

# Risikobasierte Regulierung der IT-Sicherheit von Produkten

Eine Untersuchung am Beispiel von  
Smart-Home-Geräten

von

Maximilian Leicht

# Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2024/2025 von der Rechtswissenschaftlichen Fakultät der Universität des Saarlandes als Dissertation angenommen. Sie entstand während meiner Tätigkeit am dortigen Lehrstuhl für Rechtsinformatik. Gesetzgebung, Literatur und Rechtsprechung sind auf dem Stand von September 2024, einzelne Aktualisierungen konnten noch bis Februar 2025 berücksichtigt werden.

Mein Dank gilt ganz besonders meinem Doktorvater Prof. Dr.-Ing. Christoph Sorge, der mit vielen konstruktiven Denkanstößen und jederzeit in gleichem Maße kritischen wie hilfreichen Ratschlägen den interdisziplinären Charakter dieser Arbeit erst ermöglichte. Meine Tätigkeit am Lehrstuhl für Rechtsinformatik werde ich daher stets in bester Erinnerung behalten – nicht nur wegen der zahlreichen Gelegenheiten zum ausgedehnten fachlichen Austausch, sondern auch wegen der Vielfältigkeit der Erfahrungen, die ich dort sammeln durfte.

Ebenso möchte ich Herrn Prof. Dr. Nikolaus Marsch danken, für die frühzeitige Ermunterung über eine Promotion nachzudenken gleichsam wie für die Co-Betreuung der Arbeit und die zügige Erstellung des Zweitgutachtens.

Darüber hinaus danke ich meinen wunderbaren Kolleginnen und Kollegen, die mich bei den Herausforderungen der Promotion begleitet haben. Für anregende Diskussionen zum und abseits des Themas der Arbeit, für die erforderliche Ablenkung und ihre freundschaftliche Verbundenheit danke ich Nils Wiedemann, Leo Dessani, Piotr Rataj, Simone Salemi, Bianca Steffes, Dr. rer. nat. Frederik Möllers und Andreas Rebmann.

Diese Arbeit ist meiner Familie gewidmet. Ihr gilt mein größter Dank. Ohne ihre nachdrückliche Förderung meiner Ausbildung und ihre Unterstützung auf jede erdenkliche Weise in allen Lebenslagen wäre das vorliegende Werk nicht denkbar.

Saarbrücken, im März 2025

Maximilian Leicht

# Inhaltsübersicht

<b>Vorwort</b> .....	VII
<b>Abkürzungsverzeichnis</b> .....	XIX
<b>Einleitung</b> .....	1
<b>Kapitel 1 – Ausgangsüberlegungen und Begriffsbestimmung</b> . . . .	3
A. Ausgangsüberlegungen zu Inhalt, Methodik und Motivation . . . .	3
B. Konkretisierung der Themenwahl aus rechtlicher Sicht . . . . .	4
I. Datenschutzrechtliche Fragestellungen . . . . .	6
II. GeschGehG . . . . .	7
III. Datenschutz bei digitalen Diensten . . . . .	8
IV. Regulierung von Produkten . . . . .	8
V. Übersicht der untersuchten Regelungen . . . . .	8
C. Risiko, Risikoregulierung, Risikobasierte Regulierung . . . . .	10
I. Begriffsverständnis: Risikoregulierung oder risikobasierte Regulierung . . . . .	10
II. Risikobasierte Regulierung der IT-Sicherheit von Produkten	15
III. Einordnung in den Kontext existierender Regulierungs- strategien . . . . .	17
IV. Der Risikobegriff in anderen Rechtsgebieten und Disziplinen	19
<b>Kapitel 2 – Technische Grundlagen</b> .....	31
A. Einführung .....	31
B. Konkretisierung des technischen Untersuchungsgegenstandes . . .	35
I. Beschreibung der Produktkategorien. . . . .	36
II. Übersicht der Akteure . . . . .	41
C. Ausgangsüberlegungen zu relevanten Risikoszenarien . . . . .	42
I. Risikoszenarien . . . . .	43
II. Einsatzszenarien . . . . .	49
<b>Kapitel 3 – Datenschutzrechtliche Fragestellungen</b> .....	51
A. Datenschutzrechtliche Verantwortlichkeit im Smart Home . . . . .	51
I. Datenschutzrechtliche Verantwortlichkeit. . . . .	51
II. Implikationen im Smart Home . . . . .	54
B. Rechtliche Anforderungen an die Sicherheit der Daten- verarbeitung sowie an Technikgestaltung . . . . .	63
I. IT-Sicherheit als zentraler Bestandteil des normativen Charakters der DSGVO . . . . .	63
II. Art. 32 DSGVO – Sicherheit der Datenverarbeitung . . . . .	64
III. Art. 25 DSGVO . . . . .	129

