Gerald Spindler (†), José Hernán Muriel Ciceri (Eds.)

Challenges of Law and Technology

Herausforderungen des Rechts und der Technologie

Retos del Derecho y de la Tecnología

Universitätsverlag Göttingen

Gerald Spindler (†), José Hernán Muriel Ciceri (Eds.)

Challenges of Law and Technology

Herausforderungen des Rechts und der Technologie

Retos del Derecho y de la Tecnología

erschienen im Universitätsverlag Göttingen 2023

Gerald Spindler (†),
José Hernán Muriel Ciceri (Eds.)

Challenges of Law and Technology

Herausforderungen des Rechts und der Technologie

Retos del Derecho y de la Tecnología

Universitätsverlag Göttingen
2023

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://dnb.dnb.de abrufbar.

Gefördert durch den Katholischen Akademischen Ausländer-Dienst (KAAD) und den Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht der Georg-August-Universität Göttingen (Lehrstuhl Prof. Dr. Gerald Spindler †).

Satz und Layout: José Hernán Muriel Ciceri, Hannah Böhlke
Umschlaggestaltung: Hannah Böhlke

GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN IN PUBLICA COMMODA SEIT 1737

© 2023 Universitätsverlag Göttingen, Göttingen
https://univerlag.uni-goettingen.de
ISBN: 978-3-86395-612-7
DOI: https://doi.org/10.17875/gup2023-2487

Preface

Law and technology present humanity with challenges and opportunities. It is in this context, and in cooperation with Prof. Dr. Gerald Spindler of the University of Göttingen, that this international collective research work was conceived and co-edited.

The early and unexpected death of our esteemed colleague Professor Spindler in September 2023 has deeply shocked many of us. Our sincere condolences to his family, staff and colleagues. I thank him for his friendship, his constant support, his guidance and his advice. Those of us who had the honour of knowing him personally appreciated his high academic and human qualities, his humility, simplicity, scientific profundity and humanity. He was a beacon in the legal-economic world, and his contributions and legacy as an academic and as a human being will continue to guide many of us.

The work was made possible by the invaluable participation of colleagues from three continents. In this context, part of the research was presented at an online symposium organised by us and hosted by Prof. Spindler's Chair of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia and Telecommunication Law on 22 July 2022.

This anthology's goal is to investigate three of the pillars supporting the connection between technology and law.: artificial intelligence, blockchain and digital platforms. In these areas, the authors analyse legal issues of public and private law from European, Japanese, US and Latin American perspectives.

Our heartfelt thanks go to all the authors for their contributions, their time and support in realising the work, to the memory of Prof. Dr. Gerald Spindler for his invaluable support, time and commitment, as well as to his chair, especially Dr. Andreas Seidel and Ms. Ingrid Floerke, who provided us with decisive and sustained support in all phases of the project and the publication, and to the publishing house of the University of Göttingen, its editorial team and Ms. Hannah Böhlke for their

cooperation, support and uncomplicated guidance of the project from its inception to its realisation. We would also like to thank Dr Simon Gerdemann for his support and Mr. Valentin Braun, staff member of Prof Spindler's chair, for the editorial supervision of some of the manuscripts.

Thanks are also due to the scholarship students of the Tecnológico de Monterrey for their assistance in formatting some of the contributions. Special thanks to María Teresa Ferro Hermida, Miguel Ángel Navarrete Ruiz, Jesús Eduardo Valle Villegas and Angel Axel Pérez Asiain during the publication phase and to Allison Desirée Molina Espinoza during the preparation phase.

Very special thanks are due to the Catholic Academic Foreigners' Service (KAAD), its Secretary General, Dr Nora Kalbarczyk, and its Deputy Secretary General, Dr Thomas Krüggeler, as well as the Chair of Prof. Dr Gerald Spindler, the Faculty of Law and the administration of the University of Göttingen for their support and generous financial contribution to the publication costs.

Our thanks are due to them and to all those who made this work possible.

José Hernán Muriel Ciceri,
October 2023

Vorwort

Recht und Technologie stellen die Menschheit vor Herausforderungen und Chancen. In diesem Kontext und in Zusammenarbeit mit Prof. Dr. Gerald Spindler von der Universität Göttingen wurde dieses internationale kollektive Forschungswerk konzipiert und mit herausgegeben.

Der frühe und unerwartete Tod unseres geschätzten Kollegen Prof. Spindler im September 2023 hat viele von uns tief erschüttert. Unsere aufrichtige Anteilnahme gilt seiner Familie, seinen Mitarbeitern und Kollegen. Ich danke ihm für seine Freundschaft, seine stetige Unterstützung, Anleitung und seinen Rat. Diejenigen von uns, die die Ehre hatten, ihn persönlich zu kennen, schätzten ihn u.a. wegen seiner hohen akademischen und menschlichen Qualitäten, seiner Bescheidenheit, Einfachheit, wissenschaftlicher Tiefgang und Menschlichkeit. Er war ein Leuchtturm in der juristisch-wirtschaftlichen Welt, seine Beiträge und sein Vermächtnis für die Wissenschaft und als Mensch werden für viele von uns weiterhin richtungsweisend sein.

Die Arbeit wurde durch die wichtige Beteiligung von Kollegen aus drei Kontinenten ermöglicht. In diesem Zusammenhang wurde ein Teil der Forschungsarbeiten am 22. Juli 2022 auf einem von uns organisierten und von Prof. Spindlers Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht ausgerichteten Online-Symposium vorgestellt.

Ziel dieses Sammelbandes ist es, drei der Säulen der Beziehung zwischen Recht und Technologie zu untersuchen: künstliche Intelligenz, Blockchain und digitale Plattformen. In diesen Bereichen analysieren die Autoren Rechtsfragen des öffentlichen und privaten Rechts aus europäischer, japanischer, US-amerikanischer und lateinamerikanischer Perspektive.

Unser herzlicher Dank gilt allen Autorinnen und Autoren für ihre Beiträge, ihre Zeit und Unterstützung bei der Realisierung des Werkes, dem Andenken an Prof.

Dr. Gerald Spindler für seine unschätzbare Unterstützung, seine Zeit und sein Engagement sowie seinem Lehrstuhl, insbesondere Herrn Dr. Andreas Seidel und Frau Ingrid Floerke, die uns in allen Phasen des Projektes und der Publikation entscheidend und nachhaltig begleitet und unterstützt haben, sowie dem Verlag der Universität Göttingen, seinem Redaktionsteam und Frau Hannah Böhlke für die Zusammenarbeit, Unterstützung und unkomplizierte Begleitung des Projektes von der Entstehung bis zur Realisierung. Wir danken auch Herrn Dr. Simon Gerdemann für seine Unterstützung und Herrn Valentin Braun, Mitarbeiter am Lehrstuhl von Prof. Spindler, für die redaktionelle Durchsicht eines Teils der Manuskripte.

Wir bedanken uns auch bei den Stipendiaten des Tecnológico de Monterrey, welche die Anpassung einige der Beiträge an die Formatvorlagen begleitet haben. Unser besonderer Dank gilt Frau María Teresa Ferro Hermida, Herr Miguel Ángel Navarrete Ruiz, Herr Jesús Eduardo Valle Villegas und Herr Angel Axel Pérez Asiain während der Veröffentlichungsphase sowie Frau Allison Desirée Molina Espinoza während der Vorbereitungsphase.

Ganz besonderer Dank gilt dem Katholischen Akademischen Ausländerdienst (KAAD), seiner Generalsekretärin, Dr. Nora Kalbarczyk, und seinem stellvertretenden Generalsekretär, Dr. Thomas Krüggeler, sowie dem Lehrstuhl von Prof. Dr. Gerald Spindler, der Juristischen Fakultät und der Verwaltung der Universität Göttingen für ihre Unterstützung und großzügige finanzielle Beteiligung an den Publikationskosten.

Ihnen und allen, die das vorliegende Werk ermöglicht haben, sei an dieser Stelle herzlich gedankt.

José Hernán Muriel Ciceri,
Oktober 2023

Prefacio

El derecho y la tecnología presentan retos y oportunidades a la humanidad. En este ámbito y en conjunto con el Prof. Dr. Gerald Spindler de la Universidad de Göttingen, fue trazada y coeditada la presente obra colectiva internacional de investigación.

La temprana e inesperada muerte de nuestro estimado colega el profesor Spindler en septiembre de 2023 nos conmocionó profundamente a muchos de nosotros. Las más sinceras condolencias a su familia, a su equipo de trabajo, y a sus colegas. Agradezco a él su amistad, su continuo apoyo, guía y consejo. Quienes tuvimos el honor de conocerle personalmente apreciamos sus altas cualidades académicas y humanas, su humildad, sencillez, profundidad científica y humanidad. Fue un faro en el mundo jurídico-económico, y sus aportaciones y su legado como académico y como ser humano seguirán guiándonos a muchos de nosotros.

La obra se realizó gracias a la importante participación de colegas de tres continentes. En este contexto se presentaron una parte de las investigaciones el 22 de julio de 2022 en un simposio online que organizamos y del cual fue anfitriona la cátedra del Prof. Spindler en Derecho Civil, Derecho Comercial y Económico, Derecho Comparado, Derecho Multimedia y de las Telecomunicaciones.

El objetivo de la presente obra colectiva es el examen de tres de las columnas existentes en la relación entre derecho y tecnología, como son: la inteligencia artificial, la cadena de bloques y las plataformas digitales. En estos ámbitos los autores analizan cuestiones jurídicas en derecho público y en derecho privado, desde las perspectivas estadounidense, europea, japonesa y latinoamericana.

Expresamos nuestra profunda gratitud a todos los autores por sus contribuciones, su tiempo y su apoyo en la realización de la obra, asimismo, a la memoria del Prof. Dr. Gerald Spindler por su invaluable apoyo, tiempo, y compromiso, así como a su Cátedra, en particular allí al Dr. Andreas Seidel y a la Sra. Ingrid Floerke quienes nos acompañaron y apoyaron de forma decisiva y

permanente en todas las fases del proyecto y de la publicación, igualmente a la editorial de la Universidad de Göttingen, a su equipo editorial y a la Sra. Hannah Böhlke, por su cooperación, su apoyo sin complicaciones en el proyecto, desde su inicio hasta su materialización. Asimismo, agradecemos al Dr. Simon Gerdemann por su apoyo y al Sr. Valentin Braun colaborador de la Cátedra por la supervisión editorial de una parte de los manuscritos.

También agradecemos a los estudiantes becarios del Tecnológico de Monterrey que colaboraron en formatear una parte de las contribuciones según las especificaciones editoriales. En particular expresamos nuestro agradecimiento en la fase de publicación a la Sra. María Teresa Ferro Hermida, al Sr. Miguel Ángel Navarrete Ruiz, al Sr. Jesús Eduardo Valle Villegas y al Sr. Angel Axel Pérez Asiain, así como en la fase preliminar de la publicación a la Sra. Allison Desirée Molina Espinoza.

De forma especial expreso la profunda gratitud al Katholischer Akademischer Ausländerdienst (KAAD), a su secretaria general Dra. Nora Kalbarczyk y a su secretario general adjunto Dr. Thomas Krüggeler, así como a la cátedra del Prof. Gerald Spindler, a la Facultad de Derecho y a la Administración de la Universidad de Göttingen, por su apoyo y la generosa subvención económica conjunta de gastos de publicación.

Gracias a todos ellos y a quienes hicieron realidad la presente obra.

José Hernán Muriel Ciceri,
octubre de 2023

Table of Contents

The EU Commission's Proposals for Regulation of Artificial Intelligence – Product safety and liability, A General Overview

Gerald Spindler

The EU Commission's new proposal for a regulation on artificial intelligence is the world's first attempt to get a legislative grip on the phenomenon of AI. The draft uses classic regulatory structures of product safety law to get the risks of AI under control using technical standards, certifications, risk, and quality management systems, which the Commission locates primarily in threats to fundamental rights. The article provides a first overview and assessment of the draft.

The second part is dedicated to the new proposals of the EU Commission regarding product liability and liability for AI-systems.

A. Part I: The Proposal for a Regulation of Artificial Intelligence (AI-Act-P)

I. Introduction

Artificial intelligence (AI) has emerged as one of the most important components of digitalization in recent years, alongside the platform economy and blockchain technology. However, the use of AI can have beneficial effects as well as evoke considerable risks and dangers: Well-known examples include the use of AI in the area of social scoring to filter out disliked minorities, or the creation of movement

DOI: https://doi.org/10.17875/gup2023-2494

profiles with the help of telemetric facial recognition[1], or in the area of opinion-forming platforms that evaluate and sort certain content and then present it to the user in an appropriately "prepared" form (so-called "content curation"), resulting in the well-known phenomenon of "echo chambers" arises[2]. The risks to the exercise of fundamental online rights are therefore manifold, ranging from data protection and freedom of expression to possible discrimination, for example through biased training data.

It is therefore not surprising that numerous expert panels and commissions were soon convened at the legal policy level to address the ethical and legal principles of AI and to make corresponding proposals. The current proposal of the *EU Commission*[3] results from the consultations on the Commission's White Paper[4] and explicitly incorporates the proposals of the European Parliament on ethical principles for AI[5], as well as the proposals of the Council of 21.10.2020[6] and the *High-Level Expert Group on AI*[7].

With the proposal for an AI Regulation, the *EU Commission* is pursuing a *risk-based horizontal approach* in the area of product safety law that relates to the use of AI in general and does not proceed on a sector-specific basis (as for example in the

[1] For basic information on face recognition see Andreas Kulick, "„Höchstpersönliches Merkmal" – Verfassungsrechtliche Maßstäbe der Gesichtserkennung," *NVwZ,* (2020): 1622; Jan Mysegades, "Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage," *NVwZ,* (2020): 852; Amélie P. Heldt, "Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raum," *MMR,* (2019): 285.

[2] For basic information on "echo chambers" see Boris P. Paal, Moritz Hennemann, "Meinungsbildung im digitalen Zeitalter Regulierungsinstrumente für einen gefährdungsadäquaten Rechtsrahmen," *JZ,* (2017): 641; instructive on their emergence: Josef Drexl, "Economic Efficiency Versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics" *Max Planck Institute for Innovation and Competition Research Paper,* No. 16-16 5, (2016), accessed October 31, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881191; in detail on the connected harm for the plurarity of opinions: Josef Drexl, "Bedrohung der Meinungsvielfalt durch Algorithmen," *ZUM,* (2017): 529.

[3] Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts", COM (2021) 206 final, April 21, 2021, accessed October 31, 2022, https://ec.europa.eu/newsroom/dae/redirection/document/75788, cited as AI-Act-P.

[4] Commission, "White Paper on Artificial Intelligence - A European approach to excellence and Trust", COM (2020) 65 final, 19 February 2020.

[5] Commission, "European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL)", [2021] OJ C 404/63.

[6] Council of the European Union, "Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change", [2020] OJ C 202, 11481/20.

[7] High-Level Expert Group (HLEG), "Ethics Guidelines for Trustworthy AI" (2019); HLEG, "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment" (2020).

product safety law regulations or directives,). The AI Regulation proposal is intended to be explicitly open to the future and able to consider new developments[8].

Regarding the equally much-discussed liability law[9] the focus lies on the introduction of a type of causal liability or strict liability, as proposed by the *Expert Group on Liability and New Technologies*[10] and partially taken up by the *European Parliament* in its resolution of 5.10.2020[11]. The Commission has just recently published two new proposals on AI liability and on a reform of the Product Liability, which will be dealt separately.

The AI-Act-P, on the other hand, is limited to the obligations and prohibitions described and therefore primarily follows a product safety law approach; nevertheless, if the AI-Act-P is adopted it will also have an impact on national liability law, in Germany for example via Section 823 (2) BGB,[12] even if the proposal for the introduction of causal liability, announced for the second half of 2021, is also implemented.[13]

Since various member states, including Germany, are considering implementing an AI strategy, the *EU Commission* has explicitly chosen the instrument of a regulation to counteract fragmentation within the EU[14] – which is in line with the basic approach in the context of product safety.

---

[8] Commission, Explanatory Memorandum, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts", COM (2021) 206 final, April 21, 2021, accessed October 31, 2022, 3, https://ec.europa.eu/newsroom/dae/redirection/document/75788

[9] Gerald Spindler, «823 BGB», in *BeckOGK,* ed. Beate Gsell et al. (München: C.H. Beck, 2022) paras 739 ff.; Herbert Zech, «Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung? », in *Verhandlungen des 73. Deutschen Juristentages,* ed. Ständige Deputation des Deutschen Juristentages (München: Beck, 2020), Vol. I expert opinion, Part A 11, A 87 ff.; Gerhard Wagner, "Produkthaftung für autonome Systeme," [2017] 217 *AcP* (2017): 217, 707 ff.; Gerhard Wagner, "Verantwortlichkeit im Zeichen digitaler Techniken," *VersR* (2020): 717, 724 ff.; Gerhard Wagner, «§ 823 BGB», in *Münchener Kommentar zum Bürgerlichen Gesetzbuch,* ed. Franz Jürgen Säcker, Roland Ricecker, Hartmut Oetker, Bettina Limperg, 8th edn. (München: C.H. Beck, 2020) paras 789 ff.; Maik Thöne, *Autonome Systeme und deliktsche Haftung* (Tübingen: Mohr Siebeck, 2020), passim.

[10] Expert Group on Liability and New Technologies – New Technologies Foundation, "Liability for Artificial Intelligence and other emerging digital technologies", November 27, 2019, accessed November 01, 2022, https://op.europa.eu/de/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1.

[11] Commission, Committee on Legal Affairs, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))", [2020] OJ C 404/107.

[12] BGB is an abbreviation for "Bürgerliches Gesetzbuch", which is the German Civil Code.

[13] See below A. XIV.

[14] Explanatory Memorandum, (n 8), 7.

II. The Basic Approach: Risk-Based with Regulation for High-Risk AI

Among various possibilities, the *EU Commission* has come out firmly in favour of a risk-based approach,[15] which contains mandatory regulations only for high-risk AI systems, but leaves it at moderate obligations and a *code-of-conduct concept* for other AI systems.[16] In this context, the AI-Act-P explicitly extends its scope of application to providers respectively operators located outside the EU.[17] The declared goal of regulating high-risk AI is to guarantee the fundamental rights of affected users, in particular the right of freedom of expression, non-discrimination, and fundamental data protection rights.[18] The central element of monitoring the requirements for high-risk AI systems is the product safety approach of conformity assessment on *technical standards*, accompanied by a *presumption of conformity*, which, however, also allows other alternatives, whereby on the one hand the EU Commission wants to ensure necessary flexibility and on the other hand wants to prevent overloading the supervisory authorities.[19]

In order to enforce the obligations of high-risk AI, the *EU Commission* wants to create a registration obligation for so-called *stand-alone AI* and thus an EU-wide database, whereby the activities of the AI can be monitored by supervisory authorities or other third parties with regard to compliance with the obligations, in particular the protection of the fundamental rights concerned.[20] At the same time, this rejects the demand for prior authorization under public law. [21]

This approach is flanked by obligations of the AI operators to inform the monitoring authorities about serious incidents or malfunctions of the AI that endanger fundamental rights; the corresponding information from the monitoring authorities is then to be evaluated by the *EU Commission* for the purpose of market analysis and assessment.[22]

Within this framework, the AI-Act-P also wants to provide facilitations for small and medium-sized enterprises (SMEs), for example by establishing "regulatory sandboxes" or facilitating the conformity assessment of AI systems.[23]

---

[15] In this direction already Mario Martini, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz* (Heidelberg: Springer, 2019), 226 ff.

[16] Explanatory Memorandum, (n 8), 9.

[17] See below A. III 3.

[18] Explanatory Memorandum, (n 8), 11. The memorandum lists numerous other fundamental rights affected, up to and including environmental protection.

[19] Explanatory Memorandum, (n 8),14.

[20] Explanatory Memorandum, (n 8), 11.

[21] See for this e.g. Datenethikkommission, "Gutachten der Datenethikkommission der Bundesregierung", (2019): 195, 207 f., accessed November 01, 2022, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=FF71C19934371EB93FE4A14E4C67E962.1_cid334?nn=11678504.

[22] Explanatory Memorandum, (n 8), 11.

[23] Explanatory Memorandum, (n 8), 10.

III. Scope of Application

1. Definition of AI

The definition of AI in Art. 3 No. 1 AI-Act-P already shows the broad scope of application that the AI-Act-P aims at. According to this definition, an AI system is software that uses techniques or approaches described in Annex I and that can produce certain results, such as recommendations, or influences its environment by making decisions, depending on human-set goals. Annex I to Art. 3 No. 1 AI-Act-P lists *machine learning* including *deep learning*, knowledge-based approaches including expert systems, as well as statistical approaches, search and optimization methods. In this way, the *EU Commission* wants to use a definition that is as technologically neutral and future-proof as possible, which is open to newer developments through possible adaptations of Annex I, for which the *EU Commission* is authorized under Art. 4, 73 of the AI-Act-P to issue delegated acts for updating Annex I. However, it is striking from the outset that characteristic elements of AI, such as the *unpredictability of its behaviour* and the *Black-Box-Effect*, are not mentioned at all, so that deterministic software and even normal expert systems are covered, i.e., a much broader area is addressed than was used in the definition of the *High Level Expert Group on AI*.[24]

The area of data essential for AI is also outlined: Art. 3 No. 29 AI-Act-P defines the term *training data* as data with which the AI system fills in the learning parameters including the emphasis within the neuronal networks, while *validation data* according to Art. 3 No. 30 AI-Act-P are data that serve to adjust (*tuning)* the non-learnable parameters and the learning process as such,[25] whereby the *validation data* can also be part of the *training data*. Finally, this is supplemented by the definition of *test data* according to Art. 3 No. 31 AI-Act-P, which is intended to enable an independent assessment of the trained and validated AI system before it is placed on the market or operated.[26]

The AI-Act-P also focuses on the definitions of biometric identification AI, e.g. in Article 3 No. 36 of the AI-Act-P, which defines a "remote biometric identification system" as any AI that aims to identify persons based on their biometric data, in particular facial recognition, by comparing them to a database, without the user

[24] Cf. The definition of the High Level Expert Group on AI (AI HLEG), *Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete. Für die Zwecke der Gruppe entwickelte Definition* (Brussels: European Commission, 2018) 6; similar Zech, (n 9), A 20.

[25] See also Annalyn Ng and Kenneth Soo, *Data Science – was ist das eigentlich?!* (Berlin: Springer, 2018), 16 ff.

[26] See to the definition of testdata also Claudia Niederée, Wofgang Nejdl, «§ 2 Technische Grundlagen der KI», in *Rechtshandbuch Künstliche Intelligenz und Robotik,* ed. Martin Ebers et al. (München: C.H. Beck, 2020) para 31.

of the AI knowing in advance whether the person in question is present and can be identified.

Rather en passant, however, the AI-Act-P makes another important distinction, namely between AI systems integrated into products (*"embedded"* AI systems) and those that function so to speak "alone" without such an integration, i.e. essentially as software or based in a cloud (*"stand-alone"* AI systems). While for the "embedded" AI systems the conformity assessment procedures are and remain relevant, the AI-Act-P for the first time subjects all software ("stand-alone" AI systems) to a CE procedure in a horizontal approach, however only based on internal controls, but combined with a registration obligation in databases.[27]

2. Regulatory addressees

The addressees of the AI-Act-P are, on the one hand, all *manufacturers* or *operators* of AI systems, including those who only market or operate an AI system under their name or trademark, irrespective of whether this is done in return for payment or free of charge, Art. 3 No. 2 AI-Act-P. It is noteworthy here that not even the disclosure of data, as provided for in Art. 3 (1) of the DID Directive, [28] is required to open the scope of application of the AI-Act-P. In this context, not only *private operators* of AI systems are covered, but also explicitly public authorities, Art. 3 No. 2 AI-Act-P. Open source systems are thus not excluded from the AI-Act-P, but are fully subject to its requirements. Both providers and operators are covered as "operators".

On the other hand, users of AI systems are also covered by the regulations if they use the AI for professional purposes, Art. 3 Nr. 3 AI-Act-P.

A distinction must be made between those affected by the AI systems, the *"AI subjects"*, who are subject to the influence of the AI systems in the form of recommendations or measures taken by the AI systems.

3. International Scope

Art. 2 (1) AI-Act-P declares all those who place AI systems on the market or put them into operation in the EU to be the addressees of the AI-Act-P, even if they are based outside the EU. Thus, the AI-Act-P partially goes beyond traditional product safety law, which in these cases subjects importers to the regulations of EU law, such as Art. 2 e) ii) of the General Product Safety Directive.[29]

Users, on the other hand, are only to be subject to the obligations under Article 2 (1) (b) AI-Act-P if they are based in the EU. However, if the result of an AI system

[27] See in detail below A VIII.3.

[28] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1.

[29] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2002] OJ L 11/4.

is used within the EU, not only operators but also users located outside the EU are subject to the AI-Act-P, Art. 2 (1) c) AI-Act-P.

4. Relationship with other EU Legal Acts

a) Relationship with GDPR

The GDPR shall remain unaffected regarding its regulations or be supplemented by the AI-Act-P,[30] here especially in the area of *training data*. These are one of the central problem points within technology regulation, as they form the basis of many AI applications.[31] Especially for *machine learning* techniques, the *training data* have a dominating influence on the development of the AI, so that a legislative quality control is indispensable with regard to this data.[32] Otherwise, undesirable consequences such as the development of discriminatory algorithms may occur.[33] Currently, the use of *training data* can only be controlled in a very rudimentary way by Art. 5 (1) d) GDPR, which requires a certain level of quality assurance with regard to the data used. However, since in many cases synthetic or at least anonymized *training data* is used, it often does not fall within the scope of the GDPR.[34]

In particular, the AI-Act-P also affects Art. 22 of the GDPR, which sets out requirements for *automated decision-making* based on personal data. The AI-Act-P also contains a number of breaches or mitigations of the GDPR, for example with regard to the *purpose limitation principle* for AI training or in the area of *"regulatory sandboxes"*.[35] In order to enable high-quality data sets and AI based on them, the use and processing of *sensitive data* within the meaning of the GDPR is also permitted for certain providers, see Art. 10 (5) AI-Act-P; for example, the *EU Commission* states in Recital 45 AI-Act-P that access to relevant health data for the training of AI in the health sector is to be opened up via the "European Health Data Space", although this is to be subject to institutional supervision and compliance with specific security provisions.[36] In this respect, there is a further restriction of the general prohibition of processing in Art. 9 GDPR. An exception to the strict *purpose limitation*

[30] Explanatory Memorandum, (n 8), 4.

[31] Philipp Hacker, "Europäische und nationale Regulierung von Künstlicher Intelligenz," *NJW,* (2020): 2142, 2145; Philipp Hacker, "A Legal Framework for AI Training Data," (working paper, 2020), accessed November 01, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556598.

[32] Like this now also Commission, Explanatory Memorandum, (n 8), recital 44, which above all points out that the data used can also be a source of unintentional discrimination, so that this 1st he point to start with.

[33] Explanatory Memorandum, (n 8), recital 44.

[34] In detail to this Manon *Oostveen, "Identifiability and the applicability of data protection to big date," International Data Privacy Law,* (2016): 6, 299, 307, doi:10.1093/idpl/ipw012.

[35] See to this below A. IX.

[36] Before processing it is explicitly not necessary to anonymize the dataset if this would significantly impair the pursued purpose, cf. Art 10 (5) AI-Act-P.

principle under Art. 5 (1) b) GDPR - according to which personal data may only be collected for *specified, explicit and legitimate purposes* and may not be further processed in a manner incompatible with these purposes - is made by the AI-Act-P with regard to the (further) processing of these data in *"regulatory sandboxes"* to the effect that such processing is permitted if it serves the development and testing of innovative AI systems, cf. Art. 54 Abs. 1 (a) AI-Act-P.[37]

b) Relationship to Other Product Safety Acts, in Particular Proposal for a Machinery Regulation

Since the proposal for an AI-Act ultimately follows product safety law approaches, the question of the relationship to sector-specific regulations is obvious. The *EU Commission* wants to view the AI-Act as a horizontal supplement to all regulations based on *the New Legislative Framework (NLF)*, whereby these can provide for supplementary safety requirements with regard to the specific embedding of AI in the respective product.[38]

Accordingly, the AI-Act-P, with the exception of its Art. 84, does not apply to product safety requirements according to the *"Old Approach"*, which contains precise requirements, for example in the area of aircraft or motor vehicles.[39] Accordingly, the AI-Act-P only applies to a limited extent to the following regulations or directives: (a) Regulation (EG) 300/2008[40]; (b) Regulation (EU) 167/2013[41]; (c) Regulation (EU) 168/2013[42]; (d) Directive 2014/90/EU[43]; (e) Directive (EU) 2016/797[44];

[37] In detail to "regulatory sandboxes" see below A. IX.
[38] Explanatory Memorandum, (n 8), 4.
[39] Explanatory Memorandum, (n 8), 4.
[40] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 [2008] OJ L 97/72.
[41] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles [2013] OJ L 60/1.
[42] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles [2013] OJ L 60/52.
[43] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC [2014] OJ L 257/146.
[44] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (*recast*) [2016] OJ L 138/44.

(f) Regulation (EU) 2018/858[45]; (g) Regulation (EU) 2018/1139[46]; (h) Regulation (EU) 2019/2144[47].

IV. Basic Ban on Certain AI Applications

The AI-Act-P takes a risk-based approach that distinguishes between unacceptable risks, high risks, and low or minimal risks of AI applications. Certain AI applications are subject to an unconditional ban, be-cause those AI applications are considered to create risks that are no longer acceptable:

1. Procedures for Influencing (unconscious) behaviour

A first group can be summarized according to Art. 5 (1) a), b) AI-Act-P as a prohibition of influencing the unconscious behaviour of people, which, however, according to Art. 5 (1) AI-Act-P is limited to causing physical or mental harm. Art. 5 (1) (b) AI-Act-P specifies this again regarding the exploitation of specific vulnerable groups such as persons who are physically or mentally disadvantaged due to their age. Article 5 (1) (a), (b) AI-Act-P thus specifies Article 8 and 9 of the Unfair Commercial Practice Directive.[48] of already forbidden manipulations.[49]

---

[45] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L 151/1.

[46] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [2018] OJ L 212/1.

[47] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 [2019] OJ L 325/1.

[48] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L 149/22.

[49] In detail to this Benjamin Raue, «§ 4a UWG», in *Münchener Kommentar zum Lauterkeitsrecht,* ed. by Peter W. Heermann and Jochen Schlingloff, 3rd edn. (München: C.H. Beck, 2020) paras 161; Horst-Peter Götting, «§ 4a UWG», in *UWG Handkommentar,* ed. by Horst-Peter Götting, Axel Nordemann,

2. Social Scoring

Another central concern of the Commission's proposal is the prohibition of *"social scoring"* under Art. 5 (1) (c) AI-Act-P, which assesses the trustworthiness of natural persons based on their social behaviour or personal characteristics.[50] The prohibition is directed only at public or governmental bodies, not at private operators. In addition, the prohibition is limited to impairments of these individuals in social contexts unrelated to those in which the data was collected, alternatively, to impairments or harm to those individuals in ways that are not justified or disproportionate to the social behaviour.

In this way, the AI-Act-P indirectly restricts the ban on *social scoring* by referring to the balancing of interests, thereby creating a considerable degree of legal uncertainty.

3. Biometric Recognition by AI

The AI-Act-P pays special attention to biometric identification systems in publicly accessible places – which has already led to corresponding criticism regarding a too open approach; the main criticism is that the current draft would enable mass surveillance in public spaces.[51] Article 5 (4) of the AI-Act-P contains an opening clause for Member States to decide on the admissibility of such systems under the conditions set out in Article 5 (1) (d), (2) and (4) of the AI-Act-P. Article 5 (1) (d) of the AI-Act-P prohibits in principle the use of such systems for law enforcement purposes, but allows their use for certain purposes which are likely to soften the prohibition, in particular for the search for possible victims of crime, for criminal prosecution and for purposes of ensuring the safety of life and limb of natural persons, including the prevention of acts of terrorism. It is true that Article 5 (2) of the AI-

3rd edn. (Baden-Baden: Nomos, 2016) paras 12 ff.; Ruth Janal, «§ 4a UWG», in *BeckOK IT-Recht,* ed. by Georg Borges and Marc Hilber, 7th edn. (München: C.H. Beck, 2022) para 6; Olaf Sosnitza, «§ 4a UWG», in *BeckOK IT-Recht,* ed. by Ansgar Ohly, Olaf Sosnitza, 7th edn. (München: Beck, 2016) paras 35 ff.

[50] See for this Niklas Maamar, "Eine europäische Perspektive auf Verbraucher-Scores zwischen Big Data und Big Brother," *CR,* (2018): 820, 821; Philipp Hacker, "Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht," *ZfPW*, (2019): 148, 155; Isabell Conrad, Dominik Hausen, «§ 36 Datenschutz im Internet», in *Handbuch IT- und Datenschutzrecht,* ed. Astrid Auer-Reinsdorff and Isabell Conrad, 3rd edn. (München: C.H. Beck, 2019), 244; Ulrich Hoffrage and Julian N. Marewski, «Social Scoring als Mensch-System-Interaktion», in *Social Credit Rating,* ed. by Oliver Everling (Wiesbaden: Springer Gabler, 2020), 305-16; Uwe Hartwig, Stefanie Ernst and Felizitas Pokora, "Social Scoring: Evaluation qualifizierender Beschäftigung,"Hans-Böckler-Foundation, *WSI-- Mitteilungen*, (2008): 267, 273; see also Datenethikkommission, (n 21), 99, 106.

[51] Like this it is mentioned on twitter by vice-president of the Parliament Nicola Beer, accessed November 02, 2022, https://twitter.com/nicolabeerfdp/status/1384910602485829633?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Etweet; sceptical also Member of the Parliament Patrick Beyer, who is worried about an extensive biometrical mass surveillance, interview from April 21, 2021, accessed November 03, 2022, https://www.tagesschau.de/wirtschaft/technologie/eu-gesetzentwurf-kuenstliche-intelligenz-ki-101.html.

Act-P attempts to strike further stakes in the balancing of interests by also taking into account the extent and likelihood of damage if such a system were not used, as well as the impairment of fundamental rights. However, it should not be overlooked that the relatively far-reaching opening clauses open the door to biometric recognition.

Furthermore, Art. 5 (2) sentence 2 AI-Act-P requires compliance with time, location and personal restrictions, including corresponding warranties (see also recitals 19, 20, 21 AI-Act-P); this refers in particular to the *purpose limitation* (Art. 5 (1) b) GDPR) and *data erasure obligations* (Art. 5 (1) e) GDPR), which already follow from the GDPR. Article 5 (3) of the AI-Act-P additionally safeguards this by requiring a prior decision by a court or an independent authority, except in urgent cases for which the decision can still be obtained retrospectively.

V. High-Risk AI Applications

1. Definition

For the definition of high-risk AI applications, the AI-Act-P uses a two-fold approach:

- On the one hand, the AI-Act-P focuses on the use of AI systems as safety-relevant elements in products subject to product safety law,[52] in particular conformity assessment procedures, and
- on the other hand for stand-alone AI systems on an extensive Annex II.[53] For both criteria, it is the intended use that matters, not just the specific function in which the AI system is used.

The first group of product safety requirements according to Art. 6 (1) b) Annex II AI-Act-P is characterized by a broad spectrum of directives and regulations, all of which are based on the *New Legislative Framework*, i.e. the conformity assessment procedures, beginning with the (also revised) Machinery Regulation[54] through the

[52] This, among other things, to ensure that only safe products circulate on the internal market; whereby this safety in the digital age should also be guaranteed with regard to all digital components such as AI, cf. recital 28 AI-Act-P.

[53] For their classification as high-risk AI, it is particularly relevant in accordance to their intended use, whether they pose a high risk to the health, safety or fundamental rights of Union citizens, taking into account both the severity of the potential harm and the likelihood of its occurrence, cf. recital 32 AI-Act-P.

[54] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery and amending Directive 95/16/EC [2006] OJ L 157/24.

Elevator-Directive[55] to the medical product regulations[56]. In addition, however, AI applications as safety components in product safety regulations that do not follow the conformity assessment procedure are also covered under Art. 6 (1) a), Annex II, Section B AI-Act-P, including above all vehicle type approval procedures.

According to Art. 6 (2), Annex III AI-Act-P, the *second group* covers *stand-alone AI systems* that may essentially affect substantially security aspects, such as use in critical infrastructures, or also fundamental rights, such as AI systems for pupil and student assessment, employee selection and promotion or the use of *scoring systems* in the area of essential private or public services, including the *credit scoring* system (Annex III No. 5 b) AI-Act-P. Annex III No. 6 of the AI-Act-P highlights as high-risk AI systems in particular those used in the field of criminal justice and the prosecution of criminal offences, such as predictive policing.[57] But so does the use of AI systems to detect crime. The same applies to AI systems in migration and asylum procedures, Annex III No. 7 AI-Act-P.

According to Art. 7 AI-Act-P, the *EU Commission* is to be empowered to supplement or modify Annex III under the conditions specified in Art. 7 AI-Act-P. These include, above all, damage or threats to fundamental rights that have already occurred because of an AI system (Art. 7 (2) (c) AI-Act-P), or an economic, social or knowledge imbalance of power vis-à-vis the user of the AI system (Art. 7 (2) (f) AI-Act-P).

2. Requirements for High-Risk AI Systems

In its risk-based approach anchored in product safety law, the AI-Act-P ultimately follows similar patterns to the recently presented draft of a Digital Service Act on particularly large online platforms or, as in the past, financial market regulations, in that risk and quality management systems as well as transparency and publicity obligations are introduced on a risk-graded basis. The product safety approach is also reflected in the presumption of conformity with accepted technical standards and

[55] Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts [2014] OJ L 96/251.

[56] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L 117/176.

[57] Regarding Predictive Policing Lucia M. Sommerer, *Personenbezogenes Predictive Policing. Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose* (Baden-Baden: Nomos, 2020); Ines Härtel, "Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren," *LKV,* (2019): 49; Tobias Singelnstein, "Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention," *NStZ,* (2018): 1.

the corresponding conformity assessment procedures, with which the *EU Commission* intends to implement a flexible approach. The requirements were essentially developed from the recommendations of the *High Level Expert Group on AI* and the Assessment List for trustworthy artificial intelligence derived from them.[58]

a) Riskmanagementsystems

According to Art. 9 AI-Act-P, all high-risk AI systems must be flanked by a risk management system, the details of which are specified in Art. 9 (2) AI-Act-P; at the same time, Art. 9 (2) p. 1 AI-Act-P requires a continuous update of the risk management system. According to Art. 9 (2) sentence 2 AI-Act-P, the elements include the known components of a risk management system, such as the identification and assessment of potential risks and the definition of measures. The risk management system should also include foreseeable misuse of the AI systems as well as data from product monitoring pursuant to Art. 61 AI-Act-P on additional risks. Regarding the required measures according to Art. 9 (2) p. 2 d) AI-Act-P, Art. 9 (4) p. 1 AI-Act-P makes clear that no 100% security is required, but that restrictions can be classified as "acceptable". This is reinforced by Article 9 (4) (3) (b) of the AI-Act-P when sufficient control options are required for risks that cannot be completely eliminated, flanked by corresponding information obligations about such risks and training for users, Article 9 (4) (3) (c) of the AI-Act-P.

Finally, Art. 9 (4) p. 4 AI-Act-P emphasizes the users' knowledge, training and experience, including the environment in which the AI is to be used, to eliminate or reduce the risks. The AI-Act-P also pays particular attention to the testing of AI systems, which according to Article 9 (7) of the AI-Act-P should be carried out at the latest prior to market launch; however, Article 9 (6) of the AI-Act-P limits the testing requirements to the intended area of use of the AI - abuses etc. accordingly do not need to be included.

b) Requirements for Data, Especially Training Data

AI systems require training on data; therefore, it is not surprising that Art. 10 AI-Act-P explicitly deals with data as a prerequisite for AI systems, in particular *"Data Governance"*. According to Article 10 (2) of the AI-Act-P, this includes, among other things, the choice of data sets, the relevant assumptions, possible presetting or alignments (biases), and the identification of possible data gaps and deficiencies. Article 10 (3) and (4) of AI-Act-P set out requirements that are actually self-evident, such as the representativeness, completeness and accuracy of the data, as well as the consideration of local or functional contexts in which the AI systems are to be used.

It is interesting to note that Art. 10 (5) AI-Act-P provides for a partial breakthrough of strict data protection, especially of sensitive data under Art. 9 GDPR,

[58] See for this AI HLEG, "The Assessment List for Trustworthy Artificial Intelligence for self-assessment (*ALTAI*)", European Commission, July 17, 2020, accessed November 02, 2022, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342.

with Art. 10 (5) AI-Act-P providing for corresponding safeguards, but without requiring full anonymization if the data is otherwise unusable.

c) Technical Documentation and Conformity Assessment Procedures

A prerequisite for the conformity assessment procedure is meaningful documentation, as required by Article 11 (2) of the AI-Act-P. However, even those systems that are "only" subject to monitoring by supervisory authorities must have documentation with the minimum content according to Annex IV of the AI-Act-P, Art. 11 (1) AI-Act-P. Only with this information can certification procedures, as well as subsequent checks by market surveillance authorities, be carried out.

A central role in the overall concept of the *EU Commission* is played by harmonized *technical standards*, which are commissioned by the *EU Commission*, but for which the operator can also demonstrate equivalent solutions in accordance with the *New Legislative Framework* in order to comply with the requirements. In this way, the *EU Commission* aims to achieve the necessary flexibility to manage the risks, which will naturally depend on whether, when and under what conditions such standards can be developed.

d) Traceability Instruments (logging devices)

It is well known that AI systems are often characterized by the so-called black-box problem[59], where the traceability of the results generated by the AI remains unclear.[60] In order to take this problem into account, Art. 12 (1) AI-Act-P requires the use of traceability mechanisms, so-called *logging devices*. In particular, the *logging devices* are intended to enable the monitoring of activities of the AI that may result in risks pursuant to Art. 65 (1) AI-Act-P; these mechanisms are also intended to facilitate the product monitoring obligations, Art. 12 (3) AI-Act-P in conjunction with Art. 61 AI-Act-P. Finally, special requirements are imposed on biometric recognition systems, Article 12 (4) of the AI-Act-P.

e) Human Supervision

Art. 14 AI-Act-P requires high-risk AI systems to be adequately supervised by humans when the AI is in use, with supervision aimed at preventing or reducing risks to health, safety, or fundamental rights, and including foreseeable misuse, Art. 14

[59] AI HLEG, *A definition of AI: Main capabilities and scientific disciplines* (Brussels: European Commission Directorate-General for Communication, 2018), 6, locates the problem like this "The notion of black-box AI refers to such scenarios, where it is not possible to trace back to the reason for certain decisions".

[60] Niederée and Nejdl, (n 26), 123; Hans Steege, "Künstliche Intelligenz und Mobilität," *SVR,* (2021): 1 (4); Herbert Zech, "Künstliche Intelligenz und Haftungsfragen," *ZfPW,* (2019): 198 (202); Zech, (n 9), A 33; Heinz-Uwe Dettling and Stefan Krüger, "Erste Schritte im Recht der Künstlichen Intelligenz," *MMR,* (2019): 211 (212); Friedemann Kainer and Lydia Förster, "Autonome Systeme im Kontext des Vertragsrechts," *ZfPW,* (2020): 275 (279); Dimitrios Linardatos, "Künstliche Intelligenz und Verantwortung," *ZIP,* (2019): 504 (504); Georg Borges, "Rechtsrahmen für autonome Systeme," *NJW,* (2018): 977 (978).

(2) AI-Act-P. To this end, the AI system must provide for appropriate measures, such as human-machine interfaces, which must either be built in by the operator from the outset or provided for users to implement. Article 13 (4) of the AI-Act-P specifies the requirements by stipulating that the human supervisor must be able to understand the capabilities and limitations of the AI system and to supervise it appropriately, in particular to respond immediately to malfunctions. Furthermore, the human supervisor must be aware that there is a risk of *"automation bias"*, i.e. blindly accepting the AI's recommendations. The human supervisor should also be enabled to put the results of the AI systems into perspective at any time, as well as to interrupt the operation of the AI (panic button).

Art. 14 (5) AI-Act-P again contains special provisions regarding the use of AI systems with biometric information; here, it is part of human supervision that no decisions or measures are taken until at least a second natural person has not verified and confirmed the identification of the data subjects.

f) Sturdiness, Accuracy and IT Security Requirements

Art. 15 AI-Act-P also requires sufficient security and accuracy of the AI systems. Regarding the sturdiness of the systems, the AI-Act-P leaves the exact requirements largely open, but points out that these can be achieved by technical measures such as back-up systems or *"fail-safe plans"*, Article 15 (3) AI-Act-P. It is noteworthy in this context that Art. 15 (3) sentence 3 AI-Act-P also covers so-called *"feedback loops"*, in which the self-learning system practically arrives at a path dependency of its assessments based on its own results; these are to be mitigated (and thus not necessarily prevented) by appropriate measures. With regard to cybersecurity, Art. 15(4) AI-Act-P requires that AI systems shall be secured against attacks by unauthorized third parties, also covering the manipulation of *training data* or the falsification of learning models; in the context of conformity assessments, the AI-Act-P also includes certifications under the Cybersecurity Act, for which a presumption of conformity then also applies according to Art. 42(2) AI-Act-P.[61]

g) Transparency and Instruction Obligations

Finally, Art. 13 AI-Act-P contains instructional obligations and first provides in Art. 13 (1) AI-Act-P that AI systems must be designed in such a way that they are sufficiently transparent to enable users to use the system correctly and to interpret the results. However, the real focus is on the instructions that an AI system must contain: In addition to a general clause in Art. 13(2) AI-Act-P, Art. 13(3) AI-Act-P contains a catalog of necessary instructions, which primarily refers to the degree of *sturdiness*, *accuracy* and *safety* for which the AI has been tested, as well as circumstances

[61] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15.

that may have an influence on it. Furthermore, information must be provided on risks to health, safety or impairment of fundamental rights that may occur as a result of foreseeable events within the intended purpose of the AI or from anticipated misuse; noting that Art. 13 (3) (b) (iii) AI-Act-P does not distinguish between the different fundamental rights. In addition, the required information on the *training, validation* and *test data* used for the AI is important, Art. 13 (3) b) v) AI-Act-P; only in this manner can the user assess the basis on which the AI was actually trained. Finally, information about the human monitoring measures must also be provided pursuant to Art. 14 AI-Act-P, Art. 13 (3) d) AI-Act-P.

VI. Transparency Obligations for All AI systems

For specific AI systems, the transparency obligations under Art. 52 AI-Act-P also apply, which do not have to be high-risk systems. This concerns AI systems that pose particular risks of manipulation, whether through interaction with humans, para. 1, or through emotion recognition systems or biometric categorization, para. 2, or finally through the generation or manipulation of content resembling real persons or events, in particular images or videos (so-called *"deep fakes"*), para. 3. For all groups, the AI-Act-P requires that the third parties concerned be informed that corresponding AI systems are being used, in each case with exceptions for AI systems that serve law enforcement or crime fighting purposes. In addition, Art. 52 (3) (2) AI-Act-P allows the use of *deep-fake* AI systems for necessary artistic or scientific purposes or for forming opinions, without the artificial creation of the content having to be made clear in these cases.

However, apart from informing the data subjects, Art. 52 AI-Act-P does not provide for a mandatory right for the data subjects to receive an offer or service from the operator even without the use of AI. Therefore, even with this regulation, the data subject does not (yet) have a genuine opt-out right associated with a right to contact a human being.

VII. Obligations for Operators and Users of AI systems

1. Obligations for Operators, Manufacturers and Quasi-manufacturers

Art. 16 of the AI-Act-P obliges the operators, in addition to complying with the requirements for the AI systems, to follow the (usual) components of a *conformity assessment* procedure, including the affixing of the CE mark (Art. 19 of the AI-Act-P), in particular to maintain a *quality management system* in accordance with Art. 17 of the AI-Act-P, to maintain the log files, insofar as these are under the control of the providers, or to carry out the registration in accordance with Art. 51 of the AI-Act-P. In addition to the components for the safe design and development, as well as the testing and validation of the AI systems, known from product safety, including the *risk management system* according to Art. 9 AI-Act-P, the quality management system primarily comprises comprehensive specifications relating to *data management*,

from data collection to data mining to data storage, Art. 9 (1) f) AI-Act-P. Moreover, the quality management system must include product monitoring pursuant to Art. 61 AI-Act-P as well as procedures for the notification of serious incidents pursuant to Art. 62 AI-Act-P, Art. 17 (1) h) and i) AI-Act-P. In this context, Art. 17(2) AI-Act-P also considers the size of the *operator's* organization and thus the proportionality.

Regarding the *log files* created by the AI systems pursuant to Art. 12 AI-Act-P, the *operators* will be obliged to retain them if they are under their "control", be it because of contractual agreements with the user or based on legal obligations, Art. 20 (1) AI-Act-P. The time period within the log files must be kept is limited by Art. 20 (1) (2) AI-Act-P to that which is appropriate to the purpose of the AI system and to the relevant Union and Member State regulations. Interestingly, the GDPR is neither considered nor breached here, so that the purpose of data deletion and economy, Art. 5 (1) b) and c) GDPR, must be observed.

Finally, closely interlinked with the product monitoring obligations is Article 21 of the AI-Act-P, which obliges the *operator to take corrective measures* in the event that the *operator* has indications that the AI system no longer complies with the requirements of the AI-Act-P, up to and including the obligation to recall the product. In these cases, the *dealers* involved must also be informed, as must *importers or authorized representatives*.

According to Art. 24 AI-Act-P, *manufacturers* are treated like *operators* if they fall under Annex II Section A, i.e. the *conformity assessment procedures* according to the *New Legislative Framework*, and the product is placed on the market together with the AI system under the name of the *manufacturer*. However, the operator is not released from the obligations regarding the AI system, but only with the product itself.

Similar to other product safety regulations,[62] Art. 28 AI-Act-P also treats as *operators* all those who market the AI system under their name or brand, or who have significantly modified the AI system itself or its intended use. In the latter two cases, the AI-Act-P no longer declares the actual *operator* responsible, which seems understandable because the AI system no longer corresponds to the product that the *operator* intended to market.

2. Obligations for Importers and Distributors

Similar to other product safety regulations,[63] special obligations apply to the importer, first of all the verification that the operator has complied with the conformity assessment procedure including CE marking, but also that the importer is not

[62] Thus among other things in Art. 2 e) Directive 2001/95/EC of the European Parliament and of the Council of 03 December 2001 on general product safety [2002] OJ L 11/4.

[63] See e.g. Art. 13 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002

allowed to introduce the AI system into the market if he has indications that the system does not comply with the requirements of the, Art 26 (2) AI-Act-P. Otherwise, in addition to the notification of risks to the provider and the supervisory authorities pursuant to Art. 26 (2 Sentence 2), Art. 65 (1) AI-Act-P, the importer is primarily responsible to the supervisory authorities for providing the necessary information and documentation for compliance, but also for the log files that the operator has under its control, Art. 26 (4) AI-Act-P.

If an importer cannot be identified, the authorized representative or agent of the operator of the CI located outside the EU will step in with regard to the obligations to cooperate with the *authorities*, including the documentation on compliance and access to the *log files* in accordance with Art. 25 AI-Act-P.

On the other hand, a *distributor* is responsible under Article 27(1) of AI-Act-P for checking the CE marking, including the necessary instructions, and for ensuring that the *operator* and, if applicable, the *importer* comply with the obligations under the Draft Regulation; however, it is unclear how a *distributor* is supposed to meet the latter requirement, as this includes, among other things, compliance with the risk and quality management system, etc. The *distributor* is also required to notify the *importer* of any non-compliance with the provisions of the AI-Act-P. Similar to the *importer's* obligations, the *distributor* is also required under Article 27 (2) of the AI-Act-P not to place the AI system on the market if there are corresponding indications of non-compliance with the AI-Act-P; however, in addition to the *importer* obligations the *distributor* is also required to take corrective measures itself or through the *operator*, *importer* or any other *user*, up to and including the recall of the AI system if it does not comply with the general requirements for AI systems. Art. 27 (4), Recital 23 AI-Act-P. Risks pursuant to Art. 65 (1) AI-Act-P must be reported to the supervisory authorities without delay.

3. Obligations for Users

Roughly speaking, the (commercial) *users* of AI systems are subject to three obligations: *First*, they must use the AI systems in accordance with the instructions of the operators, Art. 29 (1) AI-Act-P, *second*, that the data used for the AI systems are relevant to the intended use of the AI, Art. 29 (3) AI-Act-P, and *thirdly*, the obligation to monitor the AI system including the notification of risks according under Art. 65 (1) AI-Act-P to the *operator* or *distributor* and the temporary suspension of the AI system, in case of serious incidents according to Art. 62 (1) AI-Act-P including the interruption of the AI system. Furthermore, *users* must retain the log files that remain under their control for the period of time outlined in Article 20 AI-Act-P.

---

and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1; Art. 8 Directive 2014/29/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of simple pressure vessels [2014] OJ L 96/45.

Remarkable here are the comparatively little detailed regulations on training the AI systems, which often take place on the user side; only the passage that the *input data* must be "relevant" can be made fruitful here.

VIII. Conformity Assessments

One of the important components of the AI-Act-P is the differentiated conformity assessment procedures, which follow the *New Legislative Framework* approach, but also include the so-called *stand-alone AI systems* in a completely new way. Apart from the accreditation and notification procedures regulated in Art. 30-39 of the AI-Act-P, which contain few surprises, Art. 40 of the AI-Act-P establishes the presumption of conformity based on compliance with harmonized technical standards accepted by the EU.

The same applies to so-called *common specifications*, which the *EU Commission* can adopt by means of implementing acts if there are no technical standards or only standards that do not cover all risks, Art. 41 AI-Act-P. For products containing AI systems, the AI-Act-P acts as an additional horizontal regulation which supplements the conformity assessment procedures under the sectoral standards.

Once again, the outstanding position of harmonized technical standards becomes clear - but so far only various development projects are available, for example in the form of the roadmap of DIN and DKE with the support of the *Federal Government*,[64] as well as some standardizations of the ISO,[65] such as the trustworthiness of AI systems. (ISO/IEC TR 24028) or the IEEE (7010-2020) about "Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-being".[66]

1. Possible Procedures

In conjunction with the respective Annexes VI and VII Article 43 of the AI-Act-P sets the central course for the choice of conformity assessment procedures. According to Annex VI, the operator can prove conformity by means of internal controls, which refer to the quality management system to be established according to Art. 17 of the AI-Act-P as well as the technical documentation and product monitoring. According to Annex VII, proof of conformity is provided by an inspection of the quality management system and the technical documentation by a certification body. Section 4.6. subsection 5 Annex VII AI-Act-P contains specific requirements in case the certificate was refused due to insufficient or inadequate *training data*; in which case the AI shall be re-trained.

---

[64] See to this the Roadmap-Recommendations of the DIN and DKE, November 2020, accessed November 03, 2022, https://www.din.de/resource/blob/772438/6b5ac6680543eff9fe372603514be3e6/normungsroadmap-ki-data.pdf.

[65] See to this the overview from iSO/IEC Joint Technical Committee JTC 1/SC 42, accessed November 03, 2022, https://www.iso.org/committee/6794475/x/catalogue/.

[66] Overview of relevant standards and related standards in roadmap of the DIN and DKE, (n 64), 152 with more references.

2. Biometrical AI-Methods

However, in the case of AI systems for biometric recognition, the *operator* can only choose between the two forms of conformity assessment if harmonized technical standards or the *"common specifications"* of the *EU Commission* are available, otherwise he is instructed to use the procedure with the help of a certification body in accordance with Annex VII, Art. 43 (1) AI-Act-P. In principle, the *operator* is free to choose the certification body, unless the AI is to be used by national authorities or EU institutions for law enforcement or in the context of migration and asylum policy; in this case the market surveillance authority must act as a certifier in accordance with Article 63 (5) and (6) of the AI-Act-P.

3. Stand-Alone-AI

All other AI systems according to Annex III are only "certified" according to Annex VI with the help of internal controls by self-declaration of the manufacturer, except for creditworthiness systems, which are subject to the procedure according to Art. 97 - 101 of Directive 2016/36/EU;[67] the involvement of a certifier is explicitly not required here. For the first time, Art. 43 (2) AI-Act-P thus introduces an independent conformity assessment procedure for *stand-alone* AI systems, which, however, is only based on internal controls by the *operator*. Also, Art. 43 (2) AI-Act-P apparently does not make the conformity assessment dependent on the existence of harmonized technical standards or *"common specifications"*, as these are not mentioned in contrast to Art. 43 (1) AI-Act-P, not even in Annex VI.

4. AI Systems as a Component of Products

On the other hand, AI systems that are part of products subject to a conformity assessment procedure according to Annex II Section A of the AI-Act-P, participate in these procedures, albeit with slight modifications, since Annex VII also applies to the examination of the technical documentation by the certifier. The *operator* or *manufacturer* of the products can use the same certifiers that are also approved for the respective product certification, provided that they also meet the requirements of Art. 33 (4) (9) (10) AI-Act-P. Even if the respective regulation provides for the possibility for the manufacturer to opt out of the certification procedure, he can only do so if he applies harmonized technical standards or the *"common specifications"* of the *EU Commission* according to Art. 41 AI-Act-P.

5. AI Changes

Art. 43 (4) subpara. 2 AI-Act-P also regulates the important case of changes to AI systems due to their characteristic of self-development; if these independent further

[67] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L 176/338.

developments remain within the framework provided for by the operator and are part of the technical documentation according to Annex IV No. 2 f) AI-Act-P, they are not to be considered as a change to the AI system and therefore do not trigger a new conformity assessment. Also, against the background that issued certificates are to be valid for 5 years according to Art. 44 AI-Act-P, this regulation should not be underestimated in its scope. In practice, it will be problematic to determine precisely whether the independent changes to the AI are still within the framework set by the operator, and according to which criteria this is to be assessed.

6. Temporary Suspension of the Conformity Assessment Procedure by the Supervisory au-thority

Art. 47 (1) AI-Act-P empowers the market surveillance authority to temporarily suspend the conformity assessment procedures or to approve the market launch of an AI system for the respective Member State if this exceptionally serves public safety or the protection of life and limb, environmental protection, but also the protection of particularly important industries or critical IT infrastructures. In this case, the market surveillance authority must check if the AI systems meet the requirements, Art. 47 (2) AI-Act-P.

7. Affixing CE Marking

In addition to the preparation of the EU declaration of conformity according to Art. 48 AI-Act-P, a typical feature of EU product safety is the affixing of the CE mark. While this should still not yet be a problem for products with AI systems, it is different for *stand-alone* AI products. Art. 49 (1) AI-Act-P therefore allows the CE marking to be affixed either on the *packaging* or in the documentation to be prepared.

8. Registration in EU Database

Finally, another cornerstone of the European Commission's regulatory approach is the obligation of *operators* (or authorized representatives) under Article 51 AI-Act-P to register high-risk AI systems in the database operated by the *European Commission* under Article 60 AI-Act-P before they are launched or put into operation. Although this does not imply a reservation of approval, it facilitates ex-post control by the market surveillance authorities and the *EU Commission*.

IX. Creation of "Regulatory Sandboxes" and Facilitation of SMEs

A tool especially associated with new technologies such as blockchain and cryptocurrencies [68] which the *EU Commission* also wants to apply to AI systems, are the so-

[68] See to this also the overview regarding "Regulatory Sandboxes" in the financial sector of the ESMA/EBA/EIOPA, "FinTech: Regulatory Sandboxes and innovation hubs" 2019, accessed November 03, 2022, https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf ; see also Baker & McKenzie, "A Guide

called *regulatory sandboxes*.[69] However, this *"regulatory sandbox"* does not turn out to be an incubator for innovative AI systems that are not subject to regulation for a while, but is intended to represent a controlled test environment for the development and testing of AI systems under the direct supervision of the competent authorities of the Member States or the *European Data Protection Supervisor* in accordance with a test plan agreed with the supervisory authorities, Art. 53 (1) AI-Act-P. As far as personal data are involved, Art. 53 (2) AI-Act-P also explicitly requires the involvement of the *data protection supervisory authorities* of the respective Member States. However, Art. 53 (3) AI-Act-P can again be interpreted in such a way that the supervisory authorities have a certain leeway in applying the *"regulatory sandbox"*, in that only in the event of significant risks to health, safety or fundamental rights should an obligation to take immediate remedial action and - if this should last longer - to interrupt the development and testing process intervene. Finally, the fact that the *"regulatory sandbox"* does not represent a fundamental "grace period" for the operators of the AI systems is shown by Article 53 (4) of the AI-Act-P, which subjects all participants in the *"regulatory sandbox"* to liability in accordance with the applicable provisions of the EU and the Member States for damage caused to third parties as a result of the experiments in the *"regulatory sandbox"*; since the participants also include the supervisory authorities, state liability also applies. However, most of the provisions on the details of the *regulatory sandboxes*, including the rights and obligations of their participants, are left to delegated acts by the *EU Commission* under Article 53(6) in conjunction with Article 74(2) of the AI-Act-P.

In this context, Art. 54 AI-Act-P pays special attention to the data protection implications of the *regulatory sandboxes*, whereby the *principle of strict purpose limitation* according to Art. 5 (1) b) GDPR is opened under certain conditions. This is only permissible for "innovative" AI systems that serve either law enforcement, the fight against crime, the safeguarding of public security or public health, in particular the fight against diseases, or the improvement of environmental protection, Art. 54 (1) a) i) - iii) AI-Act-P. Furthermore, Art. 54 (1) b) AI-Act-P requires that the objectives of the development and testing of AI systems cannot be achieved with synthetic or anonymized data. Finally, Art. 54 (1) c) - h) AI-Act-P impose numerous other conditions, all of which serve to minimize the risks to data protection, such as the requirement that data be deleted after the "*sandbox*" has ended or that processing only take place in an isolated and protected space.

---

to regulatory FinTech sandboxes internationally" 2020, accessed November 03, 2022, https://www.bakermckenzie.com/-/media/files/insight/publications/2020/05/a_guide_to_regulatory_fintech_sandboxes_internationally_8734.pdf?la=en; Energiesektor in Bundesamt für Energie/Frontier Economics, "Regulatory Sandboxes – best practices für die Schweiz, Freiräume für neue Ansätze und digitale Innovation in der Stromversorgung" 2020, accessed November 03, 2022, https://pubdb.bfe.admin.ch/de/publication/download/10074 .

[69] Comprehensive on the administrative law problems of these "regulatory sandboxes", see Christoph Krönke, "Sandkastenspiele – "Regulatory Sandboxes" aus der Perspektive des Allgemeinen Verwaltungsrechts," *JZ*, (2021): 434 with further references.

On the other hand, the measures announced by the *European Commission* for the benefit of start-ups and SMEs are limited to the obligation of member states to ensure easier access to the "*sandboxes*" for these AI operators, otherwise to the creation of special communication channels in order to provide guidelines for the application of the AI-Act-P for these companies, according to Article 55 (1) a) of the AI-Act-P. In contrast, the obligation to consider the size of the company concerned when setting fees for the conformity assessment procedure, Art. 55 (2) AI-Act-P, is likely to be more significant.

X. Codes of Conduct

Art. 69 AI-Act-P creates the possibility for operators of non-high-risk AI systems to also apply the requirements that apply only to high-risk AI systems to other AI systems through voluntary *Codes of Conduct*. Within this framework, these *Codes of Conduct* shall be supported, especially for AI systems in the area of sustainable environmental protection or accessibility for severely disabled persons, including the participation of *stakeholders* in the design and development of the AI systems, up to diversity in the development teams, Art. 69 (2) AI-Act-P. Such *Codes of Conduct* require that users as well as all other interested *stakeholders* or their associations are involved in their development and adoption, Art. 69 (3) AI-Act-P.
Unlike Art. 40 i and Art. 28 (1), (4), 24 (3), 32 (3) GDPR, the AI-Act-P does not contain any relief for *operators* if they have joined such *a Code of Conduct*; in this respect, it remains more than doubtful what incentives should exist for operators to develop such *Codes of Conduct* or to join them.

XI. Supervisory and Monitoring Structures

1. Creation of a European Artificial Intelligence Board

Similar to the GDPR and the Digital Service Act proposed in December 2020, which provides for the creation of an *EU Digital Services Board*, the *EU Commission* also wants to provide for a *European Artificial Intelligence Board* for the regulation of AI according to Art. 56-58 AI-Act-P, which is essentially to advise the *EU Commission* and ensure coordination of enforcement and monitoring by the national supervisory authorities. The *European AI Board* should be composed of the national supervisory authorities and the *European Data Protection Supervisors* and be chaired by the *EU Commission*, Art. 57 AI-Act-P.

2. Monitoring Authorities

In addition to the usual obligations of the Member States to designate national supervisory authorities, which must cooperate with each other, Article 59 (1) (2) of the AI-Act-P provides that the supervisory authorities must be organized in such a way that they can carry out their activities impartially and objectively – but this does not mean that they must be fully independent as under the GDPR. Finally, Art. 59

(8) AI-Act-P designates the *European Data Protection Supervisor* as the supervisory authority over EU authorities or agencies that may be covered by the AI-Act-P when using AI systems.

3. EU-Wide Database as a Register

Since the AI-Act-P for the first time also covers *stand-alone AI systems* outside of products, their registration is of essential importance for effective market and product monitoring. Even though it is not a classic register for the creation of rights and obligations and the AI-Act-P does not provide for a requirement for approval in the narrower sense, registration in the EU database in accordance with Article 60 of the AI-Act-P is necessary for an *operator* to be able to introduce his high-risk AI system into the European market or put it into operation. According to Annex VIII AI-Act-P, the required information includes not only the usual information on the identity and accessibility of the operator and the EU declaration of conformity, but also information on the purpose of the AI (No. 5) or instructions for its use (No. 11), except if the AI is used for law enforcement or migration and asylum purposes.

XII. Monitoring and Reporting Obligations of AI Operators

1. Product Monitoring

In view of the unpredictable risks and developments that occur in self-learning AI systems in particular, the obligation to monitor products after a market launch or commissioning of an AI system is coming into focus – not only in product liability law[70], but also in product safety law –, here Art. 61 AI-Act-P. For this purpose, the *operator* must prepare a product monitoring and surveillance plan as part of its technical documentation, the details of which must comply with the requirements of an implementing act of the *EU Commission*, Art. 61 (3) AI-Act-P. If the AI system is part of a product that is subject to other conformity assessment procedures and thus also to the product surveillance obligation, the obligations according to Art. 61 (1), (2) AI-Act-P must be integrated into it, Art. 61 (4) AI-Act-P.

2. Reporting Requirements

Similar to the obligations under the GDPR in the event of data breaches (*notification of data breach*), Art. 33 GDPR, Art. 62 (1) AI-Act-P also standardizes a reporting obligation for *operators* of high-risk AI systems to the market surveillance authorities

[70] On product monitoring obligations for AI systems see Spindler, (n 9), 761 ff.; Alexander Schmid, "Pflicht zur "integrierten Produktbeobachtung" für automatisierte und vernetzte Systeme," *CR,* (2019): 141, 142; Gerald Spindler, «§ 11», in *IT-Sicherheitsrecht,* ed. by Gerrit Hornung, Martin Schallbruch, (München: C.H. Beck, 2020) para 31; Michael Denga, "Deliktische Haftung für künstliche Intelligenz," *CR,* (2018): 69, 74; Franz Hofmann, "Der Einfluss von Digitalisierung und künstlicher Intelligenz auf das Haftungsrecht," *CR,* (2020): 282, 285 f.; Wagner, (n 9), 707, 750.

in case of a serious incident or malfunctioning in the Member State where the incident or malfunctioning occurred, but only if these obligations under EU law are intended to protect fundamental rights. Thus, Art. 62 (1) AI-Act-P establishes a *general notification obligation* beyond the regulation of AI, which can affect all EU regulations that come into consideration. In this context, it is noteworthy that Article 62 of the AI-Act-P only refers to *incidents relevant to fundamental rights*, but not to the other risks to public security mentioned in the AI-Act-P.

Operators must notify without delay if they have reason to believe that the AI system is likely to be the cause of the incident or malfunction; in any case, the operator must notify within 15 days after becoming aware of the significant incident or malfunctioning, Art. 62 (1) (2) AI-Act-P.

3. Enforcement and Monitoring

The monitoring of the markets is the responsibility of the authorities under Regulation (EC) No. EU/2019/1020, whereby the term *"operator"* refers to all obligated parties under Art. 16 et seq. AI-Act-P, i.e. both *providers and distributors and users*, and also *stand-alone AI systems* as products, Article 63 (1) AI-Act-P. For products subject to the conformity assessments of the sector-specific product safety regulations and directives, the respective authorities continue to be responsible, for credit institutions the corresponding supervisory authority, for biometric systems used in the context of law enforcement or migration and asylum, the national data protection supervisory authorities, Art. 63 (3) - (5) AI-Act-P, for systems in the area of the EU institutions the *European Data Protection Supervisor*, Art. 63 (6) AI-Act-P.

On the one hand, the powers of the supervisory authorities include full *access* to the entire *training and test datasets* of the AI systems, which must also be possible through technical interfaces for remote monitoring, Art. 64 (1) AI-Act-P; on the other hand, even *access to the source code* may be requested by the supervisory authorities in order to assess compliance with the provisions for high-risk AI systems, Art. 64 (2) AI-Act-P. Other national supervisory authorities responsible for enforcing Union law relevant to fundamental rights, are also authorized to monitor, but limited to requesting the relevant documents and documentation or, if these are insufficient, may make a corresponding request to the market surveillance authority to organize tests of the AI systems, Art. 64 (3) (5) AI-Act-P.

The AI-Act-P pays particular attention to the procedure for carrying out inspections of AI systems (apparently without restriction to high-risk AI systems, which are then generally considered to be high-risk) with regard to compliance with the obligations if risks to health, safety or fundamental rights become apparent, Art. 65 (1) (2) AI-Act-P. In the event of non-compliance with the obligations under the AI-Act-P, the market surveillance authority may order all necessary measures against the operator, up to and including the obligation to recall the AI system or product, Art. 65 (3) AI-Act-P, and, in the event that the *operator* does not comply with the order, may itself initiate the product recall, in addition to other necessary measures, Art. 65 (5) AI-Act-P.

However, even if the market surveillance authority determines compliance with the requirements of the AI-Act-P in the course of the review, it remains authorized to require the *operator* to take appropriate measures, up to and including product recall, within a period of time commensurate with the risks, provided that the AI system still presents risks to the health or safety of persons or with regard to compliance with obligations under Union law with relevance to fundamental rights or – in contrast to other powers, for example – also to the protection of other public interests, Article 67 (1) AI-Act-P. The *operators* must eliminate or reduce the risks that have arisen within the period of time to be determined by the market surveillance authority, Art. 67 (2) AI-Act-P.

XIII. Sanctions, in Particular Fines

Following the example of the GDPR (cf. Art. 83 (1) and (4-6) GDPR) and other (proposed) EU legislation such as the Digital Services Act, Art. 71[71] AI-Act-P provides for drastic fines for non-compliance with the respective provisions of the AI-Act-P: Thus, violations of the prohibitions of Art. 5 AI-Act-P, which apply to every AI system, as well as of Art. 10 AI-Act-P - the requirements for *data governance* - are to be fined for companies as *operators* with up to 6% of their worldwide annual turnover, Art. 71 (3) AI-Act-P; for other violations, Art. 74 (4) AI-Act-P then "only" estimates 4% of the worldwide annual turnover. In contrast to the GDPR (cf. recital 150 and Art. 83 (4) and (5) GDPR), the AI-Act-P does not contain a group-related regulation, so that so far only the respective *operator* of the AI system, but not the group, can be used as the basis for turnover. However, all "offenders" according to Art. 71 AI-Act-P can be considered as infringers or addressees of fines, i.e. not only *operators*, but also *users* and *operators*, if they have violated the obligations incumbent on them.

XIV. Critical Evaluation

Overall, it is difficult to evaluate the AI-Act-P: The *EU Commission* can be credited with having made a courageous attempt to introduce one of the world's first regulations of AI systems. The AI-Act-P contains numerous sensible approaches, especially regarding the principle of a *risk-based approach*, since the chances of broad-based supervision are likely to be rather slim, especially in view of the possibilities of supervisory authorities to supervise the rapidly changing AI. Likewise, the broad international scope of application, which does not take into account the location of AI *operators*, is to be welcomed - although the general definition of AI systems seems somewhat eclectic and too broad, as it would also include expert systems without the characteristic properties of AI systems, such as the *"black box effect"*.

[71] Commission, "Art. 59 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", December 15, 2020, COM (2020) 825 final 2020/0361(COD).

- Risk: Insofar it concerns high-risk AI systems the *risk-based approach* in particular tends to be devalued if only registration of the AI system in an EU database is required and the prior checks are limited to internal controls to be carried out by the operator itself, at least for so-called stand-alone AI systems. It is true that the Commission points out that there is hardly any experience with auditing and certification for stand-alone systems and that the AI sector is highly innovative and subject to constant change;[72] but it seems questionable why this should be assessed differently for *embedded AI systems* in products that are subject to a certification procedure, in other words: why certification involving certification or auditing bodies should not also be required for high-risk *stand-alone AI systems*. Despite the fundamentally correct approach of relying on technical standards and their certification, the *EU Commission* continues to distinguish between *stand-alone* and *embedded AI systems*, which ultimately seems rather arbitrary in the light of cloud-based control. After all, control by an AI detached from a product and supported or located in the cloud would be such a *stand-alone* system.
- Horizon: However, the *horizontal approach* that overcomes the sectoral boundaries of product security, is to be welcomed - and should also be made fruitful for the Cybersecurity Act in the same way as a product security element. The approach that applies in principle to product safety is also correct, i.e. to resort to *harmonized technical standards*, combined with a *presumption* that the requirements will then be met; only in this way it will be possible for the developers and operators of AI systems to present alternative, equivalent solutions beyond technical standards, so that the necessary flexibility is maintained.
- Standards: However, the definition of technical standards or *common specifications* by the *EU Commission* remains problematic: If fundamental risks are to include impairments of fundamental rights, numerous undefined factors must be included, making it difficult to define *"benchmarks"* for the avoidance of such risks. This does not change the fact that the AI Regulation contains numerous reasonable requirements, such as requiring human supervision, the prevention of *bias* or the focus on proper *data governance* with regard to interpreting the training of data-based AI, as well as the prevention of *"feedback loops"* in order to avoid path dependency of the AI and self-reinforcing assessments. In addition, detailed points of criticism remain, for example with regard to the numerous exemptions for biometric identification procedures, which remain generally permissible for private *operator* and are allowed for government authorities for law enforcement and law enforcement purposes under certain conditions. Similarly, transparency obligations for certain non-high-risk AI systems are well-intentioned, but do not give those affected by the AI systems' decisions or recommendations a proper right to opt-out or contact a human. Regulatory *sandboxes* are also very rudimentary, leaving much to the delegated acts of the *EU Commission*. Finally, the scope

[72] Explanatory Memorandum, (n 8), 14.

of market surveillance raises questions, as it remains unclear what should be considered as EU acts relevant to fundamental rights, since in principle any regulation can affect fundamental rights in some way. Overall, the proposal for an AI Regulation is therefore to be welcomed, even though it still contains numerous open flanks - the further political fate of this ambitious draft remains to be seen.

B. Part 2: Proposals on Product Liability and Liability for AI systems

I. Introduction

The issues of artificial intelligence have been occupying lawyers all over the world for several years. For example, there are also reports from expert groups at the EU Commission on artificial intelligence, which take a detailed position on the various ethical and legal issues,[73] which, among other things, takes a position on the various legal issues raised. The *German Jurists' Conference* has also taken up the topic, for which *Zech* has prepared a detailed expert opinion on the associated liability issues.[74] In essence, the discussion revolves around the possibilities that already exist in the current non-contractual (tort) liability law to deal with the specific issues of autonomous systems, as well as legal policy desiderata as to whether and how existing gaps should be filled. The legal policy discussion at the national level has now been caught up with at the European level: [75]After the *EU Parliament* had already submitted a formulated proposal on liability,[76] the *EU Commission is* now submitting a directive on the formulation of liability for AI systems (AI Liability Directive-E)[77] including a reform of the Product Liability Directive (ProdHaft Directive-E) following the proposal on the regulation of AI in terms of product safety law (AI

[73] AI HLEG, "Ethical Guidelines for Trustworthy AI", European Commission, April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425; European Commission, Directorate-General for Justice and Consumers, "Liability for artificial intelligence and other emerging digital technologies", Publications Office, 2019, https://data.europa.eu/doi/10.2838/573689.

[74] *Zech*, (n 9).

[75] Commission, "Proposal of the EU Commission for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain acts of the Union (AI-Reg-E)", April 21, 2021, COM (2021) 206 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN; on this in detail Gerald Spindler, "Der Vorschlag einer Regulierung der Künstlichen Intelligenz" *CR* (2021): 361 et seq. .

[76] Zech, (n 9), (cited as *Zech*, Supplement, 2022); Gerhard Wagner, "Haftung für Künstliche Intelligenz – Eine Gesetzesinitiative des Europäischen Parlaments Aufsatz," *ZEuP,* (2021): 545 et seq.

[77] Commission, "Proposal of the EU Commission for a Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability in artificial intelligence (AI Liability-E)", September 28, 2022, COM (2022) 496 final 2022/0303 (COD).

Regulation-E).[78] Almost at the same time, the *EU Commission* has published a proposal for a new horizontal regulation on the cyberresilience of IT products, which considerably expands the product safety regulations – which cannot be dealt with here in extenso, but will also have an impact on liability. [79]

To sum it up briefly: It is not so much the proposal for the AI Liability Directive as the proposed innovations in the Product Liability Directive that make us sit up and take notice. The proposal of the Product-Liability-D-P provides for nothing less than the equalization of software and even connected services with the concept of product, which is tantamount to a small revolution and also corresponds to the proposal of the CRA-E. In contrast, the AI Liability Directive-E refrains from adopting the proposals of the *EU Parliament* for the introduction of strict liability[80], in that the AI Liability Directive-E essentially restricts itself to remedying the information asymmetries in favour of the injured party.

II. Reform of the Product Liability Directive

The proposal of the Product-Liability-D-P aims above all at the synchronization with the reforms in product safety according to the Decision and the definitions in Decision 768/2008/EC[81] , but also at the inclusion of IT products or software including AI systems and connected services up to the extension of the protected legal interests to include data. The Product-Liability-D-P also introduces considerable simplifications of proof and the extension of the responsible parties or liability addresses.

1. The redefinition of the concept of product

a) Software as a product

One of the long overdue reforms of the Product-Liability-D-P concerns the inclusion of software as a *product* - in contrast to the previous law, regardless of whether

[78] Commission, "Proposal of the EU Commission for a Directive of the European Parliament and of the Council on Liability for Defective Products (Product-Liabiltiy-D-P)", September 28, 2022, COM (2022) 495 final 2022/0302 (COD).

[79] Commission, "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU)", September 15, 2022, 2019/1020 COM (2022) 454 final, hereafter cited as CRA-E.

[80] Resolution of the European Parliament of 20 October 2020 with recommendations to the Commission on the regulation of civil liability in the use of artificial intelligence (2020/2014(INL)); Regulation of civil liability in the use of artificial intelligence, P9_TA (2020)0276; see Wagner, (n 76), 545 ff.; Zech, (n 9), supplement to the DJT Opinion, 2022, 4, 9.

[81] Decision No. 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products and repealing Council Decision 93/465/EEC, [2008] OJ L 218/82 .

the software is embodied ("embedded") in another *product* or not.[82] This is more than clearly expressed in Recital 12 of the Product-Liability-D-P, in which the *EU Commission* points out that software can also control cloud-based *products*, and is also reflected in the definition of the *product in* Art. 4 No. 1 of the Product-Liability-D-P.[83] The proposal even goes one step further and includes "digital manufacturing files" under the term "*product",* Art. 4(2)(1) Product-Liability-D-P, which primarily (but not exclusively, Recital 14 Product-Liability-D-P) means 3D data files for the manufacture of *products* in 3D printers, as Art. 4(2) Product-Liability-D-P states ("digital template of a movable").[84]

On the other hand, the *EU Commission* does not want to include pure source code in the definition of product, as this only represents information, recital 12 p. 3 of the Draft Directive on Product Liability; the Draft Directive on Product Liability thus assumes that the definition of software only includes machine-executable coding and, interestingly, deviates from Art. 1 (1) and (2) as well as recital 7 p. 2 of the Software Directive[85] in copyright law.[86] Further details, however, are not to be found in the Product-Liability-D-P, for example on the treatment of program libraries, which themselves do not have a direct controlling effect, but can be important components of a code; if one keeps in mind the goal of the *EU Commission* that controlling software should be covered, one will also have to understand such parts of a code as a *product.*

Consequently, Recital 12, Sentence 4 of the Draft Directive on Product Liability then regards the developers or producers of software, including the *operators of* AI systems, as *manufacturers within the* meaning of the Draft Directive on Product Liability.

---

[82] Herbert Zech, "Haftung für Trainingsdaten Künstlicher Intelligenz," *NJW,* (2022): 502 (505); Wagner, (n 9), 707 (716 et seq.); for copyright equivalence see ECJ Judgment of 03 July 2012 - C-128/11, ECLI:EU:C:2012:407, 47- *Used Soft = CR,* (2012): 498.

[83] Similarly, the proposal for a Cyber Resilience Act also covers software as a stand-alone "product", see Art. 3 No. 1 CRA-E.

[84] Gerhard Wagner, «§ 2 ProdHaftG», in *MüKo BGB*, ed. Franz Jürgen Säcker et al. 8th edn. (München: C.H. Beck, 2020), marginal no. 28 2020; Anne-Kathrin Müller and Martin S. Haase, "Haftungsrechtliche Aspekte des 3D-Drucks (additive Fertigung) – Teil 2," *InTer,* (2017): 124 (127); Jürgen Oechsler, "Produkthaftung beim 3D-Druck," *NJW,* (2018): 1569 (1570); in this direction also Graf von Westphalen, «§ 47 marginal no. 44.», in *Produkthaftungshandubuch,* ed. Ulrich Foerste and Friedrich Graf von Westphalen 3rd edn. (München: C.H. Beck, 2012); in general on product liability with 3D printers s. Oechsler.

[85] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, [2009] OJ L 111/17.

[86] On the protection of the source code by the Software Directive ECJ Judt. 22 December 2010 - C-393/09, ECLI:EU:C:2010:816 marginal no. 34 f. - *BSA/Ministry of Culture = CR,* (2011): 221; Gerald Spindler, «§ 69a UrhG», in *Urheberrecht*, ed. by Gerhard Schricker and Ulrich Loewenheim 6th edn. (München: C.H.Beck 2020) marginal no. 5; Andreas Wiebe, «§ 69 a UrhG», *Recht der elektronischen Medien*, ed. Gerald Spindler and Fabian Schuster, 4th edn. (München: C.H.Beck, 2019) marginal no. 4.

b) Extension to data and services

The implicit extension of liability to "components" and, above all, *services* contained in Art. 4(3) and (4) of the Draft Directive on Product Liability, for which it is sufficient that they are connected to the *product in* some way, seems almost revolutionary. According to Art. 4 No. 4 Draft Directive on Product Liability, what matters is that the *product* cannot fulfil one or more of its functions without these services. Recital 15 p. 1, 2 of the Draft Directive on Product Liability clarifies that services are not generally covered by the strict liability of the Draft Directive on Product Liability, but *services that are* essential for the function of the *product,* such as traffic data for navigation systems. However, only those *services* (and thus also data) are covered that are relevant for the safety of the *product*, including cyber security, recital 15 p. 2 of the Draft Directive on Product Liability - which is particularly important with regard to the demarcation from the interest in equivalence covered by the Digital Content Directive, which, as is well known, does not contain any statements on liability for damages.[87]

According to Recital 15, Sentence 3 of the Draft Directive on Product Liability, it is not even necessary that the *manufacturer* itself provides these *services*; rather, it shall be sufficient that the *manufacturer* merely recommends the use of such *services* or otherwise "influences" their provision by third parties. However, recital 15 p. 3 of the Draft Directive on Product Liability thus deviates from the definition of "control by the *manufacturer*" according to Art. 4 No. 5 of the Draft Directive on Product Liability, which refers to the authorization of the *services of* a third party by the *manufacturer* (including updates or upgrades). A mere recommendation may contain an authorization, but this also raises the question of the point in time to be taken into account, e.g. in the case of a modification of the *services by a* third party: Does the authorization cease to apply, for example, if the *manufacturer* only "recommends" a specific version of a *service?* Or, in the case of a general "recommendation", does it apply to all future versions of the *service* by a third party?

With this extension, the Product-Liability-D-P also covers the area of *training data,* which is so important for AI software[88] , which could already be taken into account under the fault-based producer liability according to section 823 (1) BGB in the context of supplier liability, but for which the manufacturer of the AI system

[87] Gerald Spindler and Karin Sein, "Die Richtlinie über Verträge über digitale Inhalte Aufsatz," *MMR,* (2019): 488 (491); Reiner Schulze, "Die Digitale-Inhalte-Richtlinie – Innovation und Kontinuität im europäischen Vertragsrecht;" *ZEuP,* (2019): 695 (720 f.); Lena Mischau, "Daten als „Gegenleistung" im neuen Verbrauchervertragsrecht," *ZEuP,* (2020): 335 (352).

[88] Spindler, "Neue Haftungsregelungen für autonome Systeme?," *JZ,* (2022): 793 (797); Philipp Hacker, "Ein Rechtsrahmen für KI-Trainingsdaten," *ZGE,* (2020): 239 (250); Zech, (n 82), 502 (505); *id.* Gutachten A zum 73. Deutschen Juristentag, 2020, A 68.

could exculpate himself by providing appropriate proof of due diligence.[89] In practice, such liability will also encounter problems of proof.[90] With the extension to the necessary *services,* the strict liability of the Product-Liability-D-P is now extended to the necessary data sets for an AI system - without the need to comply with Art. 10 AI-Reg-E, which further reduces the scope of application of the AI-Liability-RL-E.

c) Exception for open source software

In order not to hinder innovation and research, according to recital 13, sentences 1 and 2, open source software that is developed or made available outside of commercial "activities" is not to be covered by the concept of product under the Product-Liability-D-P. If, on the other hand, the open source software is made available in return for payment or the disclosure of personal data, the Product-Liability-D-P should apply, unless the data is used exclusively to improve security, compatibility or interoperability, recital 13 p. 3 Product-Liability-D-P. The Product-Liability-D-P thus follows the path already taken in Art. 3 (5) f) of the Digital Content Directive[91] to exempt open source software from regulation.[92]

However, here too the devil is in the detail: Open source software is often combined in distribution with proprietary software in addition to the free offer ("dual licensing"[93]). For example, *Oracle* offers its MySQL database system under the GPL v2 on the one hand and under a commercial license on the other.[94] In addition, open source software is often only offered as part of a bundled service package that

[89] Zech, (n 82), 502 (507); Grützmacher, "Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO," *CR,* (2021): 433 marginal no. 18; Spindler, (n 88), 793 (796 f.); Gerald Spindler «§ 823 BGB», in *BeckOGK,* ed. Beate Gsell et al., (München: C.H. Beck, status July 01, 2022), marginal no. 662.

[90] Zech, (n 82), 502 (507); *ibid.* (n 87) A 58.

[91] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contract law relating to the provision of digital content and digital services, [2019] OJL 136/1.

[92] Dirk Staudenmayer, «Directive (EU) 2019/770», in *EU Digital Law*, ed. Reiner Schulze and Dirk Staudenmayer, 1st edn. (Baden-Baden: Nomos, 2020), Art. 3 Scope Rn. 106 et seq.; Spindler and Sein, (n 87), 415 (418); Mischau, (n 87), 335 (342).

[93] Carsten Gerlach, "Praxisprobleme der Open-Source-Lizenzierung," *CR,* (2006): 649 (651); Till Jaeger and Axel Metzger, «2nd chapter», in *Open Source Software*, 5th edn. (München: C.H. Beck, 2020), marginal no. 144; Astrid Auer-Reinsdorff and Christian R. Kast, «§ 9 Open Source and Open Content», in *Handbuch IT- und Datenschutzrecht,* ed. by Astrid Auer-Reinsdorff and Isabell Conrad, 3rd edn. (München: Beck, 2019), marginal no. 26.

[94] Cf. Q3 "Commercial License for OEMs, ISVs and VARs", July 2010, accessed October 10, 2023, https://www.mysql.com/about/legal/licensing/oem/.

also includes support services or software maintenance.[95] If, for example, an open source software that is in itself freely available is linked to a *product* and at the same time "maintained" for a fee, the question arises for the injured party as to how he should be able to assess the character of the software, since he often lacks the necessary information. Finally, in these cases it is questionable whether it is still *non-commercially* distributed or developed open source software, especially since the Product-Liability-D-P does not focus on the license conditions. This is all the more true if one takes into account that the Product-Liability-D-P also wants to cover linked *services*.

2. Protected legal interests extended to data loss or corruption

The legal interests protected by strict product liability are also extended. First of all, the Draft Directive on Product Liability specifies for the integrity of life and limb in Art. 4 No. 6 a) Draft Directive on Product Liability that medically recognized damage to mental health is also covered.[96] In addition, injuries to the property of consumers are also covered if it is used for both private and commercial purposes, recital 19, p. 2. 2 Product-Liability-D-P; only the exclusively professional use is not covered by the Product-Liability-D-P, Art. 4 No. 6 b) iii).[97]

The most important innovation, however, is the extension of the protected legal interests to include the *loss* or *corruption of data*, unless the data was used exclusively for professional purposes, Art. 4 No. 6 c) Product-Liability-D-P. According to recital 16, sentence 1 of the Draft Directive on Product Liability, the costs of restoring the data are to be included in the damage. It apparently does not matter whether or where the data is stored, so that data in the cloud also falls under the protection of the Product-Liability-D-P. The Product-Liability-D-P would thus put an end to a

[95] Gerald Spindler*, Rechtsfragen der Open Source Software*, (München: Verband der Softwareindustrie Deutschlands e.V., 2003), 84; Jaeger, Metzger, «1st chapter», in *Open Source Software*, 5th edn., (München: Beck, 2020), marginal no. 23; specifically for the Mozilla Public Licence cf. Jaeger and Metzger, (n 93), marginal no. 100.

[96] The understanding of the protected legal interests runs parallel to the understanding known from Gerhard Wagner, «§ 823 (1) BGB», in *MüKo BGB*, ed. Franz Jürgen Säcker, 8th edn. ProdHaftG, (München: C.H. Beck, 2020) § 1 marginal no. 4; Mark Seibel, «§ 1 ProdHaftG», in *BeckOGK*, ed. Beate Gsell et al. October ProdHaftG, (München: Beck, 2020 status October 01, 2022) marginal no. 27; according to this, the concept of injury to health also covers mental illnesses and damages that are medically ascertainable and go beyond the general (life) risk, cf. Gerald Spindler, «§ 823 BGB», in *BeckOGK*, ed. Beate Gsell et al. July 01 (München: C.H. Beck, 2022 status July 01, 2022), marginal no. 108; Gerhard Wagner, «§ 823 (1) BGB», in *MüKo BGB*, ed. Franz Jürgen Säcker, 8th edn. (München: C.H. Beck, 2020), marginal no. 205 et seq.

[97] Not so for the old ProdHaft-RL Wagner, (n 96), § 1 marginal no. 13: decisive whether only private, occasional professional use causes damage; less restrictive Seibel, (n 95), § 1 marginal nos. 49, 54: even a not insignificant professional or commercial use does not harm; Ehring, «§ 1 ProdHaftG», in *Produkthaftungs- und Produktsicherheitsrecht*, ed. by Philipp Ehring and Jürgen Taeger, 1st edn. (Baden-Baden: Nomos, 2022), marginal no. 31: majority intended use in the private sphere sufficient.

long debate[98] also within the framework of section 823 (1) BGB about the quality of data as *other rights in* favour of their recognition; for it would be more than questionable why only consumers should enjoy the benefit of liability for data loss or corruption, while other data "owners" do not, without having to recognize data ownership.
Compensation for damages for the violation of data protection regulations according to Art. 82 of the GDPR[99] or the ePrivacy Directive[100] , on the other hand, shall not be affected by the Product-Liability-D-P, recital 16 p. 3 of the Product-Liability-D-P. 3 Product-Liability-D-P. The concrete calculation of damages is still to be left to the member states, as are claims for *immaterial damages* (section 253 BGB), Recital 18 Product-Liability-D-P. Here, however, it will be very important that a loss of data is not to be equated with pecuniary loss; at least for the area of damages due to loss of profit, their reimbursement will depend on the injured party being able to specifically demonstrate and prove the *liability-filling causality* between the loss of data and the loss of income.

3. Error concept or safety expectations

Another essential adjusting screw in product liability for IT products concerns the concept of error, especially in evolving and learning AI systems, but also with regard to the connection of the IT product or software with its digital environment and with connected other services, up to cybersecurity requirements.

a) Principles

The principles for determining the defectiveness of IT products remain in principle the same as in the previous Product Liability Directive, namely the *general market expectations with* regard to the safety of the *product*, Art. 6(1) Product-Liability-D-P, which is also intended to cover the intended use of the *product,* Recital 22 p. 4. 4 Product-Liability-D-P. In this context, the Draft Directive on Product Liability differentiates according to the risks of the products for the respective legal interests

[98] Spindler, (n 96), § 823 Rn. 137; Wagner, (n 96), § 823 Rn. 332; Simon Adam, "Daten als Rechtsobjekte," *NJW,* (2020): 2063 (2067); Thomas Riehm, "Rechte an Daten – Die Perspektive des Haftungsrechts," *VersR,* (2019): 714 (724); Andreas Wehlau and Klaus Meier, "Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung," *NJW,* (1998): 1585 (1588); always referring to embodiment by data carrier: BGH 14 July 1993 - VIII ZR 147/92 = *CR,* (1993): 681 (682); rejecting Andreas Spickhoff, «Der Schutz von Daten durch das Deliktsrecht», in *Unkörperliche Güter im Zivilrecht,* ed. Stefan Leible, Matthias Lehmannand, Herbert Zech (Tübingen: Mohr Siebeck, 2011), 233 (244).
[99] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.
[100] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37.

concerned, so that very high requirements can be imposed for medical devices, for example, Recital 22 p. 5 Draft Directive on Product Liability. As before, technical standards will therefore play a role in the lack of safety of a *product that should* not be underestimated. The presentation of the *product*, the installation and use instructions and the entertainment also play a major role, Art. 6 (1) a) Draft Directive on Product Liability, as does the reasonably foreseeable misuse of a *product,* Art. 6 (1) b) Draft Directive on Product Liability - here, however, defects that occur later, especially in IT products, will have considerable significance.

It is also important to clarify in Art. 6(2), Recital 25, Sentence 2 of the Draft Directive on Product Liability that newer updates or upgrades do not *per se* lead to the assumption that the previous version was defective, likewise in the case of newer or better later *products*. However, this is not entirely comprehensible, especially for security updates, since if a defect in an IT product is subsequently discovered and "fixed" by such an update, the conclusion that the previous version was defective is obvious; for security updates, therefore, Recital 25, Sentence 2 of the Product Liability Directive-E should not be applied.

Already at this point, the Draft Directive on Product Liability in recital 22 p. 5 hints at a simplification of the burden of proof for the injured party, in that it should be sufficient for courts to no longer have to establish the defectiveness of the specific product if the defectiveness of an entire *product category* is proven, provided that it belongs to the same category. The Product-Liability-D-P thus takes up the principle developed by the ECJ in the *Bosten Scientific Medizintechnik case*[101] and explicitly regulates it. While the ECJ decision still referred specifically to pacemakers and implantable cardioverted defibrillators and was thus issued against the background of the particular health and life risk associated with this *product category*, recital 22 p. 5 of the Product-Liability-D-P now extends the scope of application to all *products* or *product categories*.[102] Nevertheless, also under the Draft Directive on Product Liability, it will be necessary to adhere to the requirement that at least a risk threshold to be determined normatively must be exceeded and that "the mere possibility of a failure of the [...] implanted pacemakers [...] cannot constitute a defect"[103].[104]

However, the fundamental innovations of the Product-Liability-D-P result much more from the additionally listed factors that the courts are to consider when determining faultiness:

[101] ECJ Judgment of 05 May 2015 - C-503/13, C-504/13, ECLI:EU:C:2015: 148, 41 et seq. - *Boston Scientific Medizintechnik GmbH/AOK Sachsen-Anhalt et al = CR,* (2015): 716 (Ls.).
[102] Critical of a generalisation of this case law, Wagner, (n 96), § 3 Rn. 56; *ibid.,* Gerhard Wagner, "Der Fehlerverdacht als Produktfehler," *JZ,* (2016): 292.
[103] This is still the case in the Opinion of Advocate General *Bot* of 21 October 2014 - C-503/13, C-504/13, ECLI:EU:C:2014:2306, 31 - *Boston Scientific GmbH/AOK Sachsen-Anhalt et al.*
[104] In general on this requirement Wagner, (n 96), § 3 marginal no. 56; *ibid.,* (n 102), 292 (296).

b) Self-learning (AI) systems

An important factor for the relevant road safety expectations, especially for AI systems in the field of *machine learning, is* their possible autonomous further development after being placed on the market or put into operation. This effect, which has so far prevented liability for problems occurring after placing on the market that were not foreseeable at that time, at least for legal systems that excluded development errors (such as in Germany), is now taken into account by Art. 6 (1) c) Draft Directive on Product Liability, at least to some extent, in that special safety expectations are to be taken into account here.[105] Accordingly, learning AI systems must also be designed in such a way that they prevent dangerous behaviour of the *product* or AI system; the Draft Directive on Product Liability does not focus on a "reasonable" test, recital 23 p. 2 Draft Directive on Product Liability.

In this context, the further innovation in Art. 6(1)(e) Product-Liability-D-P on the relevant point in time for defectiveness also plays an important role for IT products that are still under the control of the *manufacturer,* which is likely to be the case for numerous connected IT products, especially AI systems; here, the Product-Liability-D-P correctly focuses on the point in time when the *manufacturer* relinquishes control over the IT product or the AI system. Especially when AI systems are continuously monitored with regard to their data sets and their use by the AI system manufacturer, which they may even be obliged to do under the AI Regulation-E ("post market monitoring", Art. 61 AI Regulation-E), they are under the "control of the *manufacturer*", so that the *manufacturer* must continuously ensure the road safety of the IT products or the AI system. Here, too, the Product-Liability-D-P goes beyond the AI Liability-RL-E, which regulates the requirements for data governance (Art. 10 AI-VO-E) only with regard to the burden of presentation and proof with regard to fault-based liability facts.

c) Interaction with other components

Art. 6 (1) d) Draft Directive on Product Liability contains quasi "explosives" for IT products, which, in the context of road safety expectations, requires that the *reasonably to be* expected effects on other *products be* taken into account, especially with regard to interconnected *products* ("inter-connected", recital 23 p. 1 Draft Directive on Product Liability). However, since IT products almost necessarily interact with each other, difficult questions arise here, such as whether the *developer of* an operating system should always take into account the effects of other IT products or software on his own *product.* Since we are dealing here with a multitude of software products that can hardly be surveyed, the criterion of the "*reasonably*" expected effects will be of particular importance. In this respect, it will probably be possible to fall back on the principles developed under the previous legal situation regarding obligations to instruct and observe products: The greater the danger posed by the *product* and its misuse, the more intensive and insistent the instruction and product monitoring

[105] Hofmann, (n 69) 282 (284); Wagner, (n 9) 707 (749); Wagner, (n 96), § 1 Rn. 61.

must be for the buyer - also with regard to such dangers that only arise through the combination of the *product* with other *products* or accessories.[106]

However, with regard to software, it must be pointed out that the standard to be applied to the catalogue of obligations is to be handled *more restrictively* due to the fast pace of development of operating systems and the abundance of combination possibilities with other software and hardware.[107] Consequently, liability for accessories can only be considered if the *manufacturer* himself provides interfaces for other programs or if the programs are in general use and the *manufacturer* must expect them from the outset.[108]

d) Cybersecurity and product safety

Last but not least, Art. 6 (1) f), Recital 24 of the Product-Liability-D-P closes a gap with regard to cyber security for *products,* which, however, only refers to requirements under product security law and has so far only been implemented in rudimentary form throughout the EU; in particular, the Cybersecurity Act[109] does not contain any mandatory schemes for *manufacturers of* IT products, but only their voluntary compliance. With regard to AI systems, however, Art. 15 of the AI-Reg-E explicitly requires "robustness, integrity and cybersecurity", so that the relevant security expectations of traffic in the sense of the Product-Liability-D-P are also defined in this regard. The new proposal for a Cyber Resilience Act (CRA-E), which explicitly provides for security requirements for *products, will also* bring significant improvements here, which are obviously already interlinked with the Product-Liability-D-P and even more so with the KI-VO-E.

e) Development errors

Somewhat hidden in Art. 10 (1) (e), the Draft Directive on Product Liability still excludes the so-called design defect from the liability of the *manufacturer*; according to this, the *manufacturer* can invoke the fact that, according to the objective state of

---

[106] BGH 16 June 2009 - VI ZR 107/08 marginal no. 24 = BGHZ 181, 253; BGH 24 January 1989 - VI ZR 112/88 = BGHZ 106, 273; BGH 16 December 2008 - VI ZR 170/07 = BGHZ 179, 157; Spindler, (n 96), § 823 marginal no. 654; Thomas M. J. Möllers, "Nationale Produzentenhaftung oder Europäische Produkthaftung? Zur Bindung der Rechtsprechung im Rahmen der deliktsrechtlichen Generalklausel an die Vorgaben des ProdHaftG und des ProdSG," *VersR,* (2000): 1177 (1181).

