

Inhaltsübersicht

Inhaltsverzeichnis	13
Abbildungsverzeichnis	21
Tabellenverzeichnis	23
Abkürzungsverzeichnis	25
1. Kapitel: Einleitung	29
A. Motivation	29
I. Digitale Entwicklung der Gesellschaft	30
II. Rechtliche Ausgangslage	36
III. Adressaten und Störungsszenario	41
IV. Übergreifende Bedeutung des Szenarios	44
V. Fazit	49
B. Untersuchungsgegenstand	50
C. Gang der Untersuchung	53
I. Funktionsweise und Manipulation von Personalisierungsalgorithmen	53
II. Resilienz in Art. 32 DSGVO	54
III. Übertragbarkeit in § 30 RegE BSIG	55
IV. Zusammenfassung und Gestaltungsempfehlung	56
2. Kapitel: Funktion und Manipulation der algorithmenbasierten Personalisierung	59
A. Ermittlung von Personenwissen nach dem DIW-Modell	59
I. Daten	60
II. (Persönliche) Information	61
III. Wissen	64
IV. Entscheidung und Verhaltenssteuerung	65
V. Zusammenfassung	67

Inhaltsübersicht

B. Technische Grundlagen	67
I. Automatisierte Verarbeitung	67
II. Autonome Verarbeitung durch maschinelles Lernen	68
III. Verarbeitung in personalisierten Dienstangeboten	69
C. Manipulation der Informationen	73
I. Allgemeine Darstellung	73
II. Singuläre Informationsmanipulation	74
III. Plurale Informationsmanipulation	77
IV. Fazit und Ansatz für das Erfordernis der Resilienz	78
 3. Kapitel: Die Resilienz in der DSGVO	 81
A. Anwendungsbereich von Art. 32 DSGVO	81
I. Normenübersicht	82
II. Verhältnis der Art. 25 Abs. 1, 32 DSGVO	87
B. Schutzgüter	101
I. Terminologie und normative Bedeutung	102
II. Die Schutzgüter der DSGVO	105
III. Bestimmung in Art. 32 DSGVO	109
C. Auslegung der Resilienz	110
I. Vorbegriffe	110
II. Auslegung nach dem Wortlaut	121
III. Systematische Auslegung	159
IV. Historische Auslegung	205
V. Teleologische Auslegung	208
VI. Ergebnis	212
D. Demonstration anhand personalisierter Dienste	215
I. Ungewissheit	215
II. Resilienzmaßnahmen	216
III. Abstrakte Angemessenheit	219
IV. Fazit	220

4. Kapitel: Übertragung in das IT-Sicherheitsrecht	221
A. Bestimmung der Schutzgüter	222
I. Historische Entwicklung des BSIG	222
II. Schutzgüter kritischer Anlagen	230
III. Schutzgüter digitaler Dienste	254
B. Systematische Beschreibung der gesetzlichen IT-Sicherheitsvorgaben	262
I. IT-Sicherheit und Schutzziele	263
II. Systeme, Dienste, Daten und Informationen	272
III. Risiko und Angemessenheit	289
IV. Zusammenfassung	296
C. Unterschiede zur DSGVO und Folgen für die Resilienz	297
I. IT-Sicherheit vs. Datensicherheit	298
II. Bedeutung der Schutzziele und des Dienstes	299
III. Verständnis des Systembegriffs	303
IV. Risiko	307
V. Zusammenfassung	311
D. Übertragung der Resilienz in den RegE BSIG	313
I. Bestehende, funktionale Resilienz-Elemente	313
II. Teleologische Gründe	316
III. Gesamtergebnis	317
E. Demonstration anhand des Szenarios	318
I. Ungewissheit	318
II. Resilienzmaßnahmen	319
III. Abstrakte Angemessenheit	321
5. Kapitel: Zusammenfassung und Implementierungsvorschlag	323
A. Zusammenfassung der Ergebnisse	323
I. Resilienz in der DSGVO	324
II. Übertragbarkeit in den RegE BSIG	328
B. Implementierungsvorschlag	333
C. Ausblick	335
Literaturverzeichnis	339

