IIC (2023) 54:1013–1043
https://doi.org/10.1007/s40319-023-01328-5

ARTICLE

Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information

Ulla-Maija Mylly

Accepted: 17 April 2023 / Published online: 3 May 2023

Abstract AI systems are nowadays employed in ever-increasing areas. This new era of technological development is exciting, but AI applications are also a cause for concern. If tasks that have hitherto normally been undertaken by human beings are now to be taken care of by ever more intelligent autonomous systems, how can we be certain that such functions are performed diligently and safely? Many areas of application of AI systems have also made the tribulations of AI utilization apparent. The EU's Artificial Intelligence Act (AIA) aims to tackle the concerns and challenges related to the utilization of AI, and to develop human-centric, secure, trustworthy, and ethical AI systems for the EU markets. The provisions of the AIA establish a system of compliance assessment that requires AI providers to disclose how high-risk AI systems have been trained and put together. This article will look at the role of disclosure obligations under the provisions of the AIA. The focus is on the tension between obligations to disclose information on the one hand and requirements to protect the trade secrets contained in the technical details of AI on the other. This article will explain how the technical details of AI contain some information that does not qualify for trade secret protection. And even when there are trade secrets, there are exceptions to trade secret protection. Rules to enable access to information form part of the Trade Secrets Directive, but other legislative instruments too enable access and make it necessary to navigate between access and confidentiality.

This article was produced in the framework of the Academy of Finland funded project Dissecting the Trade Secret Chimera in the Era of Data-driven Economy DISTRASEC (338849). The article was written while the author was a Visiting Researcher at Dickson Poon School of Law, King's College, London. I would like to thank Professor Tanya Aplin for her valuable comments on an earlier draft of this paper.

U.-M. Mylly (✉)
LL.D.; Academy Research Fellow (Associate Professor), Accounting and Commercial Law, Hanken School of Economics, Helsinki, Finland
e-mail: ulla-maija.mylly@hanken.fi

Keywords Artificial intelligence · Transparency · Trade secrets · Access to documents · Fundamental rights · Public interest

1 Introduction

Discussions on artificial intelligence (AI) are intensifying. Applications that can be defined as AI are utilized in artistic and inventive activities, in the financial sector, transportation, public administration, and the field of war.[1] While there is a lot of excitement around AI, new applications are also of concern to the ordinary person. If tasks that have hitherto normally been undertaken by human beings are now to be taken care of by ever more intelligent autonomous systems, how can we be certain that such functions are performed diligently and safely? These concerns primarily relate to our lack of understanding of how AI operates. But the issue is not just that we, the ordinary people, might not be literate in the technical details of building AI. These feelings of uneasiness are exacerbated when it is explained that even software engineers are not fully capable of capturing the inner logic of the self-learning algorithms.[2] Such systems are referred to as black boxes, which obscures our understanding and does not help in any way to generate trust in their utilization.[3]

Our concerns do not relate only to the technical opacity of the AI systems. Many areas of application of AI systems have made the tribulations of AI utilization apparent. In the area of law enforcement, potential biases regarding how AI is programmed can cause discriminatory end results that can have an enormous impact on a person's life and their fundamental rights. A particular challenge in this connection is that even in situations where the final decisions are made by human beings, humans might be too tempted to rely on the AI-based suggestions for final decisions.[4] Such over-reliance is called automation bias.[5] The issue, therefore, is

[1] When it comes to artistic activities, the question whether copyright law protects AI outputs has been subject to much discussion. *See* for example Hugenholtz and Quintais (2021). Similarly, suggestions have been made that AI should receive the status of inventor under patent law. Abbott (2016). For a discussion on how regulatory "innovation sandboxes" have been used in the area of financial sector innovations and how this model of regulation would serve well in other areas of regulating AI *see* Truby, Brown, Ibrahim and Parellada (2022). For a discussion on autonomous weapons under international law *see* for example Burri (2017).

[2] *See* for example, Burrell (2016). She describes the opacity of AI in three different forms: "(1) opacity as intentional corporate or state secrecy, (2) opacity as technical illiteracy, and (3) opacity that arises from the characteristics of machine-learning algorithms and the scale required to apply them usefully." *Ibid.* at 1–2.

[3] *See* Pasquale (2016).

[4] A very famous example from the US is the COMPAS program, which has been used in criminal sentencing decisions. The COMPAS program has been shown to be biased against black defendants. Even though it is intended to be used only as advisory guidance, judges have relied on the recommendations provided by it. *See* for example Rowe (2022), pp. 25–30. The COMPAS example shows both bias as a source of discrimination and automation bias.

[5] *See* the AIA (*see* the AIA definition in footnote 6) Art. 14(4)(b) "… remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons".

how to ensure meaningful human oversight when this is deemed necessary. What human oversight is required may depend on the AI's area of application: it is one thing if AI is used as a spam filter and another thing completely if it is used in public administration, such as for immigration decisions.