[107] Johannes Droste, "Produktbeobachtungspflichten der Automobilhersteller bei Software in Zeiten vernetzten Fahrens," *CCZ,* (2015): 105 (107); similarly BGH 09 December 1986 - VI ZR 65/86 = BGHZ 99, 167.

[108] Gerald Spindler, *Responsibilities of IT manufacturers, users and intermediaries*, study commissioned by the BSI, (Baden-Baden: Nomos, 2007), 62 with further references.

[109] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Cyber Security Agency) and on cyber security certification of information and communication technology and repealing Regulation (EU) No 526/2013 (Cyber Security Legislative Act), [2019] OJ L 151/15.

science and technology, a product defect was not recognizable at the time of placing the *product* on the market or at the time when the product was under the control of the *manufacturer*. *In* contrast to the previous Product Liability Directive, which also provided for the design defect exception as an option for the Member States[110] , this exception is now *mandatory in* nature and must therefore be implemented by all Member States. The *state of the art in science and technology*[111] will therefore be decisive, although this does not necessarily run parallel to the German understanding. This is not to be underestimated for AI systems that learn themselves, as their further development after market launch can lead to the acceptance of development errors.[112] However, AI systems in particular will usually remain under the control of the manufacturers long after their market launch, so that the exception will not apply here.

f) Updates and upgrades, machine learning

A distinction must be made between the development defect, in which the defect was already present when the *product was* placed on the market but could not be discovered, and the case where the defect in the product only occurred subsequently, i.e. after the product was placed on the market. In principle, Art. 10(1)(c) Draft Directive on Product Liability also provides for an exemption from liability of all parties involved, which is, however, considerably - and rightly - relativised by Art. 10(2) Draft Directive on Product Liability: According to this, the exemption from liability does not apply if, during the *manufacturer*'s control over the *product*, the defectiveness is caused by a *connected service*, by software including updates or upgrades or by their absence, provided that the safety of the *product is at* issue. Recital 37 S. 3 Product-Liability-D-P also includes machine learning, as long as the AI product or system is under the control of the *manufacturer*.

---

110 Cf. The implementation of Art. 7 lit. e ProdHaft-RL in § 1 para. 2 no. 5 ProdHaftG, without making use of the opening clause in Art. 15 para. 1 lit. b ProdHaft-RL; on the German implementation see Wagner, (n 96), § 1 Rn. 51; Ehring, (n 97), § 1 Rn. 97; Christian Förster, «§ 1 ProdHaftG », in *BeckOK BGB*, ed. Wolfgang Hau et al. 63rd ed. (München, C.H. Beck, 2022), Rn. 53 ff.

111 Cf. On the relevant differentiation in German law in particular BVerfG decision of August 08, 1978 - 2 BvL 8/77 = BVerfGE 49, 89 = *NJW,* (1979): 359 (362) - Kalkar; BGH of 5 February 2013 - VI ZR 1/12 marginal no. 13 = *NJW,* (2013): 1302; BGH of June 16, 2009 - VI ZR 107/08 Rn. 15 = BGHZ 181, 253 with further references; Spindler, (n 96), § 823 Rn. 633; Wagner, (n 96), § 823 Rn. 953, Thomas Klindt and Boris Handorn, "Haftung eines Herstellers für Konstruktions- und Instruktionsfehler," *NJW,* (2010): 1105; Peter Marburger, *Die Regeln der Technik im Recht*, (Köln: Heymann, 1979), 429.

112 Friedrich Graf Von Westphalen, "Haftungsfragen beim Einsatz Künstlicher Intelligenz in Ergänzung der Produkthaftungs-RL 85/374/EWG," *ZIP,* (2019): 889 (892); but much narrower Malte Grützmacher, "Die deliktische Haftung für autonome Systeme – Industrie 4.0 als Herausforderung für das bestehende Recht?," *CR,* (2016): 695 (696); see also Herbert Zech, "Künstliche Intelligenz und Haftungsfragen," *ZfPW,* (2019): 198 (213); *id.,* (n 87) A 71.

Implicitly, the Product-Liability-D-P thus introduces a non-contractual duty for updates for security, as otherwise the IT product must be considered defective. However, much depends on whether the IT product is still under the control of the *manufacturer* - because only then does the re-exception apply. This means that a *manufacturer is still* free not to opt for permanent support or updates. On the other hand, ErwGr 38 S. 3 Product-Liability-D-P explicitly refers to the Medical Devices Regulation, here Annex I Chapter I No. 3 (EU) 2017/745[113] and requires *manufacturers to* provide security updates, especially with regard to cybersecurity risks - however, the Medical Devices Regulation is not particularly clear in this respect, as it only requires reliability of the electronic components including software, which can also include security updates.[114] In contrast, the proposal for a Cyber Resilience Act apparently assumes an obligation under product safety law for lifelong updates, Annex I No. 1 k) in conjunction with Art. 5 of the proposal, which is, however, considerably relativised by the limitation to a five-year obligation to verify compliance with the requirements by the *manufacturers, Art.* 10 Para. 6, 12, Art. 23 Para. 2 CRA E.[115]

In contrast, Section 327f of the BGB provides for traders' update obligations in implementation of Art. 8(2) of the Digital Content Directive[116] . This obligation can then exist independently of the obligation under the Product-Liability-D-P. This may well result in overlaps, as the Product-Liability-D-P also covers dealers in any case, provided the actual manufacturer is not "tangible". On the other hand, unlike under the Product-Liability-D-P, the contractual obligation of the trader applies regardless of whether the trader himself still has control over the product.

Recital 38 p. 4 Product-Liability-D-P, however, establishes the – self-evident – principle that liability must be excluded if the IT product user or owner does not install the update. However, how to deal with cases in which the user is not aware of updates that have been made available remains open, as does how the *manufacturer should be* able to prove this. This, too, would tend to argue in favour of limiting liability for updates to cases in which the *manufacturer* still exercises control over the IT product.

4. Liability addressees

The Product-Liability-D-P also contains some interesting innovations with regard to the addressees of liability: In addition to the traditional concept of manufacturer

---

[113] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 concerning medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, [2017] OJ L 117/1.

[114] Gerhard Wiebe, "Produktsicherheitsrechtliche Pflicht zur Bereitstellung sicherheitsrelevanter Software-Updates," *NJW,* (2019): 625 (626).

[115] See also Yannick Zirnstein, "Der Entwurf des Cyber Resilience Act," *CR,* (2022): 707.

[116] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contract law relating to the provision of digital content and digital services, [2019] OJ L 136/1.

and the liability of *importers,* the Product-Liability-D-P now expressly extends liability to so-called "*fulfilment providers*", i.e. *services that* serve to provide logistical support for a product import (without being *importers* themselves), up to the possible liability of online platforms.

a) Manufacturers, especially software developers

First of all, Art. 7(1) of the Draft Product Liability Directive refers to the *manufacturer* as the traditional addressee of liability, which is defined in more detail in Art. 4 No. 11 of the Draft Product Liability Directive. In this respect, the Product-Liability-D-P does not contain any surprises, since just as in the still valid ProdHaft-RL, developers are also covered, as are those who distribute third-party products under their own name or trademark ("quasi-manufacturers").[117]

b) Suppliers, in particular service providers

Even if at first glance nothing changes with regard to the joint and several liability of *manufacturers* and *suppliers*, Art. 7(1) sentence 2 of the Draft Directive on Product Liability, it should not be overlooked that the extension of the *concept of product* and *component* (Recital 26 of the Draft Directive on Product Liability), e.g. to *connected IT services*[118] , entails a considerable expansion of the addressees of liability. In relation to AI systems, data suppliers, for example, can easily fall under the *definition of supplier* and thus under strict no-fault liability, but also other connected services.

c) Extension of the concept of importers to fulfilment providers

Also significant is the (subsidiary) extension of the importer's liability also contained in the ProdHaft Directive-E (Art. 7(2)) to so-called "*fulfilment providers*", who take over the logistical handling of the import of a product if neither the *manufacturer* nor the *importer is* domiciled in the EU, Art. 7(3) ProdHaft Directive-E. Article 4(14) of the Draft Directive defines this term in more detail as *commercial services that* fulfil at least two of the criteria "warehousing, packaging, addressing and dispatching of a product", excluding any freight and postal services.

For example, these criteria could apply to *Amazon Marketplace if Amazon* stores third-party products and then delivers them to the end customer if the actual retailer is not located in the EU. On the one hand, the previous Product Liability Directive did not even know the term "*fulfilment provider*" and, on the other hand, the importer activity had to take place "for the purpose of sale, hire, hire-purchase or other form of distribution with an economic purpose" according to Art. 4(2) of the Product

[117] Cf. Art. 3 para. 1 ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC, § 4 para. 1 p. 2 ProdHaftG; on this Wagner, (n 96), § 4 marginal no. 33; Andreas Spickhoff, «§ 4 ProdHaftG», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status May 01, 2021), marginal no. 26 ff.
[118] See above B. II. 1. b).

Liability Directive. Thus, the decisive factor was the control of the import and not merely its implementation.[119] With the new regulation, the *EU Commission rightly* wants to close a gap that has arisen precisely due to such business practices in which a classic *importer* cannot be found in the EU, but these service providers take over parts of their tasks without themselves being able to be qualified as *importers*. The *EU Commission uses the* parallel approach in the Market Surveillance Regulation[120] , which in its Art. 4-7 also places the "fulfilment service providers" within the meaning of Art. 3 No. 11 of Regulation (EU) 2019/1020 under the obligation. However, recital 27 of the Product-Liability-D-P only wants to make these "fulfilment service providers" liable if they cannot name a *manufacturer* or *importer* in the EU.

d) Online platforms

Art. 7(6), Recital 28 of the Draft Directive on Product Liability goes even further, which also makes online platforms that facilitate distance contracts liable, albeit in accordance with Art. 6(3) of the Digital Services Act. Accordingly, the decisive factor – in the wake of the ECJ's *Wathelet ruling*[121] – is whether the consumer perceives the platform as the actual provider or whether the *trader* or *manufacturer* is under the supervision of the platform.[122] This provision is also in line with the proposal for a general product safety regulation,[123] which provides in Art. 20(5)(a) that online marketplaces must provide "*the name, registered trade name or registered trade mark of the producer and a postal or e-mail address at which he can be contacted*". Recital 36 Product-Liability-D-P further clarifies that online marketplaces should ensure that, for product traceability purposes, traders comply with their information obligations under the DSA and the Product Safety Regulation-E and do not allow (product) listings by

[119] OGH January 26, 1995 - 6 Ob 636/94 = *JBl.*, (1995): 456 (457); Wagner, (n 96), § 4 Rn. 45; Georg Borges, «§ 4 ProdHaftG», in *BeckOK IT-Recht*, ed. Georg Borges and Marc Hilber, 7th edn. (München: C.H. Beck, 01.10.2021), Rn. 47; Friedrich Graf von Westphalen, "Das neue Produkthaftungsgesetz," *NJW,* (1990): 83 (89).

[120] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and the conformity of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, [2019] OJ L 169/1.

[121] Ec; Rupprecht Podszun and Philipp Offergeld, "Plattformregulierung im Zivilrecht zwischen Wissenschaft und Gesetzgebung: Die ELI Model Rules on Online Platforms," *ZEuP,* (2022): 244 (258).

[122] For more details see Gerald Spindler, "Der Vorschlag für ein neues Haftungsregime für Internet-Provider – der EU Digital Services Act (Teil 1)," *GRUR,* (2021): 545 (549); Busch, *EuCML,* (2021): 109 (111, 114); Rössel, *ITRB,* (2021): 35 (36); Gerald Spindler and Simon Gerdemann, "Das Gesetz über digitale Dienste (Digital Services Act) - Teil 1," *GRUR,* (2023): 3, "Das Gesetz über digitale Dienste (Digital Services Act) (Teil 2)," *GRUR,* (2023): 115.

[123] Commission, "Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council", COM (2021) 346 final June 30, 2021.

traders who do not comply with the relevant information obligations. *"However, the online marketplace should not be responsible for checking the completeness, correctness or accuracy of the information itself, as the obligation to trace the products still lies with the trader"* (recital 36 p. 5 General Product Safety Regulation-E). Liability under the Product Liability Directive remains expressly unaffected under Article 39 (2) of the Draft General Product Safety Regulation.

However, the reference to Art. 7(5) of the Draft Directive on Product Liability also requires that the injured party has unsuccessfully requested the platform operator to disclose the identity of the *manufacturer/importer,* etc. within a period of one month. On the other hand, ErwGr 28 S. 2 Product-Liability-D-P states that the liability privileges of the Digital Service Act remain applicable if they only assume an intermediary role. There are no special features for AI systems in this respect.

e) No exception for SMEs

The EU Commission explicitly excluded an exemption for SMEs in its proposal - with the correct reason that it is irrelevant for an injured party whether the damage was suffered by a larger or a small company.[124] In fact, in terms of the internalisation of external effects (i.e. damages), it does not matter what size the damaging party is.

f) Modification of products, especially recycled products

Article 7 (4) of the Draft Directive on Product Liability, which states (or clarifies)[125] that *modifications to* a *product* already placed on the market or outside the control of the *manufacturer* that have an impact on product safety must also be considered a new *product, is* aimed at a problem that at first glance seems to be outside the IT sector. In view of *modifications of* IT products or services or components in particular, which ErwGr 29 S. 2 Product-Liability-D-P states for upgrades in particular, this innovation is certainly applicable in the IT sector - even if the open source sector is explicitly excluded. Art. 10 para. 1 g), Recital 29 p. 4 of the Draft Directive on Product Liability limits the liability of the person who has modified the *product to the* corresponding modified part of the *product.*

For the liability of AI systems, this extension can be significant if the *manufacturer* itself does not control the AI system, but a third party trains or "educates" the AI system with new data sets. However, how to separate the changed from the unchanged parts of the systems seems hardly feasible in practice.

---

[124] EU Commission, "Explanatory Memorandum to the Product-Liability-D-P", COM (2022) 495 final, 10 ff.

[125] For a similar discussion under the ProdHaft-RL, Irina Rebin, «§ 2 ProdHaftG», in *BeckOGK*, ed. Beate Gsell, et al. (München: C.H. Beck, 2022 status September 01, 2022), Rn. 11: depending on individual circumstances.

5. Liability exceptions

The liability exceptions are also partly taken over from the previous ProdHaft Directive[126] , but partly modified considerably, especially with regard to the extension of the concept of product to include connected services and software.

The principle that a *manufacturer* or *importer* cannot be held liable if he proves that he did not himself place the *product on the* market remains unaffected, Art. 10(1)(a) Product-Liability-D-P.[127] The same applies to *distributors*, Art. 10(1)(b) Product-Liability-D-P. The exemption from liability in the event that the defectiveness of the *product* results from mandatory provisions of public law is also continued, Art. 10(1)(d) Product-Liability-D-P.[128]

Also known is the liability exception for *suppliers* (or "*components*") in Art. 10 (1) f) Product-Liability-D-P, if the defectiveness of the *component* results from the design of the main product or the instructions of its manufacturer.[129]

As already mentioned, the Product-Liability-D-P still provides for the exception for development defects – but now of a mandatory nature for the Member States and not as an option. The liability exceptions for updates and upgrades have also been modified (see II.3.a) above).

New, on the other hand - but in principle self-evident - is Art. 10 (1) g) Product-Liability-D-P, which limits the liability of the "new" manufacturer for *modifications of* a *product to* the modified parts.

6. Disclosure obligations and burden of presentation and proof

One of the other important adjusting screws in product liability concerns the distribution of the burden of presentation and proof, which, with regard to defectiveness

[126] Cf. The predecessor regulation in Art. 7 ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC.

[127] Cf. The predecessor regulation in Art. 7 lit. a ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC.

[128] Cf. The previous provision in Art. 7 lit. d ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC.

[129] Cf. The predecessor provision in Art. 7 lit. f ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC; on the implementation in § 1 para. 3 p. 1 ProdHaftG see Maximilian Seibl, «§ 1 ProdHaftG», in *BeckOGK*,ed. Beate Gsell et al. (München: C.H. Beck, status October 01, 2022), marginal no. 129; Wagner, (n 96), § 1 marginal no. 63. ff.

and causality, has so far been borne by the injured party in full,[130] which is a considerable obstacle for injured parties, especially for IT products and even more so for AI systems.[131]

In itself, Art. 9(1) Product-Liability-D-P adheres to the principle that the injured party must prove both the defectiveness, the infringement of the legal interest and the damage as well as the causality. However, the *EU Commission* recognises the practical problems just described of an injured party who has hardly any access to information that would allow him to prove the defectiveness of an (IT) product, as well as the causality between the defect of the *product* and the infringement of the legal interest, recital 30 p. 2, 3 Product-Liability-D-P. 2, 3 Product-Liability-D-P ("*information asymmetry*"). The *EU Commission* addresses this problem with two solutions:

a) on the one hand, an easing of the burden of proof by introducing an obligation to disclose information of the potential tortfeasor, Art. 8 Product-Liability-D-P;

b) on the other hand, through presumptions of evidence and prima facie evidence orders in Art. 9 Product-Liability-D-P.

a) Disclosure obligations

Article 8 (1) of the Draft Directive on Product Liability obliges the Member States to allow the courts to oblige a potential tortfeasor or defendant to disclose relevant facts at the request of the plaintiff, who can plausibly demonstrate that he is entitled to compensation. This is similar in approach to the US *pre-trial disclosure procedure*, but depends crucially on a pending lawsuit. The documents to be submitted do not only include the evidence already held by the defendant, but may also include new documents or reports to be created, ErwGr 31 S. 2 Product-Liability-D-P.

---

130 Art. 4, 7 ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC; on the implementation of § 1 para. 4 ProdHaftG Seibl (n 128) § 1 marginal no. 141; Wagner, (n 96), § 1 Rn. 77; Borges, (n 119), § 1 ProdHaftG Rn. 93; the injured party bears the burden of proof for the existence of the product defect, the damage, the causal connection, cf. BGH February 05, 2013 - VI ZR 1/12 marginal no. 19 = *NJW,* (2013): 1302; OLG Brandenburg, December 14, 2015 - 1 U 8/13 = *NJW-RR,* (2016): 220 (221); OLG Frankfurt a. M. June 08, 1993 - 14 U 116/92 = *NJW-RR,* (1994): 800 (801); the manufacturer bears the burden of proof for the existence of an exclusion according to § 1 para. 2, 3 ProdHaftG.

131 Gerald Spindler, "Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären", Studie im Auftrag des BSI, [*Responsibilities of IT manufacturers, users and intermediaries*, study commissioned by the BSI] 2007, 76, accessed October 1, 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2; Gerald Spindler «Haftung im IT-Bereich»*in Karlsruher Forum 2010: Haftung und Versicherung im IT-Bereich,* ed. by Egon Lorenz (Karlsruhe: Verlag Versicherungswirtschaft, 2011), 39 ff.

In order not to let the submission of facts etc. get out of hand - as is known from *pre-trial disclosure proceedings*[132] - Art. 8 (2) Product-Liability-D-P explicitly limits this duty to the *necessary* and *proportionate* facts *to* substantiate the claim.[133] In this context, Art. 8(3), (4) Product-Liability-D-P pays special attention to the observance of trade secrets and the protection of confidential information, which, however, according to Art. 8(4) Product-Liability-D-P should not be an insurmountable obstacle, as the member states are also obliged to authorise their courts to take "specific measures" to protect confidentiality if the defendant is obliged to disclose the confidential information. This is already known in Germany, for example, in patent proceedings through the "in camera" procedure, in which a third party bound to professional secrecy can inspect the documents.[134] However, recital 32 p. 2 Product-Liability-D-P goes even further, in that the *EU Commission* apparently considers a restriction of access to the secret documents to a certain group of persons to be sufficient, or in that only redacted minutes of evidentiary hearings or hearings are admitted. In any case, recital 32 p. 3 Product-Liability-D-P requires a comprehensive weighing of the interests of the plaintiff and the defendant, in particular the effects on the action as well as potential damages for the defendant or third parties affected. In contrast, a much more extensive approach is taken in US civil procedure law. In addition to third parties not involved in the proceedings who can be called upon in *pre-trial disclosure proceedings*[135] , the documents and information to be provided by the parties are subject to hardly any restrictions[136] and certainly hardly any

[132] Haimo Schack, *Einführung in das US-amerikanische Zivilprozessrecht*, 5th edn. (München: C.H.Beck 2020), 111; Hanns Prütting, *AnwBl,* (2008): 153 (154).

[133] Peter Gottwald, «Internationales Beweisrecht § 10», in *Internationales Zivilprozessrecht*, ed. Heinrich Nagel, Peter Gottwald, 8th edn. (Köln: Verlag Dr. Otto Schmidt, 2020), Rn. 10.24*;* Schack, (n 132), 48*,* DerekJ.T.Adler, «Is Discovery Necessary? Reflections on Pre-Trial Disclosure and Procedural Fairness», in *Global Wisdom on Business Transactions, International Law and Dispute Resolution, Festschrift for Gerhard Wegen* (München: C.H. Beck, 2015), 569.

[134] BGH November 16, 2009 - X ZB 37/08 = BGHZ 183, 153; see Peter Meier-Beck, "Die Rechtsprechung des Bundesgerichtshofs zum Patent- und Gebrauchsmusterrecht im Jahr 2009," *GRUR,* (2010): 1041 (1046); *ZPO*, Astrid Stadler, «§ 142», in *ZPO*, ed. by Hans-Joachim Musielak and Wolfgang Voit, 19th edn. (München: Verlag Franz Vahlen, 2022) marginal no. 7a.; Hermann Deichfuß, "Rechtsdurchsetzung unter Wahrung der Vertraulichkeit von Geschäftsgeheimnissen," *GRUR,* (2015): 436.

[135] Joachim Zekoll and Jan Bolt, *NJW,* (2002): 3129 (3133); Schack, (n 132), 111.

[136] See FRCP 26 (b) (1): "Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defence of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter".

security precautions,[137] in order to protect trade secrets, for example.[138] Criticism: As laudable as the European approach is, it tends to be too broad due to the relatively low hurdles for the protection of trade secrets; as described, an exclusive entrustment of third parties bound to secrecy would be preferable. The potential scope of Art. 8 Product-Liability-D-P also appears to be insufficiently contoured, as it does provide for the barrier of necessity and proportionality, which in practice, however, will lead to considerable legal uncertainty and will ultimately only emerge through ECJ case law, as injured parties are likely to initially make corresponding requests "out of the blue" in order to obtain corresponding information. Much depends on the requirements for a corresponding application by the plaintiff and its substantiation, e.g. whether blanket requests for surrender are sufficient or whether the application must be limited to the disclosure of the source code or the data sets. Nor has it been clarified how *ex post* disproportionate disclosure of documents could be sanctioned, in particular whether plaintiffs would have to pay damages. Nevertheless, liability is hardly conceivable in the admissible exercise of legal remedies. In the cases decided on liability for intentional immoral damage (section 826 BGB), the focus was therefore always rightly on the abuse of a formal or procedural position.[139] Particularly reprehensible circumstances must therefore be added[140].[141] Especially for producer liability for AI systems, but also for other IT products, this innovation has considerable weight, as plaintiffs may in principle demand access to the source code, as well as the surrender of training and validation data or related

[137] The courts have the instrument of protective orders at their disposal here, but they are rarely used in practice, cf. John K. Setear, "Discovery Abuse Under the Federal Rules: Causes and Cures," *92 Yale L. J.*, (1982): 352 (374).

[138] Schack, (n 132), 111.

[139] BGH July 03, 1990 - XI ZR 302/89 = BGHZ 112, 54 (57); BGH March 05, 1958 - IV ZR 307/57 = BGHZ 26, 391 (396); BSG September 26, 1986 - 2 RU 45/85 = *NJW,* (1987): 2038 (2039); regarding an arbitral award OLG Köln August 07, 2015 - 1 U 76/14 = *SchiedsVZ,* (2015): 295 (297); LAG Schleswig-Holstein August 19, 2015 - 3 Sa 90/15 = *BeckRS,* (2015): 73268 marginal no. 28; concerning the creation of a title through the dunning procedure BGH June 29, 2005 - VIII ZR 299/04 = *NJW,* (2005): 2991; BGH November 11, 2003 - VI ZR 371/02 = *NJW,* (2004): 446 (447) following BGH March 25, 2003 - VI ZR 175/02 = BGHZ 154, 269 (274).

[140] Since RG October 07, 1940 - IV 201/40 = RGZ 165, 26 (28) the RG speaks of "special circumstances", cf. on this and on the development of this term in the jurisprudence Ulrich Foerste, «Die Ausnutzung unrichtiger Urteile als sittenwidrige Schädigung», in *Gründen und Stiften : Festschrift zum 70. Geburtstag des Jenaer Gründungsdekans und Stiftungsrechtlers Olaf Werner,* ed. Ingo Saenger et al. (Baden-Baden: Nomos, 2009): 426 (427).

[141] BGH June 29, 2005 - VIII ZR 299/04 = *NJW,* (2005): 2991 (2993 f.); BGH, September 24, 1987 - III ZR 187/86 = BGHZ 101, 380 (384); OLG Köln August 07, 2015 - 1 U 76/14OLG = *SchiedsVZ,* (2015): 295 (297); OLG Hamm August 11, 2015 - 28 U 136/14 Rn. 63 = *NJOZ,* (2016): 58; KG-November 05, 2012 - 26 U 97/11 Rn. 32 et seq.; preceding LG Berlin May 06, 2011 -22 O 122/09; Musielak, «§ 322», in *ZPO*, ed. Musielak, Voit, 19th edn. (München: Verlag Franz Vahlen, 2022), Rn. 91 mwN; Gottwald, «§ 322», in *MüKo ZPO*, 6th edn. (Baden-Baden: Nomos, 2020): Rn. 223 et seq, 228; Foerste (n. 139): 426 (428) with further references.

algorithms and documentation on the behaviour of the AI systems during training, but also later after market launch.

b) Facilitation of evidence, in particular rebuttable presumptions

Defects: The Draft Directive on Product Liability also provides for significant simplifications of proof, such as the rebuttable presumption (Art. 9(5)) of the defectiveness of the *product if* the defendant does not submit any documents in contravention of an order under Art. 8(1) Draft Directive on Product Liability, Art. 9(2)(a) Draft Directive on Product Liability. Furthermore, rebuttable presumptions of the defectiveness of the *product* shall apply if the plaintiff proves that the *product* does not comply with product safety regulations intended to protect against the damage that has occurred, Art. 9 (2) b) Draft Directive on Product Liability. This includes, for example, the lack of documentation or recording devices - for AI systems, for example, set out in Art. 11, 12 AI-Reg-E - so that the violation of these obligations leads to a presumption of defectiveness. The same should apply if the plaintiff can prove an "obvious malfunction" of the *product* during normal use, Art. 9(2)(c) DRP-E, for which Recital 33 p. 7 DRP-E mentions the case of the exploding glass bottle. This corresponds *largely* to the obligation under German law to secure findings and the reversal of the burden of proof that then applies, but only in the case of fault-based producer liability.[142]

A rebuttable presumption shall also apply to the causality between the defectiveness of the *product* and the damage that has occurred, if the defectiveness has been proven beforehand and it is a typical course of events, Art. 9 (3) Draft Directive on Product Liability. However, it is apparently not sufficient for a presumption of fault pursuant to Art. 9(2) of the Draft Directive on Product Liability to apply, as Art. 9(3) expressly speaks of proof.

This is also supported by the additional presumption rules in Art. 9(4) of the Draft Directive on Product Liability: Accordingly, a court may determine that the plaintiff or injured party is facing considerable difficulties ("excessive difficulties") with regard to proving defectiveness or causality due to *technical* or *scientific complexity*. In this case, the presumption of defectiveness as well as causality will apply if the plaintiff has shown ("sufficiently relevant evidence") that the product contributed to the damage and that it was probably defective and probably caused the damage. However, Art. 9(4) of the Draft Product Liability Directive does not contain any statement on the requirements for establishing *technical* or *scientific complexity*, in particular whether the plaintiff has the burden of proof in this respect; only Art. 9(4) sentence 2 of the Draft Product Liability Directive gives the defendant the possibility to dispute the plaintiff's excessive difficulties or the probability of the defectiveness of the *product* and *causality*. What consequence this denial triggers and how this relates to the general rebuttability of the presumption in Art. 9(5) of the Draft Directive on Product Liability remains open.

[142] BGH May 09, 1995 - VI ZR 158/94 = *BGHZ,* (1995): 129, 353 (361).

Recital 34 S. 4 Product-Liability-D-P requires a case-by-case determination of the *technical complexity*, whereby recital 34 p. 5 lists individual factors, in particular the complexity of the *product, e.g. in the case* of innovative medical devices, but also of the machine learning or data that would have to be analysed by the plaintiff. The same applies to causality, for example for a pharmaceutical product and the plaintiff's state of health or if the plaintiff would have to explain the inner workings of an AI system.

In a similar way, recital 34 p. 6 Product-Liability-D-P attempts to clarify the definition of "excessive difficulties" for the plaintiff. Accordingly, within the framework of the court's consideration of the individual case, the plaintiff is not obliged to provide evidence of the existence of these difficulties; it should be sufficient for the plaintiff to provide reasons for this. In particular, recital 34 p. 7 Product-Liability-D-P mentions the case of an AI system for which the plaintiff shall not be obliged to explain its characteristics or its mode of operation or causality for the damage that occurred.

In this context, the relationship between Art. 9(4) of the Draft Directive on Product Liability and the order for the defendant to disclose relevant information under Art. 8 of the Draft Directive on Product Liability remains largely unclear. Recital 34 S. 1 of the Draft Directive on Product Liability only states that the presumptions or the determination of *complexity* by the courts should be without prejudice to the order under Art. 8 of the Draft Directive on Product Liability. However, it remains unclear why a plaintiff should have "excessive difficulties" in proving defectiveness if at the same time he has the possibility to apply for orders under Art. 8 of the Draft Directive on Product Liability; in the sense of *proportionality,* a step-by-step relationship should be assumed here.

As explained, these are rebuttable presumptions (Art. 9 (5) of the Draft Directive on Product Liability), for which the *EU Commission* refers in recital 36 of the Draft Directive on Product Liability to the fact that the defendant can present and prove extraordinary circumstances that exclude liability, for example that the *product* was placed on the market contrary to the *manufacturer*'s intention or that the defect occurred due to compliance with mandatory provisions. However, it should not be sufficient to assume, similar to the principles of *prima facie evidence, that the* rebuttal of the presumption is already based on the invalidation of a principle of experience[143]; neither do the recitals of the Draft Product Liability Directive speak in favour of

[143] BGH December 11, 2018 - KZR 26/17 marginal no. 50 = *WRP,* (2019): 474; BGH January 19, 2010 - VI ZR 33/09 marginal no. 11; BGH May 04, 2012 - V ZR 71/11 marginal no. 13; Hanns Prütting, «ZPO § 286 ZPO», in *MüKo ZPO,* ed. Thomas Rauscher and Wolfgang Krüger 6th edn. (München: C.H. Beck, 2020), Rn. 67; Robert Nober, «§ 286 ZPO», in *ZPO*, ed. Monika Anders and Burkhard Gehle, 80th edn. (München: C.H. Beck 2020), Rn. 86; Ulrich Foerste, «ZPO § 286 ZPO», in *ZPO*, ed. Hans-Joachim Musielak and Wolfgang Voit 19th edn. (München: Verlag Franz Vahlen, 2022), Rn. 23.

this, nor is there any indication in Art. 9 Draft Product Liability Directive that the *EU Commission* "only" wanted to rely on *prima facie evidence* here.

7. Joint and several liability

Art. 11 Product-Liability-D-P maintains the old principle already according to the ProdHaft-RL (Art. 5)[144] that in the case of several possible liability addressees, they are jointly and severally liable for the entire damage. More important in the context of liability for IT products and AI systems, on the other hand, is Article 12 (1) of the Draft Directive on Product Liability, which does not waive the liability of *manufacturers* and others because a third party also contributed to the damage; this also covers cases of a faulty AI system that was also poorly trained by its *operator* (who is not covered by the Draft Directive on Product Liability). However, hacker attacks also do not exonerate the *manufacturer of* a defective IT product, which only made the attack possible through the security gap.

8. No more limitation to maximum liability amounts

Also more than remarkable is the waiver of any maximum liability amount in Art. 13 of the Product-Liability-D-P, neither of a contractual nature[145] nor through member state regulations - in contrast to Art. 16 para. 1 ProdHaft-RL, which still provided for the possibility of limiting liability to 70 million ECU or 85 million Euro (section 10 para. 1 ProdHaftG) at the intervention of Germany, but which has not yet been put into practice.[146] This principle of unlimited liability regardless of fault is hardly found in other strict liability regulations and is all the more astonishing since the question of insurability is also at issue; likewise against the background that pure *data loss* or the *corruption of data is* now also to be recognized as a legal asset.

9. Limitation

Art. 14 Product-Liability-D-P also provides for a limitation regime that is largely similar to sections 195 ff, in particular section 199 BGB. According to this, claims become time-barred within 3 years after the *injured party has become aware of* the damage, the defectiveness and the identity of the possible tortfeasors. Art. 14 Product-Liability-D-P equates this with the *"reasonably" expected knowledge of the injured party, which in* this respect deviates from the standard of section 199 para. 1 no. 2 BGB, which refers to grossly negligent ignorance of the injured party; apparently the *EU Commission* uses an objective standard here, which moreover already intervenes with

144 Wagner, (n 96), § 5 Rn. 1; Georg Schäfer, «§ 5 ProdHaftG», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status October 01, 2022), Rn. 1; Langen, «§ 5 ProdHaftG», in *BGB-Schuldrecht,* ed. Barbara Dauner-Lieb and Werner Langen, (Baden-Baden: Nomos Verlag 2021), Rn. 2.

145 In this context, the contractual limitations of liability of open source products are not covered by the Product-Liabiltiy-D-P because of the general exception.

146 Report of the Commission, COM (2000) 893, January 31, 2001, 21; Spickhoff (n 116) § 10 Rn. 3; Wagner, (n 96), § 10 Rn. 1.

lower requirements for knowledge than section 199 para. 1 no. 2 BGB. In this context, the possibility to order the disclosure of information according to Art. 8 of the Draft Directive on Product Liability may also have an influence on the *"reasonably" expected knowledge of* the injured party. However, according to Art. 14 (1) sentence 2, the Draft Directive on Product Liability does not affect provisions of the Member States on the interruption of the limitation period.

In addition, Art. 14 (2) Product-Liability-D-P prescribes an *absolute* statute of limitations of 10 years after the *product has been* put on the market or has been *substantially modified*. Strangely enough, Art. 14(2) Product-Liability-D-P does not additionally refer to the *manufacturer*'s relinquishment of control over the *product*; this would result in sensitive liability gaps in the case of updates, since the actual IT product was placed on the market long before the update, and damage caused by the *product would become* statute-barred within 10 years after this point in time, despite updates having been made. Here, much depends on whether the *product* is to be considered substantially *modified by* the updates, so that the limitation period starts anew.

This *absolute* limitation period is extended to 15 years in cases where the injured party was not able to assert the claim due to late or long-term effects of an injury, Art. 14(3) Product-Liability-D-P, which only covers long-term health injuries.[147]

10. Relationship Product-Liability-D-P to the liability of internet intermediaries

Delicate problems are also posed by the provisions on the liability of operators of *interconnected services* on the liability privileges according to Art. 4 ff. Digital Services Act (formerly: Art. 12 et seq. E-Commerce Directive and sections 7 - 10 TMG). For as far as these *services* now also fall within the scope of liability of the Product-Liability-D-P, they inevitably come into conflict with the exemption from liability, e.g. of access providers, when it comes to the mediation of e.g. the access of *connected services to* a *product*. However, this does not apply to the *manufacturer*'s own services; likewise, the liability privileges in this area only affected liability for content, but not for cybersecurity risks.[148]

---

147 Cf. on late/long-term damage in German limitation law Gerald Spindler, «BGB § 199 BGB», in *BeckOK BGB*, ed. Georg Bamberger and Herbert Roth, 63rd edn., (München: C.H. Beck, 2022), marginal no. 36; Helmut Grothe, «BGB § 199 BGB», in *MüKoBGB*, ed. Franz Jürgen Säcker et al., 9th edn. (München: C.H. Beck, 2021), marginal no. 11; Andreas Piekenbrock, «BGB § 199 BGB», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status August 01, 2022), marginal no. 62 ff.

148 Gerald Spindler, «TMG before § 7», ed. Gerald Spindler and Peter Schmitz, 2nd edn. (München: C.H. Beck, 2018), marginal no. 32; Andreas Sesing, «TMG § 7», in *BeckOK IT-Recht*, ed. Georg Borges and Marc Hilber, 7th edn. (München: C.H. Beck, July 01, 2022), marginal no. 29; Ulrich Sieber and Frank Michael Höfinger, *MMR-HdB*, ed. Thomas Hoeren, Ulrich Sieber and Bernd Holznagel, 58th edn. (München: C.H. Beck, work status: March 2022), part 18.1 General principles of liability marginal no. 38.

III. The AI Liability Directive Proposal

1. Overview

Characteristic for the AI Liability Directive-E and the fundamental decision of the *EU Commission not* to develop too strict liability rules in order not to slow down the development of AI within the EU[149] is the renunciation of the introduction of strict liability and the restriction to rules on the burden of proof for fault-based non-contractual liability. The AI Liability Directive-E thus falls far short of the proposals of the European Parliament, but also of the *Expert Group on Liability and New Technologies*[150] , both of which advocated the introduction of strict liability. However, the emphasis on innovation-friendliness of the AI Liability Directive-E is in remarkable contrast to the strict liability of the ProdHaft Directive-E, which is explicitly intended to cover AI systems, including *connected services* and *suppliers*, including data suppliers. The AI Liability Directive-E therefore largely applies "only" to the *operators of* the AI systems or to *non-manufacturers, so that it* seems questionable why innovations are to be expected here in particular - instead of with the *manufacturers* and the *suppliers*.

Central to the AI Liability Directive-E is the specification of rules on the burden of proof and presumptions with regard to the interlocking with the product safety law provisions of the AI Regulation-E. The *EU Commission* sees the *autonomous behaviour* and *complexity of* AI systems as the decisive cause for the problems of injured parties in asserting claims against *operators* or *users of* AI systems, Recital 4 of the AI Liability Directive. This is all the truer as the AI Regulation provides for obligations for *operators of high-risk AI systems* to document and log, but no rights of affected parties to inspect the documentation, Recital 16 AI Liability Directive. In this way, the *EU Commission* is attempting, as in the case of the Product Liability Directive-E, to establish a parallelism between product safety and product liability – which, however, is confronted with the same concerns as with the terminology of the AI Regulation-E (see b) above).

2. Scope of application

a) Definition of AI

The AI Liability Directive-E adopts the definitions of the AI Regulation-E regarding the definition of AI itself as well as the category of *high-risk AI systems* according

[149] See EU Commission, Explanatory Memorandum to the AI Liability Directive-E, COM (2022) 496 final 2022/0303 (COD), 6.

[150] European Commission, Directorate-General for Justice and Consumers, "Liability for artificial intelligence and other emerging digital technologies", Publications Office, 2019, 39 ff., 42 ff., https://data.europa.eu/doi/10.2838/573689.

to Art. 6 (1) AI Regulation-E and those of the *operators* (Art. 3 (2) AI Regulation-E) and the *users* (Art. 3 (4) AI Regulation-E).

Thus, the AI Liability Directive-E ultimately exposes itself to the same criticism as that already voiced for the AI Regulation-E, in particular the overly broad scope of application, which, as is well known, covers a multitude of algorithm-driven processes and is not limited to machine learning[151].[152] The same applies to the definition of *high-risk AI systems*.[153] In this respect, the AI Regulation-E distinguishes between the *high-risk AI systems* mentioned in Art. 6 (1) in conjunction with Annex II AI Regulation-E, which are *products* or safety components of *products*, as well as such independent systems, which are enumerated in Art. 6 (2) in conjunction with Annex III AI Regulation-E. Particularly in view of the areas of application listed in Annex III AI-Reg-E, it is questionable whether all systems to be classified as high-risk are really included here.[154] According to Article 7 (1) of the AI-Reg-E, it is possible for the *EU Commission to* expand Annex III of the AI-Reg-E by delegated act and to include new systems that are used in one of the areas listed in Annex III Nos. 1-9 of the AI-Reg-E and that pose a particular risk as defined in Article 7 (1) of the AI-Reg. Article 7(1)(b) of the AI Regulation-E.[155] However, it remains to be seen whether the *EU Commission's* annual review of the list in Annex III of the AI Regulation is sufficient in an economic environment characterized by rapid change and innovation. There are further reservations about the list in Annex III AI-Reg-E, as it covers fields of application such as the use of AI in criminal prosecution or in court, which always require a particularly sensitive handling of the civil liberties in

[151] This is the proposal by Philipp Hacker, "Europäische und nationale Regulierung von Künstlicher Intelligenz," *NJW,* (2020): 2142 (marginal no. 6).

[152] Critical of the broad scope of application: David Bomhard and Marieke Merkle, "Europäische KI-Verordnung," *RDi,* (2021): 276 (277, para. 5 ff.); Martin Ebers et al.*,* "Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf," *RDi,* (2021): 528 (529, para. 6 ff.)*;* Roos Philipp Roos and Caspar Alexander Weitz, "Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung," *MMR,* (2021): 844 (845); Maria Heil, "Die neue KI-Verordnung (E) - Regulatorische Herausforderungen für KI-basierte Medizinprodukte-Software," *MPR,* (2022): 1 (4); Hans Steege, "Chancen und Risiken beim Einsatz künstlicher Intelligenz in der Medizin," *GuP,* (2021): 125 (126); Jan Christopher Kalbhenn, "Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung," *ZUM,* (2021): 663 (664).

[153] Irina Orssich*,* "Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz," *EuZW* (2022): 254 (258); Roos and Weitz, (n 152): 844 (845); Andreas Ebert and Indra Spiecker gen. Döhmann, "Der Kommissionsentwurf für eine KI-Verordnung der EU: Die EU als Trendsetter weltweiter KI-Regulierung," *NVwZ,* (2021): 1188 (1193).

[154] Joint Opinion 5/2021 of the EDPS and the EDPS on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) June 18, 2021, 19, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf; Roos and Weitz, *MMR,* (n 151) 844 (851); Ebers, et al.*,* (n 152), 528 (531, para. 24) ff.

[155] Kristisch zu diesen Einschränkungen Ebers, et al., (n 152), 528 (531, para. 22 ff.).

question,[156] on the other hand only play a role for liability where state liability may be involved.[157]

The AI Liability Directive-E should also only apply where an AI system has had a direct impact on an injured party. Even the involvement of a human being who bases his or her decision on the recommendations of an AI system but makes it on *his or her own responsibility is* not to be covered by the provisions of the AI Liability Directive-E, recital 15 p. 3 ff. The AI Liability Directive thus indirectly ties in with Article 22 of the GDPR, which in a similar way only subjects AI systems to its requirements if no human evaluation is interposed - and ultimately evokes the same criticism as against Article 22 of the GDPR. Since human omission is also not covered by the presumption rules of Art. 3 f. AI Liability Directive-E, it is doubtful how this is compatible with the requirement of "*human being in the loop*", i.e. the human supervision always required according to Art. 14 AI Regulation-E. In recital 15 p. 5, the AI Liability Directive justifies this restriction by stating that the causality between the fault and the damage can always be established in the case of human intervention. Why this should be different in the direct use of AI systems because of the "black-box problem" is not really clear. AI products without an intervening human are already considered defective according to the Product-Liability-D-P - with the described effects on the question of causality.

b) Restriction to non-contractual fault-based liability

Art. 1 (2) of the draft Directive on liability of insurance undertakings explicitly refers only to fault-based liability, whereby all forms of negligence and intent as well as omission are to be included. Furthermore, state liability is also covered.[158]

Conversely, the AI Liability Directive does not limit itself to purely *tortious* liability, but generally covers all liability, insofar as they are based only on fault; however, Article 1 (2) of the AI Liability Directive explicitly excludes contractual claims. Consequently, as in private international law[159], the question arises as to how *quasi-*

---

156 Ebert and Spiecker gen. Döhmann, (n 152) 1188 (1190) ask against this background whether, in a departure from the previous understanding of procedural law, the use of lie detectors by law enforcement, border and migration authorities would also be permissible, cf. Annex III No. 6 lit. b KI-VO-E.

157 The Product-Liability-D-P would not be affected, however, as the violation of relevant legal interests is unlikely to occur here, especially as freedom is not covered.

158 EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 11.

159 On the classification of c.i.c. as a tortious act, see the leading decision of the ECJ Judt., 17 September 2002 - C-334/00, ECLI:EU:C:2002:499 Rn. 19 ff. - *Tacconi*; Schinkels in *BeckOGK* Rom II-VO, status August 01, 2018, Art. 12 Rn. 3 ff.; Abbo Junker, in *MüKo BGB*, ed. Franz Jürgen Säcker, 8th edn. (München: C.H. Beck, 2021), Rom II-VO Art. 12, Rn. 6; Andreas Spickhoff, in *BeckOK BGB*, ed. Beate Gsell et al., 63. edn. (München: C.H. Beck, May 01, 2022), Regulation (EC)

contractual claims that are very similar to tortious liability are to be qualified, such as Section 311 BGB; here, there is much to be said for not including these under the exception of contractual liability.

c) Excluded areas

- Transport law: According to Art. 1(3)(a) of the Draft CLD, the Directive is not intended to cover EU liability provisions in the area of transport law, without specifying this in more detail.[160] However, this means that the AI Liability Directive applies to all national liability provisions in the area of transport, unless they are based on transpositions of EU law. In particular, the liability regulations on road traffic law, which are largely national law, such as sections 7 ff. of the Road Traffic Act (StVG) in Germany, would be affected by this. However, due to the minimum harmonization according to Art. 1 para. 4, Recital 14 p. 2 AI Liability Directive-E, this does not mean that strict liability or keeper liability would have to be abolished; "only" fault-based liability would have to be supplemented accordingly, which could affect e.g. the technical supervision according to sections 1d para. 3, 1f para. 2 StVG, section 14 AFGBV, which is liable via section 823 para. 1 BGB.[161]
- Product Liability Directive: Furthermore, Art. 1 (3) b) AI Liability Directive-E provides that the rights of injured parties under the Product Liability Directive remain unaffected, so that the *manufacturer's liability* - and in future also that of *service providers* and *data suppliers* - of AI systems always applies.[162] Nevertheless, a relevant scope of application remains for the AI Liability Directive-E.[163]
- Digital Services Act: Conversely, according to Art. 1 (3) c) AI Liability Directive-E, the *liability privileges of* the Digital Service Act are not to be affected by the AI Liability Directive-E, which is particularly important for intermediaries who provide services for AI systems. The strict feedback to the AI-Reg-E is also shown by the fact that even the regulations of the DSA on algorithms and the use of AI systems on platforms (Art. 12, Art. 14 para. 6, Art. 17 para. 6, Art. 23 para. 1

864/2007 Art. 12, marginal no. 8; Andreas Spickhoff, "Anspruchskonkurrenzen, Internationale Zuständigkeit und Internationales Privatrecht," *IPRax,* (2009): 128 (132); Jan von Hein, "Die culpa in contrahendo im europäischen Privatrecht: Wechselwirkungen zwischen IPR und Sachrecht," *GPR,* (2007): 54 (59); Maximilian Seibl, "Verbrauchergerichtsstände,vorprozessuale Dispositionen und Zuständigkeitsprobleme bei Ansprüchen aus c.i.c.," *IPRax,* (2011): 234 (239); Ansgar Staudinger, "Rechtsvereinheitlichung innerhalb Europas: Rom I und Rom II," *AnwBl,* (2008): 8 (12); Bartosz Sujecki, "Die Rom II-Verordnung," *EWS,* (2009): 310 (318).

160 An overview of relevant regulations in the transport sector can be found at https://eur-lex.europa.eu/browse/summaries.html, accessed October 1, 2023.

161 This is obviously the assumption of the legislator, Begr RegE BT-DruckS. 19/27439, 32; see also Paul T. Schrader, "Wohin steuert das autonome Fahrzeug – vorübergehend?," *ZRP,* (2021): 109 (111).

162 See above B. III. 1.

163 See below B. IV.

lit. c, Art. 27 para. 1 lit. a, Art. 29 para. 2 DSA) are apparently to be excluded from the AI Liability Directive-E or the evidentiary privileges, so that the respective member state regulations remain in place here.

- National law: Finally, Art. 1(3)(d) of the draft Directive explicitly states that the Member States' provisions on the *burden of proof* (cf. sections 138(3), 288, 291 of the Code of Civil Procedure), the assessment *of evidence or* the requirements as to when *evidence* can be presumed (section 286 of the Code of Civil Procedure) remain unaffected, as does the definition of *fault,* recital 10 of the draft Directive. Nor are rules on *damage*, the coverage of multiple tortfeasors or the statute of limitations covered by the AI Liability Directive, Recital 10, Sentence 2, AI Liability Directive-E. Accordingly, Art. 3-4 of the ELD are special provisions that only take precedence over the Member States' standards in these areas.

d) No restriction to certain legal interests or certain injured parties

By limiting itself only to supplementary provisions to Member State rules for *fault-based liability*, the AI Liability Directive deliberately refrains (unlike the ProdHaft Directive) from providing for liability only for certain legal interests[164] . This means that legal interests that do not fall under the protection of property can also fall within the scope of liability of the AI Liability Directive. This means that legal interests that are not subject to property protection can also fall within the scope of liability of the AI Liability Directive, such as *discrimination* or *equal treatment,* recital 2 of the AI Liability Directive. Accordingly, the AI Liability Directive-E is fully accessory to national liability provisions in terms of the facts, insofar as these refer to fault, whereby the form of fault can extend to negligence as well as intent. For German law, this means that, among other things, liability under section 823 (1) BGB as well as section 823 (2) BGB and section 826 BGB is covered, but also, according to the view expressed here, the *quasi-contractual bases of liability* such as section 311 BGB.

But also with regard to the injured parties covered by the protection of the AI Liability Directive-E, there are differences to the Product Liability Directive-E, as the AI Liability Directive-E does not provide for a limitation of the protection to *consumers,* but also covers commercially injured parties in principle in accordance with the Member States' liability rules.

e) Only minimum harmonisation

Moreover, the AI Liability Directive only provides for a minimum level of harmonisation, Art. 1(4), and leaves it up to the Member States to introduce or maintain stricter rules, irrespective of whether these relate to fault-based or strict liability, Recital 14 p. 2 of the AI Liability Directive.

[164] EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 3.

3. Disclosure of evidence

The central concern of the AI Liability Directive-E is to improve the evidence situation for the injured plaintiff. To this end, the AI Liability Directive-E makes use of two means: (a) on the one hand, the defendant's duty to disclose evidence (disclosure of evidence), (b) on the other hand, presumption of conformity. Both complexes have a number of parallels to the provisions in the Product-Liability-D-P[165] and are based on a common approach.

a) Disclosure of information on high-risk AI systems

Article 3 (1) of the AI Liability Directive allows the court to disclose information or evidence about *high-risk AI systems to the operator* or other parties pursuant to Article 24 or Article 28 of the AI Regulation upon a credible request by the injured party, who had previously unsuccessfully requested the *operator* or other parties to disclose the information. However, Article 3 (1) of the AI Liability Directive does not solve the problem for the injured party of knowing or demonstrating that a *high-risk AI system is* involved at all. According to recital 17, p. 5 of the draft Directive on AI Liability, the mere refusal of the *operator* (or others) should not trigger the presumption of non-compliance with the obligations under the draft CI Regulation.

Such court orders may also be issued against third parties who are not parties to the litigation, in particular if they possess the necessary documentation or information due to their obligations under the CI Liability Directive-E, Recital 19 CI Liability Directive-E. However, disclosure of evidence by third parties should only take place if the evidence cannot be obtained from the defendant, Recital 20, p. 7, CI Liability Directive-E.

In order to counteract unrestrained requests for disclosure of evidence,[166] Art. 3 (2)-(4) of the AI Liability Directive-E (similar to Art. 8 (2)-(4) of the Product-Liability-D-P[167]) also provides for restrictions with regard to *proportionality*, in particular that the plaintiff has previously made sufficient attempts to obtain the relevant information, Art. 3 (2) of the AI Liability Directive-E. Regarding the protection of confidential information or trade secrets, Art. 3(4) of the Draft ECI Liability Directive again only requires the court to take specific measures to ensure confidentiality; as in Art. 8(3) of the Draft ECI Liability Directive, there is a lack of more precise requirements.[168] Only recital 20 p. 5 of the AI Liability Directive-E mentions, similarly to recital 32 p. 2 of the draft directive on the liability of illicit persons mentions restricted access to confidential documents or to relevant negotiations or hearings.

In accordance with the AI Regulation-E, the provisions on the disclosure of evidence are limited to the *operators* etc. of *high-risk AI systems that are* subject to the

[165] See above B. II. 6.
[166] See above B. II. 6. a).
[167] See above B. II. 6. a).
[168] See above B. II. 6. a).

documentation and logging obligations under Art. 18 AI Regulation-E; less risky *AI systems are* thus not subject to the disclosure of evidence, Recital 18 p. 2 AI Liability Directive-E. However, since the AI Liability Directive-E only contains a minimum harmonization, the member states can also provide for more extensive documentation obligations and corresponding disclosures for less risky AI systems.

b) Presumption of non-compliance with obligations

As a consequence of non-compliance with corresponding disclosure orders of the court, Art. 3 (5) of the draft CLD provides for a presumption of non-compliance with the obligations of the draft CLO. Even if the AI Liability Directive-E does not contain a provision on this, such a presumption must be limited to the defendant's non-compliance with the court orders; it cannot apply in the case of a third party's refusal, as the defendant has no influence on this. In any case, the defendant has the possibility to rebut the presumption.

4. Presumption of causality

In addition to the presumption of fault or non-compliance with the obligations of the AI Regulation contained in Article 3(5) of the AI Liability Directive, the AI Liability Directive is limited to presumptions regarding the causality between fault or defective conduct and the damage that has occurred. With regard to the facilitation of proof for non-compliance with obligations or faulty conduct, the AI Liability Directive-E largely refers to national regulations or Union law, recital 22 pp. 2, 3 AI Liability Directive-E, whereby the *EU Commission* is also thinking here of the rules of the DSA in the context of platforms or drones.[169] The plaintiff is therefore not exempt from proving that the AI system was faulty in the first place.

a) Basic rebuttable presumption of causality

Art. 4(1) AI Liability Directive-E contains the *basic rule* that courts should presume causality between a defendant's misconduct and the outcome of the AI system or the plaintiff's injury, provided (a) the plaintiff proves the defendant's misconduct with regard to a duty of care under national or Union law (or it is presumed under Art. 3 para. 5 AI Liability Directive-E) - which at first glance is not limited to the duties under the AI Regulation-E, but is relativised by Art. 4 (2) AI Liability Directive-E - (b) it appears probable that the misconduct "influenced" the outcome of the AI system and (c) that the plaintiff has made a prima facie case that the outcome of the AI system caused the damage. This presumption is rebuttable according to Art. 4(7) AI Liability Directive-E.

In this context, it seems important that recital 22, p. 5-7 of the draft Directive on liability in cases of criminal offences – of course – states that only those obligations can trigger the presumption of causality that serve to protect the injured party, not,

[169] EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 13.

for example, obligations to inform authorities, which recital 25, p. 4 of the draft Directive on liability in cases of criminal offences reaffirms.

b) Presumption of causality towards operators of high-risk AI systems

Moreover, the presumption of causality only applies to *operators of high-risk AI systems* that are subject to the requirements under Chapters 2 and 3 of Title III of the AI Regulation-E or to persons with obligations under Art. 24 or 28(1) of the AI Regulation-E, Art. 4(2) of the AI Liability Directive-E. The presumption also depends on the plaintiff credibly demonstrating that the *operator* etc. has breached several of the obligations under Art. 10 et seq. AI-Reg-E have been breached. These include (*alternatively*):

- the obligations to train the AI system with data sets that meet the requirements of Art. 10 (2) - (4) AI Regulation-E,
- the transparency obligations of Art. 13 AI-Reg-E,
- the duty of human supervision according to Art. 14 AI-VO-E,
- the duty of robustness, accuracy and cybersecurity, Art. 15, 16 a) AI-Reg-E, or
- the absence of corrective or recall measures pursuant to Art. 16 g), 21 AI Regulation-E.

The AI Liability Directive-E wants to include the measures according to the risk management system according to Art. 9 of the AI Regulation-E in the consideration, although the concrete weight of the respective measures apart from the mentioned obligations remains unclear, Recital 26 p. 4 ff. 4 ff. AI Liability Directive-E. The fact that the risk management system is a comprehensive instrument under the AI Regulation does not ultimately help in assessing whether an *operator* has violated its specific obligations.

However, a court should not apply the presumption if the defendant can show that the plaintiff had sufficient access to relevant expertise to prove causation, Art. 4(4) AI Liability Directive-E. Recital 27 S. 2 of the AI Liability Directive refers to cases in which the plaintiff has access to documentation and logging tools of the AI system - ultimately cases of disclosure of evidence.[170]

c) Presumption of causality for users of high-risk AI systems

For users of AI systems, the AI Liability Directive-E restricts the presumption of causality in Art. 4(3) to cases where the plaintiff proves (and not only makes a prima facie case – "proves") that the *user did* not follow his duties to use or monitor the AI system according to the relevant instructions or interrupted the use, Art. 29 AI Regulation-E, or alternatively did not train the AI system with appropriate data (Art.

[170] So then also EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 13.

29(3) AI Regulation-E). The AI Liability Directive-E thus considerably restricts the presumption of causality vis-à-vis the *operators of AI* systems, which, however, is in line with the obligations of the AI Regulation-E – but which, conversely, also does not exclude the qualification of such *users* as *manufacturers* under the ProdHaft Directive-E who modify the AI systems on the basis of training with data.[171]

d) Non-professional users of AI systems

A further restriction of the presumption of causality is contained in Art. 4 (6) AI Liability Directive-E for the non-professional use of AI systems. Here, the presumption of causality shall only apply if the non-professional *user* materially interfered with the conditions of the operation of the AI system ("materially interfered with the conditions of the operation of the AI system") or could have determined the conditions of use but failed to do so. Recital 29 p. 6 et seq. AI Liability Directive-E clarifies the references to the *operator*'s instructions for use once again by making it clear that the non-professional *user of* an AI system can also fall under the presumption of causality if he has disregarded these instructions.

e) Presumption of causality for non-high-risk AI systems

Last but not least, Article 4(5) of the AI Liability Directive contains a provision similar to Article 9(4) of the ProdHaft Directive for *operators* or *users of* less risky AI systems: Here, the presumption of causality only applies if the court is convinced that there are considerable difficulties for the plaintiff to prove causality. However, since ErwGr 28 S. 2 of the AI Liability Directive-E again essentially refers to the "black-box" problem of AI systems, this restriction has little effect in practice, as every plaintiff is likely to face this problem. Moreover, according to Recital 28 S. 4 of the AI Liability Directive, the plaintiff should not be forced to explain the characteristics of the AI system or how these lead to the fact that causality cannot be proven – which ultimately softens this restriction considerably.

5. Collective law enforcement

Art. 2 (6) c) AI Liability Directive-E explicitly provides for the possibility that associations or other third parties can collectively assert the rights of injured parties, for which Art. 6 supplements Annex I of Directive EU 2020/1828.[172]

---

[171] See above B. II. 4. b).

[172] Directive EU 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, [2020] OJ L 409/1.

6. Evaluation of the AI Liability RL-E

Finally, Art. 5 and Recital 31 AI Liability Directive-E explicitly provide for the evaluation of the AI Liability Directive-E as a result of the two-stage process envisaged by the *EU Commission,* for example with regard to the introduction of strict liability as proposed by the *EU Parliament.*[173] This is intended to take into account the rapid technological, but also economic development, in order not to nip innovation processes in the bud through excessive liability.[174] However, this is in contrast to the extension of liability in the Product-Liability-D-P (see above B. 0).

IV. Relationship of the AI Liability Directive-E to the Product Liability-Directive-P

The relationship between the new Product-Liability-D-P and the AI Liability Directive does not appear to be simple: Article 2 (3) c), Recital 9 of the Product-Liability-D-P states that it shall not supersede other national liability regimes of both a *contractual* and *non-contractual* nature, including the regulations implementing the AI Liability Directive, but only to the extent that this liability does not relate to the defectiveness of a *product. However*, if one considers that AI itself will generally be software that is covered by the Product-Liability-D-P, since this now also concerns stand-alone software, it is difficult to distinguish defective *AI* from violations of the AI-VO-E, on which the AI Liability Directive-E is based, because every defective training of an AI with data or the lack of *logging devices* will lead to an AI software being regarded as defective.[175] Ultimately, the scope of application of the AI Liability Directive is noticeably shifted in the direction of the ProdHaft Directive.

An original scope of application therefore remains for the AI Liability Directive-E only regarding the liability based on legal interests of the ProdHaft Directive-E, furthermore its far-reaching limitation of protection to consumers, whereas the AI Liability Directive-E also covers commercially affected persons. Furthermore, the AI Liability Directive-E can also cover violations of fundamental rights, for example, if national law provides for such protection in the area of liability, e.g. in the case of discrimination.[176] Therefore, although the two areas overlap substantially, they have different focal points in *detail.*

---

[173] See above (n 80).

[174] EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 6 f., 14.

[175] See above B. II. 3. b).

[176] On liability due to discrimination in the context of labour law, see Monika Schlachter-Voll, «§ 15», in *Erfurter Kommentar zum Arbeitsrecht*, ed. Rudi Müller-Glöge, Ulrich Preis, Ingrid Schmidt 22nd edn. (München: C.H. Beck 2022), marginal no. 4 ff: Martina Benecke, «§ 15 AGG», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status September 01, 2022), marginal no. 13 ff; Boris Dzida and Naemi Groh 13 et seq.; Boris Dzida and Naemi Groh, "Diskriminierung nach

V. Conclusion

The real bang for the buck in the package of directive proposals lies in the considerable extension of the Product Liability Directive to software, even if this is to be qualified as cloud-based or stand-alone – which corresponds to a desideratum[177] that has been propagated for a long time. But the inclusion of *connected services is also* noteworthy, as is the consistent extension to *data delivery services*. Furthermore, the Product-Liabiltiy-D-P explicitly emphasises the cybersecurity requirements as well as the obligation to update, which was previously difficult to justify in terms of tort law. The extension of legal protection to data is also interesting. Thus, the waiver in the AI Liability Directive-E of the introduction of strict liability for AI systems still seems justifiable, even if there would have been some arguments in favour of extending strict liability to *operators of* AI systems. However, the provisions on the duty of disclosure, which harbours considerable "blackmail potential" comparable to *pretrial discovery,* still appear problematic in both draft directives, especially with regard to the disclosure of trade secrets; here, clarification of the conditions for the protection of trade secrets as well as the requirements for the plaintiff's submission would have been desirable. It will be exciting to see how the Member States and the *EU Parliament* will react to the partly revolutionary proposals.

dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren," *NJW,* (2018): 1917 (1921 et seq.); on liability under § 823 II BGB due to discrimination on the grounds of disability, cf. Spindler, (n 96), Rn. 278 with further references.

177 Cf. for example Zech, (n 82)., A 68; Herbert Zech, "Künstliche Intelligenz und Haftungsfragen," *ZfPW* 209, 198 (212); Wagner, (n 9), 707 (718); Spindler, (n 131), 369 ff.

Künstliche Intelligenz in der Öffentlichen Verwaltung

Annette Guckelberger

A. Einleitung

In Estland, das regelmäßig bei europäischen Vergleichsstudien zum E-Government zu den Spitzenreitern gehört, wurden im Juni 2021 laut dem „Digital Public Administration Factsheet 2022" mehr als 100 KI-basierte Werkzeuge in der Verwaltung eingesetzt.[1] Im Fokus der dortigen Überlegungen steht momentan die Entwicklung und Implementierung eines „Bürokratt" als interoperables Netzwerk von KI-Anwendungen, um Menschen den Zugang zu öffentlichen Diensten über virtuelle Assistenten und mittels Sprach-Interaktion zu ermöglichen.[2]

Demgegenüber stellen laut dem Bericht des zuständigen Bundestagsausschusses für Technikfolgenabschätzung über Künstliche Intelligenz und Distributed-Ledger-Technologie in der öffentlichen Verwaltung v. 26. September 2022 entsprechende

[1] Europäische Kommission, „Digital Public Administration Factsheet Estland 2022", 15, abgerufen am 17. Oktober 2023, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2022.

[2] Europäische Kommission, „Digital Economy and Society Index (DESI) 2022 Estland", 16, abgerufen am 17. Oktober 2023, https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022; dazu sowie zu damit verbundenen rechtlichen Fragen Ivo Pilving undMonika Mikiver, „A Kratt as an Administrative Body: Algorithmic Decisions and Principles of Administrative Law," *Juridica International 29*, (2020): 47 ff.

DOI: https://doi.org/10.17875/gup2023-2495

Anwendungen in der deutschen Verwaltungslandschaft bislang die Ausnahme dar und befinden sich oft noch in der Erkundungsphase.[3] Erklären lässt sich dieser Befund u.a. mit dem allgemeinen Rückstand Deutschlands bei der Digitalisierung sowie dem Fehlen der dafür erforderlichen IT-Infrastrukturen samt des dafür notwendigen verwaltungsinternen Sachverstands.[4] Weil laut dem Digitalen Kompass 2030 der EU-Kommission Behörden künftig nach dem Grundsatz der Plattformökonomie agieren sollen, um einen ganzheitlichen und einfachen Zugang zu den öffentlichen Diensten zu gewähren, und dabei modernste Technologien wie KI und virtuelle Realitäten nahtlos ineinander übergreifen sollen,[5] zeichnet sich auch in Deutschland der zunehmende Einsatz von KI in der Verwaltung ab.

B. KI-Technologien

Bis heute gibt es keine einheitlich akzeptierte Definition von KI.[6] Deshalb variieren die Begriffsumschreibungen. Während teilweise darunter Techniken verstanden werden, welche Maschinen die Erledigung von Aufgaben oder Lösung von Problemen erlauben, die normalerweise Menschen vorbehalten sind,[7] verstehen andere darunter IT-Systeme, die zunehmend ein indeterminiertes Verhalten aufweisen, zielorientiert handeln und über ein eigenständiges Lernreservoir verfügen,[8] oder sich durch die Fähigkeit auszeichnen, komplexe Probleme lösen zu können[9] bzw. weitgehend selbstständig zu entscheiden.[10]

---

[3] Deutscher Bundestag (BT), BT-Drs. 20/3651, 21, 71; s.a. Christoph Krönke, „Digitale Verwaltungshilfe, Die Einbindung Künstlicher Intelligenz (KI) in Verwaltungshandeln aus der Perspektive des Privatisierungsrechts," *Die Verw.* (2023): 31–74, i.E.; Hannah Ruschemeier, «„Künstliche Intelligenz" in der Verwaltung im Mehrebenensystem», in *Herausforderungen für das Verwaltungsrecht*, hrsg. Hermann Hill und Veith Mehde (Berlin: Duncker & Humblot, 2023), i.E.

[4] Thomas Wischmeyer, «Regierungs- und Verwaltungshandeln durch KI», in *Künstliche Intelligenz und Robotik*, hrsg. Martin Ebers u.a. (München: C.H. Beck, 2020), § 20 Rn. 5.

[5] Europäische Kommission, „Mitteilung Der Kommission An Das Europäische Parlament, Den Rat, Den Europäischen Wirtschafts- Und Sozialausschuss Und Den Ausschuss Der Regionen Digitaler Kompass 2030: der europäische Weg in die digitale Dekade", COM (2021) 118 final, 13.

[6] Christian Geminn, „Die Regulierung künstlicher Intelligenz – Anmerkungen zum Entwurf eines Artificial Intelligence Act," *ZD,* (2021): 354; Annette Guckelberger, *Öffentliche Verwaltung im Zeitalter der Digitalisierung*, (Baden-Baden: Nomos, 2019), Rn. 559; Arne Pilniok, „Administratives Entscheiden mit Künstlicher Intelligenz," *JZ,* (2021): 1021, 1022.

[7] Thomas Hoeren und Stefan Pinelli, *Künstliche Intelligenz – Ethik und Recht* (München: C.H. Beck, 2022), 2, die aber auch Tiere erwähnen.

[8] Jürgen Lorse, „Entscheidungsfindung durch künstliche Intelligenz," *NVwZ,* (2021): 1657, 1658.

[9] Christian Djeffal, «Digitalisierung im Verwaltungsrecht», in *Wandlungen im Öffentlichen Recht JTÖR*, hrsg. Sebastian Bretthauer u.a. (Baden-Baden: Nomos, 2020): 479, 480.

[10] Mario Martini, «§ 28», in *Handbuch des Verwaltungsrechts*, hrsg. Wolfgang Kahl und Markus Ludwigs Bd. 1 (Heidelberg: C.F. Müller GmbH, 2021), Rn. 82 ff.

In Anlehnung an den bereits erwähnten Technikfolgenabschätzungsbericht handelt es sich bei KI um einen übergeordneten Begriff für verschiedene Systeme, welche eigenständig Probleme lösen und Aspekte menschlicher Intelligenz nachbilden können, die mithin mit einem gewissen Grad an Autonomie von der menschlichen Steuerung ausgestattet sind.[11] Vor allem durch den Ausbau der Rechenkapazitäten und die dadurch gestiegenen Analysemöglichkeiten großer Datenmengen haben derartige Anwendungen einen enormen Aufschwung erfahren.[12] Die gegenwärtig zur Verfügung stehenden KI-Systeme sind von der Vision einer starken KI, welche mit weitreichenden Möglichkeiten des Wahrnehmens, Denkens und Handelns i.S.e. umfassenden Nachbildung des menschlichen Intellekts,[13] noch weit entfernt. Vielmehr beziehen sich die Überlegungen auf schwache KI-Systeme, die gezielt für die Lösung eng umrissener oder klar abgrenzbarer, formal beschriebener Probleme entwickelt werden,[14] auch wenn sie innerhalb dieser Anwendungsszenarien dem Menschen punktuell überlegen sein mögen.[15] KI-Technologien können sowohl zur Steigerung der menschlichen Handlungs- und Erkenntnismöglichkeiten als auch zum Zwecke der Automation eingesetzt werden.[16]

Ohne jeden Zweifel gehören zur KI solche Technologien, die auf Verfahren des maschinellen Lernens beruhen. Vereinfacht umschrieben werden bei diesen Programmlogiken und Regeln in Trainingsphasen durch Lernalgorithmen aufbauend auf Trainingsdaten selbst erstellt, um aufgrund vorhandener Daten und Algorithmen Muster und Gesetzmäßigkeiten samt Lösungen herauszufinden.[17] Diverse dieser Kategorie zuzuordnenden KI-Anwendungen bauen dabei auf Deep Learning auf.[18] Demgegenüber werden bei regelbasierten KI-Systemen explizite, festgelegte Regeln und lexikalisches Wissen angewendet, also die als maßgeblich erachteten Logiken und Wissensbezüge von vornherein in einen Programmcode überführt.[19] Da ihre Wirkungszusammenhänge und Prozesslogiken als Flussdiagramme darstellbar sind, unterscheiden sie sich von auf maschinellem Lernen beruhenden Systemen durch eine bessere Nachvollziehbarkeit und Erklärbarkeit.[20] Es ist umstritten, ob

[11] Deutscher Bundestag (BT), (Fn. 3), 21; zu KI als Sammelbegriff Pilniok, (Fn. 6), 1021, 1022; zu den verschiedenen Arten auch Guckelberger, (Fn. 6), Rn. 560 ff.
[12] Wolfgang Hoffmann-Riem, *Recht im Sog der digitalen Transformation*, (Tübingen: Mohr Siebeck, 2022), 39; Michael Mayrhofer und Peter Parycek, Digitalisierung des Rechts, 21. ÖJT, Bd. IV/1, (Wien: MANZ Verlag, 2022), 25; s.a. Ruschemeier, (Fn. 3), i.E.
[13]BT, (Fn. 3), 21; s.a. Guckelberger, (Fn. 6), Rn. 107.
[14] Alexander Tischbirek, „Ermessensdirigierende KI," *ZfDR,* (2021): 307, 310; BT, (Fn. 3), 21; s.a. Guckelberger, (Fn. 6), Rn. 107.
[15] Tischbirek, (Fn. 14), 307, 310; s.a. Mayrhofer und Parycek, (Fn. 12), 36.
[16] Djeffal, (Fn. 9), 479, 481.
[17] BT, (Fn. 3), 22.
[18] BT, (Fn. 3), 23.
[19] BT, (Fn. 3), 22.
[20] BT, (Fn. 3), 22; s.a. Mayrhofer und Parycek, (Fn. 12), 27.

man diese Kategorie noch als KI klassifizieren sollte.[21] Jedenfalls wenn regelbasierte Komponenten mit solchen aus maschinellem Lernen kombiniert werden, bietet sich eine Zuordnung zur KI an.[22] Im Übrigen darf nicht vernachlässigt werden, dass der Einsatz komplexer Software vergleichbare rechtliche Fragen wie bei KI-Technologie hervorrufen kann.[23]

C. Vorteile von KI-Anwendungen

Durch den Einsatz von KI in der öffentlichen Verwaltung verspricht man sich eine Reihe von Vorteilen. Aufgrund ihrer Fähigkeiten können derartige Technologien Entscheidungen anhand einer Auswertung von großen Datensätzen treffen, die entweder exakter als solche bei einer menschlichen Bearbeitung sind oder von menschlichen Amtswaltern mangels kognitiver Informationskapazitäten gar nicht getroffen werden könnten.[24] KI-Technologien können Amtswaltern die Analyse von Tatsachen und/oder des Rechtsstoffs erleichtern.[25] Von ihrem Einsatz verspricht man sich u.a. detailliertere und bessere Prognosen als Entscheidungsgrundlage für Planungs- und andere Verwaltungsprozessengen.[26] Mit dem Technologieeinsatz geht eine Rationalisierung der Entscheidungsfindung und -herstellung[27] und somit eine Qualitätssteigerung des Verwaltungshandelns einher.[28] Auch zeichnet sich am Horizont die Möglichkeit einer stärker individualisierten administrativen Leistungserbringung durch den KI-Einsatz ab.[29] Insbesondere erhofft man sich durch den Einsatz von KI-basierten Verfahren, wie der automatischen Text-, Sprach- oder Bilderkennung, eine Erschließung neuer Interaktions- oder Kommunikationswege, indem sich z.B. die Bürger mit Chatbots austauschen oder diese die Funktionen eines virtuellen Assistenten übernehmen.[30]

---

[21] Dies wird z.B. in BT, (Fn. 3), 22 befürwortet.
[22] Zur Existenz solcher Kombinationen BT, (Fn. 3), 22 sowie Mayrhofer und Parycek, (Fn. 12), 10.
[23] Martin Eifert, *Verfassung und Künstliche Intelligenz*, 2023, i.E.
[24] Gerrit Hornung, «§ 35a», in *VwVfG*, hrsg. Friedrich Schoch und Jens-Peter Schneider (München, C.H. Beck, 2. EL April 2022), Rn. 25.
[25] Wischmeyer, (Fn. 4), § 20 Rn. 2.
[26] BT, (Fn. 3), 24.
[27] Wischmeyer, (Fn. 4), § 20 Rn. 3.
[28] Arne Pilniok, „Administratives Entscheiden mit Künstlicher Intelligenz: Anwendungsfelder, Rechtsfragen und Regelungsbedarfe," *JZ,* (2022): 1021, 1024.
[29] Leonid Guggenberger, „Einsatz künstlicher Intelligenz in der Verwaltung," *NVwZ,* (2019), 844, 847; Wischmeyer, (Fn. 4), § 20 Rn. 3.
[30] BT, (Fn. 3), 24.

Ferner können gut konzipierte KI-Technologien dabei helfen, vielfach belegte kognitive Verzerrungen, Vorurteile und Zufälligkeiten administrativer Entscheidungen beim Einsatz menschlicher Amtswalter zu identifizieren[31] oder auch zu vermeiden[32] und somit zu einem Mehr an Gleichheit beitragen.[33] Weil digitale Technologien die Inklusion von Menschen mit Behinderung fördern können und bürgerfreundliche Verwaltungsdienste den Nutzern mehr entgegenkommen, kann der Staat durch den Einsatz von KI-Technologien den Anforderungen des Art. 3 Abs. 3 S. 2 GG oder dem Gebot guter Verwaltung (s. Art. 41 GRCh) besser nachkommen.[34]

Da KI-Anwendungen Probleme schneller einer Lösung zuführen können, geht mit ihrem Einsatz eine Beschleunigung der Verfahren einher.[35] Aus rechtlicher Perspektive kann eine solche Beschleunigung die Wahrnehmung von Grundrechten erleichtern oder rechtsstaatlich geboten sein.[36] Insbesondere wenn Routineaufgaben in Massenverfahren auf die IT-Systeme übertragen werden können, lassen sich die Personalressourcen der Verwaltung anders einteilen, wodurch sich menschliche Amtswalter auf besondere oder schwierige Fallkonstellationen konzentrieren können.[37] Davon verspricht man sich eine Effizienzsteigerung und jedenfalls mittel- oder langfristig Kosteneinsparungen,[38] für welche normativ u.a. der Wirtschaftlichkeitsgrundsatz in Art. 114 Abs. 2 S. 1 GG streitet.[39]

---

[31] Eifert, (Fn. 23), i.E.

[32] Leonid Guggenberger, „Einsatz künstlicher Intelligenz in der Verwaltung," *NVwZ,* (2019): 844, 847; Yoan Hermstrüwer, „Fairnessprinzipien der algorithmischen Verwaltung," *AöR,* 145 (2020): 479, 481; Wischmeyer, (Fn. 4), § 20 Rn. 3.

[33] Guggenberger, (Fn. 32), 844, 847; Dorothea Mund, *Das Recht auf menschliche Entscheidung – zu den verfassungsrechtlichen Vorgaben der technischen Erzeugung von Verwaltungsentscheidungen*, (Tübingen: Mohr Siebeck, 2021), 70.

[34] Pilniok, (Fn. 6), 1021, 1024; Meinhard Schröder, „Auftrag zur und Grenzen der Digitalisierung der Verwaltung," *ZdiW,* (2022): 269, 270.

[35] Wischmeyer, (Fn. 4), § 20 Rn. 3; s.a. Mund, (Fn. 33), 70.

[36] S.a. Meinhard Schröder, „Rahmenbedingungen der Digitalisierung der Verwaltung," *VerwArch,* 110 (2019): 328, 330, der auf das Gebot zügigen Verfahrens als Ausfluss des Rechtsstaatsprinzips verweist.

[37] Wischmeyer, (Fn. 4), § 20 Rn. 3.

[38] BT, (Fn. 3), 23; Krönke, (Fn. 3), i.E.

[39] Pilniok, (Fn. 6), 1021, 1024.

D. Vielfältige Anwendungsfelder

Aufgrund des Charakters der KI als Querschnittstechnologie[40] sind ihre Einsatzfelder breit gefächert[41] und kann sie auf Bundes-, Landes- oder kommunaler Ebene eingesetzt werden.[42] Im Hinblick auf den technologischen Fortschritt stellen Erwägungen zu möglichen Einsatzfeldern für KI immer nur Momentaufnahmen dar.[43] Im Technikfolgenabschätzungsbericht des zuständigen Bundestagsausschusses, der allerdings auch regelbasierte Verfahren als KI-Anwendungen einstuft, werden als Beispiele für KI-Anwendungen auf Bundesebene im Bereich des Bundesamts für Migration und Flüchtlinge (BAMF) die Erkennung, Indexierung und Zuweisung von Schriftgut- und Postverkehr, die automatische Gesichts-, Dialekt- und Namenstransliteration, im Bereich der Zollverwaltung KI-basierte Ansätze bei der Geldwäschebekämpfung, im Bereich der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur regelmäßigen Überwachung des Handelsgeschehens sowie zur Detektion von Insidergeschäften und Marktmissbrauch, im Bereich der Bundespolizei zur biometrischen Gesichtserkennung und der automatisierten Grenzkontrollen an mehreren Flughäfen, im Bereich des Bundesministeriums für Gesundheit (BMG) zur Mustererkennung komplexer Datensätze und des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur automatisierten Detektion von Schadprogrammen genannt.[44] In Berlin und Hamburg erfolgt die Verkehrssteuerung via Echtzeitauswertung von Kameraaufnahmen, ferner sollen in Berlin durch KI-Systeme Unregelmäßigkeiten im Rahmen des beamtenrechtlichen Beihilfesystems aufgedeckt werden und mehrere Bundesländer setzen Chatbots zur Beantwortung von Bürgeranfragen ein.[45] Letztere sind ebenfalls auf kommunaler Ebene anzutreffen. In vier Städten wird KI im Verkehrssektor eingesetzt, in rund 100 Kommunen und Landkreisen werden Straßenschäden mittels KI identifiziert.[46] Mannheim erhofft sich von einer intelligenten Videoüberwachung durch eine KI-basierte Auswertung von Kamerabildern eine verbesserte Gefahrenabwehr.[47]

Wie dieser kurze Überblick zeigt, kann sich die KI-Anwendung sowohl auf Realakte als auch auf Verwaltungsakte beziehen. Sie kann nur innerhalb des Bereichs

---

[40] Christian Djeffal, «Künstliche Intelligenz», in *Handbuch Digitalisierung in Staat und Verwaltung*, hrsg. Tanja Klenk, Frank Nullmeier, Göttrik Wewer (Wiesbaden: Springer, 2020), 51, 52; Wischmeyer, (Fn. 4), § 20 Rn. 14.

[41] Martini, (Fn. 10), § 28 Rn. 84; Wischmeyer, (Fn. 4), § 20 Rn. 14.

[42] BT, (Fn. 3), 25 f.

[43] Jan Ziekow und Bettina Engewald, «Künstliche Intelligenz in der öffentlichen Verwaltung», in *Digitale Transformation im Spiegel des öffentlichen Rechts*, hrsg. Matthias Knauff und Chien-Liang Lee (Berlin: BWV Berliner Wissenschafts-Verlag, 2021), 9, 12.

[44] BT, (Fn. 3), 27.

[45] BT, (Fn. 3), 28 f.

[46] BT, (Fn. 3), 29.

[47] BT, (Fn. 3), 29.

der Verwaltung ohne jegliche Außenwirkung eingesetzt werden,[48] etwa bei der Indexierung der Eingangspost, beim Einsatz von Text-Auto-Korrekturprogrammen,[49] bei der juristischen Recherche,[50] für die Analyse des Akteninhalts,[51] die Erstellung von Textvorschlägen[52] oder beamtenrechtlicher Beurteilungen,[53] zur Optimierung des internen Workflows[54] oder zur Gewährleistung der IT-Sicherheit.[55]

Oft erlangen KI-Anwendungen aber auch in Außenbeziehung Relevanz,[56] z.B. als Beratungsangebot, beim Ausfüllen von Formularen[57] oder zur Vorbereitung von Behördenentscheidungen mit Außenwirkung. Nur selten dürften gegenwärtig KI-Systeme vollautomatisierte Entscheidungen treffen, so etwa im Verkehrsbereich.

Betrachtet man die soeben erwähnten Anwendungsmöglichkeiten eignen sich als Referenzfelder für den Einsatz von KI-Technologien der Bereich der Sicherheitsgewährleistung[58] und der des Verkehrs.[59] Schon seit geraumer Zeit existiert ein Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG). Soweit ersichtlich hat Deutschland als erstes Land weltweit ein Gesetz zum autonomen Fahren erlassen.[60] Da sich dieses auf Fahrzeuge bezieht, die Fahraufgaben ohne eine fahrzeugführende Person selbstständig erfüllen können und über eine bestimmte technische Ausrüstung verfügen, die aber nur in festgelegten Betriebsbereichen verkehren dürfen, ist der Bereich des Öffentlichen Personennahverkehrs (ÖPNV) ein interessantes Einsatzgebiet.[61] Zu

[48] Guggenberger, (Fn. 32), 844, 849; s.a. Pilniok, (Fn. 6), 1021, 1023.
[49] Martini, (Fn. 10), § 28 Rn. 84.
[50] Mayrhofer und Parycek, (Fn. 12), 38 f., 105.
[51] Mayrhofer und Parycek, (Fn. 12), 105.
[52] Mayrhofer und Parycek, (Fn. 12), 10 f. und 21 zur Bescheidvorbereitung durch Textbausteine.
[53] Näher dazu Jürgen Lorse, „Entscheidungsfindung durch künstliche Intelligenz," *NVwZ,* (2021): 1657, 1660.
[54] Mayrhofer und Parycek, (Fn. 12), 105.
[55] Mayrhofer und Parycek, (Fn. 12), 23.
[56] Guggenberger, (Fn. 32), 844, 849.
[57] Zu letzterem Guggenberger, (Fn. 32), 844, 849.
[58] Wischmeyer, (Fn. 4), § 20 Rn. 15 ff.
[59] Dazu etwa Martin Kment und Sophie Borchert, *Künstliche Intelligenz und Algorithmen in der Rechtsanwendung*, (München: C.H. Beck, 2020), Rn. 60 ff.; Daniel Busche, „Staatliche Verantwortungsübernahme beim hoheitlichen Einsatz intransparenter Algorithmen," *DÖV,* (2022): 899, 905.
[60] BGBl. 2021 I 3108 ff.
[61] Näher dazu Annette Guckelberger, «Rechtsrahmen für hochautomatisiertes Fahren in Deutschland», in *Automatisierter ÖPNV*, hrsg. Robert Yen et al. (Berlin: Springer, 2023); Emanuele Leonetti, «Automatisiertes Fahren – ÖPNV», in *Künstliche Intelligenz,* hrsg. Kuuya Chibanguza, Christian Kuß und Hans Steege (Baden-Baden: Nomos, 2022), 431 ff.

den weiteren im Schrifttum erörterten Referenzgebieten für diese Technologien gehören staatliche Auswahl- und Zulassungsentscheidungen, etwa zum Studium,[62] oder auch Fremdsprachenübersetzungen, die u.a. für eine gelingende europäische Verwaltungszusammenarbeit (§§ 8a ff. VwVfG) wichtig sind.[63]

E. Nachteile von KI-Systemen

Weil menschlichen Amtswaltern in der Verwaltung immer wieder Fehler bei der alltäglichen Arbeit unterlaufen, verspricht man sich vom Technikeinsatz oft weniger fehlerhafte Entscheidungen. Dies kann, muss aber nicht stets so sein. Denn die KI-Systeme werden von Menschen konzipiert. Fehlerhafte KI-Entscheidungen können u. a. durch Verwendung diskriminierender Prädiktoren entstehen.[64] Des Weiteren können durch das Training eines Machine Learning-Algorithmus mit auf einem Bias beruhenden Daten auch KI-Technologien im Ergebnis diskriminierende Entscheidungen hervorbringen.[65] Da sie tatsächlich bestehende Korrelationen ausfindig machen, können ihre Aussagen möglicherweise in rechtlich unzulässigen oder zumindest problematischen Ungleichbehandlungen bestehen.[66] In den Worten von *Parycek* kann der diskriminierende Effekt eines KI-Systems flächenmäßige Auswirkungen entfalten, „wie eine individuelle Verzerrung bei einzelnen menschlichen Entscheidungsträger:innen es nicht könnte".[67] Deshalb kommt dem Aufspüren von systematischen Verzerrungen bei maschinell-lernenden Systemen entscheidende Bedeutung zu[68] und ist zu überlegen, welche Vorkehrungen für die Sicherstellung gleichheitsgerechter und nicht diskriminierender Entscheidungen notwendig sind. Im Technikfolgenabschätzungsbericht wird die Auswahl und Aufbereitung einer geeigneten Datenbasis aus Gründen der Funktionsfähigkeit und Validität der Ergebnisdarstellungen der KI-Anwendungen als zentrale Herausforderung eingestuft.[69] Damit sich die Verwaltung auf Ursachenforschung für die Gründe einer Ungleichbehandlung begeben kann, bedarf es einer Sicherung der ausgewählten und behandelten Trainingsdaten sowie einer Dokumentation der Programmentwicklung

[62] Timo Rademacher, „Digitalisierung des Zugangs zu staatlichen Leistungen: Darf – oder soll – künstliche Intelligenz über die Studienzulassung entscheiden?," *RdJB,* (2021): 254 ff.
[63] Eingehend dazu Christian Djeffal und Antonia Horst, *Übersetzung und Künstliche Intelligenz in der öffentlichen Verwaltung* (Berlin: NEGZ Bericht Nr. 17, 2021), 8 ff.
[64] Joachim Englisch und Mathias Schuh, „Algorithmengestützte Verwaltungsverfahren – Einsatzfelder, Risiken und Notwendigkeit ergänzender Kontrollen," *Die Verw.,* 55 (2022): 155, 170 ff.; s.a. Kment und Borchert, (Fn. 59), Rn. 120 ff.
[65] Hermstrüwer, (Fn. 32), 479, 492; Wischmeyer, (Fn. 4), § 20 Rn. 58.
[66] Wischmeyer, (Fn. 4), § 20 Rn. 59; s.a. Tischbirek, (Fn. 14), 307, 323.
[67] Mayrhofer und Parycek, (Fn. 12), 42.
[68] Mayrhofer und Parycek, (Fn. 12), 42.
[69] BT-Drs. 20/3652, 71; weitere Nachweise bei Guckelberger, (Fn. 6), Rn. 571 ff.

einschließlich von Protokollierungen.[70] Außerdem muss die zuständige Behörde bei Feststellung von Unzulänglichkeiten Zugang zum operativen Programmcode haben[71] und über ausreichende Möglichkeiten zum Einschreiten verfügen, etwa durch Abschalten der KI.[72] Weitere Überlegungen gehen dahin, Diskriminierungen durch den Einsatz von Begleit- und Kontrollprogrammen zu begegnen[73] oder durch Zufallsstichproben oder kontrafaktische Entscheidungsbegründungen unterschiedliche Entscheidungstypen in einer Art „Reallabor" der Verwaltung zu erproben.[74]

Für die Betroffenen einer Diskriminierung ist deren Feststellung bei Einsatz von KI-Systemen oft schwer. Dies beruht darauf, dass sich mit zunehmender Komplexität der eingesetzten Algorithmen ihr Output immer weniger nachvollziehen lässt.[75] Weil KI-Systeme einer anderen Logik folgen als menschliche Entscheidungen, die auf Kausalitäten und normative Zurechnungen abstellen, lassen sich deren Ergebnisse nur schwer verstehen.[76] Während menschliche Entscheidungen und feste Programmierungen mit Begründungen versehen werden können, die u.a. aus Gründen eines rechtsstaatlichen Verfahrens, möglicherweise des Grundrechtsschutzes durch Verfahren sowie der Rechtsschutzgarantie wichtig sind,[77] ist dies bei selbstlernenden Algorithmen momentan nicht der Fall.[78] Zwar setzt man zunehmend auf Forschungen, um die Entscheidungsfindung von KI menschlichen Nutzern verständlich zu machen (sog. explainable AI), wodurch das Vertrauen in die Systeme gefördert und die Entscheidung über den Einsatz solcher Systeme erleichtert wird.[79] Allerdings bleibt das Gelingen dieser Forschungsansätze abzuwarten und ist einzustellen, dass sich der Inhalt solcher Erklärungen von den herkömmlichen Begründungen eines Verwaltungsakts unterscheidet.[80] Momentan ist daher eine Überprüfung der Entscheidungsqualität einer KI regelmäßig nur anhand ihres

[70] Krönke, (Fn. 3), i.E.; s.a. Mayrhofer und Parycek, (Fn. 12), 56.
[71] Krönke, (Fn. 3), i.E.; zur Protokollierung der Programmablaufpläne Martini, (Fn. 10), § 28 Rn. 93.
[72] Mayrhofer und Parycek, (Fn. 12), 68; Guckelberger, (Fn. 6), Rn. 629; Viktoria Herold, *Demokratische Legitimation automatisiert erlassener Verwaltungsakte*, (Berlin: Duncker & Humblot, 2020), 226.
[73] Guckelberger, (Fn. 6), Rn. 591; Martini, (Fn. 10), § 28 Rn. 93; Krönke, (Fn. 3), i.E.; s.a. Ziekow und Engewald, (Fn. 43), 21.
[74] Hermstrüwer, (Fn. 32), 479, 497 ff.
[75] Krönke, (Fn. 3), i.E.; Kment und Borchert, (Fn. 59), Rn. 87.
[76] Eifert, (Fn. 23), i.E.
[77] David Roth-Isigkeit, „Die Begründung des vollständig automatisierten Verwaltungsakts," *DÖV,* (2020): 1018, 1020; s.a. Mayrhofer und Parycek, (Fn. 12), 90; Thomas Wischmeyer, „Regulierung intelligenter Systeme," *AöR,* 143 (2018): 1, 55.
[78] Eifert, (Fn. 23), i.E.
[79] Gerrit Hornung, „Künstliche Intelligenz zur Auswertung von Social Media Massendaten," *AöR,* 147 (2022): 1, 52 f.; zur Notwendigkeit aus Gründen der Wahrnehmung der Aufsicht Herold, (Fn. 72), 227; zur explainable AI Busche, (Fn. 59), 899, 900; Guckelberger, (Fn. 6), Rn. 613.
[80] Eifert, (Fn. 23), i.E.; dazu auch Busche, (Fn. 59), 899, 906.

Outputs möglich.[81] Sofern vollautomatisierte Behördenentscheidungen von einem KI-System getroffen werden sollen, ist daher zu überlegen, ob und bei welchen staatlichen Entscheidungen möglicherweise ganz auf eine Begründung verzichtet werden kann[82] oder etwas andere Anforderungen als bei Begründungen durch menschliche Amtswalter durch Begründungsregeln für algorithmenbasierte Verfahren vorgesehen werden können.[83]

Oft gehen einzelne KI-Anwendungen mit der Verarbeitung großer Datenmengen einher.[84] Neben Fragen der Datensicherheit wirft diese Technologie daher bei Verarbeitung personenbezogener Daten solche des Datenschutzes auf.[85] Es kommt zu Friktionen mit den in Art. 5 Abs. 1 DSGVO aufgezählten Grundsätzen der Transparenz, Zweckbindung und Datenminimierung.[86] Nach ständiger BVerfG-Rechtsprechung richten sich die Anforderungen an die weitere Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung, bei welcher sicherzustellen ist, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird.[87] Jedenfalls wenn die Daten mit nachrichtendienstlichen Mitteln erhoben wurden, ist nach dem Kriterium der hypothetischen Datenneuerhebung zu prüfen, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften.[88]

Da die Verwaltung auch bei Einsatz von KI-Technologien an Gesetz und Recht gebunden ist (Art. 20 Abs. 3 GG),[89] dürfen solche nur eingesetzt werden, wenn Sicherungsmechanismen gewährleisten, dass solchermaßen getroffene Entscheidungen mit Gesetz und Recht übereinstimmen.[90] Zu diesem Zweck sind sie vor

[81] Eifert, (Fn. 23), i.E.
[82] Busche, (Fn. 59), 899, 906 f.; Martin Eifert, «Staatliche Verantwortung für KI-Infrastruktur und Datensicherheit», *Bitburger Gespräche Jahrbuch 2020*, (München: C.H. Beck, 2021), 15, 32; Guckelberger, (Fn. 6), Rn. 616; gegen Einschränkungen der Begründung Nadja Braun Binder, „Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung," *SJZ,* (2019): 467, 472.
[83] Kment und Borchert, (Fn. 59), Rn. 207 ff.; s.a. Lothar Michael, «§ 28», in *Das Staatsrecht der Bundesrepublik Deutschland*, hrsg. Klaus Stern, Helge Sodan und Markus Möstl, Bd. I, 2. Aufl. (München: C.H. Beck, 2022), Rn. 44, 46.
[84] BT, (Fn. 3), 14, 73; dazu, dass dies nicht immer der Fall sein muss, Ziekow und Engewald, (Fn. 43), 11.
[85] Kment und Borchert, (Fn. 59), Rn. 142.
[86] BT, (Fn. 3), 14, 73.
[87] BVerfG, Beschl. v. 28.9.2022 - 1 BvR 2354/13, Rn. 121 ff., juris.
[88] BVerfG, Beschl. v. 28.9.2022 - 1 BvR 2354/13, Rn. 121 ff., juris.
[89] Dazu auch Wischmeyer, (Fn. 4), § 20 Rn. 42.
[90] Martini, (Fn. 10), § 28 Rn. 92.

ihrem Einsatz hinsichtlich des Erreichens des gebotenen Qualitätsniveaus ausreichend zu testen.[91] Im Falle einer Änderung der Rechtslage oder auch der Rechtsprechung im Einsatzbereich eines KI-Systems ist auf deren Nachjustierung zu achten.[92] Knüpfen Rechtsnormen an ein Kausalitätserfordernis an, scheiden vollautomatisierte Entscheidungen aufgrund nur Korrelationen ausfindig machender KI-Anwendungen aus.[93] Es würde sowohl dem Rechtsstaats- als auch Demokratieprinzip widersprechen, wenn Programme völlig frei über die Kriterien für zukünftige Programmentscheidungen bestimmen und gesetzliche Vorgaben außer Kraft setzen könnten.[94] Da sich KI-Systeme bis zu einem gewissen Maß selbst ändern und sich ein Stück weit von der ihnen durch die behördliche Einsatzentscheidung gebilligten Programmierung entfernen, fordern derartige Anwendungen das Demokratieprinzip heraus.[95] Zur Kompensation wird daher zutreffend darüber nachgedacht, ob man nicht durch eine Implementierung begleitender effektiver Kontrollmechanismen für eine hinreichende demokratische Legitimation solcher administrativer Entscheidungen sorgen kann.[96] Soweit KI-Technologien mit einer gewissen Autonomie ausgestattet und aufgrund ihrer Komplexität schwer nachvollziehbar sind, kommt ihrer Freigabe zum Einsatz sowie in Abhängigkeit zur wahrzunehmenden Aufgabe nachfolgenden laufenden Überwachung eine zentrale Bedeutung zu.[97] Insbesondere wenn KI-Systeme vollständig automatisierte Verwaltungsentscheidungen treffen, liegt aus verfassungsrechtlichen Gründen eine allein von Behördenmitarbeitern veranlasste Aussteuerung bestimmter Fälle zur stichprobenhaften Überprüfung derartiger Entscheidungen nahe.[98] Jedoch werden durch solche Begleitmaßnahmen die Vorteile des KI-Einsatzes in gewissem Maße wieder relativiert. Außerdem bedarf es ausreichend qualifizierten Personals für die Wahrnehmung solcher Kontrollen, das sich angesichts der Wettbewerbssituation mit dem Privatsektor nicht so einfach gewinnen lässt.[99]

---

[91] Eingehend zum Testen und deren Bedeutung Guckelberger, (Fn. 6), Rn. 585 f. m.w.N.
[92] Martini, (Fn. 10), § 28 Rn. 92.
[93] Ruschemeier, (Fn. 3), i.E.
[94] Martini, (Fn. 10), § 28 Rn. 88; Ulrich Stelkens, «§ 35a», in *VwVfG*, hrsg. Ulrich Stelkens, Heinz Joachim Bonk und Michael Sachs, 9. Aufl. (München: C.H. Beck, 2018), Rn. 47.
[95] Martini, (Fn. 10), § 28 Rn. 86 f.; s.a. Mund, (Fn. 33), 80 f. sowie Herold, (Fn. 72), 186.
[96] Martini, (Fn. 10), § 28 Rn. 89 f.; in diese Richtung auch Krönke, (Fn. 3), i.E.
[97] Englisch und Schuh, (Fn. 64), 155, 184, 186; Mayrhofer und Parycek, (Fn. 12), 71 f.; zur Überwachung auch Guckelberger, (Fn. 6), Rn. 587 ff., 595 ff. und zur Eigenschaft als Daueraufgabe Ruschemeier, (Fn. 3), i.E.
[98] Englisch und Schuh, (Fn. 64), 155, 184; Guggenberger, (Fn. 32), 844, 850; Ziekow und Engewald, (Fn. 43), 24.
[99] Daher Beleihungen in Erwägung ziehend Kment und Borchert, (Fn. 59), Rn. 246.

