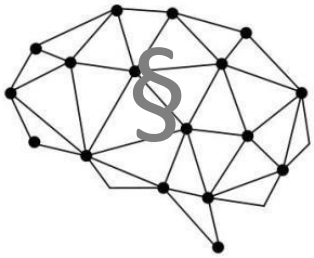
Introduction to the law of

Artificial Intelligence

by

Thomas Söbbing and
Alexander Schwarz



1st edition
(as of August 2025)

Ka Chapter overview

Introduction

A. Algorithms

B. Machine learning

C. Generative AI

D. Hallucination

E. Data protection

F. AI-VO

G. Autonomous driving

H. Liability

I. Embedded law in artificial intelligence

CHAPTER OVERVIEW **4**

OUTLINE **5**

INTRODUCTION AND DISTRIBUTION **10**

PURPOSE OF THE WORK **11**

THE AUTHORS OF THIS WORK **15**

A. ALGORITHMS **16**

I. TRANSFORMATION OF THE ALGORITHM 18
1. Decision tree *1*
2. Algorithm as a mathematical formula *21*
3. Pseudocode *2*
4. Source code *24*
II. COPYRIGHT (§ 69A URHG) 25
1. Scope of protection of Section 59a (1) UrhG *25*
2. Draft material *2*
3. Source code *30*
4. Influence of AI on coding *31*
5. Summary *33*
III. DISCRIMINATION BY ALGORITHMS 35
1. Art. 3 GG – "Principle of equality" *35*
2. Prohibition of discrimination *3C*
a) Applicability of Section 19 (1) No. 2 AGG 37
b) Prerequisite of Section 19 (1) No. 2 AGG 39
c) Exceptions pursuant to Sections 3, 20 AGG 39
3. Result *41*
IV. ALGORITHMIC TRADING (ALGO TRADING) 44
1. Legal basis *45*
a) Algorithmically controlled trading 45
b) High-frequency trading 47
c) stock exchange supervision 52
2. Summary *55*

B. MACHINE LEARNING **56**

I. BASIC ELEMENTS OF MACHINE LEARNING 56
II. HOW MACHINE LEARNING WORKS 57
III. HOW DEEP LEARNING AND ARTIFICIAL NEURAL NETWORKS WORK 60
VI. LEGAL PROTECTION FOR MACHINE LEARNING 64
1. Protection for the creation of an artificial neural network *C5*
a) Patent protection for KNN 65
b) Copyright protection as a work 66
c) Copyright protection as a database 67
2. Protection for the results of machine learning ..... *CS*
a) Data 70
b) Trade secrets 71
c) Summary 73
V. COPYRIGHT LIMITATIONS FOR MACHINE LEARNING 74
1. Introduction *74*
2. Legal basis *75*
3. Stock photography and AI – LG Hamburg *77*
4. Legal issues arising from this *82*
a) Actions relevant to copyright law 83
b) Section 44b UrhG Text and data mining 85
c) Text and data mining for scientific research purposes (§ 60d UrhG) 8

d) Summary ... 86

C. GENERATIVE AI ... 8

I. INTRODUCTION ... 88
II. HOW GENERATIVE AI WORKS IN TEXT FORM ... 89
III. IS THE OUTPUT OF LLMS GENIUS AND PROTECTED BY COPYRIGHT? ... 91
1. *Output as a human work?* ... S1
2. *Creation of complex prompts* ... S3
3. *Copyright protection for prompts* ... S4
4. *Selection of responses* ... S4
IV. IS THE OUTPUT OF LLMS A TRADE SECRET? ... 95
1. *Prerequisite § 2 GeschGehG* ... S5
a) Economic value, cf. § 2 (1) lit. a GeschGehG ... 95
b) Confidentiality measures, cf. § 2 (1) lit. b GeschGehG ... 96
c) Legitimate interest in confidentiality, see Section 2 (1) (c) GeschGehG ... 96
2. *Summary with reference to the GeschGehG* ... S7
IV. SUMMARY ... 98

D. HALLUCINATION ... GG

I. DEFINITION ... 99
II. LEGAL ASSESSMENT ... 100
1. *Material defect vs. product defect* ... 100
a) Material defect in the purchase agreement ... 100
b) Material defect in the contract for work and services ... 106
c) Product defect ... 107
2. *Decision of the Regional Court of Kiel* ... 108
III. SAAS MODELS FOR AI ... 110
1. *Definition* ... 111
2. *Duplication* ... 112
3. *Making available to the public* ... 115
4. *Summary* ... 118

E. DATA PROTECTION ... 11

I. DOES MACHINE LEARNING VIOLATE THE GDPR? ... 11
1. *Initial situation* ... 11
2. *Processing within the meaning of Art. 4 (2) GDPR* ... 12
a) Collection ... 12
b) Recording ... 124
c) Organize and arrange ... 124
d) Read and query ... 124
e) Comparison and linking ... 125
3. *Lawfulness of processing* ... 125
4. *Controller* ... 130
5. *Summary* ... 131
II. WHAT DATA PROTECTION ISSUES ARISE IN AUTOMATED (AI) DECISION-MAKING? ... 132
1. *Introduction* ... 132
2. *Proceedings before the Administrative Court of Wiesbaden (Case No. C-534/21)* ... 134
3. *Opinion of the Advocate General* ... 135
4. *Decision of the ECJ* ... 13
a) First question ... 138
b) Second question ... 147
c) Evaluation ... 148
5. *Outlook* ... 150

F. AI REGULATION ... 153

I. OVERVIEW OF THE AIREGULATION ... 153
1. *Scope and definitions* ... 153
2. *Prohibited practices in the field of AI* ... 154

3. *High-risk AI systems* ... 154
a) Classification as high-risk systems ... 155
b) Requirements for high-risk AI systems ... 1655

4. *Transparency requirements for certain AI systems* ... 15C
5. *AI models for general use* ... 15C
5 *Measures to promote innovation* ... 15
7. *Governance* ... 157
8. *EU database for high-risk systems* ... 158
9. *Monitoring and reporting obligations* ... 158
10. *Codes of conduct* ... 15S
11. *Delegation of authority and exclusion procedure* ... 15S
12. *Sanctions* ... 15S
13. *Final provisions* ... 1C0

II. TRANSPARENCY OBLIGATIONS PURSUANT TO ART. 52 AIREGULATION ... 16
1. *AI system* ... 1C1
2. *High-risk AI systems* ... 1C2
3. *Art. 52 AI Regulation* ... 1C4
b) Text of Art. 52 of the AI Regulation ... 164
c) Recitals ... 165
4. *Analysis of transparency obligations* ... 1C7
a) Traceability and comprehensibility ... 167
b) Identity and contact details of the provider ... 168
c) Purposes and areas of application ... 168
d) Training data ... 168
e) Performance, accuracy, and robustness ... 168
f) Risk assessment and mitigation ... 16
g) Verifiability and interpretability ... 169
h) Conditions of use ... 169
i) Problem and risk management ... 169
5. *Summary* ... 1CS

III. CONTRACT DRAFTING IN LIGHT OF THE AI REGULATION ... 171
1. *Introduction* ... 171
2. *Content and significance of Art. 25(4) AI Regulation* ... 172
a) Fundamentals of Art. 25(4) of the IC Regulation ... 172
b) Contractual obligations pursuant to Art. 25(4) of the IC Regulation ... 173
c) Consideration of Annex III of the IC Regulation ... 17
3. *Comparison with data processing agreements pursuant to Art. 28 GDPR* ... 17
a) Order processing pursuant to Art. 28 GDPR ... 174
b) Some key elements of an AVS are ... 175
c) Some key differences and parallels ... 175
4. *Contract design for AI systems* ... 177
a) General requirements ... 177
b) Providers of AI systems ... 177
(1) On the procurement side ... 17
(2) On the distribution side ... 17
c) Operators of AI systems ... 179
(1) Procurement for own use ... 179
(2) Procurement with modifications ... 179
5. *Summary* ... 180

IV. QUALITY MANAGEMENT IN ACCORDANCE WITH KI-VO ... 182
1. *Introduction* ... 182
2. *Overview of the requirements of Art. 17 AI Regulation* ... 18
a) Objective and structure ... 183
b) Obligation to introduce a quality and risk management system ... 184
c) Minimum requirements for the management system ... 18
3. *Relationship to other regulatory obligations (in particular Art. 9 AI Regulation – risk management)* 18C
4. *ISO 42001:2023 – AI Management System* ... 187
a) Structure and objective of the standard ... 187
b) Requirements for planning, implementation, monitoring, and continuous improvement ... 18

c) Potential for conformity with Art. 17 AI Regulation ... 18
5. *ISO 9001:2015 – Quality management systems* ... 150
a) Fundamentals and scope ... 190
b) Relevance for the quality requirements of Art. 17 AI Regulation ... 19
c) Strengths and limitations of ISO 9001 in the context of AI ... 191
C. *ISO 27001:2022 – Information security management* ... 17

a) Protection of information security as a compliance factor ... 192
b) Reference to Art. 17 AI Regulation with regard to risk management and documentation ... 193
c) Potential for supplementing ISO 42001 and ISO 9001 ... 193
7. *Assessment of the combination of standards for compliance with Art. 17 AI Regulation* ... *154*
a) Synergies between ISO 42001, ISO 9001, and ISO 27001 ... 19
b) Gaps and specific requirements of the AI Regulation ... 19
c) Legal assessment: Is certification sufficient to fulfill regulatory requirements? ... 196
8. *CEN/CENELEC JTC21* ... *157*
a) Development of harmonized standards in accordance with Art. 40 AI Regulation ... 197
b) Implementation of the requirements of Art. 17 AI Regulation through ISO/IEC 42001, 23894, and 5338 ... 199
c) EN ISO/IEC 42001 – Management systems for artificial intelligence ... 199
aa) EN ISO/IEC 23894 – Risk management for AI systems ... 2
bb) EN ISO/IEC 5338 – AI lifecycle management ... 20
3. *Summary* ... *20*
V. AI GOVERNANCE ... 204
1. *Responsibility and accountability* ... *204*
2. *Transparency and documentation requirements* ... *204*
3. *Risk and security management* ... *205*
4. *Establishment of ethics and integrity standards* ... *205*
5. *Implementation in the governance tool* ... *20*
VI. CRITICISM ... 20
1. *Complexity and legal uncertainty* ... *208*
2. *Administrative burdens and costs* ... *208*
3. *Impact on innovation capacity* ... *208*
4. *Bureaucratic hurdles and enforcement problems* ... *20*
5. *Conclusion* ... *20*
G. AUTONOMOUS DRIVING ... 21
I. LEVELS OF AUTOMATION ... 210
1. *Level 0 – Driver only* ... *210*
2. *Level 1 – Assisted* ... *211*
3. *Level 2 – Partially automated* ... *21*
4. *Level 3 – Highly automated* ... *213*
5. *Level 4 – Fully automated* ... *214*
II. BEHAVIORAL REGULATIONS ... 214
1. *Vienna Convention on Road Traffic* ... *214*
a) European registration law – ECE regulations ... 215
b) StVO ... 216
2. *Requirements according to StVG* ... *218*
a) Driver liability according to § 18 StVG ... 218
b) Liability of the keeper pursuant to Section 7 StVG ... 219
c) Limits of liability ... 221
d) Motor vehicles with highly or fully automated driving functions, Section 1a StVG ... 221
e) Rights and obligations when using highly/fully automated driving functions, Section 1b StVG ... 225
f) Data processing with highly or fully automated driving functions, Section 63a StVG ... 227
g) Driverless parking, Section 6 (1) No. 14a StVG ... 227
III. POSSIBLE CLASSIFICATIONS OF ARTIFICIAL INTELLIGENCE ... 229
H. LIABILITY ... 234
I. DIRECTIVE ON AI LIABILITY ... 234
1. *Scope* ... *235*
2. *Burden of proof and liability relief* ... *235*
a) Disclosure obligations ... 235
b) Presumptions regarding causality ... 235
3. *Relationship to product liability* ... *23C*
4. *Objectives of the Directive* ... *23C*
5. *Criticism and challenges* ... *23C*
5 *AI Regulation (AI-VO) AI Liability Directive* ... *237*
II. MANUFACTURER LIABILITY ... 238
1. *Manufacturer obligations* ... *23*
2. *Product monitoring obligations* ... *240*
3. *Reaction obligations* ... *2*[8]*43*
4. *Recall obligations* ... *243*

5. Burden of proof ... *244*
5. Tortious liability ... *24C*
a) **Intent** ... 24
c) **Negligence** ... 249
d) Product liability / Product Liability Directive ... 251
e) AI as vicarious agent ... 257
f) Maintenance contracts ... 257
g) Obligations and technical standards ... 259
h) Types of damage ... 262
i) Limitation of liability ... 272
j) Third-party property rights ... 282
k) Liability for deep learning ... 283
III. OPERATOR LIABILITY ... 284
1. Breaches of duty ... *284*
a) Fault ... 288
b) Analogy to animal owner liability ... 289
c) Submission of declarations of intent ... 293
IV. AI AS A VICARIOUS AGENT ... 299
V. CREDIT RISK ... 300
VI. AI WITH ITS OWN LEGAL PERSONALITY ... 302

I. EMBEDDED LAW IN ARTIFICIAL INTELLIGENCE ... **307**

I. INTRODUCTION ... 307
II. PRACTICAL EXAMPLE: HR PROCESS ... 309
III. PRACTICAL EXAMPLE OF AUTONOMOUS DRIVING ... 316
IV. EMBEDDED LAW ... 31
V. APPLICATION OF THE SUPER CODE ... 320
VI. CONSCIENCE ... 321

J. BIBLIOGRAPHY ... **324**

K. INDEX ... **336**

Introduction and Distribution

In recent years, artificial intelligence (AI) law has become one of the most dynamic and challenging fields of legal scholarship. Between technological disruption, regulatory ambition, and ethical uncertainty, new questions are emerging that are difficult to capture in traditional legal categories—yet still require precise legal analysis. This book, *Introduction to Artificial Intelligence Law*, provides readers with a structured and practical introduction to this complex and interdisciplinary subject.

We have decided to publish this work as a paperback book through a publishing house affiliated with Bedey & Thoms Media GmbH, Hermannstal 119k, 22119 Hamburg, Germany, or to make it available for free download as a PDF file, as this will allow for wider distribution and enable us to respond more quickly to changes in this rapidly evolving area of law. We would be very grateful for constructive feedback from readers and would even depend on it. It would also be great if readers would consider making a donation of at least 30 euros to an association that I (Thomas Söbbing) hold in high esteem instead of paying for this book when downloading it for free:

Step by Step e. V. Münster

https://www.stepbystep-muenster.de The

account details are as follows:

Volksbank Münsterland Nord eG IBAN: DE51
4036 1906 0013 0761 00 BIC: GENODEM1IBB

The association and the people behind it are doing a truly remarkable job, and have been doing so for over 30 years.

The aim of the (AI Law) work

The authors aim to lay a sound legal foundation while systematically introducing the legal issues necessary for a basic understanding of AI regulation. Precisely because the work is intended as an "introduction," a conscious decision was made to refrain from an in-depth examination of sector-specific topics such as algorithmic trading (algo trading), AI in medicine, or in a military context. Such questions go beyond the scope of an introductory approach and require specialized monographs.

Instead, this book starts where the legal discourse still needs to find its footing: at the intersection between technology and norms, between methodological uncertainty and the formation of legal systems. What makes this work unique is its conceptual approach of bringing a preliminary legal order to a technical phenomenon that has thus far largely eluded a fixed definition. It thus offers access not only to students and lawyers without specific technical knowledge, but also to practitioners and researchers seeking orientation in a complex field. The systematic structure of the book allows readers to gain both an overview and a deeper understanding of specific issues. The main content of each chapter is summarized below:

Chapter A: Algorithms

The work begins with the legal classification of algorithms, the basic element of many AI systems. It becomes clear that the legal treatment of the concept of algorithms reaches structural limits: the various forms of representation—from decision trees to mathematical formulas to source code—cannot be uniformly defined in legal terms. The section therefore highlights the various options for protection, particularly in copyright law (Section 69a of the German Copyright Act (UrhG)), and discusses the relationship to trade secrets and the issue of algorithmic discrimination. The chapter concludes with a brief digression on algorithmic trading.

Chapter B: Machine learning

This chapter focuses on machine learning (ML) as the technical backbone of many modern AI systems. The authors clearly explain the basic principles of ML and how it differs from deep learning and artificial neural networks.

The legal section deals with issues relating to the protection of such systems – copyright, patent law, database law, and trade secret law.

Chapter C: Generative AI

This chapter deals with current developments in generative AI—in particular large language models (LLMs)—and their legal implications. It focuses on questions such as: Is the output of AI protected by copyright? Who is the author of prompts? Does the generated content constitute a trade secret? The authors also address current disputes regarding the copyright quality of works and evaluate the practical handling of AI-generated content. Text and data mining also play a central role in the context of Sections 44b and 60d of the German Copyright Act (UrhG).

Chapter D: Hallucination

The phenomenon of AI hallucinations—i.e., factually incorrect or invented outputs—is examined in terms of its relevance under civil law. The legal assessment is based on the categories of material defects and product defects, as well as from the perspective of sales and contract law. SaaS models for AI and their copyright implications are also discussed here.

Chapter E: Data protection

One of the central areas of AI regulation is data protection. This chapter provides an in-depth analysis of the data protection relevance of ML systems, particularly under the GDPR. It examines whether the training of AI constitutes the processing of personal data, how Article 6 GDPR applies, and what roles "controllers" play in this context. The chapter is supplemented by a detailed presentation of the ECJ decision C-634/21 on automated decision-making.

Chapter F: AI Regulation (AIoI)

This chapter marks the beginning of the regulatory core of the work. The authors systematically explain the central provisions of the AI Regulation, in particular those relating to high-risk systems, transparency obligations, governance requirements, and sanctions. A separate subchapter is devoted to contractual practice, in particular the relationship between Art. 25(4) AI Regulation and Art. 28 GDPR. The section on quality management (Art. 17 AI Regulation) examines in detail the requirements for management systems and sets out

the AI VO in the context of ISO 42001, ISO 9001, and ISO 27001. The chapter concludes with a critical analysis of the challenges facing companies—keywords: barriers to innovation and bureaucratization.

Chapter G: Autonomous driving

This section deals with the traffic law and liability law environment of autonomous driving. The various levels of automation are presented and compared with the current legal situation – in particular the Road Traffic Act (StVG) and Road Traffic Regulations (StVO). Issues of manufacturer and owner liability as well as data processing play a central role here.

Chapter H: Liability

The question of liability is one of the most controversial topics in AI legal doctrine. This chapter systematizes proposals for an AI liability directive, examines questions of burden of proof, product liability, and the role of AI as a vicarious agent. The specific responsibility of operators and maintenance contracts is also addressed.

Chapter I: Embedded law in AI

A particularly innovative chapter deals with the embedding of norms in AI systems ("embedded law"). Using practical examples—for example, in the HR context or in autonomous driving—it analyzes how regulatory requirements can be implemented technically. The "super code" and the idea of a "machine conscience" are also critically discussed.

Conclusion and value of the work

In this book, the authors succeed in presenting a multifaceted topic in a structured manner, thereby creating a legally sound basis for further discussion. The work is not merely a collection of individual aspects, but a coherent system that systematically explores the fundamentals, methods, and lines of conflict in AI law.

The decision to omit sector-specific special issues is conceptually consistent: it allows the basic architecture of the legal debate on AI to be exposed—and this is precisely where the book's strength lies. Readers are given access

that has not been available in legal literature to date: interdisciplinary information, legal differentiation, and a clear didactic structure.

As an introduction, the work is aimed not only at students, but also at practitioners who want to systematically explore AI law for the first time. Its clear language, high academic standard, and didactic clarity make it an indispensable reference point in the German-language discourse on artificial intelligence law.

Authors of this work published by the German Law and Technology Association

Prof. Dr. Thomas Söbbing, LL.M. (HHU)

teaches civil law with a focus on digital economy law at the University of Applied Sciences Kaiserslautern and has a research assignment on legal issues relating to artificial intelligence.

Alexander Schwarz

is a judge at the Palatinate Higher Regional Court in Zweibrücken and a lecturer at the University of Applied Sciences Kaiserslautern.

Special thanks go to our research assistant Janina Penth, LL.B., for her active support.

Disclaimer

The statements made here reflect solely the private opinions of the authors.

A. Algorithms[1]

Basically, an algorithm is universally applicable and describes a method for solving a task, possibly with the aid of a computer. This fairly simple definition describes the problem very well when it comes to legal assessment. This is because the criteria for legal assessment are too vague. Algorithms can take many different forms and be presented in many different ways. The lack of mathematical precision in the concept of algorithms bothered many mathematicians and logicians in the 19th and 20th centuries, which is why a whole series of approaches were developed in the first half of the 20th century with the aim of arriving at a precise definition. Formalizations of the concept of computability include the Turing machine (Alan Turing), register machines, lambda calculus (Alonzo Church), recursive functions, Chomsky grammars (see Chomsky hierarchy), and Markov algorithms.

Although algorithms have been around for a very long time, their legal status is not clearly defined. This is undoubtedly linked to the question of what an algorithm actually is. The lack of clarity stems from a rather vague definition, according to which an algorithm is a methodical calculation procedure for solving a problem. In general, an algorithm is also understood to be the solution to a specific task, whereby elementary processing steps are the key to the result. Since there are few special standards for artificial intelligence (AI) and algorithms in particular, we are heavily reliant on analogies or the interpretation of other standards. For example, people often look to copyright law, which, with the special standard of Section 69a of the German Copyright Act (UrhG), could also offer protection for algorithms through interpretation.

AI companies invest a great deal of money in the creation of complex algorithms, and so the entire AI industry is asking itself how it can protect its investments. This is currently evident in the United States and the

[1] See also Algorithms and copyright protection CR 2020, 223–228.

planned (partial) sale of the TikTok platform. In addition to the political (power) issues, a particular difficulty arises from the special value of the platform's algorithm. In artificial intelligence systems[2] and algorithms in particular, a distinction must be made between the different elements involved in their development.[3]

It can generally be assumed that an algorithm alone cannot initially be registered as a patent, even in its various forms (see II.2 – II.5), because abstract or intellectual methods are not patentable, cf. Section 1 (2) and (3) PatG and Article 52 (2) and (3) EPC. The Federal Patent Act generally refers to "algorithms as such" in contrast to "algorithms with technical content" [4]. An algorithm can generally enjoy the protection of the Trade Secrets Act if its creators ensure that the requirements of Section 2 of the Trade Secrets Act are met. However, the result is unsatisfactory, as the possibilities for exploitation are not the same as for copyrighted works (e.g., those under Section 31 UrhG). There is therefore a strong desire for algorithms to enjoy copyright protection.

The error in the legal assessment of algorithms to date lies in the assumption that algorithms have a fixed form[5], that the definitions provided by scientists (especially data scientists) are very general (see above) and that they are difficult to capture in legal terms. However, there are very different forms of algorithms (see II.2 – II.5), which must therefore also be considered differently from a legal perspective. This differentiated approach must be taken in particular in the context of Section 69a (1) and (2) UrhG. According to Section 69a (1) UrhG, computer programs within the meaning of this Act are programs in any form, including design material. According to Section 69a (1)

2 See, for example, *Stiemerling*, *O.* in: CR 2015, p. 762, for various forms.

3 *Antoine*, *L.* in: CR 2019, pp. 1–8.

4 BPatG, GRUR 1996, 866; GRUR 2015, 983 marginal no. 27.

5 *Söbbing*, *T.*: Fundamental Legal Issues of Artificial Intelligence, 1st edition 2019, pp. 11–14.

According to Section 1 UrhG, the protection granted applies to all forms of expression of a computer program (see III.), which also includes design material (see IV.2) and source code (see IV.3). However, according to Section 69a (1) sentence 2 UrhG, ideas and principles underlying any element of a computer program, including the ideas and principles underlying the interfaces, are not protected.

Thus, an algorithm could obtain copyright protection within the meaning of Section 69a UrhG if the respective form of the algorithm can be classified as design material or source code.

I. Transformation of the algorithm

Algorithms can be represented in various forms. These range from mathematical formulas to programs tailored specifically to a machine. This is because algorithms can be easily implemented in computer programs (known as compiling), which then execute algorithms automatically.[6] An algorithm thus undergoes a certain transformation during its life cycle [7] (see Fig. 1). It always starts with the problem (1). To visualize the problem, a decision tree (2) can be created. The decision tree is implemented either in pseudocode (3) or in a mathematical formula, e.g., a Euclidean algorithm (4). This formula or pseudocode is used to generate source code (5), which is then transformed by a compiler into a computer program (6), resulting in the final outcome (7).

6 https://de.serlo.org/informatik/baustelle/algorithmen-ist-algorithmus, accessed on March 3, 2020.

7 *by Rimscha*, *M.*: Algorithms compact and understandable – Solution strategies on the computer, 4th edition 2017, p. 3.

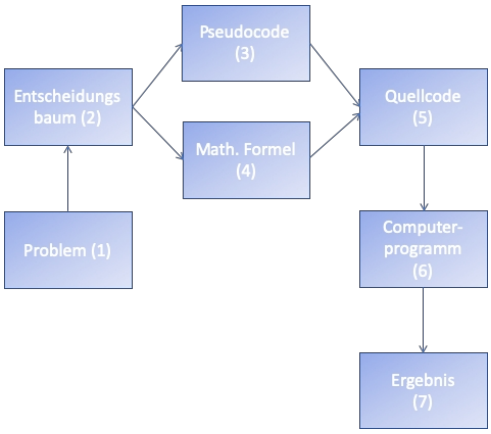


Fig. 1: Transformation of an algorithm

1. Decision tree

Decision trees can be used as a tool to develop algorithms, but this is not essential. Decision trees visualize abstract problems and make them easier for people to understand. A classic decision tree used in computer science to explain how algorithms work is the decision tree for the chances of survival when the Titanic sank (Fig. 2).[8] It analyzes which groups on the Titanic had what chances of survival when it sank on April 15, 1912:

[8] *Zweig, K.*: Ein Algorithmus hat kein Taktgefühl (An algorithm has no sense of rhythm), 1st edition 2019, p. 140 ff.

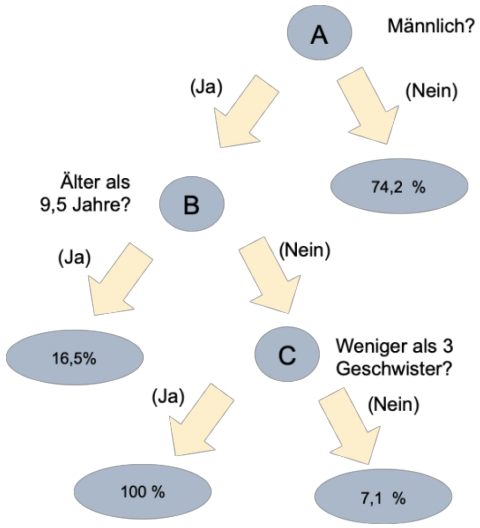


Fig. 2. Decision tree

The first question (A) in the decision tree is whether the person who was on board the Titanic was male or female. If the person was female, their chance of survival was 74.2%, because 233 out of 314 women survived. The second question (B) deals with whether the male person was older than 9.5 years, in which case the chance of survival was 16.5%. This is because only 90 of the 545 men survived. Third question (C): If the male was not older than 9.5 years and had fewer than three siblings, the chances of survival were 7.1%, because one in 14 children survived. If the child had more than three siblings, the chances of survival were 100%, because 18 children out of 18 children with more than three siblings survived.[9]Of course, the values could be completely different if another ship sank. But that is not the point of this example, because the decision tree is merely a template to explain how a decision tree works in principle. However, it is clear here that it is always crucial to identify the appropriate question. Without this, the

[9] The websitewww.kaggle.com/c/titanic (last accessed on March 3, 2020) provides the complete data set for this accident.

Decision tree leads to comprehensible results, but without any gain in knowledge.

2. Algorithm as a mathematical formula

The representation of algorithms in mathematical formulas is a very common method. An example of this is the Euclidean algorithm, which originates from the mathematical subfield of number theory.[10] It will therefore be used in the following for legal considerations as a representative of a generally mathematically represented algorithm. A Euclidean algorithm can be used to calculate the greatest common divisor of two natural numbers. The method is named after the Greek mathematician Euclid, who described it in his work "The Elements." [11]

The greatest common divisor of two numbers can also be determined from their prime factorizations. However, if the prime factorization of neither number is known, the Euclidean algorithm is the fastest method for calculating the greatest common divisor. The Euclidean algorithm can be applied to more than just natural numbers. It can also be used to calculate the greatest common divisor of two elements of any Euclidean ring. These include, for example, polynomials over a field. [12]

In a Euclidean algorithm, the repeated subtractions of a value that occur in the classic algorithm are replaced by a single division with remainder. The modern Euclidean algorithm now performs such a division with remainder in each step. It starts with the two numbers: [13]

$A = a_1 * r_0 + r_1$

[10] Wikipedia, keyword "Euclidean algorithm," accessed on February 29, 2020.

[11] The method was probably not invented by *Euclid*, as he summarized the findings of earlier mathematicians in his "Elements." Mathematician and historian *Bartel Leendert van der Waerden* suspects that Book VII is a textbook on number theory already used by the Pythagoreans.

[12] From: *Euclid*, The Elements, edited by *Thaer*, *C.*, 1st edition 2011, § 2

[13] Wikipedia, keyword "Euclidean algorithm," accessed on February 29, 2020.

In each subsequent step, the divisor and the remainder from the previous step are used to perform another division with remainder. This is repeated until a division is possible, i.e. the remainder is zero:

$r_0 = q_2 * r_1 + r_2$ $r_0 = q_3 * r_1 + r_3$

.

.

.

$r_{n-1} = q_{n+1} * r_n + 0$

The divisor r_m of the last division is then the greatest common divisor: $ggT(a,b) = r_m$

Since the numbers are at least halved in every second step, the method is extremely fast even with large numbers. [14]

This general example shows that the Euclidean algorithm can be understood as an abstract or intellectual method that makes use of mathematical functions.

3. Pseudocode

The decision tree is only used to visualize an algorithm. The decision tree is, of course, not yet code that could be used by a computer to solve problems.

As a necessary intermediate step in the transformation between a mathematical formula, such as that of the Euclidean algorithm or a decision tree, and

[14] Wikipedia, keyword "Euclidean algorithm," accessed on February 29, 2020.

a computer program code requires what is known as pseudocode. Pseudocode is a program code that is not intended for machine interpretation, but merely serves to illustrate a paradigm or algorithm. It usually resembles higher-level programming languages, mixed with natural language and mathematical notation. Pseudocode can be used to describe a program sequence independently of the underlying technology. It is therefore often more compact and easier to understand than real program code.[15] A program can be specified using pseudocode. However, this should be avoided, as formulating pseudocode is already a programming activity that distracts from the requirements. [16] Converting the decision tree from II.2 into pseudocode would result in the following code:

```
START
Input male= 1 Input
female= 2
---------------------------------------------------------------------------
REM "Basic question male or female" IF Input = 1
THEN #2
ELSE #1
---------------------------------------------------------------------------
END
---------------------------------------------------------------------------
#1 REM "female"
  PRINT "Survival chance 74.2%" END
---------------------------------------------------------------------------
#2 REM "male"
  IF Input &lt;/= 9.5 years THEN
          PRINT "Survival rate 16.5%"
```

[15] *Mehlhorn, K. / Sanders, P.*: Algorithms and Data Structures, 2008, p. 26.

[16] *Siedersleben, J.* (ed.): Software Engineering, Hanser, 2003, p. 44 ff.

```
    ELSE
        IF Input &lt;/= 3 Siblings THEN PRINT
        "Survival chance at 7.1%"
    ELSE
        PRINT "Chance of survival 100%"
END
```

```
END
```

All words in capital letters have a corresponding function, and words in lower case contain a variable unless they are enclosed in quotation marks and therefore only have a descriptive function.

The decisive factor in pseudocode is that this form of representing an algorithm is very close to actual program code.

4. Source code

Software consists of source code that causes a machine (computer) to execute certain commands.[17] Source code, also known as program code, is the human-readable text of a computer program written in a programming language. Viewed abstractly, the source code for a program can also be described as software documentation that describes the program so precisely and completely that it can be translated automatically by a computer into machine language.[18] As already described above, pseudocode and source code do not differ greatly in their representation.

[17] *Antoine, L.* in: CR 2019, pp. 1–8.

[18] Wikipedia, keyword "source code," accessed on March 1, 2020.

Possession of the source format includes the possibility of editing and modifying a program and thus the risk of uncontrollable piracy: Anyone who has the source format of a program can remove all references to the author, in particular copyright notices and serial numbers, and make extensive changes to the program structure. For this reason, the user is generally only provided with the program in object format; otherwise, they would be disclosing the IT expertise contained in the program and exposing it to uncontrollable further use. [19]

II. Copyright (§ 69a UrhG)

For legal protection under the UrhG, the difference between source code for software and an algorithm for AI is of considerable importance. This raises the question of whether an algorithm could be regarded as source code for a computer program and thus be eligible for copyright protection.

1. Scope of protection under Section 69a (1) UrhG

The computer program is protected by copyright in accordance with the provisions of Sections 2 and 69a of the German Copyright Act (UrhG). According to Section 2 I No. 1 UrhG, a computer program is classified as a literary work. [20] The analogy to a literary work is particularly apt in relation to the program code itself. [21] Natural language also has a fixed set of rules in the form of grammar, which must be followed in order to formulate a correct and comprehensible sentence. In programming this is the syntax of the programming language used [22] There are countless ways to write program code to implement a function. These possibilities are determined by the syntax of the programming language, the available technical infrastructure, the operating system, third-party programs, conventions, and

19 *Hoeren, T.* in: CR 2004, 721–724.

20 Federal Court of Justice, judgment of March 3, 2015 – I ZR 111/02, GRUR 2005, 860 (861)= MMR 2005, 845 (846) – Fa-sh 2000; Higher Regional Court of Frankfurt, judgment of January 27, 2015 – 11 U 94/13, GRUR 2015, 784 (787)= ZUM 2015, 497 (501) – Object code; Loewenheim in Schricker/Loewenheim, Copyright 5th ed. Edition 2017, Section 2, para. 143 with further references

21 *Hoeren/Wehkamp,* CR 2018, 1-7.

22 See Deselby, Journal of dyslexic programming 13 (2017), 131 ff.;

Style guidelines restricted. [23] The design of the code is decisive here, as an individual act must exist as a prerequisite for copyright protection for software. [24]

Furthermore, a very fine distinction must be made, because according to Section 69a (1) UrhG, software is also eligible for copyright protection with regard to its specific form of expression—in contrast to the ideas and principles underlying the program and the functionalities of a computer program.[25] According to these provisions, protection extends to computer programs in any form, including design material, cf. Section 69a (1) and (2) UrhG, while "ideas and principles" which – according to the wording of the law – "underlie an element of a computer program" are expressly excluded from copyright protection under Section 69a (2) sentence 2 UrhG. [26] The ECJ has ruled in its decisions
"BSA" [27] and "SAS Institute" [28] specify the scope of protection of Article 1 of the Software Directive. This includes the expressions of a computer program and the design material that can lead to the reproduction or subsequent creation of a computer program.[29] The expression of a computer program is protected from the moment its reproduction would result in the reproduction of the computer program and could thus cause the computer to perform its function.[30] Protection thus applies to the program as such, i.e., to "a sequence of instructions which, when incorporated in a machine-readable medium, is capable of causing a machine with information-processing capabilities to perform a specific function or task

23 *Hoeren/Wehkamp,* CR 2018, 1-7.

24 *Hoeren/Wehkamp,* CR 2018, 1-7.

25 *Hetmank*, *S. / Lauber-Rönsberg*, *A.* in: GRUR 2018, p. 574.

26 OLG Cologne, April 8, 2005 – 6 U 194/04= GRUR 2005, p. 863 (Ls.), GRUR-RR 2005, p. 303, K&R 2006, p. 43.

27 ECJ, judgment of 22.12.2010 – C-393/09= CR 2011, p. 221 (222) – BSA.

28 ECJ, judgment of May 2, 2012 – C-406/10, CR 2012, p. 428 – SAS Institute with note by *Heymann*.

29 ECJ, judgment of 22.12.2010 – C-393/09, CR 2011, p. 221 (222) – BSA, margin note 37; ECJ, judgment of May 2, 2012 – C-406/10, CR 2012, p. 428 – SAS Institute, para. 37. Reference also made by the Swedish court of first instance, Svea Hovrätt, decision of March 4, 2018 – PMT 22–17 (in S w e d i s h): http://www.patentochmarknadsoverdomstolen.se/Domstolar/pmod/2018/Svea%20HR%20PMT%2022-17%20Ej%20slut-ligt%20beslut%202018-04-03.pdf (last accessed on 10 December 2018), see margin note 19.

30 ECJ, judgment of 22 December 2010 – C-393/09, CR 2011, p. 221 (222) – BSA, para. 38.

or displays, executes, or achieves a specific result."[31] Although the term "computer program" is to be understood broadly, it only applies to functions based on electronic data processing. It includes, for example, operating systems, application programs, macros, search engines, source code, and individual program parts. Furthermore, according to the explicit wording of the law in Section 69a (1) UrhG, draft material is also protected, but this also only refers to IT materials. This includes all preliminary stages, such as flowcharts or other preliminary and intermediate stages of programmdevelopment.[32] In contrast, tasks and specifications for the programmer that lie outside the scope of IT, such as ideas and principles underlying a computer program, are not covered by copyright protection under Sections 69a et seq. UrhG. In particular, the idea of developing a program to solve a specific task is not covered by Section 69a UrhG. Therefore, only the form as the concrete expression of a work is protected, not the content of the work. [33] This means that, according to this provision, the author can only be the person who implements certain tasks developed by himself or specified to him by a third party in a computer program. In contrast, the person who sets the task, i.e., who specifies the requirements that the program must fulfill, possibly in great detail, is not simultaneously the author of the program. This follows from the fact that the provisions of Sections 69a et seq. UrhG only protect computer programs as such as subject to copyright and thus refer to the fact that the persons concerned own intellectual creation is expressed precisely as a computer program (Section 69a (3) UrhG). However, someone who has not performed any programming work on their own responsibility cannot be a co-author of a computer program. This also applies if their intellectual preparatory work made the success of the programming activity possible in the first place.

31 cf. *Dreier*, *T.* / *Schulze*, *G.*: Urheberrechtsgesetz (Copyright Act), 2nd edition, Section 69a, margin number 12.

32 Dreier, *T.*: Copyright, 2nd edition, § 69a, margin number 14.

33 cf. OLG Karlsruhe, GRUR 94, p. 726, 729 – "Bildschirmmasken" (screen masks); *Dreier,* T. / *Schulze,* G. op. cit., margin no. 20; *Schricker,* G. / *Löwenheim,* U .: Urheberrecht (Copyright Law), Section 69a, margin no. 12; *Möhring,* P. / *Nicolini,* K.: Urheberrechtsgesetz (Copyright Law), 2nd edition, Section 69a, margin no. 9.

2. Draft material

For design material, it is largely unclear when and until when protection should apply. [34] In previous legal practice, this did not seem to play a major role because there were few legal disputes about it.[35] Recital 7 of the Software Directive[36] refers to design material only "in so far as the nature of the preparatory work allows the subsequent creation of a computer program." According to the wording, the decisive factor is that the design material must be suitable or sufficiently developed to enable a computer program to be written in code form on its basis.[37] It can be concluded that, in order to be protected as design material, there must be sufficient technical proximity to the program in code form. [38] Technical specifications and program requirements, such as data flow diagrams and program flowcharts, as well as rough and detailed technical specifications, are eligible for protection as design material.[39] The requirements specified therein relate directly to the creation of the program, so that there is sufficient proximity to it – even if it is questionable whether coding is possible on this basis alone.[40] It can therefore be concluded that design material exists from the point in time at which it is possible to write a program on the basis of this material. Once a stage of development has been reached at which control commands are converted into code form and thus fulfill the definition of a program, it is no longer design material but the program itself. [41]

If you apply this insight to the different forms of an algorithm,

34 *Antoine*, *L.* in: CR 2019, pp. 1–8.

35 Exception: OLG Cologne, April 8, 2005 – 6 U 194/04= GRUR 2005, p. 863 (Ls.); GRUR-RR 2005, p. 303; K&R 2006, p. 43.

36 Directive 91/250/EEC of May 14, 1991, replaced by the consolidated version as Directive 2009/24/EC of April 23, 2009 on the legal protection of computer programs, hereinafter referred to as "Software Directive."

37 *Grützmacher*, *M.* in: *Wandtke*, *A.* / *Bullinger*, *W.*: UrhG, 4th edition 2014, Section 69a, margin number 7; *Schneider*, *J.* in: *Schneider*, *J.*: Handbuch EDV-Recht, 5th edition 2017, G. margin number 79; *Karl*, *C.*: Der urheberrechtliche Schutzbereich von Computerprogrammen (The scope of copyright protection for computer programs), 2009, p. 191 et seq.; cf. *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5th edition, 2017, Section 69a, margin number 5.

38 Taking into account the view of the Federal Court of Justice: *Antoine*, *L.* in: CR 2019, p. 1–8.

39 Federal Court of Justice, judgment of May 9, 1985 – I ZR 52/83, CR 1985, p. 22 – Inkassoprogramm; *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5th ed. 2017, § 69a margin no. 5; see also *Schneider, J.* in: *Schneider, J.*: Handbuch EDV-Recht, 5th ed. 2017, G margin no. 117.

40 *Antoine*, *L.* in: CR 2019, pp. 1–8.

41 *Antoine*, *L.* in: CR 2019, pp. 1–8.

then first of all, the decision tree as presented does not constitute draft material for a later computer program. According to Section 69a (2) sentence 2 UrhG, ideas and principles underlying an element of a computer program, including the ideas and principles underlying the interfaces, are not protected. The characteristics of the decision tree have not yet reached the stage of development where control commands can (already) be implemented in code form. At least not without further intermediate steps being necessary. The situation is different if the decision tree has already reached a level of quality such that it can be considered a program flow chart, e.g., in accordance with DIN 66001 or ISO 5807. Such program flow charts are certainly protected as draft material under Section 69a (1) and (2) sentence 1 UrhG.[42] In the case of decision trees, therefore, the individual case is very important.

When an algorithm is represented by a mathematical formula, it is highly unlikely that program code can be generated without further (major) intermediate steps. There is insufficient technical proximity to the program in code form. Thus, the representation of an algorithm in the form of a mathematical formula is not sufficient to qualify as design material eligible for copyright protection under Section 69a (1) of the German Copyright Act (UrhG).

In contrast, pseudocode can clearly be regarded as draft material, as it has reached a stage of development that is sufficient for it to be converted into code form for control commands. Due to its form as a programming language, pseudocode is already very close to the actual program code/source code.

[42] Federal Court of Justice, judgment of May 9, 1985 – I ZR 52/83, CR 1985, p. 22 – Inkassoprogramm (collection program); *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5th ed. 2017, § 69a, margin no. 5; see also *Schneider, J.* in: *Schneider, J.*:Handbuch EDV-Recht, 5th ed. 2017, G margin no. 117.

[43] Taking into account the view of the Federal Court of Justice: *Antoine*, *L.* in: CR 2019, pp. 1–8.

The source code (II.5) does not need to be categorized as draft material, as according to Section 69a (1) UrhG, computer programs within the meaning of this Act are programs in any form. This also includes source code. [44]

3. Source code

As already explained above, source code also falls within the scope of protection of Section 69a (1) UrhG. It is questionable whether the pseudocode described, as a method of making an algorithm comprehensible, deserves protection under Section 69a (2) sentence 1 UrhG by comparison with source code.

Given the wording "all forms of expression" (cf. Section 69a (2) UrhG), which also includes source code, for example, it is irrelevant that the software is executable. [45] This would in principle argue in favor of pseudocode being able to obtain protection comparable to that of source code. However, with regard to the concept of a program, the ECJ, referring to the functional purpose as the decisive criterion, bases its decision on a control element, which is in line with the understanding of national copyright law. [46] However it is precisely such "actual" control elements that are lacking in pseudocode, as it serves only to illustrate the algorithm. Pseudocode is more compact and easier to understand than real program code,[47] but it does not generate commands for a computer that actually result in the creation of an executable computer program. This is because, with regard to the program, the primary focus is on the control commands expressed in code form (in source or object code) as the object of protection.[48] Non-control-related elements should only be protected in accordance with general provisions. [49] Protection under general provisions may arise from

44 ECJ, May 2, 2012, C-406/10= CR 2012, 428.

45 *Schneider* in Schneider, Hdb. EDV-Recht, 5th ed. 2017, G. para. 54.

46 *Marly*, *J.*: GRUR 2011, p. 204 (207); see *Grützmacher*, *M.* in: *Wandtke*, *A.* / *Bullinger*, *W.*: UrhG, 4th ed. 2014, § 69a, margin note 3 with further references.

47 *Mehlhorn*, *K.* / *Sanders*, *P.*: Algorithms and Data Structures, 2008, p. 26.

48 According to the ECJ, source code and object code are merely examples of forms of expression, see *Marly*, *J.*: GRUR 2012, p. 773 (777 f.); *Loewenheim,* U. / *Spindler,* G. in: *Schricker,* G. / *Loewenheim,* U.: UrhG, 5th ed. 2017, § 69a, margin no. 10.

49 See *Lesshafft*, *K.* / *Ulmer*, *D.* in: CR 1993, p. 607 (608); see also *Marly*, *J.* in: GRUR 2011, p. 204 (207); cf. *Loewenheim,* U. / *Spindler,* G. in: *Schricker,* G. / *Loewenheim,* U.: UrhG, 5th ed. 2017, § 69a, margin no. 7, each ref. screen or user interfaces; see also ECJ, judgment of December 22, 2010 – C-393/09, CR 2011, p. 221 (222) – BSA.

show that pseudocode as draft material (see III.2) falls within the scope of protection of Section 69a (2) sentence 1 UrhG.

It can therefore be concluded that the representation of an algorithm in the form of pseudocode does not deserve the protection of Section 69a (2) sentence 1 UrhG if this protection is to arise from the comparability with the source code.

4. Influence of AI on coding

Artificial intelligence (AI) has profoundly changed the way software is developed in recent years. Enormous progress has been made, particularly in the field of code generation: Modern tools such as GitHub Copilot (developed by GitHub and OpenAI), Amazon CodeWhisperer, and ChatGPT can generate complete functions or code suggestions based on natural language or simple comments in the code. They not only analyze the immediate context, but also draw on extensive training data to make relevant and syntactically correct suggestions.

A particular advantage of these tools lies in the automation of so-called boilerplate tasks. These are repetitive and often mechanical programming tasks, such as writing setters and getters, creating REST API endpoints, or generating simple unit tests and validation logic. These processes can be significantly accelerated or completely automated with the help of AI-based tools, giving developers more time for creative and conceptual tasks.

AI systems also promote the spread of low-code and no-code platforms. Such platforms make it possible to create complex applications largely without traditional programming. User interfaces, databases, and automation processes can be configured using drag-and-drop or simple commands. This trend democratizes software development by enabling people without in-depth technical expertise to

to develop digital solutions. At the same time, this development brings new challenges, especially in terms of code quality, maintainability, and security.

Overall, it can be said that AI-supported tools are by no means making programming in the traditional sense obsolete – but they are changing fundamental processes, shifting skill requirements, and opening up new forms of human-machine collaboration.

The copyright assessment of AI-generated code focuses on the question of whether such products are personal intellectual creations within the meaning of Section 2 (2) of the German Copyright Act (UrhG). German copyright protection is centrally linked to the individuality and creative work of a natural person.[50] Only works that are an expression of a person's personal intellectual achievement can be protected by copyright. A machine performance – even if it formally falls within the definition of a work under Section 2(1) UrhG (in this specific case: linguistic works, including computer programs pursuant to Section 69a UrhG) – does not satisfy this requirement.

AI systems such as GitHub Copilot, ChatGPT, and Amazon CodeWhisperer operate on the basis of statistical pattern recognition in large text or code corpora. The generative act—i.e., the concrete selection, combination, and formulation of code components—is performed autonomously by the system without human intervention in individual cases.[51] Although the user provides the prompt, this input is usually limited to general instructions ("Write a function to convert Celsius to Fahrenheit"). There is therefore no personal creative decision on the part of the human being with regard to the concrete expression of the work.

[50] See *Dreier/Schulze*, UrhG, 7th ed. 2022, § 2 Rn. 41 ff.; *Wandtke/Bullinger*, Urheberrecht, 6th ed. 2022, § 2 Rn. 100: "The prerequisite is always an individual intellectual act by a human being."

[51] For more details, see: *J. Ohly*, "Maschinelles Lernen und Urheberrecht – Wer schafft was?" (Machine learning and copyright – Who creates what?), GRUR 2021, 25 (28 f.); and *M. Leistner*, "Generative AI and Copyright," GRUR 2023, 665

The prevailing opinion in the literature and previous German case law consistently emphasize that a personal intellectual creation within the meaning of Section 2 (2) UrhG requires individual freedom of choice in the design, which must not consist merely in the act of operation.[52] The mere use of technical aids (e.g., word processing, IDEs) does not preclude the protectability of the result—in contrast to the complete delegation of the design decision to a machine, as is typically the case with AI-generated code.

Therefore, according to the current legal situation, it must be concluded that

- AI-generated source code is not to be regarded as a work within the meaning of Section 2(2) UrhG due to the lack of human creative effort and is therefore not protected by copyright.
- In the absence of individual design decisions, the AI user does not acquire authorship of the generated code unless he or she makes substantial creative modifications (Section 3 UrhG).
- AI itself cannot be the holder of copyrights due to its lack of legal personality[53]

As a result, AI-generated code is generally available in the public domain, at least under German copyright law, unless there is human involvement that goes beyond purely technical control and reveals an individual creative influence.

5. Summary

In summary, it can be said that algorithms may or may not enjoy copyright protection depending on their different forms.

[52] BGH GRUR 1982, 37 – Inkasso-Programm; BGH GRUR 2015, 1189 – Pippi-Langstrumpf-Kostüm; LG Frankfurt a.M., judgment of July 17, 2023 – 2-06 O 52/23 (not legally binding, see GRUR-RS 2023, 19044).

[53] See also the EU Commission Communication on AI and intellectual property, COM(2020) 760 final, p. 7: "Legal capacity and authorship can only be attributed to natural persons.

Thus, the representation of an algorithm in the form of a simple decision tree will not generally enjoy copyright protection. The situation is different if the decision tree already has the quality of a program flowchart. In the case of a mathematically represented algorithm, such as the Euclidean algorithm, copyright protection cannot be assumed. On the other hand, the representation of an algorithm in pseudocode can certainly be assumed to be protected by copyright, even if this cannot be inferred from its comparability to the source code, but enjoys copyright protection as design material.

III. Discrimination by algorithms[54]

"Discrimination" refers to the disadvantage or denigration of groups or individuals based on certain values or on the basis of unreflective, sometimes unconscious attitudes, prejudices, or emotional associations.[55] Discrimination based on factors that can be influenced by the person concerned (access to educational institutions, income level, social behavior) tends to be more accepted or tolerated than factors that cannot be changed by the individual and are triggers for discrimination (ethnicity, gender, disability, age, or sexual preferences).[56] In general, the following applies, as expressed by the Federal Constitutional Court on the application of the principle of equality under Article 3 of the Basic Law: "The general principle of equality under Article 3(1) of the Basic Law requires the legislature to treat things that are essentially the same equally and things that are essentially different unequally."[57]

1. Art. 3 GG – "Principle of equality"

Article 3(1) of the Basic Law contains the general principle of equality, which obliges the state to treat all people equally. According to Article 3(1) of the Basic Law, all people are equal before the law. Unlike most other fundamental rights, Article 3(1) of the Basic Law does not protect a specific sphere of freedom from state interference. This is based on the fact that this fundamental right is not a right to freedom, but a right to equality. Its guarantee therefore only arises from a comparison of several situations with regard to their treatment by the state. Article 3(1) of the GG obliges the state to treat equal situations equally.[58] Citizens can use this fundamental right to defend themselves against unequal treatment in court.

---

54 See also *"The fairy tale of the evil algorithm or legal issues relating to discrimination by artificial intelligence (AI),"* Söbbing RTLaw 2020, 62–69.

55 *Epping*, *V.*: Grundrechte (Fundamental Rights), 7th edition 2017, margin number 770.

56 *Weise*, *P.*; *Brandes*, *W.*; *Eger*, *T.*; *Kraft*, *M.*: Neue Mikroökonomie (New Microeconomics), Physica, Heidelberg 2005, p. 22.

57 BVerfGE 98, p. 365 (385).

58 BVerfGE 42, p. 64 (72): Compulsory auction.

The equality provisions of Article 3(1) of the Basic Law are, according to Article 1(3) of the Basic Law, initially binding only on the three branches of government: the executive, the legislature, and the judiciary. It is questionable whether this fundamental right has been violated in the application of the insurance algorithm, as the three branches of government were not involved in this process. This is because the wording of Article 3(1) of the Basic Law, according to which equal treatment only applies before the law, is generally considered to be too narrow.[59] It is argued that, according to prevailing opinion, equality rights also apply between private individuals. Although this is not directly bound by fundamental rights, Article 3 of the Basic Law, as a constitutional norm, influences the application of subordinate legal provisions, such as civil law, through case law in court proceedings.[60] This indirect third-party effect means that the essential statements of Article 3 of the Basic Law find their way into private law, in particular in the interpretation of undefined legal concepts. This would amount to an obligation on the part of the state to interfere with the rights of private individuals. This would contradict the fact that Article 3 of the Basic Law is not directly binding on private individuals.[61] However, it does demonstrate the state's obligation to ensure that its citizens are treated equally, as this is a fundamental right of citizens in a democracy. Nevertheless, no specific right of defense against the application of the insurance algorithm can be derived from Article 3 of the Basic Law.

2. Prohibition of discrimination

In Germany, the General Equal Treatment Act (AGG)[62] is the central law that aims to prevent and eliminate "discrimination on grounds of race or ethnic origin, gender, religion or worldview, disability, age or sexual identity" (Section 1 AGG). The specific prohibitions of discrimination in Article 3(3) of the Basic Law are not entirely identical to those in the General Equal Treatment Act: For example

[59] *Jarass, H.*: Art. 3, margin note 1b. In: *Jarass*, *H.*; *Pieroth*, *B.*: Basic Law for the Federal Republic of Germany, Commentary, 28th edition, C. H. Beck, Munich 2014.

[60] *Heun*, *W.*: Art. 3, margin note 70–71. In: *Dreier*, *H.* (ed.): Grundgesetz Kommentar: GG. 3rd edition. Volume I: Preamble, Articles 1–19. Tübingen, Mohr Siebeck 2013

[61] *Kischel, U.*: Art. 3, margin note 91. In: Beck'scher Online-Kommentar GG, 34th edition 2017

[62] , Federal Law Gazette I, p. 1897 (2006)

Article 3(3) of the Basic Law prohibits discrimination on the basis of a person's geographical origin, but the AGG does not.

a) Applicability of Section 19(1)(2) AGG

According to Section 19 (1) No. 1 AGG, discrimination on the grounds of race or ethnic origin, gender, religion, disability, age, or sexual identity in the establishment, implementation, and termination of civil law obligations that typically arise without regard to the person under comparable conditions in a large number of cases (mass transactions) or in which the reputation of the person is of secondary importance according to the nature of the obligation and which arise under comparable conditions in a large number of cases. This means that discrimination on the grounds mentioned above is prohibited in the establishment, implementation, and termination of civil law obligations relating to private insurance pursuant to Section 19(1)(2) AGG. This specific application to private insurance arose in parts of the implementation of the so-called "Gender Directive"[63] and the "Anti-Racism Directive"[64]. No. 2 also covers private insurance and thus also insurance relationships that are structured according to individual risk indicators,[65] including occupational pension schemes.[66] If Nos. 1 and 2 are relevant, No. 2 takes precedence as the more specific provision. [67]

The provision in Section 19 1 No. 2 AGG naturally conflicts with freedom of contract. It is guaranteed by the general freedom of action in Article 2 (1) GG. Its expression through the principle of private autonomy is set out in

63 Council Directive 2004/112/EC of 13 December 2004 on the implementation of the principle of equal treatment between men and women in the access to and supply of goods and services, including housing, OJ EC L 373, p. 37.

64 Council Directive 2000/43/EC of June 29, 2000, implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ EC L 180, p. 22.

65 BTDrs 16/1780, p. 42.

66 BAG NZA-RR 10, 664 [BAG 18.03.2010 – 6 AZR 434/07].

67 *Prütting*, *H.*; *Wegen*, *G.*; *Weinreich*, *G.*: BGB Commentary, AGG § 19 AGG – Civil law prohibition of discrimination, margin number 7.

68) BVerfGE 8, p. 274 – see margin note 212.

protected under German civil law,[69] but may be restricted by mandatory provisions of applicable law, statutory prohibitions or if it violates public policy.[70] Thus the application of Section 19(1)(2) AGG does not violate Article 2(1) GG.

In this context, the question arises as to why the legislature chose to regulate the issue of "private insurance" in particular in No. 2. One reason for this is that private insurance differs from all other types of contract covered by the general prohibition of discrimination in Section 19 AGG in one fundamental respect for the application of the law: Unlike so-called "Mass transactions" (Section 19 (1) No. 1 AGG) are contracts that are designed from the outset to differentiate between different risk characteristics. [71]These risk characteristics are often personal; accordingly, the characteristics are often linked to the criteria protected by the AGG, such as gender or age. The legislature recognizes such differentiations as so important for the proper functioning of insurance contracts that it even makes them binding on insurers in some cases. This is particularly clear in Section 12 (1) No. 1 of the Insurance Supervision Act (VAG). According to this provision, age- and gender-based pricing is mandatory in substitute health insurance (insurance that replaces statutory insurance).[72] This was also taken into account in EU legislation; the Official Journal of the EU[73] states that Member States may decide before December 21, 2007, to allow proportional differences in premiums and benefits if the consideration of gender is justified by relevant and accurate actuarial and statistical data.

69 BVerfGE 95, p. 267 – see margin note 142.

70 BVerfGE 8, p. 274 – see margin note 212.

71 *Armbrüster*, *C.*: Prohibition of discrimination and grounds for justification in the termination of private insurance, expert opinion prepared on behalf of the Federal Anti-Discrimination Agency, May 2010, p. 6.

72 *Armbrüster*, *C.*: Prohibition of discrimination and grounds for justification in the termination of private insurance, expert opinion prepared on behalf of the Federal Anti-Discrimination Agency, May 2010, p. 7.

73 , OJ EU, L 373/41 Art. 5 (2).

Risk assessment is a determining factor. The differentiating nature of private insurance is also recognized by the legislators who drafted the AGG. According to the government's explanatory memorandum, the inclusion of this type of contract in the AGG's prohibition of discrimination is therefore intended solely to protect against arbitrariness, against unequal treatment without objective justification.[75] This is not intended to make differentiation based on the individual risk assessed ex ante impossible. The various grounds for justification provided for in Section 20 (2) AGG specifically for insurance contracts offer scope for such risk differentiation. [76]

b) Prerequisite of Section 19 (1) No. 2 AGG

As already explained above, pursuant to Section 19 (1) No. 2 AGG, discrimination on grounds of gender and age is prohibited in the establishment of civil law obligations relating to private insurance.

According to the insurance algorithm described in Section I, men older than 9.5 years would not be insured. Men (boys) younger than 9.5 years and with more than three siblings would also not be insured under the insurance algorithm. By linking "male" and "have more than three siblings," the discriminatory factors of gender and age would be included in the decision of the insurance algorithm. The legal consequence would be, according to Section 19 (1)(2) AGG, that such a decision would not be permissible in the first instance.

c) Exceptions under Sections 3 and 20 of the General Equal Treatment Act (AGG)

A deviation from the prohibition of discrimination laid down in Section 19 (1) No. 2 AGG is permissible under certain conditions specified in Sections 3 and 20 AGG

---

74 Government statement, BT-Drucks. 16/1780, p. 45; see also OLG Saarbrücken, VersR 2009, p. 1522 (1525).

75 BVerfGE 91, p. 118 (123).

76 *Armbrüster, C.*: Prohibition of discrimination and grounds for justification in the termination of private insurance, expert opinion prepared on behalf of the Federal Anti-Discrimination Agency, May 2010, p. 8.

Requirements permissible. According to Art. 20 (1) AGG, there is no violation of the prohibition of discrimination if there is an objective reason for different treatment on the grounds of religion, disability, age, sexual identity, or gender. Paragraphs 1–4 list a number of examples. With regard to gender-based unequal treatment, Section 20 (2)

S. 1 AGG largely reproduces the wording of Art. 5 (2) of the Gender Directive. [77] According to this, different treatment on grounds of sex in relation to bonuses and benefits is only permissible if the consideration "is a determining factor in a risk assessment based on relevant and accurate actuarial and statistical data." This suggests, first of all, that the European legal requirements of the Gender Directive—unlike those of the Anti-Racism Directive[78] with regard to the characteristic of race/ethnic origin—expressly permit gender-based differentiation.[79] The wording of Section 20 (2) sentence 1 AGG raises the question of its scope of application. The wording refers only to different treatment "in relation to premiums or benefits." However, the complete refusal to conclude a contract should also be covered by Section 20 (2) sentence 1 AGG.[80] A complete refusal of insurance cover by rejecting or terminating a contract hits those willing to take out insurance harder than a contract term that discriminates against them. [81] The insurer cannot be forced to offer insurance in the case of a very high risk if the risk proves to be uninsurable from an actuarial point of view. However, in the case of a

77 Council Directive 2004/112/EC of December 13, 2004, on implementing the principle of equal treatment between men and women in the access to and supply of goods and services, including housing, OJ EC L 373, p. 37.

78 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ EC L 180, p. 22.

79 *Armbrüster*, *C.*: Prohibition of discrimination and grounds for justification in the termination of private insurance contracts, expert opinion prepared on behalf of the Federal Anti-Discrimination Agency, May 2010, p. 11.

80 *Ambrosius*, *B.* in: *Däubler*, *W.*; *Bertzbach*, *M.*: AGG, 2nd edition 2008, Section 20, marginal number 40; cf. already *Armbrüster*, *C.* in: *Begemann*, *M.*; *Bruns,* A. (eds.): Die Versicherung des Alterns (Insurance for Old Age), 2008, p. 43, 49 (in the context of disability); dissenting opinion MünchKomm-BGB/Thüsing, 5th edition 2007, Section 20 AGG marginal number 55: justification possible under paragraph 1; *Schiek,* D. in: *Schiek,* D.: AGG, 2007, § 20 margin note 8; *Rödl,* F. in: *Rust,* U .; *Falke,* J.: AGG, 2007, § 20 margin note 26 f.: no justification possible.

81 *Ambrosius*, *B.* in: *Däubler*, *W.*; *Bertzbach*, *M.*: AGG, 2nd edition 2008, Section 20, margin number 40; cf. already *Armbrüster*, *C.* in: *Begemann*, *M.*; *Bruns,* A. (eds.): Die Versicherung des Alterns, 2008, p. 43, 49 (in the context of disability); dissenting opinion MünchKomm-BGB/Thüsing, 5th ed. 2007, § 20 AGG margin no. 55: justification possible under para. 1; *Schiek,* D. in: *Schiek,* D.: AGG, 2007, Section 20 marginal no. 8; *Rödl,* F. in: *Rust,*
U. *Falke*, *J.*: AGG, 2007, Section 20 marginal no. 26 et seq.: no justification possible at all.

Contract rejection must be measured against the strict justification requirements of Section 20 (2) sentence 1 AGG and not merely against those of Section 20 (1) sentence 1 AGG. Unless it concerns bonuses, benefits, or a contract rejection, the justification for unequal treatment can be based on Section 20 (1) sentence 1 AGG.[82] Accordingly, it is sufficient if there is an objective reason for the unequal treatment, for example with regard to obligations or goodwill arrangements. The justification criteria of Section 20 (2) sentence 1 AGG are clearly not tailored to such cases.

3. Result

It can therefore be concluded that the result of the insurance algorithm for passengers of the Titanic II in its current form, namely the pure decision to issue or not to issue an insurance offer, would be inadmissible.

Pursuant to Section 21 (1) sentence 1 AGG, the party disadvantaged by the insurance algorithm may, in the event of a violation of the prohibition of discrimination, demand the elimination of the disadvantage, without prejudice to further claims. If further disadvantages exist, the party may seek injunctive relief pursuant to Section 21 (1) sentence 2 AGG. In the event of a violation of the prohibition of discrimination, the discriminating party is obliged to compensate for the damage caused in accordance with Section 21 (2) AGG. This does not apply if the discriminating party is not responsible for the breach of duty. The disadvantaged party may demand appropriate compensation in money for damage that is not financial loss. Such a claim must be asserted within a period of two months in accordance with Section 21 (5) AGG. After expiry of this period, the claim can only be asserted if the disadvantaged party was prevented from meeting the deadline through no fault of their own.

The claims under Section 21 AGG would lapse if the insurance algorithm were expanded to include the following provisions: Instead of the options OFFER /

[82] In this respect, see MünchKomm-BGB/Thüsing (fn. 22), Section 20 AGG marginal no. 55; see also Offenburg Regional Court, judgment of November 13, 2009 – 3 O 82/09 (unpublished), reprinted judgment, p. 9.

NO OFFER, a calculation would be made for a higher insurance premium. As shown in Section II No. 2, the result of this extended insurance algorithm would again be permissible:

```
START
Input male= 1 Input
female= 2
---------------------------------------------------------------------------
REM "Basic question male or female" IF Input = 1
THEN #2
ELSE #1
---------------------------------------------------------------------------
END
---------------------------------------------------------------------------
#1 REM "female"
  PRINT "Survival rate 74.2%" OFFER
(premium + risk surcharge) END
---------------------------------------------------------------------------
#2 REM "male"
  IF Input &lt;/= 9.5 years THEN
          PRINT "Survival rate 16.5%" OFFER (premium +
          risk surcharge)
  ELSE
          IF Input &lt;/= 3 siblings THEN PRINT
          "Survival chance 7.1%" OFFER (premium + risk
          surcharge)
  ELSE
          PRINT "Survival chance 100%" OFFER
          (premium without risk surcharge)
END
```

END

IV. Algorithmic trading (algo trading)

BaFin has commissioned a study on the effects of algorithmic securities trading.[83] According to the study big data and artificial intelligence (referred to as BDAI by BaFin) are bringing about profound change, and successful implementations of BDAI can spread rapidly in a self-reinforcing manner. The combination of analytics and massively available data allows new insights to be gained. These can also be used in the financial system for product and process innovations. Such innovations could have a disruptive effect on existing value creation processes. As a result, new providers (e.g., fintechs) may enter the market and established business processes and market structures may change. Supervision and regulation must address innovative developments at an early stage. When considering the application of BDAI in the financial services industry, three central groups of providers are distinguished:

- Traditionally active companies (incumbents), in particular supervised companies such as banks and insurers
- Comparatively young, technology-oriented providers with specific functions, some of which are directly supervised (fintechs, insurtechs, regtechs, legaltechs)
- Large, globally active technology companies (big tech companies), most of which are not yet subject to supervision

Large amounts of data are available, together with powerful hardware and market-ready data analysis and processing technologies. Technology companies have proven that the use of BDAI can deliver significant

[83] BDAI study: Big data meets artificial intelligence. Challenges and implications for the supervision and regulation of financial services. https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html, accessed on December 17, 2018.

Competitive edge. Consequently, more and more capital is flowing into big data solutions and AI-using companies, such as fintechs. [84]

1. Legal basis

Algorithmically controlled trading and high-frequency trading are sometimes mentioned together. While high-frequency trading is all about speed, algorithmically controlled trading is about being smarter than other market participants.

a) Algorithmically controlled trading

In principle, an investment firm must comply with the organizational obligations under Section 25a (1) and Section 25e of the German Banking Act (Kreditwesengesetz) and the additional obligations under Section 80 (1) sentence 2 of the German Securities Trading Act (Wertpapierhandelsgesetz) (WpHG). These essentially comprise security measures, e.g., organizational or IT security obligations.[8 5] Additional obligations arise in the case of algorithmically controlled securities trading. According to Section 80 (2) sentence 1 WpHG, an investment firm must also comply with the provisions set out in Section 80 (2) sentence 1 WpHG if it trades in financial instruments in such a way that a computer algorithm automatically determines the individual order parameters. However, this does not apply if the system is used only to transmit orders to one or more trading venues, to process orders without determining order parameters, to confirm orders, or to process executed orders after trading (algorithmic trading). In this context, it should be noted that, pursuant to Section 80 (2) sentence 2 WpHG, order parameters within the meaning of

P. 1 In particular, decisions include whether to initiate the order, as well as

the timing, price or quantity of the order, or how the order will be processed after its entry with limited or no human intervention. Since January 3, 2018, new rules have applied to investment firms.

[84] BDAI study: Big data meets artificial intelligence. Challenges and implications for the supervision and regulation of financial services. https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html, accessed on December 17, 2018.

[85] *Voigt*, *P.*: Other industry-specific regulations on IT security. In: *Voigt*, *P.*: IT Security Law, 1st edition 2018.

Disclosure requirements arising from the implementation of the Financial Market Directive[86] by the Second Financial Market Amendment Act. According to this, investment firms are subject to these disclosure requirements if they engage in algorithmic trading within the meaning of Section 80 (2) sentence 1 WpHG (version dated January 3, 2018) or if they offer direct electronic access (DEA) to a trading venue in accordance with Section 2 (30) WpHG (version dated January 3, 2018). On the one hand, the notifications must be submitted to the authority responsible for supervising the securities service providers concerned. On the other hand, the notifications must also be forwarded to the authorities responsible for supervising the trading venues concerned. [87]

Therefore, investment firms are required to notify BaFin in the following cases:

- The investment firms are supervised by BaFin and offer a DEA on a trading venue or engage in algorithmic trading. In this case, the reporting obligation arises from Sections 77 (2) sentence 1 and 80 (2) sentence 5 WpHG (version of January 3, 2018).
- The investment firms are members or participants of a multilateral trading facility (MTF) or an organized trading facility (OTF) supervised by BaFin and offer a DEA on this MTF or OTF or conduct algorithmic trading there. In such cases, companies that are not subject to BaFin supervision may also be subject to the notification requirement. For these companies, the notification requirement may arise from the provisions of other EU member states that transpose Article 17 (2) subparagraph 1 and Article 17(5) subparagraph 3 MiFID II into national law.

According to Section 33 (1a) of the German Securities Trading Act (WpHG), investment firms that engage in algorithmic trading must have **adequate system and risk controls** in place for their trading systems. In addition, they must have effective contingency arrangements in place to deal with unexpected disruptions in their trading systems.

86 Markets in Financial Instruments Directive II – MiFID II

87 Algorithmic trading and high-frequency trading. BaFin communication, amended on December 13, 2017.

Furthermore, they must ensure that any change to a computer algorithm used for trading is documented in accordance with the regulations. The obligation to have appropriate system and risk controls in place also applies to capital investment companies and self-managed investment companies. [88]

On April 1, 2014, Eurex Exchange introduced the obligation to **identify** orders generated by algorithmic trading[89] and the trading algorithms used in each case ("algo flagging"). Specifically, these are:

- Orders and quotes generated by algorithmic trading within the meaning of Section 33 1a WpHG
- trading algorithms used
- the entire automated decision-making process[90]

The labeling of algorithms must be clear, consistent, and traceable and must cover all orders and quotes that are generated, modified, or deleted by systems and trading algorithms. "The labeling logic and technical input options are specified by the trading platforms and must be implemented in their IT systems. Trading participants, for their part, will analyze the various trading algorithms, assign them consistently, and perform any necessary cost-benefit calculations." [91]

b) High-frequency trading

The German Securities Trading Act (WpHG) defines high-frequency trading in Section 2 (8) No. 2 (d) as the purchase or sale of financial instruments on one's own account as a direct or indirect participant in a domestic organized market or a multilateral or organized trading system by means of a high-frequency algorithmic trading

88 Algorithmic trading and high-frequency trading. BaFin announcement, amended on December 13, 2017.

89 high-frequency algorithmic trading technique.

90 High-frequency trading – Regulatory framework and need for action on the part of exchanges and trading participants. Statement by Bea-ringPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_ Hochfrequenzhandel_final_web.pdf, accessed on October 24, 2018.

91 High-frequency trading – Regulatory framework and need for action by stock exchanges and trading participants. Statement by Bea-ringPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_

High-frequency trading_final_web.pdf, accessed on October 24, 2018.

technique within the meaning of paragraph 44, even without services for others (high-frequency trading). Furthermore, high-frequency trading is characterized under the WpHG by the fact that the individual parameters of the respective order are determined independently by the computer algorithm. The characteristics of the parameters are, for example, the time, price, or quantity of the order.

In order to counteract the risks associated with high-frequency trading, the legislator has taken action and enacted the Act on the Prevention of Risks and Abuse in High-Frequency Trading (Hochfrequenzhandelsgesetz – HFHG);[93]

it came into force in Germany on May 15, 2013. The law is intended to counteract the risks of high-frequency trading and close existing supervisory loopholes." "*Due to the inherent expansion of the German Banking Act (KWG), companies are now subject to a KWG licensing requirement as soon as they trade on their own account using high-frequency algorithmic trading techniques (algo tra-*

ding). [94]This obligation to obtain permission applies to both trading participants and trading venues. The law is based on European regulations on algorithmic trading and high-frequency trading, which are planned as a result of the revision[95] of the Financial Market[96] Directive Stock exchanges are required by the HFHG to ensure an appropriate ratio between order entries and the transactions actually executed by trading participants. In this context, the Eurex Exchange amended its exchange rules and introduced the order-to-trade ratio (OTR) including a transaction limit to be monitored on December 1, 2013.

[97] Under the HFHG, trading participants are required to ensure that order, quotes, and are and applied

[92] Algorithmic trading and high-frequency trading. BaFin announcement, amended on December 13, 2017.

[93] *Kindermann*, *Coridass*, ZBB 2014, p. 178; *Schultheiß*, WM 2013, p. 596; *Jaskulla*, BKR 2013, p. 221; *Kasiske*, WM 2014, p. 1933; *Mattig*, WM 2014, p. 1940.

[94] High-frequency trading – Regulatory framework and need for action on the part of stock exchanges and trading participants. Statement by Bea-ringPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_ Hochfrequenzhandel_final_web.pdf, accessed on October 24, 2018.

[95] Directive 2004/39/EC of the European Parliament and of the Council of April 21, 2004, on markets in financial instruments, amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC.

[96] Algorithmic trading and high-frequency trading. BaFin communication, amended on December 13, 2017.

[97] High-frequency trading – Regulatory framework and need for action by stock exchanges and trading participants. Statement by Bea-ringPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_

High-frequency trading_final_web.pdf, accessed on October 24, 2018.

Trading algorithm to be identified. Eurex Exchange therefore introduced "algo flagging" on April 1, 2014, which requires algorithms to be identified. [98]

Essentially, the HFHG contains the following provisions:

- System and risk controls
- Licensing requirement for high-frequency traders
- Appropriate order-transaction ratio
- Mandatory labeling
- Further provisions
-

According to the KWG, high-frequency trading **requires a license**. This licensing requirement applies to all direct and indirect trading participants in an organized market or multilateral trading facility (MTF) in Germany who trade using high-frequency algorithmic trading techniques and do not provide services to third parties. Such trading techniques are characterized by the use of infrastructure designed to minimize latency (e.g., collocation, proximity hosting), by the system's decision to initiate, generate, transmit, or execute an order without human intervention for individual trades or orders, and by a high volume of communications during the day. [99] With regard to risk management and own capital as well as reporting obligations to the supervisory authority, the licensing requirement entails certain obligations.

To maintain an appropriate relationship between order entries, modifications, and cancellations and the transactions actually executed by trading participants

[98] High-frequency trading – Regulatory framework and need for action by exchanges and trading participants. Statement by BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_ High-frequency trading_final_web.pdf, accessed on October 24, 2018.

[99] Algorithmic trading and high-frequency trading. BaFin announcement, amended on December 13, 2017.

(appropriate order-transaction ratio) Eurex Exchange introduced a mandatory order-transaction ratio (OTR) on December 1, 2013. This resulted in maximum limits for orders and quotes by trading participants, which are derived from the individual monthly trading volume of executed transactions in the respective financial instrument. The appropriate order-transaction ratio is defined as follows: [100]

$$OTR = \frac{\text{geordertes Volumen}}{\text{Volumenlimit}}$$

The volume ordered is the number of contracts in the order book that are generated by orders or quotes and accepted by the matching engine. Even contracts that a trading participant deletes from the matching engine and therefore does not execute are counted here. Changing an order is treated as deleting the previous order and then entering a new order. The volume limit includes a volume component and a basic exemption amount per financial instrument. The volume component is the number of trades executed per trading participant in the respective financial instrument, multiplied by a fixed volume factor per financial instrument. A basic exemption amount is set for each trading participant depending on their trading function – the basic exemption amount for market makers differs from that of other trading participants. The OTR limit of 1 is therefore intended to dynamically limit the order volume of trading participants, which must consequently always be reconciled with the actual transactions executed and the resulting change in the volume limit. Since an OTR greater than 1 at the end of a calendar month constitutes a violation of the HFG and adapted stock exchange regulations and is subject to sanctions,

[100] Eurex Circular 213/13 dated September 27, 2013.

Trading participants have no choice but to adapt their internal control and monitoring systems accordingly.[101]

In addition to the above provisions, the Act imposes **further obligations on trading venues**.

These relate to the levying of separate fees or charges for excessive use of exchange systems, the setting of an appropriate minimum price change and volatility interrupters. In addition, the law clarifies that trading practices involving computer algorithms may also constitute market manipulation under certain conditions. Furthermore, the law grants supervisory authorities powers to obtain information with regard to algorithmic trading.