The EU's Artificial Intelligence Act (AIA) aims to tackle the challenges related to the utilization of AI.[6] Through the provisions of the AIA, the EU aims to develop human-centric, secure, trustworthy, and ethical AI.[7] These general objectives seek to go to the heart of the uneasiness that humans feel about AI applications to address the concerns just described. A human-centric approach means that human beings will be in control of the AI systems.[8] This seems to assume that it will become possible to explain AI systems. As a corollary of human control, accountability and trust are created.[9] For the objectives associated with secure and ethical AI, more detailed provisions of the AIA aim at ensuring the protection of health, safety and fundamental rights.

This article will look at the role of transparency and disclosure obligations under the provisions of the AIA. Meaningful human control, trust and accountability depend on sufficient transparency. The focus in this article is on the tension between rules relating to obligations to disclose information on the one hand and the requirement to protect trade secrets contained in the technical details of AI on the other. As trade secrets may create an additional layer of technical opacity,[10] it is important to define the role of trade secrets in context in a way that does not lead to too many secrecy claims or place an additional obstacle in the way of human oversight.[11]

After this introduction, Sect. 2 discusses the objectives of the transparency rules more generally, inter alia as part of public administrative laws and human rights

[6] Proposal for a Regulation laying down harmonised rules on artificial intelligence, 167 final, 84 final, 85 final. For the purpose of this article, it is mainly the text of the Council compromise text reached on 6 December 2022 that is utilized and referred to here as "the AIA". 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 – General approach (6 December 2022) ST 15698 2022 INIT. This version of the proposal is used, as it was the most recent text of the proposal at the time of writing this article. However, occasionally, the EU Commission proposal text is utilized, in which case it will be referred to as "the AIA proposal". However it is noteworthy that there are no drastic differences between the original EU Commission proposal and the compromise text for the parts discussed in this article.

[7] The AIA proposal Sec. 1.1. Reasons for and objectives of the proposal.

[8] This connection is particularly highlighted in the EU Parliament's JURI opinion on the AIA proposal. As important examples *see* recitals 6(a), 48(a), and Art. 4(a), 14(1), 52(1). In the JURI opinion, for example, education on AI literacy is emphasized. On the connection between the concepts of human-centric approach and human control *see* for example. Koulu (2020), p. 15.

[9] Koulu R (2020), pp. 33–34. In her paper, Koulu is critical of the issue whether humans can have control over AI. The AIA does not regulate liability for damages related to malfunctioning AI. For that purpose, the EU Commission has proposed a new directive for AI liability. COM(2022) 496 final Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). (Text with EEA relevance) SEC(2022) 344 final – SWD(2022) 318 final – SWD(2022) 319 final – SWD(2022) 320 final. There will also be changes for the EU product liability directive COM(2022) 495 – Proposal for a Directive of the European Parliament and of the Council on liability for defective products.

[10] *See* Pasquale (2011), p. 387.

[11] *See also* Sandeen and Aplin (2022), p. 453.

instruments. Sect. 3 moves on to elaborate on the AIA's specific objectives and the disclosure obligations of high-risk AI suppliers. This analysis will firstly look at what type of technical information is to be documented and critically evaluate whether the documentation requirements enable meaningful human control. Secondly, Sect. 3 will analyze to whom such documentation is to be disclosed: in other words, who will be in control of the AI systems' safety and other requirements. After looking at the disclosure requirements, Sect. 4 will discuss the confidentiality rules of the AIA, which aim at protecting documented technical information so that trade secret protection under the Trade Secrets Directive (TSD)[12] is not undermined by the disclosure obligations under the AIA. An important aspect in this section is that not all the documentation submitted can be assumed to qualify for trade secret protection. And even in cases where there are trade secrets, there are exceptions to that protection. Section 5 will analyze these exceptions and identify possible situations where such exceptions are relevant in the context of the AIA. This analysis will be complemented by one in Sect. 6 on law beyond the TSD that enables access to information under the rules on administrative access to documents. These legislative instruments, identified in the TSD, likewise seek to regulate how to resolve the tension between transparency and secrecy.[13] Section 7 will conclude the discussion.

The contribution this article makes is to combine discourses related to the various legal provisions that delineate rules on access to information and their relationship to trade secrets. The context of this interface analysis is the AIA, under which the flow of information is investigated. The argument is that trade secrets may not create such an obstacle to accessing information as one might initially assume from the AIA's confidentiality obligations. The aim of this article is to complement an analysis of the AIA rules on transparency and disclosure with one on the rules for human rights instruments and administrative laws in order to give a more complete picture of the legal setting for the purposes of transparency and openness. The specific rules under the TSD that enable access to information will also be elaborated on. While the focus will be on the specific context of the AIA provisions, this article aims to give a more holistic picture of access to rules on information and information even where there are trade secrets for protecting certain information.

[12] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1.

[13] In such administrative rules, openness of information is likewise connected to the accountability and legitimacy of the administration. Recital 2 of the Transparency Regulation (Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43) provides that "[o]penness enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system." In this article, the author applies the concept of accountability in the same sense as it is used in these administrative rules and explained in the recital wording.