F. Zwischenfazit

Für einen sinnvollen Einsatz von KI-Systemen in der Verwaltung sind geeignete Einsatzfelder zu identifizieren. Sofern für die Entwicklung einer KI-Technologie große Datenmengen benötigt werden, kann ein Einsatz im Bereich der Verwaltung schon daran scheitern, dass es an der dafür erforderlichen Datenmasse fehlt oder die Verarbeitung personenbezogener Daten auf datenschutzrechtliche Grenzen stößt.[100] Während es Bereiche geben mag, in denen sich der Einsatz von KI positiv auf die Sachverhaltsermittlung administrativer Entscheidungen auswirkt, etwa durch den Einsatz von Sprach-, Bild- oder Texterkennungen,[101] wird KI in anderen Konstellationen für die Sachverhaltsaufklärung wenig oder gar nicht geeignet sein.[102]

Angesichts der vielen denkbaren und unterschiedlichen KI-Anwendungen ist bei der rechtlichen Beurteilung stets auf die konkrete Einsatzform abzustellen[103] und zu prüfen, ob sie mit den unions-, verfassungs- und einfachgesetzlichen Vorgaben in Einklang steht. Da zurzeit ein Großteil der Entscheidungen der Verwaltung aus diversen Gründen weiterhin durch menschliche Amtswalter erfolgt und der auf die Verwaltung bezogene KI-Einsatz auf deren Entscheidung zurückgehen muss, steht dem die Menschenwürdegarantie (Art. 1 Abs. 1 GG) regelmäßig nicht entgegen, solange sichergestellt ist, dass der KI infolge der Programmierung ausreichend Grenzen gesetzt sind und die Amtswalter sozusagen die Oberhand über das KI-System behalten sowie weitere Schutzvorkehrungen, etwa in Gestalt menschlicher Ansprechpersonen, bestehen.[104]

Je nach Art und Einsatz einer KI variiert deren Steuerungswirkung für die zu treffenden Verwaltungsentscheidungen mit entsprechenden Konsequenzen für deren demokratische Legitimation.[105] In den Worten von *Rademacher* verändern sich Informationen von IT-Systemen bei zunehmender Automatisierung und Autonomie „von einer gegenstandsbezogenen Auskunft („information *about* something") hin zu einem Element der Steuerung menschlicher und/oder technischer Reaktionen".[106] Infolgedessen wird bei der rechtlichen Beurteilung zwischen vollständig

[100] Dazu Guckelberger, (Fn. 6), Rn. 576.
[101] Ruschemeier, (Fn. 3), i.E.
[102] Generell zu den Grenzen Wischmeyer, (Fn. 4), § 20 Rn. 39 sowie Djeffal, (Fn. 40), 51, 59.
[103] Ruschemeier, (Fn. 3), i.E.; Ziekow und Engewald, (Fn. 43), 12.
[104] Krönke, (Fn. 3), i.E.; Lorse, *NVwZ,* (2021): 1657, 1659; Wischmeyer, (Fn. 4), § 20 Rn. 45; s.a. Michael, (Fn. 83), § 28 Rn. 23; Schröder, (Fn. 36), 328, 337, insbesondere, wenn die KI Verbesserungen für den Einzelnen bewirken soll.
[105] Herold, (Fn. 72), 103, 190 ff.
[106] Timo Rademacher, «Vorb. § 8a», in *VwVfG*, hrsg. Friedrich Schoch und Jens-Peter Schneider (München: C.H. Beck, 2. EL April, 2022), Rn. 3.

automatisierten, automationsgeleiteten und -gestützten Verwaltungsentscheidungen[107] oder zwischen den Kategorien des entscheidenden, entscheidungsnahen oder entscheidungsfernen KI-Einsatzes differenziert.[108] So macht es einen erheblichen Unterschied, ob eine KI-Anwendung nur einen Amtswalter bei der Vorbereitung der zu treffenden Entscheidung unterstützt (Stichwort: „digitale Verwaltungshilfe") oder selbständig endgültige Verwaltungsentscheidungen fällt.[109] Für die rechtliche Beurteilung kann auch der Einsatzzeitpunkt der KI Relevanz erlangen. Wird diese zu Beginn des Verfahrens eingesetzt, steigt die Wahrscheinlichkeit einer Vorprägung der zu treffenden Entscheidung im Vergleich zu einem KI-Einsatz zur Überprüfung einer Entscheidung eines menschlichen Amtswalters.[110] Da Menschen Maschinen aber oft ein zu großes Vertrauen entgegenbringen (sog. automation bias), sollte beim Konzept des „official in the loop" sichergestellt sein, dass den menschlichen Amtswaltern ausreichend Zeit für eigene Überlegungen zur Verfügung steht und diese für die Gefahren eines KI-Systems, etwa durch entsprechende Schulung, hinreichend sensibilisiert werden.[111] In den Worten von *Michael* eröffnet das Zusammenwirken von Mensch und Maschine die Chance, „die jeweiligen Schwächen maschinellen sowie menschlichen Entscheidens – gerade auch mit Blick auf Diskriminierung – zu minimieren".[112]

Muss ein menschlicher Amtswalter vor Erlass der letztverbindlichen Entscheidung tätig werden, kann etwaigen Anhörungserfordernissen ohne weiteres Rechnung getragen werden, während bei vollautomatisierten Entscheidungen entweder auf Aussteuerungsmöglichkeiten oder Konstellationen gesetzt wird, in denen keine Anhörung notwendig ist, sei es, weil ein begünstigender Verwaltungsakt erlassen oder nicht von den Angaben des Beteiligten abgewichen wird.[113] Trifft ein menschlicher Amtswalter eine Verwaltungsentscheidung, bereitet das Begründungserfordernis jedenfalls dann keine Probleme, wenn er dieser Anforderung Rechnung tragen kann.[114] Auch ist bei einer solchen Vorgehensweise dafür Sorge getragen, dass die KI sozusagen unter Beobachtung steht, so dass sich Bedenken hinsichtlich der Wahrung des hinreichenden demokratischen Legitimationsniveaus verringern.[115]

---

[107] So Mund, (Fn. 33), 242 ff.; s.a. Englisch und Schuh, (Fn. 64), 155, 159.
[108] Krönke, (Fn. 3), i.E.
[109] Krönke, (Fn. 3), i.E.
[110] Pilniok, (Fn. 6), 1021, 1027.
[111] Mayrhofer und Parycek, (Fn. 12), 53 f.; Pilniok, (Fn. 6), 1021, 1027.
[112] Michael, (Fn. 83), § 28 Rn. 38.
[113] Dazu Mayrhofer und Parycek, (Fn. 12), 85 ff.
[114] Dazu Busche, (Fn. 59), 888, 906; dazu und ob ggf. die Anforderungen zu modifizieren sind, Krönke, (Fn. 3), i.E.
[115] Dazu, dass sich die demokratische Legitimation nicht nur auf das Output bezieht, Ziekow und Engewald, (Fn. 43), 19. Zum Erfordernis des „Knopfdrucks" auch Herold, (Fn. 72), 247 f.; Probleme können sich aber daraus ergeben, wenn die Vorschläge und

Zudem bezieht sich die Begründungsvorschrift des § 39 Abs. 1 VwVfG nur auf Verwaltungsakte. Für Realakte oder rein interne Maßnahmen beansprucht diese Vorschrift keine Gültigkeit und ist eine Begründung mangels abweichender spezialgesetzlicher oder besonderer verfassungsrechtlicher Anforderungen auch nicht geboten. Eine verlässlich funktionierende KI zur Sortierung der bei der Verwaltung eingehenden Post unterliegt deshalb keinen Begründungsanforderungen. Für KI-Anwendungen, die lediglich der internen Verwaltungsorganisation dienen oder denen es an einem hinreichenden Bezug zu einem konkreten Verwaltungsverfahren mangelt,[116] gelten andere Maßstäbe als für Entscheidungen mit unmittelbarer Außenwirkung.

Der Umstand, dass KI-Anwendungen im Vorfeld von Verwaltungsentscheidungen mit Außenwirkung in der Regel geringere rechtliche Probleme hervorrufen, deckt sich mit dem Realbefund, wonach die weit überwiegenden Anwendungsfälle von KI-Anwendungen innerhalb der Verwaltung das Vorbereitungsstadium betreffen.[117] Da am Ende dieses Prozesses die Entscheidung mit Außenwirkung auf einen menschlichen Amtswalter zurückzuführen ist, ruft diese geringere Akzeptanzprobleme hervor[118] und ist unter dem Gesichtspunkt effektiven Rechtsschutzes oftmals weniger problematisch. Allerdings hat der EuGH in seiner Entscheidung zu Art. 6 Abs. 3 lit. b PNR-Richtlinie (EU) 2016/681, wo der Einsatz selbstlernender Systeme schon nicht dem dort vorgesehenen Abgleich anhand „im Voraus festgelegter Kriterien" entsprach, hinzugefügt, dass es angesichts der für die Funktionsweise von KI kennzeichnenden mangelnden Nachvollziehbarkeit unmöglich sein könne, den Grund für einen Treffer durch diese zu identifizieren. „Unter diesen Umständen könnte die Nutzung solcher Technologien den Betroffenen auch ihr in Art. 47 der Charta verankertes Recht auf einen wirksamen gerichtlichen Rechtsbehelf nehmen," dass die möglicherweise erzielten Ergebnisse nicht frei von Diskriminierungen seien.[119] Auch wenn bei standardisierten Geschwindigkeitsmessungen momentan keine KI-Technologien zum Einsatz kommen dürften und die Messungen keine normativ bindende Wirkung zeitigen, ist unter den Landesverfassungsgerichten in Deutschland streitig, welche Konsequenzen sich daraus für den Einsatz von Geräten ohne Speicherung von Rohmessdaten ergeben. Kürzlich judizierte der VerfGH Rheinland-Pfalz, dass dadurch Rechtspositionen der Betroffenen nicht unzumutbar verkürzt würden. So würde bereits durch die amtliche Zulassung der Messgeräte und -methoden Fehlerquellen in den Systemen entgegengewirkt, ferner könne der

Empfehlungen wegen des Vertrauens in die Fähigkeiten der Technik ohne übernommen werden, dazu Busche, (Fn. 59), 899, 903.

116 Englisch und Schuh, (Fn. 64), 155, 159.

117 Krönke, (Fn. 3), i.E.; dazu auch Guggenberger, (Fn. 32), 844, 848.

118 Pilniok, (Fn. 6), 1021, 1025.

119 EuGH, Urt. v. 21.6.2022 – C-817/19, Rn. 195, juris.

Einzelne eine Befundprüfung verlangen und werde der gemessene Wert von vornherein um einen die systemimmanenten Fehler erfassenden Toleranzwert reduziert.[120] Der Nutzen der Rohmessdaten für die Überprüfung des Messwertes werde aus technischer Sicht kontrovers beurteilt, außerdem würde der Anspruch auf Verfügbarmachung gewisser Informationen durch den Beschleunigungsgrundsatz sowie den Gedanken der Rechtsanwendungsgleichheit begrenzt.[121] Demgegenüber vertrat der VerfGH des Saarlandes 2019 den Standpunkt, dass staatliches Handeln, so gering belastend es im Einzelfall auch sein mag und trotz Bedarfs nach routinisierten Entscheidungen nicht undurchschaubar für den Bürger sein darf und dieser nicht einfach darauf verwiesen werden dürfe, alles werde schon seine Richtigkeit haben. Vielmehr würde die grundsätzliche Nachvollziehbarkeit technischer Prozesse mit der Folge belastender Erkenntnisse über einen Bürger sowie ihre staatsferne Prüfbarkeit zu den Grundvoraussetzungen eines freiheitlich-rechtsstaatlichen Verfahrens gehören.[122] Schon um auf der sicheren Seite zu stehen, sind daher mögliche Dokumentationen und Protokollierungen bei steuernden KI-Anwendungen unbedingt zu empfehlen.

Letztlich hängt es von der Konzeption der KI-Anwendung samt den bestehenden Kontrollmöglichkeiten ab, ob den Anforderungen eines effektiven gerichtlichen Rechtsschutzes noch entsprochen werden kann. Der vollständig automatisierte Erlass gebundener Verwaltungsentscheidungen durch eine KI bereitet aus der Perspektive des Rechtsschutzes weniger Probleme als eine klassische Ermessensentscheidung im Einzelfall. Während bei gebundenen Entscheidungen nach dem deutschen Recht eine Ergebniskontrolle in Gestalt einer prinzipiellen Vollkontrolle durch eigene Überzeugungsbildung des Gerichts erfolgt,[123] sind die Gerichte bei derartigen Ermessensentscheidungen aus Gründen der Gewaltenteilung auf die Prüfung bestimmter Ermessensfehler beschränkt (§ 114 S. 1 VwGO). Eine solche ist jedoch nicht möglich, wenn man gar nicht weiß, wie die KI zu ihrem Ergebnis gelangt ist. Aufgrund der Komplexität der Systeme sollte der für das deutsche Recht typische Individualrechtsschutz erweitert werden, etwa durch eine Ausweitung der Klagebefugnis für spezialisierte Verbände, weil den Betroffenen oft das Wissen zur Einordnung der Systeme fehlt oder sie aus finanziellen oder auch zeitlichen Gründen von einer Inanspruchnahme gerichtlichen Rechtsschutzes absehen.[124] Jedenfalls wenn KI-Systeme aus Gründen der Schnelligkeit vollautomatisierte Entscheidungen treffen, würde es befremdlich anmuten, wenn der Rechtsschutz nachher

[120] VerfGH RP, *NZV,* (2022): 427, 429.
[121] VerfGH RP, *NZV,* (2022): 427, 429 f.
[122] VerfGH Saarland, *NJW,* (2019): 2456, 2458.
[123] Michael Goldhammer, «Vorb. § 43», in *VwVfG*, hrsg. Friedrich Schoch und Jens-Peter Schneider (München: C.H. Beck, 2. EL April, 2022), Rn. 14d.
[124] Hoffmann-Riem, (Fn. 12), 207 f.; Kment und Borchert, (Fn. 59), Rn. 272; s.a. Guckelberger, (Fn. 6), Rn. 533.

ebenfalls unter Verweis auf den Beschleunigungsgedanken und die Funktionsfähigkeit der Rechtspflege beschnitten würde.[125] Zumindest bei solchen Entscheidungen erblickt man in der nachträglichen menschlichen Kontrolle eine zunehmend sich verbreitende Sicherung gegenüber dem KI-Einsatz,[126] die idealer Weise bereits auf der Ebene der Verwaltung, etwa in Gestalt des Widerspruchsverfahrens oder bei Realakten in anderen Form, vorzusehen ist.[127]

Eifert hat jüngst zu Recht darauf aufmerksam gemacht, dass durch die zu starke Fixierung auf das Produkt KI die Nutzungskontexte vernachlässigt werden, die für die rechtliche Beurteilung des Einsatzes einer KI-Anwendung von großer Bedeutung sind.[128] Dabei kommt dem Grundsatz der Verhältnismäßigkeit eine zentrale Bedeutung zu.[129] Je schwerwiegender eine Entscheidung für den Betroffenen mit ggf. irreversiblen Folgen wirkt und je eingeschränkter die Begründungsmöglichkeiten sind, desto schwieriger wird der KI-Einsatz zu legitimieren sein, da das Motiv der Verwaltungseffizienz von vergleichsweise schwachem Gewicht ist.[130] Ob die damit ebenfalls angestrebte Verringerung der Quote an Fehlentscheidungen mit einem etwas höheren Gewicht einzustellen ist,[131] dürfte von der Konzeption und Verlässlichkeit der jeweiligen KI-Technologie abhängen. Ein KI-Einsatz für stark persönlichkeitsbezogene Entscheidungen mit gravierenden Grundrechtseingriffen dürfte daher regelmäßig ausscheiden.[132] Demgegenüber könnten KI-geleitete Verkehrssysteme, die eindeutig besser gegenüber den herkömmlichen Methoden sind, angesichts des besseren Schutzes von Leib und Leben (Art. 2 Abs. 2 S. 1 GG) zulässig sein und etwaige Bedenken im Hinblick auf die demokratische Legitimation und geringere Nachvollziehbarkeit unter Verweis auf das Output zurücktreten lassen.[133] Auch der Einsatz von KI-basierten Chatbots, die auf einfache Fragen Auskünfte geben, dürfte mangels bezweckten Eingriffs in die Rechte des Bürgers sowie der Abgabe reiner Wissenserklärung regelmäßig möglich sein.[134] Bei der rechtlichen Beurteilung ist zudem einzustellen, welche Schutzvorkehrungen im Hinblick auf die Nachteile der KI getroffen wurden. Zu denken ist etwa an Kennzeichnungen der

125 S. dazu Annette Guckelberger, „Anmerkung zu VGH Rheinland-Pfalz, Beschl. v. 22.7.2022 – VGH B 30/21," *LTZ,* (2022): i.E.
126 Eifert, (Fn. 23), i.E.; zur menschlichen Entscheidung möglicherweise durch die Rechtsprechung Mund, (Fn. 33), 235.
127 S. dazu eingehend Guckelberger, (Fn. 6), Rn. 553 ff.; Schröder, (Fn. 36), 328 341.
128 Eifert, (Fn. 23), i.E.
129 S.a. Ruschemeier, (Fn. 3), i.E.; dazu, dass sich die Abwägungen kaum verallgemeinern lassen, Guckelberger, (Fn. 6), Rn. 631.
130 Eifert, (Fn. 23), i.E.
131 Eifert, (Fn. 23), i.E.
132 Eifert, (Fn. 23), i.E.
133 Ähnlich Eifert, (Fn. 23), i.E.; dazu, dass ggf. über die Heranziehung alternativer Legitimationsmodi nachzudenken ist, Schröder, (Fn. 36), 328, 334.
134 Guckelberger, (Fn. 6), Rn. 631.

KI, die auch dazu beitragen können, dass die menschlichen Amtswalter in der Verwaltung sich der Besonderheiten der jeweiligen Technologie bewusst sind. Da solche Kennzeichnungen zumeist unproblematisch möglich sind, sollten diese auch unabhängig von der Frage nach ihrer Erforderlichkeit zur Risikokontrolle erfolgen,[135] falls der KI-Einsatz nicht ausnahmsweise aufgrund der Umstände und des Einsatzkontextes offensichtlich ist.[136] Weil die an das Handeln menschlicher Amtswalter anknüpfende Amtshaftung im Falle eines KI-Einsatzes für den Betroffenen mit erheblichen Nachteilen einhergeht, da sich Erwägungen zur Amtspflichtverletzung und zum Verschulden oft nicht mehr anstellen lassen, sind haftungsrechtliche Nachjustierungen geboten.[137]

G. Regulierung von KI

Abgesehen von wenigen bereichsspezifischen Regelungen für KI-Anwendungen, wie für das autonome Fahren, unterfallen diese zurzeit den allgemeinen Vorschriften, etwa aus dem Datenschutzrecht oder über vollständig automatisierte Verwaltungsakte. Um zu erörtern, ob weitere Regulierungen der KI notwendig sind, soll daher zuerst ein Blick auf diese geworfen werden.

I. DSGVO-Vorgaben

Art. 22 DSGVO ist technologieneutral formuliert.[138] Deshalb gilt er auch für die Verarbeitung personenbezogener Daten unter Verwendung von KI-Systemen.[139] Nach seinem Wortlaut gewährt Art. 22 Abs. 1 DSGVO der betroffenen Person ein Recht darauf, dass sie nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen wird, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Diese Vorschrift steht nach ihrem Wortlaut bloß automationsgestützten Entscheidungen nicht entgegen.[140] Nach der Ratio des Art. 22 Abs. 1 DSGVO ist jedoch auch dann von einer vollautomatisierten Entscheidung auszugehen, wenn die Entscheidung des IT-Systems von einem menschlichen Amtswalter ohne Ausübung tatsächlicher

135 S.a. Eifert, (Fn. 82), 33.
136 Michael Backes, „Stellungnahme anlässlich der öffentlichen Anhörung am 26. September 2022 zur „EU-Verordnung zu Künstlicher Intelligenz unter Einbeziehung von Wettbewerbsfähigkeit im Bereich Künstliche Intelligenz und Blockchain-Technologie," Ausssschuss-Drs. 20(23)83, 7.
137 Ruschemeier, (Fn. 3), i.E.; s.a. Mario Martini undHannah Ruschemeier, „Künstliche Intelligenz als Instrument des Umweltschutzes," *ZUR,* (2021): 515, 521; eingehend Mario Martini, Hannah Ruschemeier, Jonathan Hain, „Staatshaftung für automatisierte Verwaltungsentscheidungen – Künstliche Intelligenz als Herausforderung für das Recht der staatlichen Ersatzleistungen," *VerwArch,* 112 (2021): 1, 32 ff.
138 Ruschemeier, (Fn. 3), i.E.
139 Pilniok, (Fn. 6), 1021, 1029.
140 Guckelberger, (Fn. 6), Rn. 83; Mayrhofer und Parycek, (Fn. 12), 74.

Entscheidungsmacht bloß übernommen wird.[141] Art. 22 Abs. 1 DSGVO gilt nach zutreffender, aber umstrittener Meinung auch für begünstigende Entscheidungen.[142] Während vollautomatisierte Entscheidungen, die der betroffenen Person gegenüber rechtliche Wirkungen entfalten, insbesondere Verwaltungsakte sind,[143] unterfallen Realakte Art. 22 Abs. 1 Var. 2 DSGVO.[144]

Jedoch folgt aus Art. 22 Abs. 2–4 DSGVO die Zulässigkeit automatisierter Entscheidungen im Einzelfall, etwa wenn die betroffene Person ausdrücklich einwilligt (Abs. 2 lit. c). Ferner können solche Entscheidungen aufgrund Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zugelassen werden, allerdings nur, wenn die Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten (Abs. 2 lit. b). In Erwägungsgrund 71 Abs. 1 S. 3 heißt es dazu: „In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung." Da Art. 22 Abs. 3 DSGVO nicht auf Abs. 2 lit. b Bezug nimmt, ist streitig, ob die dortigen Aussagen auch auf öffnende Rechtsvorschriften der Union bzw. Mitgliedstaaten entsprechende Anwendung finden.

Ferner hat der Verantwortliche nach Art. 35 Abs. 1 S. 1 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen, sofern aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen folgt. Angesichts der Formulierung „insbesondere bei Verwendung neuer Technologien" in Art. 35 Abs. 1 S. 1 DSGVO kann eine solche Datenschutz-Folgenabschätzung bei KI-Anwendungen geboten sein.[145]

II. Vollautomatisierte Verwaltungsakte

Mit Wirkung zum 1.1.2017 hat der Bundesgesetzgeber § 35a VwVfG eingefügt, wonach ein Verwaltungsakt vollständig durch automatische Einrichtungen erlassen

---

141 Guckelberger, (Fn. 6), Rn. 197; Marcus Helfrich, «Art. 22 DS-GVO», in *DS-GVO/BDSG*, hrsg. Gernot Sydow und Nikolaus Marsch, 3. Aufl. (Baden-Baden: Nomos, 2022), Rn. 44; Pilniok, (Fn. 6), 1021, 1029.

142 Guckelberger, (Fn. 6), Rn. 197; Helfrich, (Fn. 141), Art. 22 DSGVO Rn. 49; s.a. Mayrhofer und Parycek, (Fn. 12), 74 f.

143 Kai v. Lewinski, «Art. 22 DS-GVO», in *BeckOK Datenschutzrecht*, hrsg. Heinrich A. Wolff und Stefan Brink, 41. edn. (München: C.H. Beck, 2022), Rn. 30; Mayrhofer und Parycek, (Fn. 12), 74.

144 V. Lewinski, (Fn. 143), Art. 22 Rn. 37 ff.; s.a. Helfrich, (Fn. 141), Art. 22 DS-GVO Rn. 51.

145 Mario Martini, «Art. 35 DS-GVO», in *DS-GVO/BDSG*, hrsg. Boris P. Paal und Daniel A. Pauly, 3. Aufl. (München: C.H: Beck, 2021), Rn. 18; s.a. Kment und Borchert, (Fn. 59), Rn. 171.

werden kann, sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht. Durch das Erfordernis der Zulassung durch Rechtsvorschrift wollte man den Anforderungen von Art. 22 Abs. 2 lit. b DSGVO Rechnung tragen. Angesichts der technikoffenen Formulierung ist der Erlass solcher Verwaltungsakte auch durch KI-Systeme denkbar.[146] Je nachdem, ob es sich bei dem Einsatz einer KI-Anwendung um eine Entscheidung i.S.d. Wesentlichkeitstheorie handelt, bedarf es dafür einer parlamentsgesetzlichen expliziten oder impliziten Zulassung.[147] Solange „gewöhnliche" IT-Systeme unter Vermeidung gewisser Gefahren von KI-Systemen derartige Verwaltungsakte von gleicher Qualität und ebenso effektiv erlassen können, besteht zumeist kein plausibler Grund für den Einsatz von KI-Anwendungen.[148]

Die Sinnhaftigkeit des kategorischen Ausschlusses vollständig automatisierter Verwaltungsakte bei Ermessensnormen und Beurteilungsspielräumen ist umstritten. Darin liegt eine „politische Entscheidung als Ausdruck der Vorsicht",[149] um wertende Entscheidungen menschlichen Amtswaltern vorzubehalten.[150] Andere halten § 35a VwVfG für zu eng.[151] Bei manchen Ermessensnormen, bei denen auch der Gesetzgeber eine gleichmäßige Ermessensausübung für möglich erachte, seien vollautomatisierte Entscheidungen durchaus denkbar.[152] Anders verhalte es sich dagegen bei Rechtsvorschriften, bei denen durch das Ermessen gerade individuelle Fallmerkmale berücksichtigt werden sollen,[153] etwa wo die Verwaltung aufgrund der Vielschichtigkeit der Sachverhalte einzelfallsensibel auf besondere Härten reagieren soll.[154] Manche Landesgesetzgeber haben daher von der Aufnahme einer vergleichbaren Vorschrift zu § 35a VwVfG in ihr Verwaltungsverfahrensgesetz abgesehen. So regelt Art. 12 Abs. 3 Bayerisches Digitalgesetz lediglich, dass ein sofortiger Vollzug vollständig automatisiert erlassener Verwaltungsakte nur aufgrund einer gesetzlichen Ermächtigung zulässig ist. Auch kann der Fachgesetzgeber gegenüber § 35a VwVfG speziellere Regelungen erlassen. Als Paradebeispiel für automatisierte Ermessensentscheidungen werden intelligente Verkehrsbeeinflussungssysteme genannt.[155]

---

146 Kment und Borchert, (Fn. 59), Rn. 48; Wischmeyer, (Fn. 4), § 20 Rn. 65.
147 Wegen des ungleich höheren Gefährdungspotenzials von KI muss nach Guggenberger, (Fn. 32), 844, 846 der Erlaubnisvorbehalt erst recht gelten.
148 Wischmeyer, (Fn. 4), § 20 Rn. 65; s.a. Guckelberger, (Fn. 6), Rn. 576.
149 Ziekow und Engewald, (Fn. 43), 23.
150 Hornung, (Fn. 24), § 35a Rn. 31; Mund, (Fn. 33), 141 ff.
151 Schröder, (Fn. 36), 328, 332 f.
152 Herold, (Fn. 72), 220 ff.; Tischbirek, (Fn. 14), 307, 324.
153 Herold, (Fn. 72), 221.
154 In diese Richtung Tischbirek, (Fn. 14), 307, 324.
155 Djeffal, (Fn. 9), 479, 486; Alexander Tischbbirek, „Ermessensdirigierende KI," *ZfDR,* (2021): 307, 314.

III. Weiterer Regulierungsbedarf

Abgesehen von wenigen Ausnahmen konnte man sich bislang auf keine allgemeinen Regelungen für KI-Anwendungen verständigen. Stattdessen begnügte man sich vor allem mit Kodizes zur Selbstregulierung sowie politischen Erklärungen.[156] Durch bloßes soft law kann aber den Gefahren staatlicher KI-Anwendungen für die Grundrechte nicht wirksam begegnet werden.[157] Das Zögern hinsichtlich des Erlasses solcher Vorschriften dürfte mehrere Ursachen haben, etwa dass man eine ausschließlich nationale Regulierung nicht für zielführend erachtet, man sich in einer Wettbewerbssituation befindet oder aber auch Entwicklungen bei den KI-Technologien schwer abschätzbar sind.[158] Nachdem im November 2021 die UNESCO-Empfehlung zur Ethik der Künstlichen Intelligenz von 193 UNESCO-Mitgliedstaaten verabschiedet wurde, begannen die Vertragsstaaten des Europarates im September 2022 Verhandlungen über eine Konvention für Künstliche Intelligenz, Menschenrechte, Demokratie und Rechtsstaatlichkeit.[159]

Um den Mehrwert von KI-Anwendungen und dahinter stehende Potenziale nicht unnötig zu blockieren,[160] sollten die rechtlichen Rahmenbedingungen so gestaltet werden, dass positive Entwicklungen unterstützt und ihre negativen Auswirkungen oder Gefahren vermieden werden.[161] Angesichts der Bandbreite denkbarer KI-Anwendungen deutet bereits der Grundsatz der Verhältnismäßigkeit auf keine „one size fits all"-Lösung hin.[162] In jüngerer Zeit hat sich z.B. eine Forschergruppe des European Law Institutes für die Einführung eines KI-Folgenabschätzungsverfahrens ausgesprochen, das jedoch bei KI-Systemen mit einem offensichtlich geringen Risiko, wie Chatbots, oder weit verbreiteten Systemen mit bekannten und leicht zu handhabenden Risiken keine Anwendung finden soll.[163] Sachbereichsspezifischen Besonderheiten von KI-Anwendungen lässt sich am besten im Fachrecht Rechnung tragen.[164]

---

156 Kment und Borchert, (Fn. 59), Rn. 184 ff.; allgemein zur Algorithmenregulierung Indra Spiecker gen. Döhmann, «Staatliche oder private Algorithmenregulierung?», Bitburger Gespräche Jahrbuch 2020, (München: C.H. Beck, 2021), 37 ff.

157 Kment und Borchert, (Fn. 59), Rn. 191.

158 In diese Richtung allerdings bezogen auf Zertifizierungen Spiecker gen. Döhmann, (Fn. 156), 37, 50.

159 BT-Drs. 20/4413, 2.

160 Wischmeyer, (Fn. 4), § 20 Rn. 6; in diese Richtung auch Kment und Borchert, (Fn. 59), Rn. 218; zum Verbot bei unverhältnismäßigen Risiken Englisch und Schuh, (Fn. 64), 155, 187 f.

161 Mayrhofer und Parycek, (Fn. 12), 1; ähnlich Hoffmann-Riem, (Fn. 12), 194; zum Recht als Grund, Grenze und Gestaltung von Technik Djeffal, (Fn. 40), 51, 58.

162 Hoffmann-Riem, (Fn. 12), 190; s.a. Kment und Borchert, (Fn. 59), Rn. 177.

163 Report of the European Law Institute, Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration, 40.

164 Krönke, (Fn. 3), i.E.

IV. Vorschlag einer KI-Verordnung

Am 21.4.2021 hat die EU-Kommission einen Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (im Folgenden: VO-E) vorgelegt, die von dieser insbesondere auf die Art. 16 und 114 AEUV abgestützt wird.[165] Bereits der Kompetenztitel deutet darauf hin, dass die EU-Kommission die KI-Regulierung als Produktsicherheitsrecht begreift.[166] In einer solchen unionsweiten Regelung wird u.a. ein wichtiger Beitrag hin zu mehr Rechtssicherheit bei KI-Systemen gesehen.[167] Die geplante Verordnung soll für KI-Anwendungen aus dem privaten und öffentlichen Sektor gelten.[168] Der Begriff der KI wird in dem Verordnungsentwurf technologieneutral weit verstanden.[169] Nach Art. 3 Nr. 1 VO-E ist ein KI-System eine Software, die mit einer oder mehreren der im Anhang 1 aufgeführten Techniken und Konzepte entwickelt wurde (Nr. 1 Techniken maschinellen Lernens, Nr. 2 Logik- und wissensgestützte Systeme sowie Nr. 3 statistische Ansätze), und im Hinblick auf eine Reihe menschlich festgelegter Ziele Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren. Während mancherorts die Weite der Legalumschreibung begrüßt wird, weil auch „normale" Software überaus komplex sein kann, wird sie von anderen als zu weit kritisiert.

Der VO-E verfolgt einen risikobasierten Regelungsansatz.[170] Art. 5 Abs. 1 VO-E enthält eine Aufzählung verbotener Praktiken, u.a. in lit. c die des Inverkehrbringens, der Inbetriebnahme oder Verwendung von KI-Systemen durch Behörden oder in deren Auftrag zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen auf der Grundlage ihres sozialen Verhaltens oder bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, die zu bestimmten Ergebnissen führt (sog. Verbot des social scoring), oder in lit. d die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, wovon aber wiederum gewisse Ausnahmen zugelassen werden.[171] Ansonsten geht der VO-E von der grundsätzlichen Zulässigkeit von KI aus, normiert aber je nach Zuordnung zu bestimmten Risikoklassen besondere Anforderungen. So müssen die sog. Hochrisiko-KI-Sys-

---

165 COM (2021) 206 final, 20 ff.

166 Eifert, (Fn. 23), i.E.

167 Backes, Aussschuss-Drs. 20 (23) 83, 4; s. zu den Zielen auch Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung Harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung Bestimmter Rechtsakte der Union, COM (2021) 206 final, 3.

168 Pilniok, (Fn. 6), 1021, 1027.

169 Seckelmann, «Verwaltungshandeln in sozialen Netzwerken», in *Herausforderungen für das Verwaltungsrecht*, hrsg. Hermann Hill und Veith Mehde, (Berlin: Duncker & Humblot, 2023), i.E.

170 COM (2021) 206 final, 8; Ruschemeier, (Fn. 3), i.E.

171 Näher dazu Ruschemeier, (Fn. 3), i.E. sowie Margrit Seckelmann, „Künstliche Intelligenz in der Verwaltung. Der Entwurf einer europäischen KI-Verordnung und der Umgang mit informationstechnischen Risiken," *Die Verw.,* (2023): 1, 29, i.E.

teme die in Art. 8 ff. VO-E festgelegten Anforderungen erfüllen. Zu den Hochrisiko-KI-Systemen gehören auch die in Anhang III genannten KI-Systeme (Art. 6 Abs. 2 VO-E). Unter diese fallen u.a. KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten in der Verwaltung verwendet werden sollen (Nr. 2a), aus dem Bereich der allgemeinen und beruflichen Bildung (Nr. 3) oder KI-Systeme, die bestimmungsgemäß von Behörden oder in deren Namen für die Beurteilung verwendet werden sollen, ob natürliche Personen öffentliche Unterstützungsleistungen und -dienste beanspruchen können und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind (Nr. 5 lit. a). Unabhängig davon stellt Art. 52 VO-E Transparenzpflichten für bestimmte KI-Systeme auf.

Ende September 2022 hat die Kommission den Entwurf einer umfassenden Überarbeitung der Produkthaftungsrichtlinie sowie einer neuen Richtlinie über KI-Haftung[172] vorgelegt. Im November 2022 haben die Mitgliedstaaten, das EU-Parlament und die EU-Kommission ihre Verhandlungen über eine interinstitutionelle Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade abgeschlossen, die aber noch der Billigung von Rat, Kommission und Parlament bedarf.[173] Es bleibt abzuwarten, welchen Fortgang insbesondere der Entwurf der KI-Verordnung nehmen wird. Laut einer Antwort des Parlamentarischen Staatssekretärs *Straßer* vom 27.10.2022 sollte aus Sicht der Bundesregierung den Besonderheiten von KI-Systemen im Bereich der öffentlichen Verwaltung durch einen separaten, gesonderten Technologierechtsakt oder jedenfalls durch ein gesondertes Kapitel mit jeweils abschließendem Regelungsinhalt Rechnung getragen werden.[174] In der Sachverständigenanhörung vor dem zuständigen Bundestagausschuss wurde u.a. geäußert, dass für bestimmte Einsätze von Hochrisiko-KI-Systemen Opt-out-Möglichkeiten oder ein Beschwerderecht zur Überprüfung der Entscheidung bedenkenswert wäre.[175]

[172] Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM (2022) 496 final. Dazu, dass die dort vorgesehene Offenlegung von Beweismitteln und widerlegbare Vermutung eines Verstoßes nur in eingeschränktem Maße die Defizite bei der Staatshaftung zu überwinden vermag, Krönke, (Fn. 3), i.E.
[173] Council of Europe, Pressemitteilung 942/22 v. 14.11.2022, Erklärung zu digitalen Rechten und Grundsätzen: Werte und Bürgerinnen und Bürger der EU im Mittelpunkt des digitalen Wandels.
[174] BT-Drs. 20/4209, 49; zur Notwendigkeit der Unterscheidung zwischen eng gebundener staatlicher Herrschaft und dem privaten Sektor auch Eifert, (Fn. 23), i.E.
[175] Backes, Aussschuss-Drs. 20(23)83, 5.

V. Nationale KI-Regulierung

Die EU-Kommission hat ihren VO-E vorgelegt, weil einige Mitgliedstaaten zur Gewährleistung sicherer KI-Systeme und Einhaltung der Grundrechte den Erlass nationaler Vorschriften in Erwägung ziehen, womit aber eine Fragmentierung des Binnenmarktes in wesentlichen Fragen sowie eine erheblich geringere Rechtssicherheit verbunden sei.[176] Da der Erlass solcher Vorschriften aber längere Zeit in Anspruch nimmt, ist es nicht verwunderlich, dass zwei Bundesländer vorgeprescht sind. Versteht man unter Verwaltungsverfahren strukturierte Vorgänge der Informationsgewinnung und -verarbeitung, kann der Bund aufgrund Art. 84 Abs. 1 GG nur in Ausnahmefällen Regelungen zu KI-Systemen treffen, die dem Länderzugriff kategorisch entzogen sind.[177] Ferner sei auf den im Bereich der Verwaltungszusammenarbeit verorteten Art. 91c GG über informationstechnische Systeme hingewiesen. Ob und inwieweit Regelungen durch den Parlamentsgesetzgeber notwendig sind, richtet sich nach der Grundrechtsrelevanz bzw. Wesentlichkeit der KI-Anwendungen.[178]

1. Bayerisches Digitalgesetz

Obwohl im Anhörungsverfahren zum Bayerischen Digitalgesetz (BayDiG) v. 22.7.2022 vertreten wurde, dass u.a. wegen des mit KI-Systemen einhergehenden Eingriffs in das Recht auf informationelle Selbstbestimmung deren Einsatz einer parlamentarischen Rechtsgrundlage bedürfe und man dabei auf den bisherigen Erkenntnis- und Diskussionsstand aufbauen könne,[179] finden sich dort nur wenige Regelungen. Der im Laufe des Gesetzgebungsverfahrens eingefügte Art. 5 Abs. 2 S. 2 BayDiG, wonach der Einsatz von KI in der Verwaltung durch geeignete Kontroll- und Rechtsschutzmaßnahmen abzusichern ist, enthält nur eine sehr allgemein gehaltene Konkretisierung der verfassungsrechtlichen Anforderungen und lässt im Übrigen offen, wann von einer KI auszugehen ist. Art. 21 BayDiG ermöglicht erstmals die Zulassung digitaler Assistenzdienste von privaten Dienstanbietern außerhalb der Steuerverwaltung, in deren Bereich die Verwaltung Schnittstellen offenlegt, damit private Softwareanbieter ihre Dienste zur Erleichterung der elektronischen Steuererklärung anbieten können.[180] Die Staatsministerien können beim Angebot digitaler Verwaltungsleistungen den Einsatz *nicht amtlicher* digitaler Assistenzdienste gewerblicher Art durch Bekanntmachung zulassen.

---

[176] COM (2021) 206 final, 7.
[177] Pilniok, (Fn. 6), 1021, 1028.
[178] S.a. Schröder, (Fn. 34), 269, 271; gegen die Annahme eines allgemeinen technologiespezifischen Gesetzesvorbehalts Krönke, (Fn. 3), i.E.
[179] Dirk Heckmann, Sarah Rachut und Alexander Besner, „Gutachterliche Stellungnahme für den Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung im Bayerischen Landtag zum Gesetzentwurf der Staatsregierung über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG)," (2022), 22 f.
[180] Bayerischer Landtag, BayLT-Drs. 18/19572, 35.

2. IT-Einsatz-Gesetz Schleswig-Holstein

Das im Frühjahr 2022 erlassene schleswig-holsteinische IT-Einsatz-Gesetz (ITEG) enthält dagegen sehr ausführliche Regelungen für die öffentlich-rechtliche Verwaltungstätigkeit im Land Schleswig-Holstein (§ 1 Abs. 1 ITEG). Dadurch soll bei Einsatz datengetriebener Informationstechnologien die Wahrung des Rechts auf informationelle Selbstbestimmung sowie der Prinzipien des Vorrangs des menschlichen Handelns, der menschlichen Aufsicht und Verantwortlichkeit, der Transparenz, der technischen Robustheit und Sicherheit, der Vielfalt, Nicht-Diskriminierung, Fairness sowie des gesellschaftlichen und ökologischen Wohlergehens sichergestellt werden (§ 1 Abs. 2 ITEG). Aus Platzgründen kann der Inhalt dieses Gesetzes nur knapp wiedergegeben werden. Auch wenn dieses Gesetz an datengetriebenen Informationstechnologien anknüpft, hat es vor allem KI-Technologien im Visier. Nach der Legaldefinition datengetriebener Informationstechnologien in § 3 Abs. 1 Nr. 1 ITEG handelt es sich dabei um bestimmte Anwendungen, die zur effizienten Lösung einer speziellen Aufgabe oder einer komplexen Fragestellung auf der Grundlage eines Datensatzes mit Hilfe spezieller Systeme, wie künstlicher neuronaler Netze und maschineller Lernverfahren, eingesetzt werden und ohne aktiven Eingriff Parameter der Entscheidungsfindung weiterentwickeln.

§ 2 Abs. 2 S. 1 ITEG enthält eine abschließende Aufzählung von Anwendungsbereichen, in denen deren Einsatz unzulässig ist. Dazu gehört der Erlass eines Verwaltungsakts bei Bestehen eines Ermessens oder Beurteilungsspielraums (Nr. 4), die massenweise Identifikation von Personen bei Versammlungen oder Veranstaltungen anhand biometrischer Merkmale (Nr. 3), die Ausübung unmittelbaren Zwangs gegen das Leben und die Gesundheit natürlicher Personen im Verwaltungsvollzug (Nr. 1) sowie die Verarbeitung personenbezogener Daten zwecks Beurteilung der Persönlichkeit, der Arbeitsleistung, der physischen und psychischen Belastbarkeit, der kognitiven oder emotionalen Fähigkeiten von Menschen sowie der Erstellung von Prognosen über die Straffälligkeit einzelner Personen oder Personengruppen (Nr. 2). Wegen der Gesetzgebungskompetenz des Bundes für die Strafverfolgung(svorsorge) gem. Art. 74 Abs. 1 Nr. 1 GG ist äußert zweifelhaft, ob das Land eine Regelung hinsichtlich der Straffälligkeit treffen durfte.[181] § 5 Abs. 1 S. 1 ITEG verlangt eine Klassifizierung der jeweiligen datengetriebenen Informationstechnologie zu den in § 3 Abs. 2 benannten Automationsstufen: Stufe 1 (Assistenzsystem), Stufe 2 (Delegation) oder Stufe 3 (Automation). Gem. § 5 Abs. 1 S. 2 ITEG soll die Zuordnung zur jeweiligen Stufe zur Beurteilung von Risiken sowie für die Auswahl geeigneter technischer oder organisatorischer Maßnahmen herangezogen werden. § 5 Abs. 2 ITEG regelt die Übernahme der Erfüllung der Aufgaben durch einen menschlichen Amtswalter, etwa bei Hinweisen des Antragstellenden auf gewichtige Umstände, die einer automatisierten Bearbeitung entgegenstehen (Nr. 1), oder der Meldung eines Problems bei der Aufgabenbearbeitung (Nr. 2). Nach Satz 2

[181] Für diesen Hinweis möchte ich mich bei Dr. Franziska Lind bedanken.

muss jederzeit die Möglichkeit zur Abschaltung der Informationstechnologie oder zur Übernahme der Bearbeitung durch einen Beschäftigten bestehen.

Grundsätzlich müssen Behörden den Algorithmus von datenbasierten Informationstechnologien und die dieser zugrundeliegenden Datenbasis offenlegen, außer der Schutz personenbezogener Daten, sonstiger Rechte Dritter oder öffentlicher Interessen stehen entgegen (§ 6 Abs. 1 S. 1 ITEG). Gem. § 6 Abs. 3 ITEG sind beim Einsatz solcher Technologien zu Kommunikationszwecken oder vergleichbaren Aktivitäten die Beteiligten vorab zweifelsfrei in verständlicher Form auf die Kommunikation mit einem IT-System hinzuweisen und es muss daneben eine alternative Kommunikationsform ermöglicht werden, die sich unmittelbar auf menschliches Handeln zurückführen lässt. Nach Absatz 4 ist Entscheidungen, insbesondere Verwaltungsakten, ein Hinweis auf die teilweise oder vollständige Bearbeitung und gegebenenfalls Entscheidungsfindung mittels datengetriebener Informationstechnologien hinzuzufügen. Fehlt ein Hinweis i.S.d. Absatzes 4 oder ist dieser unvollständig, führt dies zur Nichtigkeit bei Verwaltungsakten mithilfe oder aufgrund datengetriebener Informationstechnologien der Stufen 2 oder 3 (§ 6 Abs. 5 ITEG). § 7 ITEG regelt die menschliche Aufsicht sowie die Abänderbarkeit der KI-Entscheidungen durch zuständige Beschäftigte. Während § 8 ITEG Vorgaben in Bezug auf die Datengrundlage und Verarbeitung personenbezogener Daten macht, sind nach § 9 Abs. 1 ITEG umso umfangreichere Maßnahmen zur Gewährleistung der Beherrschbarkeit der datengetriebenen Informationstechnologien zu ergreifen, je höher der Automationsgrad eingestuft wird. § 10 ITEG betrifft die Sicherheit, Robustheit und Resilienz.

Auf großes Interesse dürfte die in § 12 ITEG vorgesehene KI-Rüge stoßen, da diese nach Absatz 3 Satz 1 als niederschwelliger und kostenfreier Rechtsbehelf ausgestaltet wurde. Danach kann jeder Adressat einer auf datengetriebenen Informationstechnologie der Automationsstufe 2 oder 3 beruhenden Entscheidung innerhalb eines Monats ab Bekanntgabe die Überprüfung und Bestätigung, Änderung oder Aufhebung der Entscheidung durch eine natürliche Person verlangen (§ 12 Abs. 1 S. 1 ITEG). Dabei bleibt die Möglichkeit der Einlegung anderer Rechtsbehelfe unberührt, ab Einlegung eines förmlichen Rechtsbehelfs ist die KI-Rüge allerdings unzulässig und andere Rechtsbehelfe gehen im Zweifel vor (§ 12 Abs. 1 S. 4–7 ITEG). Bei einer KI-Rüge gegen einen Verwaltungsakt gilt dieser gem. § 12 Abs. 2 ITEG als nicht bekannt gegeben und ein neuer Verwaltungsakt darf ausschließlich durch eine natürliche Person erlassen werden. Es bleibt abzuwarten, ob sich die verfahrensrechtlichen Sondervorschriften zur Nichtigkeit eines Verwaltungsakts bei Unterbleiben eines Hinweises sowie zu ihrer Nichtbekanntgabe bei einer KI-Rüge als sinnvoll und praktikabel erweisen werden.

H. Fazit

Der Erlass von rechtlichen Regelungen zur Einhegung von KI-Anwendungen wird immer wahrscheinlicher. Wie der VO-E der EU-Kommission und das ITEG zeigen, setzt man auf eine risikobasierte Regulierung. Besonders gefährliche KI-Anwendungen sollen aus Gründen des Grundrechtsschutzes unterbleiben. Im Übrigen sollen diese zum Einsatz gelangen können, unterliegen aber je nach Einstufung mehr oder minder strengen Anforderungen. Gerade der Blick auf das ITEG bestätigt, dass organisatorische Maßgaben und Verfahrensanforderungen Instrumente zur rechtlichen Einhegung sind. Sollte auf Unionsebene eine vollharmonisierende Regelung getroffen werden, würden die Mitgliedstaaten dadurch am Erlass strengerer Regelungen gehindert.[182] Im Übrigen setzt der Einsatz von KI auf Seiten der Verwaltung ausreichende personelle Kapazitäten sowie entsprechende fachliche Expertise voraus.[183] Damit das Vertrauen in den Staat und die Verwaltung nicht leidet, sind alle notwendigen Anstrengungen zu unternehmen, damit keine Vielzahl fehlerhafter Entscheidungen infolge des Einsatzes von KI-Technologien getroffen wird.

[182] Hoffmann-Riem, (Fn. 12), 157.
[183] BT, (Fn. 3), 13.

Künstliche Intelligenz und dynamische Rechtsetzung

Michael Mayrhofer, Michael Denk

A. KI und Rechtsetzung – eine Herausforderung

Die Implikationen der als Künstliche Intelligenz (KI) zusammenfassend bezeichneten Technologien auf alle Bereiche unseres Lebens werden immer deutlicher und nehmen auf rasante Weise zu. Die Palette der möglichen Einsatzfelder von KI-basierten Technologien ist breit und bunt. Sie umfasst beispielsweise medizinische Anwendungen,[1] autonom fahrende Autos, „persönliche" Assistenten, Finanz- und Versicherungsdienstleistungen, prädiktive Instrumente im E-Commerce, Auswahlalgorithmen von Social Media-Plattformen und intelligente Fabriken. Mit KI-basierten Sprachgeneratoren wie ChatGPT, Bard & Co sind zuletzt die Leistungsfähigkeit und die Risiken von KI einer breiten Öffentlichkeit schlagartig bekannt geworden.

Die Gesetzgeber sind (längst) gefordert, in geeigneter und sachgerechter Weise auf KI und den von ihr ausgelösten Wandel zu reagieren.[2] KI ist kein Naturereignis, sondern vom Menschen entwickelte und eingesetzte Technik. Sie ist daher rechtlich

[1] Vgl. dazu Emily Leckenby et al., „The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review," *Applied Health Economics and Health Policy* (2021): 857-869, abgerufen am 26. Januar 2023, https://doi.org/10.1007/s40258-021-00665-1.

[2] Michael Denk, «Aktuelles zur Digitalisierung im Verwaltungs(verfahrens)recht», in *Linzer Legistik-Gespräche 2021*, hrsg. Land Oberösterreich (Linz: Schriftenreihe des Landes Oberösterreich, 2022), 98.

DOI: https://doi.org/10.17875/gup2023-2496

steuerbar. Das Recht muss einen adäquaten Rahmen für die technologischen Entwicklungen schaffen, der Gefahren eindämmt sowie Akzeptanz und Vertrauen der Menschen in die Technologien vermittelt, ohne dabei unerwünschte oder unnötige Hindernisse für Innovationen zu etablieren. Die jeweiligen Gesetzgeber stehen dabei vor der Herausforderung, nicht nur mit der raschen technologischen Entwicklung Schritt zu halten, sondern, idealerweise, die Wirkungen, Möglichkeiten und Gefahren von KI vorherzusehen und darauf mit geeigneten rechtlichen Vorschriften zu reagieren.

Auf Ebene der Europäische Union liegt derzeit ein umfassender Entwurf eines „Gesetzes über künstliche Intelligenz“[3] (in weiterer Folge KI-VO-E) vor. Dieser Rechtsakt soll erstmalig europaweite Standards für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und Verwendung von KI festlegen. Der KI-VO-E verfolgt dabei im Wesentlichen ein dem Produktrecht ähnliches Konzept[4] und legt einen starken Fokus auf die Phase der Entwicklung von KI-Systemen,[5] wobei die Vorschriften überwiegend auf sogenannte „Hochrisiko-KI“[6] abzielen. Der KI-VO-E wird zweifelsfrei bedeutsame Vorgaben für KI-Systeme schaffen, ohne allerdings den Einsatz von KI schlechthin umfassend zu regeln. Einerseits werden die überwiegenden Regelungen bei zahlreichen KI-Anwendungen mangels Einstufung als „hochriskant“ nicht relevant sein. Andererseits ist eine KI-Anwendung regelmäßig nicht bloß isoliert ein „Produkt“, bei dem es ausschließlich auf die Entwicklung und das Inverkehrbringen oder Inbetriebnahme ankommt. Vielmehr ist für den Einsatz von KI in aller Regel ein materienrechtliches Regelungsumfeld relevant. Der Einsatz von KI in unterschiedlichen (Betriebs-)Umgebungen wird auch nach dem Inkrafttreten der KI-VO im jeweiligen Sachzusammenhang rechtliche Herausforderungen mit sich bringen, so beispielsweise im Zusammenhang mit dem Anlagenrecht, dem Verkehrsrecht, dem Energierecht, dem Arbeitsrecht, dem Finanzmarkt- und Versicherungsrecht, dem Medizinrecht oder auch dem Verfahrensrecht der Verwaltungsbehörden und Gerichte. Die (Materien-)Gesetzgeber stehen dabei vor der komplexen Aufgabe sachgerechte rechtliche Rahmenbedingungen zu etablieren und dabei der dynamischen Natur von KI-Technologien gerecht zu werden.

[3] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften Für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM/2021/206 final in der überarbeiteten Fassung des Rats der Europäischen Union vom 06.12.2022, 15698/22. Zum Zeitpunkt der Abfassung dieses Beitrags, liegen drei teilweise sehr unterschiedliche Entwürfe der Organe der Europäischen Union (Kommission, Rat und Europäisches Parlament) vor. In diesem Beitrag wird in weiterer Folge auf den Vorschlag des Rates Bezug genommen.

[4] Vgl. dazu Pkt. B.III.

[5] Vgl. zB. Art. 10, 14, 15 und 19 KI-VO-E.

[6] Vgl. Art. 6 KI-VO-E.

So können Unsicherheiten darüber bestehen, wie sich (KI-basierte) Anwendungen bei realen (Markt-)Bedingungen entwickeln.[7] Selbst die Konformität mit dem geltenden Recht ist mitunter nicht abschließend ermittelbar.[8] Nicht zuletzt scheint es äußert diffizil bzw. manchmal schier unmöglich, die Funktionsweise von komplexen KI-Systemen überhaupt nachzuvollziehen. Dies führt dazu, dass die Gesetzgeber den technologischen Entwicklungen sprichwörtlich „hinterherlaufen",[9] was mitunter mit erheblichen Rechtsunsicherheiten sowie mit Regelungsdefiziten in Gestalt von Unter- und Überregulierungen und Fehlsteuerungen verbunden sein kann. Dazu kommen Unsicherheiten und Defizite auf Ebene des Vollzugs,[10] der sich mit Technologien konfrontiert sieht, auf die sich die herkömmlichen technikrechtlichen Instrumente häufig nicht oder nicht hinreichend anwenden lassen. So wird sich in technikrechtlichen Verfahren nicht immer - beispielsweise mit „klassischen" Sachverständigengutachten – abschließend klären lassen, wie sich eine KI-basierte Anlage verhalten wird und dementsprechend rechtlich zu bewerten ist.[11]

Vor diesem Hintergrund ist es angezeigt, über neue Formen rechtlicher Techniksteuerung nachzudenken, die helfen können, ein lediglich reaktives und demnach stets zeitverzögertes sowie mitunter nicht hinreichend informiertes Handeln des Gesetzgebers zu vermeiden. Eine derart neue Form kann das Instrument des Reallabors sein, dem sich auch die KI-VO bedient (dazu unten Pkt. C.IV.1.).

Dieses ergänzt den legislativen Vorgang und zudem den administrativen „Lernprozess" um ein dynamisches Element, indem es einerseits einen provisorischen, flexiblen, schnell verfügbaren und dennoch risikominimierenden Rechtsrahmen bereitstellt und es dadurch andererseits dem Gesetzgeber ermöglicht, bei der endgültigen technikrechtlichen Regelung auf fundierte Erkenntnisse des Reallabors zurückzugreifen. Dieser Beitrag widmet sich dem Instrument des Reallabors und damit einer neuen Form dynamischer Rechtsetzung. Vorangestellt wird ein Überblick über – im österreichischen und unionalen Recht – etablierte Formen dynamischer Rechtsetzung. Den Abschluss bilden Überlegungen für die inhaltliche Ausgestaltung eines (möglichst) generischen Reallabor-Rechts.

[7] Christoph Krönke, „Die Regulatory Sandbox - Maßanfertigung oder Multifunktionstool?," *ÖZW* (2022): 3, (5).
[8] Vgl. Krönke, (Fn. 7), 3 (5).
[9] Vgl. BMWi, «Neue Räume, um Innovationen zu erproben. Konzept für ein Reallabore-Gesetz» (2021) 4, abgerufen am 26. Januar 2023, https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/konzept-fur-ein-reallabore-gesetz.pdf?__blob=publicationFile&v=6.
[10] Vgl. Krönke, (Fn. 7), 3 (5).
[11] Denk, (Fn. 2), 98.

B. Etablierte Formen dynamischer Rechtsetzung

I. Technikklauseln

Der Entwicklung von Technik begegnet das Recht schon jetzt mit dynamischen Elementen. So bedient sich der Gesetzgeber sogenannter „Technikklauseln". Dabei handelt es sich um eine Regelungstechnik, bei der abstrakt auf den aktuellen Stand der wissenschaftlichen und/oder praktisch-technischen Erkenntnisse referenziert wird. Dadurch nehmen derartige Klauseln auf den bestehenden Wissensstand in einem bestimmten Fachgebiet Bezug.[12] Technikklauseln sind unbestimmte Rechtsbegriffe, wie zum Beispiel „Stand der Technik",[13] „(allgemein) anerkannte Regeln der Technik",[14] „beste verfügbare Technik" oder „Stand der Wissenschaft".

Der österreichische Bundesgesetzgeber verzichtet beispielsweise (mit gutem Grund) darauf, die konkreten technischen, medizinischen und sonstigen Anforderungen an eine gewerbliche Betriebsanlage festzulegen, sondern verwendet zur Umschreibung der Voraussetzungen unbestimmte Begriffe. Eine Betriebsanlage darf gemäß § 77 Gewerbeordnung 1994[15] ua. nur dann genehmigt werden,

> *„wenn nach dem Stand der Technik [...] und dem Stand der medizinischen und der sonst in Betracht kommenden Wissenschaften zu erwarten ist, daß überhaupt [...] Gefährdungen [...] vermieden und Belästigungen, Beeinträchtigungen [...] auf ein zumutbares Maß beschränkt werden."*

Die unbestimmte Bezugnahme auf einen aktuellen Wissens- oder Wissenschaftsstand bewirkt eine Flexibilisierung der rechtlichen Anforderungen im Hinblick auf zukünftige technische Entwicklungen. Der Gesetzgeber ist dadurch nicht einem laufenden Überprüfungs- und gegebenenfalls Novellierungsbedarf ausgesetzt.[16] Die Handhabung von Technikklauseln ist freilich der Verwaltung oder der Gerichtsbarkeit alleine nicht möglich. Was den jeweiligen „Stand der Technik" ausmacht, kann im Einzelfall in aller Regel nur auf der Grundlage von Sachverständigengutachten geklärt werden.[17]

---

[12] Gerhard Saria, «Grundsätzliches zum ‚Stand der Technik' aus rechtswissenschaftlicher Sicht», in *Der „Stand der Technik"*, hrsg. Gerhard Saria (Wien: NWV neuer wissenschaftlicher Verlag, 2007), 63 ua. mit Verweis auf OGH 24.03.1988, 7 Ob 544/88; Karl Korinek, „Zum Erfordernis einer demokratischen Legitimation des Normschaffens," *ÖZW* (2009): 40, (41); Heimo Ellmer und Roman Schremser, „Der „Stand der Technik" als Kostentreiber? Sind Stand und Regel der Technik Synonyme?," *ZVB* (2018): 278, (284).

[13] Österreich. Chemikaliengesetz 1996 – ChemG 1996, BGBl. I 53/1997 in der Fassung BGBl. I 140/2020.

[14] Österreich. Medizinproduktegesetz 2021 – MPG 2021, BGBl. I 122/2021 in der Fassung BGBl. I 27/2023.

[15] Österreich. Gewerbeordnung 1994 – GewO 1994, BGBl. 194/1994 in der Fassung BGBl. I 75/2023.

[16] Saria, (Fn. 12), 30.

[17] Vgl. zB. VfSlg. 19.804/2013.

II. Generelle Rechtsetzung der Verwaltung

Eine im Vergleich zum parlamentarischen Gesetzgebungsverfahren regelmäßig weniger aufwendige und potentiell schnellere Form der generellen Rechtsetzung ist die Erlassung von generell-abstrakten Rechtsakten – im österreichischen Recht als Verordnungen bezeichnet – durch Verwaltungsbehörden. Nach Art. 18 Abs. 2 B-VG[18] ist in Österreich jede Verwaltungsbehörde ermächtigt, innerhalb ihres Wirkungsbereiches Verordnungen zu erlassen, wobei derartige Rechtsakte grundsätzlich nur das präzisieren dürfen, was bereits im Gesetz selbst vorgezeichnet ist.[19] Die Erlassung derartiger Verordnungen bietet sich demnach (gerade auch) für die Festlegung technischer Details an,[20] zumal diese bei Bedarf (relativ) rasch aktualisiert werden können. So finden sich in Verordnungsform erlassene Sicherheitsvorschriften, etwa im Bereich des Arbeitnehmer:innenschutzes,[21] Schwellenwerte und Emissionsbegrenzungen, etwa für die Einleitung von Abwasser,[22] sowie Berechnungsmethoden, etwa für die Kapazitäten elektrischer Versorgungsnetze.[23]

Im Europarecht wird die Kommission (immer häufiger) zur Erlassung sog. delegierter Rechtsakte (zumeist Beschlüsse oder EU-Verordnungen) verhalten. So sieht etwa der Verordnungsentwurf des bereits erwähnten „Gesetzes über künstliche Intelligenz" in Art. 7 Abs. 1 und 3 KI-VO-E vor, dass die Kommission delegierte Rechtsakte zur Änderung der Liste in Anhang III erlassen kann, um dieser (weitere) Hochrisiko-KI-Systeme hinzuzufügen oder zu streichen. Art. 11 Abs. 3 KI-VO-E überträgt der Kommission die Befugnis, delegierte Rechtsakte zur Änderung des Anhangs IV zu erlassen, um die technische Dokumentation eines Hochrisiko-KI-Systems mit Blick auf den technischen Forstschritt stets aktuell zu halten. Schließlich ermöglicht Art. 43 Abs. 5 KI-VO-E der Kommission, die Anhänge VI und VII (zur Konformitätsbewertung) angesichts des technischen Fortschritts mittels delegierter Rechtsakte zu aktualisieren.

---

[18] Österreich. Bundes-Verfassungsgesetz (B-VG), BGBl. 1/1930 in der Fassung BGBl. I 222/2022.
[19] Vgl. Christoph Grabenwarter und Stefan Leo Frank, *Bundes-Verfassungsgesetz und Grundrechte B-VG* (Wien: Manz Verlag, Stand 20.06.2020, rdb.at), Art. 18 B-VG Rn. 11.
[20] Vgl. zB. die detailreichen Regelungen der Verordnung des Bundesministers für Wirtschaft und Arbeit über die Begrenzung der Emission von luftverunreinigenden Stoffen aus Anlagen zur Erzeugung von Nichteisenmetallen und Refraktärmetallen, BGBl. II 86/2008.
[21] Österreich. Verordnung optische Strahlung – VOPST, BGBl. II 221/2010.
[22] Österreich. Verordnung des Bundesministers für Land- und Forstwirtschaft über die Begrenzung von Abwasseremissionen aus der Chlor-Alkali-Elektrolyse - AEV Chlor-Alkali-Elektrolyse, BGBl. 672/1996 in der Fassung BGBl. II 128/2019; Verordnung des Bundesministers für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft über die Begrenzung von Abwasseremissionen aus grafischen oder fotografischen Prozessen - AEV Druck – Foto, BGBl. II 45/2002 in der Fassung BGBl. II 128/2019.
[23] Österreich. Kapazitätsberechnungsmethoden-Verordnung 2022 – KBM-V 2022, BGBl. II 350/2022.

III. New Approach im Europäischen Produktrecht

Die Europäische Union setzt für ihr Produktrecht auf den sogenannten „New Approach“:[24] Im Kern besteht dieser – in den 1980er-Jahren entwickelte – Ansatz auf ein Zusammenspiel von Rechtsakten (Verordnungen, Richtlinien und staatliche Umsetzungsrechtsakte) und technischen Normen. Den Rechtsakten ist es primär vorbehalten, generalklauselartig ein einheitliches Schutzniveau für Produkte festzulegen.[25, 26] Da zugleich auf die Regelung von technischen Details verzichtet wird, sind diese Rechtsakte „langlebiger“. Die Festlegung technischer Einzelheiten zur Sicherheit von Produkten ist hingegen auf (harmonisierte) technische Normen ausgelagert, die von den Europäischen Normungsgremien (CEN, CENELEC und ETSI) auszuarbeiten und zT durch nationale Normungsgremien (zB. Austrian Standards Institute) in eigene (zB. Ö-)Normen umzusetzen sind.[27, 28]

Dem Regelungsmodell des „New Approach” folgt auch der KI-VO-E (vgl. dazu Pkt. C.IV.1.), das speziell für sogenannte Hochrisiko-KI-Systeme ein Zusammenwirken von generisch formulierten – sehr abstrakten – Anforderungen der EU-Verordnung und detaillierten technischen Anforderungen an solche Systeme in Normen vorsieht.[29] In seinen Art. 8 bis Art. 15 listet der Verordnungsentwurf umfangreiche aber allgemein formulierte Anforderungen für Hochrisiko-KI-Systeme auf. Nach Art. 40 Abs. 1 KI-VO-E wird die Konformität mit diesen Anforderungen vermutet, sofern die Systeme den einschlägigen harmonisierten Normen entsprechen. Die Normung soll eine Schlüsselrolle bei der Einhaltung der Verordnung einnehmen.[30] In Ermangelung einschlägiger harmonisierter Normen wird die Kommission ermächtigt, technische Spezifikationen in Form von Durchführungsrechtsakten zu erlassen.[31]

---

[24] Der „New Approach“ wurde durch den Beschluss 768/2008/EG aktualisiert und auf eine neue rechtliche Grundlage („New Legislative Framework“) gestellt (vgl. Beschluss 768/2008/EG des Europäischen Parlaments und des Rates vom 09.07.2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates, ABl. 2008, L 218/82).

[25] Thomas Klindt, „Der ‚new approach‘ im Produktrecht des europäischen Binnenmarkts: Vermutungswirkung technischer Normung,“ *EuZW* (2002): 133, (133 f.).

[26] Michael Mayrhofer, «Produktrecht», in *Wirtschaftsverwaltungsrecht*, hrsg. Andreas Hauer, Barbara Leitl-Staudinger, Michael Mayrhofer und Katharina Pabel (Luftenberg: Pedell Wissenschaftsverlag, 2013), 234 ff.

[27] Diesen Normen kommt kein verpflichtender Charakter zu. Ihre Anwendung durch die Hersteller erfolgt auf freiwilliger Basis. Es gilt jedoch eine Vermutung dahingehend, dass ein Produkt, welches nach den verbindlichen Sicherheitsanforderungen der Richtlinie hergestellt wurde, den verbindlichen Sicherheitsanforderungen der Richtlinie entspricht.

[28] Mayrhofer, (Fn. 26), 236.

[29] Vgl. ErwGr. 52 KI-VO-E.

[30] ErwGr. 61 KI-VO-E.

[31] Vgl. ErwGr. 61 und Art. 41 KI-VO-E.

IV. Schwächen der herkömmlichen Formen dynamischer Rechtsetzung

Die beschriebenen Modelle eignen sich zu einer „Dynamisierung" des Rechts. Sie weisen gleichwohl allesamt Schwächen auf, die bei der Regelung von KI besonders gravierend ausfallen können. So ist die Verwendung unbestimmter Rechtsbegriffe in Gestalt von Technikklauseln nicht geeignet, ein vollständiges Regelungsset für die Entwicklung und/oder den Einsatz einer Technologie zu schaffen. Zudem ist zur Bestimmung des Inhalts solcher Rechtsbegriffe stets ein – zumeist für den Vollzug aufwendiger – Rückgriff auf nicht-rechtliche Emanationen, wie beispielsweise technische Normen, fachliche Leitlinien, Richtlinien von Fachgesellschaften oä., erforderlich, womit die eigentliche „Regelung" wenig vorhersehbar ist und zudem insbesondere nicht vom demokratisch legitimierten Gesetzgeber getroffen wird.

Das demokratische Defizit eines „Sachverständigen-Rechts" haftet ganz allgemein auch dem New Approach-Modell an.[32] Außerdem kann dieses Modell dazu führen, dass einige wenige (zumeist große) Wirtschaftsakteure „ihre" technischen Standards durchzusetzen versuchen. Der Leistungsfähigkeit dieses Modells sind daher Grenzen gesetzt, weil die entscheidenden Rahmenbedingungen für eine Technik aus demokratischer Perspektive dem Gesetz vorbehalten bleiben müssen und nicht der technischen Normung überlassen werden dürfen. Wenn aber, wie bei der Regelung von KI, die entscheidenden Rahmenbedingungen selbst einem laufenden Anpassungsdruck unterliegen, schafft auch der New Approach mitunter nicht genügend Flexibilität, um am Ball der technologischen Entwicklung zu bleiben: auch die Entwicklung von technischen Normen ist ein (zeit- und ressourcen-)aufwendiger Prozess.

Dazu kommt, dass sowohl Rechtsakte, die dem New Approach-Modell folgen, als auch administrative Rechtsakte für sich in Anspruch nehmen, zu einem bestimmten Zeitpunkt ein „fertiges" technikrechtliches Korsett zu schaffen. Da KI jedoch keine herkömmliche, in ihrer Funktionsweise und in ihren Auswirkungen gut fassbare Technologie ist, läuft dieser Ansatz – wohl noch viele Jahre – Gefahr, erhebliche Regelungsdefizite hervorzubringen. So können unbe- oder -erkannte, selbst der Wissenschaft noch verborgene und erst etwa bei der konkreten Verwendung auftretende Gefahrenquellen oder -szenarien Risiken begründen, die zum Zeitpunkt der Rechtsetzung oder Normung schlichtweg nicht mitbedacht werden können. Die Genese des Entwurfs eines KI-Gesetzes ist ein gutes Beispiel für dieses Problem. So hat erst Anfang 2023 das EU-Parlament – wohl unter dem „frischen" Eindruck der Leistungsfähigkeit von ChatGPT – eine (deutliche) Verbreiterung des ursprünglich bloß individualistischen Risikoansatzes des Art. 5 des Entwurfes um gesellschaftliche Risiken eingemahnt und im Juni 2023 eine Regelung für generative

[32] Vgl. Konrad Lachmayer, „Verfassungsrechtliche Probleme der Normung," *ZTR* (2015): 87, (88 ff.); Martin Ebers, „Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag," RDi (2021): 588, (593).

KI vorgelegt.[33] Was wäre gewesen, wenn das KI-Gesetz entsprechend dem ursprünglichen Fahrplan zu diesem Zeitpunkt bereits beschlossen gewesen wäre?

C. Dynamische Rechtsetzung in Form von Reallaboren

I. Begriff

Sowohl dem Staat als auch den Wirtschaftsbeteiligten fehlt es bisweilen an Möglichkeiten zur Erprobung von technologischen Innovationen, um auf diesem Weg Kenntnis von der tatsächlichen Funktionsweise und den tatsächlichen Auswirkungen einer konkreten (Anwendung einer) Technologie zu erlangen. Dem Staat bleiben in einem solchen Fall prima vista nur die Optionen, entweder mit der Regelung der Technologie zuzuwarten, oder gleichsam auf gut Glück auf einer unsicheren oder unvollständigen Informationsbasis einen generell-abstrakten Rechtsrahmen zu schaffen oder auf einer allgemeinen rechtlichen (beispielsweise produkt- oder gewerberechtlichen) Grundlage über die Zulässigkeit des Einsatzes einer Technologie individuell zu entscheiden. Die Wirtschaftsbeteiligten müssen mitunter erhebliche Rechtsunsicherheiten in Kauf nehmen, wenn sie die Technologie ungeachtet einer unklaren Rechtslage einsetzen, oder sie sehen sich rechtlichen Hürden gegenüber, die sie vom Einsatz der Technologie Abstand nehmen lassen.

Derartige Defizite kann ein neuer Ansatz zur rechtlichen Regelung von innovativen, insbesondere digitalen Technologien und deren Anwendungen durch evidenzbasierte Erprobungen unter realen Bedingungen beseitigen helfen:[34] Sog. „Reallabore" (engl. Regulatory Sandbox; span. Espacio controlado de pruebas) sind rechtlich eingerichtete Räume für die Erprobung neuer Technologien oder neuer Anwendungen einer bestimmten Technologie. Sie ermöglichen es, solche Technologien oder Anwendungen (etwa in Produkten oder Dienstleistungen) innerhalb eines begrenzten zeitlichen Rahmens und im engen Austausch mit der zuständigen Behörde unter gewissen Voraussetzungen und Modalitäten – im „Echtbetrieb" –

[33] Vgl. Abänderungen des Europäischen Parlaments vom 14.06.2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)); European Parlament Press Release, «AI Act: a step closer to the first rules on Artificial Intelligence», abgerufen am 27. Juli 2023, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence; European Parlament Press Release, «MEPs ready to negotiate first-ever rules for safe and transparent AI», abgerufen am 27. Juli 2023, https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai.

[34] BMWi, (Fn. 9), 2.

zu erproben,[35] ohne dass alle ansonsten, dh. außerhalb des Reallabors geltenden rechtlichen Anforderungen erfüllt werden müssen.

Das rechtliche Instrument des Reallabors zeichnet sohin aus, dass die praktische Erprobung einer (Anwendung einer) Technologie mit einer befristeten Abweichung (Ausnahme) von den rechtlichen Vorgaben effektuiert wird. Dies ist deshalb notwendig, weil technische und hier insbesondere KI-basierte Innovationen mitunter nicht oder nur bedingt mit diesen Vorgaben, die in aller Regel noch nicht mit diesen Innovationen „rechnen" und damit nicht auf diese zugeschnitten sind, vereinbar sind oder ihre Vereinbarkeit mit diesen Vorgaben prima vista keinem finalen Urteil zugänglich ist.[36] Durch Reallabore wird also ein rechtlicher „Erprobungs(frei)raum" für jene Innovationen eröffnet, die ansonsten (möglicherweise) an die Grenzen des geltenden Rechtsrahmens stoßen würden.[37] Nach der Definition des Rats der Europäischen Union sind Reallabore

> *„konkrete Rahmen, die, indem sie einen strukturierten Kontext für Experimente vorgeben, es ermöglichen, innovative Technologien, Produkte, Dienstleistungen oder Ansätze - aktuell insbesondere im Zusammenhang mit der Digitalisierung - wo geeignet in einer realen Umgebung für einen begrenzten Zeitraum oder in einem begrenzten Teil einer Branche oder eines Gebiets unter regulatorischer Aufsicht und Gewährleistung angemessener Schutzmaßnahmen zu erproben."*[38, 39]

Legistisch wird dieser „strukturierte Kontext" durch sogenannte „Experimentierklauseln" abgebildet. Diese sind nach der Definition des Rats

---

[35] Christoph Krönke, „Regulatory Sandboxes aus der Perspektive des Allgemeinen Verwaltungsrechts," *ÖZW* (2020): 108, (109, 111).

[36] Vgl. BMWK, «Freiräume für Innovationen. Handbuch für Reallabore», (2019), 7, abgerufen am 26. Januar 2023, https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/handbuch-fuer-reallabore.pdf?__blob=publicationFile&v=14; Denk, (Fn. 2), 99.

[37] BMWi, (Fn. 9), 2.

[38] Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln als Instrumente für einen innovationsfreundlichen, zukunftssicheren und resilienten Rechtsrahmen zur Bewältigung disruptiver Herausforderungen im digitalen Zeitalter, ABl. C 2020/447 Z. 8.

[39] Vgl. auch die Definition des deutschen BMWK, welches Reallabore als „*zeitlich und räumlich begrenzte Testräume, in denen innovative Technologien oder Geschäftsmodelle unter realen Bedingungen erprobt werden*", definiert. (BMWK, (Fn. 36), 7). Der KI-VO-E umschreibt Reallabore in ErwGr. 72 als Einrichtungen zur Förderung von Innovationen im Bereich von KI, bei denen eine kontrollierte Versuchs- und Erprobungsumgebung für die Entwicklungsphase und die dem Inverkehrbringen vorgelagerte Phase geschaffen wird, um sicherzustellen, dass die innovativen KI-Systeme mit dieser Verordnung und anderen einschlägigen Rechtsvorschriften der Union und der Mitgliedstaaten in Einklang stehen.

> *„Rechtsvorschriften, die es den für ihre Umsetzung und Durchsetzung zuständigen Behörden ermöglichen, für die Erprobung innovativer Technologien, Produkte, Dienstleistungen oder Ansätze von Fall zu Fall ein gewisses Maß an Flexibilität walten zu lassen."*[40]

Die Erkenntnisse aus der Erprobung im Reallabor verschaffen dem Staat bzw. seinen Rechtsetzungs- und Verwaltungsorganen Wissen über die Technologie. Dadurch kann er faktenbasiert die rechtliche (Non-)Konformität des Erprobungsgegenstandes erkennen und gegebenenfalls geeignete Vorschriften für den Einsatz der Technologie oder deren Anwendung erlassen. Reallabore sind demnach kein Instrument zur Deregulierung, sondern ein Vehikel für eine bessere Regulierung.

II. Funktionsweise und Ausgestaltung

Die rechtliche Etablierung des Erprobungsraums kann gesetzestechnisch auf unterschiedliche Weise erfolgen. In Betracht kommen Ausnahmeregelungen oder sonstige Modifikationen des geltenden rechtlichen Rahmens. Die Experimentierklausel kann entweder die Erprobung eines bestimmten Vorhabens, etwa ein spezielles innovatives Geschäftsmodell oder einen konkreten Einsatz einer Technologie, regeln oder vorhabensoffen formuliert sein.[41] Einschränkend kann sich eine solche, an sich „offene" Regelung auf eine bestimmte Technologie beziehen.[42] Art und Umfang der privilegierenden rechtlichen Rahmenbedingungen können ebenso auf vielfältige Weise ausgestaltet sein. Denkbar sind in materieller Hinsicht etwa Ausnahmen oder Modifikationen von herkömmlichen Sicherheitsstandards, in prozessualer Hinsicht etwa Ausnahmen von bestimmten (zB. Genehmigungs-)Verfahren oder etwa auch fiskalische Erleichterungen. Je nach Eigenart und Bedarf kann der Betrieb eines Reallabors von der Erlassung eines individuellen Verwaltungsakts abhängen oder unmittelbar auf Grundlage der generellen Rechtslage durchgeführt werden. Denkbar sind auch sogenannte „No-Action-Letters" (NAL), mit denen der erprobende Wirtschaftsbeteiligte – auf einer entsprechenden gesetzlichen Grundlage – eine behördliche Zusicherung erhält, dass keine Maßnahmen gegen das im Reallabor erprobte Vorhaben ergriffen werden.[43]

Der Betrieb eines Reallabors muss vor diesem Hintergrund von bestimmten Voraussetzungen abhängen. Übliche Voraussetzungen werden insbesondere die Erprobungsreife (Testreife) und der Innovationswert des zu erprobenden Vorhabens sein. Dazu kommen Bestimmungen über zeitliche, sachliche und/oder örtliche

---

[40] Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln Z. 9. Vgl. auch BMWi, (Fn. 9), 2.

[41] Denk, (Fn. 2), 100.

[42] Harry Armstrong, Imre Bárd und Ebba Engström, «Regulator Approaches to Facilitate, Support and Enable Innovation», (2020), 23, abgerufen am 26. Januar 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/861078/regulator-approaches-facilitate-support-enable-innovation.pdf.

[43] Siehe dazu Krönke, (Fn. 7), 3 (6).

Begrenzungen der Erprobungsphase.[44] Um die Auswirkungen der Befreiung von einem allgemeinen Regulierungsrahmen auszugleichen, wird der Betrieb eines Reallabors in der Regel von einer (engmaschigen) behördlichen Überwachung begleitet werden müssen. Damit die Funktionsweise sowie die Chancen und Risiken des erprobten Vorhabens ermittelt und allfällige Unklarheiten beseitigt werden können, bedarf es einer flankierenden und abschließenden Evaluierung der Erprobung, deren Ergebnisse als Grundlage für eine (bessere) Rechtsetzung genutzt werden können. So können die durch die Evaluierung zutage geförderten Erkenntnisse zur Beibehaltung, zur Weiterentwicklung oder auch zur Beseitigung von materiell- oder prozessrechtlichen Vorschriften führen.

Reallabore können überdies dazu beitragen, das Verwaltungshandeln evidenzbasierter zu gestalten. Behörden können Wissen über die getestete Technologie[45] generieren und so nach Abschluss der jeweiligen Erprobungsphase (besser) beurteilen, ob der Erprobungsgegenstand den einschlägigen rechtlichen Anforderungen entspricht oder nicht. Sie können demnach beispielsweise aufgrund der Erprobung über die Genehmigungsfähigkeit einer Anlage, eines Produkts oder einer Dienstleistung entscheiden.[46]

Schließlich kann auch der Betreiber eines Reallabors einen Nutzen aus diesem ziehen. Er kann eine Technologie rasch und rechtssicher im „Echtbetrieb" einsetzen, erlangt faktische Kenntnisse über den Erprobungsgegenstand und Rechtssicherheit über dessen Vereinbarkeit mit den einschlägigen rechtlichen Anforderungen, die außerhalb des Reallabors geltenden. Alle diese Aspekte zeigen, dass Reallabore eine relevante Maßnahme zur Beförderung technischer Innovationen und zur Schaffung geeigneter rechtlicher Rahmenbedingungen für diese sein können.

III. Beispiele für Reallabore im geltenden Recht

1. Finanzmarktrecht

Der Ansatz des Reallabors wurde erstmals im Jahr 2016 mit der Fintech-„Regulatory Sandbox" der britischen Finanzmarktaufsichtsbehörde Financial Conduct Authority (FCA) gewählt. Diese „Regulatory Sandbox" wird als ein sicherer Raum beschrieben, in dem Unternehmen innovative Produkte, Dienstleistungen und Ge-

[44] BMWi, (Fn. 9), 2; Iris Eisenberger und Konrad Lachmayer, «EXTRA LAW - MOBILITY Experimentierräume im Verkehrs- und Mobilitätsrecht», 16, abgerufen am 13. Juni 2022, https://www.lachmayer.eu/wp-content/uploads/2020/12/ExtraLaw-Mobility_Teil1.pdf.
[45] Krönke, (Fn. 7), 3 (5).
[46] Denk, (Fn. 2), 100.

schäftsmodelle testen können, ohne sofort alle üblichen regulatorischen Konsequenzen tragen zu müssen.[47] Den Unternehmen wird gestattet, ihre (FinTech-)Produkte in einer kontrollierten Testumgebung mit echten Kunden zu testen.

Dieses Modell wurde weltweit zur Blaupause für ähnliche Initiativen im Fintech-Sektor.[48] So haben sich „FinTech-Sandboxes" international etabliert. Sie sind bereits weltweit – etwa in Lateinamerika,[49] den VAE,[50] Singapur[51] und vielen Staaten Europas[52] – zu finden. Auch in Österreich wurde mit § 23a FMABG[53] die Möglichkeit geschaffen, innovative FinTech-Geschäftsmodelle zu testen. Durch die Erprobung sollen Unternehmen in die Lage versetzt werden, das Potenzial und die Risiken des zu testenden Geschäftsmodells besser zu verstehen.[54] Zusätzlich gewinnt die Aufsichtsbehörde einen besseren Einblick in die laufende technologische Entwicklung.[55]

2. Energierecht

Systemnutzungsentgelte bezeichnen und beinhalten jene Preise, die ein Netzbetreiber für seine Dienstleistungen (bestehend etwa aus dem Netznutzungsentgelt, dem Netzbereitstellungsentgelt und dergleichen) in Rechnung stellen darf.[56] Nach den energierechtlichen Bestimmungen der § 58a ElWOG 2010[57] und § 78a GWG 2011[58] kann die zuständige Behörde in Österreich mit einem individuellen Verwaltungsakt (Bescheid) für sogenannte „Forschungs- und Demonstrationsprojekte" unter näher

[47] Vgl. FCA, «Regulatory sandbox», abgerufen am 27. Juli 2023, https://www.fca.org.uk/publications/documents/regulatory-sandbox.
[48] Armstrong, Bárd und Engström, (Fn. 42), 21.
[49] Vgl. zB. zu Kolumbien Progreso, «Sandbox regulatorio», abgerufen am 27. Juli 2023, https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/en/sandbox-regulatorio.
[50] Vgl. «Regulatory sandboxes in the UAE», abgerufen am 27. Juli 2023, https://u.ae/en/about-the-uae/digital-uae/regulatory-framework/regulatory-sandboxes-in-the-uae#:~:text=The%20ICT%20Regulatory%20Sandbox%20is,the%20sustainability%20of%20the%20sector.
[51] Vgl. Monetary Authority of Singapore, «Sandbox», abgerufen am 27. Juli 2023, https://www.mas.gov.sg/development/fintech/sandbox.
[52] Vgl. zB. zu Spanien Tesoro Público, «Espacio controlado de pruebas (Sandbox financiero)», abgerufen am 27. Juli 2023, https://www.tesoropublico.gob.es/es/servicios/espacio-controlado-de-pruebas-sandbox-financiero.
[53] Österreich. Finanzmarktaufsichtsbehördengesetz – FMABG, BGBl. I. 97/2001 in der Fassung BGBl. I 111/2023.
[54] ErläutRV 193 BlgNR 27. GP 2.
[55] ErläutRV 193 BlgNR 27. GP 1 f.
[56] Vgl. E-Control, «Systemnutzungsentgelte», abgerufen am 27. Juli 2023, https://www.e-control.at/marktteilnehmer/strom/netzentgelte.
[57] Österreich. Elektrizitätswirtschafts- und -organisationsgesetz 2010 – ElWOG 2010, BGBl. I 110/2010 in der Fassung BGBl. I 94/2023.
[58] Österreich. Gaswirtschaftsgesetz 2011 – GWG 2011, BGBL. I 107/2011 in der Fassung BGBl. I 23/2023.

bestimmten Voraussetzungen abweichende Systemnutzungsentgelte festlegen. Voraussetzung dafür ist, dass ein Projekt zur Erreichung von mindestens zwei (von mehreren genannten) Zielen beiträgt. Ein solches Ziel ist beispielsweise die „Digitalisierung des Energiesystems und intelligente Nutzung von Energie". Außerdem muss das Projekt schon vor der Beantragung im Rahmen eines Auswahlverfahrens als innovativ und förderwürdig bewertet werden.[59]
Ferner sieht Art 15 Abs 2a der Richtlinie über den Ausbau erneuerbarer Energien[60] vor, dass die Mitgliedstaaten die Erprobung innovativer Technologien im Bereich erneuerbarer Energie zur Erzeugung, gemeinsamen Nutzung und Speicherung von Energie aus erneuerbaren Quellen während eines begrenzten Zeitraums in Pilotprojekten unter realen Bedingungen fördern sollen. Unter „innovativer Technologien" versteht die RL

> *„eine Technologie zur Erzeugung von Energie aus erneuerbaren Quellen, durch die auf mindestens eine Weise eine vergleichbare, auf dem neuesten Stand der Technik befindliche Technologie im Bereich erneuerbare Energie verbessert wird oder die eine nicht vollständig kommerzialisierte und eindeutig mit einem Risiko verbundene Technologie im Bereich erneuerbare Energie nutzbar macht".*[61]

Gemäß den üblichen Vorgaben für Reallabore soll die Erprobung unter Aufsicht der zuständigen Behörden und unter Verwendung angemessener Sicherheitsvorkehrungen stattfinden.

3. Industrieanlagenrecht

Im Bereich des Industrieanlagenrechts erlauben staatliche Vorschriften,[62] die in Umsetzung von Art. 15 Abs. 5 EU-Industrieemissionsrichtlinie (IE-RL)[63] erlassen

[59] ErläutRV 733 BlgNR 27. GP 32.
[60] Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen in der Fassung der Richtlinie (EU) 2023/2413 des Europäischen Parlaments und des Rates vom 18. Oktober 2023 zur Änderung der Richtlinie (EU) 2018/2001, der Verordnung (EU) 2018/1999 und der Richtlinie 98/70/EG im Hinblick auf die Förderung von Energie aus erneuerbaren Quellen und zur Aufhebung der Richtlinie EU) 2015/652 des Rates.
[61] Art. 2 Abs. 2 Z. 14b Erneuerbare-Energie-Richtlinie.
[62] Die Richtlinienbestimmung wurde in Österreich in § 77b Abs. 4 GewO 1994, § 47a Abs. 4 AWG 2002 (Österreich. Abfallwirtschaftsgesetz 2002 – AWG 2002, BGBl. I 102/2002 in der Fassung BGBl. I 66/2023) und § 121 Abs. 10 MinroG (Österreich. Mineralrohstoffgesetz – MinroG, BGBl. I 38/1999 in der Fassung BGBl. I 60/2022) umgesetzt.
[63] Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates vom 24.11.2010 über Industrieemissionen (integrierte Vermeidung und Verminderung der Umweltverschmutzung), ABl. L 2010/334, 17.

wurden, für die Erprobung und Anwendung von Zukunftstechniken vorübergehende Abweichungen von bestimmten Auflagen mit Emissionsgrenzwerten. Als „Zukunftstechnik" gilt gemäß Art. 3 Z. 14 IE-RL

> *„eine neue Technik für eine industrielle Tätigkeit, die bei gewerblicher Nutzung entweder ein höheres allgemeines Umweltschutzniveau oder zumindest das gleiche Umweltschutzniveau und größere Kostenersparnisse bieten könnte als bestehende beste verfügbare Techniken."*

4. Verfahrensrecht

KI wird – in unterschiedlichen Einsatzfeldern – als Chance für die Öffentliche Verwaltung angesehen.[64] So werden beispielsweise intelligente Chatbots, prädiktive Systeme und unterschiedliche Automatisierungsanwendungen (etwa für No Stop-Prozesse) bereits von Behörden verwendet.[65] Es erscheint daher naheliegend, dass der Staat selbst Reallabore für die Erprobung von Technologien nutzen wird. Zum Zweck der Erprobung von E-Government-Anwendungen sieht etwa bereits das Sächsische E-Government-Gesetz eine Experimentierklausel vor. Gemäß § 20 leg. cit. können mit Verordnung sachlich und räumlich begrenzte Ausnahmen von der Anwendung einer Reihe von Bestimmungen des Verwaltungsverfahrensrechts für einen Zeitraum von höchstens drei Jahren vorgesehen werden. Ausgebaut zu einem Reallabor, die der Öffentlichen Verwaltung eine temporäre (und mitunter räumlich begrenzte) Abweichung vom geltenden Prozessrecht gewähren und zugleich eine engmaschige Evaluierung gewährleisten, können derartige verfahrensrechtliche Experimentierklauseln eine zweckentsprechende Erprobung von digitalen (KI-basierten) Verfahrensinstrumenten ermöglichen.

5. Automatisiertes Fahren Verordnung

Die Entwicklung selbstfahrender Fahrzeuge erfordert in besonderer Weise eine kontrollierte Erprobung unter realen Bedingungen. In Österreich sieht ein genereller Verwaltungsakt, die AutomatFahrV,[66] spezielle Rahmenbedingungen für die Testung von automatisierten Fahrzeugen auf Straßen mit öffentlichem Verkehr vor.[67] Unter anderem sind automatisierte Kleinbusse, Fahrzeuge zur Personenbeförderung und Fahrzeuge zur Güterbeförderung auf vorbestimmten Teststrecken oder

---

[64] Vgl. Michael Mayrhofer und Peter Parycek, *Digitalisierung des Rechts – Herausforderungen und Voraussetzungen 21. ÖJT IV/ 1* (Wien: Manz Verlag, 2022), 17; Denk, (Fn. 2), 86; Michael Mayrhofer, Ricarda Aschauer und Michael Denk, «Algorithmen im Verwaltungsverfahren», in *Algorithmen im Wirtschaftsrecht*, hrsg. WiR – Studiengesellschaft für Wirtschaft und Recht (Wien: Linde Verlag, 2023), 46.

[65] Vgl. dazu näher Mayrhofer, Aschauer und Denk, (Fn. 64), 46-60.

[66] Österreich. Automatisiertes Fahren Verordnung – AutomatFahrV, BGBl. II 402/2016 in der Fassung BGBl. I 143/2022.

[67] Vgl. dazu näher Michael Nikowitz, „Verordnung für das Testen automatisierter Fahrzeuge: zweite Novellierung. Erweiterung der Rahmenbedingungen für Test- und Versuchsfahrten auf Straßen mit öffentlichem Verkehr in Österreich," *ZVR* (2022): 196, (198 ff.).

Testgebieten zulässig. Diese Systeme müssen so ausgeführt sein, dass die Einhaltung der Bestimmungen der Straßenverkehrsordnung (StVO) dennoch gewährleistet ist. Nach Ende des Testzeitraumes ist ein Bericht über die gewonnenen Erkenntnisse an den zuständigen Bundesminister zu übermitteln.

IV. Reallabore in Verordnungsentwürfen der Europäischen Union

1. KI-Reallabor im Entwurf des EU-KI-Gesetzes

Der bereits genannte Vorschlag für eine Verordnung, die harmonisierte Regelungen für die Herstellung, das Inverkehrbringen und die Nutzung von KI festlegen soll (KI-VO-E) enthält in den Art. 53 ff. Regelungen zur Förderung der KI-Entwicklung. Unter anderem ist vorgesehen Reallabore einzurichten, die ermöglichen, KI-Systeme zu entwickeln, zu trainieren, zu testen und zu validieren, wobei klargestellt wird, dass andere, etwa mitgliedstaatlich eingerichtete Reallabore, davon unberührt bleiben.[68] Damit soll ein innovationsfreundlicher, zukunftssicherer und widerstandsfähiger Rechtsrahmen sichergestellt werden.[69] Mit den KI-Reallaboren soll nach ErwGr. 72 eine kontrollierte Versuchs- und Testumgebung für die Entwicklungsphase und die Phase vor der Inverkehrbringung geschaffen bzw. erzielt werden.[70] Die Einrichtung von KI-Reallaboren muss gemäß Art. 53 Abs. 1b etwa der Verbesserung der Rechtssicherheit und Förderung eines behördlichen Austauschs dienen, um ua. für die künftige Einhaltung der KI-Verordnung zu sorgen (lit. c), oder einen Beitrag zum faktengestützten regulatorischen Lernen leisten (lit. d). Infolgedessen sollen die zuständigen Behörden ein verbessertes Verständnis betreffend die Möglichkeiten neu auftretender Risiken und der Auswirkungen von KI-Nutzung erhalten.[71] Gemäß Art. 53 Abs. 6 KI-VO-E werden die Modalitäten und Bedingungen für den Betrieb der KI-Reallabore in Durchführungsrechtsakten der Europäischen Kommission festgelegt.

Die Nutzung geeigneter Datensätze gilt als wesentlicher Baustein für die Entwicklung (das Training) von Machine-Learning-Systemen. In Art. 54 KI-VO-E wird eine Rechtsgrundlage für die Nutzung von Daten, die ursprünglich zu einem anderen Zweck erhoben wurden, vorgeschlagen.[72] KI-Entwickler sollen unter bestimmten Voraussetzungen personenbezogene Daten, die ursprünglich zu anderen Zwecken erhoben wurden, für die Trainingsphase von KI-Systemen verarbeiten dürfen.[73]

---

[68] Art 53 Abs. -1d KI-VO-E.
[69] ErwGr. 71 KI-VO-E.
[70] ErwGr. 72 KI-VO-E.
[71] ErwGr. 72 KI-VO-E.
[72] ErwGr. 72a KI-VO-E.
[73] Matthias Lachenmann und Dirk Reinartz, „Datenverarbeitung bei Entwicklung von KI-Systemen in einem KI-Reallabor," *DSB* (2021): 261, (262 f.).

Mit einem Budget von 4,3 Millionen Euro will Spanien in Europa eine Vorreiterrolle bei der Regulierung von KI einnehmen und plant als erster Staat, die KI-„Sandbox" der KI-VO-E (bereits vor deren Geltung) zu verwirklichen.[74] Geplant ist, dass die Ergebnisse dieses Pilotprojekts allen Mitgliedstaaten sowie der Europäischen Kommission zur Verfügung gestellt werden, die auch für die Entwicklung europäischer Leitlinien und harmonisierter Standards zur Umsetzung des KI-Gesetzes verwendet werden sollen.[75]

2. Reallabor im Entwurf des EU-Gesetzes für ein interoperables Europa

Die Europäische Kommission hat ferner einen Entwurf einer Verordnung betreffend grenzüberschreitende Interoperabilität und Zusammenarbeit im öffentlichen Sektor vorgelegt.[76, 77] Interoperabilität bezieht sich auf die Fähigkeit von Verwaltungen, über Ländergrenzen, Sektoren und Organisationsgrenzen hinweg nahtlos zusammenzuarbeiten und ihre öffentlichen Dienstleistungen zu erbringen.[78] Mit der geplanten Verordnung soll ein Rahmen für die Zusammenarbeit öffentlicher Verwaltungen in der gesamten EU geschaffen werden, der dazu beiträgt, einen sicheren grenzüberschreitenden Datenaustausch aufzubauen und gemeinsame digitale Lösungen wie quelloffene Software, Leitlinien, Checklisten, Rahmen und IT-Tools zu vereinbaren.[79]

In den Art. 10 ff. des Entwurfs wird als Innovationsmaßnahme ua. die Einrichtung von Reallaboren vorgeschlagen. Die Zielsetzung der Reallabore besteht zufolge ErwGr. 26 darin, die Interoperabilität durch innovative Lösungen zu fördern, indem insbesondere eine kontrollierte Erprobungs- und Testumgebung geschaffen wird. Dies soll die Angleichung der Lösungen an diese Verordnung und andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten gewährleisten sowie Rechtssicherheit für Innovatoren und die zuständigen Behörden herstellen. Reallabore können nach Art. 11 Abs. 3 des Entwurfs ua. zu folgenden Zwecken eingerichtet werden: Förderung der Innovation und Erleichterung der Entwicklung und Einführung innovativer digitaler Interoperabilitätslösungen für öffentliche Dienste; Erleichterung der grenzüberschreitenden Zusammenarbeit zwischen zuständigen nationalen Behörden und Erzielung von Synergien bei der Erbringung

[74] Vgl. Luis Javier Sánchez, «España invertirá 4,3 millones de euros en un 'sandbox' para testar el Reglamento de Inteligencia Artificial de la UE», (2022), abgerufen am 26. Januar 2023, https://confilegal.com/20220701-espana-invertira-43-millones-de-euros-en-un-sandbox-para-testar-el-reglamento-de-inteligencia-artificial-de-la-ue/.

[75] Concept Paper, «Spain proposes to pilot an Artificial Intelligence Sandbox to implement responsible AI with a human-centric approach», abgerufen am 26. Januar 2023, https://digital-strategy.ec.europa.eu/en/events/launch-event-spanish-regulatory-sandbox-artificial-intelligence.

[76] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Gesetz für ein interoperables Europa) COM/2022/720 final.

[77] Pressemitteilung der Europäischen Kommission vom 21.11.2022, IP/22/6907.

[78] Pressemitteilung (Fn. 77).

[79] Pressemitteilung (Fn. 77).

öffentlicher Dienste. Insgesamt sollen die Reallabore dank der Zusammenarbeit mit den am Reallabor beteiligten Behörden zur Erhöhung der Rechtssicherheit beitragen (Abs. 4). Die Reallabore sollen auf Antrag (von mindestens drei beteiligten öffentlichen Stellen) von der Europäischen Kommission genehmigt werden (Abs. 5).

D. Ausgewählte rechtliche Rahmenbedingungen für ein „Reallabor-Recht“

I. Reallabore als Ausnahme

Die rechtliche Einrichtung von Erprobungsräumen setzt regelmäßig eine Abweichung von geltenden rechtlichen Vorschriften voraus. Soweit – in Österreich – Reallabore aufgrund einfachgesetzlicher Vorschriften eingerichtet werden können, kommt eine Abweichung von höherrangigen Vorschriften nicht in Betracht. Das bedeutet zunächst, dass sich einfachgesetzliche Reallabor-Regelungen nicht über verfassungsrechtliche Vorschriften hinwegsetzen und auch keine Ausnahme von diesen gewähren können. Eine praktisch häufig wohl besonders bedeutsame Schranke für Reallabore ergibt sich damit aus der bundesverfassungsgesetzlichen Kompetenzverteilung zwischen dem Bund und den Bundesländern (dazu näher II.). Staatliche Rechtsvorschriften können überdies grundsätzlich keine Ausnahmen von unionsrechtlichen Vorgaben (einer Richtlinie oder einer Verordnung) anordnen oder ermöglichen. Lediglich dann, wenn eine EU-Richtlinie den Mitgliedstaaten einen Umsetzungsspielraum belässt, kann eine staatliche Reallabor-Regelung anstelle der eigentlich (allgemein) zur Umsetzung erlassenen staatlichen Vorschriften eine alternative Rechtslage etablieren, wenn und soweit mit dieser die Richtlinie gleichermaßen umgesetzt wird. Reallabore, die ihre Rechtsgrundlage in EU-Verordnungen finden, partizipieren vom Anwendungsvorrang der Verordnung und können deshalb ein besonders effektives Instrument darstellen, weil sie – abhängig von der konkreten Ausgestaltung des Reallabor-Rechts – auch Ausnahmen vom staatlichen Recht ermöglichen können.

II. Regelungskompetenz und Reichweite des Reallabors

Österreich ist ein Bundestaat[80] und Mitgliedstaat der Europäischen Union. Nach dem föderalen Staatskonzept der österreichischen Bundesverfassung sind die Gesetzgebungskompetenzen zwischen den (Bundes-)Ländern und dem Gesamtstaat

[80] Vgl. Art. 2 Abs. 1 B-VG.