C. Zentrale Ergebnisse und Thesen des Kapitels . . . . .	134
<b>Kapitel 4 – Fragestellungen des (weiteren) IT-Sicherheitsrechts . .</b>	<b>137</b>
A. Begriff des IT-Sicherheitsrechts i. w. S. . . . .	137
B. Bedeutung der angemessenen Geheimhaltungsmaßnahmen nach dem GeschGehG. . . . .	139
I. Schutzgegenstand des GeschGehG . . . . .	140
II. Vergleich auf sekundärer Ebene . . . . .	148
III. Zwischenergebnis . . . . .	152
IV. Spezifische Aspekte des Smart Home . . . . .	152
C. Einfluss des Telekommunikationsrechts sowie des TDDDG. . . . .	153
I. Änderungen durch das Durchführungsgesetz zum Digital Services Act. . . . .	154
II. Zum Verhältnis von TDDDG, ePrivacy-RL und DSGVO. . . . .	156
III. Datenschutz bei digitalen Diensten sowie Integrität von Endeinrichtungen. . . . .	161
IV. Telekommunikationsrecht . . . . .	184
D. Regulierung von Produkten und zugehörige Fragestellungen . . . . .	186
I. Besondere Anforderungen an Funkanlagen (Radio Equipment Directive) . . . . .	186
II. Regulierung von Produkten mit digitalen Elementen (Cyber Resilience Act). . . . .	196
E. Weitere IT-Sicherheitsregulierung . . . . .	212
I. Regulierung von Einrichtungen in kritischen Sektoren (NIS-2-RL) . . . . .	212
II. Regulierung virtueller Assistenten und Betriebssysteme im DMA . . . . .	213
F. Zentrale Ergebnisse und Thesen des Kapitels . . . . .	216
<b>Kapitel 5 – Verknüpfung der rechtlichen Anforderungen mit konkreten technischen Maßnahmen . . . . .</b>	<b>219</b>
A. Verknüpfung der rechtlichen Anforderungen. . . . .	220
I. Systematisierung durch Verknüpfung mit Schutzzielen . . . . .	220
II. Systematisierung durch Verknüpfung von Anforderungen . . . . .	222
III. Zusammenführung in kombinierter Risiko- und Folgenabschätzung . . . . .	230
IV. Zwischenergebnis . . . . .	233
B. Spezifische Konkretisierung für Smart-Home-Geräte . . . . .	235
I. Verknüpfung mit Schutzzielen: Produktkategorie Smart-Home-Zentralen. . . . .	236
II. Verknüpfung mit einem gemeinsamen Anforderungskatalog: Produktkategorie Smart TVs . . . . .	241

III. Kombinierte Risiko- und Datenschutzfolgenabschätzung: Produktkategorie digitale, cloudbasierte Sprachassistenten ..	245
C. Zentrale Ergebnisse und Thesen des Kapitels .....	248
<b>Kapitel 6 – Fazit und Ausblick .....</b>	<b>251</b>
<b>Literaturverzeichnis .....</b>	<b>255</b>
<b>Anmerkungen zur Zitierweise .....</b>	<b>277</b>



# Inhaltsverzeichnis

<b>Vorwort</b> .....	VII
<b>Abkürzungsverzeichnis</b> .....	XIX
<b>Einleitung</b> .....	1
<b>Kapitel 1 – Ausgangsüberlegungen und Begriffsbestimmung</b> . . . .	3
A. Ausgangsüberlegungen zu Inhalt, Methodik und Motivation . . . .	3
B. Konkretisierung der Themenwahl aus rechtlicher Sicht . . . . .	4
I. Datenschutzrechtliche Fragestellungen . . . . .	6
II. GeschGehG . . . . .	7
III. Datenschutz bei digitalen Diensten . . . . .	8
IV. Regulierung von Produkten . . . . .	8
V. Übersicht der untersuchten Regelungen . . . . .	8
C. Risiko, Risikoregulierung, Risikobasierte Regulierung . . . . .	10
I. Begriffsverständnis: Risikoregulierung oder risikobasierte Regulierung . . . . .	10
II. Risikobasierte Regulierung der IT-Sicherheit von Produkten	15
III. Einordnung in den Kontext existierender Regulierungs- strategien . . . . .	17
1. Parallelen zum Umweltrecht . . . . .	17
2. Folgerungen für die vorliegende Untersuchung . . . . .	19
IV. Der Risikobegriff in anderen Rechtsgebieten und Disziplinen	19
1. Risikobegriffe . . . . .	19
2. Quantifizierbarkeit von Risiko . . . . .	26
3. Fazit. . . . .	29
<b>Kapitel 2 – Technische Grundlagen</b> .....	31
A. Einführung . . . . .	31
B. Konkretisierung des technischen Untersuchungsgegenstandes . . .	35
I. Beschreibung der Produktkategorien. . . . .	36
1. Smart-Home-Zentralen . . . . .	36
2. Smart TVs . . . . .	38
3. Digitale, cloudbasierte Sprachassistenten . . . . .	39
4. Übersicht der Produktkategorien und ihre Einbindung in das Netzwerk . . . . .	40
II. Übersicht der Akteure . . . . .	41
C. Ausgangsüberlegungen zu relevanten Risikoszenarien . . . . .	42
I. Risikoszenarien . . . . .	43
1. Differenzierung nach Phasen der Datenverarbeitungen . . .	43
2. Potenzielle Angriffe . . . . .	45

