

Inhaltsverzeichnis

Abkürzungsverzeichnis	15
Einleitung	19
Teil 1: Grundlagen	21
Kapitel 1: Wechselwirkung von Technik und Recht	21
I. Wirkung der Technik auf das Recht	21
II. Wirkung des Rechts auf die Technik	22
Kapitel 2: Technische Grundlagen	23
I. Das Internet im menschlichen Privatleben	23
II. »Industrie 4.0«	24
III. Internet der Dinge	25
1. WLAN und 3G/4G/5G	26
2. RFID	27
3. Big Data und Cloud Computing	28
4. Robotik	31
Kapitel 3: Datensicherheit und Datenschutz als rechtliche Herausforderung	31
I. Datensicherheit und Datenschutz als rechtliche Herausforderung in der »Industrie 4.0«	31
II. Leitfaden für »Made in China 2025«	33
Teil 2: Datensicherheit in der »Industrie 4.0«	35
Kapitel 1: Cybercrime	36
I. Definition des Cybercrime	36
II. Ursachen des Cybercrime	36
1. Aus der Technik resultierende Ursache	37
2. Aus dem Gesetz resultierende Ursache	37
3. Aus kriminellen Gewinnen und Kosten von Strafe resultierende Ursache	38
4. Aus der Finanzkrise resultierende Ursache	39
III. Besonderheiten des Cybercrime	40
1. Distanz	40

2. Anonymität	40
3. Umfang	41
IV. Zusammenfassung	41
Kapitel 2: Hacker	42
I. Definition eines Hackers	42
II. Besonderheiten der Hackerkriminalität	43
1. Methodische Vielfältigkeit	43
2. Schnelle Auffindbarkeit von Informationen zur Tatbegehung	43
3. Tendenziell jüngere Täter	43
4. Die Beliebigkeit des Angriffsorts	44
III. Häufig angewendete Techniken des Hackers	44
1. Trojanisches Pferd	44
2. Wurm	44
3. Phishing	45
4. Keylogger	45
5. Backdoor	45
6. Exploit	46
IV. Bedrohungen für »Industrie 4.0«	46
1. Industriespionage	46
2. Industriesabotage	47
V. Zusammenfassung	47
Kapitel 3: Regelungen in Europa, Deutschland und China	48
I. Rechtsakte des Europarats, der EU und in Deutschland	48
1. Auf Ebene des Europarats und der EU	48
a) Die CyCC	48
aa) Überblick der CyCC	49
bb) Wesentliche Regelungen zur Datensicherheit	50
(1) Art. 2 CyCC	50
(2) Art. 3 CyCC	50
(3) Art. 4 CyCC	50
(4) Art. 5 CyCC	51
(5) Art. 6 CyCC	51
(6) Art. 7 CyCC	52
(7) Art. 8 CyCC	52
(8) Art. 12 CyCC	52
b) RL 2013/40/EU	53
aa) Die Zielsetzung	53
bb) Aufbau der RL 2013/40/EU	53

cc) Wesentliche Regelungen zur Datensicherheit	53
(1) Art. 3 RL 2013/40/EU	53
(2) Art. 4 RL 2013/40/EU	54
(3) Art. 5 RL 2013/40/EU	54
(4) Art. 6 RL 2013/40/EU	55
(5) Art. 7 RL 2013/40/EU	55
(6) Art. 10 RL 2013/40/EU	55
2. Die Situation in Deutschland	56
a) § 202a StGB	56
b) § 202b StGB	57
c) § 202c StGB	57
d) § 202d StGB	58
e) § 263a StGB	58
f) § 303a StGB	59
g) § 303b StGB	59
II. In China	60
1. § 285 chStGB	61
2. § 286 chStGB	63
3. § 287 chStGB	64
4. § 287a Abs. 1 Nr. 1 chStGB	65
5. § 287b chStGB	66
III. Vergleich der jeweiligen nationalen Regelungen	67
1. §§ 202a, 202b StGB und § 285 Abs. 2 chStGB	67
2. § 202c Abs. 1 Nr. 2 StGB und § 285 Abs. 3 chStGB	68
3. § 303a Abs. 1 StGB und § 286 Abs. 2 chStGB	68
4. Zwischenfazit	69
IV. Probleme der nationalen Regelungen	69
1. In Deutschland	69
a) Fehlt das Bandenausspähen von Daten in § 202a StGB?	69
b) Fehlende Versuchsstrafbarkeit in § 202a?	70
c) Grauzone in § 202c StGB?	70
2. In China	71
a) Ungeeignete Zuordnung des Objekts der Straftat?	71
b) Paradoxon in § 285 chStGB?	72
c) Regelungslücke in § 287 chStGB?	73
3. Vergleichendes Fazit	73
V. Reformempfehlung zu nationalen Regelungen	74
1. In Deutschland	74
a) § 202a StGB	74
b) § 202c StGB	74