(Bund) abschließend aufgeteilt.[81] Die Kompetenzverteilung innerhalb der Europäischen Union kennt ua. ausschließliche EU-Kompetenzen[82] und zwischen Mitgliedstaaten und Union geteilte Kompetenzen.[83] Bei der Schaffung eines Reallabor-Rechts ist zu beachten, dass die intendierten Ausnahmen die kompetenzrechtlichen Grenzen nicht überschreiten. Bundesrechtlich geregelte Reallabore können beispielsweise grundsätzlich[84] nicht von unionsrechtlichen oder landesrechtlichen Vorgaben dispensieren oder diese modifizieren. Umgekehrt können landesrechtliche Reallabor-Regelungen keine Ausnahme von bundesrechtlichen oder unionsrechtlichen Vorschriften ermöglichen. Dies äußert sich etwa im Bereich des Anlagenrechts, dass als sogenannte Querschnittsmaterie, einerseits in die Kompetenz des Bundes (insbesondere Gewerberecht gemäß Art. 10 Abs. 1 Z. 8 B-VG), andererseits in die Kompetenz der Länder (insbesondere Baurecht gemäß Art. 15 Abs. 1 B-VG) fällt.

III. Bestimmtheitsgebot

Das in Österreich verfassungsrechtlich in Art. 18 Abs. 1 B-VG verankerte Legalitätsprinzip verlangt, dass die Vollziehung nur aufgrund der Gesetze, dh. nur insoweit tätig werden darf, als dies gesetzlich vorgesehen ist. Korrespondierend dazu müssen die Gesetze hinreichend bestimmt formuliert sein (Determinierungsgebot).[85, 86] Daraus ergibt sich, dass jede Ausnahme von gesetzlichen Regelungen, die mit einem Reallabor einhergehen soll, selbst eine entsprechende, ausreichend bestimmte gesetzliche Grundlage benötigt. Eine pauschale gesetzliche Ermächtigung zugunsten der zuständigen Behörde, eine Reihe von gesetzlichen Vorschriften unangewendet zu lassen oder deren Anwendung mit Verwaltungsakt zu suspendieren, wäre vor dem Hintergrund des Determinierungsgebotes verfassungskonform nicht realisierbar.

IV. Gleichheitsgrundsatz

Die mit einem Reallabor einhergehende privilegierte Behandlung bestimmter Vorhaben gegenüber sonstigen, nicht von einem Reallabor erfassten Vorhaben wirft

---

[81] Vgl. va. die Art. 10 bis 15 B-VG.

[82] Art. 3 Vertrag über die Arbeitsweise der Europäischen Union (AEUV).

[83] Art. 4 AEUV.

[84] Spezielle Kompetenztatbestände, wie insbesondere die Bedarfskompetenz des Art. 11 Abs. 2 B-VG für das Verfahrensrecht können ausnahmsweise eine einheitliche bundesrechtliche Regelung ermöglichen. Auf die sog. Bedarfskompetenz des Art. 11 Abs. 2 B-VG könnte eine bundeseinheitliche Reallabor-Regelung für das Verwaltungsverfahren gestützt werden. Da eine solche die Art und Weise von Erprobungen im Verfahrensrecht vereinheitlichen würde, schadete der Umstand nicht, dass die jeweiligen Erprobungen selbst naturgemäß von den allgemeinen Vorschriften abweichen würden.

[85] Theo Öhlinger und Harald Eberhard, *Verfassungsrecht*, 13. Aufl. (Wien: facultas, 2022), Rn. 601.

[86] VfSlg 19.899/2014.

gleichheitsrechtliche Fragen auf. In Österreich erlaubt der verfassungsrechtliche Gleichheitsgrundsatz (Art. 7 B-VG und Art. 2 StGG[87]) dem (einfachen) Gesetzgeber nur solche Differenzierungen, die sachlich gerechtfertigt sind. Der Gesetzgeber muss – auf eine einfache Formel gebracht - „Gleiches gleich und Ungleiches ungleich behandeln".[88] Eine Ungleichbehandlung muss im Licht des Gleichheitsgrundsatzes sachlich gerechtfertigt sein.[89] Unter dieser Voraussetzung steht es dem Gesetzgeber auch offen, innerhalb eines bestehenden Ordnungssystems einzelne Tatbestände auf eine nicht der vorgefundenen Systematik entsprechenden Weise zu regeln. Das Abgehen von einem Ordnungssystem ist folglich für sich allein nicht gleichheitswidrig, solange die Regelung in sich dem Gleichheitsgrundsatz entspricht.[90]

Die rechtlichen Bedingungen in einem Reallabor, mit denen der Gesetzgeber von den ansonsten geltenden rechtlichen Anforderungen abweicht, bedürfen vor diesem Hintergrund einer sachlichen Rechtfertigung. Diese kann – abhängig von der jeweiligen Materie – in unterschiedlichen Gründen gefunden werden, die je für sich, aber jedenfalls in ihrem Zusammenspiel wirken können: Erstens im Zweck des Reallabors, wenn und soweit dieses auf die Förderung öffentlicher Interessen – zu denken ist an die Förderung des Wirtschaftsstandortes, des Umwelt- und Klimaschutzes, der Produktsicherheit und damit etwa auch des Konsumentenschutzes, der Energieversorgung usw. – gerichtet ist, wofür in erster Linie einerseits die rasche(re) Verfügbarkeit von Innovationen, andererseits die durch das Reallabor unterstützte „bessere" Rechtsetzung und Vollziehung ausschlaggebend sind. Beachtenswert ist zweitens, welche Instrumente das Reallabor-Recht an die Stelle herkömmlicher technikrechtlicher Regelungsmodelle (zB Genehmigungsverfahren) setzt. So kann die eingehende behördliche Beurteilung eines Vorhabens (z.B. Anlage, Produkt oder Dienstleistung) durch die Regelung des Rahmens – also des „Labors", in dem das Vorhaben erprobt wird, ersetzt werden, um etwa Gefährdungen von Personen (Arbeitnehmer:innen, Konsument:innen, Nachbar:innen usw.) hintanzuhalten. Als wichtige Aspekte in diesem Zusammenhang sind die Befristung der Erprobung, die laufende engmaschige Einbindung einer Behörde in das Reallabor einschließlich von behördlichen Befugnissen, (potentiellen) Gefährdungen umgehend entgegenwirken zu können, sowie die Evaluierung des Reallabors vorzunehmen. Schließlich ist ein gleichberechtigter Zugang zu Reallaboren relevant, was klar definierte und sachliche Zugangskriterien voraussetzt.[91]

---

[87] Österreich. Staatsgrundgesetz, RGBl. 142/1867 in der Fassung BGBl. 684/1988.
[88] Vgl. zB. VfGH 25.09.2021, G 130/2021.
[89] VfGH 25.09.2021, G 130/2021; Lamiss Khakzadeh, «Art. 7 B-VG», in *Kommentar zum Bundesverfassungsrecht B-VG und Grundrechte*, hsrg. Arno Kahl, Lamiss Khakzadeh und Sebastian Schmid (Wien: Facultas Stand 1.01.2021, rdb.at), Rn. 19.
[90] Lamiss Khakzadeh, (Fn. 89), Rn. 38 mit weiteren Nachweisen aus der Judikatur.
[91] Krönke, (Fn. 7), 3 (7).

Eine verfassungskonforme Ausgestaltung des Reallabor-Rechts im Hinblick auf den Gleichheitsgrundsatz erscheint daher durchaus möglich. In diesem Sinne befand in Deutschland der Bayerische VfGH zu Experimentierklauseln,

> *„dass die Gestaltungsfreiheit des Normgebers dann besonders groß ist, wenn die Vorschriften dazu dienen sollen, auf einem neuen Sachgebiet Erfahrungen zu sammeln, die später die Grundlage für dauerhafte normative Entscheidungen bilden sollen."*[92]

V. Grundrechtliche Schutzpflichten

Werden in einem Reallabor herkömmliche Schutzstandards modifiziert, können daraus spezifische Gefahren zB. für Verkehrsteilnehmer:innen, Arbeitnehmer:innen, Konsument:innen, Nachbar:innen und sonstige Dritte entstehen. Zu denken ist etwa an Erprobungen von autonomen Systemen im Straßen- und Luftverkehr oder von intelligenten Maschinen in Industrieanlagen. Je nach Gefahrenlage können dabei selbst Risiken für die von Art. 2 und 8 EMRK[93] geschützten Rechte auf Leben, körperliche Unversehrtheit und Gesundheit entstehen. Das Grundrecht auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK verpflichtet den Staat, geeignete und angemessene Schritte zu unternehmen, um die Rechte von Betroffenen zu schützen und um einen fairen Ausgleich zwischen den konfligierenden Interessen herzustellen.[94] Ferner sind verfahrensrechtliche Garantien zu gewährleisten, wie beispielsweise eine angemessene Beteiligung am Verfahren, die Möglichkeit, die eigene Position *vorzutragen* und der Zugang zu den für Parteien und sonstige Beteiligte relevanten Informationen.[95] Diesen grundrechtlichen Anforderungen hat auch ein Reallabor-Recht Genüge zu tun, weshalb dieses nicht einfach für bestimmte Vorhaben von jeglichen rechtlichen Anforderungen dispensieren darf. Gleichwohl kommt, wie bereits erwähnt wurde, ein alternatives Regelungskonzept in Betracht, bei dem der grundrechtlich gebotene Schutz vor Gefährdungen über die Rahmenbedingungen der Erprobung, also über die Regelung des „Labors" sichergestellt wird.

E. Vermeidung von Insellösungen: Struktur eines einheitlichen Reallabor-Rechts

I. Sandbox Approach – Brand New Approach

Die rechtliche Verankerung von Reallaboren erscheint in mehreren Verwaltungsbereichen – vom Anlagenrecht, über das Energierecht bis hin zum Prozessrecht –

---

[92] VerfGH Bayern 25.09.2015, Vf. 9-VII-13 Vf. 4-VII-14 Vf. 10-VII-14.
[93] Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl. 210/1958 in der Fassung BGBl. III 68/2021.
[94] EGMR 16.11.2004, 4143/02, *Moreno Gómez/Spanien*, Rn. 55.
[95] Vgl. EGMR, 10.04.2012, 59819/08, *K.A.B./ESP*, Rn. 98; 09.05.2003, 52763/99, *Covezzi u. Morselli/ ITA*, Rn. 137; 07.07.1989, 10454/83, *Gaskin/GBR*, Rn. 49.

und für unterschiedliche Technologien, insbesondere jedoch nicht ausschließlich im Bereich der Künstlichen Intelligenz, zweckmäßig. Das kann jedoch zu einem konzeptionslosen Entstehen spezifischer Experimentierklauseln führen. Zahlreiche materienspezifische Einzel- oder Insellösungen mit unterschiedlichen Regelungsansätzen schaffen ein heterogenes Reallabor-Recht.
Ein solches Vorgehen hat den Nachteil, dass es für jedes neue Reallabor ein Tätigwerden des Gesetzgebers braucht. Es fordert Verwaltung und Wirtschaft sowie in der Folge die Gerichtsbarkeit in besonderer Weise, weil diese Akteure mit unterschiedlichen Vorschriften konfrontiert werden und einmal gefundene Lösungen kaum oder gar nicht auf andere Rechtsbereiche übertragen werden können. Andererseits wäre es unrealistisch, ein (einziges) generisches, dh. materienübergreifendes Reallabor-Recht zu etablieren, weil dafür die Regelungskonzepte und -inhalte der jeweiligen Materien zu unterschiedlich sind. Auf die verfassungsrechtlichen Probleme einer (bloß) generalklauselartigen Ermächtigung, einzelne Vorschriften zu Erprobungszwecken nicht anzuwenden, wurde bereits hingewiesen.

In Betracht kommt vor diesem Hintergrund ein Mittelweg in Form eines mehrgliedrigen Regelungssystems. Dieses könnte erstens aus generischen, also allgemeinen und ergänzungsbedürftigen Reallabor-Regelungen bestehen, die einen einheitlichen Kern und Rahmen eines Reallabor-Rechts etablieren. Zu denken ist an einheitliche Begriffsdefinitionen sowie einheitliche bzw. einheitlich ergänzungsbedürftige Regelungen über den Zugang zu und die Errichtung von Reallaboren, die Interaktion von Reallaboren mit Behörden, die (z.B. Gefährdungs-)Haftung für die Erprobung sowie die Evaluierung. Materienspezifisch könnten diese Regelungen zweitens aktiviert, ergänzt und im Bedarfsfall auch modifiziert werden. Solcherart würde ein „Innovationserprobungsrecht" geschaffen werden, das den verfassungsrechtlichen Erfordernissen entspricht und die spezifischen Bedürfnisse der jeweiligen Materie berücksichtigt.

Ein solcher zweistufiger Aufbau des Reallabor-Rechts würde es außerdem ermöglichen, auf bestimmte technische Entwicklungen angemessen und flexibel zu reagieren, ohne dabei einzelne Bereiche mit „Insellösungen" zu versehen. So ist etwa in Deutschland ein einheitliches Reallabor-Gesetz mit bundesweit einheitlichen Regeln in Vorbereitung.[96] Mit diesem soll ein agiler und lernfähiger Rechtsrahmen geschaffen werden, um „fit für Innovationen" zu sein.[97]

II. Bausteine eines Reallabor-(Rahmen-)Gesetzes

1. Voraussetzungen für die Einrichtung eines Reallabors

Die Einrichtung eines Reallabors wird regelmäßig von materienspezifischen Voraussetzungen abhängig zu machen sein. Gleichwohl kann ein Reallabor-(Rahmen-)Gesetz allgemeine sachliche Voraussetzungen für die Einrichtung regeln, die

[96] Vgl. BMWi, (Fn. 9).
[97] Vgl. BMWi, (Fn. 9), 1.

den Ausnahmecharakter des Reallabors begründen und betonen. Zu diesen Voraussetzungen zählt erstens, dass die Einrichtung und der Betrieb eines Reallabors Betrieb (nicht bloß privaten, sondern auch) öffentlichen Interessen dient. Derartige Interesse können, wie erwähnt, beispielsweise die Förderung des Wirtschaftsstandorts, des Umwelt- und Klimaschutzes, der Schutz der öffentlichen Gesundheit, die Steigerung der Produktsicherheit oder, allgemein, der Konsumentenschutz sein. In diesem Zusammenhang steht zweitens die Voraussetzung, dass durch das Reallabor ein Erkenntnisgewinn für die generelle Rechtsetzung („legistisches Lernen") und/oder den Vollzug erzielt werden kann. Um eine „Flucht" in das privilegierende Regelungsumfeld eines Reallabors zu vermeiden, sollte der Zugang drittens auf innovative, über den Stand der Technik hinausgehende Vorhaben eingeschränkt sein, die überdies mit dem geltenden Recht nicht bzw. wahrscheinlich nicht vereinbar sind oder deren Rechtskonformität ex ante mit vertretbarem Aufwand keiner (abschließenden) Beurteilung unterzogen und erst durch die Erprobung, dh. durch die tatsächliche Inbetriebnahme, das tatsächliche Inverkehrbringen oder dergleichen beurteilt werden kann. Gleichzeitig sollte das zu testende Vorhaben bereits über eine gewisse Erprobungsreife verfügen.

Einheitlich strukturiert können schließlich auch jene Unterlagen werden, mit denen von einem Antragsteller, der ein Reallabor betreiben will, die Eignung des „Rahmens", also des Labors für die konkrete Erprobung nachzuweisen ist. So kann beispielsweise – mit mitunter je nach Materie noch zu spezifizierenden Vorgaben – ein Konzept für das Labor einschließlich einer Risikoanalyse, die die Gefährdungsszenarien beschreibt, welche sich aus der Natur des Erprobungsgegenstands ergeben könnten, verlangt werden. Bei besonderen Risiken kann der Betrieb eines Reallabors zusätzlich von der Vorlage einer dem Risiko entsprechenden (Haftpflicht-)Versicherung abhängig gemacht werden.

2. Genehmigung/Einrichtung des Reallabors

Soweit Reallabore nicht ohnehin ex lege betrieben werden dürfen, bedarf es Bestimmungen über die Genehmigung und/oder Einrichtung desselben durch eine Verwaltungsbehörde. Mit dem individuellen Genehmigungsakt (in Österreich: Bescheid) oder einem generellen behördlichen Rechtsakt zur Einrichtung eines Reallabors (in Österreich: Verordnung) kann das Labor auf die konkrete Erprobung rechtsverbindlich zugeschnitten werden. So können insbesondere die Modalitäten der Erprobung (Testzeitraum, Bedingungen, Selbstüberwachung und behördliche Überwachung, Austausch mit der Behörde, Evaluierung) präzisiert werden.

3. Selbstkontrolle, behördliche Überwachung und Austausch mit der Behörde

Mit der Erprobung von innovativen Technologien können unterschiedliche Gefahren und andere unerwünschte Effekte einhergehen. Gerade auch mit Blick auf den Mangel an Kenntnissen über die konkrete Wirkungsweise einer Technologie ist in Erprobungsräumen eine laufende Selbstkontrolle im Verein mit einer behördlichen Überwachung und einer aktiven Zusammenarbeit mit dem Betreiber des Reallabors

erforderlich.[98] Die Überwachungsmaßnahmen sollen der Sicherheit von Menschen und der Umwelt dienen und damit gleichsam die günstige(re)n regulatorischen Rahmenbedingungen ausgleichen. Darin liegt ein wesentliches Element der Reallabor-Idee, das gleichsam vor der Klammer in einem Rahmengesetz eine einheitliche Ausgestaltung erfahren kann, wenngleich spezielle Ergänzungen abhängig von Gefahrengeneigtheit einer Materie – autonom fahrende Autos sind anders zu behandeln, als KI-gestützte E-Commerce-Anwendungen – unumgänglich sind.

Zur Implementierung einer effektiven Überwachung, welche mögliche Gefahren (und andere unerwünschte Effekte) identifiziert und möglichst hintanhält, muss die Behörde mit einem „Set" an Befugnissen ausgestattet werden, um gegebenenfalls korrigierend in den Testablauf eingreifen zu können. Ein Reallabor-Gesetz kann daher verschiedene, auch automatisierte Überwachungsinstrumente vorsehen. Es sollte einer Behörde ohne Weiteres erlauben bzw. auftragen, bei Ungereimtheiten, die während der Erprobungsphase festgestellt werden, das Reallabor-Konzept etwa mit Hilfe nachträglicher Auflagen zu modifizieren. Gleichsam als ultima ratio ist die vorzeitige behördliche Einstellung eines Reallabors vorzusehen. Dies kann dann notwendig sein, wenn besondere, nicht behebbare Gefahren vom Reallabor ausgehen oder der Reallabor-Betreiber die behördliche Kontrolle verweigert oder vereitelt.

Eine effektive Überwachung erfordert umfassende Mitwirkungs- bzw. Mitteilungspflichten durch den Reallabor-Betreiber.[99] Diese können in Form von Auskunftsrechten, Berichtspflichten oder einer permanenten (Selbst-)Kontrolle, etwa durch den Einsatz von Sensorik, ausgestaltet werden.

Nicht unterschätzt werden soll die Relevanz eines laufenden Austausches des Reallabor-Betreibers und der Behörde abseits der behördlichen Überwachung. Beide Seiten sollen anhand des Reallabors (auch voneinander) lernen. Der Erprobungsgegenstand soll, wenn möglich, auch unter „allgemeinen" rechtlichen Bedingungen genehmigungsreif gemacht werden. Ein Reallabor-Gesetz kann diesen Austausch nicht bloß auftragen, sondern vorstrukturieren und flankierend – etwa durch Regelungen über die rechtliche Bedeutung des Ausgetauschten bis hin zu Haftungsausschlüssen – absichern.

4. Evaluierung

Reallabore bieten Betreibern, Behörden und Gesetzgebern eine wichtige Informationsquelle über Chancen und Risiken der erprobten Innovation. Ein zentraler Baustein eines Reallabor-Gesetzes sind demnach Regelungen über die Bewertung der

[98] Zur individuellen Begleitung/Unterstützung durch die Behörde vgl. Krönke, (Fn. 7), 3 (6 f.), der auch auf die Notwendigkeit umfassender Informations- und Berichtspflichten verweist, um eine effektive behördliche Kontrolle zu gewährleisten.

[99] Krönke, (Fn. 35), 108 (114).

(Aus-)Wirkungen des erprobten Vorhabens, die etwa aus einer Evaluierung unter Beiziehung von (externem) Sachverstand bestehen können.

Das Ausmaß der Evaluierung kann, je nach Eigenart des Labors, aus einer laufenden oder auch nur einer abschließenden Evaluierung am Ende der Laufzeit bestehen. Die Evaluierung dient der Gewinnung von Entscheidungsgrundlagen. Der Gesetzgeber bzw. die Verwaltung können sich anhand des Tests unter realen Bedingungen ein Urteil über die getestete Innovation bilden.[100] Dies ermöglicht schon in einem frühen Stadium, über die Wirkungen der Innovation zu lernen, um deren Regeln innovationsfreundlich, evidenzbasiert und verantwortungsvoll zu gestalten.[101] Um Entscheidungsgrundlagen für die Anpassung bestehender Rechtsvorschriften zu gewinnen, bedarf es Regelungen, die die Analyse und Beurteilung der maßgeblichen Umstände und ggf. einen strukturierten Transfer des Wissens aus der Evaluation in den Rechtsetzungsprozess vorsehen.[102]

III. Materienspezifische Experimentierklauseln

Das Chemikalienrecht verfolgt ganz andere Zielsetzungen und Wertungen als etwa das Bankenrecht. Die Rechtslandschaft des (nationalen) Verwaltungsrechts ist derart mannigfaltig, dass eine starre „one-size-fits-all"-Lösung zu unzweckmäßigen Ergebnissen führen würde. Für eine sachbereichsspezifische Ausgestaltung und ein auf die jeweilige Materie zugeschnittenes Reallabor-Recht ist es entscheidend, dass das allgemeine Reallabor-(Rahmen-)Gesetz (bloß) subsidiär gilt und von sich aus zurücktritt, soweit dies materiellrechtlich erforderlich und vorgesehen ist.

Unter Berücksichtigung der Vielfalt des Verwaltungsrechts erfolgt nach dem hier vorgestellten zweistufigen Regelungskonzept die endgültige Festlegung der konkreten Erprobung in Form von speziellen Reallabor-Vorschriften ergänzend und allenfalls modifizierend zu einem allgemeinen Reallabor-(Rahmen-)Gesetz. So können der räumliche, zeitliche und sachliche Umfang des Reallabors näher definiert und angepasst sowie die Einrichtungsvoraussetzungen und die Bedingungen des Betriebs (die Testmodalitäten) gegenüber dem Rahmengesetz präzisiert, adaptiert oder erweitert werden.

Da die Ergebnisse der Evaluierung ebenso als Grundlage für die potenzielle Überführung in den regulären Genehmigungszustand herangezogen werden können, sollten sich in einer speziellen Reallabor-Vorschrift außerdem Regelungen über den Übergang der Testphase in ein darauffolgendes reguläres Genehmigungsregime finden.

---

[100] Vgl. BMWi, (Fn. 9), 1; BMWK, (Fn. 36), 7; Eisenberger und Lachmayer, (Fn. 44), 15.

[101] Vgl BMWi, (Fn. 9), 1.

[102] Vgl. Noerr LLP, «Gutachten. Umsetzung der BMWi-Strategie ‚Reallabore als Testräume für Innovation und Regulierung': Erstellung einer Arbeitshilfe zur Formulierung von Experimentierklauseln», (2020) 113, abgerufen am 27. Juli 2023, https://www.bmwk.de/Redaktion/DE/Downloads/G/gutachten-experimentierklausel-reallabore.pdf?__blob=publicationFile&v=1.

Spezielle Reallabor-Vorschriften operationalisieren auf diese Weise das Reallabor-Recht für einen bestimmten (Verwaltungs-)Bereich. Der Betrieb eines Reallabors wird solcherart erst durch dieses Zusammenwirken des allgemeinen und des speziellen Reallabor-Rechts ermöglicht.

F. Schlussbemerkungen

Die von innovativen Technologien, insbesondere von solchen, die zusammenfassend als KI bezeichnet werden, ausgehende enorme Entwicklungsdynamik und Komplexität erfordern nicht bloß (teils) neue inhaltliche regulatorische Antworten, sondern vor allem auch neue Rechtsetzungskonzepte. Das Instrument des Reallabors ist ein solches Konzept, das vor allem der Eigenart von KI in der aktuellen – geradezu sprunghaften – Entwicklungsphase gerecht werden kann. Diesem Instrument liegt die Einsicht zu Grunde, dass ein „fertiger" rechtlicher Rahmen für solche Technologien nicht einfach gebaut werden kann, wenn und soweit der Gesetzgeber noch zu wenig über die Technologie weiß. Um das dafür notwendige Wissen zu erlangen, lässt das Reallabor-Konzept die Erprobung der Technologie oder des Vorhabens (rechtlich) für eine bestimmte Zeit zu, wobei das Labor, also der Erprobungsrahmen möglichst sicher errichtet und betrieben werden muss. Die Erprobung von innovativen Technologien kann helfen, die Rechtsordnung innovationsoffen auszurichten. Die Zusammenarbeit mit (innovativen) Unternehmen ermöglicht es den Gesetzgebern und Verwaltungsbehörden mit neuen unternehmerischen Gegebenheiten und den jüngsten technologischen Entwicklungen Schritt zu halten.[103] Die aus der Erprobung von Technologien und deren Anwendungen (in Form von Geschäftsmodellen, Produkten usw.) gewonnenen Erkenntnisse können Beiträge zu einem besseren Verständnis der digitalen Transformation sowie zu einer besseren Gesetzgebung leisten, die einen hinreichenden Schutz vor technologiebasierten Risiken bietet, ohne dabei unnötige Innovationshürden aufzustellen.[104]

[103] Vgl. dazu Armstrong, Bárd und Engström, (Fn. 42), 29.
[104] IdS auch Noerr LLP, (Fn. 102), 18.

Algunos elementos en la construcción del derecho de la IA en Latinoamérica

José Hernán Muriel Ciceri

A. Introducción*

El desarrollo tecnológico forjado por la inteligencia natural del ser humano y su entorno da origen a la modalidad tecnológica denominada inteligencia artificial (IA). Es una forma de tecnología en avance, frente a muchas otras modalidades de tecnología, tales como: la interacción de la inteligencia humana con las máquinas, en la medicina,[1] así como en la rehabilitación de seres humanos[2], o en las avenidas de

* El autor agradece de forma especial a sus colegas Annette Guckelberger, Martin Eifert, Helmut Grothe, Wolfgang Hoffmann-Riem, Matthias Lehmann, Markus Ludwigs, Frank Peter Schuster y Thomas Wischmeyer por su gran amabilidad y apoyo esencial en parte del material que permitió la realización del presente capítulo, así como alumnus expreso mi especial gratitud al muy estimado KAAD y simultáneamente, a los colegas Markus Ludwigs y †Gerald Spindler, la Hanns Seidel Stiftung y al Siebold-Collegium Institute for Advanced Studies de la Universidad de Würzburg, por su apoyo vital en las etapas del desarrollo de la presente investigación. Este capítulo corresponde a una parte de los contenidos elaborados y presentados por el autor en las clases de la materia, así como a su correspondiente investigación y las presentaciones realizadas desde 2018.

[1] Anna-Katharina Harren, "Digitalisierung und künstliche Intelligenz in Orthopädie und Unfallchirurgie," *Orthopade,* (2018):1039-1054, doi: https://doi.org/10.1007/s00132-018-3642-4; Krishnan Ganapathy, Shabbir Syed Abdul y Aldilas Achmad Nursetyo, "Artificial intelligence in neurosciences: A clinician's perspective," *Neurol India* (2018): 934-939.

[2] Milán Anton Wolf, Stefan Landgraeber y Felix Kosmalla, "Digitale Hilfsmittel in der muskuloskelettalen Rehabilitación," *Die Orthopädie,* (2023): 525–531,

DOI: https://doi.org/10.17875/gup2023-2497

tecnología como la cadena de bloques[3] y los contratos inteligentes[4], en la conexión entre estos y las criptomonedas[5], o en las plataformas digitales[6], etc. Se trata de modalidades de tecnología que también pueden converger con la inteligencia artificial[7].

La IA tiene la potencialidad de mejorar las condiciones del camino que transita la humanidad, así como de ser fuente de riesgos de daños en su aplicación como a bien considera la cercana reglamentación europea en esta materia[8].

Los riesgos pueden generarse por el desarrollo, la activación, la colocación en el mercado de esta tecnología,[9] la correspondiente seguridad de la información y la protección de datos[10], así como por la interacción de esta con otras tecnologías en el ámbito, por ejemplo, de la comunicación de máquina a máquina (M2M)[11], de la máquina con el ser humano, así como en las relaciones jurídicas con usuarios y consumidores[12], o entre empresas (B2B)[13] y en la interacción de esta tecnología con

doi: https://doi.org/10.1007/s00132-023-04392-4; Rebecca Welder, *Das Rehabilitation Gaming System: Pilotstudie bei Patienten mit Hirninfarkt,* consultado el 30 de septiembre de 2023, https://d-nb.info/1294448617; Hannes Bastians y Dajana Mohr, "Einsatz von KI und Robotik in der Medizin: Interdisziplinäre Fragen. Part 1.," *CR,* (2023): 76, "Part 2," *CR,* (2023): 77-78.

[3] Philipp Sandner and Riccarda Joas. "Blockchain, Künstliche Intelligenz und Internet der Dinge: Aktueller Stand, Möglichkeiten Und Anwendungsfelder," *Finanzierung Leasing Factoring* 67, no. 2 (2020): 39-43, desde el ámbito financiero en este volumen las contribuciones de Sebastian Omlor, "Tokenisierung im deutschen Wertpapierrecht" y Yusuke Tachibana, "Blockchain and Finance in Japanese Law".

[4] Matthias Lehmann y Felix Krysa, "Blockchain, Smart Contracts und Token aus der Sicht des (Internationalen) Privatrechts," *BRJ,* (2019): 90 (92); adicionalmente Matthias Lehmann, "La Ley aplicable a la cadena de bloques," AEDIP, (2022): 181-202.

[5] Lehmann y Krysa, (n. 4), 90 (91).

[6] Ver en el derecho europeo por ejemplo en este volumen la contribución de Teresa Rodríguez de las Heras Ballell "Solving the 'Platform Liability Quandary'".

[7] Ver en el derecho europeo las contribuciones en este volumen de Gerald Spindler, "The EU Commission's Proposals for Regulation of Artificial Intelligence – Product safety and liability"; Annette Guckelberger, "Künstliche Intelligenz in der Öffentlichen Verwaltung"; Michael Mayrhofer y Michael Denk, "Künstliche Intelligenz und dynamische Rechtsetzung".

[8] Ante todo, y de forma detallada, así como sobre el régimen de responsabilidad civil, véase la contribución de Spindler en este volumen.

[9] Véase la contribución de Spindler en este volumen.

[10] Thomas Hoffmann, and Gunnar Prause. "On the Regulatory Framework for Last-Mile Delivery Robots," *Machines* 6, núm. 3 (2018): 33, consultado el 30 de septiembre de 2023, doi:10.3390/machines6030033.

[11] Hoffmann y Prause, (n. 10).

[12] Hoffmann y Prause, (n. 10).

[13] Así ante todo, Gerald Spindler, *Gutachten zur Haftung und Regulierung von Künstlicher Intelligenz,* (die Familienunternehmer und die jungen Unternehmer: Berlin, 2023), 9, consultado el 30 de septiembre de 2023, https://www.familienunternehmer.eu/fileadmin/familienunternehmer/positionen/digitalisierung/Gutachten/230712_FamU_Gutachten_Kuenstliche_Intelligenz_WEB_ES.pdf.

el entorno[14], aspecto que incluye la consideración a la eficiencia energética y de recursos[15].

Al analizar jurídicamente esta tecnología, tal como correctamente resalta Spindler, debe tenerse presente que la IA funciona "no solamente a través de algoritmos sino también con base en datos".[16] Por su parte, el entrenamiento y la ejecución de la IA depende a su vez de tales datos, que en su tratamiento y aplicación deben proteger la dignidad humana y los derechos fundamentales. En este contexto constituyen bloques de construcción de estructuras para la protección efectiva de estos derechos y de la dignidad humana[17]: la regulación, la aplicación de las reglas tradicionales del derecho civil, por ejemplo, en los ámbitos de los derechos contractuales, de los derechos reales, de la responsabilidad contractual y extracontractual, del derecho de protección de datos, entre otras áreas jurídicas, así como la elaboración de nuevas reglas domésticas y transnacionales en los ámbitos del derecho de la IA.

Con el objeto de analizar algunos elementos para una construcción del derecho de la IA en Latinoamérica, el presente capítulo esbozará una parte del camino de la IA en los niveles de la industria contemporánea (B). Posteriormente se resaltará la necesidad de bloques de construcción de estructuras jurídicas y de la regulación frente a la IA en Latinoamérica (C). A continuación, se presentarán algunos elementos adicionales desde el derecho alemán frente a la IA (D) y se finalizará con un acápite de conclusiones (E).

[14] José Hernán Muriel Ciceri, «Auf dem Weg zur Regelung der künstlichen Intelligenz in Lateinamerika» en *Digitalization as a challenge for justice and administration*, ed. Markus Ludwigs, José Hernán Muriel Ciceri y Annika Velling (Würzburg: Würzburg University Press, 2023), 55 y s., 65, doi: 10.25972/978-3-95826-201-0-55, consultado el 30 de septiembre de 2023, https://opus.bibliothek.uni-wuerzburg.de/opus4-wuerzburg/frontdoor/deliver/index/docId/30626/file/978-3-95826-201-0_Muriel_Ciceri_AOeffR_1_OPUS_30626.pdf.

[15] Hoffmann y Prause, (n. 10).

[16] Ante todo detalladamente, véase la contribución de Gerald Spindler en este volumen; así como en "Der Vorschlag einer Regulierung der Künstlichen Intelligenz," *CR,* (2021): 361-374.

[17] Muriel Ciceri, (n. 14), 65, 66.

B. El camino de la inteligencia artificial en los niveles de la industria contemporánea

I. Planteamiento

La IA se diferencia de la inteligencia humana[18]. En este sentido y como definición, Ertel[19] y Schael[20] coinciden en la remisión al concepto de 1950 de Elaine Rich según el cual, la IA es el "estudio de cómo lograr que las computadoras realicen tareas que, por el momento, los humanos hacen mejor." A diferencia de ello, se comprende la inteligencia humana según Schael con remisión a Sternberg como un concepto dinámico[21]. En este sentido la define, como una característica dependiente del entorno a través de la capacidad de procesamiento de la información, de una relación entre inteligencia y experiencia, así como de aplicación práctica de la inteligencia[22].[23]

La IA es como indica Schael, "interdisciplinaria", y en ella se pueden distinguir con Ertel entre otras de sus áreas de estudio, el aprendizaje de máquina y la minería de datos[24] o las redes neuronales y el aprendizaje profundo o deep-learning[25]. Asimismo, se consulta la conexión en red de inteligencias artificiales especializadas para un procesamiento de datos más eficiente a través de la comunicación entre estos sistemas, por ejemplo, de reconocimiento de voz y de reconocimiento de imagen[26].

Según Ertel, en la investigación de los procedimientos inteligentes se puede también buscar comprender, el cómo trabaja el cerebro humano y modelar o simular ello en el computador. En este ámbito él resalta, que no se busca establecer, como el ser humano soluciona un problema, sino cuál es la solución más inteligente a éste, con el "objetivo de construir agentes inteligentes para una amplia variedad

---

[18] Muriel Ciceri, (n. 14), 57.
[19] Wolfgang Ertel, *Grundkurs Künstliche Intelligenz*, 5 ed. (Wiesbaden: Springer Vieweg, 2021), 3, 201.
[20] Christopher Schael, "Künstliche Intelligenz in der modernen Gesellschaft. Bedeutung der „Künstlichen Intelligenz" für die Gesellschaft," *DuD,* (2018): 547 (548).
[21] Schael, (n. 20), 348.
[22] Schael, (n. 20) 348.
[23] Robert Jeffrey Sternberg indica entre otros aspectos que: *„los componentes de la inteligencia y las representaciones mentales sobre las que actúan son universales..., las personas en todas las culturas necesitan ejecutar los meta-componentes para (a) reconocer la existencia de problemas, (b) definir cuáles son …, (c) representar*(los) *mentalmente, (d) formular una o más estrategias…* (y)*, (e) asignar recursos para resolver*(los)*…, (f) monitorear (*su) *solución …, y (g) evaluar* (su) *resolución.... Lo que varía según las culturas son los contenidos mentales (es decir, tipos y elementos de conocimiento) a los que se aplican procesos como estos y los juicios sobre lo que se consideran aplicaciones "inteligentes" de los procesos a estos contenidos",* "Culture and Intelligence", *Am Psychol* (2004): 325 (327), doi: 10.1037/0003-066X.59.5.325.
[24] Ertel, (n. 19), 201 y s.
[25] Schael, (n. 20), 285 y s, 325 y s.
[26] Schael, (n. 20), 350.

de tareas". Debido a que tales tareas pueden ser diferentes, los métodos utilizados también pueden ser distintos.[27] Adicionalmente la IA puede presentarse de forma materializada o desmaterializada en la nube[28] o como un sistema, tal como lo contempla el artículo 3.1. de la Propuesta de la Comisión Europea de Reglamento por el que se Establecen Normas Armonizadas en Materia de Inteligencia Artificial (CE-PR-NA-IA)[29] o el artículo 3a de la Propuesta del Parlamento Europeo de Reglamento relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA (PE-PR-RC-IA).[30]

Con todo, en los ámbitos de diferenciación entre la inteligencia humana y la inteligencia natural, es de interés el planteamiento de Gödel citado por Evers según el cual:

> *"resulta que cuando se establecen sistemáticamente los axiomas de las matemáticas, se hacen evidentes una y otra vez nuevos axiomas, que no se derivan formalmente de los establecidos hasta ahora [...] precisamente esta puesta en evidencia de axiomas cada vez más nuevos sobre la base del significado de los conceptos fundamentales es algo que una máquina no puede imitar".*[31]

Dentro la forma de tecnología de la inteligencia artificial, existen entonces distintas clases y etapas de desarrollo.[32] Tal como señala Ertel, una parte de la raíz de la

---

[27] Ertel, (n. 19), 3, 4.

[28] Muriel Ciceri, (n. 14), 56.

[29] Comisión Europea, "Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se Establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos De La Unión", COM/2021/206 final, consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri =celex%3A52021PC0206, En adelante CE-PR-NA-IA. Según el art. 3.1. de la Propuesta de la CE es un sistema de IA: *"el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I [del Reglamento] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa".*

[30] Parlamento Europeo, P9_TA(2020)0276, "Régimen de responsabilidad civil en materia de inteligencia artificial, Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)), (2021/C 404/05), 6.10.2021," consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri =CELEX:52020IP0276. El art. 3a de la Propuesta del PE define a un *sistema de IA* como "*todo sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la actuación, con cierto grado de autonomía, para lograr objetivos específicos*".

[31] Dirk Evers, "Der Mensch als Turing-Maschine?," *NZSTh,* (2005): 101 (108); Kurt Gödel, «Kurt Gödel, The modern development of the foundations of mathematics in the light of philosophy (*1961/?)», en *Collected Works*, Vol. 3, ed. Solomon Feferman et al. (New York y Oxford: Oxford University Press, 1995), 375 (384 y s.); Muriel Ciceri, (n. 14).

[32] Ertel, (n. 19), 9.

tecnología actual puede encontrarse desde 1931 en los aportes de Gödel, Church y Turing, a los fundamentos de la lógica y la informática teórica.[33] En este sentido, la inteligencia artificial, si bien es un segmento de la denominada industria 4.0,[34] desarrolla elementos anteriores a ella[35], y va más allá. De forma correspondiente se enfatiza en su incorporación en la industria 5.0 basada en la sostenibilidad[36], en los desarrollos a futuro de una industria 6.0.[37] así como en la consideración de las posibles etapas subsiguientes.

En especial se puede hacer referencia a aplicaciones de la IA en estos contextos. Estas aplicaciones van desde el hogar, la medicina[38], la agricultura sostenible[39], las ciudades inteligentes (smart cities)[40], la administración pública[41], hasta la exploración espacial[42], etc.[43]

Es así como, por ejemplo, Ganapathy, Abdul y Nursetyo, se refieren a una

> *"medicina 5 p del mañana", funcionalmente "predictiva, personalizada, de precisión, participativa y preventiva", la cual permita retornar a un aspecto de "humanidad en la*

[33] Ertel, (n. 19), 6 y s.
[34] František Zezulka, et al., "The Ideas of Industry 4.0: Seven Years After," *IFAC-PapersOnLine*, (2022), consultado el 30 de septiembre de 2023, https://doi.org/10.1016/j.ifacol.2022.06.024.
[35] Ashwani Sharma y Bikram Jit Singh, "Evolution of Industrial Revolutions: A Review," *IJI-TEE,* 9.11, (2020): 69 y s., consultado el 30 de septiembre de 2023, https://www.ijitee.org/wp-content/uploads/papers/v9i11/I7144079920.pdf.
[36] Sharma y Singh, (n. 35), 69, (72).
[37] Mariia Golovianko, et al., "Industry 4.0 vs. Industry 5.0: Co-existence, Transition, or a Hybrid," *Procedia Computer Science,* (2023): 102 (107), consultado el 30 de septiembre de 2023, https://www.sciencedirect.com/science/article/pii/S1877050922022840.
[38] Ganapathy, Abdul y Nursetyo, (n. 1), 934 y s.; Harren, (n. 1), 103 y s.; Wolf, Landgraeber y Kosmalla, (n. 2), 525 y s.; Welder, (n. 2); Bastians y Mohr, (n. 2).
[39] Ines Härtel, "Künstliche Intelligenz in der nachhaltigen Landwirtschaft – Datenrechte und Haftungsregime," *Nu*R, (2020): 439.
[40] En el derecho alemán y suizo, Annette Guckelberger, *Öffentliche Verwaltung Im Zeitalter Der Digitalisierung*, (Nomos Verlagsgesellschaft Baden-Baden 2019), n. 103-107, 99-105; Nadja Braun Binder et al., KI-Anwendungsbeispiele in Schweizer Verwaltungen, en: Staatskanzlei Kanton Zürich (Hrsg.), *Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen*, 2021, 24 (27). Adicionalmente véase en especial sobre la evolución del concepto de ciudades inteligentes el análisis de Mircea Eremia, Lucian Toma y Mihai Sanduleac, quienes se refieren entre otros aspectos, con remisión a la definición de 2014 del Smart Cities Council, a una *"ciudad inteligente"*, como aquella *"que utiliza las tecnologías de la información y la comunicación (TIC) para mejorar su habitabilidad, funcionalidad y sostenibilidad"*, "The Smart City Concept in the 21st Century," *Procedia Engineering* (2017): 12–19, doi:10.1016/j.proeng.2017.02.357; adicionalmente, ISO 37120:2018, "Ciudades y comunidades sostenibles Indicadores de servicios urbanos y calidad de vida".
[41] Ante todo, y de forma detalla en este volumen Annette Guckelberger, "Künstliche Intelligenz in der Öffentlichen Verwaltung".
[42] Steve Chien y Robert Morris, 'Space Applications of Artificial Intelligence," *AI Magazine*, (2014): 3.
[43] Cf. Muriel Ciceri, (n. 14), con más referencias.

atención médica al permitir que los médicos se centren en el paciente, en lugar de ahogarse en datos voluminosos".[44]

Este ámbito de humanidad aplicaría a otras profesiones y oficios en los que el desarrollo de una "inteligencia artificial cooperativa"[45] permita construir puentes sostenibles entre la dignidad humana, su entorno y los fundamentos naturales de la vida[46].

Entre otros aspectos pudiera considerarse en el sentido de Krause, el balance de la vida laboral frente las esferas privadas y familiares.[47] De modo que la aplicación de la IA permita al empleado el necesario tiempo de descanso y de regeneración con un derecho como regla general de inaccesibilidad por fuera del tiempo de trabajo, así como simultáneamente al empleador, la atención de situaciones que la IA pueda adelantar en ese momento, con la continuidad dentro de su ámbito de las funciones o tareas correspondientes.[48] Ello resalta además la necesaria sostenibilidad y el fomento empresarial, de forma armónica con el desarrollo económico sostenible, en sus componentes ambiental, social y ecológico.[49]

Es así como Hoffmann-Riem describe correctamente la digitalización, de la cual es parte la inteligencia artificial, como un "proceso de transformación" que se extiende a todos los ámbitos de la interacción humana.[50] Se trata de una era[51] de desarrollo tecnológico y social con correspondientes "oportunidades y riesgos" así como con la generación de los correspondientes retos para el derecho.[52]

---

[44] Ganapathy, Abdul y Nursetyo, (n. 1), 934 (935).
[45] Muriel Ciceri, (n. 14).
[46] Cf. Art 20a Ley Fundamental de la República Federal de Alemania (GG).
[47] Rüdiger Krause, "Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0," *NZA-Beilage,* (2017): 53 (56, 57).
[48] Nadja Groß y Jacqueline Gresse, "Entpersonalisierte Arbeitsverhältnisse als rechtliche Herausforderung – Wenn Roboter zu Kollegen und Vorgesetzten werden," *NZA,* (2016): 990 (992, 993).
[49] Vgl. World Commission on Environment and Development, "Our Common Future", *Report*, A_42_427-EN (1987), 54 y s.; Markus Ludwigs, «Grundstrukturen des Energieumweltrechts», en: Berliner Kommentar zum Energierecht, Bd. 2, ed. por *Franz Jürgen Säcker* y Markus Ludwigs, (2019), Einl. A núm. 7 s., 15 s.; United Nations, Rio Declaration on Environment and Development, ILM 31 (1992), 874 (Principle 9); Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1, 7, núm. 21.
[50] Wolfgang Hoffmann-Riem, *Recht im Sog der digitalen Transformation, Schriften zum Recht der Digitalisierung,* (Mohr Siebeck 2022), 294, 303; Muriel Ciceri, (n. 14) 57.
[51] Ertel, (n. 19), 344.
[52] Hoffmann-Riem, (n. 48) 4; Ertel, (n. 19), 344.

II. Industria 4.0

La industria 4.0 que nos retorna en su definición a la Feria de Hannover del año 2011[53], presenta una parte de la aplicación de la inteligencia artificial. Esta modalidad de industria se desenvuelve en un contexto de alto grado de digitalización de la producción, así como de la comunicación a través del internet de las cosas entre los componentes, las máquinas y las máquinas con los seres humanos, y de los sistemas ciberfísicos[54].

Adicionalmente esta industria implementa una arquitectura de control, que se distingue por el tránsito gradual desde la pirámide de automatización clásica hacia una red distribuida y organizada de forma descentralizada de participantes en el sistema de servicios.[55] La aplicación de esta tecnología, permite automatizar en esta forma de industria, los procesos de toma de decisiones, por ejemplo, en elementos de planificación así como la optimización de la eficiencia en la producción basándose en la experiencia a través de datos[56] y macrodatos[57]. Ello, además, tiene efectos en los modelos de negocio y de administración de las empresas[58], con la configuración de una estructura descentralizada.

III. Industria 5.0

En enero de 2021 la Dirección General de Investigación e Innovación de la Comisión Europea, emitió un informe de política sobre el avance de la industria 4.0 hacia una industria 5.0, en la cual (se dé un paso más allá de una visión reducida únicamente al lucro y) se tenga como objetivos "el humanocentrismo, la sostenibilidad y la resiliencia"[59].[60] En el primer aspecto, considera la Comisión que la tecnología debe responder y adaptarse a las necesidades humanas con la protección de los derechos fundamentales y la dignidad humana, la cual coloque al trabajador en el centro del proceso de producción[61]. Por su parte la sostenibilidad exige, que además del ámbito tecno-económico[62], se consideren los ámbitos

[53] Ole Wintermann, "Von der Arbeit 4.0 zur Zukunft der Arbeit," *NZA,* (2017), 537-541; Muriel Ciceri, (n. 14).
[54] Dorota Habrat, "Legal challenges of digitalization and automation in the context of Industry 4.0," *Procedia Manufacturing*, vol. 51, (2020): 938-942.
[55] Zezulka, et al., (n. 34).
[56] Zezulka, et al., (n. 34).
[57] Habrat, (n. 54).
[58] Sharma y Singh, (n. 34).
[59] European Commission, Directorate-General for Research and Innovation (EC DG RTD), "Industry 5.0 - Towards a sustainable, human-centric and resilient European industry", 13, consultado el 30 de septiembre de 2023, https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en
[60] En este sentido también Golovianko, et al., (n. 37), 102 (105).
[61] EC DG RTD, (n. 59), 14.
[62] EC DG RTD, (n. 59), 27.

ambientales y sociales[63]. En este contexto encuentra asidero el informe de la Comisión en la visión de la Organización de Naciones Unidas sobre desarrollo sostenible,[64] con sus componentes de protección social, económica y ambiental[65].

Igualmente es armónico el informe con el llamado del Parlamento Europeo a la búsqueda de la sostenibilidad en sus diferentes dimensiones a través de la IA realizado en su Resolución del 3 de mayo de 2022, sobre la IA en la era digital [66], [67] así como con el pacto verde europeo respecto a la combinación de datos con la infraestructura digital y las soluciones de inteligencia artificial, que "facilitan las decisiones basadas en datos contrastados y amplían la capacidad de comprender y abordar los retos medioambientales"[68], la Propuesta de Directiva sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, (CE-PD-RCE-IA)[69] y la Propuesta de Reglamento por el que se Establecen Normas Armonizadas en Materia de IA (Ley de Inteligencia Artificial) (CE-PR-NA-IA)[70]. Finalmente, el informe se refiere a la resiliencia, la cual debe permitir a esta forma de industria, superar los tiempos de crisis a través de cadenas de valor resistentes y de una capacidad adaptable de producción.[71] Se trata de situaciones de crisis que afronta la humanidad, tales como las pandemias, los conflictos regionales o globales, la seguridad alimentaria o el cambio climático, entre otras.

Por su parte, Golovianko et al., se refieren a la industria 5.0[72], con base en el informe de la Comisión, como aquella que además implementa sistemas ciberfísicos-sociales[73], y una colaboración entre humanos y máquinas[74]. En este

[63] EC DG RTD, (n. 59), 14.
[64] World Commission on Environment and Development, (n. 48); Ludwigs, (n. 48); United Nations, (n. 48).
[65] Así también, Golovianko, et al. (n. 37), 102 (109).
[66] Parlamento Europeo, Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)), lit b), Nr. 37, 46, 82, 137, consultado el 30 de septiembre de 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_ES.html.
[67] Muriel Ciceri, (n. 14), 55.
[68] Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, El Pacto Verde Europeo, COM/2019/640 final, 2.2.3., consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2019%3A640%3AFIN.
[69] Comisión Europea, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), COM/2022/496 final, consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496 , en adelante CE-PD-RCE-IA.
[70] Comisión Europea, (n. 29).
[71] EC DG RTD, (n. 59), 14.
[72] Golovianko, et al. (n. 37), 102 -13.
[73] Golovianko, et al. (n. 37), 102 (115 y s.).
[74] Golovianko, et al. (n. 37), 102 (107).

sentido, distinguen un epicentro en la industria 4.0 en la tecnología y la automatización de las decisiones[75], y en la industria 5.0, en el ser humano.[76]

IV. Industria 6.0

Golovianko, et al. proponen, además, la coexistencia de las industrias 4.0 y 5.0 a través de un híbrido que permita una así denominada industria 6.0[77], basada en una inteligencia de aprendizaje conjunto y colaborativa entre humanos y máquinas[78]. En este contexto, las industrias alternarían procesos dinámicos entre la participación humana y la colaborativa.[79]

En *suma*, es necesario seguir avanzando hacia una nueva forma de industria, que puede ser 6.0. o recibir otra denominación. Esta deberá tener como eje, la protección amplia y universal de la dignidad humana[80], así como al constituir una forma de realización del desarrollo sostenible, incluir la protección del entorno del ser humano, ambiental, ecológico, racional, y de los fundamentos naturales de la vida[81] en donde se estos encuentren. Concordantemente pudiera hacerse referencia mejor, a una cooperación entre humanos y máquinas, y concordantemente, a una "IA cooperativa". Esta forma de IA debería basarse, por ejemplo, en los elementos de protección expresados[82].

C. La necesidad de bloques de construcción de estructuras jurídicas y de la regulación frente a la IA en Latinoamérica

I. Planteamiento

La tecnología distinguida como IA, es fruto de un desarrollo histórico dinámico, que tiene distintas avenidas y etapas.[83] Se trata de un desarrollo que continúa y que va desde el apoyo y acompañamiento en tareas básicas a complejas.[84] Una de las cuestiones presentes en este desarrollo, es en todo caso, como indica Ertel, la probabilidad a futuro de que la IA pueda alcanzar un grado [equiparable a] la inteligencia humana, a través de una IA general y dar lugar a la denominada

[75] Golovianko, et al. (n. 37), 102 (117).
[76] Golovianko, et al. (n. 37), 102 (109).
[77] Golovianko, et al. (n. 37), 102 (110).
[78] Golovianko, et al. (n. 37), 102 (112).
[79] Golovianko, et al. (n. 37), 102 (113).
[80] Muriel Ciceri, (n. 14), 55 (66).
[81] Grundgesetz für die Bundesrepublik Deutschland (GG), Art. 20a.
[82] Muriel Ciceri, (n. 14), 66.
[83] Ertel, (n. 19), 9.
[84] Muriel Ciceri, (n. 14), 59.

"singularidad" o a una "singularidad limitada".[85] Ambos escenarios plantean alternativas, así como riesgos adicionales para el ser humano.[86]

Es por tanto una necesidad, la organización de bloques de construcción de estructuras jurídicas, tanto en la aplicación del derecho tradicional, así como en la generación de nuevos elementos, para la protección efectiva de derechos frente al desarrollo, la colocación en el mercado y la aplicación de la inteligencia artificial. Las propuestas en el contexto europeo tuvieron como antecedente el informe del grupo de expertos de alto nivel de la Comisión Europea sobre IA del año 2019[87]. Estas son, por ejemplo, la CE-PD-RCE-IA[88] y la CE-PR-NA-IA[89]. Las propuestas responden a los retos de la adaptación europea de las normas de responsabilidad civil extracontractual a la IA, así como al correcto funcionamiento del mercado interior mediante el establecimiento de normas armonizadas para la IA a través de un instrumento legislativo horizontal de la UE *que se apoye en un enfoque proporcionado basado en los riesgos*, [complementado con] *códigos de conducta para los sistemas de IA que no sean de alto riesgo*.[90].[91]

Estos instrumentos se integran con la propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos (CE-PD-RD-PD),[92] la cual realiza una revisión "de los avances de las nuevas tecnologías, incluida la … (IA), los nuevos modelos de negocio de la economía circular y las nuevas cadenas de suministro mundiales"[93]. Se trata de una reflexión que es también necesaria en el contexto del continente americano, así como en los países de Latinoamérica y del Caribe.

[85] Wolfgang Ertel, "Visionen der künstlichen Intelligenz: Science Fiction oder nahe Zukunft?," *Steinbeis Transfer-Magazin*, (21 junio, 2022), consultado el 30 de septiembre de 2023, https://transfermagazin.steinbeis.de/?p=11570.
[86] Ertel, (85).
[87] Spindler, (n. 13), 11.
[88] Comisión Europea, (n. 69).
[89] Comisión Europea, (n. 29).
[90] Cf. Opción 3+, 3.3., Evaluación de Impacto, CE-PR-IA.
[91] Spindler, (n. 13).
[92] Comisión Europea, Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52022PC0495, citada como CE-PD-RD-PD.
[93] Comisión Europea, (n. 92), considerando 3.

II. Organismos Internacionales

1. La Organización de Estados Americanos (OEA)

La Organización de Estados Americanos (OEA), es el organismo internacional que aglutina en el momento 35 países en el continente americano[94]. En septiembre de 2023 no existía aún un Tratado multilateral sobre la IA promovido por la OEA[95], que permitiría la unificación de elementos jurídicos, ni tampoco una Ley Modelo[96], que brindaría la posibilidad de armonización del derecho de la IA en el Continente. Por una parte, las propuestas europeas de Directivas y de Reglamento pueden servir en la construcción de convenciones interamericanas de la OEA, tanto en el ámbito de la responsabilidad civil extracontractual, como de "la regulación de la IA que se basa, entre otras cosas, *en el planteamiento del riesgo causado por la IA al destinatario de su aplicación o a la persona que interviene en su interacción*."[97].

Por otra parte, como se indicó anteriormente, el contenido de estas propuestas también puede servir de caja de herramientas (toolbox) al legislador latinoamericano en sus derechos domésticos.[98]

2. El Parlamento Latinoamericano y Caribeño (Parlatino)

Entre varios organismos internacionales en Latinoamérica es el Parlamento Latinoamericano y Caribeño (Parlatino), otra institución que puede desempeñar un rol especial en el desarrollo jurídico frente a los sistemas de inteligencia artificial en la región. El Parlatino fue formalizado mediante el Tratado de Institucionalización del Parlamento Latinoamericano del año 1987, como organismo regional, permanente y unicameral (art. 1). Actualmente, 23 países de América Central, del Caribe y de América del Sur[99] son miembros del Parlatino.

Este organismo tiene como objeto la salvaguarda de principios tales como: la integración latinoamericana (b.); la autodeterminación de los pueblos para darse, en su régimen interior, el sistema político, económico y social que libremente decidan

---

[94] Organización de Estados Americanos, "Estados miembros", consultado el 30 de septiembre de 2023, https://www.oas.org/es/estados_miembros/default.asp

[95] Organización de los Estados Americanos, "Tratados multilaterales", consultado el 30 de septiembre de 2023, https://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos.asp

[96] Organización de Estados Americanos, "Leyes Modelo", consultado el 30 de septiembre de 2023, https://www.oas.org/es/sla/dlc/mesicic/leyes.html#:~:text=Leyes%20Modelo&text=Son%20herramientas%20de%20cooperaci%C3%B3n%20que%20contienen%20los%20elementos%20m%C3%ADnimos%20que,a%20las%20que%20se%20refieren.

[97] Muriel Ciceri, (n. 14), 61.

[98] Muriel Ciceri, (n. 14), 65.

[99] Parlatino, "Países miembros", consultado el 30 de septiembre de 2023, https://parlatino.org/informacion-paises-miembros/#

(d.); y la igualdad jurídica de los Estados (f.).[100] En especial, según los artículos 9 y 10 del procedimiento para la elaboración, discusión y aprobación de proyectos de leyes modelo del Parlatino, la Asamblea del Parlamento tiene como parte de sus competencias, el aprobar leyes modelo, que tienen como objeto:

> *"[R]ecomendar a los Parlamentos que integran el Organismo un texto legal que establezca criterios normativos mínimos y equivalentes a alcanzarse en la región sobre una materia determinada, y que en el marco de un proceso de integración y cooperación sirva como un aporte para la elaboración de normas de avanzada en el derecho interno, tendientes a reafirmar los principios y propósitos del Parlatino y la defensa de los derechos humanos".*[101]

En el ámbito de la Tecnología, el Parlatino presenta tres Leyes Modelo que tienen su origen en su Comisión de Educación, Cultura, Ciencia, Tecnología y Comunicación. Estas son:

a. La Ley Modelo para Garantizar el Derecho Humano al acceso a las Tecnologías de la Información y la Comunicación e Internet (TICs) y eliminar la Brecha Digital, del 11 de febrero 2022.

Esta Ley considera, por una parte, en su artículo 1, el acceso a las TICs como un derecho humano y la eliminación de la brecha digital, en especial, en el ámbito de la educación. Por otra parte, según su artículo 8, se realizará la declaración estatal correspondiente, de que los Servicios de TICs son servicios públicos esenciales en un ámbito de competencia, frente a los cuales se debe garantizar "su efectiva disponibilidad de acceso para todos los habitantes (…) en condiciones de calidad, asequibilidad y a precios justos y razonables, con independencia de su localización geográfica". Asimismo, las licencias estatales que autorizan la prestación de servicios de las TICs, según su artículo 9, deberán obligar a que estos servicios se presten "en un régimen de competencia a fin de que se garanticen precios justos y razonables que cubran los costos de explotación y un margen de ganancia".[102]

---

[100] Ello es armónico con sus propósitos, tales como: el fomento del *"desarrollo económico y social integral de la comunidad latinoamericana y pugnar porque alcance, a la brevedad posible, la plena integración económica, política y cultural de sus pueblos"* (a); la garantía del *"estricto respeto a los derechos humanos fundamentales, y"* su no afectación *"en ningún Estado latinoamericano en cualquier forma que menoscabe la dignidad humana"* (c); el *"luchar en favor de la cooperación internacional, como medio para instrumentar y fomentar el desarrollo armónico de la comunidad latinoamericana, en términos de bienestar general"* (f), y el *"mantener relaciones con parlamentos de todas las regiones geográficas, así como con organismos internacionales"* (k), Parlatino, Tratado de Institucionalización del Parlamento Latinoamericano, consultado el 30 de septiembre de 2023, https://parlatino.org/documentos/

[101] Parlatino, "Procedimiento para la elaboración, discusión y aprobación de proyectos de leyes modelo", consultado el 30 de septiembre de 2023, https://parlatino.org/documentos/

[102] Parlatino, "Ley Modelo para Garantizar el Derecho Humano al acceso a las Tecnologías de la Información y la Comunicación e Internet y eliminar la Brecha Digital" 11.2.2022, consultado el 30 de septiembre de 2023, https://parlatino.org/wp-content/uploads/2017/09/plm-garantizar-derecho-acceso-digital.pdf

Por lo tanto, la Ley Modelo establece el acceso en el territorio nacional a las TICs, como derecho humano, y al mismo tiempo, la prestación de los servicios autorizados por el Estado, a través de condiciones de un régimen de competencia que garantiza este derecho, y permita un margen de ganancia a los prestadores.

b. La Ley Modelo de Ciencia, Tecnología e Innovación (CTI) para América Latina y el Caribe, del 20 y 21 de octubre de 2022.

Esta Ley Modelo tiene como objeto según su artículo 4, el "posibilitar que progresivamente los países se comprometan efectivamente en la promoción y desarrollo de la" CTI, en un contexto de desarrollo sostenible, "dentro de los criterios de ciencia abierta, ciencia para todos y la alfabetización científica universal". Para ello, el artículo prevé el establecimiento de una autoridad según la "estructura constitucional e institucional" correspondiente, la cual tendrá como misiones y funciones las dispuestas en su artículo 6.

- Según el artículo 6.16. esta autoridad deberá fomentar "el desarrollo de la IA con base en el enfoque humanista de la UNESCO", y para ello, se remite al texto del consenso de Beijing de 2019 sobre la IA y la educación. En especial el citado artículo, adopta el numeral 6 del preámbulo del Consenso, referente a la protección de los derechos humanos, y a proporcionar a todas las personas los valores y competencias "para una colaboración eficaz entre el ser humano y la máquina en la vida, el aprendizaje y el trabajo, y para el desarrollo sostenible".[103] Asimismo, el artículo adopta el numeral 7 del preámbulo del Consenso, el cual es dirigido a que "el desarrollo de la IA debe estar controlado por el ser humano y centrado en las personas" y a que la concepción de la IA debe ser "ética, no discriminatoria, equitativa, transparente y verificable". Adicionalmente establece la norma que debe realizarse un seguimiento y una evaluación del impacto de esta tecnología en las personas y la sociedad "a lo largo de las cadenas de valor".[104]
- El artículo 6.17., en armonía con el texto de la UNESCO sobre "[e]nseñar la IA en las escuelas",[105] establece como tarea de la autoridad, el fomento del "vínculo entre la IA y la educación" a través del aprendizaje con la IA (especialmente en el aula), sobre la IA y para la preparación de las personas frente a la IA, así como la comprensión de su repercusión en la vida humana. También son competencias especiales de esta autoridad, el buscar la interacción internacional en materia de "transferencia, adaptación, generación y emulación de tecnología" (6.18), la

[103] UNESCO, Consenso de Beijing sobre la inteligencia artificial y la educación, "Documento final de la Conferencia Internacional sobre la Inteligencia Artificial y la Educación, Planificación de la educación en la era de la inteligencia artificial: dirigir los avances" 16 – 18 de mayo de 2019, consultado el 30 de septiembre de 2023, https://unesdoc.unesco.org/ark:/48223/pf0000368303
[104] UNESCO, (n. 103).
[105] UNESCO, "Enseñar la inteligencia artificial en las escuelas", consultado el 30 de septiembre de 2023, https://es.unesco.org/themes/tic-educacion/inteligencia-artificial

formación de personal científico, tecnólogo e investigador, así como de emprendedores, evitando la fuga de cerebros (6.19) y el fomento de una estrategia de plausible diplomacia científica en materia de cooperación internacional para abordar los desafíos globales "en consonancia con las prioridades estratégicas definidas en los planes de nacionales de desarrollo" (6.20).

Los artículos 6.16 y 617, tienen su epicentro en el ser humano y en la colaboración entre este y la inteligencia artificial, así como establecen a la educación como un puente para la formación, comprensión y preparación del ser humano frente a la inteligencia artificial. En particular, los artículos 6.18 a 6.20 reconocen la importancia de la cooperación internacional, la formación y el emprendimiento y la diplomacia científica frente a los problemas globales con la consideración correspondiente de los planes de desarrollo de los países y en este sentido también de sus finanzas públicas.

c. La Ley Modelo de Neuroderechos para América Latina y el Caribe, del 29 de junio de 2023.

Esta Ley Modelo comprende por neuroderechos según su anexo de Marco Teórico, "los derechos del cerebro," que "se pueden definir como un nuevo marco jurídico internacional de derechos humanos destinados específicamente a proteger el cerebro y su actividad a medida que se produzcan avances en neurotecnología."[106] En este sentido, el literal f) del artículo 5 de la Ley Modelo sobre los principios y derechos fundamentales, establece la prohibición de intervención mediante la neurotecnología o cualquier sistema o dispositivo a nivel cerebral, sin el consentimiento de la persona o usuario, incluso en circunstancias médicas.[107]

De forma similar a la Ley Modelo CIT, prevé en su artículo 6 una autoridad, que según el artículo 7.13. también tiene como función el estimular "el desarrollo de la IA (IA) con base en el enfoque humanista de la UNESCO" y los numerales 6 y 7 del preámbulo del Consenso de Beijing de 2019. El artículo 7.14. coincide con la Ley Modelo CIT en su fundamento en el texto de la UNESCO sobre "Enseñar la IA en las escuelas"[108] y en el fomento del vínculo entre la IA y la educación y su ámbito de aplicación.[109]

En el contexto de esta Ley Modelo, la aplicación de la IA encuentra un indispensable límite frente a los derechos humanos destinados a proteger el cerebro

[106] Parlatino, Ley modelo de neuroderechos para América latina y el Caribe, anexo marco teórico conceptual general, consultado el 30 de septiembre de 2023, https://parlatino.org/wp-content/uploads/2017/09/leym-neuroderechos-7-3-2023.pdf

[107] Parlatino, (n. 106), literal f) art. 5, *"El derecho inalienable a no ser objeto de cualquier forma de intervención de las conexiones neuronales o cualquier forma de intrusión a nivel cerebral mediante el uso de neurotecnología, interfaz cerebro computadora[,] o cualquier otro sistema o dispositivo, sin contar con el consentimiento libre, expreso e informado, de la persona o usuario del dispositivo, inclusive en circunstancias médicas…."*.

[108] UNESCO, (n. 105):

[109] Parlatino, (n. 106).

y su actividad y de forma correspondiente, en los derechos fundamentales previstos en su artículo 5.

d. El desarrollo continúa

Adicionalmente, las Comisiones de Seguridad Ciudadana, Educación, Asuntos Políticos y Asuntos Económicos del Parlatino se reunieron el 29 de junio de 2023 con el objeto de analizar temas de inteligencia artificial, el "desarrollo de competencias digitales e inteligencia artificial" y la "creación de la oficina del futuro" del Parlatino. Según indica el Parlatino, la Ley Modelo de CTI fue elaborada con apoyo de la Oficina de Ciencias de la UNESCO y la Ley Modelo de Neuroderechos, se elaboró con el apoyo del Parlamento chileno y su equipo técnico.[110]

Con todo, es necesaria una Ley Modelo de Regulación de la IA para los países Latinoamericanos. Las Leyes Modelo mencionadas si bien no tienen como objeto esta materia, pueden constituir una parte del contexto a considerar para la formulación de, por ejemplo, una futura Ley Modelo del Parlatino que ofrezca estas posibilidades de armonización del derecho de la IA en los países de Latinoamérica y del Caribe.

III. La necesidad de normas especiales de regulación de la IA

El desarrollo, aplicación e interacción del ser humano con la inteligencia artificial, realiza un llamado por una parte a la implementación de normas jurídicas especiales de su regulación cuando ello sea requerido y proporcional. La necesidad de una actualización normativa en los regímenes jurídicos existe, así como de la construcción de un derecho de la inteligencia artificial. Por otra parte, en los ámbitos en los que normas especiales no se requieran o cuando aquellas aún no existan, debe permitirse el acceso a la justicia y la protección efectiva de derechos de las partes. Razón por la cual, deberá acudirse en este caso a las reglas tradicionales, por ejemplo, del derecho público o del derecho civil, según el caso, así como a los principios generales del derecho vigentes.

En el contexto latinoamericano a diferencia de otras materias como el derecho de protección de datos[111], no existe aún el establecimiento de una regulación masiva de la IA en los diferentes países. Sin embargo, en el ámbito de la IA, inició la elaboración y presentación de proyectos de leyes domésticas especiales, así como

[110] Parlatino, "Cuatro comisiones se reúnen en Panamá para abordar inteligencia artificial, Ciudad de Panamá, 29.6.2023", consultado el 30 de septiembre de 2023, https://parlatino.org/news/cuatro-comisiones-se-reunen-en-panama-para-abordar-inteligencia-artificial/

[111] Yarina Amoroso y Jacqueline Guerrero, "El panorama legislativo de la protección de datos en Latinoamérica en el período 2018-2022," *Desafíos Jurídicos*, (2023): 3 (4), consultado el 30 de septiembre de 2023, https://doi.org/10.29105/dj3.4-59; Ángela Moreno Bobadilla y María Isabel Serrano Maillo, (Dir.), *El Derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad* (Valencia: Tirant lo Blanch, 2021).

de actualización normativa del derecho existente, por ejemplo, regulatorio, civil y penal.

El índice latinoamericano de IA del Centro Nacional de IA (Cenia) de Chile, presentado en el mes de agosto de 2023, y elaborado con el apoyo del BID, la CAF, la OEA y la asistencia técnica de la UNESCO y el HAI de Stanford, entre otros, realiza un análisis del estado de la IA en 12 países de América Latina como son: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú y Uruguay.[112] En su capítulo D4. resalta el cómo de los países en mención, únicamente Perú, disponía en ese entonces de una legislación específica para la inteligencia artificial.[113] A continuación se indicarán algunos aspectos en la materia en Perú, Brasil y Chile.

1. Perú

a. La Ley 31814 del 2023

En el Perú la Ley 31814, "que promueve el uso de la IA en favor del desarrollo económico y social del país", fue publicada en el Diario Oficial el 5 de julio de 2023.[114]

La exposición de motivos del correspondiente Proyecto de Ley (PL) 02775/2022-CR, consideró en su formulación, las estrategias sobre IA en distintos países de mundo, la guía de la UNESCO en materia ética frente a la inteligencia artificial, así como la aplicación de esta tecnología en la salud en la pandemia de Covid 19, y en la seguridad e inteligencia nacional.[115] En especial se fundamentó la exposición de motivos por una parte, en la Estrategia Nacional de IA (ENIA)[116] 2021-2026, diseñada por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros del Gobierno del Perú.[117] La estrategia tiene como objetivos, "proponer ejes, objetivos y acciones que promuevan la

[112] Centro Nacional de Inteligencia Artificial (Cenia), "Índice latinoamericano de inteligencia Artificial", 11 de agosto de 2023, consultado el 30 de septiembre de 2023, https://indicelatam.cl/

[113] Cenia, (n. 112), 112, 113.

[114] Congreso de la República del Perú (CRP), Ley 31814, "que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país", consultado el 30 de septiembre de 2023, https://busquedas.elperuano.pe/normaslegales/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814-2192926-1/.

[115] CRP, Proyecto de Ley (PL) 02775/2022-CR, consultado el 30 de septiembre de 2023, https://wb2server.congreso.gob.pe/spley-portal-service/archivo/NDE4MjE=/pdf/PL0277520220808

[116] Cf. Secretaría de Gobierno y Transformación Digital, Presidencia del Consejo de Ministros, "Estrategia Nacional De Inteligencia Artificial, Documento de Trabajo para la Participación de la Ciudadanía 2021-2026", consultado el 30 de septiembre de 2023, https://cdn.www.gob.pe/uploads/document/file/1899077/Estrategia%20Nacional%20de%20Inteligencia%20Artificial.pdf?v=1630689418

[117] CRP, (n. 115), 31.

investigación, desarrollo y adopción de la IA", ayudar "a crear soluciones a problemas nacionales en base a la IA" y generar "nuevas oportunidades de desarrollo al país, priorizando sectores productivos y servicios públicos alineados a las estrategias y políticas nacionales." Asimismo, ella comprende la creación del Centro Nacional de Innovación e IA y del Centro Nacional de Computación de Alto Rendimiento,[118] lo que es correspondiente a la especialidad de la materia.

Por otra parte, se vincula el PL a las políticas de Estado del Acuerdo Nacional en materia tecnológica y de sostenibilidad.[119]

La Ley se divide en tres secciones:

- La primera sección contiene un título preliminar con un artículo único dirigido a establecer los principios para el desarrollo y el uso de la inteligencia artificial, tales como: a) Estándares de seguridad basados en riesgos, b) Enfoque de pluralidad de participantes, c) Gobernanza de internet, d) Sociedad digital, e) Desarrollo ético para una IA responsable, f) Privacidad de la inteligencia artificial. El primer principio que establecía el Proyecto de Ley era el denominado de seguridad supervisada, como una responsabilidad del Estado frente a la seguridad de los datos y el cual es modificado en la Ley, por el de estándares de seguridad basados en riesgos. Este principio de forma amplia indica la promoción de "un enfoque basado en riesgos para el uso y desarrollo de la inteligencia artificial". [120]
- La segunda sección corresponde a un capítulo primero, de disposiciones generales con tres artículos. El artículo 1 establece el objeto que privilegia a la persona y los derechos humanos en el uso de la inteligencia artificial, para el fomento del desarrollo económico y social del Perú en un contexto de ética, sostenibilidad, transparencia, replicabilidad y responsabilidad. El artículo 2 establece de interés nacional la promoción del talento (humano) digital, y el artículo 3 presenta las definiciones de inteligencia artificial, de sistema basado en inteligencia artificial, de tecnologías emergentes y de algoritmo. En la definición de IA se resalta que ésta debe tener el potencial de "mejorar el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad, y ayudar a responder a los desafíos globales clave." El capítulo 2 establece una autoridad técnico-normativa en el orden nacional, la cual es la Presidencia del Consejo de Ministros, a través de su Secretaría de Gobierno y Transformación Digital, que es responsable de la dirección, evaluación y supervisión del uso y la promoción del desarrollo de la IA y las tecnologías emergentes, para alcanzar los objetivos del país en materia de transformación digital y los Objetivos de Desarrollo Sostenible. Esta Autoridad, está obligada a presentar un informe anual al

[118] Estrategia Nacional de Inteligencia Artificial (ENIA), consultado el 30 de septiembre de 2023, https://guias.servicios.gob.pe/creacion-servicios-digitales/inteligencia-artificial/enia
[119] CRP, (n. 115), 32 y s.
[120] CRP, (n. 114).

Congreso de la República sobre los avances en la implementación de la Política Nacional de Transformación Digital y la Estrategia Nacional de IA y en el evento que identifique amenazas graves o vulneración de ciberseguridad nacional, deberá informar inmediatamente a la Comisión de Inteligencia del Congreso de la República. Aquí surge la cuestión del ejercicio de las competencias de la Autoridad frente a quien, por ejemplo, utilice, desarrolle, distribuya o coloque en el Perú, aquella IA que genere un riesgo lesivo a las personas superior al potencial descrito en la definición de IA del artículo 3.

- La tercera sección comprende una disposición dirigida a aprobar por el Poder Ejecutivo el Reglamento de la Ley en el plazo de noventa días hábiles, contados desde de su entrada en vigor. La Presidencia del Consejo de Ministros realizó en 2023 una convocatoria pública digital para participar del codiseño del Reglamento de la Ley 31814.

b. Proyecto de Ley 05182/2022-CR

El 30 de mayo de 2023, fue presentado este PL ante la Comisión de Transportes y Comunicaciones, el cual es dirigido a promover en particular, el uso de la IA en el sistema de transporte terrestre del Perú.[121] Se trata de un proyecto que tiene como objeto mejorar la seguridad y la eficiencia del sistema de transporte a través de tecnologías como la inteligencia artificial (art. 1) así como prevé que la IA en este sistema permita la "optimización de la logística a través de datos históricos y en tiempo real, la predicción del mantenimiento de vehículos, la optimización de la cadena de suministro y la planificación de rutas con predicción del tráfico y actualizaciones en tiempo real" (art. 3). Para ello se refiere a instituciones que serán encargadas de evaluar y controlar periódicamente el uso de esta tecnología en el sistema de transporte (art. 5).

2. Brasil

a. Tramite conjunto de proyectos

El 3 de mayo de 2023 se presentó en el Senado Federal el Proyecto de Ley 2338 de 2023 que "Prevé el uso de la Inteligencia Artificial"[122]. Este proyecto junto con

[121] CRP, PL 05182/2022-CR, "Ley que Promueve el Uso de la Inteligencia Artificial en el Sistema de Transporte Terrestre del País", consultado el 30 de septiembre de 2023, consultado el 30 de septiembre de 2023, https://wb2server.congreso.gob.pe/spley-portal/#/expediente/2021/5182, https://wb2server.congreso.gob.pe/spley-portal-service/archivo/MTAzODE5/pdf/PL0518220230525

[122] Senado Federal Brasil (SFB), Projeto de Lei (PL) 2338 de 2023, "Dispõe sobre o uso da Inteligência Artificial", consultado el 30 de septiembre de 2023, https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 ; Diario del Senado Federal, página 295 y siguientes, https://legis.senado.leg.br/diarios/ver/112653?pagina=295

cinco proyectos de Ley adicionales presentados desde el año 2019 a 2023 se tramitaron desde el 16 de agosto de 2023 de forma conjunta[123]. Los proyectos adicionales son: el 3592/2023, que "[e]stablece lineamientos para el uso de imágenes y audio de personas fallecidas a través de …(la IA), con el objetivo de preservar la dignidad, privacidad y derechos de las personas aún después de su muerte",[124] el 872/2021, que "[p]revé el uso de la" IA, el 21/2020, que "[e]stablece fundamentos, principios y directrices para el desarrollo y aplicación de la IA en Brasil; y toma otras medidas"[125], el 5691/2019, que "[e]stablece la Política Nacional de [IA]"[126] y el 5051/2019 que "[e]stablece los principios para el uso de la [IA] en Brasil"[127]. Es así como se puede contemplar un desarrollo en las materias y contenidos que va desde los principios para el uso de la IA en el PL 5051 del 16.09.2019 hasta el uso de imágenes y audio de personas fallecidas a través de esta modalidad de tecnología del PL 3592 del 19.07.2023.

b. El Proyecto de Ley 2338 del 3.5.2023

Este PL que "[p]revé el uso de la [IA]"[128] es integral y si bien no incluye la materia del proyecto 3592/2023, con su tramitación conjunta, será posiblemente dado un texto enriquecido en su contenido. El PL 2338/2023 se compone de 9 capítulos y 45 artículos, el cual refleja una importante consideración del contenido de la CE-PR-NA-IA. Asimismo, se puede distinguir la consideración en el capítulo de responsabilidad civil y frente al derecho interno, del contenido de la CE-PD-RCE-IA.

Entre muchos aspectos que vale la pena resaltar del proyecto se encuentran:

- Su artículo 1 que establece las normas nacionales generales para el desarrollo, implantación y uso responsable de los "sistemas de IA", para la protección de los derechos fundamentales y la salvaguarda de la implantación de sistemas

123 SFB, Tramitação, consultado el 30 de septiembre de 2023, https://www25.senado.leg.br/web/atividade/materias/-/materia/157233#tramitacao_10494842

124 SFB, PL 3592 de 2023, "Estabelece diretrizes para o uso de imagens e áudios de pessoas falecidas por meio de inteligência artificial (IA), com o intuito de preservar a dignidade, a privacidade e os direitos dos indivíduos mesmo após sua morte", consultado el 30 de septiembre de 2023, https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-3592-2023

125 SFB, PL 872 de 2021, consultado el 30 de septiembre de 2023, "Dispõe sobre o uso da Inteligência Artificial", https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-872-2021

126 SFB, PL 5691 de 2019, consultado el 30 de septiembre de 2023, "Institui a Política Nacional de Inteligência Artificial", https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-5691-2019

127 SFB, PL 5051, de 2019, consultado el 30 de septiembre de 2023, "Estabelece os princípios para o uso da Inteligência Artificial no Brasil", https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-5051-2019

128 SFB, PL 2338, de 2023, consultado el 30 de septiembre de 2023, "Dispõe sobre o uso da Inteligência Artificial", https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 ; Diario del Senado Federal, página 295 y siguientes, https://legis.senado.leg.br/diarios/ver/112653?pagina=295

seguros y confiables, en beneficio de la persona humana, el régimen democrático y el desarrollo científico y tecnológico. Asimismo, el artículo 2 establece diez fundamentos para los sistemas IA en el país y el artículo 3 prevé que, en el desarrollo, la implementación y el uso de los sistemas de IA se deberán respetar la buena fe y un acápite de doce principios.

- En el capítulo II indica en su artículo 5, los derechos de las personas afectadas por los sistemas de IA como, por ejemplo, "el derecho a la determinación humana y a la participación en las decisiones tomadas por los sistemas de inteligencia artificial, teniendo en cuenta el contexto y el estado del arte del desarrollo tecnológico" (IV). Su artículo 6 prevé que los derechos establecidos en el Proyecto se puedan ejercitar ante los órganos administrativos competentes, así como ante los Tribunales, según la normatividad de instrumentos de protección individual, colectiva y difusa. Dentro de otros ámbitos del derecho de información de quien interactúa con la inteligencia artificial, se incluye en el párrafo 2 del artículo 7, una obligación de información de las personas expuestas a sistemas de reconocimiento de emociones o de categorización biométrica, similar a la establecida en el numeral 2 del artículo 52 del CE-PD-RCE-IA. Asimismo, establece el párrafo 3 del artículo 7 del Proyecto de Ley, en el desarrollo de los sistemas de IA destinados a grupos vulnerables, una obligación especial de la posibilidad de comprensión de su funcionamiento y de los derechos de los usuarios frente a los que denomina agentes de IA. Estos agentes son definidos en el artículo 4 IV, II, III, como proveedores y operadores de IA que pueden ser una persona física o jurídica, pública o privada. El artículo 8 permite que la persona afectada por un sistema de IA solicite una explicación de una decisión, previsión o recomendación, con, por ejemplo, información de los mecanismos a través de los cuales una persona puede impugnar la decisión o la posibilidad de solicitar la intervención humana (IV, V). Eventualmente pudiera considerarse establecer como obligación frente a una decisión automatizada, el que ésta indique los mecanismos de impugnación y se prevea por el sistema la posibilidad de solicitar la intervención humana. La sección III establece en el artículo 9 un derecho de la persona afectada por un sistema de IA de impugnar decisiones, o previsiones generadas por el sistema, y solicitar su revisión o la intervención humana. El artículo 10 de esta sección, asigna el derecho de la persona afectada significativamente por la decisión, predicción, recomendación o la generación de perfiles o las interferencias del sistema, a solicitar la intervención humana, siempre y cuando ello sea posible. En el caso contrario, el responsable de la explotación del sistema deberá aplicar medidas alternativas para realizar un nuevo análisis de la decisión con base en los argumentos del impugnante y la reparación de daños. El artículo 11 obliga a que en los eventos en los cuales las acciones del sistema tengan un impacto irreversible o difícilmente reversible o puedan generar riesgos para la vida o integridad física de las personas, debe haber una participación humana significativa en el proceso

de toma de decisiones y una determinación humana final. En este sentido la exigencia aplicaría, por ejemplo, a los sistemas de automóviles automatizados. La sección IV que corresponde a su artículo 12 comprende el derecho a la no discriminación y a la corrección de prejuicios discriminatorios.

- El capítulo III establece en los artículos 13 a 18, la clasificación de los riesgos. Es así como el artículo 17 clasifica los casos de sistemas de alto riesgo de forma concordante, en general, con el Anexo III del CE-PR-NA-IA. En particular, el Proyecto incluye de forma expresa los vehículos autónomos (VIII). Adicionalmente el inciso VII del Proyecto referente a la administración de justicia, coincide en su esencia con el anexo III apartado 2 numeral 8 lit. a) del PR-NA-IA, y genera la cuestión de que su aplicación no vulnere la capacidad efectiva y límites de los sistemas en las materias indicadas, así como los derechos fundamentales[129] y las garantías constitucionales[130]. El artículo 18 del PL asigna a la autoridad competente una facultad de actualizar la lista de sistemas según su riesgo con base en los criterios allí determinados.
- El capítulo IV regula la gobernanza de los sistemas de IA en 3 secciones de los artículos 19 a 26.
- El capítulo V se dedica a la responsabilidad civil. En especial, su artículo 27 establece la obligación de una reparación integral de los daños patrimoniales, morales individuales o colectivos por parte del proveedor o del operador de un sistema, independientemente del grado de autonomía de ese sistema. En el caso de un sistema de alto riesgo o riesgo excesivo, su parágrafo 1 establece la responsabilidad objetiva del proveedor o el operador, según su participación. Si no se trata de un sistema de alto riesgo, el parágrafo 2 presume la culpa del agente causante del daño con una inversión de la prueba a favor de la víctima. La ausencia de responsabilidad de los agentes de IA se establece según el artículo 28, cuando no han colocado en circulación, empleado o tomado provecho del sistema (I) o cuando se prueba que el daño es un hecho exclusivo de la víctima o de un tercero o ante la imprevisibilidad de circunstancias externas (caso fortuito externo) (II). En el caso que se trate de la responsabilidad civil derivada de daños causados por los sistemas en el ámbito de relaciones de consumo, se

[129] Cf. Virgílio Afonso da Silva, "Direitos fundamentais e liberdade legislativa: o papel dos princípios formais", en *Estudos em homenagem ao Prof. Doutor José Joaquim Gomes Canotilho*, orgs. Fernando Alves Correia et al., (Coimbra: Coimbra Editora, 2012) 915 (937), consultado el 30 de septiembre de 2023, https://constituicao.direito.usp.br/wp-content/uploads/2012-Princ%C3%ADpios-formais.pdf.
[130] Cf. Dignidad humana y no discriminación, Art. 1 III, 3 IV, 5 I, II, Constitución de la República Federativa de Brasil, Supremo Tribunal Federal, Secretaria de Documentação, 2020, Constitución de la República Federativa de Brasil, consultado el 30 de septiembre de 2023, https://www.stf.jus.br/arquivo/cms/legislacaoConstituicao/anexo/CF_espanhol_web.pdf

establece la aplicación del Código de Protección al Consumidor de 1990[131], sin perjuicio de lo establecido en las demás normas del Proyecto de Ley.

- El capítulo VI establece en el artículo 30, la implementación por parte de los agentes de inteligencia artificial, de códigos de buenas prácticas y gobernanza.
- El capítulo VII establece en el artículo 31, la obligación de los agentes de notificar a la autoridad competente la ocurrencia de incidentes graves de seguridad o de riesgo para la vida y la integridad física de las personas, la interrupción del funcionamiento de infraestructuras críticas, daños graves a la propiedad o el medio ambiente o las violaciones graves a los derechos fundamentales.
- El capítulo VIII se refiere en su sección I artículo 32 a 35, a la autoridad competente designada por el poder ejecutivo y sus competencias. La sección II regula en el artículo 36 las sanciones administrativas y los criterios que pueden ser sujeto de imposición a los agentes de IA por parte de la autoridad competente previo un proceso administrativo, como consecuencia infracciones cometidas contra las normas establecidas en la Ley, que van desde la advertencia a la suspensión del desarrollo, suministro o explotación del sistema, entre otras. El artículo 37 establece la competencia de la autoridad para definir mediante reglamento el procedimiento de determinación y criterios de aplicación de las sanciones con la correspondiente motivación, y con consideración al principio de publicidad. En reflejo del artículo 53 del PR-NA-IA, sobre espacios controlados de pruebas para la inteligencia artificial, el PL prevé en la sección III de sus artículos 38 a 42, medidas para fomentar la innovación. Dentro de éstas considera, el arbitrio de la autoridad de autorizar un sandbox regulatorio experimental a las entidades que lo soliciten y cumplan los requisitos de ley. La sección IV estipula en el artículo 43 una base de datos pública de IA del alto riesgo que contengan los documentos públicos de evaluaciones impacto con los correspondientes límites de los secretos comerciales e industriales.
- El capítulo IX establece en los artículos 44 y 45 las disposiciones finales, que disponen la no exclusión de otros derechos previstos en el ordenamiento jurídico nacional o tratados internacionales de los que Brasil sea parte y la vigencia de la Ley un año después de su promulgación.

[131] Presidência da República Casa Civil Subchefia para Assuntos Jurídicos, Lei No. 8.078, de 11 de setembro de 1990, Dispõe sobre a proteção do consumidor e dá outras providências, consultado el 30 de septiembre de 2023, https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

3. Chile

a. Proyectos de Ley

En Chile se tramitan ante el Senado cuatro PL que se refieren directamente a la inteligencia artificial, de los cuales tres son en materia penal y uno en regulación de los sistemas de inteligencia artificial.[132] Los PL en materia penal se refieren a la modificación del Código Penal "en lo relativo al delito de usurpación de identidad en el contexto de uso de inteligencia artificial" (16112-07 del 17.07.2023), así como en la incorporación "…, como circunstancia agravante de la responsabilidad, el uso de IA en la comisión de un delito" (16021-07 del 13.06.2023), y "para sancionar el mal uso de la inteligencia artificial" (15935-07 del 15.05.2023). Por su parte, el PL 15869-19 del 24.04.2023 "Regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación". Tal como resaltan Weidenslaufer y Roberts, se tramitan desde 2019 a 2023 otros doce (12) proyectos de ley que hacen referencia a la inteligencia artificial.[133]

b. Proyecto de Ley 15869-19 del 24.04.2023

El PL[134] considera especialmente en sus fundamentos la Ley No. 21.383 que modificó el número 1 del artículo 19 de la Constitución Política de la República de Chile, el cual establece que el "desarrollo científico y tecnológico estará al servicio de las personas"[135], así como el PR-NA-IA[136].

El Proyecto de Ley se compone de 15 artículos:

- El artículo 1 busca establecer un marco jurídico para el desarrollo, comercialización, distribución y utilización de los sistemas de IA con la protección de los derechos fundamentales.
- El artículo 2 establece las definiciones.
- El artículo 3 clasifica los sistemas de riesgo inaceptable y la excepción del sistema de identificación biométrica remota en espacios públicos, en situaciones

---

132 República de Chile, Senado, Tramitación de Proyectos, consultado el 30 de septiembre de 2023, https://www.senado.cl/appsenado/templates/tramitacion/index.php

133 Weidenslaufer et al., "Regulación de la IA en la experiencia comparada Unión Europea y Estados Unidos, Biblioteca de Congreso Nacional de Chile", *Asesoría Técnica Parlamentaria*, (junio 2023), 27, consultado el 30 de septiembre de 2023, consultado el 30 de septiembre de 2023, https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/34367/2/BCN_regulacion_global_IA_2023_CW_RRrr_2.pdf

134 Cámara de Diputados, Chile, Proyecto de Ley (PL) 15869-19 del 24 de abril de 2023, *"que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación"*, consultado el 30 de septiembre de 2023, https://www.senado.cl/appsenado/templates/tramitacion/index.php

135 Ley 21383 de 2021, "Modifica la Carta Fundamental, Para Establecer el Desarrollo Científico y Tecnológico al Servicio de las Personas", consultado el 30 de septiembre de 2023, https://bcn.cl/2scpd

136 Comisión Europea, (n. 29); así también, Weidenslaufer, et al. (n. 133), 3.

concretas, caso en el cual está sujeta la excepción a una orden de un Tribunal de Justicia y su aplicación asigna a los Carabineros de Chile y la Policía de Investigaciones.

- El artículo 4 establece los sistemas de alto riesgo.
- El artículo 5 prevé la creación de la "Comisión Nacional de Inteligencia Artificial" por parte del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación y sus competencias. Dentro de estas facultades están el pronunciamiento sobre solicitudes de autorización de sistemas, el realizar recomendaciones de mejora regulatoria, la elaboración de un informe anual de sistemas, la creación y mantenimiento del registro de sistemas, y el pronunciarse sobre incidentes graves o defectos de funcionamiento. Esta competencia es viable en virtud de la obligación de notificación de los desarrolladores, proveedores y usuarios sobre el acaecimiento de un indicante grave o un defecto de funcionamiento establecida en el artículo 11. En todo caso es necesario establecer, de qué forma se califica un incidente como grave. La notificación obliga a la Comisión a informar a los desarrolladores, proveedores y usuarios correspondiente la suspensión temporal dada por orden de la Ley, del desarrollo, distribución, comercialización y utilización del sistema afectado (art. 11 II). En un plazo perentorio de 15 días calendario, deberá pronunciarse la comisión sobre el hecho y tiene el arbitrio de retiro de la autorización o del levantamiento de la suspensión temporal. Las solicitudes, su autorización o rechazo y los incidentes graves y defectos de funcionamiento reportados deberán ubicarse en un registro público de la Comisión (art. 13).
- El artículo 6 establece la obligación de todo desarrollador, proveedor y usuario de sistemas de solicitar autorización documentada técnicamente ante la evaluación del riesgo por la Comisión, antes de su desarrollo, comercialización, distribución y utilización en Chile. La autorización tiene una duración de 5 años, renovable en un nuevo proceso o cuando haya una modificación sustancial en el sistema.
- El artículo 7 estipula un arbitrio de la Comisión para colocar los sistemas a las pruebas necesarias con la protección de derechos de las partes.
- El artículo 8 prohíbe a la Comisión la autorización cuando el riesgo sea inaceptable.
- El artículo 9 dispone que previa calificación del sistema como de alto riesgo, la Comisión debe exigir para su autorización un plan de gestión de riesgos, así como de datos y medidas de vigilancia y ciberseguridad, entre otros aspectos.
- El artículo 10 exige en caso del objeto del sistema de interacción con personas, el que éstas estén informadas de que interactúan con un sistema. Ello pudiera ser cercano también al ámbito del principio de patencia al que se refieren en

2018 Specht y Herold en el derecho alemán[137]. Asimismo, establece la norma una obligación general de los desarrolladores, proveedores y usuarios de sistemas que generen o manipulen contenido digital que se asemeje a personas, objetos, lugares o sucesos existentes que puedan inducir al error a una persona sobre su autenticidad o veracidad, el que la persona está informada que el contenido es generado de forma artificial o manipulado por un sistema.

- El artículo 14 establece una sanción pecuniaria limitada y en el caso de que se derive ésta de una omisión en la notificación de un incidente grave o la presentación de información inexacta, incompleta o engañosa, el duplicar el valor de la sanción, así como el retiro de la autorización de la distribución, comercialización o uso, según el caso.
- Si se trata del desarrollo, distribución, comercialización o uso de sistemas de IA de riesgo inaceptable, el artículo 15 establecería la aplicación del principio de proporcionalidad en sentido estrecho.

4. Balance

La Ley 31814 del 2023 del Perú y los PL de Brasil y Chile en materia de regulación coinciden en establecer entre otros aspectos, una autoridad competente, la protección a los derechos fundamentales, una determinación de sistemas de alto riesgo con la prohibición general de algunas prácticas de IA, así como requisitos de seguridad frente a la IA y el corresponder con elementos previstos en el CE-PR-NA-IA. Adicionalmente el contenido del PL 2338 del 2023 de Brasil, es correspondiente a parte del contenido del CE-PD-RCE-IA. Por su parte, la Ley del Perú adopta en especial un enfoque basado en riesgos y establece un amplio ámbito regulatorio ejecutivo.

El grado de regulación ejecutiva dependerá en particular, entre otros aspectos, de la estructura constitucional y del derecho público interno de los países latinoamericanos, el contexto de los mercados correspondientes, así como de la indispensable seguridad jurídica[138]. Esta seguridad debería correspondientemente permanecer en los ámbitos trascendentales en la competencia de la legislación formal y material. En todos los casos, la brújula debería apuntar a la protección de la dignidad humana, de su entorno y de los fundamentos naturales de la vida.

Las constituciones en los países mencionados y en Latinoamérica en general, se refieren a la protección de la dignidad humana. En este sentido también es más cercana esta base jurídica al derecho europeo. Ello adquiere relevancia al momento de considerar aspectos jurídicos comparados que permitan construir un derecho de IA en Latinoamérica, y al mismo tiempo, sus propias realidades, sus tradiciones jurídicas y sus derechos internos en un mundo de contextos internacionales.

[137] Louisa Specht y Sophie Herold, "Roboter als Vertragspartner? Gedanken zu Vertragsabschlüssen unter Einbeziehung automatisiert und autonom agierender Systeme," *MMR*, (2018): 40 (42).
[138] Spindler, (n. 13), 6.

Por otra parte, es necesario establecer los elementos normativos de responsabilidad civil contractual y extracontractual, derivada del diseño, producción, distribución, colocación en el mercado, interacción con y aplicación de la IA.

Como hicieron algunos de los países latinoamericanos con una parte de las propuestas europeas mencionadas, pueden colocarse en consideración en Latinoamérica, los contenidos de las propuestas de la Comisión Europea de Directiva sobre la adaptación de las normas de responsabilidad civil extracontractual a la IA, (CE-PD-RCE-IA), de Reglamento por el que se Establecen Normas Armonizadas en Materia de IA, (CE-PR-NA-IA), de Directiva sobre responsabilidad por los daños causados por productos defectuosos (CE-PD-RD-PD) así como de la Propuesta del Parlamento Europeo de Reglamento relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA (PE-PR-RC-IA)[139], frente a los ámbitos de los propios derechos internos y de los mercados. Las propuestas europeas tienen además en común la salvaguarda de los derechos fundamentales y del derecho de protección de datos.[140]

En particular, debe aquí considerarse que en el caso de la CE-PD-RCE-IA y de la CE-PD-RD-PD no se prevé una inversión de la carga de la prueba. La CE-PD-RCE-IA considera que ello expondría a "los proveedores, operadores y usuarios de sistemas de IA a mayores riesgos de responsabilidad civil," así como "podría obstaculizar la innovación y reducir la adopción de productos y servicios" con IA.[141] No obstante, la propuesta aligera la carga de la prueba en las reclamaciones de indemnización de "las víctimas de daños causados por sistemas de" IA.[142] Su propuesta de armonización mínima permitiría a los demandantes "invocar normas más favorables del Derecho nacional" y en este sentido, que los derechos domésticos, conserven "la inversión de la carga de la prueba en el contexto de regímenes nacionales de responsabilidad subjetiva (basada en la culpa) o de regímenes nacionales de responsabilidad sin culpa (conocida como «responsabilidad objetiva») (…) que puedan resultar de aplicación a los daños causados por sistemas de IA."[143] Por su parte, la CE-PD-RD-PD plantea que una inversión probatoria, generaría una exposición de los fabricantes a riesgos de responsabilidad muy elevados con los efectos indicados y "un posible aumento de los precios de los productos[144]". Sin embargo, también presenta un aligeramiento de la carga de la prueba "en el marco de regímenes nacionales de responsabilidad subjetiva en los casos en que determinados sistemas de IA estén implicados en la causa de los

[139] Parlamento Europeo, (n. 30).
[140] Spindler, (n. 13).
[141] Comisión Europea, (n. 69), 2. Proporcionalidad.
[142] Comisión Europea, (n. 69), 1. Derechos fundamentales.
[143] Comisión Europea, (n. 69), Considerando 14.
[144] Comisión Europea, (n. 92), 2. Proporcionalidad.

daños"[145]. En ambos ámbitos se generaría un refuerzo "del derecho a la tutela judicial efectiva"[146].

Ahora bien, la PE-PR-RC-IA, establece en su artículo 4 una "[r]esponsabilidad objetiva de los sistemas de IA de alto riesgo", y que este Reglamento prevalecería "sobre los regímenes nacionales de responsabilidad civil en caso de clasificación divergente por responsabilidad objetiva de los sistemas de IA" (numeral 4.5). Con todo, el artículo 5 dispone un importe de la indemnización y su artículo 7 prevé plazos de prescripción. Adicionalmente considera en su artículo 8, una "[r]esponsabilidad subjetiva para otros sistemas de IA". Las demandas de responsabilidad civil estarán sometidas a "los plazos de prescripción, así como con los importes y el alcance de la indemnización", de "la legislación del Estado miembro en el que se haya producido el daño o perjuicio" (art. 9).

Concordantemente pudiera valorarse en Latinoamérica, la unificación mínima normativa de aspectos principales en esta materia o de no ser ello viable en un corto plazo, una armonización mínima[147] normativa interna. Correspondientemente sería una alternativa, el acudir al establecimiento de tratados interamericanos en estas materias desde la OEA. Otra alternativa a considerar pudiera ser, que los derechos internos tuvieran el soporte de leyes modelo desde la OEA o el Parlatino. En ambos casos quedaría un amplio espacio para el ejercicio normativo en particular de los legisladores nacionales ordinarios. Finalmente, y de forma quizás más cercana, pudieran analizarse los contenidos de las propuestas europeas como una caja de herramientas[148] del legislador nacional en su propio derecho. Ello permitiría en la región latinoamericana una mejor y efectiva protección de derechos y seguridad jurídica frente a los sistemas de inteligencia artificial, así como el consecuente establecimiento de estándares de calidad con mayores posibilidades en la fabricación y/o comercialización de estos sistemas.