## Inhaltsverzeichnis

a. Grundbegriffe .....	45
b. Konkrete Beispiele verschiedener Angriffe und Angriffsziele .....	46
II. Einsatzszenarien .....	49
<b>Kapitel 3 – Datenschutzrechtliche Fragestellungen .....</b>	<b>51</b>
A. Datenschutzrechtliche Verantwortlichkeit im Smart Home .....	51
I. Datenschutzrechtliche Verantwortlichkeit .....	51
II. Implikationen im Smart Home .....	54
1. Verantwortlichkeit der (privaten) Nutzer? .....	54
a. Persönliche und familiäre Tätigkeiten .....	54
b. Zwischenergebnis .....	60
2. Einordnung der hier untersuchten Produktkategorien. ....	61
a. Verantwortlichkeit der Akteure bei Vorliegen der Haushaltsausnahme. ....	62
b. Verantwortlichkeit der Akteure bei Nutzern innerhalb der Anwendbarkeit der DSGVO .....	62
B. Rechtliche Anforderungen an die Sicherheit der Daten- verarbeitung sowie an Technikgestaltung .....	63
I. IT-Sicherheit als zentraler Bestandteil des normativen Charakters der DSGVO .....	63
II. Art. 32 DSGVO – Sicherheit der Datenverarbeitung .....	64
1. Tatbestandsmerkmale des Art. 32 DSGVO .....	65
a. Angemessenes Schutzniveau, Art. 32 Abs. 2 DSGVO ..	66
b. Abwägungskriterien .....	66
(1) Stand der Technik. ....	67
(aa) Bestimmung des Begriffs Stand der Technik. .	67
(bb) Bestimmung des Stands der Technik .....	71
(2) Implementierungskosten .....	74
(3) Art, Umfang, Umstände, Zwecke der Verarbeitung	78
(4) Eintrittswahrscheinlichkeit .....	81
(5) Schwere des Risikos für Rechte und Freiheiten natürlicher Personen. ....	82
2. Der sog. risikobasierte Ansatz der DSGVO – Bedeutung und Reichweite .....	84
a. Zum Risikobegriff der DSGVO .....	86
b. Quantifizierung von Risiko i. S. d. DSGVO .....	95
c. Mögliche Elemente zur Strukturierung der Risiko- bewertung .....	97
d. Fazit und Bewertung. ....	98
3. Ansätze zur Ableitung technischer und organisatorischer Schutzmaßnahmen .....	101
a. Maßnahmenkatalog nach Art. 32 Abs. 1 Hs. 2 DSGVO ..	102

(1) Pseudonymisierung und Verschlüsselung (lit. a) . . .	103
(2) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (lit. b) . . . . .	106
(3) Verfügbarkeit der – und Zugang zu – personenbezogenen Daten (lit. c) . . . . .	112
(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit (lit. d) . . . . .	113
(5) Zwischenergebnis. . . . .	113
b. Verhaltensregeln und Zertifizierungen als Konkretisierungsinstrumente der DSGVO . . . . .	114
c. Weitere Zertifizierungen als Konkretisierung . . . . .	118
d. Interdisziplinäre Ansätze zur Konkretisierung . . . . .	119
e. Konkretisierung technischer Maßnahmen mit dem sog. Standard-Datenschutzmodell . . . . .	125
f. Fazit . . . . .	128
III. Art. 25 DSGVO . . . . .	129
1. Art. 25 Abs. 1 DSGVO – Privacy by Design. . . . .	129
a. Zielrichtung und Verhältnis zu Art. 32 DSGVO . . . . .	129
b. „Garantien“ . . . . .	130
c. Ansätze zur Ableitung konkreter technischer Schutzmaßnahmen. . . . .	131
2. Art. 25 Abs. 2 DSGVO – Privacy by Default . . . . .	132
3. Fazit. . . . .	133
C. Zentrale Ergebnisse und Thesen des Kapitels . . . . .	134
<b>Kapitel 4 – Fragestellungen des (weiteren) IT-Sicherheitsrechts . .</b>	<b>137</b>
A. Begriff des IT-Sicherheitsrechts i. w. S. . . . .	137
B. Bedeutung der angemessenen Geheimhaltungsmaßnahmen nach dem GeschGehG. . . . .	139
I. Schutzgegenstand des GeschGehG . . . . .	140
1. Angemessenheit i. S. d. § 2 GeschGehG . . . . .	141
a. Subjektiv-erwartungsorientierte Betrachtung der Angemessenheit . . . . .	142
b. Wirtschaftlicher Wert als Kriterium . . . . .	147
2. Fazit. . . . .	147
II. Vergleich auf sekundärer Ebene . . . . .	148
III. Zwischenergebnis . . . . .	152
IV. Spezifische Aspekte des Smart Home . . . . .	152
C. Einfluss des Telekommunikationsrechts sowie des TDDDG. . . . .	153
I. Änderungen durch das Durchführungsgesetz zum Digital Services Act. . . . .	154
II. Zum Verhältnis von TDDDG, ePrivacy-RL und DSGVO. . . . .	156

