THE GLOBAL LEGAL POST

GERMANY

Alexander Tribess
GreenGate Partners

This chapter forms part of:

ARTIFICIAL INTELLIGENCE
Law Over Borders Comparative Guide 2024

www.globallegalpost.com/lawoverborders

INTRODUCTION

The landscape of AI systems in Germany has transformed significantly over the last two years. The availability and use of AI has expanded rapidly, driven by advancements in technology and increased adoption across various sectors. A key player in this evolution is Aleph Alpha, a prominent German AI enterprise, which holds much promise in competing with leading American and Chinese AI companies. Aleph Alpha is venture capital-backed and has recently undergone several capital increases, attracting a diverse array of shareholders from Germany's traditional industries and international funds. As Germany aims to strengthen its position in the global AI landscape, Aleph Alpha's innovations and developments are seen as crucial to maintaining competitiveness and fostering growth in the industry.

1. CONSTITUTIONAL LAW AND FUNDAMENTAL HUMAN RIGHTS

The constitution of the Federal Republic of Germany (Grundgesetz) contains a catalogue of fundamental and human rights in Articles 1 to 19, starting with the protection of human dignity as an inalienable right of every human being (Article 1(1) of the Grundgesetz). The EU Charter of Fundamental Rights and the European Convention on Human Rights foster the guarantee of human rights in Germany.

1.1 Domestic constitutional provisions

The Grundgesetz does not contain any explicit provisions regulating or restricting the state's use of AI systems. However, as early as 1983, the Federal Constitutional Court (BVerfG) derived an independent fundamental right to informational self-determination from the principle of human dignity and the fundamental right to general freedom of action (Articles 1(1), 2(1) of the Grundgesetz). Since then, the BVerfG has further elaborated on this right in numerous decisions. Decisions of the BVerfG are binding on all constitutional bodies, as well as on all courts and authorities, and often acquire the force of law directly (section 31 of the Federal Constitutional Court Act).

1.2 Human rights decisions and conventions

A decision of 10 November 2020 (1 BvR 3214/15 – Antiterrordateigesetz II) indicates that the BVerfG continues to reinforce its established case law on the fundamental right to informational self-determination in the context of a possible state use of AI systems. The BVerfG nullified a federal law which purportedly allowed police authorities and intelligence services to make extended use of anti-terrorism files by way of data mining (i.e., the automated analysis of existing data). According to the court, it is constitutionally required that such state data mining must be held to protect particularly important legal interests and its usage must be bound to sufficient thresholds of intervention based on precisely defined and normatively clear regulations. The BverfG upheld its previous position, according to which human dignity requires that people are never made the mere object of state intervention, especially in the area of collecting and analysing information.

Other cornerstones of the case law on the fundamental right to informational self-determination are the purpose limitation of data processing by state agencies, (in principle), the transparency of state interventions *vis-à-vis* the persons concerned, and the preservation of structurally and organisationally separate state units, especially in the area of intelligence and security agencies.

2. INTELLECTUAL PROPERTY

In the context of intellectual property rights (IP rights) and copyright, the legal discussion about AI concerns two fundamental concepts:

- can AI be the object of IP rights (is it patentable, for example); and
- can AI be considered as the holder of rights, for example as the author of a work?

The debate centres on patent and copyright law. In principle, the questions can also be applied to other national and European Union intellectual property rights. Like the patent, it is also possible to indicate an inventor when applying for a utility model under the Utility Model Act, and design law also recognises the person of the designer in section 6(5) of the German Design Act and Article 18 of the Community Design Regulation.

With the rise of ChatGPT and other applications trained on huge amounts of publicly available texts, images and other copyrighted materials, the debate has shifted towards the applicability and scope of the text and data mining exception from copyright holders' rights (section 44 b of the Copyright Act (UrhG)).