D. Algunos elementos adicionales desde el derecho alemán

El desarrollo del análisis del derecho de la inteligencia artificial es amplio en cada una de las áreas. En este sentido se realizará un acercamiento a algunos elementos jurídicos desde la literatura sobre el derecho alemán que pueden servir de apoyo comparativo en este ámbito en el derecho latinoamericano.

145 Comisión Europea, (n. 92), 1.2.
146 Comisión Europea, (n. 92), 3. Derechos fundamentales; Comisión Europea, (n. 69) 1. Derechos fundamentales.
147 Comisión Europea, (n. 69), Considerando 14
148 Muriel Ciceri, (n. 14), 65.

I. Dignidad humana

La IA y los sistemas de IA deben atender a la dignidad humana. El respetar la dignidad humana como indican Kingreen y Poscher, es una obligación del Estado, que cumple a través de la ley y su ejecución[149]. La dignidad humana es comprendida con Jarass con base en el art. 1 de la Ley Fundamental (GG) y el desarrollo jurisprudencial como "el valor social y el derecho de respeto que una persona tiene por su humanidad". Esto es, la protección de la dignidad del ser humano como esencia genérica.[150] En concreto se refiere así Stern a la "dignitas humana" como núcleo de la personalidad del ser humano, respecto a lo cual la Ley Fundamental no le concede tal cualidad, sino que la reconoce y establece como una parte fundamental de su ordenamiento como "derecho positivo suprapositivo"[151].

Una intromisión en la dignidad humana no está permitida, cuando se coloque en duda la "igualdad de un ser humano frente a otro", esto es, "cuando alguien sea tratado como un ser humano de segunda categoría".[152]

En especial, en el sentido de Lorenz "la protección de la libertad y la dignidad humana son la finalidad de toda actividad estatal…el ser humano es modelo y medida del ordenamiento jurídico objetivo"[153]. Concordantemente, tal como el Tribunal Constitucional Federal alemán expresa: "cada individuo debe ser reconocido como un miembro igual con valor inherente"[154].

En particular, si la IA es aplicada en la ejecución de las tareas de la administración pública, esta aplicación debe ser legal, conforme a la Constitución[155] y armónica con la dignidad humana[156]. Precisamente afirma Wischmayer con remisión a la dignidad humana, que el individuo a través del uso de la IA por parte del gobierno y la administración no debe convertirse en el "objeto" de la toma de decisión de la máquina.[157] Se trata de una correcta apreciación basada en la "fórmula

---

149 Thorsten Kingreen y Ralf Poscher, *Grundrechte Staatsrecht II*, 35 ed. (Heidelberg: C.F. Müller, 2019), § 7, núm. 431.

150 Hans Dieter Jarass, «Art. 1», en *Grundgesetz für die Bundesrepublik Deutschland,* ed. Hans Dieter Jarass y Bodo Pieroht (München: C.H. Beck, 2012), 42, Art. 1 núm. 6.

151 Klaus Stern, «I. Sinn und Form der Grundrechte. § 184 Idee der Menschenrechte und Positivität der Grundrechte», en *Handbuch des Staatsrechts der Bundesrepublik Deutschland. Band 12, Normativität und Schutz der Verfassung*, ed. Peter Badura et al. (Heidelberg: C.F. Müller, 2014), núm. 4, 5.

152 Jarass, (n. 150), 42, Art. 1 núm. 12.

153 Dieter Lorenz, *Der Rechtsschutz des Bürgers und die Rechtsweggarantie* (München: C.H. Beck'sche, 1973), 50, 51.

154 BVerfGE 45, 187, 1977, 144, Jarass, (n. 150), 42, Art. 1 núm. 12.

155 Hans Peter Bull, "Vom „Verwaltungsfabrikat" zur „Produktion von Dienstleistungen": Ein halbes Jahrhundert Diskussion über Informationstechnik und Verwaltung," *VM,* (2010): 65 (68).

156 Stern, (n. 151), núm. 4, 5.

157 Thomas Wischmeyer, «§20 Regierungs-und Verwaltungshandeln durch KI», en *Künstliche Intelligenz und Robotik*, ed. Martin Ebers et al. (München: C.H. Beck, 2020), núm. 45.

del fin en sí mismo" de Kant[158]. En particular, tiene aplicación el postulado kantiano según el cual "el ser humano y cada ser racional en general existe como un fin en sí mismo, no sólo como un medio de uso arbitrario para esta o aquella voluntad (…)"[159].[160] Es así como este pilar de Kant debe ser también atendido en el ámbito de la creación, desarrollo, interacción y avance de la IA.

II. Una posible clasificación de las modalidades de IA

Con base en una parte de la literatura pudiera plantearse una eventual clasificación de modalidades de IA:[161]

- *Agentes automatizados* que actúan, por ejemplo, sobre la base de algoritmos de reconocimiento de voz.[162] Este sería el caso de Cortana Alexa, Siri y ok-Google, etc.[163].[164]
- *Sistemas de actuación autónoma*. Se trata de la denominada "inteligencia [simulada]"[165]. Esto puede verse, por ejemplo, en los coches de conducción (parcialmente) autónoma.[166]
- Adicionalmente, *las máquinas que actúan más allá de los sistemas operativos autónomos*. Keßler lo ilustra con el ejemplo de un Trader-Robot "que, además de las transacciones de terceros en la bolsa (gestión de activos), gestiona paralelamente sus propias transacciones para refinanciar sus costos".[167] Igualmente, esta modalidad tecnológica permite analizar la interacción entre humanos y máquinas y su posible aplicación en las actividades de los mercados financieros.[168]

158 Immanuel Kant, *Grundlegung zur Metaphysik der Sitten*, ed. J.H. von Kirchmann (Berlin: Verlag von L. Heimann 1870), 53, 54.
159 Kant, (n. 158), 52, 53.
160 Robert Alexy, "Data und die Menschenrechte", 2000, 17, consultado el 30 de septiembre de 2023, https://www.alexy.jura.uni-kiel.de/de/download/data-und-die-menschenrechte, Kingreen y Poscher, (n. 149) § 7, 412; Muriel Ciceri, (n. 14) 65, 66.
161 Muriel Ciceri, (n. 14), 59, 60.
162 Specht y Herold, (n. 137), 40 (41 s.).
163 Specht y Herold, (n. 137), 40; Schael, (n. 20), 547 (551).
164 Schael, (n. 20), 547 (551).
165 Schael, (n. 20), 547 (551).
166 Specht y Herold, (n. 137), 40 (41 y s.)
167 Oliver Keßler, "Intelligente Roboter – neue Technologien im Einsatz," *MMR,* (2017): 589 (593).
168 Arthur le Calvez, Dave Cliff, "Deep Learning can Replicate Adaptive Traders in a Limit-Order-Book Financial Market", *EEE Symposium Series on Computational Intelligence* (2018), consultado el 30 de septiembre de 2023, https://arxiv.org/abs/1811.02880.

III. Implementación de la IA y relaciones contractuales

1. Agentes automatizados

Specht y Herold se refieren a estos sistemas como agentes que operan automáticamente, y tienen un ámbito de acción más amplio que los sistemas parcialmente automatizados como los de compra en línea automático de tinta de impresora. En tal sentido, si uno de estos agentes realiza una adquisición de un producto no solicitado "directamente" por el dueño, pero si por un tercero, como un menor de edad, surge la cuestión, de a quién es asignable la declaración de voluntad[169].

Por una parte, el aparato no es consciente de dar una declaración de voluntad. No se puede suponer que éste pudiera reconocer y evitar que su declaración se interpretara como una de voluntad de buena fe y de acuerdo con la costumbre[170]. Razón por la cual correctamente, no pudiera considerarse en el ámbito de la representación, el que la máquina dio una propia declaración de voluntad[171].

Adicionalmente indican ellas que tales requisitos de una declaración de voluntad sin conciencia de la declaración que sería impugnable según los artículos 119, 121, 143 del BGB[172], no están dados en el presente caso. De forma especial proponen una regulación similar de contratos a la del derecho de menores alemán, que establezca la obligación al fabricante de que las declaraciones de voluntad transmitidas por el agente cumplan el requisito previo de consentimiento de su propietario, de modo que se pueda derivar de ello una responsabilidad del productor.[173]

Desde la perspectiva contractual Oliver Keßler analiza el sí según los métodos de la inteligencia artificial se puede desarrollar una voluntad equiparable a la humana, caso en el cual sería viable la representación (Stellvertretung) y en caso

---

169 Specht y Herold, (n. 137), 40 (42).

170 Aquí encuentra aplicación, el caso formulado por Hermann Isay en: *"Die Willenserklärung im Tatbestande des Rechtsgeschäfts"* de 1899. Según el caso citado por Detlef Leenen, *"Un extranjero entra en una bodega en Trier, donde se realiza una subasta de vino. Entre los invitados, A ve a un conocido al que saluda. Esto es comprendido por el subastador como una oferta. Para sorpresa de A, le es adjudicado un barril de vino.", BGB Allgemeiner Teil: Rechtsgeschäftslehre* (Berlín: De Gruyter, 2011), § 30 Fallsammlung, 443.

171 Specht y Herold, (n. 137), 40 (42). Debe indicarse, además, que según la Sala Civil de la Corte Federal de Justicia de Alemania: *"…ante la ausencia de conciencia en la declaración, una declaración de voluntad sólo está presente, cuando ésta puede atribuirse como tal a la persona que hace la declaración. Esto presupone que el declarante en aplicación de la diligencia requerida en la actividad negocial (de obrar) podría haber reconocido y evitado, que su declaración o su conducta pudiera haber sido entendida por el receptor como una declaración de voluntad de acuerdo con la buena fe y con la debida consideración a los usos y costumbres del comercio".* BGHZ 91, 324, núm. 20.

172 Bürgerliches Gesetzbuch, consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/bgb/

173 Specht y Herold, (n. 137), 40 (42).

contrario, la figura del "mensajero" (Bote) para el agente, al no tener una propia voluntad sino una actuación de hecho.[174] Lo anterior se basa en que el "mensajero" (Bote), se distingue del representante o sustituto (Stellvertreter) según el § 164 BGB. La diferencia radica en dos ámbitos. Primero, el representante (Stellvertreter) actúa en nombre ajeno, pero entrega una propia declaración[175]. A diferencia del mensajero (Bote), que debe solamente[176] transmitir una declaración de voluntad ajena[177] o recibirla[178].

Adicionalmente, mientras el mensajero que puede ser un incapaz negocialmente transmite una declaración concluida[179] del dueño del negocio[180], el representante, que puede estar limitado en su capacidad negocial (de obrar)[181], y solo quiere vincular jurídicamente al representado, tiene un propio margen de decisión[182], que concierne al contenido de la declaración de voluntad[183]. Para esta delimitación es relevante la presentación externa de la persona auxiliar[184] frente a la otra parte[185]. Concordantemente, al realizar el "mensajero" (Bote) acciones fácticas (Tathandlungen)[186], puede ser éste[187], incluso un incapaz jurídicamente[188].[189]

---

174 Keßler, (n. 167), 589 (592).
175 Wolfgang Kallwass y Peter Abels, Privatrecht (München: Franz Vahlen, 2015), 89.
176 Bernd Rüthers y Astrid Stadler, Allgemeiner Teil des BGB (München: C.H. Beck, 2006), 436, núm. 8.
177 Haimo Schack, *BGB - Allgemeiner Teil* (Heidelberg: C.F. Müller., 2006) 134, núm. 453; Othmar Jauering, «§ 164», en *BGB - Bürgerliches Gesetzbuch Kommentar*, ed. Othmar Jauering (München: C.H. Beck. 2011), núm. 14.
178 Jauering, (n. 177), núm. 14.
179 Kallwass y Abels, (n. 175), 89.
180 Schack, (n. 177), 134, núm. 453.
181 Kallwass y Abels, (n. 175), 89.
182 Rüthers y Stadler, (n. 176), 436, núm. 8; Kallwass y Abels, (n. 175), 89.
183 Rüthers y Stadler, (n. 176), 436, núm. 8.
184 Schack, (n. 177), 134, núm. 453.
185 Georg Maier-Reimer, «Vor § 164 núm. 44», en *BGB: Kommentar*, ed. Harm Peter Westermann et al. (Köln: Verlag Dr. Otto Schmidt, 2014), 473, núm. 25.
186 Jauering, (n. 177), § 164, núm. 14.
187 Jauering, (n. 177), § 164, núm. 14; Kallwass y Abels, (n. 175) 89.
188 Schack, (n. 177), 134, núm. 453.
189 Debe distinguirse el *"mensajero"* (Bote) del *"representante indirecto"* (mittelbarer Stellvertreter), no regulado en el BGB (Rüthers y Stadler, (n. 176), 435, núm. 4) y el cual de acuerdo con Jauering no es representante según el § 164 BGB (Jauering, (n. 177), § 164, núm. 11), sino que como indica Leenen, *"hace declaraciones de intención...* (y)*, celebra contratos en su propio nombre y se convierte él mismo en socio contractual."* Sin embargo, ello lo realiza *"en interés de otro (el mandante), que se beneficiará de las transacciones legales en el resultado"* (Leenen, (núm. 170) 45, núm. 72). Aquí se considera la comisión según los parágrafos §§ 383 y siguientes del HGB (Código de Comercio). (Leenen, (n. 170), 45, núm. 73. Acorde con Stadler y Rüthers el comisionista según el § 383 HGB, adquiere o enajena comercialmente mercancías o valores por cuenta de otro en su propio nombre Rüthers y Stadler, (n. 176), 435, núm. 4.

El si estos procesos de pensamiento de la maquina son comparables, lo analiza Keßler con base en la inteligencia artificial fuerte. Según esta modalidad las maquinas disponen "de una comprensión en el sentido de una inteligencia o la cual está cercana a lograrse". Por el contrario, percibe a la inteligencia artificial débil como una simulación por parte del robot y no a una duplicación, en razón a que no disponen de un pensamiento autónomo. Según él, ello debe resolverse funcionalmente en cada caso, desde una perspectiva de protección a las transacciones.[190]

También analiza Keßler, la posibilidad de clasificación de los robots inteligentes como "agentes indirectos" (Erfüllungsgehilfen) de los humanos, caso en el cual según el § 276 del Código Civil (BGB) y el § 278 frase 1 BGB, también responde el deudor o dueño del negocio por los comportamientos culpables del "Erfüllungsgehilfe"[191]. Un agente indirecto (Erfüllungsgehilfe) es según Jauering, aquel que, de acuerdo con las circunstancias puramente fácticas y con la voluntad del deudor, actúa como persona auxiliar en el cumplimiento de una obligación que incumbe a éste. Por lo tanto, la actividad asistencial debe presentarse como una cooperación en el cumplimiento del contrato que el deudor quiso y aprobó[192]. Empero, Keßler no considera a tales robots como una simple herramienta técnica[193]. Por su parte Wendehorst y Grinzinger son de la opinión que, ante los daños causados como consecuencia del uso de un agente de software para la ejecución de un contrato, si bien la mayoría de la literatura descarta "la aplicación análoga del artículo 278" BGB, sería ésta "preferible".[194] Adicionalmente resaltan que la aplicación de la IA puede darse en ambas partes del contrato (Machine to Machine (M2M)).[195] En todo caso, descartan la aplicación a los agentes de software de los principios desarrollados para una "declaración computacional"[196].[197] Sin

[190] Keßler, (n. 167), 589 (592).
[191] Keßler, (n. 167), 589 (592).
[192] Jauering, (n. 177), § 278, núm. 6.
[193] Keßler, (n. 167), 589 (592).
[194] Christiane Wendehorst y Julia Grinzinger, «§ 4 Vertragsrechtliche Fragestellungen beim Einsatz intelligenter Agenten», en *Künstliche Intelligenz und Robotik*, ed. Martin Ebers et al. (München: C.H.Beck, 2020), núm. 91.
[195] Wendehorst y Grinzinger, (n. 194), núm. 87.
[196] Wendehorst y Grinzinger, (n. 194), núm. 87.
[197] Una declaración computacional se entiende por Christoph Sorge, como una declaración de voluntad generada automáticamente por una computadora, y asimismo transmitida a la computadora del receptor, *Softwareagenten. Vertragsschluss, Vertragsstrafe, Reugeld* (Karlsruhe: Universitätsverlag Karlsruhe, 2006), 24. Según Harald J. Th. Hahn y Thomas Wilmer, se presenta una declaración computacional, cuando el comerciante de una tienda en línea permite que la computadora sin la intervención de un ser humano trabaje la orden de compra debido a un programa dado y conteste con un email, lo que configura una declaración de voluntad automatizada, comprendida como declaración computacional, «Der Vertragsschluss», en *Handbuch Des Fernabsatzrechts* (Wien: Springer, 2005), 29, núm. 16. Este método se utiliza también según Frank Fechner, cuando la decisión de

embargo son de la opinión, que los problemas contractuales de los puntos que requieren regulación se pueden solucionar previamente a través de la autonomía de la voluntad en contratos marco o contratos de plataforma.[198]

2. Sistemas de actuación autónoma

De los agentes que operan automáticamente, Specht y Herold distinguen los sistemas operativos autónomos[199]. En estos el propietario no adopta una configuración predeterminada o instrucciones que permitan establecer la declaración de voluntad dada como propia, sino que controla únicamente las condiciones generales técnicas en las que se basa la decisión del sistema[200]. En este ámbito consideran que la figura del mensajero (Bote) no tiene aplicación, toda vez que no hay una declaración de voluntad del propietario del sistema sino una declaración producida a través de algoritmos por el sistema[201], basada en el deep-learning[202]. Entonces si estos sistemas no transmitieran una declaración de voluntad de su propietario, sería acorde con Specht y Herold, su no cualificación como "mensajeros". Independientemente de si tales pueden formar una propia voluntad, consideran las autoras que los instrumentos de la representación pudieran ser comparativamente aplicables, al analizar que según los §§ 164 y siguientes del BGB su declaración puede tener efectos a favor y en contra del propietario del sistema cuando esta resulta de un poder de representación[203].

Simultáneamente reflexionan su tratamiento similar como un representante menor de edad, toda vez que, en armonía con el § 165 BGB la limitación de capacidad no afecta la eficacia de la declaración de voluntad, sin embargo, debido a la ausencia de un propio patrimonio, el sistema tampoco puede responder en el sentido del § 179 III BGB[204]. Concordantemente establecen que hasta tanto no sea posible técnicamente asegurar que el sistema mediante una configuración no supera su poder de representación, se debe dar la posibilidad al contratante de reconocer

celebrar un contrato depende de la observación del mercado como en la venta de acciones ante la caída del precio o en su oferta en un umbral específico. En tales operaciones según Frank Fechner, ante la imposibilidad de determinar si la declaración fue dada por un ser humano, se consideran como vinculantes las confirmaciones de pedidos generadas automáticamente por la computadora del vendedor y en este sentido a quien se sirvió a través de la programación de la computadora para dar la declaración de voluntad, *Medienrecht* (Tübingen: Mohr Siebeck UTB, 2008), 197, núm. 197.

198 Wendehorst y Grinzinger, (n. 194), núm. 88.

199 Specht y Herold, (n. 137), 40 (42, 43).

200 Specht y Herold, (n. 137), 40 (42, 43).

201 Specht y Herold, (n. 137), 40 (43).

202 Specht y Herold, (n. 137), 40 (41).

203 Specht y Herold, (n. 137), 40 (42, 43).

204 Specht y Herold, (n. 137), 40 (43).

según el principio de patencia (Offenkundigkeitsprinzip)[205], que el acuerdo sería con un sistema autónomo y de ser el caso rechazarlo[206].

Este principio se refiere a que el representante en su declaración dirigida a crear un negocio jurídico debe expresar claramente que actúa para otra persona como representada, y las consecuencias jurídicas de su declaración afectan a ésta[207]. Por tal motivo debe existir un acuerdo "sobre la referencia a terceros", de modo que el contrato se realice entre el representado y el contratante[208]. Esta es la exigencia del § 164 II BGB respecto a que sea reconocible la voluntad de actuar en nombre de otro. En caso contrario según Leenen "las declaraciones se consideran hechas en nombre propio y el contrato se celebra entre las personas de las que proceden las declaraciones de intención"[209]. Por ello indican Specht y Herold la necesidad de que el contratante pueda reconocer que el sistema actúa en nombre de un tercero[210].

Finalmente, Specht y Herold proponen regular la celebración de contratos con la participación de sistemas automatizados y sistemas operativos autónomos. Respecto a quienes consideran que la representación es humana, se refieren a la perspectiva de aquellos sobre la posibilidad del reconocimiento de la categoría de personas electrónicas a los sistemas autónomos, quienes tendrían una capacidad limitada para cerrar contratos de su titular. No obstante, precisamente Specht y Herold al analizar la exclusión de responsabilidad del representante limitado en su capacidad negocial según el § 179 III BGB, y en semejanza con la situación del menor de edad, no consideran que tal persona electrónica sería responsable directamente y debería tener bienes[211].

Por las razones indicadas más adelante, no se considera viable jurídicamente, así como tampoco adecuado o proporcional la creación de una categoría de personas electrónicas en el estadio actual del desarrollo de la civilización humana y de la tecnología con sus correspondientes límites, (D. III. 3, IV. 6).

3. Más allá de los sistemas operativos autónomos

Keßler planteó en el año 2017, en el evento que el "robot inteligente" cause un daño y actúe autónomamente según la inteligencia fuerte, el análisis de la posibilidad de que actuó con culpa en el sentido del § 276 BGB (responsabilidad del deudor). En este contexto propone la ampliación de la obligación de seguros conforme a la ley

205 Leenen, (n. 170), 48, núm. 88.
206 Specht y Herold, (n. 137), 40 (43).
207 Rüthers y Stadler, (n. 176), 440, núm. 5, Leenen, (n. 170) 49, núm. 88.
208 Leenen, (n. 170), 49, núm. 88.
209 Leenen, (n. 170), 49, 50, núm. 88, 50, núm. 89.
210 Specht y Herold, (n. 137), 40 (43).
211 Specht y Herold, (n. 137), 40 (43).

de seguro obligatorio de automóviles[212] aplicable a los vehículos autónomos.[213] Adicionalmente plantea el analizar la posibilidad de la adquisición de propiedad por el robot, de modo que el mismo pueda reparar los daños causados. Como ejemplo se refiere al Trader-Robot, que además de realizar negocios en bolsa para terceros, pudiera desarrollar negocios y ganancias para refinanciar sus costos.[214] Ahora bien, frente a ello debe considerarse, que el disponer de un porcentaje de recursos de una operación económica es viable, sin la necesidad de un reconocimiento parcial de derechos o similar a una máquina, que podrá en consecuencia, generar, motivar y fomentar la evasión de responsabilidades y de las obligaciones legales, en detrimento de los derechos de los afectados[215] y consecuentemente también, causar perjuicios en los mercados.

El segundo planteamiento genera además de cuestiones como las referentes al reconocimiento legal a una máquina de capacidad jurídica (Rechtsfähigkeit), comprendida como aquella, que permite ser titular de derechos y obligaciones[216] así como de capacidad negocial (Geschäftsfähigkeit), "que permite fundar derechos y obligaciones a través de declaraciones de voluntad propias"[217], y la de reconocimiento de patrimonio, comprendido como derechos[218] de la persona sobre objetos del derecho[219]. Con todo, como a bien indican Wendehorst y Grinzinger, por ejemplo, los agentes de software "no tienen voluntad", sino que *se limitan "a ajustar su" proceder "mediante el aprendizaje automático en función de determinados objetivos de optimización según la experiencia adquirida a través del reconocimiento de patrones"*.[220]

En especial, *los elementos de una propia voluntad por parte de la IA o una conciencia de ésta respecto a la declaración de un tercero*[221], *no están presentes en el ámbito de los sistemas de IA*, por ello, consecuentemente, una categoría de persona electrónica o de reconocimiento de capacidad jurídica o similar frente a ésta, no debe ser admisible.

Tal como indica Ebers, *tampoco debe darse un reconocimiento de subjetividad jurídica parcial de las máquinas inteligentes*[222]. Los sistemas de inteligencia artificial pueden contener problemas de localización frente a su estructura, reproducción, modificación, fusión, duplicación etc., que no son superables simplemente desde un

212 Gesetz über die Pflichtversicherung für Kraftfahrzeughalter, consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/pflvg/BJNR102130965.html
213 Keßler, (n. 167), 589 (593).
214 Keßler, (n. 167), 589 (593).
215 Martin Ebers, «Regulierung von KI und Robotik», *Künstliche Intelligenz und Robotik. Rechtshandbuch,* ed. Martin Ebers et al. (München: C.H. Beck, 2020), § 3, 75-80.
216 Rüthers y Stadler, (n. 176), 90, núm. 2.
217 Schack, (n. 177), 15, núm. 53.
218 Kallwass y Abels, (n. 175), 116.
219 Rüthers y Stadler, (n. 176), 86, núm. 1.
220 Wendehorst y Grinzinger, (n. 194), núm. 92.
221 Specht y Herold, (n. 137), 40 (42).
222 Ebers, (n. 215), § 3, 76.

sistema de registro.[223] También pudiera ello generar la desventaja de activos inmovilizados sin daño, así como un aumento desproporcional del riesgo de las personas perjudicadas cuando se agotaran los recursos asignados a los sistemas de IA por ejemplo en fondos de responsabilidad.[224] Estos fondos además generarían la problemática de quienes serían los obligados a su financiación. [225] Asimismo, generarían estos eventos más obstáculos que soluciones a la protección efectiva de derechos.[226]

IV. El derecho de regulación y otros aspectos

Como se indicó anteriormente,[227] la regulación es una parte de la tipología de la actuación de la administración pública.[228] En este contexto, el concepto de regulación de tres niveles en el sentido de Schmidt-Preuß encuentra aplicación en el ámbito del derecho de la inteligencia artificial en los niveles II y III. Según el análisis de Merk de esta clasificación, en la categoría I se presentan monopolios naturales que generan la necesidad de regulación en las industrias de red.[229] En la categoría II, la "regulación sistémica-infraestructural" se implementa frente a sectores de la economía significativos para el equilibrio y el funcionamiento de la economía. El mercado de capitales y el sector de seguros son ejemplos de ello.[230] En la categoría III se encuentra la regulación social, comprendida como aquella con la que busca la regulación "orientar objetivos de bienestar público en otros ámbitos de la economía diferentes a las industrias de red y los mercados financieros".[231] Esta regulación se refleja en medidas de política económica expresadas "en normas y restricciones"[232].

Adicionalmente debe considerarse, que una parte general del derecho de regulación respecto a la estructura y formas de actuación de la administración reguladora, son aquellas correspondientes al "ingreso al mercado", así como las que "afectan el comportamiento" en este y las de "ampliación de infraestructuras"[233].[234] En consecuencia, en la regulación en materia de IA, puede acudirse a los niveles I y II

[223] Ebers, (n. 215), § 3, 76.
[224] Ebers, (n. 215), § 3, 77.
[225] Ebers, (n. 215), § 3, 78.
[226] Ebers, (n. 215), § 3, 79,80.
[227] Muriel Ciceri, (n. 14), 61.
[228] Josef Ruthig, «§ 22. Gewährleistungs- und Regulierungsverwaltung», en *Handbuch des Verwaltungsrechts*, *Bd. I*, ed. Wolfgang Kahl y Markus Ludwigs (Heidelberg: C.F. Müller GmbH, 2021).
[229] Sebastian Merk, "Grenzen der Regulierung", en *Regulierender Staat und konfliktschlichtendes Recht, Festschrift für Matthias Schmidt-Preuß zum 70. Geburtstag* (Berlin: Duncker & Humblot, 2018), 719.
[230] Merk, (n. 229), 719.
[231] Merk, (n. 229), 720.
[232] Merk, (n. 229), 715.
[233] Ruthig, (n. 228), § 22, núm. 27 y s.
[234] Muriel Ciceri, (n. 14), 61.

del concepto de regulación así como las formas de actuación de la administración reguladora correspondientes. Lo anterior no debe conducir a una sobrerregulación y al mismo tiempo, debe realizarse dentro de la proporcionalidad.

Es así como Windoffer es de la opinión que más allá del planteamiento basado en los riesgos de la Comisión Europea, es necesario regular ámbitos especiales de aplicación de la IA.[235] En armonía con este contexto, se realizará una remisión a autores adicionales de la doctrina alemana y a un propio planteamiento.

1. Límites a la inserción de la IA en las intervenciones estatales

El primero de ellos se refiere a la inserción de la IA en las intervenciones estatales, la cual por regla general no es admisible en los derechos fundamentales de ciudadanos y de las empresas en el ámbito civil.[236]

a. Límite frente a una completa automatización de actos administrativos a proferirse en ámbitos de discrecionalidad y de margen de apreciación:

Este límite y en consecuencia, *la no admisibilidad de la inserción de la IA en las intervenciones estatales* se encuentra también, a la luz del § 35a de la Ley de Procedimiento Administrativo (VwVfG)[237] (emisión completamente automatizada de un acto administrativo) y el artículo 22 del Reglamento Europeo General de Protección de Datos[238] (Decisiones individuales automatizadas, incluida la elaboración de perfiles) en la *no admisibilidad de una completa automatización de actos administrativos*[239] *a proferirse en ámbitos de discrecionalidad y de margen de apreciación*. El límite

---

235 Alexander Windoffer, "Öffentlich-rechtliche Regulierung des Einsatzes künstlicher Intelligenz," *GewArch,* (2022): 130 (132 y s.).

236 Windoffer, (n. 235), 130 (132).

237 § 35a, Verwaltungsverfahrensgesetz (VwVfG), consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/vwvfg/__35a.html

238 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679

239 Sobre los límites a las decisiones completamente automatizadas, Annette Guckelberger, "E-Government: Ein Paradigmenwechsel in Verwaltung und Verwaltungsrecht?", en *Gleichheit, Vielfalt, technischer Wandel, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, VVDStRL* 78 (Berlin: De Gruyter 2019), 235 (272), doi: https://doi.org/10.1515/9783110645651; Annette Guckelberger, *Öffentliche Verwaltung im Zeitalter der Digitalisierung. Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht*, (Baden-Baden: Nomos, 2019), núm. 428, 429; Gabriele Britz y Martin Eifert, «Digitale Verwaltung», en *Grundlagen des Verwaltungsrechts*, ed. Andreas Voßkuhle, Martin Eifert y Christoph Möllers, 3. ed. (München: C.H. Beck, 2022), § 26 núm. 90; Markus Ludwigs, y Annika Velling, «Vollautomatisierte Verwaltungsakte im deutschen Recht», en *Digitalization as a challenge for justice and administration*, ed. Markus Ludwigs, José Hernán Muriel Ciceri y Annika Velling (Würzburg: Würzburg University Press, 2023), 53 y s.; adicionalmente desde la perspectiva de los límites del de-

se presenta ante esta modalidad de actos administrativos, por virtud del "mandato de vinculación de la administración y de la justicia a la ley", así como de "la garantía de protección jurídica efectiva".[240] En particular, Ludwigs y Velling se refieren además entre otros aspectos a que este límite está dado por la consideración de la "justicia en el caso concreto", de la "no disminución de las garantías constitucionales"[241] así como del derecho de protección de datos[242]. Adicionalmente consideran Ludwigs y Velling en este contexto, que la completa automatización de un acto administrativo pudiera ser viable "en el caso de una reducción a cero", derivada "de disposiciones administrativas u otras razones generalizables"[243].[244] Sin embargo, descartan esta posibilidad frente a "una reducción basada en las particularidades del caso concreto", toda vez que ello requeriría la evaluación y la determinación por un algoritmo, situación que descartan técnicamente en la actualidad.[245]

b. Límite frente a la inserción de la inteligencia artificial en la intervención estatal frente a la interpretación de conceptos jurídicos indeterminados:

El *límite y no admisibilidad de inserción de la inteligencia artificial en la intervención estatal* en mención se presenta también *frente a la interpretación de conceptos jurídicos indeterminados*, por razón de desbordar esa forma de análisis las posibilidades de la tecnología contemporánea[246], frente al caso concreto, así como en este ámbito, los propios límites de la tecnología.

---

recho europeo y del derecho constitucional, Markus Ludwigs y Annika Velling, „Der vollständig automatisierte Verwaltungsakt in den Grenzen des Europa- und Verfassungsrechts," *VerwArch* (2023): 72-106., Muriel Ciceri, (n. 14), 67.

[240] Windoffer, (n. 235), 130 (132).

[241] Ludwigs y Velling, (n. 239), 53, 54; Ludwigs y Velling, (n. 239) 72-106.

[242] En particular del artículo 22 del reglamento europeo general de protección de datos Ludwigs y Velling, (n. 239), 72 (86 y s., 106); cf. Reglamento (UE) 2016/679, (n. 238).

[243] Ludwigs y Velling, (n. 239), 72 (81).

[244] Como se indicó en *"el caso especial de una reducción de la discrecionalidad a cero, [...] sólo una de las opciones de actuación resulta libre de error discrecional, de modo que la autoridad está obligada a "elegirla""*, Markus Ludwigs y José Hernán Muriel Ciceri, «Densidad de control de los tribunales administrativos en Alemania – Fundamentos dogmáticos y marco constitucional», en *Derecho administrativo y desarrollo sostenible, Verwaltungsrecht und nachhaltige Entwicklung,* ed. Markus Ludwigs y José Hernán Muriel Ciceri (Würzburg: Würzburg University Press), (17 (n. 7)), con remisión a Hartmut Maurer y Christian Waldhoff, *Allgemeines Verwaltungsrecht*, 2017, (§ 7 núm. 24 y s.), consultado el 30 de septiembre de 2023, https://opus.bibliothek.uni-wuerzburg.de/opus4-wuerzburg/frontdoor/deliver/index/docId/32352/file/978-3-95826-149-5_Ludwigs_MurielCiceri_OPUS_32352.pdf.

[245] Ludwigs y Velling, (n. 239), 72 (81).

[246] Windoffer, (n. 235), 130 (132), Ludwigs y Velling, (n. 239), 53.

c. Límite frente al sopesamiento de intereses, un margen de apreciación y una valoración:

Ahora bien, si se consideran las diferencias entre la inteligencia natural y la IA, así como el planteamiento de Gödel referente a los límites de las máquinas[247], *tampoco debe ser viable a los sistemas de inteligencia artificial un sopesamiento de intereses, un margen de apreciación y una valoración en los sentidos mencionados*.[248] Razón por la cual los actos administrativos a proferirse en los ámbitos de discrecionalidad y de margen de apreciación así como la interpretación de los conceptos jurídicos indeterminados en los casos concretos*, deben permanecer en el ámbito de la inteligencia humana.*[249] Este planteamiento, (que incluye la protección constitucional de derechos fundamentales y el derecho de protección de datos), también debe aplicar como límite, a la adopción de decisiones en otros ámbitos, como por ejemplo, en la administración de justicia[250], en la apreciación racional de la prueba, o en el ejercicio del derecho privado y en las demás áreas del derecho, que exijan tales *formas y dimensiones de sopesamiento y valoración correspondientes al ser humano y en cada caso en particular*.

2. Prestaciones estatales

En el caso de prestaciones estatales como las sociales o en el caso de acceso a la infraestructura estatal de servicios de interés general como previsiones de existencia ("Daseinsvorsorge"[251]),[252] tales como el suministro de energía o de eliminación de residuos o de salud o de educación etc., debe existir una regulación estricta para evitar a través de la IA una exclusión vulneradora de los derechos fundamentales de los beneficiarios. Con este objeto propone Windoffer un control preventivo del titular administrativo de la prestación por la autoridad competente, por ejemplo, de protección de datos, ante la cual deberá por una parte exponer los códigos de programación, bases de datos y procedimientos de aprendizaje y de forma similar a

247 Evers, (n. 31), 101 (108); Gödel, (n. 31), 375 (384 y s.), Muriel Ciceri, (n. 14).
248 Muriel Ciceri, (n. 14).
249 Muriel Ciceri, (n. 14).
250 Windoffer, (n. 235) 130 (134).
251 Concepto acuñado por Ernst Forsthoff en el derecho alemán. Cf. Ernts Forsthoff, *Lehrbuch des Verwaltungsrechts*, 1 Band, 9. Auflage, Vorbem. Vor § 19, (München: Ed. C.H. Beck´sche Verlags-buchhandlung, 1966), 342. El cual es correspondiente a la *"administración de prestaciones"*. En este sentido, Stefan Fisch, «§ 2 Verwaltung im langen 19. Jahrhundert», en *Handbuch des Verwaltungsrechts*, *Bd. I*, ed. Wolfgang Kahl y Markus Ludwigs (Heidelberg: C.F. Müller GmbH, 2021), núm. 74; José Hernán Muriel Ciceri, "¿La concesión portuaria, como una modalidad de privatización?," Pensamiento Jurídico (2011), 343 (378), consultado el 30 de septiembre de 2023, https://repositorio.unal.edu.co/bitstream/handle/unal/71716/36722-155146-1-PB.pdf?sequence=2&isAllowed=y.
252 En virtud de las cuales, correctamente en el sentido de Lorenz, es obligación del Estado la creación, mejora y conservación de las posibilidades de vida, así como de calidad de ésta para sus miembros, Dieter Lorenz, "Die öffentliche Sache als Instrument des Umweltschutzes," *NVwZ* (1989): 812, (814); sobre ello Muriel Ciceri, (n. 251), 343 (378).

un análisis de impacto ambiental, deberá elaborar y presentar una evaluación de impacto del riesgo. La autoridad competente decidiría la autorización en discrecionalidad sobre la base de un análisis de riesgos y utilidades, la cual continuaría frente a la entidad solicitante, en una función de supervisión.[253]

3. Regulación sectorial

Adicionalmente aboga Windoffer por una regulación sectorial, en el evento que se tratara de decisiones de particulares con la aplicación de la IA sobre prestaciones substitutas o equivalentes de las estatales que son esenciales para la existencia de la humanidad, como el abastecimiento de energía o los seguros de salud en cumplimiento de un encargo estatal o cuando el particular tiene una posición monopolista o dominante en el mercado o si, en caso de pluralidad de sistemas, el uso de la IA podría modificar las condiciones marco en detrimento de los clientes potenciales de la oferta de servicios del sector privado.[254]

4. Prohibición preventiva con reserva autorización

En los demás ámbitos de actividad del sector privado de intensidad en los derechos fundamentales con la aplicación de la IA, se refiere a una menor dimensión en la regulación, que permitiera según el potencial de riesgo en el ámbito de "una prohibición preventiva con reserva autorización", en lugar de una obligación de licencia, como sería, por ejemplo, un deber de comunicación o una menor dimensión de los deberes de información o en la frecuencia de la supervisión.[255]

5. Límite de la regulación

En el ámbito de las decisiones privadas con ánimo de lucro que no son intensivas en los derechos fundamentales, y frente a las cuales los proveedores de productos o servicios apoyados en la IA y sus clientes deben ser tratados "por el Estado como responsables, autónomos y autodeterminados" en el ejercicio jurídico y "en principio fáctico" de sus derechos fundamentales, es de la opinión de limitar, la regulación estatal a obligaciones de transparencia y a la reducción de las asimetrías de la información existentes. Caso en el cual, las "patologías de estas interacciones" puedan contrarrestarse con la normativa general y el derecho de la competencia.[256]

6. Límite a una categoría de personas electrónicas frente a los sistemas de IA

En especial, tampoco se requiere una categoría de personas electrónicas frente a los sistemas de IA. [257] Ello en razón a que el objeto de la regulación es la aplicación de

[253] Windoffer, (n. 235) 130 (133).
[254] Windoffer, (n. 235), 130 (133).
[255] Windoffer, (n. 235), 130 (133, 134).
[256] Windoffer, (n. 235), 130 (134).
[257] Windoffer, (n. 235), 130 (134).

la IA "por parte de personas físicas o jurídicas como fabricantes, proveedores o usuarios de productos o servicios". [258] Son tales personas las destinatarias de las normas de control preventivo y posterior por el uso de la IA. Este planteamiento aplicaría aún ante una creación futura de una IA fuerte por los sistemas de IA. [259] La razón de ello es que estos sistemas "no actúan por voluntad propia para sí mismos, sino para un usuario con una finalidad determinada por éste". [260] Asimismo, la existencia y utilización de esta IA se deriva de "un proceso de desarrollo y producción del que son responsables personas físicas o jurídicas, a quienes puede vincularse legalmente" a través de la atribución a los responsables de la conducta, de la condición o de la infracción. [261] *Concordantemente no es necesario dotar "de derechos y obligaciones a [un] objeto de esa responsabilidad".* [262]

7. Administración estatal mediata, public–private partnership, public– public partnership

Adicionalmente a los aspectos propuestos por Windoffer, puede fomentarse el desarrollo de la IA a través de modalidades de administración estatal mediata (mittelbare Staatsverwaltung), como sería en particular, la modalidad del Estado como empresario[263] (y cooperativo) en el ámbito de asociaciones público-privadas (public–private partnership) o público-públicas (public– public partnership).[264] En este caso, por ejemplo, la aplicación de herramientas del derecho privado en el mercado por parte de una asociación público pública no le exime de su vinculación permanente a las obligaciones de derecho público en el sentido de Ehlers[265].[266] Ello permitiría además, el fomento de la innovación, el desarrollo sostenible y la competitividad, a través del Estado, como un jugador más en un mercado regulado de IA, así como en los ámbitos "donde aún es necesario desarrollar la oferta[267]", y

[258] Windoffer, (n. 235), 130 (134).
[259] Windoffer, (n. 235), 130 (134).
[260] Windoffer, (n. 235), 130 (134).
[261] Windoffer, (n. 235), 130 (134).
[262] Windoffer, (n. 235), 130 (134).
[263] Ante todo, Stefan Storr, *Der Staat als Unternehmer*, (Tübingen: Mohr Siebeck, 2001), 471 y s.; sobre ello Muriel Ciceri, (n. 251), 343 (379, n. 123).
[264] Hartmut Maurer y Christian Waldhoff, *Allgemeines Verwaltungsrecht,* (München: C.H.Beck, 2018), 628; Martin Burgi, *Funktionale Privatisierung und Verwaltungshilfe: Staatsaufgabendogmatik, Phänomenologie, Verfassungsrecht*, (Tübingen: Ed. Mohr Siebeck, 1999), 98; Wolfgang Kahl, " Die Privatisierung der Wasserversorgung," GewArch, (2007): 441 (446); Muriel Ciceri, (n. 251), 343 (378); José Hernán Muriel Ciceri, *Die Übertragung der Abfallentsorgung auf Dritte*, (Konstanz: Ed. Hartung-Gorre Verlag, 2006).
[265] Dirk Ehlers, «Verwaltungsverfahren», *Allgemeines Verwaltungsrecht*, ed. Hans-Uwe Erichsen y Dirk Ehlers (Berlin: Ed. De Gruyter Recht, 2006), 154, núm. 81; Muriel Ciceri, (n. 251) 343 (375); (n. 264).
[266] Muriel Ciceri, (n. 251), 343 (374, 376).
[267] Wolfgang Durner, «§ 21 Infrastrukturverwaltung», en *Handbuch des Verwaltungsrechts*, *Bd. I*, ed. Wolfgang Kahl y Markus Ludwigs (Heidelberg: C.F. Müller GmbH, 2021), núm. 31.

el cual tendría así, otra posibilidad de consecución de recursos para el cumplimiento de sus obligaciones asignadas constitucional- y legislativamente.

V. Riesgos en la conducción autónoma

Adicionalmente a las reglas de las propuestas europeas de responsabilidad civil extracontractual y de responsabilidad por productos defectuosos a las que se ha hecho referencia, considera Keßler en 2017, según los principios del derecho civil que el robot debe ser programado, de modo que pueda reconocer diferentes bienes jurídicos, como el distinguir entre un animal o una cosa, y en caso de bienes jurídicos del mismo rango es él de la opinión que pudiera utilizarse un generador aleatorio[268]. Con todo, desde el derecho penal, Schuster analiza la responsabilidad derivada de accidentes de tránsito con automotores con función de conducción alta- o totalmente automatizada, sobre la base de la regulación de la Ley alemana de Transporte por Carretera (StVG)[269].[270] Esta regulación autoriza el funcionamiento de tales vehículos con el cumplimiento de los requisitos establecidos en el § 1a II Nro. 1 a 6 StVG (Vehículos de motor con función de conducción altamente automatizada o totalmente automatizada). Al examinar el § 1b I StVG (Derechos y obligaciones del conductor del vehículo al utilizar funciones de conducción alta- o totalmente automatizadas), se establece la ausencia de una exigencia de vigilancia permanente del sistema por el conductor durante una conducción alta- o totalmente automatizada. Por ello se dirige la atención al productor y entran en consideración las reglas del derecho civil y de la Ley de Responsabilidad por Productos Defectuosos (ProdHaftG[271]).[272]

Sin embargo no asegura la ausencia de accidentes automovilísticos por una persona física o un vehículo de conducción automatizada, la aplicación del deber de cuidado del § 1a Nro. 2 II StVG, y los §§ 2 siguientes del Código de Circulación (StVO)[273], así como la exigencia de una mayor precaución según el § 3 Nro. 2a StVO respecto a niños, personas necesitadas de asistencia y personas de edad, con la reducción de velocidad del vehículo y frenado, de modo que no se ponga en peligro

[268] Keßler, (n. 167) 589 (593).
[269] Straßenverkehrsgesetz, consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/stvg/.
[270] Frank Peter Schuster, "Strafrechtliche Verantwortlichkeit der Hersteller beim automatisierten Fahren," *DAR* 1 (2019): 6-11.
[271] Gesetz über die Haftung für fehlerhafte Produkte, consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/prodhaftg/.
[272] Schuster, (n. 270), 6.
[273] Straßenverkehrs-Ordnung, consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/stvo_2013/.

a estos usuarios de la vía pública. Toda vez que al ejecutarse la operación de conducción permanecen elementos impredecibles.[274]

Si bien ante vulneraciones graves a la vida y la integridad pudiera pensarse en los contenidos del derecho penal,[275] debe considerarse que en el derecho alemán la sanción penal se dirige a las personas naturales[276]. En particular como indica Schuster, el análisis se dirigiría a la identificación de las personas que participaron en el proceso de desarrollo y producción, como gerentes, empleados etc., quienes pueden ser llegar a ser acusados de negligencia personal[277]. Así indica la posibilidad de la aplicación según el § 212 del Código Penal (StGB)[278] del tipo penal de homicidio, al fabricante o a empleados individuales, en el evento que un automóvil de conducción automatizada sea programado para que, de ser necesario, pudiera ser atropellado un peatón para salvar a un mayor número de personas[279]. Frente a lo cual pudiera considerarse un dolo eventual (bedingter Vorsatz), cuando el desarrollador prevé como posible el poner en marcha una cadena causal que ocasiona la muerte de una persona. No obstante, ante la baja probabilidad de acaecimiento del hecho dañino, plantea él la posibilidad de la programación de algoritmos de emergencia.[280] Adicionalmente expresa Schuster, la inaplicabilidad de un estado de necesidad justificante en el sentido del § 34 StGB, en razón a "que toda vida humana tiene el mismo rango y escapa a cualquier cuantificación". Tampoco considera eficaz el exigir al fabricante del automotor una programación según la cual, en una situación de dilema, tuviera que tomar el relevo el ser humano (§ 1a II Nro. 5 StVG).[281] Es el sistema como él indica, el que debería tener una capacidad de reacción superior a la humana[282]. Ello al considerar que el § 1a Nro. 5 II StVG se refiere a que tales automotores disponen de un equipo técnico que además de lo regulado en los numerales 1-4 y 6 es capaz de indicar al conductor, visualmente, acústicamente, táctilmente o de otra manera, la necesidad de un control

274 Schuster, (n. 270), 6 (8).
275 Schuster, (n. 270), 6, (7).
276 Schuster, (n. 270), 6 (9); Lars Teigelack y Christian Dolff, "Kapitalmarktrechtliche Sanktionen nach dem Regierungsentwurf eines Ersten Finanzmarktnovellierungsgesetzes - 1. FimanoG," *BB* (2016): 387 (390, 391, 393); Wilfried Bottke, "Täterschaft und Teilnahme im deutschen Wirtschaftskriminalrecht – de lege lata und de lege ferenda," *JuS* (2002): 320-324; Wilfried Bottke, «Bestrafungen von Unternehmen und Betrieben nach dem Recht der Europäischen Union in Deutschland?», en *Europa, Festgabe zum 30-jährigen Bestehen der Juristischen Fakultät Augsburg*, ed. Wilfried Bottke, Thomas M. J. Möllers y Reiner Schmid (Baden-Baden: Nomos, 2003) 63-86.
277 Schuster, (n. 270), 6 (7).
278 Strafgesetzbuch (StGB), consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/stgb/index.html#BJNR001270871BJNE038302307
279 Schuster, (n. 270), 6 (10).
280 Schuster, (n. 270), 6 (10).
281 Schuster, (n. 270), 6 (10).
282 Schuster, (n. 270), 6 (10).

manual del vehículo con suficiente reserva de tiempo antes de que el control del vehículo sea entregado al conductor.

La decisión del cómo se debe comportar el automotor no se adopta en general, en el momento o directamente antes del accidente, sino mucho antes.[283] Esto es, al momento de la programación, con miras a un posible acontecimiento peligroso con participantes aún desconocidos, sin que alguien tenga una posición jurídica asegurada.[284] Debe analizarse que en el momento de la programación no existen fundamentos jurídicos obligatorios para privilegiar a una u otra víctima potencial, tampoco puede ser un factor de distinción aquel que vulnere la dignidad humana.[285]

Por otra parte, tal como él indica "el ordenamiento jurídico no puede exigir a nadie lo imposible". Es así como un programador que reduce el riesgo de accidente para cada persona, que es aceptado hasta el momento como "permitido" (y no tiene una mejor alternativa), no crea en el momento del hecho un peligro jurídico-penalmente desaprobado (§ 8 StGB). Ello sería incompatible con la creación de un privilegio para un grupo específico con el aumento general del riesgo para los demás.[286]

En particular establece Schuster que el conductor tiene responsabilidad solamente en tanto él domine y controle el sistema automático. Por ello adquiere relevancia la responsabilidad del productor. Concordantemente entran en consideración los §§ 222 sobre homicidio culposo y 229 sobre lesión personal culposa, así como el § 315b StGB sobre intervenciones peligrosas en el tráfico vial por daños en bienes o la simple puesta en peligro.[287] Sin embargo, resalta como el productor actúa diligentemente cuando coloca el producto en el mercado de forma acorde al estado de la ciencia y la técnica, quien, a la vez, tiene una obligación de cuidado del producto y de asesoría.[288] La pregunta según Schuster sería, el cómo ex – ante, la nueva tecnología está en capacidad de disminuir el número de víctimas. Aquí propone él la aplicación de algoritmos de emergencia en automotores con función de conducción alta- o totalmente automatizada que considera sería "armónica con el derecho penal alemán aplicable y la garantía de la dignidad humana" en el sentido del artículo 1 I de la Ley Fundamental.[289]

VI. Relaciones jurídicas entre empresas

En especial, tal como Spindler resaltó, en el ámbito de las propuestas europeas de derecho de responsabilidad de IA es necesario tener presente, que su objeto está

[283] Schuster, (n. 270), 6 (11).
[284] Schuster, (n. 270), 6 (11).
[285] Frank Peter Schuster, "Notstandsalgorithmen beim autonomen Fahrzeug," *RAW* (2017): 13 (16).
[286] Schuster, (n. 270), 6 (11).
[287] Schuster, (n. 270), 6 (11).
[288] Schuster, (n. 270), 6 (11).
[289] Schuster, (n. 285), 13, 18.

dirigido a la protección de derechos del consumidor.[290] Razón por la cual debe considerarse también la construcción de la normatividad correspondiente para la protección de derechos en las relaciones jurídicas entre empresas (B2B).[291] Su planteamiento en materia de responsabilidad civil en el derecho interno de Alemania, también pudiera tenerse en cuenta en los derechos internos latinoamericanos en lo aplicable.

Es así como Spindler propone la creación de una responsabilidad objetiva de los operadores comerciales, en virtud del entrenamiento con los datos y su posible beneficio de la imprevisibilidad de los sistemas de inteligencia artificial, que aumentan en su conexión en red, con los sistemas informáticos y en la nube[292]. Asimismo, se refiere a los problemas derivados de la causalidad ("Black-Box"), en un caso de mal funcionamiento de un sistema de IA, cuando se requiere establecer, si los daños causados se originaron en una programación incorrecta, un uso inadecuado o en "decisiones erróneas" de la IA.[293]

Frente a la responsabilidad de los fabricantes en las relaciones jurídicas entre empresas (B2B), en los casos de aplicación de la inteligencia artificial, considera él la aplicación de un límite máximo de responsabilidad,[294] así como el establecimiento de una obligación de seguro de los riesgos de la IA similar a los seguros de responsabilidad civil por productos defectuosos, que puede ser combinada con una obligación de seguros similar a la de los depósitos en los bancos y la posible participación del Estado en el sistema de seguros, a través de una especie de fondo de solidaridad[295].

El límite máximo o un límite mínimo de responsabilidad no es permisible frente a la protección de derechos del consumidor en el ámbito de la CE-PD-RD-PD.[296] En este sentido considera Spindler que pudiera establecerse el límite máximo de responsabilidad en el caso de operadores o usuarios comerciales. Este límite se establecería según "las cifras de ingresos o volumen de negocios de cada sector en función de los riesgos de los sistemas de IA".[297] Adicionalmente se refiere él entre otros aspectos, a que la responsabilidad de los fabricantes en el sector B2B y de los operadores de sistemas de IA debería limitarse a los sistemas de alto riesgo, así como que en caso de pérdida de datos se restrinja a los daños para la restauración de estos, y al que las vulneraciones a derechos fundamentales sean analizadas desde la

290 Spindler, (n. 13), 6.
291 Spindler, (n. 13), 6.
292 Spindler, (n. 13), 11.
293 Spindler, (n. 13), 12.
294 Spindler, (n. 13), 53.
295 Spindler, (n. 13), 8.
296 Comisión Europea, (n. 92).
297 Spindler, (n. 13), 53.

responsabilidad, pero no desde la objetiva, de modo que no sea ésta desbordada.[298] Más allá de ello, los sistemas de IA certificados según la propuesta de Reglamento de Responsabilidad de la IA en el ámbito de la responsabilidad basada en la culpa, tendrían un rol especial, por razón de la confianza que generan en los operadores y los fabricantes. Finalmente indica en su concepto, el cómo la normatividad sobre los "sandboxes" regulatorios pudiera considerar mitigaciones de la responsabilidad, que permitieran el uso experimental de los sistemas de IA.[299]

VII. Smart contracts

Sobre la naturaleza y el derecho aplicable a smart contracts, Matthias Lehman y Felix Krysa analizan en 2019 la conexión entre estos y criptomonedas, detallando entre otros ejemplos de casos, el arrendamiento de un automóvil donde por cada kilómetro recorrido se transfieren criptomonedas del arrendatario al arrendador y el cumplimiento del contrato es automatizado, así como la automática recarga electrónica de un auto de conducción autónoma o la compra automática desde un refrigerador de un nuevo producto en internet cuando se extrae otro, y se paga el producto con criptomonedas[300] Asimismo serían viables más casos a través de la tecnología y los límites de la cadena de bloques. Concordantemente pudiera considerarse aquí también la implementación de los correspondientes "smart contracts" a través de sistemas de IA.

En los ámbitos mencionados por Lehman y Krysa, se formula la pregunta, de la responsabilidad derivada de un error técnico u otro que genere la transferencia de las criptomonedas.[301]

Acorde con Keßler los smart contracts son implementados por "agentes de software", que aseguran "se realicen las operaciones informáticas necesarias", así como que "los resultados se almacenen de forma descentralizada" y "se produzcan los efectos legales".[302] Ello emplea la tecnología de "cadena de bloques" (blockchain)[303], que, no obstante ser concebida para la moneda criptográfica "bitcoin", encuentra más aplicaciones[304].[305] Es así como Lehman se refiere a la cadena de bloques como una "emanación de la Tecnología de Libro Mayor Distribuido" (DTL) que constituye "una base de datos" de registro de "eventos de

[298] Spindler, (n. 13), 53.
[299] Spindler, (n. 13), 53.
[300] Matthias Lehmann y Felix Krysa, "Blockchain, Smart Contracts und Token aus der Sicht des (Internationalen) Privatrechts," *BRJ* 02 (2019): 90 (91).
[301] Lehmann y Krysa, (n. 300), 90 (91).
[302] Keßler, (n. 167), 589 (592, 593).
[303] Aquí ver detalladamente la contribución en materia financiera europea en este volumen Omlor, (n. 3).
[304] Ver de forma detallada en el derecho privado e internacional privado Lehmann, (n. 4), 181-202.
[305] Keßler, (n. 167), 589 (592, 593).

forma permanente e inmutable" y la cual "[p]uede utilizarse para almacenar todo tipo de información".[306] Lehman y Krysa la detallan como una forma de banco de datos enlazado con una tecnología de encriptación.[307] Aquí los datos no se encuentran grabados en una central, sino en distintos servidores que pueden encontrarse en diferentes partes del mundo (DTL), los cuales deben verificar cada transferencia y validarla (de forma descentralizada).[308] Esta tecnología sirve también para transmitir otros valores como propiedades, derechos inmateriales, o información confidencial como datos de salud o de clientes,[309] y tal como indica Lehman, generó la creación de "criptoactivos" y "tokens"[310],[311] así como *propone con razón frente a ello y con base en Savigny*[312], *el "pensar en las relaciones jurídicas"*[313] *y concordantemente, en "la ley aplicable a las transacciones"*[314].

Por ejemplo, sobre la aplicación de un "agente informático" en materia financiera, se refiere Keßler al "Polymorphes Banking", que combina la "cadena de bloques para registrar y validar las transacciones de pago," con "una aplicación de inteligencia artificial para analizar los datos y asegurar la comunicación entre el banco y el cliente" así como con "una interfaz" dirigida a "controlar técnicamente los procesos de pago masivo".[315] En su opinión en ese momento, esta forma de operación sería objeto del ámbito de aplicación de la Ley de supervisión de servicios de pago (Zahlungsdiensteaufsichtsgesetz – ZAG 2017)[316], en armonía con la Directiva (UE) 2015/2366[317] así como de su transposición en los § 675c (servicios de pago y dinero electrónico) y siguientes del BGB.[318]

En los smart contracts cuya concepción por Nick Szabo data de los años 90, se busca según Jörn Heckmann y Markus Kaulartz, "representar los contratos en el software y el hardware para que la prestación y la contraprestación sean establecidos

306 Lehmann, (n. 4), 181 (182).
307 Lehmann y Krysa, (n. 300), 90.
308 Lehmann y Krysa, (n. 300), 90.
309 Lehmann y Krysa, (n. 300), 90.
310 Omlor, (n. 3).
311 Lehmann, (n. 4), 181 (182).
312 Lehmann, (n. 4), 181 (195).
313 Lehmann, (n. 4), 181 (195).
314 Lehmann, (n. 4), 181 (196).
315 Keßler, (n. 167), 589 (592, 593).
316 Gesetz über die Beaufsichtigung von Zahlungsdiensten, consultado el 30 de septiembre de 2023, https://www.gesetze-im-internet.de/zag_2018/
317 Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE (Texto pertinente a efectos del EEE), consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32015L2366
318 Keßler, (n. 167), 589 (593).

por la lógica del programa".[319] En estos, al encajar las condiciones programadas y registradas en un código fuente, las computadoras que son parte en una red "peer-to-peer" descentralizada de la cadena de bloques, ejecutan sin intermediarios y necesidad de supervisión humana, el intercambio de las prestaciones previstas.[320] Tales prestaciones deben ser representables digitalmente y requieren de interfaces (oráculos) para interactuar en el mundo físico, que permiten entre otros aspectos, el pago y envío de una mercancía. Su aplicación en el mercado financiero reduce entre otros aspectos, costos y riesgos.[321] Empero como a bien indican, aquí *el negocio jurídico no se reduce al código fuente, toda vez que el contrato no se restringe a su tenor literal, esto sería al código, sino que debe analizarse la voluntad de las partes conforme a las circunstancias que rodean su celebración*.[322] Concordantemente, surgen cuestiones tales como: la responsabilidad derivada de la incorrecta programación del código, la posible aplicación no conforme a derecho, o también su programación sin el apoyo jurídico correspondiente.[323]

En particular Lehman y Krysa, no consideran por regla general a los "smart contracts" como contratos, según su clasificación común en el derecho alemán, *sino adecuadamente, como procedimientos automatizados que sirven al cumplimiento de un contrato (que puede) ser realizado, por ejemplo, por fuera de la cadena de bloques*.[324] En este sentido, serían *"smart contracts de cumplimiento que generan las prestaciones y la extinción de la obligación por razón de la prestación"* según el § 362 I BGB.[325] Concordantemente la relación obligacional se extingue, si la prestación debida se ejecuta al acreedor.[326] En el caso que la modalidad del "smart contract" sea aquella en la cual una parte entrega su declaración de voluntad, en el año 2019 Lehman y Krysa le equipararon con razón con base en la literatura alemana mayoritaria: *"a la de un expendedor automático de mercancías" con la configuración de una oferta "ad incertas personas"*.[327] Con todo, como a bien consideran, es necesario enlazar al ser humano que está detrás de los aparatos como los serían en los casos planteados, el propietario de la estación de abastecimiento de recarga para vehículos eléctricos o el poseedor del auto de conducción autónoma, etc.[328]

Como ellos también adecuadamente indican, en las modalidades de "smart contracts" realizados y ejecutados en el ámbito transnacional, tendrían aplicación

[319] Jörn Heckmann y Markus Kaulartz, "Smart Contracts auf dem rechtlichen Prüfstand," *Die Bank* (2017): 60.
[320] Heckmann y Kaulartz, (n. 319), 60.
[321] Heckmann y Kaulartz, (n. 319), 60.
[322] Heckmann y Kaulartz, (n. 319), 60.
[323] Heckmann y Kaulartz, (n. 319), 61.
[324] Lehmann y Krysa, (n. 300), 90 (92).
[325] Lehmann y Krysa, (n. 300), 90 (92).
[326] Lehmann y Krysa, (n. 300), 90 (92).
[327] Lehmann y Krysa, (n. 300), 90 (92).
[328] Lehmann y Krysa, (n. 300), 90 (92).

las reglas de determinación del derecho aplicable, como es el caso del Reglamento Roma I europeo sobre la ley aplicable a las obligaciones contractuales (RRI)[329]. Estas reglas son comparables con las de la aún no vigente Convención de México de 1994 (CM) sobre derecho aplicable a los contratos internacionales[330].[331] En este sentido aplican el artículo 12 II del RRI a la forma y manera de cumplimiento del "smart contract".[332] Según esta disposición, se debe tener en cuenta la ley del país donde tenga lugar el cumplimiento de la obligación. Adicionalmente, la autonomía conflictual permite según el artículo 3 I del RRI, la elección por las partes del derecho aplicable, de forma expresa o de forma concluyente, esto es, que se derive claramente[333] de forma distinguible e inteligible de los términos del contrato o de las circunstancias del caso[334]. Ello correspondería al ámbito del "primer párrafo del inciso 1 del art. 7 de la CM, que se refiere específicamente a que el contrato se rige por el derecho elegido por las partes".[335]

En el evento de ausencia de ésta, se da aplicación al derecho del Estado con el cual se tenga los vínculos más estrechos, considerando los elementos objetivos y subjetivos derivados del contrato.[336] Por ejemplo, se establece por el punto de contacto objetivo del artículo 4 Nro. 1 a) del RRI, que el contrato de compraventa de mercaderías se regirá por la ley del país donde el vendedor tenga su residencia habitual.[337] Disposición que también puede "servir vía interpretativa y en el contexto del art. 9 de la CM, como base para la elección del derecho aplicable".[338] En todo caso como a bien indican Lehman y Krysa, en materia de contratos de consumo según el artículo 6 del Reglamento, se establecen reglas respecto a la

[329] Reglamento (CE) 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I), consultado el 30 de septiembre de 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32008R0593.
[330] OEA, Convención Interamericana sobre Derecho Aplicable a los Contratos Internacionales, Suscrita en México, D.F., México el 17 de marzo de 1994, en la Quinta Conferencia Especializada Interamericana sobre Derecho Internacional Privado (CIDIP-V), consultado el 30 de septiembre de 2023, https://www.oas.org/juridico/spanish/tratados/b-56.html.
[331] José Hernán Muriel Ciceri, "Aspectos de la unificación de Derecho Internacional Privado en Europa y América Latina (derecho de obligaciones contractuales) una comparación entre el Reglamento Roma I y la Convención de México de 1994, desde la óptica de la elección del derecho aplicable," *AEDIP* 8, (2008): 645-652.
[332] Lehmann y Krysa, (n. 300), 90 (94).
[333] Rolf Wagner, "Der Grundsatz der Rechtswahl und des mangels Rechtswahl anwendbares Recht (Rom I-Verordnung) Ein Bericht über die Entstehungsgeschichte und den Inhalt der Artikel 3 und 4 Rom I-Verordnung," *IPRax* (2008): 377 (379); Thomas Pfeiffer, "Neues Internationales Vertragsrecht – Zur Rom I Verordnung," *EuZW* (2008): 622 (625); Stefan Leible y Matthias Lehmann, "Die Rom I-Verordnung," *RIW*, 528 (532).
[334] Muriel Ciceri, (n. 331), 645 (649).
[335] Muriel Ciceri, (n. 331), 645 (648).
[336] Muriel Ciceri, (n. 331), 645 (650).
[337] Lehmann y Krysa, (n. 300), 90 (94).
[338] Muriel Ciceri, (n. 331), 645 (650).

aplicación de la ley del país en que el consumidor tenga su residencia habitual.[339]. Se trata de una disposición a considerar dentro del contexto del artículo 9 de la CM.[340] Respecto a la validez de la celebración de contratos parcialmente automatizados y pagados con criptomonedas, se basan en la aplicación del artículo 10 I del RRI.[341] Según esta norma, "la validez del contrato, o de cualquiera de sus disposiciones, estarán sometidas a la ley que sería aplicable en virtud del presente Reglamento si el contrato o la disposición fueran válidos". Para ello es necesario como a bien indican, que en ausencia de elección se establezca, a que persona deben atribuirse las acciones del programa. Esta interpretación aplicaría en el contexto del artículo 12 de la CM.[342] En el caso alemán descartan acudir al artículo 8 de la Ley de Introducción al Código Civil correspondiente a la representación voluntaria, toda vez que la representación exige al menos dos personas.[343] Si se analiza que la concesión de la declaración de voluntad sobre el contrato no se da en un margen de decisión al estar establecida en detalle por el código de programación, adoptan entonces la institución del mensajero (Botenschaft) en el derecho civil.[344] En el evento que no sea viable interpretar el comportamiento de una parte como consentimiento del contrato, esta podrá acudir conforme al artículo 10 II del Reglamento, a la ley del país en la que tenga su residencia habitual.[345] Esta disposición "concede mayor claridad frente a la [CM]"[346]. Sin embargo, en el inciso II del art. 12 de la CM y el inciso II del art. 10 RRI, "tiene vigencia un análisis integral de cada caso en particular".[347]

Tratándose de contratos celebrados sin un actuar humano, señalan que su validez debe sujetarse al artículo 10 I del RRI, determinando previamente a quien deben atribuirse las declaraciones del programa.[348] Ello sería concordante al ámbito del artículo 12 de la CM.[349]

En *suma*, los "smart contracts" se encuentran generalmente en el ámbito de una modalidad de cumplimento[350] de las prestaciones previstas de un contrato[351]. Estos además de la posibilidad de disminuir costos y riesgos[352], así como de permitir

339 Lehmann y Krysa, (n. 300), 90 (94).
340 Muriel Ciceri, (n. 331), 645 (650).
341 Lehmann y Krysa, (n. 300), 90 (94).
342 Muriel Ciceri, (n. 331), 645 (649 n. 39).
343 Lehmann y Krysa, (n. 300), 90 (95)
344 Lehmann y Krysa, (n. 300), 90 (95)
345 Lehmann y Krysa, (n. 300), 90 (95)
346 Muriel Ciceri, (n. 331), 645 (649).
347 Muriel Ciceri, (n. 331), 645 (649 n. 41).
348 Lehmann y Krysa, (n. 300), 90 (95).
349 Muriel Ciceri, (n. 331), 645 (649 n. 39).
350 Lehmann y Krysa, (n. 300), 90 (94)
351 Heckmann y Kaulartz, (n. 319), 60.
352 Heckmann y Kaulartz, (n. 319), 60.

mayor eficiencia en la operación encomendada por el código de programación, pueden realizarse a través de sistemas de IA, según sus etapas de desarrollo y, asimismo, según el caso, desde la relación jurídica concreta[353], pueden ingresar en el ámbito de aplicación del derecho internacional privado[354].

E. Conclusiones

- La IA como una forma de tecnología con diferentes variantes y etapas de desarrollo en avance, presenta a la humanidad oportunidades, riesgos y retos, de los cuales se ocupa la ciencia del derecho a través de sus funciones. En el contexto jurídico, también debe tenerse presente la interdisciplinariedad de la tecnología de la IA, su contenido y sus límites tecnológicos y jurídicos.
- El camino recorrido a través de la industria contemporánea permite plantear frente a ella, el avance hacia una nueva etapa de desarrollo sostenible, que tenga como eje la protección de la dignidad humana, de su entorno ambiental, ecológico, racional, y de los fundamentos naturales de la vida en donde estos se encuentren. En esta etapa y desarrollo posterior, puede considerarse una cooperación entre los humanos y las máquinas, a través del fomento y del desarrollo de una "IA cooperativa".
- La protección de derechos, el acceso a la protección jurídica efectiva y la seguridad jurídica deben ser asimismo una constante frente a la IA. En este ámbito, las reglas tradicionales y principios del derecho encuentran aplicación en lo correspondiente, así como es necesaria también, la construcción y consolidación de las correspondientes estructuras jurídicas y de regulación.
- La base jurídica en general en la región latinoamericana es cercana al derecho europeo, y los aspectos jurídicos comparados, pueden ofrecer herramientas de análisis del derecho frente a la IA, que a la vez complementan la consideración de sus propias realidades, tradiciones jurídicas y derechos internos, en un mundo de contextos internacionales. Concordantemente pueden colocarse en consideración las propuestas jurídicas presentadas por la Comisión Europea, así como por el Parlamento Europeo. En Latinoamérica debe resaltarse el esfuerzo y la importante iniciativa de varios países a través de proyectos de Ley y de nueva regulación vigente, como son los casos expresados según su contexto de Brasil, Chile y Perú. Asimismo, pudiera contemplarse en el ámbito latinoamericano, por ejemplo, entre otros aspectos, en favor de la seguridad jurídica, la protección efectiva y la previsibilidad jurídica frente a los operadores económicos, la

353 Lehmann, (n. 4), 181 (195).

354 Véase sobre cadena de bloques, smart contracts y tokenes Lehmann y Krysa, (n. 4), 90 y s.; sobre la ley aplicable a la cadena de bloques, Lehmann, (n. 4), 181 (196), adicionalmente, sobre la comparación entre el Reglamento Roma I y la Convención de México de 1994, desde la óptica de la elección del derecho aplicable, Muriel Ciceri, (n. 331), 645 y s.

generación de una unificación mínima normativa de aspectos principales en materia de la IA o de no ser ello viable en un corto o mediano plazo, de una armonización mínima[355] del correspondiente derecho interno. Serían así eventuales alternativas: La elaboración de tratados o leyes modelo sobre la materia desde la OEA, así como la realización de una Ley Modelo específica desde el Parlatino. En ambos casos el ejercicio normativo de los legisladores nacionales ordinarios permanece ampliamente vigente. Una alternativa adicional acogida por algunos países latinoamericanos es el análisis de los contenidos de las propuestas europeas y del derecho comparado, así como su aplicación, como una caja de herramientas del legislador nacional frente a su propio derecho.

- El derecho alemán, así como otros derechos internos de los Estados europeos pueden constituir desde el derecho comparado, un apoyo en el análisis, la construcción y la interpretación de normas del derecho doméstico[356] en Latinoamérica en materia de la IA.
- En la sección D. I a VII., se realiza en especial un planteamiento de análisis, valoración y aplicación de algunos componentes jurídicos frente a la IA y su interacción.
- La aplicación, el fomento y los límites de la modalidad tecnológica de la IA debe considerarse en particular frente a la protección, a la solución de problemas y al futuro de la humanidad, así como en la construcción de puentes sostenibles entre ella. Una guía en el camino, en la construcción y en el desarrollo del derecho de la IA, debe ser el principio de protección de la dignidad humana[357], en su extensión más amplia.

[355] Comisión Europea, (n. 69), considerando 14.
[356] Konrad Zweigert y Hein Kötz, *Einführung in die Rechtsvergleichung*, 3. ed., (Tübingen: J.C.B. Mohr, 1996).
[357] Lorenz (153); Jarass, (n. 150); Kingreen y Poscher, (n. 149); Stern (n. 151), Muriel Ciceri, (n. 14), 65 y s.; (n. 251) 343 (375).

A Quantitative Approach to Artificial Intelligence Legal Risk Management

Luis Enríquez

A. Introduction

The emergent European legal regulation on artificial intelligence known as *Artificial Intelligence Act*[1] *(AIA)*, is following a risk-based approach for the protection of the fundamental rights of natural persons[2]. This risk-based approach seems to follow the footprints already established by the GDPR in 2016, but in the field of Artificial Intelligence services. The GDPR relies on a risk-based approach, and data protection impact assessments belong to a meta-regulatory nature[3], where regulators delegate the immense task of protecting the rights and freedoms to regulatees[4] through risk management. However, the legal world still has a lot of gaps and misunderstandings about what is *risk*, and the nature of compliance within *risk-based regulations*. New legal regulations on artificial intelligence must avoid past mistakes regarding risk management, especially due to the potential high impact of the consequences of AI-based technologies on the fundamental rights of natural persons.

[1] European Union, Proposal for a Regulation of The European Parliament and of the Council, *Laying Down Harmonised Rules on Artificial Intelligence.*

[2] *"This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach"*. European Union, (n 1), explanatory memorandum, clause 3.5.

[3] Christine Parker, *The Open Corporation* (Cambridge: Cambridge University Press, 2002), 245.

[4] GDPR, article 5 § 1(d).

DOI: https://doi.org/10.17875/gup2023-2498

The proposal of an Artificial Intelligence Act has improved the need of risk assessment methods for justifying the release of AI products through technical reports, but that do not provide the details of what an effective risk-based approach is. Unfortunately, the legal world seems to still take for granted that risk management works by default, taking a dangerous path that can lead to an ineffective protection of the fundamental rights of natural persons.

The truth is that there is a lot of confusion about legal risk management, due to the nature of a legal decision-making tradition based on rules, principles, and criteria, against a risk-based approach measured in numbers, quantiles, and percentiles[5]. This paper aims to define the nature of artificial intelligence compliance risks, and to propose a quantitative approach to Artificial Intelligence Impact Assessments (AIIAs).

B. Artificial intelligence and legal risk management

Artificial intelligence was earlier defined as *"the science of making machines do things that would require intelligence if done by men"*[6]. Consequently, artificial intelligence requires methods for achieving its goals, and those methods mostly rely on machine learning models. Machine learning paradigms are classified into supervised machine learning, unsupervised machine learning, deep learning, and reinforcement learning. Concisely, machine learning is about educating information systems, to transform them into intelligent systems, where data sets are the feeding input. The language of machine learning is about assessing probabilities for problem solving, *"whose results cannot be predicted with certainty"*[7].

Risk management is the right approach to reduce uncertainty, since it consists in *"the identification, analysis, and prioritization of risks followed by coordinated and economical application of resources to reduce, monitor, and control the probability and/or impact of unfortunate events"*[8]. Artificial intelligence methodologies have become a ubiquitous tool for risk assessment[9], and legal risk assessment related areas such as predictive justice[10]. This

[5] Marcel B. Finnan, *An Introductory Guide in the Construction of Actuarial Models: A Preparation for the Actuarial Exam C/4* (Arkansas: Arkansas Tech University, 2017), 62.

[6] Marvin Minsky, *Semantics Information Processing*, ed. Marvin Minsky (Cambridge: MIT Press, 1968), v.s.

[7] Finnan, (n 5), 6.

[8] Douglas Hubbard, *The Failure of Risk Management*, 2nd edn. (United States: John Wiley & sons Inc, 2020), 11.

[9] *"One suitable approach to reduce risk is to instrument this lifecycle to collect and govern relevant facts about the process to ensure they comply with regulatory and organization policies intended to mitigate specific risks and prevent societal harm".* David Piorkowsky, Michael Hind and John Richards, "Quantitative AI Risk Assessments: Opportunities and Challenges*,"* 1, arXiv:2209.06317.

[10] *"In developing these models, researchers address such questions as how to represent what a legal rule means so that a computer program can decide whether it applies to a situation, how to distinguish hard from easy legal issues, and the*

section is divided into the regulatory nature established in the Artificial Intelligence Act (I.), and the Artificial Intelligence Impact Assessments (II.).

I. The regulatory nature established in the Artificial Intelligence Act

The European Artificial Intelligence Act has the purpose of improving *"the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values"*[11]. For accomplishing this mission, it relies on a risk-based approach since *"in order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed"*[12]. However, the proposal does not define what is *clearly defined risk-based approach*, as it does not even define what is risk[13]. The Act introduces the obligation of performing high-risk AI Assessments, where *"a risk management system shall be maintained in relation to high AI systems"*[14]. Yet, it delegates to regulatees *"the adoption of suitable risk management measures in accordance with the provisions of the following papers"*[15]. This means that AI providers have the obligation to perform risk management, and they shall figure out an effective *risk-based approach*, with the aim of complying with the imposed legal obligations.

This risk management delegation to regulatees unveils the nature of this Act. In the corporate governance area, Braithwaite and Ayres proposed a model of enforced regulation, which *"is about negotiation occurring between the state and individual firms to establish regulations that are particularized to each firm"*[16]. Parker defined meta-regulation as *"the regulation of self-regulation"*[17]. Both approaches have in common the regulator's control of the regulatees' compliance processes, fulfilled by the accountability principle. This means that AI risk management is an instance of the AI Act that fulfils a meta-regulatory approach, as risk management is delegated to AI providers. Some authors, such as Gellert and Binns, have applied these corporate governance models to the GDPR's regulatory nature. For Gellert, the risk-based approach to data protection *"is only a partial implementation of a meta-regulation, insofar as it doesn't fully*

role that cases and values play in interpreting legal rules". Kevin Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age* (Cambridge: Cambridge University Press, 2017), 4.

[11] European Commission, "Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence", recital 1.

[12] EC, (n 11), recital 14.

[13] EC, (n 11), article 3.

[14] EC, (n 11), article 9.

[15] EC, (n 11), article 9 2(d).

[16] Ian Ayres and John Braithwaite, *Responsive Regulation* (New York: Oxford University Press, 1992), 101.

[17] Parker, (n 3), 245.

delegate the standard setting functions to the regulatees"[18]. Binns considered the Data Protection Impact Assessments as a meta-regulatory instance of the GDPR, since *"mandatory DPIAs could allow both the flexibility associated with self-regulation and the benefits of external pressure associated with legal regulation"*[19]. These previous works can may us conclude that the direction of high-risk AI systems risk management follows a meta-regulatory approach, in which AI impact Assessments (AIAs) become the meta-regulatory instance of it.

However, risk management does not work by default, and legislators keep repeating a huge assumption mistake. The AI providers need to find the right risk-based approach, but there are different approaches to risk management that may have to be considered. Hubbard identifies four risk management approaches belonging to four kinds of risk professionals, *the actuaries, the war quants, the economists, and the management consultants*[20]. He arguments about the actuaries that *"these original professional risk managers use a variety of scientific and mathematical methods. Originally, they focused on assessing and managing the risks in insurance and pensions, but they have branched out into other areas of risk"*[21]. The war quants are the descendants of World War II engineers and scientists, users of *"probabilistic risk analysis, decision analysis, and operations research"*[22]. The economists are focused on finance, *"to assess and manage risk and return of various instruments and portfolios"*[23]. Finally, he mentions the management consultants, which *"use more intuitive approaches to risk management that rely heavily on individual experience"*[24], a non-scientific risk management approach. The current question that arises is about *which risk management approach should regulatees follow for managing high-risk AI systems?* With the aim of answering this question, it is compulsory to understand the purposes of Artificial Intelligence Impact Assessments.

II. Artificial Intelligence Impact Assessments (AIIAs)

Understanding risk is compulsory in order to understand AIIAs. Unfortunately, the basics of risk are not well understood in the legal area, a considerable drawback for the emergence of effective AI legal regulations. From a scientific harm-based approach, risk may be defined as "*a potential loss, disaster, or other undesirable event measured*

[18] Raphael Guellert, *The Risk Based Approach to Data Protection* (Oxford: Oxford University Press, 2020), 136.
[19] Reuben Binns, "Data Protection Impact assessments: a meta-regulatory approach," *International Data Privacy Law,* 7.1: 22-35 (2017): 22 (34).
[20] Hubbard, (n 8), 82.
[21] Hubbard, (n 8), 82.
[22] Hubbard, (n 8), 82.
[23] Hubbard, (n 8), 83.
[24] Hubbard, (n 8), 83.

with probabilities assigned to losses of various magnitudes"[25]. From an operational risk context, the notion of harm is "*the risk of loss, arising from inadequate or failed processes, people and systems, or from external events"*[26], where operational risks are related to all AI related areas of application. From an AI legal context, the notion of harm can affect the fundamental rights of natural persons, and there is a need of implementing human oversight in AI-based products, since *"human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse"*[27].

However, we must consider that algorithm performance is measured in a risk-based approach, and there is always a remaining residual risk. For instance, a Natural Language Processing model used in the context of Large Language Models, may fail its goals of providing the right information to users, when the text interpretation contains humoristic or ironic meanings. Similarly, a facial recognition system trained by using a dimension reduction unsupervised model that uses logistic regression for taking decisions in a production environment, may still make mistakes when authenticating users, due to fake positives and fake negatives. Furthermore, AI hallucinations are a probable drawback, as predictive responses may not be justified in its training data risk assessment. These mistakes are common in the AI systems production environments, as they rely on a risk-based probabilistic environment. However, the concept of loss only requires measuring harm in a financial dimension, as regulatees may have primary losses such as the loss on productivity, incident response and asset replacement, and secondary losses such as the loss of reputation, the loss of competitive advantage, and the probability of receiving administrative fines[28], and other kind of fines and judgements.

Nevertheless, risk assessment is usually confused with risk analysis. The ISO defines risk assessment as the *"overall process of risk identification, risk analysis, and risk evaluation"*[29], while some risk analysis definitions may already represent the whole risk assessment task, such as "*how to figure out what your risks are (so you can do something*

[25] Hubbard, (n 8), p.9.
[26] Society of Actuaries, "Actuaries and Operational Risk Management," (AAE Discussion Paper, 2021), 43, accessed October 20, 2022, https://actuary.eu/wp-content/uploads/2021/01/Actuaries-and-Operational-Risk-Management-FINAL.pdf
[27] European Comission, (n 2), article 14.
[28] See, Jack Freund and Jack Jones, *Measuring and Managing Information Risk: A FAIR Approach* (United States: Elsevier Inc., 2015), 65 – 73.
[29] ISO/IEC 27005:2022, clause 3.2.3.

about it)"[30]. Another argument is that *"impact assessment goes further by considering implications, both positive and negative, for people and their environment"*[31], where the consequences are not necessarily an undesired harm. In this sense, AIIAs do not reinventing the wheel, and follow previously established approaches, but in the field of AI. From a legal perspective, an AIIA may become a risk assessment procedure for protecting fundamental rights of natural persons[32], just like the GDPR's Data Protection Impact Assessments (DPIAs) were conceived as risk assessment procedures for the protection of the rights and freedoms of natural persons[33]. Some of the relevant AI legal risks include *"bias, lack of transparency, discrimination, invasion of privacy, misuse of personal data and damaging trust"*[34]. In this sense, AI risk-based regulations might have many reasons to be considered as *"the law of everything"*[35], just like data protection. Purtova's anticipated regarding this *law of everything* fact, when analysing the obligation to protect the rights and freedoms of data subjects in the European Union, since it *"is growing so broad that the good intentions to provide the most complete protection possible are likely to backfire in a very near future, resulting in system overload"*[36]. Furthermore, the goal of protecting rights and freedoms must be carefully assessed in AIIAs, by following a scientific-based approach for risk assessment, considering the huge responsibility of protecting fundamental rights, delegated to AI providers.

The main purpose of risk assessment is providing data for an efficient and costly-effective risk management. The risk management stack must follow these stages: *"accurate models, meaningful measurements, effective comparisons, well-informed decisions, and effective risk management"*[37]. A quantitative approach is fundamental to risk management stack, and the main mission that AIIAs have today, is to avoid following only a superficial management consultant approach to risk, that only relies on assumptions of best practices standards, some of them from well-known international organizations such as the ISO. Regulatees must understand that such guidelines have been conceived for project management, but that do not provide the metric methods for measuring risk and complying with a scientific-based risk management stack.

---

[30] Hubbard, (n 8), 12.

[31] Ansgar Koene, Gabriella Ezeani, et al., *A Survey of Artificial Intelligence Risk Assessment Methodologies* (Ernst & Young LLP, 2021), 6, accessed October 20, 2023, https://trilateralresearch.com/publications/a-survey-of-artificial-intelligence-risk-assessment-methodologies

[32] European Union, (n 1), article 9.

[33] GDPR, *The official PDF of the Regulation (EU),* article 35.

[34] Koene, Ezeani, et al., (n 31), 5.

[35] See, Nadezhda Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law," *Law, Innovation and Technology*, vol. 10, 1, (2018): 40–81, doi: 10.1080/17579961.2018.1452176

[36] Purtova, (n 35), 2.

[37] Freund and Jones, (n 28), 279.

C. The challenges of Artificial Intelligence Impact Assessments

AIIAs must follow the right risk-based approach due to the immense risks that AI presents to the fundamental rights of natural persons. From actuary's perspective, risk is about measuring for reducing uncertainty. In the field of insurers and pension funds, the European Union obligates to the actuary's sector the *Own Risk and Solvency Assessment (ORSA)* and *the Own Risk Assessment (ORA)*[38], both based on measurement, as measuring is the actuary's way to manage risk, coming from a more than 200 years tradition. Considering the long tradition of the actuarial science, we may affirm that there is a clear risk-based approach in their area. However, AI law is deeply connected with data protection law, considering that

> *"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions"*[39], and that *"the data subject shall have 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"*[40].

Even though that AI is still an emergent field, there is not yet a clear risk-based approach, and the huge risk is that it follows a data protection risk-based approach that is also still, undefined.

The GDPR's Data Protection Impact Assessments, in practice, have followed a different orientation based on a management consultant's subjective risk-based approach inherited from the information security area, and a superficial checklist-oriented vision of PIAs inherited from the FIPPs principles[41]. Unfortunately, the information security area is still in an immature phase of development that data protection broadly adopted, perhaps due to a superficial an undefined vision of data protection risk, that shall not be replied in AI regulations. On the other hand, and due to the deep relationship among AI risk management and data protection risk management, there has already been considerable developments on such domain since the application entry of the GDPR in 2018. A remarkable one has been the idea of algorithmic impact assessments, with the aim *"to address problems of algorithmic discrimination, bias, and unfairness"*[42]. For fulfilling the purposes of this section, it has

[38] Society of Actuaries, (n 26).
[39] GDPR, (n 33), article 21 1.
[40] GDPR, (n 33), article 22.
[41] Stuart S. Shapiro, "Time to Modernize Privacy Risk Assessment," *Issues in Science and Technology*, Vol. 38 No.1: 20-22 (2022): 20.
[42] Margot E. Kaminski and Gianclaudio Malgieri, "Algorithmic Impact Assessments under the GDPR: producing multi-layered explanations," *International data Privacy Law*, Vol 11, No. 2: 125-144 (2021): 134.

been divided into the urgent need of choosing the right risk assessment methods (I.), and towards a new kind of accountability (II.).

I. The urgent need of choosing the right risk assessment methods

There are a considerable number of new standards and guidelines currently emerging in the field of AI risk management. The current most relevant ones are the ISO/IEC 23894:2023 and the NIST AI 100-1. On one hand, the ISO standard still follows the same traditional approach of previous standards, providing guidelines for AI risk management such as *"AI risks should be identified, quantified or qualitatively described and prioritized against risk criteria and objectives relevant to the organization"*[43]. It also provides a useful AI risk identification guide consisting of several issues labelled as general risk, complexity of the environment, lack of transparency and explainability, level of automation, risk sources related to machine learning, system hardware issues, system life cycle issues, and technology readiness[44]. Despite that it may be a useful guideline for AI risk identification, it remains as a generic approach to risk analysis and risk evaluation, relying on former ISO standards such as the ISO/IEC 31000:2018 and the ISO/IEC 27005:2022. Yet, regulatees must understand that the real value of ISO standards is a methodology for project implementation, and not for risk measuring[45], as it mostly remains informative, since it is only based on criteria[46].

On the other hand, The NIST AI 100-1 proposes a risk management framework composed of four stages: *"govern, map, measure and manage"*[47]. It recommends risk measuring since *"AI risks or failures that are not well-defined or adequately understood are difficult to measure quantitatively or qualitatively. The inability to appropriately measure AI risks does not imply that an AI system necessarily poses either a high or low risk"*[48]. However, measuring is only feasible through quantitative risk analysis. Common qualitative failed methods are based on personal's subjective opinions[49] and represented through failed risk representation methods such as risk matrices[50]. For instance, the ISO /IEC 29134:2017 for Privacy Impact Assessments relied on a subjective analysis logic, as probability is not measured on a given time-frame, and impact criteria rely

[43] ISO / IEC 23894:2023, clause 6.4.1.
[44] ISO/ IEC, (n 42), Annex B.
[45] The ISO/IEC 27004 is sold as a *metrics model standard*. However, it is about measuring guidelines and criteria, not quantitative metrics on the ground.
[46] ISO, (n 42)
[47] NIST AI 100-1, part 2: Core and Profiles, clause 5.
[48] NIST AI 100-1, (n 46), clause 1.2.
[49] A main problem of a person's subjective opinion for risk analysis relies on overconfidence. See, Douglas Hubbard and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk* (New Jersey: John Wiley & sons Inc, 2016), 68.
[50] Hubbard and Seiersen, (n 49), 90.

on criteria such as negligent, limited, important and maximum, without recommending a financial range loss reference[51]. In the field of AIIAs, the World Economic Forum has already published guidelines for AIIAs, which consists of many questions, but many some of them require a technical justification. For instance, the question *"Does the supplier explain the metrics and evaluation methods used and how they have impacted the selection of data that will be used in the proposed AI system?"*[52] is still a guideline, but it requires the strategic, tactical, and operational methods for achieving compliance.

An integrated approach requires measuring several dimensions of AI risks. In this sense, the capAI methodology[53] seems to have taken a better direction, tackling on operational risks, security risks, and legal risks[54], a well-defined AI life cycle, and the need of metrics. The cap AI methodology suggests the use of machine learning models, and probabilistic methods, for properly modelling AI risk. Therefore, the most important is, *"what is the understanding level of the risk-based approach by regulators and regulatees?"* This issue is crucial in order to interpret the AI act provision *"the technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date"*[55]. The final truth is that technical documentation requirements can only be justified by using quantitative risk analysis.

Furthermore, the cap AI provides divides AI conformity assessments in two fundamental areas: robustness and fairness. Robustness may be understood as the strength of algorithm performance, and uses several metrics such as MSE, MAE, F-score, and so forth[56]. It also recommends several fairness-oriented metrics such as theil index, demographic parity, treatment equality, and so forth[57]. However, the outcomes of such metrics need to be incorporated in cybersecurity and legal risk-scenarios, beyond the algorithm performance dimension. The current state of the art is that the problem of measuring the impacts of AI in physical persons has not been resolved yet. We can identify two main dependencies of an Algorithm Impact Assessment (AIIA): Data Protection Impact Assessments (DPIA), and Algorithm Impact Assessments (AIA). In this context, all risks related to data protection must be previously assessed in a DPIAs, and all risks related to algorithm performance

[51] ISO / IEC 29134:2017, Annex A.
[52] World Economic Forum, "Unlocking Public Sector Ai: AI Procurement in a Box," (2020): 20.
[53] Luciano Floridi, et al., "capAI A procedure for conducting conformity assessment of AI systems in line with the EU Artificial Intelligence Act," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091
[54] Floridi, (n 53), 38, 39.
[55] European Union, (n 1), article 11.
[56] Floridi, et al., (n 53), 36, 37.
[57] Floridi, et al., (n 53), 50–51.

must be assessed in an AIA. But merging them in only possible through quantitative risk analysis.
Quantitative analysis employs:

> *"a set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment. This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action"*[58].

Quantitative analysis is based on data, and different methods can be applied such as Montecarlo methods[59], Bayesian methods[60], loss distributions[61], where all machine learning models can add value as input gathering tools. Measuring AI risk by using AI based methodologies has already been implemented, but it should be considered that supervised machine learning models measure accuracy in quantiles and percentages, which depend on a level of confidence[62]. In the field of legal analytics, legal risk can certainly be enhanced Computer Models for Legal Reasoning (CMLA), for forecasting the outcome of legal disputes[63]. In the field of information security, we are living a quantitative risk transformation promoted by several institutions. The World Economic Forum promoted an initiative to quantify risk, proposing *"for organizations and industry stakeholders to be better positioned to make sound investment and risk mitigation decisions, they need to be able to quantify cyber risk"*[64]. The FAIR institute has promoted this transformation in the last decade, changing the mindset of cybersecurity risk management professionals into a quantitative risk analysis approach for taking informed decisions.

Therefore, the main recommendation for AIIAs must be to take advantage of the benefits of quantitative risk analysis, provided by AI risk measuring. Yet, the quantitative risk approach shall not be understood as a replacement of human being criteria, as its purpose is only about enhancing informed decision making. The best risk analysis practices may be using scientific methods and models for measuring

---

[58] NIST SP 800-30, clause 2.3.2.

[59] *"Monte Carlo Analysis is a computer-based method of analysis developed in the 1940's that uses statistical sampling techniques in obtaining a probabilistic approximation to the solution of a mathematical equation or model"*. Michael Firestone, et al., "Guiding Principles for Monte Carlo Analysis", EPA/630/R-97/001 (Washington, DC: U.S. Environmental Protection Agency, 1997), 7.

[60] Firestone, et al. (n 59), 6.

[61] Society of Actuaries, (n 26).

[62] *"Consider a model that predicts the price a customer is willing to pay for a particular service. If its predictions are too high, the business may lose customers. If its predictions are too low, the business may lose revenue"*. Piorkowsky, Hind and Richards, (n 9), 3.

[63] Kevin Ashley, (n 10), 4.

[64] World Economic Forum, Parterning for Cyber Resilience Towards the Quantification of Cyber Threats (WEF, 2015), 4.

risk[65], using machine learning models to automatize the accuracy of the risk outcomes for informing decision takers, and by using international standards such as the ISO/IEC 23894:2023 and the NIST AI 100-1, for the generic purposes of risk project management.

II. Towards a new kind of accountability

The AI act is not clear about the type of accountability that requires.

> *"The CE marking shall be affixed visibly, legibly, and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate"*[66].

The compliance obligation seems to rely on obtaining the CE marking, but then the main challenge would be avoiding a box-ticking approach to obtain them, and to rely on scientific methods that can certainly mitigate risks that threat fundamental rights, in areas such as high safety, health and environmental protection. This is the task of national supervisory authorities, as they also need to follow a risk transformation of their regulatory practices[67], through effective proactive controlling strategies, and not only relying on reactive ones.

In the context of GDPR compliance, Kaminsky and Maglieri proposed a vision of algorithmic accountability, related to the need of explanation in certain rules, such as the right not to be subject to solely automated decision making[68]. From this perspective, an Algorithm Impact Assessment (AIA) *« could serve as a basis for what we call multi-layered explanations of algorithmic decision-making »*[69], a perspective that is like the World Economic Forum's approach to AIIAs. However, both contributions stay in the *what to do* domain, and whether they are important for the evolution of AIIAs, they do not contribute in the *how to do* domain. The capAI methodology presented an ethical-based auditing of AI systems, consisting of several ethical failures of AI systems, such as privacy intrusion, algorithm bias, lack of explainability[70]. It is somehow setting a path for a transition into AI quantitative risk assessment, but still lacking mechanisms to measure the impact of AI failures in the fundamental rights of natural persons, as it was previously mentioned. Algorithmic accountability

---

[65] Such as actuarial models and the FAIR model.

[66] European Union, (n 1), article 49.

[67] See, Malcolm Sparrow, *The Regulatory Craft* (Washington DC: Brookings Institution Press, 2000), 239.

[68] Kaminski and Malgieri, "*A*lgorithm Impact Assessments Under the GPDR: Producing Multi-Layered Explanations," *International Data Privacy Law,* Vol 11 No. 2: 125-144 (2021): 125 (127).

[69] Kaminski and Malgieri, (n 68), 125 (134).

[70] Floridi, et al., (n 53), 56 – 58.

may be about addressing risks such as *"algorithmic discrimination, bias, and unfairness"*[71], but we must consider that the nature of algorithms can be either deterministic or stochastic.

A deterministic algorithm produces *"a unique set of outputs for a given set of input"*[72]. In this sense, complying with a deterministic rule requires a deterministic algorithm. However, when risk is involved, we are talking about uncertainty, which requires the use of stochastic/probabilistic models. In a stochastic algorithm, *"the outputs or/and some of the inputs are random variables"*[73]. Algorithm compliance may involve two different situations: rule-based accountability for deterministic rules, and risk-based accountability for the stochastic requirements related to risk measuring. In the context of the GDPR, Gellert proposed that *"meta-regulation relies upon risk-management as the main regulatory tool"*[74]. But we still need to find the right scientific risk-based accountability processes, that can measure in an interconnected way between the financial harm brought by AI failures, and useful metrics of the harm produced on the fundamental rights of natural persons. Thus, risk-based compliance shall consist of showing regulators how AI providers are mitigating the risks against the fundamental rights of natural persons, and regulators than can understand a risk-based language. This mission also requires that regulators get deep into the science of measuring risk, in order to evaluate the right risk-based approach to new AI products, which goes far beyond a simple description in a natural language documentation.

A quantitative approach to legal risk management consists of finding out the right mechanisms for proving risk-based compliance. A probabilistic language must be based on measuring probabilities, forecasting future events, objectivity, and to be accurate in the outcome ranges[75]. The administrative fines for noncompliance with the AI act have three ranges. The higher range is:

> "*Up to 30 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year",* for forbidden practices. The middle range is *"up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year"*, for high AI risks. The lower range is "*up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year"*[76].

Regulatees must find the right risk models and the appropriate metrics for quantifying risk. The useful data can be obtained by different approaches, as everything is

[71] Floridi, et al., (n 53), 133.
[72] Finnan, (n 5), 2.
[73] Finnan, (n 5), 2.
[74] Guellert, (n 18), 154.
[75] Freund and Jones, (n. 28), 13–23.
[76] European Union, (n 1), article 71.

measurable[77]. One of them is the Value at Risk approach (VaR), which comes from the financial world[78], and consists of calculating the worst probable loss within a given time frame, at a confidence interval. Many more risk-based methods can be found in the actuarial science, such as discrete and continuous distributions[79], stochastic simulations[80], Bayesian inference[81], and so on. All these naive quantitative methods can also be applied for managing AI risks and proving risk-based compliance to regulators. Finally, a good example of a quantitative risk analysis model is the FAIR model[82]. Despite that it was created for information security and operational risk management, it is a very flexible model that can also help for different areas of risk management, due to its holistic and quantitative approach to risk. The model divides follow a top-down approach, and obtains the cyber value at risk from two factors: *Loss Event Frequency*[83] and *Loss Magnitude*[84].

If obtaining such values is not reliable, their values can be derived from other bottom-oriented factors. Once the values have been obtained, the FAIR model uses a Montecarlo simulation for obtaining a range of quantitative/financial risk of loss in a certain period of time. *Robustness* risk control measures can be merged as the FAIR's model resistance strength branch, in operational risk scenarios such as data poisoning in an adversarial machine learning risk scenario. However, *fairness* risk control measures require a deeper analysis, and a particularly good alternative is to understand the sanctioning psychology of national supervisory authorities, just like in Data Protection and other regulatory compliance domains. This legal analytics approach is a promising alternative to measure fairness, since National Supervisory authorities are the only competent ones to interpret AI law and quantify the impact of AI systems on the fundamental rights of natural persons, through administrative fines and penalties.

D. Conclusion

Artificial Intelligence regulations are beginning to emerge, due to the fast development of artificial intelligence products. In the European Union, legislators have chosen a meta-regulatory approach, by delegating AI risk management to regulatees, in order to protect the fundamental rights of natural persons. However, there are

---

[77] For Hubbard, *"this claim is almost always made without actually doing any proper math"*. Hubbard and Seiersen, (n 49), 59.

[78] *"VAR was first used by major financial firms in the late 1980s to measure the risk of their trading portfolios [..] J.P.Morgan's attempt to establish a market standard through its Risk Metrics system in 1994"*. Thomas J. Linsmeiter and Neil D. Pearson, "Value at Risk," *Financial Analyst Journal*, Vol. 56 No. 2, 47-67, 47.