III. Datenschutz bei digitalen Diensten sowie Integrität von Endeinrichtungen. . . . .	161
1. Anbieter von digitalen Diensten im Smart Home. . . . .	161
2. Digitale Dienste im Smart Home . . . . .	161
3. § 19 TDDDG . . . . .	163
a. § 19 Abs. 1–3 TDDDG . . . . .	165
b. § 19 Abs. 4 TDDDG . . . . .	169
4. § 25 TDDDG . . . . .	173
a. Föderierte Lernsysteme . . . . .	176
b. Sicherheitsupdates . . . . .	182
c. Verwendung von Drittanbieterapps . . . . .	183
d. Rechtfertigung nach § 25 Abs. 2 TDDDG. . . . .	183
5. Fazit. . . . .	184
IV. Telekommunikationsrecht . . . . .	184
D. Regulierung von Produkten und zugehörige Fragestellungen . . . . .	186
I. Besondere Anforderungen an Funkanlagen (Radio Equip- ment Directive) . . . . .	186
1. Schutz personenbezogener Daten und der Privatsphäre (Art. 3 Abs. 3 lit. e RED) . . . . .	186
2. Schutz des Netzes (Art. 3 Abs. 3 lit. d RED) . . . . .	189
3. Smart-Home-Geräte als „mit dem Internet verbundene Funkanlagen“ . . . . .	190
4. Anforderungen die zu treffenden Sicherheitsvorkehrungen . . . . .	193
II. Regulierung von Produkten mit digitalen Elementen (Cyber Resilience Act). . . . .	196
1. Produkte mit digitalen Elementen. . . . .	197
a. Abgrenzung: Grundsätzlich keine Anwendbarkeit des CRA auf Software-as-a-Service . . . . .	198
b. Smart-Home-Geräte als wichtige Produkte mit digitalen Elementen . . . . .	202
2. IT-Sicherheitsanforderungen, insbesondere im Vergleich zur DSGVO. . . . .	203
a. Explizit geregeltes Verhältnis zur DSGVO . . . . .	204
b. Weitere Fragestellungen im Verhältnis CRA zu DSGVO . . . . .	205
E. Weitere IT-Sicherheitsregulierung . . . . .	212
I. Regulierung von Einrichtungen in kritischen Sektoren (NIS-2-RL) . . . . .	212
II. Regulierung virtueller Assistenten und Betriebssysteme im DMA . . . . .	213
F. Zentrale Ergebnisse und Thesen des Kapitels . . . . .	216
<b>Kapitel 5 – Verknüpfung der rechtlichen Anforderungen mit konkreten technischen Maßnahmen . . . . .</b>	<b>219</b>

A. Verknüpfung der rechtlichen Anforderungen . . . . .	220
I. Systematisierung durch Verknüpfung mit Schutzziele . . . . .	220
II. Systematisierung durch Verknüpfung von Anforderungen . . . . .	222
1. Vergleichsmaßstab für Verknüpfungen . . . . .	224
2. Erläuterung der festgestellten Verknüpfungen . . . . .	225
3. Fazit. . . . .	228
III. Zusammenführung in kombinierter Risiko- und Folgen- abschätzung . . . . .	230
IV. Zwischenergebnis . . . . .	233
B. Spezifische Konkretisierung für Smart-Home-Geräte . . . . .	235
I. Verknüpfung mit Schutzziele: Produktkategorie Smart- Home-Zentralen. . . . .	236
1. Mögliche Risiken und entsprechende Schutzmaßnahmen . . . . .	237
2. Verknüpfung mit rechtlichen Anforderungen und Syner- gieeffekte. . . . .	239
II. Verknüpfung mit einem gemeinsamen Anforderungskatalog: Produktkategorie Smart TVs . . . . .	241
1. Mögliche Risiken und entsprechende Schutzmaßnahmen . . . . .	241
2. Verknüpfung mit rechtlichen Anforderungen und Syner- gieeffekte. . . . .	243
III. Kombinierte Risiko- und Datenschutzfolgenabschätzung: Produktkategorie digitale, cloudbasierte Sprachassistenten . . . . .	245
1. Mögliche Risiken und entsprechende Schutzmaßnahmen . . . . .	245
2. Verknüpfung mit rechtlichen Anforderungen und Syner- gieeffekte. . . . .	247
C. Zentrale Ergebnisse und Thesen des Kapitels . . . . .	248
<b>Kapitel 6 – Fazit und Ausblick . . . . .</b>	<b>251</b>
<b>Literaturverzeichnis . . . . .</b>	<b>255</b>
<b>Anmerkungen zur Zitierweise . . . . .</b>	<b>277</b>



# Einleitung

Das Datenschutz- und IT-Sicherheitsrecht hat sich in den letzten Jahren geradezu sprunghaft weiterentwickelt. Mit der zunehmenden Bedeutung digitaler Technologien im Alltag wächst auch das Bewusstsein für die zahlreichen und teils schwerwiegenden Bedrohungen für die IT-Sicherheit der eingesetzten Produkte. Dies hat der Gesetzgeber erkannt und mit der Schaffung eines vielschichtigen Regelungsgefüges zur Adressierung der IT-Sicherheit reagiert.