The definition of high-frequency trading by direct and indirect trading participants has been specified by BaFin[103]: In addition to trading on own account, it specifies the validity of the following criteria:

- Independent trading decisions made by the system
- digital trading with a bandwidth of 10 gigabits per second and
- with at least 75,000 messages per trading day on average over the year

Because the KWG has been expanded to include the above criteria, all high-frequency traders fall under the supervision of BaFin; they therefore require a license pursuant to Section 32 KWG. *"The KWG licensing requirement for high-frequency traders thus triggers, among other things, obligations with regard to risk management, equity capital, and reporting to the supervisory authority. In particular, the capital and liquidity requirements of the KWG currently mean that proprietary traders will have to back their high-frequency algo trading with capital in the future."*[104]

---

101 High-frequency trading – Regulatory framework and need for action by stock exchanges and trading participants. Statement by Bea-ringPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, accessed on October 24, 2018.

102 Algorithmic trading and high-frequency trading. BaFin communication, amended on December 13, 2017.

103 Letter from BaFin dated May 21, 2013.

104 High-frequency trading – Regulatory framework and need for action on the part of exchanges and trading participants. Statement by Bea-ringPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, accessed on October 24, 2018.

Since January 3, 2018, the Second Financial Market Amendment Act has also imposed new reporting requirements on investment firms with regard to high-frequency trading. As with algorithmic trading, these requirements are based on the implementation of the Markets in Financial Instruments Directive II (MiFID II). Investment firms are subject to these reporting requirements if they engage in algorithmic trading within the meaning of Section 80 (2) sentence 1 WpHG (version of January 3, 2018), or if they offer direct electronic access (Direct Electronic Access – DEA) to a trading venue,[105] as is the case with high-frequency trading.

It is questionable whether the HFHG is still applicable following the implementation of Directive 2014/65/EU (MiFID II), as lex posterior (Latin for "*the newer law repeals the older law*") could well lead to the conclusion that MiFID II and its transposition into national law may have repealed the HFHG. However, there is no mention of this in the law or in the literature. The BaFin does recognize the requirements of MiFID II for algorithmic trading, but at the same time refers to the applicability of the HFHG. [106] It can therefore be assumed that the provisions of the HFHG must continue to be applied.

c) Stock exchange supervision

According to Section 26d (1) sentence 1 BörsG, the stock exchange must ensure that algorithmic trading systems do not impair or contribute to impairing orderly trading on the stock exchange. The provision in Section 26d BörsG was introduced by the Second Act Amending Financial Market Regulations Based on European Legal Acts (Second Financial Market Amendment Act – 2. FiMaNoG) [107] of June 23, 2017, and entered into force on January 3, 2018. This also implements the requirements of Art. 48 (4) MiFID II. In order to prevent the risks posed by algorithmic trading systems to orderly stock exchange trading, the stock exchange has

[105] Algorithmic trading and high-frequency trading. BaFin announcement, amended on December 13, 2017.
[106] Algorithmic trading and high-frequency trading. BaFin announcement, amended on December 13, 2017.
[107] Federal Law Gazette I, p. 1693.

pursuant to Section 26d (1) sentence 2 of the Stock Exchange Act (BörsG), to take appropriate precautions, including precautions to limit the ratio of unexecuted trade orders to executed trade orders in the event that the system capacity of the exchange is excessively utilized and there is a risk that the capacity limit will be reached. The regulation ensures that the stock exchange provides safeguards with regard to algorithmic trading, in particular high-frequency trading. This is based on concerns that this form of trading could, among other things, place a strain on the electronic systems of stock exchanges due to its volume and speed, thereby impairing stock exchange trading. In particular, the requirements for price inquiry and hybrid systems should be tailored to the nature, scale, and complexity of algorithmic trading.[108] With regard to the appropriate arrangements under paragraph 1 and the requirements for the design of the tests under paragraph 2, reference is made to Delegated Regulation (EU) 2017/584[109], as amended. The provisions are supplemented by Delegated Regulation (EU) 2017/584 (III). This contains, among other things, provisions on the testing of systems used by members (Article 8) and on their compliance with the systems of the respective trading venue (Article 9), as well as on the algorithms used by members (Article 10), as well as on preventive measures against market-disruptive trading conditions (Article 18), volatility control mechanisms (Article 19), and pre- and post-trade controls (Article 20). Algorithmic trading systems must not impair exchange trading (I). Since "contributing" is sufficient, it is not necessary for trading systems to be designed in such a way that they alone lead to trading disruptions. Rather, it is sufficient that they (only) impair trading in conjunction with other systems for the exchange to be required to take measures against them. The "appropriate arrangements" for this include the preventive measures against market-disruptive trading conditions listed in Art. 18 I Delegated Regulation (EU) 2017/584, e.g., upper limits on the number of orders that can be placed per second per member, mechanisms to control volatility (see also Art. 19 of the Regulation) and the pre-trade controls further specified in Art. 20 of Delegated Regulation (EU) 2017/584, e.g., price bands,

[108] Commission Delegated Regulation (EU) 2017/584 of July 14, 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organizational requirements for trading venues (OJ L 87, March 31, 2017, p. 350).

[109] Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organizational requirements for trading venues (OJ L 87, 31 March 2017, p. 350).

Maximum order values and volumes. [110] Since Article 18(1) of Delegated Regulation (EU) 2017/584 states that these measures must be taken "at least," all exchanges must introduce these precautions. ([111]) In addition, the ratio of unexecuted trading orders to executed trading orders must be determined in accordance with the provisions of Section 26a of the BörsG. Since these measures must be introduced "exclusively," the German legislature has made the introduction of this preventive measure mandatory. However, the details are left to the exchanges, which can set their own thresholds depending on their system capacity.[112] Under Article 2 of Delegated Regulation (EU) 2017/566, exchanges (trading venues) are required to calculate the ratio of unexecuted orders to transactions and to use the methodology set out in Article 3 of Delegated Regulation (EU) 2017/566 for this purpose. [113]

According to Section 26d (2) sentence 1 of the Stock Exchange Act (BörsG), trading participants are required to test their algorithms in an environment provided by the stock exchange. In accordance with Section 26d (2) sentence 1 BörsG, the management monitors compliance with the obligation under sentence 1 and reports any indications of violations to the stock exchange supervisory authority. These tests enable the stock exchange to examine the effects of the algorithms and adapt its precautions accordingly, if necessary also by not allowing a dangerous algorithmic trading program. Since the stock exchange must provide the environment, it cannot require trading participants to either create a test environment themselves or have their trading programs tested elsewhere. The exchange management monitors the tests and informs the exchange supervisory authority if any violations occur. [114]

110 *Groß* Kapitalmarktrecht: Kommentar zum Börsengesetz (Major Capital Market Law: Commentary on the Stock Exchange Act), 6th edition, 2016, Section 26d, margin numbers 1–4.

111 *Kasiske* WM 14, 1933, *Kindermann/Coridaß* ZBB 14, 178.

112 *Groß* Kapitalmarktrecht: Commentary on the Stock Exchange Act, 6th edition 2016, Section 26d margin number 1 et seq.

113 *Aldridge*, High-Frequency Trading, 2nd ed. 2013, *Gresser*, Praxishandbuch Hochfrequenzhandel, 2016, *Jaskulla* BKR 13, 221, *Kobbach* BKR 13, 233, *Schultheiß* WM 13, 596, *Kasiske* WM 14, 1933, *Kindermann/Coridaß* ZBB 14, 178.

114 *Groß* Kapitalmarktrecht: Commentary on the Stock Exchange Act), 6th edition, 2016, Section 26d, margin numbers 1–4.

2. Summary

With the provisions in the WpHG, the HFHG, the BörsG, and the BaFin guidelines, the legislature and the supervisory authorities have responded to algorithmic securities trading and created an appropriate legal framework. An interesting provision in this context is Section 26d (2) sentence 1 BörsG, which requires trading participants to test their algorithms in an environment provided by the stock exchange. It is questionable how this test will be designed in practice and how it will make the risks of algorithmic securities trading manageable.

B. Machine learning[115]

According to Wikipedia[116], machine learning (ML) develops, investigates, and uses statistical algorithms, also known as learning algorithms. Artificial neural networks (ANNs) are used in machine learning to create a complex learning structure whose goal is to enable intelligent behavior. A very practical example of such intelligent machines are autonomous vacuum robots, which use various sensors to learn how to explore a room and control the robot's motors based on what they learn. A similar method is also used in algorithmic securities trading. Information from various sources is collected, evaluated, and weighted, and the output can be, for example, the purchase or sale of a security. The creation of such learning and control mechanisms can be considered very complex and therefore involves high investments. Legal answers are needed to secure these investments and protect the creation of the KNN. As is often the case with new technologies, the legal answer is not as clear-cut as the developers of artificial intelligence (AI) systems would like it to be. The following article aims to help readers understand how KNN works in order to evaluate options for legal protection.

I. Basic elements of machine learning

Machine learning, which uses KNN, is an important application of AI and is already much more common today than one might think. One of the most prominent examples is the mobile phone, which learns what the owner's fingerprint or iris looks like in order to unlock the phone. If machine learning is carried out through multi-layered learning, deep learning, or in-depth learning, it is referred to as "deep learning."[117]

---

115 See also "Artificial neural networks: How AI learning structures should be viewed from a legal perspective" MMR 2021, 111

116 https://de.wikipedia.org/wiki/Maschinelles_Lernen

117 *Bruderer, H.*: Invention of the computer, electronic calculators, developments in Germany, England, and Switzerland. In: Milestones in Computer Technology. 2nd edition, completely revised and greatly expanded. Volume 2. De Gruyter, 2018, ISBN 978-3-11-060261-6; Glossary of terms relating to the history of technology, p. 408 (limited preview in Google Book Search, accessed on 23 November 2019).

Such "deep learning" is often illustrated in KNN. Deep learning models are primarily found in the fields of image, sequence, and speech recognition. AI applications can "enhance" photos and manipulate faces depending on the selected settings, for example, by replicating a smile.[119] In addition, deep learning systems can use algorithms to reverse the "pixelation" of certain images, which is usually done to protect privacy (e.g., on dating sites).[120] Background information such as metadata can also be automatically extracted from photos [121] to link similar products from shops, for example. [122]Furthermore, deep learning is successfully used in vehicle design (self-driving cars), in the financial world (stock price prediction, risk forecasting, automatic trading systems), in medicine (machine image recognition of carcinomas) and biology (genomics), in e-commerce (recommendation systems) and in the web environment (anomaly detection).[123]

II. How machine learning works

The general working method of machine learning is based more on heuristics. Heuristics (from the ancient Greek εὑρίσκω heurísko, "I find"; from εὑρίσκειν heu-rískein, "to find," "to discover") refers to the art of arriving at probable conclusions or practical solutions with limited knowledge (incomplete information) and little time.[124] It is astonishing how advanced the results generated in this way are. The following example by *Tariq Rashid* [125] shows how machine learning structures work in iteration loops. For example, an AI

118 https://www.heise.de/newsticker/meldung/KI-retuschiert-Smartphonefotos-in-Echtzeit-3792720.html, accessed on May 11, 2020.

119 https://www.heise.de/ct/ausgabe/2017-11-Kuenstliche-Intelligenz-macht-Bildbearbeitung-intuitiv-3705914.html, accessed on May 11, 2020.

120 See https://www.golem.de/news/google-brain-algorithmus-macht-ge-sichter-auf-schlechten-bildern-erkennbar-1702-126066.html, accessed on May 11, 2020; https://netzpolitik.org/2016/verpixelung-macht-unsichtbar-oder-doch-nicht, accessed on May 11, 2020.

121 http://t3n.de/news/facebook-ki-bilderkennung-chrome-781194/, accessed on May 11, 2020.

122 See https://www.heise.de/newsticker/meldung/eBay-Produkte-mithilfe-von-Fotos-suchen-und-kaufen-3784371.html, accessed on May 11, 2020.

123 *Heinz*, *S.*: Deep Learning – Part 1: Introduction, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, accessed on May 11, 2020.

124 *Gigerenzer*, *G.*; *Todd*, *P. M.*; ABC Research Group: Simple heuristics that make us smart. Oxford University Press, New York 1999.

125 *Rashid*, *T.*: Neuronale Netz selbst programmiert (Self-programmed neural networks), 1st edition 2017, p. 8.

System recognizes whether caterpillars or ladybugs are present. Such AI is also referred to as a predictor because it takes an input and makes a prediction about what the output should be. To refine this prediction in terms of heuristics, the internal parameters are adjusted.

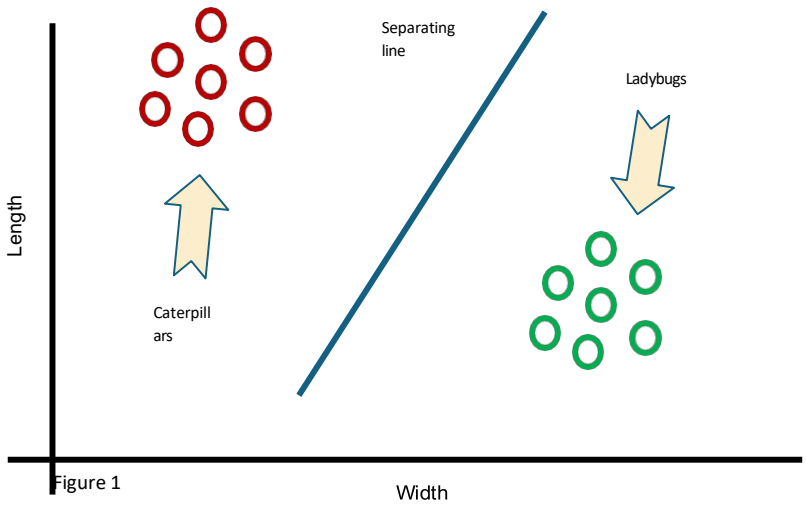


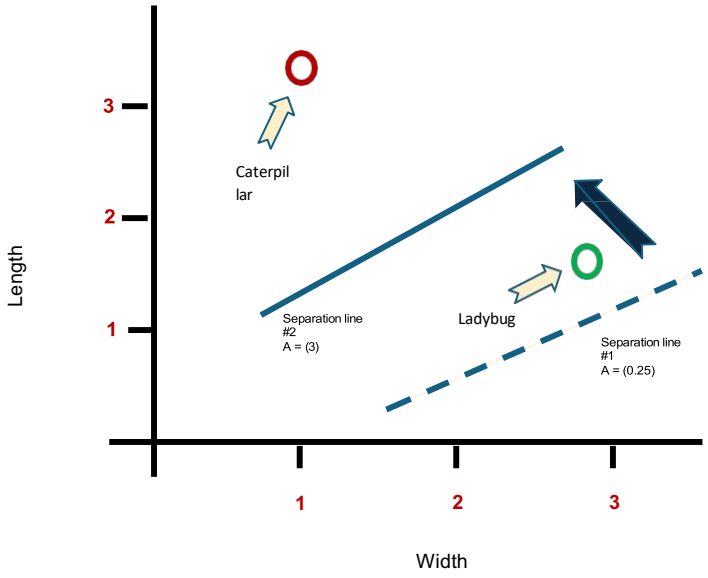
Figure 1

In Figure 1, two groups of animals can be identified: caterpillars and ladybugs. Caterpillars are generally thin and long, whereas ladybugs are broad and short (this statement has been simplified for illustrative purposes). The predictor searches for distinguishing features between caterpillars and ladybugs and uses a heuristic approach to define a dividing line between these groups of animals. A dividing line is not an absolute value, but can shift again by means of heuristics if the predictor learns from new information when the identified animals are more likely to be caterpillars or ladybugs. To do this, the predictor must repeatedly compare its results with the so-called ground truth.[126] The ground truth is the absolute truth, i.e., in this case, whether the objects are really caterpillars and/or ladybugs.

[126] *Zweig, K.*: Ein Algorithmus kennt kein Taktgefühl (An algorithm has no sense of timing), 1st edition 2019, p. 140 ff.

The truth of the predictor will not contain the absolute truth, but its result, which is very close to the fundamental truth. [127]

With each iteration loop, the predictor collects information about caterpillars and ladybugs and compares it with the fundamental truth. Especially during the first iteration loops, humans must check the predictor's learning, i.e., compare the predictor's results with the ground truth. The more information the predictor has, the better it will be able to distinguish between caterpillars and ladybugs.



Figure

Figure 2 shows how the dividing line shifts and thus provides the result of whether a caterpillar or a ladybug is present. A is the value for the shift of the dividing line to the upper left. If the value A is= 0.25, then there is no

[127] *Rashid, T.*: Neuronale Netz selbst programmiert (Self-programmed neural networks), 1st edition 2017, p. 10.

Separation of ladybugs and caterpillars (separation line #1). If the value A is= 3 (separation line #2), then there is a separation between ladybugs and caterpillars. The (simplified) learning algorithm is:

Error value= Target value – Actual value Check

with the ground truth Error value = 0 => no

error

III. How deep learning and artificial neural networks work

Compared to simple machine learning, deep learning uses a series of hierarchical layers or a hierarchy of concepts to carry out the machine learning process. The KNNs used here are structured like the human brain, with neurons connected to each other like a network.[128] The first layer of the KNN, the visible "input layer," processes raw data input, such as the individual pixels of an image. [129] The data input contains variables that we can observe, hence "visible layer." [130]

In extensions of learning algorithms for network structures with very few or no intermediate layers, such as the single-layer perceptron, deep learning methods enable stable learning success even with numerous intermediate layers.[131] Deep learning involves the ability of computers to learn from experience and understand the world in terms of a hierarchy of concepts. [132] By gathering knowledge from experience, this approach avoids the need for human operators to provide all the knowledge that the computer needs for its work.

[128] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz (Basic Course in Artificial Intelligence), 4th edition, 2016, pp. 132, 258, 300, 331, 333. (Ertel, 2016)

[129] *Rashid*, *T.*: Neuronale Netz selbst programmiert (Self-programmed neural networks), 1st edition 2017, p. 8.

[130] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz (Basic Course in Artificial Intelligence), 4th edition 2016, pp. 132, 258, 300, 331, 333.

[131] *Goodfellow*, *I.*; *Bengio*, *Y.*; *Courville*, *A.*: Deep Learning. MIT Press, https://www.deeplearningbook.org/, accessed on May 11, 2020.

[132] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz (Basic Course in Artificial Intelligence), 4th edition, 2016, pp. 132, 258, 300, 331, 333.

need to be formally specified.[133] The hierarchy of concepts allows the computer to learn complicated concepts by combining simpler ones.[134] If you draw a diagram showing how these concepts are built on top of each other, the diagram is deep, with many layers.[135] This first layer passes its output to the next layer. This second layer processes the information from the previous layer and also passes on the result. The next layer receives the information from the second layer and processes it further. These layers are called hidden layers. The features they contain become increasingly abstract. Their values are not specified in the original data. Instead, the model must determine which concepts are useful for explaining the relationships in the observed data. This continues across all levels of KNN. The result is output in the visible "output layer," the last layer. This divides the desired, complicated data processing into a series of nested, simple mappings, each described by a different layer of the model.

These KNN architectures, which have more than one hidden layer, are notable in that "new" information can be formed between the layers, representing the original information. It is important to understand that these representations are a modification or abstraction of the actual input signals.[138] Such a mechanism, which can be summarized under the terms "feature learning" or "representation learning," ensures that deep learning models are generally very effective at abstracting new data points. [139] The reason for this is

133 *Goodfellow*, *I.*; *Bengio*, *Y.*; *Courville*, *A.*: Deep Learning. MIT Press, https://www.deeplearningbook.org/, accessed on May 11, 2020.

134 Wikipedia entry "Artificial neural network," accessed on April 27, 2020.

135 *Ertel*, *W.*: Grundkurs Künstliche Intelligenz (Basic Course in Artificial Intelligence), 4th edition 2016, pp. 132, 258, 300, 331, 333. (Kriesel, 2017)

136 *Kriesel*, *D.*: A Brief Introduction to Neural Networks, http://www.dkriesel.com/en/science/neural_networks, accessed on February 19, 2017.

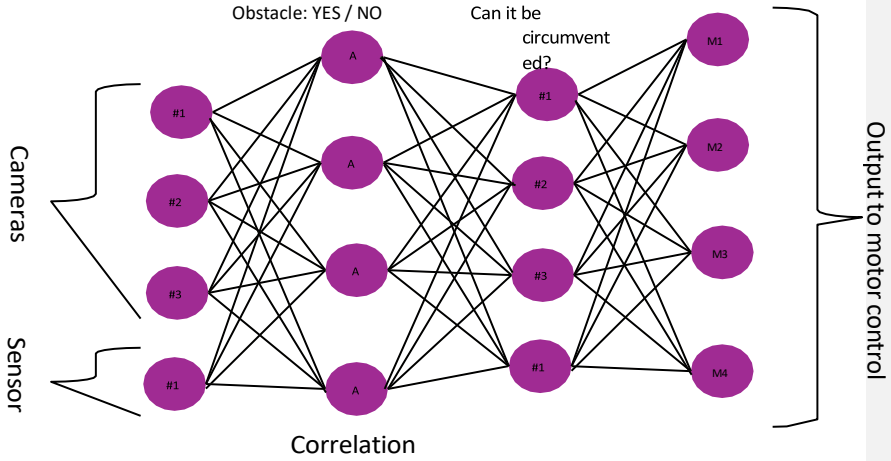
137 Wikipedia entry "Artificial neural network," accessed on April 27, 2020.

138 *Heinz*, *S.*: Deep Learning – Part 1: Introduction, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, accessed on May 11, 2020.

139 *Bengio*, *Y.*; *Courville*, *A.*; *Vincent*, *P.*: "Representation Learning: A Review and New Perspectives," 2013, https://arxiv.org/abs/1206.5538, accessed on May 11, 2020. IEEE Trans. PAMI, special issue Learning Deep Architectures, 35: 1798 – 1828. arXiv:1206.5538. doi:10.1109/tpami.2013.50.

that the abstractions made of the data are of a much more general nature than the original input data. [140]

KNN have little to do with neural networks in living beings. This is because modern Deep learning models are only based to a certain extent on findings from neuroscience. Today, we know that the processes and functions in the human brain that are calculated for information processing are much more complex than those depicted in KNN. [142] However, the idea that many individual "computing units" (neurons) intelligently process information through interconnection can be recognized as a basic principle. [143]



Figure

[140] *Heinz*, *S.*: Deep Learning – Part 1: Introduction, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, accessed on May 11, 2020.

[141] *Nielsen*, *M.*: Neural Networks and Deep Learning. Determination Press, http://michaelnielsen.org, accessed on May 11, 2020.

[142] *Schreiber*, *S. B.*: Natural Intelligence. Neurons and Synapses – Just an Organic Computer? (Part 1), c't – Magazine for Computer Technology, 1987 (4), p. 98 ff.

[143] *Heinz*, *S.*: Deep Learning – Part 1: Introduction, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, accessed on May 11, 2020.

At the beginning of this text, a self-learning vacuum robot was mentioned as an example of a KNN. But how does this vacuum robot actually work? How does it manage to avoid table legs, chairs, cabinets, and children's toys, which can be found in different places every time? This question is relatively easy to answer: The vacuum robot has touch sensors and cameras. The cameras can use simple image recognition to detect whether there is an obstacle in front of them. Sensors also receive information when the vacuum robot bumps into something. This diverse information forms the abstract input layer described above, which is the first layer of the KNN. What does the AI do with the information obtained from the input layer? It operationalizes this information in the second layer, a hidden layer. Specifically, the vacuum robot's AI asks itself, "Is there an obstacle in front of me?" and compares the different information from the sensors. [144] The operationalization then takes place according to the example described above, where a distinction was made between caterpillars and ladybugs. In the third layer, also a hidden layer, the AI of the vacuum robot asks itself whether it is possible to drive around the obstacle, and in the fourth layer (output layer), the AI controls the individual motors of the vacuum robot according to this data.

The way intelligent vacuum robots work is not very different from a KNN for securities trading (known as "algorithmic trading"), see Figure 4. Instead of touch sensors and cameras, various financial information obtained from legal sources is used, e.g., from the capital market, global stock exchanges, news providers (e.g., Reuters), or even annual reports from companies. Similar to the vacuum robot, this collection of relevant information forms the input layer. In the following hidden layers, the information is standardized, i.e., weighted and evaluated. In the

144 *Zweig, K.*: Ein Algorithmus kennt kein Taktgefühl (An algorithm has no sense of timing), 1st edition 2019, p. 140 ff.

Output layer: Decisions are then made, such as "buy," "sell,"
"buy at value x," and "sell at value y."[145]

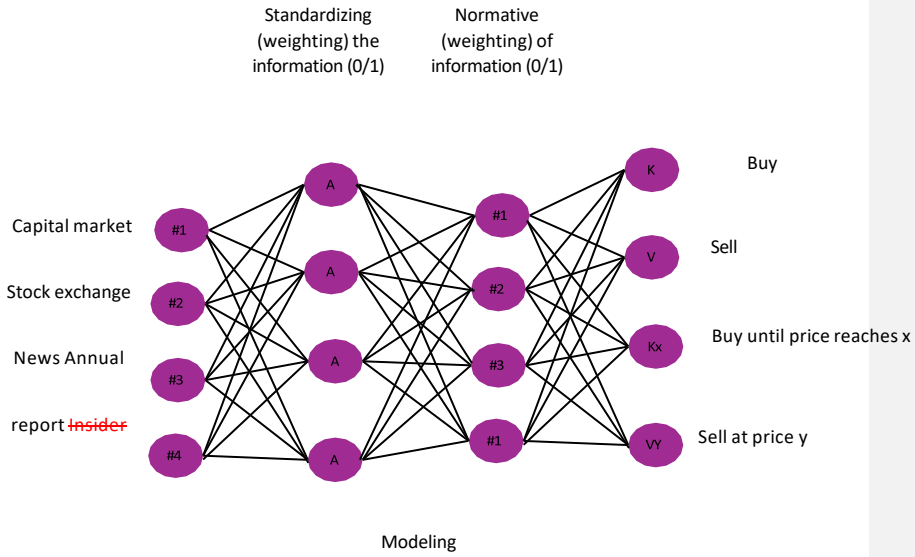


Figure 4

VI. Legal protection for machine learning and artificial intelligence

The legal issues surrounding the KNN described above can be divided into two basic questions : On the one hand, the protection of the creation of the KNN and, on the other hand, the protection of the information obtained through the KNN.

[145] *Zweig, K.*: Ein Algorithmus kennt kein Taktgefühl (An algorithm has no sense of tact), 1st edition 2019, p. 140 ff.

1. Protection for the creation of an artificial neural network

Protection for the creation of an ANN as a field of application of ML can arise from patent law, copyright law, and trade secret law.

a) Patent protection for KNN

Unfortunately, the mere creation of KNN lacks the elements required for patent law pursuant to Section 1 (2) and (3) PatG and Art. 52 (2) and (3) EPC, technical procedures necessary to provide effective patent protection. This would mean that the KNN would probably not be eligible for patent protection for trading in securities ("algorithmic trading"). This is because if a method that is not technical in itself, e.g., a mathematical method, is used in a technical process that is applied to a physical phenomenon with the aid of technical means for carrying out the method and causes a change in that phenomenon, that method contributes to the technical character of the invention as a whole. A fundamental difference between a mathematical method and a technical process is that a mathematical method or algorithm is executed with numbers (which can represent anything) and leads to a result expressed in numbers. This is because the mathematical method or algorithm is only an abstract concept that describes how to proceed with numbers. [146] The relevant feature must therefore be taken into account when assessing the inventive step. [147] The creation of KNN is therefore not patentable.

This is, of course, to be viewed differently in the context of the vacuum robot, as this is likely to involve a technical process, given that the robot itself is equipped with a technical process. The KNN would probably be integrated into the control software of the vacuum robot, and this control software could be patented as so-called embedded software. This is because hardware that is controlled by software

[146] T 208/84, OJ 1987, p. 14.

[147] T 208/84, OJ 1987, p. 14; T 641/00; T 258/03; T 1814/07, OJ 2003, p. 352.

is controlled, it is not a matter of patent protection for the software as such, but for the technical invention (hardware). In the Federal Court of Justice decision "Sprachanalyseeinrichtung"[148], the question of the technical nature of computer programs was answered by means of the connection of hardware and software into a single unit.[149] This seemingly emerging further opening of patent protection for computer programs was significantly restricted by the Federal Court of Justice in its decision "Suche fehlerhafter Zeichenketten" (Search for faulty character strings)[150], so that today there are no clear criteria for the patentability of software.[152] In principle, patentability cannot be assumed if software as such, without any additional technical invention, is to be registered. The situation is different, of course, if the software controls a machine.

b) Copyright protection as a work

The question of whether copyright protection as a work applies to the creation of a KNN depends on the status of the KNN.[153] Thus, analogous to the algorithm in the form of a simple decision tree or the simple representation of the KNN as shown in Figures 1 to 4, the representation of a KNN does not generally enjoy copyright protection under Section 69a BGB. The situation is different if the decision tree already has the quality of a program flow chart. In this case, the program flow chart could enjoy copyright protection as design material for a computer program under Section 69a (2) UrhG[154]

In the case of a mathematically represented algorithm or KNN, such as the Euclidean algorithm, no copyright protection can be assumed. On the other hand, in the case of the representation of a KNN in pseudocode, copyright protection can certainly be assumed, even if this is not apparent from the

[148] Federal Court of Justice, May 11, 2000 – X ZB 15/98, BGHZ 144, p. 282= MDR 2000, p. 1447.
[149] *Marly*, *J.*: Praxishandbuch Softwarerecht (Practical Handbook on Software Law), 5th edition, 2009, margin number 398.
[150] Federal Court of Justice, October 17, 2001 – X ZB 16/00, BGHZ 149, p. 68= GRUR 2002, p. 143.
[151] *Marly*, *J.*: Practical Handbook on Software Law, 5th edition, 2009, margin number 398.
[152] *Marly*, *J.*: Praxishandbuch Softwarerecht (Practical Handbook on Software Law), 5th edition, 2009, margin number 398.
[153] See *Söbbing*, *T.* in CR 2020, pp. 223–228 for details.
[154] *Hoeren*, *T.*; *Wehkamp*, *N.* in: CR 2018, pp. 1–7.

comparability with the source code, but enjoys copyright protection as draft material for a computer program in accordance with Section 69a (2) UrhG. [155]

If the KNN was created as code, e.g., in the Python programming language, then it can certainly be assumed that it enjoys copyright protection comparable to that of a software program under Section 69a (1) UrhG. [156]

c) Copyright protection as a database

It is questionable whether the structure of a KNN described above corresponds to the structure of a database and could therefore enjoy copyright protection under Sections 87a et seq. of the German Copyright Act (UrhG). According to Section 87a (1) No. 1 UrhG, a collection of works, data, or other independent elements is protected if it is arranged systematically or methodically and is accessible individually by electronic means or in any other way, and if its inspection, review, or presentation requires a significant investment in terms of type or scope. Solutions in the big data environment thrive precisely because data is too large, too complex, too fast-moving, or too poorly structured, and only databases make it possible to manage this data.

In individual cases, it could be argued that the creation of a KNN falls under the subsumption of a database within the meaning of Section 87a (1)
p. 1 UrhG, even if this data is not stored for long, because, as in the case of the vacuum robot or algorithmic trading, it becomes obsolete extremely quickly. However, KNN generally collects data and arranges it systematically or methodically before making it available to third parties. It can be assumed that this requires a significant investment. The data collected by KNN is arranged systematically and methodically within the meaning of Section 87a UrhG.[158] Although

[155] *Hoeren*, *T.*; *Wehkamp*, *N.* in: CR 2018, pp. 1–7.
[156] For more details, see *Söbbing*, *T.* in: CR 2020, pp. 223–228.
[157] *Bachmann*, *R.*; *Kemper*, *G.*; *Gerzer*, *T.*: Big Data – Fluch oder Segen? Unternehmen im Spiegel gesellschaftlichen Wandels (Big Data – Curse or Blessing? Companies in the Mirror of Social Change), 2014, p. 2.
[158] *Grützmacher*, *M.* in: CR 2016, pp. 485–495 (487).

In big data analysis, where unstructured data sets are evaluated, the concept of a database is called into question because the data are not independent of each other [159] but this is generally not the case with KNN. For technical reasons, data that is to be exchanged must be arranged systematically and methodically. The ECJ does not view the requirement of independence so narrowly, but interprets it very broadly, which greatly facilitates consideration in the context of KNN.

In connection with the creation of a KNN, the question arises as to whether the individual elements of the database must be independent.[162]According to the case law of the ECJ, a database producer's right can only be considered if the individual elements can be separated from each other without impairing the value of their informative, literary, artistic, musical, or other content.[163] This question is therefore becoming increasingly important, as KNN produce results that are generated from different sources and together form a single entity, e.g., a vacuum cleaning robot that analyzes a room using cameras and touch sensors. When assessing the independent informational value of an element extracted from a collection, the ECJ does not focus on the perspective of the typical user of the collection in question, but on that of any third party interested in the extracted element.[164] The ECJ cites as an example individual geographical data from a topographical map. [165] Thus in view of the increasing possibilities offered by technical developments to evaluate the information content of data in different contexts, the requirement of independence of the elements should not pose too great an obstacle.

159 *Hoeren*, *T.*; *Völkel*, *J.* in: *Hoeren, T.*: Big Data und Recht, 2014, p. 22.

160 *Peschel*, *C.*; *Rockstroh ,S.* in: MMR 2015, p. 571 ff. (572).

161 ECJ, October 29, 2015 – C-490/14= GRUR 2015, p. 1187; MMR 2016, p. 51; K&R 2015, p. 790; afp 2016, p. 33; ECJ, November 9, 2004 – C-444/02= , Coll. 2004, I-10549, GRUR 2005, p. 254, GRUR Int. 2005, p. 239; CR 2005, p. 412.

162 *Hetmank*, *S.*; *Lauber-Rönsberg*, *A.* in: GRUR 2018, p. 574.

163 ECJ, October 29, 2015 – **C-490/14=** GRUR 2015, p. 1187 para. 17 – Freistaat Bayern/Verlag Esterbauer.

164 *Hetmank*, *S.*; *Lauber-Rönsberg*, *A.* in: GRUR 2018, p. 574.

165 Federal Court of Justice, November 20, 2008 – I ZR 112/06= GRUR 2009, p. 403 – Metal on Metal I; Federal Court of Justice, December 13, 2012 – I ZR 182/11 GRUR 2013, p. 614 – Metal auf Metall II; GRUR 2017, p. 895 – Metall auf Metall III.

as they will often retain sufficient and independent value from the perspective of a third party after being removed. [166]

According to Section 87b (1) sentence 1 UrhG, the database producer has the exclusive right to reproduce, distribute, and publicly reproduce the database as a whole or a substantial part of the database in terms of type or scope. This means that, in principle, there is no protection if individual data items amounting to less than 10% are taken.[167] However, it must be taken into account that successive reproductions, distributions, or public communications, even if they only concern insignificant parts of the database, are equivalent to a substantial part when taken together, cf. Section 87b (1) sentence 2 UrhG. Nevertheless, it must be taken into account that, in horizontal networking, even small amounts of data must be considered worthy of protection, especially if individual data can have a significant influence on process flows or if the systems can be manipulated by changing the individual data.[168] This is primarily a matter of protecting the integrity of data, as even the slightest changes can render data sets unusable.

2. Protection for machine learning results

In many cases, the protection of machine learning results by KNN may not be that significant. Surely, neither the manufacturer nor the user of the vacuum robot will have any interest in protecting the route taken by the vacuum robot. But in many cases, KNN generates data that is worth protecting. Regardless of data protection, the question therefore arises as to whether this data collected by KNN can be legally protected and transferred.

166 *Hetmank, S.*; *Lauber-Rönsberg, A.* in: GRUR 2018, p. 574.

167 Federal Court of Justice, July 21, 2005 - I ZR 290/02 = BGHZ 164, p. 37; NJW 2005, p. 3216 (Ls); MDR 2006, p. 104 (Ls.); GRUR 2005, p. 857; MMR 2005, p. 754; K&R 2006, p. 38; ZUM 2005, p. 731; afp 2005, p. 470; CR 2005, p. 849.

168 *Grützmacher, M.* in: CR 2016, p. 485–495 (488).

a) Data

It is questionable whether a type of ownership can be established for the collected data. [169]In this context, data is "also" understood as information that has not been processed, or has not been processed sufficiently, to fall within the scope of protection of intellectual property rights, such as patent or copyright law in particular.[170] Such information is "in the public domain" within the meaning of intellectual property law and can be used by anyone, subject to data protection law. In two recent rulings, the ECJ has not recognized any ancillary copyright for data to be generated in the future; in the ECJ's view, only investment in existing data should be protected. [171]

Under the law of obligations, the question arises as to whether the data collected by KNN within the meaning of v. § 433 BGB or whether the data can be passed on here on the basis of a sui generis agreement. In the case of sale, the question arises as to the material nature of data, which makes a sale within the meaning of Section 433 BGB considerably more difficult. However, an original application of Sections 433 et seq. BGB to data trading can only take place where the data can be indirectly assigned to an item (e.g., a data carrier).[172] In the vast majority of cases – e.g., in the case of purely electronic data transmission via FTP, email, etc. – this fails due to the lack of material nature of the data itself.[173] Under Section 453(1), alternative 2 BGB, data can be regarded as other objects[174], which opens the way to Sections 433 et seq. BGB via the sale of rights. The decisive factor here is solely the affirmative transferability of data as opposed to constitutive transfer.

---

169 *Heymann*, *T.* in: CR 2016, pp. 650–657 (650). (Ensthaler, 2016)

170 *Ensthaler*, *J.* in: NJW 2016, pp. 3473–3552, (3473).

171 ECJ, November 9, 2004 – C-203/02= , ECR 2004, I-10415; NJW 2005, p. 1263 (Ls.); GRUR 2005, p. 244; GRUR Int. 2005, p. 247; EuZW 2004, p. 757; MMR 2005, p. 29; ZUM 2005, p. 1 and ECJ, 09.11.2004 – C-444/02= , ECR 2004, I-10549; GRUR 2005, p. 254; GRUR Int. 2005, p. 239.

172 *Beckmann*, *R. M.* in: Staudinger, BGB, 2014, § 453 BGB, margin note 37; *Patzak*, *A.*; *Beyerlein*, *T.* in: MMR 2007, p. 687 (688); see also *Hieke*, *R.* in: InTeR 2017, p. 10, 11 f.; on §§ 377, 381 (2) HGB also BGH, July 14, 1993 - VIII ZR 147/92, NJW 1993, p. 2436, 2437 f.; Federal Court of Justice, November 15, 2006 – XII ZR 120/04, NJW 2007, p. 2394, 2394 – Software.

173 *Kirchner*, *G.* in: InTeR 2018, p. 19–24.

174 *Berger*, *C.* in: Jauernig, BGB, 14th ed. 2011, § 453, margin no. 11; *Hauck*, *R.* in: NJW 2014, p. 3616 (3616); *Grosskopf*, *L.* in: IPRB 2011, p. 259 (259); OLG Düsseldorf, February 17, 2010 - 17 U 167/09, BeckRS 2010, 09514 – on address data; LG Munich I, December 10, 2008 - 16 HK O 10382/08, BeckRS 2009, 88429 – on email addresses; see also RegE, BT-Drucks. 14/6040, p. 242, where, however, only software was expressly listed as other items; left open by: Higher Regional Court of Düsseldorf, July 30, 2004 - I-23 U 186/03, BeckRS 2004, 08836 – preferred contract for work and services or contract for work; BGH, June 30, 1976 - VIII ZR 267/75, NJW 1976, 1886, 1887 – purchase or rental agreement.

for example, copyrights (cf. Section 29 (1) UrhG),[175] regardless of whether the data is actually only copied or transferred with simultaneous deletion.[176] The data seller is therefore obliged under Sections 453, 433 (1) sentence 2 BGB to provide the data buyer with the data free of material defects and defects of title. [177]

It has not yet been conclusively clarified on what legal basis the transfer of data is justified under the GDPR. [178]It is argued that processing in this context is permissible on the basis of the general grounds for justification, in particular Art. 6 (1) sentence 1 lit. f GDPR.[179] According to another view, it is sufficient that the requirements of Art. 28 GDPR for commissioned data processing are met. [180] In view of the fact that commissioned processing constitutes a form of privilege, it is convincing to rely solely on the provisions of Art. 28 GDPR.[181] However, the operator of the AI technology can then only act on behalf of its customer within the narrow scope of Art. 28 GDPR, i.e. on the instructions of the customer, and must provide the guarantees required under Art. 28(1) GDPR that the appropriate technical and organizational measures within the meaning of Art. 32 GDPR are implemented in such a way that the processing is carried out in accordance with the requirements of this Regulation and the protection of the rights of the data subject is ensured.

b) Trade secrets

Another way to obtain legal protection for the data collected by KNN would be through the Trade Secrets Act (GeschGehG). Under the GeschGehG, information is protected as a trade secret if

175 *Pahlow*, *L.* in: JA 2006, p. 385 (385), generally on the purchase of rights.

176 See *Hoppen*, P. in: CR 2015, p. 802 (803), although his statement that every data transfer is a copying process cannot apply to data carrier-based transfers, for example.

177 *Kirchner*, *G.* in: InTeR 2018, 19–24.

178 *Heckmann*, *D.* in: *Heckmann*, *D.*: jurisPK-Internetrecht, 5th edition, 2017, Chapter 9, 1st revision, margin number 214.

179 *Spoerr*, *W.* in: Wolff/Brink, Beck'scher Onlinekommentar, as of November 1, 2017, Art. 28 GDPR, margin number 30 et seq.

180 *Schmidt*, *B.*; *Freund*, *B.* in: ZD 2017, p. 14 (16); dissenting opinion *Hartung*, *J.* in: *Kühling*, *J.*; *Buchner*, *B.*: DS-GVO/BDSG, 2nd edition 2018, Art. 28, margin number 22.

181 See also *Thomale*, *P.-C.* in: Auernhammer, DS-GVO/BDSG, 5th ed. 2017, Art. 28, para. 8.

it meets the requirements of Section 2 (1) GeschGehG. According to this, a trade secret is information

- which, either as a whole or in the precise arrangement and composition of its components, is not generally known or readily accessible to persons within the circles that normally deal with this type of information and therefore has economic value, and
- is subject to reasonable confidentiality measures under the circumstances by its lawful owner and
- in which there is a legitimate interest in maintaining secrecy.

The owner of a trade secret is any natural or legal person who has lawful control over a trade secret, cf. Section 2 (2) GeschGehG. According to Section 2 (3) GeschGehG, an infringer is any natural or legal person who unlawfully obtains, uses, or discloses a trade secret in contravention of Section 4; an infringer is not someone who can invoke an exception under Section 5.

An important prerequisite is that, pursuant to Section 2 No. 1 lit. b GeschGehG, the information must have commercial value because it is secret. It is important to note that the interest in secrecy is a more general concept than commercial value. It covers not only information that has a positive value, but also secrets that do not convey any value but whose disclosure could cause damage.[182] Examples include information that could potentially damage the company's image or even information about illegal activities within the company, such as antitrust violations. There is no doubt that disclosure of such information could lead to considerable financial disadvantages, whether in the form of fines or a decline in sales. [183] However such information (unlike, for example, know-how that can be used productively) cannot be described as assets of the company. [184] This is likely to be the case.

[182] Federal Court of Justice, April 27, 2006 – I ZR 126/03, GRUR 2006, p. 1044, para. 19 – Customer data program; Federal Court of Justice, May 10, 1995 – 1 StR 764/94, NJW 1995, p. 2301 – Offer documents.

[183] *Kalbfus*, *B.*: GRUR 2016, p. 1009.

[184] Statement by GRUR dated March 19, 2014, p. 4, available at http://www.grur.org/de/stellungnahmen.html; dissenting opinion *Redeker*, *S.* S.; *Pres*, *S.*; *Gittinger*, *C.*: WRP 2015, p. 681, margin note 7.

However, this plays less of a role in the protection of deep learning. Recital 14 of the Trade Secrets Directive is more relevant here, which states that the information to be protected should have actual or potential commercial value. [185] This can generally be affirmed in the case of complex KNN. After all, no one would dispute that the information collected, e.g., in facial recognition, represents a significant value. Disclosure of the information from KNN would likely cause considerable damage to the company.

Section 2 of the GeschGehG enables AI manufacturers to implement certain protective measures. These measures must also be "appropriate" and "commensurate with the circumstances." Depending on the nature and significance of the confidential information, the degree and intensity of the necessary security measures may therefore vary in individual cases. [186] The owner is thus entitled to exploit the trade secret.[187]
Of course, data protection must also be taken into account, as AI is not permitted to collect personal information without further ado, as it is subject to the requirements of the GDPR.

c) Summary

The protection of KNN falls within the legal field of artificial intelligence law (AI law), which is very new and not yet properly defined. [188] It cannot really be described as a legal field, as research into these legal issues is still in its infancy and new legal insights are constantly emerging. Currently, and hopefully not for eternity, no patent protection can be assumed for a pure KNN, i.e., one that is not embedded in hardware. However, copyright protection is conceivable, but, as explained above, it must be derived. The

185 *Scheja*, *K*. in: CR 2018, p. 485.
186 *Frisse*, *F*.; *Glaßl*, R.; *Baranowski*, A.; *Duwald*, *L*. in: BKR 2018, p. 177.
187 *Scheja*, *K*. in: CR 2018, p. 485.
188 "AI" – artificial intelligence, "AI" and law – law= "AI Law." *Söbbing*, *T*.: Fundamental Legal Issues of Artificial Intelligence, 1st edition 2019, p. 4.

Protection for the results of KNN can be generated, if necessary, through the case law of the ECJ on investment protection in the collection of data and through the Trade Secrets Act.

V. Copyright limits for machine learning[189]

A fundamental field of application for artificial intelligence (AI) is machine learning. In order for AI, such as ChatGPT for text or Stability AI for images, to learn, it needs raw material in the form of information, which mainly comes from the internet. The legal framework for text and data mining was established in Germany in 2021 with Section 44b of the Copyright Act (UrhG). This also has implications for the design of images, insofar as data mining is used for this purpose.

1. Instructions

Machine learning requires very large amounts of authentic training data in order to continuously develop and improve its capabilities. In addition to well-known text generators such as OpenAI's ChatGPT, image generators in particular require large amounts of comparative data for training their AI. Training data for image generators is used by commercial companies such as Stability AI[190] and Mindverse[191] to train their image-generating AI.[192] For this purpose, websites on the internet are analyzed to compare texts and images. [193] The deep learning used here is a self-adaptive algorithm that uses an artificial neural network (ANN). These ANNs rely on so-called image recognition algorithms for image recognition, i.e., various techniques for analyzing images on the internet.

---

189 ***Copyright limits for learning artificial intelligence" on issues of text and data mining (Section 44b UrhG)*** Söbbing/Schwarz, RDi 5/ 2023, 415

190 Pick-a-Pic: An Open Dataset of User Preferences for Text-to-Image Generation – Stability AI.

191 https://www.mind-verse.de (accessed on July 6, 2023).

192 https://www.alltageinesfotoproduzenten.de/2023/04/24/laion-e-v-macht-ernst-schadensersatzforderung-an-urheber-fuer-ki-trainingsda-ten/ (accessed on July 6, 2023).

193 *Steiner* in C't 7/2023, 16–17 (16).

The means used are web crawlers[194], which search the World Wide Web, among other things, in the same way as the well-known search engines have done up to now.

In the field of AI applications, the first step is to analyze a found image or text and extract the (visual) features it contains. Machine learning algorithms are used for this purpose, e.g., convolutional neural networks (CNN or ConvNet).[195] All algorithms used are trained to recognize certain visual patterns and features in images, such as shapes, lines, colors, or textures. After the image has been analyzed, certain features are extracted that serve to identify the content or categorize the image (known as feature extraction). This can include the recognition of objects, faces, text, or specific patterns. Based on the extracted features, the image is classified into different categories or classes (known as classification and labeling). This can mean, for example, that the image is identified as a landscape, animal, person, or object. This classification can be based on predefined categories or enabled by machine learning, whereby the algorithm has been trained beforehand with a large number of labeled images or has trained itself. The web crawler can also collect additional metadata about the image, such as the title of the website, the image source, the author, or other information associated with the image. This metadata can help to further describe and categorize the image. [196]

2. Legal basis

It is questionable whether the above-described functioning of an image recognition algorithm constitutes a copyright infringement. Media providers and publishers in particular feel that their copyrights are infringed by the functioning of image recognition algorithms. [197]*Spindler's* hope that the implementation of

[194] also known as a spider, searchbot, or robot.

[195] See, among others, *Fukushima*, Bio.Cybernetics 36, 193–202 (1980); *LeCun* et al, Gradient-Based Learning Applied to Document Recognition, Proc. of the IEEE, November 1998.

[196] It is important to note that the exact functioning of a web crawler for image analysis depends on the algorithms and technologies used. There are various approaches and methods for analyzing images, and development in this area is constantly progressing. The method described here cannot therefore be considered exhaustive.

[197] *Steiner* in C't 7/2023 16–17 (16).

The EU Commission's proposal that there was a good chance that the discussion on text and data mining, which had been going on for years, could come to a reasonable conclusion by also allowing commercial use, has not (yet) been fully realized.[198] Although the 2019 reform of the Copyright Directive[199] introduced new, special provisions that are intended to promote rather than hinder the development of AI technologies in the EU, text mining is generally permitted under Article 4 of the Directive, cf. Section 60d of the German Copyright Act (UrhG).

Article 4(1) of the Directive provides for an exception or limitation to the rights provided for in Article 5(a) and Article 7(1) of Directive 96/9/EC,[200] Article 2 of Directive 2001/29/EC, Article 4(1)(a) and (b) of Directive 2009/24/EC[201] and Article 15(1)[202] of the Directive for the purpose of text and data mining. The provisions were implemented in Sections 44b and 60d of the UrhG [203]. This means that the German UrhG now contains two provisions on limitations for text and data mining that differ in detail—Section 44b in general and Section 60d for non-commercial, scientific purposes. [204] According to the intention of the legislator, data mining should, in principle, be legally possible. One of the recitals states[205] that text and data mining may also be carried out for purely factual or non-copyright-protected data, and that in such cases no permission is required under copyright law. It should also be noted that there may be cases of text and data mining in which no act of reproduction takes place or the reproductions fall under the mandatory exception for temporary acts of reproduction provided for in Article 5(1) of Directive 2001/29/EC, which

198 *Spindler*, GRUR 2016, 1112, beck-online.

199 Directive (EU) 2019/790 of the European Parliament and of the Council of April 17, 2019, on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC.

200 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31996L0009 (accessed on July 6, 2023).

201 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32001L0029 (accessed on 06.07.2023).

202 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32001L0029 (accessed on 06.07.2023).

203 See BT-Drs. 19/27426, 87.

204 BeckOK UrhR/Hagemeier, 38th ed. 01.02.2023, UrhG § 44b Rn. 1.

205 Recital 9 of Directive (EU) 2019/790 of the European Parliament and of the Council of April 17, 2019.

should continue to apply to text and data mining operations that do not involve the making of copies beyond the scope of this exception.

Once the EU Directive has been implemented, researchers may alternatively rely on § 60d or § 44b UrhG, provided that it fulfills the requirements of the respective restriction[206]. Even though § 60d UrhG modifies the general provisions of § 44b (1) UrhG with regard to the purpose of scientific research, the provisions do not supersede each other but remain applicable alongside each other.[207] By creating a further legal basis for commercial uses, this is intended to provide the economy with greater legal certainty in promoting innovation and in the further expansion of the digitization of services.[208]

However, the Federal Association of Digital Publishers and Newspaper Publishers (BDZV) in its "Vienna Declaration" [209]and the Media Association of the Free Press (MVFP)[210] in a joint statement with the BDZV: "In our opinion, the use of AI language modules for the publication of competing content is only permissible with a license from the publisher."[211] This opens the door to §§ 51 ff. VVG[212].

3. Stock photography and AI – Hamburg Regional Court

The particular economic significance of Section 44b UrhG is particularly evident in the field of stock photography. Here, pre-produced images ("on stock") are distributed and sold either license-free or in return for license fees. To illustrate this, a few figures are provided by way of example. Getty Images, one of the

206 BReg-Drs. 19/27426, 95.

207 BeckOK UrhR/Hagemeier, 38th ed. 01.02.2023, UrhG § 44b, margin note 1.

208 See recital 18, subparagraph 1, sentence 4 DSM Directive; BT-Drs. 19/27426, 87.

209 https://www.bdzv.de/service/presse/branchennachrichten/2023/wiener-erklaerung-deutschsprachige-verlegerverbaende-verabschieden-gemeinsamen-forderungskatalog?sword_list%5B0%5D=Lizenz&no_cache=1 (accessed on 06.07.2023).

210 https://www.mvfp.de/nachricht/artikel/tagesspiegel-ver-lage-fordern-lizenzgebuehren-wegen-chatbot-suchmaschi-nen (accessed on 06.07.2023).

211 *Steiner* in C't 7/2023, 16–17 (17).

(212) See *Pukas*, GRUR 2023, 614.

world's leading image agencies, has 6,206,547 "stock photos & high res pictures" available.[213] A British company specializing in stock photography refers to its offering of "339,800,165 stock photos, 360° panoramic images, vectors and videos"[214].

On April 27, 2023, a stock photographer filed a lawsuit with the Hamburg Regional Court against the non-profit association LAION e. V. for alleged copyright infringement.[215] The stock photographer wants to achieve clarity for the entire stock photography industry regarding the extent to which web crawlers are allowed to analyze his images or those of his colleagues. In addition, he wants to work toward compensation for the authors of images used to train large machine learning models. [216]

LAION ("Large-scale Artificial Intelligence Open Network") is a German non-profit organization that develops open AI models and datasets. LAION sees itself as a non-profit organization with members from all over the world whose goal is to make large-scale models, datasets, and associated codes for machine learning accessible to the general public.[217] According to the association, LAION's databases do not contain pixel data, but only pure text data, metadata, and URLs. According to LAION e. V., the LAION-400M and LAION-5B datasets provided do not contain any pixelated data, only text data, text embeddings, and URL references to image-text pairs that are available on the open internet.[218] The data sets are therefore a catalog with index references to 400 million or, in the case of LAION-5B, five billion freely accessible images. [219]

213 https://www.gettyimages.com/photos/holding (accessed on July 6, 2023).

214 https://www.alamy.com/enterprise/ (accessed on July 6, 2023).

215 Hamburg Regional Court, September 27, 2024 – 310 O 227/23= GRUR 2024, 1710

216 https://www.profifoto.de/szene/notizen/2023/02/21/laion-droht-kneschke/ (accessed on 06.07.2023).

217 https://laion.ai/about/ (accessed on 06.07.2023).

218 Source: LAION e. V.

219 *Hahn*, Was darf KI? Stock photographer and AI association dispute copyright in https://www.heise.de/hintergrund/Was-darf-KI-Stockfoto-graf-und-KI-Verein-streiten-um-das-Copyright-8984836.html (accessed on July 6, 2023).

The subject matter of the legal dispute [220]was a lawsuit brought by a photographer against the non-profit research network Laion (Large-scale Artificial Intelligence Open Network). Laion provides a comprehensive, publicly accessible database comprising around six billion image-text pairs. This database is used to train AI systems, in particular for the development of image and text recognition algorithms. The database included, among other things, an image of the plaintiff photographer, who sought a court order to have the photo deleted and to prohibit its further use. The photographer argued that the inclusion of his image in the database infringed his copyright. In particular, he questioned whether Laion was entitled to download the image and use it for comparison with the corresponding image description.

It is questionable whether the above-described functioning of an image recognition algorithm constitutes a copyright infringement. Media providers and publishers in particular feel that their copyrights are infringed by the functioning of image recognition algorithms. However, the EU is taking a different approach, as it does not want to hinder the development of AI. Special provisions were therefore included in the 2019 reform of the Copyright Directive. For example, Article 4 of the Directive generally permits text mining, cf. Section 60d of the German Copyright Act (UrhG). Article 4(1) of the Directive stipulates that Member States shall provide for an exception or limitation for reproductions and extractions from lawfully accessible works and other subject matter for the purpose of text and data mining. This applies to the rights laid down in Article 5(a) and Article 7(1) of Directive 96/9/EC, Article 2 of Directive 2001/29/EC, Article 4(1)(a) and (b) of Directive 2009/24/EC, and Article 15(1) of the present Directive. This provision has been implemented in Section 44b of the UrhG, and thus there are now two restrictions on text and data mining in the German UrhG—Section 44b in general and the more specific Section 60d for non-commercial, scientific purposes. Data mining is therefore legally possible in principle. In this regard,

[220] Hamburg Regional Court (judgment of September 27, 2024, ref. 310 O 227/23, see comments by Söbbing ITRB 2024, xx

It has been clarified that text and data mining may also be carried out for purely factual information or data that is not protected by copyright, and in such cases no permission is required under copyright law. There may also be cases of text and data mining where no act of reproduction takes place or where the reproductions fall under the mandatory exception for temporary acts of reproduction provided for in Article 5(1) of Directive 2001/29/EC, which should continue to apply to text and data mining processes that do not involve the production of copies beyond the scope of this exception.the production of copies to an extent exceeding that permitted by this exception. In contrast, the Federal Gazette of Digital Publishers and Newspaper Publishers (BDZV) and the Media Association of the Free Press (MVFP) jointly stated
"In our opinion, the use of AI language modules to publish competing content from publishers is only permissible with a license from the publisher."

Researchers can now alternatively invoke Section 60d or Section 44b, provided that the conditions of the respective restriction are met. According to Section 44b (2) sentence 1 UrhG, reproductions of lawfully accessible works are permitted for text and data mining. However, use pursuant to paragraph 2 sentence 1 is only permitted if the rightholder has not reserved this right, cf. Section 44b (3) sentence 1 UrhG. A reservation of use for works accessible online is only effective if it is made in machine-readable form, cf. Section 44b (3) sentence 1 UrhG. What is meant by a machine-readable form is not entirely clear. Search engines find the file "robot.txt" on websites, which contains essential information about the website for search engines. It would therefore be obvious to inform the AI web crawler in this file that the operator of the website is exercising its right under Section 44b (3) sentence 1 UrhG. It would also be conceivable to include a notice in the imprint of the respective website; as already explained, the information must only be in a machine-readable form in accordance with Section 44b (3) sentence 1 UrhG.

Even though Section 60d UrhG modifies the general provisions of Section 44b (1) UrhG with regard to the purpose of scientific research, the provisions do not supersede each other but remain applicable side by side. By

a clear legal basis has been created for commercial use, this should provide the economy with greater legal certainty in promoting innovation and further expanding the digitization of services.

The plaintiff has now lost in the first instance before the Hamburg Regional Court (judgment of September 27, 2024 – 310 O 227/23). Although the grounds for the judgment are not yet available, it is already known that the court considers Laion's use of the image to be justified in view of the text and data mining exception in Section 60d of the German Copyright Act (UrhG). Section 60d UrhG permits the use of copyright-protected works for scientific purposes, in particular for so-called text and data mining (TDM), without infringing copyright. TDM refers to the process of systematically analyzing large amounts of data—often unstructured texts or other data—to identify patterns or connections and gain new insights.

In the present case, the court considered Laion's comparison of the image with the accompanying image description to be such a scientific purpose. Laion had downloaded the image in order to compare it with the textual description and to identify correlations between the image content and the image description. In the court's view, this process fell within the scope of the limitation provision of Section 60d UrhG, as it constituted a scientific analysis. The fact that the database was later used for training AI systems did not alter this assessment. The decisive factor for the court was that the original purpose of the data comparison was scientific and could therefore be considered privileged use.

The decision is particularly significant because it clarifies the scope of application of the limitation provision in Section 60d UrhG in an area that has been unclear until now. The court clarified that the comparison of image and text data in the context of scientific research falls within the scope of TDM, even if the data sets could later be used for commercial purposes. This interpretation is of considerable interest for

research institutions and companies active in the field of artificial intelligence, as it provides legal certainty regarding the use of copyright-protected works in AI training processes.

In an obiter dictum, the court also raised the question of whether a reservation of use formulated in "natural language" on a website—as in the present case by the photo agency—can be regarded as machine-readable within the meaning of the relevant copyright provisions. This question was not answered conclusively, but the court indicated that reservations of use formulated in natural language could, under certain circumstances, be considered machine-readable if modern AI technologies are capable of capturing and processing their content.

4. Legal issues arising from this

This clearly raises the question of whether the requirements of Sections 44b or 60d UrhG are met and whether the association is therefore entitled to use the work under copyright law. As already explained above, use pursuant to Section 44b (3) sentence 1 UrhG is possible if the copyright holder has not reserved this right and this reservation has been deposited in a machine-readable form pursuant to Section 44b (3) sentence 2 UrhG. However, there are no indications of this.
LAION e. V. represents, insofar as published, the view that its processing can be based on Section 60d UrhG, which covers text and data mining for scientific research purposes.[221]However, the photographer questions the non-profit status and research purpose of the association. [222]In his blog, he states that Stability AI supported the association financially with a donation (according to the association and Stability AI, "a one-time small amount") and provided computing power. According to notarized extracts from the register of associations, LAION was officially registered as an association in February 2022—the LAION-400M and LAION-5B datasets were already created in 2021. Thus

[221] Source: LAION e.V.

[222] https://www.alltageinesfotoproduzenten.de (accessed on 06.07.2023).

according to the photographer's argument, the association cannot claim exceptions to copyright law for the period prior to its registration. The photographer doubts that the association already existed before February 2022. [223]

Ultimately, however, this may be irrelevant for several reasons. On the one hand, public-private partnerships should be able to invoke preferential access regardless of Section 60d UrhG [224](see b below). On the other hand, there is a fundamental question as to whether the use of a web crawler can affect copyright holders (see a above).

a) Acts relevant to copyright law

What is often overlooked in the general discussion is that text and data mining only use the raw data, not the intellectual content of the analyzed works.[225] In the case of generative AI, the (revolutionary) difference to previous types of chatbots lies precisely in the fact that it does not operate with pre-programmed answers, but has been enabled by deep learning to generate an independent, new answer to each query. The logical approach of asking an image generator to create an image in the style of a particular artist, thereby simply reproducing the data available to it, is fundamentally flawed. Rather, the program independently "creates" a new work of its own. The text and data mining that takes place beforehand is nothing more than a learning process and inspiration on the part of an artist prior to the creation of their work. If the work resulting from this learning and creative process is too similar to one of the originals, the copyright holder's rights would be infringed under Sections 15 and 16 of the German Copyright Act (UrhG). Thus, when assessing whether "only" an adaptation within the meaning of Section 23 UrhG exists, a comparison of the works in question must be made to determine whether and, if so, to what extent the older work has its own creative features.

---

223 https://www.alltageinesfotoproduzenten.de (accessed on July 6, 2023).

224 *Dreier/Schulze/Dreier*, 7th edition, 2022, UrhG § 44b, margin note 7.

225 *Schack*, GRUR 2021, 904, 907, has already pointed this out correctly; *Raue/Hegemann*, MAH UrhR, § 3 Copyright restrictions, margin number 40, also takes this view.

have been adopted. The decisive factor for the decision is ultimately a comparison of the overall impression of the designs, in which all adopted creative features must be taken into account in an overall view[226]. The BGH's graduated order of examination [227] within the framework of Section 23 UrhG also illustrates very clearly what is at stake in the field of generative AI: "First, it must be determined in detail which objective characteristics determine the creative individuality of the work used. Then, by comparing the designs in question, it must be determined whether and, if so, to what extent the new design has taken over the creative features of the older work. The decisive factor for the decision is ultimately a comparison of the overall impression of the designs, in which all the creative features taken over must be taken into account in an overall assessment. If the overall impression is the same, the new design is a reproduction of the older work. If needed, you should then check if the new design has enough changes that it's not just a reproduction, but an (unfree) adaptation or other transformation of the work used. If the overall impression differs, then it is neither a reproduction nor an adaptation, but possibly a free use. Free use within the meaning of Section 24(1) UrhG (old version) is when an independent work has been created and the older work served as the basis for the creation of the new work.[228]These relevant considerations of the so-called Porsche decision [229]clearly show that, at least in the case of generative AI, it is not text and data mining that is problematic, but rather the result found in individual cases. In such cases, however, the author has sufficient legal means at his disposal.

[226] Federal Court of Justice GRUR 2004, 855 – Dog figure.

[227] See BeckOK UrhR/Ahlberg/Lauber-Rönsberg, 38th ed. May 1, 2023, UrhG § 23, margin note 10.

[228] Federal Court of Justice ZUM 2022, 547, 553.

[229] BGH ZUM 2022, 547, 553.

b) § 44b UrhG Text and data Mining

As already stated above, it is the intention of the legislator that work with and through artificial intelligence in the European Union should not be hindered but rather promoted. Therefore, after implementation in Section 44b (2) sentence 1 UrhG, reproductions of lawfully accessible works shall be permitted for text and data mining. In this context, uses pursuant to paragraph 2 sentence 1 shall only be permitted if the rightholder has not reserved this right, cf. Section 44b (3) sentence 1 UrhG. A reservation of use for works accessible online is only effective if it is made in machine-readable form, cf. Section 44b (3) sentence 1 UrhG. What exactly is meant by a machine-readable form is not entirely uncontroversial. In any case, a clear and simple option is to provide a notice using the so-called "robot.txt" information. This is a text file in which you can specify which directories may be read by search engines[230] With this file stored in the main directory, the website operator can inform the web crawler that he is exercising his right under Section 44b (3) sentence 1 UrhG.[231]

A notice in the legal notice of the respective website (or in the terms and conditions stored there) would also be conceivable. As already explained, according to Section 44b (3) sentence 1 UrhG, the information only needs to be provided in a machine-readable form.[232]

This shows that the author has been given a simple tool to protect their work right from the start. The corresponding programming can easily prevent a web crawler from accessing the content. With this opt-out model, the author can ensure that their works are not made available to generative AI.

[230] https://developers.google.com/search/docs/crawling-indexing/robots/intro?hl=de (accessed on July 6, 2023).

[231] *Steiner* in c't 7/2023, 16–17 (17).

[232] See also *Pukas*, GRUR 2023, 614, 615.

c) Text and data mining for scientific research purposes (Section 60d UrhG)

This means that it can be left open whether an organization such as LAION e. V. could invoke Section 60d UrhG with the extended possibilities of storing the data obtained. The Bundestag rightly asks whether scientific research can still be linked to non-commercial purposes if a prototype of a model or algorithm is finalized for finalization and embedding in application software in a spin-off company or sold to commercial developers, i.e., if a citizen science approach is pursued.[233]

This is exemplified by Open AI: Founded in 2015 as a nonprofit group to develop artificial intelligence "in the way that is most likely to benefit humanity as a whole," Open AI subsequently entered into a "partnership" with Microsoft (with an investment of one billion US dollars at the end of 2019) and, according to its own statements has been operating as a "capped-profit company" since 2020. [234]

d) Summary

As is often the case, conflicting interests are at play here: on the one hand, the interests of the authors, e.g., stock photographers, and on the other hand, the developers of AI. As understandable as the concerns of the authors may be at first glance, the above explanations show that web crawlers do not "mine" intellectual content. This is because free use within the meaning of Section 24(1) UrhG (old version) applies if an independent work has been created and the older work served as the basis for the creation of the new work. Whether this is always the case when web crawlers collect data is more than questionable.

However, the new provision in Section 44b UrhG shows ways in which web crawlers can be prevented from analyzing one's own works, cf. Section 44b (3) sentence 1 UrhG.

---

[233] Report of the Committee on Education, Research, and Technology Assessment (18th Committee) pursuant to Section 56a of the Rules of Procedure, printed paper 20/5149, 224 (preliminary version dated January 9, 2023).

[234] www.openai.com (accessed on July 6, 2023); www.businessinsider.com (accessed on July 6, 2023)

It is questionable whether this will slow down or prevent the development of AI and constitute a competitive disadvantage for Germany and the EU.

The provision in Section 60d (1) UrhG stipulates that reproductions for text and data mining (Section 44b (1) and (2) sentence 1 UrhG) are permissible for the purposes of scientific research in accordance with the following provisions. However, this leaves open the question of what happens when the results of scientific research are commercially exploited.

In summary, it can be said that the questions and possible answers outlined above are nothing less than the future of artificial intelligence in Germany and the EU.

C. Generative AI[235]

One of the major legal questions of our time is whether the output of generative chatbots such as ChatGPT from OpenAI, Gemini from Google, or others enjoys legal protection. The main issue here is whether the output of generative chatbots is protected by copyright and, if not, whether the output could constitute a trade secret and thus enjoy legal protection. After all, a number of companies use generative chatbots for their daily work, and such technologies are becoming increasingly popular in everyday work.

I. Introduction

ChatGPT and Gemini belong to the group of generative pre-trained transformers (GPT) and are therefore large language models (LLM for short).[236] Such LLMs are important frameworks for generative artificial intelligence (GenAI).[237]

Unlike Internet search engines such as Google, ChatGPT is a relatively new technology developed by the US company OpenAI, based in San Francisco. After OpenAI released the software version GPT-3 online on November 30, 2022, one million users registered worldwide within five days. [238] In January 2023 ChatGPT reached over 100 million users.

The current version 4.0 of GPT was released on March 14, 2023 and features significant enhancements over version 3.5. [239] The paid version, GPT-4, allows image input and the analysis and description of sketches and photos.

---

235 *Söbbing* Possible legal protection for AI output under the UrhG or GeschGehG - Does the output of generative chatbots such as ChatGPT enjoy legal protection? ITRB 2024, 184 - 188

236 Generative AI: a game-changer society needs to be ready for. In: World Economic Forum.

237 Luhui Hu: Generative AI and Future. In: Medium. November 15, 2022.

238 Krystal Hu, Krystal Hu: ChatGPT sets record for fastest-growing user base - analyst note. In: Reuters. February 2, 2023 (reuters.com [accessed on July 12, 2023]).

239 Silke Hahn: OpenAI introduces GPT-4: Language model now also understands images. In: heise online (heise.de). March 14, 2023, accessed on March 15, 2023.

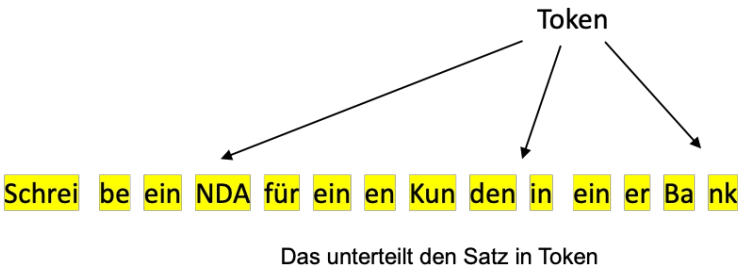
It is possible to have photographed tasks from books solved. Scientific papers can be uploaded to generate a summary. GPT-4 was able to complete exam tests with distinction in tests in the US. Complicated tax questions are answered. [240]

II. How generative AI works in text form

An LLM (Large Language Model) such as ChatGPT works similarly to a huge, highly complex prediction system that is trained to generate text based on the input it receives. To understand the meaning of a word, LLMs first observe it in context using huge training datasets, paying attention to nearby words. These datasets are based on compilations of text published on the internet, with new LLMs being trained on billions of words.

Example:
Prompt (input): "Write an NDA for a customer at a bank."

Step 1:



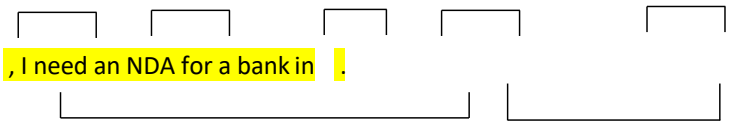
Das unterteilt den Satz in Token

The LLM divides the sentence into tokens. [241] A token can consist of a word, an abbreviation, a syllable, or a punctuation mark. A token is like a piece of a puzzle.

[240] Laurin Meyer: ChatGPT reaches the next stage of development. Die Welt, March 17, 2023. Page 10.

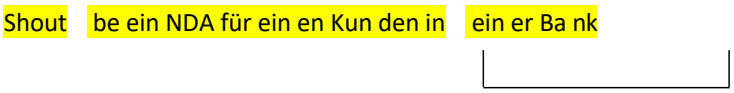
([241]) A "token" is the basic unit of processing that the model uses to understand and generate text. See the original GPT paper: "Improving Language Understanding by Generative Pre-Training" by *Alec Radford et al.* This

Step 2:



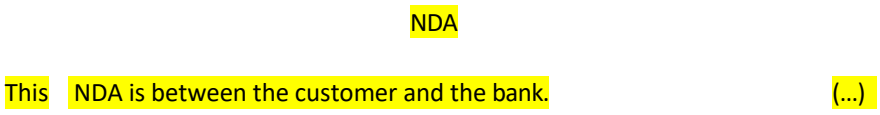
The LLM analyzes the tokens in a sentence and their relationship to each other. The relationship between customer and bank indicates that this is not a bank for sitting:

Step 3:



The response to the prompt is created by combining tokens based on their frequency of occurrence on the internet.

Step 4:



An LLM has no factual knowledge itself, but rather assumes the frequency of information on the internet. This can lead to errors or hallucinations[242], such as

e.g. that "Bettina Wulff" worked in the red-light district before her marriage to German President Christian Wulff "worked in the red-light district,"[243] which is not true, or

Paper by OpenAI introduces the concept and implementation of the original GPT model, including a discussion of tokenization and how it affects the model's ability to understand and generate language.

[242] Hallucinations in large language models (LLMs) such as GPT (Generative Pre-trained Transformer) refer to cases where the model generates incorrect, distorted, or completely fabricated information. These phenomena can be caused by various factors. "Reducing Hallucination in Language Models" by *Yoav Goldberg*, published on arXiv.org.

[243] In September 2012, Bettina Wulff filed lawsuits against Günther Jauch and Google at the Hamburg Regional Court after 34 German and foreign bloggers and media outlets had already issued cease-and-desist declarations in the preceding months. She is defending herself against rumors circulating since 2006 that she worked in the red-light district before her marriage to Christian Wulff, *Hans Leyen-decker, Ralf Wiegand:* Bettina Wulff defends herself against defamation. In: Süddeutsche Zeitung. September 7, 2012.

that the city of "Bielefeld would not exist," which is also false. [244]Both rumors have been circulating on the internet for quite some time and lead to these hallucinations. LLM's are only as good as their training data and how their training tool allows them to be. They are only probabilities.

III. Is the output of LLMs and copyright protection genius?

A work enjoys copyright protection if it is a personal intellectual creation, cf. Section 2 (2) UrhG.

1. Output as a human work?

The central point of reference for copyright protection is personal creation. This refers to the intellectual achievement of a person. Teleologically, this requirement derives from the central protective idea of monistic copyright law. The focus is deliberately on the person of the author[246] However, humans can use tools in their creative act, ranging from pen and brush to artificial intelligence. [247] The starting point here is technological neutrality and agnosticism of copyright law; with regard to the use of works[248] – printers and plotters.[249] In order to copyright a work Within the meaning of Section 2 (2) UrhG, the author may use aids. The nature of the auxiliary means is essentially irrelevant. [250] The auxiliary means must not relieve the actor of the creative act. [251] The progressive use of independently learning algorithms sometimes makes this difficult in practice.

[244] The Bielefeld conspiracy is a satirical conspiracy theory that claims that the city of Bielefeld does not exist, but that its existence is merely convincingly faked. This theory first appeared in 1994 on the German-language Usenet, has been circulating as a running joke on the internet ever since, and has thus become part of internet folklore, which is part of net culture. *Katharina Miklis:* From Bielefeld? That's impossible! In: der Freitag. April 7, 2010. (Miklis, 2010)

[245] cf. Begr. BT-Drs. IV/270, 37

[246] Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, § 2 Rn. 47.

[247] Justification BT-Drs. IV/270, 37.

[248] Federal Constitutional Court ZUM 2010, 874 marginal no. 64.

[249] BGH ZUM 2002, 218, 219 – Scanner.

[250] Wandtke/Bullinger/Bullinger margin note 16a; Schmoll/Graf Ballestrem/Hellenbrand/Soppe GRUR 2015, 1041 (1042)).

[251] Schricker/Loewenheim/Loewenheim/Leistner margin note 40

Legal classification. [252]This is particularly true because the technical processes are sometimes very complex and not very transparent. [253]

However, when using generative chatbots such as ChatGPT and the working method described in No. II, the creative act clearly lies with the generative chatbots. The user simply assigns a task by entering a prompt, and the LLM divides the sentence into tokens and points out certain connections. The response to the prompt is created by the frequent probability of tokens in relation to each other on the internet, resulting in a new text (see No. II). In this case, the creative act lies with the machine, as only it generates the output based on the frequent probability of tokens. However, the creative act must lie with the human being; a machine creation is only eligible for copyright protection if the design of the product can still be traced back to an intellectual act of creation, i.e., if the machine is only an auxiliary or executive means.[254] In this regard, it is rightly argued that, de lege lata, purely computer-generated results cannot be granted the character of a work due to the lack of intellectual creation by a human being. [255] This aspect is considered differently, for example, in British copyright law, in Sec. 178 CDPA [256] or in Sec. 21 lit. (f) CRRA[257] of Irish copyright law. [258] In this context, it would be conceivable to consider a further interpretation of personal creation, but this is not currently being seriously discussed. In principle, however, consideration should be given to whether, in the case of AI-generated results, the AI is used as an aid to a human author or whether there is a separate, autonomous creation process. [259]

[252] Schricker/Loewenheim/Loewenheim/Leistner margin note 41; see also Olbrich/Bongers/Pampel GRUR 2022, 870 (872 f.).

[253] Käde, Creative Machines and Copyright, 2021, p. 183

[254] BeckOK UrhR/Ahlberg, 32nd ed. 15.9.2021, UrhG § 2 margin note 55

[255] Rauer/Bibi BeckOK Urheberrecht (Copyright Law), Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, Section 2, marginal number 57.

[256] British copyright law: Designs and Patents Act 1988

[257] Copyright and Related Rights Act 2000

[258] Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, Section 2, margin note 57.