[79] Finnan, (n. 5), 177.

[80] Finnan, (n 5), 667.

[81] Finnan, (n 5), 474.

[82] Factor Analysis of Information Risk. See, accessed April 13, 2023, https://www.fairinstitute.org/.

[83] *"The probable frequency, within a given time-frame, that loss will materialize from a threat agent's action"*. Freund and Jones, (n 28), 28.

[84] *"The probable magnitude of primary and secondary loss resulting from an event"*. Freund and Jones, (n 28) 35.

many uncertainties about what it means a well-defined risk-based regulatory approach, due to the different contemporary approaches to risk management, and especially the immature states of risk management in several industry areas, such as information security risk management, and even more, in the legal risk management domain. Artificial Intelligence law is closely related to data protection law, as data sets are the input for machine learning models. Nevertheless, there is a huge risk that Artificial Intelligence regulatees choose a non-scientific approach for AI risk management, just like it has happened in the data protection ecosystem. Regulators must be aware that if the AI emergent frameworks do not promote a scientific approach for AI risk management, regulatees may not be able to fulfil the huge mission of protecting the fundamental rights of natural persons. Therefore, the way to perceive compliance must change. Regulators must start by defining basic things such as *risk*, and a *risk-based approach*. Then, they shall promote the right risk-based mechanisms for justifying the risk metrics used for filling up technical documentation. Finally, regulators must not take for granted that a risk-based approach works by default. Promoting a quantitative approach for Artificial Intelligence Risk Assessment that is based on an adequate risk management stack, shall be compulsory.

AI Decision-making in Smart Cities, Japan's Society 5.0

Ruben E. Rodriguez Samudio

A. Introduction

Population trends reveal that citizens are increasingly moving to cities. According to the UN, in 2018, 55.3% of the world's population (4.4 billion people) lived in cities. By 2030, this number will rise to 60.4%.[1] Furthermore, the higher the income of a particular country, the higher percentage of its population that chooses to live in an urban environment.[2] Therefore, the importance of city development goes hand in hand with a country's economic and population growth. This phenomenon is not limited to large cities. A disproportionate number of fastest-growing cities are in the lower-middle-income range.[3] As this trend continues, cities will require better administration to accommodate the population increase if this trend continues.

[1] United Nations, "World Urbanization Prospects: The 2018 Revition", Department of Economic and Social Affairs, 2019, https://population.un.org/wup/publications/Files/WUP2018-Report.pdf.
[2] OECD/European Comission, *Cities in the World: A New Perspective on Urbanization* (Paris: OECD Publishing, 2020), https://doi.org/10.1787/d0efcbda-en.
[3] World Bank, *Competitive Cities for Jobs and Growth: What, Who, and How*, (Washington: The World Bank Group, 2015), https://documents1.worldbank.org/curated/en/902411467990995484/pdf/101546-REVISED-Competitive-Cities-for-Jobs-and-Growth.pdf.

DOI: https://doi.org/10.17875/gup2023-2499

Smart cities are becoming the preferred model of urban development to face the challenges of an increasingly urban population. Governments utilize Information and Communications Technologies (ICT), namely the Internet of Things (IoT), big data analytics, and cloud computing, to collect, transfer, process, and store data. *Edwards* observes that in developed countries, smart cities tend to be "retrofitted" to meet environmental, social, political, or business targets. By contrast, in developing countries, cities are "created from scratch" to enable modernization and development to address population, climate, and migratory issues.[4]
Japan introduced its approach to smart cities in its 5th Science and Technology Basic Plan[5]. Under the title Society 5.0, the Japanese government aims to create a smart society, defined as:

> "[A] *society where the various needs of society are finely differentiated and met by providing the necessary products and services in the required amounts to the people who need them when they need them, and in which all the people can receive high-quality services and live a comfortable, vigorous life that makes allowances for their various differences such as age, sex, region, or language."*

Even before the unveiling of the Society 5.0 plan, there were over 200 smart city projects in Japan.[6] In addition, Japanese industry giants are also actively developing and implementing new initiatives. For example, Panasonic is developing "sustainable smart towns" in existing cities. The first one, Fujisawa SST, was created in 2014 on one of its closed factory sites.[7] Similarly, Toyota's Woven city, currently under construction in Susono City, Shizuoka, is a 708,000 m^2 project fueled by hydrogen cells and is envisioned as a "living laboratory." Its purpose is to serve as a home to full-time residents and researchers who will be able to test and develop technologies such as autonomy, robotics, personal mobility, smart homes, and artificial intelligence in a real-world environment."[8]

---

[4] Lilian Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." *European Data Protection Law Review (EDPL)* 2, no. 1 (2016): 28 (33),
[5] CAO, "The 5th Science and Technology Basic Plan", Council for Science, Technology and Innovation Cabinet Office, Government of Japan, 2015,
The Science and Technology Basic Plan is a five-year plan mandated by the 1995 Science and Technology Basic Law. It maps the science and technology policy of the Japanese government. The first plan was presented in 1996 and the 6th version was published in 2021.
[6] Andrew DeWit, "Japan's Rollout of Smart Cities: What Role for the Citizens?" *The Asia-Pacific Journal* , no. 24 (2013), accessed October 22, 2023, https://apjjf.org/2014/11/24/Andrew-DeWit/4131/article.html.
[7] Tim Hornyak, "Why Japan is Building Smart Cities from Scratch," *Nature Spotlight* 608, no. 32 (2022), accessed October 22, 2023, https://www.nature.com/articles/d41586-022-02218-5.
[8] "Toyota to Build Prototype City of the Future", Toyota, January 7, 2020, accessed October 22, 2023, https://global.toyota/en/newsroom/corporate/31171023.html.

Gassman, *Böhm*, and *Palmié* indicate that as a city's products, processes, and services become intelligent, autonomous, interconnected, and integrated to facilitate ecological and social improvements, they obtain a digital shadow. Initially neutral and without purpose, this shadow is imbued with meaning and significance by its surroundings.[9]

Traditional analysis methods cannot keep up with processing the sheer amount of data that makes up a city's digital shadow. Hence, to mold that initially purposeless shadow, smart cities utilize algorithms in the form of big data analytics. AI allows for data-based, also called evidence-based, decision-making using a city's digital shadow.

This data-driven approach to decision-making receives multiple names: autonomous or automated decision-making, AI-driven decision-making, AI-integrated decision-making support systems, or intelligent decision-making support systems, to name a few. This chapter will refer to these systems as autonomous decision-making (ADM). ADM is already being used to improve public services in areas such as finance, healthcare, marketing, commerce, command and control, and cybersecurity.[10] In addition, commercially available applications also utilize AI to guide users in multiple areas: from autonomous vehicles to map applications that track traffic in real-time to applications suggesting exercise programs or diets based on user preferences.

In contrast to other issues, such as privacy or data protection, rules on AI use are still in their infancy. Thus, the various legal aspects of its use are actively being discussed at the academic and lawmaking level. This chapter presents a brief overview of Japanese efforts in the matter. It begins with an introduction to the concept of smart cities. Next, it explores issues regarding the risk of utilizing AI, followed by an exposition of current regulatory challenges and efforts. Finally, the chapter concludes with Japan's efforts to regulate AI in Society 5.0 and a brief discussion on a recent AI profiling scandal.

I. Smart cities

While the origins of the term smart city can be traced to the 1990s, currently, there is no single accepted definition. The UN's United for Smart Sustainable Cities (U4SSC) initiative focuses on the sustainability aspect of smart cities, which it defines as:

> *"A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation*

[9] Oliver Gassmann, Jonas Böhm and Maximilian Palmié, *Smart Cities: Introducing Digital Innovation to Cities.* (Bingley: Emerald Publishing, 2019), 28.

[10] Gloria Phillips-Wren,"AI Tools in Decision Making Support Systems: A Review," *International Journal of Artificial Intelligence 20*, no.10(2012): 1 (1).

> *and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects."*[11]

The European Commission provides a broader definition of smart cities:

> *"A smart city is a place where traditional networks and services are made more efficient with the use of digital solutions for the benefit of its inhabitants and business.*
>
> *A smart city goes beyond the use of digital technologies for better resource use and less emissions. It means smarter urban transport networks, upgraded water supply and waste disposal facilities and more efficient ways to light and heat buildings. It also means a more interactive and responsive city administration, safer public spaces and meeting the needs of an ageing population."*

Even at the academic level, there is no consensus on a smart city definition. *Albino*, *Berardi*, and *Dangelico* list over 20 definitions dating back to 2000.[12] *Hollands* highlights the difficulties of portraying a city as smart, from the terms used to describe them, the marketing hype, and the uncritical stance towards the urban development model they adopt.[13] A solution, as presented by *Kitchin*, is to approach the issue via classification. For example, by dividing smart cities' definitions into two camps. The first emphasizes the pervasiveness of digitally instrumented devices in the urban environment to monitor, manage and regulate city flows. The second camp prioritizes the knowledge economy within a region where the economy and governance are guided by innovation, creativity, and entrepreneurship.[14]

As the integration of digital devices has become the norm, classification efforts have shifted to the specific goals of a city. For example, *Alexopolous et al.* report that most initiatives focus on any combination of transportation, environment, tourism, health, waste management & water resources, energy-sustainable development, ICT infrastructure, economic development, security, and e-government goals.[15] Indeed, while most publications still tout the perceived benefits of smart cities, there seems to be a trend to focus on specific achievable goals. A possible reason is that most

---

[11] UNECE, "Guidelines for the Development of a Smart Sustainable City Action Plan". UNECE, 2018, https://unece.org/DAM/hlm/documents/Publications/Guidelines_for_SSC_City_Action_Plan.pdf

[12] Vito Albino, Umberto Berardi, and Rosa Maria Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives," *Journal of Urban Technology* 22, no. 1 (2015) 3 (6-8), doi: 10.1080/10630732.2014.942092.

[13] Robert G. Hollands, "Will the real smart city please stand up?," *City* 12, no. 3 (2008): 303 (305-307), doi: 10.1080/13604810802479126.

[14] Rob Kitchin. "The Real-time city? Big data and smart urbanism," *GeoJournal* 79, no. 1 (2014): 1 (1-2), doi: 10.1007/s10708-013-9516-8.

[15] Charalampos Alexopoulos, Gabriela Viale Pereira, Yannis Charalabidis, and Lorenzo Madrid, "A Taxonomy of Smart Cities Initiatives." *ICEGOV* '19: 281 (285), doi: 10.1145/3326365.3326402.

countries in the position to implement these initiatives have already gone through adapting or building the necessary infrastructure and can, therefore, shift their efforts to specific goals.

However, smart cities are not without their critics. *Shelton* and *Lodato* point out that even though they masquerade as a public good, these cities are essentially indistinguishable from earlier iterations of neoliberal urbanism. Instead of providing a cure-all to lagging cities, they reinscribe substantial urban social and spatial inequalities by privileging free market, technology-centric, and expert-driven forms of urban planning and governance.[16] *Kitchin* warns that the promotion of smart cities by several of the world's largest software services and hardware companies might lead to the corporatization of city governance and technological lock-in.[17]

From a legal perspective, the increased participation of the private sector in the administration of cities presents a new set of challenges. Smart city initiatives follow each country's constitutional principles; those that adhere to a western political ideology usually highlight individual rights, while those based on eastern political thought tend to focus more on social order and control.[18] There are numerous examples of countries limiting internet access in times of social turmoil. Hence, the issue of whether traditional constitutional and human rights protection are suited for a smart society is still undecided.

Additionally, the vast amount of data collected also raises privacy and data protection concerns, far too many to tackle in this chapter. *Edwards*[19] and *Van Zoonen*[20] describe the privacy challenges in a smart society. These range from data collection, protection, and combined use of data points to identify individuals to the difficulties of obtaining consent. Regarding this last point, *Finch* and *Tene* note that public services have captive populations who cannot opt-out of information collection without paying a steep price for safety, convenience, and quality of life. Thus, under this urban model, citizens might not have a choice which raises questions as to whether they can consent to provide it in the first place.[21]

---

[16] Taylor Shelton and Thomas Lodato,"Actually Existing Smart Citizens Expertise and (Non)participation in the Making of the Smart City." *City* 23 (2019): 35 (35), doi: 10.1080/13604813.2019.1575115.

[17] Rob Kitchin, (n 14) 10.

[18] Ruben Rodriguez Samudio, "Desafíos constitucionales de las ciudades inteligentes," *CES Derecho* 12, no. 2 (2021): 3 (9-11), doi: 10.21615/cesder.6174.

[19] Lilian Edwards, (n 4) 28-58.

[20] Liesbet Van Zoonen, "Privacy concerns in smart cities," *Government Information Quarterly* 33 (2016): 472-80.

[21] Kelsey Finch and Omer Tene, "Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town." *Fordham Urban Law Journal* 41 (2014): 1581 (1596).

II. Smart cities' citizens

Beyond an academic or industry definition, there is also the question of who makes up smart cities. *Sadowski* and *Bendor* note that the sensors, networks, and algorithms associated with a smart city can be deployed in other settings and contexts. These technologies are neither strictly technical nor social, becoming smart only by their link to the idea of a smart city and the symbolism it embodies.[22]

The citizens, governments, and corporations share this imaginary, and this relationship can be observed in how smart cities are designed and built.
Using a Triple-Helix model, *Leydesdorff* and *Deakin* posit that

> "*[C]ities can be considered as densities in networks among at least these three relevant dynamics: that is, in the intellectual capital of universities, the industry wealth creation, and their participation in the democratic government which forms the rule of law in civil society."*[23]

While Leydesdorff and Deakin approach the city as the convergence of collaboration efforts between government, academia, and industry, their model does not consider direct citizen participation. To address this, other authors[24] propose a modified Quadruple-Helix model that includes civil society in developing smart cities. Recently, a Penta-Helix (Quintuple-Helix) model has appeared. This model provides for the public and private sectors, academia, civic society, and social entrepreneurs. [25] In addition, more and more governments have begun including citizen participation in the design of their policies. As a result, citizens are no longer mere users but both drivers and subjects of change. This increased emphasis on citizen participation responds to the mounting criticism of smart cities.[26]

Two of the four models *Niarios* described in his taxonomy smart cities center on citizen participation: resilient smart cities and commons-based smart cities.[27] Resilient smart cities adopt a bottom-up approach to foster new participatory planning and governance forms. Under this model, communities have ownership and control of the infrastructure, and users can interact privately within a local network and avoid sharing details beyond it. On the other hand, commons-based smart cities are

---

[22] Jathan Sadowski and Roy Bendor, "Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary." *Science, Technology, & Human Values* 4, no. 3 (2018): 540 (541), doi: 10.1177/0162243918806061.
[23] Leydesdorff and Deakin, "The Triple-Helix Model of Smart Cities: A Neo-Evolutionary Perspective." *Journal of Urban Technology* 18, no. 2 (2011): 53 (63), doi:10.1080/10630732.2011.601111.
[24] Patrizia Lombardi, et al., "Modelling the Smart City Performance," *The European Journal of Social Science* 25, no. 2 (2012): 137-149, doi: 10.1080/13511610.2012.660325.
[25] Igor Calzada, «From Smart Cities to Experimental Cities?» In Co-Designing Economies in Transition, ed. Vincenzo Giorgino and Zack Walsh (Cham, Switzerland: Palgrave Macmillan, 2018)
[26] Taylor Shelton and Thomas Lodato, "Actually Existing Smart Citizens," *City* (2019) 35 (36), doi: 10.1080/13604813.2019.1575115.
[27] Vasilis Niaros, "Introducing a Taxonomy of the "Smart City": Towards a Commons-Oriented Approach?" *tripleC* 14, no. 1 (2016): 51 (57-58), doi: 10.31269/triplec.v14i1.718.

characterized by wide citizen engagement in the design and implementation of technological infrastructures. Furthermore, they promote continuous innovation and knowledge diffusion on a global scale via an ongoing circulation of the commons.

Resilient smart cities and commons-based smart cities are indeed enticing. However, the technical knowledge required to participate in these cities is by no means low. There is the risk that compulsory technological engagement in city services could alienate a significant part of the population, particularly in countries with aging populations, such as Japan. Even without the obstacle of age, economic differences might exacerbate inequality by limiting access to those services that require digital devices. In addition, not everyone can achieve the necessary level to collaborate constructively on specific topics, such as AI.

A technologically developed country does not necessarily translate into digital literate citizenship. For example, in a study on perceived surveillance, *Jameson*, *Ritchner,* and *Taylor* report how the citizens of Amsterdam participants often spoke about "the government" as a monolithic entity. In reality, there is no data department of the city municipality, and in some cases, the municipality does not have the technical capabilities and so must outsource some of the analytics.[28] Thus, citizens' expectations might not align with the services they receive, regarding results and how said services operate.

In the case of Japan, a poll from the Ministry of Internal Affairs and Communications reveals that over 89 % of polled individuals have smartphones. Still, only 48 % of respondents have laptops, and a lower percentage of people (26.5 %) use desktop computers.[29] Furthermore, the country ranks 62nd out of 63 countries on digital literacy[30], and there is a marked shortage of skilled labor, with over 89 % of businesses expressing a need for IT-experienced employees.[31]

B. AI in smart cities

Big data analytics is one of the pillars that support smart cities. As collected data increases, the algorithms required to process and use said data become more complex, so it is no longer possible for human actors to perform these tasks. Instead,

[28] Shazade Jameson, Christine Richter, and Linnet Taylor, "People's strategies for perceived surveillance in Amsterdam Smart City," *Urban Geography* 40, no. 10 (2019): 1467 (1474-1475), doi: 10.1080/02723638.2019.1614369.

[29] MIC. Reiwa 2 Nendo Uizu Korona ni okeru Dejitaru Katsuyo no Jitsumu to Riyosha Ishi no Henk ani kansuru Chosa Kenkyu no Ukeoi – Hokokusho-. (Tokyo: Ministry of Internal Affairs and Communications, 2021) (in Japanese).

[30] IMD. "World Digital Competitiveness Ranking". IMD.International Institute for Management Development, 2022. https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/#:~:text=The%20yearly%20ranking%20%E2%80%93%20one%20of,the%20first%20time%20since%202017.

[31] MIC. Dejitaru de Sasaeru Kurashi to Keizai. (Tokyo: Ministry of Internal Affairs and Communications, 2021) (in Japanese).

AI makes sense of the collected data and provides fast, accurate results that can be applied immediately to run public services or within the private sector.

Same as with smart cities, defining AI is a challenging endeavor. As a guide, we turn to *Russell* and *Norvigs* classification.[32] They classify AI definitions based on whether they describe thought processes, reasoning, or behavior, and how they fare against human or ideal (rational) performance. Hence, AI can be defined based on whether they act "humanly" or "rationally", or whether they think "humanly" or "rationally".

There is also a philosophical definition of AI that classifies AI into weak AI, machines that *simulate* or *act* as if they were intelligent, and strong AI, machines that can *actually think*.[33] Moreover, these terms have a narrower meaning when referring to practical application. For example, IBM defines them as follows:

> *"Weak AI, also known as narrow AI, focuses on performing a specific task, such as answering questions based on user input or playing chess. It can perform one type of task, but not both, whereas Strong AI can perform a variety of functions, eventually teaching itself to solve for new problems. Weak AI relies on human interference to define the parameters of its learning algorithms and to provide the relevant training data to ensure accuracy. While human input accelerates the growth phase of Strong AI, it is not required, and over time, it develops a human-like consciousness instead of simulating it, like Weak AI."*[34]

While weak AI has already been achieved and is used to solve multiple issues across various fields, the consensus is that strong AI still belongs to sci-fi. In a review of big data analytics in smart cities, *Soomro et al.* report that AI benefits cut across multiple domains such as transportation planning, urban planning, smart buildings, weather prediction, and analysis.

I. Smarter cities?

The vast quantities of data collected by smart cities make it unusable with traditional methods. *Gassman*, *Böhm*, and *Palmié* explain that modern data analytics through algorithms identify patterns and autonomously improve systems without human intervention.[35] Therefore, arguably, the role of AI in smart cities is effectively to make the city smart enough to use the collected data.

---

[32] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, third edition (NewJersey: Pearson, 2016), 1-2.
[33] John Searle, "Minds, brains, and programs," *Behavioral and Brain Sciences* 3, no. 3 (1980): 417-424, doi: 10.1017/S0140525X00005756.
[34] "Strong AI," IBM, August 31, 2020, accessed October 22, 2023, https://www.ibm.com/cloud/learn/strong-ai.
[35] Gassmann, Böhm and Palmié, (n 9) 273-274.

Soomoro et al. point out that smart cities function by sharing data and information among their various domains and that these domains have traditionally acted as information silos. However, there is an expectation for these barriers to be broken and for information to flow freely, with policymaking being an integrated and holistic process.[36] By combining the data gathered via IoT technologies, ADM can link these information silos to provide multiple solutions to achieve specific goals within the city.

As *Del Gamba* indicates, ADM is a comprehensive concept not limited to one type of decision-making process. In examining the possible application of the GDPR to ADM systems, the author classifies them into those with profiling and those without. The former refers to systems that reach a solution based on a deterministic firm rule that guides the decision-making process automatically, such as speeding fines imposed by speed cameras. On the other hand, ADM uses profiling techniques to collect personal data, process it to identify correlations and apply a model to identify present or future behavior.[37]

Even though *Del Gamba* approach to ADM focuses on GDPR obligations, this classification can be applied to all ADM systems within the city. Furthermore, profiling ADM is not limited to identifiable personal data; it also extends to decisions that might affect certain groups, either via policies directed at them or indirectly via policies that affect the areas where they reside or work.

As *O'Neil* observes, there is always the possibility that the mathematical models that fuel ADM are encoded with human prejudice, misunderstanding, and bias. She coined the term 'weapons of math destruction' to refer to these mathematical models and argues how, while promising efficiency and fairness, they distort higher education, drive up debt, spur mass incarceration, pummel the poor at nearly every juncture, and undermine democracy.[38] Likewise, *Eubanks* posits that the skyrocketing economic insecurity of the last decade has been accompanied by an equally rapid rise of sophisticated data-based technologies in public services, such as predictive algorithms, risk models, and automated eligibility systems. These new systems of digital poverty, as the author calls them, target the poor and the working class.[39]

---

[36] Kamran Soomro, Muhammad Nasir, Mumtaz Bhutta, and Zaheer Khan, "Smart City Big Data Analytics: An Advanced Review", *WIREs Data Mining and Knowledge Discovery* 9, no. 5 (2019). , doi: 10.1002/widm.1319.

[37] Giulia Del Gamba, «Machine Learning Decision-Making: When Algorithms Can Make Decisions According to the GDPR.» In *Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech*, ed. George Borges and Christoph Sorge, (Springer, Cham, 2022), 76-77.

[38] Cathy O'Neil, *Weapons of Math Destruction* (New York: Crown, 2016).

[39] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, (St. Martin's Press, 2018), 9-11.

Both authors call attention to a characteristic of ADM that, while evident, is not necessarily considered in their implementation: their complexity. In this sense, complexity is not limited to the required technical knowledge or the complex systems they link; it also refers to the complex social requirements and effects they produce either by design or by accident[40].

On the technical side, one criticism of ADM systems is that they are usually "black boxes", i.e., they produce accurate results without giving a detailed explanation or reasoning as to how they arrived at that solution. Moreover, because of the opaqueness of such decisions, it is difficult for people to assess whether they were discriminated against based on racial origin.[41]

Pasquale's book "The Black Box Society" is a grim reminder of the risks these systems entail. Specifically, he describes how companies race to keep their methods secret and how, even if they were willing to expose them, some sectors, such as banking or the Internet, pose a thought challenge because of their very nature.[42]

One proposed solution to the black box issue is explainable AI (XAI), programmed to explain its purpose and rationalize the decision process in a way the average user can understand.[43] *Longo et al.* note that there are multiple challenges surrounding XAI. First, in an ideal world, machine explanations and human understanding would be identical and congruent with the ground truth. However, in practice, the ground truth cannot always be fully defined in highly uncertain areas, such as medical diagnoses. Moreover, human models are often based on causality, which is particularly challenging as current machine learning follows pure correlation.[44]

The authors further indicate that current XAI methods highlight input–relevant parts that significantly contributed to a particular output or the most pertinent features of a training data set most influential to the model's accuracy. Unfortunately, XAI methods do not incorporate the notion of human models. They, therefore, do

---

[40] Barocas and Selbst identify five possible ways in which AI might accidentally create discrimination: 1. The way variables are defined; 2. The labeling of training data; 3. Issues with the data used as training data; 4. Issues with the attributes used to reach a decision or "feature selection"; and 5. When criteria that are genuinely relevant to make rational and well-informed decisions nevertheless serve as a reliable proxy for a class. Solon Barocas and Adrew Selbst. "Big Data's Disparate Impact" *California Law Review* 104, no.3 (2019): 671 (677-693), doi: 10.15779/Z38BG31.

[41] Frederik Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making*, (Strasbourg: Council of Europe, Directorate General of Democracy, 2018), 15.

[42] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*,(Harvard University Press, 2015).

[43]Ana Carolina Borges, et al., «An Overview of Explainable Artificial Intelligence (XAI) from a Modern Perspective», In *Explainable Artificial Intelligence for Smart Cities*, ed. Mohamed Lahby, Utku Kose and Akash Kumar Bhoi(CRC Press, 2021), 4.

[44] Luca Longo, et al.., «Explainable Artificial Intelligence: Concepts, Applications, Research Challenges and Visions», In *Machine Learning and Knowledge Extraction,* ed. Holzinger A, Kieseberg P, Tjoa A, Weippl E (Dublin: Springer, Cham, 2020), 10.

not consider causability, defined as "the extent to which an explanation of a statement to a human expert achieves a specified level of causal understanding with effectiveness, efficiency, and satisfaction in a specified context of use and the particular contextual understanding capabilities of a human."[45]

Technical difficulties aside, ADM, powered either by traditional AI or XAI, expert-focused explainability does not solve the trust issue. In other words, even if XAI is developed to the point that human experts can understand and replicate the decision-making process, this would not benefit most citizens. Particularly in those cities that aim for a Penta-helix model, citizen participation will most likely be hindered if only those with advanced technical knowledge can provide input.

While most smart cities are developed under governmental auspices, their success depends on a large part of the citizens, particularly their willingness to adopt certain technologies. In the case of ADM, this means that once a certain usage threshold has been achieved, the technology can continue to grow and evolve, albeit it might do so with incomplete or biased data.

It could be argued that since the average citizen does not have a working knowledge of most city services, such as trains or energy grids, ADM need not be treated differently than other public services. However, this argument fails to convince for multiple reasons. First, while it is true that an average citizen could not perform complex tasks associated with city administration, most citizens would be able to observe, or at the very least have a clue, that these services are not operating correctly. By contrast, as *O'Neil, Eubanks*, and *Pasquale*' demonstrate, identifying issues in ADM systems, such as biases in the data or adverse outcomes, is a time-consuming process that most citizens would most likely not be able to perform.

Another issue has to do with the type of decision being taken. Decisions, as *Phillip-Wren* explicates, can be divided into structured, those with a clear answer; unstructured, where there is no agreed solution and depend on the decision maker; and semi-structured, which can be represented with analytical models or are based on data.[46] Although citizens may agree with most structured decisions, particularly those that do not rely on collecting personal data, the same cannot be said about unstructured and semi-structured decisions.

In the case of unstructured decisions, ADM systems might provide multiple options, all of them valid. However, since there is no agreement on a solution, it will depend on politics and the personal beliefs of decision-makers. In a sense, ADM systems provide the decision-maker with the tools to make a more informed decision, but at the same time, they also might bring questions of responsibility. For example, who is to blame if a particular policy, based on ADM recommendations,

[45] Luca Longo, et al., (n 44).
[46] Gloria Phillips-Wren, (no 10)1-2.

creates problems down the line? The decision-maker? The contractor? Or citizens who did not understand the system enough yet initially benefitted from it?

In privacy and data protection literature, there is the phenomenon known as privacy fatigue, defined as a sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet.[47] Hence, it is not unreasonable to believe that a similar issue could arise regarding ADM systems, where decision-makers, be it public officials, corporations, or citizens, might decide to follow ADM suggestions without questioning them. For example, suppose a decision based on a model that provides what appears to be an adequate solution. Then, what incentives do decision-makers have to question a solution provided via ADM? In other words, ADM runs the risk of creating systems where human's sole role as decision-makers is to put a stamp of approval, regardless of whether they understand or agree with said solution.

II. Regulating AI

An immediate response to the challenges mentioned would be to regulate. However, and the same as any emerging technology, regulatory efforts also face several difficulties. Black and Murray argue current discourse on regulation is drawing us away from the law, or even traditional models of command and control or co-regulation and governance, towards soft self-regulation and codes of practice.[48]

They describe this as an ethical model that has seen the adoption of codes of practice for general AI and data-driven health and care technology, among others. However, the authors caution that ethical standards for such systemic risks are insufficient, particularly in assuming that risks are individualized and that the key to their management is the individual consumer's choices within the marketplace.

Scherer observes that traditional regulation methods are unsuited to manage the risk associated with intelligent and autonomous machines. Particularly, he argues that ex-ante regulation would be difficult because AI research and development may be discreet (requiring little physical infrastructure), discrete (different components of an AI system may be designed without conscious coordination), diffuse (dozens of individuals in widely dispersed geographic locations can participate in an AI project), and opaque (outside observers may not be able to detect potential harmful features of an AI system). Furthermore, the autonomous nature of AI creates issues of foreseeability and control that might render ex-post regulation ineffective, particularly if an AI system poses a catastrophic risk.[49]

---

[47] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung, "The Role of Privacy Fatigue in Online Privacy Behavior." *Computers in Human Behavior* 81, (2018): 42 (42), doi: 10.1016/j.chb.2017.12.001.
[48] Julia Black, and Andrew Murray, "Regulating AI and Machine Learning: Setting the Regulatory Agenda," *European Journal of Law and Technology* 10, no. 3 (2019).
[49] Matthew U Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies," *Harvard Journal of Law & Technology* 29, no. 2 (2016): 354 (356-357).

Regardless of these challenges, the push for regulation has gained momentum, with many countries enacting laws or publishing guidelines that regulate AI. [50] For example, in 2020, the US passed the National Artificial Intelligence Act to coordinate efforts regarding AI research at the Federal Level. Likewise, the are multiple bills at the state level that aim to regulate or promote various aspects of AI. More recently, the White House published the Blueprint for an AI Bill of Rights, which sets forth five principles: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human alternatives, consideration, and fallback.[51]

The AI Bill of Rights establishes that Designers, developers, and deployers should take proactive measures to protect individuals, including equity assessments, use of representative data, protection against proxies for demographic features, accessibility, organizational oversight, independent evaluation, and plain language reporting. Furthermore, the human alternatives, consideration, and fallback principle requires that individuals have the option to opt out of automated systems in favor of a human alternative, where appropriate.

At the European level, the European Parliament's proposal for harmonized rules on artificial intelligence (Artificial Intelligence Act) aims for a comprehensive set of regulations concerning AI. The draft classifies AI depending on its objectives and uses into limited or minimal-risk, high-risk, and unacceptable-risk. The European Commission's website[52] explains minimal-risk AI encompasses most current applications, such as video games or spam filters. Limited-risk applications, such as chatbots, are subject to some transparency obligations that would allow the user to know they are interacting with an AI.

An AI is considered high-risk if it meets the following two criteria: 1. It is intended to be used as a safety component of a product or is itself a product; and 2. The product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product according to various harmonization legislations.

In addition, Articles 12, 13, and 14 establish record-keeping, transparency, and human oversight requirements, respectively. Thus, AI must create an automatic recording of events (logs) that ensure that AI functioning can be traced during its lifetime. Moreover, AI systems must be developed to ensure their operation is transparent enough to allow users to interpret their output and use it appropriately.

50 The OECD has a comprehensive database on various countries AI initiatives, "National AI policies and Strategies", OECD.AI Policy Observatory, OECD.AI, 2022, https://oecd.ai/en/dashboards/overview.

51 "Blueprint for an AI Bill of Rights", The White House, accessed October 22, 2023, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

52 "Regulatory Framework Proposal on Artificial Intelligence," European Commission, accessed October 22, 2022, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

Lastly, AI systems must be designed and developed in a manner that will enable human oversight.

The draft also lists numerous examples of unacceptable-risk AI. For example, when used by public authorities or on their behalf, AI is considered unacceptable if used to evaluate or classify the trustworthiness of natural persons based on their social behavior or known or predicted personal or personality characteristics. Furthermore, AI is also prohibited if such classification leads to detrimental or unfavorable treatment unrelated to the context where the data originated or was collected or is unjustified or disproportionate to their social behavior or its gravity.

III. AI in Society 5.0

Japan has redoubled its efforts to implement AI. The 2017 Strategic Council for AI Technology's "Artificial Intelligence Technology Strategy" established a three-phase roadmap.

The goal is to fuse AI with other technologies to improve productivity, health, medical care, welfare, and mobility. Phase one focuses on the utilization and application of data-driven AI. Productivity-wise, this translates into mass customization, on-demand supply services, and smart factories using IoT and AI. In the healthcare industry, the roadmap aims to implement telemedicine, home medical care, AI-assisted examination, and smart operating rooms. Lastly, some mobility-related goals are to increase car-sharing services, expand GPS-related industries, diversify transportation services, and spread telecommuting in IT.

Phase two, which was supposed to begin around 2020 and should end from 2025 to 2030, emphasizes the public use of AI and data. Specific goals to increase productivity include implementing dynamic pricing, automatic replenishment services, house and home appliances powered by AI, eliminating energy waste, and automatic maintenance of machinery and equipment. Health-wise, some of this phase's objectives are complete medical checkups at home, constant health monitoring services, artificial organs, and even nanobots. Concerning mobility, phase two concentrates on expanding the sharing economy, autonomous transportation and delivery, level 4 autonomous cars, and privatization of travel time and space.

Lastly, phase three aims ecosystem built by connecting multiplying domains. This translates into a society "where innovative services and products are continuously developed" (productivity), "that enjoys healthful lifestyle and longevity" (health), and "that enables safe and free travel" (mobility).

So far, results have been mixed. Some goals, such as increasing car-sharing services, have indeed been achieved. The global pandemic also forced companies to adopt work from home, though it is unclear whether the trend will continue once the situation normalizes. It also helped to increase the use of digital payment services. By contrast, other areas, such as telemedicine, home medical care, and complete medical checkups at home, are still far from being a reality.

In addition, the 2019 report "Social Principles of Human-Centric AI" sets forth the principles that guide the role of AI in Society 5.0. These social principles are

based on three philosophies. First, respect for human dignity translates into a society that does not try to control human behavior through the pursuit of efficiency and convenience and where AI is used only as a tool. The second philosophy is diversity and inclusion, under which people with diverse backgrounds, values, and ways of thinking can pursue their own well-being. Last is creating a sustainable society where AI is used to resolve social disparities while tackling issues such as climate change.

Moreover, the report presents two categories of principles: social and R&D. The socials principles of AI, as detailed in the report, are as follows:

- Human-centric principle: AI should not infringe upon fundamental human rights. Furthermore, AI use should be an individual decision. Stakeholders involved in the development, delivery, and utilization of AI should, depending on the nature of the problem, be responsible for the consequences of AI utilization.
- Education/literacy principle: policymakers and managers of businesses involved in AI must accurately understand AI. By contrast, AI users should have a general understanding. Therefore, educational environments should foster this knowledge by providing a system that allows anyone to understand the basics of AI, mathematics, and data science.
- Privacy protection principle: when utilizing AI, a higher level of discretion may be required than the mere handling of personal data according to the data's level of importance and sensitivity. This principle is a restatement of current privacy laws adapted to AI applications.
- Security principle: Society should always be aware of the balance between the benefits and risks that AI entails.
- Fair competition principle: AI should create a competitive environment that promotes new business. In addition, a country or company's dominant position regarding AI should not determine sovereignty, data collection, or competition practices.
- Fairness, accountability, and transparency principle: AI uses should also translate into a fair and transparent decision-making process with appropriate accountability for the results. Moreover, appropriate explanations should be given on a case-by-case basis depending on the application of AI with adequate opportunities for an open dialogue, as required, regarding the use, adoption, and operation of AI.
- Innovation principle: Society 5.0 should aim for continuous innovation that transcends boundaries, promoting total globalization, diversification, and industry-academia-government cooperation.

Regulation-wise, Japan falls behind other jurisdictions. For one, there is no statutory definition of AI. However, the government's AI Strategy defines AI as a system that realizes an intelligent function. In 2021, the Expert Group on How AI Principles should be implemented published the "AI Governance in Japan Ver. 1.1" report. The expert group adopts an industry-centered approach and recommends

legally non-binding corporate governance guidelines as the most desirable solution. Specifically, the report argues that:

> *"In developing guidelines, not only companies that use AI but also a wide range of stakeholders, including users, engineers, academics, and law/audit experts, should engage in the discussion. It is desirable that the government functions as a facilitator in the discussion and objectively evaluates whether companies satisfy the guidelines developed, thereby enhancing society's trust in the companies that meet the guidelines."*

Specifically, the report calls for guidelines to avoid using standards based on a specific level of experience and one-size-fits-all application to all companies. In addition, guidelines should support the improvement of AI risk management, and function as a benchmark of the trustworthiness of AI systems in inter-company transactions. Ideally, these guidelines should also include helpful practices for companies that have just started using AI, and facilitate the provision of explanations to consumers, etc.

Moreover, the expert group considers that legally binding horizontal requirements for AI systems are unnecessary and that efforts should focus on customer literacy instead. They also oppose mandatory AI-based technology regulation, and even when it is needed, its scope should be limited to prevent them from impacting unintended areas. The report goes one step beyond and argues that it is desirable to respect rulemaking in the respective sectors by making the most of the existing concept of regulations and design philosophy" in some specific industries, such as the automotive and healthcare sectors.

Interestingly, the expert group does not tackle the issue of education/literacy and the impact it might have in protecting users. Instead, it merely points out that the Consumer Affairs Agency released a handbook titled "Handbook on Use of AI-Keys to Effectively Using AI" in 2021. The expert group report explicitly states that one of the reasons for deeming legally binding horizontal regulation unnecessary is the "direction of improvement of literacy through the Handbook on Use of AI."

Recently, Japan faced its first scandal regarding AI profiling. In 2019, the Rikunabi Data Scandal in which a recruitment company sold student's data to prospective employers. Fudo, Arai, and Ema[53] explicate that the Japanese custom of "simultaneous recruitment of new graduates" provides the necessary social background for the scandal to occur. Since most new graduates engage in job hunting simultaneously, some may receive informal job offers from several companies. Therefore, there is always the possibility that some of them might reject an offer,

[53] Kudo Fumiko, Hiromi Arai, and Arisa Ema, "Ethical Issues Regarding the Use of AI Profiling Services for Recruiting: The Japanese Rikunabi Data Scandal.". Arvix, 2020. https://arxiv.org/ftp/arxiv/papers/2005/2005.08663.pdf#:~:text=Ethical%20Concerns%20on%20Power%20Structure&text=The%20incident%20illustrates%20that%20Recruit,should%20recognize%20the%20power%20structure.

thus putting the rejected employers at a disadvantage since they might be unable to fill alternative employees.

The recruitment company operates the Rikunabi job-placement website, which matches employers with job seekers. This website requires job seekers to access its database. In 2018, the company unveiled its "Rikunabi DMP follow" service, which collected and analyzed demographic information and cookies to calculate the probability of students declining informal job offers for a specific company. The algorithms used for profiling were unique for each company and were derived from comparing the users who accepted the offer and those who declined the previous year. The specific algorithms are not published[54].

The main issue in the Rikunabi Data Scandal was not one of profiling via AI, instead it was one of privacy. In 2019, the Rikunabi DMP follow service calculated the score for 74,878 users. At the time, cookies or machine-generated identifiers did not fall within the purview of the Japanese Personal Data Protection Act if they could not be used to identify a person. Since the company was only with data disconnected from names and other personal identifiers, systematically unready to collate additional information to identify individuals, it was not collecting, processing, and providing any personal data and did not need to get user consent to calculate and deliver algorithmic scores to client companies.[55] Moreover, due to a change in the privacy policy, 7983 users were not informed that their information could be provided to companies. This scandal resulted in amendments to the Personal Data Protection Act that established stricter rules on using personal data and its transfer to third parties.

While the social impact of the scandal was primarily felt in privacy circles, since this was the first case concerning "artificial intelligence," it prompted discussions on its use. Due to this publicity, some engineers are concerned that the idea that artificial intelligence is used in recruitment might be linked to a negative image in the public's eye.[56]

C. Conclusions

While discussions on the rights of robots and AI consciousness are still the domain of Sci-fi novels, ADM systems are already being used in government, industry, and entertainment. As a result, there is a renewed emphasis on AI regulation. Japan's Society 5.0 initiative plans to make extensive use of AI technologies.

---

[54] Fumiko, Arai, and Ema, (n 53).

[55] Hinako Sugiyama, Katitza Rodriguez, and Bennet Cyphers. "Japan's Rikunabi Scandal Shows the Dangers of Privacy Law Loopholes," Electronic Frontier Foundation, May 12, 2021, accessed October 22, 2023. https://www.eff.org/deeplinks/2021/05/japans-rikunabi-scandal-shows-dangers-privacy-law-loopholes.

[56] Fumiko, Arai and Ema, (n 53).

In contrast to the EU's Artificial Intelligence Act, Japan has yet to develop or present clear rules concerning ADM systems. Instead, the Japanese approach to regulation, or at the very least the Expert Group's recommendations, are based on an industry-centric regulatory model while trusting users to develop the required knowledge on AI to be able to judge by themselves.

However, this approach does not consider the current reality of the Japanese population's digital literacy. While technologically advanced, Japan has a relatively low level of digital literacy compared to similar countries, both at the general population level and in the IT field. Even though the literacy principle calls for a focus on AI-related subjects and the AI Strategy sets forth specific goals, in practice, whether these goals are achieved does not depend on a single government policy or strategy. Instead, AI use is driven by the cost-benefit analysis companies and individuals make when deciding whether to use a particular application or software. This analysis is based on economic costs, ease of use, results, etc.

Japanese society has a long tradition of seamlessly incorporating technologies into daily activities, and there is no reason to believe that AI will be any different. Nevertheless, a seamless implementation does not equal understanding. If the response, or lack thereof, to Rikunabi scandal is any indication, the Japanese government and the population at large still do not grasp the risks associated with ADM systems.

While still in the drafting stage, if the EU's Artificial Intelligence Act requires GDPR l of adequacy, the current Japanese approach, based on a lack of legally binding rules coupled with low digital literacy and an industry-focused approach to regulation, could lead to the two systems being incompatible.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP 22K13274.

Tokenisierung im deutschen Wertpapierrecht

Sebastian Omlor

A. Verkehrsfähigkeit von unkörperlichen Vermögenswerten

Unkörperliche Vermögenswerte werden klassischerweise durch ihre Verbriefung in einem Wertpapier oder ihre Eintragung in ein Register verkehrsfähig gemacht. Die Blockchain-Technologie eröffnet die technische Möglichkeit, eine solche rechtliche Verknüpfung von Vermögenswert und Transportvehikel ohne eine Verkörperung in einer gegenständlichen Urkunde zu vollziehen. Die Verbriefung des Vermögenswerts erfolgt nicht mehr in einer Papierurkunde, sondern in einem Blockchain-Token: der Prozess der Tokenisierung. Damit könnte ein Wertpapier ohne Papier entstehen. Den ersten Schritt dazu ist der deutsche Gesetzgeber mit der Einführung von elektronischen Wertpapieren durch das eWpG gegangen.

Der nachfolgende Beitrag befasst sich mit der empirischen wie rechtlichen Entwicklung vom klassisch-körperlichen zum funktional-dematerialisierten Wertpapierverständnis. Dabei wird zunächst das Wertpapier als Rechtskonstrukt beleuchtet, das konzeptionell zumindest de lege ferenda eine Entwicklungsoffenheit gegenüber der technischen Entwicklung aufweist (nachfolgend, sub B.). Sodann wird auf den Token als Rechtsobjekt eingegangen, der durch eine Tokenisierung von Vermögenswerten zum Wertpapier im funktionellen Sinn werden kann (nachfolgend, sub C.). Abschließend folgt ein zusammenfassender Ausblick (nachfolgend, sub D.).

DOI: https://doi.org/10.17875/gup2023-2500

B. Das Wertpapier als Rechtskonstrukt

Das Wertpapier kennt in der deutschen Rechtsordnung keine übergreifende Legaldefinition. Seine Rechtsquellen sind anders als etwa in der Schweiz (Art. 965 ff. OR) oder den USA (Art. 3 und 8 UCC) nicht zusammenfassend kodifiziert, sondern über das Privat-, Handels- und Kapitalmarktrecht verstreut.[1] Dennoch hat sich zur Systembildung im Wertpapierrecht und zur Bestimmung seines Anwendungsbereichs eine rechtliche Begriffsbildung vollzogen. Mangels einer Kodifizierung dieser Definition besteht aber eine gewisse Entwicklungsoffenheit.

I. Ausgangspunkt: Wertpapiere im rechtlich-formalen Sinne

1. Wertpapierdefinition

Wertpapiere als Gegenstand des gleichnamigen Wertpapierrechts werden klassischerweise nicht nach ihren wirtschaftlichen Funktionen, sondern nach ihren rechtlichen Eigenschaften definiert. Nach dem ganz überwiegend vertretenen Wertpapierbegriff handelt es sich um eine Urkunde, die ein subjektives Recht in der Weise verbrieft, dass es nur der Inhaber der Urkunde ausüben kann.[2] Irrelevant aus Sicht des Wertpapierzivilrechts ist dabei ein wirtschaftlicher Wertpapierbegriff, der eine funktionellen Betrachtungsweise folgt. Danach bedürfte es lediglich eines verbrieften Schuldtitels, der fungibel und liquide ist.[3] Diese Funktionalität kann je nach der technischen Spezifikation auch eine unkörperliche Urkunde erfüllen.

2. Token im Wertpapierzivilrecht

Blockchain-Token stellen keine Wertpapiere im Sinne des Wertpapierzivilrechts dar.[4] Die Anforderungen des § 793 BGB an Inhaberschuldverschreibungen erfüllen

[1] Überblick bei Matthias Casper, «A. Grundzüge des Wertpapierrechts», in *Wechselgesetz, Scheckgesetz, Recht des Zahlungsverkehrs*, hrsg. Adolf Baumbach, Wolfgang Hefermehl und Matthias Casper, 24. Aufl., (München: C.H. Beck, 2020), A. Rn. 1.

[2] Stellvertretend Matthias Habersack, «vor § 793», in *Münchener Kommentar BGB*, hrsg. Franz Saecker et al., 8. Aufl. (München: C.H. Beck, 2020), Rn. 9, 11; Dirk Bliesener und Hannes Schneider, « 17. Kapitel SchVG – Gesetz über Schuldverschreibungen aus Gesamtemissionen», in *Bankrechts-Kommentar*, hrsg. Katja Langenbucher, Dirk Bliesener und Gerald Spindler, 3. Aufl. (München: C.H. Beck, 2020), Rn. 16; Lutz Haertlein, «28. Kapitel Pfandrecht an Forderungen und Wertpapieren – §§ 1273–1296 BGB», in *Bankrechts-Kommentar*, hrsg. Katja Langenbucher, Dirk Bliesener und Gerald Spindler, 3. Aufl. (München: C.H. Beck, 2020), Rn. 16; Markus Gehrlein, «§ 793», in *BeckOK BGB*, hrsg. Wolfgang Hau und Roman Poseck, 64. Aufl (München: C.H. Beck, 01.11.2022), Rn. 1; a.A. Eugen Ulmer, *Das Recht Der Wertpapiere* (Berlin: Kolhammer, 1936), 21.

[3] Sebastian Hartrott, «§ 193», in *KAGB-Kommentar*, hrsg. Wolfgang Weitnauer, Lutz Boxberger und Dietmar Anders, 3. Aufl. (München: C.H. Beck, 2021), Rn. 13.

[4] Für die Einordnung als Wertpapier: Markus Kaulartz und Robin Matzke, „Die Tokenisierung des Rechts," *NJW,* (2018): 3278, 3282 f.; Robin Matzke und Markus Kaulartz, «Kapitel 14 Smart Contracts und die Tokenisierung», in *Rechtshandbuch Smart Contracts*, hrsg. Tom Braegelmann und

autonome Token[5] bereits deshalb nicht, weil ihnen kein Leistungsversprechen innewohnt.[6] Sowohl autonome als auch aufgeladene Token scheitern de lege lata jedoch am Erfordernis der Urkunde.[7] Der Urkundenbegriff des § 793 BGB beschränkt sich auf schriftliche Gedankenäußerungen.[8] Erwägenswert wäre allenfalls eine Analogie zu § 793 BGB,[9] die sich jedoch seit dem Inkrafttreten der Sonderregel (nur) für elektronische Wertpapiere in § 2 eWpG Zweifeln an der Planwidrigkeit einer Regelungslücke ausgesetzt sieht. Eine unmittelbare wie analoge Anwendung von § 952 BGB kommt ebenfalls nicht in Betracht. Eine direkte Anwendung scheitert ebenso wie im Fall von § 793 BGB an der fehlenden Verkörperung von Token.[10] Für einen Analogieschluss fehlt es an der vergleichbaren Interessenlage, weil eine dingliche Tokenisierung, wie sie § 952 BGB funktional zugrunde liegt, außerhalb des eWpG nicht möglich ist.[11]

II. Entwicklungsperspektive: Wertpapiere im rechtlich-funktionellen Sinn

1. Wertpapierfunktionen

Zu den zentralen Wertpapierfunktionen gehören die Mobilisierungs-, die Legitimations- und die Präsentationsfunktion sowie der Ausschluss von Einwendungen.[12] Ein unkörperliches Recht kann durch die wertpapierrechtliche Verbriefung dem

---

Markus Kaulartz (München: C.H. Beck, 2019), Rn. 25 ff.; gegen die Einordnung als Wertpapier: Ursula Kleinert und Volker Mayer, „Elektronische Wertpapiere und Krypto-Token," *EuZW,* (2019): 857, 859; Sebastian Omlor und Florian Möslein, «§ 34 FinTech und PayTech», in *Bankrechts-Handbuch*, hrsg. Jürgen Ellenberger und Hermann-Josef Bunte, 6. Aufl. (München: C.H. Beck, 2022), Rn. 39 f.

[5] Zum Begriff vgl. Sebastian Omlor, «Kapitel 6: Allgemeines Privatrecht», in *Handbuch Kryptowährungen und Token*, hrsg. Sebastian Omlor und Mathias Link, 2. Aufl. (Frankfurt am Main: Fachmedien Recht und Wirtschaft, dfv Mediengruppe, 2023), Rn. 25 ff.

[6] Sebastian Omlor, „Digitales Eigentum an Blockchain-Token – rechtsvergleichende Entwicklungen," *ZVglRWiss,* 119 (2020): 41, 50 f.

[7] Eingehend Kaulartz und Matzke, (Fn. 4), 3278, 3281 ff.

[8] Peter Marburger, «§ 793», in *Staudingers Kommentar zum Bürgerlichen Gesetzbuch: §§ 779-811*, hrsg. Peter Marburger (Berlin: Sellier - de Gruyter, 2015), Rn. 2; Gehrlein, (Fn. 2), § 793 Rn. 1, jeweils m.w.N.

[9] Ablehnend Stefan Möllenkamp und Leonid Shmatenko, «Teil 13.6. Blockchain und Kryptowährungen», in *Multimedia-Recht*, hrsg. Thomas Hoeren, Ulrich Sieber und Bernd Holznagel, 56. Aufl. (München: C.H. Beck, 2022) Rn. 49; befürwortend Philipp Koch, „Die „Tokenisierung" von Rechtspositionen als Digitale Verbriefung," *ZBB*, (2018): 359, 364; offen auch Kaulartz und Matzke, (Fn. 4), 3278, 3281 ff.

[10] Omlor, (Fn. 5), Kap. 6 Rn. 47; Kaulartz und Matzke, (Fn. 4), 3278, 3281; Martin Schermaier, «§ 952», in *BeckOKG/BGB*, hrsg. Beate Gsell et al. (München: C.H. Beck, 01.12.2022), Rn. 6, 20.

[11] Kaulartz und Matzke, (Fn. 4), 3278, 3281.

[12] Überblick zum Folgenden bei Casper, (Fn. 1), A. Rn. 4 ff.; Matthias Casper, «§ 28 Elektronische Schuldverschreibungen», in *FinTech-Handbuch*, hrsg. Sebastian Omlor und Florian Möslein, 2. Aufl. (München: C.H. Beck, 2021), § 28 Rn. 1-5.

Sachenrecht unterworfen und damit mobilisiert werden. In der Folge kommt ihm ein Verkehrsschutz durch gutgläubigen Erwerb nach §§ 932 ff. BGB zugute. Weiterhin legitimiert die Innehabung der Urkunde, indem daran eine Rechtsvermutung zugunsten des Gläubigers und des Schuldners geknüpft wird. Nicht nur entfällt die Notwendigkeit eines Nachweises der Rechtinhaberschaft (vgl. § 793 Abs. 1 Satz 1 BGB), sondern überdies kann befreiend an den Inhaber der Urkunde geleistet werden (vgl. § 793 Abs. 1 Satz 2 BGB). Zudem kann die Urkunde als einfaches Präsentationspapier den Schuldner befugen, seine Leistung von der Präsentation der Urkunde abhängig zu machen. Schließlich wird dem Schuldner ein Berufen auf §§ 404 ff. BGB verwehrt, indem lediglich aus dem Wertpapier ersichtliche Einwendungen aus dem Grundverhältnis mit dem Zedenten vorgebracht werden können (vgl. § 796 BGB, § 364 Abs. 2 HGB).

2. Elektronische Wertpapiere als Zwischenschritt

Mit der Einführung von elektronischen Wertpapieren hat sich der deutsche Gesetzgeber einen Schritt auf das dematerialisierte Zukunftsmodell von Wertpapieren im rechtlich-funktionellen Sinn zubewegt. Durch die rechtliche Äquivalenzanordnung in § 2 Abs. 2 eWpG werden elektronische und klassisch-körperliche Wertpapiere gleichgestellt. Da elektronische Wertpapiere namentlich in Gestalt von Kryptowertpapieren auch auf Blockchain-Basis ausgegeben werden können,[13] handelt es sich dabei um den historisch ersten Fall einer dinglichen Tokenisierung nach deutschem Recht.

Allerdings wurde der Übergang vom rechtlich-formalen zum rechtlich-funktionalen Wertpapiersystem mit dem eWpG noch nicht vollendet. Am augenscheinlichsten zeigt sich der Hybridcharakter der elektronischen Wertpapiere an der Sachfiktion des § 2 Abs. 3 eWpG.[14] Das dematerialisierte Wertpapier wird rechtlich als ein körperlicher Gegenstand behandelt. Damit soll das auf körperliche Gegenstände i.S.d. § 90 BGB zugeschnittene BGB-Sachenrecht auf Datensätze in einer dezentralen Datenbank erstreckt werden.[15] Unabhängig von der rechtspolitischen Kritik[16] an der verfehlten Sachfiktion führt sie jedenfalls zu einem Hybridcharakter der elektronischen Wertpapiere: zwischen dem rechtlich-formalen und dem rechtlich-funktionalen Wertpapierbegriff.

---

[13] Julia von Buttlar und Sebastian Omlor, „Tokenisierung von Eigentums-, Benutzungs-, Zutritts- und Pfandrechten," *ZRP,* (2021): 169 f.; BT-Drucks. 19/26925 S. 41 f.

[14] Zur Kritik Sebastian Omlor, „Re- statt Dematerialisierung des Sachenrechts," *RDi,* (2021): 236, 240; Ulrich Segna, „Elektronische Wertpapiere im zentralen Register," *WM,* (2020): 2301, 2304; Matthias Lehmann, „Zeitenwende im Wertpapierrecht," *BKR,* (2020): 431, 433.

[15] Vgl. zu Grenzen Sebastian Omlor, «§ 6 Verfügungen über elektronische Wertpapiere», in *Elektronische Wertpapiere*, hrsg. Sebastian Omlor, Florian Möslein und Stefan Grundmann (Tübingen: Mohr Siebeck, 2021), 141.

[16] Zutreffend Benjamin Lahusen, „Das Sachenrecht der elektronischen Wertpapiere," *RDi,* (2021): 161, 166, 167 (Rn. 25-32).

3. Wertpapiere im rechtlich-funktionellen Sinn

a. Legitimations- und Repräsentationsfunktion

Wertpapiere im rechtlich-funktionellen Sinn lösen die rechtliche Wertpapierdefinition von den formalen Begrenzungen eines vorgegebenen Bezugsobjekts mit bestimmten Eigenschaften wie beispielsweise Körperlichkeit. An ihre Stelle setzt der rechtlich-funktionale Begriff die Einhaltung der rechtlich anerkannten Wertpapierfunktionen. Damit wird der wertpapierzivilrechtliche Tatbestand nicht der Beliebigkeit oder Konturenlosigkeit preisgegeben. Lediglich das Tatbestandsmerkmal der Urkunde etwa in § 793 Abs. 1 Satz 1 BGB oder § 952 BGB wird an den Prozess der Dematerialisierung angepasst. Auch führt eine Ausrichtung an der Funktionalität nicht zu einer Aufgabe normativ-rechtlicher Anforderungen. Diese kommen vor allem in der Erfüllung der Wertpapierfunktionen zum Tragen. Hervorzuheben sind dabei die Repräsentations- und Legitimationsfunktion. Ob ein Vermögenswert in einem Wertpapier in der Form verbrieft ist, dass seine Innehabung eine rechtliche Vermutung zugunsten der materiellen Inhaberschaft auslöst, ist eine exklusiv rechtliche Dimension. Eine dinglich-absolute Verknüpfung von verbrieftem Vermögenswert und Wertpapier geschieht wegen der inter omnes-Wirkungen nicht durch Parteivereinbarung, sondern nur durch gesetzliche Anordnung; ebenso wurde mit § 2 Abs. 2 eWpG verfahren.

b. Mobilisierungsfunktion

Angepasst werden müsste jedoch die Mobilisierungs- oder Transportfunktion. Im klassisch-körperlichen Wertpapierzivilrecht wird die Mobilisierung der verbrieften Vermögenswerte durch eine Anbindung an das Sachenrecht erzeugt. Die Verkehrsfähigkeit stellen die Vorschriften zum gutgläubigen Erwerb von beweglichen Sachen sicher. Von einer solchen exklusiven Ausrichtung auf eine Mobilisierung durch das Sachenrecht müsste sich ein dematerialisiertes und auf die Erfüllung der Wertpapierfunktionen ausgerichtetes Wertpapierzivilrecht lösen. Eine Mobilisierung der verbrieften Vermögenswerte könnte alternativ über ein registerrechtliches Modell erfolgen, wie es beispielsweise für schweizerische Wertrechte vorgesehen ist. Mit dem DLT-Gesetz[17] hat die Schweiz ihr Bucheffektenrecht für die Blockchain-Technologie geöffnet.[18] Nach Art. 973e OR werden klassische Wertpapier-

[17] Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, 25.09.2020, abgerufen am 7. Januar 2023, https://www.fedlex.admin.ch/eli/oc/2021/33/de.

[18] Dazu im Überblick Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilten elektronischen Registern vom 27. November 2019, *BBI,* (2020): 258 ff.

funktionen bei Registerwertrechten unter Rückgriff auf das Wertrechteregister erfüllt. Das in Art. 973d Abs. 2 OR technologieneutral geregelte Wertrechteregister kann insbesondere in Gestalt einer Blockchain geführt werden.[19] Dabei nimmt es u.a. die Funktion eines Rechtsscheinträgers ein, auf dessen Inhalt der Rechtsverkehr in Gestalt des gutgläubigen Erwerbers vertrauen kann (Art. 973e Abs. 3 OR).

c. Parallele zum Geldbegriff

Diese Funktionalisierung und Abstrahierung des Wertpapierbegriffs steht in gedanklicher Nähe zu den unterschiedlichen Geldbegriffen. Weder der Wertpapier- noch der Geldbegriff kennt eine Verankerung in einer Legaldefinition. Der rechtliche Begriff des Geldes stellt vielmehr eine Nominaldefinition dar. Zu unterscheiden ist auf Grundlage des zweigliedrigen Geldbegriffs zwischen dem Geld im konkreten und abstrakten Sinn.[20] Der konkrete Geldbegriff beschränkt sich auf das materiegebundene Sachgeld (Bargeld), soweit es als gesetzliches Zahlungsmittel mit einem Annahmezwang ausgestattet ist.[21] Ihm steht der abstrakt-funktionale Geldbegriff gegenüber, der unabhängig von einer Verkörperung besteht.[22] Zentral ist die Erfüllung der Geldfunktionen, Recheneinheit und neutrales Universaltauschmittel zu sein. Hinzu tritt die Notwendigkeit einer normativen Anerkennung, an welche aber nur geringe Anforderungen zu stellen sind.

Geldgeschichtlich stellt die Erweiterung des konkret-gegenständlichen um einen abstrakt-funktionalen Geldbegriff eher ein jüngeres Phänomen dar.[23] Geldgeschichte ist immer auch Technikgeschichte. Die Erscheinungsformen des Geldes unterlagen stets auch einem an den technischen Möglichkeiten orientierten Wandel. Exakt ein solcher Evolutionsschritt ist auch im Wertpapierzivilrecht überfällig. Im Unterschied zum Geldrecht bedarf es im Wertpapierzivilrecht jedoch eines Nachvollziehens der technologisch-empirischen Dematerialisierungsentwicklung. Zwar kennt auch das Wertpapierzivilrecht keine Legaldefinition des Wertpapiers. Allerdings zeichnen sich die Wertpapierfunktionen durch eine originäre Dinglichkeit und Drittwirkung aus, die lediglich der demokratisch legitimierte Gesetzgeber anordnen kann.

C. Token als Wertpapiere im funktionellen Sinn

Der Prozess der Dematerialisierung prägt nicht nur das Geld und seine Erscheinungsformen, sondern auch die Wertpapiere und ihren Rechtsrahmen. Blockchain-

[19] Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019, *BBl*, (2020): 281.
[20] Eingehend dazu Sebastian Omlor, *Geldprivatrecht* (Tübingen: Mohr Siebeck, 2014), 96 ff.
[21] Sebastian Omlor, «Vorbem zu §§ 244-248», in *Staudingers Kommentar zum Bürgerlichen Gesetzbuch: §§ 244-248,* hrsg. Volker Rieble (Berlin: Otto Schmidt - De Gruyter, 2021), Vorbem A84.
[22] Omlor, (Fn. 21), Vorbem A64.
[23] Überblick bei Omlor, (Fn. 20), 96 ff.

Token bieten sich als dematerialisierte Bezugsobjekte für die klassischen Wertpapierfunktionen an; sie werden durch eine dingliche Tokenisierung zu Wertpapieren im funktionellen Sinne.

I. Typenbildung

Zur rechtlichen Umsetzung dieser Transformation bedarf es eines zivilrechtlichen Blicks auf die Typenbildung bei Blockchain-Token.

1. *Funktionsorientierte Einordnung*

Aus der vor allem in der Anfangszeit, aber auch weiterhin fortdauernden Dominanz der aufsichtsrechtlichen Perspektive auf die Kryptomärkte und die Blockchain-Technologie resultiert, dass in der Literatur[24] und in öffentlichen Stellungnahmen[25] eine Typenbildung von Token nach Funktion vorherrschend war. Auch die Unterscheidung zwischen wertreferenzierten Token, E-Geld-Token und Utility Token in der MiCA-Verordnung[26] folgt zum Teil diesem Muster. Typisiert existieren danach drei Arten von Token: Asset/Security Token, Utility Token und Currency Token. Anlage-Token dienen der Kapitalanlage; sie unterteilen sich in die Unterkategorien Security (Equity) Token und Asset Token. Die wertpapierähnlichen Security Token gewähren Mitsprache-, Beteiligungs- oder Gewinnbezugsrechte,[27] während Asset Token die Inhaberschaft an einem Recht oder einer Forderungen repräsentieren.[28] Nutzungstoken (Utility Token) fungieren als „Gutscheine" und gewähren einen Zugang zu einer Leistung, die nicht aus einer Kapitalanlage oder unternehmerischen Beteiligung stammt.[29] Schließlich dienen Zahlungstoken (Currency Token) als Zahlungsmittel, ohne einen wie auch immer gearteten Leistungsanspruch gegen einen

---

[24] Stellvertretend Philipp Hacker und Chris Thomale, „Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law," *ECFR,* 15 (2018): 645, 652 f.; Peter Zickgraf, „Initial Coin Offerings - Ein Fall für das Kapitalmarktrecht?," *AG,* (2018): 293, 295 f.; Rüdiger Veil, „Token-Emissionen im europäischen Kapitalmarktrecht," *ZHR,* 183 (2019): 346, 348 f.; Michaela Hönig, *ICO und Kryptowährungen*, (Wiesbaden: Springer Fachmedien, 2020), 33 ff.

[25] Siehe Blockchain-Strategie der Bundesregierung, 6, 18.09.2019, abgerufen am 7. Januar 2023, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.html, BaFin, Merkblatt – Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token WA 51-Wp 7100-2019/0011 auch IF 1-AZB 1505-2019/0003, 5 f.; FIMNA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings, 16.02.2018, 3; ESMA, Advice: Initial Coin Offering and Crypto-Assets, 19.10.2018, 9 ff.; UK Cryptocurreny Taskforce (Final Report), 30.07.2018, 11 ff.

[26] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937.

[27] Hönig, (Fn. 24), 35; Caspar Behme und Peter Zickgraf, „Zivil- und gesellschaftsrechtliche Aspekte von Initial Coin Offerings (ICOs)," *ZfpW,* (2019): 66, 69.

[28] Kaulartz und Matzke, (Fn. 4), 3278, 3280.

[29] Omlor, (Fn. 5), Kap. 6 Rn. 20; Mathias Fromberger und Patrick Zimmermann, «§ 1 Technische und rechtstatsächliche Grundlagen», in *Rechtshandbuch Kryptowerte*, hrsg. Philipp Maume und Lena

Emittenten vorauszusetzen. Hybride Mischformen dieser drei Typen sind konstruktiv möglich und empirisch verbreitet.

2. Inhaltsorientierte Einordnung

Der vor allem für die Regulierungszwecke des Aufsichtsrechts dienenden Typenbildung nach Funktionen steht die namentlich für die Regelungsanliegen des Zivilrechts vorzugswürdige Unterteilung nach dem Tokeninhalt gegenüber.[30] Auch für die kollisionsrechtliche Anknüpfung ist dieses Differenzierungsmerkmal tauglicher.[31] Das Wesen von Token lässt sich nicht ohne Einbeziehung ihres materiellrechtlichen Gehalts bestimmen; es bestimmt über die Einordnung in das Regelungskonzept des BGB, insbesondere zum absoluten Schutz von Token. Vorzunehmen ist danach eine typisierende Zweiteilung nach dem materiell-rechtlichen Gehalt von Token. Insofern stehen sich aufgeladene Token (Charged Token) und autonome Token (Natural Token) gegenüber.[32] Auf eine terminologische Abweichung ist die Unterscheidung zwischen intrinsischen und extrinsischen Token im Wesentlichen beschränkt.[33] Ein aufgeladener Token bildet das Produkt einer Tokenisierung von Vermögenswerten, die außerhalb dieser Blockchain existieren. Dieser Tokenkategorie kommt damit eine Containerfunktion zu, da sie als Wertpapier im funktionalen Sinn auf einer Verbriefung von Vermögenswerten führt. Demgegenüber beschränken sich autonome Token auf ein Eigenleben innerhalb ihres Blockchain-Netzwerks. Sie repräsentieren keine sonstigen Vermögenswerte. Den Hauptanwendungsfall bilden Zahlungstoken (Kryptowährungen).

II. Prozess der Tokenisierung

1. *Begriff der Tokenisierung*

Durch eine Tokenisierung von Vermögenswerten werden Token zu Wertpapieren im funktionellen Sinn. Bei einer Tokenisierung handelt es sich um den Prozess der Aufladung eines Token und damit um die Schaffung eines aufgeladenen Token.[34]

Maute (München: C.H. Beck, 2020), § 1 Rn. 73; Mathias Fromberger und Philipp Maume, "Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws," *Chicago Journal of International Law* 19, (2019): 548, 560; Lars Haffke, Mathias Fromberger und Patrick Zimmermann, "Kryptowerte und Geldwäsche," *BKR,* (2019): 377, 378.

[30] Dazu eingehend Omlor, (Fn. 5), Kap. 6 Rn. 24 ff.

[31] Christiane Wendehorst, «Art. 43 EGBGB», in *Münchener Kommentar BGB*, hrsg. Franz Saecker et al., 8. Aufl. (München: C.H. Beck, 2021), Rn. 309-311.

[32] Omlor und Möslein, (Fn. 4), § 34 Rn. 38.

[33] Dazu Möllenkamp und Shmatenko, (Fn. 9), Teil 13.6 Rn. 29 ff.; dem folgend Wendehorst, (Fn. 31), Rn. 309.

[34] Matzke und Kaulartz, (Fn. 4), Kap. 14 Rn. 5; Omlor und Möslein, (Fn. 4), § 34 Rn. 39; Omlor, (Fn. 5), Kap. 6 Rn. 93; ungenau BaFin, Fachartikel Tokenisierung, 15.4.2019, abgerufen am 7. Januar

Konzeptionell kann der zugeordnete Vermögenswert beliebiger Art sein: physische Sachen, Forderungen, Immaterialgüterrechte, andere Rechte i.S.d. § 413 BGB und Token, die auf einer anderen Blockchain verwaltet werden. Welche Bezugsobjekte für eine Tokenisierung verwendet werden, ist eine privatautonome Entscheidung innerhalb des gesetzlichen Rahmens.

2. Vorteile einer Tokenisierung

Mit einer Tokenisierung werden ähnliche Zwecke wie mit einer wertpapierrechtlichen Verbriefung verfolgt.[35] Idealiter soll ein Inhaberpapier nach dem Vorbild des § 793 Abs. 1 BGB geschaffen werden. Für die schweizerischen Registerwertrechte existiert eine ähnliche Ausgestaltung bereits in Art. 973e Abs. 1-2 OR. Der digitale Eintrag in die Blockchain würde als Rechtsscheinträger fungieren,[36] wie es Art. 973e Abs. 3 OR bereits für das schweizerische Wertrechteregister vorsieht. Zudem eröffnet die technische Anschlussfähigkeit für Smart Contracts und dezentrale Applikationen (DApps) zahlreiche Anwendungsfelder innerhalb desselben Ökosystems.[37] Beispielhaft zu nennen ist die Schaffung eines Blockchain-Kapitalgesellschaftsrechts mit einer tokenisierten Mitgliedschaft.[38]

Nicht notwendigerweise exklusiv mit einer Tokenisierung verbunden wäre hingegen die Übertragbarkeit ohne Intermediäre und in Echtzeit.[39] Diese Ziele könnten technisch potenziell auch ohne Einbeziehung einer Blockchain erreicht werden, auch wenn die Blockchain-Technologie typischerweise mit einer Disintermediation in Verbindung steht. Grenzen der Disintermediation können vielmehr aus technologieneutralem Aufsichtsrecht folgen, wie es beispielsweise die CSD-Verordnung („CSDR")[40] vorgibt; daraus folgt beispielsweise die Notwendigkeit von Zentralregisterwertpapieren und den zugehörigen zentralen Registern (§ 4 Abs. 5-6, § 12 Abs. 2 eWpG).

2023, https://www.bafin.de/SharedDocs/Ver&leer;oeffentlichungen/DE/Fachartikel/2019/fa_bj_1904_Tokenisierung.html.

[35] Markus Kaulartz, Katharina Hirzle und Benedikt Holl, „Tokenisierung durch das Auslobungsmodell," *RDi,* (2022): 324 Rn. 5.

[36] Zur Bedeutung von Registertransparenz infolge einer Tokenisierung Robin Matzke, «§ 10 Tokenisierung», in *FinTech-Handbuch*, hrsg. Sebastian Omlor und Florian Möslein, 2. Aufl. (München: C.H. Beck, 2021), Rn. 26 ff., 46.

[37] Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 6.

[38] Grundlegend Florian Möslein, Sebastian Omlor und Nils Urbach, „Grundfragen eines Blockchain-Kapitalgesellschaftsrecht," *ZIP*, (2020): 2149 ff.

[39] Zu weitgehend Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 6.

[40] Art. 3 der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012.

3. Rechtliche Modelle

In ihrer Rechtsnatur, aber auch in ihren rechtlichen Wirkungen ist zwischen einer schuldrechtlichen und einer dinglichen Tokenisierung zu unterscheiden.

a. Schuldrechtliche Ausgestaltung

aa. Grundlagen

Jenseits des eWpG lässt die deutsche Privatrechtsordnung gegenwärtig nur eine schuldrechtliche Tokenisierung zu. Ihr Defizit liegt in der Relativität der Schuldverhältnisse begründet. Eine dinglich-absolute Wirkung erga omnes ist mit diesen Gestaltungen nicht verbunden. Selbst ein rechtsgeschäftliches Verfügungsverbot hätte keine dingliche Wirkung (§ 137 BGB). Ein dematerialisiertes Wertpapier im funktionellen Sinn lässt sich durch rein schuldrechtliche Vereinbarungen nicht erschaffen. Stets besteht das Risiko eines Auseinanderfallens von Token und zugehörigem Vermögenswert.[41] Daher handelt es sich insofern zumeist lediglich um Hilfskonstruktionen in Ermangelung eines tauglichen gesetzlichen Rahmens für eine dingliche Tokenisierung.

In der vertragstechnischen Umsetzung ist zwischen dem Ausgabe- und Begebungsvertrag zu differenzieren. Ebenso wie im Wertpapierrecht[42] stellt der Ausgabevertrag den Rechtsgrund i.S.d. § 812 Abs. 1 BGB für die Tokenübertragung und die Zuordnung des Vermögenswerts dar.[43] Der Begebungsvertrag hingegen bringt den tokenisierten Vermögenswert zur Entstehung.[44] Seiner Rechtsnatur nach kommen ein Vorvertrag oder ein Optionsvertrag in Betracht.[45] Nicht enthalten ist jedoch eine dingliche Einigung. Auch eine schuldrechtlich-dingliche Rechtsnatur fehlt ihm, da eine dingliche Tokenisierung jenseits des eWpG ausgeschlossen ist.[46]

bb. Auslobungsmodell

Eine Unterform der schuldrechtlichen Tokenisierung verwendet eine Auslobung nach § 657 BGB.[47] Die Auslobungserklärung als einseitige, nicht empfangsbedürftige Willenserklärung[48] kann auf einer Website oder in einem White Paper durch

[41] Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 9 ff. unter Darstellung der einzelnen Gestaltungsoptionen.

[42] Casper, (Fn. 1), A. Rn. 28 ff.

[43] Lena Maute, «§ 6 Verträge über Kryptotoken», in *Rechtshandbuch Kryptowerte*, hrsg. Philipp Maume und Lena Maute (München: C.H. Beck, 2020), Rn. 163 ff.

[44] Michael Jünemann und Johannes Wirtz, „ICO: Rechtliche Einordnung von Token," *Kreditwesen,* 21/23, (2018): 2.

[45] Maute, (Fn. 43), Rn. 168 ff.

[46] Jünemann und Wirtz, (Fn. 44), 5.

[47] Im Einzelnen Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 20-29.

[48] Frank Schäfer, «§ 657», in *Münchener Kommentar BGB*, hrsg. Franz Saecker et al., 9. Aufl. (München: C.H. Beck, 2023), Rn. 6.

den Emittenten veröffentlicht werden. Die Widerruflichkeit der Auslobung ließe sich ausschließen (§ 658 Abs. 2 Halbsatz 2 BGB). Die mehrfache Herbeiführung des Erfolgs (§ 659 Abs. 1 BGB) unter Abweichung vom Prioritätsgrundsatz (§ 659 Abs. 2 BGB) müsste zugelassen werden.[49] Die von § 657 BGB geforderte Herbeiführung eines Erfolgs könnte in der Einreichung eines Token z.B. beim Emittenten in einer bestimmten Form bestehen. In der Folge würde der Token-Inhaber bei Herbeiführung des Erfolgs – etwa in Gestalt einer Einreichung seines Token – einen Anspruch auf die ausgelobte Belohnung erlangen. Der Anspruch entsteht erst mit Eintritt aller Auslobungsbedingungen.[50]

Die Belohnung kann privatautonom frei innerhalb der allgemeinen Grenzen (§§ 134, 138 BGB) ausgestaltet werden.[51] Jeder Vorteil materieller oder immaterielle Art taugt als Belohnung.[52] Insofern können namentlich jegliche Leistungen, die mit einem Utility Token verbunden werden, zum Gegenstand einer Belohnung gemacht werden. Natürlich kann die Belohnung auch in der Übereignung einer Sache oder der Übertragung eines Rechts bestehen. Grenzen setzen jedoch die Formvorschriften für schuldrechtliche[53] Verpflichtungsgeschäfte über Immobilien (§ 311b Abs. 1 BGB, § 4 Abs. 3 WEG) und GmbH-Geschäftsanteile (§ 15 Abs. 4 GmbHG), die auch bei der Auslobungserklärung einzuhalten sind.[54] Daher kommen diese Vermögenswerte nicht als Objekte einer schuldrechtlichen Tokenisierung mittels Auslobung in Betracht.

Bei einer Unwiderruflichkeit der Auslobung erlangt der Token-Inhaber tatsächlich eine gesicherte Rechtsposition im Hinblick auf die Erlangung der Belohnung. Allerdings besteht auch diese nur in einem schuldrechtlichen Anspruch, der dinglich nicht abgesichert ist. Das Bild einer „Anwartschaft“[55] erscheint daher zumindest terminologisch unscharf, lässt sich aber jedenfalls nicht mit einem sachenrechtlichen Anwartschaftsrecht vergleichen. Der Berechtigte trägt nicht nur die Leistungsgefahr (§ 275 BGB), sondern auch das Insolvenzrisiko des Auslobenden. Da der Anspruch auf die Belohnung erst mit Erfüllung der Auslobungsbedingungen entsteht, wird der Token-Inhaber nicht Insolvenzgläubiger (§ 38 InsO), wenn er die erforderliche Handlung nicht vor Eröffnung des Insolvenzverfahrens (§ 27 Abs. 1

[49] Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 24 f.
[50] Schäfer, (Fn. 48), § 657, Rn. 36.
[51] Andreas Bergmann, «§ 657», in *Staudingers Kommentar zum Bürgerlichen Gesetzbuch: §§ 655a-656; 657-661a*, hrsg. Sebastian Herrler (Berlin: Sellier - de Gruyter, 2020), § 657 Rn. 59.
[52] OLG Brandenburg 27.01.2012 – 6 W 122/11, *ZfWG*, (2012): 144, 146.
[53] Die Formvorschriften für die dingliche Einigung (§§ 873, 925 BGB, § 15 Abs. 3 GmbHG) sind hingegen auf die Auslobungserklärung nicht anwendbar; a.A. wohl Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 31.
[54] Bergmann, (Fn. 51), § 657 Rn. 56; Schäfer, (Fn. 48), § 657, Rn. 28; Klaus Berger, «§ 657», in *Erman BGB*, hrsg. Harm Westermann, Barbara Grunewald und Georg Maier-Reimer, 16. Aufl. (Köln: Verlag Dr. Otto Schmidt, 2022), § 657 Rn. 6
[55] Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 27.

InsO) vornimmt. Dieses Insolvenzrisiko lässt sich durch vorsorgende Maßnahmen wirtschaftlich reduzieren,[56] aber nicht vermeiden. Daher stellt auch das Auslobungsmodell nur eine Hilfskonstruktion dar, die aber durchaus vor allem für Utility Token eine gewisse Rechtssicherheit verspricht.

b. Dinglich-absolute Ausgestaltung

aa. Elektronische Wertpapiere

Seit dem Inkrafttreten des eWpG lässt die deutsche Rechtsordnung erstmals auch eine dingliche Tokenisierung zu. Beschränkt ist sie allerdings auf Inhaberschuldverschreibungen (§ 1 eWpG) und Fondsanteile (§ 95 Abs. 1 Satz 1 KABG).[57] Neu geschaffen wurde die Möglichkeit, ein Wertpapier als elektronisches Wertpapier auszugeben (§ 2 Abs. 1 eWpG). Durch die Äquivalenzanordnung in § 2 Abs. 2 eWpG wird eine Funktionsgleichheit mit klassisch-körperlichen Wertpapieren erreicht.[58] Damit erfüllen auch elektronische Wertpapiere die Wertpapierfunktionen der Mobilisierung, Repräsentation und Liberation.[59] Subsidiär kann auf § 793 Abs. 1 BGB zurückgegriffen werden.[60]

Mit der Übereignung des elektronischen Wertpapiers geht auch das darin verbriefte Recht über: Das Recht aus dem Papier folgt dem Recht am Papier. Für elektronische Wertpapiere in Einzeleintragung formuliert § 25 Abs. 2 eWpG diese Regel nochmals gesondert.[61] Angesichts des beide Formen des elektronischen Wertpapiers umfassenden Verweises von § 2 Abs. 2 eWpG auf § 793 Abs. 1 Satz 1 BGB kommt der Regelung aber nur deklaratorische Wirkung zu.[62]

[56] Kaulartz, Hirzle und Holl, (Fn. 35), 324 Rn. 36.

[57] Zum sachlichen Anwendungsbereich Matthias Lehmann, «§3 Wertpapierarten», in *Elektronische Wertpapiere*, hrsg. Sebastian Omlor, Florian Möslein und Stefan Grundmann (Tübingen: Mohr Siebeck 2021), 59, 60 ff.; Christian Conreder, «§ 1», in *eWpG Kommentar*, hrsg. Christian Conreder und Johannes Meier (Berlin: Erich Schmidt Verlag, 2022), Rn. 8 ff.

[58] David Bartlitz, «§ 1», in *eWpG Kommentar*, hrsg. Christian Conreder und Johannes Meier (Berlin: Erich Schmidt Verlag, 2022), Rn. 31.

[59] Casper, (Fn. 12), Rn. 59-66.

[60] Bartlitz, (Fn. 58), § 1 Rn. 33.

[61] Johannes Meier, «§ 25», in *eWpG Kommentar*, hrsg. Christian Conreder und Johannes Meier (Berlin: Erich Schmidt Verlag, 2022), Rn. 20.

[62] Karl Döding und Kilian Wentz, „Der Referentenentwurf zur Einführung von elektronischen Wertpapieren und Kryptowertpapieren," *WM,* (2020): 2312, 2316; Thomas Preuße, Karsten Wöckener und Daniel Gillenkirch, „Der Gesetzesentwurf zur Einführung elektronischer Wertpapiere," *BKR,* (2020): 551, 554; Omlor, (Fn. 15), 137, 147.

bb. Wertrechte auf Blockchain-Basis

Das eWpG-Modell basiert noch auf einer dogmatischen Anbindung an das sachenrechtliche Wertpapierkonzept.[63] Die elektronischen Wertpapiere werden zum einen durch die Sachfiktion des § 2 Abs. 3 eWpG dem Publizitätsmodell des BGB-Sachenrechts unterworfen. Zum anderen aber stellt das eWpG sachnähere Sonderregeln für die Übertragung und den Verkehrsschutz von elektronischen Wertpapieren in Einzeleintragung auf (§§ 24-27 eWpG), die sich nur in Teilen und modifiziert an einem sachenrechtlichen Vorbild orientieren. Materiell handelt es sich daher bei elektronischen Wertpapieren um eine elektronische Sache sui generis, auf welche das BGB-Sachenrecht nicht pauschal übertragen werden kann.[64]

Das eWpG bildet daher einen wichtigen, aber nur ersten Schritt zur Schaffung eines tauglichen und umfassenden Rechtsrahmens für eine dingliche Tokenisierung. Zum einen fehlt weiterhin ein kohärentes und allgemeines Privatrecht der Token.[65] Zum anderen muss sich ein dematerialisiertes Wertpapierrecht vom Sachenrecht emanzipieren.[66] Das Sachenrecht bedarf einer Rematerialisierung,[67] während das Recht der Token und der Tokenisierung eine Dematerialisierung erfordert. Im Bereich des Aktien- und Depotrechts folgt daraus, dass sich Deutschland am Beispiel der Schweiz orientieren sollte, die bereits 2010 mit den Bucheffekten zu einem System der Wertrechte übergegangen ist und über das DLT-Gesetz[68] eine Öffnung für ein Wertrechteregister auf Blockchain-Basis geschaffen hat. Erforderlich hierfür ist eine grundlegende Reform des Aktien- und Depotrechts, keine schlichte Erweiterung des eWpG.[69]

D. Ausblick

Mit der Einführung von elektronischen Wertpapieren im Sommer 2021 hat der deutsche Gesetzgeber erstmals eine dingliche Tokenisierung zugelassen. „Wertpapiere ohne Papier" wurden erschaffen. Solche Wertpapiere im funktionalen Sinn

---

[63] Zutreffende rechtspolitische Kritik bei Lahusen, (Fn. 16), 161 Rn. 25-32.

[64] Omlor, (Fn. 15), 138, 141 f.; a.A. Casper, (Fn. 12), Rn 40.

[65] Eingehend dazu Sebastian Omlor, Hans Wilke und Tim Blöcher, Zukunftsfinanzierungsgesetz, *MMR*, (2022): 1044 ff.; Omlor, (Fn. 5), Kap. 6 Rn. 76 ff.; Möslein/Omlor/Burbach, Grundfragen eines Blockchain-Kapitalgesellschaftsrechts, 2151 f.; Omlor und Möslein, (Fn. 4), § 34 Rn. 33 ff.

[66] Stellvertretend zur Debatte Casper, (Fn. 12), Rn. 14 ff.; Lahusen, (Fn. 16), 161 Rn. 25 ff.; Matthias Casper und Ludwig Richter, „Die elektronische Schuldverschreibung – eine Sache?," *ZBB*, (2022): 81 ff.

[67] Dazu bereits Omlor, (Fn. 14), 236 ff.

[68] Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, 25.09.2020, abgerufen am 7. Januar 2023, https://www.fedlex.admin.ch/eli/oc/2021/33/de; dazu im Überblick Rolf Weber, „Neue Blockchain-Gesetzgebung in der Schweiz," *RDi*, (2021): 186 ff.; Urs Bertschinger, «§ 37 FinTech-Regulierung in der Schweiz», in FinTech-Handbuch, hrsg. Sebastian Omlor und Florian Möslein, 2. Aufl. (München: C.H. Beck, 2021), Rn. 3.

[69] Omlor, Wilke und Blöcher, (Fn. 65), 1044, 1046 f.

bilden einen zentralen *use case* für die Blockchain-Technologie, die damit einen echten Mehrwert gegenüber dem klassisch-körperlichen Wertpapier liefert. Bereits absehbar ist der nächste Schritt des Gesetzgebers, auch Aktien als elektronische Wertpapiere zuzulassen. Damit würde erstmals die Mitgliedschaft in einer Gesellschaft dinglich tokenisiert. Zugleich prüft das Bundesministerium der Justiz derzeit, ob ein Privatrecht der Token im BGB geregelt werden sollte, um bestehende Rechtsunsicherheiten namentlich bei der Übertragung von Token abzubauen. Spätestens damit wäre die Blockchain-Technologie vollends in der deutschen (Privat-)Rechtsordnung angekommen.

Blockchain and Finance in Japanese Law

Yusuke Tachibana

A. Overviews

This section explains the development of Japanese legal policy (e.g., Payment Services Act) for legal relationships of cryptographic assets, or crypto assets. There is no law in Japan that comprehensively defines the legal relationship of crypto assets. Broadly speaking, four laws govern the legal relationship of crypto assets. First, the "the Civil Code"[1] establishes the legal relationships regarding property rights and claims on crypto assets. For example, as discussed below, it is interpreted that crypto assets are not "property" that can be owned, but only claims against crypto asset exchange operators, which is based on the interpretation of the Civil Code. However, the Civil Code only provides for general principles and does not have provisions specific to crypto assets.

Second, certain laws supplement the legal relationship under the Civil Code and relates to user (consumer) protection. In other words, while legal relationships under the Civil Code assume equal actors, crypto assets are speculative as financial instruments, and there is an information gap between crypto asset exchange opera-

[1] Act No. 89 of April 27, 1896, english translation is available in Japanese Law Translation, "Civil Code (Part I, Part II and Part III), Act No. 89 of April 27, 1896," accessed March 28, 2023, https://www.japaneselawtranslation.go.jp/ja/laws/view/3494.

DOI: https://doi.org/10.17875/gup2023-2501

tors and users in the exchange of crypto assets. One of them is "the Financial Instruments and Exchange Act (FIEA)"[2] , which was amended in 2019[3] to add crypto assets to the list of regulated financial instruments and to introduce regulations for operators offering crypto assets as financial instruments. As a result, businesses are obliged to register as financial instruments business operators, etc., and fraudulent activities using crypto assets are prohibited. In fact, although this is a civil case, there was a court case that approved a claim for damages on the grounds that there was a breach of duty to explain when soliciting the purchase of crypto assets.[4] Lawsuits may also be filed by consumer groups.[5]

The other is "the Payment Services Act (PSA)."[6] Since the 2016 amendment,[7] the PSA defines crypto assets and imposes administrative regulations such as registration on crypto asset exchange operators. In addition, in response to cyber-attacks against crypto asset exchange operators, an amendment was made in 2019 to strengthen the security obligations of crypto asset exchange operators.[8]

---

[2] Act No. 25 of 1948, english translation is available at Japanese Law Translation, "Financial Instruments and Exchange Act (Tentative translation), Act No. 25 of April 13, 1948," accessed March 28, 2023, https://www. japaneselawtranslation.go.jp/en/laws/view/3986.

[3] See generally 守屋貴之ほか（編著）＝小森卓郎ほか（監修）『逐条解説2019年資金決済法等改正』（商事法務、2020年） [Takayuki Moriya, et al., supervised by Takuro Komori, et al., *Article-by-Article Commentary: 2019 Amendments to the Payment Services Act, etc.* (Tokyo: Shojihomu, 2020)].

[4] 東京地判令和3.5.27令和1年（ワ）第30715号 [Tokyo District Court, May 27, 2021].

[5] *See* 東京高判令和3.12.22判時2526号14頁 [Tokyo High Court, December 22, 2021]; 東京地判令和3.5.14判時2526号20頁 [Tokyo District Court, May 14, 2021].

[6] Act No. 59 of 2009, english translation is available in Japanese Law Translation, "Payment Services Act, Act No. 59 of June 24, 2009," accesed March 28, 2023, https://www.japaneselawtranslation.go.jp/ja/laws/view/3965. *See generally* 高橋康文（編著）＝堀天子＝森毅『新・逐条解説資金決済法』（きんざい、2021年） [Yasufumi Takahashi, et al., *New Article-by-Article Commentary: Payment Services Act* (Tokyo: Kinzai, 2021); 堀天子『実務解説資金決済法』（第5版、商事法務、2022年） [Takane Hori, *Practical Explanation of Payment Services Act* 5th ed (Tokyo: Shojihomu, 2022).

[7] See generally 湯山壮一郎ほか（編著）＝佐藤則夫（監修）『逐条解説2016年銀行法、資金決済法等改正』（商事法務、2017年） [Soichiro Yuyama, et al., supervised by Norio Sato, *Article-by-Article Commentary: 2016 Amendments to the Banking Act, the Payment Services Act and Others* (Tokyo: Shojihomu, 2017)].

[8] See generally Moriya et al. (n 3).

The third is certain laws on anti-money laundering.[9] One of the leading laws is the Act on Prevention of Transfer of Criminal Proceeds.[10] Since crypto assets can be used as consideration for illegal activities, the 2016 revised Act[11] imposes on crypto asset exchange operators the obligation to verify the identity of their customers and to report suspicious transactions to the Financial Services Agency (FSA), among other things.

The other is "the Foreign Exchange and Foreign Trade Act (Foreign Exchange Act)."[12] The Japanese government may target certain countries or individuals for economic sanctions, and crypto assets may be used to circumvent such sanctions. Therefore, in order to prevent the transfer of crypto assets to those subject to sanctions, the Foreign Exchange and Foreign Trade Act was revised in 2022[13] and administrative legal restrictions were imposed on crypto asset exchange operators, including the obligation to confirm whether the party to which crypto assets are transferred is subject to asset freezing measures (so-called "legality confirmation obligation").

Other often-implemented laws that crack down on money laundering include the "Act on Punishment of Organized Crimes and Control of Proceeds of Crime,"[14] which makes it a violation of the Act to purchase crypto assets stolen through unauthorized access.

---

[9] In addition, industry association guidelines are also important in practice. *See* 日本暗号資産取引業協会「暗号資産交換業に係るマネー・ローンダリング及びテロ資金供与対策に関する規則・ガイドライン」（2022年） [Japan Virtual and Crypto assets Exchange Association, "Rules and Guidelines on Anti-Money Laundering and Anti-Terrorist Financing Related to Crypto Asset Exchange Business", 2022], accessed March 28, 2023, https://jvcea.or.jp/about/rule/.

[10] Act No. 22 of 2007.

[11] See generally Yuyama et al., (n 7).

[12] Act No. 228 of 1949, english translation is available in Japanese Law Translation, "Foreign Exchange and Foreign Trade Act, Act No. 228 of December 1, 1949," accessed March 28, 2023, https://www.japaneselawtranslation.go.jp/en/laws/view/4412.

[13] Act No. 28 of 2022. *See* 財務省「「関税暫定措置法の一部を改正する法律案」及び「外国為替及び外国貿易法の一部を改正する法律案」について」（2022年） [Ministry of Finance, "Draft Laws Amending a Portion of the Act on Temporary Measures concerning Customs and a Portion of the Foreign Exchange and Foreign Trade Act", 2022], accessed March, 2023, https://www.mof.go.jp/about_mof/bills/208diet/20220404112528.html. *See generally* 中崎隆「令和４年外為法の改正と暗号資産交換取引」（2022年） [Takashi Nakasaki, "2022 Amendments to the Foreign Exchange Law and Crypto Asset Exchange Transactions", 2022], accessed March 28, 2023, https://nakasaki-law.com/fatf/.

[14] Act No. 136 of 1999, english translation is available in Japanese Law Translation, "Act on Punishment of Organized Crimes and Control of Proceeds of Crime (Tentative translation), Act No. 136 of August 18, 1999," accessed March 28, 2023, https://www.japaneselawtranslation.go.jp/ja/laws/view/3587.

Fourth, there are laws regarding blockchain-based property other than crypto assets. First, there is a law on digital securities.[15] Digital securities, also called "security tokens (STs)," are securities issued using blockchain technology. They are backed by property value[16] and are distinguished from crypto assets.[17] The aforementioned FIEA defines digital securities as "electronically recorded transferable rights" and regulates digital securities from the 2019 amendment[18]

Next, there is a law on stablecoins. The 2022 amendment to the PSA[19] positioned digital money-like stablecoins as a "electronic payment instrument" and imposed regulations to protect users by limiting the businesses handling such transactions to banks and funds transfer operators. The legal status of stablecoin has been unclear in the past. On the other hand, unlike crypto assets, stable coins are designed to have a stable value, but are similar to exchange transactions because they can be easily converted into cash. Therefore, they are now subject to the provisions of the PSA in the revision.[20]

Other issues include the issue of NFTs.[21] Regarding whether NFTs constitute crypto assets, the definition of which is discussed below, the FSA has adopted the view that, in principle, NFTs do not constitute crypto assets, although it says that it

[15] See generally 河合健＝高松志直＝田中貴一＝三宅章仁『暗号資産・デジタル証券法』（商事法務、2020年） [Ken Kawai, et al., *Laws on Crypto Assets and Digital Securities* (Tokyo: Shoji-homu, 2020)].

[16] FIEA, (n 2) § 2(3).

[17] PSA, (n 6) § 2 (5).

[18] Act No. 28 of 2019.

[19] Act No. 61 of 2022. See generally 西村あさひ法律事務所「電子移転可能型前払式支払手段に関する規制の整備：パブコメ案を踏まえて」金融ニューズレター2023年1月31日号 [Nishimura and Asahi, "Development of Regulations Concerning Electronic Transferable Prepaid Payment Instruments: Based on the Draft Public Comment, January 31, 2023,], accessed January 31. 2023, https://www.nishimura.com/ja/newsletters/finance-law_230131.html?__CAMVID=iIPe-fDHhFgDocH&_c_d=1&uns_flg=1&__ urlmid=8158217&__CAMSID=iKfGEMIcfgD-88&__CAMCID=zNIVerwxIZ-949&adtype=mail.

[20] Hori, (n 6 18-19.

[21] 全国銀行協会金融法務研究会「報告書：仮想通貨に関する私法上・監督法上の諸問題の検討」（2019年） [Financial Law Study Group of the Japanese Bankers Association, "Report: a Study of Various Private Law and Supervisory Law Issues Related to Virtual Currencies" (working paper, 2019), accessed December 8, 2022, https://www.zenginkyo.or.jp/abstract/affiliate/kinpo/2016/#c37900; Web3.0研究会「Web3.0 研究会報告書：Web3.0の健全な発展に向けて」（2022年） [Web 3.0 Study Group, " Web3.0 Research Group's Report: Toward Sound Development of Web3.0", (working paper, 2022)], accessed March 28, 2023, https://www.digital.go.jp/councils/web3#report.

depends on individual cases.[22] The office said that "NFTs are generally digital assets, and unless they are used as crypto assets or other financial regulatory subterfuge, the FSA does not consider them to be something in which the financial authorities should be involved."[23] As a result, NFTs are currently not regulated by existing legislation such as the law on crypto assets.

Of the above, this paper introduces the Japanese legal system regarding crypto assets, focusing on the PSA, the basic law regarding crypto assets.

B. What is Blockchain in the area of Finance in Japan?

I. What is Blockchain?

In Japan, blockchain is disciplined in the financial sector as "crypto assets" and "electronically recorded transferable rights" (so-called digital securities).

The definition of crypto assets is set forth by the PSA. The Aact aims "to the improvement of the safety, efficiency, and convenience of the payment and settlement system." The Act acknowledges the potential property value inherent in cryptographic assets, and their potential efficacy as a medium for payment and settlement. Nevertheless, it posits that, presently, cryptographic assets lack the identical attributes associated with traditional currencies. Based on such understanding, The Act provides for certain regulations on exchangers of crypto assets and legal currencies. To this end, the Act defines crypto assets as having "property value," being "used in relation to unspecified persons "and" purchased... and sold," and being "transferred by means of an electronic data processing system."

Payment Services Act § 2(5):

> *"The term 'crypto-assets' as used in this Act means any of the following; provided, however, that those indicating electronically recorded transferable rights prescribed in Article 2, paragraph (3) of the Financial Instruments and Exchange Act (Act No. 25 of 1948) are excluded:*

---

[22] 金融庁「事務ガイドライン（第三分冊：金融会社関係）：16 暗号資産交換業者関係」 [Financial Services Agency, "Guideline for Supervision of Crypto-Asset Exchange Service Providers"] at I-1-1①, accessed March 28, 2023, https://www.fsa.go.jp/common/law/guide/kaisya/index.html.

[23] 109 曽根康司「暗号資産交換所ビジネスの現状とモニタリングの方向性：規制とイノベーション促進の両立を通じて、業界全体の健全な発展を促す」金融財政事情73 巻18号18頁（2022年） [Koji Sone, "Current Status and Monitoring Direction of Crypto Asset Exchange Business: Promoting Healthy Development of the Industry as a Whole through Balancing Regulation and Innovation Promotion", 27(2), *The financial economist,* (2022): 18], accessed December 8, 2022, https://www.fsa.go.jp/frtc/kikou/2022/20220517_1.pdf.

(i)property value (limited to that which is recorded on an electronic device or any other object by electronic means, and excluding the Japanese currency, foreign currencies, and currency-denominated assets; the same applies in the following item) which can be used in relation to unspecified persons for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services and can also be purchased from and sold to unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system; and

(ii)property value which can be mutually exchanged with what is set forth in the preceding item with unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system."[24]

Specifically, Bitcoin, Ethereum, and NEM are considered crypto assets,[25] while electronic money, in-game currency, and business points are not considered crypto assets.[26] In addition, the following three are excluded from crypto assets: "electronically recorded transferable rights", "legal currency", and "currency- denominated assets".[27] Currency-denominated assets include government bonds, municipal bonds, deposit currencies, and bonds issued by corporations.[28]

Note that in 2016, when the provisions on crypto assets were added to the PSA, the blockchain was named "virtual currency". However, since then, the term "crypto asset" has been increasingly used internationally, and the term "currency" can be misinterpreted as a legal currency. Therefore, the name was changed to "crypto asset" in the 2019 amendment to the PSA.[29] However, the definition remains unchanged.

[24] Japanese Law Translation, (n 66) (emphasits added).
[25] See **金融庁「暗号資産交換業者登録一覧」**（2023**年**3**月**9**日**） [FSA, "List of Registered Crypto Asset Exchangers", March 9, 2023], accessed March 28, 2023, https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf; **日本暗号資産取引業協会「取扱暗号資産及び暗号資産概要説明書」**（2023**年**4**月**6**日**） [Japan Virtual and Crypto assets Exchange Association, "Crypto Assets Handled and Summary Description, April 6, 2023], accessed April 10, 2023, https://jvcea.or.jp/about/document/#gaiyo.
[26] Takahashi et al., (n 6 49; Hori, (n 6 339-40.
[27] PSA, (n 6) § 2 (5).
[28] PSA, (n 6) § 2(6).
[29] Moriya et al., (n 3 12-13.