Bereits die seit 25. Mai 2018 geltende Datenschutz-Grundverordnung enthält zentrale Anforderungen an die Sicherheit von Datenverarbeitungen, die von Verantwortlichen und Auftragsverarbeitern einzuhalten sind. Daneben wird der Cyber Resilience Act als unionsweite, horizontale Regelung aufgrund der unmittelbaren Adressierung von Herstellern eine große Bedeutung erlangen. Außerdem ist seit dem 18. Oktober 2024 die NIS-2-Richtlinie anzuwenden, die die Sicherheit von Einrichtungen in bestimmten Sektoren reguliert.

Zusätzlich sind weitere gesetzliche Entwicklungen zu verzeichnen, wie etwa die Schaffung des Telekommunikation-Telemedien-Datenschutz-Gesetzes – sowie die kurz darauffolgenden Änderungen durch das Durchführungsgesetz zum Digital Services Act, die neben der Schaffung des Digitale-Dienste-Gesetzes unter anderem die Ersetzung des Begriffs des Telemediums mit sich brachten. Damit war auch die Umbenennung in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz verbunden.

Ebenso relevant für die Implementierung von Schutzmaßnahmen zur Verbesserung der IT-Sicherheit sind das auf Basis unionsrechtlicher Vorgaben geschaffene Gesetz zum Schutz von Geschäftsgeheimnissen sowie die Neuerungen aufgrund der delegierten Verordnung 2022/30 i. V. m. dem Funkanlagengesetz. Auch diese Regelungen werden in dieser Untersuchung als Bestandteile des IT-Sicherheitsrechts i. w. S. verstanden.

Denn aus all diesen Rechtsakten ergeben sich – wenn auch in unterschiedlichem Ausmaß – abstrakte rechtliche Anforderungen an die IT-Sicherheit von Produkten. Dabei ist sowohl das Verhältnis dieser Anforderungen als auch deren Verknüpfung mit konkreten Schutzmaßnahmen bisher überwiegend ungeklärt. Die vorliegende Untersuchung hat sich zum Ziel gesetzt, diese bestehende Unklarheit zu adressieren. Insoweit verfolgt die Untersuchung einen sowohl in der Rechtswissenschaft als auch in der Informatik bisher nur vereinzelt zugrunde gelegten interdisziplinären Ansatz.

Als exemplarischer technischer Untersuchungsgegenstand dienen vorliegend Smart-Home-Geräte. Diese sind vielfach Bestandteil des alltäglichen Lebens, bieten diverse Möglichkeiten zur Vernetzung mit weiteren Geräten

und werden sowohl in der privaten als auch in der beruflichen Sphäre eingesetzt. Zugleich weisen diese Geräte vielfach IT-Sicherheitsrisiken auf. Anhand dieses technischen Untersuchungsgegenstandes werden die einschlägigen rechtlichen Anforderungen analysiert und es wird ein systematisches, interdisziplinär begründetes Verhältnis der Normen herausgearbeitet. Auf dieser Basis werden schließlich die Anforderungen mit konkreten technischen Maßnahmen verknüpft, die die genannten Sicherheitsrisiken adressieren. Diese Verknüpfung ermöglicht die Identifikation und methodische Begründung von Synergieeffekten hinsichtlich der umzusetzenden Maßnahmen. Die vorliegend entwickelten Ansätze sind dabei auch auf weitere technische Untersuchungsgegenstände anwendbar.

Kapitel 1 stellt die dazu erforderlichen Ausgangsüberlegungen und Begriffsbestimmungen dar. Darauf aufbauend werden in Kapitel 2 technische Grundlagen erläutert. In Kapitel 3 stehen sodann die datenschutzrechtlichen Anforderungen an die Sicherheit von Datenverarbeitungen sowie an die technische Gestaltung der Produkte im Fokus. Kapitel 4 widmet sich Anforderungen aus dem weiteren (risikobasierten) IT-Sicherheitsrecht. Thematisiert wird neben Aspekten des Geschäftsgeheimnisschutzes auch der Datenschutz bei digitalen Diensten sowie die Regulierung von Produkten. Kapitel 5 stellt schließlich Ansätze vor, wie die erarbeiteten rechtlichen Anforderungen verknüpft werden können, um eine Ableitung konkreter Schutzmaßnahmen zu ermöglichen. Kapitel 6 schließt die Untersuchung mit einem Fazit ab und gibt einen Ausblick auf die zukünftige Entwicklung der risikobasierten IT-Sicherheitsregulierung von Produkten.

