

Inhaltsverzeichnis

A. Algorithmen als DNA der digitalen Zukunft	1
I. Implikationen für das gesellschaftliche Miteinander und die Erfahrbarkeit der individuellen Privatsphäre	4
1. Charakteristika und Leistungspotenziale von Algorithmen	4
2. Algorithmen, Dein Freund und Helfer? – ein Blick auf die gesellschaftliche Risikoperzeption	6
3. Politischer Steuerungsauftrag: Algokratie versus Nomokratie?	9
4. Stunde der Algorithmen – Algorithmen als kognitives Schlüsselement der Mensch-Maschine-Interaktion	12
II. Gesellschaftliche und wirtschaftliche Chancen	14
1. Privater Sektor	14
2. Öffentlicher Sektor	16
III. Technische Grundlagen und Grundbegriffe	17
1. Algorithmen als Herzstück von Softwareanwendungen	17
2. Der Einfluss Künstlicher Intelligenz: lernende Algorithmen und lernfähige Softwareanwendungen	19
a) Anwendungsfelder	22
b) Erscheinungsformen lernender Algorithmen	23
c) Macht der Algorithmen – ein Ausblick	25
B. Regulierungsbedarf	27
I. Risikopotenziale einer Welt algorithmischer Entscheidungen.	27
1. Digitale Alchemie: Intransparenz der Entscheidungen lernfähiger Softwareanwendungen als doppelte Blackbox	28
a) Auswirkungen auf die Grundrechte und den Wettbewerb.	29
aa) Persönlichkeitsentfaltung.	29
bb) Implikationen für die Wettbewerbsentwicklung	31
b) Ursachen der Intransparenz	33
aa) Algorithmen als Amts- bzw. Geschäfts- und Betriebsgeheimnis	33

(1) Private als Verwender algorithmenbasierter Entscheidungssysteme.	33
(a) Urheberrechtlicher Schutz?	33
(b) Patentrechtlicher Schutz?	35
(c) Schutz als Geschäfts- und Betriebsgeheimnis ...	37
(α) Schutzinhalt	37
(β) Grundrechtliche Absicherung	38
(γ) Legislative Entwicklungen.	39
(2) Der Staat als Verwender algorithmenbasierter Entscheidungssysteme.	40
bb) Undurchdringbarkeit des maschinellen Lernens als technische und regulatorische Herausforderung	41
(1) Technische Besonderheiten	42
(2) Erkenntnismethoden: Blackbox- und Whitebox-Tests	44
2. Diskriminierungspotenzial: „machine bias“ und Voreingenommenheit des Codes.	47
a) Algorithmen als Ausdruck der Werteinstellungen ihrer Schöpfer.	48
b) Pfadabhängigkeiten und Fehler des Trainingsmaterials	49
aa) Auswahl diskriminierungsfreier Trainingsdatenmaterials.	50
bb) Diskriminierungsanfällige Wertentscheidungen	52
(1) Referenzfall Preisdiskriminierung.	52
(2) Referenzfall Bewerberauswahl	53
(3) Referenzfall COMPAS: Vorbereitung der Entscheidung über die Strafaussetzung zur Bewährung.	55
c) Technikimmanente Erkenntnisgrenzen	58
aa) Soziale und emotionale Intelligenz; common sense	59
bb) Sensomotorische Intelligenz	60
cc) Anfälligkeit für <i>Cum-hoc-ergo-propter-hoc</i> -Fehlschlüsse.	60
dd) Kreativität	61
ee) Ausblick.	61
3. Monopolisierung von Wissen und Marktmacht	62
a) Markt-Macht-Spirale	62
b) Implikationen für die gesellschaftliche Ordnung und die öffentliche Meinungsbildung.	64
II. Rechtliche Schutzimplikationen strukturtypischer Risiken beim Einsatz algorithmenbasierter Verfahren.	66
1. Verfassungsrechtliches Transparenzgebot?	68
a) Transparenz staatlichen Handelns	68
b) Transparenz des Handelns Privater	72

