISK	20.042
1.	Discrimination	20.042
(a)	The law	20.042
2.	AI-assisted risk assessment; direct discrimination	20.054
3.	AI-assisted risk assessment; indirect discrimination	20.056
4.	Genetics and genetic testing	20.063
F.	DATA PROTECTION AND DATA RETENTION	20.068
1.	The law	20.068
(a)	GDPR post-Brexit	20.070
(b)	Personal data	20.072
(c)	Duties of the data controller, and the data subject's access rights	20.075
(d)	Automated decision-making	20.082

EXTENDED CONTENTS

2.	Application to insurers employing risk-rating AI systems	
(a)	Data examination and collection	20.062
(b)	Use of data to train and educate the AI's algorithms	20.066
(c)	Use of personal data to rate the individual risk	20.068
(d)	Use of AI in (automated) decision-making	20.069
(e)	Retention of personal data	20.094
G.	THE INSURER'S REMEDIES FOR MISREPRESENTATION AND UNFAIR PRESENTATION OF RISK	20.118
1.	Consumer insurance contracts	20.118
(a)	Misrepresentation; remedies	20.118
2.	Non-consumer insurance contracts	20.118
(a)	Knowledge of the insurer	20.118
(b)	Breach of the duty of fair presentation; remedies	20.118
H.	CONCLUSION	20.119
21	Retail and consumer	20.114
	<i>Matthew Bennett</i>	
A.	INTRODUCTION	21.001
B.	RETAIL JOURNEY	21.001
1.	Stage 1 – awareness, influence	21.001
(a)	Personalisation	21.001
(b)	Product recommendations	21.001
2.	Stage 2 – research and consideration, awareness and channel	21.001
(a)	Chatbots, virtual assistants, self-service kiosks and in-store robots	21.001
(b)	Virtual reality and augmented reality	21.001
(c)	Product descriptions and review	21.001
(d)	AI-powered omnichannel	21.001
(e)	Remote stock checking	21.001
3.	Stage 3 – purchase	21.001
(a)	Checkout-less payment	21.001
(b)	Dynamic pricing	21.001
4.	Stage 4 – fulfilment	21.001
(a)	Drones	21.001
(b)	In-home delivery	21.001
(c)	Distribution	21.001
(d)	Inventory management	21.001
5.	Stage 5 – service and support, retention and loyalty	21.001
(a)	Back to chatbots, virtual reality and augmented reality	21.001
(b)	Returns	21.001
(c)	Next best action/post-sales analysis	21.001
C.	LEGAL CHALLENGES	21.053
1.	Customer trust	21.053
2.	Data protection	21.056
3.	EU AI Act	21.063
4.	UK AI regulation	21.066
5.	Competition law issues	21.068
6.	Dynamic pricing	21.068
7.	Personalised pricing	21.068
8.	Intellectual property	21.070
9.	Transparency/consumer protection issues	21.071
D.	CONCLUSION	21.075
22	Healthcare	21.084
	<i>Roland Wiring</i>	
A.	INTRODUCTION	22.001
B.	ARTIFICIAL INTELLIGENCE USE CASES IN HEALTHCARE	22.004

EXTENDED CONTENTS

1.	Impact and potential of AI in healthcare	22.005
2.	Diagnostics	22.010
3.	Therapeutic options	22.017
4.	Clinical trials	22.022
5.	Surgery robotics	22.026
C.	LEGAL CHALLENGES TO THE USE OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE	22.032
1.	Regulatory	22.033
2.	Liability for the use of AI	22.045
3.	Intellectual property	22.060
4.	Reimbursement	22.065
D.	CONCLUSION	22.068
23	Telecoms	
	<i>Anne Chitan</i>	
A.	INTRODUCTION	23.001
B.	A COMPLEX LEGISLATIVE LANDSCAPE	23.008
C.	THE TELECOM INDUSTRY AS USER OF AI	23.017
1.	Examples of AI applications in the telecom sector	23.020
2.	Regulatory measures impacting the use of AI by the telecom sector	23.027
(a)	EU AI Act	23.028
(b)	Data regulations	23.037
(c)	Transparency requirements	23.055
(d)	Network neutrality	23.059
(e)	Fraud prevention	23.065
D.	AI AS USER OF THE TELECOM INDUSTRY	23.068
1.	Role of telecom in AI enablement	23.069
2.	Regulatory measures impacting AI as a user of communication and digital infrastructure	23.076
(a)	Network improvement measures	23.077
(b)	Cybersecurity and safety rules	23.083
(c)	Regulation of liability	23.106
(d)	Sustainability rules	23.120
(e)	Data sovereignty protection laws	23.125
E.	CONCLUSION	23.128
24	Real estate	
	<i>Alastair Moore, Claudia Giannoni, Nick Kirby, Nick Doffman and Edmond Boulle</i>	
A.	INTRODUCTION	24.001
B.	KEY DEVELOPMENTS IN GENERATIVE AI AND THEIR IMPLICATIONS FOR CONVEYANCING	24.015
1.	Advances in AI intelligence	24.015
2.	Expanded context windows and multimodal capabilities	24.017
3.	AI agents	24.022
C.	DEVELOPMENT AND CONSTRUCTION	24.025
D.	TITLE AND TRANSFER	24.032
E.	LEASING OF COMMERCIAL REAL ESTATE	24.051
F.	PROPERTY LISTING, SEARCH AND MARKETING	24.059
G.	REAL ESTATE MARKETS	24.065
H.	PROPERTY MANAGEMENT, MAINTENANCE AND INSURANCE	24.079
I.	CONCLUSION	24.087
25	Taxation	
	<i>Xavier Oberson</i>	
A.	INTRODUCTION	25.001
B.	CURRENT TAXATION OF AI	25.005

EXTENDED CONTENTS

1.	Taxation of the use of AI as production factors of enterprises	25.005
2.	Application of VAT to the use of AI	25.014
3.	Automation taxes	25.020
4.	Tax on drones or self-driving vehicles	25.022
C.	PROPOSALS OF SPECIFIC AI TAXES	25.025
1.	A tax on the use of AI	25.025
2.	A tax on AI as such	25.031
D.	AI AND THE TAX AUTHORITIES	25.037
E.	CONCLUSION	25.052
PART IV HUMAN AI		
26	Cybersecurity	
	<i>Craig Kennedy</i>	
A.	INTRODUCTION	26.001
B.	THE EVOLVING CYBERSECURITY LANDSCAPE	26.005
1.	Early 2000s	26.006
2.	The 2010s	26.010
3.	The 2020s	26.012
C.	OPERATIONAL RESILIENCE	26.014
D.	THE PRE-AI CYBERSECURITY LANDSCAPE	26.019
E.	THE REGULATION OF AI IN THE UK AND BEYOND	26.030
1.	Core principles	26.031
2.	Implementation strategy	26.033
(a)	Utilising existing regulators	26.033
(b)	Non-statutory approach with potential statutory duties	26.034
(c)	Consultation period	26.035
3.	The UK regulatory landscape of the future?	26.037
4.	The regulatory position further afield	26.041
F.	THE ROLE OF AI IN COMMON CYBER-ATTACKS	26.048
1.	Phishing	26.051
2.	AI and phishing	26.053
3.	Payment diversion	26.060
4.	Ransomware	26.065
5.	Ransomware: double and triple extortion attempts	26.072
(a)	Double extortion ransomware	26.073
(b)	Triple extortion ransomware	26.074
6.	Denial of service attacks	26.075
G.	EMERGING THREATS	26.077
1.	Cyber threats to critical national infrastructure	26.077
H.	THE AMPLIFICATION OF THREATS BY AI	26.083
1.	Data poisoning	26.084
2.	Espionage	26.089
3.	The new human threat	26.092
I.	THE NEW LEGAL THREAT	26.098
1.	Discrimination and bias	26.099
2.	Health and safety	26.102
3.	Constructive/unfair dismissal	26.105
4.	Data protection and GDPR compliance	26.108
J.	LOOKING FORWARD	26.113
1.	Incident response plans	26.118
2.	Tabletop exercises	26.119
3.	Cyber exercises	26.120
K.	NICE TO HAVE OR ESSENTIAL TO HAVE?	26.121
L.	CONCLUSION	26.126