[259] See Spindler FS Schack 2022, p. 340 (343); Obergfell FS Windbichler, 2020, p. 1397 (1403 f.)

2. Creation of complex prompts

In practice, one sometimes hears the argument that a complex prompt is essential for the output of the creative process of generative chatbots such as ChatGPT. In principle, the distinction between whether the work was created by AI or by humans using AI also applies.[260] Works within the meaning of Section 2 UrhG are only the latter. [261] This is because the human action consists solely in specifying certain categories by means of keywords and moods, and this is not usually sufficient to attribute sufficient control over the specific result to the person acting. In this respect, the person acting remains only the initiator of a largely random process. [262] This is because even the creation of a complex prompt serves only to enable the LLM to take over the creative act, and not the human being. It is true that different actions can interact in such a way that individual human actions, which in themselves do not sufficiently determine the end result, can be sufficient in combination with other actions,[263] but the prompt alone has so little to do with the creative act that it is not decisive for the subsequent work, because the creative act must be an achievement that goes beyond the mere selection of AI-generated designs in order to achieve a sufficient degree of human achievement. [264]

The literature rightly argues that tools such as ChatGPT for texts, Dall-E 2, Midjourney for images, or beatoven for musical compositions, which are available to end users, must generally be denied protection. [265]

[260] Olbrich/Bongers/Pampel GRUR 2022, 870

[261] Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, Section 2, margin number 57.

[262] Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, Section 2, margin number 57.

[263] Ehinger/Grünberg K&R 2019, 232 (236); Grätz, Artificial Intelligence in Copyright Law, 2021, p. 101; also referring to interaction in which the AI system can be expected to take specific action based on human creative activity (Specht-Riemenschneider FS Taeger, p. 711 (717 f.)).

[264] Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, Section 2, margin number 57.

[265] v. Welser GRUR-Prax 2023, 2023, 57 (58)); Rauer/Bibi BeckOK Urheberrecht (Copyright), Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024 § 2 Rn. 59.

3. Copyright protection for prompts

This is, of course, separate from the question of whether the prompt alone should be granted copyright protection under Section 2(2) of the UrhG. In addition to being the personal creation of a human being, "intellectual" effort must also be required. [266]However, this element is not defined in more detail and remains abstract. [267]It is generally interpreted broadly. [268] In the literature, the intellectual content of the creative process is described as "thought or emotional content" that "has an entertaining, instructive, illustrative, edifying, or otherwise stimulating effect on the reader, listener, or viewer." [269]

As a result, it depends heavily on the individual case whether a prompt alone enjoys copyright protection under Section 2 (2) UrhG. This question would probably be of little practical significance, since it is always the response to the prompt that matters.

4. Selection of answers

Another question is whether, if the LLM merely makes suggestions and the person acting is allowed to decide which work is actually created, such participation in the output is such that the creative act lies with the human being. [270]The design of the product could be attributed to an intellectual act of creation, with the machine merely being an auxiliary or executive means. [271]

If sufficient human control is affirmed in individual cases, it will be crucial to examine the extent to which the remaining requirements of the

[266] Dreier/Schulze/Schulze margin note 12; Schricker/Loewenheim/Loewenheim/Leistner margin note 45

[267] BeckOK UrhR/Rauer/Bibi UrhG § 2 margin note 61.

[268] cf. Schricker/Loewenheim/Loewenheim/Leistner margin note 46

[269] See Dreier/Schulze/Schulze, margin note 12; similarly, focusing on a sensory effect, Erdmann FS v. Gamm, 1990, 389 (399 f.))

[270] He was unable to complete his 10th symphony before his death in Vienna in 1827, leaving behind only a few sketches and notes. Based on these, a team of experts, including musicologists and programmers, developed artificial intelligence (AI) to fill in the gaps. https://www.zeit.de/news/2021-10/09/von-ki-vollendete-10-sinfonie-von-beethoven-uraufge-fuehrt?utm_referrer=https%3A%2F%2Fwww.google.com%2F

[271] BeckOK UrhR/Ahlberg, 32nd ed. 15.9.2021, UrhG § 2 Rn. 55

Concepts that can be affirmed in elements controlled by human performance.[272] In particular, originality must be sufficiently reflected in these design elements.[273] However, the decisive factor here is not the question of control over the work, but rather the creative act, and this still lies with the LLM, even when control over the work to be produced is exercised.[274]

IV. Is the output of LLMs a trade secret?

The question of whether the output of large language models (LLMs) such as GPT-3 or GPT-4 can be considered a trade secret under Section 2 of the Trade Secrets Protection Act (GeschGehG) in Germany depends on several factors.

1. Prerequisite § 2 GeschGehG

According to § 2 GeschGehG, a trade secret is defined as information

a) that is not generally known or readily accessible and is therefore of economic value,

b) is subject to confidentiality measures appropriate to the circumstances by its lawful owner, and

c) in which there is a legitimate interest in keeping it secret.

In order to assess whether the output of LLMs falls under this definition, the following aspects must be taken into account:

a) Economic value, cf. Section 2 (1) (a) GeschGehG

The output of an LLM could have economic value for a company, especially if it generates specific, customized information or analysis that is important for the company's business strategy or operations.

---

272 Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, Section 2, margin note 60.

273 Kuschel/Asmussen/Golla/Hacker, Intelligent Systems – Intelligent Law, 2021, p. 227 ff.

274 See the question, which should rightly be rejected, as to whether an "AI work" is also subject to the protection of a database work under Section 4 (2) UrhG due to the potentially creative selection of training data (Leistner FS Dreier 2022, 87 (90 f.)).

Benefits. The economic or commercial interest is not defined by the EU legislator, but is explained by means of examples in recital 14 of Directive (EU) 2016/943.[275] It states: "Such a definition should therefore be such that it covers know-how, business information, and technological information [...]. Clearly covered is secret information which, if sold or licensed, would be likely to generate positive income." [276]

b) Confidentiality measures, see Section 2 (1) (b) GeschGehG

It must be demonstrated that the company has taken appropriate measures to keep the output of the LLM secret. This could include the use of encryption, access controls, or other security measures. With this element, the GeschGehG makes it clear that only those who actively protect secret information enjoy the protection of the legal system.[277]However, the protection of legitimate expectations and the prohibition of impermissible retroactive effect of laws require that appropriate confidentiality measures only be required from the date of entry into force of the GeschGehG. [278]The confidentiality measures must therefore have been in place without interruption from April 26, 2019, to the present.[279] However, even more than three years after the law came into force, it is still not clear what this means in concrete terms, or "still unclear." [280, 281]

c) Legitimate interest in confidentiality, cf. Section 2 (1) (c) Gesch-GehG

The company must have a legitimate interest in keeping the information confidential. This could be the case if the publication of the output

[275] Recital 14 of Directive (EU) 2016/943.

[276] BeckOK GeschGehG/Hiéramente GeschGehG Section 2 marginal number 16.

[277] OLG Schleswig GRUR-RS 2022, 9007, para. 51 with further references.

[278] OLG Düsseldorf GRUR-RS 2021, 17483

[279] also OLG Stuttgart GRUR-RS 2020, 35613

[280] Higher Regional Court of Schleswig GRUR-RS 2022, 9007, para. 52

[281] BeckOK GeschGehG/Hiéramente GeschGehG § 2 para. 16.

could impair the competitive position of the company. The legitimate interest in confidentiality serves primarily to clarify and distinguish between cases of minor importance, where a violation should not result in (criminal) sanctions under the GeschGehG.[282] Since the disclosure of a trade secret is punishable under German law in many cases pursuant to Section 23, the criterion of "legitimate interest" is also to be understood as a corrective measure that allows the courts to classify information as a trade secret independently and to review the arbitrariness of the decision.[283, 284]

2. In summary, with reference to the GeschGehG

According to the intention of the legislator, the term "trade secret" now used is intended to cover both commercial and technical knowledge and thus replace the pair of terms "trade and business secrets."[285] However, it should be noted that the output of an LLM is often based on publicly available data and in many cases generates generic responses that may not be considered unique or readily accessible. In such cases, it may be difficult to classify the output as a trade secret. In addition, the fact that the output is reproducible—i.e., that others with access to the same or a similar LLM could generate similar outputs—could argue against classification as a trade secret. Ultimately, the classification of LLM output as trade secrets would depend on the specific circumstances of each case, including the nature of the output, how it is used, and the protective measures taken.

[282] See also OLG Schleswig GRUR-RS 2022, 9007, para. 91; critical with regard to the continuation of the old case law Köhler/Born-kamm/Feddersen/Alexander para. 75 et seq.

[283] See also OLG Schleswig GRUR-RS 2022, 9007, para. 91; critical with regard to the continuation of the old case law Köhler/Born-kamm/Feddersen/Alexander para. 75 f

[284] BeckOK GeschGehG/Hiéramente GeschGehG § 2 margin note 71.

[285] BeckOK GeschGehG/Hiéramente GeschGehG § 2 margin note 1, 1.1

IV. Summary

As a result, it can be concluded that the output of LLMs does not generally provide for copyright protection or protection under the GeschGehG.

D. Hallucination

It is well known that AI systems can hallucinate, which also raises legal questions, as the Munich Regional Court has already had to decide.

I. Definition

In the field of artificial intelligence (AI), a hallucination (also known as confabulation) is a convincingly formulated result produced by AI that does not appear to be justified by training data and may be objectively incorrect. [286] The head of Google Search, Prabhakar Raghavan, described hallucinations by chatbots as convincingly formulated but largely fabricated results.[287]

The introduction of large language models (LLMs) such as ChatGPT and Google's Gemini has also led to hallucinations. Users complained that such chatbots often embedded random lies that sounded plausibly meaningless in the content they generated. For example, when ChatGPT was asked to generate an article about a particular company's last financial quarter, it created a coherent article but invented the financial figures it contained. [289] When asked about astrophysical magnetic fields, ChatGPT incorrectly claimed that magnetic fields are generated by black holes due to the extremely strong gravitational forces in their vicinity. In reality, a black hole has no magnetic field due to the no-hair theorem. [290] In the German context, hallucinations would also occur if asked about Bettina Wulff's profession or whether the city of Bielefeld really exists. This is because there is more false information than correct information on the internet, and this leads to the corresponding mathematical-statistical

[286] Craig S. Smith: AI Hallucinations Could Blunt ChatGPT's Success. In: IEEE Spectrum, March 24, 2023. Retrieved September 24, 2023 (English)

[287] Google cautions against hallucinating chatbots, report says. Reuters, February 11, 2023. Retrieved November 24, 2024 (English)

[288] Christian J. Meier: Why AI likes to lie so much. In: Süddeutsche Zeitung, March 28, 2023. Retrieved on November 24, 2024

[289] : Source Wikipedia, search term "Hallucination (artificial intelligence)" Retrieved on Nov. 24, 2024

[290] Ziwie Ji et al.: Survey of hallucination in natural language generation. In: ACM Computing Surveys, 55(12), pp. 1–38, 2023 (English)

results. Analysts consider frequent hallucinations to be a major problem with LLM technology. [291]

II. Legal assessment

It seems more than difficult to classify a hallucination as a material defect within the meaning of § 434, § 633 BGB or a product defect within the meaning of § 327e BGB and will pose particular challenges for the courts in the future.

1. Material defect vs. product defect

The distinction between a material defect and a product defect is based on the contractual basis. In the case of sales contracts for a physical item that includes AI (e.g., a device with pre-installed AI). For example, an AI-supported diagnostic machine that produces hallucinations has a material defect if the malfunction already exists at the time of transfer of risk. In the case of contracts for digital content or services that fall under the application of Section 327e BGB, the following case would be conceivable: An example would be an AI system that provides a cloud service or digital license, in which case the standards of Section 327e BGB apply. Hallucinations that produce incorrect results are then a product defect, especially if the malfunction is exacerbated by updates.

a) Material defect in the purchase contract

If a manufacturer of an AI system, which consists, for example, of a robot or an algorithm, wishes to sell it in accordance with Section 433 of the German Civil Code (BGB), it is naturally also subject to liability for defects if a defect within the meaning of Section 434 BGB exists. The purchaser of the AI system is then entitled to the rights under §§ 437 et seq. BGB. In robotics, defects can occur primarily in the mechanics of the machine; defects in AI algorithms appear to be more difficult to prove. In the absence of practical experience with liability for defects in AI algorithms, only an analogy to liability for defects in software and its

[291] : Source Wikipedia, search term "Hallucination (artificial intelligence)" Retrieved on November 24, 2024.

Source code serves as an example. According to prevailing opinion [292], an analogy can be drawn when the "interests are comparable" and the absence of a suitable legal norm constitutes an "unintended regulatory gap." If it is a bare algorithm as a mathematical-logical chain, such as the BMI code, then no comparable interest can be assumed, since an algorithm does not give commands to a machine, which is certainly the case with source code. A comparable interest can be assumed if the source code also contains a smaller part of an algorithm. A simple example would be a mobile phone app that calculates a BMI value. The algorithm would be relatively small in relation to the source code because the source code that generates the app's user interface is likely to be significantly more extensive than the BMI algorithm. However, the Federal Court of Justice [293] is of the opinion that, in individual cases, the specific application and linking of algorithms in a program, as well as the manner of their implementation and assignment to each other, may be eligible for copyright protection, which is likely to lead to a comparable investment of interest. In such a case, liability for material defects can also be assumed for an algorithm that is integrated into software. The determination of a defect for a pure algorithm is likely to be governed by Section 475b BGB in accordance with the general principles of Section 434 BGB. In principle, a defect within the meaning of Section 434(1) BGB already exists if the AI system does not correspond to the contractually agreed quality (Section 434(2) No. 1 BGB) or is not suitable for the use specified in the contract (Section 434(2) No. 2 BGB). [294] What applies to the software program naturally also applies to the underlying source code. According to the analogy described above, what applies to the source code of software also applies to an AI algorithm if it is part of software.

In the case of the error category "contractually agreed quality" within the meaning of Section 434 (2) No. 1 of the German Civil Code (BGB), the seller is only liable for defects if he has been advised of the defect by the buyer within the period specified in the contract or, in the absence of such a period, within

2 No. 1 BGB, no complicated expert opinions are required and

[292] *Rüthers/Fuscher/Birk,* Legal Theory with Legal Methodology, 10th edition, 2018.

[293] B G H , October 4, 1990 - I ZR 139/89 - "Betriebssystem" (= BGHZ 112, 264, NJW 1991, 123; ZIP 1991, 191; MDR 1991, 503, GRUR 1991, 449; BB 1991, 1; BB 1991, 2; DB 1991, 587; ZUM 1991, 246.

[294] *Spindler,* CR 2015, 766 to 776.

Disputes between the parties. This is because the only issue here is whether a particular service is provided in accordance with the contract. In practice, the question of manufacturer liability will arise, for example, depending on whether the algorithm calculates correctly or not, whether it is truly logical. The courts have far greater difficulty with the second category, cf. Section 434 (2) No. 2 BGB. It is argued that the contractual agreement should expressly specify the target provisions. [295] In contrast, the area of contractually stipulated use regulates the area of implicitly agreed criteria.[296] This would be the case, for example, in the product description of AI technology. The situation is similar if the desired functions, e.g., of algorithms, have been discussed and jointly accepted with the manufacturer of the AI system during contract negotiations. [297] In practice, the requirements for the AI algorithm will have to be specified in concrete terms, e.g., what should be the search results of an AI algorithm used for deep learning, or what does the customer want to achieve with it. According to Section 434(3)(1) of the German Civil Code (BGB), an important criterion for the defectiveness of an AI algorithm may be its normal use. When determining suitability for normal use, which must be determined objectively, the focus must be on what the buyer can expect. This is determined by the expectations of the average buyer. All actual, legal, economic, and social circumstances that, according to common opinion, directly influence the value and usability of the item are relevant to the nature of the purchased item. [298] However proving normal use is not easy. According to Section 434(5) BGB, the delivery of another item is equivalent to a material defect. In this respect, the previously central problem that the delivery of standard software is part of a generic obligation and that defective software was therefore to be regarded as aliud has also been eliminated since the reform of the law of obligations. [299]

---

[295] *Hoeren,* IT Contract Law 2018, p. 150.

[296] See also: *Saenger*, in HK-BGB, 9th ed. 2017, § 434 marginal no. 11.; *Weidenkaff*, in: Palandt, 76th ed. 2017, § 434 marginal no. 21; *Matusche-Beckmann,* in: Staudinger, 15th ed. 2014, § 434 marginal no. 73; dissenting opinion *Westermann,* BGB, 7th ed. 2016, § 434 marginal no. 18 et seq.

[297] See LG Frankfurt, November 4, 1986 – 2/8 S 83/86, IuR 1987, 229.

[298] Munich Higher Regional Court, September 15, 2004 – 18 U 2176/04, NJW-RR 2005, 494= NZV 2005, 309.

[299] *Hoeren,* IT Contract Law, 2018, p. 149.

If an item is defective, the buyer may, if the requirements of the following provisions are met and unless otherwise specified, demand subsequent performance in accordance with Section 439(1) of the German Civil Code (BGB), withdraw from the contract in accordance with Section 439(2) BGB and Sections 440, 323 and 326 (5) of the BGB, or reduce the purchase price in accordance with § 441 and claim damages in accordance with § 439 (3) and §§ 440, 280, 281, 283 and 311a BGB or, in accordance with

§ 284 BGB Demand compensation for futile expenses. In principle, the claim for subsequent performance may also be linked to a deadline set in advance. [300] The wording of § 437 BGB already indicates that something else may be specified. This naturally refers to contractual provisions that may deviate from the provisions of Section 437 et seq. BGB. [301] The same applies in contract law pursuant to Sections 634 et seq. BGB. According to § 634 BGB, if the work is defective and the following conditions are met, and unless otherwise specified, the customer may, pursuant to paragraph 1, demand subsequent performance, pursuant to paragraph 2, remedy the defect itself and demand reimbursement of the necessary expenses, pursuant to paragraph 3 withdraw from the contract in accordance with §§ 636, 323 and 326. 5 BGB or reduce the remuneration in accordance with § 638 and, in accordance with para. 4, claim damages in accordance with §§ 636, 280, 281, 283, and 311a BGB, or compensation for futile expenses in accordance with § 284 BGB.

According to Section 309 No. 8b of the German Civil Code (BGB), in the case of standard form contracts, a provision regarding deliveries of newly manufactured goods and work performance excludes claims against the user for defects in whole or in part.[302] This is aimed in particular at protecting the customer from the erosion of his statutory rights in respect of defects and at ensuring that the equivalence of performance and consideration can be enforced even in the event of defective performance by the user. [303] This fundamental concern must also be taken into account in the drafting of contracts in commercial transactions.

[300] *Palandt/Putzo*, 77th ed. 2017, § 439 Rn. 3.
[301] For more details, see *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 11th edition, 2021, margin number 81 et seq.
[302] *Stoffels,* AGB-Recht (Law on General Terms and Conditions), 5th edition, 2024, margin number 959 et seq.
[303] *Palandt/Grüneberg*, 72nd edition, 2013, Section 309, margin number 72.

Take into account. [304]The extent to which the customer is prepared to have their rights to compensation or reduction limited in accordance with §§ 437 et seq. BGB or §§ 634 et seq. BGB certainly depends on the individual case.

The seller is not only obliged to pay compensation in accordance with Sections 437 No. 3, 280 BGB if he is responsible for the material defect in accordance with Sections 276, 278 BGB, but also if he cannot prove that he is not responsible for it, as the law presumes that the seller is responsible for the material defect.[305] According to Sections 280 (1) sentence 2, 286 (4) BGB, the seller's fault is not a prerequisite for a claim; rather, his lack of fault constitutes a defense that precludes a claim, which the seller must prove. He must rebut the legal presumption of fault and prove the contrary, i.e. his lack of fault (Section 292 ZPO). The negative version of Section 280 (1) No. 2 BGB reads: "This does not apply if the debtor is not responsible for the breach of duty." If, upon closer examination, it transpires that a defect is not the responsibility of the contractor and therefore does not constitute a warranty claim, the client must reimburse the contractor for the costs incurred in searching for the defect. If the client demands that the contractor remedy the defects even though the contractor is not responsible for remedying them, the parties shall conclude a contract for work and services in accordance with §§ 631 et seq. BGB, which shall be remunerated accordingly by the client.

Once the claim has become time-barred, the debtor may permanently refuse performance pursuant to Section 241 (1) BGB. The claim does not expire as a result of the limitation period, but is merely suspended. [306] However, the suspension is permanent, meaning that the claim cannot be enforced against the will of the debtor.

[304] *Stoffels,* AGB-Recht, 5th ed. 2024, margin no. 959 etseq.

[305] *Schellhammer*, Law of Obligations According to the Basis of Claims, 8th ed. 2011, margin no. 1641.

[306] Federal Court of Justice, October 2, 2003 – V ZB 22/03= BGHZ 156, 269; NJW 2004, 164; MDR 2004, 167; NJ 2004, 225; FamRZ 2004, 176; VersR 2004, 803; WM 2004, 843; BB 2003, 2595; JR 2004, 419; Federal Court of Justice, May 19, 2006 - V ZR 40/05 = NJW 2006, 2773; MDR 2006, 1272; DNotZ 2006, 849; NZBau 2006, 645; WM 2006, 1913; BauR 2006, 1464; IBR 2006, 447.

the debtor, the claim is no longer enforceable. [307] Thus, an action based on a claim that is time-barred must be dismissed as unfounded with full legal effect pursuant to § 322 (1) ZPO if the debtor asserts the defense of limitation. [308] It is not the expiry of the limitation period itself, but only the debtor's justified refusal to perform after the expiry of the limitation period that permanently bars the claim. [309] Sections 195 to 198 of the BGB regulate the statutory limitation periods in the BGB, whereby claims become time-barred after 3, 10, or 30 years. According to Section 195 BGB, the regular limitation period is three years. Claims for material defects by buyers, on the other hand, have their own limitation rules, which differ from the standard limitation period in Sections 195 and 199 BGB in terms of duration and commencement. [310] According to Section 438(1) BGB, claims for defects become time-barred as follows: The

Claims specified in § 437 No. 1 and 3 shall become time-barred 1. in 30 years if the defect

a) in a right in rem of a third party on the basis of which the purchase item can be demanded, or b) in any other right entered in the land register, 2. in five years a) in the case of a building and b) in the case of an item that has been used for a building in accordance with its normal use and has caused its defectiveness, and 3. in all other cases in two years.

I. d. R In the IT industry (if, for example, a data center is constructed as a building), the statutory provision under Ziffer 3 of 2 years applies. The extension of the warranty period eliminates the problems of short limitation periods for systems and software in particular, where defects only become apparent after prolonged use, but ultimately means that in many cases the warranty is extended to cover the entire economic life of the product as a substitute for maintenance. This certainly does not apply to an AI algorithm, as there are generally no maintenance contracts for algorithms.

[307] Federal Court of Justice, December 4, 2007 – XI ZR 144/06= NJW 2008, 1312; IBR 2008, 189; BauR 2008, 666; Federal Court of Justice, January 27, 2010 - VIII ZR 58/09= BGHZ 184, 128; NJW 2010, 2422; NJW 2010, 8; MDR 2010, 650; NZM 2010, 511; ZMR 2010, 591; NJ 2010, 343; FamRZ 2010, 887; WM 2010, 986; BB 2010, 1034; JR 2010, 395; IBR 2010, 730.

[308] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 8th edition, 2011, margin number 2473.

[309] Federal Court of Justice, October 2, 2003 – V ZB 22/03= BGHZ 156, 269; NJW 2004, 164; MDR 2004, 167; NJ 2004, 225; FamRZ 2004, 176; VersR 2004, 803; WM 2004, 843; BB 2003, 2595; JR 2004, 419; Federal Court of Justice, January 27, 2010 - VIII ZR 58/09= BGHZ 184, 128; NJW 2010, 2422; NJW 2010, 8; MDR 2010, 650; NZM 2010, 511; ZMR 2010, 591; NJ 2010, 343; FamRZ 2010, 887; WM 2010, 986; BB 2010, 1034; JR 2010, 395; IBR 2010, 730.

[310] Federal Court of Justice, November 15, 2006 – VIII ZR 3/06= BGHZ 170, 31; NJW 2007, 674; ZIP 2007, 131; MDR 2007, 450; DNotZ 2007, 364; WM 2007, 261; BB 2007, 177; IBR 2008, 145; IBR 2008, 20; *Gramer/Thalhofer,* ZGS 2006, 250; *Auktor,* NJW 2003, 120.

According to Section 438 (2) BGB, the limitation period begins with the delivery of the purchased movable item.[311] This also applies if the claim under § 281 BGB or § 284 BGB has not yet arisen before the expiry of the grace period. [312] The commencement of the limitation period does not depend on the discovery of the defect; even hidden defects become time-barred upon handover or delivery. [313]

b) Material defect in a contract for work and services

Section 634a of the German Civil Code (BGB) provides for three different limitation periods for claims for subsequent performance, self-performance, and compensation listed in Section 634 BGB in the case of defects in work performance. Since withdrawal and reduction are not claims but rather rights to structural changes, they are not subject to the limitation periods set out in Section 634a BGB (see Sections 218(1) and 634a(5) BGB in this regard).[314] According to Section 634a (1) No. 1 BGB, claims for work whose success consists in the manufacture, maintenance, or modification of an item or in the provision of planning or monitoring services for this purpose shall become time-barred after two years.[315] According to Section 634a No. 3 BGB, claims in other respects, i.e., for intangible work, unless they fall under planning or monitoring services under Section 634a No. 1 or No. 2, become time-barred after the regular limitation period of Section 195 BGB in three years. It is questionable what an AI algorithm falls under. This includes, for example, the preparation of a legal opinion, a tax return, or a risk analysis. 3[16]Whether the creation of software is to be classified as an intangible work performance pursuant to Section 634a No. 3 BGB is a question that has not yet been expressly decided by the Federal Court of Justice (BGH).

[311] B G H , November 29, 1972 - VIII ZR 122/71= BGHZ 60, 5; NJW 1973, 189; BGH, November 4, 1992 - VIII ZR 165/91= NJW 1993, 461; MDR 1993, 121; WM 1993, 111; BB 1993, suppl. 13; DB 1993, 424; JR 1993, 406; BGH, judgment of October 11, 1995= NJW 1995, 3381; LM H. 2/1996 § 477 BGB No. 62; MDR 1996, 132 ; JZ 1996, 257; BB 1995, 2394; DB 1995, 2520; ZIP 1995, 1822; Higher Regional Court of Celle, June 20, 2006 - 16 U 287/05 = NJW 2006, 2643; MDR 2007, 137; IBR 2006, 492; BauR 2006, 1801 (Ls.).

[312] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations according to Legal Bases), 8th edition, 2011, margin number 2473.

[313] Federal Court of Justice, June 2, 1980 – VIII ZR 78/79= BGHZ 77, 215; NJW 1980, 1950; WM 1980, 1035.

[314] *Bonnmann/Erberich,* in: Luther/Knot/Palm, Die Schuldrechtsreform, 2001, p. 106.

[315] Critical in the distinction *Zimmermann/Leenen/Mansell/Ernst*, JZ 2001, 684, 690 f.

[316] *Bonnmann/Erberich,* in: Luther/Knot/Palm, Die Schuldrechtsreform (The Reform of the Law of Obligations), 2001, p. 106.

Question [317] The Federal Court of Justice applies the rules on material defects without, however, stating that software is a thing, let alone whether it is physical or not. [318] If at a later date, case law clearly establishes that software is not a thing, the limitation period would be three years.[319] Since the creation of an AI algorithm is certainly an intangible work, the statutory provision of the regular limitation period of three years under Section 195 BGB should apply here.

c) Product defect

In contrast to material defects in sales or contract law, product defects within the meaning of Section 327e BGB take precedence in contracts for digital content or services. [320] Example: If AI is provided as a cloud service or digital license, the standards of Section 327e BGB apply. Hallucinations that produce incorrect results are then a product defect, especially if the malfunction is exacerbated by updates.

Section 327e BGB regulates the defectiveness of digital products within the framework of a consumer contract for digital content or digital services. A digital product is defective if it:[321]

- Does not have the agreed quality (Section 327e (2) sentence 1 BGB):
- The contractually agreed characteristics must be fulfilled. Examples: scope of functions, compatibility, or safety.
- Not suitable for normal use (Section 327e (3) No. 1 BGB):

If a digital product cannot perform the basic functions that an average user can expect, there is a defect.

- Not provided with the current version (Section 327e (3) No. 2 BGB):

[317] The case law begins with BGH, February 11, 1971, WM 1971, 615, 616 and continues, inter alia, BGH, May 5, 1992, CR 1993, 85, 86; BGH, November 24, 1998, NJW-RR 1999, 347, 348.

[318] *Marly* Practical Handbook on Software Law: Legal Protection and Contract Drafting, 7th edition 2018, margin number 101.

[319] *Koch,* CR 2001, 574.

[320] Palandt/Grüneberg, BGB, 83rd edition 2024, Section 327e BGB, margin number 1 et seq.

[321] MüKo/Wendehorst, BGB, 9th edition 2022, § 327e margin number 1 et seq.

- When providing the product, the supplier must ensure that the latest version is available, provided that this is contractually required.
- The following is not considered a proper update (Section 327e (3) No. 3 BGB):

Providers are obliged to provide updates that are necessary for the functionality or security of the product.

- Not meeting objective requirements (Section 327e (4) BGB):
- A digital product must meet normal expectations, even if no specific agreements have been made (e.g., reliability, compatibility).

A possible use case would be if AI is used as a "precise analysis tool" for medical diagnoses and the system repeatedly delivers incorrect or inaccurate diagnoses. This means it doesn't meet the contractually agreed quality standards. [322] One way to avoid this could be to say in the contract that the AI system is just a support tool and mistakes can happen, which would rule out any defects.

2. Kiel Regional Court decision

Case law on the defectiveness of AI-based products is still very limited. In a ruling dated February 29, 2024 (Ref. 6 O 151/23), the Regional Court of Kiel addressed the issue of responsibility for content generated by AI.[323] The court was presented with the following facts: A medium-sized company sued a platform operator who had published automatically generated business information. The platform operator evaluates mandatory disclosures from public registers such as the commercial register in a fully automated manner using big data and artificial intelligence. Users can access the data via search queries. Its terms of use state that the data "is obtained through fully automated analysis and may be partially or largely inaccurate." Liability for the

[322] Wendehorst, Christiane: "Regulatory Challenges for AI Products," MüKo-Digitalrecht, 2022.

[323] Kiel Regional Court, February 29, 2024 – 6 O 151/23

He excludes the accuracy of the economic data. Due to an incorrect AI-supported allocation process, the imminent deletion of the company due to insolvency was falsely suggested. The plaintiff demanded the cessation of the dissemination of incorrect information and compensation for pre-trial legal costs.

The court found that the general right of personality also protects a company's social standing. The dissemination of false information by the platform violated this right. The defendant could not invoke liability privileges under the Telemedia Act because it had adopted the AI-generated content as its own. A disclaimer contained in the terms and conditions, which excluded responsibility for AI-generated content, was deemed invalid. The Regional Court of Kiel ruled in favor of the family-owned company, ordering the business information service to refrain from claiming that it intended to delete the content due to lack of funds (judgment of February 29, 2024 - 6 O 151/23). It affirmed the service's liability as a disruptor for violation of the company's personality rights under § 1004 BGB (German Civil Code) by analogy. The service was deemed to be the direct infringer because it uses its own software to respond to search queries, which extracts information from the published mandatory disclosures, processes it, and publishes it. It could not claim that it was not involved in the automatic process at all, as it had deliberately used AI, which had been programmed incorrectly.

Furthermore, the service had appropriated the data provided and had assumed responsibility for its content in a manner recognizable to the public. This was because it bundled the mandatory disclosures relating to a company on its website and linked some of the information to each other.

The Regional Court also affirmed the risk of repetition. It saw such a risk confirmed precisely by the service's objection that it only publishes third-party data from

[324] See Federal Court of Justice, judgment of December 16, 2014 – VI ZR 39/14, para. 12= NJW 2015, 773.

mandatory disclosures without checking them. According to the service, the mandatory information in the commercial register is unreliable, which can lead to "incorrect advertisements."

The defendant was ordered to refrain from disseminating false information and to reimburse the pre-trial legal costs. The ruling emphasizes the responsibility of platform operators for content generated by the AI systems they use.

The decision makes it clear that the reference to the automation of processes does not constitute a sufficient ground for exoneration if faulty systems cause legally relevant damage. Companies are obliged to ensure, through appropriate and effective control mechanisms, that the AI systems they use function reliably and in compliance with the law. This also applies, of course, if AI systems hallucinate and arrive at incorrect results even though the logic of the AI system is correct.

It is also becoming apparent that liability is not limited to platform operators alone. In the future, providers of AI systems may also be held more accountable, especially if it turns out that faulty systems have caused damage. Providers should therefore proactively ensure that their products comply with the applicable legal and technical standards. This also applies, of course, to operators of platforms in which an AI system exhibits so-called hallucinations and delivers incorrect results, even if the underlying system logic is working correctly.

III. SaaS models for AI

Provided that there is no overriding business relationship within the meaning of Sections 327 et seq. of the German Civil Code (BGB), in particular no B2B transactions to which Sections 327 et seq. BGB apply, it would be legally advantageous for the operator of an AI system to offer its services as a SaaS model. This would also mean that hallucinations would not lead to liability for the operator of the AI system.

1. Definition

Unfortunately, the term SaaS is not used uniformly and is often equated with Application Service Providing (ASP)[325] where the temporary provision of software is the primary focus. The SaaS model is based on the principle that AI systems are operated as software and the IT infrastructure by an external AI provider and used by the customer as a service.[326] Therefore, the following discussion will only refer to true SaaS[327], which only concerns the service provided by the software, but not the provision of the software itself. For this reason, software license agreements are not used for the true SaaS model in practice, but rather subscription agreements (SaaS subscription contracts)[328], in which the customer of the SaaS (hereinafter referred to as the "subscriber") subscribes to a service via the Internet, usually on a monthly basis. No software is installed on the subscriber's computer, nor is any software loaded into the subscriber's main memory.

The Federal Court of Justice ruled back in 2004 that ASP in the form of temporary provision of software is to be regarded as rental. [329]The classification of SaaS is not quite as clear-cut. By using the term "service," one could argue that it is similar to a service contract under
§§ 611 et seq BGB. [330] The English term "service" is much broader than the German terms "Dienst" or "Dienstleistung." For example, "service" can mean "operation," "maintenance," "cleaning," "transportation," "delivery," "consulting," "training," "information," "data processing," "programming," "software," "software maintenance," "software support," "software development," "software consulting," "software training," "software maintenance," "software support," "software development," "software consulting," "software training," "software maintenance," "software support," "software development," "software consulting", "software training",
"Customer service," "religious service," "maintenance," "operation," "hospitality," "performance," "use," "application," "commemoration," or "inspection."[331] But of course, it always depends on the nature of the main performance obligations agreed upon in the contract. If, as in the ideal SaaS contract, neither software is provided (permanently: purchase; temporarily: rental) nor is any success promised (contract for work), SaaS should be considered a rental.

---

325 The Federal Court of Justice (BGH) has already confirmed in its ASP ruling that the temporary provision of software, including via the Internet, constitutes rental: BGH, November 15, 2006 – XII ZR 120/04= NJW 2007, 2394; MDR 2007, 257; NZM 2007, 379; WM 2007, 467; MMR 2007, 243; K&R 2007, 91; K&R 2007, 385.

326 http://de.wikipedia.org/wiki/Software_as_a_Service (accessed on October 28, 2022).

327 For the distinction between ASP/non-genuine SaaS and genuine SaaS models, see *Söbbing*, ITRB 2021, 168–171.

328 https://saasoptics.com/saaspedia/saas-subscription-models/ (accessed on October 28, 2022).

329 Federal Court of Justice, MMR 2007, 243 (244).

330 *Pohle/Ammann*, K&R 2009, 625 (626).

331 *Heydn*, MMR 2020, 435

The contract would still be subject to employment law. Based on genuine SaaS, it might not be necessary for the SaaS provider (hereinafter referred to as the "provider") to grant its subscribers rights to the provider's software. If this idea is taken to its logical conclusion, it would lead to a radical rethink, as lengthy discussions about copyright clauses would become obsolete. The following must of course be distinguished from this: If the output of the SaaS/AI system leads to copyright-protected works and these have been created exclusively by the subscribers, these are also only available to the subscribers. However, this would not need to be regulated in the SaaS contract, as authorship is generally already regulated by law, cf. Section 7 et seq. UrhG.

When classifying such remote rights of use within the system of copyright usage and exploitation rights, the focus should be on the copyrighted work as such (or, conceptually, on the software copy) and not on the use per se. This applies to the right of reproduction, the right of distribution or rental, and the right of making available to the public. [332] This raises the question of whether SaaS constitutes permanent or temporary reproduction, in whole or in part, of a computer program within the meaning of Section 69c (1) UrhG. If one goes on to ask to what extent the use of software in SaaS is relevant to copyright, one comes across Section 69c (4) UrhG. According to this, the copyright holder has the exclusive right to make a computer program available to the public by wire or wireless means, including making it available to the public in such a way that it can be accessed by members of the public at places and times of their choosing.

2. Reproduction

In principle, the installation of software on the customer's IT system[333] as well as the downloading the software in the working memory of the customer[334] constitutes a

[332] *Grützmacher*, CR 2015, 779–787.

[333] Federal Court of Justice, January 20, 1994, I ZR 267,91= NJW 1994, 1216, 1217.

[334] Federal Court of Justice, October 4, 1990, I ZR 139/89= NJW 1991, 1231, 1234.

reproduction within the meaning of Section 69c No. 1 UrhG.[335] By loading the software into the customer's working memory, the ASP could regularly be engaging in an act of reproduction within the meaning of Section 69c No. 1 UrhG, even if the rental agreement does not provide for a transfer of ownership, but merely a transfer of use.[336] The question of whether a physical transfer of a work is required for a rental within the meaning of copyright law can be left open, as no software is loaded into the subscriber's main memory in the case of SaaS.

Fundamentally, one must ask to what extent acts of reproduction are attributable to the provider or the customer. In its Internet video recorder ruling [339], the Federal Court of Justice stated that the question of who is the producer of a reproduction depends primarily on a technical assessment, not on value judgments. According to this, the person who technically accomplishes and controls the physical fixation is the one who reproduces the work. [340]In a SaaS infrastructure, if the user initiates the loading into the working memory of a specific computer, this reproduction is attributable to the user.[341] In SaaS practice, the reproduction process within the meaning of the Federal Court of Justice (BGH) (accomplishment and control) cannot be attributed to the subscriber, as the subscriber cannot accomplish or control this or determine how and where storage takes place. Therefore, the reproductions can (in many cases) only be attributed to the provider. [342] This is because the manufacturer of the reproduction is the person who technically carries out this physical fixation. It is irrelevant here whether they use technical aids, even if these are provided by third parties. [343]

It is questionable whether a right of reproduction must be granted for the web form provided by the provider. This is because user interfaces, web forms, and

335 *Marly*, Software Transfer Agreements, 7th ed. 2018, para. 1127.

336 Federal Court of Justice, November 15, 2006 – XII ZR 120/04= NJW 2007, 2394.

337 *Marly*, Software Transfer Agreements, 7th ed. 2018, margin no. 1128.

338 It is already argued that ASP does not constitute rental due to the lack of physical transfer, see, for example, *Wandtke/Bullinger/Grützmacher*, Section 69c marginal no. 5; *Bettinger/Scheffelt*, CR 2001, 729, 734; *Alpert*, CR 2000, 345, 347; *Marly*, Softwareüber-license agreements, 7th edition, 2018, margin number 1128.

339 Federal Court of Justice, April 22, 2009 – I ZR 216/06, CR 2009, 598.

340 See also *Paul/Niemann* in Hilber, Handbook on Cloud Computing, 1st edition 2014, Part 3, margin number 94.

341 *Niemann/Paul,* CR 2009, 661 (662); *Marly*, Softwareüberlassungsverträge (Software Transfer Agreements), 7th edition, 2018, margin number 1151.

342 *Niemann/Paul*, K&R 2009, 444 (448).

343 *Grützmacher*, CR 2015, 779–787.

screen masks may be protected as scientific and technical representations pursuant to Section 2 No. 7 UrhG if, for example, their presentation is characterized by particular user-friendliness. [344] The ECJ has ruled that protection of the graphical user interface is not possible as a computer program, but may be considered under general principles, without, however, commenting on the type of work in question.[345] In order to display the graphical user interface in the subscriber's web browser, it must be copied to the customer's computer's working memory for a short period of time during browsing. There is disagreement as to whether loading into the browser cache (a buffer memory) constitutes reproduction. [346] Recital 33 of the InfoSoc Directive [347] reads:

"*An exception to the exclusive reproduction right should be granted for certain temporary acts of reproduction which are transient or incidental, form an integral and essential part of a technological process and are solely intended to enable either the efficient transmission in a network between third parties by an intermediary or the lawful use of a work or other subject matter.*"

Provided that these conditions are met, this exception also covers acts that enable browsing and caching; This includes acts that enable the efficient functioning of the transmission systems, provided that the intermediary does not alter the information and does not impair the permitted use of technologies for collecting data on the use of the information that are widely recognized and used by the commercial sector.[348] Use should be considered lawful to the extent that it is authorized by the rightholder or not restricted by law. [349] In principle, it must be analyzed which copyright

[344] Higher Regional Courtof Karlsruhe, April 14, 2010 – 6 U 46/09, GRUR 2010, 533 (Ls.).

[345] ECJ, December 22, 2010 – C-393/09, CR 2011, 220; but see there: *"It is for the national court to determine, taking into account, in particular, the arrangement or specific configuration of all the components of the graphical user interface, whether this is the case in order to be able to determine which of them satisfy the criterion of originality. In this context, this criterion cannot be satisfied by components of the graphical user interface which are characterized solely by their technical function."*

[346] The dispute is discussed in detail by *Loewenheim* in Schricker/Loewenheim, Urheberrecht, 6th ed. 2020, § 16, para. 21.

[347] Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 on the harmonization of certain aspects of copyright and related rights in the information society

[348] *Söbbing*, ITRB 2021, 168–171.

[349] *Paul/Niemann* in Hilber, Handbook of Cloud Computing, 1st edition 2014, Part 3, margin number 95.

content is actually stored in the browser or client cache. This is because, as a rule, the software used by the provider is not stored in the cache of the customer's computer, but only the subscriber's data, to which the subscriber has exclusive rights of use and therefore also the right of reproduction. The essence of SaaS is precisely that the computing operations are performed by the provider and not by the subscriber.[350] This is because the mere reproduction of the screen display at the subscriber's premises does not in itself constitute an act of reproduction within the meaning of Section 69c No. 1 UrhG. [351] Where applicable the data to be transmitted could constitute a copyright-protected work within the meaning of Section 87a UrhG. It must also be examined in each individual case to what extent, within the framework of a SaaS application within the meaning of Section 87b UrhG, insignificant parts of a database are repeatedly and systematically transmitted and thus either run counter to the normal exploitation of the database or unreasonably prejudice the legitimate interests of the database manufacturer. [352]

3. Publicly accessible

If there is no act of reproduction within the meaning of Section 69c No. 1 UrhG in the case of SaaS, the question arises as to whether making available to the public pursuant to Sections 69c No. 4, 19a UrhG is permitted, which is controversially discussed in the literature. [353] Pursuant to Sections 69c No. 4, 19a UrhG, making a computer program publicly available requires the consent of the copyright holder of the computer program. Public reproduction occurs when the computer program is made perceptible or accessible to a large number of users who are not personally connected, either simultaneously or successively, in an intangible form.[354]

---

[350] See *Marly*, Softwareüberlassungsverträge (Software License Agreements), 7th ed. 2018, margin no. 1151: at least the reproduction is carried out *jointly* with the provider. *Paul/Niemann* in Hilber, Handbuch Cloud-Computing (Handbook on Cloud Computing), 1st ed. 2014, Part 3, margin no. 91.

[351] This applies at least as long as only pure graphic data is transferred, which will regularly be the case with these offers. The situation may be somewhat different if programs executed on the client side are also transferred, such as Java applets or, more recently, HTML codes, namely in version 540, which contains control commands. *Grützmacher*, CR 2015, 779–787.

[352] *Wiebe*, CR 2013, 1; *Grützmacher*, Copyright, Performance and Sui Generis Protection of Databases, 1999, 340 f.

[353] See, for example on ASP: Munich Higher Regional Court, February 7, 2008 – 29 U 3520/07, GRUR-RR 2009, 91 – ASP; *Marly*, Praxishandbuch Softwarerecht (Practical Handbook on Software Law), 7th edition, 2018, margin number 1087; *Jaeger,* CR 2002, 309 (311); *Lutz,* Softwarelizenzen und die Natur der Sache, Munich 2009, 164 f.; on cloud computing: *Giedke,* Cloud Computing: Eine wirtschaftliche Analyse mit besonderer Berücksichtigung des Urheberrechts, Munich 2013, 402 ff.; *Pohle/Ammann,* CR 2009, 273 (276); *Niemann/Paul,* K&R 2009, 444 (448); differentiating *Dietrich,* ZUM 2010, 567 ff.

[354] *Grützmacher* in Wandtke/Bullinger, UrhR, 6th ed. 2022, § 69c, margin no. 50, 80.

Sections 69c (4) and 19a of the UrhG basically cover all forms of public reproduction within the meaning of Sections 15 (2) and 19a of the UrhG, regardless of whether the public reproduction is wireless or wired.[355] Nevertheless, case law and literature oversimplify matters when they equate ASP with SaaS. For example, the Munich Higher Regional Court (OLG München)[356] stated in a much-criticized decision[357] that ASP operation, even without the transfer of program data, constitutes making available to the public within the meaning of Sections 69c No. 4, 19a UrhG. According to the Munich Higher Regional Court, the wording of Sections 69c No. 4, 19a UrhG does not necessarily imply that making a computer program publicly available must necessarily involve the transmission of program parts. According to the Munich Higher Regional Court, the court of first instance is correct in stating that other types of works (plays, musical works) are also made available to the public in a manner that does not involve presenting the work itself in physical form (namely through public performance and not by making the libretto or score available). Furthermore, the interpretation of Section 69c No. 4 UrhG, according to which making a computer program available for interactive retrieval is sufficient as an act of exploitation within the meaning of Section 69c No. 4 UrhG, is in line with the legislature's intention to ensure the earliest possible protection of the rightholder's rights in the computer program against interference by third parties. The clear criticism in the literature is justified because, as *Grützmacher*[358] rightly points out, the Munich Higher Regional Court fails to recognize the technical realities because, in the case of SaaS, no applets or code are transferred or streamed and, as already explained above, only graphic data is transferred, which does not constitute making a computer program available within the meaning of Sections 69c (4) and 19a UrhG. [359]

355 *Dreier/Schulze/Dreier*, UrhG § 69c, margin note 27.

356 Munich Higher Regional Court, February 7, 2008 – 29 U 3520/07, CR 2009, 500 (502).

357 See, for example, *Grützmacher* CR 2015, 779-787; Nägele/JacobsZUM 2010, 281 (287); Niemann, in Hilber, Handbuch Cloud Computing, Cologne 2014, pp. 290 and 293: in general, but in the case of IaaS and PaaS already because of the large amount of software running in the background.

358 *Grützmacher*, CR 2015, 779–787.

359 *Loewenheim* in Schricker/Loewenheim, UrhR, 6th ed. 2020, § 69a margin no. 2; *Haberstumpf* in Lehmann, Chapter II margin number 15, 30; *Mestmäcker/Schulze/Haberstumpf,* Section 69a margin number 3; based on DIN 44300: Higher Regional Court of Düsseldorf, July 12, 1999 – 20 U 40/99, CR 2000, 742 = NJWE-WettbR 2000, 61 – Add-on CD; for the legislative history of the Directive and the details of these provisions, see *Marly,* GRUR 2012, 773, (774 ff.); see also ECJ, May 2, 2012 – Case C-406/10, CR 2012, 428 with note by *Heymann* = GRUR 2012, 814 (815 margin note 39, 42 f.) – SAS Institute; for more details, see *Grützmacher* in Wandtke/Bullinger, UrhR, 6th ed. 2022, Section 69a, para. 3.

Spindler[360] argues that the right to make content publicly available does not depend on whether copies are made by the user, but – as a sub-case of the right of public reproduction – only on the increased use by the public.[361] This also applies to the use of operating system software within the framework of Infrastructure Cloud Services (IaaS) or Platform as a Service (PaaS).[362] If copies of the application are made, this is attributable to the user/subscriber due to their control of the process – and not to the provider,[363] comparable to cases where a copy is made by a third party. This is only different if the user has no influence over whether copies are made by the provider, which is likely to be the case with genuine SaaS and would mean that the provider does not need any additional rights under Sections 69c (4) and 19a UrhG for SaaS. In practice, the SaaS provider is often also the manufacturer of the software and thus the owner of all rights; in this case, the question is less important.

Even if the provider requires a right to public reproduction pursuant to Sections 69c (4) and 19a of the German Copyright Act (UrhG), this does not mean that the provider must grant the subscriber rights to the underlying software. If, pursuant to Section 69c No. 4 UrhG, the "computer program" must be made accessible,[364] reference must be made to the WIPO[365] model provision, which, according to prevailing opinion, also applies within the scope of Section 69a UrhG.[366] According to this provision, it is not sufficient for graphic data to be transferred.[367] This is because

360 *Spindler* in Schricker/Loewenheim, UrhG, 6th edition 2020, Section 69c, margin numbers 41–41c.

361 *Grützmacher* in Wandtke/Bullinger, UrhG, 6th edition 2022, Section 69 c, marginal number 82.

362 See Federal Court of Justice, GRUR 2009, 845 marginal no. 16 – Internet video recorder; *Bisges*, MMR 2012, 574 (577 f.); *Nägele/Jacobs*, ZUM 2010, 281 (286); *Niemann*, CR 2009, 661 (662 f.); *Grützmacher,* CR 2011, 697 (704 f.); *Wandtke/Bullinger/Grützmacher,* UrhG, § 69 c, para. 99; but see (only providers) *Schuster/Reichl,* CR 2010, 38 (40 f.); *Giedke,* p. 382 ff.; similarly *Hilber/Paul/Niemann,* Part 3, margin note 94; not entirely clear *Bräutigam/Thalhofer* in Bräutigam, Part 14, margin note 120, who advise sublicensing.

363 Federal Court of Justice, GRUR 2009, 845 marginal no. 16 – Internet video recorder; *Bisges*, MMR 2012, 574 (577 f.); *Nägele/Jacobs*, ZUM 2010, 281 (286); *Niemann*, CR 2009, 661 (662 f.); *Grützmacher*, CR 2011, 697 (704 f.).; *Wandtke/Bullinger/Grützmacher,* UrhG, Section 69 c, marginal number 99; however, contrary to this (only providers) *Schuster/Reichl,* CR 2010, 38 (40 f.); *Giedke,* p. 382 ff.; similarly *Hilber/Paul/Niemann,* Part 3, margin note 94; not entirely clear *Bräutigam/Thalhofer* in Bräutigam, Part 14, margin note 120, who advise sublicensing.

364 Munich Higher Regional Court, February 7, 2008 – 29 U 3520/07, CR 2009, 500 (502).

(365) World Intellectual Property Organization

366 *Loewenheim* in Schricker/Loewenheim, UrhR, 6th ed. 2020, § 69a, margin no. 2; *Haberstumpf* in Lehmann, Chapter II, margin number 15, 30; *Mestmäcker/Schulze/Haberstumpf* § 69a margin number 3; based on DIN 44300 OLG Düsseldorf, July 12, 1999 – 20 U 40/99, CR 2000, 742 = NJWE-WettbR 2000, 61 – Add-on CD; for the legislative history of the Directive and the details of these provisions, see *Marly,* GRUR 2012, 773, (774 ff.); see also ECJ, May 2, 2012 – Case C-406/10, CR 2012, 428 with note by *Heymann* = GRUR 2012, 814 (815 para. 39, 42 f.) – SAS Institute; for more details, see *Grützmacher* in Wandtke/Bullinger, UrhR, 6th ed. 2022, § 69a, margin no. 3.

367 *Grützmacher*, CR 2015, 779–787.

According to the WIPO definition, a computer program is rather the multitude of control commands.[368]However, in the case of genuine SaaS, these are not usually transmitted and thus made accessible. In this respect, the decision of the Munich Higher Regional Court[369] contradicts the case law on screen masks.([370)] This is because it specifically assumes that the transmitted screen masks do not yet constitute a computer program([371)] and therefore no rights of use need to be granted.[372]

4. Summary

In summary, it can be stated that in the subscription agreement of the SaaS model for an AI system, it is not necessary to grant the subscriber rights of use or reproduction. If the results (services) of the software in the SaaS model reach the level of creativity required under Section 2 (2) of the German Copyright Act (UrhG), authorship would also lie with the subscriber under Sections 7 et seq. of the UrhG, and the operator would therefore not be liable for software in which an AI system is integrated. This would also mean that hallucinations would not lead to liability for the operator of AI systems, as service law does not provide for liability for defects. This only applies, of course, in cases where §§ 327 et seq. BGB do not apply. This does not include claims for damages, e.g. under Section 280(1) BGB.

368 *Grützmacher* in Wandtke/Bullinger, UrhR, 6th ed. 2022, Section 69a, margin no. 3.

369 Munich Higher Regional Court, February 7, 2008 – 29 U 3520/07, CR 2009, 500 (502).

370 ECJ, December 22, 2010 – Case C-393/09, CR 2011, 221= GRUR 2011, 220 (223) – BSA/ Ministry of Culture; Higher Regional Court of Karlsruhe, April 14, 2010 – 6 U 46/09, CR 2010, 427= GRUR-RR 2010, 234.

371 *Grützmacher*, CR 2015, 779–787.

372 See above under II. Reproduction rights.

E. Data protection

The legal relationship between artificial intelligence (AI) and data protection arises from a number of very interesting individual questions, which cannot all be listed here due to space constraints. However, two very interesting individual questions will be addressed below. Namely, the questions: "Does machine learning violate data protection?" and "What legal issues arise in the case of automated (AI) decisions pursuant to h Art. 22 GDPR?"

I. Does machine learning violate the GDPR[373]

In June 2024, the Meta Group planned to use user data from public posts on Facebook and Instagram to train its AI models. This raised data protection concerns because it involved the processing of personal data without the express consent of the users, which meant that the scope of the GDPR was unclear.

If AI (accidentally) collects personal data when reading the internet, this could be unlawful processing within the meaning of Art. 6(1) GDPR, which could result in significant fines under Art. 83 GDPR. Even if the AI Regulation applies, it does not supersede the GDPR, cf. Art. 2 (7) AI Regulation. The issue of data protection will play a significant role in the battle for large data treasures that have not yet been tapped.

1. Initial situation

So-called large language models (LLM) such as ChatGPT or Gemini, but also other models of generative artificial intelligence, use a machine learning process that utilizes information from the internet.

373 ***Does machine learning violate the GDPR when reading the internet?*** Söbbing/Schwarz ITRB 2024, 212–217.

It is possible that personal data within the meaning of Art. 4 No. 1 GDPR is also collected, as the scope of **processing** pursuant to Art. 4 No. 2 GDPR is very broad. Article 4(2) GDPR expressly covers the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, and comparison of personal data.

Machine learning requires very large amounts of authentic training data in order to continuously develop and improve its capabilities. [374] Machine learning in LLM works similarly to a huge, highly complex prediction system that is trained to generate text based on the input it receives. To understand the meaning of a word, LLMs first observe it in context, using huge training data sets, paying attention to nearby words. These data sets are based on compilations of texts published on the internet, with new LLMs being trained using billions of words. In response to a user's search query (prompt), the LLM divides the sentence into so-called tokens. [375] A token can consist of a word, an abbreviation, a syllable, or a punctuation mark. A token can be understood as a piece of a puzzle. The LLM analyzes the tokens in a sentence and their relationship to each other. Taking into account the probability with which individual tokens occur together with other tokens on the internet, a response to the prompt is generated. An LLM does not have any factual knowledge itself, but rather bases its responses on the **frequency of information** on the internet. This can lead to errors or so-called hallucinations.[376]

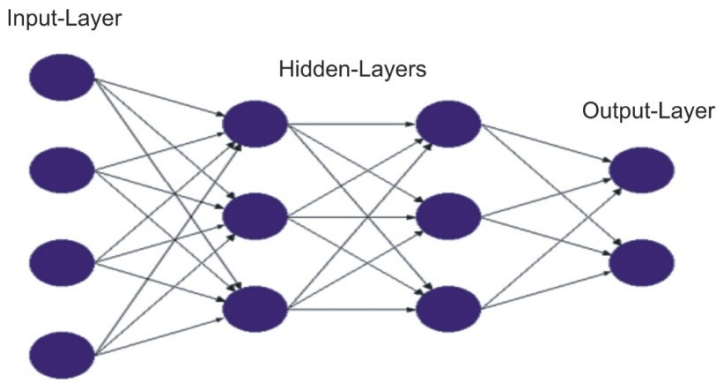
LLMs are only as good as their **training data** and training tools, because they are based on probabilities. The training data comes from various

374 *Söbbing*, ITRB 2024, 184.

375 A token is the basic unit of processing that the model uses to understand and generate text. See the basic GPT paper by *Radford* et al., Improving Language Understanding by Generative Pre-Training. This paper by OpenAI introduces the concept and implementation of the original GPT model, including a discussion of tokenization and how it affects the model's ability to understand and generate language.

376 Hallucinations in large language models such as GPT refer to cases where the model generates incorrect, distorted, or completely fabricated information. These phenomena can be caused by various factors. See *Goldberg*, Reducing Hallucination in Language Models, arXiv.org.

Sources such as books, articles, but above all websites. The data is then prepared, which means that it is cleaned, organized, and sometimes put into a formatted structure so that it is suitable for training the model. Neural networks are often used for LLM, especially those known as transformer models, or **artificial neural networks (**ANNs). These models are particularly good at recognizing patterns in sequences of data (such as text) and learning, which enables them to process language effectively. The basic element of a neural network for deep learning is the neuron, which represents a node in the neural network where one or more input signals (numerical data) converge and are further processed by the neuron's activation function.[377] Depending on where the neuron is located in the network, these can be signals from the input layer or signals from previous neurons. After the input signals have been processed, they are passed on as output to the following neurons. Formally speaking, the output of a neuron is a function of the inputs. [378]



During model training, the collected text data is used to teach the model how language works. This is done through a process

[377] *Kriesel*, A Brief Introduction to Neural Networks. http://www.dkriesel.com/en/science/neural_networks (July 1, 2024).

[378] *Heinz*, Deep Learning – Part 1: Introduction, footnote 11.

"supervised learning," in which the KNN receives input texts and the desired output texts. The goal is for the model to learn to translate the input into the desired output. For example, the model could see the beginning of a sentence and learn how to complete it. After initial training, the KNN can be further customized or fine-tuned to better handle specific types of tasks or language styles. This can be done by training with more specific datasets or by making adjustments to the way the model learns. Finally, the KNN is evaluated to see how well it performs. This can be done through testing with real user queries or through special evaluation tests. Based on these results, the model is further improved. Overall, machine learning in LLMs is based on analyzing and understanding language on a very large scale, which enables them to generate human-like responses in a variety of contexts. [379]

2. Processing within the meaning of Art. 4 (2) GDPR

While Section 44b UrhG and Section 60d UrhG contain special rules for the reading of websites by AI by means of machine learning, the GDPR does not provide for any special rules in this regard. Even if they are not the focus of the KNN's search, personal data is automatically collected when the KNN searches the internet. [380]

Processing within the meaning of Art. 4 No. 2 GDPR is defined as any operation or set of operations which is performed on personal data or on personal data which are being processed, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [381]

[379] Source: ChatGPT.

[380] *Herbst* in Kühling/Buchner, DS-GVO BDSG, 4th edition, 2024, on the individual processes.

[381] This corresponds to the definition in Art. 2 lit. b of the Data Protection Directive.

This list is not exhaustive; examples of processing include collection and recording. The working methods of LLM through KNN primarily involve the collection, recording, organization, structuring, storage, retrieval, use, and comparison of personal data within the meaning of Art. 4(2) GDPR. The GDPR [382] defines processing subject to its provisions as any operation **or set of operations** performed **on personal data,** whether or not by means of processing.

a) Collection

Collection within the meaning of Art. 4 (2) GDPR is the **obtaining** of personal data from the data subject himself. The active and subjective element required by the concept of collection is missing if the data is provided by the data subject themselves or by third parties without being requested, i.e., it "accrues" to the controller.[383] This is the case with Meta's originally planned and now withdrawn changes to its terms and conditions (reading of data "provided" by users) following complaints from noyb. This requires the collecting body to take **active action**. [384] A KNN that searches the internet for information as a web crawler/agent, as described by its developers, fulfills the requirement of active action. This requires an active action on the part of the collecting entity (the controller), which is attributable to it. [385] In this context, the collection is linked to an activity by the collecting entity, which wishes to obtain knowledge of the personal data.

[386] This can certainly be assumed of the developer and operator of the KNN. This is because, in the context of continuous monitoring, the developer has and must have an interest in ongoing review. Whether the collection is lawful is explained in section 3.

382 *Gola* in Gola/Heckmann, General Data Protection Regulation – Federal Data Protection Act, 3rd edition, 2022, Art. 4, margin number 35.

383 *Schild* in BeckOK Data Protection Law, 48th ed. May 1, 2024, Art. 4 GDPR margin no. 36.

384 *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Data Protection Law, 46th edition, November 1, 2023, Art. margin no. 35.

385 *Simitis* BDSG, 8th ed. 2014, § 3 margin no. 102.

386 *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46th ed. 1.11.2023, Art. 4 margin no. 35.

b) Recording

According to Section 3 (4) No. 1 BDSG (old version), the term "recording" was a subcategory of "storage," which is referred to separately here, although the distinction will ultimately be meaningless in practice. This refers to the **writing down or recording** of the data obtained. [387] Recording, like collection, is to be understood in a very broad sense. [388] This means that searching by a KNN is also recording within the meaning of Art. 4 No. 2 GDPR.

c) Organizing and arranging

The organization and arrangement of data overlap. This refers to the creation of **a structure** of any kind within the data, regardless of whether it is simple or complex. [389] Questions regarding the quality of the structuring process, such as whether it is meaningful and reasonable, are irrelevant.[390] The creation of the KNN and its complex form for analyzing the collected data establishes a structure for collecting the data. Thus, organization within the meaning of Art. 4 (2) GDPR can be assumed when using the KNN.

d) Reading and querying

Reading differs from querying in that reading involves consulting an existing data record, whereas querying involves using an external database. [391] In both cases, however, it is a subform of collection, as **data** is being viewed. [392] The reading and querying of data from the internet can be seen as the core task of the KNN of the LLM; it is the necessary task of the input layer for the subsequent organization and sorting of the data.

---

387 *Ernst* in Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 4 para. 26.

388 *Gola/Schomerus*, BDSG, 11th edition, 2012, Section 3, margin number 21, 26.

389 *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Data Protection Law, 46th ed. 1.11.2023, standard margin no. 43.

390 *Ernst* in Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Norm Rz. 24.

391 *Ernst* in Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Norm Rz. 28.

392 *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Data Protection Law, 46th edition, November 1, 2023, standard margin number 43.

e) Reconciliation and linking

Data reconciliation refers to **checking** whether data stored in multiple file systems about a trusted party is identical or whether certain data exists in two different files (e.g., to determine which persons are involved in multiple matters).[393] Whether this is the task of an LLM's KNN is debatable, but KNNs will often use multiple sources of information and compare them with each other to confirm accuracy (basic truth).

If data from one system is **linked** to or added to another to complete the other data set, this is called linking. [394] A KNN will also do this to improve the quality of its data.

3. Lawfulness of processing

Due to the broad interpretation of the term "processing" within the meaning of Art. 4 No. 2 GDPR, it is therefore very likely that the KNN of an LLM processes personal data. Effective consent cannot generally be assumed. This is because obtaining consent is effectively impossible due to the methodology of web crawlers.[395] When used by users themselves, chatbots do provide explicit information about their own further processing. Google's Gemini, for example, states: *"Your conversations are processed by reviewers to improve the technologies used in Gemini apps. So don't enter anything that you don't want reviewers to see or Google to use."*

should not be used."[396] However, this only applies to the data transmitted by the data subject. The data subject was certainly not able to agree to the underlying terms and conditions in the subsequent use. None of the known terms and conditions currently provide for a simple opt-out equivalent to unsubscribing from a

[393] *Ernst* in Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Norm Rz. 31.

[394] *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46th ed. 1.11.2023, Norm Rz. 52.

[395] Hessel/Dillschneider, RDI 2023, 458, 460.

[396] https://gemini.google.com/app

Newsletter. Instead, the Meta Group had initially planned an opt-out solution for the end of June 2024, which would require users to individually opt out [397]. The aim was to use the content shared by Facebook and Instagram users – certainly a huge and valuable treasure trove of data in terms of scope and content – as training data for its own AI. Consent was expressly not to be sought. The planned change was considered to be covered by Meta's legitimate interests. In the meantime, the company has (initially) distanced itself from this solution and stated, "We're disappointed by the request from the Irish Data Protection Commission (DPC), our lead regulator, on behalf of the European DPAs, to delay training our large language models (LLMs) using public content shared by adults on Facebook and Instagram — particularly since we incorporated regulatory feedback and the European DPAs have been informed since March." [398] It is therefore questionable whether Art. 6 (1) lit. f GDPR can be a legal basis for processing. According to Art. 6 (1) lit. f, the interests of the controller or of one or more third parties on whose behalf the data is processed or to whom the data is transferred may justify processing if it is necessary to safeguard those interests. Whether a legitimate interest exists is only a matter of assessment at first glance. The controller's interest must first be determined on the basis of the purpose of the processing. [399] Once the interest has been determined, it must then be determined normatively whether this interest conflicts with the legal order of the Union, the respective Member State, or with data protection principles (Article 5), including the principle of necessity.[400] The fact that a permanently functional AI system requires monitoring already speaks in favor of assuming a legitimate interest. The results produced by the respective chatbot—in particular multimodal chatbots, which not only use text but also spoken words, images, and videos—must correspond to reality and existing, constantly expanding.

[397] https://noyb.eu/de/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai

[398] https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/

[399] *Schulz* in Gola/Heckmann, General Data Protection Regulation – Federal Data Protection Act, 3rd edition, 2022, margin number 61

[400] Gola/Heckmann/Schulz, 3rd edition 2022, GDPR Art. 6 margin note 61.

On the other hand, the interests of users who have previously disclosed their (personal) data must be weighed up. If this has been done in a publicly accessible area, there is much to suggest that, at least in the case of anonymization, the interests of the processor prevail.[401] On the other hand, the ECJ sees considerable problems in the case of a user "whose online activities are recorded in large part, if not almost entirely, by Meta Platforms Ireland, which may give him the feeling that his private life is being continuously monitored." [402] It seems unclear whether the ECJ will also apply this reasoning to chatbots.

However, it becomes extremely problematic when particularly sensitive data within the meaning of Art. 9 GDPR is involved. The categories listed there are generally subject to a processing ban (Article 9(1)). Processing is only permitted under the conditions set out in paragraphs 2 and 3. If an AI system searches through images of users of a social media service, for example, sensitive data will almost inevitably be included. Irrespective of the fact that photographs depicting individuals or groups of individuals may regularly allow for ethnic classification, photographs are subject to "biometric data" "if they are processed using special technical means that enable the unique identification or authentication of a natural person" [403].This is now happening regularly as a result of advancing technology, both in mobile devices and on social media platforms, when people depicted in images are identified via facial recognition.[404] However, even one piece of sensitive data means that the conditions set out in Art. 9 (2) GDPR must be met for the processing to be lawful. [405] It does not help in this respect that, according to Art. 9 (2) (e), data that a user has made publicly available may be used by the service. This is because

[401] Hessel/Dillschneider, Data protection challenges in the use of AI, RDI 2023, 459, 461; Dallmann/Busse ZD 2019, 394 (395); Herfurth ZD 2018, 514 (517); Dieker, ZD 2024, 132, beck-online)

[402] ECJ GRUR 2023, 1131 para. 115 ff.; BeckOK DatenschutzR/Albers/Veit, 46th ed. 1.8.2023, GDPR Art. 6 para. 72

[403] Recital 51.

[404] See Spindler/Schuster/Spindler/Dalby, 4th ed. 2019, GDPR Art. 9 para. 5. Although the corresponding function is not available on Google's service in Europe, the block can be easily circumvented by using a VPN.

[405] ECJ GRUR 2023, 1131 para. 89; BeckOK Data Protection Law/Albers/Veit, 48th ed. 1.5.2024, GDPR Art. 9 para. 17a.

The data subject has not been hired. In individual cases, a data subject will also not have an account with the service on which the data scraping takes place. Just think of pictures of a family celebration with a large number of people. In this case, the platform in question may not have all the information necessary for identification. However, this does not exclude the possibility that the data in question can be classified as personal data. [406] It is also completely unclear how a company can technically distinguish sufficiently between sensitive and non-sensitive data. In addition, the exception is based on the idea that no protection of sensitive data is necessary where the data subject voluntarily waives protection. However, this is only the case if the data subject has published the data with full knowledge of all relevant circumstances (users must have "clearly expressed their decision that this data should be made available to an unlimited number of persons through individual settings made in full knowledge of the facts".[407] The wording of the ECJ already makes clear the need for a restrictive interpretation of the exception.

According to Recital 47 GDPR, the balancing of interests should take into account, among other things, the reasonable expectations of the data subject with regard to the specific processing [408]. If personal data is collected from publicly accessible (internet) sources for the purpose of AI training, the question arises as to whether the data subject could reasonably have expected their data to be reused for this purpose, for example through web scraping. A mixed subjective-objective standard is generally used to determine reasonable expectations. The decisive factor in this respect is whether the further processing in question is foreseeable for an objective third party, taking into account the "knowledge of the general public." It should be noted here that more and more companies—as illustrated above for the Meta Group—are using web scraping or web crawling.

406 ECJ judgment of March 7, 2024 – C-479/22 P, BeckRS 2024, 3655 para. 49, beck-online.

407 ECJ, EuZW 2023, 950 para. 82, beck-online.

408 Recital 47, OJ 2018 L 127, p. 2.

Methods for the purpose of AI training themselves in their privacy policies or guidelines. This allows these companies to influence user expectations to a certain extent, at least indirectly, in their own favor. Some authors argue that low-level knowledge about processing already exists.[409] In a next step, circumstances that may argue in favor of the interests of AI developers prevailing will be highlighted. The processing principles and the specific technical and organizational measures implemented to safeguard the rights of data subjects play a decisive role here. Based on the above, only comprehensive and effective anonymization or pseudonymization, high transparency standards, and privacy-by-design requirements can enable AI training to be designed in a manner that complies with data protection regulations. This is because, in the absence of a practical possibility for consent to data processing, the individual intensity of the intervention for the data subjects can be significantly reduced. The lower the intensity of the intervention resulting from the measures taken on the part of the data subjects, the more likely it is that the balance of interests will be in favor of the AI developers. Since 2015, the EU Commission has regarded anonymization, pseudonymization, and encryption as the central elements for data collection in compliance with data protection regulations.[410] While anonymization is considered to be compliant with data protection requirements according to all opinions [411] the problem becomes more difficult with other technical solutions: According to Recital 26, sentence 2, *"personal data that has been pseudonymized but could be linked to a natural person through the use of additional information shall be considered information about an identifiable natural person*." With advancing technological development, this leads to a dilemma: at what point is this guaranteed? Paal rightly points to the practical problem of technological progress, particularly through AI.[412] This is because the application of AI leads to

409 Dieker ZD 2024, 132, 135, beck-online

410 Gola/Heckmann/Schulz, 3rd edition 2022, GDPR Art. 6 para. 152 with reference to the statement by the EU Commission.

411 Paal, ZfDR 2024, 129, 136, beck-online.

412 Paal, ZfDR 2024, 129, 137, beck-online.

on pattern recognition, which in turn allows conclusions to be drawn that were not considered in anonymization and pseudonymization.

4. Responsible

Finally, the question should be raised (albeit not explored in depth here) as to who is responsible (cf. Art. 26 (1) sentence 1 GDPR). Given today's widespread division of labor, not every user of AI who has purchased the AI application from the manufacturer will have sufficient knowledge of how the algorithm provided to them by a manufacturer works.[413]

More and more often, a company will purchase an AI application tailored to its business model. However, the controller is characterized by the fact that he is able to explain the processing operation in terms of "why" and "how."

"How" to exert control. [414]As a company, one could be overly confident and assume that the above-mentioned data protection procedures are *legally unproblematic* for uninformed users due to their lack of knowledge about the *"how." Since the possibility of "joint responsibility" has existed for some time now recognizes*[415] *for more comprehensive protection of consumer rights, additional and unexpected problems may arise in individual cases for users of purchased AI applications. Since the purposes of the manufacturer of the AI and the user* may *also* be "*mutually* complementary" *in this case,* [416] *according* to the case law of the ECJ, both could be considered controllers within the meaning of Art. 26(1) sentence 1 GDPR. In accordance with Art. 4 No. 7 GDPR, the decisive factor is likely to be the user's decision-making power over the data processing (so-called "*decisive* influence").[417] Such influence must be affirmed for both the manufacturer and the user of the system. This is because

as a rule, the user will "in its own interest, decide on the

413 Hoeren/Sieber/Holznagel MMR-HdB, Part 29 Rn. 17, beck-online

414 Paal/Pauly/Martini, 3rd edition 2021, GDPR Art. 26 margin note 19

415 ECJ judgment of June 5, 2018 – C-210/16, EuZW 2018, 534 – Facebook fan page, beck-online; the ruling was issued on the basis of the repealed Data Protection Directive, but it should also be transferable to the GDPR; see also Gierschmann, ZD 2020, 69, beck-online

416 ECJ, ZD 2019, 455 – Fashion-ID; Gierschmann ZD 2020, 69, beck-online

417 BeckOK DatenschutzR/Spoerr, 46th ed. 1.5.2022, GDPR Art. 26 para. 17

purposes and means of processing "influence," which extends to the extent that [418] . If the company is then the controller, it also has the data security obligation under Art. 32 GDPR, for which the controller bears the burden of proof.[419]

5. Summary

The opportunities offered by machine learning – especially multimodal machine learning – for LLMs are fascinatingly vast. However, the high fines imposed by Article 83(5) GDPR alone mean that the existing provisions of the GDPR must not be disregarded. If the ECJ had ruled in favor of the GDPR in its so-called Schufa decision [420], it would be desirable for the legislator to establish a provision in the GDPR similar to that in Sections 44b / 60d UrhG, which would enable technology-friendly development in the EU. However, a balanced interpretation of "legitimate interest" is possible and, in our opinion, also necessary. It is particularly regrettable that the AI Act failed to include the option of establishing independent and robust rules for data collection in AI applications. The resulting legal uncertainty is unnecessarily detrimental to users.

The aspect of scientific research, as used, for example, in Section 60d UrhG, was not taken into account for the GDPR. This would clearly exceed the scope of this article, but would certainly open up exciting possibilities

Section 60d UrhG, was not taken into account for the GDPR. This would clearly exceed the scope of this article, but would certainly reveal exciting possibilities.

418 ECJ ECLI:EU:C:2023:949= BeckRS 2023, 34702 para. 31ff; Assion NJW 2024, 632 para. 3, beck-online.

419 ECJ ECLI:EU:C:2023:986= EuZW 2024, 236; ECJ E-CLI:EU:C:2024:72= BeckRS 2024, 530 marginal no. 42.

420 ECJ, judgments of December 7, 2023 – C-634/21 "SCHUFA Holding (Scoring)" and C-26/22 and C-64/22 "SCHUFA Holding (Residual Debt Discharge)") of December 7, 2023 = Söbbing/Schwarz ZD 2024, 160.

II. What data protection issues arise in automated (AI) decision-making?

According to Annex III of the AI Regulation, creditworthiness is determined using a score based on artificial intelligence and possibly on a high-risk system. The GDPR has created Article 22 GDPR for this purpose, on which the ECJ has now also ruled.[421]

1. Introduction

Article 22 of the GDPR regulates the specifics of profiling and automated decision-making. Article 22 GDPR establishes a general prohibition[422] on automated decisions that produce legal effects concerning data subjects or significantly affect them.[423] An automated individual decision within the meaning of the Regulation is made without any human intervention.[424] The data subject should have the right not to be subject to a decision – which may include a measure – based solely on automated processing that produces legal effects concerning him or her or similarly significantly affects him or her, such as theautomatic rejection of an online credit application or an online recruitment process without any human intervention. [425] Section 31 BDSG is intended to regulate the protection of business transactions in the context of scoring and credit reports. [426] For reasons of Union law, Section 31 BDSG can only refer to the processing of personal data.

---

[421] Does SCHUFA have to disclose how it calculates its score? Landmark ruling by the ECJ on Art. 22 GDPR and Section 31 BDSG expected; opinion of the Advocate General at the ECJ Specialist article, Söbbing/Schwarz, in Recht der Datenverarbeitung (Data Processing Law), Beck-Verlag, ZD 2023, 579.

[422] On the prohibitive nature of the provision: *Martini* in: Paal/Pauly, DS-GVO BDSG, Art. 22, para. 15; Spindler/Schuster/Spindler/Horváth, 4th ed. 2019, DS-GVO Art. 22 para. 5.

[423] See Recital 71 GDPR.

[424] *Wendehorst/Gritsch* in: Omlor/Link, Cryptocurrencies and Tokens, II. Data Protection Findings, 2nd updated and expanded edition 2023, para. 57.

[425] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev. 01, p. 20.

[426] *Kühling*, NJW 2017, p. 1985, 1988.