2 Transparency as an Objective and Its Importance for Society

In discussions on law and technology, it has been acknowledged that technology may have an impact on human behavior in a similar way that the law does. Lessig has famously defined code as a law.[14] However, there is a legitimacy gap for such technology architectures if their production is not governed by democratic practices or subject to state authority.[15] One may expect the legitimacy gap for AI systems specifically to be addressed through the AIA's disclosure obligations when a public authority is given control over AI design. Furthermore, disclosure and transparency obligations under the AIA give the impression that we can gain access to the inner logic of the AI. We can see inside the black box. This leads to the assumption that it could be possible to have power and control over the design of the technology.[16]

One may question whether it is genuinely possible to achieve explainable AI or for the average person to understand the logic of self-learning algorithms if even software engineers may not be fully capable of grasping it. Essentially, in order for transparency to ensure accountability, information sharing must be meaningful.[17] The information needs to be both understandable and exact enough to allow for profound oversight. If technical information is over-simplified to make it more understandable for people, then it is no longer sufficiently exact.[18] And scrutinizing such information becomes futile. However, it has been pointed out that transparency does not necessarily mean full transparency. In essence, even though an explanation may not be complete, it may still be sufficient for the purpose of achieving meaningful control.[19] Furthermore, it has been highlighted that, because transparency as a governance model is an important part of democratic societies, the opacity and complexity of AI systems should not be used to make demands for transparency negligible.[20]

Alongside the theoretical discussions, in relation to law and technology, on the transparency of technology as a tool to tackle the legitimacy gap, transparency and openness principles are also an important part of administrative laws. Transparency is important for strengthening legitimacy and for ensuring control and accountability. Other important objectives of transparency under administrative laws relate to the promotion of good governance, to enabling participation and influence, and to supporting freedom of expression.[21] The administrative law that relates to transparency at the EU level and is relevant within the scope of the AIA too is the Transparency Regulation, which enables access to documents held by EU

[14] Lessig (2006).

[15] Hildebrandt (2008), pp. 176–178.

[16] Koulu (2021). In her article, Koulu argues that we should be able to see how the design process has been conducted, not so much how the end product operates. She further argues for the right to access the actual design processes. Such access rights should be given to users of a technology.

[17] Keller (2019), pp. 15–16.

[18] Hakkarainen, Koulu and Markkanen (2020), p. 23.

[19] Diakopoulos (2020), p. 212.

[20] Keller and Drake (2021).

[21] Mäenpää (2020) pp. 11–13.

institutions.[22] At the national level there are similar rules that enable access to documents held by national public authorities.[23] These rules will be discussed in depth in Sect. 6 below. They will operate in areas where public authorities make decisions, and are therefore applicable also in the context of the AIA when the public authorities become privy to relevant technical information after having carried out a conformity assessment.

In addition to being regulated by EU secondary legislation and corresponding national legislations, the need for access to documents is also recognized in the EU Treaty provisions[24] and as a human right under the EU's own fundamental rights instrument. Article 42 of the EU Charter of Fundamental Rights ("Charter") provides for the right to access European Parliament, Council and Commission documents.[25] This right of access is very closely connected to the right to freedom of expression, most importantly because one component of freedom of expression is access to information.[26] Article 11(1) of the Charter provides that "[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to *receive* and impart *information and ideas* without interference by public authority and regardless of frontiers" (emphasis added).[27] This provision is in line with Art. 10 of the European Convention on Human Rights (ECHR) (on freedom of expression).[28] At the international level, a very similar freedom of expression provision is stipulated in Art. 19 of the International Covenant on Civil and Political Rights.[29]

Consequently, the AIA's rules on disclosure and transparency fulfill very important objectives. These objectives form part of core fundamental rights as well

[22] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

[23] In Finland the relevant legislation is the Act on the Openness of Government Activities 21.5.1999/621. The Act stipulates that official documents are in the public domain unless specifically provided otherwise in that Act or another Act (para. 1 of the Act). The Act contains provisions on the right of access to official documents (paragraph 2 of the Act).

[24] Article 10 of the Treaty on European Union stipulates that open decision-making is carried out "as closely as possible to the citizen". The Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390. The Treaty on the Functioning of the European Union (TFEU) stipulates in Art. 15 that the EU institutions are obliged to act publicly and to ensure that individuals and any natural or legal person residing or having its registered office in an EU Member State can access documents. The Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390.

[25] All EU citizens and residents, including legal entities having their registered office in any EU Member State, have this right. The Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

[26] The access-to-information component of freedom of expression has been recognized in the ECtHR case law. *See* for example, *Youth Initiative for Human Rights v. Serbia*, 2013 ECtHR Appeal No. 48135/06; *Erhaltung v. Austria*, 2013 ECtHR Appeal No. 39534/07.

[27] Article 11(2) of the Charter further provides an explicit right to freedom for the media by stipulating: "the freedom and pluralism of the media shall be respected".