2. Normative Vorgaben für den Schutz vor Diskriminierung	73
a) Verfassungsrechtliche und unionsrechtliche Vorgaben	75
b) Einfachgesetzlicher Rahmen de lege lata	76
aa) Zivilrechtliche Massengeschäfte unter Privaten – AGG	77
(1) Anwendungsbereich	77
(2) Abgrenzung zum Datenschutzrecht – eine komplexe Beziehung	77
(a) Gemeinsamkeiten des AGG und des Datenschutzrechts unter dem BDSG a. F.	78
(b) Rechtslage unter der DSGVO	80
bb) Öffentliche Stellen	82
(1) Analoge Welt	82
(a) Praxisphänomen Racial Profiling	82
(b) Verfassungsrechtliche Würdigung	84
(2) Digitale Welt; Diskriminierungsschutz bei algorithmengestützter staatlicher Aufgabenerfüllung	86
3. Schutz der Persönlichkeit, insbesondere der informationellen Selbstbestimmung und der Vertraulichkeit sowie Integrität informationstechnischer Systeme	91
a) Lebensweltlicher Wandel der Erfahrbarkeit von Privatheit in einer digitalen Welt	91
b) Das allgemeine Persönlichkeitsrecht als verfassungsrechtliche Schutzkoordinate der Privatheit	93
c) Das Recht auf informationelle Selbstbestimmung	93
d) Schutzgehalt des sog. IT-Grundrechts	94
e) Geltungsbereich, insbesondere gegenüber Privaten	96
aa) Konzept der kontextspezifischen Vertraulichkeits- und Integritätserwartung als Schutzphilosophie	97
bb) Rechtspolitische Schlussfolgerungen	98
4. Schutz der Informations- und Meinungsbildungsfreiheit	99
a) Erscheinungsformen des Wandels der Medienordnung in einer digitalen Welt	99
b) Regulierungsherausforderungen und Schlussfolgerungen	102
5. Schutzpflicht zur Gewährleistung freien Wettbewerbs	103
a) Tektonische Verschiebungen im Zeitalter der Digitalisierung	104
aa) Plattformen als Priorisierungsmaschinen einer Aufmerksamkeitsökonomie	104
bb) Netzwerkeffekte	105
b) Regulatorische Schlussfolgerungen	106
III. Zwischenfazit	109

C. Algorithmen und lernfähige Softwareanwendungen als Risikotechnologie – Regulierungsstrategien klassischer Risikoverwaltung als Blaupause	113
I. Das Recht der Risikoregulierung als Vergleichsfolie.	114
II. Nanotechnologie: regulatorisch vorsorgen und Nichtwissen bewältigen	117
1. Charakteristika der Nanotechnologie	117
2. Vergleich zu (lernenden) Algorithmen	119
3. Das Vorsorgeprinzip als regulatorische Antwort des Risikotechnologierechts	120
4. Abgestufte Risikoanalyse	121
5. Regulatorische Ansätze	123
6. Schlussfolgerungen	124
III. Humangenetik: Qualitätssicherung und Vorsorgestimulierung	126
1. Risikoregulierung in der Gendiagnostik	127
2. Implikationen für die Algorithmenregulierung	129
IV. Arzneimittelrecht: beschränktes Wissen über biologische Wirkungszusammenhänge und Ergebnissicherheit	131
1. Grundsätzliche Zulassungspflicht, fortlaufende Risikoregulierung und Informationspflichten	131
2. Schlussfolgerungen für die Regulierung der Risiken algorithmenbasierter Systeme	135
V. Umweltrecht als Erprobungsraum für Instrumente regulierter Selbstregulierung	137
1. Grundzüge des Konzepts einer regulierten Selbstregulierung	138
2. Anwendungsfelder de lege lata	140
a) EMAS-Verordnung	140
b) „Blauer Engel“	140
3. Implikationen für die Algorithmenregulierung	141
VI. Hochfrequenz- und algorithmischer Handel mit Finanzinstrumenten: risikoverwaltungsrechtliche Ansätze der MiFiD II, MAR, MAD sowie des KWG, WpHG und BörsG	142
1. Grundzüge des algorithmischen Handels und Hochfrequenzhandels	143
2. Vorteile und Risiken	144
3. Regulierung und Aufsicht	146
a) Anzeigepflicht	147
b) Erlaubnispflicht für Hochfrequenzhändler	147
c) Kennzeichnungspflicht	148
d) Organisatorische Anforderungen für algorithmische Händler	148
aa) Angemessene System- und Risikokontrollen	149
bb) Belastbarkeit der Handelssysteme	150
e) Aufzeichnungs- und Aufbewahrungspflicht	151
f) Anforderungen an Handelsplätze	152