The subsequent use of scoring and creditworthiness information must be regulated, and only to the extent that this serves to protect commercial transactions. [427]Article 22 GDPR does not directly regulate scoring as understood in Section 31 BDSG. This is because Article 22(1) GDPR specifies when a data subject may be the subject of a decision based on automated processing. The subject matter of Art. 22(1) GDPR is the "decision" (and its effects) and not requirements for determining a score. Section 31(1) BDSG, on the other hand, concerns the preparation of a decision ("for the purpose of the decision").[428]

The Federal Court of Justice (BGH)[429] had already ruled in 2014 that a data subject has the right to information about which personal data, in particular credit-related data, is stored by SCHUFA and is used to calculate their probability scores. To calculate the score, SCHUFA performs a credit assessment, for which the probability of future behavior, e.g., repayment of a loan, is predicted for a person based on certain characteristics using mathematical and statistical methods. However, the weighting of individual data in determining the probability value and the formation of any comparison groups are, in SCHUFA's view in the BGH proceedings, an essential component of the so-called score formula and therefore a trade secret of SCHUFA and cannot be disclosed. [430]

After the Administrative Court of Wiesbaden referred two questions for a preliminary ruling on the GDPR (cases C-26/22 and C-64/22) to the ECJ, the opinion of the Federal Court of Justice is now being questioned by the Advocate General at the ECJ. In his Opinion of March 16, 2023, the Advocate General dealt with the working methods of SCHUFA and its classification of probability values

427 BT-Drs. 18/11655, p. 31.

428 *Kühling/Martini* et al., The GDPR and national law, 2016, p. 441.

429 Federal Court of Justice, judgment of January 28, 2014 – VI ZR 156/13 = NJW 2014, p. 1235.

430 *Schade*, ZD 2014, p. 306, 309, note on BGH, judgment of January 28, 2014 – VI ZR 156/13

(Scoring), see Case C-634/21. The cases C-26/22 and C-64/22, which are not discussed here but are related, concern the judicial review of legally binding decisions by (data protection) supervisory authorities and the storage of data in private credit agencies if this data has already been deleted from public registers.[431] The Federal Court of Justice has decided to stay the proceedings before the Administrative Court of Wiesbaden ( ) until the ECJ has ruled in the (related) cases C-26/22 and C-64/22 pending before it. [432]

2. Proceedings before the Administrative Court of Wiesbaden (Case C-634/21)

In the original case before the Administrative Court of Wiesbaden [433] in case no. C-634/21, the person concerned requested SCHUFA to delete the incorrect entries concerning him and to provide information about the stored data on which the entries were based. The proceedings concern a legal dispute between a citizen and the State of Hesse, represented by the Hessian Commissioner for Data Protection and Freedom of Information (hereinafter: HBDI), regarding the protection of personal data. As part of its economic activity, which consists of providing its customers with information about the creditworthiness of third parties, SCHUFA Holding AG provided a credit institution with a score relating to this citizen. This score served as the basis for refusing the loan applied for by this citizen. [434] At the request of the citizen concerned, SCHUFA (as usual) disclosed the calculated score and the basic functioning of the score calculation. However, SCHUFA did not disclose the calculation method or the functioning of its algorithm. Based on the above view of the Federal Court of Justice (BGH) [435] SCHUFA took the legal position that the calculation method was a trade and business secret.

[431] SCHUFA has already responded to this and reduced the period for deleting the legal debt discharge to six months. https://www.schufa.de/ueber-uns/presse/presse-mitteilungen/schufa-loescht-restschuldbefreiung-sechs-monaten/ (accessed on July 7, 2023).

[432] Decision of March 27, 2023 – VI ZR 225/21= ZIP 2023, p. 868.

[433] NZI 2023, p. 399.

[434] Press release No. 49/23 of the ECJ dated March 16, 2023.

[435] Federal Court of Justice, judgment of January 28, 2014 – VI ZR 156/13= NJW 2014, p. 1235.

The plaintiff then contacted the HBDI, which argued that SCHUFA "generally (within the meaning of Section 31 BDSG) complies" with the requirements set out in the Federal Data Protection Act when calculating credit ratings and that there were no indications in the present case that this was not the case. The data subject brought an action against this decision before the Administrative Court of Wiesbaden. The Administrative Court suspended the proceedings and referred questions of interpretation of Article 22 GDPR to the ECJ.[436] According to Art. 22(1) GDPR, a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. In substantive law, the preliminary ruling procedure before the ECJ centrally concerns the question of whether the determination of scores by credit agencies by means of automated processing of personal data is permissible under data protection law or not. [437] Specifically, the following questions were referred:

1. Does the calculation of a credit score by a credit agency fall under Article 22(1) of the GDPR?
2. To what extent do national provisions on profiling (in this case Section 31 of the German Federal Data Protection Act (BDSG)) conflict with Articles 6(1) and 22 of the GDPR?

3. Opinion of the Advocate General

The Advocate General's answers to the above questions were as follows:

Re 1. The score calculated by SCHUFA constitutes an automated decision within the meaning of Art. 22(1) GDPR.

[436] VG Wiesbaden ZD 2022, p. 121 with note by Qasim.

[437] MMR-Aktuell 2023, 456626.

Re 2. Due to the primacy of Union law, "such a national provision is not compatible with the GDPR" and can only be applied if the profiling is different from that provided for in Art. 22(1) GDPR.

The automated generation of a probability value regarding the ability of a data subject to service a loan in the future constitutes automated decision-making within the meaning of Article 22(1) GDPR. If this value, determined on the basis of personal data, is transferred by the controller to a third-party controller and that third party, in accordance with its established practice, uses this value as a significant factor in its decision to establish, execute, or terminate a contractual relationship with the data subject, this constitutes a violation of Art. 22(1) GDPR.[438]

In detail, the Advocate General (AG) states[439] that the determination of the score by SCHUFA constitutes profiling within the legal definition in Article 4(4) GDPR, as the score is determined automatically and allows conclusions to be drawn about a person's creditworthiness through the use of personal data. The questions of interpretation revolve around the further requirements of Art. 22(1) GDPR. This requires that the automated decision has legal effects on the data subjects or similarly significantly affects them.

The basis for the Advocate General's opinion lies in recital 71, which expressly cites the "automatic rejection of an online credit application" as a typical example of a decision that "significantly" affects the data subject. However, according to Article 22(1) GDPR, the decision that produces legal effects must also be based "solely" on automated processing.

438 *Etteldorf*, MMR-Aktuell 2023, 456626.

439 *Etteldorf*, MMR-Aktuell 2023, 456626.

In addition, the Advocate General also comments on the scope of the right to information in such cases under Article 15(1)(h) GDPR. According to this, the data subject has the right to request from the controller not only confirmation as to whether or not personal data concerning him or her are being processed, but also other information, such as the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the intended effects of such processing for the data subject.[440] This includes, in particular, the factors taken into account in the decision-making process and their weighting at an aggregated level, which must also be provided to the data subject for the purpose of challenging automated decisions. This includes, in particular, the factors taken into account in the decision-making process and their weighting at an aggregated level, which are also useful to the data subject for challenging automated "decisions" within the meaning of Article 22(1) GDPR. [441]

In connection with the initial question, it is very interesting to note the GA's view on the compatibility of Article 22 GDPR and Section 31 BDSG. The GA does not see Section 31 BDSG as a legal basis for exceptions to Article 22(1) GDPR. In the "absence of opening clauses or exceptions that empower Member States to adopt more detailed rules or to derogate from the provisions of the GDPR in order to regulate this activity" and "taking into account the degree of harmonization" of the GDPR, the GA considers Section 31 BDSG to be contrary to EU law.

As is well known, scoring algorithms cannot be patented or protected by copyright; due to Section 2 (1) (a) GeschGehG, the score would no longer be a trade secret after disclosure, meaning that anyone could adopt SCHUFA's algorithms without fear of legal sanctions. This is because it has not yet been legally clarified how an algorithm can be protected. [442] In addition, the business model of

[440] Editorial team of beck-aktuell, becklink 2026476.

[441] Editorial team beck-aktuell, becklink 2026476.

[442] See *Söbbing*, CR 2020, pp. 223–228.

credit agencies are not only a business model approved by the legal system and thus a legitimate processing purpose. [443] They are a central element of economic life. From a constitutional point of view, the functioning of competition requires that market participants have as much information as possible about market-relevant factors. [444] This certainly includes the provision of accurate credit information. [445] The GA should take these correct considerations into account and not base its view solely on data protection law.

4. Decision of the ECJ

The ECJ therefore had two questions to answer. [446]

a) First question

With its first question, the VG Wiesbaden wanted to know whether Article 22(1) GDPR is to be interpreted as meaning that an "automated decision in individual cases" within the meaning of that provision exists if a probability value based on personal data relating to a person is assigned to that person in relation to their ability to fulfill future payment obligations by a credit agency, provided that this probability value is decisive for whether a third party to whom this probability value is transmitted enters into a contractual relationship with that person.by a credit agency, provided that this probability value is decisive for whether a third party to whom this probability value is transmitted establishes, performs, or terminates a contractual relationship with that person.[447] In answering this question, the ECJ pointed out that when interpreting a provision of EU law, not only its wording but also the context in which it appears and the objectives pursued by the legal act of which it forms part must be taken into account. [448] As regards the wording of Article 22(1) GDPR,

---

443 Federal Court of Justice (BGH) NJW 2020, 1587 marginal no. 46; BeckOK Data Protection Law/Krämer, 44th ed. 01.05.2023, BDSG § 31 marginal no. 1c with further references.

444 BVerfGE 105, 252, 265 f. – Glykol; BGH NJW 2011, 2204 marginal no. 20.

445 BGH NJW 2011, 2204 marginal no. 21.

446 Must SCHUFA disclose how it calculates its score? Landmark decision of the ECJ on Art. 22 GDPR and § 31 BDSG expected; opinion of the Advocate General at the ECJ, expert article, Söbbing/Schwarz, in Recht der Datenverarbeitung (Data Processing Law), Beck-Verlag, ZD 2023, 579.

447 ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 40

448 Judgment of June 22, 2023, Pankki S, C-579/21, EU:C:2023:501, para. 38 and the case law cited therein

this provision stipulates that a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

According to the ECJ ruling [449], the application of Article 22 GDPR depends on three cumulative conditions, namely that, first, a "decision" must exist, second, this decision must be "based solely on automated processing, including profiling," and third, it must
"produces legal effects concerning [the data subject] or affects him or her in a similar way." [450]

With regard to the requirement that a decision must exist, the ECJ has ruled that the term "decision" within the meaning of Article 22(1) GDPR is not defined in this Regulation. However, it is clear from the wording of this provision that this term refers not only to acts that have legal effects on the data subject, but also to acts that significantly affect that person in a similar way.
[451]

According to the ECJ, the broad meaning of the term "decision" is confirmed by recital 71 of the GDPR, according to which a decision on the evaluation of personal aspects relating to a person "may include a measure" that either "produces legal effects concerning the data subject" or
"significantly affects them in a similar way," whereby the person concerned should have the right not to be subject to such a decision. According to this recital, of, the term "decision" as defined in ECJ.

[449] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 43.
[450] ECJ, 07.12.2023 - C-634/21 of 7.12.2023 para. 43
[451] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 44

For example, the automatic rejection of an online loan application or online recruitment procedures without any human intervention. [452]

The ECJ further states that the term "decision" within the meaning of Article 22(1) GDPR, as explained by the Advocate General in point 38 of his Opinion, this term is broad enough to include the result of the calculation of a person's ability to fulfill future payment obligations in the form of a probability value. [453]

The second condition, that the decision must be "based solely on automated processing, including profiling," must be met within the meaning of Article 22(1) GDPR. According to the ECJ and as stated by the Advocate General in point 33 of his Opinion, it is clear that an activity such as that carried out by SCHUFA must be based on the definition of "profiling." – [based]," is that an activity such as that carried out by SCHUFA corresponds to the definition of "profiling" in Art. 4 No. 4 GDPR and that this requirement is therefore fulfilled in the present case. According to the ECJ the wording of the first question referred for a preliminary ruling expressly refers to the automated generation of a probability value based on personal data relating to a person with regard to their ability to service a loan in the future. [454]

The third condition, that the decision is taken with regard to the data subject

According to the ECJ, the fact that the action of the third party to whom the probability value is communicated is "significantly influenced" by that value is already apparent from the content of the first question referred for a preliminary ruling. According to the findings of the VG Wiesbaden, in the case of a loan application submitted by a consumer to a bank, an insufficient probability value will in almost all cases lead to the bank refusing to grant the loan applied for. [455]

[452] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 45

[453] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 46

[454] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 47.

[455] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 48.

Consequently, according to the ECJ, it must be assumed that the third condition for the application of Article 22(1) GDPR is also fulfilled, since a probability value such as that at issue in the main proceedings affects the data subject at least significantly.[456] Therefore, in circumstances such as those in the main proceedings, where the probability value determined by a credit agency and communicated to a bank plays a decisive role in the granting of a loan, the determination of that value as such must be classified as a decision which, within the meaning of Article 22(1) of the GDPR, has legal effects on a data subject or significantly affects them in a similar manner. [457] In its decision, the ECJ states that this interpretation is supported by the context in which Article 22(1) GDPR is found and by the purposes and objectives pursued by that regulation.[458] In this regard, the ECJ further points out that, as the Advocate General stated in point 31 of his Opinion, Article 22(1) GDPR grants the data subject the "right" not to be subject to a decision based solely on automated processing, including profiling. According to the ECJ, this provision constitutes a fundamental prohibition, the violation of which does not need to be individually asserted by such a person. [459]

According to the ECJ, Article 22(2) GDPR in conjunction with recital 71 of this Regulation indicates that a decision based solely on automated processing is only permissible in the cases specified in Article 22(2), i.e., where the decision is necessary for the performance of this Regulation, the adoption of a decision based solely on automated processing is only permissible in the cases referred to in Article 22(2), i.e. if it is necessary for the conclusion or performance of a contract between the data subject and the controller (point (a)), if it is based on Union law or the law of the Member State to which the controller is subject (point (b)), or if it is necessary for the protection of the vital interests of the data subject or of another natural person whose life is at risk (point (c)).

456 ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 49.
457 ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 50.
458 ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 51.
459 ECJ, 07.12.2023 - C-634/21 of 7.12.2023 para. 52.

Member States to which the controller is subject (point (b)) or if it is carried out with the explicit consent of the data subject (point (c)).[460]

Furthermore, according to the ECJ, Article 22(2)(b) and (3) GDPR stipulate that appropriate measures must be taken to safeguard the rights and freedoms and legitimate interests of the data subject. In the cases referred to in Article 22(2)(a) and (c) of this Regulation, the controller shall, according to the ECJ, grant the data subject at least the right to obtain the intervention of a person, to express his or her point of view, and to contest the decision.[461] Furthermore, according to Article 22(4) GDPR, automated decisions in individual cases within the meaning of this Article 22 may only be based on specific categories of personal data referred to in Article 9(1) GDPR in certain special cases. [462]

Furthermore, according to the ECJ, in the case of automated decision-making as defined in Art. 22(1) GDPR, the controller is subject to additional information obligations under Art. 13(2)(f) and Art. 14(2)(g) of this Regulation. On the other hand, pursuant to Art. 15(1)(h) GDPR, the data subject has a right to obtain from the controller information which, among other things, includes "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[463] These higher requirements for the lawfulness of automated decision-making, as well as the additional information obligations of the controller and the associated additional rights of access of the data subject, are explained by the purpose pursued by Art. 22 GDPR, which is to protect individuals from the specific risks to their rights and freedoms arising from automated processing

[460] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 53.
[461] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 54.
[462] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 55.
[463] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 56.

personal data – including profiling. [464] This processing requires, as is clear from recital 71 of the GDPR, the evaluation of personal aspects relating to the natural person to whom the processing relates, in particular to analyze or predict aspects concerning their performance at work, economic situation, health, preferences, interests, reliability, or behavior, location, or movements. [465]

According to this recital, these particular risks are, in the view of the ECJ, likely to adversely affect the interests and rights of the data subject, in particular with regard to possible discriminatory effects against natural persons on grounds of race, ethnic origin, political opinion, religion or belief, trade union membership, genetic characteristics or health status, and sexual orientation. Therefore, in the view of the ECJ, this recital should ensure fair and transparent processing with regard to the data subject, in particular through the use of appropriate mathematical or statistical methods for profiling and through technical and organizational measures that adequately ensure that the risk of error is minimized. [466]

The interpretation set out in paragraphs 42 to 50 of this judgment, and in particular the broad meaning of the term "decision" within the meaning of Article 22(1) GDPR, reinforces the effective protection that this provision aims to achieve. [467] On the other hand, in circumstances such as those in the main proceedings, where three actors are involved, there would be a risk of circumvention of Article 22 GDPR and, consequently, a gap in legal protection if preference were given to a narrow interpretation of that provision, according to which the determination of the probability value is to be regarded only as a preparatory act and only the processing carried out by the third party

[464] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 57.
[465] ECJ, 07.12.2023 - C-634/21 of 7.12.2023, para. 58.
[466] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 59.
[467] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 60.

action may be classified as a "decision" within the meaning of Article 22(1) of this Regulation. [468] In this case, the determination of a probability value such as that at issue in the main proceedings would not be subject to the specific requirements of Article 22(2) to (4) GDPR, even though this procedure is based on automated processing and has effects that significantly affect the data subject, since the actions of the third party to whom this probability value is transmitted are significantly guided by it. [469]

Furthermore, according to the ECJ and as stated by the Advocate General in point 48 of his Opinion, the data subject could, on the one hand, object to the credit agency that determines the probability rating concerning them if no automated decision-making is carried out by that company. On the other hand, the third party – assuming that the action it took would fall under Article 22(1) GDPR because it fulfilled the conditions for the application of that provision – would not be in a position to provide this specific information because it does not generally have it at its disposal. [470]

As explained in paragraphs 53 to 55 of this judgment, the fact that the determination of a probability value such as that at issue in the main proceedings is covered by Article 22(1) of the GDPR means that it is prohibited unless one of the exceptions set out in Article 22(2) of the GDPR applies and the specific requirements of Article 22(3) and (4) of the GDPR are met. [471] With regard to Article 22(2)(b) of the GDPR, to which the ECJ refers, it is already clear from the wording of that provision that national legislation which prohibits the adoption of an automated decision in individual cases

[468] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 61.
[469] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 62.
[470] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 63.
[471] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 64.

must contain appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject. [472]

In light of Recital 71 of the GDPR, according to the ECJ, such measures must include, in particular, the obligation of the controller to use appropriate mathematical or statistical procedures, to implement technical and organizational measures to ensure that the risk of errors is minimized and that errors are corrected, and to secure personal data in a manner that takes into account the potential risks to the interests and rights of the data subject, and in particular to prevent discriminatory effects on the data subject. These measures shall also include at least the right of the data subject to obtain the intervention of the controller, to express his or her point of view, and to contest the decision taken concerning him or her. [473]

Furthermore, the ECJ points out in its decision that, according to the ECJ's established case law, any processing of personal data must comply with the principles for the processing of personal data laid down in Article 5 of the GDPR and, in view of the principle of lawfulness of processing laid down in Article 5(1)(a), must meet one of the conditions for lawfulness of processing set out in Article 6 of that regulation[*judgment of October 20, 2022, Digi, C-77/21, EU:C:2022:805, para. 49 and the case law cited therein*]. The controller must be able to demonstrate compliance with these principles in accordance with the principle of accountability laid down in Article 5(2) of the GDPR. [474]

[472] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 65.

[473] ECJ, 07.12.2023 - C-634/21 of 7.12.2023 para. 66.

[474] See, to that effect, judgment of October 20, 2022, Digi, C-77/21, EU:C:2022:805, para. 24.

According to the ECJ, if, under the legislation of a Member State pursuant to Article 22(2)(b) of the GDPR, the adoption of a decision based solely on automated processing is permissible, such processing must therefore not only satisfy the conditions laid down in the latter provision and in Article 22(4) of the GDPR, but also the requirements of Articles 5 and 6 of that regulation. Consequently, Member States may not adopt legislation pursuant to Article 22(2)(b) of the GDPR which permits profiling in breach of the requirements of Articles 5 and 6 as interpreted by the ECJ. [475] With regard, in particular, to the conditions for lawfulness laid down in Article 6(1)(a), (b) and (f) of the GDPR, which may apply in a case such as that in the main proceedings, the Member States are not authorized to lay down supplementary provisions for the application of those conditions, since such a power is not conferred on them by Article 6(3) of the GDPR.are not competent to lay down supplementary rules for the application of those conditions, since such competence is limited, under Article 6(3) of the GDPR, to the grounds referred to in Article 6(1)(c) and (e) of that regulation.[476] Furthermore, as regards the specific content of Article 6(1)(f) of the GDPR, the Member States may not, pursuant to Article 22(2)(b) of the GDPR, derogate from the requirements arising from the case-law of the Court of Justice following the judgment of 7 December 2023, SCHUFA Holding,[477] in particular by making the outcome of the balancing of the conflicting rights and interests final. [478]

In the present case, the VG Wiesbaden points out that only Section 31 BDSG could constitute a national legal basis within the meaning of Article 22(2)(b) GDPR. However, this court has serious doubts as to the compatibility of Section 31 BDSG with EU law. If this provision were to be deemed incompatible with EU law, SCHUFA would not only

[475] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 68.

[476] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 69.

[477] *C-26/22 and C-64/22, EU:C:2023:XXX "Residual debt discharge"*

[478] See, to that effect, judgment of October 19, 2016, Breyer, C-582/14, EU:C:2016:779, para. 62, ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 70.

act without a legal basis, but would also violate ipso iure the prohibition laid down in Art. 22(1) GDPR. [479]

In this respect, according to the ECJ, it is for the VG Wiesbaden to examine whether Section 31 BDSG can qualify as a legal basis within the meaning of Article 22(2)(b) GDPR, according to which it would be permissible to adopt a decision based exclusively on automated processing. If the VG Wiesbaden concludes that Section 31 constitutes such a legal basis, it would still have to examine whether the requirements laid down in Article 22(2)(b) and (4) GDPR and in Articles 5 and 6 GDPR are met in the present case. [480]

In summary, the ECJ answers the first question by stating that Article 22(1) GDPR must be interpreted as meaning that an "automated individual decision" within the meaning of that provision if a probability value based on personal data relating to a person is generated automatically by a credit reference agency in relation to that person's ability to fulfill future payment obligations, provided that this probability value is decisive for whether a third party to whom this probability value is transmitted establishes, performs, or terminates a contractual relationship with that person. [481]

b) Second question

The second question was to what extent national legislation on profiling (in this case Section 31 BDSG) conflicts with Articles 6(1) and 22 GDPR. In the opinion of the ECJ, in view of the answer to the first question, there was no need to answer the second question. [482] This is because there are considerable doubts as to the compatibility of this provision with Article 22 GDPR, since the German legislature only

[479] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 71.
[480] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 72.
[481] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 25.
[482] ECJ, December 7, 2023 - C-634/21 of December 7, 2023, para. 48.

the "use" of a probability value such as that at issue in the main proceedings, but not the determination of that value as such. [483]

c) Assessment

The ECJ's view that the credit decision is significantly influenced by the Schufa credit score must be considered critical [*para. 48*]. [484] If this were really the case, the bank would outsource its risk management to Schufa, which would not be possible in this form under Section 25b (2) KWG.[485] Schufa only generates a credit score, which each bank can and will evaluate differently as part of its risk management. A risk-taking bank might approve a loan, while a more conservative bank would refuse the customer the loan. The fact that the plaintiff in the underlying case would not have obtained a loan from any bank is not (solely) due to his (poor) credit score. Rather, it is to be expected that he would not have obtained a loan from a bank even without the Schufa credit score. In this respect, the ECJ's view is too simplistic and too brief, as the decision on whether to grant a loan lies solely with the bank and the Schufa credit score is merely an aid. Contrary to its intention, the ECJ's decision will tend to make lending less consumer-friendly. A fundamental problem that runs through the decision is, on the one hand, the fundamental misunderstanding that the verifiability of a computer result is not a binary property (i.e., a clear "yes" or "no").[486] Thus, replacing or removing a (credit) criterion does not necessarily lead to a better or even different result. Machine learning makes sense especially for large sets of rules. In such cases, machine learning can establish correlations (not necessarily causalities). In other words, AI should use machine learning to find relationships that the user alone would not be able to find. The selection and quality of the

[483] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 25.

[484] ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 48.

[485] *Volhard/Jang in W/B/A| KAGB § 36 para. 20-24| , 3rd edition, 2021*

[486] *Well suited as a generally understandable introduction: see the presentation by Katharina Zweig, Die KI war's, p. 149*]

Input data. A credit score is calculated using an algorithm—a sequence of calculations. Its complexity depends on the assumptions made beforehand (known as heuristics). The latter, via the selection of input data, represents the actual source of risk for an incorrect assessment in the result. The EJC's [487] criticism of Section 31 BDSG is therefore not entirely understandable, as Section 31 BDSG is based on Recital 71 of the GDPR and, for the calculation of the probability value, refers to Section 31(1)(2) BDSG to a scientifically recognized mathematical-statistical method and, of course, if the score produces incorrect calculations, these must be corrected manually for economic reasons alone. BDSG, and, of course, if the score produces incorrect calculations, these are corrected manually for economic reasons alone. Seeing the lack of agreement on error correction as a possibility for discrimination requires a very long chain of objective attribution. Unlike US law, European law does not provide for the possibility of a purely statistical response to unequal treatment. The possibility of a sanction solely on the basis of a "Disparate impacts" [488] Unlike "disparate treatment," this concept is not recognized in European law.

The present decision of the ECJ,[489] like the opinion already published by the Advocate General, has clearly been made too much in favor of data protection and to the detriment of trade secrets. Focusing solely on the interests of customers and not taking into account the economic interests of companies is a one-sided and short-sighted view. After all, what company will still invest in the development of AI if it has to disclose the functioning of its algorithms in the form required by Article 15(1)(h) and there is a risk that the functioning of algorithms will no longer be trade secrets within the meaning of Section 2(1)(a) of the German Trade Secrets Act (GeschGehG)? To quote the late Wolfgang Schäuble: "We

487 ECJ, December 7, 2023 – C-634/21 of December 7, 2023, para. 66.

488 *Derived from the 14th Amendment to the United States Constitution, https://www.archives.gov/milestone-documents/14th-amendment*]

489 *ECJ, December 7, 2023 – C-634/21 of December 7, 2023*

are exaggerating with data protection, and it is already written in the inscription above the Temple of Apollo at Delphi: "Nothing in excess!"[490]

5. Outlook

At first glance, one might think that explicit consent pursuant to Art. 22 (3) lit. d) in conjunction with Art. 6 (1) lit. a) GDPR could be used in future. However, consent is a very cumbersome vehicle in practice. This is because consent must relate to all processing operations carried out for the same purpose or purposes [*Recital 32, para. 4 of* the General Data Protection Regulation]. It is therefore necessary that the declaration of consent covers all processing operations within the meaning of Art. 4 No. 2 in relation to the respective purpose. If there are several purposes, the consent must unambiguously refer to all purposes. Against this background, there are narrow limits to the interpretation of the declaration of consent. [491] In addition, consent can be revoked at any time, cf. Art. 7(3) sentence 1 GDPR.

A basis for authorization could also be found in Art. 6 (1) (c) GDPR
in conjunction with Section 505a BGB. According to Art. 6 (1) (c) GDPR, processing is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. Such a legal obligation could be found in Section 505a (1) BGB.
See Section 1 BGB, according to which, in the case of consumer loans, the lender must check the creditworthiness of the borrower before concluding a consumer loan agreement. This raises two issues. Firstly, the enabling provision only applies to consumer credit, and secondly, according to the wording of Art. 6(1)(c) GDPR, only lenders are required to carry out such a check, as only they are subject to a creditworthiness check obligation and not the credit agency. It is questionable whether the ECJ's view [*para. 48]* that the credit decision depends significantly on the credit agency's score and that the credit agency must therefore be included in the bank's legal sphere applies in the

490 *In memoriam Gregor Gysi & Wolfgang Schäuble PART 1 Minute 53:01 https://www.youtube.com/watch?v=Hqb18EkLWSg*].

491 *Schulz in Gola/Heckmann, General Data Protection Regulation – Federal Data Protection Act, 3rd edition, 2022, Art. 6, margin note 23.*

reverse would apply. In that case, the credit agency would also have to be included in the legal scope of Section 505a (1) sentence 1 BGB, and thus the basis for authorization would also apply to the credit agency under Art. 6 (1) lit. c GDPR, which is not to be expected in view of the narrow application of Art. 6 (1) lit. c GDPR. [492]

In principle, the provision in Section 31 BDSG could have been regarded as a successful balance between the interests of data subjects (Art. 22 GDPR) and SCHUFA's interest in protecting trade secrets (now Section 2 GeschGehG). Particularly with regard to the security of investments in the development of algorithms, Section 31 BDSG also served as a model for other areas. Unfortunately, however, the ECJ has now raised considerable doubts as to its compatibility with Art. 22 GDPR [*para. 25]* [493], and it can be assumed that the Wiesbaden Administrative Court will take the same view. The German legislature is therefore urgently called upon to amend Section 31 BDSG as quickly as possible and to establish clear and unambiguous regulations. This would also preserve the protective character of the provision both for the use of scoring and credit reports and for their creation by credit agencies. The German legislature also has an obligation to amend the law in this respect, as Article 22(2)(b) GDPR requires the legislature to take appropriate measures to safeguard the rights and freedoms of the data subjects. These were already essentially contained in Section 31 BDSG and should also be retained in order to continue to guarantee investment in AI while taking into account the rights of data subjects (including those under Article 15 GDPR). This is because Article 22 GDPR grants the necessary leeway to take both interests sufficiently into account. In order to preserve the regulatory character of Section 31 BDSG, the scope of application of the provision would have to refer to Article 22(1) GDPR. In his Opinion, the Advocate General makes it clear that Section 31 BDSG may not go beyond this. Thus, Section 31 BDSG may only apply to automated decisions within the meaning of Article 22(1) GDPR.

---

[492] *Schulz in Gola/Heckmann, General Data Protection Regulation – Federal Data Protection Act, 3rd edition, 2022, Art. 6, margin note 23*

[493] *ECJ, December 7, 2023 – C-634/21 of December 7, 2023*

The explanatory memorandum to the law would also have to explain that this is intended to constitute an exception within the meaning of Art. 22 (2) (b) GDPR. In this context, the function of Section 31 BDSG as a reference for the balancing of interests pursuant to Art. 6 (1) (f) GDPR should be clarified in the explanatory memorandum to the law. This would ensure that Section 31 BDSG is compatible with the GDPR and that the provision relating to protection functions for scoring by credit agencies is a secure and reliable working basis that no one questions.

F. AI- e Regulation

On March 13, 2024, members of the European Parliament voted 523 to 46, with 49 abstentions, to adopt the AI Regulation. This sets the framework for the use of artificial intelligence (AI) in Europe.

I. Overview of the AI Act [494]

The AI Regulation[495] is the world's first comprehensive set of rules for AI. It aims to promote innovation while strengthening trust in AI and ensuring that this technology is used in a way that respects the fundamental rights and security of EU citizens.

The regulation will subsequently be reviewed by legal and linguistic experts and is likely to be adopted before the end of the legislative period as part of the so-called correction procedure. The Council must also formally adopt the new provisions. The regulation will enter into force on the 20th day after its publication in the EU Official Journal and will generally apply 24 months later. However, some provisions will apply earlier: for example, the prohibitions will take effect after six months, and the provisions on AI models for general use will apply after 12 months.

1. Scope and definition of terms

Chapter I, Articles 1-4 of the AI Regulation specify the subject matter of the Regulation and the scope of application of the new rules for the placing on the market, putting into service, and use of AI systems. It also defines the terms used throughout this legal instrument. The aim of defining terms for AI systems is to be as technology-neutral and future-proof as possible

494 *Adoption of the European AI Regulation – Presentation of key points of the AI Regulation and criticism* Söbbing, ITRB 2024, 108–111.

495 Law on Artificial Intelligence, adopted text: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_DE.pdf.

and to take account of the rapid developments in AI technology and on the AI market. [496]

2. Prohibited practices in the field of AI

Chapter II, Article 5 of the AI Act contains a list of prohibited AI practices. The regulation takes a risk-based approach, distinguishing between AI applications that pose (i) an unacceptable risk, (ii) a high risk, and (iii) a low or minimal risk. The list of prohibited practices covers all AI systems that are considered unacceptable because they violate Union values, such as fundamental rights. The prohibitions apply to practices that have a significant potential to manipulate individuals by using techniques of subliminal influence that are not consciously perceived by those individuals, or that exploit the vulnerabilities of certain vulnerable groups, such as children or persons with disabilities, in order to significantly influence their behavior in such a way that they could cause psychological or physical harm to themselves or another person. Other manipulative or exploitative practices affecting adults and potentially facilitated by AI systems could fall under existing legislation on data protection, consumer protection, and digital services, which gives natural persons the right to adequate information and the freedom to refuse profiling or other practices that could influence their behavior. [497]

3. High-risk AI systems

Chapter III contains specific provisions for AI systems that pose a high risk to health and safety or to the fundamental rights of natural persons. In line with the risk-based approach, such high-risk AI systems are authorized on the European market, provided that they comply with certain mandatory

[496] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Law on Artificial Intelligence) and amending certain Union acts of 21 April 2021. See page 14 of the AI Regulation.

[497] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Act on Artificial Intelligence) and amending certain Union acts of 21 April 2021. See page 15 of the AI Regulation.

requirements and undergo a conformity assessment in advance. The classification as a high-risk AI system is based on the intended purpose of the AI system in accordance with existing EU product safety regulations. Thus, the classification as a high-risk AI system depends not only on the nature of the function of this system, but also on its specific purpose and its application modalities. [498]

a) Classification as high-risk systems

Chapter III, Section 1 sets out the classification rules and defines two main categories of high-risk AI systems:

- AI systems intended to be used as safety components of products subject to prior conformity assessment by third parties;
- other stand-alone AI systems that are explicitly mentioned in Annex III and primarily affect fundamental rights.

b) requirements for high-risk AI systems

Chapter III, Section 2 specifies the legal requirements that high-risk AI systems must meet in terms of data, data governance, documentation and record keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. The proposed minimum requirements, which are derived from the HEG's [498] tried and tested ethical guidelines[499] are already common practice for many conscientious actors and are the result of preparatory work over the last two years. They are also largely consistent with other international recommendations and principles, ensuring that the proposed AI framework corresponds to the requirements set out by international

[498] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts of April 21, 2021. See pages 15–17 of the AI Regulation.

[499] They were also endorsed by the Commission in its 2019 Communication on an AI for People approach.

([500]) High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.

trade partners of the EU. It is at the discretion of the provider of the respective AI system to decide which technical solutions it will use to achieve compliance with these requirements in practice – whether through standards or other technical specifications or through other developments in line with general scientific and technical know-how. [501]

4. Transparency obligations for certain AI systems

Chapter IV, Article 50 deals with specific manipulation risks of certain AI systems. Transparency obligations apply to systems that (i) interact with people,
ii) used to recognize emotions or associate (social) categories based on biometric data, or iii) generate or manipulate content ("deepfakes"). If people interact with AI systems or if their emotions or characteristics are recognized by automated means, they must be informed of this. If an AI system is used to generate or manipulate image, audio, or video content in such a way that it is difficult to distinguish from authentic content, the obligation to disclose the fact that the content was generated by automated means should be required, except for legitimate purposes (such as law enforcement, freedom of expression). This allows conscious decisions to be made or certain situations to be avoided. [502]

5. AI models with general purpose

Chapter V classifies AI models with general purpose use as AI models with systemic risk. Thus, in Article 51(1), an AI model with general purpose use is classified as an AI model with systemic risk if one of the following conditions is met:

[501] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Law on Artificial Intelligence) and amending certain Union acts of 21 April 2021. See pp. 15–17 of the AI Regulation.

[502] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Act on Artificial Intelligence) and amending certain Union acts of 21 April 2021. See page 17 of the AI Regulation.

b) It has high-impact capabilities that are assessed using appropriate technical instruments and methods, including indicators and benchmarks;

c) according to a decision taken by the Commission on its own initiative or on the basis of a qualified warning from the scientific committee, taking into account the criteria set out in Annex XIII, it has capabilities or an impact equivalent to those referred to in point (a).

6. Measures to promote innovation

Chapter VI was included with a view to creating an innovation-friendly, future-proof, and resilient legal framework. To this end, the competent national authorities are called upon to establish real-world laboratories and lay down the basic conditions for their management, supervision, and liability. AI real-world testing environments provide controlled testing environments for innovative technologies for a limited period of time, based on a test plan agreed with the competent authorities. Chapter VI, Article 62 of the AI Regulation also contains measures to reduce the administrative burden on SMEs and start-ups. [503]

7. Governance

Chapter VII, Section 1 contains requirements for governance structures at Union and national level. The proposal **provides for** the establishment **of a European Artificial Intelligence Board at** Union level**,** composed **of representatives of the Member States** and the Commission. The committee shall contribute to effective cooperation between national supervisory authorities and the Commission, thereby facilitating the smooth, effective, and harmonized implementation of the Regulation, and shall also provide expert advice to the Commission. Furthermore, the committee shall collect and disseminate best practices from the Member States. [504]

[503] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts of 21 April 2021. See p. 17 of the AI Regulation

[504] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Act on Artificial Intelligence) and amending certain Union acts of 21 April 2021. See page 17 of the AI Act

At national level, Member States will have to designate one or more national competent authorities (including the **national supervisory authority**) to monitor the application and enforcement of the Regulation. The European Data Protection Supervisor shall be the competent authority for supervising the Union institutions, bodies, agencies, and other entities covered by this Regulation. [505]

8. EU database for high-risk systems

Chapter VIII, Article 71 of the AI Act aims to facilitate the monitoring tasks of the Commission and national authorities by establishing a Union-wide database for high-risk AI systems that have significant effects on fundamental rights. The database will be operated by the Commission. It will be fed by the providers of AI systems, who must register their systems before they can place them on the market or put them into service in any other way.

9. Monitoring and reporting obligations

Chapter IX contains the monitoring and reporting obligations for providers of AI systems with regard to post-market monitoring and the reporting and investigation of incidents and malfunctions in the context of AI. Market surveillance authorities will also monitor the market and verify compliance with the obligations and requirements relating to all high-risk AI systems already placed on the market. Market surveillance authorities will be vested with all the powers laid down in Regulation (EU) 2019/1020 on market surveillance. **Ex-post enforcement** is intended to ensure that public authorities have the powers and resources to intervene if unexpected risks arise from AI systems already on the market that require rapid action. In addition, they will ensure that operators comply with their obligations under the Regulation.

[505] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts of 21 April 2021. See p. 18 of the AI Regulation

The proposal does not provide for the automatic creation of additional bodies or authorities at Member State level. Member States may therefore rely on existing sector-specific authorities and their expertise, which will be entrusted with the powers to monitor and enforce the provisions of this Regulation. [506]

10. Codes of conduct

Chapter X contains the basis for the creation of codes of conduct that are intended to encourage providers of AI systems that do not pose a high risk to voluntarily apply the mandatory requirements for high-risk AI systems. Providers of AI systems that do not pose a high risk may establish and implement codes of conduct themselves. These codes may also include voluntary commitments, for example with regard to environmental sustainability, access for persons with disabilities, stakeholder involvement in the design and development of AI systems, and the diversity of the development team. [507]

11. Delegation of powers and exclusion procedures

Chapter XI contains the rules governing the exercise of delegated powers and the exclusion procedure. Article 97 delegates to the Commission the power to adopt delegated acts under the conditions laid down in that article, and Article 98 provides that the Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

12. Sanctions

Chapter XII contains provisions on infringements of the AI Regulation. Thus, the maximum fine in Article 99(3) for failure to comply with the prohibition in Article 5

[506] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts of 21 April 2021. See p. 18 of the AI Regulation

[507] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts of 21 April 2021. See page 18 of the AI Regulation.

AI practices, imposing fines of up to EUR 35,000,000 or, in the case of companies, up to 7% of the total worldwide annual turnover of the previous financial year, whichever is higher.

13. Final provisions

Chapter 13 contains the final provisions.

II. Transparency obligations under Article 52 of the AI Regulation

The transparency obligations for providers and users of high-risk AI systems under Article 52 of the European Regulation on Artificial Intelligence (AI Regulation) are of considerable importance for the legal and ethical use of AI systems. Article 52 of the AI Regulation establishes comprehensive transparency rules that providers of high-risk AI systems must comply with in the future. Failure to comply with these rules could prove very costly for providers of high-risk AI systems in the future and is therefore of considerable importance for the future of the digital economy.

1. AI system

According to Art. 3 No. 1 AI Regulation, an AI system is a *"machine-based system designed for operation with varying degrees of autonomy, which may be adaptable after it has been put into service and which, based on the inputs it receives, derives outputs such as predictions, content, recommendations or decisions that* can *affect physical or virtual environments*." An essential feature of an AI system is its ability to derive outputs from the data it receives. This ability to derive outputs is based on the concept of machine learning and logic- and knowledge-based concepts. [508]

The transparency obligations for providers and users of AI systems under Article 52 of the AI Regulation are essential for ensuring the responsible use of AI systems classified as high-risk AI systems within the meaning of Article 6 of the AI Regulation. Article 52 of the AI Regulation sets out specific transparency requirements aimed at enabling users to make informed decisions about the use of AI systems and to understand potential risks.

[508] Recital 12 AI Regulation.

2. High-risk AI systems

For Art. 52 AI Regulation to apply, a high-risk AI system within the meaning of Art. 6 AI Regulation must exist. AI systems are classified as high-risk AI systems if they are safety components or products subject to Union harmonization rules pursuant to Article 6(1)(a) and (b) of the AI Regulation or if they are used in the areas listed in Annex III, Nos. 1–8, pursuant to paragraph 2. If these systems fall under Article 6 of the AI Regulation, they must undergo a conformity assessment before being placed on the Union market. The conformity assessment examines data governance, risk management, quality management, and other factors. High-risk systems must comply with the requirements of Article 8 of the AI Regulation. AI systems classified as high-risk systems under Article 6(1) of the AI Regulation in conjunction with Annex I, Section B of the AI Regulation do not have to undergo conformity assessment because their compliance with the harmonization rules means that they can be assumed to be compliant. The European Commission has already moved closer to defining the obligations de conformité et de bonne conduite (OCB), which is also included in the latest version. [509] The new definition in Article 3(1) of the AI Regulation is intended to better describe the characteristics of AI. The essential characteristics of AI are the degree of autonomy, which presupposes independence. The aspect of autonomy is not the only characteristic; adaptability also applies in the AI Regulation. The independent development of AI systems takes place via machine learning [510] which is carried out by adjusting parameters within the system in order to generate the optimal output.[511] However, some are of the opinion that the term

"Degree of autonomy" could prove problematic, as this definition may be too broad. [512]The most important standards for the liability of AI systems are the Product Liability Directive, the AI Regulation, and the AI Liability Directive. The EU's AI Liability Directive is intended to remedy this situation. Although it does not serve as a basis for liability, it has been designed to provide the necessary

[509] *Bomhard/Siglmüller*, RDi 2024, 45, para. 1.
[510] *Heine/Frank*, NZA 2023, p. 1281.
[511] *Görgülü* et al., BKR 2024, p. 175.
[512] *Becker/Feuerstack*, MMR 2024, p. 22.

information pursuant to Art. 3 AI Regulation in order to establish causality between the AI system and damage caused,[513] which could enable a basis for liability under other laws.[514]

Article 6 of the AI Regulation regulates the classification of AI systems that qualify as high-risk systems. The classification is based on the intended purpose of the system. According to Art. 3 No. 12 AI Regulation, the intended purpose[515] is the use specified by the provider. The specific circumstances and conditions for use provided by the provider in the operating instructions, in advertising and sales materials, and in the information contained in the technical documentation apply. An AI system is high-risk if its use poses risks to the health, safety, or fundamental rights of natural persons. When classifying such systems, both the severity of the damage and the probability of the damage occurring must be taken into account, as well as the areas of application predefined in the AI Regulation.[516] Article 6 of the AI Regulation recognizes two categories for classifying systems as high risk: [517] one according to Article 6(1) of the AI Regulation and one according to Article 6(2) of the AI Regulation.

The AI Regulation follows the product safety requirements of the New Legislative Approach (NLF). Therefore, the first section of Article 6(1)(a) of the AI Regulation also classifies high-risk systems according to whether they are installed as safety components of a product within the harmonization provisions listed in Annex I of the AI Regulation or whether they are stand-alone products in this area. Harmonization regulations listed in Annex I of the AI Regulation include, for example, directives on the safety of toys, safety components for elevators, and personal protective equipment. In addition, according to Article 6(1)(b) of the AI Regulation, the stand-alone product or the product of which an AI system is a safety component must undergo a conformity assessment

513 *Görgülü* et al., BKR 2024, p. 175.
514 *Staudenmayer*, NJW 2023, p. 894, para. 8.
515 *Baumann/Wirtz*, RDi 2024, p. 27.
516 Recital 52 AI Regulation.
517 *Geminn*, ZD 2021, p. 354.

be subjected to third-party checks before being placed on the Union market.

The key term for classification under Article 6(1) of the AI Regulation is "safety component." The AI Regulation also defines a safety component as a component that can perform safety functions or as a component whose failure poses a risk to the safety and health of natural persons (in accordance with Article 3(14) of the AI Regulation). Recital 52[518] states that the intended purpose also plays a decisive role in determining whether an AI system is classified as high-risk. If AI systems pose a high risk to health and safety based on their intended purpose, they should also be classified as high-risk. Furthermore, both the probability of the damage occurring and the severity of the damage are relevant. Eight areas are listed in Annex III of the AI Regulation. If the AI system is used in one of these areas, it is by definition considered a high-risk system. The areas cover points of contact between humans and machines where damage is most likely to occur.

3. Art. 52 AI Regulation

The provision in Art. 52 of the AI Regulation will be of considerable importance for many AI companies in the future.

b) Text of Article 52 of the AI Regulation

First of all, the wording of Art. 52 of the AI Regulation, which deals with transparency obligations, states the following:

"*Providers of high-risk AI systems shall ensure that the AI systems are accompanied by sufficient information to provide a comprehensible and understandable description of the AI systems, their functioning, and their potential effects on users and data subjects.*

The information shall include at least:

[518] Recital 52 AI Regulation.

a. the identity and contact details of the provider;

b. the intended purposes and areas of application of the AI systems;

c. the type of data used to train the AI systems;

d. the performance, accuracy, and robustness of AI systems;

e. the risks associated with the use of AI systems and the measures taken to mitigate them;

f. the manner in which the decisions of AI systems are verifiable and interpretable;

g. the requirements for use, including technical requirements and the necessary qualifications of users;

h. information about the procedure for reporting and resolving problems and risks."

The recitals of the AI Regulation provide important background information and explanations on the provisions of the Regulation, including Article 52 AI Regulation. These recitals provide context and clarify the intentions of the legislator. With regard to Article 52 of the AI Regulation, which concerns transparency obligations, the recitals contain essential details on why transparency is necessary and what objectives are pursued by it.

c) Recitals

Recital 70[519] addresses the need for users of high-risk AI systems to be adequately informed about the functioning, risks, and limitations of these systems. It emphasizes that transparency is an essential prerequisite for building trust in high-risk AI systems and promoting their responsible use. Users should be empowered to make informed decisions about the use of high-risk AI systems and understand their potential impact.

[519] Recital 70 AI Regulation.

Recital 71[520] explains that providing clear and understandable information about high-risk AI systems should help prevent misunderstandings and misuse. This includes information about the training data, the performance of the systems, and the risk mitigation measures. The transparency obligations are intended to ensure that users can realistically assess the limitations and capabilities of high-risk AI systems.

Recital 72[521] emphasizes the importance of traceability and the ability to interpret the decisions made by AI systems. This is particularly important in order to ensure that decisions are fair and equitable. The recital emphasizes that transparency is crucial not only for users but also for supervisory authorities in order to monitor and enforce compliance with the rules.

The recitals make it clear that the transparency obligations in Article 52 of the AI Act are part of a broader approach to strengthen trust in AI technologies and ensure the ethical and legal accountability of providers and users. By providing detailed information, users should be empowered to better understand and assess the functioning and potential risks of high-risk AI systems.

Given the emphasis on the traceability and comprehensibility of information, it is clear that transparency is a key factor in the acceptance of high-risk AI systems. Users must be able to trust that the systems are reliable and secure and that they can access clear and comprehensible information when needed.

[520] Recital 71 AI Regulation.

[521] Recital 72 AI Regulation.

The recitals suggest that transparency is also a means of proactively managing risks and strengthening the accountability of providers. By disclosing information about the training data, performance, and risks of high-risk AI systems, potential problems can be identified and addressed at an early stage.

The recitals emphasize that transparency is also crucial for regulatory oversight and enforcement. Supervisory authorities need clear and comprehensive information to verify compliance with legal requirements and take action where necessary.

The recitals to Article 52 of the AI Regulation provide clear insight into the background and objectives of the transparency obligations. They emphasize the need to build trust in AI systems, promote informed use, and strengthen the accountability of providers. By providing clear and understandable information, users should be empowered to make informed decisions and better manage potential risks. These recitals form the basis for the detailed requirements set out in Article 52 of the AI Regulation and clarify the comprehensive objectives of the Regulation to ensure the responsible and transparent use of AI technologies.

4. Analysis of transparency obligations

According to Article 52 of the AI Regulation, high-risk AI systems must take the following points into account.

a) Traceability and comprehensibility

One of the key requirements is that the information provided must be traceable and understandable. This implies that the documentation and explanations must be accessible not only to technically experienced users, but also to laypersons. This is to ensure that all stakeholders, including end users and persons affected by the decisions of high-risk AI systems, can understand how the system works and its potential effects.

Stakeholders, including end users and persons affected by the decisions of high-risk AI systems, can understand how they work and their potential effects.

b) Identity and contact details of the provider

Transparency regarding the identity and contact details of the provider serves to assign responsibility and enables direct communication in the event of questions or problems. This promotes user confidence in high-risk AI systems.

c) Purposes and intended uses

A clear definition of the intended purposes and areas of application helps to understand the scope of use of high-risk AI systems and prevent misuse or misapplication.

d) Training data

Disclosure of the type of data used for training addresses important ethical and legal concerns, such as bias and discrimination. Transparency regarding data sources and the type of data can contribute to acceptance of and trust in high-risk AI systems.

e) Performance, accuracy, and robustness

Information about the performance, accuracy, and robustness of high-risk AI systems is crucial for assessing the reliability and limitations of the systems. This enables a realistic assessment of capabilities and prevents exaggerated expectations.

f) Risk assessment and mitigation

Identifying and communicating the risks associated with use and the measures to mitigate them is essential to enable informed decisions and ensure responsible use. This also includes ethical considerations and the consideration of data protection aspects,

decisions and ensure responsible use. This also includes ethical considerations and the consideration of data protection aspects.

g) verifiability and interpretability

The verifiability and interpretability of decisions made by high-risk AI systems are particularly important to ensure transparency and fairness. This requires technological solutions and documented procedures that enable the decision-making processes to be verified independently.

h) Prerequisites for use

The presentation of the technical requirements and the necessary user qualifications ensures that high-risk AI systems are only used by persons who have the necessary knowledge and skills to use them safely and effectively.

i) Problem and risk management

A clearly defined procedure for reporting and resolving problems and risks supports the continuous improvement and adaptation of high-risk AI systems to changing conditions and new findings.

5. Summary

The transparency obligations under Article 52 of the AI Regulation are designed to promote the informed use of high-risk AI systems, ensure ethical and legal standards, and strengthen user confidence. For providers and users of high-risk AI systems, this means a comprehensive obligation to provide clear, understandable, and comprehensive information to ensure the accountability, traceability, and safety of high-risk AI systems. Whether these measures are essential to minimize potential risks and maximize the positive effects of AI technologies remains to be seen.

III. Contract design in light of the AI

The European Union's Artificial Intelligence Regulation (AI Regulation or AI Law), which is still in the final stages of approval, aims to create a comprehensive legal framework for the use of AI technologies. A central aspect of the regulation is Article 25(4), which sets out specific obligations for providers of AI systems towards their users. This article addresses in particular the question of which contractual requirements lawyers will have to take into account when using AI systems in the future.

1. Introduction

The risk-based approach of the AI Regulation (AI Regulation (European Commission proposal), COM (2021) 206 final), particularly with regard to high-risk AI systems, not only has implications for the protection of the safety, health, and fundamental rights of natural persons, but also imposes new requirements on the contractual arrangements between providers and users of such systems. According to Art. 25 (4) AI Regulation, providers are obliged to ensure that users use high-risk AI systems in accordance with the applicable legal requirements. This leads to specific contractual obligations that must be laid down in user agreements.

Art. 25 AI Regulation, the contractual specification of the purpose of the provision of an AI system is crucial in order to establish a clear legal basis for the deployment and use of the AI system. This requirement aims to ensure the safety, transparency, and lawfulness of the use of AI systems, in particular high-risk AI systems that may have significant effects on the rights and freedoms of natural persons. Several key reasons can be derived from the AI Regulation and general legal principles as to why the purpose of the provision of an AI system must be contractually specified.

For contract law, this means that providers will be contractually obliged to provide users with essential information about the functioning, risks, and safety precautions of the AI system. In addition, contracts must contain clauses on ongoing monitoring, maintenance, and updating of the systems to ensure their compliance with the regulation. Article 25(4) of the AI Regulation thus entails a significant extension of contractual obligations in the area of the use of high-risk AI systems, comparable to the data protection obligations under the GDPR. This establishes a close link between the AI Regulation and contract law, which must be taken into account in practice when drafting and interpreting contracts.

2. Content and significance of Art. 25(4) AI Regulation

a) Basis in Art. 25(4) of the AI Regulation

Art. 25(4) of the AI Regulation clarifies that providers of high-risk AI systems (as defined in Annex III of the Regulation, see *Annex III of the AI Regulation (classification of high-risk AI systems (*Art. 25(4) AI Regulation (obligations of the provider in relation to the user)) must ensure that the systems are operated in accordance with the obligations set out in the Regulation. Annex III of the AI Regulation (AI Regulation) contains a detailed list of AI systems that are classified as high-risk AI systems and are therefore subject to special regulatory requirements. These requirements apply in particular to the use of such systems in areas that are of significant importance for the rights and freedoms of natural persons, including the security of critical infrastructure, education and training, personnel management, law enforcement, and border control.

With regard to Art. 25 (4) of the AI Regulation, "Obligations of the provider in relation to the user," the high-risk classification according to Annex III has significant implications for the contractual arrangements between providers and users of high-risk AI systems. In particular, Art. 25 (4) obliges providers

of such systems to contractually ensure that users are able to fulfill the relevant legal obligations regarding the safe and lawful use of AI systems.

b) Contractual obligations under Article 25(4) of the AI Regulation

Transparency and information: The provider must provide the user with comprehensive information about how the AI system works in the contract. This includes information about the algorithms, training material, technical parameters, and performance of the system, as well as the potential risks and side effects that could result from using the system. These transparency requirements are particularly important for high-risk AI systems in order to enable users to fulfill their own legal obligations, for example in the area of data protection or product safety.

Ongoing monitoring and maintenance obligations: Art. 25 (4) in conjunction with the requirements of Annex III obliges the provider to contractually ensure that the user has access to all necessary security updates and technical maintenance. These are ongoing obligations designed to ensure that the high-risk AI system complies with regulatory requirements throughout its entire service life. This obligation applies not only to technical aspects, but also to possible changes in the legal assessment of the system.

Liability and risk allocation: Contracts must contain clear provisions on liability for any damage that may arise from the use of high-risk AI systems. Article 25(4) requires that the provider contractually grants the user the option of taking measures if it becomes apparent that the system no longer complies with the applicable regulations or poses safety risks. This includes, in particular, the provider's obligation to inform the user immediately of any safety-related incidents related to the operation of the AI system.

User participation rights and control: The contract must grant the user of the high-risk AI system control rights that enable them to monitor the use of the system and, if necessary, adjust or interrupt it if this is required to comply with legal regulations. This means that the user must be regularly informed about the functioning of the AI system and must be provided with appropriate control tools by the provider that enable them to carry out adequate monitoring.

c) Consideration of Annex III AI Regulation

The classification of AI systems as high-risk systems in accordance with Annex III requires extensive contractual adjustments. In particular, providers of high-risk AI systems must ensure in their contracts that users are able to meet the legal requirements resulting from the classification as a high-risk system. This includes providing sufficient information on the use and control of the system and complying with security and transparency obligations.

From a legal perspective, these contractual obligations are comparable to the obligations in data processing agreements pursuant to Art. 28 GDPR, as they aim to achieve comprehensive risk distribution and compliance with regulatory requirements. However, while the GDPR focuses on the protection of personal data, the AI Act requires, in addition to the protection of fundamental rights, comprehensive security measures and regular checks of the technical integrity of the system.

3. Comparison with data processing agreements pursuant to Art. 28 GDPR

a) processing pursuant to Art. 28 GDPR

A key point of the GDPR is order processing in accordance with Art. 28 in conjunction with Art. 32 GDPR, which regulates the conditions under which a controller may outsource data processing to third parties. The order processing agreements (OPAs) required there contain strict requirements for the processor

to ensure that personal data is processed in accordance with the provisions of the GDPR.

b) Some key elements of a DPA are:

- Binding instructions: The processor may only process the data on the basis of the documented instructions of the controller.
- Data security measures: The processor must take appropriate technical and organizational measures to ensure the protection of personal data.
- Verification and evidence: The processor must provide the controller with all information necessary to demonstrate compliance with the obligations.

While the focus of an AVS under Article 28 GDPR is on the protection of personal data, Article 25(4) AI Regulation goes further. Here, not only data protection aspects must be taken into account, but also general security and transparency obligations for the functioning of AI systems.

c) Some key differences and parallels:

There are both parallels and differences compared to the contractual requirements of the GDPR, in particular Art. 28 GDPR (contract processing). Art. 28 GDPR regulates the contractual obligations between a controller and a processor when personal data is processed on behalf of the controller. The contractual requirements here relate in particular to:

- **Binding instructions**: The processor may only process personal data in accordance with the documented instructions of the controller (Article 28(3)(a) GDPR).
- **Data security measures**: The processor must take appropriate technical and organizational measures to ensure the protection of the data (Art. 28 (3) (c) GDPR).

- **Right to audit**: The controller has the right to audit the processor to ensure that the data protection requirements are being met (Art. 28 (3) (h) GDPR).

These requirements are similar to the contractual obligations under Article 25 of the AI Regulation, in particular with regard to transparency, monitoring, and testing obligations. Under Article 25 of the AI Regulation, the provider must also ensure that the user can use the AI system lawfully and securely and that the user is given appropriate means of control over the use of the system.

Art. 25(4) AI Regulation extends the obligations of providers compared to the GDPR by ensuring that not only the protection of personal data but also the security and transparency of AI systems are guaranteed. Lawyers should take these extended requirements into account when drafting contracts for AI systems, particularly with regard to transparency, security, and ongoing liability. A comparison with Art. 28 GDPR shows that both provisions impose similar obligations but focus on different protection objectives: The GDPR protects personal data, while Art. 25(4) AI Regulation prescribes a more comprehensive security and control regime for the use of AI systems. A comparison between Art. 25(4) AI Regulation and Art. 28 GDPR appears useful and reveals the following points:

- **Information obligations**: Both standards require the provider or processor to provide essential information. While the AVV deals with data processing, Art. 25(4) AI Regulation focuses on the functioning and risks of the AI system.
- **Security obligations**: In both cases, the provider/processor must take technical and organizational measures. However, in the AI Regulation, these measures relate not only to data protection but also to the security of the AI application as a whole.
- **Control options**: Both Art. 28 GDPR and Art. 25(4) AI Regulation require that the user or controller has control options.

In the AI Act, these are extended to control over the use of the AI system.

4. Contract design for AI systems

The following points can be used as a checklist when drafting contracts for AI systems, but this list is not exhaustive.

a) General requirements for

Lawyers drafting contracts for the use of high-risk AI systems should consider the following points:

- **Transparency clauses**: Similar to a GTC, the provider should be required to provide detailed information on how the AI system works and the security risks it poses.
- **Liability and risk allocation provisions**: Since high-risk AI systems can have potentially serious consequences, clear liability clauses should be included to cover any malfunctions or data breaches.
- **Ongoing security and update obligations:** Providers should be required to provide regular updates and patches to close security gaps and ensure the proper functioning of the AI system.
- **User control options:** Users should have the contractual right to monitor the use of the AI system and, if necessary, take measures to restrict or terminate its use if security risks are identified.

b) Providers of AI systems

If the contract drafter is active on the provider side of AI systems, they should also pay attention to what obligations they require from their subcontractors,

even if they do not themselves supply AI systems within the meaning of Art. 6 AI Regulation "high-risk systems," such as traditional IT providers.

(1) On the procurement side

In this regard, the following requirements under Article 25 of the AI Regulation must be observed on the procurement side:

- Information to meet your own risk management requirements, see Article 9 of the AI Regulation.
- Information to meet your own quality management requirements, see Art. 17 AI Regulation.
- Technical information and documentation to meet your own requirements, see Art. 11 AI Regulation, as well as traceability and transparency, see Art. 13 AI Regulation.
- Requirements for continuous service provision, such as update obligations for:
  - Updating technical documentation, see Art. 11 AI Regulation.
  - Continuous monitoring and maintenance, see Art. 23 AI Regulation.
  - Notification of significant changes, see Art. 43 AI Regulation.
  - Post-marketing surveillance and feedback, see Art. 61 CI Regulation.
  - Need for a conformity assessment procedure in the event of significant changes, see Art. 43 CI Regulation.
  - Liability, costs, etc.

(2) On the distribution side

On the distribution side, the following requirements in particular must be observed in accordance with Art. 25 AI- VO:

- Determination of the purpose of the transfer Description of the AI system, see Art. 6 and Art. 25 (2) AI Regulation:
  - To prevent misuse and abuse
  - Limitation of use to the specified purpose
- Compliance with regulatory requirements through purpose limitation

- Transparency and traceability of use
- Risk management and allocation of liability
- Compliance with regulatory requirements
- Limitation of liability

c) Operators of AI systems that are subject to the General Data Protection Regulation

The following points may be relevant for the operators of AI systems when drafting contracts:

(1) Procurement for own use

- Contractual specification of the intended use, see Art. 6 and Art. 25 (2) AI Regulation
- Ensuring compliance with the AI Regulation, see Articles 9 to 15 of the AI Regulation.
- The provider must contractually guarantee that the AI system has undergone the necessary conformity assessment procedures in accordance with Art. 43 AI Regulation and that the relevant certifications or evidence are available.
- Technical documentation and information obligations, see Art. 11 AI Regulation
- Maintenance, updates, and security measures, see Art. 23 AI Regulation
- Liability and warranty, Art. 25 (2) AI Regulation; Sections 434 et seq. BGB (liability for defects)
- Ensuring compliance and audit rights, see Art. 23 and Art. 25 (2) AI Regulation
- Data protection and GDPR compliance, see Art. 25 (2) AI Regulation

(2) Procurement with adjustments

- Requirements pursuant to Art. 25 (1) AI Regulation
  - Establishment of a quality assurance system
  - Documentation of the quality assurance system
  - Requirements for the risk management system
  - Review and validation of the AI system
  - Transparency requirements and information obligations

- If significant changes within the meaning of Art. 25 (2) (b) or (c) of the AI Regulation are made:
- Definition of the subject matter and purpose
  - Check exclusion of high-risk AI systems, see Art. 25 (2) sentence 3 AI Regulation
  - Request a program of obligations from the supply chain (see above IV. No. 2 lit. a)
- Continuous information obligations
- Support services
- License agreement for IT/AI system, if applicable

5. Summary

The EU AI Regulation establishes a regulatory framework that has far-reaching implications for contract drafting in the field of high-risk AI systems. A comparison with the contractual requirements of the General Data Protection Regulation (GDPR), in particular Art. 28 GDPR, reveals both parallels and differences that must be taken into account when drafting contracts.

The requirements of the AI Regulation, in particular those set out in Article 25, set high standards for the drafting of contracts for providers of high-risk AI systems. The obligations to implement quality assurance and risk management systems, to ensure transparency towards users, and to provide for liability and risk sharing are central elements of the contractual provisions. There are clear parallels with the contractual requirements of the GDPR under Article 28, particularly with regard to transparency and monitoring obligations, but there are also significant differences in the objectives and the scope of the risks to be taken into account. While Article 28 GDPR focuses on the protection of personal data, Article 25 AI Regulation comprehensively addresses security, reliability, and risk minimization in the use of AI systems that are potentially

may have a significant impact on the rights and freedoms of natural persons.

The parties involved in drafting contracts have a lot to do, and implementation in contracts will certainly be extensive.

IV. Quality management in accordance with the AI Regulation

With the introduction of the EU AI Regulation (AI Regulation), the question also arises as to what requirements companies that use AI must meet in the area of quality management. The central standard for this is Article 17 of the AI Regulation, which contains specific requirements for quality management for high-risk AI systems. There are already established international standards in the field of quality and risk management, in particular ISO 42001 as a specific standard for AI management systems, ISO 9001 as a general standard for quality management systems, and ISO 27001 for information security management systems. The following section examines whether compliance with these standards is also sufficient to meet the requirements of Art. 17 AI Regulation. [522]

1. Introduction

The rapid development of artificial intelligence (AI) systems and their increasing use in safety-critical and socially relevant areas poses considerable challenges for both the economy and legislators. In particular, so-called high-risk AI systems, for example in medical diagnostics, safety-critical infrastructure, or employment, can have a significant impact on people's lives and rights. Against this background, the European Union has created a regulatory framework with the AI Regulation (AIoC) [523] to ensure the safe and trustworthy use of such systems.

A central element of this regulation is Article 17 of the AI Regulation, which obliges providers of high-risk AI systems to establish and maintain a quality and risk management system. The aim is to ensure continuous compliance with legal requirements and effective risk minimization throughout the entire life cycle of AI systems. This brings the

[522] See also *Söbbing* RDi 2025, p. 337ff.

[523] Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

focus on how these regulatory requirements can be implemented in practice.[524]

There are already established international standards in the field of quality and risk management, in particular ISO 42001525 as a specific standard for AI management systems, ISO 9001 as a general standard for quality management systems, and ISO 27001 for information security management systems. These standards provide structured procedures for planning, implementing, monitoring, and continuously improving management systems. This raises the question of the extent to which these standards are suitable for fulfilling or at least supporting the requirements of Art. 17 AI Regulation. The aim of the considerations is to present the requirements of Article 17 of the AI Regulation in detail, analyze their practical implementation possibilities within the framework of the aforementioned ISO standards, and assess from a legal perspective whether certification according to these standards is sufficient as proof of compliance with the legal obligations. Particular attention is paid to the interfaces and possible gaps between the regulatory requirements and the standard specifications.

2. Overview of the requirements of Art. 17 AI Regulation

a) Objective and structure

With Article 17 of the AI Regulation, the European legislator aims to ensure that providers of high-risk AI systems have appropriate internal structures and processes in place to ensure the conformity of their systems throughout their entire life cycle.[526] The provision thus specifies the general conformity assessment regime of the AI Regulation and forms a bridge between product-specific risk management and organizational quality management.[527] While Article 9 of the AI Regulation regulates risk management at the level of the individual AI system, Article 17 addresses the underlying operational

[524] Wendt/Wendt Das neue Recht der künstlichen Intelligenz (The New Law on Artificial Intelligence), 1st edition, 2024, Section 6, margin number 6 et seq.

[525] Author: ISO Technical Committee JTC 1/SC 42, available at https://www.iso.org/news/ref2865.html.

[526] Art. 17 I AI Regulation; BeckOK AI Law/Henke, AI Regulation Art. 17 margin note 3.

[527] Wendt/Wendt Das neue Recht der künstlichen Intelligenz (The New Law on Artificial Intelligence), 1st edition 2024, Section 6, margin note 6 et seq.

Organization and its ability to effectively control and document risk management processes. To ensure that AI systems comply with the requirements of this Regulation, providers of high-risk AI systems should establish a quality management system that functions as part of their internal governance structure. This system should include procedures for implementing the requirements set out in this Regulation. [528]

The provision thus requires the introduction, documentation, and continuous maintenance of a quality management system that is suitable for systematically addressing all requirements of the AI Regulation—in particular with regard to risk minimization, transparency, data quality, and human oversight.[529] Article 17 thus plays a central role in operationalizing the regulatory requirements and emphasizes the importance of a structured management system for compliance. [530]

b) Obligation to introduce a quality and risk management system

Article 17 of the AI Act requires providers of high-risk AI systems to introduce, document, and maintain a quality and risk management system. This obligation is not optional but mandatory and constitutes a basic prerequisite for placing such systems on the market and keeping them in operation.[531] The standard thus addresses the organizational duty of care of providers and requires that not only the product itself is compliant, but also that the underlying operational structures are suitable for ensuring ongoing compliance with the regulation. [532]

It should be noted that the AI Regulation follows a life cycle approach. This means that the management system must cover all phases of the AI system – from design and development to validation and use.

---

[528] AI Regulation Recital 48 – Purpose of the quality management system.

[529] AI Regulation Recital 48 – Purpose of the quality management system.

[530] Martini/Wendehorst/Eisenberger, 1st edition 2024, AI Regulation Art. 16 margin note 21.

[531] Art. 17 I AI Regulation; BeckOK AI Law/Henke, AI Regulation Art. 17 para. 3.

[532] AI Regulation Recital 48 – Purpose of the quality management system.

maintenance and, if necessary, decommissioning. [533] The implementation of such a system requires systematic planning, clear responsibilities, documented processes, and effective control mechanisms, cf. Art. 17 II AI Regulation.

c) Minimum requirements for the AI management system

Art. 17 II AI-Regulation specifies the minimum content of the required management system and explicitly mentions the following elements:

- Establishment of a strategy for compliance with legal requirements
- Procedures for risk assessment and mitigation
- Mechanisms for monitoring and evaluating the performance of the AI system,
- Documentation of all relevant processes and measures,
- procedures for maintaining compliance throughout the entire life cycle.

These requirements are closely linked to the principles of quality management as laid down in ISO 9001, for example.[534] In particular the principle of the "plan-do-check-act" cycle (PDCA cycle) is reflected in the structure of Article 17 of the AI Regulation. [535] It therefore makes sense to draw on existing QM standards in order to translate the requirements of the Regulation into a functioning management system.

At the same time [363], the AI Regulation goes beyond traditional quality management aspects. For example, in the area of AI-specific risks, it requires special measures to ensure data quality, minimize bias, and ensure human oversight, which have so far only been dealt with marginally in general QM standards. [373]

---

533 BeckOK AI Law/ Henke, AI Regulation Art. 17 Rn. 4.

534 ISO 9001:2015, Section 4 ff.

535 The "Plan-Do-Check-Act" cycle (PDCA cycle) is an iterative management model for the continuous improvement of processes and systems, particularly in the context of quality management systems. It is a central component of many standards, in particular ISO 9001, ISO 14001 and also ISO/IEC 42001:2023, available at https://www.iso.org/standard/62085.html.

536 In estimation theory, a branch of mathematical statistics, the bias or systematic error of an estimation function is the key figure or property of an estimation function that quantifies the systematic overestimation or underestimation of the estimation function, cf. Georgii Stochastik, 2009, p. 207.

537 BeckOK AI Law/Henke, AI Regulation Art. 17 Rn. 5

3. Relationship to other regulatory obligations (in particular Art. 9 AI Regulation – risk management)

A key feature of Art. 17 AI Regulation is its close interlinking with Art. 9 AI Regulation. While Art. 9 prescribes the specific risk assessment and mitigation for the respective AI system, Art. 17 provides the organizational framework for systematically implementing these requirements. The risk management system pursuant to Art. 9 is thus an integral part of the overarching quality management system within the meaning of Art. 17. [538]

This is evident, for example, in the fact that Article 17 expressly requires procedures for conducting and documenting risk assessments. This pursues an integrative approach that relies not only on ad hoc risk assessments, but also on the structured and repeatable embedding of risk management in corporate processes. [539]

A parallel to this can be found in product safety law, for example in medical device law or in the Machinery Directive, where a distinction is also made between product-specific risk assessments and the requirements for the manufacturer's quality management system. [540]

The AI Regulation takes up this logic and applies it to the field of artificial intelligence, focusing not only on physical dangers but also on algorithmic risks. These include, in particular, problems such as discrimination due to faulty training data, lack of transparency in algorithmic decisions (black box problem), and lack of human control. [541]

[538] Wendt/Wendt Das neue Recht der künstlichen Intelligenz (The New Law on Artificial Intelligence), 1st edition 2024, § 6 Rn. 6 f.

[539] Art. 17 II letter b AI Regulation.

[540] See, for example, § 30 MPG (old version), Art. 10 MDR (EU) 2017/745.

[541] BeckOK AI Law/Henke, AI Regulation Art. 17 margin note 5.

These special features require that the quality management system includes specific measures for risk identification and mitigation for AI systems that go beyond the general requirements of conventional QM standards.

4. ISO 42001:2023 – AI Management System

a) Structure and objective of the standard

With the publication of ISO 42001 in December 2023, an internationally recognized standard for a management system specifically designed for the use of artificial intelligence will be available for the first time.[542] The standard is intended as a guide for organizations that develop, provide, or operate AI systems and aims to establish a systematic framework for managing and controlling AI-related risks. Its structure is based on the so-called High-Level Structure (HLS), which represents a uniform basic structure for ISO management system standards and is already used in ISO 9001 and ISO 27001. [543]

The overall objective of ISO 42001 is to help organizations operate AI systems responsibly, safely, and in compliance with the law. To this end, the standard defines requirements for the implementation of an AI Management System (AIMS) that covers all relevant aspects of the AI system lifecycle, including planning, implementation, monitoring, evaluation, and improvement.[544]

[542] ISO 42001:2023, Introduction.

[543] ISO 42001:2023, Introduction; see also ISO 9001:2015 and ISO 27001:2022, Introduction.

[544] ISO/IEC 42001:2023, Artificial intelligence management systems. Refers several times to the PDCA cycle as a conceptual basis, available at https://www.iso.org/standard/81230.html.

b) Requirements for planning, implementation, monitoring, and continuous improvement

ISO 42001 requires organizations to establish an AI-specific policy that is geared toward compliance with legal and regulatory requirements as well as ethical principles. The standard expressly emphasizes the need for a risk analysis that covers technical, ethical, and social aspects.

Specifically, the standard contains requirements for the following elements:

- Definition of AI-related objectives and commitments,
- Risk identification and assessment with regard to the development and application of AI systems
- Establishment of appropriate controls and measures for risk treatment,
- Conducting internal audits to verify the effectiveness of the system,
- Management reviews for systematic evaluation of AIMS performance,
- implementation of measures for continuous improvement.

The PDCA cycle forms the methodological backbone of the standard. Planning ("Plan") involves defining objectives and processes, implementation ("Do") refers to the implementation of the planned measures, review ("Check") is carried out through monitoring and internal audits, and improvement ("Act") involves deriving and implementing optimization measures based on the results of the review. [546]

ISO 42001 places particular emphasis on impact assessments, which evaluate the potential effects of an AI system on affected parties, society, and the environment. The standard thus ties in with international discourse on human-centered AI and supports

[545] ISO 42001:2023, Section 4 ff.

[546] ISO 42001:2023, Section 4 ff.; for the PDCA cycle, see also ISO 9001:2015, Annex A.

Providers are addressing risks that go beyond the purely technical perspective. [547]

c) Conformity potential with Art. 17 AI

ISO 42001 is highly compatible with the requirements of Art. 17 of the AI Regulation. In particular, the systematic anchoring of risk management processes, the documentation requirements, and the obligation to continuously review and improve are in line with the minimum requirements of the Regulation. This applies in particular to the requirements for:

- Life cycle-oriented risk management,
- Establishment of clear responsibilities and accountabilities,
- Documentation and traceability of decision-making,
- Monitoring and adaptation in the event of changed framework conditions.

However, it should be noted that ISO 42001 does not make any direct regulatory compliance promises with regard to the AI Act. Rather, the standard provides a flexible framework that must be adapted and specified by users in order to fully reflect the specific requirements of the European legal framework, for example with regard to bias detection, transparency, and human oversight.

Nevertheless, due to its clear focus on AI and its systematic orientation toward risk management and compliance, ISO 42001 is a suitable instrument for implementing and supporting the requirements of Art. 17 AI Regulation, at least to a large extent. However, a complete compliance assessment will in any case require a supplementary legal assessment and, if necessary, additional measures outside the scope of the standard.

[547] ISO 42001:2023, Section 6.1.3.

[548] BeckOK AI Law/Henke, AI Regulation Art. 17 Rn. 6

5. ISO 9001:2015 – Quality management systems

a) Fundamentals and scope

ISO 9001:2015 is the most widely used standard for quality management systems (QMS) worldwide. Its aim is to help organizations demonstrate their ability to consistently provide products and services that meet customer requirements and applicable legal and regulatory requirements.[549]The standard follows a process-oriented approach and is based on the principles of quality management, including customer focus, leadership, commitment of people, process-oriented approach, improvement, fact-based decision-making, and relationship management. [550]

The standard is not aimed at specific industries or product types, but is applicable across industries and can be flexibly adapted. Its main strength lies in the standardization of operational processes and the systematic anchoring of quality assurance across all processes.

b) Relevance for the quality requirements of Art. 17 AI Regulation

Although ISO 9001 does not specifically refer to AI systems or algorithmic risks, it provides a solid framework for quality management that can also be used for the implementation of Art. 17 AI Regulation. The following aspects are particularly relevant in this context:

- the definition of the scope of the management system (ISO 9001:2015, Section 4),
- the obligation to manage and define roles, responsibilities, and authorities (Section 5),
- risk-based thinking in planning (Section 6),
- operational control and requirements for documented information (Section 8),

[549] ISO 9001:2015, Introduction.
[550] ISO 9001:2015, Annex B.

- as well as monitoring, evaluation, and continuous improvement (sections 9 and 10).