# Kapitel 1 – Ausgangsüberlegungen und Begriffsbestimmung

Im Folgenden werden zunächst Ausgangsüberlegungen zur Auswahl der untersuchten Fragestellungen sowie zu Methodik und Motivation erläutert (vgl. Abschnitt A.). Darauf aufbauend wird der Untersuchungsgegenstand aus rechtlicher (vgl. Abschnitt B.) – sowie an späterer Stelle aus technischer (vgl. Kapitel 2 B.) – Sicht konkretisiert. Kapitel 1 enthält zudem Ausgangsüberlegungen zum Begriff des Risikos, der Risikoregulierung sowie der risikobasierten Regulierung (vgl. Abschnitt C.).

## A. Ausgangsüberlegungen zu Inhalt, Methodik und Motivation

Der Ausgangspunkt der Arbeit liegt schwerpunktmäßig in folgender Fragestellung:

*Welche rechtlichen Anforderungen an technische Maßnahmen der IT-Sicherheit für Produkte des Internet of Things ergeben sich nach der aktuellen Rechtslage und wie lassen sich diese zu implementierenden Maßnahmen konkretisieren?*

Eine naheliegende Ausgangsüberlegung hinsichtlich der Konkretisierung ist, dass der Begriff Internet of Things einen zu weiten Interpretationsspielraum zulässt, um ausreichend konkrete technische Vorgaben zu definieren. Deshalb wird die Fragestellung insoweit spezifiziert, dass bei der Analyse der rechtlich hierfür relevanten Normen die gewonnenen Erkenntnisse exemplarisch auf einen bestimmten Untersuchungsgegenstand angewandt und – unter Hinzuziehung entsprechender technischer Literatur – mit konkreten technischen Maßnahmen verknüpft werden. Die Arbeit verfolgt methodisch insoweit einen interdisziplinären Ansatz. Neben der Analyse der rechtlichen Forschungsfragen – welche überblicksartig im Folgenden (Kapitel 1 B.) skizziert werden – soll gerade diese Verknüpfung der (abstrakten) rechtlichen Anforderungen und die darauf basierende Ableitung (konkreter) technischer Maßnahmen den Mehrwert der Untersuchung darstellen.

Die Analyse konzentriert sich daher zum einen auf die Ermittlung der einschlägigen rechtlichen Anforderungen für den Untersuchungsgegenstand. Ziel ist es, die Anforderungen exemplarisch im Bereich der Smart-Home-Geräte zu konkretisieren, sodass sie handhabbar für eine Verknüpfung mit einzelnen technischen Maßnahmen werden. Die Vorgehensweise soll daher nicht zu vom Untersuchungsgegenstand losgelösten Erkenntnissen über die

rechtlichen Anforderungen führen. Es wird also etwa nicht nur analysiert, welche Anforderungen nach Art. 32 DSGVO allgemein gelten und wie sich die Auslegung des Stands der Technik und des sog. risikobasierten Ansatzes hierauf auswirken. Vielmehr wird des Weiteren dargelegt, wie sich diese Anforderungen auf den Untersuchungsgegenstand der Smart-Home-Geräte auswirken. Der Grund hierfür liegt in der Prämisse, dass eine allgemeine Betrachtung der Anforderungen keine ausreichend konkrete Untersuchung zulässt, weshalb für die bezweckte interdisziplinäre Verknüpfung eine Beschränkung des Untersuchungsgegenstandes erforderlich ist.

Die vorliegende Untersuchung nimmt – im Zuge ihrer Zielsetzung einer Konkretisierung der zu treffenden Schutzmaßnahmen – auch auf übergreifende Aspekte von Regulierung Bezug. Berücksichtigt wird dabei insbesondere, dass auch in anderen Rechtsgebieten aus abstrakt gehaltenen Prinzipien und Normen konkrete Maßnahmen abgeleitet werden müssen. Dies gilt etwa für das Umweltrecht, das – im Vergleich zum Datenschutzrecht – bereits seit längerer Zeit Aspekte der Risikoregulierung enthält. Die Untersuchung zieht daher die Grundgedanken der dort verwendeten Methodik der Regulierung heran und prüft eine Übertragbarkeit auf die hinsichtlich des Untersuchungsgegenstands relevante Regulierung von IT-Sicherheit. Denn obwohl die im Folgenden untersuchten Normen nicht in jedem Fall explizit in ihrem Wortlaut einen Risikobezug aufweisen, lautet eine These dieser Untersuchung, dass alle schwerpunktmäßig untersuchten Normen zumindest in ihrer konkreten Anwendung Aspekte einer risikobasierten Regulierung von IT-Sicherheit aufweisen. Diese These wird in den folgenden Ausführungen iterativ aufgegriffen und daraufhin untersucht, inwieweit sie auf die konkreten Normen zutrifft.

## **B. Konkretisierung der Themenwahl aus rechtlicher Sicht**

Aus rechtlicher Sicht<sup>1</sup> werden alle für die o.g. Fragestellung relevanten Normen analysiert. Dies umfasst einerseits schwerpunktmäßig Normen des Datenschutzrechts. Neben den Vorgaben aus Art. 25 Abs. 1 DSGVO (Privacy by Default) und Art. 25 Abs. 2 DSGVO (Privacy by Design) ist vor allem Art. 32 DSGVO hierfür relevant. Untersucht wird der genaue Regelungsinhalt der einzelnen Normen sowie deren Verhältnis zueinander. Ein besonderer Fokus liegt dabei auf der Analyse des sog. risikobasierten Ansatzes der DSGVO, der eine Skalierung der technischen Maßnahmen verspricht.