Inhaltsverzeichnis

Abbildungsverzeichnis	21
Tabellenverzeichnis	23
Abkürzungsverzeichnis	25
1. Kapitel: Einleitung	29
A. Motivation	29
I. Digitale Entwicklung der Gesellschaft	30
1. Die Welt der personenbezogenen Daten	30
2. Die kritischen Dienste der Gesellschaft	32
3. Zweifache Bedeutung digitaler Dienste	33
4. Technische Innovation in Ungewissheit	34
5. Fazit	35
II. Rechtliche Ausgangslage	36
1. Datensicherheitsrecht und IT-Sicherheitsrecht	37
2. Unterschiede beider Rechtsgebiete	38
3. Überschneidungsbereich	39
III. Adressaten und Störungsszenario	41
IV. Übergreifende Bedeutung des Szenarios	44
1. Energierecht	45
2. Gesundheitsversorgung	46
3. Dienste in digitalen Ökosystemen	46
4. Telekommunikationsrecht	48
V. Fazit	49
B. Untersuchungsgegenstand	50
C. Gang der Untersuchung	53
I. Funktionsweise und Manipulation von Personalisierungsalgorithmen	53
II. Resilienz in Art. 32 DSGVO	54
III. Übertragbarkeit in § 30 RegE BSIG	55
IV. Zusammenfassung und Gestaltungsempfehlung	56

2. Kapitel: Funktion und Manipulation der algorithmenbasierten Personalisierung	59
A. Ermittlung von Personenwissen nach dem DIW-Modell	59
I. Daten	60
II. (Persönliche) Information	61
III. Wissen	64
IV. Entscheidung und Verhaltenssteuerung	65
V. Zusammenfassung	67
B. Technische Grundlagen	67
I. Automatisierte Verarbeitung	67
II. Autonome Verarbeitung durch maschinelles Lernen	68
III. Verarbeitung in personalisierten Dienstangeboten	69
C. Manipulation der Informationen	73
I. Allgemeine Darstellung	73
II. Singuläre Informationsmanipulation	74
1. Wirkung nach dem DIW-Modell	74
2. Technische Ausgestaltung	75
III. Plurale Informationsmanipulation	77
1. Wirkung nach dem Informationsmodell	77
2. Technische Gestaltung	77
IV. Fazit und Ansatz für das Erfordernis der Resilienz	78
3. Kapitel: Die Resilienz in der DSGVO	81
A. Anwendungsbereich von Art. 32 DSGVO	81
I. Normenübersicht	82
1. Dekomposition der einzelnen Normen	83
a. Art. 24 DSGVO	83
b. Art. 25 DSGVO	84
c. Art 32 Abs. 1 DSGVO	85
2. Tabellarische Übersicht	86
II. Verhältnis der Art. 25 Abs. 1, 32 DSGVO	87
1. Inhaltliche Unterschiede der Normen	88
a. Perspektiven	88
b. Umsetzung der Verarbeitung durch Systeme und Dienste	89
c. Rollenansprache	89

d. Voluntative Schutzrichtungen	90
i. Vertraulichkeit	90
ii. Verfügbarkeit/Integrität	92
2. Übergreifende Zuordnung in Erwägungsgrund 83	94
3. Normaufträge und Fazit	95
a. Keine eindeutige Differenzierung nach voluntativem Element und Quelle	95
b. Art. 25 Abs. 1 DSGVO	97
c. Art. 32 DSGVO	98
B. Schutzgüter	101
I. Terminologie und normative Bedeutung	102
II. Die Schutzgüter der DSGVO	105
1. Sachliche Bestimmung der „Grundrechte und Grundfreiheiten“	106
2. Kreis der geschützten „natürliche Personen“	108
III. Bestimmung in Art. 32 DSGVO	109
C. Auslegung der Resilienz	110
I. Vorbegriffe	110
1. Datensicherheit / Sicherheit der Verarbeitung	111
2. Maßnahmen	112
3. Systeme	114
a. Erfassung personenbezogener Daten	115
b. Soziotechnisches Systemverständnis	117
4. Dienste	119
a. Ökonomische Betrachtung	119
b. Rechtliche Betrachtung	119
c. Technische Betrachtung	120
II. Auslegung nach dem Wortlaut	121
1. „Belastbarkeit“ oder Resilienz	121
2. Allgemeine Wortbedeutung und domänenspezifische Verwendung	124
a. Psychologie	126
b. Ökologie, Umwelt- und Klimaforschung	129
c. Technische Resilienz	132
i. Material- und Ingenieurwissenschaft	132
ii. Informationstechnik	133
(1) Verlässlichkeit	133