g) Auskunftspflicht	153
h) Marktmissbrauchsverbot	154
4. Analogiefähigkeit des Regelungsmodells	154
D. Bausteine einer Regulierung algorithmenbasierter Systeme auf der Zeitachse	157
I. Übergreifende regulatorische Ansatzpunkte	158
1. Wandel des datenschutzrechtlichen Regulierungsansatzes: von der Verengung auf den Personenbezug zur Risikoregulierung	159
a) Fokusverschiebung vom „Ob“ zum „Wie“	159
b) Ausformung des Risikogedankens in der DSGVO und im BDSG	161
2. Kollektive Ansätze des Datenschutzes	162
a) Rechtlicher Autonomieschutz der Einwilligung	164
b) Verfahrensrechtlicher Schutz	166
3. Notwendigkeit einer internationalen Regulierungsstrategie	167
II. Präventive Risikoregulierung	168
1. Schutz vor einer „Computer says no“-Dystopie: Art. 22 DSGVO als Antwort des europäischen Gesetzgebers auf voll automatisierte Verfahren	169
a) Grundsatz	170
b) Grenzen des Regelungsanspruchs	170
aa) Ausnahmen	171
bb) Beschränkung auf voll automatisierte Verfahren	172
cc) (Un-)Vereinbarkeit des § 31 BDSG mit dem Unionsrecht	174
2. Transparenzanforderungen an den Einsatz algorithmenbasierter Verfahren	176
a) Ex-ante-Information	177
aa) Kennzeichnungspflicht („Ob“)	177
(1) De lege lata	177
(2) De lege ferenda	178
bb) Erläuterungspflicht („Wie“)	181
(1) De lege lata	182
(a) Historischer Hintergrund	182
(b) Semantik und Sachlogik des Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO	183
(2) De lege ferenda	185
(a) Ausweitung der Informationspflicht „über die involvierte Logik“ auf alle grundrechtssensitiven Algorithmenanwendungen, insbesondere maschinelle Lernverfahren	185

(b)	Informationspflicht über getroffene bzw. zu treffende Schutzmaßnahmen (Art. 22 Abs. 3 DSGVO)	187
(c)	Visuelle Nachvollziehbarkeit der Informationen – faktische Wirkgrenzen informationsrechtlicher Pflichten	188
b)	Ex-post-Information	189
aa)	Begründungspflicht?	189
(1)	Rechtslage de lege lata	190
(2)	Sinnhaftigkeit und technische Grenzen – die Begründung als Schranke der Privatautonomie	192
(a)	Privatautonomie als verfassungsrechtlich geschütztes Gut	192
(b)	Technische Herausforderungen	193
(3)	Reichweite einer Begründungspflicht	195
(a)	Legitimationsfelder („Ob“)	195
(b)	Tiefe der Begründung („Wie“)	197
(c)	Rechte Dritter	197
bb)	Recht auf Einblick in die Datengrundlage und Profiling-Ergebnisse	197
(1)	Art. 15 Abs. 1, Abs. 3 S. 1 DSGVO	198
(2)	Recht auf Auskunft über Profiling-Ergebnisse?	198
(a)	Profiling-Ergebnisse als personenbezogene Daten	198
(b)	Anspruchsumfang des Art. 15 Abs. 1 DSGVO ...	199
(c)	Recht auf Berichtigung angreifbarer Profiling-Wertungen aus Art. 16 S. 1 DSGVO? ...	201
(d)	Recht auf Erläuterung von Profiling-Ergebnissen als Schutzmaßnahme i. S. d. Art. 22 Abs. 3 DSGVO?	202
(e)	Offenlegung der Profiling-Ergebnisse de lege ferenda?	202
(3)	Recht auf angemessene Schlussfolgerungen?	205
c)	Veröffentlichung einer Risiko-/Folgenabschätzung und angewandeter Maßstäbe	207
aa)	Rechtslage de lege lata	208
bb)	Regulierungsvorschläge	209
(1)	Inhaltliche Ausweitung der Folgenabschätzung	209
(2)	Pflicht zur allgemeinen Veröffentlichung	210
(3)	Unionsrechtliche Vorgaben und kompetenzrechtliche Grenzen	212
d)	Sonderregulierungsfeld „Schutzinstrumente für die öffentliche Meinungsbildung steuernde Algorithmen von News-Aggregatoren“	213