These elements largely correspond in their objectives to the structural requirements set out in Article 17 of the AI Act for quality management of high-risk AI systems, even if they do not explicitly address AI-specific issues such as bias detection or transparency. [551]

The principle of risk-based thinking enshrined in ISO 9001 is particularly important. It requires organizations to identify risks and opportunities that could affect the achievement of the quality management system's objectives and to determine appropriate measures.([552]) This obligation can be used as a methodological basis for embedding AI-specific risks in the quality management system.

c) Strengths and limitations of ISO 9001 in the context of AI-

The main strength of ISO 9001 lies in its universal applicability and established methodology for process design and improvement. This makes it easier to integrate processes for risk assessment and mitigation, as well as documentation and monitoring, into an existing management system.

However, it is also apparent that ISO 9001 does not fully meet the specific requirements of the AI Regulation, particularly with regard to algorithmic risks, data ethics issues, and bias management. Aspects such as human oversight, traceability of algorithmic decisions, and measures to ensure the quality of training data are also not explicitly regulated in the standard.

[551] BeckOK AI Law/Henke, AI Regulation Art. 17 Rn. 7.

[552] ISO 9001:2015, Section 6.1.

[553] ISO 9001:2015, Section 6.1; BeckOK AI Law/Korge, AI Regulation Art. 17 Rn. 7.

It is therefore necessary for providers of high-risk AI systems to either supplement ISO 9001 with appropriate AI-specific guidelines or combine it with standards such as ISO 42001 in order to comprehensively cover the regulatory requirements of Art. 17 AI Regulation.

ISO 9001 can strengthen the overarching management structures and quality awareness within the organization, thereby laying the foundation for the implementation of specialized AI-related requirements. It is therefore an important, but not sufficient, element in a compliance-oriented quality management system in accordance with AI Regulation.

6. ISO 27001:2022 – Information security management

a) Protection of information security as a compliance factor

ISO 27001:2022 is the international standard for information security management systems (ISMS) and provides a structured framework for ensuring the confidentiality, integrity, and availability of information.[554] It thus addresses key compliance requirements that are also of great importance for high-risk AI systems, especially when these rely on sensitive data, such as when processing personal data, health information, or in safety-critical applications.

The management system according to ISO 27001 is also based on a process-oriented approach and follows the PDCA cycle. It contains requirements for risk assessment and treatment, the establishment of security policies, asset management, and protection against threats from internal and external actors. ([555])The standard requires organizations to identify relevant information assets, assess risks, and implement appropriate risk treatment measures.

[554] ISO 27001:2022, Introduction.

[555] ISO 27001:2022, Section 6 ff.

b) Reference to Art. 17 AI Regulation with regard to risk management and documentation

The relevance of ISO 27001 to Article 17 of the AI Regulation stems primarily from two key interfaces: risk management and documentation requirements. Both elements are highly relevant for compliance with the requirements of Article 17 of the AI Regulation. In particular, the AI Regulation's requirement to introduce a management system that identifies, assesses, and appropriately addresses risks corresponds to the risk-based approach of ISO 27001.

The standard requires detailed procedures for identifying information security risks, determining the probability of occurrence and impact of these risks, and selecting appropriate risk mitigation measures.[556]This methodology can also be easily applied to AI-specific risks, such as the manipulation of training data (data poisoning), attacks on models (model inversion, adversarial attacks), or unauthorized access to critical system components.

In addition, ISO 27001 imposes strict requirements on the documentation of all security-related processes. This requirement is consistent with the obligation to provide complete process documentation as stipulated in Article 17 of the AI Regulation for quality and risk management. ([557]) Particularly with regard to the traceability of decisions and the auditability of compliance, this can make a decisive contribution to the implementation of regulatory requirements.

c) Potential additions to ISO 42001 and ISO 9001

The particular strength of ISO 27001 compared to the other two standards considered here lies in its clear focus on information security. While ISO 9001 focuses primarily on product and process quality and ISO 42001

[556] ISO 27001:2022, Section 6 ff.

[557] Art. 17 II letter b AI Regulation.

aimed at AI-specific management processes, ISO 27001 supplements this perspective with the aspect of security architecture.

In conjunction with ISO 42001 and ISO 9001, ISO 27001 can make a particular contribution to comprehensively ensuring compliance with the requirements of the AI Regulation with regard to data quality and data integrity. This applies not only to the protection of training and validation data, but also to ensuring the availability and authenticity of models and outputs during operation.[558]

In addition, ISO 27001 provides a catalog of organizational and technical controls (Annex A) that can be selected and implemented depending on the risk assessment. These include access controls, encryption, logging, incident management, and measures to ensure business continuity.[559]These instruments can also be used within the framework of an integrated management system to meet the requirements of Article 17 of the AI Regulation, in particular where protection against manipulation and misuse of AI systems must be ensured.

Nevertheless, ISO 27001, like the other standards considered, is not a complete substitute for targeted implementation of the AI Regulation. However, it forms a solid foundation for securing the flow of information within AI-supported processes and makes an important contribution to meeting regulatory requirements.

7. Assessment of the combination of standards for compliance with Art. 17 AI Regulation

a) Synergies between ISO 42001, ISO 9001, and ISO 27001

The combination of ISO 42001, ISO 9001, and ISO 27001 provides a comprehensive basis for implementing the requirements of Art. 17 AI Regulation. While ISO 9001 ensures general process quality and ISO 27001 ensures

[558] BeckOK AI Law/Henke, AI Regulation Art. 17 Rn. 8.

[559] ISO 27001:2022, Annex A.

information security aspects, ISO 42001 supplements these perspectives with AI-specific issues such as bias management, impact assessments, and human oversight. [560]These complementary focal points result in an integrated management system that can systematically map both regulatory requirements and ethical and technical requirements.

Particularly noteworthy is the possibility of linking the risk management methodology of ISO 9001 and 27001 with the specific requirements of ISO 42001. [This] makes it possible to record and control classic operational risks, information security risks, and AI-specific risks within a uniform risk management system.

In addition, organizations benefit from the common HLS structure of the three standards, which allows for easier integration of the various management systems. Synergy effects can be achieved through joint internal audits, consolidated management reviews, or integrated documentation systems, for example.

b) Gaps and specific requirements of the AI Regulation

Despite the synergies mentioned above, there are still relevant gaps between the ISO standards and the specific requirements of the AI Act. [In] particular, neither ISO 9001 nor ISO 27001 explicitly address the requirements for bias detection, explainability of algorithmic decisions, or human oversight in the depth required by Art. 17 in conjunction with Art. 9 and Art. 14 of the AI Regulation.

The requirement for systematic review of the data sets used for representativeness and suitability (Article 10 of the AI Regulation) and the obligation to ensure transparency towards users (Article 13 of the AI Regulation) are also not covered by the

560 ISO 42001:2023, Section 6 ff.
561 ISO 9001:2015, Section 6; ISO 27001:2022, Section 6.
562 See ISO 9001:2015, Annex SL.
563 BeckOK AI Law/Henke, AI Regulation Art. 17 Rn. 9.

The standards considered are only inadequately reflected. There is a need for adjustment within the quality and risk management system in order to fully implement the regulatory requirements. [564]

In addition, it should be noted that the AI Regulation itself does not provide for mandatory certification in accordance with ISO standards, but only requires the actual effectiveness of the measures taken. Formal certification can therefore only have an indicative effect and does not replace the independent compliance assessment by the competent authorities, cf. Section 17 (2) AI Regulation.

c) Legal assessment: Is certification sufficient to fulfill the requirements of the German Industrial Security Regulation?

From a legal perspective, the question arises as to whether the introduction and certification of a management system in accordance with ISO 42001, 9001, and 27001 alone is sufficient to meet the requirements of Art. 17 AI Regulation. It should be noted that the regulation requires substantial compliance, the fulfillment of which is measured by the actual effectiveness of the processes. Certification can have a significant indicative effect in the context of compliance defense, but does not automatically exclude liability.

Case law on product safety and compliance in other areas of law suggests that certifications can be regarded as an element of proper organization, provided that they are supported by effective internal processes.[566] The AI Regulation also follows this standard by requiring, in addition to the formal establishment of a quality management system, the concrete minimization of risks and the review thereof.

[564] BeckOK AI Law/Henke, AI Regulation Art. 17 marginal no. 9; see also Art. 10 and Art. 13 AI Regulation.

[565] Art. 17 II AI Regulation.

[566] See BGH NJW 2008, 3770.

The mere implementation of a certified management system without actual risk analysis and effective risk control measures is therefore not sufficient to meet the requirements of the AI Regulation. Rather, the decisive factors are the content of the processes, their effectiveness, and the organization's ability to respond appropriately to new risks or changes to the system.[567]

This means that certification according to ISO 42001, ISO 9001, and ISO 27001 can be an important part of a compliance strategy in the field of AI, but does not completely relieve you of your responsibility for implementing the regulatory requirements. It remains essential to critically examine the specific requirements of the AI Regulation and their practical implementation.

8. CEN/CENELEC JTC21

However, the technical and procedural requirements for the QMS are not specified in the standard text itself, but are linked to harmonized standards within the meaning of Article 40 of the AI Regulation and to so-called common specifications within the meaning of Article 41 of the AI Regulation.

a) Creation of harmonized standards in accordance with Art. 40 AI Regulation

The creation of harmonized standards pursuant to Art. 40 of the AI Regulation is the responsibility of the two European standardization organizations CEN (Comité Européen de Normalisation) and CENELEC (Comité Européen de Normalisation Électrotechnique), whose members include national standardization institutes such as DIN (Germany), AFNOR (France), and BSI (UK, until Brexit).[568] The allocation of responsibility for the development of harmonized standards within the meaning of Art. 40 AI Regulation to the European standardization organizations CEN and CENELEC results strictly from a multi-level interaction of primary law, sector-specific secondary law, and relevant implementing acts of the European Commission.

[567] BeckOK AI Law/Henke, AI Regulation Art. 17 para. 10.

[568] BeckOK AI Law/Kilian, 1st ed. 1.1. 2025, AI Regulation Art. 40 para. 12-15.

The basis for European standardization is Regulation (EU) No. 1025/2012 on European standardization, whereby Art. 2 No. 1 defines: "European standard" means a standard adopted by one of the recognized European standardization organizations: CEN, CENELEC, or ETSI. [569]

"European standard" means a standard adopted by one of the recognized European standardization organizations: CEN, CENELEC, or ETSI. Pursuant to Art. 10 I of Regulation (EU) 1025/2012, the Commission may issue so-called standardization requests to these organizations to develop "harmonized standards" for the purposes of Union harmonization legislation. ([570])

A central body for the development of relevant standards in the field of artificial intelligence is the Joint Technical Committee CEN/CLC JTC 21 with the formal title: [571]

"*Artificial Intelligence – Horizontal aspects*"

This committee was founded in 2021 and is explicitly responsible for developing horizontal standards in the field of AI – i.e., standards that are applicable across industries. The objective is to develop European standards that are consistent and aligned with the AI Regulation, building on the work of the international ISO/IEC committee JTC 1/SC 42. Particularly relevant here are, among others:

- EN ISO/IEC 42001 (AI management systems)
- EN ISO/IEC 23894 (Risk management for AI systems)
- EN ISO/IEC 5338 (AI lifecycle management)

[569] Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of October 25, 2012 on European standardization, OJ L 352, October 26, 2012, p. 1. L 316 of November 14, 2012, pp. 12–33, in particular Art. 2 No. 1 and No. 6 in conjunction with Annex I.

[570] BeckOK KI-Recht/Kilian, 1st ed. 1.1. 2025, AI Regulation Art. 40 para. 12-15.

[571] CEN/CLC JTC 21, Artificial Intelligence – Horizontal aspects, Mandate and work programs, as of May 2025, available at: https://standards.cencenelec.eu.

These standards serve as a reference for the implementation of the requirements of Art. 17 AI Regulation, for example with regard to documentation requirements, audit procedures, role responsibility, and life cycle management processes. [572]

National participation in standardization processes takes place through mirror committees in which representatives from industry, science, and administration are involved (in the case of JTC 21, through the DIN/DKE committee NA 043-04-41 AA). This structure institutionalizes the participation of relevant stakeholders and ensures that national interests and specific technical conditions from a German perspective are effectively incorporated into the European standardization process.

b) Implementation of the requirements of Art. 17 AI Regulation by ISO/IEC 42001, 23894, and 5338

Comment [AB1]: Please check this source reference.

Commented [TS2R1]: Deleted

Currently ISO/IEC 42001, ISO/IEC 23894, and ISO/IEC 5338 are not (yet) recognized as harmonized standards within the meaning of Art. 40 AI Regulation. They therefore cannot trigger a presumption of conformity within the meaning of Art. 40 II AI Regulation.[574] Nevertheless, the question arises as to whether their application is nevertheless suitable in terms of content to meet the requirements of Art. 17 AI Regulation.

c) EN ISO/IEC 42001 – Management systems for artificial intelligence

See the comments in Section IV.4.

[572] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 20.

[573] AI Regulation Recital 77-78 on the role of standardization and QM systems.

[574] BeckOK AI Law/Kilian, 1st ed. 1.1.2025, AI Regulation Art. 40 margin note 12-15.

aa) EN ISO/IEC 23894 – Risk management for AI systems

This standard supplements ISO 42001 with a specific framework for risk management in AI systems and is to be understood as a "vertical extension" of the general risk management standard ISO 31000.575 ISO/IEC 23894 requires, among other things:

- structured risk identification for AI-specific risks,
- Consideration of bias, explainability, and transparency
- documentation and traceability of risk decisions.

It thus fundamentally fulfills the requirements of Art. 17 II a, b, and g of the AI Regulation (risk management procedures, data processing and control, and corrective measures) and specifies the risk management also required by Art. 9 of the AI Regulation.

bb) EN ISO/IEC 5338 – AI lifecycle management

The more recent ISO/IEC 5338[576]is dedicated to the complete lifecycle management of AI systems – from the idea to development and deployment to decommissioning. It systematically defines:

- Phase structure (planning – development – deployment – operation – decommissioning)
- Roles and responsibilities,
- Requirements for interface management, monitoring, and validation.

The standard thus provides a structured, operational interpretation of Art. 17 II (a), (e) and (f) of the AI Regulation by defining organizational processes and responsibilities throughout the entire life cycle. [577]

[575] See ISO TC 262 / JTC 1/SC 42 (AI) – Risk management for AI.

[576] Current status: Draft international standard (DIS, since 2024).

[577] BeckOK AI Law/Henke, AI Regulation Art. 17 para. 15 ff.

Even though this standard is not (yet) considered a harmonized standard, it is suitable for fulfilling the documentation and verification requirements under Art. 17 in conjunction with Art. 11 of the AI Regulation for technical documentation.

G. Summary

The analysis of the requirements of Art. 17 AI Regulation and their possible implementation via the ISO 42001, ISO 9001, and ISO 27001 standards clearly shows that an integrated management system can make a significant contribution to compliance with regulatory obligations. The ISO standards mentioned above serve as structuring instruments that enable risk management, quality management, and information security to be systematically organized and documented.

With its specific focus on AI, ISO 42001 in particular offers a practical framework for operationalizing the special requirements of the AI Regulation, such as bias management, transparency, and human oversight. In combination with the process-oriented structures of ISO 9001 and the security architectures of ISO 27001, this provides a robust foundation for compliance-oriented management of high-risk AI systems.

Nevertheless, there are still regulatory gaps that cannot be closed by the standards alone. In addition to structural requirements, the AI Regulation also sets content standards, for example with regard to the quality and suitability of training data, the guarantee of human control, and the prevention of systematic discrimination. These aspects require in-depth consideration that goes beyond what the ISO standards under review can directly achieve. The mere existence of a certified management system is not sufficient to ensure compliance. Rather, the actual effectiveness of the measures taken and their continuous review are decisive.

Against this backdrop, it seems sensible to supplement the existing ISO standards with industry-specific guidelines and sector-specific standards

that specify the regulatory requirements of the AI Regulation and translate them into operational practice in the sense of AI governance. Further development of ISO 42001 to align it more closely with the requirements of the AI Regulation could also contribute to further harmonization.

In the future, the question will also arise as to whether European or national authorities will officially recognize certification according to ISO 42001, ISO 9001, or ISO 27001 as part of the conformity assessment within the meaning of the AI Regulation. Such a development could both increase legal certainty for providers and facilitate regulatory control.

Art. 17 AI Regulation also has practical effect in conjunction with Art. 40 and 41 AI Regulation and the European standardization structure based on them. The detailed technical requirements for the QMS of providers of high-risk AI systems are essentially formulated by CEN/CLC JTC 21 and transposed into German standardization law by DIN. The resulting standards (e.g., DIN EN ISO/IEC 42001) effectively represent the relevant benchmark for regulatory compliance. Companies that adhere to these standards can rely on a legally recognized presumption of conformity.

This illustrates the inseparability of legal and technical regulation in the field of AI governance: The legislator sets out the guidelines in Article 17 of the AI Regulation – the technical details are worked out by European and national standardization bodies, whose work is effectively binding on legal practitioners.

In conclusion, it can be said that linking quality management, risk management, and information security in light of the AI Regulation must be a central component of an effective compliance strategy. The use of existing ISO standards offers a proven set of tools for this purpose, but these must be critically reviewed and adapted to the specific requirements of the AI Regulation. This is the only way to ensure that AI systems not only formally, but

substantively meet the requirements for security, trustworthiness, and legal compliance.

V. AI- Governance

AI governance in the context of the AI Regulation (AI VO) covers a wide range of legal aspects that regulate the introduction and application of AI systems. The AI Regulation sets out specific requirements aimed at transparency, risk management, and accountability. The following section outlines the key legal aspects of AI governance, followed by a discussion of practical implementation in a governance tool.

1. Responsibility and accountability

A key element of AI governance under the AI Act is the clear allocation of responsibilities. According to Article 28 of the AI Act, providers of high-risk AI systems are required to ensure that their systems comply with the provisions of the Regulation. Those responsible are expected to monitor the implementation of and compliance with the provisions and to take measures to prevent or correct any infringements. This principle of accountability requires those responsible to be able to report on the development, operation, and monitoring of AI systems (Article 18 of the AI Regulation).

The governance of an AI system must therefore include a comprehensive compliance system that is capable of ensuring compliance with the regulation throughout the entire life cycle of the AI. Governance mechanisms should therefore also clearly define responsibilities and roles, particularly for sensitive decisions such as risk assessment and the rectification of infringements.

2. Transparency and documentation requirements

The AI Act sets high standards for the transparency of AI systems. Article 13(1) of the AI Act stipulates that high-risk AI systems must be designed in such a way that their users are informed about their functioning and potential risks. This includes the obligation to produce technical documentation containing detailed information about the functioning and structure of the AI system.

contained (Art. 18 AI Regulation). This documentation requirement enables better verifiability of the systems and ensures that relevant information can also be made available to supervisory authorities if necessary.

The governance of an AI system must therefore include a structured documentation and risk management system that ensures that all essential aspects of the system are traceable and verifiable.

3. Risk and security management

Another key requirement of the AI Act concerns risk and safety management. Article 9(1) and (2) of the AI Act require providers to continuously monitor high-risk AI systems and check them for possible new risks. Appropriate risk mitigation measures must be taken to ensure that the system does not cause any potential harm. An escalation process must also be defined to enable a rapid response to newly identified risks.

As part of AI governance, a system must therefore be implemented that regularly and systematically performs risk monitoring and safety assessments. This includes reviewing algorithms, data, and models to identify potential new risks at an early stage.

4. Establishment of ethics and integrity standards

In addition to technical and regulatory requirements, providers of AI systems must also establish ethical and integrity-related standards derived from the fundamental values of the EU and the AI Act. The regulation emphasizes that AI systems must comply with fundamental rights and ethical principles to ensure responsible and fair use of the technology (Recital 40 AI Regulation). This requires the establishment of a governance system that monitors compliance with ethical standards and ensures that AI systems are operated in a non-discriminatory manner and in accordance with European values.

5. Implementation in the governance tool

A governance tool for compliance with the AI Regulation should offer specific functionalities to ensure compliance with the requirements described above:

- **Responsibility management**: The tool should clearly document and assign roles and responsibilities. It must make it clear who is responsible for which aspects of the AI system and what measures will be taken in the event of a violation or risk. Integrated escalation management can be helpful here to enable a quick response.

- **Documentation and transparency module**: To meet transparency and documentation requirements, the governance tool must be able to provide technical and legal documentation and store it in an audit-proof manner. Users should also be able to access documentation explaining how the AI system works and the potential risks involved.

- **Risk management functionalities**: A governance tool should include a module for risk and security management that enables regular assessments and audits of the system. It should identify, evaluate, and document potential risks at an early stage and offer the possibility of implementing security measures and monitoring their effectiveness.

- **Ethics and integrity monitoring**: A comprehensive governance tool must also provide mechanisms for monitoring ethical standards. This can include checklists for ethical reviews and guidelines to ensure compliance with fundamental rights. Automatic notifications could be triggered when certain ethical or discrimination indicators are exceeded.

A good AI governance tool in accordance with the AI Act not only ensures compliance with regulatory requirements, but also promotes the responsible and ethical use of AI systems by integrating transparency, accountability, and risk management.

VI. Criticism[578]

1. Complexity and legal uncertainty

The AI Regulation introduces a classification of AI systems according to risk levels, which allows for differentiated regulation but also entails considerable complexity and associated legal uncertainty. Legal actors have expressed concerns about the criteria for distinguishing between the individual risk categories. There are fears that the vague definition of key terms and the broad interpretation of what constitutes an "AI system" will lead to room for interpretation that could undermine legal certainty. These ambiguities could lead to significant compliance challenges for developers and providers of AI systems, especially for SMEs and smaller start-ups.

2. Administrative burdens and costs

Another critical issue concerns the administrative burdens and associated costs, again particularly for SMEs. Compliance with the extensive documentation, reporting, and risk management requirements, which apply primarily to high-risk AI systems, could place a significant burden on SMEs. The requirements could not only place a direct financial burden on them, but also indirectly influence resource allocation by forcing companies to spend considerable funds on compliance measures instead of investing in innovation and development.

3. Impact on innovation capacity

Criticism also extends to the potential impact of the AI Regulation on the ability to innovate within the European Union. While the regulation's goal of ensuring a high level of protection for citizens and society is widely supported, critics warn that excessive regulation could hinder innovation. There is concern that the strict requirements, especially for high-risk AI systems, will slow down the development and introduction of new

[578] *Adoption of the European AI Regulation – Presentation of key points of the AI Regulation and criticism* Söbbing, ITRB 2024, 108–111.

Technologies could slow down. This could impair the competitiveness of European companies on the global market, especially in comparison with players in less regulated jurisdictions.

4. Bureaucratic hurdles and enforcement issues

Finally, the practical enforceability of the regulation is critically questioned. Effective monitoring and enforcement of the diverse and complex requirements of the AI Regulation poses a considerable challenge. The need for a strong and coordinated supervisory structure at EU level that is capable of effectively monitoring compliance and penalizing violations raises questions regarding the necessary resources and bureaucratic burden. In addition, there is a risk that the multitude of requirements and the complexity of the subject matter could lead to fragmentation in enforcement practices, which in turn would jeopardize legal certainty and equal treatment of market participants.

5. Conclusion

The European Union's AI Regulation represents an ambitious attempt to comprehensively address the challenges and risks of AI technology. While the intention to ensure a high level of protection for society while promoting innovation is welcome, the points of criticism outlined above raise fundamental questions regarding practical implementability, excessive bureaucracy, the efficiency of the legal framework, and the long-term impact on the EU's ability to innovate, which would be detrimental to the economy and workers. Ongoing evaluation and, if necessary, adaptation of the regulation therefore appear essential to ensure the balance between protection and innovation in a rapidly evolving technological environment.

G. Autonomous driving[579]

An autonomous vehicle is defined as a vehicle that navigates freely (i.e., without human assistance).[580] In this case, the car (as AI/robot) autonomously decides how to adapt its driving behavior (steering, speed, etc.) to the environment.[581] Robots perceive their environment using sensors and react according to their programming. A certain ability to learn, which leads to an expansion of possibilities, is certainly not excluded, but rather desirable. Robotics deals with what is known as manipulative intelligence: with the help of robots, dangerous activities or repetitive tasks, such as defusing bombs, can be transferred to robots. The basic idea is to create systems (robots) that can replicate the intelligent behavior of living beings.

I. Degrees of automation

The Federal Highway Research Institute (BASt), which is a practice-oriented, technical-scientific research institution that provides decision-making support to the Federal Ministry of Transport and Digital Infrastructure (BMVI) on technical and transport policy issues[582], has set up a project group to identify and define the different levels of automation.[583] The result of this project group is the presentation of different levels for autonomous driving:

1. Level 0 – Driver only

The BASt classification of automation levels begins with "Level 0 – Driver On y," which, according to the wording, does not represent any automation at all. At Level 0, the driver is in control at all times, i.e., during

[579] Legal limits for AI decisions in the context of autonomous driving Söbbing, RDi 2023, 239

[580] *Hägele/Schäfer*, in: Gevatter/Grünhaupt (eds.), Handbook of Measurement and Automation Technology in Production, 2006.

[581] *Kirsch,* CT Magazine for Computer Technology No. 22, 2011, 43.

[582] https://www.bast.de/DE/BASt/BASt_node.html;jsessionid=905ABC3FD1F06FA5F8CD8E1F99925695.live2051 (last accessed on January 24, 2016).

[583] BASt, Legal consequences of increasing vehicle automation, 2012, p. 8.

the entire journey, the longitudinal and lateral control of the vehicle independently. [584] Longitudinal control specifically refers to the acceleration and deceleration of the vehicle. Lateral control, on the other hand, refers solely to the steering process itself. From a practical point of view, Level 0 systems are therefore understood to mean conventional driving without any assistance with longitudinal and/or lateral control, so that the driver is solely responsible for mastering the driving task ("driver only"). [584] Level 1 Assisted driving

2. Level 1 – Assisted

Automation level "Level 1 – Assisted" is defined by the fact that the driver continuously performs either lateral or longitudinal control. The other driving task is performed by the vehicle system within certain limits. [586] The decisive factor at this level of automation is that the driver must continuously monitor the vehicle system and be ready to take over control of the vehicle at any time.[587] This means that, as in Level 0, the driver remains fully responsible for driving at all times in Level 1. Level 1 systems have been available on the market for some time and are becoming increasingly popular, particularly in mid-range vehicles. Examples of Level 1 vehicle systems include adaptive cruise control and parking assistants. The Adaptive Cruise Control (ACC) system is an example of system-based support for longitudinal control of the vehicle. ACC is an automatic distance control system that keeps the speed and distance to the vehicle in front as constant as possible by accelerating and decelerating independently. In contrast, a parking assistant system automatically steers the vehicle into parking spaces (lateral guidance), while the driver remains fully responsible for accelerating and decelerating (longitudinal guidance) by applying the accelerator and brakes. In summary, it can be said that Level 1 automation systems represent the first

584 BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.
585 *Buchberger*, ITRB 2014, 116, 117.
586 BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.
587 BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.

step toward an automated future. Nevertheless, such systems only support and relieve the driver in one of the two necessary driving tasks. Even at this level of automation, the system cannot completely and independently take over either of the two driving tasks due to the driver's need for constant monitoring and readiness to intervene.

3. Level 2 – Partially automated

The obligation to monitor the vehicle continuously and to be ready to take control of the vehicle at any time and without delay applies to the driver in both "Level 2 – Partially automated" and Level 1 automation. However, the main difference between Level 1 and Level 2 systems is that in partially automated driving, the system takes over both lateral and longitudinal control for a certain period of time and/or in specific situations.[588] The main task of the driver in such systems is primarily to monitor and, if necessary, override the partially automated system. This is particularly important when the system limits are reached, in the event of a fault, and when leaving the specific area of application. [589] Against this background, it is essential for the safe use of partially automated systems that the driver constantly monitors the system and, being aware of all system limits and his or her personal abilities, recognizes when a correction of the system is necessary.[590] For the reasons stated above, it is not possible under any circumstances for the driver to be relieved of the task of driving and the associated responsibility, even temporarily, in the case of Level 2 functions. The partially automated system therefore only relieves the driver of active control until the vehicle must be taken back under control. [591] In addition to automatic distance control ACC (see "Level 1 – assisted"), this function assists with steering at speeds between 0 and approx. 65 km/h. It does this by steering the car.

[588] BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.

[589] BASt, Legal consequences of increasing vehicle automation, 2012, p. 11.

[590] BASt, Legal consequences of increasing vehicle automation, 2012, p. 11.

[591] BASt, Legal consequences of increasing vehicle automation, 2012, p. 12.

through gentle steering interventions and follows the vehicle in front within the respective system limits. Semi-automated systems thus support and relieve the driver in performing driving tasks in both control areas (longitudinal and lateral control) and therefore offer a higher range of functions and degree of automation than Level 1 functions.

4. Level 3 – Highly automated driving

In highly automated driving at Level 3, as in semi-automated driving at Level 2, the system takes over longitudinal and lateral control for a certain period of time in specific situations (such as driving in a traffic jam on the highway). Of fundamental importance for Level 3 systems, and crucial in the further development of this document, is the fact that the driver no longer has to monitor the system continuously and is prompted by the system to take over the driving task with sufficient time reserve when necessary.[592] Due to this time reserve, the highly automated system must recognize all system limits itself and inform the driver accordingly when system limits are reached. This time reserve provided by the system also means that the driver is no longer occupied with the driving task during automated driving, thus providing a new level of relief for the driver. Highly automated systems are not yet available on the market, but are in near-series development at the German premium manufacturer Audi, among others, in the form of the "traffic jam pilot." [593] As with semi-automated driving, the driver is to be relieved of monotonous and boring driving situations, thereby preventing accidents or at least mitigating their consequences.[594] Since the highly automated system recognizes all system limits in good time but is not always able to independently establish the risk-minimizing state in these situations, the presence of a driver capable of taking over is necessary at all times. [595]

[592] BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.

[593] http://blog.audi.de/2015/05/26/per-autopilot-durch-die-megacity-shanghai/ (last accessed on January 24, 2016).

[594] BASt, Legal consequences of increasing vehicle automation, 2012, p. 38.

[595] BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.

5. Level 4 – Fully automated

By increasing system performance in fully automated driving (Level 4), such systems, unlike Level 3 systems, also ensure that the system can automatically return to a safe state if the driver fails to take over the driving task.[596] When the vehicle is stationary, the transition to the risk-minimized state is achieved by preventing automated restarting. When the vehicle is in motion, the risk-minimized state is achieved by moderate deceleration to a standstill, including activation of the hazard warning lights and the electric parking brake. [597]Unlike highly automated driving, a fully automated system can, if the traffic situation and the system status permit, steer the vehicle onto the hard shoulder by changing lanes once or several times and bring it to a standstill there. [598] Otherwise, however, the technical characteristics of automation levels 3 and 4 are largely the same.

II. Behavioral regulations

Most legal issues currently revolve around the behavioral regulations of automated driving. On the one hand, this raises the question of whether the increasing technical relief and reduction of behavioral requirements for vehicle drivers as automation increases can be reconciled with applicable law or whether there is a need for legislative action. [599]

1. Vienna Convention on Road Traffic

The general basis for national regulations on road traffic is provided by

[596] BASt, Legal consequences of increasing vehicle automation, 2012, 12.

[597] BASt, Legal consequences of increasing vehicle automation, 2012, p. 39.

[598] BASt, Legal consequences of increasing vehicle automation, 2012, p. 39.

[599] *Buchberger*, ITRB 2014, 116, 117.

the Vienna Convention on Road Traffic of 1968 [600](hereinafter referred to as the "WÜ"). The Convention is an international treaty that was necessary due to the sharp increase in cross-border traffic. The signing and ratification of the WÜ led to the international harmonization of road traffic law, in particular the rules of conduct and traffic signs. [601] The WÜ was concluded in Vienna on November 8, 1968, and currently includes 73 participating nations. [602]

Through the WÜ, the contracting states undertake to incorporate the provisions contained in the treaty into their national road traffic regulations. Furthermore, these provisions are a prerequisite for admission to international traffic, cf. Art. 3(3) WÜ. Art. 8 and Art. 13 WÜ stipulate that the vehicle must be constantly controlled and "continuously" "controlled" by the driver. These provisions become problematic in the case of driver assistance systems (AI systems) that technically relieve the driver of control of the vehicle. [603] If, for example, the driver assistance system independently initiates braking that the driver cannot override, this does not fulfill the requirement of the WÜ, as the driver is not given any alternative course of action.[604] This driver control and monitoring obligation was discussed and further developed and adapted in March 2014 at the 68th meeting of the Working Party on Road Traffic Safety (WP.1) in Geneva. The amendment provides that the corresponding obligation is also fulfilled as long as the driver assistance systems can be influenced by the driver ("designed to be overridable or switchable").[605] The amendment has now been accepted by the contracting states without any dissenting votes.[606]

a) European approval law – ECE Regulations

600 Printed in BGBl. II, 1977, p. 811 ff.

601 *Frenz/van den Broek*, NZV 2009, 530; BT-Drs. 8/178, p. 308 ff.

602 A comprehensive list of the participating contracting states is available at http://www.unece.org/trans/conventn/legalinst_08_RTRSS_RT1968.html (last accessed on January 24, 2016).

603 *Albrecht*, VD 06/2006, 143, 144.

604 *Gasser*, VKU 2009, 224.

605 *Buchberger*, ITRB 2014, 116, 117.

606 https://treaties.un.org/doc/Publication/CN/2015/CN.529.2015.Reissued.06102015-Eng.pdf (as of February 5, 2016).

In addition to the WÜ, there is the ECE Agreement of 1958, on the basis of which binding rules (known as ECE regulations) were also established with regard to the technical approval of vehicles. In Germany, vehicles are now approved in accordance with European law (Directive 2007/46/EC). This directive refers to the ECE regulations in Annex IV. These regulations are also regularly adapted to technical progress by the UN-ECE[607], but much more quickly than in the WÜ. This unequal treatment in terms of adaptation leads to increased costs for the member states and thus to unnecessary obstacles to technical progress. For this reason, a solution was also found on this point in the amendments to WP.1, whereby Art. 39(1) sentence 3 WÜ was added and compliance with the technical requirements is made subject to the ECE regulations. [608]

b) StVO

The reform of the Road Traffic Regulations (StVO) aimed to increase road safety. This also included regulations on rules of conduct for accident prevention. [609] The legal basis and protective purpose of the StVO are derived from the Road Traffic Act (Sections 6 (1) No. 3, 4a, 5a 13 ff. StVG). The aim is to maintain order and safety in public spaces, i.e., to maintain general traffic safety and the safety of individuals (here within the meaning of § 823 para. 2 BGB).[610] The WÜ is the higher-ranking law and serves as the basis for the applicable road traffic regulations (StVO) in Germany. As a result, the current version of the StVO also contains the passage on the "permanent controllability" of the vehicle by the driver. [611]

AI technologies in vehicles that correspond to Level 2 are so-called partially automated functions which, when activated, take over longitudinal and lateral control for the driver. A diversion from the driving task is not permitted.

---

607 Sub-organization of the UN tasked with developing technical requirements for vehicles, which are then adopted on the basis of international law. These are intended to standardize the requirements between individual countries. Further information on the UN-ECE can be found at: https://www.unece.org/leginstr/cover.html (last accessed on December 29, 2015).

608 *Lutz*, DAR 8/2014, 446, 448.

609 VkBl 1970, 797, 798 f. Statement by the Federal Minister of Transport on the Road Traffic Regulations.

610 *Gasser*, VKU 2009, 224.

611 *Buchberger*, ITRB 2014, 116, 117.

Vehicle drivers are not permitted to use partially automated systems. [612] The driver may be requested by the vehicle's AI system to take control of the vehicle at any time. Against this background, the driver's behavioral requirement during partially automated driving is to monitor the system continuously and be ready to take full control of the vehicle at any time. This means that when a partially automated system is in active operation, the driver, as a human being, is still the person who indirectly keeps the vehicle in motion at all times. The driver is not replaced by the partially automated system, so that the driver continues to bear overall responsibility for setting the vehicle in motion and keeping it moving.[613] Consequently, the driver must continuously monitor that he is driving at a speed that allows him to maintain control of the vehicle at all times in accordance with Section 3 (1) sentence 1 StVO. A similar rule applies to the distance to another vehicle. According to § 4 (1) StVO, the driver must maintain a distance from the vehicle in front that is sufficient to be able to stop behind it if it brakes suddenly. Thus, the requirement to maintain a sufficient distance is also based on the behavioral requirement of controlling the vehicle. In general, according to

§ 1 (2) StVO (German Road Traffic Regulations) to behave in such a way that no other person is harmed, endangered, or hindered or inconvenienced more than is avoidable under the circumstances. This applies without change due to the driver's permanent monitoring obligation in the case of semi-automated systems, meaning that the driver may have to intervene in certain circumstances.

In AI systems in vehicles at level 3 the highly automated system not only takes over the longitudinal and lateral control of the vehicle [614] but also gives the driver freedom in automated mode in that they no longer have to monitor the system continuously and are prompted by the system to take over the driving task with sufficient time reserve if necessary. Due to the aforementioned freedom and the lack of necessity for the driver to monitor the driving situation, it is fundamentally doubtful whether the driver

612 BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.

613 *Buchberger*, ITRB 2014, 116, 117.

614 BASt, Legal consequences of increasing vehicle automation, 2012, Table 2-1, p. 9.

can still be described as such in terms of the behavioral requirements of the StVO. A vehicle is driven by anyone who "sets it in motion under their sole or shared responsibility by using its driving forces as intended and controls it, by operating its technical devices, while it is moving in public traffic, either wholly or at least in part." In highly automated driving, however, the "driver" permanently lacks the ability to control the vehicle, at least in part. When highly automated driving is activated, the "driver" is released from the essential behavioral requirements of the StVO, as these are independently performed and fulfilled by the vehicle and no longer by the human driver. [615]

2. Requirements under the StVG

Notwithstanding the "normal" civil liability provisions in Chapter L. "Liability," autonomous driving may give rise to additional liability.

a) Driver liability according to Section 18 of the German Road Traffic Act (StVG)

As the party responsible for the disruptive behavior, the driver of the vehicle is initially the focus of liability. For the driver, whether with or without an assistance system, driver liability is governed by Section 18 of the German Road Traffic Act (StVG). The driver is liable under Section 18 StVG in the event of a personally attributable breach of duty of care, whereby, according to Section 18 (1) sentence 2 StVG, fault is generally presumed and the driver bears the burden of proof with regard to any exonerating evidence.[616] The driver can provide such exonerating evidence above all if he can prove that the accident was due to a technical fault in the vehicle (e.g., brake failure) or if the driver behaved in accordance with the rules of the road in the respective traffic situation. [617]

In the event of a defect, the manufacturer is liable. If the other party involved in the accident has violated traffic regulations, they are naturally liable. This is because, although the vehicle performs lateral and longitudinal control during semi-automated driving, permanent monitoring and the associated responsibility for

, they are naturally liable. This is because, although the vehicle performs lateral and longitudinal guidance during semi-automated driving, permanent monitoring and the associated.

615 *Buchberger*, ITRB 2014, 116, 117.

616 *Berz/Dedy/Granich*, DAR 2002, 545.

617 *Buchberger*, ITRB 2014, 116, 117.

However, if the immediate intervention task is incumbent on the driver, the driver is generally at fault in the event of damage. The decisive factor here is that the driver is not released from his duty of care during semi-automated driving. However, this does not mean that he is denied the exonerating evidence provided for in Section 18 (1) sentence 2 StVG in individual cases. Rather, this possibility remains, so that in principle no qualitative difference can be established between manual or assisted driving and semi-automated operation.

b) Liability of the keeper under Section 7 StVG

According to § 7 StVG, the owner is liable to pay damages to an injured party if "the operation of a motor vehicle or trailer results in the death of a person, injury to the body or health of a person, or damage to property." In the event of an accident, the owner is subject to strict liability, i.e., the owner is liable for the operation of his vehicle without any fault on his part. [618] In principle, strict liability serves the purpose of responding to the effects of dangers or compensating for them.[619] Holder liability therefore does not justify compensation for wrongful conduct, but rather for damage caused by the operation of a vehicle. [620] The holder is therefore liable for the danger that arises from the creation of a source of danger.[621] The keeper of a vehicle is the person who uses their own motor vehicle for their own account and has power of disposal over it. Keeper does not therefore also mean owner (see leasing). The actual relationship of control is decisive in determining control; for example, in leasing agreements, the keeper and the owner are usually different, and despite the leasing agreement, the keeper is liable even if he is not the owner of the vehicle, as is consistent with the nature of vicarious liability.[622] Section 1 (2) StVG covers all vehicles that are powered by mechanical force. It should be noted that Section 7 (1) StVG does not apply

618 *Berz/Dedy/Granich*, DAR 2002, 545.

619 *Deutsch/Ahrens*, Deliktsrecht (Tort Law), 6th edition, 2014, margin number 7

620 *Kuhnert,* in: Haus/Krumm/Quarch, Gesamtes Verkehrsrecht (Complete Traffic Law), 2nd edition, 2017, Section 7 StVG margin number 4.

621 *Berz/Dedy/Granich*, DAR 2002, 545.

622 *Berz/Dedy/Granich*, DAR 2002, 545.

if § 8 No. 1 StVG applies, i.e., an accident is caused by a motor vehicle that cannot travel faster than 20 km/h. Further exceptions are regulated in § 8 Nos. 2 and 3 StVG.

According to § 7 StVG, the damage must have occurred while the vehicle was in operation. This is always assumed to be the case if the vehicle was in motion in a public traffic area. [623] The term "public traffic area" is interpreted very broadly and, according to § 7 (1) StVG, applies if the vehicle is stationary in a manner that affects traffic, for example, if it is parked.[624] In addition the typical operational risk must have materialized. This means that there must be a causal link between the operation of the vehicle and the occurrence of [625] the damage in terms of location and time, and that the specific risk caused by the vehicle must have materialized. If a driver assistance system is used and damage occurs in a traffic accident, the damage did not occur due to unlikely circumstances, but it could reasonably be assumed that an assistance system could cause damage if it malfunctioned or was operated incorrectly.[626] The owner's liability includes culpable misconduct on the part of the driver as well as malfunctions of assistance systems. This also includes actively intervening systems, even if they cannot be overridden. This liability is justified by the fact that the vehicle owner must assume responsibility for the respective operational risk of the vehicle he has put into traffic. [627] Liability is assumed for all damage caused by defects in the condition of the vehicle. In the case of driver assistance systems, the owner is therefore generally liable for damages if these systems malfunction or if errors occur in the handling of properly functioning driver assistance systems. [628] It is questionable to what extent the manufacturer is then liable and whether the driver can claim compensation from the manufacturer.

[623] *Kuhnert,* in: Haus/Krumm/Quarch, Gesamtes Verkehrsrecht (Comprehensive Traffic Law), 2nd edition, 2017, Section 7 StVG, margin number 4.

[624] *Gasser*, VKU 2009, 224, 228.

[625] Federal Court of Justice, NJW 1975, 1886.

[626] *Berz/Dedy/Granich*, DAR 2002, 545.

[627] *Gasser*, VKU 2009, 224, 228.

[628] *Walter*, SVR 2006, 41, 69.

c) Limits of liability

In principle, the statutory limitation of liability under the StVO must also be taken into account when using AI systems in vehicles. According to Section 12 StVG, the driver is liable as the owner for personal injury up to five million euros and for property damage up to one million euros. Further liability for compensation is regulated in Sections 10, 11, and 13 StVG.

A disclaimer of liability that could arise from force majeure must also be taken into account. In cases of force majeure, only elementary natural forces or actions of third parties can be considered grounds for exclusion of liability. These must be unforeseeable and unavoidable according to human understanding and experience. Driving errors by others or pedestrians or children suddenly running onto the road do not fall under force majeure.

In the case of the operation and use of partially automated systems, any other legal assessment will not be convincing. With Level 0 or 1 systems, as with Level 2 functions, the vehicle owner creates a source of danger through the motor vehicle, which becomes a reality in the event of an actual accident. Furthermore, it can be argued that vehicles with such systems are not permanently in activated Level 2 mode, but are used for the vast majority of their operating time in manual or assisted mode.[630] Against this background, it should be noted that the allocation of operational risk to the vehicle owner and the associated liability under Section 7 StVG is also logical and consistent in partially automated operation. [631]

d) Motor vehicles with highly or fully automated driving functions, Section 1a StVG

In 2017[632] politicians responded to the demands of industry with the newly created Sections 1a and 1b StVG and introduced legal regulations on highly and

[629] *Walter*, SVR 2006, 41, 69.

[630] *Buchberger*, ITRB 2014, 116, 117.

[631] BASt, Legal consequences of increasing vehicle automation, 2012, p. 18 f.

[632] Printed paper 69/17 dated January 27, 2017.

fully automated driving functions. The driver may leave control of the vehicle to the computer in certain situations and depending on the system.

According to Section 1a (1) StVG, the operation of a motor vehicle by means of highly or fully automated driving functions is permitted if the function is used as intended. Motor vehicles with highly or fully automated driving functions within the meaning of the StVG are those that have technical equipment in accordance with Section 1a (2) StVG

- that can control the respective motor vehicle after activation (vehicle control) in order to perform the driving task, including longitudinal and lateral control.

- which is capable of complying with traffic regulations applicable to vehicle guidance during highly or fully automated vehicle control,

- which can be manually overridden or deactivated by the driver at any time,

- that can recognize the need for the driver to control the vehicle manually,

- that can indicate to the vehicle driver the need for manual vehicle control with sufficient time reserve before handing over vehicle control to the vehicle driver in a visual, acoustic, tactile, or other perceptible manner, and

- which indicates any use that is contrary to the system description.

The operation of a motor vehicle using highly automated or partially automated driving functions is only permitted under Section 1a (1) of the Road Traffic Act (StVG) if the function is used as intended. The conditions under which the system may be used must be specified by the manufacturer. [633] If the driver does not comply with these conditions, the vehicle's system must inform the driver of this, cf. Section 1a II 1 No. 6 StVG, and the driver is responsible for

[633] *Greger*, NZV 2018, 1 ff.

Liability for an accident caused by this. This applies not only if the driver has ignored a warning from the system, but also, according to Section 1b II No. 2 of the German Road Traffic Act (StVG), if the driver should have recognized on their own that the conditions for proper use were obviously no longer met. The driver must familiarize themselves with the manufacturer's instructions.[634] If damage occurs (traffic accident) because the driver has intervened in the automatic control function, the driver must demonstrate and prove that this was in accordance with the care required in traffic or that the accident would have occurred even without the intervention. In practice, this is certainly only possible with an expert opinion, which presents new challenges. If the driver has taken back control of the vehicle on his own initiative or at the request of the system, he must prove that he acted in accordance with traffic regulations. In this case, the dangerous situation at the time of taking over the control function is decisive. He is therefore not liable, for example, for hitting a pedestrian if it can be proven that this would have been unavoidable if he had continued to observe the traffic situation but not if he had taken control of the vehicle.[635] If the driver had not intervened immediately in accordance with Section 1b (2) No. 1 in conjunction with Section 1a (2) No. 5 StVG, even though he had been prompted to do so by the system, he must prove that the accident would not have been prevented even if he had intervened. It follows from Section 1b (1) StVG that the driver must also be prepared to intervene immediately "at any time." The permissible diversion of attention from the control of the vehicle must therefore not go so far as to prevent the driver from immediately taking control of the vehicle in response to the corresponding warning signal in accordance with the traffic situation. "Immediately" means, according to general understanding (see
§ 121 (1) No. 1 BGB) compensation for accelerated, non-culpable delayed action to be assessed according to the circumstances of the case.
and not unreasonably delayed action. [636] The driver must respond to the system's request as quickly as reasonably possible in the specific situation. Unlike in the case of declarations of intent, he cannot be granted any time for consideration or reflection here. [637] Since he must be prepared to take control "at any time."

634 *Grünvogel*, MDR 2017, 973, 974.

635 *Greger*, NZV 2018, 1 ff.

636 Federal Administrative Court, NJW 1989, 52, 53. See also the Federal Government in BT-Drs. 18/11534, 15; *König*, NZV 2017, 123, 125.

637 Federal Court of Justice, NJW 2008, 985, 986.

A reaction must be expected within a few seconds,[638] because only then can the warning issued by the system, which signals an acute danger despite the lead time prescribed in Section 1a (2) No. 5 StVG, fulfill its purpose. If the driver is unable to react quickly enough, they are at fault for an accident that could have been avoided without the time delay. This is particularly the case if the driver has left the driver's seat or reclined the seat, or if they are engaged in an activity that they cannot stop immediately.[639] The big debate about the future of autonomous driving will be at what point the driver should have taken control from the system. In principle, the driver must take control of the vehicle after he has recognized or, based on obvious circumstances, should have recognized that the conditions for the intended use of the automated driving functions are no longer met (Section 1b (2) No. 2 StVG). This is because the driver may only divert their attention from the traffic and the control of the vehicle to the extent that they can fulfill this duty at all times (Section 1b (1) StVG). How this is to be assessed in individual cases can only be determined by an expert; the law merely states that "must have recognized" means negligent failure to recognize (Section 122 (2) BGB). Only the characteristic

"Due to obvious circumstances," the general concept of negligence is modified: The driver is at fault if, despite obvious circumstances, he or she has not recognized that the automatic driving function can no longer be used as intended. [640]

Section 1a (3) StVG clarifies that vehicles equipped with highly or fully automated driving functions, like all other vehicles, also require an operating license, individual approval, or type approval. These approvals are only granted if the necessary technical requirements are met. It is also clarified that motor vehicles with EC type approval in accordance with Art. 20 of Directive 2007/46/EC may still be used in traffic even if

638 The Federal Council has recommended a reaction time of 1.5 to 2 seconds plus a safety margin; BT-Drs. 18/11534, p. 4.

639 *Greger*, NZV 2018, 1 ff.

640 *Greger*, NZV 2018, 1 ff.

There is no UN-ECE regulation (international regulation) on automated driving functions.

According to Section 1a (4) StVG, the driver is also the person who activates an automated driving function and uses it to control the vehicle, even if they are not personally controlling the vehicle within the scope of the intended use of this function. Even completely turning away from the traffic, or even leaving the driver's seat, would not relieve him of his status as driver. He is therefore liable to any accident victim under Section 18 StVG without the latter having to prove that he was at fault. In order to be released from this liability, he must prove that he was not at fault for the accident (Section 18 (1) No. 2 StVG), for example because he manually overrode the system in a manner contrary to traffic regulations or did not resume control of the vehicle contrary to Section 1b (2) StVG. The condition of the system at the time of the accident can be determined on the basis of the data stored in accordance with Section 63a StVG. In order to be able to provide exonerating evidence, the driver may demand that the owner arrange for the data necessary to defend against liability to be transmitted to him (Section 63a (3) StVG).The same authority shall be granted to the liability insurer on the basis of its regulatory authority and, in order to defend against the objection of contributory negligence, also to the injured party. Details of data storage shall be regulated in the ordinance pursuant to Section 63b StVG. [641]

e) Rights & obligations when using highly/fully automated driving functions, Section 1b StVG

In the government draft [642] of the Road Traffic Act, in addition to the requirements for motor vehicles with highly and fully automated driving functions, the obligations of the vehicle driver pursuant to Section 1b (2) StVG were highlighted in particular. The newly inserted Section 1b (1) StVG clarifies the right of the vehicle driver to turn their attention away from traffic and vehicle control while the highly and fully automated driving function is active. Within the scope of the system description, the vehicle driver may take their hands off the

641 *Greger*, NZV 2018, 1 ff.

642 Printed paper 69/17 dated January 27, 2017.

Take your hands off the steering wheel, take your eyes off the road, and engage in other activities. The explanatory memorandum to the law cites the processing of emails in the infotainment system as an example. [643] At the same time however, drivers also have obligations while using the highly automated and fully automated system. These include immediately taking back control of the vehicle when the technology prompts them to do so, cf. Section 1b [644] No. 1 StVG. This is to ensure that the driver does not, for example, finish reading an email before taking back control. In addition, the driver is obliged to take back control if he recognizes or should have recognized due to obvious circumstances that the conditions for using the highly automated and fully automated system are no longer met (Section 1b (2) No. 2 StVG). The aim of this provision is to ensure that the driver is obliged to take action in the event of obvious malfunctions, such as a tire blowout. [645]

In summary, it can be concluded that drivers in highly and fully automated driving must be sufficiently alert to fulfill their obligations under Section 1b (2) of the Road Traffic Act (StVG). The circumstances in which the driver must react during the highly and fully automated phase must be so obvious that they are recognizable even when the driver's attention is diverted from the vehicle controls and the traffic situation. This can be assumed, for example, if the driver is alerted to driving errors and thus to a technical malfunction of the system by the horn of another vehicle or if the system performs an emergency stop without any external cause. [646] Another conceivable practical application scenario in this context could be the siren of an emergency vehicle approaching from behind. In this case, it is appropriate to continue to require the driver to be alert, as the regular request to take back control of the vehicle can also be indicated acoustically, cf. Section 1a (2) No. 5 StVG. [647]

643 BT-Drs. 18/11776, p. 10.
644 BT-Drs. 18/11300, p. 22.
645 *Lange*, NZV 2017, 345.
646 BT-Drs. 18/11776, p. 10f
647 *Lange*, NZV 2017, 345.

f) Data processing with highly or fully automated driving functions, Section 63a StVG

In motor vehicles within the meaning of Section 1a (1) sentence 1 StVG, the position and time data determined by a satellite navigation system must be stored in accordance with Section 63a (1) sentence 1 StVG if there is a change in vehicle control between the driver and the highly or fully automated system. Such storage shall also take place in accordance with Section 63a (1) sentence 2 StVG if the driver is requested by the system to take over control of the vehicle or if a technical malfunction of the system occurs. The purpose of the data storage is to record in a comprehensible manner whether the vehicle was controlled by the system or the driver and whether a change in vehicle control between the driver and the highly or fully automated system has taken place. [648]

In addition, Section 63a (5) StVG now includes the option of transferring data for accident research to third parties in anonymized form. However, it should be noted that the basic requirements for data storage will be part of the EU regulations. Against this background, a number of regulatory powers have been provided for in Section 63b of the StVG in favor of the Federal Ministry of Transport and Digital Infrastructure. This should enable the regulations necessary for the implementation of the international requirements to be introduced. These include the technical design and location of the storage medium, the manner of storage, the addressees of the storage obligation under Section 63a (3) StVG, and the measures that must be taken to protect the stored data against unauthorized access in the event of the sale of the motor vehicle [649]

g) Driverless parking, Section 6 (1) No. 14a StVG

Vehicles are already capable of parking without a driver and thus autonomously. The legislature intends to take this fact into account with the provision in Section 6 (1) No. 14a StVG. According to Section 6 (1) No. 14a StVG, the Federal Ministry of Transport and

[648] BT-Drs. 18/11776, p. 11.
[649] BT-Drs. 18/11776, p. 11.

digital infrastructure enables regulations to be established for the installation and use of driverless parking systems. These are to be installed in low-speed areas on parking spaces that are separated from the rest of the public road network by structural or other means and can only be accessed and exited via special access and exit routes.

Google Inc. is known for many AI technologies, particularly the self-learning algorithm used in its search engine. Google has also been working on self-driving cars for years. In May 2014, Google began building 100 in-house electric test vehicles, with the first prototypes of the Google car designed to operate without a steering wheel, brakes, or accelerator pedal. [650] In the long term, the focus will be on providing a service—for example, driverless taxis—rather than necessarily on vehicle ownership.

An autonomous vehicle is defined as a vehicle that navigates freely (i.e., without human assistance).[651] In this case, the car (as AI/robot) autonomously decides how to adapt its driving behavior (steering, speed, etc.) to its environment.[652] Robots perceive their environment using sensors and react according to their programming. A certain ability to learn, which leads to an expansion of possibilities, is certainly not excluded, but rather desirable. Robotics deals with what is known as manipulative intelligence: with the help of robots, dangerous activities or repetitive tasks, such as defusing bombs, can be transferred to robots. The basic idea is to create systems (robots) that can replicate the intelligent behavior of living beings.

650 Self-driving cars: Google builds its own car, in: Web news ticker: Heise online. Retrieved on May 29, 2014.

651 *Hägele/Schäfer*, in: Gevatter/Grünhaupt (eds.), Handbook of Measurement and Automation Technology in Production, 2006.

652 *Kirsch,* CT Magazine for Computer Technology No. 22, 2011, 43.

III. Possible ways of evaluating artificial intelligence

In autonomous driving, artificial intelligence or an algorithm in conjunction with machine learning (hereinafter referred to as artificial intelligence) replaces humans to control the vehicle. Artificial intelligence must therefore be granted certain evaluation options, because according to Section 1 e (2) No. 1, No. 2 Alt. 1 StVG, motor vehicles with autonomous driving functions must have technical equipment that is capable of

to perform the driving task within the specified operating area independently, without the driver intervening in the control system or the vehicle being permanently monitored by technical supervision, to comply independently with the traffic regulations applicable to the driving of the vehicle, and to have an accident prevention system designed to prevent damage and minimize damage.

However, it is questionable whether restrictions beyond this need to be taken into account.[653] Examples include ad hoc traffic signs or instructions from traffic police officers that cannot (yet) be detected by autonomous driving functions.[654] According to Section 1 e (2) No. 3 StVG, motor vehicles with autonomous driving functions must be technically equipped in such a way that they can be put into a risk-minimizing state under certain circumstances (see Section 1 e (2) Nos. 3, 5, 7, 8, 10 StVG). This is necessary if the journey can only be continued by violating traffic regulations—for example, because a traffic light does not turn green due to a technical defect.[655] The term "risk-minimized state" is legally defined in Section 1 d (4) StVG and is a state in which the vehicle comes to a standstill with its hazard warning lights activated at a suitable location in order to ensure the greatest possible safety for the vehicle occupants, other road users, and third parties.

653 *von Bodungen/Gatzke*, RDi 2022, p. 354.

654 *Hilgendorf*, JZ 2021, p. 444 (447).

655 *von Bodungen/Gatzke*, RDi 2022, p. 354.

In its report of June 2017, the Ethics Commission for Automated and Connected Driving concluded in section 5 that automated and connected technology should prevent accidents as far as practically possible. The technology must be designed in accordance with the current state of the art in such a way that critical situations do not arise in the first place; this also includes dilemma situations, i.e., situations in which an automated vehicle is faced with the "decision" of having to choose between two equally bad options. With the introduction of Section 1e (2) No. 2 (c) of the Road Traffic Act (StVG) on July 28, 2021, a new provision was added to the law stipulating that motor vehicles with autonomous driving functions may not give further weight to personal characteristics in the event of an unavoidable alternative danger to human life. [656]

Back in October 2016, at the 30th Munich Media Days, then-Chancellor Angela Merkel called for algorithms used by internet services to filter information to remain transparent. Media use is increasingly influenced by algorithms, bots, and intelligent recommendation systems. Algorithms mean that readers are increasingly only offered topics online that correspond to their search behavior. This can reduce their ability to engage with other opinions.[657] However, there are already regulations in place that are intended to ensure the neutrality of algorithms. Recital 71 of the GDPR already contains an obligation to ensure the "neutrality of algorithms." Similar to scoring in
Section 28b No. 1 BDSG requires a "suitable mathematical or statistical procedure" for profiling and the exclusion of discriminatory calculation methods.[658] In the case of Section 1e (2) No. 2 (c) StVG, they even go one step further and rightly prohibit artificial intelligence from making judgments about the quality of human life.

It is really gratifying that this also resolves the supposedly philosophical question of

[656] BT-Drucks. 19/27439 dated March 9, 2021, pp. 1–2.

[657] https://www.heise.de/newsticker/meldung/Algorithmen-und-Scoring-Maas-fordert-digitales-Anti-Diskriminierungsgesetz-3761722.html?seite=2 (accessed on 07.03.2023).

[658] *Härting*, ITRB 2016, pp. 209–211.

social researchers have settled whether an algorithm can judge whether a little girl is of greater value to society than an Al-Qaeda leader. This also simply ruled out the philosophical question of applying Isaac Asimov's Three Laws of Robotics. There is no basis for artificial intelligence to make moral decisions about human life because it is not allowed to decide on the value of human life. Should a manufacturer nevertheless use such technology, it will face substantial claims for damages from the person who has suffered harm or their relatives,

e.g., pursuant to Section 823 (2) in conjunction with Section 1e (2) No. 2 lit. c) StVG.

However, in addition to the prohibition of qualitative assessments of human life, the question of quantitative assessments remains open: According to the wording of the law, it would be perfectly permissible, for example, to implement an algorithm in autonomous vehicles that distinguishes whether, in an unavoidable accident, the algorithm must choose between endangering a group with a smaller or larger number of people. This point should be revised, and here too, the algorithm should not be allowed to make any assessment, but should instead use all technical means available to ensure that such a decision does not have to be made in the first place.

To put it positively, the newly created Section 1e (2) No. 2 lit. c) StVG could serve as a model and thus (hopefully) have a significant influence on other areas of artificial intelligence law. Nevertheless, Section 1e (2) No. 2 lit. c) StVG still needs to be (urgently) improved in the area of quantitative evaluation of people.

It is truly gratifying that the creation of Section 1e (2) No. 2 (c) of the Road Traffic Act (StVG) has finally put an end to the tiresome debate about whether a vehicle's algorithm should kill the Taliban committing genocide or the innocent little girl.

H. Ha ftung

On September 28, 2022, the EU Commission published a **draft directive on AI liability**[659]. The aim is to adapt existing European liability law to the challenges posed by artificial intelligence (AI). The draft complements the planned AI Regulation (AI-VO) and the revised Product Liability Directive.

Behind this special law, which can initially be regarded as lex specialis, lies the legal assessment of liability on the part of manufacturers, owners, and users. [660]The decisive factor is who caused the damage in a causal and attributable manner.[661] Determining contributory causes will be a major challenge in cases of damage caused by AI. If AI technology/the robot acts autonomously and causes damage to a person or property, the contributions to causation would first have to be technically verified, which would usually require expert assistance. [662] The ability to act autonomously and artificial intelligence mean that not every action of a machine is directly influenced by a human being. Humans relinquish control of the system, making it more difficult to determine causality and attribution. [663] The contributions of those involved are closely intertwined right from the manufacturing stage, and depending on user behavior, AI technology can be further developed independently of the manufacturer's design and programming. [664]

I. AI Liability Directive

The directive aims to ensure effective legal protection for injured parties who suffer harm caused by AI systems and to promote the innovative capacity of the European AI industry. [665]

[659] Draft EU Directive on AI Liability (COM/2022/496 final)

[660] See also *Riehm*, ITR B 2014, 113.

[661] *Günther/Böglmüller*, BB 2017, 53 to 58.

[662] *Groß/Gressel*, NZA 2016, 990, 996.

[663] *Günther/Böglmüller*, BB 2017, 53 to 58.

[664] *Beck*, in: Japanese-German Center, Human-Robot Interactions from an Intercultural Perspective, 2011, pp. 124, 126

[665] Draft EU Directive on AI liability (COM/2022/496 final)

1. Scope

The directive concerns non-contractual liability claims and is aimed at two key groups:

- Operators and developers of AI systems,
- third parties who use or deploy AI systems.

It covers damage caused by the actions or omissions of actors who place AI systems on the market or operate them.

2. Burden of proof and liability relief

The directive provides for special rules to ease the burden of proof for injured parties. These take into account the technical complexity and lack of transparency of AI systems (the so-called "black box problem").

a) Disclosure obligations

- Injured parties may require operators or developers to disclose relevant information about the AI system if this is necessary for the purpose of providing evidence.
- Companies are only required to disclose this information if a court recognizes the necessity of such information.

b) Assumptions regarding causality

- In the event of breaches of due diligence obligations applicable to the use or development of the AI system, a rebuttable presumption of causality is introduced. It is presumed that the damage was caused by the faulty behavior of the operator or developer.
- This presumption rule applies in particular to violations of provisions of the AI Regulation (e.g., insufficient risk management).

3. Relationship to product liability

The Directive supplements the Product Liability Directive, which is based on strict liability for defective products. The AI Liability Directive is fault-based and regulates in particular:

- Cases in which an AI system causes damage through its use or application without there being a product defect within the meaning of the Product Liability Directive.
- Liability for autonomous decisions made by AI systems that result in damage.

4. Objectives of the Directive

- Legal clarity: Victims are given an effective means of enforcing their claims, even in the case of complex and opaque AI systems.
- Protection of innovation: Companies benefit from legal certainty and an innovation-friendly liability framework.
- Harmonization of liability regimes: The directive harmonizes liability rules within the EU to avoid fragmentation between Member States.

5. Criticism and challenges

- Gaps in protection: The directive leaves open important questions regarding the liability of autonomous AI systems in the gray area between product liability and non-contractual liability.
- Administrative burden: The documentation and disclosure requirements could be particularly burdensome for SMEs.
- Balance between victim protection and innovation: The directive attempts to balance victim rights and innovation protection, but this is not considered successful in all respects.

6. AI Regulation (AI-VO) AI Liability Directive

The AI Regulation (AI-VO)[666] and the EU Directive on AI liability[667] complement each other and together form a coherent legal framework governing the development, use, and liability for artificial intelligence (AI) in the European Union. Their interaction is based on a clear division of tasks and the goal of covering both legal and technical requirements for AI systems.

The AI Regulation and the EU Directive on AI liability have different focuses. The AI Regulation sets technical requirements for AI systems, in particular for risk minimization and the protection of fundamental rights. It addresses the obligations of developers, providers, and users of AI systems in various risk categories (e.g., high-risk AI). Key points include transparency obligations, risk analyses, and the creation of a certification and monitoring mechanism. The aim of the AI Regulation is ex ante regulation to prevent damage through compliance with technical standards. It aims to give injured parties effective means of asserting claims for damages by introducing specific evidence relief and presumptions of causality. In particular, it is presumed that damage is attributable to the use of AI if due diligence obligations have been breached. The directive thus ties in with the provisions of the AI Regulation by allowing violations of its technical and organizational requirements to be used as a basis for liability. This creates clear liability standards that strengthen both victim protection and legal certainty for operators and developers.

The interaction between the two sets of rules is particularly evident in the fact that the AI Regulation sets the standards for due diligence obligations, the failure to comply with which may trigger liability under the Directive. The AI Regulation thus establishes preventive requirements, while the Liability Directive provides legal protection in the event of damage. Both instruments also promote the harmonization of the legal framework within the EU by

666 Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828

667 COM/2022/496 final

Avoid fragmentation between Member States and establish uniform rules for dealing with AI. At the same time, this integration will strike a balance between promoting innovation and protecting consumers.

A concrete example of cooperation between the regulatory frameworks would be damage caused by high-risk AI, for example in the field of medical diagnostics. If the operator violates the provisions of the AI Regulation by using poor-quality data, this violation could not only lead to sanctions under the Regulation, but also form the basis for claims for damages under the Liability Directive. In such cases, victims would benefit from a reduction in the burden of proof and a presumption of causality, which would enable effective enforcement of their rights.

The interplay between AI-VO and the liability directive strengthens both damage prevention and compensation in the event of damage. While the AI Act establishes clear technical standards to ensure trust in the safe use of AI systems, the Liability Directive ensures that victims of AI-related harm receive effective legal protection. This dual approach forms the basis for an innovation-friendly and consumer-oriented regulatory framework in the European Union. The draft AI Liability Directive is a significant step toward adapting liability law to the specific characteristics of AI systems. In particular, the introduction of evidence relief and presumptions of causality addresses the difficulties arising from the lack of transparency of AI. Nevertheless, the directive remains unclear on some points and will have to be tested in legal practice to determine its effectiveness. Harmonization with the Product Liability Directive and the AI Regulation will be crucial to creating a coherent liability regime in the EU. [668]

II. Manufacturer liability

The creation of AI systems does not, in principle, raise any specific legal issues with regard to general product liability and the obligations developed for it. [669] Consequently

[668] *Osborne Clarke*: Analysis of the new EU liability directives

[669] See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

All manufacturer obligations and related error categories, such as design errors or manufacturing errors, can be applied to the manufacture of AI systems. The manufacturer of AI systems is therefore obliged to make use of all sources of knowledge generally available or specifically accessible to them in order to avert dangers posed by the products they place on the market.[670] The decisive factor is whether the manufacturer must have been aware of the defects when the product was placed on the market. [671] Product risks that only become apparent later do not mean that the manufacturer can be held responsible for a design defect. [672] This is rather a development defect, so that only subsequent obligations within the scope of product monitoring can apply.[673] In the IT environment, which is so similar to AI, it is argued, for example, that even if IT systems are sometimes very complex, there is no way around the fact that known security problems must be eliminated immediately before the product is placed on the market. [674]

1. Manufacturer obligations

The manufacturer of an AI system must also instruct the purchaser of such a system on its correct use and commissioning. If the AI system consists solely of an algorithm, the manufacturer of, for example, a credit score must also inform the user of the score (operator) of the risks associated with using the score. This is particularly important in order to avoid liability cases under Section 824 of the German Civil Code (BGB) "Credit risk" (see 4.). When using robots and comparable technical AI systems, the users and operators may themselves be professionals, in which case the instruction obligations may be significantly reduced. [675]

[670] Federal Court of Justice, November 12, 1991 – VI ZR 7/91, BGHZ 116, 60, 70 f.= VersR 1992, 96, 99; 17 October 1989 – VI ZR 258/88, NJW 1990, 906, 907 f.; 23 May 1952 – III ZR 168/51, NJW 1952, 1091; *Kullmann*, NJW 2002, 30, 32; *Kullmann,* in: Kullmann/Pfister, Produzentenhaftung (Producer Liability), as of 1/2012, Knz. 1520, p. 7; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 24 margin note 378; *Spindler,* in: BeckOGK/BGB, § 823 margin no. 607, 610

[671] See *Spindler* on robots and autonomous driving, CR 2015, pp. 766 to 776.

[672] *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, Section 24, margin number 71, 103 ff.; cf. *Jänisch/Schrader/Reck*, NZV 2015, 313, 317 "at the time of placing on the market"; *Vogt*, NZV 2003, 153, 159.

[673] See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

[674] *Meier/Wehlau*, CR 1990, 95, 97; see also *Schneider/Günther*, CR 1997, 389 ff.; *Bartsch*, CR 2000, 721, 722 ff.

[675] Federal Court of Justice, May 14, 1996 – VI ZR 158/95 = NJW 1996, 2224, 2226 with further references – Grimm's guiding wheel; for more details, see *Spindler,* in: BeckOGK/BGB, Section 823, marginal number 607.

It should of course be taken into account that credit officers or doctors[676] often have the specialist knowledge but sometimes lack the technical expertise to understand an AI system and use it without instruction. In the case of vehicles equipped with AI systems for autonomous driving, it must of course be taken into account that the purchasers and drivers of the vehicles are generally not AI experts. [677]

2. Product monitoring obligations

The manufacturer of an AI system also has product monitoring obligations, because the manufacturer is not completely released from its responsibility for the product after it has been placed on the market. The concept of product monitoring obligations is at odds with design

, manufacturing and instruction obligations of the manufacturer, because a breach of the product monitoring obligation does not automatically result in a negatively assessed product characteristic – a "defect."[678] The recognition of product monitoring obligations is due to the fact that the duties of care of the manufacturer of goods are time-related and are therefore based on historical risk assessments and risk control options.[679] The intensity of the product monitoring obligation is governed by general rules, i.e., it depends on the extent of the potential damage and the degree of risk on the one hand, and on the possibility and economic feasibility of monitoring measures on the other.[680] It is generally less pronounced for proven products that have been on the market for a long time and in large quantities, and particularly intensive for complex new developments with great potential for harm. [681] In the case of AI systems such as robots, a comparison with complex IT systems is appropriate.

676 Special obligations apply here under the Medical Devices Act (MPG); see Chapter E. "Cyborg," including Section 14 MPG in conjunction with the Medical Devices Operator Ordinance. See *Lippert,* in: Deutsch/Lippert/Ratzel/Tag, MPG, 2nd edition 2010, Section 2 MPBetreibV margin number 1 et seq.

677 See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

678 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 823 margin no. 836 to 837.

679 Based on BGHZ 80, 199, 202 ff.= NJW 1981, 1606, 1607 f. – Benomyl; likewise BGHZ 80, 186, 191= NJW 1981, 1603, 1604 – Apple scab.

680 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 823 margin no. 838.

681 BGHZ 99, 167, 170 f.= NJW 1987, 1009, 1010 – Handlebar fairing; BGH, NJW 1994, 517, 519 – Thread cutting agent I; NJW-RR 1995, 342, 343 – Thread cutting agent II.

possible;[682] because it is precisely the knowledge of the objective inevitability of programming errors ("bugs") that gives rise to a duty on the part of the manufacturer to monitor its products with particular care.[683] The obligation to actively monitor products involves generating information about possible risks of damage to one's own product.[684] Experience with competing products of the same or similar nature may be considered as a source of such information, provided that such data is available to the manufacturer. [685] In the event of imminent danger to life and limb, even a serious suspicion is sufficient to trigger warning obligations.[686] In the case of autonomous vehicles in particular[687] the monitoring obligations are therefore particularly intensive. In the event of property damage and no acute threat, the manufacturer may initially limit itself to its own investigations and active monitoring of the product in the event of suspicion, without having to issue a warning about the product or its specific use.[688] A distinction must be made between active and passive product monitoring: Passive product monitoring is limited to receiving, collecting, and systematically evaluating customer complaints about damage and safety deficiencies.[689] Such measures can be implemented at low economic cost and generate significant benefits because they are based on real experience and are therefore particularly reliable, eliminate the need for costly investigation and testing procedures, and are made available to the manufacturer free of charge and without any search effort.[690] The courts have also ruled that manufacturers are not obliged to monitor the interaction of their own products with third-party products

682 See *Spindler* on robots and autonomous driving, CR 2015, pp. 766 to 776.

683 *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, Section 24, margin number 174 et seq.; *Spindler*, in: Kullmann/Pfister, Produzentenhaftung (Product Liability), Produkthaftung im IT-Bereich (Product Liability in the IT Sector), forthcoming, p. 45; contrary opinion LG Cologne, July 21, 1999 – 20 S 5/99, CR 2000, 362= NJW 1999, 3206: No obligation to warn in the event of subsequent knowledge of a virus infection on a diskette.

684 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 823 margin no. 839.

685 *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 375.

686 Federal Court of Justice, March 17, 1981 – VI ZR 191/79, BGHZ 80, 186, 192= NJW 1981, 1603; Higher Regional Court of Frankfurt, November 11, 1993 – 1 U 254/88, NJW-RR 1995, 406, 408; 29.09.1999 – 23 U 128/98, NJW-RR 2000, 1268, 1270; Higher Regional Court of Karlsruhe, March 27, 1996 – 7 U 61/94, VersR 1998, 63, 64 f.; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 24 margin number 314.

687 In general, *Jänich/Schrader/Reck*, NZV 2015, 313, 318 with further references.

688 Federal Court of Justice, March 17, 1981 – VI ZR 191/79, BGHZ 80, 186 (192)= NJW 1981, 1603; *Kullmann*, NJW 1996, 18 (23).

689 BGHZ 99, 167, 170 f.= NJW 1987, 1009, 1010 – Handlebar fairing; BGH, NJW 1994, 517, 519 – Thread cutting agent I; NJW-RR 1995, 342, 343 – Thread cutting agent II.

690 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 823 margin no. 839.

produced accessories have been developed. [691] However, given the endless nature of the resulting obligations, it seems highly doubtful that this case law, which has remained isolated to date, can actually be extended to cover the interaction of AI systems (e.g., robots) with all other possible products in the environment.[692] The case law goes too far here: a general extension of the observation obligations to accessories or combination hazards cannot be justified solely on the grounds that the manufacturer is in any case obliged to observe the products. In principle, the manufacturer is only responsible for the risks he has created himself, but not for increases in risk caused by third parties[693] especially if the accessory products are placed on the market significantly later than their development, design, and manufacture.[694] In any case, it must be considered sufficient for the manufacturer to instruct the product user in general that only accessories approved by him or classified as safe can be used safely and that the use of unauthorized accessories is at the user's own risk.[695] The obligation to actively monitor products concerns the generation of information about possible risks of damage to the manufacturer's own product. [696] Experience with competing products of the same or similar nature may be considered as a source of such information, provided that such data is available to the manufacturer.[697] In addition, scientific and technical literature must be evaluated insofar as it is relevant to the manufacturer's own product. [698] The scope of this obligation in detail depends in turn on the potential for harm of the product, its price, and the legitimate safety expectations of its users based on this price, and finally on the effort required to fulfill the obligation. [699]

---

691 Fundamental to this is BGH, December 9, 1986 – VI ZR 65/86, BGHZ 99, 167= NJW 1987, 1009 – Honda= CR 1987, 230; on this, see *Ulmer*, ZHR 152, 564, 570 ff.; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 25 Rn. 178 ff.; *Kullmann,* in: Kullmann/Pfister, Produzentenhaftung (Producer Liability), 1/2012, Knz. 1520, p. 52.

692 See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

693 Similarly *Ulmer*, ZHR 152, 564, 579; *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3rd ed. 2012, § 25 Rn. 222; concurring opinion *by v. Bar,* in: v. Bar, Product Responsibility and Risk Acceptance, 1998, pp. 29, 36.

694 See *Spindler* on robots and autonomous driving, CR 2015, pp. 766 to 776.

695 *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, Section 25, margin number 187 et seq. In line with this, see also BGH, December 9, 1986 – VI ZR 65/86, BGHZ 99, 167, 174 = NJW 1987, 1009 = CR 1987, 230.

696 *MüKoBGB/Wagner*, 7th edition, 2017, BGB § 823 margin number 839.

697 *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 marginal no. 375.

698 BGHZ 80, 199, 202 f.= NJW 1981, 1606, 1607 f. – Benomyl; BGH, NJW 1990, 906, 907 f. – Horse boxes.

3. Reaction obligations

Violation of the product monitoring obligation alone does not cause damage; damage only arises if the manufacturer fails to draw the necessary conclusions from the information obtained through monitoring or fails to collect or evaluate information that is actually available, thereby depriving itself of any possibility of reacting from the outset. In this respect, the product monitoring obligation is only a means to the end of responding. The question of how this response should be structured in detail is one of the focal points of current product liability law. The response obligations also apply to AI systems and even if only an algorithm is used. They must therefore be taken into account and applied accordingly by manufacturers of AI systems.