2. In China	75
a) Geeignete Zuordnung des Objekts der Straftat	75
b) § 285 chStGB	75
c) § 287 chStGB	76
VI. Zusammenfassung	76
Kapitel 4: Cybersicherheitsstrategie, Umsetzung und Ausblick	76
I. Cybersicherheitsstrategie und Umsetzung	76
1. Cybersicherheitsstrategie auf nationaler Ebene	76
a) Umsetzung in Deutschland	78
b) Umsetzung in China	79
2. Auf transnationaler Ebene: in der EU	83
a) Die NIS-Richtlinie	84
b) Die Cybersecurity-Verordnung	86
3. Fazit	87
II. Ausblick	88
1. Ultima-Ratio	88
2. China: Schaffung eines Datenstrafrechts?	88
3. Deutschland: Schaffung eines Technikstrafrechts?	89
4. Enge Zusammenarbeit	90
Teil 3: Datenschutz in der »Industrie 4.0«	92
Kapitel 1: Rechtslage in der EU, Deutschland und China	93
I. In der EU und Deutschland	93
1. In der EU	93
a) Grundrechte	94
aa) Art. 8 EMRK	94
bb) Art. 8 EU-GRCh	94
b) DSRL	95
c) Wesentliche Änderungen in der DS-GVO	97
2. In Deutschland	101
a) Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG	101
b) BDSG	102
aa) Einwirkung der Technik	102
bb) Orientierung an dem EU-Recht	103
cc) Sicherstellung interner und externer Kontrolle	104
c) Zusammenfassung	105
II. In China	106
1. Beschluss über den verstärkten Schutz der personenbezogenen elektronischen Daten	107

2. § 253a chStGB	108
3. Das Cybersicherheitsgesetz (chCSG)	109
4. § 111 des Allgemeinen Teils des Zivilgesetzbuches	111
III. Vergleichendes Zwischenfazit	112
Kapitel 2: Cloud Computing in Deutschland und Big Data in China	113
I. Cloud Computing in Deutschland	113
1. Probleme bei der Anwendung des BDSG a.F.	114
a) § 11 Abs. 2 S. 2 BDSG a.F.	114
b) § 11 Abs. 2 S. 4 BDSG a.F.	115
c) § 11 Abs. 3 S. 1 BDSG a.F.	117
2. »Safe-Harbor«-Abkommen	117
3. Veränderungen durch die neue Rechtslage	119
a) Vor dem Inkrafttreten der DS-GVO	119
aa) »Safe-Harbor«-Urteil des EuGHs	119
bb) EU-US-Privacy-Shield	121
b) Nach dem Inkrafttreten der DS-GVO und BDSG n.F.	123
aa) Cloud Computing	123
bb) Einsatz der neuen Techniken	124
II. Big Data in China: das Sozialkreditsystem	126
1. Begriffserklärung und Einführung	128
2. Umsetzungsschwerpunkte des Sozialkreditsystems	130
a) Die Zuverlässigkeit in Regierungsangelegenheiten	130
b) Die Zuverlässigkeit in Handelsangelegenheiten	131
c) Die Zuverlässigkeit innerhalb der Gesellschaft	132
d) Öffentliches Vertrauen in die Justiz	133
3. Entwicklungstendenz des Sozialkreditsystems	134
a) Das bestehende kommerzielle Kreditnachweissystem in China	134
b) Pilotprojekte am Beispiel von Rongcheng	136
c) Das öffentliche Vertrauenswürdigkeitsnachweissystem	138
d) Mechanismus zur Anreizsetzung und Bußen	139
4. Eine neutrale Bewertung	141
III. Fazit	145
Teil 4: Abschließende Überlegung	149
Kapitel 1: Technikrecht, Gesetzgebung und ihre Qualitätsanforderung	149
I. Technikrecht	149
1. Verbindung von Technik und Recht	150

2. Konflikte von Technik und Recht	150
II. Gesetzgebung und ihre Qualitätsanforderung	151
Kapitel 2: Eine interdisziplinäre Umsetzung	152
I. Schlüsselbegriffe	152
1. Das gesetzgeberische Dilemma	152
2. Das technische Risiko	154
3. Die Gesetzesfolgenabschätzung (GFA)	154
II. Die Möglichkeiten	155
1. Einführung der Abschätzung des technischen Risikos in die pGFA	156
2. Kooperation zwischen Staat und Unternehmen	159
3. Selbstregulierung	160
a) Verhaltensregeln in der Technikbranche	160
b) Verbindliche unternehmerische Compliance-Regeln	161
Zusammenfassende Thesen	164
Literaturverzeichnis	167