aa) Inhaltliche Prüfpflicht	215
(1) De lege lata	215
(a) Medienanbieter zwischen Haftungsprivileg des TMG und besonderer Verantwortung für die politische Willensbildung	215
(b) NetzDG	216
(α) Anbieter sozialer Netzwerke	216
(β) Journalistisch-redaktionell gestaltete Angebote	218
(c) § 54 Abs. 2, 3 RStV	219
(2) De lege ferenda?	220
bb) Transparenz über die Mechanismen der Nachrichtenselektion	221
cc) Meinungsneutralität?	224
3. Zulassungskontrolle	225
a) Herausforderungen und Grenzen, insbesondere Standardisierung von Trainingsprozessen	227
b) Reichweite einer Ex-ante-Kontrolle	229
aa) Private Stellen	229
bb) Öffentliche Stellen	230
4. Ausdehnung des Diskriminierungsschutzes des AGG	230
a) Erweiterung des sachlichen Anwendungsbereichs des AGG auf algorithmenbasierte Entscheidungen?	231
aa) Verhältnis zwischen § 2 und § 19 AGG de lege lata	232
(1) Anwendungsreichweite des § 2 Abs. 1 Nr. 8 AGG: öffentliche Einrichtung vs. invitatio ad offerendum ad incertas personas	232
(2) § 19 AGG als Ausweitung des Anwendungsbereichs des AGG	234
bb) Zwischenfazit.	235
b) De lege lata verbleibende Regelungslücken	236
aa) Ausweitung des Anwendungsbereichs	236
bb) Rechtsgebot technischer Vorkehrungen gegen mittelbare Diskriminierungen	239
(1) Abgrenzungsschwierigkeiten zwischen mittelbarer Drittwirkung und der Spiegelung realer Individualpräferenzen	239
(2) Technisch-organisatorische Umsetzungswege für faire Algorithmen	243
(3) Zwischenergebnis	246
cc) Implikationen für die Beweislastverteilung	247
c) Nationaler Regelungsspielraum?	248
III. Begleitende Rechtmäßigkeitskontrolle	249
1. Instrumente	250
a) Ergebniskontrolle	250

aa)	Behördliche Ergebniskontrolle, insbesondere Kontrollalgorithmen	250
bb)	Berücksichtigung von Nutzerkontrollen?	251
b)	Kontrolle des Prozesses der Verarbeitungsmechanismen: behördliche Auskunfts- und Einsichtsrechte (insbesondere) bei sensiblen maschinellen Lernverfahren	253
aa)	Einblick in den Programmcode	253
(1)	Behördliche Verfahren	253
(2)	Gerichtliche Verfahren	254
(a)	Ausschluss der Öffentlichkeit	254
(b)	Waffengleichheit im Prozess	255
bb)	Einblick in das Ökosystem der Verarbeitung, insbesondere Zugangsrechte/Schnittstellen für Tests und externe Kontrollen	256
c)	Betreiber- und Mitwirkungspflichten	256
aa)	Betriebspflicht, den rechtmäßigen, diskriminierungsfreien Einsatz des Programms zu kontrollieren und sicherzustellen	257
(1)	Gebot hinreichender mathematisch-statistischer Evidenz algorithmenbasierter Verarbeitungen sowie normative Vorgaben für die Gewichtung der Entscheidungsparameter	257
(2)	Qualitätsvorgaben für die Verfahrensrichtigkeit	259
bb)	Protokollierung und Beweissicherung	260
(1)	Erforderlichkeit	260
(2)	Regulierungsansätze	260
(a)	WpHG	260
(b)	Art. 30 DSGVO	261
(c)	Art. 5 Abs. 2 DSGVO	261
(α)	Reichweite des Pflichtengehalts	261
(β)	Gesetzgebungshistorie	262
(γ)	Arg. e contrario aus sonstigen Protokollpflichten der DSGVO	263
(d)	Art. 24 Abs. 1 S. 1, Art. 25 Abs. 1, Art. 32 Abs. 1 DSGVO	264
(3)	Normative Ausgestaltung de lege ferenda	265
cc)	Verpflichtung, ein Risikomanagementsystem zu installieren, insbesondere einen verantwortlichen Risikomanager zu bestellen	266
2.	Aufsichtsstruktur	268
a)	Rechtspolitische Gestaltungsoptionen für eine einheitliche Vollzugsbehörde	269
b)	Unterstützungseinheit	271
c)	Markt- und Produktüberwachungseinheit	272
IV.	Ex-post-Kontrolle: Haftung, Sanktionen und Rechtsschutz	274