---

<sup>1</sup> Für die Konkretisierung des Untersuchungsgegenstandes aus technischer Perspektive vgl. Kapitel 2 B.

Andererseits sind auch weitere Normen außerhalb des Datenschutzrechts für die o. g. Fragestellung relevant. Auch deren Verhältnis untereinander sowie zu den datenschutzrechtlichen Normen wird daher untersucht.

So sieht etwa das GeschGehG in § 2 Nr. 1 lit. b GeschGehG sog. angemessene Geheimhaltungsmaßnahmen vor. Enthalten Geschäftsgeheimnisse personenbezogene Daten, stellt sich u. a. die Frage der inhaltlichen Abgrenzung zum gleichzeitig geltenden Datenschutzrecht.

Das Unionsrecht reguliert zudem auch abseits von Datenschutznormen und dem Recht der Geschäftsgeheimnisse immer mehr Aspekte der IT-Sicherheit. Vorliegend relevant sind besonders der kürzlich verabschiedete Cyber Resilience Act sowie das unionsrechtlich determinierte Funkanlagengesetz.

Zu dem hier relevanten Unionsrecht könnten darüber hinaus Vorschriften des Datenschutzes bei digitalen Diensten sowie des Telekommunikationsdatenschutzes gezählt werden. Dabei wirft etwa die ePrivacy-RL insbesondere im Zusammenhang mit ihrer nationalen Umsetzung im TDDDG sowie deren Verhältnis zur DSGVO relevante Fragestellungen auf. Dabei sind auch die Neuerungen durch das Durchführungsgesetz zum Digital Services Act relevant.<sup>2</sup>

Zugleich ergibt sich eine inhaltliche Begrenzung der Untersuchung, die auf zwei Grundüberlegungen basiert. Einerseits soll die Arbeit keine rein abstrakte Analyse der relevanten Normen und ihrem Verhältnis untereinander darstellen. Vielmehr ist das Ziel der Arbeit eine möglichst konkrete Verknüpfung der rechtlichen Anforderungen mit technischen Schutzmaßnahmen. Hieraus ergibt sich eine Begrenzung auf für den Untersuchungsgegenstand typischerweise einschlägige Normen. Andere Verpflichtungen, wie bspw. solche die nur bestimmte, etwa gesellschaftlich besonders relevante und daher kritische Einrichtungen adressieren, sind daher nicht primär relevant für die Untersuchung und fließen entsprechend nur am Rande in die Analyse ein.

Andererseits erfolgt eine inhaltliche Begrenzung anhand der Zielsetzung der zu untersuchenden Normen: Analysiert werden sollen gesetzliche Rahmenbedingungen an die IT-Sicherheit von Smart-Home-Geräten. Im Fokus stehen somit Normen, die eine präventive Schutzausrichtung aufweisen. Nicht behandelt werden sollen dagegen etwa Vorschriften, die den Ausgleich eines bereits eingetretenen Schadens zum Ziel haben. Ebenfalls nicht schwer-

---

<sup>2</sup> Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze.

punktmäßig betrachtet werden sollen Fragestellungen nach dem Nachweis der Erfüllung der gesetzlichen Rahmenbedingungen an den Datenschutz und die IT-Sicherheit.

Als technischen Untersuchungsgegenstand legt diese Untersuchung Geräte des sog. Smart Home zugrunde, was wie folgt definiert wird.

*Der Begriff Smart Home umfasst Informationstechnik, die im alltäglichen Umfeld von Menschen eingesetzt wird und dazu bestimmt ist, den Wohnkomfort oder die Sicherheit in Wohnungen und Büros zu erhöhen (z. B. elektrische Rollläden oder sog. Smart Locks), Unterhaltung zu bieten (z. B. Smart TVs) oder Menschen zu assistieren (z. B. cloudbasierte, digitale Sprachassistenten). Die Geräte verarbeiten dazu (potenziell jederzeit) Daten, können typischerweise untereinander vernetzt werden und sehen oft eine Fernsteuerung ihrer Funktionalitäten vor.<sup>3</sup>*

Dieser Untersuchungsgegenstand wird in Kapitel 2 B. weiter konkretisiert; insbesondere werden einzelne hier betrachtete Produktkategorien sowie mögliche Risiken für die IT-Sicherheit dieser Produktkategorien beschrieben.<sup>4</sup> Als geeignet wird der Untersuchungsgegenstand angesehen, da diese Geräte sowohl im privaten Bereich als auch im beruflichen Bereich („Smart Office“) Einsatz finden können. Die Geräte werden zunehmend zu Alltagsgegenständen und werden so fester Bestandteil des täglichen Lebens. Zugleich liegt oft kein ausschließliches Hersteller-Nutzer-Verhältnis vor. Vielmehr ist für die Funktionalität der Geräte die Rolle weiterer Akteure relevant, die etwa als Drittanbieter zusätzliche Apps bereitstellen. Unter anderem dadurch können sich – im beruflichen wie im privaten Kontext – besondere Risiken ergeben, welche durch die untersuchten gesetzlichen Normen adressiert werden. Im Folgenden wird die Relevanz der schwerpunktmäßig adressierten Normen bzw. Rechtsakte skizziert.