EXTENDED CONTENTS

27	Misinformation and disinformation	
	<i>Erica Stanford</i>	
A.	INTRODUCTION	27.001
B.	TYPES OF MISINFORMATION AND DISINFORMATION	27.006
C.	DIRECTLY APPLICABLE LEGISLATION	27.027
1.	UK	27.028
2.	EU	27.048
3.	US	27.054
D.	FRAUD	27.058
E.	INFORMATION AND POLITICS	27.066
1.	UK	27.073
2.	EU	27.075
3.	US	27.078
F.	COMMERCIAL TRANSACTIONS	27.082
1.	UK	27.082
2.	EU	27.086
3.	US	27.089
4.	Judicial responses to generative AI	27.092
G.	SOCIAL HARM	27.094
1.	UK	27.096
2.	EU	27.099
3.	US	27.100
H.	FINANCE AND FUNDING	27.103
I.	CONTENT MODERATION	27.109
J.	ADVOCACY	27.112
K.	CONCLUSION	27.117
28	Ethics	
	<i>Patricia Shaw</i>	
A.	INTRODUCTION	28.001
1.	Generative AI	28.006
2.	AI as a learning machine	28.011
3.	Anthropomorphised AI	28.013
4.	AI and decision-making	28.014
5.	AI and the iHuman	28.019
6.	Education and awareness	28.022
B.	FORMS OF PRACTICAL APPLICATION OF ETHICS IN AI	28.025
1.	Frameworks	28.030
2.	Risk and impact assessment tools	28.034
3.	Principles	28.041
4.	Standards	28.054
(a)	IEEE	28.059
(b)	ISO	28.060
(c)	BSI	28.062
(d)	NIST	28.066
(e)	Consolidated Standards of Reporting Trials – Artificial Intelligence (CONSORT-AI)	28.067
5.	Regulatory guidance	28.071
6.	Certification	28.084
7.	Audit	28.089
C.	AI REGULATION TAKING ACCOUNT OF ETHICS AND POWER	28.094
D.	BEST PRACTICE FOR REGULATORS	28.105
1.	AI regulation	28.110
2.	Risk and impact assessment	28.115
3.	More effective human oversight	28.118
E.	CONCLUSION	28.122

29	Bias and discrimination <i>Minesh Tanna and William Dunning</i>	
	A. INTRODUCTION	29.000
	B. WHAT ARE BIAS AND DISCRIMINATION?	29.004
	1. What is bias?	29.004
	2. What is discrimination?	29.006
	C. DIFFERENT TYPES OF AI BIAS	29.012
	1. Biases introduced by data	29.013
	2. Biases introduced by developers	29.015
	3. Stability bias	29.020
	4. Biases introduced by AI systems	29.024
	5. The role of human users of AI systems	29.025
	D. THE CURRENT LEGAL POSITION ON AI BIAS AND DISCRIMINATION	29.027
	1. Anti-discrimination law	29.028
	(a) Direct discrimination	29.030
	(b) Indirect discrimination	29.034
	2. Data protection law	29.038
	E. BIAS AND DISCRIMINATION IN THE CONTEXT OF ETHICAL/RESPONSIBLE AI	29.050
	1. Understanding ethical/responsible AI	29.050
	2. Bias and discrimination in the context of ethical/responsible AI	29.055
	3. Fairness	29.058
	4. Transparency and explainability	29.064
	5. Technical robustness or accuracy	29.067
	6. Accountability and oversight	29.071
	F. SIGNIFICANCE OF EMERGENT AI REGULATION	29.075
	1. Increased focus on bias and discrimination through ethical/responsible AI	29.075
	2. Regulation of facial recognition technology	29.076
	3. Emergent AI regulation addressing bias and discrimination	29.081
	(a) EU	29.084
	(b) United States	29.089
	4. Challenges of regulating bias and discrimination in AI	29.091
	G. CONCLUSION	29.094
30	AI and human rights <i>Mando Rachovitsa</i>	
	A. INTRODUCTION	30.000
	B. STATES' HUMAN RIGHTS OBLIGATIONS WITHIN THE LIFECYCLE OF AI SYSTEMS	30.006
	1. The challenges of algorithmic opacity to human rights law	30.010
	(a) Unintentional algorithmic opacity and the 'black box' effect	30.011
	(b) The challenges for prohibited discrimination in law to capture bias in AI systems	30.012
	(c) Intentional algorithmic opacity	30.014
	(d) (Un)intentional algorithmic opacity and the implications for judicial scrutiny	30.016
	2. States' responsibility to regulate AI systems via impact assessments	30.018
	C. NON-STATE ACTORS' HUMAN RIGHTS DUTIES	30.022
	D. AI SYSTEMS INCOMPATIBLE WITH HUMAN RIGHTS LAW?	30.031
	1. Sentiment detection in the workplace or educational setting	30.032
	2. Social scoring	30.033
	3. Predictive policing	30.034
	(a) Biometric recognition and categorisation	30.035
	(b) Manipulation and exploitation of vulnerabilities	30.038
	(c) Automated individual decision-making	30.043
	E. CONCLUSION	30.044

31	Public policy and government <i>Charles Kerrigan and Erica Stanford</i>	
	A. INTRODUCTION	31.001
	B. AI POLICY GOALS AND STRATEGIES IN THE UNITED KINGDOM	31.002
	C. BEST PRACTICE OUTSIDE THE UK	31.007
	1. Singapore	31.008
	2. Estonia	31.011
	D. GOVERNMENT USE OF AI IN PUBLIC SERVICES	31.018
	1. AI for automation, decision support and service enhancement	31.019
	2. Case studies of AI applications in government	31.025
	3. Ethical, legal and practical challenges in AI adoption	31.032
	(a) Ethical and societal challenges	31.033
	(b) Legal and regulatory challenges	31.035
	(c) Practical and operational challenges	31.038
	E. THINK TANKS ON AI IN PUBLIC POLICY	31.044
	F. CONCLUSION	31.046
	PART V TECHNICAL AND CONSULTING	
32	Education <i>Charles Kerrigan</i>	
	A. INTRODUCTION	32.001
	B. AI IN EDUCATION	32.003
	1. AI as teacher	32.006
	2. AI as student	32.013
	3. Economic effects on students and institutions	32.018
	4. Law firms	32.023
	5. Staff	32.026
	6. Social and moral implications	32.029
	7. Future of work	32.033
	C. CONCLUSION	32.040
33	AI taxonomies and emergent issues in intelligence <i>Tirath Virdee and Alex Flom</i>	
	A. INTRODUCTION	33.001
	B. BACKGROUND MATTERS	33.002
	C. DIMENSIONS OF AI TAXONOMY	33.017
	1. Intelligence or functional paradigm	33.019
	2. Historical development paradigm	33.020
	3. Architectural paradigm	33.021
	4. Learning paradigm	33.022
	5. Data utilisation paradigm	33.023
	6. Cognitive capabilities paradigm	33.024
	7. Emergent properties paradigm	33.025
	8. Deployment paradigm	33.026
	9. Interaction modalities paradigm	33.027
	10. Temporal dynamics paradigm	33.028
	11. Scale and complexity paradigm	33.029
	12. Safety oriented taxonomy paradigm	33.030
	13. Natural intelligence paradigm	33.031
	14. Metacognition paradigm	33.032
	15. Universal intelligence paradigm	33.033
	D. TAXONOMY OF AI: PARADIGMS AND IMPLICATIONS	33.036
	1. Intelligence or functional paradigm	33.036
	2. Historical development paradigm	33.040