2.1 Patents

Patentability of AI

The number of applications for AI-related patents at the German Patent and Trademark Office (Deutsches Patent- und Markenamt, DPMA) has been rising for years. As a rule, it is not the AI application as such that is patentable, because AI methods are mostly mathematical solutions implemented in software, i.e., computer-implemented processes. These are only accessible to patent protection to a limited extent, since computer programs are not patentable *per se* (section 1(3) No. 3 of the Patent Act; the same applies to utility models: section 1(2) No. 3 of the Utility Model Act). Patentability requires a contribution to the solution of a concrete technical problem by technical means, such as the control of an autonomous vehicle, or the processing of measured values (e.g., if camera images from a vehicle are analysed to determine which traffic signs can be recognised on them, or if medical image data are being analysed for tumour detection in preparation for a medical diagnosis — examples from the report on the AI conference at the DPMA 2018 (see DPMA: Artificial intelligence and property rights at *www.dpma.de/dpma/veroeffentlichungen/hintergrund/ki/kuenstlicheintelligenzundschutzrechte*)).

AI as inventor

The Legal Board of Appeal of the European Patent Office ruled on 21 December 2021 that only a human being can be an inventor within the meaning of Article 81 of the European Patent Convention. An AI could not be an inventor, and a human being cannot be regarded as the legal successor of an AI as the actual inventor of a patent (J 8/20 and J 9/20).

2.2 Copyright

Copyright Protection of AI

According to the established case law of the German Federal Court of Justice (BGH), algorithms as such are not amenable to copyright protection (judgment of 9 May 1985, I ZR 52/83, *Inkasso-Programm*). However, the manner of implementation and assignment of different algorithms to each other may be protectable. Note that the calculation rule, the idea, and/or the mathematical formula are not the subject of protection here, but rather the "fabric" (BGH, judgment of 4 October 1990, I ZR 139/89, *Betriebssystem*). Copyright protection of algorithms as computer programs under section 69a of the Copyright Act (UrhG) will therefore not generally exist in Germany.

Works Created by AI

German copyright law is strongly influenced by the idea of the author as the creative head behind the work. The work is the expression and object of a moral right. This moral right permeates the entirety of German copyright law, especially to the extent that it has not been harmonised under European law. The right to be named as the author (section 13 of the UrhG), the author's rights of access to the original of his work (section 25 of the UrhG) or a right of recall due to changed opinion (section 42 of the UrhG) are only a few manifestations of this guiding idea. This basic conception of copyright law does not allow recognition of non-human systems as creators of works. Therefore, works created solely by AI systems are not amenable to copyright protection. If there is a sufficiently large human influence on the act of creation, only the natural persons behind the AI would be recognised as authors.

Apart from the conceptional question of whether AI can be considered an author, recent legal discussions have focused on the training of Large Language Models and similar AI tools. Under EU copyright law, storing training data in a *corpus* constitutes a relevant reproduction of the original work, even if it does not reach the public. AI vendors must ensure they have the right to collect and store such data, as direct licensing of terabytes of web-scraped training data is impracticable and unlikely to be achieved. The Digital Single Market (DSM) Directive (Directive (EU) 2019/790) introduced in 2019 allows reproductions necessary for automated analysis unless the rights holder has expressly reserved this type of exploitation. This legal permission has been incorporated in German copyright law as section 44b of the UrhG and is intended to facilitate large-scale data collection for creating training *corpora*. However, it is debated whether this exception applies to generative AI models, which were not foreseen when the DSM Directive was adopted. The applicability has become even more important with the advent of EU regulation of AI. Under Article 53(1)(c) of the AI Act, organisations using works for AI training must prove that the data was legally obtained. The AI Act also mandates that AI model providers have a policy to respect EU copyright law, specifically to identify and respect reservations of use expressed under the DSM Directive.

2.3 Trade secrets and confidentiality

Since AI applications are regularly not subject to patentability or copyright protection, safeguarding the confidentiality of algorithms, data and their network of relationships is all the more important. In Germany, the protection of trade secrets is governed by

the Act on the Protection of Trade Secrets (GeschGehG), which came into force in 2019 as an implementation of Directive (EU) 2016/943 ([2016] OJ L157/1). Associated with the GeschGehG was a paradigm shift from the traditional principles of trade secret protection in Germany. In contrast to the older case law, section 2 of the GeschGehG now requires the owner to apply reasonable secrecy measures to obtain statutory protection against unauthorised use of trade secrets. The need-to-know principle is of central importance: information may only be disclosed to or made accessible to those persons, both within the company and to external parties, who absolutely require it for the performance of their duties. In addition, physical, technical and legal measures (in particular, the conclusion of non-disclosure agreements) must be used to prevent unauthorised access to or use of trade secrets (Stuttgart Higher Regional Court, judgment of 19 November 2020, 2 U 575/19).