1. Zivilrechtliche Haftung, insbesondere Beweiserleichterungen und Gefährdungshaftung	274
a) Zivilrechtliche Beweislastumkehr für Verletzungen und haftungsausfüllende Kausalität in Art. 82 Abs. 1, Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO?	276
b) Beweiserleichterungen und Haftungsmodifizierungen nach dem Vorbild de lege lata bestehender Zurechnungskonzepte ...	278
aa) Anwendbarkeit des Produkthaftungsgesetzes de lege lata?	278
bb) Grundsätze der Produzentenhaftung aus § 823 Abs. 1 BGB	280
(1) Sorgfaltsmaßstab	280
(2) Nachweispflicht, Anforderungen an die Sicherheit, Update-Pflicht?	281
cc) Beweiserleichterung nach dem Vorbild der Produzentenhaftung	283
dd) Zwischenergebnis	287
c) Gefährdungshaftung	287
aa) Klassische Anwendungskonstellationen: Tierhalter-, Kfz- und Arzneimittelhaftung	288
bb) Gefährdungshaftung für Softwareanwendungen?	288
(1) Parallelen zu bestehenden Gefährdungshaftungstatbeständen	288
(2) Strukturelle Unterschiede	289
d) Etablierung einer elektronischen Person?	290
aa) Anleihe bei der Figur der juristischen Person	291
bb) Regelungslücken?	292
(1) Selbstständige Teilnahme am Rechtsverkehr	292
(2) Deliktische Haftung	293
(3) Schlussfolgerungen	294
2. Sanktionen	295
a) Die Geldbuße als prominente Sanktionsform	295
aa) DSGVO	295
bb) Antidiskriminierungsrecht	296
b) Weitere Sanktionsformen	296
3. Erweiterung des prozessualen Handlungsbestecks	297
a) Konkurrenten-Abmahnung und Unterlassungsklage bei Rechtsverletzungen	297
aa) Marktverhaltensregelende Implikation und Regelungsentention der DSGVO	299
(1) Recht auf Datenübertragbarkeit (Art. 20 DSGVO) ...	300
(2) Vorschriften zum Adresshandel sowie §§ 13, 15 TMG	301
(3) Art. 22 DSGVO?	301
(4) Sonstige Vorschriften der DSGVO	302