3.	Architectural paradigm	33.048
4.	Learning paradigm	33.054
	(a) The five tribes of machine learning	33.061
	(b) Unification of the tribes of machine learning	33.067
	(c) Simple versus deep learning	33.071
5.	Data utilisation paradigm	33.075
6.	Cognitive capabilities paradigm	33.081
7.	Emergent properties paradigm	33.088
8.	Deployment paradigm	33.094
9.	Interaction modalities paradigm	33.100
10.	Temporal dynamics paradigm	33.105
11.	Scale and complexity paradigm	33.111
12.	AI safety paradigm	33.117
13.	Natural intelligence paradigm	33.123
	(a) The AI Periodic Table	33.129
	(b) The 14 groups of the AI Periodic Table	33.135
	(c) Relationship between natural intelligence and taxonomy	33.138
14.	Metacognition paradigm – thinking about thinking	33.146
15.	Emotional and irrational intelligence paradigm	33.159
16.	Universal intelligence paradigm – what problem is the universe trying to solve?	33.166
	(a) Implications for current philosophical discourses	33.177
E.	THE LEGAL IMPLICATIONS OF AI TAXONOMY	33.182
F.	ETHICS, GOVERNANCE – DIFFERENCES AND SIMILARITIES BETWEEN NATURAL AND ARTIFICIAL INTELLIGENCE	33.184
G.	THE ROAD TO DEMOCRATISATION	33.185
H.	OTHER ISSUES AROUND AI	33.190
I.	COUNCIL OF THE WISE – THE CURRENT STATE OF THE ART IN AI	33.198
J.	CONCLUSION	33.204
34.	Federated learning	
	<i>Tom Marshall and Nicolas D. Lane</i>	
A.	INTRODUCTION	34.001
B.	TYPES OF LEARNING	34.005
C.	CATEGORISATIONS	34.006
	1. Horizontal federated learning	34.007
	2. Vertical federated learning	34.008
	3. Federated transfer learning	34.009
D.	USE CASES	34.010
	1. Personalised recommendation systems	34.012
	2. Healthcare analytics	34.013
	3. Edge computing and IoT	34.014
E.	CARBON FOOTPRINT	34.015
F.	CHALLENGES	34.017
	1. Privacy attacks and poisoning attacks	34.018
	2. Computational efficiency	34.019
	3. Transparency	34.020
	4. Incentive mechanisms	34.021
	5. Intellectual property	34.022
G.	FEDERATED LEARNING AND DAOs	34.023
H.	REGULATION	34.025
	1. Data protection and privacy laws	34.025
	2. Ethical and social norms	34.028
	3. Technical and industry standards	34.030
	4. Intellectual property rights	34.032
I.	CONCLUSION	34.035

35.	Autonomy and fairness	
	<i>Emre Kazim, Adriano Koshiyama, Airlie Hilliard, Anisha Chadha, Charles Kerrigan and Jeremy Barnett</i>	
A.	INTRODUCTION	35.001
B.	FAIRNESS	35.002
	1. Unfairness in systems	35.004
	2. Automation is unfair	35.005
C.	WHAT IS FAIRNESS?	35.009
	1. Outcome	35.010
	2. Procedural	35.011
	3. Mutual exclusivity of fairness definitions	35.013
	4. Pick one(!)	35.015
	5. Prioritise notions of fairness	35.016
	6. Fairness and discernment	35.020
	7. Who discerns?	35.025
D.	WHEN AND WHAT TO AUTOMATE	35.030
	1. Automating implementation	35.030
	2. Amplification of unfairness	35.031
	3. Automating fairness	35.032
	4. Automated intentionality	35.033
E.	BENCHMARKING OR DETECTION AND ASSESSMENT OF DISCRIMINATION	35.035
F.	OPACITY AND THE LEGITIMACY OF PUBLIC REASONING	35.051
G.	CONCLUSION	35.061
36.	Risk management	
	<i>Stephen Ashurst</i>	
A.	INTRODUCTION	36.001
B.	A CASE STUDY IN AI AND MACHINE LEARNING	36.014
C.	THE BOUNDARIES AND RULES OF RISK MANAGEMENT	36.025
D.	HOW RISK MANAGEMENT CAN HELP AND HINDER	36.030
E.	PHILOSOPHICAL LOGIC AND A LACK OF REASONABLENESS	36.036
F.	THE VALUE OF DISCRETION	36.046
G.	CREATIVITY AND INSIGHT	36.048
H.	DESCRIPTION OF THE RISK MANAGEMENT INDUSTRY AND PROCESS	36.056
I.	A PRACTICAL INTRODUCTION TO RISK MANAGEMENT IN THE REAL WORLD	36.064
J.	APPLIED AI IN THE REAL WORLD	36.071
K.	A POSSIBLE FUTURE FOR AI IN RISK MANAGEMENT	36.083
L.	CONCLUSION	36.086
37.	Business models and procurement	
	<i>Petko Karamotchev</i>	
A.	INTRODUCTION	37.001
	1. Key shifts in the AI landscape	37.002
	2. Predictions fulfilled and those ahead of their time	37.004
	3. AI sets new challenges in regulation and procurement	37.006
B.	MODERN AI BUSINESS MODELS AND HOW TO PROCURE THEM	37.011
	1. Modern AI business models and their procurement	37.011
	2. AI business models and procurement	37.013
	(a) AI as a Service (AlaaS)	37.014
	(b) Product/feature enhancement	37.018
	(c) Data monetisation	37.020
	(d) Autonomous operations	37.022
	(e) AI-driven innovation	37.026
	(f) Freemium AI models	37.029
	(g) Marketplace models	37.031
	(h) Subscription-based AI models	37.034