[28] Article 52(3) of the Charter links the interpretation of the Charter to the ECHR by providing that "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and the scope of those rights shall be the same as those laid down by the said Convention [...]".

[29] The International Covenant on Civil and Political Rights. Adopted by the General Assembly of the United Nations on 19 December 1966 (ICCPR).

as of administrative rules related to good governance, all of which are vital for democratic societies in both Europe and other countries. Therefore, matters of transparency are by no means only theoretical. For that reason, it is crucial to analyze the objectives of the AIA rules and whether the new legal setting under the AIA is in line with the fundamental values just described.

3 The AIA Rules on AI System Providers' Disclosure Obligations

3.1 What Type of Documentation is Required for Technical Information

The AIA aims, inter alia, to address questions related to the fact that AI systems are opaque, complex, biased, unpredictable, and autonomous.[30] In order to tackle these challenges, the AIA defines clear rules on the detailed technical requirements to be met by high-risk AI systems before they are placed on EU markets.[31] In the AIA, the mandatory requirements regarding technology and the documentation thereof are quite comprehensive. The discussion here will cover some important examples of the requirements in order to shed some light on the layers of technical documentation requirements and how these help achieve the AIA's objectives. In addition to the requirements for technical documentation, the AIA lays down rules for assessing compliance on the basis of this documentation and, for that purpose, disclosing documentation to the various compliance assessment institutions. To whom the documentation is disclosed will be discussed after this sub-section.

When it comes to the bias problem, the proposal complements existing EU law on non-discrimination.[32] To mitigate the risks related to potential biases underlying the technical details of the AI systems, the AIA sets out clear rules on data quality and documentation requirements.[33] The objective of high data quality is to ensure that an AI system does not become a source of discrimination.[34] Therefore, training, validation and testing data used in building the AI should be relevant, representative and, as far as possible, free of errors and complete.[35] It is noteworthy that the AIA

[30] The AIA proposal's background text referring to Council of the European Union, Presidency conclusions – The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20, 2020.

[31] In this article, the discussion will not cover challenges with regard to the evaluation of risk. The AIA lays down the requirements, which are discussed in this article only for high-risk AI. For discussion about problems related to the risk-based approach *see* Mahler (2022).

[32] AIA Proposal's background text Sect. 1.2. Discussion on how non-discrimination law is insufficient in tackling the biases in AI systems *see*, for example, Grozdanovski (2021).

[33] Article 10 of the AIA and Annex IV. 2(d) and 2(g). Quality management systems are also applicable to the datasets (Art. 17(1)(f) of the AIA).

[34] Recital 44 of the AIA.

[35] Article 10(3) of the AIA. The requirement that data be representative relates to the issue that any misrepresentation in the data sample of part of the population might lead to biases in respect of that group of people. In essence, any shortfall in the sample makes the data invalid and therefore more prone to errors. This type of error is very common. Hacker (2018).

rules require also monitoring, detection, and correction of biases subsequently.[36] Requirements with regard to data quality have been attributed specific importance under the AIA: infringements of these requirements are subject to higher administrative fines than other forms of non-compliance.[37]

The AIA aims to mitigate not only the biases related to data quality, but also the automation bias. Automation bias is the tendency that human beings have to automatically rely or over-rely on output produced by a high-risk AI system. To tackle automation bias, the AIA establishes rules that enable human beings to remain aware of the bias. This is a particularly important issue for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons.[38] If human beings were to rely solely on recommendations produced by AI, the human oversight required in specific situations would become meaningless. The importance of human oversight is part of the EU's aim to have human-centric AI.[39] To this end, AI system providers must include in the documentation also an assessment of the human oversight measures needed.[40]

Another important requirement is that when AI is used, there must be record-keeping measures in place, for example, in the form of logs.[41] These record-keeping details can be seen as important ways of monitoring the system features in the event, for example, of any malfunctioning of self-learning algorithms. These rules enable *ex ante* detection of errors. With these requirements, the AIA aims to reduce the risks involved in using autonomous systems. Human oversight, control and participation in all phases is of paramount importance. When we have meaningful human oversight for AI systems, we simultaneously generate trust in the utilization of AI.[42] The rules in place that require human control over AI systems seem like one option for demystifying AI, which can be seen as an important factor in enabling the creation of trust.

When it comes to other details of the technical documentation, the AIA requires information on the hardware and software environment that the AI system will form part of. Descriptions of the methods and steps performed for developing the AI system also need to form part of the documentation. In cases where an AI provider has utilized pre-trained systems or third-party tools, the description needs to give details of how these have been used, integrated, or modified by the provider. Such requirements are more focused on the question of how AI will work together with other systems and components, in other words the technological environment in which it is intended to operate.[43] Likewise, the documentation requirements for a

[36] Articles 9, 10(5) and 61 of the AIA. For this purpose, it may be possible for AI providers to process personal data. Discussion of the General Data Protection Regulation (Regulation (EU) 2016/679) is outside the scope of this article.

