

Contents

<i>List of contributors</i>	x
1 Emerging technologies and the criminal law	1
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
2 Financial technology: opportunities and challenges to law and regulation	31
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
3 Between prevention and enforcement: the role of “disruption” in confronting cybercrime	49
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. *China's current practice concerning virtual property* 118
7. *The value of virtual property* 121
8. *Conclusion* 125

6 Criminalising cybercrime facilitation by omission and its remote harm form in China 126

LIANG GENLIN AND DENNIS J. BAKER

1. *Introduction* 126
2. *Cybercrime: extending the reach of the current law* 128
3. *Liability for indirect remote harm and direct pre-inchoate harm* 132
4. *Internet service provider offences* 139
 - (a) *Criminalisation and the duty of the ISP to act* 139
 - (b) *Allowing others to cause harm through failures to prevent* 141
 - (c) *Responsibility for allowing others to leak data* 143
 - (d) *Allowing the loss of criminal evidence* 144
 - (e) *The crime of fabricating and disseminating false information* 146
5. *Obstacles to applying complicity liability to cybercrimes* 147
6. *The limits of national jurisdiction* 151
7. *Conclusion* 152

7 Rethinking personal data protection in the criminal law of China 156

DONGYAN LAO AND DENNIS J. BAKER

1. *Introduction* 156
2. *The legal status of personal data* 158
 - (a) *Is privacy a public good?* 160
 - (b) *The current law in China* 165
3. *Difference from GDPR* 170
4. *Related criminal offences in China* 173
5. *Fair labelling and applying the right crime* 175
6. *Conclusion* 177

8 Using conspiracy and complicity for criminalising cyberfraud in China: lessons from the common law 180

LI LIFENG, TIANHONG ZHAO AND DENNIS J. BAKER

1. *Introduction* 180
2. *Cyberfraud in China* 183
3. *Remote harm offences vs. inchoate and pre-inchoate offences* 190
4. *Complicity* 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) <i>Direct liability</i>	234
(d) <i>Combination liability</i>	240
4. <i>Punishing AI</i>	241
5. <i>Conclusion</i>	244
11 Don't panic: artificial intelligence and Criminal Law	101
MARK DSOUZA	247
1. <i>Introduction</i>	247
(a) <i>The defendant</i>	248
2. <i>The actus reus</i>	249
(a) <i>Specific conduct offences</i>	249
(b) <i>Specific consequence offences</i>	251
(c) <i>State of affairs offences</i>	253
3. <i>The mens rea</i>	254
(a) <i>Preliminaries</i>	254
(b) <i>Intention</i>	255
(c) <i>Knowledge/belief</i>	256
(d) <i>Recklessness and negligence</i>	257
(e) <i>Consent</i>	259
(f) <i>Contemporaneity</i>	259
(g) <i>Rationale-based defences</i>	260
(h) <i>Application</i>	261
4. <i>Complicity liability</i>	262
5. <i>Inchoate offences</i>	263
6. <i>Conclusion</i>	264
<i>Index</i>	265