EXTENDED CONTENTS

(i) Consultancy and custom solutions	37.020
(j) Partner ecosystems	37.040
3. Transformative shift ahead	37.040
4. Steps for AI procurement	37.044
5. AI in procurement: business models and market implications	37.044
6. Redefining business models through AI	37.048
7. Barriers and strategic recommendations	37.051
8. Policy implications and market infrastructure	37.051
9. Legal considerations in procurement	37.054
10. Direct AI regulation	37.055
11. Contracts terms	37.055
C. CONCLUSION	37.058
38. Explainable AI and responsible AI	37.060
<i>Charles Kerrigan</i>	
A. INTRODUCTION	38.000
B. DEFINITIONS AND USE	38.000
C. CURRENT STATUS OF EXPLAINABLE AI	38.011
D. NEED FOR RESPONSIBLE AI	38.011
E. CHALLENGES	38.020
F. CURRENT RESEARCH	38.020
G. CONCLUSION	38.040
39. Legaltech and law firms	38.040
<i>Erica Stanford and Charles Kerrigan</i>	
A. INTRODUCTION	39.000
B. ROLES	39.000
1. The role of AI in legal tech	39.000
2. The role of generative AI in law and legal tech	39.000
C. USE CASES AND EXAMPLES	39.000
1. Use cases for AI in legal practice	39.000
(a) Contract and document review	39.000
(b) Knowledge and eDiscovery	39.005
(c) Litigation	39.011
(d) Dispute resolution and changes to justice	39.012
(e) Regulatory compliance	39.013
(f) Data analytics	39.014
(g) Predictive analytics	39.015
(h) Project management	39.018
(i) Fraud detection and risk assessment	39.017
(j) Plagiarism and writing checkers	39.018
(k) AI alerts	39.019
(l) Client visualisations and presentations	39.020
(m) AI in recruitment	39.021
(n) Education	39.021
2. Examples of AI-enabled legal tech tools	39.023
(a) Harvey	39.023
(b) Kira	39.024
(c) Relativity	39.025
(d) Westlaw Edge	39.026
D. BUSINESS	39.027
1. The legal industry	39.027
2. The billing model	39.027
3. Organisational structures	39.031
4. Integrating new legal tech and AI tools	39.034

EXTENDED CONTENTS

5. Return on investment	39.041
E. RISK MANAGEMENT	39.044
1. Principles for how lawyers might safely, ethically and beneficially use AI	39.044
2. Risks and considerations of using AI	39.048
(a) Unknown and future risks	39.048
(b) Data privacy	39.049
(c) Data acquisition and training data	39.050
(d) Misinformation and hallucinations	39.051
(e) Bias and discrimination	39.052
(f) Cybersecurity risks	39.053
(g) Lack of transparency	39.054
(h) Over-reliance and bias confirmation	39.055
F. CONCLUSION	39.056

Index	982
-------	-----

ARTIFICIAL INTELLIGENCE AND STANDARDS

Sam De Silva and Barbara Zapisetskaya

A. INTRODUCTION	9.001	H. INTERNATIONAL STANDARDS AND AI GOVERNANCE	
B. HOW STANDARDS ARE DEVELOPED AND THE ROLE OF NATIONAL STANDARDS' BODIES	9.005	1. AI Governance Standard: scope	9.045
1. Relationship between European and international standards	9.008	2. Accountability of governing bodies	9.046
2. International AI standards development	9.009	3. Appropriate level of oversight of AI	9.048
C. HOW STANDARDS WORK	9.011	4. Practical steps organisations can take to alleviate constraints on the use of AI	9.051
1. Overview	9.011	(a) Increase oversight of compliance	9.053
2. How do standards work for AI?	9.014	(b) Address the scope of AI use	9.054
D. THE ROLE THAT THE AI ACT GIVES TO STANDARDISATION	9.016	(c) Assess and address the impact on stakeholders	9.055
E. THE COMMISSION'S STANDARDISATION REQUEST	9.018	(d) Determine legal requirements or obligations of using the technology	9.056
1. Alignment with the AI Act	9.022	(e) Align the use of AI to the organisation's objectives, culture and values	9.057
F. RISK MANAGEMENT – ARTICLE 9 AND AI RISK MANAGEMENT STANDARD (ISO/IEC 23894)	9.024	(f) Ensure that problem solving takes due account of context	9.058
1. Gaps with Article 9	9.030	(g) Examine the additional risk that the use of AI can bring to an organisation	9.059
G. QUALITY MANAGEMENT – ARTICLE 17 AND AI MANAGEMENT SYSTEM STANDARD (ISO/IEC 42001)	9.033		9.060
1. AI Management System Standard (ISO/IEC 42001)	9.038	I. CONCLUSION	9.061
2. Gaps with Article 17	9.042		

A. INTRODUCTION

9.001 Standards have a crucial role to play in the information communications and telecommunications (ICT) sector generally, and in particular in relation to AI. ICT standards are essential in achieving interoperability of new technologies and can bring significant benefits to both industry, consumers and society. The development of ICT standards is integral to AI technologies and systems, in that these standards address inter-

alia the capture, storage, retrieval, processing, display, representation, security, privacy and interchange of data and information.¹

A standard is a document established by consensus and approved by a recognised body. It provides rules, guidelines or characteristics for activities or their results so that they can be repeated. The aim is to achieve the greatest degree of order in a given context.² In addition, according to NIST, standards allow technology to work seamlessly and establish trust so that markets can operate smoothly. They:

- provide a common language to measure and evaluate performance;
- make interoperability of components made by different companies possible; and
- protect consumers by ensuring safety, durability, and market equity.³

The European Union (EU) in particular has acknowledged the critical role of standards in transformative technologies with broad societal implications, such as AI. Over the past few years, the EU and its member countries have been proactive in establishing a unified European strategy for AI governance and standardisation. The EU has consistently utilised the dynamic relationship between regulation and standards as a key component of both its internal market and international commerce, particularly in relation to AI. Therefore, the EU's recognition of this interplay, along with the ongoing efforts to revamp European standardisation in conjunction with the EU AI Act, should be viewed as essential to the future governance of AI, both within the EU and on a global scale.

In this chapter we will consider how standards are developed, the two main types of standards and the role of standardisation in the implementation of the AI Act. We provide an overview of three international AI standards which relate to AI risk management, AI quality management and AI governance and explore how two of these standards could be useful in the implementation of the AI Act.

B. HOW STANDARDS ARE DEVELOPED AND THE ROLE OF NATIONAL STANDARDS' BODIES

9.005 Standards are developed at national, European and international level through designated bodies. Standards are developed at international level by the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) and at European level by the CEN (European Committee for

¹ https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf
² <https://www.gov.uk/guidance/standardisation>
³ <https://www.nist.gov/services-resources/standards-and-measurements>

Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute), referred to collectively as the European Standardisation Organisations (ESOs).

9.006 Standards are developed by bringing together all interested parties such as manufacturers, consumers, regulators, researchers and experts regarding a particular material, product, process or service. Standardisation is the process through which requirements and recommendations for products, processes and services are developed by experts and agreed upon through a consensus-based mechanism.

9.007 National standards bodies (such as the British Standards Institute (BSI),⁴ for the United Kingdom) are usually members of both European and international standards organisations, including the CEN, CENELEC, ISO and IEC, as well as ETSI. To engage with and influence the work of these international bodies, the relevant national body forms 'national mirror committees' composed of national experts. These committees align with their counterparts at ISO, IEC, CEN and CENELEC levels, tracking and participating in international standardisation efforts and recording national positions on work items.

1. Relationship between European and international standards

9.008 The ongoing collaboration between the CEN and ISO, as well as CENELEC and IEC, facilitates a degree of alignment between European and international standards. International standardisation is prioritised whenever feasible to harness the advantages of global standards in fostering international trade and market harmonisation. Due to existing agreements between the ISO and CEN and the IEC and CENELEC, certain internationally developed standards may be adopted as European standards by these entities. It needs to be seen how this alignment will continue to evolve in the context of the AI Act once the European standards to support its implementation are developed. We discuss potential areas of divergence in further detail below.

2. International AI standards development

9.009 In a world that is increasingly interconnected, the development of international AI standards is crucial for fostering a unified global perspective on reliable AI systems and enhancing public confidence in AI technologies. The surge of interest and activity in AI in recent years has underscored the need for a consistent set of international AI standards. To address this global requirement, the ISO and IEC have established a joint standardisation committee for AI, known as ISO/IEC JTC 1/SC 42 (Subcommittee

⁴ Refer to the section on BSI in the AI Ethics chapter for more details.