2.4 Notable cases

AI litigation is also progressing in Germany, similar to prominent cases in the US. The Regional Court (Landgericht) Hamburg is set to decide a case where a photographer claims that LAION infringed his copyright under EU law by scraping the internet to train its AI model. LAION's defence is based on the text and data mining exception of section 44b of the UrhG. Unlike in the well-known U.S. cases, the plaintiff did not discover its photos by use of the AI model, but LAION had published a list of all links used for AI training via web scraping. In July 2024, in a first hearing, the court expressed the following preliminary views on the case:

- Works do not require a license from the copyright holder to be "lawfully accessible"; a watermarked representation of a photo or thumbnail is lawfully accessible on the Internet.
- Crawling the Internet to create a *corpus* for an AI model is an "automated analytical technique aimed at analysing text and data" and serves the purpose of generating "correlations" in this case.
- Article 5(5) of the EU InfoSoc Directive (Directive 2001/29/EC as amended), which protects the right holder against copyright exceptions that "unreasonably prejudice the legitimate interests of the right holder," cannot be invoked against preparatory works where the later use of an AI model is not controlled by the person performing the crawl.

The court leans towards allowing crawling for AI training purposes. However, it will focus on whether the applicable license terms should be understood as an express reservation of rights in machine-readable form, which will be critical to its decision. The court and the parties discussed both broad and narrow interpretations of machine-readability, considering general website text availability and specific technical integrations like robots.txt. If the court adopts a narrower interpretation, the focus will shift to whether the defendant qualifies as a research organisation and can rely on broader text and data mining rights.

3. DATA

3.1 Domestic data law treatment

In principle, only the provisions of the General Data Protection Regulation (GDPR) apply to the processing of personal data. Insofar as the EU Member States

continue to have legislative competence for individual areas of law (e.g., in the area of employee data protection), Germany has minimal legislation in this space. The German regulations created in order to implement Directive (EU) 2016/680 ([2016] OJ L119/89) on data processing by police and judicial authorities also do not contain any special legal requirements for the use of AI systems.

3.2 General Data Protection Regulation

AI and its use for processing personal data is in tension with fundamental principles of the GDPR. The Conference of Independent Data Protection Supervisory Authorities of the Federal Government and the Länder (DSK) published the Hambach Declaration on 3 April 2019 which reveals great scepticism on the part of the supervisory authorities toward AI systems (see *www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2019/2019-DSK-Hambach_Declaration_AI-en.pdf*).

The Hambach Declaration lists seven basic principles of data protection that should be upheld in the context of AI:

- AI must not turn human beings into objects, meaning that AI systems must not make decisions without the possibility of human intervention and only in a lawful and fair manner (Articles 5(1)(a), 22 of the GDPR);
- AI may only be used for constitutionally legitimate purposes and may not abrogate the requirement of purpose limitation (Articles 5(1)(b), 6(4) of the GDPR);
- AI must be transparent, comprehensible and explainable (Articles 5(1)(a), (2), 12 of the GDPR);
- AI must avoid discrimination, particularly through countermeasures applied before an AI system is being used with appropriate risk monitoring during the application of AI systems;
- the principle of data minimisation applies to AI (Article 5(1)(c) of the GDPR);
- AI needs responsibility, meaning that controllers of AI systems must ensure compliance with the aforementioned principles, provide clear and comprehensible information to data subjects, and ensure the security of the processing (Articles 12 *et seq*., 32, 35 of the GDPR); and
- AI requires technical and organisational standards for which best practices must be developed (Articles 24, 25 of the GDPR).

