

# Contents

<i>List of contributors</i>	x
<b>1 Emerging technologies and the criminal law</b>	<b>1</b>
DENNIS J. BAKER AND PAUL H. ROBINSON	
1. <i>Introduction</i>	1
2. <i>Artificial intelligence and criminal justice</i>	1
(a) <i>Artificial intelligence</i>	1
3. <i>Privacy, surveillance and biometrics</i>	7
4. <i>Censoring the Internet at large to prevent online harms</i>	21
5. <i>Overview of the chapters herein</i>	27
<b>2 Financial technology: opportunities and challenges to law and regulation</b>	<b>31</b>
THE RIGHT HON. LORD HODGE	
1. <i>Introduction</i>	31
2. <i>Fintech</i>	34
3. <i>DLT</i>	34
4. <i>Contract law</i>	40
5. <i>Tort/delict</i>	42
6. <i>Property law</i>	43
7. <i>Separate legal personality</i>	44
(a) <i>How the law should be adapted</i>	45
(b) <i>International conventions and model laws</i>	46
(c) <i>Regulation and regulatory sandboxes</i>	46
8. <i>Conclusion</i>	48
<b>3 Between prevention and enforcement: the role of “disruption” in confronting cybercrime</b>	<b>49</b>
JONATHAN CLOUGH	
1. <i>Introduction</i>	49
2. <i>The nature of disruption</i>	49

3. *The role of intelligence* 51
4. *The role of disruption in cybercrime* 52
  - (a) *Enforcement* 54
  - (b) *Technical means* 57
  - (c) *Intelligence gathering* 59
5. *Legislative frameworks and oversight* 60
6. *Criminal offences* 61
7. *Investigation powers* 62
8. *International cooperation* 66
9. *Conclusion* 72

#### 4 Preventive cybercrime and cybercrime by omission in China

74

HE RONGGONG AND JING LIJIA

1. *Introduction* 74
2. *Pre-inchoate criminalisation and early harm prevention* 76
  - (a) *Background of the latest amendments to PRC criminal law* 76
  - (b) *The harm justification for criminalising pre-inchoate cyberharm* 78
3. *Omissions liability for internet service providers* 84
  - (a) *Effective governance of cybercrime and the addition of citizens' positive duties* 86
4. *The constitutional dilemma: the deviation from marketplace norms* 90
  - (a) *The principle of personal responsibility* 92
5. *The normativity of private censorship and pre-inchoate criminalisation* 94
6. *Conclusion* 95

#### 5 Criminal law protection of virtual property in China

97

ZHANG MINGKAI AND WANG WENJING

1. *Introduction* 97
2. *Conceptualising virtual property* 98
  - (a) *General concept of a virtual asset* 98
3. *Categorising virtual property* 99
  - (a) *The problem with virtual property in China* 100
  - (b) *Virtual property articles* 102
  - (c) *Virtual currency as property* 104
  - (d) *Questions raised* 106
4. *Virtual property as property* 106
5. *The principle of legality* 110