Inhaltsverzeichnis

(2) IT-Sicherheit	137
(3) Weitere Teilbereiche und Fazit	139
iii. Kritische Infrastrukturen	141
d. Gesellschaftliche Resilienz / Katastrophenschutz	142
e. IT-Sicherheitsrecht	145
i. Einführung	145
ii. RegE BSIG und NIS2-RL	147
iii. RefE KRITIS-DachG	148
iv. Digital Operational Resilience Act (DORA)	149
v. Cybersecurity-Act (CSA)	149
vi. Strategie zum Schutz kritischer Infrastrukturen (Schweiz)	150
vii. Strategic Plan 2023-2025 (USA)	151
viii. Fazit	152
3. Synthese	153
4. Fazit	158
III. Systematische Auslegung	159
1. Risiko	159
a. Einleitung	159
b. Begriffsdefinition	160
c. Methodik	163
i. Einleitung	163
ii. Identifizieren von Datenschutzrisiken	165
iii. Analysieren der Datenschutzrisiken	166
iv. Bewerten von Datenschutzrisiken	166
v. (Angemessene) Behandlung von Datenschutzrisiken	167
vi. Iteration	168
d. Gegenüberstellung der Resilienz	169
i. Resilienz als Umgang mit Ungewissheit	169
(1) Ungewissheit als (Un)bekanntheit und (Nicht)-Wissen	170
(2) Was ist unbekannt und worüber besteht kein Wissen?	176
(3) Resilienz als spezifische Antwort	178
(4) Folgen für die Risikodefinition	179

ii. Methodische Einordnung	180
(1) Adressierung unterschiedlicher Formen der Ungewissheit	181
(2) Angemessenheit von Resilienzmaßnahmen	182
(3) Resilienzlernen und Risikomanagement-Iteration	183
(4) Zusammenfassung der Methodik	185
iii. Ergebnis und Folgen für den Resilienzbegriff	185
2. Schutzziele nach Art. 32 Abs. 1 lit b) DSGVO	187
a. Historische Entwicklung	187
b. Einführung im deutschen und europäischen Datenschutzrecht	189
c. Vorkommen und Auslegung in der DSGVO	190
i. Verfügbarkeit	192
ii. Integrität	193
iii. Vertraulichkeit	195
d. Zusammenfassung	196
e. Einordnung der Resilienz	198
3. Systeme und Dienste	201
4. Fazit	203
IV. Historische Auslegung	205
1. Vorgängervorschrift Art. 17 DS-RL	206
2. Entwicklung der DSGVO	206
3. Fazit	207
V. Teleologische Auslegung	208
1. Ungewissheit in komplexen, offenen Systemen	209
2. KI als ungewisse Komponente	210
3. Ermöglichung von Resilienz durch Komplexität und Autonomie	211
4. Fazit	212
VI. Ergebnis	212
D. Demonstration anhand personalisierter Dienste	215
I. Ungewissheit	215
II. Resilienzmaßnahmen	216
1. Ereigniserkennung	216
2. Anpassungsfähigkeit	217
3. Erholung	218
III. Abstrakte Angemessenheit	219