[37] Article 71(3) of the AIA. High fines in addition to data management requirements relate only to the complete prohibitions of certain AI systems under Art. 5 of the AIA.

[38] Article 14, fourth paragraph, indent (b) of the AIA.

[39] Koulu (2020), p. 15.

[40] Annex IV.2(e) of the AIA.

[41] Article 12 of the AIA.

[42] Koulu (2020).

[43] The technical documentation requirements in Annex IV of the AIA include a lot of references to this type of information.

specific AI system have various levels of abstraction. First of all, the documentation needs to include the design specifications of the system, the general logic of the AI system and the logic of the algorithms. Documentation must also describe the key design choices, including the rationale and any assumptions made, as well as the relevance of the different parameters. This illustrates how comprehensive the documentation requirements are.[44]

However, the documentation requirements are rather abstract. For example, the general logic of the algorithms needs to be defined. Even though algorithms may sometimes be understood as a reference to the source code, they cannot be interpreted in this way in the AIA. This is clear because there is a specific reference to the source code in another provision of the AIA.[45] The question arises whether documentation without source code is sufficient: whether a profound evaluation can be made of safety and risk in relation to fundamental rights without sufficient details.[46] As explained in Sect. 2 on the objectives of transparency, information for transparency purposes needs to be sufficiently meaningful. Otherwise, oversight of the information provided is pointless. We can assume that source code at least will provide sufficiently detailed information. Even though the initial *ex ante* evaluation and disclosure obligation do not include source code, when the market surveillance authorities (public authorities) later assess AI systems' compliance with the AIA requirements, they will have access to the source code in cases where they have made a reasoned request and where specific cumulative conditions have been fulfilled.[47] This later reference to access to the source code for compliance assessment purposes suggests that, with regard to *ex ante* evaluation too, a proper assessment of the AI system may require analysis of the source code. In academic discourse, it has been highlighted that different stakeholders may require different types of access to explanations of AI logic. It has been suggested that regulatory bodies and external audit bodies in particular need access to a wide range of information. The same is true for NGOs who serve the public interest by checking that AIs are safe and do not infringe privacy issues.[48]

This is not the first time that academic discussion has focused on the requirements for software source code disclosure. In the area of software patents, the fact that patent offices do not require patent applicants to disclose the source code of their software-related inventions has drawn criticism both in Europe and on

[44] For more *see* Annex IV of the AIA.

[45] Article 63(9). Under the White Paper the requirement referred to the documentation on the programming. EU Commission (2020) 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust', Brussels, 19.2.2020 COM (2020) 65 final, p. 19. Some have understood this White Paper reference as requiring both object and source code documentation for the AI system. Alì and Yu (2021), Sect. 5.1.

[46] It has been pointed out also that source code alone is not sufficient for the analysis. This is because, for the detection of biases and other errors, it is the model rather than the exact implementation that is more important. *See* for example Rowe (2022), p. 22. The AIA's provisions already require various design features to be described. These include documentation on the key design choices, including the rationale and any assumptions made, and the relevance of the different parameters.

[47] Article 63(9) of the AIA.

[48] Matulionyte and Aranovich (2022), p. 414.

the other side of the Atlantic.[49] Under patent law, shortcomings in the disclosure requirements have consequences in the form of uncertainty about the scope of patent rights. Such uncertainty may mean that third parties have insufficient information to analyze whether their own product implementations infringe a patent. Moreover, insufficiency of disclosure goes against the fundamental theory and objective of patent law. Under the patent systems' "bargain" theory, a patent monopoly is given in return for the disclosure of a patentable invention. Therefore, the disclosure obligation and its sufficiency are of paramount importance for the patent system.

Similarly, under the AIA rules, insufficient requirements for technical documentation and their disclosure lead to uncertainty. And, within the context of the AIA, such uncertainty affects fundamental issues underlying an important objective of the AIA, namely, that of evaluating whether AI systems are safe, ethical and non-discriminatory. The question is whether, without source code, the information provided for the initial *ex ante* compliance assessment is sufficient for the purposes of detecting potential errors and biases.

It is not only the details of the technical documentation that are important for carrying out the assessment under the AIA rules. What is also crucial is who is conducting the evaluation and in what capacity, since this will have an impact on the legitimacy of AI systems. As explained in Sect. 2, one of the objectives of transparency is to address the legitimacy gap related to technology architectures. The next section will examine the key features and problems in the AIA's evaluation system.

3.2 To Whom the Information will be Provided and When

The first phase of evaluation, *ex ante*, is done either by the AI system provider itself or by the notified bodies (compliance assessment bodies), which may be private entities qualified to assess the technology in question. In cases where there is already an evaluation procedure in place, for example for machinery and medical devices, the evaluation procedure will continue to follow the same route and evaluation system under those previous rules. Such evaluation will also cover the requirements that will become operational through the AIA if a product has an AI component.[50] It has been estimated that, because of the possibility of relying on self-assessment and because of the pre-existing assessment procedures, the new notified bodies, which will be established under the AIA, will have only a very limited role in the *ex ante* evaluation procedures.[51] However, their involvement is required, for example, in specific high-risk AI categories if the AI system is not fully compliant with the existing standards or if there are no standards or common specifications.[52]

[49] For European discussion *see* for example Mylly (2011); for US *see* Lemley and Cohen (2001); for Canada *see* Tomkowicz (2010), p. 221.