42),⁵ which is actively engaged in AI and big data. At the time of writing, its working groups are in the process of creating standards that cover various facets of AI.

The Institute of Electrical & Electronics Engineers (IEEE) is also active in AI standardisation, especially regarding autonomous and intelligent systems. At the time of writing, the IEEE is in the process of developing its 7000 Series, which addresses ethical considerations across a wide array of issues related to autonomous and intelligent systems.⁶ These include aspects such as transparency, privacy, algorithmic bias, personal data categories, the creation of machine-readable privacy terms for individuals and the ethical ramifications of simulated empathy in AI systems. 9.010

C. HOW STANDARDS WORK

1. Overview

Standards were initially established to ensure safety, quality and interoperability. For businesses aiming to operate on a global scale, international standards are preferred over national or regional ones, as they provide a uniform framework for market operations worldwide. Historically, older standards primarily focused on interoperability as the main societal benefit. However, many modern standards also encompass social, economic and political goals or consequences, thereby setting contemporary norms. 9.011

General standards can encompass a variety of forms, from best practice documents and deployment guidance to specifications for interoperability at different levels, such as physical, network or application. Generally, compliance with these standards is voluntary. 9.012

The other type of standard is a management system standard (MSS). The ISO defines an MSS as the way in which an organisation manages the interrelated parts of its business in order to achieve its objectives. These objectives can relate to a number of different topics, including product or service quality, operational efficiency, environmental performance, health and safety in the workplace and many more. Organisations can get their MSS certified by a third-party auditor. 9.013

2. How do standards work for AI?

Standardisation for AI is still in the early stages. In Europe, organisations such as ETSI and CENELEC have set out ambitious agendas for standardisation, partly 9.014

⁵ Refer to the section on ISO in the AI Ethics chapter for more details.

⁶ Refer to the section on IEEE in the AI Ethics chapter for more details.

driven by the AI Act's framework for standards. ETSI has been concentrating on security aspects of AI and machine learning, while CENELEC has been focusing on trustworthiness and ethics. As mentioned above, European-focused standardisation bodies are particularly significant to both the European Commission and the AI Act because they are the only entities capable of developing harmonised standards.

9.015 In addition to security, trust and ethics, the standardisation of AI is poised to significantly influence the cross-sector application of AI. Currently, many AI solutions are sector-specific, such as those in healthcare or intelligent transportation. The ability to utilise large datasets across different sectors is expected to spur even greater innovation in AI. The safe and ethical exchange of data between sectors is anticipated to be a major advancement in AI. Standards that ensure the safe, ethical, efficient and reliable transfer of information will be among the most impactful developments for AI in the years ahead. ETSI is currently focusing on workstreams related to the data supply chain and the availability of training data, while the ISO is engaged in several projects concerning AI and big data.

D. THE ROLE THAT THE AI ACT GIVES TO STANDARDISATION

9.016 As described in detail in Chapter 8, the AI Act categorises three main categories of risk relevant to AI systems that are within scope: (i) unacceptable risk, (ii) high risk (iii) low risk. The majority of the AI Act establishes the framework that applies to high-risk systems.

9.017 AI systems deemed high-risk are considered to meet the AI Act's requirements if they conform to harmonised standards published in the Official Journal of the European Union (OJEU) (Article 40) or to common specifications set by the European Commission (Article 41). In essence, compliance to established standards or common specifications significantly reduces the compliance obligations for providers of high-risk AI under the AI Act. In certain cases, meeting harmonised standards or common specifications allows for conformity assessment through internal control instead of external evaluation.

E. THE COMMISSION'S STANDARDISATION REQUEST

9.018 The AI Act includes provisions for the use of harmonised standards to comply with the requirements of the AI Act. The Commission's request for standardisation sets the stage for the development of these standards, guiding the creation of technical specifications that align with the EU's regulatory objectives and ensuring that high-risk AI systems meet the necessary safety, quality and ethical standards.

In December 2022, the European Commission published a draft standardisation request to the CEN and CENELEC in support of the 'key technical areas covered' by the EU AI Act. This request was finally adopted by the European Commission in May 2023 (Standardisation Request) and accepted by the CEN and CENELEC.⁷ The CEN and CENELEC are the primary recipients of the Commission Request, with ETSI also mentioned as a potential contributor. Under the Standardisation Request the following new European standards (European Standards) or (Deliverables) that address the following areas are required to be developed, each of which are referred to as Standardisation Requests (SR) numbered from 1 to 10:

- SR1: Risk management system for AI systems: These ESDs will specify the requirements for a risk management system for AI systems. The aim is to establish a continuous iterative process throughout the AI system's lifecycle that prevents or minimises risks to health, safety or fundamental rights. The requirement is for ESDs to be drafted in such a way as to enable usability by relevant operators and market surveillance authorities.
- SR2: Governance and quality of datasets used to build AI systems: These ESDs will include specifications for adequate data governance and data management procedures to be implemented by AI system providers. They will focus on data generation and collection, data preparation operations, addressing biases and ensuring the quality of datasets used to train, validate and test AI systems.
- SR3: Record keeping through logging capabilities by AI systems: These ESDs will define specifications for automatic logging of events by AI systems. The aim is to enable traceability throughout the system's lifecycle, monitor operations and facilitate post-market monitoring by providers.
- SR4: Transparency and information provisions to the users of AI systems: These ESDs will provide specifications for design and development solutions that ensure transparency of AI system operations, enabling users to understand the system's output and use it appropriately. They will also include instructions for use, including system capabilities and limitations, as well as maintenance and care measures.
- SR5: Human oversight of AI systems: These ESDs will specify measures and procedures for human oversight of AI systems. Providers will be required to identify and build these measures into the system before placing it on the market or putting it into service. Users should also be able to implement appropriate oversight measures. These ESDs shall also establish, where appropriate, appropriate oversight measures that are specific to certain AI systems in consideration of their intended purpose. With respect to AI systems intended for remote biometric identification of persons, human oversight measures will need to provide for the possibility that no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons.
- SR6: Accuracy specifications for AI systems: These ESDs will outline specifications to ensure an appropriate level of accuracy for AI systems. For the purpose of these ESDs, 'accuracy' shall be understood as referring to the capability of the AI system to perform

⁷ https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_en.

the task for which it has been designed. This should not be confused with the narrower definition of statistical accuracy, which is one of several possible metrics for evaluating the performance of AI systems. Providers will be able to declare relevant accuracy metrics and levels, and appropriate tools and metrics will be defined to measure accuracy against defined levels.

- Providers will be able to declare relevant accuracy metrics and levels, and appropriate tools and metrics will be defined to measure accuracy against defined levels.
- SR7: Robustness specifications for AI systems: These ESDs will lay down specifications for the robustness of AI systems, taking into account sources of errors, faults, inconsistencies and interactions with the environment. They will also consider AI systems that continue to learn after being deployed.
- SR8: Cybersecurity specifications for AI systems: These ESDs will provide suitable organisational and technical solutions, to ensure that AI systems are resilient against attempts to alter their use, behaviour or performance or to compromise their security properties by malicious third parties exploiting the systems' vulnerabilities. Organisational and technical solutions shall therefore include, where appropriate, measures to prevent and control cyberattacks trying to manipulate AI-specific assets, such as training datasets (for example, data poisoning) or trained models (for example, adversarial examples) or trying to exploit vulnerabilities in an AI system's digital assets or the underlying ICT infrastructure.
- SR9: Quality management system: These ESDs will be drafted for providers of AI systems to be implemented within their organisation, with particular consideration given to small and medium-sized organisations. Specifications shall be drafted such that the quality management system aspects related to the AI system may be integrated into the overall management system of the provider.
- SR10: Conformity assessment for AI systems: These ESDs will provide procedures and processes for conformity assessment activities related to AI systems and the quality management system of AI providers. They will also include criteria for assessing the competence of individuals involved in conformity assessment activities, considering scenarios where the assessment is carried out by the provider or a professional external third-party organisation.