6.	<i>China's current practice concerning virtual property</i>	118
7.	<i>The value of virtual property</i>	121
8.	<i>Conclusion</i>	125
<b>6</b>	<b>Criminalising cybercrime facilitation by omission and its remote harm form in China</b>	<b>126</b>
	LIANG GENLIN AND DENNIS J. BAKER	
1.	<i>Introduction</i>	126
2.	<i>Cybercrime: extending the reach of the current law</i>	128
3.	<i>Liability for indirect remote harm and direct pre-inchoate harm</i>	132
4.	<i>Internet service provider offences</i>	139
	(a) <i>Criminalisation and the duty of the ISP to act</i>	139
	(b) <i>Allowing others to cause harm through failures to prevent</i>	141
	(c) <i>Responsibility for allowing others to leak data</i>	143
	(d) <i>Allowing the loss of criminal evidence</i>	144
	(e) <i>The crime of fabricating and disseminating false information</i>	146
5.	<i>Obstacles to applying complicity liability to cybercrimes</i>	147
6.	<i>The limits of national jurisdiction</i>	151
7.	<i>Conclusion</i>	152
<b>7</b>	<b>Rethinking personal data protection in the criminal law of China</b>	<b>156</b>
	DONGYAN LAO AND DENNIS J. BAKER	
1.	<i>Introduction</i>	156
2.	<i>The legal status of personal data</i>	158
	(a) <i>Is privacy a public good?</i>	160
	(b) <i>The current law in China</i>	165
3.	<i>Difference from GDPR</i>	170
4.	<i>Related criminal offences in China</i>	173
5.	<i>Fair labelling and applying the right crime</i>	175
6.	<i>Conclusion</i>	177
<b>8</b>	<b>Using conspiracy and complicity for criminalising cyberfraud in China: lessons from the common law</b>	<b>180</b>
	LI LIFENG, TIANHONG ZHAO AND DENNIS J. BAKER	
1.	<i>Introduction</i>	180
2.	<i>Cyberfraud in China</i>	183
3.	<i>Remote harm offences vs. inchoate and pre-inchoate offences</i>	190
4.	<i>Complicity</i>	193

5. *Successive complicity in Japanese law* 197
6. *Conclusion* 199

## 9 **The threat from AI**

201

SADIE CREESE

1. *Introduction of risk* 201
2. *The nature of the threat* 202
3. *Definition and scope of AI* 203
  - (a) *Machine learning methods* 204
  - (b) *Learning from incomplete data* 206
  - (c) *Predicting behaviours and outcomes* 207
  - (d) *Incomprehension of decisions* 208
4. *Four apertures of cyberharm* 208
5. *AI as a weapon* 210
  - (a) *Targeting and control enhancements due to AI* 211
  - (b) *Attacker persistence, covertness and effects enhancement due to AI* 212
  - (c) *Attack (un)mitigatability enhancements due to AI* 213
  - (d) *Threat to individuals* 213
  - (e) *Threat to businesses or organisations* 214
  - (f) *Threat to nations or societies* 215
  - (g) *Global threats* 217
6. *AI as an environmental threat* 217
  - (a) *The question of dual-use* 218
  - (b) *Vulnerability introduction* 218
  - (c) *Growth of threat environment* 219
  - (d) *Polarisation of wealth* 220
  - (e) *Outliers and oversimplification* 220
  - (f) *Rule of law and responsibility for harm* 221
7. *Reflection* 221

## 10 **AI vs. IP: criminal liability for intellectual property offences of artificial intelligence entities**

222

GABRIEL HALLEVY

1. *Introduction: the legal problem* 222
2. *AI entities* 225
3. *Three models of criminal liability of artificial intelligence entities for commission of IP offences* 226
  - (a) *Perpetration-by-Another liability* 228
  - (b) *Natural-Probable-Consequence liability* 231

- (c) *Direct liability* 234
- (d) *Combination liability* 240
- 4. *Punishing AI* 241
- 5. *Conclusion* 244

11 **Don't panic: artificial intelligence and Criminal Law** 101 247

MARK DSOUZA

- 1. *Introduction* 247
  - (a) *The defendant* 248
- 2. *The actus reus* 249
  - (a) *Specific conduct offences* 249
  - (b) *Specific consequence offences* 251
  - (c) *State of affairs offences* 253
- 3. *The mens rea* 254
  - (a) *Preliminaries* 254
  - (b) *Intention* 255
  - (c) *Knowledge/belief* 256
  - (d) *Recklessness and negligence* 257
  - (e) *Consent* 259
  - (f) *Contemporaneity* 259
  - (g) *Rationale-based defences* 260
  - (h) *Application* 261
- 4. *Complicity liability* 262
- 5. *Inchoate offences* 263
- 6. *Conclusion* 264

*Index* 265