## I. Datenschutzrechtliche Fragestellungen

Als ein Schwerpunkt der Untersuchung wird der Regelungsgehalt und das Verhältnis der für den Untersuchungsgegenstand relevanten Normen der

3 Die Definition basiert auf den Ausführungen von Roßnagel/Geminn/Jandt/Richter, Datenschutzrecht 2016. „Smart“ genug für die Zukunft?, S. 8–10, 12. Sie wurde für die Zwecke dieser Ausarbeitungen um den Einsatzbereich außerhalb des Wohnumfeldes erweitert. In der technischen Literatur finden sich tendenziell weitere Definitionsansätze, die insoweit als mit der vorliegenden Arbeitsdefinition vereinbar eingeordnet werden können, vgl. etwa: ENISA, Threat Landscape and Good Practice Guide for Smart Home and Converged Media v. 01.12.2014, S. 5–6. Verbreitet sind auch Definitionen, die sich auf eine private Nutzung im Wohnumfeld beschränken, vgl. nur: Zitzelsberger, Smart Strafrecht, S. 81 f.

4 Vgl. hierzu Kapitel 2 B. I sowie Kapitel 2 C.

DSGVO analysiert. Zum einen umfasst dies die Analyse der Anforderungen von Art. 32 DSGVO sowie von Art. 25 Abs. 1 und Abs. 2 DSGVO. Zum anderen werden auch daraus folgende Fragestellungen untersucht – etwa inwieweit bereits der in Art. 32 Abs. 1 Hs. 2 DSGVO geregelte Maßnahmenkatalog zur Ableitung technischer Maßnahmen dienlich ist.

Gemeinsam haben diese Normen der DSGVO u. a. ein zentrales Kriterium: Den sog. risikobasierten Ansatz. Dieser wird in der Literatur als Möglichkeit zur Skalierung der dem Normadressaten auferlegten Pflichten begriffen.<sup>5</sup> Demnach erfordern besonders risikoreiche Datenverarbeitungen entsprechend strenge, weniger risikoreiche Verarbeitungen weniger strenge Maßnahmen.<sup>6</sup> Jedoch wurde dieser Ansatz im Gesetzgebungsprozess durchaus kritisch begleitet.<sup>7</sup> Untersucht werden daher bspw. die Auswirkungen dieses Ansatzes sowie das Verständnis und die Messbarkeit des Risikos i. S. d. DSGVO.

## II. GeschGehG

Das GeschGehG soll dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung dienen (§ 1 Abs. 1 GeschGehG). Unter solchen Geheimnissen versteht das Gesetz nur Informationen, die – u. a. – „Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber“ sind, § 2 Nr. 1 lit. b GeschGehG. Relevant ist aktuell insbesondere die Fragestellung, welche Anforderungen an die konkreten Maßnahmen hierfür gestellt werden müssen und welche Maßnahmen sodann in Frage kommen.<sup>8</sup> Des Weiteren wird diskutiert, in welchem Verhältnis die im GeschGehG genannten angemessenen Geheimhaltungsmaßnahmen zu den in der DSGVO an verschiedenen Stellen genannten technischen und organisatorischen Maßnahmen stehen.<sup>9</sup> Diese Fragestellungen können insbesondere relevant werden, wenn Geräte mit digitalen Sprachassistenten im beruflichen Umfeld eingesetzt werden. Die hiesige Untersuchung analysiert insbesondere, inwieweit der Schutz von Geschäftsgeheimnissen als risikobasiert einzuordnen ist sowie welche

---

5 Veil, ZD 2018, 9 (13); Raji, ZD 2020, 279 (281 f.); Schröder, ZD 2019, 503 (503).

6 Veil, ZD 2018, 9 (13); Raji, ZD 2020, 279 (281 f.).

7 Vgl. die Darstellung des Gesetzgebungsprozesses in Bezug auf den risikobasierten Ansatz bei Schröder, ZD 2019, 503 (503 f., 505 f.); vgl. daneben Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmman DSGVO, Einleitung Rn. 225, 227; Hornung/Spiecker gen. Döhmman, in: Simitis/Hornung/Spiecker gen. Döhmman DSGVO, Einleitung Rn. 277.

8 Vgl. Partsch/Rump, NJW 2020, 118 (119 ff.); Dorner, in: Schuster/Grützmacher, IT-Recht, § 2 GeschGehG Rn. 38 f.; Ohly, GRUR 2019, 441 (443 f.).

9 Lauck, GRUR 2019, 1132 (1132); Schuster, CR 2020, 726 (729); Gola, DuD 2019, 569 (570).