9.020 According to the Standardisation Request, while it is not always possible to develop ESDs that consider each specific intended purpose, such ESDs shall cover at the minimum a range of technical solutions and options, which the product manufacturer can assess and implement, taking into consideration the intended purpose of their specific system. ESDs shall also possibly include guidance on how such assessment and implementation of solutions and options shall be executed.

9.021 All ten SRs must be completed by 30 April 2025. However, this is a very challenging timeframe given that on average it takes at least 3–4 years to develop a standard.

1. Alignment with the AI Act

Several of the ten areas identified in the Standardisation Request are covered (in part) 9.022 by international standards that are either published or currently under development. For example, at the time of writing, there are standards addressing risk management (ISO/IEC 23894), data quality and governance (ISO/IEC CD 5259 series), transparency (IEEE 7001, ISO/IEC AWI 12792), human oversight (ISO/IEC 8200, ISO/IEC PWI 18966), accuracy (ISO/IEC TS 4213:2022), robustness (ISO/IEC TR 24029-1, ISO/IEC DIS 24029-2) and cybersecurity (ETSI SAI series). Other standards, although not directly related to the ten areas mentioned in the Standardisation Request, are relevant to some of the requirements of the AI Act, for example, standards on bias (ISO/IEC AWI TS 12791, ISO/IEC TR 24027, P7003), testing (ISO/IEC TR 29119-11) and verification and validation (ISO/IEC TS 17847).

We will now focus on two key standards relevant to the Standardisation Request: (1) 9.023 the standard addressing risk management (ISO/IEC 23894); and (2) the AI management system standard (ISO/IEC 42001).

F. RISK MANAGEMENT – ARTICLE 9 AND AI RISK MANAGEMENT STANDARD (ISO/IEC 23894)

Article 9 of the AI Act mandates the creation and maintenance of a risk management 9.024 system (RMS) for high-risk AI systems throughout their lifecycle. This RMS should be a systematic process that includes identifying and analysing known and foreseeable risks, estimating and evaluating risks from intended use and potential misuse, and considering additional risks from post-market monitoring. After this analysis, appropriate risk management measures must be implemented.

The objective of the RMS as required by Article 9 of the AI Act is to ensure that the 9.025 overall residual risk associated with high-risk AI systems is at an acceptable level. This residual risk should be communicated to users. In implementing risk management measures, priority should be given to eliminating or mitigating risks through thoughtful design and development. For risks that cannot be eliminated, measures should be put in place to control them, and users should be provided with sufficient information and training.

Article 9 of the AI Act also stipulates that high-risk AI systems must undergo test- 9.026 ing to identify appropriate risk management measures and to verify their consistent performance. The testing procedures should be tailored to the AI system's intended purpose and conducted at appropriate stages during the development process, prior to

market release. This ensures that the high-risk AI systems are evaluated for safety and efficacy before they are made available for use.

9.027 Currently, the only existing standard relating to AI risk management is ISO/IEC 23894 (the AI Risk Management Standard). The AI Risk Management Standard builds upon the ISO 31000:2018 (the 'General Risk Management Standard') which provides general guidance on risk assessment. The General Risk Management Standard describes: (i) the underlying principles of risk management (integrated, inclusive, continual improvement, structured and comprehensive risk management); (ii) how risk management frameworks should be integrated into significant activities and functions of an organisation; and (iii) how risk assessment processes and practices help to identify risk and ways to manage risk (as more fully discussed below). Similar to the General Risk Management Standard, the AI Risk Management Standard is not an MSS.

9.028 The AI Risk Management Standard uses the General Risk Management Standard as its base but goes further by suggesting that organisations that develop, deploy or use AI products, systems and services need to manage specific risks relating to this technology and consider the context of AI in an organisation. It is not intended for the specific risk management of products and services using AI for objectives such as safety and security.

9.029 The AI Risk Management Standard states that AI systems can introduce new or emergent risks for an organisation, with positive or negative consequences on objectives, or changes in the likelihood of existing risks. The following principles have been incorporated into the AI Risk Management Standard:

- Inclusivity of stakeholders: As the use of AI systems can result in engagement with multiple stakeholders, organisations should seek dialogue with diverse internal and external groups, both to communicate harms and benefits and to incorporate feedback and awareness in the risk management process. Input from stakeholders will be beneficial for machine learning use cases, and generally for automated decision-making processes and ensuring overall transparency and explainability of AI systems.
- Dynamic risk management: As AI systems are dynamic and require continuous learning, refining and validating, legal and regulatory requirements related to AI need to be frequently updated. Organisations should seek to understand how AI will be integrated with management systems, and how it will impact their environmental footprints, health and safety and legal or corporate responsibilities.
- Best available information: As AI impacts the way individuals interact with and react to technology, it is advisable for organisations to retain information regarding ongoing use of AI systems throughout the entire lifetime of the AI system.
- Human and cultural factors: Human behaviour and culture significantly influence all aspects of risk management at each level and stage. Organisations engaged in the design,

development or deployment of AI systems, or any combination of these, should monitor their evolving cultural landscape. Organisations should focus particularly on effects of AI systems or their components on privacy, freedom of expression, fairness, safety, security, employment and environment, and more generally on human rights. Biases in decision-making are overlooked without human interpretation.

- Continual improvement: The identification of previously unknown risks related to the use of AI systems should be considered in the continual improvement process. Organisations engaged in the design, development or deployment of AI systems or system components, or any combination of these, should monitor the AI ecosystem for performance successes, shortcomings and lessons learned, and maintain awareness of new AI research findings and techniques.

1. Gaps with Article 9

While the AI Risk Management Standard appears to incorporate certain elements of Article 9 and the related Standardisation Request, it unfortunately omits other elements. The AI Risk Management Standard aligns with Article 9 by ensuring that risk management is an iterative process throughout the AI system's lifecycle, thoroughly documented and aimed at mitigating risk to acceptable levels. However, it does not require the communication of residual risks to users or address risks associated with foreseeable misuse. The AI Risk Management Standard also does not specify particular testing procedures for identifying risk management measures, nor does it set metrics or probabilistic thresholds for testing. 9.030

The AI Risk Management Standard diverges from Article 9 of the AI Act in its underlying concept of risk. The AI Risk Management Standard emphasises organisational risks, which are uncertainties that could affect an organisation's goals, whereas the AI Act views risk as potential harm to individuals' health, safety and fundamental rights. This difference limits the AI Risk Management Standard's effectiveness in implementing the AI Act's RMS requirements. 9.031

One of the key limitations is that the AI Risk Management Standard primarily offers recommendations rather than explicit requirements. In the field of standardisation, the distinction between requirements, typically indicated by 'shall', and recommendations, indicated by 'should', is critical because only standards with requirements can be utilised for conformity assessment. Standards that support the AI Act must be suitable for conformity assessment to verify that an AI system complies with the AI Act's requirements. However, since compliance with the AI Risk Management Standard cannot be demonstrated (as it is not an MSS), the AI Risk Management Standard as currently drafted unfortunately does not adequately operationalise the RMS requirements of the AI Act. 9.032