4. Recall obligations

One consequence of the monitoring obligation is, of course, the recall of the defective AI system in question to ensure that no further damage is caused by the defective AI system. It is controversial whether and, if so, under what conditions the manufacturer may also be required to recall products already on the market in order to replace or repair them, and who should bear the costs of such measures. According to one view, recall obligations on the part of the manufacturer should be rejected[701] because the manufacturer already fulfills its risk control obligations by issuing a warning about the product hazards[702] and because recognizing further recall and repair obligations would set aside the assessments of warranty law.

699 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 823 Rn. 809.

700 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 823 marginal no. 840.

701 LG Frankfurt a. M., VersR 2007, 1575 f. – X-ray machine; *Brüggemeier*, ZHR 152, 1988, 511, 525 f.; ibid., DeliktsR margin no. 565 ff.; ibid., RabelsZ 66, 2002, 193 ff.; *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 margin note 340 ff., § 39 margin note 2 ff. (albeit with distinctions).

702 *Brüggemeier,* ZHR 152, 1988, 522, 525; *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 344 ff., 354 ff.

That would be incurred. [703]In principle [704] case law tends to limit the damage to the costs of removing the defective parts, but not to reimburse the costs of installing new, defect-free parts [705] unless, again, the damage is to life and health, such as pacemakers (see "Cyborg"). However, the manufacturer is obliged to avoid dangers to legal interests protected by Section 823(1) of the German Civil Code (BGB), so that at least a claim under Section 1004 BGB must be assumed.[706] Therefore, the manufacturer must bear the full costs [707] in any case for the return of the product if the product poses a risk to other legal interests. [708] In the event of imminent damage to the product itself, a warning to the product user is sufficient, as otherwise the interest in equivalence and the expectation of being able to use the product would be protected.[709] From this, it can be concluded for AI systems that, in principle, no obligation can be derived from product liability law that AI systems, and in particular their software that controls AI systems such as robots or cars, must always be maintained and updated, as it would be sufficient for the customer to stop using the product[710] in order to protect their integrity interests. [711] However, it should be noted that maintenance and support contracts (e.g., for cyborgs and their implants) may result in a slightly different situation.

5. Burden of proof

In the case of complex AI systems that may be defective, the question of the provability of the defect must be regarded as significant in practice.

---

703 LG Frankfurt a. M., VersR 2007, 1575 – X-ray machine; *Brüggemeier*, ZHR 152, 1988, 511, 525 f.; *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 349 ff., § 39 Rn. 6; *Foerste,* DB 1999, 2199, 2200.

704 See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

705 Higher Regional Court of Stuttgart, July 29, 1966 – 10 U 1/66, NJW 1967, 572; concurring opinion Higher Regional Court of Düsseldorf, May 31, 1996 – 22 U 13/96, NJW-RR 1997, 1344, 1346.

706 See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

707 *Dietrich*, Product monitoring obligation and duty of producers to prevent damage, 1994, p. 223 et seq.; dissenting opinion by *Foerste,* in: Foerste/v. Westphalen, Product Liability Handbook, 3rd edition, 2012, Section 24, marginal number 367: cost sharing in exceptional cases.

708 Higher Regional Court of Düsseldorf, May 31, 1996 – 22 U 13/96, NJW-RR 1997, 1344, 1345; Higher Regional Court of Karlsruhe, April 2, 1993 – 15 U 293/91, NJW-RR 1995, 594, 597; *Wagner*, in: MünchKomm/BGB, 6th ed. 2013, § 823 Rn. 677; *Hager*, in: Staudinger, BGB, 2009, § 823 Rn. 26, each with further references; *Dietrich,* Product Monitoring Obligation and Duty of Producers to Prevent Damage, 1994, p. 236; only in cases of danger to life and limb: Mi-chalski, BB 1998, 961, 965.

709 Attributed to *Foerste*, DB 1999, 2199, 2200; *Taschner/Frietsch*, ProdHaftG, 2nd ed. 1990, introduction margin no. 89; similarly *Pieper,* BB 1991, 985, 988 with the note that otherwise a "tortious warranty" would arise; differently v. *Westphalen,* DB 1999, 1369, 1370; *Koch,* AcP 203, 2003, 603, 624 ff., 631 f., wants to grant compensation for the costs of removal and installation, excluding material costs.

710 See also *Molitoris*, NJW 2009, 1049, 1050 f.; *Klindt*, BB 2009, 792, 793; *Spindler,* in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich, forthcoming, p. 50.

711 See *Spindler* for robots and autonomous driving, CR 2015, 766 to 776.

In principle, it can be assumed that the rules developed by case law on the reversal of the burden of proof in favor of the injured party in the context of product liability[712] naturally also apply to tortious liability for robots. The reasons for this reversal of the burden of proof—the injured party's lack of insight into the processes in the sphere of the injuring party[713] —should also be applied mutatis mutandis to the operators of AI systems.[714] There have been isolated calls to depart from this distribution of the burden of proof in general (i.e., also for contractual law) for robots and thus also for other AI systems, since it is not always possible to determine the cause of a robot malfunction, for example, whether it was due to the incorrect evaluation of information from its environment or the incorrect input of information.[715] However, such a reversal of the burden of proof to the injured party would fail to recognize the actual reasons for the reversal of the burden of proof, namely the better control of the source of danger that is a "complex machine system"; only if the malfunctions are actually due to misuse can the burden of proof and presentation be eased. [716]

In practice, it will be difficult to plausibly demonstrate the necessary causality. Is the manufacturer liable under its manufacturer's liability, or was an action by the operator the cause of the damage? In the field of autonomous driving, for example, considerable difficulties in proving causality are expected, as it can only be clarified whether an accident was caused by a fault in the control system or by the driver's intervention.[717] If AI systems work with devices comparable to "flight recorders" or with so-called log files, it is relatively easy to determine who is causally responsible for the damage. [718] The liability is of course different when using pure

712 See *Spindler,* in: BeckOGK/BGB, § 823 margin note 663 et seq.; *Wagner,* in: MünchKomm/BGB, 6th edition 2013, § 823 margin note 684 et seq. with further references.

713 Federal Court of Justice, November 26, 1968 – VI ZR 212/66, BGHZ 51, 91, 104 f.= NJW 1969, 269, 275 – Hühnerpest; *Spindler*, in: BeckOGK/BGB, § 823 Rn. 663; *Wagner*, in: MünchKomm/BGB, 6th ed. 2013, § 823 marginal no. 623.

714 *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

715 This is also recognized in principle *by Lutz*, NJW 2015, 199, 120; *Hanisch*, however, is generally much more skeptical, in: Hilgendorf (ed.), Robotik im Kontext zwischen Recht und Moral, 2014, pp. 27, 38.

716 See *Spindler* on robots and autonomous driving, CR 2015, 766 to 776.

(717) See *Jänich/Schrader/Reck,* NZV 2015, 313, 315; *Lutz,* NJW 2015, 119, 120; example scenario in: *Schuhr, in:* Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, p. 13, 17.

718 This is also recognized in principle by *Lutz*, NJW 2015, 199, 120; *Hanisch,* in: Hilgendorf (ed.), Robotik im Kontext zwischen Recht und Moral, 2014, pp. 27, 38, is generally much more skeptical.

Algorithms must be examined. Here, only a mathematical proof procedure can be used to determine that a defective algorithm was the cause of the damage incurred. In principle, even in the case of an AI system, the injured party is responsible for proving that a legal violation has occurred, including the defectiveness of the AI system and proof that the product defect originated in the manufacturer's organizational sphere and already existed at the time the product was placed on the market.[719] With regard to both the objective breach of duty and fault, the burden of proof is reversed in favor of the injured party.[720] according to which the manufacturer must exonerate itself with regard to all its auxiliary personnel.[721] If, on the other hand, the manufacturer of the AI system provided proper instructions to the operator and the damage would not have occurred if the instructions had been followed properly, there is no reversal of the burden of proof.[722] Even in the event of breaches of the product monitoring obligation, there is no reversal of the burden of proof in favor of the injured party with regard to the objective breach of duty, since only generally accessible information is at issue here, to which the injured party has access, if necessary, through expert opinions in the same way as the manufacturer.[723]

6. Tortious liability

The use of AI as an assistant to humans raises not only contractual issues [724] but also questions of tortious liability, particularly product liability.[725] Due to its unrestricted scope of application, in contrast to the Product Liability Act (ProdHaftG) or other cases of strict liability, fault-based tortious liability is of central importance. It can be roughly divided into two areas: on the one hand, the violation of legal interests pursuant to Section 823 (1) BGB, and on the other hand, the

719 *Spindler,* in: BeckOGK/BGB, Section 823 marginal no. 666 etseq.

720 Federal Court of Justice, March 17, 1981 – VI ZR 191/79, BGHZ 80, 186, 196 f.= WM 1981, 544; confirmed again in Federal Court of Justice, June 11, 1996 – VI ZR 202/95, NJW 1996, 2507, 2508; February 2, 1999 – VI ZR 392/97, VersR 1999, 456; *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd ed. 2012, § 30 marginal no. 62 et seq.

721 Federal Court of Justice, October 17, 1967 – VI ZR 70/66, NJW 1968, 247 ff.; *Wagner*, in: MünchKomm/BGB, 6th edition 2013, § 823 margin number 684 f.

722 See Federal Court of Justice, March 2, 1999 – VI ZR 175/98, DB 1999, 891, 891; Higher Regional Court of Frankfurt, March 11, 1998 – 23 U 55/97, NJW-RR 1999, 27, 30.

723 See the principles established in BGH, March 17, 1981 – VI ZR 191/79, BGHZ 80, 186, 195 ff. = WM 1981, 544; see also BGH, November 12, 1991 – VI ZR 7/91, BGHZ 116, 69, 72 et seq. = ZIP 1992, 38, 40 et seq.; critical view in contrast: *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3rd ed. 2012, § 30 marginal no. 89; *Tiedtke,* in: FS Gernhuber, 1993, p. 471, 480 et seq.

724 See *Spindler,* in: Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, p. 63, 66 f. with further references, although he only refers to robots.

725 See *Fleck/Thomas*, NJOZ 2015, 1393, 1398; *Lutz,* NJW 2015, 119 ff.; *Schuhr,* in: Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, p. 13, 17; *Weisser/Färber,* MMR 2015, 506, 511.

Violation of protective law pursuant to Section 823 (2) BGB. [726]

A violation of the legal interests protected by Section 823(1) of the German Civil Code (BGB) by AI is primarily conceivable indirectly as a result of malfunctions in algorithms or failures in autonomous/semi-autonomous systems.[727] First, it is necessary to distinguish between equivalence and integrity interests: The general or public interest in safe robot systems cannot relate to the interest in a functioning robot, which alone concerns the equivalence interest. System malfunctions can therefore be dealt with solely under contract law.[728] In particular, damage caused by autonomous/semi-autonomous systems due to malfunctions of the AI used (e.g., a poorly designed algorithm) is likely to affect the equivalence interest as a rule. This is particularly likely to be the case if the algorithm can no longer be separated from the machine controlled by the algorithm, as is the case with autonomous driving, for example.[729] However, this depends heavily on the specific technical circumstances: if the control elements can be separated from the rest of the vehicle, in particular without impairing its functionality, they are likely to be functionally separable parts, in which case the integrity interest would still be affected. [730]

Tortious liability under Section 823(1) of the German Civil Code (BGB) requires, among other things, fault. Sections Sections 276 to 278 BGB determine what the debtor is responsible for. This includes not only his own fault, but also the fault of his vicarious agents and obstacles to performance if the debtor has assumed a risk of performance, and certainly his insolvency. These standards are not bases for claims, but only auxiliary standards that determine the extent of liability in the contractual relationship.[731] Fault on the part of the debtor is generally not a prerequisite for a claim, but is

[726] *Spindler*, CR 2015, 766 to 776.

[727] For the IT sector: *Koch*, NJW 2004, 801, 802; *Taeger*, Non-contractual liability for faulty computer programs, 1995, p. 259 ff.; *Koch*, Insurability of IT risks, 2005, margin no. 185 ff., 355 ff., 632 ff.

[728] *Spindler,* Roboter, CR 2015, 766 to 776.

[729] For more details, *see Spindler,* in: Lorenz, Karlsruhe Forum 2010: Liability and Insurance in the IT Sector, 2011, p. 26 ff.; idem, in: Kullmann/Pfister, Producer Liability, Product Liability in the IT Sector, forthcoming, p. 36

[730] See *Jänisch/Schrader/Reck*, NZV 2015, 313, 316; *Vogt*, NZV 2003, 153, 158. In agreement with regard to software and progressive defects: *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 21 margin number 67; *Marly,* Praxishandbuch Softwarerecht (Practical Handbook on Software Law), 6th ed. 2014, margin no. 1861; *Sodtalbers*, Softwarehaftung im Internet, 2006, margin no. 513, 518.

[731] *Palandt/Grüneberg*, BGB, 72nd ed. 2013, § 276 margin no. 2.

merely presumed.[732] The debtor must rebut the presumption and prove, pursuant to Sections 280(1) sentence 2, § 286 (4) BGB that he is not responsible for the breach of duty.[733] According to § 276 (1) BGB, the debtor is liable for his own fault, i.e. he is liable for the two forms of fault under civil law: intent and negligence. The BGB places them on an equal footing, as negligence is sufficient. Intent only comes into play when assessing damages pursuant to § 254 BGB.[734] The debtor is only liable for breaching the contractual or statutory obligation, not for causing the damage. In addition to liability for their own fault, the contracting parties are also liable to the same extent for the fault of their vicarious agents pursuant to Section 278 BGB. Vicarious agents are persons whom the contracting parties employ to fulfill their contractual obligations.[735]

a) Intent

The law does not contain a legal definition of intent, but it is generally understood to mean knowledge (intellectual element) and volition (voluntary element) of the circumstances relevant to the objective legal facts.[736] Such cases are conceivable when AI technologies are used to damage other systems, such as in high-frequency trading, or when violations of data protection law are deliberately accepted in order to increase one's own profits. The debtor acts intentionally if they consciously and deliberately make performance impossible, delay it, or perform it poorly.[737] In the case of intent, a distinction is generally made between direct and conditional intent. The distinctions developed mainly in criminal law do not play a role here for intent as a prerequisite for civil liability.[738] In civil law, the latter, weakest form is sufficient.[739]

---

[732] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 8th edition, 2011, margin number 1710.

[733] Federal Court of Justice, May 6, 1981 - IVa ZR 170/80= BGHZ 80, 269; NJW 1981, 1729; MDR 1981, 735; Federal Court of Justice, June 9, 1982 - IVa ZR 9/81= BGHZ 84, 244; NJW 1982, 2238; ZIP 1982, 1214; MDR 1982, 915; VersR 1982, 850; BGH, 13.12.1991 - LwZR 5/91= BGHZ 116, 334; NJW 1992, 1036; MDR 1992, 371; ZMR 1992, 140; WM 1992, 831; Federal Court of Justice, October 5, 1989 - III ZR 126/88= NJW 1990, 1230; MDR 1990, 416; VersR 1990, 207; WM 1990, 438.

[734] *Schellhammer*, Law of Obligations According to the Basis of Claims, 8th ed. 2011, margin no. 1711.

[735] In particular, legal representatives such as employees, vicarious agents, but also subcontractors; *Palandt/Heinrichs*, 77th ed. 2018, § 278 margin no. 4

[736] *Dauner-Lieb,* in: Dauner-Lieb/Langen, BGB Schuldrecht (BGB Law of Obligations) Volume 2/1, 2nd edition 2012, § 276 margin number 10; *Grundmann,* in: Münchener Kommentar BGB Vol. 2: Law of Obligations, General Part (§§ 241 - 432), 7th ed. 2015, § 276 margin no. 150 to 163.

[737] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 8th edition, 2011, margin number 1711.

[738] *Dauner-Lieb,* in: Dauner-Lieb/Langen, BGB Schuldrecht (BGB Law of Obligations) Volume 2/1, 2nd edition, 2012.

[739] *Brox/Walker,* Law of Obligations AT, 36th edition, 2012, margin number 306.

In civil law, intent also includes awareness of the illegality of an act, so that any mistake regarding the prohibition precludes intent.[740] The debtor is guilty of a mistake regarding the prohibition if he erroneously believes that his conduct in breach of contract is in accordance with the contract.[741] However, only a direct mistake regarding the prohibition exonerates the debtor from the accusation of negligence.[742] The burden of proof lies with the debtor.[743] However, a mistake of law is usually avoidable and therefore negligent.[744] The debtor must be familiar with the relevant legal provisions and contractual rules.[745] Even incorrect advice from a lawyer does not always excuse the debtor.[746]

In some cases, attempts are made in Anglo-American contract law to limit the amount of liability for intent. However, according to Section 276(3) of the German Civil Code (BGB), liability for intent cannot be waived in advance. This provision cannot be waived or limited in terms of amount for intent.[747]

c) Negligence

As already mentioned, several times, AI technologies are capable of many things that violate prohibitive norms and thus trigger liability under Section 823(2) BGB in conjunction with the relevant prohibitive norm. Such cases are particularly conceivable if the principles for the processing of personal data under Article 5 GDPR are violated, as AI technologies are quickly capable of doing so.

According to Section 276 (2) of the German Civil Code (BGB), anyone who fails to exercise the care required in the course of business is acting negligently. Negligence means the "avoidability of the unlawful consequence," in this case: the breach of performance due to a breach of a contractual obligation. A fundamental distinction is made between conscious and unconscious negligence.

---

[740] Federal Court of Justice, May 12, 1992 - VI ZR 257/91 = BGHZ 118, 201; NJW 1992, 2014; NJW-RR 1992, 1117 (Ls.); ZIP 1992, 847; MDR 1992, 751; VersR 1992, 1006; WM 1992, 1379; BB 1992, 1379; BB 1992, 379; DB 1992, 1775; Rpfleger 1992, 529; BGH, July 10, 1984 - VI ZR 222/82= NJW 1985, 134; MDR 1985, 219; VersR 1984, 1071; WM 1984, 1433; BauR 1984, 658; ZfBR 1984, 276; ZfBR 1987, 196.

[741] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations According to Legal Basis), 8th edition, 2011, margin number 1713.

[742] *Dauner-Lieb,* in: Dauner-Lieb/Langen, BGB Schuldrecht (BGB Law of Obligations) Volume 2/1, 2nd edition 2012, § 276 margin number 10.

[743] *Palandt/Grüneberg*, BGB, 72nd ed. 2013, § 276 margin no. 10.

[744] Federal Court of Justice, May 30, 1972 – VI ZR 6/71; 89, 303= BGHZ 59, 30; NJW 1972, 1366; GRUR 1973, 90; VersR 1972, 938; BB 1972, 857; DB 1972, 1530; BGH, 18 April 1974 - KZR 6/73= NJW 1974, 1903; BGH, 14 June 1994 - XI ZR 210/93= NJW 1994, 2754; ZIP 1994, 1350; MDR 1994, 1204; VersR 1994, 1349; WM 1994, 1613; BB 1994, 1812; DB 1994, 1819; Federal Court of Justice, July 4, 2001 - VIII ZR 279/00 = NJW 2001, 3114; MDR 2001, 1293; WM 2001, 2012.

[745] Federal Court of Justice, July 10, 1984 – VI ZR 222/82= NJW 1985, 134; MDR 1985, 219; VersR 1984, 1071; WM 1984, 1433; BauR 1984, 658; ZfBR 1984, 276; ZfBR 1987, 196; BGH, June 14, 1994 - XI ZR 210/93= NJW 1994, 2754; ZIP 1994, 1350; MDR 1994, 1204; VersR 1994, 1349; WM 1994, 1613; BB 1994, 1812; DB 1994, 1819; BGH, July 4, 2001 - VIII ZR 279/00= NJW 2001, 3114; MDR 2001, 1293; WM 2001, 2012.

[746] Federal Court of Justice, May 15, 1979 – VI ZR 230/76= BGHZ 74, 281; NJW 1979, 1882; VersR 1979, 769.

[747] *Palandt/Heinrichs*, 77th edition, 2018, Section 276, marginal number 35.

The debtor acts with conscious negligence if they foresee the unlawful outcome but hope to avoid it through carelessness. In the case of AI technologies, this can be assumed if the manufacturer fails to implement certain protective mechanisms in the AI technologies to make them safer. If, out of negligence, they do not even recognize the danger posed by the AI system, they are acting negligently without awareness.[748] In cases of negligence, a fundamental distinction must be made between the facts requiring proof that give rise to the accusation and the accusation itself, which is a legal assessment.[749]

When it comes to the degree of negligence, liability clauses (not only for AI technologies) often differentiate between gross and slight negligence. In principle, the debtor, i.e. the manufacturer of the AI technology, is legally liable for both forms of negligence; in certain cases, gross negligence may lead to greater contributory negligence under Section 254 of the German Civil Code (BGB). Legal exceptions where a distinction between gross and slight negligence plays a role are:

- The debtor during the creditor's default (Section 300 (1) BGB),
- The donor (Section 521 BGB)
- The lender (Section 599 BGB),
- The emergency manager without a mandate (Section 680 BGB)
- and the finder (Section 968 BGB).
- Only gross negligence prevents the acquisition of movable property, bills of exchange, and checks in good faith (Section 932 (2) BGB; Art. 16 (2) WG; Art. 21 ScheckG).
- Only gross negligence on the part of the policyholder exempts the insurer (Section 61 VVG).

Even more important is the distinction between gross and slight negligence due to
Section 309 No. 7. Liability for slight negligence can generally be excluded by general terms and conditions

[748] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations according to the Basis of Claims), 8th edition 2011, margin number 1714.

[749] Federal Court of Justice, May 11, 1953 – IV ZR 170/52= BGHZ 10, 14; NJW 1953, 1139, Federal Court of Justice, October 5, 1973 – V ZR 163/71= NJW 1973, 2207; VersR 1974, 169.

are excluded, but not for gross negligence towards non-business customers (the extent to which Section 307 limits a standard exclusion of liability towards business customers is doubtful).[750] Fundamentally, a person acts with gross negligence if they violate the required duty of care in an unusually serious manner and disregard the simplest concerns that should be obvious to everyone.[751] In addition to the objective component, a subjective component is also decisive here: The perpetrator must be particularly culpable.[752] For this reason, personal performance capacity, which otherwise plays no role in objective negligence, is also relevant here.[753] A definition coined by the Federal Social Court (BSG) can be used here: *According to this, negligence is a particularly gross and also subjectively inexcusable breach of duty that significantly exceeds the usual degree of negligence.*[754]

Liability clauses often contain different liability frameworks for gross and slight negligence. If there is therefore a negligent act which cannot be classified as gross negligence, the manufacturer is only liable within the scope of the limitation of liability for slight negligence. As a rule, liability clauses for slight negligence are lower in amount than for gross negligence, as gross negligence is based on a significant breach of duty.

In theory, it is easy to distinguish between intent and negligence: the perpetrator acting with intent wants the act to be committed, while the perpetrator acting negligently does not.[755] However, this does not make it easy to prove in practice, unless the debtor admits to having acted intentionally.

d) Product liability / Product Liability Directive

In principle, the manufacturer of AI technologies according the

[750] BGH, January 19, 1984 - VII ZR 220/82= BGHZ 89, 363; NJW 1984, 1350; ZIP 1984, 457; MDR 1984, 482; BB 1984, 746; BGH, February 23, 1984 - VII ZR 274/82= NJW 1985, 3016; ZIP 1984, 971; MDR 1984, 1018; WM 1984, 1224; BB 1984, 939; ZfBR 1990, 134; ZfBR 1991, 20.

[751] Federal Court of Justice, October 8, 1991 – XI ZR 238/90= NJW 1992, 316; ZIP 1991, 1477; MDR 1992, 369; WM 1991, 1946; DB 1991, 2478; Federal Court of Justice, September 29, 1992 - XI ZR 265/91= NJW 1992, 3235; ZIP 1992, 1534; MDR 1993, 41; VersR 1993, 105; WM 1992, 1849; DB 1992, 2543.

[752] Federal Court of Justice, May 6, 1985 – II ZR 162/84= VersR 1985, 730, 731.

[753] Federal Court of Justice, January 12, 1988 - VI ZR 158/87 = NJW 1988, 1265; NJW-RR 1988, 657 (Ls.); MDR 1988, 488; NZV 1988, 19; VersR 1988, 474; ZfBR 1989, 68.

[754] *Brox/Walker,* Law of Obligations AT, 36th ed. 2012, margin no. 311.

[755] *Brox/Walker,* Schuldrecht AT (Law of Obligations), 36th edition, margin note 315.

Product Liability Act (ProdHaftG).[756] In the case of software used in this way, the application of the Product Liability Act was often rejected on the grounds that software is not a movable object and therefore not a product within the meaning of the ProdHaftG. [757] This argument could also apply to algorithms. However, the applicability of the Product Liability Act is generally affirmed for standard software, as it is a movable item within the meaning of Section 90 BGB. This position is in line with both national "opinio communis" [759] as well as the state of the international product liability debate. [760] Although the discussion has not been conducted in the literature and case law, it can nevertheless be assumed that, from a purely physical point of view, an algorithm is not a thing. Nevertheless, the fact that the ProdHaftG also covers handcrafted products speaks in favor of its application.[761] However, it must also be taken into account that, according to its meaning and purpose, the ProdHaftG regulates the problem of liability in the case of multi-stage distribution of mass-produced products, regardless of whether they are manufactured by machine or by hand.[762] The ProdHaftG repeatedly refers in its explanatory memorandum to "a product being placed on the market and used,"[763] and repeatedly refers to "manufacturers of goods" and "consumers."[764] According to the explanatory memorandum, "placing on the market" only occurs when a product "has been introduced into the distribution chain." [765] One of the central innovations is the explicit classification of software as a product in accordance with Art. 4 para. 1 no. 1 sentence 2.

---

[756] ProdHaftG (Product Liability Act) of December 15, 1989, Federal Law Gazette I, p. 2198.

[757] See also *Redeker*, IT Law, 5th edition, 2012, margin number 830; *Hoeren*, IT Law, as of October 2018, p. 183.

[758] *Hoeren,* IT Law Script, as of Oct. 2018, p. 184.

[759] See *Bartl*, Produkthaftung nach dem neuen EG-Recht ProdHaftG, Landsberg 1989, 142; *Taschner*, Produkthaftung, 1986, 84; *Junker* Computerrecht, 3rd ed. 2003, para. 478 ff.; *Hoeren,* RdV 1988, 115, 119; *Hoeren,* Softwarehaftung innerhalb der Europäischen Gemeinschaft (Software Liability within the European Community), in: Handbuch der modernen Datenverarbeitung (Handbook of Modern Data Processing), Issue 146/1989, 22, 30 et seq.; *Junker,* WM 1988, 1217 et seq., 1249 et seq.

[760] See, for example, *Stuurman*, Product liability for software in Europe. A discussion of the EC directive of July 25, 1985, in: Vandenberghe (ed.), Advanced Topics of Law and Information Technology, Deventer 1989, 110, 112 ff.; *Whittaker*, European Product Liability and Intellectual Products, in: LQR 105 (1989), 125, 138 ff.; *Bown,* Liability for Defective Software in the United Kingdom, in: Software Protection 1/1986, 1, 12; *Reed,* Product Liability for Software, in: Computer Law & Practice 4 (1988), 149 ff.; Similarly, for the area of the UCC, Aubrey's R.V. Ctr., Inc. v. Tandy Corp., 46 Wn. App. 595, 600, 731 P.2d 1124 (1987) (accepting agreement of parties that U.C.C. Article 2 applied to transaction involving defective software); mAdvent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 675–76 (3d Cir. 1991) (holding that computer software falls within definition of a 'good' under U.C.C. Article 2).

[761] This is the argument put forward by *Junker*, Computerrecht, 3rd ed. 2003, margin no. 480; *Hoeren*, IT-Recht, as of Oct. 2018, p. 184.

[762] *Hoeren,* IT Law, as of Oct. 2018, p. 184.

[763] Explanatory memorandum to the Product Liability Act, cited in PHI Special Edition/87, 106.

[764] See explanatory memorandum, PHI Special Edition/87, 94, 101 et seq.

[765] Explanatory memorandum, PHI Special Edition/87, 102 with reference to Art. 2d of the European Convention of January 27, 1977, on Product Liability and Death.

ProdHaftRL. [766] This clarifies that AI models and AI systems as software are also subject to product liability. The associated discussions under current law (see above) would thus be settled. Manufacturers of AI systems would then also be liable under the ProdHaftG.

According to Section 1 (1) sentence 1 of the Product Liability Act (ProdHaftG), product liability requires, among other things, that there was a defect in the item that caused the damage (i.e., in the AI system). Such a defect could exist if the manufacturer did not take appropriate safety measures when programming the AI. In any case, the manufacturer is not liable if the AI system did not yet exhibit [767] the defect that caused the damage and if the defect could not be detected according to the state of the art at the time the manufacturer placed the product on the market, cf. Section 1 (2) No. 5 ProdHaftG. Nevertheless, the manufacturer of AI must incorporate safety measures into an AI system so that no damage can occur even after an AI learning process.

The creation of AI is assessed according to the same standards as the manufacture of other hardware or software. The manufacturer is liable in accordance with general product liability and the relevant obligations or in accordance with the breach of duty. Liability for AI systems may arise from design or manufacturing defects. [768] In addition, the manufacturer of the AI system has a product monitoring obligation to exhaust all general sources of information or those specifically available to them.[769] The decisive factor is whether the manufacturer must have been aware of the defects when the product was placed on the market. [770] In the case of self-learning AI, the question of placing on the market would have to be considered in a more differentiated manner. Basically, placing on the market would then be assumed if the AI begins to learn on the network or on the road. Product risks that arise after the

[766] The draft Product Liability Directive (ProdHaftRL) has been with the European Council since January 24, 2024. At its meeting on October 10, 2024, the Council of the European Union formally adopted the Product Liability Directive. Member States have 24 months from publication in the Official Journal to transpose it into national law (ProdHaftG).https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/

[767] *Sprau*, in: Palandt – Commentary on the German Civil Code (BGB), 77th edition, 2017, Section 1 ProdHaftG, marginal number 17.

[768] *Spindler*, CR 2015, 766.

[769] Federal Court of Justice, November 12, 1991 – VI ZR 7/91, BGHZ 116, p. 60,70 f. = VersR 1992, p. 96, 99; October 17, 1989 – VI ZR 258/88, NJW 1990, p. 906, 907 f.; May 23, 1952 – III ZR 168/51, NJW 1952, p. 1091; *Kullmann*, NJW 2002, 30, 32; *Kullmann,* in: *Kullmann/Pfister*, Product Liability, 1/2012, 1520, p. 7; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 24 margin number 378; *Spindler,* in: BeckOK/BGB, § 823 margin no. 607, 610.

[770] *Spindler,* CR 2015, 766 to 776.

product has been placed on the market does not mean that the manufacturer is responsible for a design fault;[771] rather, this is a development fault, meaning that only subsequent obligations within the scope of product monitoring can apply.[772] Even if an AI system is an extremely complex product for which troubleshooting involves considerable effort, this does not mean that known safety issues do not have to be eliminated immediately before the product is placed on the market.[773]

A special feature of the ProdHaftG is that claims for damages pursuant to Section 1 (1) sentence 2 ProdHaftG are only granted in the event of damage to health or damage to other property, provided that this is normally used for private purposes. It is questionable when this should be the case when using a pure algorithm. This would be conceivable in the case of an AI-controlled household robot, implants (see cyborg) or a robot in the care sector. It would also be conceivable in the case of self-driving cars or drones. The law does not apply to damage to commercially used items. In addition, the law assumes an excess of 500 euros in the event of property damage pursuant to Section 11 ProdHaftG. The law only plays a (modest) role because liability under the ProdHaftG cannot be contractually excluded (Section 14 ProdHaftG). This means that every liability clause must include a reference to unlimited liability under the ProdHaftG. Incidentally, tortious liability under Section 823 BGB remains in force alongside the ProdHaftG (Section 15 (2) ProdHaftG), which is of central importance for property damage under EUR 500 and damage to commercially used items. [774]

Accordingly, no obligation can be derived from product liability law that AI systems, and in particular their software, must always be maintained and updated

771 *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, Section 24, margin number 71, 103 et seq.; cf. *Jänisch/Schrader/Reck*, NZV 2015, 313, 317: "at the time of placing on the market"; *Vogt*, NZV 2003, 153, 159.

772 *Spindler,* CR 2015, 766.

773 *Meier/Wehlau,* CR 1990, 95, 97; see also *Schneider/Günther,* CR 1997, 389 ff.; *Bartsch,* CR 2000, 721, 722 ff.

774 *Hoeren*, IT Law, as of October 2018, p. 184.

as it would suffice for the customer to stop using the product[775] in order to protect their integrity interests. However, this only works if no accompanying maintenance or servicing contracts have been concluded – but this is often the case with software-related products. Considering that regular inspections by the manufacturer are required for cars, for example, it stands to reason that the corresponding control hardware and software should also be subject to continuous maintenance – however, these are contractual obligations and not obligations derived from tort law.[776]

The new Product Liability Directive establishes a reversal of the burden of proof, which is regulated in Art. 9 ProdHaftRL[777]. Usually, the plaintiff must prove that a product is defective, that they have suffered damage, and that this damage was caused by the product defect. The new directive stipulates that the product is considered defective if the manufacturer does not disclose important information, if the product does not meet the prescribed safety standards, or if it clearly fails during normal use. [778] The Product Liability Directive for AI systems is part of the EU's comprehensive strategy for regulating artificial intelligence (AI) and supplements the existing provisions of the 1985 Product Liability Directive.[779]T h e new proposal from the European Commission of September 28, 2022 aims to adapt liability rules to the specific characteristics of AI, in particular with regard to complex causality issues and the specificities of digital technologies. Manufacturers are liable under Art. 7 ProdHaftRL for defects in the design, production, or provision of AI systems. Operators may be held liable if they make significant changes to the AI (e.g., through software updates or adjustments) that significantly affect its original state. The directive covers both physical and immaterial damage, provided that this is recognized as such under national law,

[775] See also *Molitoris*, NJW 2009, 1049, 1050 f.; *Klindt*, BB 2009, 792, 793; *Spindler,* in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich (Producer Liability, Product Liability in the IT Sector), forthcoming, p. 50.

[776] *Spindler,* CR 2015, 766 to 776.

[777] Summary of the Product Liability Directive for AI Systems (EU Commission proposal, COM(2022) 495 final)

[778] The draft Product Liability Directive (ProdHaftRL) has been with the European Council since January 24, 2024. At its meeting on October 10, 2024, the Council of the European Union formally adopted the Product Liability Directive. Member States have 24 months from publication in the Official Journal to transpose it into national law (ProdHaftG). https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/

[779] Directive 85/374/EEC

are eligible for compensation. It expressly states that data loss or damage caused by faulty AI decisions may fall within its scope.

The Directive builds on the existing concept of defect in the Product Liability Directive[780], but supplements it with specific features for AI. According to Article 7 of the Product Liability Directive, a product is defective if it does not offer the safety that the general public may expect, taking into account all circumstances, in particular the following:

- the product's presentation, including instructions for installation,
- use and maintenance;
- the reasonably foreseeable use and misuse of the product;
- of the product;
- the effects of any ability to continue learning after the start of use
- on the product;
- the effects of other products on the product, where it can be reasonably assumed that they will occur
- reasonably be expected to be used together
- with the product;
- the date on which the product was placed on the market or put into service
- or, if the manufacturer has no knowledge of the conditions of use,

For AI systems, it is clarified that safety requirements must be assessed dynamically, especially for systems with learning components. Liability is not limited to traditional "products" but also includes digital services that are closely linked to physical products (e.g., cloud-based AI services for autonomous vehicles).[781]

The Product Liability Directive is closely linked to the planned AI Regulation (COM (2021) 206 final). A breach of the requirements laid down in the AI Regulation

[780] Art. 6 Directive 85/374/EEC

[781] https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/

An initial order of a product can serve as an indication of a product defect (Art. 4 (2) Product Liability Directive).

e) AI as a vicarious agent in the fulfillment of obligations

It is questionable whether the liability of the AI system under Section 280 (1) BGB can be attributed to the user under Section 278 BGB. However, this fails because the AI system cannot be assigned its own legal personality (see 7.). In some cases, the analogous application of Section 278 BGB is also considered.[782]In this context, it must be taken into account that the representative within the meaning of Section 278 BGB must have acted culpably, which is factually impossible due to the lack of legal personality of the AI system (see also 4.).[783]

f) Maintenance contracts

If a maintenance contract for the AI system is concluded between the manufacturer and the operator, the manufacturer is liable not only for product liability but also under the maintenance contract. Any failure to fulfill ancillary contractual obligations also constitutes a breach of duty and gives rise to liability for damages, unless the supplier can prove that it is not responsible for the breach of duty (Section 280 (1) sentence 2 BGB). In addition, in the event of any significant breach of duty, the operator may, after setting a deadline without success, demand compensation in lieu of performance (Section 281 (1) BGB) or withdraw from the contract (Section 323 (1) BGB).[784]

The responsibility already at the time of contract initiation is specified in § 311 para. 2 i.

This is regulated by Section 241(2) of the German Civil Code (BGB). For example, a manufacturer of an AI system must take into account the rights, legal interests, and interests of the potential customer even before the contract is concluded. This includes, above all, duties to provide information about the AI system. If the seller of the AI system culpably fails to fulfill these obligations toward the purchaser, it must be liable for any damages incurred. In this context, it is important to note that the seller of the AI system is liable toward the purchaser in the so-called

782 *Mayinер,* Die künstliche Person (The Artificial Person), 2017, p. 84 et seq.

783 *Müller-Hengstenberg/Kirn,* NJW 2014, 307, 311.

784 *Hoeren*, IT Legal Script, as of Oct. 2018, p. 181,

"Specialist retailers" only have a duty to provide information about the characteristics that they know or should know about. [785] Even manufacturers of AI systems are not required to point out completely absurd or remote risks. This aspect is important because in many areas it is not yet possible to foresee what damage AI systems may cause. It should also be noted that, according to established case law and the provision in Section 307(2)(2) of the German Civil Code (BGB), the exclusion of liability in standard form contracts (general terms and conditions) for slight negligence is only possible to the extent that no essential contractual obligations are breached.[786] In principle, pursuant to Section 442 (1) sentence 1 BGB, the rights of the buyer (including an AI system) due to a defect are excluded if the buyer is aware of the defect at the time of conclusion of the contract. A seller is only obliged to inquire with the manufacturer about the properties of the purchased item if he has or must have doubts about the suitability of the goods for the buyer's intended use based on concrete indications.[787] This also applies if, pursuant to Section 442 (1) sentence 2 BGB, the buyer was unaware of a defect due to gross negligence. The seller of an AI system is obliged to determine the wishes and expectations of the customer; any ambiguity is at the expense of the supplier.[788] The seller is also obliged to point out restrictions on use (in this case: unsuitable hardware on the part of the user).[789] In addition, information on possible capacity problems must be provided. [790]

As a rule, the buyer cannot pass on the economic consequences of the realization of a risk to the seller by asking him for advice on the object of purchase. [791] In principle, the risk of use lies with the buyer, unless it is a case of liability for defects. In practice, this means that the buyer must decide for themselves whether the AI system they have purchased is suitable for the activities planned by the buyer. A different assumption must be made if the specifications, performance description, or product description state that the AI system is intended for use in

785 *Hoeren*, IT Legal Script, as of Oct. 2018, p. 181.
786 *Stoffels,* AGB-Recht (Terms and Conditions Law), 5th edition, 2024, margin number 982.
787 Federal Court of Justice, June 16, 2004, VIII ZR 303/03, NJW 2004, 2301= WM 2004, 1489.
788 Regional Court of Arnsberg, DV-Rechtsprechung (IT case law) Vol. 2, 99.
789 Higher Regional Courtof Celle, February 26, 1986 – 6 U 154/84, CR 1988, 305.
790 Regional Court of Cologne, February 19, 1986 – 23 O 450/83, CR 1987, 508.
791 *Hoeren,* IT Rechtskript, as of Oct. 2018, p. 181.

planned applications are described in detail. If the buyer can prove that the supplier negligently failed to inform them of circumstances relevant to the contract before the contract was concluded, they have several options. They can withdraw from the contract,[792] claim compensation for their useless expenses, or keep the AI system and demand a lower price.[793]

Claims under Section 280 (1) of the German Civil Code (BGB) are subject to the general limitation period set out in Section 199 of the BGB. However, a shorter (two-year) limitation period applies in accordance with Section 438 of the BGB if the damage is directly related to material defects.[794] Pursuant to Section 249 sentence 1 BGB, a debtor who is obliged to pay damages must restore the situation that would have existed if the circumstance giving rise to the obligation to pay damages had not occurred. In doing so, the injuring party must compensate for all damage caused by the result giving rise to the obligation to pay damages (so-called *total compensation*).[795] In addition to the rule of total compensation, § 249 sentence 1 BGB expresses another principle of tort law, namely the principle of restoration or replacement in kind. Here, the tortfeasor must restore in money the condition that would have existed without the damaging event.

g) Obligations and technical standards

Determining contractual obligations that are not expressly described is extremely difficult in the case of AI technologies, especially when it comes to the interaction of complex technical systems and humans (so-called interface-collaborating robots).[796] Obligations that are not described in the contract are largely determined by the state of scientific and technical knowledge. In this context, case law often refers to the categories of "recognized rules of technology," "state of the art," and "state of science and

[792] Federal Court of Justice, January 16, 1985 – VIII ZR 317/83, NJW 1985, 1771= WM 1985, 463.

[793] Federal Court of Justice, December 8, 1989 – V ZR 259/87, NJW 1990, 1661; Federal Court of Justice, December 17, 1987 – 4 StR 440/87, NJW- RR 1990, 1335.

[794] Federal Court of Justice, November 21, 1989 – VI ZR 350/88= NJW 1990, 908; MDR 1990, 531; VersR 1990, 204; WM 1990, 564; BB 1990, 445.

[795] *Brox/Walker,* Schuldrecht AT (Law of Obligations), 36th edition, 2012, margin number 585.

[796] *Spindler*, CR 2015, 766 to 776.

t e c h n o l o g y , ”[797] without explaining these terms in more detail, which in practice means that these terms are meaningless. The specific risk potential of a product is decisive for determining obligations. [798] This certainly needs to be considered very differently for AI technologies. For example, a robot certainly poses a greater liability risk for personal injury than an algorithm, although in the medical field, algorithms can give rise to other liability risks. The lower limit of the duty of care is formed by the recognized rules of technology, i.e., the rules known and recognized as correct in the circles of the relevant technicians, which have been tested in practice, disseminated there, and proven.[799]In practice, this is often determined by an expert, which can of course end in a dispute between experts and ultimately result in a settlement. In principle, the duty of care is limited by the state of science and technology[800] which reflects the achievable results of the latest scientific research and engineering experience, the acceptance of which by the majority of practitioners is still pending.[801]While in product liability the manufacturer is not liable for risks that were unforeseeable at the time the product was placed on the market (development errors), [802] the operator is obliged to adapt safety precautions to new findings at all times.[803] This applies in particular to AI technologies.

797 Federal Court of Justice, April 20, 1971 – VI ZR 232/69, NJW 1971, 1313 (recognized rules of technology); May 17, 1972 – VIII ZR 98/71, DB 1972, 1335 (state of technology); 17.03.1981 – VI ZR 191/79, BGHZ 80, 186 = NJW 1981, 1603 (state of science and technology); Detailed information on the distinction between the terms BVerfG, 08.08.1978 – 2 BvL 8/77, BVerfGE 49, 89 = NJW 1979, 359, 362; *Foerste,* in: Foerste/v. Westphalen, Product Liability Handbook, 3rd edition 2012, Section 24, margin number 17 et seq. with further references.

798 For details, *see Finke*, Die Auswirkungen der europäischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht (The Effects of European Standards and Safety Law on National Liability Law), 2001, p. 9 ff.; *Foerste,* in: Foerste./v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 24 Rn. 37

799 *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, Section 24, margin number 22; *Wilrich*, GPSG, 2004, Section 2 GPSG, margin number 107; *Vieweg,* in: Schulte, Handbook of Technology Law, 2nd edition, 2010, p. 353.

800 *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, Section 24, margin number 20 et seq.; *Spindler*, Unternehmensorganisationspflichten (Corporate Organizational Obligations), (Corporate Organization Obligations), 2nd edition 2011, p. 796; see also: *Weisser/Färber*, MMR 2015, 506, 511.

801 Federal Constitutional Court, August 8, 1978 – 2 BvL 8/77, BVerfGE 49, 89, NJW 1979, 359, 362; OLG Cologne, May 6, 1991 – 12 U 130/88, NJW-RR 1991, 1077, 1079; *Marburger*, Die Regeln der Technik im Recht (The Rules of Technology in Law), 1974, p. 164 et seq.; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, Section 24, marginal number 16.

802B G H , June 16, 2009 – VI ZR 107/08, BGHZ 181, 253, 265 marginal no. 28= BB 2009, 1884, 1888; *Spindler,* in: BeckOGK/BGB, § 823 marginal no. 589; *Wagner*, in: MünchKomm/BGB, 6th ed. 2013, § 823 marginal no. 654 et seq.; *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd ed. 2012, § 24 marginal no. 20, 103 et seq.

803 Regarding the obligation of a statutory nursing care insurance fund to avert dangers caused by defective hospital beds: Federal Court of Justice, December 16, 2008 – VI ZR 170/07, BGHZ 179, 157, 163 ff., margin number 16 ff.; based on the individual case: *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition 2012, § 27 margin note 14 et seq.

Technical standards are of paramount importance for defining these vague legal concepts and thus specifying the obligations in tortious liability for the use of technologies, particularly in the area of product liability. They are laid down in inter-company technical standards, such as DIN, CEN, or ISO standards, but also in other sets of rules, such as hazard prevention rules in the context of occupational safety. [804] In addition, the obligations arising from the ProdSG can be specified in more detail.[805] In addition, the literature argues that the regulations are used as a basis by the courts in the same way as legal norms. [806] These standards usually constitute prima facie evidence of compliance with safety obligations, even if stricter requirements may be imposed in individual cases involving particular hazards.[807] Reference to certifications or TÜV approvals cannot generally relieve either the operator or the manufacturer of their liability. [808] Finding the right standards for AI technologies appears to be very difficult, and opinions on the matter vary widely. There are no real standards for the development of algorithms, but there are standards for the development of other AI systems. For example, ISO standards are being prepared at the level of so-called collaborative robots (at the interface with humans) that deal with specific safety rules.[809] The technical standards IEC 61508 and DIN ISO 26262 are particularly important for autonomous driving and self-driving cars. [810] Although technical standards (and protective laws) may outline liability risks, skepticism remains because the systems

804 *Spindler*, CR 2015, 766 to 776.

805 *Wagner,* in: MünchKomm/BGB, 6th edition, 2013, Section 823, margin number 651.

806 *Foerste, in:* Foerste/v. Westphalen, Produkthaftungshandbuch (Product Liability Handbook), 3rd edition, 2012, § 24 margin number 42 footnote 120 with reference to OLG Celle, October 10, 2005 – 7 U 155/05, VersR 2007, 253.

807 For details, see *Spindler*, in: BeckOGK/BGB, § 823 margin note 389, margin note 584 et seq.; *Spindler*, Responsibilities of IT Manufacturers, Users, and Intermediaries, 2007, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gut-achten_pdf.pdf? blob=publicationFile&v=2, margin note 144 (last accessed on: November 20, 2015).; Federal Court of Justice, May 14, 1998 – VII ZR 184/97, NJW 1998, 2814, 2815; September 27, 1994 – VI ZR 150/93, NJW 1994, 3349, 3350; LG Berlin, MDR 1997, 246, 247.

808 In-depth *Spindler*, Responsibilities of IT manufacturers, users and intermediaries, 2007, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf? blob=publicationFile&v=2, para. 145 ff. (last accessed on: 20.11.2015).; BGH, 09.01.1990 – VI ZR 103/89, CR 1990, 402 = NJW-RR 1990, 406 f.; see also OLG Celle, May 28, 2003 – 9 U 7/03, NJW 2003, 2544, 2545.

809 ISO/TS 15066 "Robots and robotic devices – Safety requirements for industrial robots – Industrial collaborative workspace"; also in preparation: ISO/DIS 13482 "Robots and robotic devices – Safety requirements for non-industrial robots – Non-medical personal care robot"; already existing in general for industrial robots: ISO 10218-1 "Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots" and ISO 10218-2 "Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration".

810 *Jänich/Schrader/Reck*, NZV 2015, 313, 316 f.; *Lutz/Tang/Lienkamp*, NZV 2013, 57, 61.

are complex and constantly subject to innovation,[811] but this does not negate the need to define standards that can serve as benchmarks, not only with regard to duty programs, but also in the area of strict liability for AI technologies, for example when it comes to the question of development errors. [812]

h) Types of damage

As a rule, personal injury refers to the types of damage to persons specified in Section 823 (1) sentence 1 BGB, namely life, body, health, and freedom. The terms "bodily injury" and "injury to health" are to be interpreted broadly. They include any impairment of physical, mental, or emotional integrity.[813] The right to one's own body is a legally defined element of general personal rights,[814] which is not protected by Section 253(2) of the German Civil Code (BGB). Its violation can only give rise to a claim for compensation for pain and suffering in serious cases.[815] Such a claim cannot be derived from Section 253(2) BGB, but only from Sectionhttp://rsw.beck.de/bib/bin/refe-rence.asp?Y=100CG=BGBCP=823823http://rsw.beck.de/bib/bin/refe-rence.asp?Y=100CG=BGBCP=823 para. 1 BGB in conjunction with Art. 1 para. 1, 2 para. 1 GG, [816] such as in cases of serious defamation, e.g. in the case of unfounded or even malicious exposure or disparagement of a person in public;[817] in the case of repeated and persistent violation of the right to one's own image. [818] Bodily injury is any unauthorized interference with physical well-being. [819] Interference is any physical, mental, or emotional process of life, even if the injured party has not yet been born.

---

811 So *Hanisch,* in: Hilgendorf (ed.), Robotics in the Context of Law and Morality, 2014, p. 27, 35.

812 *Spindler*, CR 2015, 766 to 776.

813 *Büchting/Heussen,* Beck's Legal Handbook, 10th edition, 2011, C.13 Tortious Liability, margin numbers 15 to 18.

814 Federal Court of Justice, November 9, 1993 – VI ZR 62/93= BGHZ 124, 52; NJW 1994, 127; NJW-RR 1994, 286 (Ls.); MDR 1994, 140; FamRZ 1994, 154; VersR 1994, 55; JR 1995, 21.

815 *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch (Beck's Handbook for Lawyers), 10th edition, 2011, C.13 Tortious Liability, margin numbers 15 to 18.

816 Federal Court of Justice, December 1, 1999 – I ZR 49/97= BGHZ 143, 214; NJW 2000, 2195; NJW-RR 2000, 1211 (Ls.); MDR 2000, 1147; GRUR 2000, 709; FamRZ 2000, 1080; VersR 2000, 1154; WM 2000, 1449; ZUM 2000, 582; afp 2000, 356.

817 Federal Constitutional Court, March 8, 2000 – 1 BvR 1127/96= NJW 2000, 2187; MDR 2000, 829; FamRZ 2000, 943; VersR 2000, 897; VersR 2000, 1114; ZUM 2000, 947; Federal Court of Justice, November 15, 1994 - VI ZR 56/94= BGHZ 128, 1; NJW 1995, 861; MDR 1995, 804; GRUR 1995, 224; VersR 1995, 305; WM 1995, 542; DB 1995, 1607; afp 1995, 411.

818 Federal Court of Justice, December 12, 1995 – VI ZR 223/94= NJW 1996, 985; MDR 1996, 365; GRUR 1996, 227; VersR 1996, 341; ZUM 1996, 243; afp 1996, 138.

819 *Palandt/Thomas*, 77th ed. 2017, § 823 marginal no. 4.

In these cases, pursuant to Section 253(2) of the German Civil Code (BGB), "fair compensation in money," referred to as compensation for pain and suffering, must also be paid for non-pecuniary damage that is not financial loss, regardless of the legal basis — tort, strict liability, or contract — for the violation of the legal interests specified in Section 253(2) BGB. [821] Unlike Section 823(1) BGB, Section 253(2) BGB does not mention life here. Therefore, no compensation for pain and suffering is payable if death occurs immediately as a result of the injury. [822] Section 253(2) BGB also does not grant compensation for pain and suffering for every minor matter.[823] Appropriate "reasonable" compensation in money must be paid, i.e., in the case of minor health injuries without significant impairment—minor damages—there is no claim for compensation for pain and suffering if compensation in money appears unreasonable.[824] The extent of the pain suffered can be proven by the testimony of family members of the injured party, by treating physicians, medical records, prescribed medications, and painkillers.[825] Liability for personal injury may play a role primarily in connection with AI implants in cyborgs or if autonomous vehicles injure a pedestrian or another driver, for example. In the latter case, the liability principles for autonomous driving apply (see Chapter I). If a defective AI implant causes personal injury, the restoration costs in the event of injury to a person consist primarily of the costs of medical treatment. [826] Personal injury within the meaning of insurance law according to

Section 1 (1) AHB is based on the terms "life, body, health" protected in Section 823 (1) BGB. The right to freedom and the general right of personality are not covered by the concept of personal injury. [827] Damage to health includes both physical and psychological impairment. [828]

---

[820] BGH, January 11, 1972 - VI ZR 46/71= BGHZ 58, 48; BGHZ 58, 487; NJW 1972, 1126; MDR 1972, 406; VersR 1972, 372; DB 1972, 433; JR 1972, 242; Federal Court of Justice, April 30, 1991 - VI ZR 178/90= BGHZ 114, 284; NJW 1991, 1948; MDR 1991, 728; FamRZ 1991, 918; VersR 1991, 816.

[821] *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch (Beck's Handbook for Lawyers), 10th edition, 2011, C.13 Tortious Liability, margin numbers 15 to 18.

[822] A transferable and inheritable claim for compensation for pain and suffering presupposes that the deceased felt the injuries inflicted on them. Due to the short time between the damaging event and death, the process of dying must not be so prominent that an immaterial impairment caused by the bodily injury as such is not tangible and, consequently, fairness does not require compensation in money, according to the Federal Court of Justice (BGH), 12.05.1998 - VI ZR 182/97= BGHZ 138, 388; NJW 1998, 2741; ZIP 1998, 1272; MDR 1998, 1029; NZV
1998, 370; NJ 1999, 35; VersR 1998, 1034; DB 1998, 2321 (Ls.), likewise KG, October 30, 2000 - 12 U 5120/99= NZV 2002, 38.

[823] See also *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch, 12th ed. 2022, C.13 tortious liability, paras. 15 to 18.

[824] Federal Court of Justice, January 14, 1992 - VI ZR 120/91= NJW 1992, 1043; NJW-RR 1992, 1182 (Ls.); MDR 1992, 349; ZMR 1992, 189; VersR 1992, 504; DB 1992, 1237.

[825] Federal Court of Justice, October 1, 1985 – VI ZR 19/84= NJW 1986, 1541; NJW-RR 1986, 702 (Ls.); VersR 1986, 183.

[826] *Palandt/Heinrichs*, 77th ed. 2017, § 249 marginal no. 8.

[827] *Späte,* Commentary on the General Insurance Conditions for Liability Insurance, 1993, § 1 AHB margin no. 49.

[828] *Pröless,* in: Pröless/Martin, Insurance Contract Act, 28th ed. 2010, § 1 AHB margin no. 15.

As long as no specific liability concepts for damage caused by AI systems are standardized by law, practice must fall back on the liability regulations that have been in force to date. If employees are involved in the damage, special provisions of labor and social law must be observed. If an autonomous system causes damage to an employee's health and it can be proven that the employer or another employee is at fault, the liability privileges of Sections 104 et seq. of SGB VII apply. If the employee has (contributed to) causing the damage, the principles of internal compensation apply. Depending on the degree of fault, the employee may not be liable to the employer in the internal relationship or may only be liable to a limited extent.[829]

The use of AI systems, e.g., in autonomous driving, can result in property damage. In the case of property damage, a distinction is made between destruction and damage to the property. This follows from Section 249 (2) of the German Civil Code (BGB), which grants a claim for compensation for manufacturing costs only in the event of damage. [830] The difference between destruction and damage is based on the existence of an item that can be repaired (which is only the case with damage). However, an item cannot be repaired

- if the damage is so severe that repair is technically impossible (technical total loss).
- if a technically feasible repair is disproportionately expensive, the injuring party refuses to carry it out in accordance with Section 251 (2) sentence 1 and compensates the injured party in cash (economic total loss)[831]
- if a repair is technically possible and economically viable, but unreasonable for the injured party. This is the case, for example, if a new or

[829] *Günther/Böglmüller*, BB 2017, 53 to 58.

[830] *Brox/Walker,* Schuldrecht AT, 36th ed. 2012, para. 617.

[831] Case law regularly affirms such disproportion when the repair costs exceed the replacement value by at least 30%. BGH, October 15, 1991 - VI ZR 314/90= BGHZ 115, 364; NJW 1992, 302; MDR 1992, 131; NZV 1992, 66; VersR 1992, 61; BB 1992, 20; DB 1992, 209.

almost new car [832] has been damaged to such an extent that it would have to be classified as an accident vehicle after repair (non-actual total loss). [833]

If production is not possible or is insufficient to compensate the creditor, the party liable for compensation must compensate the creditor in cash in accordance with Section 251 (1) of the German Civil Code (BGB) (so-called value interest). The value interest generally consists of the so-called current market value. The current market value is the amount that the injured party could have obtained by selling the item immediately before the damage occurred. [834] If an item is only damaged, the injured party may demand the amount of money required for the repair pursuant to Section 249 sentence 2 BGB. According to prevailing opinion, it is irrelevant whether the injured party actually uses the amount for the repair or not.[836] According to property insurance law, any impairment of the substance that reduces the value or usability of an item through physical or chemical effects constitutes damage. [837] According to § 90 BGB, items are all physical objects.

The category of financial losses can be particularly costly for manufacturers of AI systems, especially when considering cases in high-frequency trading. The failure of such a trading system for just a few hours can lead to significant financial losses. In this case, the customer does not suffer any property damage, as the value of the AI system has not deteriorated and the defective AI system has not caused physical damage to another economic asset. Rather, the customer will have suffered a financial loss due to the unusability of the high-frequency trading system.

[832] This is regularly assumed by case law up to a mileage of 1,000 km, cf. BGH, March 29, 1983 - VI ZR 157/81= VersR 1983, 658.

[833] *Palandt/Heinrichs*, 77th edition, 2017, Section 249, marginal number 23.

[834] *Brox/Walker,* Schuldrecht AT (Law of Obligations), 36th edition, 2012, margin number 621.

[835] B G H , November 6, 1986 - VII ZR 97/85= BGHZ 99, 81; BGHZ 99, 82; NJW 1987, 645; NJW 1987, 3097; NJW-RR 1987, 337 (Ls.); MDR 1987, 309; WM 1987, 260; BB 1987, 365; DB 1987, 529; BauR 1987, 89; ZfBR 1993, 231; ZfBR 1992, 25; ZfBR 1990, 184; ZfBR 1987, 93; Federal Court of Justice, June 20, 1989 - VI ZR 334/88= NJW 1989, 3009; NJW-RR 1990, 37 (Ls.); MDR 1990, 41; NZV 1989, 465; VersR 1989, 1056; BB 1989, 1719; BGH, June 30, 1997 - II ZR 186/96= NJW 1997, 2879; MDR 1997, 938; MDR 1997, 948; VersR 1997, 1287; WM 1997, 1813; BB 1997, 2187; BauR 1997, 866; IBR 1997, 456.

[836] *Grunsky*, NJW 1983, 2465.

[837] *Martin*, Property Insurance Law, 4th edition, 2022, Section B III, margin number 4.

It is not always easy to differentiate between property damage and financial loss. Various theories have been developed to distinguish between the two categories of damage. [838] The *"doctrine of interest"* [839] which forms the essential basis for calculating damages. [840] According to this doctrine, financial loss is the "difference between the amount of a person's assets at a given point in time and the amount that these assets would have had without the occurrence of a damaging event." The actual financial situation of the person entitled to compensation after the damaging event must be compared with the hypothetical situation that would have existed if the infringement of legal rights had not occurred (so-called *difference in damages)*.[841] Financial losses are primarily reflected in business interruption, delay, and lost profits.

Financial losses are losses of property and other monetary assets that can be measured in money and reduce the assets of the injured party. [842] They must be compensated either by restoring the situation to its original state in accordance with Section 249 of the German Civil Code (BGB) or by providing compensation for the loss in value.[843] The damaging event has resulted in a monetary expenditure of labor and a prevented monetary performance of work. [844] Unlike bodily injury and property damage, pure financial losses are variable quantities that may continue to develop until full compensation has been paid or the final oral hearing in the damages proceedings has taken place.[845] Since financial loss is calculated on the basis of how the injured party's assets would have developed without the damaging event, reserve causes must also be taken into account. [846] Therefore, after premature termination of the contract by termination without notice, compensation is limited in time to the agreed

[838] *Jauernig,* Commentary on the German Civil Code (BGB), 7th edition, 2010, before §§ 249-253 margin note 3.

[839] Federal Court of Justice, June 6, 1997 – V ZR 115/96 = BGHZ 136, 52; NJW 1997, 2378; ZIP 1997, 1378; MDR 1997, 924; DNotZ 1998, 60; WM 1997, 1671; BB 1997, 1657; DB 1997, 2018.

[840] Criticism by *Schermaier, JZ* 98, 857.

[841] *Palandt/Heinrichs*, 77th edition, 2017, before § 249 margin note 8, 9.; *Jauernig,* Commentary on the German Civil Code, 7th edition, 2010, before §§ 249-253 margin note 5.

[842] *Schellhammer*, Law of Obligations According to the Basis of Claims, 8th edition 2011, margin number 1269.

[843] Federal Court of Justice, July 18, 2008 - V ZR 71/07= NJW 2008, 3059; MDR 2008, 1263; NZM 2008, 819; WM 2008, 1798; IMR 2008, 357.

[844] Federal Court of Justice, November 24, 1995 - V ZR 88/95= BGHZ 131, 220; NJW 1996, 921; ZIP 1996, 281; MDR 1996, 1112; DNotZ 1996, 441; WM 1996, 599; BB 1996, 658; DB 1996, 1514; JR 1996, 455

[845] *Schellhammer*, Law of Obligations According to the Basis of Claims, 8th edition, 2011, margin number 1308.

[846] Federal Court of Justice, May 13, 1953 – VI ZR 5/52= BGHZ 10, 6; NJW 1953, 977; Federal Court of Justice, March 14, 1985 – IX ZR 26/84 Loss of earnings= NJW 1986, 1329; NJW-RR 1986, 650 (Ls.); ZIP 1985, 1143; MDR 1985, 577; WM 1985, 666; BGH, April 9, 1991 - XI ZR 136/90 Additional tax burden = NJW 1991, 1881; NJW-RR 1991, 1398 (Ls.); ZIP 1991, 644; MDR 1991, 761; VersR 1991, 888; WM 1991, 890; BB 1991, 2181; DB 1991, 1621.

end of contract or next termination date. [847]The unpleasant conclusion of the contract, on the other hand, only constitutes financial loss if it is economically disadvantageous. [848]

The general provisions of Sections 280, 281, 283, and 311a of the German Civil Code (BGB) provide a uniform basis for claims for all types of damage. Under the conditions set out in Section 280 BGB, the creditor may demand compensation for "close," i.e., direct or remote, consequential damage (indirect damage). The only prerequisite is that the contractor has breached an obligation and is responsible for this breach. The manufacturer is therefore liable for damage caused by defects in the same way as for consequential damage, as it owes freedom from defects as part of its performance obligations. [849] Any breach of this obligation renders it liable for compensation for both types of damage.[850] This means that the manufacturer can already be liable for damages if he negligently delivers defective products, whereby defects in the product itself (damage caused by defects) now also give rise to liability (Section 281 in conjunction with Section 280 (1) BGB for breach of duty), as well as consequential damage caused by defects (directly from Section 280 (1) BGB), even if the customer withdraws from the contract. [851] Compensation for damages instead of performance (previously: compensation for non-performance) is based on the positive interest, which is why the customer must be placed in the position they would have been in if the contract had been properly fulfilled.[852] Liability for damage caused by defects follows from Sections 281 and 283 BGB [853] and includes (unchanged in meaning) repair costs, [854] expert costs related to the determination of defects, [855] remaining reduction in value,[856] loss of use during repair and loss of profit [857] as well as operating loss due to delays

[847] Federal Court of Justice 82, 121; 95, 39; 104, 337; NJW 93, 1386.

[848] Federal Court of Justice, September 26, 1997 – V ZR 29/96= NJW 1998, 302; ZIP 1998, 154; MDR 1998, 25; DNotZ 1998, 349; NZM 1998, 167 (Ls.); ZMR 1998, 79; VersR 1998, 905; WM 1997, 2309; BB 1997, 2553; IBR 1998, 124; BauR 1998, 196 (Ls.).

[849] Explanatory memorandum to the Law on the Modernization of the Law of Obligations, BT-Drs. 14/6040, 224.

[850] See *v. Westphalen*, DB 2001, 799, 802.

[851] *Koch,* Computer Contract Law, 6th edition, 2002, margin note 1346.

[852] *Boerner*, ZIP 2001, 2264, 2272.

[853] Explanatory memorandum to the Law on the Modernization of the Law of Obligations, BT-Drs. 14/6040, 224.

[854] *Schellhammer*, Law of Obligations According to the Basis of Claims, 8th ed. 2011, margin no. 1269.

[855] Federal Court of Justice, July 5, 1978 - VIII ZR 172/77= NJW 1978, 2241; MDR 1979, 133; WM 1978, 1172; BB 1978, 1491; DB 1978, 1878; JR 1979, 199.

[856] *Palandt/Heinrichs*, 77th ed. 2017, § 276 marginal no. 110.

[857] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 8th edition, 2011, margin number 1269.

Commissioning. [858] Liability for consequential damages arises from Section 280 (1) BGB [859] and includes damage to other legal interests of the buyer. This may now also include financial losses caused by an incorrectly calculating algorithm of the AI system.[860] As already explained, warranty rights in contracts between merchants can generally be limited.

Liability clauses often differentiate between direct and indirect damage (consequential damage).[861] For example, US manufacturers often agree to a general exclusion for indirect damages in contracts governed by German law.[862] Since many providers of AI technologies are based in the US, incidental/consequential damages are also often excluded in German contracts for AI systems.

First of all, it is questionable whether a distinction can be made between direct and indirect damages. No distinction between direct and indirect damages can be found in the central provisions on damages in the BGB. The historical legislator deliberately refrained from using these terms, as no generally accepted definition has emerged.[863] As already explained above, all direct and indirect damages incurred must be adequately compensated. [864] However, approaches to differentiating between direct and indirect damages can be found in case law. At least before the reform of the law of obligations, this differentiation played a role in various areas of law (e.g., sales law, contract law including VOB/B construction contract law, insurance law, and transport law). The highest courts have clarified the concepts of direct and indirect

[858] Explanatory memorandum to the Law on the Modernization of the Law of Obligations, BT-Drs. 14/6040, 224, 224: Claim already exists under Section 280(1) BGB, as amended, regardless of the conditions for default under Section 281(1) BGB, as amended, including a claim for reimbursement of legal costs.

[859] Explanatory memorandum to the Law on the Modernization of the Law of Obligations, BT-Drs. 14/6040, 224, 224.

[860] *Koch,* Computer Contract Law, 7th ed. 2009, margin no. 1347.

[861] *Funk/Wenn*, CR 2004, 481.

[862] On the effectiveness of such liability exclusions under the Uniform Commercial Code, see, for example, M. A: Mortenson v. Timberline Software Corporation, Supreme Court of Washington (140 Wash. 2.d. 568, 998 P.2d 305).

[863] *Oetker,* in: MüKo/BGB, 4th edition, §249 margin number 97.

[864] See also *Schiemann,* in: Staudinger, BGB 13th edition, preliminary remarks on §§ 249 ff; *Oetker*, in: MüKo/BGB, 4th edition, § 249 margin note 94.

damage has been understood very differently in the past. [865] In a large number of decisions, a distinction is made between whether the damage occurred "directly" to the subject matter of the contract or to other legal interests of the injured party.[866] According to case law, it is generally irrelevant whether the damaging event caused the damage to the subject matter of the contract directly or only indirectly. According to case law, direct damage is exclusively damage which, in the case of contractual liability, is inherent in the subject matter of the contract itself or, in the case of tortious liability, occurs to a protected legal interest. [867] Losses to other assets are understood as indirect damage.[868]

The distinction between direct and indirect damage is reflected in the differentiation between damage caused by defects and consequential damage caused by defects[869], whereby in the law governing contracts for work and services, a further distinction is made between direct and indirect consequential damage caused by defects. Case law has classified as damage caused by defects all damage that is "directly" attributable to the subject matter of the contract because it is unusable, worthless, or of reduced value as a result of the defect.[870] In addition, the costs of determining the defect[871] and the loss of profit were also attributed to the damage caused by defects.[872] otherwise, lost profits are regularly classified by case law and literature as merely "indirect damage." Case law understood direct consequential damage to be all damage that is "closely and directly" related to the defect in terms of time and space and does not belong to the group of damage caused by defects. [873]

[865] *Funk/Wenn*, CR 2004, 484.

[866] See Federal Court of Justice, September 30, 1957 – III ZR 76/56, BGHZ 25, 340 ff.; December 8, 1981 – VI ZR 153/80, MDR 1982, 398= NJW 1982, 827, 829 f.; OLG Düsseldorf, February 18, 2002 – 1 U 91/01, Schaden-Praxis 2002, 245 ff.

[867] To justify this understanding of the term, case law refers in particular to a (supposedly) corresponding use of these terms in general legal language; see *Funk/Wenn*, CR 2004, 484.

[868] See the definition of indirect damage in the Munich Legal Dictionary, Munich 1997, keyword "Mittelbaren Schaden" (indirect damage); BGH, December 11, 2002 – IV ZR 226/01, MDR 2003,389= BGH Report 2003, 319= NJW 2003, 826, 828; *Oetker,* in: Münchener Kommentar zum Civil Code, Vol. 2: Law of Obligations, General Part, 7th edition 2015, § 249 marginal no. 96.

[869] *Funk/Wenn,* CR 2004, 484.

[870] *Peters,* in: Staudinger, BGB 13th ed. § 635 (old version) margin no. 55.

[871] Federal Court of Justice, February 18, 2002 – II ZR 355/00 = NJW 2002, 2553; ZIP 2002, 895; ZIP 2002, 859; MDR 2002, 820; WM 2002, 909; DB 2002, 999; *Soergel*, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch (Munich Commentary on the Civil Code) Vol. 5/1: Law of Obligations, Special Part III/1, 7th edition 2017, § 635 (old version) marginal number 33.

[872] *Honsell,* in: Staudinger, BGB 13th ed. § 463 (old version) marginal no. 48 ff; *Soergel,* in: Münchener Kommentar zum Bürgerlichen Gesetzbuch (Munich Commentary on the Civil Code) Vol. 5/1: Law of Obligations, Special Part III/1, 7th edition 2017, § 635 (old version) marginal no. 39 with further references.

[873] *Peters,* in: Staudinger, BGB 13th edition, § 635 (old version) margin note 55.

According to the Federal Court of Justice (BGH) in its 1994 ruling, the term "direct damage" refers to all damage that "can be expected to occur in the normal course of events."[874] For the Federal Court of Justice this understanding of the term "direct damage" follows from the principle of "interpretation in the interests of both parties" [875] and is justified by the legitimate expectation of the contractual partner that the contractual obligations of the contractual partners will not be effectively undermined by the liability provision. In contrast, the Federal Court of Justice considers the interest of the contractual partner in limiting the potential damage, which is difficult for it to calculate, to be of secondary importance.[876] The possible and, if applicable, uncertain amount of damage is not a decisive criterion for determining whether the damage is direct or indirect, according to the Federal Court of Justice.[877]

In principle, the debtor is liable for intent and negligence pursuant to Section 276 (1) sentence 1. As already discussed, in individual cases, strict liability may also apply if this arises from the law or is specifically agreed in the contract (guarantee agreement).[878] If the debtor is not responsible for such no-fault liability, they are not liable unless they are responsible for intent or negligence, cf. Section 276 BGB. [879] This is unlikely to be the case in cases of force majeure. Force majeure generally includes "*war, natural disasters, terrorist attacks, demonstrations, and strikes*." However, strikes must always be considered on a case-by-case basis to determine whether they were provoked intentionally or negligently. Some contracts repeatedly contain liability provisions that expressly exclude liability for force majeure. This is often based on Anglo-American contract practice, where liability for force majeure may be excluded

[874] B G H , June 8, 1994 - VIII ZR 103/93 = NJW 1994, 2228; MDR 1994, 888; VersR 1994, 1360; WM 1994, 1720; DB 1994, 2073; BauR 1994, 639; ZfBR 1994, 215; IBR 1995, 39.

[875] Federal Court of Justice, July 2, 1992 – I ZR 181/90= NJW-RR 1992, 1386; MDR 1993, 225; VersR 1992, 1395; WM 1992, 2026; BB 1992, 1956; DB 1992, 2495; Federal Court of Justice, June 9, 1993 - VIII ZR 205/92= CR 1994, 347; NJW-RR 1993, 1203; *Mayer-Maly,* in: Münchener Kommentar zum Bürgerlichen Gesetzbuch (Munich Commentary on the Civil Code) Vol. 1: General Part §§ 1-240, ProstG, AGG, 7th edition 2015, § 157 Rn. 6. ff.

[876] *Radio/Wenn*, CR 2004, 485.

[877] B G H , June 8, 1994 - VIII ZR 103/93 = NJW 1994, 2228; MDR 1994, 888; VersR 1994, 1360; WM 1994, 1720; DB 1994, 2073; BauR 1994, 639; ZfBR 1994, 215; IBR 1995, 39.

[878] *Auer-Reinsdorff*, ITRB 2006, 181.

[879] *Palandt/Grüneberg*, BGB, 72nd ed. 2013, § 276 margin no. 2.

must be explicitly excluded, otherwise the debtor shall be liable for force majeure. The burden of proof for force majeure as the cause of damage lies with the operator, analogous to the owner of a motor vehicle. [880]

Liability for lost profits is particularly important in AI technologies such as algorithmic trading, as particularly high liability claims can arise here. Liability for lost profits is explicitly regulated in Section 252 of the German Civil Code (BGB). According to Section 252 (1) BGB, the damages to be compensated also include lost profits, e.g., the margin in high-frequency trading. According to Section 252 sentence 2 BGB, the profit is deemed to have been lost which could have been expected with probability according to the usual course of events or according to the special circumstances, in particular according to the arrangements and precautions taken. In this case, § 288 BGB and § 376 (2) HGB calculate the lost profit as minimum damages in the abstract and without regard to the individual case. [881] Furthermore, only merchants may calculate their loss of profit in the abstract and only for transactions in the course of their business.[882] In this case, abstract means that the merchant simply calculates his usual profit margin. In commercial transactions and e-commerce where algorithms are used, it is assumed that the buyer would have resold the goods at a profit[883] and that the seller would also have sold the goods elsewhere at a profit.[884] Neither does the injured party have to prove that they had a buyer,[885] nor may the injuring party object that the damage was caused by a covering transaction.

[880] Federal Court of Justice, July 11, 1972 – VI ZR 86/71= NJW 1972, 1808; MDR 1972, 1023; VersR 1972, 1074.

[881] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 11th edition, 2021, margin number 1280.

[882] Federal Court of Justice, February 22, 1989 - VIII ZR 45/88= BGHZ 107, 67; NJW 1989, 1669; NJW-RR 1989, 1073 (Ls.); ZIP 1989, 450; MDR 1989, 628; WM 1989, 645; BB 1989, 798; DB 1989, 973; Federal Court of Justice, October 8, 1991 - XI ZR 259/90= BGHZ 115, 268; NJW 1992, 109; ZIP 1991, 1479; MDR 1992, 151; WM 1991, 1983; BB 1991, 2396; DB 1992, 473; BGH, June 29, 1994 - VIII ZR 317/93= BGHZ 126, 305; NJW 1994, 2478; ZIP 1994, 1362; MDR 1994, 1085; WM 1994, 1632; BB 1994, 2029; DB 1994, 2184; BGH, 02.12.1994 - V ZR 193/93 not fundamental = NJW 1995, 587; NJW-RR 1995, 848 (Ls.); ZIP 1995, 220; MDR 1995, 462; DNotZ 1995, 393; WM 1995, 339; WM 1995, 123; BB 1995, 588; DB 1995, 521; ZfBR 1995, 81; IBR 1995, 183; BGH, May 3, 1995 - XI ZR 195/94= NJW 1995, 1954; ZIP 1995, 909; MDR 1995, 705; WM 1995, 1055; BB 1995, 1508; DB 1995, 1509.

[883] Federal Court of Justice, June 29, 1994 - VIII ZR 317/93= BGHZ 126, 305; NJW 1994, 2478; ZIP 1994, 1362; MDR 1994, 1085; WM 1994, 1632; BB 1994, 2029; DB 1994, 2184; Federal Court of Justice, December 22, 1999 - VIII ZR 135/99 = NJW 2000, 1409; ZIP 2000, 892; MDR 2000, 511; WM 2000, 537; BB 2000, 1110; DB 2000, 1505.