[50] Articles 43(1) and 43(3) of the AIA.

[51] Veale and Zuiderveen Borgesius (2021), p. 106.

[52] Article 43(1) of the AIA. At the moment, the AIA only lists, in Annex III, point 1, remote biometric identification systems in this category. Mökander, Axente, Casolari and Floridi (2022), p. 250. The EU

In cases where AI providers for AI systems can apply harmonized standards, they are allowed to rely on the presumption of conformity under Art. 40 of the AIA.[53] This further means that, when AI systems are built in compliance with the standards, it will be sufficient for the AI system provider to rely on its self-assessment of conformity even in cases that would otherwise require a third-party assessment. Consequently, applying standards and self-assessment is assumed to become a preferred route for *ex ante* control for compliance, because standards will provide more legal certainty for an AI supplier than when an AI provider fixes the parameters for fulfilling technical requirements itself.[54] Yet it is noteworthy that, for many high-risk AI systems, self-assessment is allowed even where AI systems are not in compliance with existing standards.[55]

The role of self-assessment has been heavily criticized.[56] It is true that, from the outset, self-assessment does not seem to contribute much to transparency, trust, or accountability. However, all providers of AI systems must register high-risk AI systems in an EU-wide database before placing the system on the market or putting it into service.[57] The EU database will contain inter alia the contact details of the AI provider and identification of the AI system. It will also contain information on the EU declaration of conformity in cases where there has been self-assessment. In the case of third-party assessment, the database will contain information about the certificate issued by the notified body.[58] The database will be managed by the EU Commission. Most of the information contained in the EU database must be made accessible to the public.[59]

With the information registered, citizens and compliance assessment bodies can, arguably, verify whether the high-risk AI system complies with the requirements laid down in the AIA and can in this way exercise enhanced oversight over AI systems.[60] The shortcoming in the database and in the possibility of having oversight of AI systems lies in the fact that the database itself will not contain any technical documentation.[61] But a natural or legal person who has reason to believe

Footnote 52 continued
Commission has estimated that the relevant standards will become available when the AIA enters into force. European Commission, Impact Assessment accompanying the 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), 57. Even though there are a lot of standardization efforts on-going around AI technologies, it has been questioned whether such standards will be applicable when the AIA comes into force. Ebers (2022), Sec. 22.3.3.

[53] Similarly, conformity can be presumed when AI systems comply with the common specifications set up by the EU Commission. Article 41 of the AIA.

[54] Ebers (2022), Sect. 22.4.7

[55] Article. 43(2) of the AIA, Annex III, points 2–8.

[56] Veale and Zuiderveen Borgesius (2021), p. 105.

[57] Articles 16(f), 51(1), 60, and Annex VIII of the AIA.

[58] Annex VIII of the AIA.

[59] Article 60(5a) of the AIA.

[60] The AIA proposal background text, Sect. 5.1.

[61] *See also* Ebers, Hoch, Rosenkranz, Ruschemeierand Steinrötter (2021), p. 597.

that there has been an infringement of the provisions of the AIA may make a complaint to the relevant market surveillance authority, which will then conduct an assessment.[62]

When it comes to the possibility of relying on self-assessment, it is noteworthy that, in specific cases, self-assessment requires AI implementation to comply with the relevant standards. Information on how to implement a technology in accordance with a standard must be made available on the markets to everyone.[63] Consequently, information on standard-compliant AI systems' technical details is transparent to some degree.[64]

Trust and accountability in these situations depend to a high degree on the robustness in the standard-setting procedure and on the AI provider's self-assessment. Even though the standardization process is open to participation, many stakeholders, including consumer organizations, may not have sufficient resources and expertise to participate. Moreover, the procedure is essentially vested with private entities, and the EU Parliament, for example, does not have a say on the outcome. In the standard-setting procedure, private entities' decisions are beyond democratic control. Hence, the AIA's reliance on standards has been criticized also for a lack of legitimacy.[65]

When the *ex ante* compliance assessment is done by third-party notified bodies, the suppliers of high-risk AI systems need to provide technical documentation to these bodies so that they can examine the AI systems' compliance with technical and other requirements under the AIA.[66] The technical information about AI implementations in these cases will not become part of public knowledge or be provided to the EU database, and technical details cannot be detected even as well as standards can. Therefore, the role of private entities in the compliance-assessment procedure does not generate much transparency for the underlying details of AI systems. However, the EU database will contain information about the compliance assessment conducted and any certificate received.[67] Yet the AIA requires that, in cases where the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as by EU institutions, bodies or agencies, then the *ex ante* third-party evaluation will be carried out by the market surveillance authority, which in these cases will serve as a notified body.[68] This requirement shows that there is a clear need to assign important assessments to the public authorities. However, one might assume that this type of requirement would be needed for all high-risk AI systems and at least in those cases where these systems have consequences for fundamental rights.