G. QUALITY MANAGEMENT – ARTICLE 17 AND AI MANAGEMENT SYSTEM STANDARD (ISO/IEC 42001)

- 9.033 Article 17 of the AI Act requires a quality management system to be put in place and be fully documented.
- 9.034 Specifically, compliance with Article 17 requires coverage of how to take into account the high-risk AI ecosystem by defining how to set up: (a) strategy for regulatory compliance; (b) technical specifications to be applied, including standards; (c) communication handling with national authorities; and (d) an accountability framework.
- 9.035 Article 17 also requires techniques and procedures for: (a) AI design, design verification and development; (b) AI examination, testing and validation; (c) data management; (d) quality control and assurance; (e) reporting of serious incidents and of malfunctioning; (f) record keeping of all relevant documentation and information; (g) conformity assessment; and (h) management of AI modifications.
- 9.036 Systems for risk management, post-marketing monitoring and resource management also need to be established.
- 9.037 While a single standard is very unlikely to provide the necessary technical specifications to comply with all requirements of Article 17, a standard that establishes a quality system encompassing all of the above-mentioned aspects is crucial for ensuring compliance with the AI Act. Such a standard would integrate these elements into a systematic quality management system which should facilitate both conformity assessment and post-market quality monitoring.
1. AI Management System Standard (ISO/IEC 42001)
- 9.038 The AI Management System Standard provides considerable overlap with Article 17 requirement and is a management system standard on the responsible development and use of AI and is developed in relation to a circular process of establishing, implementing, maintaining and continually improving AI systems. It is comparable with other management system standards such as ISO 9000 (Quality) and ISO 27001 (Information Security) and similar to ISO 9000 and ISO 27001. The AI Management System Standard is an MSS.
- 9.039 In essence, an MSS helps organisations to: (a) improve their performance by specifying repeatable steps that they can implement to achieve their goals and objectives; and (b) create an organisational culture that reflexively engages in a continuous cycle of self-evaluation, correction and improvement of operations and processes through heightened employee awareness and management leadership and commitment.

The AI Management System Standard focuses on: (a) AI systems that have the potential to change their behaviour through use, presenting a challenge to ensure continuing monitoring and compliance with rules and/or accepted practices; (b) AI systems involved in automatic decision-making (possibly in a non-explainable or transparent way), which require specific management beyond that of a traditional system; and (c) the replacement of human interaction with machine learning, insight and data analysis, which increases the opportunities for applying AI systems while also changing the way those systems are justified, developed or deployed. 9.040

The AI Management System Standard is an auditable and certifiable standard. Audits are a vital part of the management system approach as they enable organisations to check how well their achievements meet their objectives and show conformity to the standard. 9.041

2. Gaps with Article 17

The content in Annex B of the AI Management System Standard, which provides implementation guidelines for AI controls, is highly relevant to Article 17. However, as the AI Management System Standard aims to offer organisations as much flexibility as possible in selecting necessary controls, it may not fully align with the regulatory requirements of the AI Act. This is because the AI Management System Standard allows organisations to determine the relevance of controls and choose which to adopt and does not provide a comprehensive set of justifications for control selection, nor does it establish a connection to regulatory requirements. 9.042

While the AI Management System Standard covers a broad range of Article 17's requirements, it often lacks sufficient technical implementation details. As the AI Management System Standard primarily offers guidance rather than mandatory controls, additional specifications that provide more explicit methodologies and implementation requirements will be required. Such additional specifications could include AI design considerations, quality control and assurance, testing or data management to ensure comprehensive coverage and regulatory compliance. 9.043

Other current gaps with the AI Management System Standard when compared with Article 17 requirements include: 9.044

- Post-marketing monitoring system coverage: To enhance compliance with the AI Act, more detailed requirements tailored to the AI Act's concerns and risks are necessary, as AI Management System Standard currently only mandates minimal system and performance monitoring, repairs, updates and support. The existing considerations in the AI Management System Standard should be expanded to include specific mechanisms for monitoring the potential adverse effects of AI system operations on individuals and

society. Additionally, there is a need for measures to identify risks that were not detected during the initial risk assessment and early stages of the AI lifecycle, as well as to recognise risks in the context of continuously learning systems.

- Management of AI modifications: To provide a more detailed framework for managing modifications to the AI system, it is necessary to specify the actions required for continuous assessment and management of risks, particularly when significant changes are made to the AI system. This includes establishing clear requirements for ongoing monitoring and evaluation to ensure the AI system remains compliant with the AI Act throughout its lifecycle.
- Documentation needs: The AI Management System Standard requires the production of multiple documentation items, and there is a need for more clarity and consolidation of these documentation requirements to streamline the application of this standard.

H. INTERNATIONAL STANDARDS AND AI GOVERNANCE

9.045 Although the Standardisation Request does not expressly refer to AI governance in general (as SR2 is limited to governance of datasets), the market had already acknowledged the need for a clear governance framework for AI and accordingly ISO had developed ISO/IEC 38507 (the AI Governance Standard) in 2022. The remainder of this chapter explores the AI Governance Standard.

1. AI Governance Standard: scope

9.046 The AI Governance Standard seeks, in its own words, 'to provide guidance for the governing body of an organization that is using, or is considering the use of, artificial intelligence'.⁸ In addition, the AI Governance Standard also provides guidance to:

- internal and external service providers (including consultants);
- executive managers;
- public authorities and policymakers;
- external businesses or technical specialists (including professional bodies, lawyers, accountants or other retail/industrial associations); and
- assessors and auditors.

9.047 The AI Governance Standard is not an MSS.

2. Accountability of governing bodies

9.048 According to the AI Governance Standard, given the potentially diverse applications of AI,⁹ which can impact any single area or function of an organisation, responsibility

⁸ ISO/IEC 38507:2022, p.1.

⁹ The AI Governance Standard states that reference to 'AI' is intended to be understood to refer to a whole family of technologies and methods, and not to any specific technology, method or application and 'use of AI' is defined in the

and accountability for AI governance should largely sit with an organisation's governing body, as opposed to delegating this to either a lower body (such as managers) or the AI itself. This is also important from an accountability perspective, as it ensures that accountability for AI governance sits alongside the governance of any other process, measure or tool operated by an organisation. As AI develops and takes on more human tasks and characteristics, governing bodies should not fall into the trap of anthropomorphising AI' and giving it human characteristics out of proportion to its actual role and capabilities.¹⁰

The AI Governance Standard states that as part of ensuring good and adequate AI accountability, organisations should ensure that they review their procedures and practices to ensure they are suitable for and adequately reflect their uses of AI. On a practical level, this could involve considering:

- Oversight: Does an organisation's use of AI correspond with its risk appetite and are all of the associated procedures (such as measurement, decision assurance and monitoring) fit for purpose? In light of the implications of using AI, the value of its use should also be captured.
- Direction: How does using AI advance the strategy or objectives of the organisation? Are existing organisational statements of values, codes of conduct or ethics appropriate for AI and is the level of resource allocated to AI commensurate to its use?
- Reporting: Is there communication and reporting to an organisation's stakeholders on how AI is used?
- Evaluation: Considering how AI has worked (both internally and externally) and other factors such as future opportunities and risks, are the governance processes (and any decisions taken under them) effective and can they be improved going forward?

