
Contents

Introduction	ix
Chapter 1. Security: Actors and Rights	1
1.1. Numerous actors	1
1.1.1. Nation-states	1
1.1.2. Multinationals	3
1.1.3. The GAFAM	9
1.2. Rights and security	10
1.2.1. The law of armed conflict	10
1.2.2. Environmental law	16
Chapter 2. Interceptions	25
2.1. International interceptions	25
2.1.1. Interceptions in the 20th century	25
2.1.2. Interceptions in the 21st century	27
2.2. Interceptions in France	37
2.2.1. The 1991 law	38
2.2.2. The law of March 9, 2004	41
2.2.3. The 2015 Intelligence Act	42
2.2.4. Reform of the code of criminal procedure	52
Chapter 3. Geolocation and Video Protection	59
3.1. International standards for both geolocation and video protection/video surveillance	59
3.1.1. Comparative legal issues in the era of geolocalization	59
3.1.2. Belgian legislation on geolocation	61
3.1.3. Video surveillance/video protection	63

3.2. France	67
3.2.1. The legislative and regulatory framework	67
3.2.2. The case law just before the LOPPSI 2 and the Jean-Marc Philippe establishments	69
3.2.3. The entry into force of the LOPPSI 2	74
3.2.4. Jurisprudence after LOPPSI 2	74
3.2.5. Video protection and terrorism	88
Chapter 4. Biometrics or “the Second Circle”	89
4.1. Biometrics and international law	90
4.1.1. The United States: a historical outline	90
4.1.2. Standardization	93
4.1.3. The European Union and biometrics	94
4.2. France	98
4.2.1. Visa control	98
4.2.2. Passports	99
4.2.3. The TES database	101
4.2.4. Setting up Alicem	117
4.3. Facial recognition at the heart of globalization	119
Chapter 5. Personal Data in the United States and Europe	121
5.1. The United States and the protection of personal data in the European Union: Directive 95/46	122
5.1.1. Sensitive data	122
5.1.2. The right of access	123
5.1.3. Security	123
5.1.4. The directive of December 15, 1997, followed by the directive of July 12, 2002 and supplemented by the directive of November 25, 2009	124
5.1.5. Geolocalization	125
5.1.6. Cookies	125
5.2. The GDPR	126
5.2.1. Consent	127
5.2.2. Metadata and the “Privacy” bill	134
5.3. Cloud computing	138
5.3.1. Definition	138
5.3.2. The Safe Harbor Principles agreement	139
5.3.3. Privacy Shields	140
5.3.4. Two models	140

Chapter 6. Cybersecurity and Privacy	145
6.1. Cybersecurity itself	146
6.1.1. Cybersecurity in the United States	146
6.1.2. Cybersecurity in China	147
6.1.3. Cybersecurity in Japan	147
6.1.4. Cybersecurity and the European Union	148
6.1.5. Cybersecurity in the United Kingdom	149
6.1.6. Cybersecurity in France	149
6.1.7. The dangers of cyber-attacks.	151
6.1.8. Two interesting cases.	154
6.2. Cybersecurity and cryptology.	158
6.2.1. Cryptology: the science of secrecy	158
6.2.2. Risks	161
6.3. PNR data	164
6.3.1. Element of definition	164
6.3.2. PNR data and nation-states.	166
6.4. Smart cities	179
6.4.1. The development of standardization and certification	181
6.4.2. Strategies and CSIRTs	182
Chapter 7. Security Instruments in Texts Relating to Terrorism	185
7.1. Security instruments.	185
7.1.1. The millimeter-wave scanner	185
7.1.2. The body camera	196
7.1.3. UAVs: a dual use – military and civilian	202
7.2. Standards in relation to terrorism.	208
7.2.1. The law of 2014.	209
7.2.2. The law strengthening internal security and the fight against terrorism	219
Chapter 8. Security and Democracy	225
8.1. Fake news	226
8.1.1. The definition	227
8.1.2. Obligations	227
8.2. Hate speech.	237
8.2.1. The report	237
8.2.2. The proposed new mechanism.	239

Conclusion	245
References	249
Index	251