[62] Article 63(11) of the AIA. This provision was added in the compromise text adopted 6 December 2022.

[63] However, exact documentation is subject to fees. Veale and Zuiderveen Borgesius (2021), p. 105.

[64] However, it will be challenging to identify when AI systems have been built in compliance with the standards, especially in those cases where AI providers are allowed to conduct self-assessment anyway.

[65] Veale and Zuiderveen Borgesius (2021), p. 105.

[66] Articles 11 and 19 of the AIA.

[67] Annex VIII of the AIA.

[68] Article 43(1) of the AIA.

In addition to *ex ante* evaluations, there are also *ex post* control mechanisms in place. If an AI provider detects any serious incidents with the AI system, a provider needs to inform the national market surveillance authority within a short time frame. "Serious incident" means any incident or malfunctioning that directly or indirectly leads, might have led, or might potentially lead, to death or to serious damage to a person's health, to property or to the environment. Serious incidents also cover situations where the management and operation of critical infrastructure are seriously and irreversibly disrupted.[69] Another example of a situation where market surveillance authorities will play a role is when the market surveillance authority of a Member State has sufficient reason to believe that an AI system presents a risk to health, safety or fundamental rights.[70] This may, for example, stem from a complaint made by a natural or legal person. In these situations, the market surveillance authorities will evaluate compliance on the basis of documentation already gathered but may also ask for further information. Importantly, they may be granted access to the source code of the AI system.[71] It is notable that access to the source code is quite restricted.

The *ex post* evaluation is conducted by entities referred to as public authorities under the provisions of the AIA.[72] In specific situations, the EU Commission may also become involved, for example when the risks related to an AI system are not restricted to the territory of one Member State. In specific cases, the EU Commission will evaluate whether, in the case of non-compliant AI systems, national measures taken by market surveillance authorities can be considered justified.[73] In these instances, the EU Commission will also become privy to the relevant technical information.[74]

The fact that the first phase of evaluation is conducted by AI providers themselves or by notified bodies, which are most likely private entities, does not seem to address the legitimacy question sufficiently. Moreover, the reliance on standards has been criticized owing to lack of democratic control in the setting of standards. It is noteworthy here that the initial plan was to have a centralized EU agency for *ex ante* evaluation.[75] This would have meant that AI systems were under, and reliant on, public authority control from the beginning. Now the proposal takes a decentralized approach to compliance assessment. One possible reason for the current approach may lie with the aim of finding proportionate regulatory solutions.[76] The fact that public authorities are not conducting the *ex ante* evaluation is not only problematic for reasons of legitimacy, but also has important

[69] Article 3(44) of the AIA.

[70] Article 65 of the AIA.

[71] Article 64 of the AIA.

[72] Article 3(26) of the AIA.

[73] Article 65 and 66 of the AIA.

[74] Article 65(6) of the AIA.

[75] White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, Brussels, 19.2.2020 COM(2020) 65 final.

[76] Also, the categorization of risks and the focus in the AIA proposal on tackling a specific type of risk is considered to stem from the objective of proportionality. Mahler (2022), p. 247.

consequences for the scope of transparency of the technical information. These effects will be discussed more thoroughly in Sect. 6, which elaborates on the possibilities for the general public of having access to and oversight of the relevant documentation.

4 The Specific Rules on Confidentiality Under the AIA and the TSD

When public authorities and notified bodies carry out their tasks to check compliance of AI systems, they are given access to vast amounts of detailed information on how those AI systems are put together. As explained above in Sect. 3, this information might sometimes include the source code of an AI system. The AIA rules impose obligations on those public authorities and notified bodies with regard to confidentiality. Article 70 of the AIA requires that:

> [n]ational competent authorities, notified bodies, the Commission, the Board, and any other natural or legal person involved in the application of this Regulation shall, in accordance with EU or national law, put appropriate technical and organisational measures in place to ensure the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:
> (a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply.

This is the specific Article in the AIA that mentions intellectual property rights and trade secrets and the requirements for protecting them. The other references to confidentiality throughout the AIA relate explicitly to this Article. It is important to note that, unlike in some other recent or pending EU proposals and regulations that relate to the data economy, such as the proposed Data Act,[77] the disclosure obligations and rules on access to information under the AIA do not aim to give others a right to utilize information for their own commercial purposes. As already explained, the objective of the AIA is to ensure that AI systems used within EU markets are safe and respect fundamental rights. Any information provided is for checking that systems comply with the set requirements. The importance of such provisions under the AIA is to ensure that disclosure obligations for the purpose of compliance assessment do not compromise trade secrets or the protection of intellectual property. In essence, trade secret protection is protection against unlawful access to information.[78] However, the TSD already defines rules that enable access to information notwithstanding trade secret protection. Article 70 of

[77] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.