The DSK has further refined its position in a recent publication that aims at providing practical guidance to companies and public institutions using AI applications (see Orientierungshilfe Künstliche Intelligenz und Datenschutz, Version 1.0 of 6 May 2024, at *www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf*). In light of the various use cases that have emerged with the release of publicly accessible large language models (LLMs) like ChatGPT, the DSK emphasises the need to comply with data protection laws when processing personal data with AI. Legal bases are required for outputs containing personal data, and individuals should be transparently informed about how their data is used. For implementing AI applications, the DSK highlights the importance of lawful purposes and advises against processing personal data unless essential. When using AI applications, the document advises caution in handling personal data, especially sensitive categories. The DSK advocates for creating anonymous accounts for AI application use rather than having employees subscribe with personalised credentials.

In October 2023, the data protection authority of the German Land of Baden-Württemberg published a discussion paper on legal bases for the processing of personal data when using AI systems (see *www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki*). Following public consultation, the document is still awaiting its finalisation and publication. However, the draft status currently available underlines again the scepticism of data protection authorities in Germany with respect to the GDPR compliant use of AI applications.

A position paper from the DSK on recommended technical and organisational measures in the development and operation of AI systems contains initial indications of the bar that the supervisory authorities will set for AI systems (see *www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf*).

3.3 Open data and data sharing

In 2017, Germany laid the foundation for open administrative data with the first Open Data Act. Section 12a of the eGovernment Act (EGovG) obliged numerous federal authorities to publish the "raw data" they collect. At the same time, central criteria for open data were specified, such as making the data available to access free of charge, and specifying further criteria as to machine readability. The Second Open Data Act, which came into force on 23 July 2021, significantly expanded its applicability to further federal authorities. In addition, since summer 2024, federal agencies collecting research data are also subject to the obligation to publish their results as open data.

Similar laws also exist at the level of the Länder (German States). The GovData portal is a central online platform for retrieving administrative data from the federal, state and local governments. Open data laws have been criticised because, although government agencies are obliged to make data available, citizens have no individual right to publication. In this respect, citizens are referred to transparency laws, which have been enacted separately at the federal and state levels.

3.4 Biometric data: voice data and facial recognition data

The guidelines of the European Data Protection Board on virtual voice assistants contain valuable information on the use of voice assistance systems (both in consumer electronics devices and in driver assistance systems).

The use of facial recognition systems is regularly the subject of much criticism in Germany. Plans to introduce nationwide video surveillance systems with biometric facial recognition (for example at train stations), were scrapped after protests from data protectionists. So it remains that this technology is only used by largely voluntary projects, such as the biometric check-in at Hamburg Airport (see *www.hamburg-airport.de/en/star-alliance-biometrics-at-hamburg-airport-50722*).

The decision of the Hamburg Administrative Court (VG Hamburg) on the reference database of Hamburg law enforcement has been the subject of much debate in Germany. In this case, security authorities had brought together recordings from public video surveillance systems, private image and film recordings, and internet sources after the riots at the G20 summit in 2017, analysed them biometrically, and used them for criminal prosecution. When the Hamburg data protection supervisory authority demanded deletion, the VG Hamburg held that the processing was lawful under section 48 of the Federal Data Protection Act (judgment of 23 October 2019, 17 K 203/19).

FREQUENTLY ASKED QUESTIONS (FAQS)

Are text and data mining generally allowed for the purposes of AI training?
Section 44b of the UrhG contains a restriction on copyright exploitation rights: the reproduction of legally accessible works is permitted for their automated analysis in order to obtain information from them, in particular about patterns, trends and correlations. However, the author has the option of reserving this right for himself by means of a machine-readable notice. Ongoing litigation may have a significant impact on the application of this so-called text and data mining exception.

Is the use of personal data for AI training purposes prohibited?
It is not expressly prohibited to use personal data to train an AI application. However, the principles of data protection law must be observed: data subjects must be informed in a transparent manner that their data will be used for this purpose. And there must be a legal basis for the processing, which in most cases can only be explicit consent.

Do I need to use special licence terms for systems that use or include AI?
There is no special contract law or other statutory regulations for the licensing of AI systems. It is therefore even more important to contractually fix rights of use, in particular to the data generated by the AI application.