As part of the evaluation process, governing bodies need to ensure that they themselves are equipped to effectively govern the use or introduction of AI across their organisation. The AI Governance Standard states that it is advisable to:

- work with stakeholders to build an understanding of AI and address any concerns they may have; or
- review internal processes, timelines and criteria to establish their adequacy in responding to the evolution of AI and its uses. This could involve creating a specialised AI subcommittee or working with other pre-existing committees (such as on strategy) to establish how AI impacts their work.

¹⁰ broadest sense as developing or applying an AI system through any part of its lifecycle to fulfil objectives and create value for the organisation. This includes relationships with any party providing or using such systems.

At p.4.

3. Appropriate level of oversight of AI

9.051 The AI Governance Standard acknowledges that the differing uses of AI and its enduring complexity dictate that organisations should take various factors into account when deciding the appropriate level of oversight, including:

- the type of AI used and the purpose of using it;
- the envisaged risks and benefits associated with the AI system;
- the functional layer of the AI ecosystem used;
- the role played by the organisation in the AI value chain (such as a customer, producer or provider) and the stage of implementation of the AI system.¹¹

9.052 While the majority of the above would initially be considered by governing bodies at the initial stage of introducing and using AI, it is important to ensure that AI is governed appropriately and effectively throughout its lifecycle.

4. Practical steps organisations can take to alleviate constraints on the use of AI

9.053 The AI Governance Standard emphasises the importance of not only appreciating the benefits of AI, but also understanding the potential risks and constraints it can introduce. To mitigate such issues, organisations can:

(a) Increase oversight of compliance

9.054 Governance oversight within organisations should be based on policies set by the organisation and should identify effective individual and collective accountability in an appropriate chain of responsibility, which is set alongside the context of use of AI. This includes putting policies in place to make sure that AI is used appropriately, that there is sufficient human oversight in place and that any persons using AI are properly trained and know how to raise concerns. Legal requirements or obligations may be determined for using such technologies alongside the risk appetite of the organisation. The AI Governance Standard notes that governing bodies should be aware of new sources of risk posed by AI technologies, including unwanted bias, cyber-threats and a lack of AI expertise.

(b) Address the scope of AI use

9.055 This principle involves considering the formulation of relevant assumptions on data and conducting a prior assessment on the availability, quality, quantity and suitability of data and an examination of potential biases. Formulating a description of the AI system, by way of its algorithms, data and models, would assist in ensuring the AI

¹¹ At p.17.

technology is being deployed for its intended use.¹² The foregoing principle needs to be considered in parallel with the importance of governance of data use, also addressed in the AI Governance Standard, when acknowledging that data is being used for the correct purpose and sensitive data is protected and secured.

(c) Assess and address the impact on stakeholders

The AI Governance Standard notes that the governing body is responsible outside of the context of AI for shaping and defining the organisation's desired culture, which has an impact on stakeholders connected to the organisation. It also notes the human impact on an organisation's culture and values, which are implicitly embedded in the behaviour of staff, and advocates for human involvement to a degree in the AI process, ensuring that AI systems can be monitored and corrected when needed. Conversely, the AI Governance Standard also highlights that the AI system can itself identify where human decision-making is flawed through bias and discrimination. A 'Cultures and Values Board' or an 'Ethics Review Board' might be set up to supervise the impact of AI systems and make sure they are aligned to an organisation's values and culture.¹³

(d) Determine legal requirements or obligations of using the technology

As AI and other technologies often used together with it (such as machine learning) develop, they will likely be subject to increasing regulation. Practical examples of this are facial recognition software or automated vehicles. Governing bodies need to ensure that as new legislation or other requirements are introduced, their use of AI remains compliant.¹⁴

(e) Align the use of AI to the organisation's objectives, culture and values

The use of AI will likely require an assessment of its impact on an organisation's objectives and strategy, whether it be to drive innovation and development or cut costs. Organisations should also take into account the effect of AI on their culture and values and take appropriate measures to safeguard those, if necessary.¹⁵

(f) Ensure that problem solving takes due account of context

Where using AI to solve problems, organisations should ensure that none of the context that would usually be apparent to a human (such as culture, values or behaviour) is lost, lest this lack of background affect the AI's output.¹⁶

¹² At p.10.
¹³ At p.10.
¹⁴ At p.11.
¹⁵ At p.11.
¹⁶ At p.11.

- (g) Examine the additional risk that the use of AI can bring to an organisation
- 9.060 Organisations should ensure that their use of AI remains within their appetite for risk and that appropriate processes and controls are in place to manage that risk.¹⁷

I. CONCLUSION

- 9.061 Given the transformative impact of AI, similar to the advent of computers, AI standards play a pivotal role in promoting its broad acceptance and adoption as a technology that is trustworthy, ethical and safe. These standards facilitate the integration of AI by addressing critical concerns such as safety, fairness, reliability, accountability and transparency, thereby supporting the ethical principles and guidelines that are essential for its widespread adoption. The three AI standards discussed in this chapter in relation to risk management (ISO/IEC 23894), AI management systems (ISO/IEC 42001) and AI governance (ISO/IEC 38507) should contribute to the practical and meaningful application of these ethical principles, fostering the adoption of AI on a global scale.
- 9.062 Standards are going to play a very important part in the implementation of the AI Act, and it remains to be seen to what extent international standards on AI will play a role in creation of the European standards on AI.

COMMERCIAL CONTRACTS

Iain Sheridan

A. INTRODUCTION	10.001	E. AI STANDARDS IN TERMS AND CONDITIONS	10.027
B. PRINCIPLES OF ENGLISH CONTRACT LAW	10.004	1. Leading AI standards	10.027
1. Intention to create legal relations	10.006	2. Common principles in AI standards	10.030
2. Offer and acceptance	10.007	(a) Technical transparency	10.031
3. Consideration	10.008	(b) Explainability	10.036
4. Certainty of the subject matter	10.009	(c) Robustness	10.038
5. Compliance	10.010	3. AI allocation of liability chart	10.040
C. MACHINE LEARNING	10.012	4. Drafting AI standards in contracts	10.041
1. Definitions	10.012	5. Miscellaneous AI risks to cover in contracts	10.043
2. Three key types of machine learning methods	10.013	(a) Trade secret risk exposure	10.043
3. Clause drafting for machine learning methods	10.016	(b) Key partner risk	10.044
4. Machine learning concepts relevant to contract management	10.018	(c) Data risk	10.045
D. AI AUGMENTING HEDGING AND INVESTMENT DECISIONS	10.019	F. AI AUGMENTING CONTRACT CLAUSES AND PROCESSES	10.046
1. Example of a company using unsupervised classification	10.020	1. AI image recognition of authorised contract signatures	10.047
2. Example of a company providing products relying on IBM Watson	10.023	2. AI prediction of <i>force majeure</i> events	10.058
3. Example of a company supplying an investment scoring system	10.025	(a) Backpropagation of errors	10.066
4. Example of a company providing trading strategies	10.026	3. AI calculation of termination payments	10.075
		4. Key questions to answer on any AI augmentation	10.086
		G. CONCLUSION	10.087

A. INTRODUCTION

Pre-contract due diligence requires not only precise drafting of agreed terms but also the foresight to accommodate worst-case scenarios. Commercial contracts across diverse sectors, especially those involving high-value subject matter, require both types of expertise. This need is evidenced by English High Court decisions, which often reveal deficiencies in pre-contract due diligence and imperfect drafting. Additionally,

10.001