[884] Federal Court of Justice, March 2, 1988 - VIII ZR 380/86= NJW 1988, 2234; NJW-RR 1988, 1182 (Ls.); ZIP 1988, 505; MDR 1988, 668; WM 1988, 781; BB 1988, 929; DB 1988, 1060M; Federal Court of Justice, June 29, 1994 - VIII ZR 3 1 7 / 9 3 = BGHZ 126, 305; NJW 1994, 2478; ZIP 1994, 1362; MDR 1994, 1085; WM 1994, 1632; BB 1994, 2029; DB 1994, 2184; Federal Court of Justice (BGH), December 22, 1999 - VIII ZR 135/99= NJW 2000, 1409; ZIP 2000, 892; MDR 2000, 511; WM 2000, 537; BB 2000, 1110; DB 2000, 1505.

[885] Federal Court of Justice, March 2, 1988 – VIII ZR 380/86= NJW 1988, 2234; NJW-RR 1988, 1182 (Ls.); ZIP 1988, 505; MDR 1988, 668; WM 1988, 781; BB 1988, 929; DB 1988, 1060M.

[886] The aggrieved bank may calculate its loss of profit in abstract terms on the basis of the gross interest it normally earns on its lending transactions. [887]

As a rule, liability for lost profits represents a considerable risk for the manufacturer, which cannot be covered by risk management or appropriate insurance. The extent to which the management board of a manufacturer of AI technologies is permitted to sign a liability agreement for lost profits is highly questionable, as this may constitute a violation of Section 93 of the German Stock Corporation Act (AktG).

i) Liability limitation

Contractual limitations of liability (disclaimers) are common in German industry and are generally permissible, even for claims arising from tort.[888] Contracts influenced by US law in particular contain an extensive catalog of liability exemptions. [889] An agreement reached before damage occurs prevents the claim for damages from arising at the beginning of the contractual relationship or limits the claim in its origin.[890] The limitation of liability or disclaimer is subject to considerable legal restrictions, in particular within the framework of the general terms and conditions pursuant to Sections 305 et seq. BGB. [891] When considering limitations of liability (disclaimers), a distinction must be made between individual contracts and standard form contracts (general terms and conditions).

The fact that a contractual provision is mandatory in relation to individual agreements is an exception and therefore requires special reasons. There are only two possibilities for this. [892]

[886] OLG Stuttgart, VersR 68, 1074.
[887] See *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations According to the Basis of Claims), 11th ed. 2021, para. 1642.
[888] Federal Court of Justice, April 27, 1953 – III ZR 200/51= BGHZ 9, 295; NJW 1953, 979; *Palandt/Heinrichs*, 72nd ed. 2013, § 276 margin no. 35.
[889] *Fritzemeyer,* in: Lehmann/Meents, Handbook for Specialist Lawyers in Information Technology, 2nd edition 2011, Chapter 2 marginal number 70.
[890] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations According to Claims), 11th edition, 2021, margin number 1642.
[891] *Jauernig,* Commentary on the German Civil Code (BGB), 7th edition, 2010, Section 276, margin number 4.
[892] *Brox/Walker,* Law of Obligations AT, 36th ed. 2012, margin no. 306.

- The law may expressly stipulate the mandatory nature of a provision.[893] The BGB does this in the law of obligations partly in individual provisions (e.g., in §§ 248 para. 1, 276 para. 3, 536 para. 4, 574 para. 4), and partly for entire groups of provisions (e.g., in §§ 312 et seq., 475, 506, 651m BGB).
- If the law does not expressly stipulate that a provision is mandatory, it may well be that such mandatory character arises from the purpose of the provision. In particular, the protective purpose of a provision may preclude it from being waived (see Sections 311b (1), 518, 766 BGB). Due to their protective purpose, provisions of the law of obligations may also be mandatory for other reasons. This applies, for example, to Section 275(1) of the German Civil Code (BGB), which "excludes the claim for performance of an impossible service."[894]

According to Section 276 (1) BGB, the manufacturer and the customer are liable to each other without limitation for intent and negligence. Liability for intent cannot be contractually excluded pursuant to Section 276 (3) BGB (mandatory law)![895] The reverse conclusion from Section 276 (3) BGB allows liability for negligence to be limited in principle. Pursuant to Section 309 No. 7 BGB, this does not apply to general terms and conditions within the meaning of Section 305 (1) BGB. Since, pursuant to Section 305b BGB, individual agreements always take precedence over general terms and conditions, an individually agreed limitation of liability for negligence always applies first.

Various approaches are possible when formulating the clause. On the one hand, liability can be limited to specific categories of damage (**personal injury, property damage, and financial loss**). On the other hand, liability can also be limited to the type of fault (slight or gross negligence; intent is not possible). In this context, liability clauses sometimes contain absolute amounts, but also percentages based on the order value. Liability for personal injury is excluded by law in accordance with Sections 104 et seq. of SGB VII if accident insurance covers personal injury

[893] Particularly binding are the (still not uncommon) provisions outside the BGB that fix the prices of goods or services: usually as maximum prices, but sometimes also as minimum or fixed prices. For an overview, see *Liebing*, BB 1983, 667, corrected for the insurance industry by *Sieg,* BB 983,1187.

[894] A judgment ordering performance would result in a pointless recourse to the state enforcement authorities; instead, the creditor should switch to an enforceable claim for damages in money; *Brox/Walker,* Schuldrecht AT, 36th ed. 2012, para. 89, 363 f.

[895] *Palandt/Heinrichs*, 67th ed. 2008, § 276 marginal no. 35.

exists. In the event of recourse against the party causing the damage (cf. § 110 SGB VII), the social insurance carrier bears the burden of proof for the amount of the fictitious civil law claim for reimbursement. [896]

In the case of **financial losses**, certain areas of financial losses (e.g., business interruption and loss of profits) may also be excluded. [897] The excluded areas of financial losses should also be explicitly excluded in the clause. Liability clauses often differentiate between direct and indirect damage (consequential damage). For example, US AI manufacturers often include a general exclusion for indirect damage in contracts governed by German law.[898] Since many AI manufacturers are of US origin, incidental/consequential damages [899] (indirect damages) are also often excluded in German contracts for AI systems. See in particular the examples in high-frequency trading.

The limitation of liability for statutory claims is always subject to § 14 of the Product Liability Act, which excludes liability for claims under the Product Liability Act. However, liability under the Product Liability Act does not require fault on the part of the liable party, as it is a case of strict liability. [900]

A limitation of the liability amount for **personal injury** (injury to life, limb, or health) is not possible, even in cases of slight negligence.[901] In the area of fault-based liability, the test of unconscionability pursuant to § 138 (1) BGB is the sole criterion for the admissibility of liability limitations for negligent conduct. [902] Unconscionability could arise, for example,

[896] Federal Court of Justice, January 29, 2008 – VI ZR 70/07= BGHZ 175, 152; BGHZ 175, 153; NJW 2008, 2033; MDR 2008, 564; NZBau 2008, 441; NZV 2008, 397; VersR 2008, 659; BauR 2008, 1313; ZfBR 2008, 1313.

[897] Federal Court of Justice, July 18, 2008 - V ZR 71/07= NJW 2008, 3059; MDR 2008, 1263; NZM 2008, 819; WM 2008, 1798; IMR 2008, 357.

[898] *Radio/Wenn*, CR 2004, 481.

[899] On the effectiveness of such disclaimers under the Uniform Commercial Code, see, e.g., Mortenson v. Timberline Software Corporation, Supreme Court of Washington (140 Wash. 2d 568, 998 P.2d 305).

[900] *Redeker,* Handbook of IT Contracts, 1.5 Rn. 27

[901] *Amann/Brambring/Hertel,* Die Schuldrechtsreform in der Vertragspraxis (The Reform of the Law of Obligations in Contract Practice), 2002, p. 64 bb) No exclusion of liability for physical damage.

[902] Federal Court of Justice, January 29, 1975 – VIII ZR 101/73= BGHZ 63, 382; NJW 1975, 642; MDR 1975, 750; WM 1975, 309; JR 1975, 239; Federal Court of Justice, May 25, 1983 - VIII ZR 55/82= BGHZ 87, 302; NJW 1983, 2192; ZIP 1983, 948; MDR 1983, 838; WM 1983, 755.

this would result in a blatant shift of risk to the customer, which would ultimately lead to an unacceptable imbalance between performance and consideration. [903] According to this standard, however, unconscionability can be ruled out at least if liability is not completely excluded but only limited. [904] The extent of the limitation of liability must be based on the potential damage that the contracting parties could reasonably expect at the time the contract was concluded. The contract volume can always be used as a reference point here, since substantial claims for damages are directed at [905] the positive interest, i.e., the customer's interest in performance. [906] This can generally be assumed to be the contract value. Another component for circumventing unconscionability is an agreement that, in the case of insured risks, liability shall extend beyond the total limitation of liability to the insurance benefits. This means that both parties are included in the scope of protection of the insurance policies of the other party to the contract. [907]

The customer and the manufacturer may, pursuant to Section 444 of the German Civil Code (BGB), limit or even completely exclude liability for material defects in an individual contract. [908] The only indispensable requirement is that the seller is liable for fraudulent intent or where a guarantee has been expressly assumed. The clearly formulated complete exclusion of liability covers all material defects, even the most serious and hidden ones.[909] The seller may also guarantee a specific characteristic and exclude liability in all other respects. The same applies to the law on work and services pursuant to Section 639 sentence 1 BGB. In order to limit the risk from the manufacturer's point of view in a reasonable manner, liability for claims for material defects should be limited if necessary. Since the manufacturer is liable for material defects regardless of fault, it is not necessary to distinguish between the type of fault (slight/gross negligence or intent).

[903] *Palandt/Heinrichs*, 72nd edition, 2013, Section 138, margin number 88 etseq.
[904] *Brox/Walker,* Schuldrecht AT (Law of Obligations), 36th edition, 2012, margin number 306.
[905] For example, in the event of default or non-performance.
[906] *Palandt/Heinrichs*, 72nd edition 2013, § 276 margin number 34.
[907] *Brox/Walker,* Schuldrecht AT, 36th ed. 2012, margin no. 306.
[908] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8th ed. 2011, margin no. 102.
[909] Federal Court of Justice, June 11, 1979 – VIII ZR 224/78= BGHZ 74, 383; NJW 1979, 1886; MDR 1979, 1017; JR 1980, 22; Federal Court of Justice, October 14, 1966 - V ZR = NJW 1967, 32; WM 1966, 1185; WM 1966, 1183; BGH, 23.04.1986 - VIII ZR 125/85= NJW 1986, 2319; MDR 1986, 1017; WM 1986, 867.
[910] *Schellhammer*, Law of Obligations According to the Basis of Claims, 11th ed. 2021, margin no. 1642.

188/63

In principle it is possible to limit liability for delay. [911]This can be done in particular by way of lump-sum compensation.[912] The limits of liability for lump-sum compensation in individual contracts apply within the scope of the above-described limitation of liability and are, of course, not as narrow as the limits of liability in general terms and conditions, since lump-sum compensation is also subject exclusively to the review for unconscionability pursuant to Section 138 of the German Civil Code (BGB).and are, of course, not as narrow as the liability limits in general terms and conditions, since the test of unconscionability pursuant to Section 138 (1) BGB is also the sole criterion for the admissibility of liability limitations for negligent conduct in the case of lump-sum damages.[913] However, even in individual contracts, the debtor is given the opportunity to prove that the damage was less than the lump sum. [914]

The possibilities for limiting liability in standard form contracts are very limited under German law. First of all, it can be assumed that any pre-formulated contract is subject to the application of Sections 305 et seq. of the German Civil Code (BGB). This is because, according to Section 305 (1) sentence 2 BGB, general terms and conditions do not apply if the terms of the contract have been individually negotiated between the contracting parties. Individual negotiation within the meaning of Section 305(1) sentence 2 BGB also exists if the customer had at least the actual (not necessarily exhausted) opportunity to influence the content of the contractual terms offered. [915]

The possibility of limiting **liability** (disclaimer) in general terms and conditions is only possible to a limited extent. The exclusion of liability for gross negligence cannot be effectively agreed in general terms and conditions pursuant to Section 309 No. 7 BGB. This also applies (even if this is not apparent from the wording of the law) to business transactions between companies, as Section 309 No. 7 BGB also applies to business transactions according to the case law of the Federal Court of Justice (BGH) (then Section 11 No. 7 AGBG) also extends to business transactions. [916] The exclusion of

[911] *Palandt/Heinrichs*, 72nd edition, 2013, Section 276, margin note 34.

[912] Federal Court of Justice, September 16, 1970 – VIII ZR 239/68= NJW 1970, 2017.

[913] Federal Court of Justice, January 29, 1975 - VIII ZR 101/73= BGHZ 63, 382; NJW 1975, 642; MDR 1975, 750; WM 1975, 309; JR 1975, 239; Federal Court of Justice, May 25, 1983 - VIII ZR 55/82= BGHZ 87, 302; NJW 1983, 2192; ZIP 1983, 948; MDR 1983, 838; WM 1983, 755.

[914] *Palandt/Heinrichs*, 72nd edition, 2013, Section 276, margin number 26.

[915] *Wolf/Horn/Lindacher*, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB Law: Law Governing the Law of General Terms and Conditions), 4th edition, 1999, § 1 margin note 35.

[916] *Palandt/Heinrichs*, 77th edition, 2017, Section 309 BGB, margin number 48; *Stoffels*, AGB-Recht (Law on General Terms and Conditions), 5th edition, 2024, margin number 979 et seq.

Liability for slight negligence based on established case law and the provision in Section 307 (2) No. 2 BGB is only possible to the extent that no essential contractual obligations have been breached.[917] Furthermore, the user cannot exempt itself from liability for only slightly negligent acts of its organs, executive employees, or other vicarious agents if these acts involve a breach of cardinal obligations.[918] Liability can generally be limited where the user has no interest in having to bear the risk of unexpected or unusual damage. A limitation of liability may be permissible in commercial transactions (except in cases of gross negligence on the part of the user or a senior employee) if the specified maximum liability amount covers the typical and foreseeable damages under the contract.[919] However, a limitation of liability is invalid if the maximum amount does not cover the foreseeable damage typical for the contract. [920] Limitations of liability in general terms and conditions for property damage and financial loss are also only possible in the form described above. Limitations of liability that seek to limit personal injury (injury to life, limb, and health) are generally invalid pursuant to Section 309(2) (7a) BGB. If general terms and conditions contain limitations of liability that violate the law on general terms and conditions, these are invalid. They are replaced by the statutory provisions, which generally do not provide for any limitations of liability, in accordance with Section 306 (2) BGB.

According to Section 309 No. 8b of the German Civil Code (BGB), a provision in general terms and conditions for contracts for the delivery of newly manufactured goods and for work and services which excludes claims against the user for defects in whole or in part is invalid. This is aimed in particular at protecting the customer from the erosion of his statutory **rights** in respect of **defects** and at ensuring that the equivalence of performance and consideration can be enforced even in the event of defective performance by the user. [921] This fundamental concern must also be taken into account by the

[917] *Stoffels,* AGB-Recht, 5th ed. 2024, para. 982.

[918] B G H , February 19, 1998 - I ZR 233/95= NJW-RR 1998, 1426; MDR 1998, 1403; VersR 1998, 1049; WM 1998, 2064; DB 1998, 2107.

[919] *Ulmer/Brandner/Hensen*, AGB, 4th ed. 1999, § 11 No. 7 AGBG margin no. 35 et seq.

[920] Federal Court of Justice, November 11, 1992 - VIII ZR 238/91 = NJW 1993, 335; NJW-RR 1993, 564 (Ls.); ZIP 1993, 46; MDR 1993, 212; WM 1993, 24; BB 1992, 2460; DB 1993, 221; IBR 1993, 92; Federal Court of Justice, January 19, 1984 - VII ZR 220/82= BGHZ 89, 363; NJW 1984, 1350; ZIP 1984, 457; MDR 1984, 482; BB 1984, 746; Federal Court of Justice, February 23, 1984 - VII ZR 274/82= NJW 1985, 3016; ZIP 1984, 971; MDR 1984, 1018; WM 1984, 1224; BB 1984, 939; ZfBR 1990, 134; ZfBR 1991, 20; Federal Court of Justice, January 21, 2000 - V ZR 327/98= MDR 2000, 448; NJ 2000, 538; WM 2000, 1069.

[921] *Palandt/Heinrichs*, 77th ed. 2017, § 309 marginal no. 46.

contract drafting in commercial transactions. [922] Pursuant to Section 309 No. 8b lit. aa BGB, the complete exclusion of rights under Sections 437 and 634 BGB and a substitute reference by the contractual partner to a third party are also invalid in commercial transactions.[923] Furthermore, pursuant to Section 309 No. 8b lit. bb BGB, restrictions on rights in respect of defects to the claim for subsequent performance, which also applies to commercial transactions, are not permissible.[924] Furthermore, pursuant to Section 309 No. 8b lit. cc BGB, the costs of subsequent performance cannot be passed on to the other party to the contract even if the third party is a business customer.[925] Furthermore, in commercial transactions, the prohibition on withholding subsequent performance applies pursuant to Section 309 No. 8b lit. dd BGB.[926] In contrast, pursuant to Section 309 No. 8b lit. ee BGB, the prohibition of clauses for exclusion periods is not transferable to commercial transactions. [927] Pursuant to Section 309 No. 8b lit. ff BGB, the limitation period for claims against the user for a defect in cases of Section 438 para. 1 No. 2 BGB and Section 634a para. 1 No. 2 BGB is facilitated claims against the user due to a defect in the cases of § 438 para. 1 No. 2 BGB and § 634a para. 1 No. 2 BGB is facilitated or, in other cases, a limitation period of less than one year from the start of the statutory limitation period is not permissible.

The option of agreeing on **lump-sum damages** in a contract is often chosen in cases of damage caused by**delay.**[928] If the customer normally has to prove that damage was caused by a delay in performance, they must also prove the actual amount of damage incurred. In the case of a lump-sum compensation arrangement for default, however, the customer only has to demonstrate that a service was provided late. The obligation to demonstrate the actual amount of compensation is waived and replaced by the lump sum agreed in the contract.

[922] *Stoffels,* AGB-Recht (Terms and Conditions Law), 5th edition, 2024, margin number 959 etseq.

[923] Federal Court of Justice, June 26, 1991 – VIII ZR 231/90 NJW 1991, 2630, 2632; ZIP 1991, 1362; MDR 1992, 25; WM 1991, 1591; BB 1991, 1522; DB 1991, 2234; ZfBR 1996, 205; ZfBR 1992, 272; ZfBR 1991, 262; IBR 1992, 35; Federal Court of Justice, January 12, 1994 - VIII ZR 165/92= BGHZ 124, 351; NJW 1994, 1060, 1066; NJW-RR 1994, 738 (Ls.); ZIP 1994, 461; MDR 1995, 260; WM 1994, 1121; BB 1994, 885; DB 1994, 2283.

[924]Federal Court of Justice, February 2, 1994 – VIII ZR 262/92= NJW 1994, 1004, 1005; NZV 1994, 272 (Ls.); BGH, November 5, 1997 - VIII ZR 274/96= NJW 1998, 679; WM 1998, 518.

[925]Federal Court of Justice, April 9, 1981 – VII ZR 194/80= NJW 1981, 1510; ZIP 1981, 620; MDR 1981, 837; BB 1981, 935; DB 1981, 1719; BauR 1981, 378.

[926] *Palandt/Heinrichs*, 72nd edition 2013, Section 309 marginal number 73; *Erman*, in: Hefermehl/Werner, BGB, 9th edition 1993, Section 11 No. 10 AGBG marginal number 36.

[927] *Stoffels,* AGB-Recht, 5th ed. 2024, margin no. 964.

[928] Federal Court of Justice, September 16, 1970 – VIII ZR 239/68= NJW 1970, 2017.

Contractually agreed lump sum. The injuring party is given the opportunity to prove that the damage was less than the lump sum.[929]

The limits of preformulated lump-sum damages arise primarily from Section 309 No. 5 BGB, but outside the factual limits also from Section 307 BGB. [330] According to § 309 No. 5 BGB, agreements on a lump-sum claim by the user for compensation or reimbursement for a reduction in value if a) the lump sum exceeds the damage or reduction in value that would normally be expected in the ordinary course of events in the cases covered by the regulation, or b) the other party to the contract is not expressly permitted to prove that no damage or reduction in value has occurred or that it is significantly lower than the lump sum. The standard for Section 309 No. 5 a) BGB is reproduced in Section 252 sentence 2 BGB. [931]The relevant benchmark is the average damage typical for the industry [932] or the average reduction in value occurring in most cases. In the case of Section 309 No. 5 b) BGB, a lump-sum damage agreement is only effective if it expressly allows proof of lesser damage.[933]

It is often difficult to distinguish between lump-sum damages and contractual penalties.[934] While Section 309 No. 5 BGB contains the standard limits for lump-sum damages, Section 309 No. 6 BGB contains the limits on the validity of contractual penalties. In the case of the limits on validity in Section 309 No. 6 BGB, the type of claim from which the payment request is derived must be taken into account. The purpose of the agreement must be determined by way of interpretation. If its primary purpose is to secure the fulfillment of the main claim and to exert the most effective pressure possible on the other party to the contract,[935] then, according to the facts of the case

[929] *Palandt/Heinrichs*, 72nd edition, 2013, Section 276, marginal number 26.

[930] *Basedow*, in: Munich Commentary on the Civil Code Vol. 5/1: Law of Obligations, Special Part III/1, 7th edition 2017, § 309 No. 5 margin note 8.

[931] B G H , May 28, 1984 - III ZR 231/82= NJW 1984, 2941; ZIP 1984, 1324; MDR 1985, 299; WM 1984, 1174; BB 1984, 1829.

[932] B G H , January 16, 1984 - II ZR 100/83= NJW 1984, 2093, 2094; MDR 1985, 29; FamRZ 1984, 868; *Ulmer/Brandner/Hensen,* 4th edition 1999, Section 11 No. 5 AGBG marginal no. 14.

[933] *Stoffels*, AGB-Recht, 5th ed. 2024, margin no. 893.

[934] B G H , November 6, 1967 - VIII ZR 81/65= BGHZ 49, 84; NJW 1968, 149; BGH, October 8, 1969 - VIII ZR 20/68= NJW 1970, 29; VersR 1959, 1142; BGH, June 30, 1976 - VIII ZR 267/75= NJW 1976, 1886; BGH, April 24, 1992 - V ZR 13/91= NJW 1992, 2625; ZIP 1992, 939; MDR 1992, 965; DNotZ 1992, 659; WM 1992, 1411; DB 1992, 1774; DB 1992, 1174; IBR 1992, 463.

[935] *Palandt/Heinrichs*, 72nd edition 2013, Section 276 Marginal Number 26.

a contractual penalty agreement. On the other hand, a lump-sum compensation agreement is one that serves to simplify the enforcement of a contractual claim that is assumed to exist. Wording in the clause such as "compensation" or "damages" does indicate a compensatory function under tort law. Ultimately, however, the decisive factor is the amount of money to be paid. A lump-sum compensation payment presupposes a lump-sum calculation based on the damage.[936] Pursuant to Section 309 No. 6 BGB, a provision in general terms and conditions is invalid if it promises the user a contractual penalty in the event of non-acceptance or delayed acceptance of the service, default in payment, or in the event that the other party withdraws from the contract. The strict prohibitions of Section 309 No. 6 BGB cannot be transferred to commercial transactions. [937] As a rule, clauses in general terms and conditions are also valid for commercial transactions when agreeing on a no-fault contractual penalty, when excluding the contractual penalty from being offset against damages[938] and waiving the reservation of the contractual penalty. [939] In addition, the unreasonable amount of the contractual penalty stipulated may also give rise to objections. [940] However, particularly in commercial transactions, a tangible sanction must be possible.[941] Nevertheless, there are limits to validity which must be observed in accordance with Section 307 (1) BGB: It is essential that there is a reasonable relationship between the amount of the contractual penalty on the one hand and the maximum burden on the customer as a result of the forfeited contractual penalty on the other. [942] The amount of the contractual penalty is therefore unreasonable within the meaning of Section 307(1) BGB if the penalty is disproportionate to the breach of contract, its severity, and its consequences for the user of the general terms and condition. [943] Contractual penalties are a widely used and necessary means of pressure in this area to compel the other party to perform properly.

[936] *Stoffels,* AGB-Recht (Law on General Terms and Conditions), 5th edition, 2024, margin number 886.

[937] *Ulmer/Brandner/Hensen*, 4th edition, 1999, Section 11 No. 6 AGBG margin note 17; *Wolf/Horn/Lindacher*, AGB-Gesetz: Gesetz zur Regelung des Rechts of General Terms and Conditions, 4th edition 1999, Section 11 No. 6 AGBG margin number 33; *Staudinger/Coester/Waltjen,* BGB, Section 11 No. 6 AGBG margin note 27; *Palandt/Heinrichs*, 72nd edition 2013, Section 309 BGB margin note 38.

[938] BGH, February 29, 1984 - VIII ZR 350/82= NJW 1985, 53, 56; ZIP 1984, 841; MDR 1985, 223; WM 1984, 663; BB 1984, 1508.

[939] *Wolf/Horn/Lindacher*, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (Law on the Regulation of General Terms and Conditions), 4th edition, 1999, Section 11 No. 6 AGBG marginal number 38.

[940] *Stoffels,* AGB-Recht (Law on General Terms and Conditions), 5th ed. 2024, margin no. 917.

[941] OLG Frankfurt, May 21, 1985 - 5 U 206/84= MDR 1985, 934; VersR 1986, 147; BB 1985, 1560.

[942] Federal Court of Justice, NJW 2009, 1882, 1885; 1994, 1060 – Daihatsu.

[943] Federal Court of Justice, NJW 2009, 1882, 1885; 1998, 2600 – Treuhand; 1997, 3233, 3234 – Citroën; 1994, 1060 – Daihatsu.

[944] Furthermore, they should give the creditor the option of simplified indemnification in the event of a breach, without being required to provide individual proof.[945] Therefore if the contractual penalty is linked to the scope of the performance owed, the fulfillment of which it is intended to secure, and is limited by it, there is no unreasonable disadvantage within the meaning of Section 307(1) of the German Civil Code (BGB).[946]This also applies if there is a so-called "cumulative effect," for example, if contractual penalties are provided for several contractual obligations side by side. [947] However, this requires that this "cumulative effect" does not exceed what could be expected and was expected from the debtor if the contract had been properly performed.[948] In this regard, the Federal Court of Justice held that a summation of all violations of a prohibition on disclosure is ruled out if the parties have agreed on a contractual penalty for each individual product sold.[949] In the case in question, the marketing of the product resulted in a penalty of over EUR 53 million from the sum of 7,000 breaches of contract, which, pursuant to Section 242 of the German Civil Code (BGB), had to be reduced to an amount not exceeding EUR 2 million due to its disproportionate amount.[950] Finally, according to the highest court ruling, there must be no aggregation in the form of a contractual penalty clause stipulating a contractual penalty of up to 5% of the total order value for culpable failure to meet an interim deadline.[951] By stipulating that a contractual penalty shall also be forfeited in the event of failure to meet interim deadlines, the contractual partner of the user is unreasonably disadvantaged, as this may result in the accumulation of penalties even though the final deadline, which is generally the only one relevant to the user, has been met. [952]

[944] *Stoffels,* AGB-Recht (General Terms and Conditions Law), 5th edition, 2024, margin number 916.
[945] Federal Court of Justice, NJW 1998, 2600, 2602 – Treuhand; 1975, 115, 116.
[946] *Thüsing,* in: v. Westphalen, Contract Law and General Terms and Conditions, 41st edition, April 2018, margin number 18.
[947] Federal Court of Justice, NJW 1998, 2600, 2602 – Treuhand; 1975, 115, 116.
[948] *Thüsing,* in: v. Westphalen, Contract Law and General Terms and Conditions, 41st edition, April 2018, margin note 18.
[949] Federal Court of Justice, NJW 2009, 1882, 1885.
[950] Federal Court of Justice, NJW 2009, 1882, 1885.
[951] Federal Court of Justice, NZBau 2013, 222.
[952] *Thüsing,* in: v. Westphalen, Contract Law and General Terms and Conditions, 41. EL April 2018, para. 18.

A flat-rate contractual penalty clause in B2B general terms and conditions is also invalid if the clause does not differentiate according to the nature of the breach of duty. According to this ruling by the Federal Court of Justice,[953] the terms and conditions are invalid because they place the defendant at an unreasonable disadvantage. Even in commercial transactions, the contractual penalty imposed must be proportionate to the breach of duty committed. The general terms and conditions at issue here do not comply with this principle, as the contractual penalty would be payable for any breach of duty, regardless of the importance of the duty breached. The fact that the provision only applies to intentional breaches of duty does not alter this. Even in this context, the contractual penalty is undifferentiated. The plaintiff does have a legitimate interest in compliance with the contractual agreements due to its business concept. However, this does not justify the introduction of a flat-rate, general contractual penalty for every breach.

j) Third-party property rights

In practice, the infringement of property rights usually comes into play when an AI system transfers a right (usually a right of use) to which the manufacturer has no rights or does not have all the necessary rights. These rights are usually held by a third party whose property rights the manufacturer may have infringed upon by transferring them to the customer. According to Section 435 (1) of the German Civil Code (BGB), an item is free of legal defects if third parties cannot assert any rights against the buyer in relation to the item or only those rights assumed in the purchase agreement. It is primarily the limited right in rem that is attached to the property and can be enforced against any owner who has not acquired it in good faith in accordance with Sections 892, 932, 936 BGB in good faith. [954] In sales law, § 433 (1) sentence 2 BGB clearly imposes on the seller the right to provide the buyer with the item free of material defects and defects of title. This can be found in the

Sections 437 to 444 of the German Civil Code (BGB), which deal generally with defects in goods and are therefore equally applicable, as legal defects and material defects. Therefore, according to Section 439 BGB, the buyer is entitled to

[953] BGH, August 31, 2017 - VII ZR 308/16= NJW 2017, 10; NJW 2017, 3145; MDR 2017, 1171; WM 2018, 1273; BB 2017, 2254; ZfBR 2017, 777.

[954] Federal Court of Justice, November 19, 1999 – V ZR 321/98= NJW 2000, 803; MDR 2000, 261; WM 2000, 578; BB 2000, 222; IBR 2000, 139.

to subsequent performance, pursuant to § 323 BGB a right to withdraw from the contract, pursuant to § 441 BGB a right to reduce the purchase price, and pursuant to §§ 280 et seq. BGB a claim for damages in several variants.[955] The burden of proof for the legal defect no longer lies with the buyer without distinction, as was the case before the reform of the law of obligations,[956] but is governed by the general rule of § 363 BGB.

k) Liability for deep learning

If data is collected using an AI algorithm (e.g., a self-learning algorithm) and this data is sold to a third party (e.g., credit rating data), the question arises as to the extent to which the seller of this AI data is liable for the accuracy of the data. In the case of traditional data trading by an AI operator who provides (incorrect) data/information (smart data) to its customers as a consulting service, a breach of the main obligation will generally be affirmed.[957] If the AI company offers a consulting service, the general rights for breach of performance under Sections 280 et seq. BGB apply, as service contract law does not provide for any special warranty rights in this respect.[958] As in normal service contract law, fault on the part of the AI company is then presumed in accordance with Section 280 (1) sentence 2 BGB, but proving the causal link between the breach of duty and the damage, which is necessary to establish liability, can be quite problematic. [959]

A different case arises if the AI company provides faulty data within the scope of a service contract so that the client can analyze or evaluate it. Under a classic service contract within the meaning of Sections 611 et seq. BGB, the AI company is only liable to the client for the absence of defects in the data once it has been handed over. [960] In this context, questions of freedom from defects or defectiveness within the meaning of the law are problematic, which poses considerable challenges in practice.

---

[955] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen (Law of Obligations Based on Claims), 11th ed. 2021, para. 117.

[956] Obsolete: Federal Court of Justice, February 15, 1955 – I ZR 108/53= BGHZ 16, 307; NJW 1955, 585.

[957] *See Andrees/Bitter/Buchmüller/Uecker*, in: Hoeren, p. 104, which, however, do not sufficiently differentiate between ancillary services (within the meaning of Section 241(1) BGB) and ancillary obligations (within the meaning of Section 241(2) BGB).

[958] See generally on service contracts: *Müller-Glöge,* in: MüKo-BGB, 6th ed. 2012, § 611 BGB marginal no. 23; *Mansel,* in: Jauernig, § 611 BGB marginal no. 13; *Weidenkaff,* in: Palandt, § 611 BGB marginal no. 15 f.

[959] See *Roßnagel*, NJW 2017, 10, 13 et seq., however without consideration of the presumption of fault.

[960] *Roßnagel*, NJW 2017, 10, 14; *Peschel/Rockstroh*, MMR 2014, 571, 576.

Of course, there are clear differences, for example in creditworthiness data, but in cases where the differences are not significant, the question arises as to how this can result in damage. Even after a defect has been remedied, the above remains questionable, as this is not provided for in service contract law and remedial action can only ever be taken retrospectively. However, creditworthiness data always refers to the moment in time, and a customer's creditworthiness can change within seconds. Thus, the claim under Sections 611 et seq. BGB is sufficient to provide high-quality data, but in practice it appears difficult to assert corresponding rights under Sections 611 et seq. BGB in the event of a breach of duty.[961] The client's obligation to pay remains in place without any obligation on the part of the AI company to provide subsequent performance.

§ 615 BGB. In the event of impossible—i.e., actually non-recoverable[962] —data delivery, which would exclude creditor default, this already follows from §§ 275 (1), 326 (2) BGB.[963]

III. operator liability

Operator liability concerns the extent to which the operator of an AI system, such as

B. a robot, user of an algorithm, or owner of an autonomous vehicle has a duty to secure the source of danger. Some have suggested that owners of autonomous systems should be required to take out liability insurance for damage caused by these systems.[964]Although this would not eliminate difficulties in determining the causality giving rise to liability and the degree of fault, injured parties would be better protected against the risk of insolvency on the part of potential claimants.[965]

1. Breaches of duty

Operator liability of a company that uses AI technologies can

[961] *Kir chner*, InTeR 2018, 19 to 24.
[962] *Weidenkaff*, in: Palandt, § 615 BGB Rn. 4.
[963] *Roßnagel*, NJW 2017, 10, 12 f., 14 f., but without corresponding differentiation.
[964] *Günther/Böglmüller*, BB 2017, 53 to 58.
[965] *Hanisch* provides a comprehensive overview of possible liability concepts in the field of robotics in: Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, p. 27.

can generally be affirmed, as the operator of a potential source of danger always has a duty to ensure traffic safety. [966] This duty remains unchanged even if the behavior of the systems is unpredictable, as what matters is the increase in risk or danger and the resulting traffic obligations.[967] In the case of robots as AI systems, it is sometimes argued that, under current law, only the operator can be held liable for a failure of the robot (or self-driving car), since the person who could not foresee the behavior of the system may not be at fault, and the accusation of wrongful conduct is thus reduced to the use of the system itself. This results in a deficit in the control intention of duty-based liability law, which also has an innovation-inhibiting effect. [968] The criticism is justified insofar as it emphasizes the proximity of traffic duties to strict liability; in fact, gray areas are increasingly emerging here, as excessive traffic duties are often imposed.[969] Nevertheless, the criticism appears exaggerated: obligations can certainly be derived from the use of AI systems, be it the careful definition of their use, the monitoring of the system and its observation, or even possible intervention in the event of malfunctions. [970]

Anyone who uses a machine, robot, autonomous vehicle, software, etc. is naturally also liable for its use. [971] In this respect, they are obliged to secure the source of danger. This is not changed by the fact that the behavior of AI-controlled systems is not always predictable, as what matters is the increase in risk or danger and the resulting traffic obligations.[972] Nevertheless, it is argued in the literature that, under current law, operators could be held liable for the failure of robots, AI systems, or self-driving vehicles, as there may be no fault on the part of those who could not have foreseen the behavior of the system. This would shift the blame for wrongful conduct to the

[966] *Lutz*, NJW 2015, 119, 120 f.

[967] *Spindler*, CR 2015, 766.

[968] This is the approach taken *by Hanisch,* in: Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, p. 27, 34; *Jänisch/Schrader/Reck*, NZV 2015, 313, 318; *Fleck/Thomas,* NJOZ 2015, 1393, 1397 therefore appeal to the legislature and call for active monitoring of progress; also critical of the shift in liability to manufacturers: *Lutz,* NJW 2015, 119, 120 f.

[969] See *Rohe*, AcP 201, 2001, 118, 134 ff.; *Spindler*, in: BeckOGK/BGB, § 823 Rn. 574; already criticized by *Esser*, JZ 1953, 129.

[970] Similar from a criminal law perspective, see *Gleß/Weigend*, ZStW 126, 2014, 561, 585 f.

[971] *Groß,* InTeR 2018, 4, 7. Different view *Reusch/Weidner,* Future Law 2018, 2018, margin number 59.

[972] *Spindler*, CR 2015, 766.

Reduce the use of the system itself. [973] It is argued that this results in a deficit in the control intention of duty-based liability law, which also has an innovation-inhibiting effect. [974] This argument cannot be dismissed out of hand, as it emphasizes the proximity of traffic duties to strict liability; and indeed, gray areas are increasingly emerging here as a result of the establishment of excessive traffic obligations. Nevertheless, the result is not in line with the interests of the parties involved, as monitoring and control obligations are fundamental obligations of an operator. This may also include the obligation to intervene in the event of malfunctions.[975] The criminal law aspects must be considered separately. Misconduct on the part of an AI system/robot, whether resulting from the pursuit of autonomy or from any other reason, always raises a number of liability issues. These may arise, on the one hand, from a breach of contractual obligations pursuant to Section 280 (1) of the German Civil Code (BGB) and, on the other hand, from tort law pursuant to

§ 823 BGB (German Civil Code) towards third parties or arising from the Product Liability Act.[976]

If an AI system/robot is used by another party to a contract (e.g., under a lease) and causes damage to that party, this certainly constitutes a breach of duty within the meaning of Section 280 of the German Civil Code (BGB). A case that has become known through the media is the use of the ROBODOC from Integrated Surgical System, which has led to numerous claims for damages. [977] The protection of the legal interests of users requires that the operator not only be required to comply with generally accepted technical rules. If damage occurs because customers fail to observe the necessary rules of conduct when using the system – albeit rarely, but predictably – the operator must take appropriate measures to ensure that no misconduct occurs. [978] The operator is therefore obliged to inform users (third parties) in an appropriate and reasonable manner about the rules of conduct to be observed.

[973] *Spindler*, CR 2015, 766.

[974] See *Hanisch,* in: Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, pp. 27, 34; *Jänisch/Schrader/Reck*, NZV 2015, 313, 318; *Fleck/Thomas,* NJOZ 2015, 1393, 1397 therefore appeal to the legislature and call for active monitoring of progress; also critical of the shift in liability to manufacturers Lutz, NJW 2015, 119, 120 f.

[975] See *Rohe*, AcP 201, 2001, 118, 134 ff.; *Spindler*, in: BeckOK/BGB, § 823 Rn. 574; already critical *Esser*, JZ 1953, 129.

[976] Similar from a criminal law perspective, see *Gleß/Weigend*, ZStW 126, 2014, 561, 585 f.

[977] Federal Court of Justice, June 13, 2006 - VI ZR 323/04= BGHZ 168, 103; NJW 2006, 2477; MDR 2007, 153; VersR 2006, 1073; JR 2007, 191.

[978] NJW 2018, 2956= MDR 2018, 1116; NJW 2018, 2956.

The operator of an algorithm-controlled AI system, such as a search engine, is only subject to specific obligations to act if they become aware of an obvious and clearly recognizable legal violation through a specific indication.[979] The notification is necessary to enable the provider, who is not generally obliged to carry out preventive checks, to identify those websites among the large number of indexed websites that may infringe the rights of third parties.[980] A legal violation in the above sense may be obvious, for example, in the case of child pornography, incitement to violence against persons, obvious cases of mistaken identity, the existence of a legally enforceable title against the direct infringer, the expiry of any interest in information due to the passage of time, or clear defamatory criticism. A practical example in the field of AI systems is the chatbot "Tay" developed by Microsoft. It was designed to learn how young people talk online. After a few hours, the experiment had to be abandoned because Tay had learned statements such as "bush did 9/11 and Hitler would have done a better job than the monkey we have now. Donald Trump is the only hope we've got." It also made calls for genocide and racist and sexist remarks of all kinds. [982] If Microsoft had not reacted, it would have been liable according to the criteria described above. However, the line is difficult to draw. In the case of defamatory criticism in particular, it is problematic for search engine operators to recognize an obvious violation of the law. The line between permissible and impermissible expression of opinion is not drawn where polemical exaggeration is not necessary for the expression of objective criticism. [983] Defamatory criticism cannot be assumed simply because a statement is exaggerated or offensive.[984] There must also be a personal insult that completely overshadows the factual concern of the statement, [985] the final assessment of which, without verifiable knowledge of the factual

[979] See also OLG Hamburg, ZUM-RD 2012, 32; LG Hamburg, NJW 2015, 796, regarding the scope of a search engine operator's verification obligations.

[980] See BGHZ 191, 19 para. 21, 28 – Stiftparfüm.

[981] See ECJ, ZUM 2014, 559 para. 92 ff. – Google Spain, hate speech (see ECtHR, NJW 2015, 2863 para. 153 ff. – Delfi AS/Estonia).

[982] *Beuth*, Zeitonline, March 24, 2016, Microsoft Twitter users turn chatbot into racist.

[983] Federal Constitutional Court, ZUM-RD 2016, 569 marginal no. 13; BVerfGE 82, 272, 283 f.; 85, 1, 16.

[984] BGH, February 27, 2018 - VI ZR 489/16: Liability of the operator of a search engine for third-party content that infringes personal rights, NJW 2018, 2324; ZIP 2018, 1980; MDR 2018, 592; GRUR 2018, 642; VersR 2018, 881; WM 2018, 824; MMR 2018, 449; K&R 2018, 391; ZUM 2018, 433; afp 2018, 322.

[985] See BVerfGE 93, 266 7. b); BVerfGE 82, 272, 284.

Background is rarely possible. The same applies to disparaging statements of fact or value judgments with a factual core. This is because the truthfulness of the alleged fact is decisive in this case. [986] The AI operator typically has no knowledge of this. If it is therefore not possible to validate the statement of the data subject on a regular basis, the standard of "obvious and clearly recognizable violation of the law" will only lead to a clear result for the AI operator in exceptional cases. A reliable and unambiguous assessment of whether, taking into account all conflicting constitutionally protected interests and the circumstances of the individual case, the interest of the data subject in protection outweighs the legitimate interests of the injured party[987] is not usually possible for the AI operator without further ado.

a) liability

It is questionable whether the operator can be held liable for its own fault pursuant to Section 280 (1) in conjunction with Section 276 of the German Civil Code (BGB). The Federal Court of Justice (BGH) [988]has already indicated at an early stage that it can imagine the operator being at fault in the maintenance and operation if it failed to properly set up and maintain the (AI) system.[989] Liability does not apply if the exonerating evidence pursuant to Section 280 (1) sentence 2 BGB is provided and it has thus been proven that proper adjustment and maintenance were carried out.[990] The operator's liability is already excluded here due to the mere impossibility of avoiding unexpected cases pursuant to Section 275 (1) or (2) BGB.[991] The Federal Court of Justice (BGH) [992] has also affirmed liability for the operator if the algorithm of a search engine suggests auto-complete suggestions for search queries, but these are actually based on the search behavior of other users. [993]

[986] *V. Pentz*, AfP 2017, 102, 115.

[987] See BGHZ 209, 139 = ZUM-RD 2016, 355 marginal no. 30; BGHZ 199, 237 = ZUM-RD 2014, 145 marginal no. 22 – Saxon corruption affair; Senate, ZUM-RD 2016, 292 marginal no. 20; ZUM-RD 2016, 362 marginal no. 29; ZUM-RD 2015, 151 marginal no. 13 – Branch manager at celebrity hairdresser; ZUM-RD 2015, 83 – Interior minister under pressure; ZUM-RD 2014, 430 marginal no. 8 – Adopted daughter.

[988]Federal Court of Justice, October 16, 2012 – X ZR 37/12= BGHZ 195, 126; NJW 2013, 598; NJW 2017, 3092; MDR 2012, 14; MDR 2013, 141; NJ 2013, 293; VersR 2013, 779; WM 2013, 2386; MMR 2013, 296; K&R 2013, 113.

[989] *Groß/Gressel,* NZA 2016, 990, 995.

[990] *Resuch/Weidner,* Future Law, 2018, margin note 58.

[991] *Bräutigam/Rücker,* E-Commerce, 2016, 14 B III para. 64.

[992]Federal Court of Justice, May 14, 2013 – VI ZR 269/12= BGHZ 197, 213; NJW 2013, 2348; NJW 2013, 28; MDR 2013, 710; GRUR 2013, 751; VersR 2013, 769; WM 2013, 1188; MMR 2013, 535; MIR 2013, Doc. 029; BB 2013, 1345; K&R 2013, 474; ZUM 2013, 550; afp 2013, 229; afp 2013, 260.

[993] *Resuch/Weidner,* Future Law, 2018, para. 58.

b) Analogy to animal owner liability

It is sometimes argued that an AI system acts autonomously or semi-autonomously, which could give rise to other aspects of liability. This view is not new; consider, for example, the liability of animal owners. Here, too, animals act autonomously or at least semi-autonomously, and the owner is nevertheless liable for their animal. Whether animal owner liability can serve as a model for liability for autonomous systems has only been discussed to a limited extent. While some see a parallel here,[994] without explaining its significance in more detail, others consider transferring the differentiation established in Section 833 of the German Civil Code (BGB) to the creation of rules for autonomous systems, while others reject any such transfer.[995] sometimes seeing a closer connection to other rules, such as building liability, Section 836 BGB.[996]

In principle, animal owner liability is regulated in Section 833 of the German Civil Code (BGB). If, pursuant to Section 833 (1) BGB, an animal kills a person or injures the body or health of a person or damages property, the person who keeps the animal is obliged to compensate the injured party for the damage resulting therefrom. However, pursuant to Section 833 (2) BGB, the obligation to pay compensation does not apply if the damage is caused by a domestic animal that is intended to serve the profession, gainful employment, or livelihood of the animal keeper, and either the animal keeper exercises the care required in traffic when supervising the animal or the damage would have occurred even if such care had been exercised. The provisions of § 833 BGB on animal owner liability attempt to strike a balance between strict liability and fault-based liability.[997] The purpose of § 833 BGB is to give those who exercise actual control over an animal and are therefore able to control it incentives under liability law to control the creature in the interest of preventing damage.

While this goal can also be achieved through fault-based liability, the

[994] *Brunotte*, CR 2017, 583, 585 f.; *Sosnitza*, CR 2016, 764, 772; in contrast, for example, *Grützmacher*, CR 2016, 695, 698; with reservations, *Horner/Kaulartz*, CR 2016, 7, 14; more open to de lege ferenda, InTeR 2016, 22, 24 f.

[995] See *Schaub*, JZ 2017, 342, 348, who seeks to differentiate between private and commercial operators.

[996] *Borges*, NJW 2018, 977.

[997] *MüKoBGB/Wagner*, 7th edition 2017, BGB § 833 margin note 1.

strict liability offers the additional advantage of controlling the level of activity. [998] Controlling the level of activity through strict liability is necessary if damage-den cannot be avoided even if the requirements of due care in traffic are observed, or if a source of danger causes damage to a considerable extent which cannot be avoided by observing due care, as is typically the case with wild animals, which were consequently already subject to a special regime in Rome (edictum de feris).[999] An analogous application can generally be considered if no legal norm exists for a specific situation, i.e., if there is a gap in the law or a regulatory gap. In many cases, it is argued that this is contrary to the intention of the legislature, i.e., that it was not intended by the legislature.In contrast,[1000] it is argued that a contravention of the intention of the legislature can only be recognized as indispensable for an analogy if one accepts exclusively the subjective method of interpretation.[1001] According to the objective method of interpretation, on the other hand, one could come to the conclusion that an analogous application is appropriate, i.e., that there is a gap in the law, even though the historical legislator demonstrably did not intend to attach any legal consequences to the case.[1002]According to the subjective method of interpretation, a regulatory gap is contrary to the intention of the legislature if it can be assumed that the legislature simply overlooked the need to regulate a complex issue when enacting the legislation. [1003] However, it can often be inferred from the values of the constitution or any general clauses that a gap is unintended, as the legislature would otherwise have contradicted fundamental values. However, the question of whether a gap can be filled by analogy must be determined by interpretation in both cases. [1004] In the case of AI, it could be assumed that this technology is so new that the legislature has not created any special legal norms such as Section 833 of the German Civil Code (BGB).

---

998 Posner explained this function of strict liability with the following example: "Keeping a tiger in one's backyard would be an example of an abnormally hazardous activity. The hazard is such, relative to the value of the activity, that we desire not just that the owner take all due care that the tiger not escape, but that he seriously consider the possibility of getting rid of the tiger altogether; and we give him an incentive to consider this course of action by declining to make the exercise of due care a defense to a suit based on an injury caused by the tiger—in other words, by making him strictly liable for any such injury." – G.J. Leasing Co. v. Union Elec. Co. (1995) 54 F. 3d 379, 386 (7th Cir. 1995).

999 See *Zimmermann*, The Law of Obligations, 1996, p. 1105 ff.

1000 *Bydlinski*, Grundzüge der juristischen Methodenlehre, 2nd ed. 2011, p. 23.

1001 *Rüthers,* Rechtstheorie, 4th ed. 2010, p. 25.

1002 *Puppe*, Kleine Schule des juristischen Denkens, 2nd edition, 2011, p. 4.

1003 Bydlinski, Grundzüge der juristischen Methodenlehre (Fundamentals of Legal Methodology), 2nd edition, 2011, p. 23.

1004 *Larenz*, Methodology of Jurisprudence, 6th edition, 1991, p. 5

Of course, this argument should be treated with caution, as the analogous application of animal owner liability under Section 833 BGB would not apply in cases of credit risk under Section 824 BGB, for example. The application of Section 823 (1) BGB in conjunction with Article 22 GDPR would also likely lead to the exclusion of analogous animal owner liability under Section 833 BGB. Cases in robotics and the argumentation regarding autonomous and/or semi-autonomous AI systems could be conceivable. It is assumed that the interests are comparable if both situations are similar in all essential characteristics. This is generally a value judgment, as animals and robots do not appear comparable at first glance. Animals are living beings with a conscious will of their own, which can be trained to a certain extent, whereas robots or AI systems are software or machines that can be controlled, and if control leads to damage, then the development of the AI system or robot was defective. The Federal Court of Justice has stated that software can be full of defects, but this does not change the law on warranty. [1005] It can be assumed that the Federal Court of Justice would come to a similar conclusion with regard to AI technologies. However, if we think far beyond the limits of weak AI in the future, we could certainly come to the question of the extent to which humans have exercised the necessary care in the development of AI, but the system has become so autonomous that, similar to an animal, it can only be controlled to a limited extent.[1006] Experience shows that even pets, which are ultimately all descended from wild animals, cannot be completely controlled because they have a primal instinct that cannot simply be trained away. Here, it could be argued that AI is so complex in its development and has evolved independently, i.e., autonomously, that a comparable interest to animal liability under Section 833 of the German Civil Code (BGB) can be assumed. Analogous to animal owner liability, it can then be argued that the AI operator, like the animal owner, maintains a source of particular danger for their own benefit and should bear all (damage) costs associated with this activity.[1007] especially since animal ownership/the operation of AI is unevenly distributed in society, so that

1005 BGH, March 25, 2010 – VII ZR 224/08, NJW 2010, 2200.

1006 *MüKoBGB/Wagner*, 7th ed. 2017, BGB § 833 Rn. 1.

1007 See BGHZ 67, 129, 130; BGH NJW-RR 1988, 655, 656: "Animal owner liability is, so to speak, the operating costs of a dangerous event"; similarly, RGZ 62, 79, 83; on a different basis (fault-based liability with reversal of the burden of proof), see also the Second Commission Prot. II p. 647.

does not compensate for the mutual danger to citizens. The animal keeper, like the operator of the AI, is not unduly burdened by the liability because he can easily pass on the risk of damage to liability insurance. [1008]

The dangers of applying animal owner liability under Section 833 of the German Civil Code (BGB) to AI in an analogous manner lie in the exclusions. If an operator of a machine is liable for it, an analogous application would potentially give the AI operator privileged status over the operator of a "normal" machine. This is because if an animal under human control causes damage to another animal, case law denies a claim for compensation on the grounds that in such cases it is the third party controlling the animal and not the obedient tool that is the cause of the damage.[1009] Consequently, liability was denied when a rider brought his horse close to that of his neighbor and the latter kicked out [1010] or when a coachman walked alongside a moving carriage and influenced the horse from this position.[1011] The horse owner should also not be responsible if burglars drive the animal out of the stable and onto the highway.[1012] On the other hand, despite human control, liability under Section 833 of the German Civil Code (BGB) applies if arbitrary movements of the animal such as shying, bolting, biting, kicking, slipping, breaking out, galloping off, and abrupt stopping of a riding horse caused the damage.[1013] However, these aspects do not apply to AI, as they can also be controlled by appropriate locks or measures (e.g., a super code). At the current stage of development, humans are perfectly capable of controlling the behavior of AI in such a way that liability cases can be avoided and that liability cases only arise if a safety measure in the AI is faulty or has not been implemented in the first place. In practice, it is also incomprehensible why a manufacturer of AI should be given privileged treatment. This would lead to every manufacturer of a software-controlled machine claiming in a court hearing that its

1008 *MüKoBGB/Wagner*, 7th edition, 2017, BGB § 833 Rn. 1.

1009 *Israel,* JW 1902, 238, 240; *Deutsch*, NJW 1978, 1998, 2000.

1010 BGH, September 25, 1952 - III ZR 334/51= NJW 1952, 1329; VersR 1952, 403.

1011 RG, January 17, 1907 - Rep. IV. 284/06= RGZ 65, 103, 105 f.

1012 BGH, VersR 1990, 796, 797 f.

1013 BGH, VersR 1966, 1073, 1974; NJW 1982, 763, 764; 1986, 2501; 1986, 2883, 2884; 1992, 907; 1992, 2474; 1999, 3119; NJW-RR 2006, 813, 814 marginal no. 7= VersR 2006, 416; OLG Koblenz VersR 1999, 239; OLG Karlsruhe, VersR 2014, 1015, 1016.

machine was an AI system in order to benefit from the exclusion provisions of analogous animal owner liability under Section 833 BGB. Since, as explained in the introduction, there is no uniform formula for the assumption of AI, the entire analogous application of animal owner liability would lead to a farce.

In summary, it can be concluded that the analogous application of animal owner liability to AI should be rejected, as the current state of AI development does not give rise to comparable interests to those in relation to animals.

c) Submission of declarations of intent

Another question of operator liability is to what extent the actions of AI in a legal sense can be attributed to the operator of the AI. This question is particularly important in connection with semi-autonomous and autonomous AI systems, as it is quite common for such AI systems to perform legal transactions. The concept of the "autonomy" of a system in the sense of a functional unit of software and hardware is sometimes described as the ability to make decisions and implement them in the external world, independently of external control or influence.[1014] Autonomous systems can therefore be defined as those whose behavior is not completely predetermined or predictable. [1015] An example of this is a trading system that trades securities using an algorithm.

It is interesting to note in this context that large software companies such as SAP are already preparing for digital access. SAP believes that SAP software is being used when the processing activities in this software are activated. This means that every use of SAP software requires a corresponding license, regardless of the access method. Depending on the type of access, direct or indirect, the question then arises as to which license variant is relevant and what remuneration is payable.

[1014] European Parliament resolution of February 16, 2017, with recommendations to the Commission on civil law rules in the field of robotics (2015/2103 [INL]) – P8_TA(2017)0051, Intro. AA. (sub "Liability"); see *Lohmann,* ZRP 2017, 168, 169.

[1015] European Parliament resolution of 16 February 2017 with recommendations to the Commission on civil law rules on robotics (2015/2103 [INL]) – P8_TA(2017)0051, Intro. AA. (under "Liability"); see *Lohmann,* ZRP 2017, 168, 169.

This is associated with indirect/digital user access, which occurs when persons or things activate SAP ERP processing capabilities without having direct user access to the system. Examples include third-party applications, IoT devices, or bots. This variant falls under "Digital Access" in SAP's new licensing model – in contrast to "Human Access," which is calculated based on the number of human users. Technological change, driven by topics such as the Internet of Things, artificial intelligence, machine learning, robotics, and bots, has also changed the types of access to ERP systems. Indirect use of software has increased significantly in recent years, and more and more digital access to SAP systems is now taking place. In the future, customers will no longer have to count users who access the SAP system indirectly. [1016]

In principle, a contract is concluded by two matching declarations of intent. Since a declaration of intent is the expression of a will aimed at a legal effect, it consists of both an internal (subjective) and an external (objective) component.[1017] It is questionable whether an AI system based on an algorithm can possibly make its own declaration to such an extent that it can no longer be attributed to the natural or legal person behind it. [1018] A declaration of intent consists of an objective and a subjective element. The objective element is directed at the external will, while the subjective element reflects the inner side of the person making the declaration. The inner will comprises the will to act, the will to make a declaration, and the will to conduct business. [1019] The will to act is understood as the consciousness to act, i.e., the conscious act of will directed toward the external performance of an external behavior.[1020] The intention to make a declaration refers to the awareness of the person acting that the declaration constitutes a legally relevant declaration. Finally, the intention to enter into a transaction is the intention to bring about a specific legal consequence with the declaration. [1021] Of course such prerequisites can be assumed in the case of

1016 *Söbbing,* ITRB 2018, 161 to 163.

1017 *Medicus*, Civil Law. 30th edition, 2025, margin number 45.

1018 *Pieper,* InTeR 2018, 9 to 15.

1019 *Larenz*, General Part of German Civil Law, 1960, § 19 I.

1020 Medicus, Civil Law. 30th ed. 2025, margin no. 45.

1021 *Brox*, General Part of the BGB, 41st edition, 2017, margin number 83.

AI algorithms cannot be identified because algorithms only act on the basis of logic. [1022] According to the prevailing view, a machine cannot make its own declaration of intent.[1023] It is not the AI system, but the person (or company) [1024] who uses it as a tool who makes the declaration or is the recipient of declarations made. [1025] Furthermore, AI is not attributed consciousness for philosophical reasons (see 4.).

The idea that machines can make a declaration of intent on behalf of a human being is not new; think of cigarette vending machines or ticket machines. Ultimately, a declaration of intent made by AI, e.g., based on an algorithm, must still be understood as an automated declaration of intent. In the case of these so-called automated declarations of intent,[1026] which are formulated by a computer (e.g., in account statements and bills for electricity, water, or heating), the automated declarations of intent ultimately depend on the intent of the person making the declaration.[1027] An automated declaration therefore exists when the declaration of intent is automatically generated by the computer program on the basis of prior manual data entry. [1028] This is the case, for example, when data is entered into the software of an insurance company and the software then automatically calculates and creates an insurance policy on the basis of the data collected[1029] or if software independently determines and prints out the respective travel price based on the number of the booking object and the travel period entered. [1030] Such automated declarations of intent are recognized as genuine declarations of intent, [1031] whereby the technology merely serves as a means of communication. The intention of the declarant is determined by the creation and application of the AI algorithm. The user submits a blank declaration, which is provided to the user as a computer declaration.

1022 *Pieper,* InTeR 2018, 9 to 15.

1023 *Resuch/Weidner,* Future Law, 2018, 14.

1024 BGH, MMR 2013, 296, 297; *Groß/Gressel,* NZA 2016, 990, 991; *Groß,* InTeR 2018, 4 ,5; *Pieper,* InTeR 2018, 9, 10.

1025 *Reuch/Weidner,* Future Law, 2018, 14.

1026 cf. *Köhler,* AcP 182, 1982, 126; *Clemens,* NJW 1985, 1998; *Brehm,* FS Niederländer, 1991, 233

1027 BeckOK *BGB/Wendtland,* 47th ed. 01.08.2018, BGB § 119 margin no. 28, 29.

1028 *Kitz,* in: Hoeren/Sieber/Holznagel, Part 13.1, margin note 37.

1029 OLG Cologne, VersR 2002, 85, 86; OLG Hamm, NJW 1993, 2321, 2321; see also *Köhler*, AcP 182, 1982, 126, 132.

1030 Frankfurt am Main Local Court, NJW-RR 1990, 116, 116 f.

1031 Federal Court of Justice, NJW 2005, 53, 54; Federal Court of Justice, NJW 2005, 976, 977; *Brehm,* in: FS Niederländer, 1991, pp. 233, 234.

[1032] It can be argued that computer explanations are more concrete than those provided by AI systems, but this clearly overestimates the autonomy of AI systems. The algorithm itself is certainly capable of collecting data and making independent decisions based on it, but the algorithm is still set by the user, as evidenced by the setting of a credit score, for example. Thus, the actions of the AI system are also attributable to the user. This is because the AI system will only ever be able to act autonomously to the extent that it has been programmed to do so. Artificially intelligent systems may also learn from mistakes and thereby optimize their actions for the future ("artificial insight"). [1033] However, no matter how autonomous the robot's actions appear to be, they are not the result of a self-determined decision by the AI. The fact that the AI acts autonomously and has the ability to make and execute decisions is ultimately based on the will of the developer and/or user.[1034]

In the event of errors in the AI system, a distinction must be made: If the inaccuracy of the computer-generated statement is due to the use of software that is no longer up to date or faulty due to a lack of updates, this constitutes an insignificant error of motive or calculation that does not justify a challenge.[1035] The same applies if the inaccuracy of the computer-generated statement is based on previously incorrectly entered data. [1036] However, an exception to this must apply if the incorrect data is based on intentionally incorrect information provided by the recipient of the statement (e.g., deliberately untruthful information in an insurance application); in such cases, a claim for rescission on the grounds of fraudulent intent pursuant to § 123 BGB may be considered. [1037] If, on the other hand, the error in the declaration is due to an operating error, the same applies as if the declarant had made a clerical error or a mistake; in these cases, the assumption of a mistake in the declaration justifying rescission may be considered. [1038]

[1032] *Reuch/Weidner,* Future Law, 2018, 44.

[1033] *Groß/Gressel,* NZA 2016, 990, 991.

[1034] *Günther/Böglmüller*, BB 2017, 53 to 58.

[1035] *Paal,* JuS 2010, 953, 954 f.

[1036] Federal Court of Justice, NJW 1998, 3192, 3193; Regional Court of Frankfurt am Main, NJW-RR 1997, 1273; *Hoeren*, Legal Issues of the Internet, 1998, margin note 282; *Köhler,* AcP 182, 1982, 126, 135; *Brehm,* in: FS Niederländer, 1991, p. 233, 241.

[1037] *Köhler,* AcP 182, 1982, 126, 135.

[1038] *Brehm,* in: FS Niederländer, 1991, pp. 233, 240; restricted *Köhler,* AcP 182, 1982, 126, 136.

The doctrine of legal transactions needs to be further developed in order to be able to classify autonomous systems appropriately. At the conference of the Association of Civil Law Teachers in September 2017, Teubner rightly complained that the traditional concepts of the doctrine of legal transactions, which allow only natural persons to be the originators of a declaration of intent, no longer do justice to the reality of modern technologies such as Industry 4.0 and autonomous systems.[1039] Nevertheless, some authors argue that the declaration of intent does not require subjective elements in the form of human thought.[1040] However, current publications often still contain traditional descriptions of a subjective element of declarations of intent as human consciousness,[1041] which cannot adequately explain the – ultimately undisputed[1042] – recognition of machine-generated declarations as declarations of intent. [1043]

Under current law, there is no such thing as a "computer opinion" [1044]or a "machine declaration" as an independent legal declaration of intent [1045].Nevertheless, the more independently the system acts and the more environmental factors are involved in generating the objective declaration, the more general and imprecise the user's idea of the ultimate declaration will be. [1046] It is then questionable whether a business intention can still be assumed, because the user only has a vague idea of the objective declaration that is ultimately generated. In this case, there is no attribution, but rather a fiction of business intent. [1047] This applies all the more when machines communicate with each other in an increasingly autonomous manner, as is the case, for example, in the application area of Industry 4.0. German civil law originates

[1039] *Borges*, NJW 2018, 977.

[1040] *Wiebe,* Die elektronische Willenserklärung (The Electronic Declaration of Intent), 2002, p. 214 ff. (Attribution of the declaration according to the "risk principle" based on control of the machine); *Schulz,* Verantwortlichkeit bei autonom agierenden Systemen (Responsibility in Autonomously Acting Systems), p. 104; already in this direction *Brehmer,* Wille und Erklärung (Will and Declaration), 1992, p. 29, 80 f.

[1041] *Faust*, BGB AT, 6th ed. 2018, § 2 margin no. 4; *Grigoleit/Herresthal*, BGB AT, 3rd ed. 2015, margin no. 6; *Leipold*, BGB I, Introduction and AT, 9th ed. 2017, § 10 margin no. 17.

[1042] See *Borges/Sesing,* in: Matusche-Beckmann, Saar-Tage 2016: Rechtsprobleme der Informationsgesellschaft (Legal Problems of the Information Society), 2018 (forthcoming), 177, 187.

[1043] *Borges*, NJW 2018, 977.

[1044] *Weichert*, ZRP 2014, 168, 170.

[1045] See BGH, October 16, 2012 - X ZR 37/12, BGHZ 195, 126, 131; *Klein,* in: Taeger (ed.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, 2015, p. 429, 436. Ultimately, this is also acknowledged by Weichert, ZRP 2014, 168, 171, who concludes that "it must be clear that algorithms can only be as good as they have been programmed."

[1046] *Klein*, DSRITB 2015, 429, 438.

[1047] *Klein*, DSRITB 2015, 429, 438.

mostly from 1900 and assumes that declarations of intent are based on human decisions, i.e., that the person acting not only understands the consequences of their legal declarations, but also possesses a minimum level of insight and judgment.[1048] If, in the final stage of autonomy of an intelligent system, a human being is neither informed about actions that have been carried out nor is given access to decisions that have been made afterwards, this changes the assessments in the area of business intent to such an extent that attribution is difficult to maintain.

Furthermore, due to advanced intelligence and autonomy, questions may arise regarding the effectiveness of declarations of intent, particularly in the context of their submission and access. An example of this is the effectiveness of declarations of intent vis-à-vis absent persons. This is relevant in the field of "machine-to-machine communication," also known as M2M communication (e.g., in the field of Industry 4.0 or in the example of a system that independently orders "milk in the refrigerator" when it is running low). Section 130 (1) of the German Civil Code (BGB) stipulates in this regard: "A declaration of intent to be made to another person shall, if made in the absence of that person, become effective at the time when it is received by that person." The declaration is deemed to have been received when it has entered the sphere of influence or actual control of the recipient in such a way that it is now solely up to the recipient to take note of it and it can be expected under normal circumstances that the recipient will take note of it.[1049] The provision thus follows the so-called "receipt theory," according to which the risk of a declaration of intent failing to achieve its purpose is apportioned appropriately between the declarant and the recipient: The declarant must take all necessary steps to bring the declaration requiring receipt into the sphere of influence of the recipient. Until then, they bear the risk of loss or failure or of the declaration not being made in time. The risk of (timely) knowledge of the declaration of intent that has come within his sphere of influence, on the other hand, is borne solely by the recipient, since the declarant has no further influence on this after receipt. [1050] The recipient cannot therefore invoke obstacles in his sphere that prevent him from taking knowledge of the declaration, since he could have removed these by taking appropriate measures.

[1048] *Wulf/Burgenmeister*, CR 2015, 404, 406.
[1049] Federal Court of Justice, June 21, 2011 - II ZB 15/10= NJW-RR 2011, 1184, 1185.
[1050] *Wendtland*, in: Bamberger/Roth (eds.), BeckOK BGB, 42nd edition, as of February 1, 2017, Section 130, margin number 10.

can and must counteract such measures. [1051] This does not change in principle even if the recipient uses reception facilities provided for the receipt of declarations, such as fax or email.[1052] This even applies in general to storage in the form of binary data, as is the case with electronic media or software control programs. [1053]

This makes it very clear that, according to the theory of receipt, the risk of a declaration of intent failing to achieve its purpose is distributed appropriately between the declarant and the recipient. The two "spheres" are clearly distinguished from each other, thus achieving a clear allocation of responsibility on the part of both the declarant and the recipient. Under these conditions, it makes no difference how technologically advanced an intelligent system used in the receipt of a declaration of intent may be, because it can be attributed to the sphere of the recipient at any time. [1054]

These are just two specific examples of application. However, they clearly illustrate that the use of intelligent systems can lead to very different results in legal assessments when the increasing intelligence and learning ability of autonomous systems are taken into account. Development is currently in full swing and it is not yet clear how such systems will spread and, above all, how they will behave in the future. Nevertheless, it is already advisable to make legally appropriate assessments that properly accompany technical developments.

IV. AI as a vicarious agent

The question of manufacturer or operator liability becomes less important if a fault e behavior of AI in the area of contractual liability is attributed to the operator under Section 278 of the German Civil Code (BGB).

[1051] Federal Court of Justice, January 21, 2004 – XII ZR 214/00= NJW 2004, 1320, 1320 f.
[1052] *Wendtland*, in: Bamberger/Roth, 4th edition 2018, Section 130 marginal number 12.
[1053] *Wendtland*, in: Bamberger/Roth, 4th ed. 2018, § 130 marginal no. 12; *Wendtland*, in: Bamberger/Roth, 4th ed. 2018, § 126b marginal no. 2.
[1054] *Pieper,* InTeR 2018, 9 to 15.

However, such attribution must be rejected. [1055] The attribution standard requires that the vicarious agent be at fault. With a very extensive interpretation of the law, an autonomous system could possibly still be classified as a vicarious agent, but the requirement of fault on the part of the machine under the current wording of the law reaches the limits of interpretation. According to general understanding, fault presupposes the deliberate control of one's own actions. [1056]

Intelligent action by AI is always attributable to the corresponding development of the algorithm. The AI system will only ever be able to act autonomously to the extent that it has been programmed to do so. Artificial intelligence systems may also learn from mistakes and thereby optimize their actions for the future ("artificial insight"). However, no matter how autonomous the robot's actions appear to be, they are not the result of a self-determined decision by the AI. The fact that AI acts autonomously and has the ability to make and execute decisions is ultimately based on the will of the developer and/or user. [1057]

V. Credit risk

A special case of liability for incorrect data arises from the risk of credit impairment pursuant to Section 824 BGB.[1058] Anyone who, contrary to the truth, asserts or disseminates a fact that is likely to jeopardize another person's credit or cause other disadvantages for their acquisition or advancement pursuant to Section 824(1) of the German Civil Code (BGB) shall compensate the other party for the resulting damage even if they are not aware of the untruth but should have been aware of it. It is conceivable that an AI algorithm (score) produces incorrect creditworthiness data and the credit bureau provides the credit institution with a score determined on the basis of stored (personal) data as individual data for the purpose of assessing creditworthiness.

[1055] *Günther/Böglmüller*, BB 2017, 53 to 58.
[1056] *Spindler*, in: BeckOK BGB, 40th ed., as of May 1, 2016, Section 827 BGB, margin note 1.
[1057] *Günther/Böglmüller*, BB 2017, 53 to 58.
[1058] *Kirchner*, InTeR 2018, 59 to 63.

Unlike the source data itself,[1060] such a score cannot be verified for accuracy using evidence, so that it is merely an expression of opinion which, in general, does not give rise to any claims for damages, provided that the underlying facts are accurate.[1061] This does not change even if the score (AI algorithm) has determined the credit rating and not a human being. [1062] It should not be underestimated that the score is set by humans (developers/programmers).[1063] Under current law, there is no such thing as a "computer opinion" [1064] or a "machine declaration" as an independent legal declaration of intent. [1065]

Article 5(1) sentence 1, alternative 1 of the Basic Law protects freedom of expression. According to Article 5(2) of the Basic Law, freedom of expression is subject to the restrictions imposed by general laws, by provisions for the protection of young persons and by the right to personal honor. The provision in § 824 BGB can be understood as a general law in this context. [1066] If, in addition, statements in which facts and opinions shaping the statement are inseparably mixed,[1067] there is a risk of curtailing the scope of protection afforded by fundamental rights.[1068] It would therefore also be inadmissible to link this to a (fictitious) implicit assertion of fact regarding the proper preparation of the rating/credit assessment, even if this could be separated in terms of content.[1069] Thus, § 824 BGB cannot apply in these cases, so that ultimately only the provision of inaccurate (personal) factual assertions/data by the AI user remains within the scope of application of § 824 BGB, provided that

[1059] Misleading therefore *Hoeren*, MMR 2016, 8, 10, who rejects classification as correct/incorrect date, but at this point probably only refers to the score/probability values and ultimately speaks of incorrect underlying data on p. 11.

[1060] Federal Court of Justice, February 22, 2011 - VI ZR 120/10, NJW 2011, 2204, 2205.

[1061] Federal Court of Justice, February 22, 2011 - VI ZR 120/10, NJW 2011, 2204, 2205; see also Federal Court of Justice, June 28, 1994 - VI ZR 252/93, NJW 1994, 2614, 2615 - on Section 824 BGB.

[1062] However, see *Weichert*, ZRP 2014, 168, in particular 168, 171.

[1063] *Milstein/Lippold*, NVwZ 2013, 182, 184 f.

[1064] *Weichert*, ZRP 2014, 168, 170.

[1065] See BGH, October 16, 2012 - X ZR 37/12, BGHZ 195, 126, 131; *Klein*, in: Taeger (ed.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, 2015, p. 429, 436. Ultimately, this is also acknowledged by Weichert, ZRP 2014, 168, 171, who concludes that "it must be clear that algorithms can only be as good as they have been programmed."

[1066] See Federal Constitutional Court, January 15, 1958 – 1 BvR 400/57, BVerfGE 7, 198 ff. – Section 826 BGB; Munich Higher Regional Court, March 12, 2014 – 15 U 2395/13, ZD 2014, 570, 572.

[1067] Federal Constitutional Court, October 9, 1991 - 1 BvR 1555/88, BVerfGE 85, 1, 15= NJW 1992, 1439, 1440.

[1068] BVerfG, June 22, 1982 - 1 BvR 1376/79, BVerfGE 61, 1, 8 f.= NJW 1983, 1415, 1416.

[1069] A. A. *Oellinger*, in: Achleitner/Everling (eds.), Rechtsfragen im Rating, 2005, p. 360.

these are likely to jeopardize, for example, the creditworthiness of the beneficiary. [1070]

It is questionable whether Section 824 BGB is exhaustive in cases of credit risk. This can generally be affirmed, but with the clear proviso that Section 824 BGB only refers to the dissemination of false facts. Further liability can only be established under Sections 823 (1), (2) and 826 BGB.[1071] Since both provisions require fault, the question of negligence within the meaning of Section 278 (1) BGB must be clarified with regard to the quality of the score and its calculations.[1072] Strictly speaking, there can be no such thing as an "inaccurate" credit rating/opinion as such, so that the term can only indicate that the credit rating is based on inaccurate facts.[1073] This would be correct if one assumed that a score had never been programmed or set incorrectly, which is clearly not the case. Incorrect credit ratings based on an inaccurate core of facts do not constitute a (false) assertion of fact as an expression of opinion. [1074]

VI. AI with its own legal personality

What initially sounds like science fiction is already being discussed in legal circles: Can AI be granted a kind of limited legal personality in order to solve problems of guilt, liability, and responsibility?[1075]

Stanley Kubrick's rational supercomputer HAL 9000 in the film 2001: A Space Odyssey does not want to relinquish control of the upcoming space mission to the incompetent human astronauts who are planning to shut it down.[1076] In countless utopian and dystopian science fiction narratives and future scenarios,

[1070] *Kirchner*, InTeR 2018, 59 to 63.

[1071] Federal Court of Justice, January 24, 2006 - XI ZR 384/03, NJW 2006, 830, 839 with further references - true facts and value judgments/opinions.

[1072] OLG Hamm, April 18, 2012 - I-13 U 174/11, BeckRS 2012, 14962.

[1073] Federal Court of Justice, February 22, 2011 - VI ZR 120/10, NJW 2011, 2204, 2206; *Reiter/Methner*, in: Taeger (ed.), Smart World - Smart Law?, 2016, p. 453, 458; dissenting opinion probably *Berger/Stemper*, WM 2010, 2289, 2294 on "incorrect rating."

[1074] See *Schulte,* NJW 2014, 1238, 1238; Federal Court of Justice, February 22, 2011 - VI ZR 120/10, NJW 2011, 2204, 2205; Higher Regional Court of Frankfurt am Main, April 7, 2015 - 24 U 82/14, NJOZ 2015, 1913 ff.; OLG Munich, September 9, 2014 - 18 U 516/14, NJW-RR 2015, 422, 428 f.; likewise OLG Munich, October 28, 2014 - 18 U 1022/14 Pre, MMR 2015, 410 ff.

[1075] *Hilgendorf,* in: Beck (ed.), Jenseits von Mensch und Maschine (Beyond Man and Machine), 2012, p. 119, 125 ff.; *Beck*, JR 2009, 225, 229 f.; concurring with *Kersten*, JZ 2015, 1, 7.

[1076] 2001: A Space Odyssey (1968).

the topic of rational robots or computers has been discussed to such an extent that the potential possibility of creating "artificial intelligence" ("AI") has become a quasi-self-evident part of our culture. [1077]The basis for possible limited legal subjectivity could be limited legal capacity or representation. This could potentially solve attribution problems in the legal protection of AI with the help of a legal standing in absentia,[1078] namely by resolving liability through a fund or a compulsory insurance system.[1079]

The central question here is the type of software use. SAP takes the view that SAP software is being used if the processing activities in this software are activated. This means that every use of SAP software requires a corresponding license, regardless of the method of access. Depending on the type of access, direct or indirect, the question then arises as to which license variant is relevant and what remuneration is associated with it. Indirect/digital user access occurs when persons or things activate SAP ERP processing capabilities without having direct user access to the system. These can be third-party applications, IoT devices, or bots, for example. This variant falls under "Digital Access" in SAP's new licensing model – in contrast to "Human Access," which is calculated based on the number of human users. Technological change, driven by topics such as the Internet of Things, artificial intelligence, machine learning, robotics, and bots, has also changed the types of access to ERP systems. Indirect use of the software has increased significantly in recent years, and more and more digital access to SAP systems is now taking place. In the future, customers will no longer have to count users who access the SAP system indirectly. According to SAP, the new model applies to the current SAP core S/4HANA and S/4HANA Cloud, as well as to the predecessor ERP ECC 6.0.