4. BIAS AND DISCRIMINATION

The non-discriminatory use of AI systems is often discussed from a data protection perspective. For example, discriminatory AI applications would violate the fairness principle in Article 5(1)(a) of the GDPR. Transparency requirements can also be taken directly from the GDPR (Article 12 *et seq*. of the GDPR). In Germany, they are flanked by the strict law on general terms and conditions, which also applies in the area of data protection, for example to pre-formulated declarations of consent (BGH, judgment of 28 May 2020, I ZR 7/16). Clauses which are so unusual or surprising that they would not reasonably be expected to be encountered by a counterparty to a contract do not become part of the contract (section 305c(1) of the Civil Code) and clauses that unreasonably disadvantage the contractual partner are void (section 307(1) of the Civil Code).

4.1 Domestic anti-discrimination and equality legislation treatment

With respect to the use of AI, the provisions of the General Equal Treatment Act (AGG) must also be taken into account (see the large-scale study conducted by the Karlsruhe Institute of Technology at *www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/publikationen/Expertisen/studie_diskriminierungsrisiken_durch_verwendung_von_algorithmen.pdf*). The law prohibits discrimination in numerous areas of private legal transactions on the grounds of race or ethnic origin, gender, religion or belief, disability, age or sexual identity (section 1 of the AGG). Employment relationships or application procedures for filling a position are also affected (section 2(1) No. 1 of the AGG). Pursuant to section 22 of the AGG, it is not the person affected by discrimination who must provide proof of actual discrimination, but the party accused of discrimination must justify the non-

discriminatory nature of their decision. However, this facilitation of proof only applies if the person discriminated against can at least prove unequal treatment compared to other persons. This can be difficult, especially in the case of AI systems used online, because the person concerned will often have no knowledge of other comparable decision-making processes.

5. CYBERSECURITY AND RESILIENCE

The legal landscape in cybersecurity and resilience is dominated by EU legislative acts, some of which require implementation at the domestic level. Most recently, the EU has adopted a comprehensive Cyber Resilience Act (CRA), which will fully apply in all Member States by 2027. This regulation will be directly applicable across the EU. Additionally, the EU has reviewed and refined its Directive on the security of Network and Information Systems (NIS) (Directive (EU) 2016/1148), significantly expanding its application to businesses throughout the Union when implemented into national laws. These developments underscore the EU's commitment to enhancing cybersecurity and ensuring robust resilience against cyber threats.

5.1 Domestic technology infrastructure requirements

Though the CRA and NIS2 Directive (Directive (EU) 2022/2555) do not specifically regulate AI, both laws will have a significant impact on the industries of both AI development and use. The CRA aims to enhance cybersecurity for consumers and businesses by introducing mandatory requirements for products and software with digital components. It addresses two main issues: the currently inadequate cybersecurity levels of many products and the difficulty for consumers and businesses to assess and ensure cybersecurity. The Act establishes harmonised rules for bringing such products to market and mandates cybersecurity measures throughout their lifecycle. Products meeting these standards will bear a CE marking, indicating compliance.

The CRA complements existing legislation like the recently extended NIS2 Framework, which enhances cybersecurity preparedness and cooperation among EU Member States. The NIS2 Directive requires Member States to establish cybersecurity measures and cooperation mechanisms, particularly in critical sectors like energy, finance and healthcare. Additionally, it mandates security measures for essential service operators and digital service providers. The German law implementing the NIS2 Directive should have passed by October 2024. In the course of the legislative procedure, the Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSIG) will undergo significant changes.

6. TRADE, ANTI-TRUST AND COMPETITION

In the area of anti-trust and competition law, AI applications raise new questions. They are likely to exacerbate existing imbalances in digital markets. Regulations specifically tailored to AI do not yet exist.

6.1 AI related anti-competitive behaviour

In a joint study, the German Federal Cartel Office (BKartA) and the French Autorité de la concurrence concluded in 2019 that the use of algorithms could increase existing threats to free competition. Nevertheless, the existing legal framework was found sufficient to counter market abuse based on the use of algorithms (see Working Paper — Algorithms and Competition at *www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf*). However, the BKartA identified major problems in 2019 as part of a sector inquiry in the area of user ratings on the internet. Widespread use of algorithms could lead to incomprehensible decisions and rankings of different offers. In these circumstances the view of the BKartA was that the existing legal framework was insufficient to adequately punish such violations of consumer interests, especially because of the protection of algorithms as trade secrets (see Sector inquiry into comparison portals — final report at *www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Vergleichsportale_Bericht.html?nn=9624654*).