II. Blockchain is Property?[30]

An issue that has frequently arisen in Japan is the determination of the legal status of crypto assets. This is particularly contentious in bankruptcy cases. Under Japanese law, as a creditor may recover his property from a debtor,[31] this means that he is entitled to superior payment in relation to other creditors. If crypto assets are subject to ownership rights, for example, if a crypto asset exchange provider goes bankrupt, the user can demand delivery of the crypto assets in priority to others.

In this regard, the court ruled that no ownership rights were established in bitcoin, but only a claim for the transfer of crypto assets to the crypto asset exchanger (Tokyo District Court [Mt. Gox I][32]). In this case, a user sought to recover bitcoins from the crypto asset exchanger in question following the bankruptcy of Mt. Gox, Inc. in 2014, which was a bitcoin exchanger. The court held that ownership is the right to freely use, profit from, and dispose of one's property within legal limits,[33] and that the "property" that is the object of ownership is defined as a "tangible object" in Civil Code.[34] The court determined that bitcoin lacks the tangible attributes and exclusive controllability requisite for classification as an object of ownership, and that bitcoin was not an object of ownership Therefore, in the Mt. Cox bankruptcy proceeding, the customers were treated as having bankruptcy claims, as they only had a contractual claim to return the bitcoins they deposited with the exchange (*See* Tokyo District Court [Mt. Gox II];[35] Tokyo High Court [bitFlyer (Bitcoin) II][36]).

In response to these legal precedents, in 2019, the PSA was amended to rectify the precarious legal rights of users concerning crypto assets; the amended law does not define the judicial nature of crypto assets, but assumes that users have a claim against crypto asset exchangers for the transfer of crypto assets. On that basis, the

---

[30] See generally 原謙一「仮想通貨（暗号通貨）の法的性質決定及び法的処遇：ビットコインを中心として」横浜法学27巻2号79頁（2018年）[Hara Kenichi , "Determination of Legal Nature of Virtual Currency (Crypto Currency) and Legal Treatment: Focusing on Bitcoin,"27(2) Yokohama Law Review, (2018) 79], accessed October 13, 2023, https://ynu.repo.nii.ac.jp/?action=repository_action_common_download&item_id=9432&item_no=1&attribute_id=20&file_no=1.

[31] Bankruptcy Act § 62 (Act No. 75 of 2004). 2004), english translation is available in Japanese Law Translation, "Bankruptcy Act (Tentative translation), Act No. 75 of June 2, 2004," accessed March 28, 2023, https://www.japaneselawtranslation.go.jp/ja/ laws/view/2304.

[32] 東京地判平成27.8.5平成26年（ワ）第33320号 [Tokyo District Court, August 5, 2015] [Mt. Gox I].

[33] Civil Code, (n 1) § 206.

[34] Civil Code, (n 1) § 85.

[35] 東京地判平成30.1.31判時2387号108頁 [Tokyo District Court, January 31, 2018] [Mt. Gox II].

[36] 東京高判令2.12.10金判1615号40頁 [Tokyo High Court, December 10, 2020] [bitFlyer (Bitcoin) II]. The decision affirmed the lower court of 東京地判令和2.3.2金判1598号42頁 [Tokyo District Court, March 2, 2020] [bitFlyer (Bitcoin) II].

users of crypto asset exchangers shall have the right to receive payment in priority before other creditors.[37]

C. Payment Services Act

I. History

1. 2016 Amendment to the Payment Services Act

From here, the central law regarding crypto assets, the Payment Services Act, will be explained in detail. The PSA is not a law specific to crypto assets, but rather a law on funds settlement and exchange transactions, the purpose of which is to ensure the safety and other aspects of the funds settlement system and to protect users.[38] Since crypto assets are also similar to fund settlement, a chapter on crypto asset exchange business was added in the 2016 amendment and crypto asset exchangers were newly regulated.[39] The amended law has been in effect since April 1, 2017.

Payment Services Act § 1 (Purpose):

> *"The purpose of this Act is to enforce registration and provide other necessary measures with respect to the issuance of prepaid payment instruments, or exchange transactions carried out by persons other than deposit-taking institutions, exchange of crypto-assets, etc., and the clearing of exchange transactions between deposit-taking institutions, in order to ensure the appropriate provision of payment services, and protection of the users, etc. thereof, and to promote the provision of those services, thereby contributing to the improvement of the safety, efficiency, and convenience of the payment and settlement system."*[40]

The PSA delegates detailed regulations to a Cabinet Office Order, and the "Cabinet Office Order on Crypto-Asset Exchange Service Providers (Crypto-Asset Office Order)"[41] has been established. The Financial Services Agency has established guidelines for the interpretation of the PSA (hereinafter referred to as "FSA Guidelines")[42]. The said guidelines are not binding on the courts, but serve as a practical

---

[37] PSA, (n 6) § 63 bis 19 bis 2 (1). See Moriya et al., (n 3 57.

[38] PSA, (n 6) § 1.

[39] Takahashi et al., (n 6 33.

[40] Japanese Law Translation, (n 6.

[41] Cabinet Office Order No. 7 of 2009, english Translation is available in Japanese Law Translation, "Cabinet Office Order on Crypto-Asset Exchange Service Providers (Tentative translation), Cabinet Office Order No. 7 of 2017," accessed March 28, 2023, https://www.japaneselawtranslation.go.jp/ja/laws/view/4107.

[42] FSA, (n 22). For a contrast between those guidelines and the provisions of PSA, see Takahashi et al., (n 6 Appendix.

guide. In practice, the Japan Virtual and Crypto assets Exchange Association (JVCEA) documents[43] and guidelines, etc.[44] are also referred to.

2. Coincheck case

The PSA underwent a major revision in 2019, as discussed below, and the incident that led to the revision was the 2018 Coincheck incident. In this incident, crypto asset exchanger Coincheck, which was previously referred to as a virtual currency exchanger, was hacked in January 2018, resulting in the outflow of crypto assets NEM worth about 58 billion yen, equivalent to about 400 million dollars at the time. This was widely reported around the world.[45]

The incident was discovered on 26 January 2018, when NEM leaked from an account managed by Coincheck and was deposited into about 150 accounts on the web. Subsequently, a dark site appeared on the dark web to exchange NEM for other crypto assets, and a number of people exchanged NEM knowing it was fraudulent, and it is believed that almost all of them were exchanged in about a month and a half.[46]

The cause of the outflow was the theft by hackers of the encryption keys for the accounts where customers' crypto assets were stored. The hackers allegedly infected the computers of Coincheck employees with malware, which is a malicious program, and hacked into the company's network servers. The person who caused the leak is not known.[47]

In the case in question, a civil lawsuit was filed by the user against the exchange operator, as described below. In addition, the purchaser of the leaked crypto assets was criminally punished because the act of purchasing the leaked crypto assets is an

[43] **日本暗号資産取引業協会「各種資料」** [Japan Virtual and Crypto assets Exchange Association, "Various Materials"], accessed March 28, 2023, https://jvcea.or.jp/about/document/#gaiyo.

[44] **日本暗号資産取引業協会「定款・諸規則」** [Japan Virtual and Crypto assets Exchange Association, "Articles of Incorporation and Regulations"], accessed March 28, 2023, https://jvcea.or.jp/about/rule/.

[45] See Bloomberg, "Coincheck Says It Lost Crypto Coins Valued at About $400 Million", January 26, 2018, accessed July 22, 2022, https://www.bloomberg.com/news/articles/2018-01-26/cryptocurrencies-drop-after-japanese-exchange-halts-withdrawals#xj4y7vzkg.

[46] See **朝日新聞デジタル「NEM流出、不正交換容疑で31人を立件：主犯者は不明」**(2021**年1月22日**) [Asahi Shimbun Digital, "NEM leak, 31 people charged with illicit exchange: main culprits unknown", January 22, 2021], accessed July 22, 2022, https://www.asahi.com/articles/ASP1Q3TWBP1QUTIL00B.html.

[47] Asahi Shimbun Digital, (n 46).

act of complicity in money laundering and constitutes a violation of the Act on Punishment of Organized Crimes and Control of Proceeds of Crime.[48, 49]

3. 2019 Amendment

In response to the Coincheck incident, the PSA was significantly amended in 2019. Specifically, regulations for exchange operators were tightened, information security obligations were strengthened, as discussed below, and user protection measures were introduced, such as obligation to distinguish between properties.

I. Explanation of the Money-Lending Settlement Act

1. Big picture

The PSA (1) defines crypto assets, (2) requires crypto asset exchange operators to be registered, and (3) imposes obligations on exchange operators to protect users. Since the definition of crypto assets has been discussed above, this article will discuss the registration system, and the obligation to protect users in detail below.

The competent authority for the PSA is the Financial Services Agency, which has the authority to enforce the Act and draft its amendments.[50] However, part of the FSA's authority is delegated to the Director-Generals of Local Finance Bureaus or Local Finance Branch Bureaus of the Ministry of Finance.[51]

2. Registration Obligation

a. What is a Crypto Asset Exchanger?

In order to operate a crypto asset exchange business, it is necessary to be registered with the director of the competent finance bureau.[52]

The crypto asset exchange business, which is referred to in legal terms as "crypto-asset exchange service," means the buying, selling, and brokering of crypto assets, as well as the management of crypto assets.[53] For example, the act of managing the private key required for the transfer of crypto assets on behalf of the user, or the act of receiving and managing the transfer of crypto assets from the user's crypto asset address to the business's own address fall under the crypto asset exchange business.[54]

Payment Services Act § 2(7):

---

[48] Act on Punishment of Organized Crimes and Control of Proceeds of Crime, (n 14) § 11.

[49] 東京地判令和3.7.8令和2年（特わ）第884号ほか [Tokyo District Court, July 8, 2021] [Coincheck (criminal case)].

[50] PSA, (n 6) § 104 (1).

[51] PSA, (n 6) § 104(2).

[52] PSA, (n 6) § 63 bis 2.

[53] PSA, (n 6) § 2(7).

[54] Hori, (n 6 340-42.

> *"The term 'crypto-asset exchange services' as used in this Act means carrying out any of the following acts in the course of trade, the term "exchange of crypto-assets, etc." as used in this Act means the acts set forth in items (i) and (ii), and the term "management of crypto-assets" as used in this Act means the act set forth in item (iv):*
> *(i)purchase and sale of a crypto-asset or exchange with another crypto-asset;*
> *(ii)intermediary, brokerage or agency services for the act set forth in the preceding item;*
> *(iii)management of users' money, carried out by persons in connection with their acts set forth in the preceding two items; and*
> *(iv)management of crypto-assets on behalf of another person (excluding cases where the relevant management in the course of trade is governed by special provisions of other Acts)."*[55]

A person who wishes to obtain this registration must submit an application for registration, along with the required documents, to the director of the competent finance bureau,[56] as stipulated in the Crypto-Assets Office Order[57].[58] Such registered operators are referred to as "crypto-asset exchange service providers."[59]

b. Requirements for registration

If the applicant for registration lacks a system for the proper and reliable conduct of the crypto asset exchange business, the registration will be denied.[60] The following three points are important.

First, the applicant for registration must have the financial substrate to carry out the business.[61] Specifically, the amount of capital must be at least 10 million yen, equivalent to about 67 thousand dollars and the amount of net assets must not be negative.[62]

Second, the applicant for registration must have a system to carry out the work.[63]

Third, it is necessary to establish a system that complies with the user protection requirements described below, and anti-money laundering measures.[64]

c. Registration of foreign companies

Additional requirements are necessary for a foreign company to become a crypto-asset exchange operator under the PSA.

---

[55] Japanese Law Translation, (n 6.
[56] PSA, (n 6) § 63 bis 3.
[57] Cabinet Office Order on Crypto-Asset Exchange Service Providers, (n 41) § 4-6.
[58] PSA, (n 6) § 63 bis 5 (1)(i).
[59] PSA, (n 6) § 2(8).
[60] PSA, (n 6) § 63 bis 5 (1)(iii) -(xi).
[61] PSA, (n 6) § 63 bis 5 (1)(iii).
[62] Cabinet Office Order on Crypto-Asset Exchange Service Providers, (n 41) § 9.
[63] PSA, (n 6) § 63 bis 5 (1)(iv).
[64] PSA, (n 6) § 63 bis 5 (1)(v).

First, the company must be registered in a foreign country equivalent to registration under the PSA.[65] Second, in order for a foreign company to register as a crypto asset exchanger in Japan, it must have a business office[66] and a representative in Japan.[67]

Upon registration as a crypto-asset exchange service provider, a foreign company is treated as a "crypto-asset exchange service provider" under the PSA,[68] just like any other registered domestic crypto-asset exchange service provider. A foreign company that has obtained such registration is called a "foreign crypto-asset exchange service provider."[69] The crypto-asset exchange business that may be operated and the requirements to be complied with as described below are the same for foreign crypto-asset exchange service providers and domestic operators.

3. Information Security Obligations

a. Obligations

Crypto assets are electronic information on the Internet; hence, the crypto asset exchange business is premised on computer systems and the Internet. Therefore, the crypto asset exchange business entails information security risks, i.e., the risk of compromising the confidentiality, integrity, and availability of information in its operations.[70] FSA Guidelines refer to such risks as "system risk."[71]

> *"Information technology (IT) system risk refers to the risk of loss incurred by a user or a Crypto-Asset Exchange Service Provider due to a computer system failure, malfunction, or other inadequacies, and/or the risk that a user or a Crypto-Asset Exchange Service Provide incurs a loss due to the unauthorized use of a computer."*[72]

Therefore, the PSA imposes an obligation on crypto asset exchange operators to ensure information security.[73]

Payment Services Act § 63 bis 8 (Information Security Management):

> *"A crypto-asset exchange service provider must, pursuant to the provisions of Cabinet Office Order, take necessary measures for preventing leakage, loss, or damage to information*

[65] PSA, (n 6) § 2(9).
[66] PSA, (n 6) § 63 bis 5 (1)(i).
[67] PSA, (n 6) § 63 bis 5 (1)(ii).
[68] PSA, (n 6) § 63 bis 2.
[69] PSA, (n 6) § 2(9).
[70] FSA, (n 2242 II-2-3-1-1; Hori, (n 6 366.
[71] FSA, (n 4222) II-2-3-1-1.
[72] FSA, (n 22).
[73] PSA, (n 6) § 63 bis 8.

pertaining to the crypto-asset exchange services and other measures for the security management of relevant information."[74]

b. Information Security Duties

The information to be protected here is said to include all information pertaining to the crypto asset exchange business, such as money, crypto asset information, and transaction information.[75] Such information is also referred to as "information assets" in information security terms, meaning both information and the information systems that handle it.[76]

The PSA does not place specific provisions on the details of the required information security. In this regard, the FSA Guidelines concretizes the content of information security. The duties include:

(i) System Development: Information security is a management matter, and management is obligated[77].[78] On top of that;
(ii) Risk Assessment:[79]
(iii) Information Security Control Measures: Management should ensure that information security managers maintain the confidentiality, integrity, and availability of information,[80] and
(iv) Incident Reporting: If an information security incident occurs, the company is required to report it to the Local Finance Bureaus of Ministry of Finance.[81]

However, the FSA Guidelines also do not set forth specific control measures. Therefore, whether information security is sufficient or not depends on what information security was required by contract and business practice at the time the information security incident occurred.[82] This is ultimately a matter for the courts to decide. In court cases, the following have been challenged.

Regarding whether or not there was an obligation to adopt a cold wallet, court decisions have dismissed users' claims for damages against crypto asset exchange operators on the grounds that they were not obligated to adopt a cold wallet at the time of the incident (Tokyo District Court [bitFlyer (Bitcoin) I];[83] Tokyo District

[74] Japanese Law Translation, (n 6.
[75] Hori, (n 6 366.
[76] FSA, (n 4222) II-2-3-1-2 (4).
[77] FSA, (n 22) II-2-3-1-1.
[78] FSA, (n 22) II-2-3-1-2 (1)-(2).
[79] FSA, (n 22) II-2-3-1-2 (3).
[80] FSA, (n 22) II-2-3-1-2 (4).
[81] FSA, (n 22) II-2-3-1-3.
[82] See Hori, (n 6 366.
[83] **東京地判平成**31.1.25**判時**2436**号**68**頁** [Tokyo District Court, January 25, 2019] [bitFlyer (Bitcoin) I].

Court [bitFlyer (Bitcoin) II];[84] Tokyo District Court [Coincheck (NEM)];[85] Tokyo District Court [Coincheck[86]). In addition, as discussed below, cold wallets were made mandatory by the 2019 amendment to the PSA[87] as stipulated in the Crypto-Assets Office Order[88]

The authentication method used to log in users is also disputed. In the Tokyo District Court case [bitFlyer],[89] there was an unauthorized login to a user's account, and the issue was whether the crypto asset exchange provider was negligent in setting the authentication method. The crypto asset exchange operator had adopted a method in which both a login password and a one-time password were entered, so-called two-step authentication, but the former password did not need to be changed from the initial password automatically set by the operator, and the latter password could not only be issued via SMS or authentication app, but could also be issued via email. The court denied negligence because it recommended changing the former password and issuing the latter password via SMS or authentication app. The Court of Appeals also upheld this decision (Tokyo High Court [bitFlyer (Bitcoin) II[90]).

c. Sanctions

In the event of a breach of information security obligations, the business operator may be liable for damages under contract[91] and tort law,[92] and management may be liable for damages under the Companies Act[93].[94]

It is also subject to administrative sanctions by the authorities, as discussed below.

[84] bitFlyer (Bitcoin) II, (n 36.

[85] **東京地判令和**2.10.30**金判**1609**号**26**頁** [Tokyo District Court, October 30, 2020] [Coincheck (NEM)].

[86] **東京地判令和**2.12.21**平成**31**年（ワ）第**8789**号** [Tokyo District Court, December 21, 2020] [Coincheck (Ethereum)].

[87] PSA, (n 6) § 63 bis 11(2).

[88] Cabinet Office Order on Crypto-Asset Exchange Service Providers, (n 41) § 27(3).

[89] bitFlyer (Bitcoin) II, (n 36.

[90] bitFlyer (Bitcoin) II, (n 36.

[91] Civil Code, (n 1) § 415.

[92] Civil Code, (n 1) § 709.

[93] Act No. 86 of 2005, english translation is available in Japanese Law Translation, "Companies Act (Part I, Part II, Part III and Part IV), Act No. 86 of July 26, 2005," accessed March 28, 2023, https://www.japaneselawtranslation.go.jp/en/laws/view/3206.

[94] Companies Act, (n 93) § 423.

II. Contractual relationship between operators and users

The contract, such as terms and conditions, determine what rights the user has against the crypto asset exchange operator.[95] For example, when a crypto asset exchange operator provides services such as buying and selling crypto assets, it may provide users with a wallet that manages the crypto assets, or it may open an exchange account for the users and the crypto assets are deposited in a wallet managed by the operator. Many crypto asset exchanges usually receive crypto assets sent to a wallet managed by the business, display the number of amounts in the account, and conduct transactions as an exchange on said account. In this case, the user is said to have the right to request the crypto asset exchanger to send the crypto assets in the wallet to an address specified by the user.[96]

In this regard, the Tokyo District Court [Coincheck (Ethereum)][97] addressed the issue of the obligation to transmit crypto assets. The case concerned the aforementioned Coincheck incident, in which the crypto asset exchange operator suspended all crypto asset transmission services following the theft of crypto assets. In response, the plaintiff, a user, instructed the operator to send Ethereum held in his account to an exchange outside of Japan, hereinafter referred to as the transmission instruction, but the operator failed to do so. Subsequently, the suspension was lifted and the service for the transmission of crypto assets resumed, and the plaintiff again gave the transmission instruction and sold the Ethereum. However, the value of Ethereum had fallen compared to the time of the transmission instruction. Therefore, the plaintiff claimed damages against the operator for this decrease in value. The court held that although the operator was contractually obligated to immediately respond to the transmission of the crypto assets, if it continued the transmission service at the time of the transmission instruction in question, there was a possibility of further theft and no default was found (*See* Tokyo District Court [Coincheck (Ripple)][98]).

However, if left to the contract of the parties, the protection of users would be lacking. Therefore, the PSA imposes user protection obligations on crypto asset exchange operators. In particular, following the Coincheck incident, the requirements for user protection were strengthened in the 2019 amendment to the PSA. That is, crypto asset exchange operators have had an obligation to manage users' money and crypto assets separately from their own crypto assets from the past, so-called segregated management obligation, but to further protect users, crypto asset exchange operators are obligated to trust users' money to a trust company, etc.,[99]

---

[95] Hori, (n 6 357-58.

[96] Hori, (n 6) 345-46.

[97] Coincheck (Ethereum), (n 86.

[98] **東京地判平成**31.2.4**金法**2128**号**88**頁** [Tokyo District Court, February 4, 2019] [Coincheck (Ripple)].

[99] PSA, (n 6) § 63 bis 11(1). See Moriya, (n 3) 52-53; Takahashi, (n 6) 307-08.

and users' crypto assets by a method that is less likely to fail to protect users, e.g., cold wallet.[100]

With regard to the governing law of the contract, even if the terms of use of the service provider stipulate that a law other than Japanese law shall apply, if the consumer's place of residence is in Japan and the consumer requests the application of Japanese law, the mandatory Japanese consumer law shall apply under the Act on General Rules for Application of Laws[101].[102]

III. Execution

In the event of a violation of the above obligations of a business operator, the director of the competent finance bureau may issue a business improvement order to the business operator,[103] and in the event that such violation falls under the aforementioned grounds for denial of registration or in violation of the business improvement order, a suspension order and cancellation of registration may be issued.[104]

Serious violations of laws and regulations, such as conducting crypto asset exchange business without registration,[105] violating segregated management obligation[106] or violating a business suspension order,[107] are subject to criminal penalties. In the case of a violation of the segregated management obligation or a business suspension order, the individual who has committed the act in question, such as the manager, will be punished, as well as the legal entity.[108]

It should be noted that in recent times, the FSA is reportedly focusing on monitoring cyber security measures and countering consumer damage caused by unregistered businesses.[109]

The above are sanctions under administrative and criminal law, but in addition to these, the exchange operator can be held liable to the user for the performance of the contract and for damages.[110]

---

[100] PSA, (n. 6) § 63 bis 11(2). See Moriya, (n 3) 53-54; Takahashi, (n 6) 308-09.
[101] Act No. 78 of 2006, english translation is available in Japanese Law Translation, "Act on General Rules for Application of Laws, Act No. 78 of June 21, 2006," accessed March 28, 2023, https://www.japaneselawtranslation. go.jp/en/laws/view/3783/tb.
[102] Act on General Rules for Application of Laws, (n 101) § 11(3).
[103] PSA, (n 6) § 63 bis 16.
[104] PSA, (n 6) § 63 bis 17.
[105] PSA, (n 6) § 107(vi).
[106] PSA, (n 6) § 108(iii).
[107] PSA, (n 6) § 108(v).
[108] PSA, (n 6) §115(1)(i).
[109] Sone, (n 23).
[110] See generally 柳原悠輝「仮想通貨に関する強制執行：裁判例の考察と今後の展望」金融法務事情67巻19号13頁（2019年） [Yuki Yanagihara, "Compulsory Execution Concerning Virtual Currency: Consideration of Court Decisions and Future Prospects" 67 (19) *Banking law journal*, (2019): 13].

Solving the 'Platform Liability Quandary': continuity and innovation in the DSA

Teresa Rodríguez de las Heras Ballell

A. Introduction: Continuity and Innovation in the DSA to Solve the Platform Liability Quandary

The publication in the Official Journal of 27 October 2022 of *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)* marks an important turning point in Europe's regulatory strategy for the digital economy. With its adoption and publication, the DSA completes the regulatory tandem with which the EU is approaching the profound transformation of digital markets in recent decades - the DMA (*Digital Markets Act*) was published on 12 October[1] - and is part of a profusely growing and increasingly dense legislative and regulatory environment for the digital economy, which includes rules (or proposals) on artificial intelligence, cybersecurity, cloud computing, data and digital assets.

Since the Directive on Electronic Commerce,[2] which has been the centerpiece and backbone of the regulatory framework for digital services in the Union and the driver of their expansion and development over the last two decades, the digital

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Regulation*) [2022] OJ L 265/1.

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (*Directive on electronic commerce*), [2000] OJ L 178/1.

DOI: https://doi.org/10.17875/gup2023-2502

economy has been profoundly transformed, evolving into a platform economy and expanding dramatically beyond the cautious and discrete contours of the Directive on Electronic Commerce (hereinafter ECD).

The essential building block of the ECD and the fundamental reason for its valuable facilitating function for the digital economy was precisely the liability (exclusion/exemption) rules ('safe harbour') for intermediary service providers. Just over two decades of the Directive have put this cornerstone of the European regulatory framework to the test. The presence and overwhelming expansion of platforms as major players in the contemporary digital economy (a 'platform economy')[3] , the voluntary implementation by platforms of content moderation practices and algorithmic monitoring and control mechanisms, and a progressive but growing trend[4] towards greater responsibility[5] of platforms in the prevention and counter of illegal content and illegal activities have challenged the simple 'safe harbour' system.

While the core of the liability exemption proves still to be effective and robust and to respond to a reasonable balance of rights and interests, it nevertheless appears, in the new context of the platform economy, to require adaptations and improvements. The DSA faces the 'platform liability quandary' by trying to strike a stable and appropriate balance between continuity and innovation.

The core of the liability exemption regime is retained and placed at the center of the DSA, at the first level of a tiered model of obligations, but accompanied by several innovations, some of them subtle, others much more forceful and visible, which refine, refine and even update the liability rules on the basis of accrued market experience, case law and the enhanced interpretation of the regulatory framework. Thus, the 'good Samaritan' provision (Art. 7); the tantalising solution, with as yet uncertain effects and scope, hidden in Art. 6(3); and the range of rules governing notification and action mechanisms and the statement of reasons (Arts. 16 and 17) are the main novelties.

This paper analyses the implications of these new solutions in a context defined by the preservation of the 'safe harbour' model and critically assesses how the DSA

[3] As we have argued in previous works, for example, among the most recent and precisely on the occasion of the DSA proposal, Teresa Rodríguez de las Heras Ballell, "The background of the Digital Services Act: looking towards a platform economy," *ERA Forum*, 22(1), (2021): 75-86. doi: 10.1007/s12027-021-00654-w.

[4] Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms*", COM (2017) 555 final, September 28, 2017.

[5] As we noted in a previous co-authored paper Teresa Rodríguez de las Heras Ballell and Jorge Feliu Rey, «Digital Intermediary Liability or Greater Responsibility: A Remedy for Fake News?» in *Twenty-First Century Remedies,* collective work*,* ed. Russel Weaver (North Carolina: Carolina Academic Press, 2019), 91-114 in line with Commission, (n 4), 555 final, September 28, 2017.

strikes a balance between continuity and innovation in addressing the platform liability dilemma.

B. The Drivers for Change: The Exhaustion of the E-Commerce Directive and the Need for the DSA

I. Towards a platform economy

In the context of the creation of a Digital Single Market for Europe,[6] the European Union has understood the essential role that platforms play in the digital society and the need to ensure a suitable environment for their development and consolidation.[7]

On the one hand, platforms are drivers of innovation and growth and constitute a fundamental strategic component for the region's competitiveness. On the other hand, platforms occupy a critical position in an increasingly visible strategy of co-regulation, involvement of intermediaries in the prevention and protection of rights, and the implementation of voluntary enforcement mechanisms. In this sense, platforms and intermediaries become priority partners in detecting and removing illegal content, stemming the tide of fake news and information manipulation, and preventing and monitoring acts of incitement to terrorism.[8]

Any decision to initiate legislative action to establish a European regulatory framework for platforms must therefore take both considerations into account.

The first is to ensure that the regulatory environment is adequate, removing unnecessary obstacles and eliminating the risk of divergences between national regulations inconsistent with the natural cross-border dimension of platform activity.[9] Indeed, the absence of a harmonised framework in the European market would not only transfer an undesired territorial fragmentation to the digital environment, but would also fuel a new phenomenon of regulatory arbitrage for which I have coined

[6] Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, A Strategy for Europe's Digital Single Market*" COM (2015) 192 final, Brussels, May 05, 2015

[7] Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Online platforms and the Digital Single Market. Challenges and opportunities for Europe*" COM (2016) 288 final, May 05, 2016.

[8] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, replacing Council Framework Decision 2002/475/JHA and amending Council Decision *2005/671/JHA*, OJ L 88/6, March 31, 2017.

[9] On the inadequacy of national or regional legislative strategies that fragment this new global or globalised reality represented by the platform economy, which we call "digitality" rather than simply "globality", we refer to Teresa Rodríguez de las Heras Ballell, «The Emergence of Digital Communities: Generating Trust, Managing Conflicts, and Regulating Globality... Digitality» in *Landscapes of Law: Practicing Sovereignty in Transnational Terrain,* collective work, ed. Carol Greenhouse, Christina Davies (Philadelphia: University of Pennsylvania Press, 2020), 250-77.

the term *platform shopping*.[10] In particular, the lack of harmonisation in the liability model (or exemption/exclusion of liability) of platforms aggravates the most pernicious effects of this regulatory arbitrage[11] which I call *platform shopping*. Therefore, a coherent, common and unified approach is key to regulating the platform economy in a global context.

The second is to design a regime of obligations and responsibilities that assigns the right incentives for the collaboration of intermediaries and platforms in the prevention and protection of rights and interests. This is a transfer of functions and powers that is based on the realisation of the disabling limitations of the more traditional formulas for detecting and preventing unlawful acts and resolving conflicts in state-based systems. The platforms, on the other hand, are agile and effective in detecting and sanctioning, and even in preventing certain infringements with content management and location methods. As a result, the 'responsibility'[12] for combating illegal and harmful content,[13] which subtly coexists with the liability regime enshrined in the ECD as a 'safe harbour', is progressively being transferred to them.

The profound transformation of the digital economy to today's platform economy, a prelude to an emerging next evolutionary stage driven by augmented and extended reality technologies (and metaverses) and a truly explosive expansion of

[10] Teresa Rodríguez de las Heras Ballell, «Rules for a Platform Economy: A Case for Harmonization to Counter "Platform shopping" in the Digital Economy» in *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales - Actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne,* collective work co-ordinated by Ilaria Pretelli (Zurich: Shulthess, 2018), 55-79. In the aforementioned work (62) I coined the term "platform shopping", a new variant of regulatory arbitrage, *"to describe the intentional search for those platforms that offer a more favourable climate or friendlier regulation for a specific activity. In a non-harmonised regulatory environment, platforms compete with each other as private ordering systems to attract users to join their community and operate in their "private jurisdiction". Thus, in the absence of harmonised platform rules, regulatory competition would allow digital market players to deploy strategic actions and search for the most suitable platform. While these efforts could be a natural response by private actors to healthy competition between platforms, platform shopping rather describes the risks of the lack of a harmonised legal framework, setting out the duties, obligations and responsibilities of platform operators, leading to the proliferation of illegal content, hate speech, fake news, illicit activities within platforms subject to less stringent applicable laws and exploiting the non-harmonised legal background".*

[11] I refer to the development of this approach in a previous work that addresses the impact on the control of "fake news" of a non-harmonised model (or change of model) of platform liability. Teresa Rodríguez de las Heras Ballell, "Credibility-enhancing regulatory models to counter Fake News: Risks of a Non-harmonized intermediary liability paradigm shift" *Journal of International Media and Entertainment Law,* vol. 8, num. 2, (2020): 129-62.

[12] In the sense of a greater social responsibility towards users and society ("responsibility") that does not compromise the application of the civil liability regime that corresponds to them as providers of intermediary services, insofar as they satisfy the requirements of the "safe harbour". Giancarlo F. Frosio, Martin Husovec, «Accountability and Responsibility of Online Intermediaries» in *The Oxford Handbook of Online Intermediary Liability*, ed. Giancarlo Frosio (Oxford: Oxford University Press, 2020); Rodríguez de las Heras Ballell, Feliu Rey, (n 5), 91-114.

[13] Commission, (n 4), 555 final, September 28, 2017; Commission Recommendation (EU) 2018/334 of 1 March 2018 on *measures to effectively combat illegal content online*, OJ L 63/50, March 06, 2018.

artificial intelligence, needs to recalibrate the foundations on which the European Union had solidly anchored the growth of digital services and markets.

If we trace a path between the foundations of the Union's legal framework for digital services that took shape in the ECD and the rationale behind the launch of the current, and already approved, initiatives for a true platform economy (DSA and DMA), we can assess which of these already established foundations should be preserved, and reveal the limitations that the minimalist and essentially facilitative approach of the Directive was beginning to present.

II. The Exhaustion of the E-Commerce Directive: Strengths and Weaknesses

The adoption of the ECD in 2000 laid the foundations of the EU legal framework for digital services. Since then, the legal framework has remained largely unchanged, while the digital economy has undergone a profound transformation.

Despite its pivotal role, the ECD had started to show shortcomings in meeting the new challenges of today's digital economy. Some shortcomings stem simply from disparate implementation of the ECD by Member States, while others reveal gaps to be filled or the possible inadequacy of certain rules to manage the new challenges posed by the platform economy.[14]

1. Inharmonious application: calibrating the 'legal distance'.

The provisions of the ECD have been transposed differently in national legal systems. Differences in national rules have led to legal fragmentation and, in practice, compartmentalisation of the digital services market. The 'legal distance' caused by legislative divergences has turned into 'commercial distance', due to higher compliance costs and less predictability. The disparate implementation of provisions in national legal systems may be due to a different interpretation of the remedies foreseen in the Directive or simply to a different development of those issues where the Directive does not contain specific rules for the design, content or functioning of mechanisms, procedures or systems, as regards the liability of hyperlink providers or 'notice and take down' procedures. In these cases, national disparity increases, in the absence of a harmonised regime at EU level.

The hampering effect of 'legal distance' has been aggravated by other indirect national barriers to entry related to the complexity of administrative procedures, the cost of cross-border dispute resolution mechanisms or the lack of availability of regulatory information for the provision of digital services. This combination of

[14] EPRS - European Parliamentary Research Service, "Digital Services Act. European added value assessment", October 2020, accessed October 04, 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf.

legal fragmentation and indirect national barriers can hamper the effective delivery of digital services across the EU.

The legal divergence is difficult to reconcile with the global nature of digital models (the 'digitality' factor).[15] Beyond the provision of digital services, the emergence of digital platforms as the new architecture of the digital economy breaks the underlying logic of legislative territoriality.[16] The real challenge posed by the platform economy goes beyond the transnational character of digital activity: platforms aim to emulate and manage a 'private legal system'. The challenge is therefore how to regulate platform operators as regulators, supervisors, trust-builders and facilitators of dispute resolution without promoting *platform shopping*.

While the central role of the internal market clause of the ECD is not contested, the determination of appropriate connecting factors and the delimitation of the scope of application of EU rules – even if harmonised – are key challenging decisions. A stable balance needs to be found between ensuring the provision of digital services in the EU, both for providers established in the EU and outside the EU (as long as they direct services to the EU) and minimising the risk of regulatory arbitrage and its impact on EU users' accessibility to digital services.

2. *Coping with the transformation of the digital economy: the malleability of technology-neutral rules*

While the technology-neutral provisions of the ECD did not ignore the dynamism of business models and were by no means unaware of technological progress, some concepts underpinning the ECD seem inadequate to fully embrace the contours of today's digital economy.

While key principles may endure, the transformation of the context is too drastic and substantial to simply force adaptation of existing rules. Undoubtedly, context-specific solutions are needed. The intensive and extensive use of algorithms to sort, filter, prioritise or remove digital content challenges the classical interpretation of 'obtaining knowledge' under Art. 14 of the Directive and extends the traditional interpretation of the 'general obligation to monitor' prohibited in Art. 15 of the Directive.

The technologically neutral solutions underpinning the DCE legal regime for electronic contracting may be overtaken by the challenges of smart contracts[17] and

[15] Beyond the concept of globality or universality, intended to describe the expansion of international trade and the nature of cross-border transactions, the author argues for the coining of a new concept that better reflects the genuine nature of digital activities: "digitality". Rodríguez de las Heras Ballell, (n 9), 250-77.

[16] Therefore, a harmonised global legal approach to platforms would be highly advisable and desirable, as advocated by the author in Rodríguez de las Heras Ballell, (n 10), 55-79.

[17] Jorge Feliu Rey, "Smart Contract: concept, ecosystem and main private law issues", *La Ley Mercantil,* nª 47, (2018): 1-27.

the extensive application of artificial intelligence and learning techniques.[18] As precisely revealed, in another context but with the same underlying logic, by the UNCITRAL project in its Working Group IV on Use of Artificial Intelligence and Automated Contracting[19] .

3. Rethinking the horizontal approach

Since the entry into force of the Directive, sector-specific rules have been adopted in the EU that have had an impact on the scope and objectives of the ECD. Both the 2019 Copyright Directive[20] and the 2018 Audiovisual Media Services Directive[21] provide for rules that will apply to information society service providers within the meaning of the ECD: provider of online content sharing services and provider of video-sharing platforms, respectively. However, the approach of the two sectoral regimes differs. While the Audiovisual Services Directive opts for an explicit recognition of the applicability to video-sharing service providers of the 'safe harbour' regime (Article 28b and Recitals 44 and 48), the Copyright Directive (Article 17(3) and Recital 65) expressly provides for liability of online content sharing service providers for certain acts in breach of Article 14(1) of the Directive. 14(1) ECD.[22] Thus, the monolithic horizontal approach of the ECD was gradually beginning to fragment with the adoption of sector-specific rules[23] aimed at striking the right balance between conflicting interests.

---

[18] As the EU Expert Group on Liability and New Technologies has assessed in the *Report on Liability for Artificial Intelligence and other emerging digital technologies,* European Union (2019), accessed October 21, 2023, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.

[19] UNCITRAL, "Working Group IV: Electronic Commerce", Documentation of the work of Working Group IV, accessed September 29, 2023, at www.uncitral.org.

[20] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance) [2019] *OJ L 130/92*.

[21] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in the light of changing market realities [2018] *OJ L 303/69*.

[22] The complexity underlying the compatibility of Art. 17 of the Copyright Directive and the prohibition of the general monitoring obligation under Art. 15 of the Copyright Directive has been rightly highlighted by Gerald Spindler, "The liability system of Art. 17 DSMD and national implementation. Contravening prohibition of general monitoring duties?", *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law,* (2019): 344-74.

[23] Giancarlo F. Frosio, "From horizontal to vertical: an intermediary liability earthquake in Europe", *Journal of Intellectual Property Law & Practice*, vol. 12, (2016): 565-75.

Moreover, the P2B Regulation[24] provides for certain rules applicable to 'online intermediation service providers' that fall within its scope. According to Art. 2(2)(a) of the P2B Regulation, online intermediation services constitute information society services.

The ECD, the cornerstone of the EU's legal framework for digital services, was therefore beginning to require a thorough and comprehensive overhaul. Modernising the legal framework for the provision of digital services to embrace technological innovation and level the playing field in the platform economy was essential for the consolidation and strengthening of the digital single market. A digital strategy for Europe must address and accommodate the transformation of the architecture of the digital economy.

The new Digital Services Package (DSA and DMA) has been the vehicle through which the EU's firm commitment to lay the foundations for a renewed strategy to address the challenges and opportunities of a platform economy is channelled.

III. The Need for the DSA: Platform-Oriented Rules

In this process of incorporating platforms into the European regulatory framework, it is observed, first, an interesting substantive permeability with references to the 'platform economy' and, finally, a definitive conceptual and terminological adoption of the phenomenon in the most recent initiatives. Indeed, platforms enter the regulatory arena as descriptors of the new architecture of the digital economy,[25] the platform economy, but without a terminological entity of their own. They continue to be classified as 'intermediation services' in the dual model that the ECD had installed to classify information society services.

This continuity of the existing terminology is particularly graphic in Regulation 2019/1150 which, although popularly known as the Platform-to-Business Regulation, resorts to an elusive definition of platforms as providers of 'online intermediation services' that meet certain requirements (Art. 2.2 b and c), which do no more than highlight their transactional purpose ('with the objective of facilitating the initiation of direct transactions') and delve into the contractual basis ('on the basis of contractual relations between the service provider and the professional users') that

[24] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for professional users of online intermediation services (Text with EEA relevance) [2019] OJ L 186/57.

[25] The Expert Group of the Observatory of the Platform Economy is thus constituted by Commission Decision C (2018)2393 of 26 April 2018 setting up the Expert Group of the Observatory of the Online Platform Economy. The author is a member of the Expert Group since its first mandate, now renewed for a second mandate. All views expressed in this paper are personal to the co-author and do not represent the position of the European Commission, the Expert Group or the Observatory.

makes up the anatomy of platforms.[26] This P2B Regulation, which entered into force on 12 July 2020, seems to have been conceived for pandemic times, despite the fact that at the time of its adoption in 2019, there was nothing to predict what the following year would bring for the global economy. And it is precisely this Regulation that stems from the acknowledgment of the importance of platforms for innovation, entrepreneurship, social welfare and access to new markets, from which stems the concern about the intense, growing and ever-increasing economic dependence of companies ('professional users') established in the EU on the platforms they use to offer their products and services to consumers ('located in the Union') (Art. 1.2). It is thus an effort to iron out the frictions of the platform economy without compromising the advantages of its take-off and consolidation in the common market.

It is curious to note how the circumvention of the term in the P2B Regulation had been preceded, however, by its express use in two crucial Directives that fuel the debate on the durability of the monolithic 'safe harbour' regime[27] in the face of certain signs of sectoral change[28] that we have already mentioned on audiovisual services and on copyright that break with terminological prudence and expressly incorporate video-sharing platforms and video-on-demand platforms.

However, despite the decisive steps that these initiatives represent, the definitive shift in EU law to look at the platform economy head on has not yet materialised. The turning point came with the adoption of the proposed Regulations for a Digital

[26] Sharing very obvious legislative policy purposes with Regulation 2019/1150, the ELI (*European Law Institute*) *Model Rules on Online Intermediary Platforms* choose to standardise the use of the term platform in the body of the legislative proposal and to determine the scope of application of the instrument. The *ELI Project for Model Rules on Online Intermediary Platforms* was approved by the ELI Council on 7 September 2019. The author joined the ELI Project Team in 2016. The rapporteurs of the Project are Christoph Busch, Gerhard Dannemann, Hans Schulte-Nölke, Aneta Wiewiórowska-Domagalska, Fryderyk Zoll. The views expressed in this paper are solely those of the author and do not necessarily represent the position or opinion of the Project team. Text of the Model Rules at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf. In particular, the efforts to proceed to a proper conceptualisation, delimitation and definition of platforms in the project represent an important milestone in the terminological alignment of the European regulatory framework. Teresa Rodríguez de las Heras Ballell, "Article 2. Definitions", in *Discussion Draft of a Directive on Online Intermediary Platforms. Commentary,* collective work coordinated by Busch, Dannemann, Schulte-Nölke, Wiewiórowska-Domagalska & Zoll (Krakow: Jagiellonian University Press, 2019), 41-53.

[27] Teresa Rodríguez de las Heras Ballell, "Il Paradigma della Responsabilità degli Intermediari Digitali nel Contesto di una Economia di Piattaforme (Platform Economy)", *Diritto Comunitario E Degli Scambi Internazionali*, Fasc. 1-2/ (2018): 203-221.

[28] Giancarlo Frosio, "From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe", *Oxford Journal of Intellectual Property and Practice*, vol. 12, (2017): 65, Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2017-05, https://ssrn.com/abstract=3009156 or http://dx.doi.org/10.2139/ssrn.3009156.

Services Act[29] and a Digital Markets Act[30], in the critical year of the pandemic (2020). The prominence of platforms was already undisputed. The DSA builds a framework of tiered obligations from data hosting services to very large platforms that thus incorporates platforms as central subjects. The DMA articulates a complex machinery based on the designation of providers of 'core platform services' as gatekeepers on the basis of a combination of qualitative and quantitative thresholds.

This conquest of the normative terrain by platforms is not purely terminological, nor should it be understood as merely symbolic, it is substantive and crucial in many respects.

Firstly, the DSA retains the logic of the liability exemptions of the ECD, but sets them in the new context that the decisions of the CJEU had been paying for, but, above all, taking into account the extraordinary advances in practices, mechanisms and policies for moderation and control of content implemented by the platforms (private detection and removal systems, automated filtering mechanisms, content management models). The envisaged regime is much more complex and sophisticated, because of the delicate balance of interests involved in the exercise of fundamental rights in the digital society.[31]

The liability exemption (exclusion) rules of the ECD retain their essence and scope in the DSA, but are set in a context that brings three extremely important new features.

First, in view of the disparate transposition of the Directive, they are contained in a Regulation.

Secondly, a clause, commonly referred to as the *Good Samaritan clause*, is incorporated, which closes the gap and adjusts the unstable tension between the absence of a duty to supervise and the logic of the exemption based on knowledge and control. Thus, the new Article 7 DSA clarifies that providers who "conduct, in good faith and in a diligent manner, investigations on their own initiative on a voluntary basis, or take measures for the purpose of detecting, identifying, removing or blocking access to illegal content, or take the measures necessary to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation" will not lose the possibility of being protected by the "safe harbor". In other words, the extraordinary potential of plat-

[29] Commission, "Proposal for a Regulation of the European Parliament and of the Council on a digital single market for services (Digital Services Act) and amending Directive 2000/31/EC", December 15, 2020, COM (2020) 825 final 2020/0361 (COD).

[30] Proposal for a Regulation of the European Parliament and of the Council on fair and contestable markets in the digital sector (*Digital Markets Act*), December 15, 2020, COM(2020) 842 final2020/0374 (COD).

[31] Giancarlo Frosio and Christophe Geiger, "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime", *European Law Journal*, (2022), December 12, 2020, at https://ssrn.com/abstract=3747756 or http://dx.doi.org/10.2139/ssrn.3747756 .

forms in the prevention and moderation of illegal content is thus harnessed, removing the disincentives to implement these proactive measures that a broad concept of 'knowledge' might imply, and indeed did.

Third, a very interesting exception is included in Art. 6(3) DSA based on the consumer's reasonable reliance on the appearance that the operator (hosting provider, but essentially a platform) is the direct provider of the product or service or information or that these are offered or provided under its authority or control. Thus, this provision specifies that the exemption does not apply with regard to the "liability under consumer protection law of online platforms which enable consumers to conclude distance contracts with traders, where that online platform presents the particular information element, or otherwise makes possible the particular transaction in question, in such a way as to lead an average consumer to believe that this information, or the product or service which is the subject of the transaction, is provided by the online platform itself or by a recipient of the service acting under its authority or control".

Secondly, the DSA faces the tricky question of the law applicable to platforms and the determination of a substantial connection with the Union in order to apply the rules contained in this Regulation to platforms established outside the EU (Art. 2.1 DSA). The need, not only to clearly determine the application of European rules to platforms because they direct and provide their services to recipients in the EU, but also, and above all, to constitute an infrastructure that ensures the effectiveness of supervision and compliance measures on providers not established in the EU, explains the adoption of rules, which appear to be purely procedural, on contact points and legal representatives (Art. 11 and 13 DSA).

Finally, the DSA crystallises, without nuances, the regulatory essence of the platforms as contract-based legal systems, which define their conditions, policies, procedures and internal mechanisms (Art. 14 DSA). And it is on the basis of the acceptance of this regulatory and supervisory autonomy that the DSA specifies the rules aimed at ensuring the motivation of decisions, transparency, the effective management of complaints, conflict resolution, measures to limit misuse or report suspected offences, the traceability of traders or even efforts to verify the reliability of information. These are not mere obligations capriciously imposed on a service provider, but a recognition of its capacity to regulate, manage conflicts, prevent and resolve offences, limit the exercise of fundamental rights and freedoms in its space of interaction.[32] In short, they are tailor-made obligations to subject the functions

[32] As we have previously advocated, understanding this (multifaceted) functional profile of platforms and their contractually based anatomy is essential to design an appropriate regulatory strategy and to design an adequate formula to address and largely resolve the dilemma of platform liability. Teresa Rodríguez de las Heras Ballell, "The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU", *The Italian Law Journal*, num. 1/3, (2017): 149, 171

of true regulators, supervisors and generators of trust to certain rules.[33] It is not a change of tone, but of approach.

C. The DSA Faced with the Platform Liability Quandary

The model of exemption/exclusion of platform liability based on the 'safe harbour' for intermediary service providers, which crystallised in the ECD, addresses the dilemma of platform liability and solves it, from a theoretical perspective, in a reasonable and correct way. Practice shows the complexity of the competing interests and the instability of the balance struck, and thus demonstrates that the solution is not perfect.

The dilemma facing the regulator is to achieve a satisfactory and stable balance of incentives so that the cooperation of platforms in the detection, prevention and removal or suspension of illegal content and unlawful activities does not censor or interfere with the exercise of rights and freedoms, but confers the effectiveness and immediacy that their moderation, notification and action mechanisms allow. The regulator seeks to ward off the risk of censorship without renouncing the cooperation of platforms on the front line of *enforcement* in the face of the inability and inadequacy of conventional systems and procedures to efficiently manage and resolve conflicts of rights and interests in the digital economy. To this end, the liability waiver solution is formulated, which places the incentives for platform cooperation in the game between knowledge and control.

The dilemma that the regulator believes has thus been resolved is transferred to the platforms. Faced with the 'safe harbour', platforms face another dilemma: how to strike a balance between generating credibility, supervising, moderating and intervening in platform activity, and minimising their exposure to the risk of incurring liability. In sum, how to maximise the benefits and reduce the costs of the knowledge-control binomial. And this dilemma is, in fact, a platform dilemma, i.e. a dilemma associated with the transformation of the digital economy into a platform economy in which, naturally, platforms are the predominant model and platform operators the main players. Therefore, a liability exemption/exclusion regime designed and formulated for intermediary service providers inevitably has shortcomings when it is to be transferred, without adjustment, to platform operators.

This is the first challenge, to understand and appreciate when and to what extent platform operators are providers of intermediation services. The fit is neither full nor always convincing, and certainly uncertain and changing. Hence, the 'safe harbour' can be preserved in essence, but needs to be nuanced, calibrated, and certain

[33] This thesis has been defended and reiterated in previous works. We refer, for example, to one of the most recent ones. Teresa Rodríguez de las Heras Ballell, "Las plataformas: nuevos actores (y reguladores) de la actividad económica", in *Derecho y política ante la pandemia: Reacciones y transformaciones. Tomo II. Reacciones y transformaciones en el Derecho Privado* (Madrid: Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid, (2021), núm. Extra 3, 403, 417.

frictions to be refined. This is the objective of innovating while maintaining the continuity of the previous rules. The main novelties of the DSA can be interpreted as solutions aimed at adjusting the previous rules and accommodating them to the economics of the platforms.

In the context of the ECD, the debate focused on the extent to which the intensive use of automation in detection, filtering and removal may jeopardise the solid basis of the "safe harbor". Although it had previously been anticipated[34] that the adoption of encouraged proactive monitoring does not imply the loss of the benefit of the exemption from liability for cooperating platforms, it is undeniable that it can be seen as a tool for gaining knowledge and thus capable of triggering the duty to act swiftly. How the adequacy of measures will be assessed, and what consequences defective or ineffective measures will have, is critical. Even whether the duty of supervision, even on a voluntary basis, is an obligation of result or an obligation of means remains unclear. It is debatable whether and when proactive monitoring measures serve to actually know about the illegality or potential illegality of an activity or content and when this knowledge materialises.

Whether an algorithm-based removal system respects the logic of notice and takedown or constitutes *de facto* general platform monitoring is also an interesting question that was not resolved in the ECD and is at least addressed by the DSA. Should the use of an automated system improve efficiency, but at the same time increase exposure to liability or at least create uncertainty, platforms would be discouraged from implementing more sophisticated monitoring mechanisms. The DSA therefore explicitly addresses this dilemma, even if it does not do so in all nuances or resolve all issues.

I. Recalibrating the Absence of a General Duty to Supervise

The first pillar of the 'safe harbour' is the absence of a general duty to supervise. This accentuates incentives towards a strategy of passivity or inhibition by intermediaries, focused on designing clear and effective mechanisms for obtaining the knowledge that triggers the need to act. Risk is therefore calibrated at this stage of the process and is simply avoided in the period leading up to it.

The platform economy challenges, contradicts and even perverts this logic. The contrast between models is increasingly evident. The value-creating capacity of a platform depends to a large extent on its strategy of regulation, oversight and trust-building, moving at different distances, depending on the specific model, from the strategy of passivity and inaction.

---

[34] According to the *Illegal Content Notice*, par. 3.3.1.: *"The Commission considers that the adoption of these voluntary and proactive measures does not automatically cause the online platform to lose the benefit of the exemption from liability under Article 14 of the e-commerce Directive."* As reiterated in the Commission Recommendation of 01 March 2018 on measures to effectively tackle illegal content online, C (2018) 1177 final (26).

Beyond enhancing the provision of digital services by leveraging their network efficiencies, economies of scale and value creation benefits, platforms aspire to create contract-based private orders. Within a huge variety of business models, platform operators act as (contractual) regulators by adopting platform rules and policies, monitoring compliance and sanctioning infringements (centrally or, more often, applying decentralised P2P monitoring mechanisms and adopting sanction policies), facilitating dispute resolution and providing systems to create and preserve reputation.

These functions of platform operators break the type created by the ECD for intermediary service providers. Indeed, the variety of platform operators in the market hardly fits into the ECD's binary taxonomy: (general) service providers and intermediary service providers. While it is true that platform operators act as facilitators, enablers or even intermediaries, their functional profile is far from the passive or purely technical conception of an intermediary service provider as originally conceived by the ECD. While the hallmarks of intermediary service providers covered by the safe harbour are precisely the absence of control and lack of knowledge, platform operators strive to create an environment of trust for users by providing mechanisms to obtain knowledge, manage warnings, remove content or ensure compliance with the platforms' internal policies. In this regard, platforms implement notice-and-takedown systems, algorithmic filtering or rating mechanisms that rely on fact-checkers and trust markers, and strive to adopt common standards and ensure effective compliance. Platforms therefore need to move away from the position of mere passive intermediaries, as envisaged by the ECD, in order to improve their services, attract and retain users and be attractive in a competitive 'platform market'.

Thus, given the constellation of varied business models that platforms can adopt, the legal categorisation of a platform operator has to be based on a prior analysis of its functions, duties and obligations as set out in the access agreement (and other related contracts) and the functioning of all systems and mechanisms in place for rating, notification management, removal, flagging or classification. This is the path followed by the European Court of Justice in its latest decisions on platforms (*Uber* and *Airbnb*). The analysis of each platform reveals whether the platform operator has control and decisive influence over the activity of users within the platform and, if so, to what extent.[35] Accordingly, the Court of Justice incorporates into the binary taxonomy of service providers the relevant factors of control and decisive influence to assess the role of the platform operator. A natural consequence of the ECJ's multi-factor assessment should be the impact on the liability regime. Without altering the 'safe harbour', the assessment of influence and control inevitably affects the passive role of the platform operator underpinning the exemption from liability.

[35] Alberto De Francheschi, "Uber Spain and the "Identity Crisis" of Online Platforms", *EuCML-Journal of European Consumer and Market Law*, num. 1, (2018): 1-4.

This reality does not require a definitive abandonment of the 'safe harbour' model. The DSA does not, in fact, do so, but it does require recontextualising it. On the one hand, it clearly preserves the absence of a general duty to supervise or to actively search. Thus, Article 8 DSA recalls that "(n)o general obligation shall be imposed on intermediary service providers to monitor the information they transmit or store, or to actively search for facts or circumstances indicating the existence of unlawful activities". This continuity is even eloquently stressed in Recital 30 by insisting that (n)othing in the Regulation should be interpreted as imposing a general obligation to monitor or actively search for facts generally, or a general obligation on providers to take proactive measures in relation to illegal content, but also in clarifying that this absence of a general duty does not affect monitoring obligations in a specific case and furthermore that it does not interfere with orders by national authorities in accordance with national law, in compliance with Union law, and in accordance with the conditions of the Regulation. But the continuity of this fundamental pillar is qualified by two particular developments in the DSA that point in this direction and respond to these frictions (Recital 16 DSA). In the tiered structure of the DSA, these provisions constitute the first level.

First, the explicit reference to the relevance of the active role that the operator may play and which is of such a nature as to confer knowledge or control (Recital 18 DSA). Thus, the DSA recognises and incorporates the case law of the Court of Justice which shapes and modulates the scope and extent of the 'safe harbour' rules.

The ECJ's decision in the eBay case[36] confirmed eBay's qualification as an intermediary, but leaved open an avenue of interpretation by making its answer conditional on a finding that the operator does not play an active role. It is unrealistic to reduce the role of a platform operator to the storage of data and content or the mere provision of search engines. In the exercise of its functions as regulator, overseer or trust-builder, it is unlikely that a certain active intervention of the operator in the community can be denied.

In its analysis of the Uber case[37] , which the Court outlines with particular care and which it rigorously maintains as the factual scope of its ruling, the ECJ resorts

[36] CJEU 12 Jul. 2011, C-324/09 *L'Oréal SA and Others* v. *eBay International AG and Others,* http://curia.europa.eu/juris/liste.jsf?language=en&num=C-324/09: "Article 14(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) must be interpreted as applying to the operator of an electronic marketplace where that operator does not play an active role in acquiring knowledge or control of the stored data.

[37] The judgment of the ECJ in Case C-434/15 of 20 December 2017 concerns a reference for a preliminary ruling from the Juzgado de lo Mercantil nº 3 de Barcelona, by order of 16 July 2015, in the proceedings between *Asociación Profesional Élite Taxi* and *Uber Systems Spain, S. L. The decision of the CJEU in this case, preceded by an important and much discussed Opinion of Advocate General Szpunar, issued in May 2017, was awaited in the market with great expectation.L.* The ECJ's decision in this case, preceded by

to three fundamental criteria on which it bases its legal classification of the operator and the services provided.

First, in the UberPop case, in which the drivers are not professionals, the Court assessed the operator's role as the creator of a market which would not be feasible without its intervention. In the view of the ECJ, the non-professional status of the drivers means that the operator's task is not merely to intermediate between an existing supply and a demand for such journeys, but that the platform itself constitutes the supply of transport services by drivers who would not otherwise be in a position to provide the service. With this first argument, the Court is giving substantive value to the aggregation function of the digital technology used (applications, mobile devices, platform). In other words, the Court does not understand the causal vector of the service provided by Uber to stop at the offering and provision of a digital environment for interaction and transactions between drivers and passengers, but projects it onto the very nature of the service itself. In this way, it confers the causal meaning of the transport service provided by the drivers registered on the platform.

This criterion, which the Court delimits very well and applies convincingly in the case under analysis, becomes diffuse and ambiguous when transposed to other sectors. In reality, peer-to-peer (P2P) models all start from a very similar starting point. The supply does not exist beforehand because it is atomised and does not have sufficient reach to address a latent but also dispersed demand, so the platform aggregates and structures it, allowing the activity to become feasible and viable. At the heart of the purest collaborative economy, the platform inevitably acts as a market maker by facilitating interaction and cooperation. Moreover, one of the traditional core functions of an intermediary in the economic sense is precisely to aggregate and centralise, enabling interaction, selection and contracting.[38] Indeed, in the case of UberPop, despite the non-professional status of the drivers, the activity is carried out for profit and the transport service is provided for remuneration. The Court's ruling is therefore made in accordance with these benchmarks. However, it is a criterion whose application may become very uncertain when applied in other sectors. As the sole criterion for the legal qualification of the operator, it therefore seems to us to be insufficient and, to a certain extent, inadequate.

Secondly, however, the ECJ supplements its doctrine on the legal qualification of the operator with two other factors: decisive influence and capacity to control. Both criteria would act as bridges between the operator stratum and the user community. As a consequence, the separation between the two levels is narrowed and the argument of the operator's non-intervention in the activity of the community beyond the management of the platform is weakened.

---

an important and controversial Opinion of Advocate General Szpunar, issued on 11 May 2017, was awaited in the market with great expectation due to its expected impact on the configuration of the sector and the delimitation of the concept of the collaborative economy.

[38] Joseph Bailey and Yannis Bako, "An Exploratory Study of the Emerging Role of Electronic Intermediaries", *Internatinal Journal of Electronic Commerce,* vol. 1, no. 3, Spring (1997): 7-20.

Neither of these criteria is part of the definition with which the ECD describes information society service providers. Therefore, the first question is whether the concurrence of both factors inevitably and automatically transforms the legal status of the provider into a principal provider of the service, transport in this case, ceasing to be an information society service provider, or whether it may, in other cases, only affect the application of the liability regime. For if it were to be argued that the platform operator is nevertheless an intermediary, the presence of control and decisive influence would trigger the non-application of the liability exclusion regime (Article 14.2 DCE). In this sense, the effect of the concurrence of the factors of control and decisive influence beyond the specific case analysed by the Court are not evident.

It is even more difficult to assess what kind of activities, behaviour, practices or functions of the operators of a platform would reveal the existence of decisive influence and control. The Court identifies in this case, in particular, that (par. 39) the operator "sets at least the maximum price of the ride, receives this price from the customer and then pays a part of it to the non-professional driver of the vehicle and exercises some control over the quality of the vehicles as well as over the suitability and behaviour of the drivers, which may lead to their exclusion". It would therefore be necessary to analyse in each business model the scope, content and control effect of the functions performed by the operator in relation to the operation of the platform in order to assess whether they have a decisive influence. This assessment is not straightforward because it is precisely the value-creating capacity of a platform that derives from its regulatory, supervisory, monitoring and sometimes conflict resolution functions. Therefore, a trust-building strategy based on the extensive development of these functions would clearly expose the operator to a legal qualification as a direct provider or to a non-application of the safe harbour.

Second, the incorporation of the so-called "good Samaritan" provision. In Article 7 DSA, the Regulation introduces a notable novelty:

> *Intermediary service providers shall not be regarded as not qualifying for the exemptions from liability referred to in Articles 4, 5 and 6 solely on the ground that they carry out, in good faith and in a diligent manner, investigations on their own initiative on a voluntary basis, or take measures for the purpose of detecting, identifying and removing illegal content, or blocking access to it, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements laid down in this Regulation.*

This solution is directly aimed at attacking the 'undesired' effect of passivity that the pure 'safe harbour' model encourages. This provision has, at least in its literal wording, two elements. Their objective is one and the same: to build a bridge between the absence of the obligation to actively seek and the preservation of the exemption from liability. Thus, proactive behaviour does not prevent providers from benefiting from the exemption from liability. The first element seems to be the broadest: to carry out, in good faith and in a diligent manner, investigations on their own

initiative on a voluntary basis. The second element would connect the exemptions from liability with the obligations that the DSA itself lays down in its subsequent articles in a staggered manner. As Recital 26 explains, the impact of these voluntary practices and measures on the applicability of the exemptions from liability was uncertain and therefore the inclusion of this provision expressly confers legal certainty and is precisely aimed at promoting proactive strategies of intermediaries. Moreover, it is, above all, a full and express incorporation of the functional and strategic model of the platforms that seek and need to generate a trustworthy space by regulating, supervising, with content moderation mechanisms.

This recognition is undoubtedly an 'extension' of the 'safe harbour' insofar as it clarifies the scope and extent of this buffer zone in which intermediaries (especially platforms) develop and deploy their strategy to build trust and credibility, limit their exposure to risk and articulate their business practices. Particularly revealing is the express reference in the Recital to the use of automated tools (*algorithmic content moderation*), which it will be discussed below. Thus, the practices widely implemented by platforms to detect, identify or remove content (*flagging systems, automated moderation,* the widest variety of private detection and removal systems) gain a foothold in the DSA.

The provision is, however, not without uncertainties that platforms will have to manage. The maintenance of the exemption is not full, but is subject to the measures being taken in good faith and with diligence. Recital 26 elaborates these requirements into action under objective, non-discriminatory and proportionate criteria, taking due account of the rights and legitimate interests of all parties involved, and providing the necessary safeguards against unjustified removal of lawful content. Again, although with a better-defined framework, the efforts of platforms to design, articulate and operate detection, identification and removal (and reinstatement) mechanisms that accredit and align with these criteria will be essential. In this case, it seems that we should interpret them as advocating a *procedural fairness* approach. That is, policies, procedures and mechanisms implemented should be designed to operate in an objective, proportionate and non-discriminatory manner. For this is what keeps the platform under the protection of Article 8 and maintains its eligibility for exemptions. It is an overall analysis that qualifies the specific provider for exemptions, although it does not ensure that this is necessarily the case. Ultimately, the mere adoption of measures, the procedural element, does not, by itself, deactivate the exemptions.

II. The Impact of Automation on the Liability Paradigm

The effectiveness of monitoring and removal of illegal content can be significantly improved by incorporating automatic filtering, algorithm-based mechanisms and

artificial intelligence systems.[39] Automation poses, however, worrying risks of excessive removal and arouses censorship concernd. A growing trend towards increased transparency in the configuration, operation and self-learning process of algorithms echoes these concerns. Full disclosure and clear explanation of platforms' content policy in the terms of service, notification and action procedures and automatic filtering criteria should mitigate these concerns. In market terms, transparency would increase competition in the platform market and allow for reasonable choice and informed decisions.

Other safeguards against excessive removal and abuse of the system could also be adopted to alleviate the risk of curtailing freedom of expression. Reasonable notification procedures, well-designed and continuously monitored automatic filtering, and a balanced removal policy should be complemented by trusted flagging systems, counter-notification procedures, and measures to prevent and penalise bad faith notifications and counter-notifications.

Recital 22 of the DSA tries to come closer to some issues, clarifying, for example, that the fact that "the provider automatically indexes the information uploaded to its service, has a search function and recommends information based on the profiles or preferences of the recipients of the service is not sufficient grounds for considering that the provider has 'specific' knowledge of the illegal activities carried out on that platform or of the illegal content stored on that platform". But the uncertainty remains in the use of automated algorithmic mechanisms that respond to predetermined criteria of 'illegality' or 'incompatibility' with the platform's rules, or to patterns by which the filtering or moderation mechanism will identify suspicious content (for *demoting*) or even remove or suspend it. It is inevitable to ask when knowledge is obtained for the purposes of liability exemption: in the determination of the criteria, in the specific identification of the content, in the assessment of the content, or in the decision (automated or not) to remove or suspend.

III. The Protection of Consumer Expectations

Article 6, which reproduces in the DSA the provision on data hosting service providers (Art. 14 ECD), incorporates an interesting novelty whose effects and scope may, however, be somewhat uncertain.

A paragraph 3 is added which presents, in the delimitation of its scope of application, a curious deviation in the structure of the DSA. In the DSA's logic of tiered obligations, the exemptions from liability represent the first layer that applies to intermediary service providers. Successive layers stack up specific obligations and

[39] ELI, "Guiding Principles for Automated Decision Making in Europe", May 09, 2022, accessed October 04, 2023, https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-innovation-paper-on-guiding-principles-for-automated-decision-making-in-the-eu-now-available-f/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=03993b4a3ed4554fc518ba024d45c801.

rules for data hosting services, including platforms, for platforms enabling the conclusion of contracts between traders and consumers, and to very large platforms and search engines. The new rule, which is in fact an exception to the exemption, applies exclusively to certain hosting providers, namely B2C transactional platforms. In other words, it applies to platforms that allow the conclusion of contracts between traders and consumers. Paragraph 3 thus brings to the first level an exception applicable to categories of providers to which it devotes later sections of the text with specific provisions.

With this specific scope of application, the new provision excludes from the protection of the 'safe harbour', with a specific scope that it will be analysed below, the operators of these platforms to the extent that, by the way in which they present the information or allow the transactions to be concluded, they lead consumers to believe that the platform operator is the one presenting the information or offering the product or service or that the trader is doing so under their authority or control. The underlying idea is that certain elements in the platform's operations create the 'expectations' that it is not merely an intermediary but is somehow involved in the transaction and therefore the average consumer has a reasonable expectation that the platform controls, knows or even provides the service or offers the final product.

With the transcribed provision, it can be completed the analysis of the exception with an important nuance:

> *Paragraph 1 shall not apply in respect of the liability under consumer protection law of online platforms that enable consumers to conclude distance contracts with traders, where that online platform presents the particular item of information, or otherwise makes possible the particular transaction in question, in such a way as to lead an average consumer to believe that that information, or the product or service which is the subject of the transaction, is provided by the online platform itself or by a recipient of the service acting under its authority or control.*

The provision is designed to derogate from the liability exemption of hosting service providers, but it is not absolute and total, but limited in scope: *with regard to liability, under consumer protection law.* So, the platform operator becomes liable to the consumer in the same way as the trader would be liable under consumer protection law. Conversely, we should understand that these platforms could still be protected by the exemption in relation to liability that is not related to consumer protection law.

The key piece of this exception is what factors will determine the application of this provision. The wording of paragraph 3 seems to revolve around the idea of reasonable expectations of the average consumer relying on appearance, this includes design, functioning and operation and the way in which information is presented, accessible or verified, and on its content.
Recital 24 provides some illustrations.

> *Examples of such practices include an online platform not clearly displaying the identity of the trader as required by this Regulation, an online platform not disclosing the identity or contact details of the trader until after the conclusion of the contract concluded between the trader and the consumer, or an online platform marketing the product or service in its own name rather than on behalf of the trader who will supply the product or service.*

And it warns that this assessment must be made in an objective manner and taking into account *all relevant circumstances*. Clearly this reference to the identity of the trader connects with Article 30 DSA on traceability of traders (KYBU - *Know Your Business User*).[40] But with this allusion, without direct reference in the regulatory provision, a debate of uncertain contours opens up. To what extent does non-compliance with any of the provisions applicable to platforms enabling consumers to conclude contracts with traders, in particular Articles 30 (traceability), 31 (compliance by design) and 32 (right to information), automatically trigger the exception or is it, in any case, a factor in determining whether precisely this non-compliance is sufficient to induce the average consumer to reasonably expect that the platform controls, supervises or provides the service and/or information.

This debate also raises a second issue as to whether they are obligations of means or of result. The references to 'best efforts' put us in the former category. But even so, the interesting question is whether compliance with the requirements of these articles, which may in practice be procedural in nature – enabling processes, designing the interface, obtaining information from the trader and making best efforts to verify it - is nevertheless in itself a guarantee that the average consumer is 'not induced' to place reasonable reliance on the influence of the platform operator.

Looking for the background to this novel provision, we find a very revealing anchor[41] in the *ELI Model Rules on Online Platforms*.[42] Two of the provisions of these model rules shed light on the ultimate purpose that would seem to inspire this novelty of the DSA. Article 19[43] , *Liability of the Platform Operator for Lack of Transparency*, clearly explains that the triggering breach is the violation of Article 13[44] whereby the platform must expressly and prominently inform the consumer that the contract to be concluded by the consumer is not with the platform operator but with the trader

---

[40] On the scope of this obligation and its implications, Teresa Rodríguez de las Heras Ballell, "Supervision and Enforcement in the DSA - Key Factors for Enhancing the Effectiveness of Enforcement: Analytical Framework and Proposals", in Policy Department for Economic, Scientific and Quality of Life Policies for the committee on Internal Market and Consumer Protection (IMCO), *The Digital Services Act and the Digital Markets Act - a forward-looking and consumer-centred perspective*, (2021).

[41] With overlapping areas of application, Rodríguez de las Heras Ballell, (n 26), 41-53.

[42] Details of the project and its results can be found at https://www.europeanlawinstitute.eu/projects-publications/completed-projects/online-platforms/.

[43] Article 19 Model Rules on Online Platforms: *"In the case of a violation of Article 13, the customer can exercise the rights and remedies available against the supplier under the supplier-customer contract also against the platform operator".*

[44] Article 13: Duty to Inform About the Role of the Platform *"At the earliest opportunity and directly before the conclusion of the supplier-customer contract, the platform operator must inform the customer, in a prominent manner, that the customer will be entering into a contract with a supplier and not with the platform operator".*

who will be his counterparty. Unlike the 'safe harbour' which does not contain rules on attribution of liability, Article 19 of the *Model Rules on Online Platforms* is formulated in a positive way by recognising the consumer's ability to exercise the rights and remedies he would have against the trader under the contract he has concluded with the platform. Article 6(3) of the DSA exempts the exemption, thus making the application of the consumer rules possible, without express attribution.

But it is Article 20 of the *Model Rules on Online Platforms* that is most inspiring for understanding the scope and calibration of the application of Article 6(3) of the DSA. Its wording supports the 'can reasonably rely on' approach of the consumer who, on the basis of certain criteria, believes and trusts that the platform operator has predominant influence over the trader. Interestingly, this provision lists certain criteria that would reveal this appearance and reinforce reasonable reliance: a) The supplier-customer contract is concluded exclusively through the mechanisms provided on the platform; b) The platform operator retains the supplier's identity or contact details until after the conclusion of the supplier-customer contract; c) The platform operator exclusively uses payment systems that allow the platform operator to retain payments made by the customer to the supplier; d) The terms of the supplier-customer contract are essentially determined by the platform operator; e) The price to be paid by the customer is set by the platform operator; f) Marketing is focused on the platform operator and not on the suppliers; or g) The platform operator undertakes to monitor the conduct of suppliers and to ensure compliance with its standards beyond what is required by law.

The above criteria are not fixed factors, nor do they represent a closed and exhaustive list. They are factors that should be taken into account in assessing whether the consumer reasonably relied on the operator to have predominant influence.

These are interesting factors that define the business model, the design of the transactional operation, the marketing strategy or even the algorithmic model for setting conditions and prices. They can serve as a reference in the application of Article 6(3) of the DSA.

However, the way in which the *Model Rules on Online Platforms* determine the scope and effects on liability triggered by this reasonable reliance of the consumer is particularly clarifying. The consumer's ability to exercise against the platform operator the actions and rights that he would have in case of non-compliance against the trader who is his/her counterparty. The DSA is much more subtle and the wording is more ambiguous. It is not a positive rule of attribution but an exception to the exemption. Moreover, it refers extensively to liability arising from consumer protection law. The discussion within the framework of the Model Rules concerned precisely what actions and remedies the consumer is entitled to exercise against the platform. For while compensation of damages will always be possible, an action for specific performance in the event of non-performance could, in practice, be impossible for the platform operator, who is not in fact the seller or the provider of the product or service, to perform.

Consumer Protection on Digital Platforms in Japan: Towards bridging the gap between regulatory requirements and civil liability

Michiyo Maeda

A. Introduction

This chapter focuses on the regulatory framework governing digital platforms in Japan. At the time of writing, two acts govern digital platforms under Japanese law. The first is the Act on Improving Transparency and Fairness of Digital Platforms (TFDPA), enacted in 2020. This act, which came into force in February 2021, regulates the relationship between digital platform providers and suppliers. The TFDPA requires designated specified digital platform providers (SDPP) to work to ensure transparency and fairness in the digital market to prevent violations of the Antimonopoly Act (AMA). The designation as an SDPP is made based on the category and scale of the business.

The AMA establishes the abuse of superior bargaining position (ASBP) as a type of unfair trade practice (Art. 19). ASBP is subject to cease-and-desist orders by the Japan Fair Trade Commission (JFTC) and administrative fines (Art. 20).[1] Although

[1]Under Art. 206, the fine is equivalent to one percent of the enterprise's sales to the counterparty. Administrative fines were introduced in the 2009 amendment of AMA. See: (Kaori Ishii, "A Study on Abusing Superior Bargaining Position in the Anti-Monopoly Act and Its Relation to the Act on the Protection of Personal Information in Japan", Human-Centric Computing in a Data-Driven Society: 14th IFIP TC 9 International Conference on Human Choice and Computers, HCC 14 2020 Tokyo, Japan, September 9-11, 2020," ed. David Kreps, et al. (Berlin: Springer, 2020), 5-15.

DOI: https://doi.org/10.17875/gup2023-2503

both AMA and TFDPA promote fair and free market competition, the latter takes a different approach. This is so-called "co-regulation" which is a promising, strength-based approach to supporting self-regulation that aims to replace punishing fines for deterring others from practices that defy competition rules.

The second act regulating digital platforms is the Protection of Consumers Who Use Digital Platforms (PCDPA). The PCDPA mainly governs the relationship between digital platform providers (DPPs) and consumers, and it was passed in April 2021 and came into force in May 2022. Although TFDPA and PCDPA share the same definition for digital platform provider (DPP), the PCDPA covers all digital platforms for online transactions, regardless of business size and types of goods or services. Even though the PCDPA focuses more on consumers when compared to the TFDPA, DPPs remain an intermediary of the contract between consumer and supplier on digital platforms. In this sense, regulation is limited to administrative matters, as is the case in TFDPA, without covering any civil liabilities directly applicable to DPPs in connection with suppliers' contractual or tortious responsibilities towards consumers.

In this chapter, we discuss how these new laws were brought into shape, including their legislative backgrounds and current and future challenges to explain the changes in the digital market brought about by these two Acts. For this reason, the chapter is divided into two parts: the first introduces the antimonopoly regulation approach, and the second analyses TFDPA and PCDPA from a consumer protection approach.

B. Antimonopoly Regulation Approach

I. Legislative background

1. Interim Report on the New Industrial Structure Vision (27 April 2016)

The reference to digital platforms first appeared in the 2016 "Interim Report on the New Industrial Structure Vision" issued by the New Industrial Structure Committee of the Industrial Structure Council of the Ministry of Economy, Trade and Industry (METI).[2] This report covered a wide range of new technology-related topics such as IoT, big data, AI, data utilization, smart society, digital platforms, ICT in education, workforce diversity, industry-academia-government collaboration, venture capital funds, and fintech.

As for digital platforms, the report explored the challenges Japanese platforms would face under the fourth industrial revolution from a global competitiveness perspective. The primary concern expressed by the committee was the dominant power exerted by American tech giants over Japanese retailers, explicitly referring

[2] METI. Shin Sangyo Kozo Bijon. Ministry of Economy, Trade and Industry, 2016. https://www.meti.go.jp/shingikai/sankoshin/shinsangyo_kozo/pdf/008_04_00.pdf (in Japanese).

to the acronym "GAFA" (Google, Apple, Facebook, and Amazon). A survey conducted by METI in the same year in response to the report mentioned above revealed certain abusive commercial practices such as no alternative payment methods available other than the ones offered by the platform provider, higher transaction fees, restrictions on pricing by retailers, exclusion of apps competing with those owned by the platform provider, and preventing app downloads from a source other than the official app store.[3]

In addition, the survey also revealed that the GAFA platform providers would rapidly expand their market shares by securing competitive advantage and staying in an even more dominant position resulting from economies of scale that build up automatic barriers to entry against competition and getting commoditized. Furthermore, the nearly zero marginal cost of reproduction means that they could scale up at little to no cost, not to mention that each new user adds value to the existing users.

2. Growth Strategy 2018/ Future Investment Strategy 2018 (15 June 2018)

The Japanese Cabinet's Growth Strategy 2018/ Future Investment Strategy 2018 devoted little space to discussing digital platforms. Nevertheless, the strategy considered that a set of rules should be implemented to deal with the rise of digital platform businesses.

> "*As digital platforms continue to dominate the market, the rise in businesses with platform business models has brought a need to sustain a competitive business environment. Data portability on selected platforms and open APIs ensure a transparent and level playing field inclusive of SMEs and venture firms. Fundamental principles regarding this new business model shall be finalized and rolled out during this year to ensure fairness to users and clarify corporate social responsibility of platform businesses. Deregulation aimed to stimulate innovation (relaxation of entry requirements, etc.) will be also considered.*[4]"

3. Interim Discussion Paper of the Joint Study Group (12 December 2018)

Based on the aforementioned cabinet decision, the METI, JFTC, and Ministry of Internal Affairs and Communications (MIC) launched the "Study Group on Improvement of Trading Environment surrounding Digital Platforms" in July 2018.

[3] METI. Dai Yoji Sangyo Kakumei ni muketa Oudanteki Seido Kenkyukai Houkokusho. Ministry of Economy, Trade and Industry, 2016. https://www.meti.go.jp/committee/kenkyukai/sansei/daiyoji_sangyo/pdf/report01_01.pdf (in Japanese).

[4] Prime Minister Office of Japan. Future Investment Strategy 2018. Prime Minister Office of Japan, 2018. https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_en.pdf.

The Study Group published the "Interim Discussion Paper: Improvement of Trading Environment surrounding Digital Platforms."[5] Following the paper's publication, the METI, JFTC, and MIC jointly formulated the "Fundamental Principles for Improvement of Rules Corresponding to the Rise of Digital Platform Businesses."

The Interim Discussion Paper first acknowledges the positive role of platforms in facilitating innovations that result in new businesses and markets, providing opportunities to small and medium enterprises and startups, and bringing benefits to consumers. It then reiterates the concerns expressed in the Vision Report that these platforms tend to hold monopolistic or oligopolistic positions because of the network effect they have on account of their nature and due to the economies of scale. Based on such findings, the paper suggests that the relevant regulations be revised as existing rules tailored to specific modes of business hinder market entry by the new types of businesses using platforms. The paper also demands the "rules," including technological setups known as "code" or "architecture," be transparent and fair vis à vis both retailers and consumers.[6]

4. Fundamental Principles for Improvement of Rules Corresponding to the Rise of Digital Platform Businesses (18 December 2018)

Based on the Interim Discussion Paper of the Joint Study Group, the three government agencies (METI, JFTC, and MIC) officially announced seven Fundamental Principles for Improvement of Rules Corresponding to the Rise of Digital Platform Businesses.[7] The first principle gives us the perspective of the legal evaluation of DPPs. (1) They provide an essential basis for socio-economy. (2) They design, operate, and manage a field that many consumers (individuals) and businesses participate in. (3) Said field is essentially highly manipulative and technically non-transparent. The second principle is about the Promotion of Sound Development of Platform Businesses, which has been discussed since the Vision Report of 2016.

The third and fourth principles directly address the concerns expressed by the Joint Study Group and emphasize ensuring transparency to achieve fairness concerning DPPs (3rd principle) and fair and free competition in digital markets (4th principle). The third principle appears to address unfair contract terms, while the fourth principle deals with the competition law issue. Although there is no sugges-

[5] METI. "Digital Platforms," METI, 23 March 2023. accessed October 22, 2023, https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html.

[6] Souichirou Kozuka, "Japan's regulatory response to digital platforms: Comparisons with European and Asian Approaches," *ZJapanR/J.Japan*. L. Bd. 24 Nr. 48 (2019): 95 (99).

[7] METI. Fundamental Principles for Improvement of Rules Corresponding to the Rise of Digital Platform Businesses. Ministry of Economy, Trade and Industry, 2018. accessed October 22, 2023, https://www.jftc.go.jp/en/policy_enforcement/survey/index_files/190220.1.pdf.

tion made for any special contract law reform regarding the third principle, the operation of the AMA and related institutions to ensure fair and free competition in digital markets is explicitly suggested to be considered in the fourth principle.

The fifth principle deals with considering rules on data transfer and open data. The sixth principle, regarding the establishment of balanced, flexible, and effective rules, is designed to take into account flexible ways such as co-regulation.[8] It combines voluntary and legal regulations to sufficiently and appropriately ensure the effectiveness of rules while considering innovation in the digital sector. Finally, the seventh principle is about the international application of laws and harmonization.

5. [Survey] Interim report regarding trade practices on digital platforms (17 April 2019)

The JFTC surveyed sellers on online retail platforms and app vendors on app stores regarding trade practices. The survey revealed that (1) there were unfavorable contents concerning the unilateral revision of contracts for opening stores and selling products on the platforms or for providing apps and digital content on the app stores; (2) when the platform operators rejected a request for opening stores or selling products from sellers or for providing apps and digital content, they did not explain their reasoning or it was unconvincing; (3) sellers received requests or directions concerning their price or product variety on the platforms without any convincing explanation, and high commissions ("30%" out of the price which the users pay for the apps and digital content).

These results are interpreted as follows: the platform operators impose unfair disadvantages to the sellers and vendors who have no other option than to the platform; they also act as a provider of their products or apps on the platform and unfairly exclude their competitors' products or apps from their platform; platform operators restrict the business activities unfairly; transparency or trade terms between the operators and the sellers or vendors is not sufficiently secured.[9]

6. [Survey] Report regarding consumer e-commerce (29 January 2019)

In the wake of the B2C e-commerce market rapid increase in recent years, the JFTC conducted a survey on trade practices regarding B2C e-commerce in general, such as trade terms between manufacturers and distributors, the sales methods of manufacturers and distributors' websites, and the state of transactions at online shopping malls. The survey was conducted broadly from two viewpoints: the pro-competition and anti-competitive effects based on the acts of manufacturers, retailers,

[8] Glen Hepburn, "Alternatives to traditional regulation," OECD Report, accessed April 11, 2023, http://www.oecd.org/regreform/regulatory-policy/42245468.pdf.

[9] JFTC. Outline of interim report regarding trade practices on digital platforms. Japan Fair Trade Commission, 2019, accessed October 22, 2023, https://www.jftc.go.jp/en/pressreleases/yearly-2019/April/190417_1.pdf.

and online shopping mall operators while comparing the trade practices of brick-and-mortar stores. In addition, a different survey was conducted on the consumption habits of consumers pertaining to e-commerce.[10]
The survey found that specific online shopping malls are more likely to have a superior position in the market owing to an indirect network effect. Therefore, these specific online shopping malls should continue to work on making their trade terms with stores as transparent as possible without changing them unilaterally and unfairly.[11] As long as manufacturers and online shopping mall operators do not engage in prohibited conducts under the AMA in B2C e-commerce markets, the competition in the entire retail market will be further promoted, and the consumers will be able to obtain low-priced good quality products more efficiently.

7. Options for Rulemaking to Address the Rise of Platform Businesses (21 May 2019)
Conforming to the Options for Rulemaking to Address the Rise of Platform Businesses, the Study Group concluded that the AMA should be applied to deal with platform businesses. However, instead of traditional prior control regulation, both self and co-regulatory approaches have the potential to be very efficient policy instruments because of their flexibility. They can be tailored to the specific issue they are designed to address and can change quickly in response to changing circumstances.

8. [Survey] Report regarding trade practices on digital platforms (B2B transactions on online retail platform and app store) (31 October 2019)
According to the survey conducted by JFTC regarding B2B transactions on online retail platforms and app stores, there are three types of acts relating to anti-competitive behavior. This survey shed light on conducts that should be revisited to improve fairness and transparency of trade from the viewpoint of competition policy. First, a DPP has a high degree of probability of being at a superior bargaining position over sellers because of the network effect and advantage of scale that a digital platform generates and the lock-in effect through increasing a switching cost. A

[10] JFTC. Survey Report Regarding Transactions in B2C E-Commerce. Japan Fair Trade Commission, 2019, accessed October 22, 2023, https://www.jftc.go.jp/en/pressreleases/yearly-2019/April/190409_1.pdf (in English).
[11] A number of retailers were dissatisfied with the trade terms imposed by the online shopping mall operators since the online shopping malls were able to unilaterally increase the usage fees or the enterprises were only able to use the stipulated payment methods.
Although it was not confirmed through the survey whether online-shopping-mall operators imposed restrictions on stores in connection with opening a store at other online shopping malls, if an influential enterprise in the market engages in such conduct, there is the possibility that such acts will hinder the business activities of existing competitors or raise entry barriers to the market.
Some retailers responded that the screening criteria by online shopping mall operators were not disclosed at the time of the screening of the opening of a store or the display of products at the online shopping mall.

DPP unreasonably affects sellers compared to standard business practices by raising commission rates unilaterally through a contract revision.

Second, since DPPs compete to attract sellers and consumers, a DPP unjustly interfering with a transaction between other DPPs and their sellers or consumers could violate the AMA as Interference with a Competitor's Transactions. In addition, a DPP can directly offer its goods or services to consumers on its digital platform, competing with sellers who provide the same products or services. Hence, DPPs might give themselves or their related companies preferential treatment by; for example, using transaction data collected by sellers, such as sales data or customers' data, arbitrarily manipulating the platform's search algorithm, etc. These conducts might violate the AMA as Interference with Competitor's Transactions.

Third, acts that could restrict sellers' business might fall within the purview of the AMA, such as MFN clauses (Most Favored Nation clause[12]) or requesting sellers to match prices or conditions of other online platforms. App developers are also under restrictions to set higher prices for content offered outside of the app. In cases where a DPP sets an MFN clause against sellers, the latter are placed under restrictions in terms of discounting prices and increasing a product variety outside of the digital platform, which leads to less competition on price and product variety. Accordingly, it makes the market less accessible to new entrants and disincentives competitors who could offer a wider product variety. A strong DPP, alone or in collaboration with other DPPs, forcing an MFN clause could lead to price maintenance effects[13] or market foreclosure effects[14], thus infringing the AMA (Trading on Restrictive Terms).

Maintaining a competitive environment in the digital platform sector requires widespread discussion and actions from multiple perspectives, such as appropriate control by sector-specific regulations, implementing a scheme to promote data transfer and openness, appropriate protection of personal information, and enforcement of the AMA.[15]

---

[12] An MFN clause refers to provisions in which a DPP requires sellers/developers to offer, in its digital platform, sales prices and product variety which are equal or superior to those offered by them in other sales channels.

[13] Cases where the price maintenance effects arise refer to cases where a vertical non-price restraint tends to impede competition among a counterparty to the restraint and its competitors and enable the counterparty to control its prices reasonably freely for a product or products in question in its own discretion and thus maintain or raise market price of such product(s).

[14] Cases where foreclosure effects arise refer to cases where a vertical non-price restraint tends to cause situation that new entrants to the relevant market and the enterprise's existing competitors are excluded and/or opportunities available to them are reduced (for example, a situation where such restraint makes difficult for them to easily acquire alternative trading partners, and causes increase of their expenses for conduct of business and/or their discouragement from entering the market or developing new products).

[15] JFTC. Survey Report Regarding Trade Practices on Digital Platforms – Business-to-Business transactions on online retail platform and app store. Japan Fair Trade Commission, 2019, accessed October 22, 2023, https://www.jftc.go.jp/en/pressreleases/yearly-2019/October/191031Report.pdf (in English).

II. Overview and critique of Act on Improving Transparency and Fairness of Digital Platforms (TFDPA)

1. Key characteristics

The TFDPA's basic philosophy stipulates that the government should secure the minimally necessary commitments and enforce regulations on DPPs, on the basis that those providers must make voluntary and proactive efforts toward improving the transparency and fairness of their digital platforms. This is called "co-regulatory approach" where the law only gives them the general legal framework and leaves details to businesses' voluntary efforts.

Some DPPs, such as Amazon, Rakuten, Yahoo, Apple, and Google, were designated as SDPPs in April 2021 because of their business size. Amazon, Rakuten, and Yahoo Shopping are online shopping malls selling goods. Apple Store and Google Play Store are App stores. In October 2022, the METI designated Google LLC, Meta Platforms, Inc., and Yahoo Japan Corporation as SDPPs in the digital advertising sector.

The TFDPA requires SDPPs to disclose terms and conditions of trading and other information, develop procedures and systems voluntarily and submit a report every fiscal year on the overview of measures and businesses they have conducted, to which self-assessment results are attached. These are three necessary measures for digital platforms that the act stipulates: disclosure of "provision conditions" (Art. 5[16]), promotion of mutual understanding in transactional relationships between the SDPP and User Providers of Goods (Art. 7[17]) and monitoring and evaluation (Art. 9[18]). The act specifically requires SDPPs to send prior notification of

[16] There is a provisional translation of TFDPA available on METI website, accessed October 22, 2023,https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html.
Art. 5. When a Specified Digital Platform Provider discloses the conditions for provision of Specified Digital Platforms (hereinafter referred to as "Provision Conditions" in this article and paragraph (1) of the following article) in this article and the following article to users (limited to users of Specified Digital Platforms; hereinafter the same shall apply in this paragraph, Article 9, paragraph (4), and Article 10, paragraph (1) and paragraph (2)), the Specified Digital Platform Provider must do so in accordance with the method prescribed by an Order of the Ministry of Economy, Trade and Industry in order to promote understanding of those Provision Conditions by users.

[17] Art. 7. A Specified Digital Platform Provider must take measures necessary to promote mutual understanding in transactional relationships between the Specified Digital Platform Provider and User Providers of Goods, etc.

[18] Article 9.1. A Specified Digital Platform Provider must submit a report stating the following information to the Minister of Economy, Trade and Industry once annually as provided by Order of the Ministry of Economy, Trade and Industry:
(i) matters relating to an overview of the business of the Specified Digital Platform;
(ii) matters relating to handling of complaints and resolution of disputes regarding the Specified Digital Platform;

changes in their terms and conditions, etc. to users and to voluntarily develop systems for settling complaints and disputes.

Regarding "provision conditions" in detail to be disclosed, SDPPs must reveal the main factors used to determine their ranking results. If there is any payment of advertising and publicity expenses or other monies to the relevant SDPP by User Provider of Goods, etc. that may have an influence on such rankings, they must include a statement to that effect.[19] In this sense, the rule can help combat stealth marketing and other such activities. They also must disclose how they collect customer data, including purchase history, browsing data, and preferences.[20] Along with provision conditions that are disclosed to general users, including consumers, these disclosures will be used to support compliance with consumer protection regulations, even though the TFDPA is designed to apply to the relationship between DPPs and suppliers.

Now as to the roles of administrative bodies, the TFDPA requires the METI Minister to review the current situation of platform operation following the submitted yearly report and publicize the assessment results together with an overview of the report. In those reviews, administrative authorities are expected to hold interviews with academic experts, customers and consumers of the target SDPP, and other stakeholders in order to hear their opinions and encourage stakeholders to share challenges and enhance mutual understanding. The act also authorized the METI Minister to request that the JFTC take appropriate measures if a digital platform provider is suspected of infringing the AMA.

(iii) matters relating to the status of disclosure pursuant to the provisions of Article 5, paragraphs (1) to (4).
(iv) matters relating to the measures to be taken pursuant to provisions of Article 7, paragraph (1); and
(v) matters relating to evaluations performed by the Specified Digital Platform Provider regarding the matters set forth in the preceding three items.

[19] Art. 5.2.1. In cases where information relating to Goods, etc. sought by General Users (limited to General Users who use the Specified Digital Platform; hereinafter the same shall apply in this article) through searches and other information relating to Goods, etc. is displayed with ranks indicated in a location provided by the relevant Specified Digital Platform, the main factors used to determine such ranks (in cases where payment of advertising and publicity expenses or other monies to the relevant Specified Digital Platform Provider by User Provider of Goods, etc. may have an influence on such rankings, including a statement to that effect).

[20] Art. 5.2.2. In cases where the relevant Specified Digital Platform Provider acquires or uses purchase data concerning Goods, etc. (data pertaining to searches for or viewing of information relating to Goods, etc. or purchases of Goods, etc. by General Users; hereinafter the same shall apply in this sub item (b)), the particulars of the relevant purchase data concerning Goods, etc. and the conditions relating to the acquisition or use thereof.

2. Future work

"Monitoring Review" is another essential element of the TFDPA. As mentioned above, TFDPA specifies that the Minister of METI will review the transparency and fairness of the specified digital platforms and make the results of the review public. In preparation for the review, the METI held a "Monitoring Meeting" to hear opinions from stakeholders, such as academic experts, business users, consumers, and others. Furthermore, TFDPA requires that SDPPs make efforts to make voluntary improvements based on evaluation results by the METI. The METI Minister publicized the first assessment results on 22 December 2022.[21] According to the assessment results, 70-80 % of suppliers are more satisfied with SDPPs' disclosure of provision conditions and consultation services than the previous year. SDPPs also reported launching different approaches and programs corresponding to the requirements described in the TFDPA.

The METI also publicized processing status information regarding some suspected violations of the TFDPA as an attached document to the assessment results. According to this document, SDPPs voluntarily took steps to recover the suppliers' loss caused by their violation of the TFDPA and made an effort to prevent similar situations.

Arts. 6 and 8 of the TFDPA stipulate that the METI Minister can recommend to the relevant SDPP that it take necessary measures when not in compliance with the prescribed provisions in those articles. If the METI Minister has made this recommendation, he shall issue a public announcement to that effect. However, according to the attached document to the assessment results, making a recommendation or not depends on the extent of efforts on the part of the relevant SDPP on voluntary reporting to the METI, collaborating with them in an investigation, as well as loss recovery and remedial actions.

This structure incentivizes SDPPs to commit to collaborating in improving their trading environment. This is important, especially when there is a need to bridge the information gap between the METI and SDPPs. This is also a key for co-regulatory approach as the TFDPA only provides SDPPs with a general legal framework and leaves details to businesses' voluntary efforts. This rule is constructed around the premise that the METI should build trusted relationships among all the stakeholders, including foreign SDPPs. The participation of foreign business users in monitoring meetings held by the METI allows an effective assessment of the compliance of the internal audit function with the requirements of the international framework for business users. It would also provide an external evaluation of the Japanese market that help reveal the business challenges it faces.

[21] There is an English translation of Minister's Evaluation available on METI website, (n 16).

For all these reasons, the TFDPA is expected to be a model for future government regulations on business.[22] While the EU has just stepped-up control of DPPs by introducing new rules prohibiting certain activities under Digital Markets Act (DMA)[23], Japanese regulators will continue with the co-regulatory approach working together with DPPs equitably.

C. Consumer Protection Approach

I. Legislative background

1. Report of the Expert Examination Committee regarding Transactions on Online Platforms (11 April 2019)

Having lagged far behind the METI and JFTC for years, the Consumer Affairs Agency (CAA) established a special committee on online platforms that serve as a connection between third-party businesses and consumers in December 2019. This move was quite slow and coincided with the first cases of COVID-19 detected in China and later spreading. This led to the WHO declaring a Public Health Emergency of International Concern on 30 January 2020 and a pandemic on 11 March 2020. The Japanese government declared a state of emergency in response to COVID-19 on 7 April 2020.

The COVID-19 outbreak has meant significant life changes for all of us, including adjusting to new ways of working and living. During the global pandemic, there was a rapid increase in staying home and working from home that looked to ensure social distancing. According to a survey conducted by UNCTAD and others[24], the pandemic has accelerated the shift towards a more digital world and triggered changes in online shopping behaviors that are likely to have lasting effects. In this sense, the fresh start of the special committee at CAA was a wonderfully well-timed move for consumer transactions via online platforms to be discussed.

---

[22] There have been some environmental regulations that gives greater flexibility and encourage technological innovation, particularly if existing regulations cannot meet the regulatory requirements (Government of Canada, "Literature Review to assess the relevance of outcome-based regulations to innovation," Natural Resources Canada CanmetMINING-Green Mining Initiative, Minerals and Metals Sector (2013), accessed October 22, 2023, https://natural-resources.canada.ca/science-data/science-research/earth-sciences/earth-sciences-resources/earth-sciences-federal-programs/literature-review-assess-relevance-outcome-based-regulations-innovation/11732#e0.

[23] Andrea Renda, "Can the EU Digital Markets Act Achieve Its Goals?". The Digital Revolution and the New Social Contract series, Center for the Governance of Change, IE University (June, 2022), 1-13., accessed October 22, 2023, https://www.ie.edu/cgc/news-and-events/news/new-policy-paper-eu-digital-markets-act-achieve-goals/

[24] The survey entitled "COVID-19 and E-commerce" was conducted by UNCTAD and Netcomm Suisse eCommerce Association, in collaboration with the Brazilian Network Information Center (NIC.br) and Inveon. It shows that online purchases have increased by 6 to 10 percentage points across most product categories.

The committee's main goal was to identify the essential rules that would monitor and promote the safe use of online platforms and support consumers in making safe choices by analyzing the roles that business operators and users should play. According to Professor *Kunihiro Nakata*, the chairperson of the committee, all the members shared the same concern that the reviews and rating system play a crucial role in the buying process. Still, nobody was sure who would be responsible for fake reviews (fake review providers or platform owners) and how it would be.

The report concluded that DPPs should incorporate the consumer perspective in developing their businesses by considering consumers as one of their essential partners in the market. DPPs set up their terms and conditions that are supposed to serve as a customer acquisition tool, assuming that their platform becomes more valuable to each user as the number of users on the platform increases. In other words, digital platforms hold significant control in the flow of information between the suppliers and the consumers to optimize the matching sequence. In addition, they play a significant role in shaping consumers' decision-making process during the formation of contracts and creating an online payment system in connection with contract performance. For these reasons, DPPs should play a vital role in providing a secure trading environment for everyone involved in the online platform transaction and creating a rational decision-making system that supports consumers to exercise choice and independence.

The report was not supposed to directly propose any legal reform. However, the inescapable conclusion is that DPPs should be responsible for fake reviews or counterfeit products as long as they can take preventive measures by eliminating fake reviewers and unethical suppliers.

2. Summary of Issues on Consumer Transactions on Digital Platforms (24 August 2020)

a. Policy framework for combating counterfeiting and defective products

Eight months after the publication of the Report of the Expert Examination Committee regarding Transactions on Online Platforms, the CAA was finally ready to tackle Digital Platforms across the Agency and started to pave the way toward the future legislative proposal.

The Report of Expert Examination Committee articulated a couple of crucial points for the debate on regulating digital platforms. The first point is to ensure the safety and security of consumer products and download materials. The second one is the collaboration of all stakeholders (DPPs, suppliers, the executive branch, etc.). The third and ultimate point is that a workable set of rules is needed to combat all the cases involving serious or malicious violations of laws and ordinances.

According to Professor *Takehisa Nakagawa*, the alternate chairperson of the committee, the first step to meet those requirements is grouping targeted business operators and suppliers into three categories (least compliant, middle, and compliant) depending on the threat they pose to the safe transactions on Digital Platforms. Firstly, most DPPs would be categorized as the middle group because they usually

provide high-tech services that could cause legal problems in certain jurisdictions. In such cases, they would be prepared to take the case as far as required, up to the Supreme Court. This means that they are not totally compliant.