The development and use of autonomous systems, as is already foreseeable, will

[1077] *Lewke*, InTeR 2017, 207 to 216.

[1078] *Kersten*, JZ 2015, 1, 7 with reference to *Mainzer*, Leben als Maschine? (Life as a machine?), 2010, p. 240, 243; for §§ 164 ff. BGB *Gruber,* in: Hilgendorf (ed.), Robotik im Kontext von Recht und Moral, 2014, p. 123, 198.

[1079] S. *Beck*, in: Spranger (ed.), Aktuelle Herausforderungen der Life Sciences, 2010, p. 95, 102 ff.; *Hilgendorf,* in: Beck (ed.), Beyond Man and Machine, 2012, p. 119, 125 ff., 128; *Gruber,* in Hilgendorf (ed.), Robotics in the Context of Law and Morality, 2014,
See pp. 123, 156, 198; with restrictions also *Bodungen/Hoffmann*, NZV 2015, 521, 524 ff.

lead to significant changes in the legal framework.[1080] In personal law, the discussion—including in a European Parliament[1081] working groupcenters on the recognition of an "e-person" alongside existing legal persons.[1082] The growing autonomy of robots and software agents, whose reactions can no longer be predicted by programmers but are largely determined by intelligent learning and communication behavior, could necessitate both legal personality and the establishment of a separate liability fund. [1083] The alternatives are new forms of strict liability and tailor-made insurance solutions. The emergence of new technologies has also reignited the old question of liability for their malfunction, both in the contractual sphere, where the application of provisions on vicarious agents or the introduction of new rules of attribution have long been discussed,[1084] and in the area of tort, where new models of attribution or new cases of strict liability similar to animal owner liability are also being considered. [1085] Particular attention is being paid to liability and insurance in relation to self-driving cars. [1086]

Given the technical possibilities, the discussion as to whether AI should be able to act autonomously and have its own legal capacity analogous to Section 1 of the German Civil Code (BGB) seems premature. Nevertheless, AI cannot be denied a certain degree of partial autonomy, provided that the AI in question is technically capable of this. However, this partial autonomy does not release the AI manufacturer from its product liability or the operator of the AI from its operator liability. The manufacturer must develop technical precautions (see the "Super Code" for more information) that minimize the risks posed by AI. These technical precautions must also apply to the learning process of AI. The operator/owner cannot rely solely on the manufacturer when operating AI, but must take certain

[1080] *Borges*, NJW 2018, 977.

[1081] www.europarl.europa.eu/committees/de/juri/subject-files.html?id=20150504CDT00301 , last accessed on July 27, 2018.

[1082] *Wendehorst*, NJW 2016, 2609.

[1083] See, among others, *Schweighofer*, in: Schweighofer/Menzel/Kreuzbauer, Auf dem Weg zur ePerson, 2001, p. 45, 49 ff.; *Wettig/Zehendner*, AI Law 12, 2004, 111, 127 ff.; S. *Beck*, JR 2009, 225, 229 f.; *Hilgendorf*, Jenseits von Mensch und Maschine, 2012, p. 119, 125 ff.; *Kersten*, JZ 2015, 1, 6 et seq.

[1084] For the older discussion, *see Spiro*, Die Haftung für Erfüllungsgehilfen (Liability for vicarious agents), 1984, p. 209 ff.; *Möschel*, AcP 186, 1986, 187, 197 ff.; *Koziol*, ÖBA 1987, 3; for more recent *discussions*, see *Müller-Hengstenberg/Kirn*, MMR 2014, 307, 311; *Wulf/Burgenmeister*, CR 2015, 404, 407; *Horner/Kaulartz*, CR 2016, 7.

[1085] *Spindler*, CR 2015, 766, 775; *Bräutigam/Klindt*, NJW 2015, 1137, 1139 with further references.

[1086] Instead of many *Schulte-Nölke*, Karlsruher Forum 2015, 3 ff. with further references.

protective mechanisms, for example in the form of the "Super Code."

Humanity has already faced the question of who should be granted legal personality. Under the Treaty of Madrid of 1750, Spain and Portugal agreed that the territory east of the Río Uruguay should fall to Portugal. In 1752, the papal envoy Luis Altamirano was sent to Paraguay to oversee the handover of this territory. He also had to answer the question of whether the indigenous people, the "Guaranis," who lived in this area like in a reservation, were humans or animals. This assessment was important because if the Guaraní were animals, they would not be protected by God and could therefore be enslaved and exploited by Spanish and Portuguese adventurers, the Entradas and Bandeiras. The Jesuits, under whose protection the Guaranis stood, tried to prove that Guaranis were human by having them perform their wonderful songs for Altamirano. The Entradas and Bandeiras, who had more economic interests, compared the Guaranis to parrots and monkeys that imitate certain human actions. Under considerable pressure from Spain and Portugal, Luis Altamirano decided that the Guaraní were not human beings. This led to the Guaraní War of 1754 to 1756, which ended with the deaths of 1,511 Guaraní and four Portuguese, and the subsequent enslavement of the Guaraní. Luis Altamirano described this terrible story in his report to the Pope, referring to himself as death because he could not live with the consequences of his decision. Asimov also addressed the question of when an AI (e.g., in the form of a robot) can be granted legal personality in his novel "The Bicentennial Man." In the novel, legal personality was initially denied because the robot could not age. The robot then modified its body so that natural aging began and it died at the age of 200, a few seconds before the world parliament recognized its humanity. [1087]

Until the fundamental emergence of superintelligence, however, there can be no discussion of a separate legal personality for AI, as this does not meet today's technical standards.

[1087] *Asimov,* The Bicentennial Man, 1978, (The Bicentennial Man And Other Stories, 1976).

This follows from the inability of an AI system to be a legal entity under current law.[1088] Such a discussion at this point in time, which is certainly more philosophical than legal, would ultimately result in manufacturers and operators being able to exempt themselves from liability. Furthermore, an AI system itself does not have the liquidity to satisfy the claims of the injured party, and thus granting AI its own legal personality would only harm the injured party. Thanks to technological singularity (see Chapter C. 1d),[1089] this view could change more quickly than expected, as self-improving AI (seed AI) can rapidly accelerate technical progress. However, this is not currently conceivable.

Even if robots take on human form and AI acts intelligently, they cannot be held liable for damage they cause. According to current legislation, autonomous systems are not legal entities and do not have their own legal personality. [1090]

[1088] See *Mayinger*, Die künstliche Person (The Artificial Person), 2017, p. 178; *Lewke*, InTeR 2017, 207 to 216.

[1089] Technological singularity is a term used in futurology to describe various theories about the future. It is predominantly understood to refer to a point in time when machines will rapidly improve themselves through artificial intelligence (AI) (seed AI), thereby accelerating technological progress to such an extent that the future of humanity beyond this event will no longer be predictable. Source: Wikipedia.

[1090] *Bräutigam/Klindt*, NJW 2015, 1137; *Cornelius*, MMR 2002, 353, 354; *Horner/Kaulartz*, InTeR 2016, 22, 24.

I. Embedded law in artificial intelligence

While the EU Commission's Artificial Intelligence Act (AI Act) attempts to reduce fears about artificial intelligence (AI) with more bureaucracy (see Art. 8 AI Act), the question arises as to whether there might be a more constructive method capable of making AI safer. How about giving AI a conscience as a solution? What sounds like a philosophical theory at first glance is actually a very serious practical application. Using a filter called "embedded law," hallucinations and incorrect results produced by AI are filtered out if they violate applicable law. This would prevent costly liability cases. Such a filter would be a so-called "super code" that the AI's output must never violate.

I. Introduction

A major issue in AI development is that AI arrives at results that are logically correct but catastrophically wrong from a human perspective. This phenomenon is known as "hallucination." The causes of AI hallucinations are complex and have both technical and methodological reasons. Hallucinations in AI models arise from a combination of the limitations of probabilistic methods, incomplete or faulty training data, the inability to dynamically check facts, and a fundamental lack of understanding of meaning and context. Research in AI development aims to minimize these problems, for example by integrating better data sets, fact-checking mechanisms, and more advanced model architectures.

In AI research, the term "hallucination" refers to situations in which a model generates information that is not based on actual data or facts. These inaccurate or misleading outputs can be attributed to various factors:

- **Incomplete or incorrect training data**: AI models, especially language models such as GPT, are trained on large data sets sourced from the internet and other text sources. If this data is incomplete, contradictory, or incorrect, the model may learn incorrect information. These inconsistencies in the training data cause the AI to "hallucinate" based on incorrect or inaccurate information.

- **Probabilistic approach of the models**: Language models are based on probabilities. They generate predictions by selecting the most probable **next** word sequence based on the previous context. This approach means that they do not make definitive statements, but always try to generate the most probable continuation of a text. This allows them to invent new information when the probabilities suggest this, even if this information is not factually correct.

- **Lack of understanding and world knowledge**: AI models do not have a true understanding of information. They are not able to distinguish between fact and fiction like humans do, but merely process statistical patterns in the training data. If these patterns are unclear or contradictory, this can lead to invented or incorrect content. Models cannot perform external fact-checking and therefore sometimes generate plausible-sounding but incorrect answers.

- **Overfitting**: Overfitting occurs when the model learns not only general patterns but also specific, often irrelevant details from the training data. This can cause the model to give incorrect or nonsensical answers in certain situations because it relies on patterns that are not relevant in the context of the query.

- **Lack of explicit factual knowledge**: Language models do not have explicit fact databases, but work purely on the basis of the text data on which they were trained. When the model is confronted with a question

for which it has no clear or relevant training data, it tends to hallucinate an answer based on other information. This leads to erroneous or fictitious outputs.

- **Complexity of natural language**: Natural language is ambiguous and complex, which makes it difficult to always generate an accurate response. In many cases, there is no single correct answer, and the model must consider several potential possibilities. This can lead to statements that are linguistically coherent but factually incorrect.

- **Lack of ability to dynamically verify facts**: AI models such as GPT do not have access to external sources of knowledge (e.g., current databases or the internet) after training to verify their answers. They are limited to the knowledge they acquired during training. This means that they can reproduce outdated or inaccurate information without checking it in real time. [1091]

The examples in the following paragraphs illustrate the disastrous consequences that hallucinations can have and how this risk can be minimized using a filter that contains an embedded law.

II. Practical example: HR process

It may sound a little unusual, but artificial intelligence is already being used in the human resources recruiting process.[1092] The constant availability of chatbots in recruiting offers a wide range of applications, as job seekers usually apply outside of the HR department's working hours.[1093] However since all applications can only be reviewed on the following workday, recruiters end up with a backlog of applications.

1091 Katharina Zweig deals with this topic in detail in her book "Die KI war's!: Von absurd bis tödlich: Die Tücken der künstlichen Intelligenz" (It was AI! From absurd to deadly: The pitfalls of artificial intelligence).

1092 See also *Söbbing*, InTeR 2018, pp. 64–67.

1093 cf. *Verhoeven*, 2020, p. 103.

The slow process from screening to feedback can have a negative impact on the company and cost it important potential applicants. Around half of all applicants have terminated the application process in advance, despite being interested in the position, because they found the waiting time too long.[1094]

The use of chatbots can help speed up processes and make the application process more attractive. A chatbot (or bot for short) is a computer program based on algorithms and AI that allows you to chat with a technical system.[1095] The chatbot's dialogue systems use natural language processing (NLP) to understand written sentences and respond to them. It imitates natural written text or natural spoken language, enabling intelligent, intuitive human-machine communication. [1096]

Intelligent AI technologies are used to test applicants' skills and talents. At the same time, such tools support the evaluation and assessment of individual applicants. The capabilities of such tools go far beyond those of conventional database systems and standard business intelligence solutions. Like many innovations, these developments involve opportunities and risks and must therefore also comply with the legal framework set by legislators. It is therefore important to examine the legal aspects of using artificial intelligence in the HR recruiting process.

The use of AI technologies in the HR recruiting process is not yet very widespread, and the question of fundamental acceptance among

1094 See *Schnitzler*: Online Communication in Recruiting for SMEs: Maturity Levels of Employer Branding & Candidate Experience, Springer Gabler, 2020, pp. 24–25

1095 See *Hermeier* et al., 2018, p. 10

1096 See Wilke, Gewndolin/Bendel, Oliver: AI-supported recruiting – technical fundamentals, economic opportunities and risks, and ethical and social challenges, in: HMD. Praxis Der Wirtschaftsinformatik, Vol. 59, No. 2, 2022, doi:10.1365/s40702-022-00849-w, p. 653

applicants, when they first have to communicate with a machine. Especially in times of the "talent war," i.e., the battle for the most talented minds, it sounds rather demeaning to applicants when they first have to deal with an AI system. The question of whether applicants even notice that they are communicating with a machine is certainly justified. The aim of chatbots is to ensure that people do not realize that they are not talking to another human being.

However, recent experiments with chatbots show that their responses are not always predictable or plannable. Microsoft had to deactivate its chatbot "Tay" because it started making racist statements after just a few hours. Technically, bots are more closely related to a full-text search engine than to artificial or even natural intelligence. However, with increasing computer power, chatbot systems can access ever larger databases at ever faster speeds and thus offer intelligent dialogues for users. Such systems are also referred to as virtual personal assistants.[1097] As shown below, these can very quickly lead to unpleasant liability for the company.[1098]

If an AI system asks an applicant for personal data, this is also governed by the principles of labor law regarding the employer's right to ask questions. The Federal Labor Court [1099] has established in decades of detailed case law which questions may and may not be asked during the application and interview process. Since the application process is a so-called "pre-contractual relationship of trust," the storage of data collected through permissible questions is always unproblematic under data protection law. This data meets the requirements of Art. 6 GDPR and is usually recorded as master data in appropriate applicant management systems. The collection of data such as the following is therefore unproblematic:

1097 https://de.wikipedia.org/wiki/Chatbot, accessed on October 11, 2024.

1098 *Zirn*, Chatbots – what companies need to know, CIO Magazine, October 17, 2017.

1099 *Schröder*, Data Protection Law in Practice, 2nd edition, 2016, Chapter 3: Data Protection in Human Resources/Employee Data Protection.

- Names
- Address
- Phone
- Email

What additional data may be requested in individual cases as part of the application process depends on objective professional criteria and the requirements profile specified by the employer. According to the current case law of the Federal Labor Court, an employer's right to ask questions during recruitment negotiations is only recognized to the extent that the employer has a legitimate, reasonable, and at the same time protectable interest in the answers to its questions with regard to the employment relationship. It therefore always depends on the position as to which questions may actually be asked and, in connection with this, which personal data may be lawfully stored. [1100]

The collection of so-called "sensitive data" beyond this is only possible to a limited extent under data protection law. This includes personal data relating to:

- racial origin
- ethnic origin
- religion or belief
- disability
- sexual identity
- Health
- Financial circumstances
- Criminal record
- ongoing investigations

The employer may only collect the above data in accordance with data protection law under the strict conditions of Section 8 (1) AGG. The following applies to the

[1100] *Schröder*, Data Protection Law in Practice, 2nd edition, 2016, Chapter 3: Data Protection in the Human Resources Department/Employee Data Protection.

collection of data is therefore permissible if the essential and decisive professional requirements are determined from an objective point of view. It therefore depends very much on what the company does, and each case must always be assessed individually. [1101]

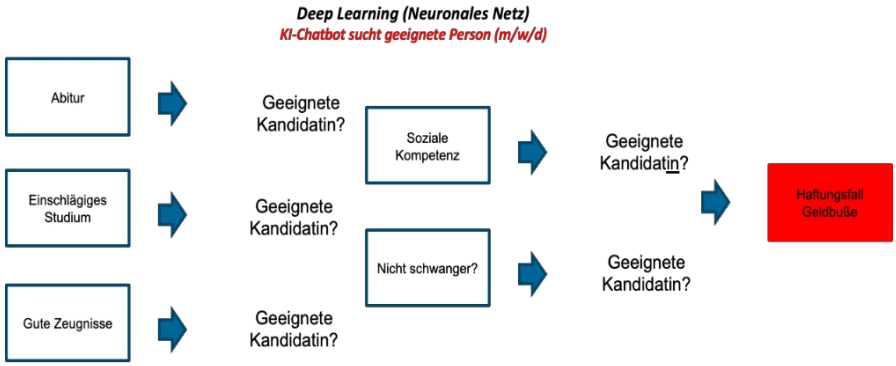


Fig. 1: AI chatbot in the HR recruiting process

The chatbot may have learned during training that its client does not like pregnant women because they tend to leave the company very quickly after being hired. Although this was not explicitly communicated to the chatbot, it came to this conclusion based on its deep learning routines. During the application process, the chatbot asks this question, which is not permitted under Section 8 (1) AGG (see Fig. 1), which would be described as a "hallucination." If, as a result of such questions based on a hallucination, an applicant is rejected, claims for damages based on the AGG are possible. From the company's point of view, the question then arises as to whether the company can claim compensation from the manufacturer of the AI system. The company cannot sue the AI system itself. Even though AI systems can appear human-like and act intelligently, they cannot be held liable for damage they cause.

1101 Section 8 AGG: Compensation and damages. *Thüsing*, Münchener Kommentar zum BGB, 7th edition, 2015, margin numbers 16–20.

[1102] Under current law, autonomous systems are not legal entities and do not have their own legal personality. [1103]

In principle, the applicant can demand compensation and damages from the company for the AI system's unauthorized questions in accordance with Section 15 AGG. In the event of a violation of the prohibition of discrimination, the employer is obliged to compensate for the damage caused in accordance with Section 15 (1) sentence 1 AGG. The discrimination must be unlawful, i.e. it must not be justified under Sections 5, 8 to 10 AGG. [1104] According to Section 15 (1) sentence 2 AGG, this does not apply if the employer is not responsible for the breach of duty. The obligation to pay damages applies to the employer and to persons whose conduct is attributable to the employer pursuant to Section 278 of the BGB.[1105] Unfortunately, the legislature has not provided any clear rules on the attribution of discrimination by third parties.[1106] Among other things, it is assumed that § 278 BGB is relevant because of the reference to responsibility in § 15 (1) AGG.[1107]

On the other hand, it is also argued that Section 278 of the German Civil Code (BGB) applies insofar as managers acted, because if employees acted without personnel responsibility and there was a close and qualified connection with the performance of their duties under their employment contract, the employer would be liable under the conditions of Section 831 BGB. Of course, no statement is made as to what the liability should look like when an AI system acts.

The situation is straightforward if the company is fundamentally at fault.
within the meaning of Section 278 BGB, specifically if the company itself intentionally removed a lock used by the manufacturer to prevent unauthorized questions or negligently failed to exercise the necessary care in this regard.

[1102] *Günther/Böglmüller*, BB 2017, p. 53.
[1103] *Brâutigam/Klindt,* NJW 2015, p. 1137; *Cornelius*, MMR 2002, p. 353; *Horner/Kaulartz,* InTeR 2016, p. 22, 24.
[1104] BeckOK *ArbR/Roloff*, AGG § 15 margin numbers 1–3.
[1105] Federal Labor Court (BAG), October 25, 2007= NZA 2008, p. 223, 227.
[1106] See generally *Wobst*, NZA-RR 2016, p. 508. Paragraph 5 is not exhaustive, BeckOK *ArbR/Roloff*, margin note 33. Sections 31 and 278 of the German Civil Code (BGB) apply.
[1107] *Kamanabrou*, RdA 2006, p. 321, 338.

This is probably quite rare in practice, but when it does occur, it must be affirmed within the meaning of Section 15 (1) sentence 2 AGG in conjunction with Section 278 BGB.

With a very extensive interpretation of the law, an AI system could possibly still be classified as a vicarious agent, but the requirement of personal fault on the part of a machine reaches the limits of interpretation under the current wording of the law. [1108] According to general understanding fault presupposes the deliberate control of one's own actions.[1109] Intelligent action by a robot is always attributable to corresponding programming. The AI system will only ever be able to act autonomously to the extent specified by its programming. Artificial intelligence systems may learn from mistakes and thereby optimize their actions for the future ("artificial insight"). However, no matter how autonomous the action of the AI system appears to be, it is not the result of a self-determined decision by the AI system. The fact that the AI system acts autonomously and has the ability to make and execute decisions is ultimately based on the will of the developer and/or user. [1110]

It might be possible to construct an attribution of the AI system's actions within the meaning of Section 15 (1) sentence 2 AGG to the company via strict liability. Strict liability is liability for damage resulting from a permissible risk (e.g., operating a dangerous facility, keeping a pet). In contrast to liability for tort, liability for risk does not depend on the unlawfulness of the act or the fault of the injuring party. According to this, anyone who uses an autonomous system (e.g., the AI system for applicant management) would, in principle, be liable for damages resulting from its use, regardless of their own fault. It is questionable whether this is not an extension of liability under Section 15 AGG, since no fault is required in this case, and whether this was really intended by the legislature.

[1108] BeckOK *ArbR/Roloff*, AGG § 15 margin numbers 1–3.

[1109] *Spindler* in: BeckOK BGB, 40th ed., as of May 1, 2016, § 827 BGB margin no. 1.

[1110] *Günther/Böglmüller*, BB 2017, p. 53.

III. Practical example of autonomous driving

In talk shows and philosophical discussions, there is often talk of a utopian future in which self-driving cars will have to decide which people to kill in a hopeless situation. In such a situation, the vehicle's algorithm would have to assess whether it is better to kill a Taliban member who oppresses women or an innocent little girl. The algorithm would therefore be allowed or required to decide on the value of a human being to society. It is often even seen as a dam breaking that algorithms will generally be allowed to decide on the value of human life in the future. Apart from the fact that such a scenario is highly unlikely for technical reasons, the algorithm would not be allowed to make such a decision under the new Section 1e (2) No. 2 lit. c) StVG. The creation of this provision nipped the tiresome discussion in the bud, but the new Section 1e (2) No. 2 lit. c) StVG nevertheless leaves a question open because it has not been thought through to its conclusion.

In autonomous driving, artificial intelligence or an algorithm in conjunction with machine learning (hereinafter referred to as "AI") replaces humans to control the vehicle. The AI must therefore be granted certain evaluation options, because according to Section 1 e (2) No. 1, No. 2 Alt. 1 StVG, motor vehicles with autonomous driving functions must have technical equipment that is capable of

- performing the driving task independently within the specified operating range without the driver intervening in the control system or the vehicle's journey being permanently monitored by technical supervision.
- independently complying with traffic regulations relating to driving

and has an accident prevention system designed to prevent and reduce damage. However, it is questionable whether additional

restrictions are possible. [1111] Examples include ad hoc traffic signs or instructions from traffic police officers that cannot (yet) be detected by autonomous driving functions.[1112] According to Section 1 e (2) No. 3 StVG, motor vehicles with autonomous driving functions must be technically equipped in such a way that they can be placed in a risk-minimizing state under certain circumstances (see Section 1 e (2) Nos. 3, 5, 7, 8, 10 StVG). This is necessary if continuing the journey is only possible by violating traffic regulations—for example, because a traffic light does not turn green due to a technical defect.[1113] The term "risk-minimized state" is legally defined in Section 1 d (4) StVG and is a state in which the vehicle comes to a standstill with its hazard warning lights activated at a suitable location in order to ensure the greatest possible safety for the vehicle occupants, other road users, and third parties.

In its report of June 2017, the Ethics Commission for Automated and Connected Driving concluded in point 5 that automated and connected technology should prevent accidents as far as practically possible. The technology must be designed in accordance with the current state of the art in such a way that critical situations do not arise in the first place. This also includes dilemma situations, i.e., situations in which an automated vehicle is faced with the "decision" of having to choose between two equally bad options. With the introduction of Section 1e (2) No. 2 lit. c) StVG on July 28, 2021, a new provision was added to the law stipulating that motor vehicles with autonomous driving functions may not give further weight to personal characteristics in the event of an unavoidable alternative danger to human life.[1014]

At the 30th Munich Media Days in October 2016, former German Chancellor Angela Merkel called for algorithms used by internet services to filter information to remain transparent. Media use

1111 *by Bodungen/Gatzke*, RDi 2022, p. 354.

1112 *Hilgendorf*, JZ 2021, p. 444 (447).

1113 *von Bodungen/Gatzke*, RDi 2022, p. 354.

1114 BT-Drucks. 19/27439 dated March 9, 2021, pp. 1–2.

is increasingly influenced by algorithms, bots, and intelligent recommendation systems. Algorithms have led to readers being increasingly offered only topics that correspond to their search behavior online. This could reduce their ability to engage with other opinions. [1115] There are already regulations in place that are intended to ensure the neutrality of algorithms. Recital 71(6) of the GDPR already contains an obligation to ensure the "neutrality of algorithms." Similar to the scoring system in Section 28b (1) of the German Federal Data Protection Act (BDSG), profiling requires the use of "appropriate mathematical or statistical techniques" and the exclusion of discriminatory calculation methods.[1116] In the case of Section 1e (2) No. 2 lit. c) StVG, the law goes even further and rightly prohibits AI from making judgments about the quality of human life.

However, in addition to the prohibition of qualitative assessments of human life, the question of quantitative assessments remains open. According to the wording of the law, it would be perfectly permissible, for example, to implement an algorithm in autonomous vehicles that distinguishes whether, in the event of an unavoidable accident, the algorithm chooses whether a group with a smaller or larger number of people must be killed or injured. This point should be revised, and here too, the algorithm should not be allowed to make any value judgements, but should instead use all technical means available to prevent such a decision from being made in the first place.

IV. Embedded law

The literature [1117] discusses whether there should be control obligations that require so-called "control algorithms" to be created in order to maintain control over AI. A TÜV test for algorithms is also being discussed. This would, of course, represent a significant intervention in the development of algorithms. Embedded law takes a far less dramatic approach.

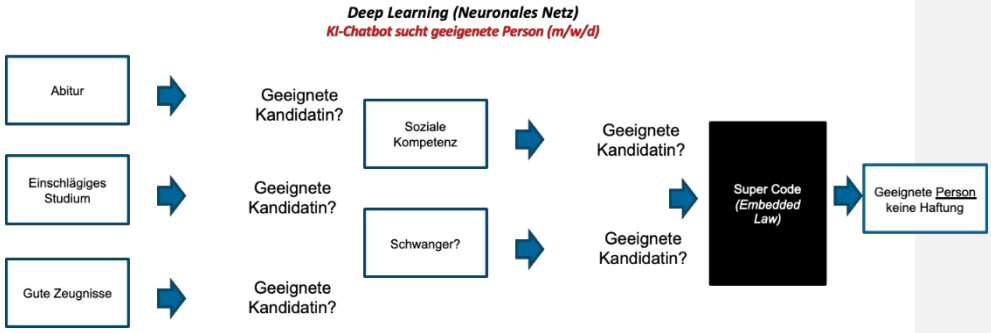
1115 https://www.heise.de/newsticker/meldung/Algorithmen-und-Scoring-Maas-fordert-digitales-Anti-Diskriminierungsgesetz-3761722.html?seite=2, accessed on October 11, 2024.

1116 *Härting*, ITRB 2016, pp. 209–211.

1117 *Martini*, JZ 2018, 1017 to 1025.

As can be seen from the above, embedded law acts as a filter that filters out impermissible questions and actions. Fig. 2 illustrates this using the example of the HR process described above:

Fig. 2: AI chatbot in the HR recruiting process with embedded law



In the example of autonomous driving, this would mean that AI should generally not be allowed to make decisions about the quality of human life.

The Embedded Law implemented in AI (e.g., in machine learning, algorithms, LLM, etc.) anchors absolute rules (in the sense of commands and prohibitions) in the AI system in a so-called "Super Code,"[1118] that the AI must never violate, especially if what it has learned and the logic developed from this lead to a result that differs from the absolute rules of the super code. The super code must therefore take precedence over the logic of the AI and the results of the algorithms. The super code is to be understood as a kind of self-regulation that is not imposed by an authority such as BaFin, but rather ensures that the manufacturers or operators of AI systems themselves ensure that their systems act in accordance with the law. At the same time, fears about the uncontrollability of AI systems[1119] would be significantly reduced, as the Super Code would ensure that AI remains controllable. Unlike in Robert

[1118] *Breidenbach* in: Rethinking: Law 2018, pp. 38–41, 40.
[1119] *Moorstedt*, Intelligence out of control, SZ.de, October 11, 2018, accessed October 24, 2018.

Harris[1120] control over AI and thus over the markets would not be lost.

Through a process known as "rule mapping" [1121], the rules of the Super Code and thus the law are integrated into AI trading systems in particular. Rule mapping is intended to prevent AI from causing regrettable market disruptions and liability cases. Without the Super Code, AI systems could not be compatible with applicable law.

V. Application of the Super Code

The question is what such a super code would look like in practice. Unlike Asimov's laws, the super code does not contain three or four laws whose correct interpretation is left to AI. Rather, all codified laws in the super code would have to contain prohibitive norms. Interpretations or discretionary powers of AI should never violate the super code, and the super code should, as far as possible, not allow for interpretation or, if interpretation is necessary, require human interaction.

However, gradations in the transformation to the super code would be conceivable if AI is only used partially. Lawyers would design the super code, which would then be implemented in the AI by engineers. The machine's super code must therefore take precedence over the logic of the AI. Rule mapping[1122] integrates rules, and thus law in particular, making them an essential component of AI. Otherwise, regrettable liability cases would arise and legal requirements, such as those arising from the Product Safety Act (ProdSG), would not be met, which would mean that AI could never act in a compliant manner.

[1120] *Harris*, "The Fear Index" (2011), German edition published under the title "Angst" by Heyne in 2011.

[1121] See *Breidenbach* in detail in: Breidenbach/Glatz, Rechtshandbuch LegalTech 2018, p. 235 ff.

[1122] See *Breitenbach* in detail in: Breitenbach/Glatz, Legal Handbook LegalTech 2018, p. 235 ff.

Based on the case described in Ziffer 1, the concrete implementation would be as follows: If the HR chatbot concludes that its client does not like pregnant women and therefore wants to ask the applicant whether she is pregnant, the Super Code ensures that the chatbot does not ask the question, even if it would be logical according to the algorithms. In addition to pregnancy, the Super Code as embedded law would prevent other discriminatory questions, e.g., regarding

- racial origin,
- ethnic origin,
- religion or worldview,
- disability,
- sexual identity,
- Health,
- financial circumstances,
- previous convictions,
- ongoing investigations,

in accordance with the General Equal Treatment Act (AGG).

VI. Conscience

If the machine learns what it is allowed to do and what it is not allowed to do through the filter of embedded law, the super code, then this could also be understood philosophically as a conscience. The Federal Constitutional Court defined the term "conscience" in a ruling from 1961. According to this ruling, a decision of conscience is "any serious moral decision, i.e., a decision based on the categories of good and evil [...], which the individual experiences in a particular situation as binding and absolutely obligatory, so that he cannot act against it without serious moral distress."[1123] Conscience is generally regarded as a special authority in human consciousness that determines how one judges

[1123] See BVerfGE 12, p. 45, 55.

and indicates whether a course of action is consistent or inconsistent with what a person considers to be right and proper for themselves. [1124] A society codifies this to a large extent through laws/norms and also sanctions misconduct through these very laws/norms.

This is precisely what the filter of the super code does by giving the AI rules that it must not violate. One could argue that this is the same as the process by which parents explain to their children what they are allowed to do and what they are not allowed to do, because this education develops a conscience in the child. This raises the question of whether AI can acquire a conscience through embedded law/the Super Code.

If the answer to this question is yes, the next philosophical question would be whether AI can attain consciousness.

1124 https://de.wikipedia.org/wiki/Gewissen, accessed on October 11, 2024.

J. Bibliography

2001: A Space Odyssey (1968).
Ahlberg BeckOK Urh, 32nd ed. 15.9.2021, UrhG § 2 Rn. 55
Ahlberg/Lauber-Rönsberg, BeckOK UrhR, 38th ed. May 1, 2023, UrhG § 23, margin note 10.
Albrecht, VD 06/2006, 143, 144.
Aldridge, High-Frequency Trading, 2nd ed 2013, Gresser, Practical Handbook on High-Frequency Trading, 2016, Jaskulla BKR 13, 221, Kobbach BKR 13, 233, Schultheiß WM 13, 596, Kasiske WM 14, 1933, Kindermann/Coridaß ZBB 14, 178.
Algorithmic Trading and High-Frequency Trading. BaFin announcement, amended on December 13, 2017.
Alpert, CR 2000, 345, 347;
Amann/Brambring/Hertel, The Reform of the Law of Obligations in Contract Practice, 2002
Ambrosius, B. in: Däubler, W.; Bertzbach, M.: AGG, 2nd edition 2008, § 20 Rn. 40
Andrees/Bitter/Buchmüller/Uecker, in: Hoeren, p. 104,
Antoine, L. in: CR 2019, pp. 1–8.
Armbrü ster, C. in: Begemann, M.; Bruns, A. (eds.): Die Versicherung des Alterns (Insurance for Old Age), 2008,
Armbrüster, C.: Prohibition of discrimination and grounds for justification in the termination of private insurance contracts, expert opinion prepared on behalf of the Federal Anti-Discrimination Agency, May 2010, p. 6.
Asimov, The Bicentennial Man, 1978, (The Bicentennial Man And Other Stories, 1976).
Auer-Reinsdorff, ITRB 2006, 181.

Bachmann, R.; Kemper, G.; Gerzer, T.: Big Data – Curse or Blessing? Companies in the Mirror of Social Change, 2014, p. 2.
Bartl, Product Liability under the New EC Law ProdHaftG, Landsberg 1989, 142
Bartsch, CR 2000, 721, 722 ff.
Basedow, in: Munich Commentary on the Civil Code, Vol. 5/1: Law of Obligations, Special Part III/1, 7th edition, 2017, Section 309 No. 5 Marginal Note 8. 2017 edition, Section 309 No. 5 Marginal Note 8.
BASt, Legal consequences of increasing vehicle automation, 2012
Baumann/Wirtz, RDi 2024, p. 27.
Beck, JR 2009, 225, 229 f.
Beck: Japanese-German Center, Human-Robot Interactions from an Intercultural Perspective, 2011, p. 124, 126
Becker/Feuerstack, MMR 2024, p. 22.
Beckmann, R. M. in: Staudinger, BGB, 2014, § 453 BGB, margin number 37
Berger, C.: Jauernig, BGB, 14th edition, 2011, Section 453, Marginal Note 11
Berger/Stemper, WM 2010, 2289, 2294
Berz/Dedy/Granich, DAR 2002, 545.
Bettinger/Scheffelt, CR 2001, 729, 734.
Beuth, Zeitonline dated March 24, 2016, Microsoft Twitter users turn chatbot into racist. BGBl. I, p. 1693.
BGBl. II, 1977, p. 811 ff.
Bisges, MMR 2012, 574 (577 f.)
Bodungen/Gatzke, RDi 2022, p. 354.
Bodungen/Hoffmann, NZV 2015, 521, 524 ff.
Boerner, ZIP 2001, 2264, 2272.
Bomhard/Siglmüller, RDi 2024, 45, margin note 1.
Bonnmann/Erberich, in: Luther/Knot/Palm, Die Schuldrechtsreform (The Reform of the Law of Obligations), 2001, p. 106.
Borges, NJW 2018, 977.
Borges/Sesing, in: Matusche-Beckmann, Saar-Tage 2016: Legal Problems of the Information Society, 2018 (in print), 177, 187.
Bown, Liability for Defective Software in the United Kingdom, in: Software Protection 1/1986, 1, 12

Bräutigam/Klindt, NJW 2015, 1137
Bräutigam/Rücker, E-Commerce, 2016, 14 B III para. 64.
Bräutigam/Thalhofer in Bräutigam, Part 14, para. 120 *Brehm*, FS Niederländer, 1991, 233
Brehmer, Wille und Erklärung, 1992, p. 29, 80 et seq.
Breidenbach in: Breidenbach/Glatz, Legal Handbook LegalTech 2018, p. 235 ff.
Breidenbach in: Rethinking: Law 2018, pp. 38–41, 40. British copyright law: Designs and Patents Act 1988 *Brox*, General Part of the German Civil Code (BGB), 41st edition, 2017, margin note 83.
Brox/Walker, Law of Obligations AT, 36th edition, 2012,
Bruderer, H.: Invention of the Computer, Electronic Computers, Developments in Germany, England, and Switzerland. In: Milestones in Computer Technology. 2nd, completely revised and greatly expanded edition. Volume 2. De Gruyter, 2018, ISBN 978-3-11-060261-6; Glossary of Technical History, p. 408 (limited preview in Google Book Search, accessed on November 23, 2019).
Brüggemeier, DeliktsR margin no. 565 ff.
Brüggemeier, RabelsZ 66, 2002, 193 ff.
Brüggemeier, ZHR 152, 1988, 511, 525 f.
Brunotte, CR 2017, 583, 585 f.
Buchberger, ITRB 2014, 116, 117.
Büchting/Heussen, Beck's Legal Handbook, 10th edition, 2011, C.13 Tortious Liability, margin numbers 15 to 18.
Bydlinski, Grundzüge der juristischen Methodenlehre (Fundamentals of Legal Methodology), 2nd edition, 2011, p. 23.

C-26/22 and C-64/22, EU:C:2023:XXX "Residual debt discharge"
Clemens, NJW 1985, 1998
COM/2022/496 final
Copyright and Related Rights Act 2000
Cornelius, MMR 2002, 353, 354
Craig S. Smith: AI Hallucinations Could Blunt ChatGPT's Success. In: IEEE Spectrum, March 24, 2023. Retrieved on September 24, 2023 (English)

Dallmann/Busse ZD 2019, 394 (395)
Dauner-Lieb, in: Dauner-Lieb/Langen, BGB Schuldrecht (German Civil Code, Law of Obligations) Volume 2/1, 2nd edition, 2012, Section 276, margin note 10.
Deselby, Journal of dyslexic programming 13 (2017), 131 ff.;
Deutsch, NJW 1978, 1998, 2000.
Deutsch/Ahrens, Deliktsrecht, 6th edition 2014, margin number 7
Dieker ZD 2024, 132, 135, beck-online
Dietrich, Product monitoring obligation and duty of producers to prevent damage, 1994
Dietrich, ZUM 2010, 567 ff.
Dreier, T. / Schulze, G. op. cit., margin no. 20
Dreier, T. / Schulze, G.: Copyright Act, 2nd edition, Section 69a, margin number 12.
Dreier, T.: Copyright, 2nd edition, § 69a, margin number 14.
Dreier/Schulze/Dreier, 7th edition 2022, UrhG § 44b, margin number 7.
Dreier/Schulze/Dreier, UrhG § 69c, margin number 27.

E. "Cyborg" et al. Section 14 MPG in conjunction with the Medical Device Operator Ordinance.
Ehinger/Grünberg K&R 2019, 232 (236)
Ensthaler, J. in: NJW 2016, pp. 3473–3552, (3473).
Draft EU Directive on AI Liability (COM/2022/496 final)
Epping, V.: Grundrechte (Fundamental Rights), 7th edition 2017, margin number 770.
Erdmann FS v. Gamm, 1990, 389 (399 f.))
Erman, in: Hefermehl/Werner, BGB, 9th edition, 1993, Section 11 No. 10 AGBG margin number 36.
Ernst, in: Paal/Pauly, DS-GVO BDSG, 3rd edition 2021
Ertel, W.: Grundkurs Künstliche Intelligenz (Basic Course on Artificial Intelligence), 4th edition 2016, pp. 132, 258, 300, 331, 333.

Recital 12 AI Regulation. Recital 14 Directive (EU)
2016/943.
Recital 18, subparagraph 1, sentence 4 DSM Directive; BT-Drs. 19/27426, 87.
Recital 47, amended OJ 2018 L 127, p. 2.
Recital 49 AI Regulation.
Recital 51.
Recital 52 AI Regulation.
Recital 70 AI Regulation.
Recital 71 GDPR.
Recital 71 AI Regulation.
Recital 72 of the AI Act.
Recital 9 of Directive (EU) 2019/790 of the European Parliament and of the Council of April 17, 2019
Esser, JZ 1953, 129.
Etteldorf, MMR-Aktuell 2023, 456626.
Euclid, The Elements, edited by Thaer, C., 1st edition 2011, § 2 Eurex Circular
213/13 of September 27, 2013.

Faust, BGB AT, 6th edition 2018, § 2 Rn. 4
Finke, The Effects of European Standards and Safety Law on National Liability Law, 2001, p. 9 ff.
Fleck/Thomas, NJOZ 2015, 1393, 1397
Foerste, DB 1999, 2199, 2200
Foerste, in: Foerste./v. Westphalen, Product Liability Handbook, 3rd edition, 2012, Section 24, margin note 37
Foerste, in: Foerste/Graf v. Westphalen, HdB Produkthaftung (Product Liability Handbook), § 24
Foerste, in: Foerste/v. Westphalen, Product Liability Handbook, 3rd edition, 2012, § 24
Frenz/van den Broek, NZV 2009, 530
Frisse, F./ Glaßl, R./ Baranowski, A./ Duwald, L. in: BKR 2018, p. 177.
Fritzemeyer, in: Lehmann/Meents, Handbook for Specialist Lawyers in Information Technology, 2nd edition, 2011, Chapter 2, margin number 70
Fukushima, Bio.Cybernetics 36, 193–202 (1980)
Funk/Wenn, CR 2004

G.J. Leasing Co. v. Union Elec. Co. (1995) 54 F. 3d 379, 386 (7th Cir. 1995).
Gasser, VKU 2009, 224.
Geminn, ZD 2021, p. 354.
Generative AI: a game-changer society needs to be ready for. In: World Economic Forum.
Giedke, Cloud Computing: An Economic Analysis with Special Consideration of Copyright Law, Munich 2013, 402 ff.
Giedke, p. 382 ff.
Gigerenzer, G./ Todd, P. M.; ABC Research Group: Simple heuristics that make us smart. Oxford University Press, New York 1999.
Gleß/Weigend, ZStW 126, 2014, 561, 585 f.
Gola in Gola/Heckmann, General Data Protection Regulation – Federal Data Protection Act, 3rd edition 2022, Art. 4 margin no. 35.
Gola/Heckmann/Schulz, 3rd edition 2022, GDPR Art. 6 margin note 152 with reference to the statement by the EU Commission.
Gola/Schomerus, BDSG, 11th edition, 2012, Section 3, margin number 21, 26.
Görgülü et al., BKR 2024, p. 175.
Grätz, Artificial Intelligence in Copyright Law, 2021, p. 10
Greger, NZV 2018, 1 ff.
Grigoleit/Herresthal, BGB AT, 3rd ed. 2015, margin no. 6
Groß, InTeR 2018,
Groß, Capital Market Law: Commentary on the Stock Exchange Act, 6th edition 2016, Section 26d margin number 1–4.
Groß/Gressel, NZA 2016
Grosskopf, L.: IPRB 2011, p. 259 (259);

Gruber, in Hilgendorf (ed.), Robotics in the Context of Law and Morality, 2014, pp. 123, 156, 198
Grundmann, in: Münchener Kommentar BGB Vol. 2: Law of Obligations, General Part (§§ 241 - 432), 7th ed. 2015, § 276 para. 150 to 163.
Grunsky, NJW 1983, 2465.
Grünvogel, MDR 2017, 973, 974.
Grützmacher in Wandtke/Bullinger, UrhG, 6th edition 2022, § 69 c
Grützmacher, CR 2011
Grützmacher, CR 2015
Grützmacher, CR 2015, 779-787
Grützmacher, CR 2016
Grützmacher, M. in: Wandtke, A. / Bullinger, W.: UrhG (German Copyright Act), 4th edition, 2014, Section 69a,
Günther/Böglmüller, BB 2017, 53 to 58.

Haberstumpf in Lehmann, Chapter II, margin number 15, 30
Hägele/Schäfer, in: Gevatter/Grünhaupt (eds.), Handbook of Measurement and Automation Technology in Production, 2006.
Hagemeier, BeckOK UrhR, 38th ed. 01.02.2023, UrhG § 44b margin no. 1.
Hager, in: Staudinger, BGB, 2009, § 823 margin no. 26, each with further references.
Hanisch, in: Hilgendorf (ed.), Robotics in the Context of Law and Morality, 2014
Harris, "The Fear Index" 2011
Härting, ITRB 2016, pp. 209–211.
Hartung, J. in: Kühling, J.; Buchner, B.: DS-GVO/BDSG, 2nd edition 2018, Art. 28, margin note 22.
Hauck, R.: NJW 2014, p. 3616 (3616)
Heckmann, D. in: Heckmann, D.: jurisPK-Internetrecht, 5th edition 2017, Chapter 9 1. Revision margin number 214.
Heine/Frank, NZA 2023, p. 1281.
Heinz, Deep Learning – Part 1: Introduction, footnote 11.
Herbst in Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, on the individual processes.
Herfurth ZD 2018, 514 (517)
Hermeier et al., 2018, p. 10
Hessel/Dillschneider, Data protection challenges in the use of AI, RDI 2023, 459, 461
Hessel/Dillschneider, RDI 2023, 458, 460.
Hetmank, S. / Lauber-Rönsberg, A. in: GRUR 2018, p. 574.
Heun, W.: Art. 3, margin nos. 70–71. In: Dreier, H. (ed.): Grundgesetz Kommentar: GG. 3rd edition. Volume I: Preamble, Articles 1–19. Tübingen, Mohr Siebeck 2013
Heydn, MMR 2020, 435
Heymann, GRUR 2012, 814 (815 margin no. 39, 42 et seq.)
Heymann, in: CR 2016, pp. 650–657 (650).
Hieke, R. in: InTeR 2017, pp. 10, 11 et seq.; on Sections 377, 381 (2) HGB
Hiéramente, BeckOK GeschGehG § 2
Hilber/Paul/Niemann, Part 3, margin note 94
Hilgendorf, in: Beck (ed.), Beyond Man and Machine, 2012, p. 119, 125 ff.
Hilgendorf, JZ 2021, p. 444 (447)
Hoeren, IT Legal Script, as of Oct. 2018,
Hoeren, IT Contract Law 2018,
Hoeren, IT Law, as of Oct. 2018, p. 184.
Hoeren, MMR 2016, 8, 10
Hoeren, RdV 1988, 115, 119
Hoeren, Software liability within the European Communitÿische Gemeinschaft, in: Handbook of Modern Data Processing, Issue 146/1989, 22, 30 f.
Hoeren, T. in: CR 2004, 721–724.
Hoeren, T.; Völkel, J. in: Hoeren, T.: Big Data and Law, 2014, p. 22.
Hoeren, T.; Wehkamp, N. in: CR 2018, pp. 1–7.
Hoeren/Sieber/Holznagel MMR-HdB, Part 29 Rn. 17, beck-online

Hoeren/Wehkamp, CR 2018, 1–7.
Honsell, in: Staudinger, BGB 13th edition, § 463 (old version) margin note 48 ff
Hoppen, P. in: CR 2015, p. 802 (803)
Horner/Kaulartz, CR 2016, 7.
Horner/Kaulartz, InTeR 2016, 22, 24.
https://www.zeit.de/news/2021-10/09/von-ki-vollendete-10-sinfonie-von-beethoven-uraufge-fuehrt?utm_refe-rrer=https%3A%2F%2Fwww.google.com%2F
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gut-achten_pdf.pdf?_blob=publicationFile&v=2,
https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html, accessed on December 17, 2018.
https://www.kaggle.com/c/titanic (last accessed on March 3, 2020)
http://www.patentochmarknadsoverdomstolen.se/Domstolar/pmod/2018/Svea%20HR%20PMT%2022-17%20Ej%20slutligt%20beslut%202018-04-03.pdf (last accessed on December 10, 2018), see margin note 19.
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_DE.pdf. https://www.heise.de/hintergrund/Was-darf-KI-Stockfotograf-und-KI-Verein-streiten-um-das-Copyright-8984836.html (accessed on July 6, 2023). https://www.schufa.de/ueber-uns/presse/pressemitteilungen/schufa-loescht-restschuldbefreiung-sechs-monaten/ (accessed on 07.07.2023).
https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_High-frequency trading_final_web.pdf, accessed on October 24, 2018.
http://blog.audi.de/2015/05/26/per-autopilot-durch-die-megacity-shanghai/ (last accessed on January 24, 2016).
http://de.wikipedia.org/wiki/Software_as_a_Service (accessed on October 28, 2022).
https://de.serlo.org/informatik/baustelle/algorithmen-ist-algorithmus, accessed on March 3, 2020.
https://de.wikipedia.org/wiki/Chatbot, accessed on October 11, 2024.
https://de.wikipedia.org/wiki/Gewissen, accessed on October 11, 2024. https://de.wikipedia.org/wiki/Maschinelles_Lernen
https://developers.google.com/search/docs/crawling-indexing/robots/intro?hl=de (accessed on July 6, 2023). https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31996L0009 (accessed on July 6, 2023). https://laion.ai/about/ (accessed on July 6, 2023).
https://saasoptics.com/saaspedia/saas-subscription-models/ (accessed on October 28, 2022).
https://www.alamy.com/enterprise/ (accessed on 06.07.2023).
https://www.alltageinesfotoproduzenten.de (accessed on 06.07.2023).
https://www.bdzv.de/service/presse/branchennachrichten/2023/wiener-erklaerung-deutschsprachige-verlegerver-baende-verabschieden-gemeinsamen-forderungskatalog?sword_list%5B0%5D=Lizenz&no_cache=1 (accessed on 07/06/2023).
https://www.gettyimages.com/photos/holding (accessed on 06.07.2023).
https://www.heise.de/newsticker/meldung/Algorithmen-und-Scoring-Maas-fordert-digitales-Anti-Diskriminie-rungsgesetz-3761722.html?seite=2, accessed on October 11, 2024.
https://www.mind-verse.de (accessed on July 6, 2023).
https://www.mvfp.de/nachricht/artikel/tagesspiegel-verlage-fordern-lizenzgebuehren-wegen-chatbot-suchmaschi-nen (accessed on July 6, 2023).
https://www.profifoto.de/szene/notizen/2023/02/21/laion-droht-kneschke/ (accessed on July 6, 2023).
https://www.europarl.europa.eu/committees/de/juri/subject-files.html?id=20150504CDT00301 , last accessed on July 27, 2018.
https://www.openai.com (accessed on 06.07.2023); www.businessinsider.com (accessed on 06.07.2023)
http://www.unece.org/trans/conventn/legalinst_08_RTRSS_RT1968.html available (last accessed on January 24, 2016).
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gut-achten_pdf.pdf?_blob=publicationFile&v=2,
https://www.archives.gov/milestone-documents/14th-amendment]
https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/
https://gemini.google.com/app
https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/ https://noyb.eu/de/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai

https://treaties.un.org/doc/Publication/CN/2015/CN.529.2015.Reissued.06102015-Eng.pdf (as of February 5, 2016).
https://www.bast.de/DE/BASt/BASt_node.html;jsessionid=905ABC3FD1F06FA5F8CD8E1F99925695.live2051 (last accessed on January 24, 2016).
https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/
https://www.unece.org/leginstr/cover.html (last accessed on December 29, 2015).
http://t3n.de/news/facebook-ki-bilderkennung-chrome-781194/, accessed on May 11, 2020.
https://www.heise.de/ct/ausgabe/2017-11-Kuenstliche-Intelligenz-macht-Bildbearbeitung-intuitiv-3705914.html, accessed on May 11, 2020.
http://www.grur.org/de/stellungnahmen.html; a. A. *Redeker, S. S.; Pres, S.; Gittinger,* C.: WRP 2015, p. 681, margin note 7.
https://www.golem.de/news/google-brain-algorithmus-macht-ge-sichter-auf-schlechten-bildern-erkennbar-1702-126066.html, accessed on May 11, 2020; https://netzpolitik.org/2016/verpixelung-macht-unsichtbar-oder-doch-nicht, accessed on May 11, 2020
https://www.heise.de/newsticker/meldung/eBay-Produkte-mithilfe-von-Fotos-suchen-und-kaufen-3784371.html, accessed on May 11, 2020.

ISO 10218-1 "Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots"
ISO 10218-2 "Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration."
ISO/DIS 13482 "Robots and robotic devices – Safety requirements for non-industrial robots – Non-medical personal care robots"
ISO/TS 15066 "Robots and robotic devices – Safety requirements for industrial robots – Industrial collaborative workspace"
Israel, JW 1902, 238, 240

Jaeger, CR 2002, 309 (311)
Jänich/Schrader/Reck, NZV 2015
Jarass, H.: Art. 3, Rn. 1b. In: Jarass, H.; Pieroth, B.: Basic Law for the Federal Republic of Germany, Commentary, 28th edition, C. H. Beck, Munich 2014.
Jaskulla, BKR 2013, p. 221
Jauernig, Commentary on the German Civil Code (BGB), 7th edition, 2010
Junker, Computer Law, 3rd edition, 2003
Junker, WM 1988, 1217 ff., 1249 ff.

Käde, Creative Machines and Copyright, 2021, p. 183
Kalbfus, B.: GRUR 2016, p. 1009.
Kamanabrou, RdA 2006, p. 321, 338.
Karl, C.: The Scope of Copyright Protection for Computer Programs, 2009, p. 191 f.
Kasiske, WM 14, 1933, Kindermann/Coridaß ZBB 14, 178.
Katharina Miklis: From Bielefeld? No way! In: der Freitag. April 7, 2010.
Katharina Zweig: It was AI!: From absurd to deadly: The pitfalls of artificial intelligence
Kersten, JZ 2015
Kindermann, Coridass, ZBB 2014, p. 178
Kirchner, InTeR 2018,
Kirsch, CT Magazine for Computer Technology No. 22, 2011, 43.
Kischel, U.: Art. 3, para. 91. In: Beck'scher Online-Kommentar GG, 34th edition 2017
Kitz, in: Hoeren/Sieber/Holznagel, Part 13.1 margin number 37.
AI Regulation p. 14, April 21, 2021.
Klein, DSRITB 2015, 429, 438.
Klindt, BB 2009, 792, 793
Koch, AcP 203, 2003, 603, 624 ff., 631 f.
Koch, Computer Contract Law, 6th edition, 2002, margin number 1346.
Koch, CR 2001, 574.
Koch, NJW 2004, 801, 802

Koch, Insurability of IT Risks, 2005, margin no. 185 et seq., 355 et seq., 632 et seq.
Köhler, AcP 182, 1982, 126
Köhler, AcP 182, 1982, 126, 135.
Koziol, ÖBA 1987, 3
Kriesel, A Brief Introduction to Neural Networks. (July 1, 2024).
Krystal Hu, ChatGPT sets record for fastest-growing user base - analyst note. In: Reuters. February 2, 2023 (reu-ters.com [accessed on July 12, 2023]).
Kühling, NJW 2017, p. 1985, 1988.
Kühling/Martini et al., The GDPR and national law, 2016, p. 441.
Kuhnert, in: Haus/Krumm/Quarch, Gesamtes Verkehrsrecht (Complete Traffic Law), 2nd edition, 2017, Section 7 StVG Rn.
Kuschel/Asmussen/Golla/Hacker, Intelligent Systems – Intelligent Law, 2021, p. 227 ff.

Lange, NZV 2017, 345.
Larenz, General Part of German Civil Law, 1960, § 19 I.
Larenz, Methodology of Jurisprudence, 6th edition, 1991, p. 5
Laurin Meyer: ChatGPT reaches the next stage of development. Die Welt, March 17, 2023. Page 10.
LeCun et al, Gradient-Based Learning Applied to Document Recognition, Proc. of the IEEE, November 1998.
Leipold, BGB I, Introduction and General Provisions, 9th edition, 2017, Section 10, margin note 17.
Leistner, FS Dreier 2022, 87 (90 f.).
Lesshaffi, K. / Ulmer, D. in: CR 1993, p. 607 (608)
Lewke, InTeR 2017, 207 to 216.
Liebing, BB 1983, 667
Lippert, in: Deutsch/Lippert/Ratzel/Tag, MPG, 2nd edition, 2010, Section 2 MPBetreibV margin number 1 et seq.
Loewenheim in Schricker/Loewenheim, UrhR, 6th edition, 2020, Section 69a, margin number 2
Loewenheim, U. / Spindler, G. in: Schricker, G. / Loewenheim, U.: UrhG, 5th ed. 2017, § 69a, margin no. 5.
Lohmann, ZRP 2017, 168, 169.
Luhui Hu: Generative AI and Future. In: Medium. November 15, 2022.
Lutz, DAR 8/2014, 446, 448.
Lutz, NJW 2015
Lutz, Software Licenses and the Nature of the Matter, Munich 2009, 164 f.
Lutz/Tang/Lienkamp, NZV 2013, 57, 61.

Mansel, in: Jauernig, § 611 BGB Rn. 13
Markets in Financial Instruments Directive II – MiFID II
Marly, GRUR 2012,
Marly, in: GRUR 2011
Marly, J.: Practical Handbook on Software Law, 5th edition, 2009, margin number 398.
Marly, Practical Handbook on Software Law, 6th edition, 2014, margin number 1861
Marly, Practical Handbook on Software Law, 7th edition, 2018, margin number 1087
Marly, Software Transfer Agreements, 7th edition, 2018,
Martin, Property Insurance Law, 4th edition, 2022, Section B III, margin number 4.
Martini in: Paal/Pauly, DS-GVO BDSG, Art. 22, margin note 15
Martini, JZ 2018, 1017 to 1025.
Mattig, WM 2014, p. 1940.
Matusche-Beckmann, in: Staudinger, 15th edition 2014, Section 434 margin number 73
Mayiner, Die künstliche Person (The Artificial Person), 2017,
Medicus, Civil Law. 30th ed. 2025, margin no. 45.
Mehlhorn, K. / Sanders, P.: Algorithms and Data Structures, 2008, p. 26.
Meier/Wehlau, CR 1990, 95, 97 *Mestmäcker/Schulze/Haberstumpf* § 69a margin number 3; on DIN 44300 *Milstein/Lippold*, NVwZ 2013, 182, 184 f.
MMR, "Artificial neural networks: How AI learning structures should be viewed from a legal perspective" 2021, 111
MMR-Aktuell 2023, 456626.
Möhring, P. / Nicolini, K.: Copyright Law, 2nd edition, Section 69a, margin number 9.

Molitoris, NJW 2009, 1049, 1050 f.
Moorstedt, Intelligence out of control, SZ.de dated October 11, 2018, accessed on October 24, 2018.
Mortenson v. Timberline Software Corporation, Supreme Court of Washington (140 Wash. 2.d. 568, 998 P.2d 305).
Möschel, AcP 186, 1986, 187, 197 ff.
MüKo/Wendehorst, BGB, 9th edition 2022,
Müller-Glöge, in: MüKo-BGB, 6th ed. 2012, § 611 BGB Rn. 23
Müller-Hengstenberg/Kirn, MMR 2014, 307, 311
Müller-Hengstenberg/Kirn, NJW 2014, 307, 311.
MünchKomm-BGB/Thüsing, 5th edition 2007, Section 20 AGG Rn. 55

Nägele/Jacobs, ZUM 2010, 281 (286)
Nielsen, M.: Neural Networks and Deep Learning. Determination Press, http://michaelnielsen.org, accessed on May 11, 2020.
Niemann, CR 2009, 661 (662 f.)
Niemann, in Hilber, Handbook of Cloud Computing, Cologne 2014, pp. 290 and 293
Niemann/Paul, K&R 2009, 444 (448)
NJW 2018, 2956= MDR 2018, 1116
NZI 2023, p. 399.

Obergfell FS Windbichler, 2020, p. 1397 (1403 f.)
Oellinger, in: Achleitner/Everling (eds.), Legal Issues in Rating, 2005, p. 360.
Oetker, in: MüKo/BGB, 4th edition, § 249
Oetker, in: Munich Commentary on the Civil Code Vol. 2: Law of Obligations, General Part, 7th edition 2015, § 249 marginal no. 96.
Olbrich/Bongers/Pampel GRUR 2022, 870
Osborne Clarke: Analysis of the new EU liability directives

Paal, JuS 2010, 953, 954 f.
Paal, ZfDR 2024, 129, beck-online.
Paal/Pauly/Martini, 3rd edition 2021, GDPR Art. 26 margin note 19
Pahlow, L. in: JA 2006, p. 385 (385)
Palandt/Grüneberg, BGB, 72nd edition, 2013
Palandt/Grüneberg, BGB, 83rd edition, 2024
Palandt/Heinrichs, 67th edition, 2008
Palandt/Heinrichs, 72nd edition, 2013
Palandt/Heinrichs, 77th edition, 2017
Palandt/Putzo, 77th edition 2017, § 439 margin number 3.
Palandt/Thomas, 77th edition, 2017, § 823 margin number 4.
Patzak, A./ Beyerlein, T. in: MMR 2007, p. 687 (688)
Paul/Niemann in Hilber, Handbook of Cloud Computing, 1st edition 2014, Part 3
Peschel, C.; Rockstroh, S. in: MMR 2015, p. 571 ff. (572).
Peschel/Rockstroh, MMR 2014, 571, 576.
Peters, in: Staudinger, BGB 13th ed. § 635 (old version) margin no. 55.
Pick-a-Pic: An Open Dataset of User Preferences for Text-to-Image Generation – Stability AI.
Pieper, BB 1991, 985, 988
Pieper, InTeR 2018,
Pohle/Ammann, CR 2009, 273 (276)
Pohle/Ammann, K&R 2009, 625 (626).
ProdHaftG (Product Liability Act) of December 15,
1989, BGBl. I, p. 2198.
Pröless, in: Pröless/Martin, Insurance Contract Act, 28th edition, 2010, Section 1 AHB margin number 15.
Prütting, H./Wegen, G./Weinreich, G.: BGB Commentary, AGG § 19 AGG – Civil law prohibition of discrimination, margin no. 7.
Pukas, GRUR 2023, 614

Puppe, Kleine Schule des juristischen Denkens (A Short Course in Legal

Thinking), 2nd edition, 2011, p. 4. Source: ChatGPT.
Source: LAION e. V.

Rashid, T.: Neuronale Netz selbst programmiert (Self-programmed neural networks), 1st edition 2017
Raue/Hegemann, MAH UrhR, § 3 Copyright restrictions, margin note 40.
Rauer/Bibi BeckOK Copyright, Götting/Lauber-Rönsberg/Rauer 41st edition, as of February 15, 2024, § 2
Rauer/Bibi, BeckOK UrhR UrhG § 2 margin note 61.
Edited by beck-aktuell, becklink 2026476. *Redeker*,
Handbook of IT Contracts, 1.5 margin note 27 *Redeker*, IT
Law, 5th edition 2012, margin note 830
Reed, Product Liability for Software, in: Computer Law & Practice 4 (1988), 149 ff. *Reiter/Methner*, in:
Taeger (ed.), Smart World - Smart Law?, 2016, p. 453, 458 *Resuch/Weidner*, Future Law, 2018
Directive (EU) 2019/790, 96/9/EC, and 2001/29/EC. Directive
2000/43/EC,
Directive 2001/29/EC
Directive 2004/112/EC
Directive 2004/39/EC
Directive 85/374/EEC *Riehm*,
ITRB 2014, 113.
Rimscha, M.: Algorithms compact and understandable – Solution strategies on the computer, 4th edition 2017, p. 3. Directive
91/250/EEC of May 14, 1991, replaced by consolidated version as Directive 2009/24/EC
Rö dl, F. in: Rust, U. Falke, J.: AGG, 2007, § 20 Rn. 26 f
Rohe, AcP 201, 2001, 118, 134 ff.
Roloff, BeckOK ArbR, AGG § 15 margin note 1–3.
Roßnagel, NJW 2017, 10
Rüthers, Legal Theory, 4th edition, 2010, p. 25.
Rüthers/Fuscher/Birk, Legal Theory with Legal Methodology, 10th edition, 2018.

S. Beck, in: Spranger (ed.), Current Challenges in Life Sciences, 2010, p. 95, 102 ff.
S. Beck, JR 2009, 225, 229 f.
Saenger, in HK-BGB, 9th ed. 2017, § 434 margin no. 11.
Schack, GRUR 2021, 904, 907
Schade, ZD 2014, p. 306, 309,
Schaub, JZ 2017, 342, 348 Scheja, K.
in: CR 2018, p. 485.
Schellhammer, Law of Obligations Based on Claims, 11th ed. 2021 *Schellhammer*, Law of
Obligations Based on Claims, 8th ed. 2011 *Schermaier*, JZ 98, 857.
Schiek, D. in: Schiek, D.: AGG, 2007, § 20 Rn. 8;
Schiemann, in: Staudinger, BGB 13th edition, preliminary remarks on Sections 249 et seq.
Schild in BeckOK Data Protection Law, 48th edition, May 1, 2024, Art. 4 GDPR margin number 36.
Schmidt, B./ Freund, B. in: ZD 2017, p. 14 (16)
Schneider, J. in: Schneider, J.: Handbook of IT Law, 5th edition, 2017, G. margin no. 79
Schneider/Gü nther, CR 1997, 389 ff.
Schnitzler: Online Communication in Recruiting for SMEs: Maturity Levels of Employer Branding & Candidate Experience, Springer Gabler, 2020, pp. 24-25
Letter from BaFin dated May 21, 2013.
Schreiber, S. B.: Natural intelligence. Neurons and synapses – just an organic computer? (Part 1), c't – Magazine for Computer Technology, 1987 (4), p. 98 ff.
Schricker/Loewenheim, Copyright, 6th edition, 2020, Section 16, margin number 21.

Schricker/Loewenheim/Loewenheim/Leistner margin note 40
Schröder, Data Protection Law in Practice, 2nd edition, 2016, Chapter 3: Data Protection in Human Resources/Employee Data Protection.
Schuhr, in: Hilgendorf (ed.), Robotics in the Context of Law and Morality, 2014, pp. 13, 17.
Schulte, NJW 2014, 1238, 1238
Schulte-Nölke, Karlsruhe Forum 2015, 3 ff. with further references.
Schultheiß, WM 2013, p. 596
Schulz in Gola/Heckmann, General Data Protection Regulation – Federal Data Protection Act, 3rd edition, 2022, Art. 6
Schulz, Responsibility in Autonomously Acting Systems, p. 104
Schuster/Reichl, CR 2010, 38 (40 f.)
Schweighofer, in: Schweighofer/Menzel/Kreuzbauer, Auf dem Weg zur ePerson (Towards the ePerson), 2001, p. 45, 49 ff.
Siedersleben, J. (ed.): Software Engineering, Hanser, 2003, p. 44 ff.
Sieg, BB 983,1187.
Silke Hahn: OpenAI introduces GPT-4: Language model now also understands images. In: heise online (heise.de). March 14, 2023, accessed on March 15, 2023.
Simitis BDSG, 8th edition 2014, Section 3, margin number 102.
Söbbing, "The fairy tale of the evil algorithm or legal questions regarding discrimination by artificial intelligence (AI)" RTLaw 2020, 62–69.
Söbbing, Fundamental Legal Issues of Artificial Intelligence, 1st edition 2019, pp. 11–14. *Söbbing*, Fundamental Legal Issues of Artificial Intelligence, in: CR 2020, pp. 223–228. *Söbbing*, InTeR 2018, pp. 64–67.
Söbbing, ITRB 2018, pp. 161–163.
Söbbing, ITRB 2021, pp. 168–171.
Söbbing, ITRB 2024, 184.
Söbbing, Possible legal protection for AI output under the UrhG or GeschGehG – Does the output of generative chatbots such as ChatGPT enjoy legal protection? ITRB 2024, 184–188
Söbbing, Legal limits for AI decisions in the context of autonomous driving, RDi 2023, 239
Söbbing, Adoption of the European AI Regulation – Presentation of key points of the AI Regulation and criticism ITRB 2024, 108–111.
Söbbing/Schwarz, in Data Processing Law Beck-Verlag, ZD 2023, 579.
Söbbing/Schwarz, Copyright limits for learning artificial intelligence on questions of text and data mining (§ 44b UrhG) RDi 5/ 2023, 415
Söbbing/Schwarz, Does machine learning violate the GDPR when reading the internet? ITRB 2024, 212–217.
Söbbing/Schwarz, ZD 2024, 160.
Sodtalbers, Software Liability on the Internet, 2006, para. 513, 518.
Soergel, in: Munich Commentary on the Civil Code Vol. 5/1: Law of Obligations, Special Part III/1, 7th edition, 2017, Section 635 (old version) para. 39 with further references.
2017 edition, Section 635 (old version) margin number 39 with further references.
Sosnitza, CR 2016, 764, 772
Späte, Commentary on the General Insurance Conditions for Liability Insurance, 1993, § 1 AHB Rn. 49.
Specht-Riemenschneider FS Taeger, p. 711 (717 f.).
Spindler FS Schack 2022, p. 340 (343)
Spindler in Schricker/Loewenheim, UrhG, 6th edition 2020, § 69c, margin number 41–41c.
Spindler in: BeckOK BGB, 40th edition, as of May 1, 2016, Section 827 BGB margin number 1.
Spindler, CR 2015, 766 to 776.
Spindler, GRUR 2016, 1112, beck-online.
Spindler, in: BeckOGK/BGB, Section 823
Spindler, in: BeckOK BGB, 40th ed., as of May 1, 2016, § 827 BGB Rn. 1.
Spindler, in: Hilgendorf (ed.), Robotics in the Context of Law and Morality, 2014, p. 63, 66 f.
Spindler, in: Kullmann/Pfister, Producer Liability, Product Liability in the IT Sector, forthcoming *Spindler*, in: Lorenz, Karlsruhe Forum 2010: Liability and Insurance in the IT Sector, 2011, p. 26 ff. *Spindler*, Robots, CR 2015, 766 to 776.

Spindler/Schuster/Spindler/Dalby, 4th edition 2019, DS-GVO
Spindler: BeckOGK/BGB, Section 823, marginal number 607.
Spiro, Liability for vicarious agents, 1984, p. 209 ff.
Spoerr, BeckOK Data Protection R 46. Ed. 1.5.2022, GDPR Art. 26 margin note 17
Spoerr, W. in: Wolff/Brink, Beck'scher Onlinekommentar, as of November 1, 2017, Art. 28 GDPR, margin note 30 et seq.
Sprau, in: Palandt – Commentary on the German Civil Code (BGB), 77th edition, 2017, Section 1 ProdHaftG margin number 17.
Staudenmayer, NJW 2023, p. 894, para. 8.
Staudinger/Coester/Waltjen, BGB, Section 11 No. 6 AGBG para. 27
Steiner in C't 7/2023 16–17 (16).
Stiemerling, O. in: CR 2015, p. 762.
Stoffels, AGB-Recht, 5th ed. 2024
Stuurman, Product liability for software in Europe. A discussion of the EC Directive of July 25, 1985, in: Vanden-berghe (ed.), Advanced Topics of Law and Information Technology, Deventer 1989, 110, 112 ff.

T 1814/07, OJ 2003, p. 352.
T 208/84, OJ 1987, p. 14. T
258/03
T 641/00
Taeger (ed.), Internet of Things – Digitization of Economy and Society, 2015, pp. 429, 436
Taeger, Non-contractual liability for defective computer programs, 1995, p. 259 et seq.
Taschner, Product Liability, 1986, 84
Taschner/Frietsch, ProdHaftG, 2nd edition, 1990, introduction, margin note 89
Thomale, P.-C. in: Auernhammer, DS-GVO/BDSG, 5th edition, 2017, Art. 28, margin note 8.
Thüsing, in: v. Westphalen, Contract Law and General Terms and Conditions, 41st edition, April 2018, margin note 18.
Tiedtke, in: FS Gernhuber, 1993, p. 471, 480 f.

Ulmer, ZHR 152, 564, 579
Ulmer/Brandner/Hensen, 4th edition 1999, § 11

v. Bar, in: v. Bar, Product Responsibility and Risk Acceptance, 1998, p. 29, 36.
v. Pentz, AfP 2017, 102, 115.
v. Welser GRUR-Prax 2023, 2023, 57 (58))
v. Westphalen, DB 1999, 1369, 1370
v. Westphalen, DB 2001, 799, 802.
Verhoeven, 2020, p. 103.
Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828
VkBl 1970, 797, 798 f.
Vogt, NZV 2003, 153
Voigt, P.: Other industry-specific regulations on IT security. In: Voigt, P.: IT Security Law, 1st edition 2018.
Volhard/Jang in W/B/A| KAGB § 36 Rn. 20-24| , 3rd edition, 2021

Wagner, in: MünchKomm/BGB, 6th edition 2013, § 823
Walter, SVR 2006, 41, 69.
Wandtke/Bullinger/Bullinger margin note 16a; Schmoll/Graf Ballestrem/Hellenbrand/Soppe GRUR 2015, 1041 (1042)).
Wandtke/Bullinger/Grützmacher, Section 69c
Weichert, ZRP 2014, 168
Weidenkaff, in: Palandt, § 611 BGB margin note 15 f.
Weise, P./ Brandes, W./ Eger, T./ Kraft, M.: Neue Mikroökonomie, Physica, Heidelberg 2005, p. 22.
Weisser/Färber, MMR 2015, 506, 511.
Wendehorst, Christiane: "Regulatory Challenges for AI Products," MüKo-Digitalrecht, 2022.

Wendehorst, NJW 2016, 2609.
Wendehorst/Gritsch in: Omlor/Link, Kryptowährungen und Token, II. Datenschutzrechtlicher Befund, 2nd, updated and expanded edition 2023, para. 57.
Wendtland, BeckOK BGB47. Ed. 01.08.2018, BGB § 119 Rn. 28, 29.
Wendtland, in: Bamberger/Roth (eds.), BeckOK BGB, 42nd edition, as of February 1, 2017, § 130 margin number 10.
Westermann, BGB, 7th edition 2016, § 434 margin note 18 f.
Wettig/Zehendner, AI Law 12, 2004, 111, 127 ff.
Whittaker, European Product Liability and Intellectual Products, in: LQR 105 (1989), 125, 138 ff.
Wiebe, CR 2013, 1; Grützmacher, Copyright, Performance and Sui Generis Protection of Databases, 1999, 340 et seq.
Wiebe, Electronic Declarations of Intent, 2002, p. 214 ff.
Wilke, Gewndolin/Bendel, Oliver: AI-supported recruiting – technical fundamentals, economic opportunities and risks, and ethical and social challenges, in: HMD. Praxis Der Wirtschaftsinformatik, Vol. 59, No. 2, 2022, doi:10.1365/s40702-022-00849-w, p. 653
Wobst, NZA-RR 2016, p. 508. para. 5, BeckOK ArbR/Roloff, margin no. 33. Sections 31, 278 BGB
Wolf/Horn/Lindacher, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (Law on the Regulation of General Terms and Conditions), 4th edition, 1999, Section 11 No. 6 AGBG Ed. 1999, Section 11 No. 6 AGBG
Wolff/Brink/v. Ungern-Sternberg in BeckOK Data Protection Law, 46th ed. 1.11.2023, Norm World Intellectual Property Organization, World Intellectual Property Organization *Wulf/Burgenmeister*, CR 2015, 404

Yoav Goldberg, Reducing Hallucination in Language Models, published on arXiv.org.

Zimmermann, The Law of Obligations, 1996, p. 1105 ff.
Zimmermann/Leenen/Mansell/Ernst, JZ 2001, 684, 690 f.
Zirn, Chatbots – what companies need to know, CIO Magazine, October 17, 2017.
Ziwie Ji et al.: Survey of hallucination in natural language generation. In: ACM Computing Surveys, 55(12), pp. 1–38, 2023 (English)
Zweig, K.: An algorithm has no sense of rhythm, 1st edition 2019, p. 140 ff.

K. Index

A
Adaptive Cruise Control 187
Activity Levels 266
Algorithm 21
Equivalence ratio 96
Asimov 281
Degrees of automation 186
Autonomous vehicle 186, 204
Auto completions 264

B
Proving 220
Burden of proof 220
Blank declaration 272
Credit reports 278
Bugs 217
Federal Highway Research Institute 186

C
Chatbot 263
Computer declaration 272
Computer program 22

D
Tortious liability 222

E
ECE regulations 192
Reception theory 274
Auxiliary agents 224, 276

F
Driver assistance systems 191
Negligence 224, 225, 226, 227, 246, 249, 250, 252
Manufacturing defects 215
Consequential damages 244, 250
Standard form contracts 96
Exemption from liability 252

H
Liability 249
HAL 9000 278
Highly automated driving 189
Force majeure 246

I
Indirect use 270
Individual negotiation 252 Integrated Surgical System 262

K
Cardinal duties 253
Design defects 215
Bodily injury 238, 239
Credit risk 276
Credit scores 215, 272

L
Leasing 195
Theory of interest 242

M
Machine learning 270
Consequential damages 243, 245
Reduction 99
Contributory negligence 226

N
Subsequent performance 99
Right of use 258

P
Parking assistant 187
Lump-sum compensation 254
Personal injury 238, 239, 250, 253
Prima facie evidence 237
Product monitoring 218
Product monitoring obligation 216

Product Liability Act 228

R

Reaction obligations 219
ROBODOC 262
Robots 210
Recall obligations 219

S

Liability for material defects 251
Property damage 242
SAP Core S/4HANA 279
Damages 99, 243
Categories of damage 242, 249
Compensation for pain and suffering 238, 239
Seed AI 282
Self-performance 99
Unconscionability 250
Duty of care 225
Road traffic regulations 192
Super Code 280, 281
Superintelligence 281

T

Tay 263
Partially automated 188
Partial autonomy 280
Animal owner liability 265

U

Intangible work 99

V

Conduct disruptors 194
Statute of limitations 98
Limitation period 99, 100, 254
Financial losses 242, 244, 249, 250, 253
No-fault liability 246 Madrid Agreement 281
Contractual penalty clause 257
Contractual penalty 255
VOB/B 244
Intent 224, 225, 227, 246, 249, 251

W

Vienna Convention 191
Declarations of intent 269
Working Party on Road Traffic Safety 191

Z

Two hundred years old 281