bb)	Nicht abschließender Charakter der Art. 77–84 DSGVO . . .	303
(1)	Art. 80 Abs. 2 DSGVO	303
(2)	Art. 82 DSGVO	304
cc)	Schlussfolgerungen	305
b)	Abmahn- bzw. Klagerechte für Verbraucherverbände (vgl. Art. 80 DSGVO i. V. m. § 2 Abs. 2 S. 1 Nr. 11 UKlaG) . . .	306
aa)	Erweiterung des § 5 UWG i. V. m. § 8 Abs. 3 Nr. 3 UWG?	307
bb)	Erweiterung des § 2 Abs. 2 S. 1 Nr. 11 UKlaG	308
(1)	Reichweite des Art. 80 DSGVO	309
(2)	Regelungsvorschlag für diskriminierende Rechtsverletzungen	310
c)	Prozessuale Ausweitungen der Wirkmacht gerichtlicher Verurteilungen	311
aa)	Musterfeststellungsklage	311
(1)	Implementierung de lege lata	311
(2)	Abgrenzung zu anderen Verbraucherschutzklagetypen	312
(3)	Musterfeststellungsklage für algorithmenbasierte Verfahren	313
bb)	Streitbeitrittsrecht	313
cc)	Rechtskrafterstreckung; Ergänzungskompetenz der Zivilgerichte?	314
d)	Digitale Schlichtungsstelle	317
V.	Flankierende (Selbst-)Regulierung: Verhaltenskodex mit Entsprechenserklärung	320
1.	Gütesiegel, Prüfzeichen, Zertifizierung bzw. Auditierung auf der Grundlage von algorithmic accountability standards	323
2.	Verhaltenskodizes als Instrumente der regulierten Selbstregulierung	324
a)	Blaupause Deutscher Corporate Governance Kodex	327
b)	Konzeptionslinien eines „Algorithmic Responsibility“-Kodex	328
c)	Zwischenergebnis	331
E.	Zusammenfassung der Schlussfolgerungen	333
I.	Risiken	333
1.	Intransparenz	333
2.	Diskriminierungsrisiken	334
3.	Markt-Macht-Bündelungen	336
4.	Diagnose: Algorithmenregulierung als Risikotechnologierecht . . .	337
II.	Regulierungsvorschläge	339
1.	Transparenz	340
a)	Kennzeichnungspflicht („Ob“)	341
b)	Informationspflicht zum Inhalt algorithmenbasierter Verfahren („Wie“)	341

aa)	Ex ante	341
(1)	Offenlegung des Algorithmus? – nur ausnahmsweise bei öffentlichen Stellen	342
(2)	Ausweitung der Informationspflicht auf persönlichkeitsensitive Algorithmenanwendungen über Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h DSGVO hinaus	343
bb)	Ex post: Begründungspflicht für algorithmenbasierte Entscheidungen und Recht auf Einblick in die Datengrundlage	343
cc)	Wirkungsanalyse: visuelle Symbole als Teil eines gestuften Informationssystems und Nutzercockpit	345
c)	Art. 15 Abs. 1, Abs. 3 S. 1 DSGVO	345
d)	Inhaltliche Ausweitung und Veröffentlichung einer Folgenabschätzung	346
e)	Besondere Transparenzanforderungen an algorithmenbasierte News-Aggregatordienste	347
2.	Inhaltskontrolle	348
a)	Diskriminierungsschutz, Fortentwicklung des AGG	348
aa)	Technischer Schutz gegen (insbesondere mittelbare) Diskriminierung	348
bb)	Ausweitung des Anwendungsbereichs des AGG	349
cc)	Anpassung der Beweislastverteilung	350
b)	Zulassungskontrolle für besonders sensible Softwareanwendungen	350
c)	Kontrollalgorithmen und Überprüfung der Trainingsumgebung	351
d)	Risikomanagementsystem, Auskunfts- und Mitwirkungspflichten, Gebot mathematisch-statistischer Validität	352
e)	Protokollierung der Programmabläufe	353
f)	Institutionelle Ausgestaltung der Aufsicht	354
3.	Haftung, Rechtsschutz und Sanktionen	355
a)	Beweiserleichterungen	355
b)	Gefährdungshaftung; elektronische Person?	355
c)	Sanktionen	356
d)	Abmahnbefugnisse für Wettbewerber	356
e)	Verbandsklagerecht der Verbraucherverbände und Einrichtung von Schiedsstellen	357
f)	Rechtskrafterstreckung bzw. Ergänzungskompetenz der Zivilgerichte	358
4.	Selbstregulierung: „Algorithmic-Responsibility“-Kodex nach dem Vorbild des Corporate Governance Kodex	358

5. Epilog: Auf der Suche nach dem kategorischen Imperativ für Algorithmen im Kompetenzgeflecht zwischen der Union und den Mitgliedstaaten	360
a) Augenmaß als Leitvorgabe der Rationalität	360
b) Unionale Regelungen als Ziel	360
c) Nutzervertrauen als Legitimation und Handlungsschranke	362
d) Digitaler Humanismus als Leitstern	362
Literaturverzeichnis	365