6.2 Domestic regulation

Section 19a of the Act against Restraints of Competition (GWB) has provided the BKartA with a special option since 2021: companies which, due to their strategic position and resources, are of particular importance for competition across markets can be prohibited by the BKartA from certain conduct as a preventive measure. Examples of such conduct include self-preferential treatment of the group's own services or obstructing the market entry of third parties by processing competition-relevant data.

Sections 5 and 5a of the German Unfair Competition Act (UWG) prohibit misleading statements or misleading by omitting certain information. Personal price calculations or dynamic prices can be misleading according to these standards if information is not provided about the individual price calculation. If there are discrepancies between the prices stated in advertising and the actual, personally calculated prices, further competition violations could be possible due to infringements of the Price Indication Ordinance (PAngV), which focuses on price clarity and price truth. The processing of personal data necessary for personal pricing can also be punished under competition law if a legal basis is missing or exceeded.

7. DOMESTIC LEGISLATIVE DEVELOPMENTS

Following the federal elections in September 2021, the parties forming the new government have formulated their plans under the title "Mehr Fortschritt wagen" (translated as "Dare More Progress") (see *https://cms.gruene.de/uploads/documents/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf*). The federal government agreed on some key aspects for fostering trust in AI systems: Digital civil rights, in particular freedom from discrimination, are to be strengthened and liability rules defined. In this context, the German government makes specific reference to the protection of employee rights in the context of the use of AI in the workplace. Innovation-inhibiting *ex ante* regulations are to be avoided.

7.1 Proposed and/or enacted AI legislation

The legal framework for AI in Germany is determined at the EU level. The upcoming AI Act and existing EU legislation (such as the GDPR, the new EU cybersecurity laws or EU copyright Directives), shape the legal landscape in Germany. There are currently no legislative initiatives at the domestic level that would focus specifically on AI.

7.2 Proposed and/or implemented Government strategy

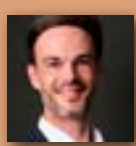
The German government formulated an AI strategy in 2018 (see Strategie Künstliche Intelligenz der Bundesregierung at *www.bundesregierung.de/resource/blob/997532/1550276/3f7d3c41c6e05695741273e78b8039f2/2018-11-15-ki-strategie-data.pdf*) and continuously emphasises the importance of AI to bolster Germany's position as a leading economic power. However the legal framework will continue to be significantly determined by initiatives at the European level, such as the AI Act.

The AI strategy sets out three core objectives for Germany:

- To become a leading AI location in order to secure future German competitiveness. This is to be achieved, in particular, through the creation or expansion of scientific research facilities and easier access to government funding programs for start-up companies.
- To ensure responsible and public welfare-oriented development and use of AI. The protection of human rights, including safeguarding workers' rights in the use of AI systems in the workplace, is a core objective.
- To ensure that AI applications are considered ethically, legally, culturally and institutionally, and brought into line with existing basic principles of social coexistence. The strategy emphasises the right to privacy and the preservation of existing data protection standards.

As early as December 2020, the German government contextualised and further developed its AI strategy (see *www.bmwk.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-fortschreibung-2020.pdf*) in the light of the backdrop of the COVID-19 pandemic, which highlighted widespread IT backwardness of small and medium-sized enterprises, and also of public services. The centrepiece of the German government's updated strategy was an increase in the budgetary resources earmarked for the development of Germany as an AI location to EUR 5 billion by 2025.

AUTHOR BIOGRAPHY



Alexander Tribess

Alexander Tribess is a founding partner at GreenGate Partners. He is a legal advisor to start-up/scale-up as well as well-established technology enterprises. His main focus is to reflect new technological developments in contracts and company compliance structures and processes. Alexander Tribess has published various articles on technology law and data protection matters in Germany and has contributed to international publications on the development of a legal framework for AI. He chairs the AI Substantive Law Committee of the ITechLaw Association.