IV. Fazit	220
4. Kapitel: Übertragung in das IT-Sicherheitsrecht	221
A. Bestimmung der Schutzgüter	222
I. Historische Entwicklung des BSIG	222
1. Novelle 2015 – Schutz kritischer Infrastrukturen	224
2. Novelle 2017 – Schutz digitaler Dienste	225
3. Novelle 2021 – Unternehmen im besonderen öffentlichen Interesse	227
4. Novelle 2024 – NIS2-RL	228
5. Fazit	230
II. Schutzgüter kritischer Anlagen	230
1. Begriff der Daseinsvorsorge	230
a. Verfassungsrechtliche Pflichten zur Leistungsbereitstellung	235
i. Leistungsansprüche aus Grundrechten	235
ii. Grundrechtliche Schutzpflichten	237
iii. Gemeinwohlziele	238
iv. Sozialstaatsprinzip	242
v. Zwischenfazit	243
b. Originäre Wahrnehmung durch den Staat	244
c. Heutige Gewährleistungsverantwortung	247
d. Fazit	249
2. Öffentliche Sicherheit	250
3. Erhalt der Umwelt	251
4. Zusammenfassung	252
III. Schutzgüter digitaler Dienste	254
1. Individualrechtsgüter	256
a. Ausfälle des Dienstes	256
b. Manipulationen des Dienstes	256
c. Eingeschränkter Schutz von Individualrechtsgütern im IT-Sicherheitsrecht	257
2. Gemeinwohlziele und Sozialstaatsprinzip	259
3. Öffentliche Sicherheit	261
4. Fazit	261

B. Systematische Beschreibung der gesetzlichen IT-Sicherheitsvorgaben	262
I. IT-Sicherheit und Schutzziele	263
1. IT-Sicherheit	263
2. Verfügbarkeit, Vertraulichkeit und Integrität	269
3. Authentizität	271
II. Systeme, Dienste, Daten und Informationen	272
1. Systeme	272
a. Systeme, Komponenten und Prozesse	273
b. Netz- und Informationssysteme	274
i. Netzsystem	275
ii. Informationssystem	276
iii. Digitale Daten	276
c. Zusammenführung und soziotechnisches Verständnis	277
2. Dienste	279
a. Dienstbegriffe nach der NIS2-RL	279
i. Der ökonomische Dienst: Art. 21 Abs. 1 NIS2-RL	280
ii. Der IT-Dienst: Art. 6 Nr. 2 NIS2-RL	281
iii. Der IKT-Dienst und der digitale Dienst	282
b. Dienstverständnisse im RegE BSIG	283
i. Verständnis des nationalen Gesetzgebers	283
ii. Folgen der unionsrechtswidrigen IT-Sicherheitsdefinition	285
c. Fazit	286
3. (Digitale) Daten und Informationen	288
III. Risiko und Angemessenheit	289
1. Risiko	289
a. Beschränkung auf den „vernünftigen Aufwand“	289
b. Bezugspunkt des Risikos	290
2. Methodik, einschließlich Angemessenheit	293
3. Fazit	295
IV. Zusammenfassung	296
C. Unterschiede zur DSGVO und Folgen für die Resilienz	297
I. IT-Sicherheit vs. Datensicherheit	298
II. Bedeutung der Schutzziele und des Dienstes	299
1. Schutzziele	299
2. Dienst	300
a. Im Datensicherheitsrecht	301

Inhaltsverzeichnis

b. Im IT-Sicherheitsrecht	301
c. Fazit und Folgen für die Resilienz	302
III. Verständnis des Systembegriffs	303
1. Maßnahmenträger oder Schutzobjekt	303
2. Systembestandteile	304
3. Fazit und Folgen für die Resilienz	305
IV. Risiko	307
1. Definitionen des Risikos	307
a. Vergleich	307
b. Folgen für die Resilienz	310
2. Methodik, einschließlich Angemessenheit	311
V. Zusammenfassung	311
D. Übertragung der Resilienz in den RegE BSIG	313
I. Bestehende, funktionale Resilienz-Elemente	313
II. Teleologische Gründe	316
III. Gesamtergebnis	317
E. Demonstration anhand des Szenarios	318
I. Ungewissheit	318
II. Resilienzmaßnahmen	319
1. Ereigniserkennung	319
2. Anpassungsfähigkeit	320
3. Erholung	321
III. Abstrakte Angemessenheit	321
5. Kapitel: Zusammenfassung und Implementierungsvorschlag	323
A. Zusammenfassung der Ergebnisse	323
I. Resilienz in der DSGVO	324
II. Übertragbarkeit in den RegE BSIG	328
B. Implementierungsvorschlag	333
C. Ausblick	335
Literaturverzeichnis	339