On the other hand, the suppliers may vary depending on the different assumptions. In 2020, the CAA ordered 13 suppliers to suspend business upon constructive service because they were selling counterfeit products on the internet and found them registered on false addresses. These suppliers are to be considered as the least compliant and should be eliminated from the market. However, since DPPs also benefit from the least compliant suppliers, there is little incentive to eliminate them if this significantly decreases the number of users. Nevertheless, this situation would be different if DPPs were legally responsible for those least compliant suppliers' transactions.

When it comes to the middle and compliant suppliers, they happen to be able to widen sales thanks to digital platforms, which means there would be a situation where their faulty products cause damage to much more consumers than they could cover. Therefore, DPP is expected to take action to prevent or reduce the risk of customer injury and property damage and provide mechanisms for dispute settlement.

In these situations, DPP would play a key role in both eliminating the least compliant suppliers, and preventing and addressing significant harm to consumers arising from the middle and compliant suppliers, by making sure of mandatory required vendor information and certifications as well as labeling requirements. DPPs could also be (jointly) liable in some instances involving any visible defects or knowable risks.[25]

b. Misleading advertising

Regarding exaggerated advertisements that can mislead consumers, the report concludes that DPP can easily find if all the suppliers' products meet regulatory labeling requirements. However, this is not the case with the investigation into whether their labeling violates the Act against Unjustifiable Premiums and Misleading Representations.

There are different attitudes towards misleading ads in the world.

[25] In the US, product liability cases involving Amazon.com. Cases with rulings against online platforms include: *Oberdorf v. Amazon.com Inc.*, *930 F.3d 136* (*3rd Cir. 2019*); Bolger v. Amazon.com, LLC, 53 Cal.App.5th 431, 267 Cal.Rptr.3d 601 (2020); *State Farm Fire & Cas. Co. v. Amazon.com Servs.,* 137 N.Y.S.3d 884, 889 (N.Y. Sup. Ct. 2020); Loomis v. Amazon.com, LLC, 63 Cal.App.5th 466, 277 Cal.Rptr.3d 769 (2021). Cases with ruling in favor of online platforms include: *State Farm Fire & Casualty Co. v. Amazon.com,* 835 F. App'x 213, 216 (9th Cir. 2020); Great N. Ins. Co. v. Amazon.com, Inc., 524 F. Supp. 3d 852 (N.D. Ill. 2021); State Farm Fire & Cas. Co. v. Amazon.com, Inc., 528 F. Supp. 3d 686 (W.D. Ky. 2021); Berkley Reg'l Ins. Co. v. John Doe Battery Mfr., Civ. 20-2382 (WMW/DJF) (D. Minn. Oct. 7, 2022).

In 2016, Google took down 1.7 billion misleading advertisements that violated their advertising policies. In 2020, as part of its commitment to protecting consumers online, the European Commission coordinated a screening ('sweep') of websites, intending to find out where consumers in the EU are being subjected to content promoting false claims or scam products in the context of the coronavirus. The results show that, following the commission's call, platforms have removed or blocked millions of misleading advertisements or product listings.[26]

Also in India, The Department of Consumer Affairs runs an online portal, namely "Grievances Against Misleading Advertisements" where consumers can lodge complaints relating to misleading advertisements on any media, including digital platforms.

Recent news reported that the Federal Trade Commission (FTC) issued orders to Social Media and Video Streaming Platforms regarding efforts to address the surge in advertising for fraudulent products and scams.[27]

c. Fake reviews

The report points out that a joint commitment of public authorities and digital platforms is required to fight fake reviews effectively. They can work together by exchanging information, reporting offenders, and educating their users.

For their part, digital platforms should reinforce their commitment to creating more transparent online marketplaces. This commitment can be materialized by designing more transparent rating systems, which entails the implementation of quality controls for improved authenticity of reviews, and the effort to encourage more real consumers to leave accurate reviews.[28]

An upcoming legal change prohibits covert advertising for the first time in Japan. The CAA designated covert advertisements[29] as a prohibited practice in the

[26] The sweep – carried out by the Consumer Protection Cooperation (CPC) Network – consisted of two parts: a high-level screening of online platforms, and an in-depth analysis of specific advertisements and websites linked to products in high demand because of the coronavirus.

[27] The orders will collect information about the companies' standards and policies related to paid commercial ads and their processes for screening and monitoring for compliance with those standards and policies, including through human review and the use of automated systems. The orders also require the companies to report their ad revenue, the number of ad views, and other performance metrics, including for ads involving categories of products and services more prone to deception such as those intended to treat, prevent, or cure substance use disorders and tout income opportunities.

[28] Juan María Martínez Otero, "Fake reviews on online platforms: perspectives from the US, UK and EU legislations," SN Social Sciences, num. 1 (July 2021): 181.

[29] Various advertising regulations promote four main principles that every advertisement must respect: authenticity, truthfulness, fair competition and legality. The first two principles primarily aim to protect consumers. The principle of authenticity guarantees that consumers, being aware of the persuasive and biased nature of the message, can interpret it correctly. Covert advertising is the most typical way of violating the principle of authenticity. It is an advertising in disguise, under the mask

Act against Unjustifiable Premiums and Misleading Representations. The new rule enters into force in October 2023.

d. Targeted adverting and Personalized pricing

Personalized pricing is a potentially discriminatory practice where prices are set at a different level for each individual consumer, based on an assessment of what they are willing and able to pay. The data-driven personalization of prices has expanded the practice into new and potentially harmful territory. Companies can now make use of advanced data collection, machine learning algorithms, and the ability to make real-time offers to sharpen their personalized pricing – techniques that are invisible to consumers. This hidden pricing practice puts consumers at a double disadvantage – firstly, being targeted based on a sophisticated analysis of their likely behavior by a company, and secondly, being unable to compare prices and shop around for a better deal.[30]

There are two main problems regarding personalized pricing: one is related to unfair commercial practices, and the other is privacy and data protection.

Marketing practices such as online price discrimination, dynamic pricing, and personalized pricing could be considered unfair commercial practices under Directive 2005/29/EC. According to the updated version of Guidance Notice on the Unfair Commercial Practice Directive in 2021, the European Commission allows personalized prices based on online tracking and profiling but requires traders to inform consumers of how that price was decided. The Directive also recognizes that customized pricing and offers may be combined with other unfair commercial practices such as aggressive marketing, to create more significant disadvantages for consumers.

In Japan, the TFDPA requires that SDPPs inform users of how their product recommendation system works and the essential factors in determining the ranking, including any seller fee.

As to privacy and data protection, whilst privacy and data protection laws cannot directly regulate business pricing decisions, the GDPR governs personal data collection, storage, and processing, often used to implement personalized pricing. Under the GDPR, using personal data (including internet identifiers) to tailor a price to an individual must comply with the fundamental principles of transparency, fairness, and lawfulness.

---

of different appearances such as a piece of news, a blog post, or a consumer review (Martínez Otero, n 28).

[30] According to a report from Consumers International, personalized pricing is not being implemented fairly, transparently or with proper oversight., accessed October 22, 2023, https://www.consumersinternational.org/news-resources/news/releases/new-research-consumers-worldwide-concerned-by-opaque-online-pricing/.

Japan's data protection law, the Act on the Protection of Personal Information (APPI) was amended in 2020 and entered into force in April 2022. The amendments brought the APPI to an even closer alignment with the GDPR by expanding Japanese data subjects' rights, making data breach notifications mandatory, and limiting the range of personal information that can be provided to third parties. Especially the third amendment on data transfer restrictions would enormously affect targeted advertising and personalized pricing as companies that wish to transfer personal data to third parties must obtain direct consent from the data subject.[31]

e. Terms and conditions (T&Cs)

The committee has agreed on new rules to make sure DPPs have clear terms and conditions (T&Cs), explaining to the user in comprehensible language when their content or their account can be affected by certain restrictions and an obligation to apply such restrictions in a diligent, objective, and proportionate manner.

T&Cs usually seem excessively lengthy, covering a wide range of eventualities, making it difficult for consumers to identify the terms which might interest them most. Still, legal protections mean that hidden, misleading, or unfair terms do not bind consumers. However, there is a danger that T&Cs do not help empower customers but rather risk undermining their confidence and hindering them in asserting their rights. Moreover, the T&Cs of digital platforms tend to have a larger volume by adding new services or functions, making it more difficult to keep track of every change. Therefore, it is necessary to revise in a general way the criteria for assessing the unfair character contract terms of digital platforms that can apply to two or multi-sided relationships involving DPPs, consumers, and suppliers.[32]

---

[31] There is a positive side of discussion about ownership and transferability of user data for the platform users. A related concrete policy measure is the current GDPR with which the European Commission intends to give citizens back control of their personal data within the European Union. The aim of the regulation is that a person could transfer their personal data from one platform to another in a structured and commonly used electronic format. According to the paper, data transferability reduces switching costs for platform users. (Sampsa Ruutu, Thomas Casey and Ville Kotovirta, "Development and competition of digital service platforms: A system dynamics approach," *Technological Forecasting and Social Change*, Volume 117 (2017): 119-130).

[32] From a critical point of view, terms of online services are not contracts for service in the traditional sense, since they often do not contain any obligations or promises on the side of the providers. Moreover, the question of whether these documents are contracts at all remains open. They always contain some contractual elements (licensing of software and/or content), but primarily set the rules specifying what users are (not) allowed to do, resembling more an exercise of property rights than contracts. In addition, the relations between online service providers and their users should be viewed through the lens of horizontal/vertical (private/public) relations. Online service providers might be *de lege* private entities, but the type of power they enjoy is public in nature. Fourthly, what should be noticed is their unilateral control of the code and algorithms behind their platforms. The unequal power position they enjoy towards the consumers comes not only from what is written in

3. (Final) Report on Consumer Transactions on Digital Platforms (25 January 2021)

a. Fundamental Principles

First, it is essential to consider the structural characteristics of two-sided platform businesses that serve distinct groups of customers (consumers and suppliers) and need each other in some way. This situation makes it difficult for DPPs to simultaneously meet and satisfy both sides of their customers' needs. Even if digital platforms want to be more responsible in content governance on behalf of consumers, removing content is subject to certain restrictions in terms of T&Cs between digital platforms and suppliers. Therefore, there should be a clear rule or any exclusion of liability that allows DPP to take steps to protect consumers without any restrictions.

Second, there should be a cooperative system for controlling digital platform businesses among all stakeholders, including customers, suppliers, digital platforms, and the government. Especially digital platforms and the government need to work in collaboration to achieve a shared goal, taking the rapidly evolving digital technologies into account. DPPs are already pushing forward their relations in promoting independent efforts for consumer protection. Accordingly, there should be a legal framework to support these voluntary activities undertaken by DPPs. Such a framework should be extended globally to include foreign operators.

b. Expected roles of DPP

The supply contract for goods or services is concluded between suppliers and customers. DPPs are not a party to this contract. Indeed, most DPPs go through great lengths to make it clear in their T&Cs that they only provide an intermediation service and are not involved in the supply contract. Even where a DPP is a stranger to the supply contract, there is some influence over the terms of that contract. For instance, a DPP may require that the supply contract is based on standard terms set by the platform, or that some of the contractual obligations, such as payment, are performed through facilities provided by the platform.

Considering these kinds of platform operators' control as an intermediary over supply contracts concluded between consumer and supplier, DPPs should monitor suppliers and take timely action to correct any deficiencies or breaches of duty under administrative law identified by an assessment, investigation, or review. This is because any violation of administrative regulations is likely to result in damage to many other consumers.

---

the terms, but most of all from the unconstrained control of the code. Finally, to mitigate this inequality, consumer law should concentrate not only on the substance of the terms, but predominantly on what the providers *do* with the code and the algorithms, and constrain the exercise of this power in a way that would benefit the consumers (Przemyslaw Jacek Palka, "Terms of service are not contracts – Beyond Contract Law in the Regulation of Online Platforms," in *European Contract Law in the Digital Age,* ed. by Stefan Grundmann (Cambridge: Intersentia, 2018), 135-162).

c. Challenges and possible solutions

Considering that the supply contract is concluded via a mail-order system online, the first challenge is resolving the problem of deceptive and misleading advertising. The Act against Unjustifiable Premiums and Misleading Representations only applies to the suppliers. Still, there are specific difficulties in enforcing the rule because of their fake contact information registered with DPP. In this situation, DPP should ensure their registered contact information and any possible removal or corrective action of their illegal representations.

The second challenge is somewhat similar to the first one. Nevertheless, DPPs are expected to request that the suppliers registered with them provide materials that support their identity information and take any other measures to request that suppliers provide information that helps identify them as needed.

The third challenge is promoting voluntary efforts and information disclosure by DPPs to improve transparency.

d. Possible legislative proposal

There are four points to keep in mind for the future legislative proposal.

First, the rules are to be reviewed in an agile and flexible manner by considering the status of enforcement and changes in the circumstances surrounding digital platforms.[33] DPPs have accumulated knowledge and skills that is reflected in innovation. Thus, there should be more room for trying out informal instances of control through operator-led digital initiatives.[34].

Second, considering that DPPs cannot check and control every single supplier, they are expected to make the best efforts in taking appropriate and effective measures according to the actual conditions of their business operations by voluntarily and continuously exercising their creativity and ingenuity. These measures taken by DPPs should be disclosed because this is helpful information for consumers to choose the digital platform.

Third, there should be close coordination among all the stakeholders, including the government, consumer organizations, etc., to produce a functioning system for problem prevention and settlement of conflicts.

Fourth, it is crucial to put national and foreign digital platforms on an equal footing by developing rules that apply to both whenever Japanese consumers are involved.

---

[33] Nicola Ens, Philipp Hukal, Tina Blegind Jensen, "Dynamics of control on digital platforms," *Information System Journal* (2023): 890-911, https://doi.org/10.1111/isj.12429.

[34] N. Simcheko, S. Tsohla and I. Pavlenko, "Digital Platforms of Networking in Industry," IOP Conference Series: Materials Science and Engineering. 753 (2020) 062005, doi: 10.1088/1757-899X/753/6/062005.

Under the above-mentioned points of view, DPPs are obligated to do their best as intermediaries[35] in taking measures for smooth communication between consumer and supplier, appropriate removal or corrective action of illegal representations and request for more documentation for identity verification of suppliers.

When the suppliers responsible for illegal representations do not provide any identifying documentation, DPPs, at the request of the Prime Minister (CAA), can suspend the sales of products with illegal representations without judicial order and subsequent liability towards the supplier.

Also, consumers preparing for a lawsuit can request the disclosure of suppliers' contact information registered with the DPP. In this case, there are two limitations: one is the amount of claim, and the other is that platform operators must notify the suppliers to get their permission when their registered contact information is correct.

Lastly, there should be a broad opportunity for everybody to give notice of all possible risks to consumers using digital platforms. The Prime Minister (CAA) can take care of the notices whenever they receive them. There should be no limit on the person or organization giving this notice.

II. Overview and critique of the Act on the Protection of Consumers Who Use Digital Platforms (PCDPA)

1. Key characteristics of the Act

The PCDPA is a special legislation aimed at protecting consumers from unsafe products and seller-related identity fraud on e-commerce platforms. As to the targeted DPPs, the PCDPA covers all digital platforms for online transactions, regardless of business size and types of goods or services. The act also covers online shopping malls, auction websites, flea markets, sharing economy, App stores, etc. as far as a B2C purchase is concerned.

The PCDPA establishes the following digital platforms' obligations on a "best efforts" basis (Art. 3)[36]: (1) taking measures for smooth communication between sellers and consumers, (2) conducting any necessary investigation in the event of complaints about displayed info on goods, etc., and (3) making identity confirmation of sellers where necessary.

When the suppliers responsible for illegal representations do not provide any identifying documentation, the DPPs, at the request of the CAA, can suspend the

[35] From a comparative point of view, Christian Twigg-Flesner, "Online Intermediary Platforms and English Contract Law," in *Intermediaries in Commercial Law,* ed. Paul S Davies and Tan Cheng-Han (Oxford: Hart, 2022), 171-192.

[36] There is English translation of PCDPA available on Japanese Law Translation website, accessed October 22, 2023, https://www.japaneselawtranslation.go.jp/en/laws/view/4195.

sales of products with illegal representations without judicial order and subsequent liability towards the supplier (art. 4).

The PCDPA also stipulates the right of consumers to request information disclosure on business users only to the extent necessary for consumers to bring claims of compensation (Art. 5). Specifically, there is a limit to the amount of the claim over 10,000 yen (Art. 4 of Ordinance for Enforcement of the PCDPA[37]) and the seller's information is limited to their name, address, telephone number, fax number, email address and EIN (enterprise identification number) (Art. 5 of Ordinance for Enforcement of the Act). Furthermore, consumers who request information disclosure must make a written statement of non-use for illicit purposes (Art. 5.2 of Ordinance for Enforcement of the Act). If the DPP ignores the request for information disclosure and causes damage to consumers, the latter would be entitled to compensation even in the case of ordinary negligence. In this sense, the DPPs are in the opposite situation where internet providers are discharged except for liability for the loss caused by gross negligence or intentional misconduct.[38]

There is also a consumer reporting system available through the official website of the CAA if there is any risk of damage to the interests of general consumers using digital platforms (Art. 10).

2. Future work

There are a few issues left to discuss.

First, the PCDPA only covers B2C transactions because they are considered mail-order sales governed by Act on Specified Commercial Transactions.[39] The Act on Specified Commercial Transactions is an administrative regulation applicable to sellers. The DPPs are expected to support the enforcement of the Act on Specified Commercial Transactions by imposing subsidiary responsibility on them in case of the violation of administrative provisions. However, many consumer troubles need to be fixed even in C2C transactions, especially in online flea markets.

In any online market, consumers generally do not interact face-to-face with sellers. This suggests that online sellers should be required to disclose more information about themselves (location and contact information, etc.) than offline

[37] There is English translation of Ordinance for Enforcement of the PCDPA available on Japanese Law Translation website, accessed October 22, 2023, https://www.japaneselawtranslation.go.jp/en/laws/view/4197.

[38] Art. 4.4 of Provider Liability Limitation Act stipulates, "The provider of disclosure-related service shall not be liable for any loss incurred by the person who demanded for said disclosure in accordance with the provisions of paragraph (1) arising from said provider's refusal of said demand, unless there is any willful act or gross negligence on the part of said provider".

[39] There is an information website of Act on Specified Commercial Transactions in a few foreign languages (English, Korean and Chinese), accessed October 22, 2023, https://www.no-trouble.caa.go.jp/foreignlanguage/.

sellers. Similarly, online consumers generally are unable physically to evaluate products before purchase. This suggests that online quality indicators (product reviews and ratings, etc.) take on heightened importance online and should be policed with heightened scrutiny.[40] To turn these suggested ideas into reality, it is necessary to regulate online C2C transactions supported by DPPs in the future.

Second, in the case of a contract, a contractual obligation to use "best," "reasonable," or "all reasonable" efforts to achieve something is not regarded as too uncertain to be enforceable, even where that is to enter into a further agreement. However, this is subject to the object of the efforts being capable of being ascertained with sufficient certainty. Similarly, there would be cases where the DPP does not store accurate identity information of sellers, or the disclosed information is incorrect, due to which the consumer fails to file a lawsuit against the seller. In these cases, it would be difficult to lodge a claim against the DPP for having provided incorrect information[41] because their obligations are on a "best efforts" basis if necessary, according to the Art. 3.1.1 of the PCDPA.

Third, there should be a regulation concerning the civil liability of DPPs directly toward the consumers. Other than the product liability cases from the US discussed earlier, there are also Italian cases where the Italian Competition Authority (ICA) sanctioned DPPs for unfair commercial practices and violating the pre-contractual information duties. The ICA held that Tripadvisor was a "trader" under the Consumer Code (Codice del Consumo), not limiting itself to storing information but actively classifying and systematizing it. The investigation led by the ICA found that consumers were often influenced to purchase goods by the false impression that Amazon was the immediate supplier and learned about the actual seller's identity only after the purchase.[42]

There are three legal approaches suggested in Japan that should be adopted in future legal reforms related to the liability of online platforms: contractual, tort, and systemic liabilities.[43] In such future legal reforms, privatization of rulemaking should

[40] Amelia Fletcher et al., "Consumer Protection for Online Markets and Large Digital Platforms," *Yale Journal on Regulation* 40, (2023): 875 (914).

[41] There is a dismissed case where the plaintiff argued that the defendant (DPP) was responsible for offering a safe space for secure transactions organized online in accordance with the principle of good faith that enables a court to find unusual misconduct in performance in breach of contract between consumer and DPP. The plaintiff alleged that DPPs had a duty to screen all the sellers aiming at validating their identity based on good faith and fair dealing (Tōkyō Chihō Saibansho [Tokyo Dist. Ct.] April 15, 2022, Rei 2 (wa) no. 27469, LEX/DB25572161 (Japan)).

[42] Giorgio Resta, "Digital platforms and the law: contested issues," Media Laws/ Rivista di Diritto dei Media (January 2018): 231(241-242).

[43] Antonios Karaiskos, "Liability of online platforms in Japan: An overview", *ZJapanR/J.Japan.L.* Bd. 24 Nr. 48 (2019): 57-69.

be considered to overcome the difficulties in formulating rules that effectively regulate online platforms.[44]

D. Conclusions

Even though the TFDPA and PCDPA set different goals and have different scopes of application in terms of targeted DPPs, they provide similar rules that work best for participation in committing to improving their trading environment collaboratively.

The rules include disclosure of terms and conditions of trading, promotion of mutual understanding in transactional relationships between DPPs and suppliers, and smooth communication between consumers and suppliers, including their identity confirmation and development of measures to protect consumers from misleading advertising and dispute settlement systems. In addition, they have a lot in common with rules in other jurisdictions that impose due diligence and disclosure requirements, such as the EU's Digital Service Act (DSA), SHOP SAFE Act (rejected), and the INFORM Consumer Act from the US.

Although those requirements are of an administrative nature in TFDPA and PCDPA, there have been national case laws to the effect that the violation of administrative requirements amounts to tort liability in certain circumstances. Likewise, although a DPP who presents itself to customers and suppliers as an intermediary in a prominent way is not liable for non-performance under supplier-customer contracts, it could be liable for damages caused by misleading information presented on the platform, if the DPP was notified about such content, and failed to take appropriate measures to remove or rectify it.

Moreover, the DPP might still be held jointly liable for the non-performance if the consumer can reasonably rely on the platform's influence on the supplier, as well as for damages caused to customers because of the misleading information given about suppliers, goods, services, or digital content offered by its users acting as suppliers, and for the specific warranties on their quality. ELI Model Rules on Online Platforms introduce these rules. An eminent professor of Consumer Law,

[44] As far as telecommunications are concerned, it should be mentioned that private entities play a large role in the rulemaking process. As a prominent example, in Japan, a private committee titled the "Provider Liability Limitation Act Guidelines Review Council" (hereinafter "the Council") establishes the "Guidelines" to specify a code of conduct for telecommunications service providers. The Guidelines provide for adequate measures that must be taken by service providers, and it is assumed that when the service providers follow the Guidelines, they will not be held liable under tort law. Indeed, the Guidelines are of private nature and are not legally binding, but it is nevertheless expected that the courts will take them into account when deciding whether there was "a reasonable ground" on the part of the service providers (Tomohiro Yoshimasa, "A theoretical perspective on the civil liability of online platform operators: Comment on Karaiskos", *ZJapanR/J.Japan.L.* Bd. 24 Nr. 48 (2019): 71 (75)).

Kunihiro Nakata, goes even further with his doctrine and posits that DPPs are primarily responsible for supplier non-performance based on platform service agreements concluded between DPPs and consumers. As a corollary, suppliers stay as a mere party assisting the performance of the obligations on the part of DPP, even if they are jointly responsible.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Numbers JP18K01224 and JP22KK0014.

Rediseñar el divorcio a partir del derecho procesal civil administrativo en la era digital

Arán García Sánchez, Oscar Pérez Carreto

A. Introducción

La presente investigación surge a partir del siguiente cuestionamiento ¿Cuál es la situación actual del proceso de divorcio administrativo en México en la era digital? lo anterior permite formularnos la siguiente hipótesis: El divorcio administrativo se puede rediseñar a partir del derecho procesal civil administrativo en la era digital, para dar respuesta a la hipótesis planteada, iniciamos con el estudio de los antecedentes histórico-jurídicos del divorcio en México, a partir de la consumación de la independencia en 1821. Iniciando con la codificación Oaxaqueña de 1827, pasando por algunas leyes de carácter federal de mediados del siglo XIX, hasta llegar a las codificaciones decimonónicas federales de 1870 y 1884,

Del mismo modo, se estudia el iter del divorcio en siglo XX, partiendo del estudio de las reformas carrancistas de los años veinte, continuando con la codificación civil de 1928, originaria del divorcio administrativo en mexicano. Asimismo, consideramos la multijurisdiccionalidad del divorcio como condición actual del divorcio y su consecuente tipología en el sistema jurídico mexicano, con base en la reforma del 3 de octubre de 2008, que permite por primera vez en nuestro país el divorcio incausado en la hoy Ciudad de México. Por último, se analiza la figura del divorcio administrativo en la era digital, considerando su situación estadística actual, seguido de su procedimiento y tramitología. Finalizando, con una propuesta de viabilidad tomando en consideración los índices de conectividad en México para la implementación del divorcio administrativo digital.

DOI: https://doi.org/10.17875/gup2023-2504

B. Antecedentes histórico-jurídicos del divorcio en el periodo decimonónico mexicano

I. Codificación civil oaxaqueña

En el presente apartado realizaremos un estudio jurídico legislativo del divorcio en México, a partir de las legislaciones decimonónicas mexicanas locales y federales.

Nuestro punto de partida es la legislación civil oaxaqueña de 1827, cuya jurisdicción era local. En dicha codificación se regula en su título sexto al divorcio del artículo 144 a 168. "Por divorcio se entiende la separación de marido y mujer, en cuanto al lecho y habitación, con autoridad del juez" (Soberano Congreso de Oaxaca 1828)[1], es decir, que el divorcio solo era por separación de cuerpos y no extingue el vínculo jurídico matrimonial, su tramitación era judicial y no administrativa. El artículo en cita en su parte final señalaba las clases de divorcio al señalar "Hay divorcio perpetuo y temporal[2]".

El divorcio perpetuo estaba basado en una causal sanción, partiendo de una conducta adúltera por parte de cualquiera de los cónyuges, dando la posibilidad de promoverlo.[3] El tribunal competente para conocer de la acción de divorcio perpetuo eran los tribunales eclesiásticos.[4]

El divorcio temporal era regulado por el artículo 162, y podía ser solicitado por los cónyuges con base en determinadas causales.[5]

II. Ley del matrimonio de 1859

Su principal incidencia en el divorcio fue que el matrimonio mutó de un sacramento religioso a un contrato civil, que se contrae lícita y válidamente ante la autoridad civil. Para su validez bastará que los contrayentes, previas las formalidades que

---

[1] Gobernador del Estado Libre de Oajaca (sic.), Código Civil Para Gobierno del Estado Libre de Oajaca (sic.), (Oaxaca: Imprenta del Gobierno, 1828), artículo 144, consultado el 10 de octubre de 2023, http://cdigital.dgb.uanl.mx/la/1190000714/1190000714_MA.PDF.

[2] Gobernador del Estado Libre de Oajaca (sic.), Código Civil Para Gobierno del Estado Libre de Oajaca (sic.), (n. 1).

[3] Gobernador del Estado Libre de Oajaca (sic.), Código Civil Para Gobierno del Estado Libre de Oajaca (sic.), (n. 1), artículo 145.

[4] Gobernador del Estado Libre de Oajaca (sic.), Código Civil Para Gobierno del Estado Libre de Oajaca (sic.), (n. 1), artículo 146.

[5] Gobernador del Estado Libre de Oajaca (sic.), Código Civil Para Gobierno del Estado Libre de Oajaca (sic.), (n. 1), artículo 162. *"Primero, porque uno de los consortes caiga en herejía o apostasía, en caso de convertirse en católico se termina la temporalidad del divorcio, ya que el otro cónyuge está obligado a reunirse nuevamente. Segundo, cuando la mujer tuviera temor de ser involucrada como cómplice en los actos criminales de su marido y estos le pudieran causar afectaciones en su vida, honor o sus bienes. Tercero, por locura o furor de uno de los consortes y que esto ponga en peligro la vida o genere un daño al otro consorte. Cuarto, por violencia física o moral consistente en crueldad, malos tratos y amenazas. La acción derivada de las causales antes mencionadas compete al varón y a la mujer".*

establece la ley, se presenten ante aquella y expresen libremente la voluntad de unirse en matrimonio.[6]

En cuanto al divorcio la ley del matrimonio contemplaba el divorcio temporal y en su artículo 4° señalaba la indisolubilidad del matrimonio, la única forma de disolver el matrimonio era de forma natural a partir de la muerte de uno de los cónyuges, pero los casados podrían separarse temporalmente (divorcio temporal), con base en VII causas expresadas en su artículo 21.[7]

III. Código civil de 1870 y 1884

En la codificación civil de 1870, el matrimonio conserva la indisolubilidad, tal y como lo señala su artículo 159 al señalar: "El matrimonio es la sociedad legítima de un solo hombre y una sola mujer, que se unen en vínculo indisoluble para perpetuar su especie y ayudarse a llevar el peso de la vida"[8] Por lo tanto, la ley en comento regula en los artículos 239 al 279, al divorcio por separación de cuerpos y este puede ser necesario o voluntario.

El divorcio necesario tiene 7 causales al igual que las establecidas en la Ley de matrimonio de 1859, que varían en cuanto a su redacción.[9] El voluntario se establece en el artículo 246 al señalar*: "Cuando ambos consortes convengan en divorciarse en cuanto al lecho y habitación, no podrán verificarlo sino ocurriendo por escrito al juez…en caso contrario, aunque vivan separados, se tendrán como unidos para todos los efectos legales del matrimonio.*[10] Lo anterior nos permite distinguir una separación de hecho y otra de derecho derivada del escrito de demanda presentado al juez. Además, debían acompañar a su demanda una escritura, derivada de un convenio, respecto a la situación de los hijos y la administración para el periodo de separación.[11]

Por lo tanto, en la codificación en comento los divorcios eran judiciales y se dividían en necesarios y voluntarios.

---

[6] Fernando Serrano Migallón, *150 años de Las Leyes de Reforma, 1859-2009* (México, D.F.: Instituto de Investigaciones Jurídicas UNAM, 2009).

[7] *"Artículo 21.- en ellas encontramos las siguientes causales legítimas: I. El adulterio, II. La acusación de adulterio hecha entre los cónyuges y no probada en juicio, III. El acto sexual con la mujer, que atente contra el fin esencial del matrimonio, IV. La inducción a la comisión de un crimen, V. La crueldad excesiva. VI. La enfermedad grave y contagiosa, VII. La demencia de uno de los cónyuges. La separación derivada de las causales antes mencionadas no da la posibilidad de casarse con otras personas".*

[8] México, *Código Civil de 1870*, artículo 159, consultado el 10 de octubre de 2023, https://catalogo.iib.unam.mx/F/9QEFU3SU5F3UH2NM8821E2LQEBK22HX6JBRSQAIFUFDMT24PIG-00437?func=full-set-set&set_number=025996&set_entry=000014&format=040.

[9] *"1° El adulterio, 2° La incitación del marido para prostituir a su mujer, 3° La incitación o la violencia hecha por un cónyuge para cometer algún delito, 4° El conato para corromper a los hijos, 5° El abandono injustificado del domicilio conyugal por más de dos años, 6° La sevicia entre los cónyuges, 7°La acusación falsa entre cónyuges".*

[10] Ley de Matrimonio de 1859, artículo 246.

[11] Ley de Matrimonio de 1859, artículo 248.

La codificación de 1884 en su artículo 226 [12] al igual que la de 1870, sigue preservando la indisolubilidad del matrimonio. En cuanto al divorcio, conserva el divorcio necesario[13] y el voluntario.[14] La principal diferencia radica en el incremento del número de causales pasando de 7 que contemplaba la codificación de 1870 a 13, en la última de ellas contempla el mutuo consentimiento.[15] En la presente codificación no fue reconocido el divorcio administrativo.

C. El divorcio en el siglo XX en México.

I. Ley sobre el divorcio

El 29 de diciembre de 1914, fue expedida por Venustiano Carranza, encargado del Poder Ejecutivo Federal a través de un decreto.

Consistente, en reformar la fracción IX del artículo 23 de la Ley de 14 de diciembre de 1874, reglamentaria de las adiciones y reformas de la Constitución Federal decretadas el 25 de diciembre de 1873 que señalaba:

> "*El matrimonio civil no se disolverá más que por la muerte de uno de los cónyuges; pero las leyes pueden admitir la separación temporal por causas graves que serán determinadas por el legislador, sin que por la separación quede hábil ninguno de los consortes para unirse con otra persona".*[16]

La reforma permitió que, por primera vez en México, el divorcio disolviera el vínculo jurídico matrimonial, dejando a los cónyuges en aptitud de contraer nuevas nupcias e incluyendo como clases de divorcios el derivado del mutuo consentimiento de los cónyuges y el necesario para quedar de la siguiente manera:

> *"El matrimonio podrá disolverse en cuanto al vínculo, ya sea por el mutuo y libre consentimiento de los cónyuges cuando el matrimonio tenga más de tres años de celebrado, o en cualquier tiempo por causas que hagan imposible o indebida la realización de los fines del matrimonio, o por faltas graves de alguno de los cónyuges, que hagan irreparable la desavenencia conyugal. Disuelto el matrimonio, los cónyuges pueden contraer una nueva unión legítima*."[17]

---

[12] Código Civil (CC) de 1884, artículo 226

[13] CC 1884 (n. 12), artículo 227.

[14] CC 1884 (n. 12), artículo 231.

[15] CC 1884 (n. 12), artículo 227.

[16] Memoria Política de México, "1874 Sobre leyes de Reforma. Decreto del Congreso 14 de diciembre de 1874", Edición Perenne 2023, Selección de textos y documentos; Doralicia Carmona Dávila (2005), consultado el 10 de octubre de 2023, https://www.memoriapoliticademexico.org/Textos/5RepDictadura/1874LRD.html.

[17] Oscar Cruz Barney, *Derecho Privado y Revolución Mexicana* (México, D.F.: Instituto de Investigaciones Jurídicas de la UNAM, 2016), p.169, consultado el 10 de octubre de 2023.

II. Ley sobre relaciones familiares

La ley sobre relaciones familiares de fecha 9 de abril de 1917, al igual que la ley sobre el divorcio forman parte de un conjunto de leyes pertenecientes al periodo carrancista de la revolución mexicana.

Su ámbito espacial de validez fue el Distrito Federal y los territorios federales. Por lo tanto, las entidades federativas tenían la potestad de legislar en materia familiar. Su objetivo fue separar las relaciones jurídicas familiares reguladas en el Código Civil de 1884.

La ley consideraba al matrimonio disoluble al señalar: *"El matrimonio es un contrato civil entre un solo hombre y una sola mujer, que se unen con vínculo disoluble para perpetuar su especie y ayudarse a llevar el peso de la vida"*[18] En consecuencia, el artículo 75 de la ley señala: *"El divorcio disuelve el vínculo del matrimonio y deja a los cónyuges en aptitud de contraer otro".* Al mismo tiempo establece en su artículo 76, fracción XII, las causales de divorcio, las primeras XI, son causales de divorcio necesario y la XII, contempla el divorcio por mutuo consentimiento.

III. Código Civil de 1928

El Código Civil para el Distrito y Territorios Federales en Materia Común, y para toda la República en Materia Federal de 1928, promulgado el 30 de agosto del mismo año, incorpora nuevamente el derecho de las familias y sus relaciones jurídicas que habían sido separadas del código de 1870 a través de la Ley sobre relaciones familiares. Su ámbito espacial de validez lo deducimos de su denominación, es decir, federal para los territorios federales.

La codificación en comento sigue preservando al divorcio como disoluble en su artículo 266, fracción XVII del artículo siguiente contempla el mutuo consentimiento de los cónyuges para divorciarse, es decir, divorcio voluntario. (México 1928)[19]

Lo novedoso en cuanto al divorcio, es la incorporación del divorcio administrativo en su artículo 272 al señalar: "Cuando ambos consortes convengan en divorciarse y sean mayores de edad, no tengan hijos y de común acuerdo hubieren liquidado la sociedad conyugal, si bajo ese régimen se casaron, se presentarán personalmente ante el Oficial del Registro Civil del lugar de su domicilio; comprobarán con las copias certificadas respectivas que son casados y mayores de edad, y manifestarán de una manera terminante y explícita la voluntad de divorciarse"[20]

Después de expresar la voluntad de divorciarse, y previa identificación, se levantará un acta haciendo constar la solicitud y el Oficial del Registro Civil, citará a los cónyuges a su ratificación en los próximos quince días.

---

[18] Secretaría de Estado, Ley sobre relaciones familiares (México, 1917), artículo 13, 15, consultado el 10 de octubre de 2023, https://www.constitucion1917-2017.pjf.gob.mx/sites/default/files/venustianocarranza/archivos/Leysobrerelacionesfamiliares1917.pdf.

[19] Secretaría de Estado, Ley sobre relaciones familiares, (n. 18), artículo 266.

[20] Secretaría de Estado, Ley sobre relaciones familiares, (n. 18), artículo 272.

Una vez terminado el desarrollo histórico de divorcio en las legislaciones mexicanas desde la codificación civil oaxaqueña de 1827, hasta la aparición del divorcio incausado en la codificación civil de 1928. Ahora es pertinente pasar al análisis del divorcio administrativo y su procedimiento.

D. Tipología del divorcio en México

I. Situación actual del divorcio

En México, el divorcio es regulado por una multijurisdiccionalidad, conformada por 33 legislaciones sustantivas y adjetivas civiles. Una con jurisdicción federal y el resto con jurisdicción local.

En el presente siglo la última reforma relacionada con el divorcio fue el 3 de octubre de 2008. En ella el Distrito Federal, hoy Ciudad de México, decreta la posibilidad de divorciarse por la vía judicial sin señalar ninguna causal, generando la posibilidad de solicitar el divorcio por uno cónyuges (unilateral) o por ambos (bilateral). Además, de preservar al divorcio voluntario administrativo. Lo anterior permite observar los distintos tipos de divorcio en el Sistema Jurídico Mexicano.

II. Tipología del divorcio en México

En México, existe una falta de coincidencia legislativa en cuanto a los tipos divorcio, un ejemplo de ello es el Código Civil Federal que en su artículo 267, sigue regulando al divorcio necesario con XX causales a pesar de que eso vulnera el libre desarrollo de la personalidad. Dicha situación ya ha sido declarada inconstitucional por parte de la Suprema Corte de Justicia de la Nación.[21]

Es por ello por lo que, para referirnos a los tipos de divorcio en México, basamos el estudio en la legislación civil de la Ciudad de México, en ella se establece un sistema de divorcio: "vincular y separación de cuerpos. Sólo que el divorcio vincular ahora puede tramitarse en forma administrativa, o a través del divorcio denominado expedito o sin causa".[22] En lo particular considero que la separación de cuerpos es una medida garantista en favor de los cónyuges y no un tipo de divorcio.

El divorcio administrativo es uno de los subtipos de divorcios vinculares previstos por las codificaciones civiles de nuestro país, su fuente es la voluntad de las partes. Además, intervienen el Registro Civil o el notariado en algunos estados del país.

---

[21] Suprema Corte de Justicia de la Nación, Contradicción de tesis 73/2014 (México, 2014), 41, consultado el 10 de octubre de 2023, https://www.sitios.scjn.gob.mx/cec/sites/default/files/page/files/2020-09/CT%2073%202014%20V.%20P%C3%BAblica%20Inconstitucionalidad%20Divorcio%20Necesario.pdf.

[22] Guzmán Ávalos, Aníbal y Valdés Martínez, María del Carmen, "Del matrimonio indisoluble al divorcio exprés del Distrito Federal," *Revista IUS*, (2012): 77 (83), consultado el 10 de octubre de 2023, https://www.revistaius.com/index.php/ius/article/view/56/51.

Sus requisitos son: no tener necesidad alimentaria entre cónyuges, en caso de estar casado bajo el régimen de sociedad conyugal haberla liquidado, que la cónyuge no esté embarazada, no tener hijos en común, de ser así que sean mayores de edad y que no tengan necesidad de recibir alimentos, para continuar el estudio del presente trabajo de investigación es necesario reflexionar sobre procedimiento civil administrativo para divorciarse y relación con el orden de la realidad tecnológica.

E. El divorcio administrativo en la era digital

I. Situación actual del divorcio administrativo

Como bien se ha señalado en los párrafos anteriores, el divorcio administrativo es la disolución del vínculo matrimonial, mediante un procedimiento que se sigue ante una autoridad administrativa y no de carácter judicial.

De igual manera resulta de suma importancia conocer la situación actual en México, para ello, es necesario hacer referencia a lo que establece la base de datos statista, en cuanto número de divorcios que se tramitan bajo la figura del divorcio administrativo, refiere que, en el año 2018, en México aproximadamente acontecieron 14,000 divorcios. (Statista 2023)

Una vez hecha la referencia anterior, es preciso señalar la relación entre la figura del matrimonio y el divorcio en México, a lo que en la estadística del año 2021 realizada por el Instituto Nacional de Estadística y Geografía (INEGI), resulta que el número de matrimonios celebrados asciende a la cantidad de 453,085 y el número de divorcios a la cantidad de 149,674 (INEGI 2022)[23]. De lo que, del número de divorcios registrados, 90% corresponde a divorcios tramitados en la vía judicial, y el 10%, es decir, 15,012 fueron mediante la vía administrativa. (INEGI 2022)[24]

Ahora bien, una vez que se han establecido las cifras derivadas del procedimiento del divorcio administrativo, cabe señalar, el procedimiento y los requisitos para la realización de este procedimiento civil administrativo, con base en la legislación del Distrito Federal.

II. El divorcio y su procedimiento civil administrativo

El divorcio administrativo encuentra su fundamento jurídico en el artículo 272 del Código Civil para el Distrito Federal[25], del cual se desprende que el procedimiento

[23] INEGI, Comunicado de prensa núm. 561/22 (México, 2022), 09, consultado el 10 de octubre de 2023, https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/EstDiv/Divorcios2021.pdf.

[24] INEGI, (n. 23).

[25] Congreso de la Ciudad de México, Código civil para el Distrito Federal, *"Artículo 272.- Procede el divorcio administrativo cuando ambos cónyuges convengan en divorciarse, hayan liquidado la sociedad conyugal de bienes, si están casados bajo ese régimen patrimonial, la cónyuge no esté embarazada, no tengan hijos en común o*

se realiza directamente ante el Juez del Registro Civil, quien para efectos de la presente investigación no funge como una autoridad judicial, sino que es una autoridad de carácter administrativo, para ello cabe precisar que el Reglamento del Registro Civil del Distrito Federal lo define así como establece de forma clara y precisa que la organización, funciones y procedimientos del Registro Civil del Distrito Federal, estarán a cargo de la Administración Pública Federal.[26]

Cómo se puede observar, corresponde al registro civil un procedimiento administrativo civil, puesto que de su misma esencia se desprende que será la autoridad encargada de realizar la inscripción de las resoluciones y sentencias judiciales que la ley autoriza, es decir, los procedimientos tramitados en la vía judicial, toda vez que del mismo reglamento se desprende que para que surtan efectos dichas resoluciones o sentencias, deben de ser inscritas ante el registro civil, lo cual corresponde a un procedimiento completamente diferente al judicial.

En esencia se puede ver a todas luces que, el divorcio administrativo, al ser tramitado ante el juez del registro civil, tal y como lo establece el artículo 76 del Reglamento del Registro Civil del Distrito Federal, el mismo se podría considerar como un procedimiento administrativo civil, al tramitarse ante dicha dependencia perteneciente a la administración pública.

Dicho procedimiento civil administrativo, deberá tramitarse ante el registro civil, que sigue una serie de requisitos a cumplir[27] desde el llenado de un formato de solicitud, el anexar los datos del acta de matrimonio, así como identificación oficial de los solicitantes, acompañado la protesta de ser mayores de edad, requisito indispensable también referido en el artículo 76 del Reglamento del Registro Civil del Distrito Federal, así como el formato de solicitud debidamente firmado[28].

---

teniéndolos sean mayores de edad, y éstos no requieran alimentos o alguno de los cónyuges. El Juez del Registro Civil, previa identificación de los cónyuges, y ratificando en el mismo acto la solicitud de divorcio, levantará un acta en que los declarará divorciados y hará la anotación correspondiente en la del matrimonio anterior", consultado el 10 de octubre de 2023, https://www.congresocdmx.gob.mx/media/documentos/ad63a5bd2aef33e50ef1ed68d82450cf368578c0.pdf.

[26] Jefe de Gobierno del Distrito Federal, Reglamento del Registro Civil del Distrito Federal, (México, 2022), "Artículo 1.- Las disposiciones del presente ordenamiento son de orden público e interés social y tienen por objeto regular la organización, funciones y procedimientos del Registro Civil del Distrito Federal, a cargo de la Administración Pública del Distrito Federal. El Registro Civil es la Institución de buena fe, cuya función pública es conocer, autorizar, inscribir, resguardar y dar constancia de los hechos y actos del estado civil de las personas, que dispone el Código Civil para el Distrito Federal, con legalidad, honradez, lealtad, imparcialidad y eficiencia, por conducto de los Jueces del Registro Civil, debidamente autorizados para dichos fines", consultado el 10 de octubre de 2023, http://cgservicios.df.gob.mx/prontuario/vigente/5506.htm.

[27] Consejería Jurídica y Servicios Legales del DF, Divorcio Administrativo Requisitos, (México) consultado el 10 de octubre de 2023, https://data.consejeria.cdmx.gob.mx/index.php/component/content/article/285-micrositio-direccion-registro-civil/plecas-secciones-dgrc/1077-divorcio-administrativo.

[28] Gobierno de la Ciudad de México, Registro de Actos del Estado civil de las Personas (Divorcio Administrativo – Sociedad Conyugal) (México) consultado el 10 de octubre de 2023, https://registrodetramites.cdmx.gob.mx/statics/formatos/TCEJUR-DGRC_RAD_3.pdf.

El procedimiento civil administrativo del divorcio ante el Registro Civil de la Ciudad de México, del mismo se puede observar que se trata de un trámite que debe de ser presentado de manera física, lo cual se vuelve un problema para las personas que no radican en el país y tienen el interés de disolver el vínculo matrimonial. Aunado lo anterior, el artículo 76 del multicitado Reglamento, sólo establece un supuesto para el caso de que los solicitantes no pudiesen comparecer de manera personal, de cual establece que dicho trámite podrá ser realizado por un mandatario expreso, pero con la condicionante de que dicho mandato sea otorgado ante Notario Público.

Dicho precepto, ha sido rebasado por la realidad, tan es así que la mayoría de las personas que en su voluntad deseen realizar el trámite y las mismas ya no residen dentro del país se vuelve un gran problema, por lo que, para efectos de la presente investigación, el procedimiento debería poderse realizar en línea.

Lo anterior no resulta ajeno al sistema jurídico mexicano, ya que para la realización de diversos trámites o procedimientos judiciales, las solicitudes pueden ser firmadas de manera electrónica mediante la conocida e.firma, como lo es el trámite de la cédula profesional, dicha firma electrónica es tramitada ante el Sistema de Administración Tributaria. De igual manera los organismos judiciales como lo son el Poder Judicial de la Federación y el Poder Judicial de la Ciudad de México, ha gestionado la obtención de la Firma electrónica para los procedimientos judiciales, expedida por dichos organismos.

Para el caso de la firma electrónica expedida por las autoridades judiciales, las mismas pueden ser tramitadas en línea, sin la necesidad de que el solicitante acuda a las instalaciones de dichos organismos. Para el caso de la firma electrónica que expide el Poder Judicial de la Ciudad de México, dicho trámite puede ser iniciado de manera electrónica en el portal de internet[29], así como la tramitación de la firma digital por parte del poder judicial de la federación, la cual también puede ser tramitada vía internet.[30]

Con la referida firma electrónica, se pueden iniciar los procedimientos judiciales ante dichas autoridades, sin la necesidad de que el solicitante acuda, por lo que resulta viable que, dentro del Registro Civil del Distrito Federal, o de cualquier entidad federativa, puedan implementar la firma de las solicitudes mediante esta herramienta y así poder dar un mejor servicio y garantizar los derechos de todos sus usuarios.

[29] Firma Judicial Electrónica del Poder Judicial de la CDMX (México), consultado el 10 de octubre de 2023, https://firmajudicial.poderjudicialcdmx.gob.mx/.

[30] Poder Judicial de la Federación, Solicitud de un certificado digital de firma electrónica (FIREL), (México, 2023), consultado el 10 de octubre de 2023, https://www.firel.pjf.gob.mx/peticion_certificado.aspx.

III. La tramitología en México

Ahora bien, como se ha señalado en los párrafos anteriores, el divorcio administrativo, podría ser considerado como un trámite, toda vez que como se ha referido en los párrafos anteriores, el mismo se tramita ante una dependencia que no es de carácter judicial, por lo que se debe precisar el concepto de trámite, el cual para la Real Academia Española lo define como *"Cada uno de los pasos y diligencias que hay que recorrer en un asunto hasta su conclusión"*[31].

La definición de trámite conforme a lo que establecen Roseth, Reyes y Farías, un trámite es:

> *"el conjunto de requisitos, pasos o acciones a través de los cuales los individuos o las empresas piden o entregan información a una entidad pública, con el fin de obtener un derecho generación de un registro, acceso a un servicio, obtención de un permiso o para cumplir con una obligación".*[32]

De igual manera, cabe hacer la precisión de que el estado mexicano, al igual que Brasil y Uruguay, ofrecen más del 50% de que los trámites a realizarse se comienzan en la vía electrónica, siendo que los trámites a realizar se encuentran contemplados en el Catálogo Nacional de Regulaciones Trámites y Servicios.[33]

Ahora bien, hasta el año 2017, en México tal y como lo refiere el Catálogo Nacional de Regulaciones Trámites y Servicios, se tenían un total de 2,708 trámites que podían ser iniciados mediante la vía electrónica, siendo que solo el 74% de estos pueden ser concluidos mediante la misma vía.

Como bien se ha mencionado a lo largo de la presente investigación, el trámite en línea dejó de ser un privilegio y se ha convertido en una necesidad para todas y cada una de las personas que desean agilizar sus trámites, Derivado de lo que antecede, resulta importante traer a colación el tiempo promedio que ocupa un mexicano en realizar un trámite, el cual asciende a 6.9 horas[34], lo cual equivale casi al total de la jornada laboral en México establecida en el artículo 61[35] de la Ley Federal del Trabajo, el cual establece que la jornada máxima será de 08 horas. Por

---

[31] DRAE, 2023.

[32] Benjamín Roseth, Angela Reyes y Pedro Farías, *El Fin del Trámite Eterno*, ed. Benjamín Roseth, Angela Reyes y Carlos Santiso (Washington D.C.: Editorial BID, 2018), 36, consultado el 10 de octubre de 2023, https://publications.iadb.org/publications/spanish/viewer/El-fin-del-tr%C3%A1mite-eterno-Ciudadanos-burocracia-y-gobierno-digital.pdf.

[33] Comisión Nacional de Mejora Regulatoria, El Catálogo Nacional de trámites, servicios, inspecciones y regulaciones de todo México, (México 2023), consultado del 10 de octubre de 2023, https://catalogonacional.gob.mx/Home.

[34] Roseth, Reyes y Santiso, (n. 32) 19.

[35] Cámara de Diputados del H. Congreso de la Unión, Ley Federal del Trabajo, 2022, México, artículo 61. La duración máxima de la jornada será: ocho horas la diurna, siete la nocturna y siete horas y media la mixta, consultado el 10 de octubre de 2023, https://www.diputados.gob.mx/LeyesBiblio/pdf/LFT.pdf.

lo que en consecuencia se puede dilucidar que un mexicano para la realización de un trámite tiene que ausentarse un día entero de trabajo para la gestión de este, lo cual puede convertirse en consecuencias económicas para el mismo.

En ese orden de ideas, el trámite electrónico resulta muy factible y eficaz en el estado mexicano, ya que como bien se ha referido, ya se ha implementado el trámite en línea que puede ser concluido mediante la misma vía, por lo que resultaría factible que el trámite del procedimiento civil administrativo de divorcio sea realizado en línea.

Otro de los problemas que se podría dilucidar del trámite en línea, lo es la conectividad, o acceso a internet, para lo cual, el Gobierno Federal, mediante el Plan Nacional de Desarrollo 2019-2024, específicamente en su punto número 3 dedicado al rubro de economía una de las metas del sexenio actual es la cobertura de internet para todo el país[36].[37].

IV. Conectividad en México

La propuesta encuentra su viabilidad, con base en la conectividad con la que cuenta el país actualmente y su prospectiva para el año 2026. La información más reciente señala que el 67% de la población mexicana tiene acceso a internet y se pronostica que para el año 2026 será un 71%. (Statista 2023). Otra referencia en el mismo sentido señaló que en 2020, 84.1 millones de la población mexicana eran usuarios de internet lo que representaba el 72% de la población a partir de los seis años y que los tres medios para la conexión a internet fueron: los smartphones con un 96%, las computadoras portátiles con 33% y con un 22.2 % a través de televisiones con acceso a internet. El objetivo principal del universo de usuarios a internet en 2020 fue comunicarse con un 93.8%, búsqueda de información 91% y acceso a redes sociales 89%.[38] Lo anterior sustenta que hay altas posibilidades de que, en México, se pueda realizar el proceso civil administrativo en línea como otros trámites.

F. Conclusión

Se ha podido analizar el desarrollo y evolución jurídico-histórica del vínculo matrimonial, así como su procedimiento para disolverse vía divorcio, concluyendo que su evolución en nuestro país ha sido conforme a la época en la que se vive como sociedad, considerando al matrimonio y al divorcio como instituciones jurídicas dúctiles, conforme a las problemáticas y necesidades del orden de la realidad.

---

[36] Secretaría de Gobernación, PLAN Nacional de Desarrollo 2019-2024 (México 2019), consultado el 10 de octubre de 2023, https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019#gsc.tab=0.

[37] Secretaría de Gobernación, 2019.

[38] INEGI, Comunicado de prensa núm. 352/21 (México, 2021), 07, consultado el 10 de octubre de 2023, https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf.

En cuanto a la longevidad del divorcio administrativo, se pensaría idéntica a la del matrimonio en México, pero no es así, su antigüedad es menor a un siglo, y su finalidad es extinguir el matrimonio sobre bases de un proceso civil administrativo ante el Registro Civil de las Personas, con requisitos que impidan vulnerar otras relaciones jurídicas familiares.

De manera que la situación actual del divorcio en general y en lo particular el administrativo en México, es compleja al estar tipificado y regulado por 32 legislaciones locales, una de índole federal, conformando la multijurisdiccionalidad del proceso civil administrativo para divorciarse. Dicho lo anterior, en el país, se generó una tipología diversa del divorcio en las entidades federativas al considerar la reforma de divorcio incausado de 3 de octubre de 2008 en la hoy Ciudad de México.

En suma, es importante señalar que en la actualidad resulta complejo y tardado realizar un trámite en México, conllevando a sufrir pérdida de tiempo, económicas, desidia para los usuarios en la realización de dichos trámites, lo anterior justifica el procedimiento civil administrativo de divorcio en la era digital, para las personas que deseen realizarlo, ya sea porque se han visto limitadas por situaciones personales o profesionales, o por no radicar dentro del territorio nacional.

Finalmente, su viabilidad es amplia y encuentra justificación ya que en la actualidad 67% de la población mexicana tiene acceso a internet y se pronostica que para el año 2026 será un 71%. Otra incidencia en la justificación, son los diversos elementos de firma electrónica, por lo que dichos procedimientos civiles administrativos, pueden ser solicitados en la plataforma que se habilite, y de igual manera que en un procedimiento judicial, quede estampada la voluntad de los solicitantes mediante la firma electrónica en el trámite del divorcio administrativo en línea.

Opportunities and Challenges of Digital Music

Olufunmilayo B. Arewa

A. Music in the Digital Era

I. Digital Era Challenges for the Recording Industry

The music industry has experienced significant opportunities and challenges in the transition to the digital era. The music industry was the first of the cultural industries to confront and experience the full impact of the digital era.[1] It has had one of the most difficult transitions to digital era economic, business, and cultural realities.[2] Changing technologies, particularly the introduction of compressed digital music files and the Internet, have enabled widespread dissemination of digital music and many uncompensated and unauthorized uses of digital music content.[3] The appearance of digital music downloads and later dominance of streamed music reflect new iterations of a familiar pattern in music and other creative industry sectors of new technologies challenging existing business models, artistic practices, and legal

[1] Simon Frith and Lee Marshall, «Making Sense of Copyright» in *Music and Copyright,* ed. Simon Frith, Lee Marshall., 2d edn. (New York: Routledge, 2004), 1, 3.
[2] Hugh McIntyre, "What Exactly Is Stream-Ripping, The New Way People Are Stealing Music", *Forbes* (August 11, 2017), accessed October 24, 2023, https://www.forbes.com/sites/hughmcintyre/2017/08/11/what-exactly-is-stream-ripping-the-new-way-people-are-stealing-music/.
[3] Olufunmilayo B. Arewa, "YouTube, UGC, and Digital Music: Competing Business and Cultural Models in the Internet Age," *Northwestern University Law Review* (2010): 431 (440).

DOI: https://doi.org/10.17875/gup2023-2505

frameworks. Challenges to music in the digital era bear similarities to past eras, including earlier in the twentieth century, when the advent of records, player pianos, and other new technologies posed a significant challenge to existing legal, institutional, and business arrangements.

The creative industries have used key aspects of pre-digital era business models well into the digital era. Industry contracting practices with artists reflect the impact of pre-digital era business models that continue to be core features in digital era contexts. The music industry transition to the digital era has led to the emergence of new intermediaries, including YouTube,[4] Apple Music,[5] and Spotify, the latter of which has become an important force in streaming, with a dominant market share combined with uneven financial performance.[6] More recently, TikTok, a destination for short-form mobile videos,[7] has become a major music industry player.[8] Although new technologies have been a core factor in digital era disruption in music, contractual arrangements with recording artists have continued to be largely based on pre-digital models.[9]

In recent years, a broad range of artists have drawn attention to their not receiving a fair share of industry revenues.[10] Disputes about proceeds from streaming

[4] Jean-Samuel Beuscart, Samuel Coavoux and Jean-Baptiste Garrocq, "Listening to Music Videos on YouTube. Digital Consumption Practices and the Environmental Impact of Streaming," *Journal of Consumer Culture,* 23 (2023): 654 (667).

[5] Dan Gallagher, "Apple Faces the Music", *Wall Street Journal* (April 18, 2018), accessed November 14, 2023, https://www.wsj.com/articles/apple-faces-the-music-1524043801.

[6] Joan E. Solsman, "Spotify Eclipses 205 Million Paid Subscribers, Better Than Predicted", *CNet.com*, (January 31, 2023), accessed October 24, 2023, ; Manuel Paul Dipold, "Spotify's Future Financial Performance Is Too Much Of A Guessing Game*", SeekingAlpha.com,* (January 13, 2023),accessed October 24, 2023; Ashley Kapoot, "Spotify Shares Fall 14% on Revenue Miss and Weak Guidance", *CNBC.com*, (Jul. 25, 2023), accessed October 24, 2023, https://www.cnbc.com/2023/07/25/spotify-spot-earnings-.html.

[7] Our Mission, "TikTok", accessed October 24, 2023, https://www.tiktok.com/about?lang=en; D. Bondy Valdovinos Kaye, Jing Zeng and Patrik Wikstrom, *TikTok: Creativity and Culture in Short Video* (Cambridge: Polity, 2022).

[8] "TikTok's Effect on the Music Industry", *Quartz.com*, (February 24, 2021), accessed October 24 2023, https://qz.com/1974505/tiktoks-effect-on-the-music-industry; Elias Leight, "'If You Can Get Famous Easily, You're Gonna Do It': How TikTok Took Over Music"*, Rolling Stone*, (August 12, 2019), accessed October 24, 2023, https://www.rollingstone.com/pro/features/tiktok-video-app-growth-867587/.

[9] Olufunmilayo Arewa and Matt Stahl, "Prospecting Sharecropping, and the Recording Industry," *Vanderbilt Journal of Entertainment and Technology Law,* 25, (2023): 267, (267-268).

[10] Ben Sisario, "Musicians Say Streaming Doesn't Pay. Can the Industry Change?", *N.Y. Times*, (May 10, 2021), accessed October 24, 2023, https://www.nytimes.com/2021/05/07/arts/music/streaming-music-payments.html.

have intensified as recording industry revenues have rebounded in recent years.[11] Although some have discussed modifying underlying payment models in the streaming era,[12] contestation about artists receiving a fair share has often focused on payments received by artists for streaming rather than the typically disadvantageous contracting norms upon which such payments are based:

> "*Is music streaming bad for musicians? It may well be the case that more musicians rather than fewer can now earn money from recorded music. But it seems clear that the current system retains the striking inequalities and generally poor working conditions that its predecessors. Public debate would benefit from more careful formulation of critique and consideration of evidence – which might well depend upon MSS and music-industry businesses being more open and transparent about usage and payments. Nevertheless, it is surely a good thing that issues of justice and fairness regarding musicians are now so widely aired, and reform is being actively discussed."*[13]

Contention about streaming is not limited to the music industry. In 2023, a series of strikes in Hollywood drew attention to deep contestation about the distribution of entertainment industry benefits from streaming.[14] The advent of streaming in music initially reduced levels of unauthorized uses.[15] However, recent technologies continue to offer opportunities for varied unauthorized uses, including through practices such as stream ripping,[16] which nables people to download streams.[17] By

---

[11] Sisario (n 10); Manatt, Phelps & Phillips, LLP, "U.S. Music Streaming Royalties Explained", (2016), accessed October 24, 2023, https://www.manatt.com/Manatt/media/Media/PDF/US-Streaming-Royalties-Explained.pdf.

[12] Anna Nicolaou, "Universal Music in Talks with Big Platforms to Overhaul Streaming Model", *Financial Times*, (January 31, 2023), accessed October 24, 2023, https://www.ft.com/content/d20ee15d-cbdb-46d9-a7c5-264617e96c72.

[13] Desmond Hesmondhalgh, D., "Is Music Streaming Bad for Musicians? Problems of Evidence and Argument," *New Media & Society,* 23 (2021): 3593 (3610).

[14] Katie Campione, "Inside The Battle For A New Streaming Residuals Model: Data, Transparency & A Fight For Power", *Deadline*, (July 27, 2023), accessed October 24, 2023, https://deadline.com/2023/07/hollywood-strikes-streaming-residuals-fight-actors-writers-1235448649/; Joe Flint and Amol Sharma, "Streaming Brought Hollywood to a Standstill. Now Comes the Pain", *Wall Street Journal* (July 21, 2023), accessed October 24, 2023, https://www.wsj.com/articles/streaming-brought-hollywood-to-a-standstill-now-comes-the-pain-3afcbb68.

[15] Andre Paine, ""Spotify has everything": Piracy Drops as Streaming Wins over Illegal Downloaders", *MusicWeek*, (August 2, 2018), accessed October 24, 2023, https://www.musicweek.com/digital/read/spotify-has-everything-piracy-drops-as-streaming-wins-over-illegal-downloaders/073373.

[16] Eriq Gardner, "Stream-Ripping Is Next Frontier for Piracy Wars", *Hollywood Reporter* , (December 4, 2020), accessed October 24, 2023, https://www.hollywoodreporter.com/business/business-news/stream-ripping-is-next-frontier-for-piracy-wars-4099909/

[17] Disputes about the legality of technologies that facilitate downloads of streams have tended to follow familiar patterns from past digital era debates. Gardner, (n 16); Letter from Mitchell L. Stoltz, Senior Staff Attorney, Electronic Frontier Foundation to GitHub DMCA Agent, dated (November

2022, visits to music pirate websites were again increasing.[18] Such recent technologies also may also offer opportunities for new forms of manipulation. Although manipulation of industry metrics is a longstanding issue,[19] streaming has offered opportunities for various forms of fraud and manipulation.[20]

Creative industry businesses in the United States have also long played a role in the development of intellectual property laws and enforcement strategies.[21] The intellectual property frameworks put in place in the pre-digital era have been stressed significantly in the digital era, particularly with respect to unauthorized distribution of digital content, which posed a particular challenge prior to the advent of streaming. Although such unauthorized distribution is often referred to as "piracy," the topography of unauthorized uses may be both complex and multifaceted. How content should be accessed, consumed, and used in the digital era remains a focal point of a major digital era divide.

Digital era divides are not always clearly demarcated or uniformly experienced. As a result, an array of technologies and methods for owning, accessing, consuming, and using content has become increasingly evident. The digital era draws attention to the complexities of copyright, particularly as applied to music. As the business fortunes of some participants in the creative industries waned in the early digital era, many industry players sought to bolster their business fortunes through reliance on copyright law enforcement. This focus on copyright law has influenced legislative activity and copyright lawmaking.

Digital era events highlight continuing conflicts about how creative works should be produced, consumed, and disseminated in varied contexts and geographic locations. These events also underscore changing cultural, artistic, and business norms and practices that underlie the pervasive contestation that has come to characterize significant portions of digital life. Full understanding of such disputes requires bottom-up understanding of changing cultural and business practices and

15, 2020), accessed October 24, 2023, https://github.com/github/dmca/blob/master/2020/11/2020-11-16-RIAA-reversal-effletter.pdf.

[18] Elias Leight, "Music Piracy Is Rising — And the U.S. Is a Trouble Spot", *Billboard*, (March 9, 2023), accessed October 24, 2023, https://www.billboard.com/pro/music-piracy-2022-stream-ripping/.

[19] Neil Strauss, "Are Pop Charts Manipulated?"*, N.Y. Times*, (January 25, 1996), accessed October 24, 2023, https://www.nytimes.com/1996/01/25/arts/are-pop-charts-manipulated.html.

[20] Elias Leight, "Inside the "Black Market" Where Artists Can Pay for Millions of Streams", *Rolling Stone*, (March 10, 2021), accessed October 24, 2023, https://www.rollingstone.com/music/music-features/digital-marketing-streaming-manipulation-1138529/; Glenn Peoples, "Fraudulent Streaming is on the Rise – But Solutions Exist" (Music Biz 2022*), Billboard*, (May 12, 2022), accessed October 24, 2023, https://www.billboard.com/pro/fraudulent-streaming-panel-solutions-music-biz-2022/ .

[21] Jessica D. Litman, "Copyright, Compromise, and Legislative History," *Cornell Law Review, 72* (1987): 857 (859, 861).

how such changes relate to dominant assumptions about both copyright and social norms.

Copyright is based on implicit yet often incomplete and at times even incorrect assumptions about cultural transmission. On the creation side, the typical copyright incentive story that copyright promotes creativity is incomplete n depicting creative practices in several contexts.[22] As a result, how people create, why people create, and factors that motivate creation may not be well understood. By providing widespread access to technological means of creating professional quality content, the digital era has contributed to disruption in creative activities that even prior to the digital era did not always conform to dominant copyright assumptions about creativity.

The experiences of the recording industry also draw attention to digital era disruption on the distribution side. In the past, copyright involved discussions to a significant degree among a community with a high degree of shared experiences and assumptions. Copyright in this era did not overtly touch to a significant degree on everyday practices and ordinary people. Although the terrain of unauthorized uses was pervasive, such uses were separated from formal creative industry businesses in varied ways. Although copyright has long served as a gatekeeper for determining availability and access to cultural material, technological realities meant that dominant pre-digital era business models rested to a significant degree on control of access to technologies or reproduction and dissemination. As a consequence, ordinary users' access and use of materials was significantly circumscribed. Thus, if an average user wanted to make a copy of a record album, available technologies meant that the user's copy would likely be of a significantly lesser quality than the original. This also made such copies not readily commercially exploitable, at least on a level that could really compete with the original. Although some market might have existed for such copies, this market is not likely one that would create serious competition with the original prior to the digital era. The fabric of meaning of such copying has changed in the digital era, largely because of the convergence of changing cultural norms and technological change, including digital technologies that enable near perfect copying, as well as the Internet.[23]

[22] Olufunmilayo B, Arewa, "From J.C. Bach to Hip Hop: Musical Borrowing, Copyright and Cultural Context," *North Carolina Law Review,* 84. (2006): 547.
[23] Arewa, (n 3.

II. Digital Era Opportunities – Changing Artist Practices and Changing Business Models

In December 2013, global superstar Beyoncé Knowles-Carter released a surprise album through the iTunes Store.[24] The album *Beyoncé* quickly became the then bestselling album in iTunes Store history,[25] reaching the top spot on the iTunes charts in 104 countries, selling over 800,000 copies in the first three days of its release.[26] Beyoncé also became the first woman to have her first five albums debut at No. 1 on the Billboard 200 chart.[27] Beyoncé's album release is an important data point from which to consider profound changes in the music industry in the digital era. The digital era has had a particularly strong impact on the record industry, which suffered declining sales during the early digital era.[28]

Although the causes and consequences of digital era technologies have long been contested,[29] much discussion about the early experiences of music industry in the digital era initially focused on the plight of the record industry that many within the industry typically attribute to "piracy" or peer-to-peer (P2P) file sharing.[30] Filesharing received particular attention because it became widespread at a time of declining record industry sales.[31] With the advent of streaming, the fortunes of many recording companies have improved significantly. In 2022, recording industry revenues reached an all-time high with seven years of consecutive growth in the U.S.

---

[24] Zach O'Malley Greenburg, "Breaking Down Beyonce's Record-Breaking Album Launch", *Forbes*, (December 17, 2013), accessed October 24, 2023, http://www.forbes.com/sites/zackomalleygreenburg/2013/12/17/breaking-down-beyonces-record-breaking-album-launch/

[25] Keith Caulfield, "Beyonce Breaks U.S. iTunes Sales Record, Sells 617,000 in Three Days", *Billboard*, (December 16, 2013), accessed October 24, 2023, http://www.billboard.com/biz/articles/news/chart-alert/5839819/beyonce-breaks-us-itunes-sales-record-sells-617000-in-three.

[26] Greenburg, (n 24).

[27] Keith Caulfield, "Beyonce Makes Billboard 200 History with Fifth No. 1 Album*"*, *Billboard*, (December 17, 2014), accessed October 24, 2023, http://www.billboard.com/biz/articles/news/5840087/beyonce-makes-billboard-200-history-with-fifth-no-1-album .

[28] Steve Knopper, *Appetite For Self-Destruction: The Spectacular Crash of the Recording Industry in the Digital Age* (New York: Catapult, 2009); Eric Pfanner, "Music Industry Sales Rise, and Digital Revenue Gets the Credit", *N.Y. Times*, (February 26, 2013), accessed October 24, 2023, http://www.nytimes.com/2013/02/27/technology/music-industry-records-first-revenue-increase-since-1999.html?_r=0.

[29] Felix Oberholzer-Gee & Koleman Strumpf, "The Effect of File Sharing on Record Sales: An Empirical Analysis," *Journal of Political Economy,* 115 (2007): 1 (2); Stan J. Liebowitz, File-Sharing: "Creative Destruction or Just Plain Destruction?", *Journal of Law and Economics,* 49(2008): 1 (24).

[30] Michael Degusta, "The REAL Death Of The Music Industry", *BusinessInsider*, (February 18, 2011), accessed October 24, 2023, http://www.businessinsider.com/these-charts-explain-the-real-death-of-the-music-industry-2011-2.

[31] Arewa, (n 3441 Christian Handke, "Economic Effects of Copyright: The Empirical Evidence So Far", at 9*, The Committee on the Impact of Copyright Policy on Innovation in the Digital Era,* (Working Paper, Apr-il 2011), accessed October 24, 2023, http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_063399.pdf.).

and 2022 revenues in the U.S. of almost $16 billion.[32] Global recording industry revenues were $26.2 billion.[33] In 2022, streaming constituted 67% of global and 84% of total U.S. recording industry revenues. [34]

Continuing disputes surrounding allocation of proceeds from record sales highlight the importance of touring as primary source of income for many recording artists: "Of the top forty-eight musicians who toured in 2017, on average they earned 80 percent of their income from touring, 15 percent from recorded music, and 5 percent from publishing fees."[35] Notably, in the early digital era, most successful popular musicians earned far more from concert ticket sales than from royalties from record sales,[36] despite the fact that aggregate revenue from records at that time far exceeded aggregate revenue from concert performances.[37] Even with proceeds from touring, a 2018 report indicated that artists captured just 12 percent of total 2017 music industry revenues of $43 billion:

> *"Artists' share of music revenues is small. In 2017, artists captured just 12% of music revenue with most of the value leakage driven by the costs of running a myriad of distribution platforms — AM/FM radio, satellite radio, Internet distributors — augmented by the costs (and profits) of the record labels.*
>
> *The proportion captured by artists is, however, on the rise (it was just 7% of industry revenues in 2000). The bulk of the improvement is not driven by the growth in music subscription services. Rather, it's driven by the strength in the concert business. Music labels act as intermediaries for subscription services (Apple, Spotify) but are largely excluded from the economics of the concert business. As such, growth in concert revenue is particularly helpful to artists."*[38]

Notably, 2017 music industry revenues matched a prior peak in 2006.

---

[32] Jem Aswad, "U.S. Recorded Music Revenue Scores All-Time High of $15.9 Billion in 2022, Per RIAA Report", *Variety*, (March 9, 2023), accessed October 24, 2023, https://variety.com/2023/music/news/riaa-2022-report-revenue-all-time-high-15-billion-1235547400/; Joshua P. Friedlander and Matthew Bass, "Year-End 2022 RIAA Revenue Statistics", accessed October 24, 2023, https://www.riaa.com/wp-content/uploads/2023/03/2022-Year-End-Music-Industry-Revenue-Report.pdf.

[33] IFPI, *Int'l Fed'n Of The Phonographic Indus., Global Music Report* (2023), accessed October 24, 2023, https://www.ifpi.org/ifpi-global-music-report-global-recorded-music-revenues-grew-9-in-2022/.

[34] IFPI, (n 33); Friedlander and Bass (n 32) 34.

[35] Alan B. Krueger, *Rockonomics: A Backstage Tour of What the Music Industry Can Teach Us about Economics and Life* (New York: Crown Currency, 2019), 36-37.

[36] Marie Connolly and Alan B. Krueger, «Rockonomics: The Economics of Popular Music » in *Handbook of the Economics of Art and Culture*, ed. Victor A. Ginsberg, David Throsby (Oxford: Elsevier, 2006), 669 (670).

[37] Connolly and Krueger, (n 36), 673.

[38] Citi GPS, "Putting the Band Back Together: Remastering the World of Music"*, Citi GPS: Global Perspectives and Solutions*, at 3, (August, 2018), accessed October 24, 2023, https://ir.citi.com/NhxmHW7xb0tkWiqOOG0NuPDM3pVGJpVzXMw7n+Zg4AfFFX+eFqDYNfND+0hUxxXA

Tours by top-earning musicians have a significant broader economic impact. In 2023, tours by Taylor Swift and Beyoncé underscored the global economic impact of two of the most significant digital era music superstars. Estimates suggest that a Beyoncé concert in Stockholm, Sweden in May 2003 may have increased the Swedish inflation rate due to the inflationary impact on hotel prices from fans taking advantage of favorable exchange rates to see the tour in Sweden:

> *"Michael Grahn, an economist at Danske Bank, said the start of Beyoncé's tour might have had an effect on the inflation data. 'How much is uncertain,' he wrote on Twitter, but it could be responsible for most of the 0.3 percentage points that restaurant and hotel prices added to the monthly increase in inflation."*[39]

The economic impact of Taylor Swift's Eras Tour drew the attention of the Federal Reserve Bank of Philadelphia, which noted: "Despite the slowing recovery in tourism in the region overall, one contact highlighted that May was the strongest month for hotel revenue in Philadelphia since the onset of the pandemic, in large part due to an influx of guests for the Taylor Swift concerts in the city."[40]

The topography of music creation, dissemination, consumption, and sharing has, however, changed to a significant degree in the digital era. This changing landscape has significant implications for a broad range of concerns and participants, including industry business models, consumers, and creators. Beyoncé's album release highlights implications of the digital era for varied music industry participants. This release also raises questions concerning the adequacy of common narratives about the music industry, consumers, and creators in the digital era. Changing music industry digital era landscapes also have implications for intellectual property frameworks that touch upon many aspects of industry practice and consumer access.

Beyoncé's album release draws attention to the incomplete nature of existing narratives about the fate of the music industry in the digital era. It also followed album releases by other artists, including Radiohead and Nine Inch Nails, who distributed music over the Internet at no cost or at a price determined by users.[41] Ear-

[39] Hunter Harris, "The Renaissance Started in Sweden: The first shows of her tour make it clear: We are living in the Beyoncéverse", *Vulture.com*, (May 13, 2023), accessed October 24, 2023, https://www.vulture.com/article/beyonce-renaissance-tour-stockholm-concert.html; Eshe Nelson, "The Unexpected Beyoncé Effect: Hotter Inflation", *N.Y. Times*, (June 15, 2023), accessed October 24, 2023, https://www.nytimes.com/2023/06/15/business/beyonce-inflation-sweden.html..

[40] The Beige Book, Federal Reserve Bank of Philadelphia, at C-2, (July 12, 2023), accessed October 24, 2023, https://www.federalreserve.gov/monetarypolicy/beigebook202307.htm

[41] Sean Michaels, "Amazon's Bestselling Album of 2008 Was Available as a Free Download", *The Guardian*, accessed October 24, 2023, http://www.guardian.co.uk/music/2009/jan/08/nine-inch-nails-amazon-bestseller); Mike Nizza, "Radiohead Album Price Tag: "It's Up to You"", *The Lede, N.Y. Times News Blog*, (October 01, 2007), accessed October 24, 2023, https://archive.ny-

lier in 2013, David Bowie had released a single online in anticipation of a forthcoming album release.[42] These online music releases, taken together, suggest that dominant core business models of the recording industry itself may have contributed to ongoing business problems in the digital era.

Beyoncé's album release changed the playbook for future album releases, becoming the template for later approaches to the promotion and marketing of albums, as well as visual images accompanying albums.[43] Further, Beyoncé's album illustrates that consumers will pay for music they desire. Beyoncé's album was priced at $15.99, which at that time was more expensive than the typical album on iTunes.[44] At the time of its release, purchasers of the album could not download any of the 14 songs on the album individually, but also received 17 exclusive music videos paired with each track on the album with their purchase.[45]

In a further challenge to widespread industry business practices, Beyoncé's album was released "with no warning, no other promotion, no launch parties, no advance radio play, none of the traditional pre-sale retail hype."[46] The album release was kept secret and even high-level staff at Beyoncé's record company were unaware of the forthcoming release.[47] Beyoncé's initially iTunes only album release upended the retail distribution chain for album releases, which led some music sellers

---

times.com/thelede.blogs.nytimes.com/2007/10/01/radiohead-album-price-tag-its-up-to-you/; "Radiohead Reveal How Successful "In Rainbows" Download Really Was", *NME NEWS*, (October 15, 2008), accessed October 24, 2023, http://www.nme.com/news/radiohead/40444; David Byrne, "David Byrne and Thom Yorke on the Real Value of Music", *Wired*, (December 18, 2007). accessed October 24, 2023, http://www.wired.com/entertainment/music/magazine/16-01/ff_yorke?currentPage=all

[42] Alice Vincent, "David Bowie Releases New Song Online Ahead of Mercury Awards", *The Telegraph*, (October 30, 2013), accessed October 24, 2023, http://www.telegraph.co.uk/culture/music/music-news/10415610/David-Bowie-releases-new-song-online-ahead-of-Mercury-Awards.html

[43] Alex Gonzalez, "Beyoncé's Surprise Drop Changed the Industry. Now It's A "Familiar" Process", *MTV.com*, (January 18, 2023), accessed October 24, 2023, https://www.mtv.com/news/l36y58/beyonce-surprise-drop-legacy-new-retro.

[44] Editorial: Beyonce: "The Future of Music?", *BOSTON GLOBE*, (December 18, 2013), accessed October 24, 2023, http://www.bostonglobe.com/opinion/editorials/2013/12/18/beyonce-new-album-may-breakthrough-for-recording-industry/gk34ps8bxFY3gIJJ2iKKdI/story.html

[45] Editorial, (n 44).

[46] Teddy Riley, "No Stunt: Beyonce's Sneak Attack on the Music Industry Resets the Rules", (December 14, 2013), accessed October 24, 2023, http://www.cnn.com/2013/12/23/opinion/beyonce-teddy-riley-opinion/.

[47] Marianne Garvey, Brian Niemietz and Lachlan Cartwright, "Beyoncé Ordered Tight Secrecy on New Album, Which Had Help from Jay Z and Terry Richardson", *N.Y. Daily News*, (December 24, 2013), accessed October 24, 2023, https://www.nydailynews.com/2013/12/14/beyonc-ordered-tight-secrecy-on-new-album-which-had-help-from-jay-z-and-terry-richardson/; Claire Suddath, "Why Beyoncé Didn't Tell Anyone About Her New Album, Bloomberg BusinessWeek", (December 16, 2013), accessed October 24, 2023, https://www.bloomberg.com/news/articles/2013-12-16/beyonc-s-surprise-album-release-on-itunes-defies-pop-star-marketing?embedded-checkout=true

such as Amazon and Target, to refuse to sell physical copies of the album.[48] In response to the Target boycott, Beyoncé went shopping at a Walmart store in Tewsbury, Massachusetts and distributed some $37,000 in $50 Walmart gift cards during her visit.[49]

Even successful releases by superstars such as Beyoncé cannot entirely obscure the increased instability that the digital era has brought to the music business. Rather, Beyoncé's release underscored shortcomings of existing recording business models. Beyoncé's release raised significant questions about existing industry models that still rely to a significant degree on assumptions derived from an era when physical distribution was the norm.[50] In relying to a significant degree on business models that arose in an era of physical distribution, existing models may not take sufficient account of the full implications of consumer preferences for downloads and streamed content. The continued industry reliance on business models that arose in an era of physical distribution of records also has significant implications for musicians, who may not be able to make a living with the current revenue streams that they receive from digital music streaming and downloads.[51]

III. Creators and Consumers in the Digital Era

Digital era artistic practices and business models highlight important consequences of digital disruption in the music industry and entertainment industry more generally. This digital disruption extends beyond issues related to intermediation and business models for distribution of content. Rather, disruption extends to virtually all aspects of the creation, distribution, and consumption of content, as well as intellectual property frameworks which are a foundation upon which existing cultural industry business were built.

Discussions of intellectual property as property often implicitly rely upon conceptions of value that give primacy to economic and business value while dismissing

---

[48] Thomas Lee, "Target Says No To New Beyoncé Album", *StarTribune*, (December 18, 2013), accessed October 24, 2023, http://www.startribune.com/entertainment/music/236258751.html Bobby Owsinski, "Beyonce Fights Back Against The Amazon/Target Boycott", *Forbes*, (December 23, 2013), accessed October 24, 2023, http://www.forbes.com/sites/bobbyowsinski/2013/12/23/beyonce-fights-back-against-the-amazontarget-boycott/

[49] Owsinski, (n 48).

[50] Om Malik, "In Beyonce We Trust & Then On iTunes We Buy: End Nears For Physical Media", *Gigaom.com*, (December 18, 2013), accessed October 24, 2023, https://om.co/gigaom/in-beyonce-we-trust-then-on-itunes-we-buy-end-nears-for-physical-media/.

[51] David Byrne, "How Will The Wolf Survive: Can Musicians Make A Living In The Streaming Era?", Features, (March 31, 2014), accessed October 24, 2023, http://davidbyrne.com/how-will-the-wolf-survive-can-musicians-make-a-living-in-the-streaming-era); Zac Shaw, "How the Wolf Will Survive: How Musicians Make a Living in the Streaming Era", *Mediapocalyps*e, (April 3, 2014), accessed October 24, 2023, http://www.mediapocalypse.com/how-the-wolf-will-survive-how-musicians-make-a-living-in-the-streaming-era/

or even ignoring questions of cultural value. This is important in the context of practices of many artists in part because artists' relationships with their fans, mediated by social media, have become key aspects of the appeal and ability of many successful artists to rapidly sell large amounts of music.[52] The emergence of TikTok as a powerful force in music attests to the critical importance of social media. Lil Nas X's viral hit song "Old Town Road" emerged on TikTok to achieve unparalleled success,[53] and a viral moment that has become an aspirational model that has been difficult to replicate more broadly.[54]

B. The Value of Music and the Meaning of Ownership

I. How Much is Music Worth? Music as a Valuable Asset

Divergent views about the value and uses of content are at tension in digital era disputes. A continued tendency to view content through the lens of valuable asset models of culture has led to a disproportionate industry focus on restricting access to content. Such restrictions have traditionally been made possible and mediated to a significant degree by available technologies, intellectual property laws, and contractual and business practices. The cultural industries emerged and became powerful forces in a technological environment in which such control was a norm. Digital era technologies have transformed the ability of creators, users, and others to access existing content in ways that has lessened industry control in many instances. This reality of less actual control, however, underscores divergent assumptions about the value and uses of content, which has contributed to continuing disputes.

Recent catalog sales for successful artists, including Bob Dylan, Stevie Nicks, Tina Turner, and Bruce Springsteen, highlight the potentially enormous returns to successful artists: music catalogs for some artists have been selling for as much as 30 times average annual royalties.[55] These sales typically involve the sale of publishing and potentially other music rights. Catalog and music rights purchasers are then

[52] "Social Media's Critical Role in the Music Industry", *College of Contemporary Music*, (April 14, 2021), accessed October 24, 2023, https://www.mi.edu/in-the-know/social-medias-critical-role-music-industry/.

[53] Elise Shafer, "Started on TikTok, Now We're Here: A Look Back at the Meme-Tastic Beginning of Lil Nas X's "Old Town Road"", *Billboard*, (July 29, 2019), accessed October 24, 2023, https://www.billboard.com/music/music-news/lil-nas-x-old-town-road-tiktok-beginning-8524319/.

[54] John Herman, "Viral Spiral", *N.Y. Times*, (June 24, 2022), accessed October 24, 2023, https://www.nytimes.com/2022/06/16/style/tiktok-viral-music-marketing.html

[55] Anne Steel, "From Bruce Springsteen to Tina Turner: Why are Artists Selling Their Music Catalogs", *Wall Street Journal,* (January 18, 2022), accessed October 24, 2023, https://www.wsj.com/story/why-are-so-many-rock-stars-selling-their-music-catalogs-a64667cd.

able to "reap the money from royalties, licensing, brand deals, and other revenue streams that would have gone to the artist."[56] Purchasers of catalogs clearly see value in the catalogs of successful artists, which may have been heightened during the Covid-19 pandemic when many artists were forced to reduce or stop touring.[57] The prices of recent catalog sales may also, however, reflect some degree of overvaluation.[58]

Further, for many consumers, music may simply not be worth as much as many industry players may think it is.[59] The digitization of music, the seemingly unlimited supply of music available through streaming, and the fundamental intangibility of digital music may have fostered a technologically driven diminution of the value of music from the perspective of many consumers:

> *"It's a little dark, but I am leaning towards the sentiment that recorded music inherently doesn't have a lot of monetary value, and maybe it never really did. It may have always been visibility that sustained album retail valuation. Listening to music is about as complicated and expensive as having an email account (it's free). There is real value in music… but today it's more intangible than ever. Listening to music is something you can do, like walking down a sidewalk or breathing. Is air valuable? Yes, very! It is also just kinda there, all around us, at all times."*[60]

In addition, music has never faced as many other competing options as are available today. Consumers may choose from music with or without streamed or other video, a variety of streamed television programs and movies, video games, social media, a variety of mobile and other apps, consumption of content through various types of physical media, and varied live entertainment options, to name just a few. The increasing prominence of valuable asset models of culture by cultural industry businesses may be at odds with how people consuming cultural products value them.

---

[56] Tim Ingham and Amy X. Wang, "Why Superstar Artists Are Clamoring to Sell Their Music Rights", *Rolling Stone*, (January 15, 2021), accessed October 24, 2023, https://www.rollingstone.com/pro/features/famous-musicians-selling-catalog-music-rights-1114580/

[57] Steel, (n 55).

[58] Ted Gioia, "Investment Funds Are Now Selling the Rock Songs They Bought", *The Honest Broker*, (September 16, 2023), accessed October 24, 2023, https://www.honest-broker.com/p/investment-funds-are-now-selling

[59] John Caramanica, "How Much Is an Album Worth in 2020: $3.49? $77? $1,000? Maybe $0", *N.Y. Times*, (August 19, 2020 (updated August 24, 2020)), accessed October 24, 2023, https://www.nytimes.com/2020/08/19/arts/music/albums-price.html

[60] Caleb Dolister, "What is the Value of Recorded Music Anymore?", *Medium.com*, (March 11, 2019), accessed October 24, 2023, https://calebdolister.medium.com/what-is-the-value-of-recorded-music-anymore-37abc3a07438#:~:text=Recorded%20music%20is%20only%20valuable,label%2C%20even%20if%20it's%20tiny.

The global economic and business significance of the cultural industries is reflected in industry statistics. In 2022, the economic contribution of "core" copyright industries, including motion pictures, sound recordings, music publishing, print publishing, computer software, theater, advertising, radio, television, and cable, surpassed $1.8 trillion.[61]

The In the digital era, many cultural industry players have focused on using technology and other mechanisms of control to maintain and enhance the value of content. The music industry, for example, has typically maximized the value of the musical content through control mechanisms on both the creation and distribution side with respect to artists and consumers.[62] During the digital era, dominant industry players in cultural industries sectors such as the music industry have experienced at least some degree of digital era disintermediation, which has been in part rooted in the development digital content and alternative technologies of dissemination of such content, both authorized and unauthorized, such as content available through the Internet.[63] The availability of such alternatives on both the creation and distribution side has led to significant and deleterious business consequences in the music industry.

Copyright unfolds in the business arena significantly in the shadow of contract. The contractual terms granted creators in such contracts suggest that the value of creation and need for rewards to incentive new creations expressed in copyright policy debates is not always reflected in the business terms to which many creators are actually subject. Contractual terms in the recording industry, for example, reveal significant power asymmetries both in the allocation of intellectual property rights and relative economic benefits: *"[a]n artist in a strong position when contracts are negotiated . . . may be able to remove" certain contractual clauses, but that the "mantra of 'take it or leave it' on the part of the music industry potentially puts them in a very strong bargaining position . . . while the ideology of copyright law might be to protect the rights of the artists, the reality of the music business is that such rights are, in effect, exercised by their publishers and record companies."*[64]

The treatment of many creators in current cultural industry business structures belies the incentive story of copyright and reveals the extent to which perception may

[61] Robert Stoner and Jéssica Dutra, "Copyright Industries in the U.S. Economy: The 2022 Report", *Prepared for the International Intellectual Property Alliance*, (July 15, 2021), accessed October 24, 2023, https://www.iipa.org/files/uploads/2022/12/IIPA-Report-2022_Interactive_12-12-2022-1.pdf

[62] Nicola F. Sharpe and Olufunmilayo B. Arewa, "Is Apple Playing Fair? Navigating the iPod DRM Controversy," *Northwestern Journal of Technology and Intellectual Property,* 5, (Number 2, 2007).

[63] Sharpe and Arewa, (n 62).

[64] Steve Greenfield and Guy Osborn, «Copyright Law and Power in the Music Industry», in *Music and Copyright,* ed. Simon Frith and Lee Marshall., 2nd edn. (New York: Routledge, 2004), 89, (99).

diverge from reality in the context of prominent business models as currently deployed.[65] In the case of the recording industry, control on the creative side has been a core element in industry business models and profitability.[66]

II. What Does It Mean to Own Music in the Age of Social Media?

Intangibility may have an impact on perceptions of music's value. Digitization may mean that consumers value music less because they "may place greater value (emotional and monetary) on the physical product because of the lack of legal ownership and/or absence of perceived ownership associated with streaming."[67] In addition to technology potentially driving changes in how consumers value music, streaming and the general intangibility of digital era music possession changes the nature of the ownership of music itself.[68] Use rights for streamed music may at times be tenuous and uncertain, with digital content disappearing in unpredictable ways.[69] Treatment of streamed content by businesses reflect values that may in fact parallel the lesser value and loyalty that consumers may ascribe to streamed content.[70]

From a business perspective, in the aftermath of Covid-19, problems with the economics of many streaming models have become increasingly apparent.[71] In addition, the value of music and other content may have diminished considerably:

---

[65] Keith Negus, "Cultural Production and the Corporation: Musical Genres and the Strategic Management of Creativity in the US Recording Industry", *Media, Culture & Society,* 20 (1998): 359, (361).
[66] Jason Toynbee, «Musicians», in *Music and Copyright,* ed. Simon Frith and Lee Marshall, 2d edn. (New York: Routledge, 2004), 123, (124).
[67] Gary Sinclair and Julie Tinson, "Psychological Ownership and Music Streaming Consumption", *Journal of Business Research,* 71 (2017): 1 (1).
[68] Shelley Hepworth, "Streaming spells the end of the "ownership" era of music, but are we ready to let go?", *The Guardian*, (February 1, 2020), accessed October 24, 2023, https://www.theguardian.com/music/2020/feb/02/streaming-spells-the-end-of-the-ownership-era-of-music-but-are-we-ready-to-let-go.
[69] Lynette Rice and Nellie Andreeva, "The Streaming Purge: Behind the Wave of Library Content Removals & Its Impact on The Creative Community", *Deadline*, (February 14, 2023), accessed October 24, 2023, https://deadline.com/2023/02/the-streaming-purge-library-content-removals-impact-creative-community-1235256840/; Kathryn VanArendonk, "TV Has Always Disappeared. This Feels Different", *Vulture.com*, (December 14, 2022), accessed October 24, 2023, https://www.vulture.com/article/hbo-max-warner-cancelations-disappearing-tv-streaming-future.html; Chloe Paglia, "Frustrated Fans Flee Spotify after Hundreds of K-Pop Songs Disappear from Platform", *Scenes*, (March 3, 2021), accessed October 24, 2023,https://scenesmedia.com/2021/03/frustrated-fans-flee-spotify-after-hundreds-of-k-pop-songs-disappear-from-platform/
[70] Ted Gioia, "Why Ownership Matters", *The Smart Set,* (February 13, 2017), accessed October 24, 2023, https://www.thesmartset.com/why-music-ownership-matters/
[71] Meredith Rose, "Streaming in the Dark: Where Music Listeners' Money Goes – and Doesn't", *Public Knowledge Report*, (March 2023), accessed October 24, 2023, https://publicknowledge.org/policy/streaming-in-the-dark-where-music-listeners-money-goes-and-doesnt/; House of Commons, "Digital, Culture, Media and Sport Committee, Economics of Music Streaming, Second Report of Session 2021-22", *House of Commons*, (July 15, 2021), accessed October 24, 2023, https://committees.parliament.uk/publications/6739/documents/72525/default/; Lillian Rizzo and Sarah Whitten,

"Music seems to have returned to the medieval era, when starving bards survived by serving the nobility, providing the playlist at a banquet where others were feasting. That's a fitting metaphor for the new reality in music. The shift in economic models has been rapid and devastating. Apple could now acquire every major record label with just the spare cash in its bank account. But Apple CEO Tim Cook is too smart to do that. He knows there's no money as a content creator — in fact, his company has worked to ensure that state of affairs."[72] Business practices such as the now common 360 deal, in which record labels may receive additional revenue and income streams from activities beyond record sales[73].[74]

How we value music, particularly from a business perspective, may not give sufficient recognition to the importance of sharing as a core attribute of what makes music valuable to many creators and consumers. Borrowing and creolization are endemic in human culture. Current discussions of music, value, and intellectual property may reflect tensions inherent between different understandings of culture. These tensions are pervasive in intellectual property discussions in a broad range of areas. that borrowing and the forces of diffusion interact with and extensively affect cultural systems.

Cultural hybridity highlights the importance of sharing in the cultural realm. Some conceptions of authority in intellectual property discussions do not take adequate account of the importance of sharing in music and other cultural arenas, including as a significant element of cultural innovation.[75] This recognition is an important one when considering digital era consumer sharing practices, the meanings and significance of which may vary significantly. Ultimately, understanding digital music trends requires understanding music not only as a valuable asset, but also through a lens that takes account of cultural attributes and values. In particular, the relationships between Taylor Swift,[76] Beyoncé,[77] other prominent artists and their

"Hollywood is Paying a Steep Price for Never Really Figuring Out the Streaming Model", *CNBC.com,* (September 23, 2023), accessed October 24, 2023, https://www.cnbc.com/2023/09/17/hollywood-streaming-profits-struggles.html; OlaOluwa Adeyemo, "Why Spotify Struggles to Make Money from Music Streaming," *Medium.com,* (August 24, 2023), accessed October 24, 2023, https://medium.com/brain-labs/why-spotify-struggles-to-make-money-from-music-streaming-ba940fc56ebd.

[72] Gioia, (n 70).

[73] Lee Marshall, "The 360 Deal and the "New" Music Industry," *European Journal of Cultural Studies,* (2013): 77 (78).

[74] Sara Karubian, "360° Deals: An Industry Reaction to the Devaluation of Recorded Music," *Southern California Interdisciplinary Law Journal,* 18 (2009): 395.

[75] Peter Burke, *Cultural Hybridity* (Cambridge: Polity, 2009).

[76] Maryn Wilkinson, "Taylor Swift: The Hardest Working, Zaniest Girl in Show Business…", *Celebrity Studies,* (2019): 441-444.

[77] Melissa Avdeeff, «Beyoncé and Social Media: Authenticity and the Presentation of Self», in *The Beyoncé Effect: Essays on Sexuality, Race and Feminism*, ed. Adrienne Trier-Bieniek (Jefferson, N.C.: McFarland, 2016), 109.

fans reflect elements of a sharing culture that can enrich our understanding fandom[78] as well as other practices, including unauthorized uses, in the digital era in the case of Beyoncé, part of the relationship with at least some of her fans may make such fans more likely to actually purchase[79].[80]

[78] Nancy Baym, Daniel Cavicchi, Norma Coates, «Music Fandom in the Digital Age: A Conversation», in *The Routledge Companion to Media Fandom*, ed. Melissa A. Click and Suzanne Scott (New York: Routledge, 2018), 141.

[79] Emma Jacobs, "How to Market Brand Beyoncé", *Financial Times,* (September 25, 2014), accessed October 24, 2023, http://www.ft.com/intl/cms/s/2/9ebce5a6-43d0-11e4-8abd-00144feabdc0.html #axzz3EOJK29RE.

[80] Nolan Feeney, "How Beyoncé Keeps the Internet Obsessed with Her," *The Atlantic*, (August 14, 2013) accessed October 24, 2023, http://www.theatlantic.com/entertainment/archive/2013/08/how-beyonc-keeps-the-internet-obsessed-with-her/278681/; Ben Sisario, "Beyoncé Rejects Tradition for Social Media's Power", *N.Y. Times*, (December 16, 2013), accessed October 24, 2023, http://www.nytimes.com/2013/12/16/business/media/beyonce-rejects-tradition-for-social-medias-power.html?_r=0.

List of authors

Prof. Dr. Gerald Spindler (†): Universität Göttingen.

Prof. Dr. Annette Guckelberger: Universität des Saarlandes.

Prof. Dr. Michael Mayrhofer: Johannes Kepler Universität Linz.

Mag. Michael Denk: Johannes Kepler Universität Linz.

Prof. Dr. José Hernán Muriel Ciceri, LL.M.: Tecnologico de Monterrey.

Prof. Luis Enríquez, LL.M.: Universidad Andina Simón Bolívar, Université de Lille.

Asst. -Prof. Dr. Ruben E. Rodriguez Samudio: Waseda University.

Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur.: Philipps-Universität Marburg.

Assoc.-Prof. Dr. Yusuke Tachibana: Fukuoka Institute of Technology.

Prof. Dr. Teresa Rodríguez de las Heras Ballell: Universidad Carlos III de Madrid.

Prof. Michiyo Maeda: Keio University.

Prof. Dr. Aran García Sánchez: Tecnologico de Monterrey.

Prof. de Cátedra Oscar Pérez Carreto, Mag.: Tecnologico de Monterrey.

Prof. Dr. Olufunmilayo B. Arewa: Temple University Beasley School of Law.

Law and technology present humanity with challenges and opportunities. This international research volume is dedicated to three of their pillars: artificial intelligence, blockchain and digital platforms. The authors' contributions analyze these topics from different perspectives of public and private law in the German, Austrian, European, American, Japanese, and Latin American contexts.

Recht und Technologie stellen die Menschheit vor Herausforderungen und Chancen. Dieser internationale Forschungsband widmet sich drei ihrer Säulen: Künstliche Intelligenz, Blockchain und digitale Plattformen. Die Beiträge der Autoren analysieren diese Themen aus unterschiedlichen Perspektiven des öffentlichen und privaten Rechts im deutschen, österreichischen, europäischen, amerikanischen, japanischen und lateinamerikanischen Kontext.

El derecho y la tecnología presentan retos y oportunidades a la humanidad. Este volumen internacional de investigación se ocupa de tres de sus columnas como son: la inteligencia artificial, la cadena de bloques y las plataformas digitales. Las contribuciones de los autores analizan estas temáticas desde diferentes perspectivas del derecho público y privado en el contexto alemán, austriaco, europeo, estadounidense, japonés y latinoamericano.

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

ISBN: 978-3-86395-612-7

Universitätsverlag Göttingen