[78] Wiebe and Schur (2019), p. 814.

the AIA refers to these and clarifies that exceptions under Art. 5 of the TSD are fully applicable.

When analyzing Art. 70 of the AIA, the first issue that catches the attention is the phrase regarding the requirement for protection for intellectual property rights *and confidential business information or trade secrets*. It is somewhat ambiguous how this should be interpreted. One way of understanding it is that confidential business information might not have an independent meaning in this phrase. This interpretation can be derived from the fact that "confidential information" is referred to as an alternative to "trade secrets"; this is done by use of the word "or" instead of "and", and by the separation, using commas, of this part of the sentence from the rest of the provision. The expression seems to refer to the longer name of the TSD where "undisclosed know-how and business information" is correlated with "trade secrets".[79] Later, the TSD uses only the concept "trade secret", which it defines. Therefore, it is possible to interpret this phrase of the AIA in the sense that "trade secrets" and "confidential business information" are used interchangeably to mean the same thing and that the TSD's definition of trade secrets will be decisive here.[80] In this article, the focus is in any case on the role of trade secrets under the AIA and any relevant exceptions to that protection.

In this respect the dilemma at hand relates to the uncertain nature of trade secrets. Trade secrets are not registered rights. Therefore, when notified bodies or public authorities are deciding whether there is a trade secret subject to confidentiality obligations, there might be only the putative trade secret holder's claim or belief that a trade secret exists. However, this is not sufficient for establishing trade secret status and keeping information confidential.

The TSD lays down clear criteria for trade secrets. Article 2(1) of the TSD defines trade secrets as "information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; [and] (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret". The criteria under Art. 2(1) of the TSD

[79] This interpretation is also supported by the German language version of the Art. 70(1)(a) "Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen, auch Quellcodes, mit Ausnahme der in Artikel 5 der Richtlinie 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung genannten Fälle". The German version of the text uses the concept of "confidential business information" consistently without reference to "undisclosed business information". Similarly, the German version of the title of the TSD does not refer to the term "undisclosed" but applies the term "confidential know-how" and "confidential business information" for trade secrets. "RICHTLINIE (EU) 2016/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung".

[80] However, it is not denied by the author of this article that, under the first sentence of Art. 70(1) of the AIA, obligations re confidentiality also cover obligations other than those deriving from the TSD. However, Art. 70 provides the most relevant reasons for protecting confidentiality under the AIA by providing the most important examples and rules therefor.

are in line with the TRIPS Agreement definition of undisclosed information in Art. 39(1) thereof.[81] This definition also resembles the definition applicable in the US, albeit with some slight differences.[82]

Sandeen and Aplin recently highlighted in their academic work that AI systems, while potentially very complex, might not contain much information that qualifies for trade secret protection. They emphasize that, if trade secret rules were applied appropriately, some concerns relating to the lack of transparency in AI systems would be addressed.[83] Therefore, for reasons of transparency, it is of paramount importance to dissect what information does not qualify for protection.

The first important threshold for trade secret protection is that the information be secret in the sense of not being generally known or readily accessible to persons that normally deal with that kind of information. This does not mean that the information has to be known to the general public: it is sufficient that it be generally known in relevant industry circles.[84] Therefore, information that is common knowledge to AI experts in a specific field should not be considered to fulfill the requirement of secrecy. The development of AI systems may depend on a great deal of basic science components and pre-existing software modules. In addition, AI systems contain many components that utilize data and information gathered from publicly available sources. One relevant example is third-party mapping information and photographs utilized in the development of automated vehicles. Such components are publicly available information that does not meet the secrecy requirement.[85] Likewise, methods used in training AI might apply known methods commonly utilized in the non-digital environment.[86] However, the specific way in which such generally known components are put together might qualify as a trade secret.[87] There is also a time dimension to trade secrets as, over time, secrecy might also be lost. This may occur, for example, through third-party reverse engineering or independent development, both of which are lawful practices under the TSD. These lawful acquisitions may lead to information disclosures, which cause a loss of secrecy.[88]

[81] Schovsbo (2020), p. 17.

[82] Sandeen (2020), pp. 49–50. Owing to similarities, US materials are also occasionally used in this article as a reference material for possible interpretations.

[83] Sandeen and Aplin (2022), pp. 444–445.

[84] Sandeen (2020), p. 48.

[85] Sandeen and Aplin (2022), pp. 445–447. Likewise, Drexl explains how information on public roads that has been collected by autonomous vehicles does not meet the secrecy prerequisite. Drexl (2017), p. 269.

[86] Sandeen and Aplin (2022), p. 452.

[87] This is referred to as a "combination trade secret". Graves and Macgillivray (2004), p. 266. The TSD seems to explicitly recognize the possibility of combination trade secrets because the definition in Art. 2(1)(a) refers to "a body or […] the precise configuration and assembly of its components" that needs to be secret. Nordberg has argued that, for example in the area of big data analytics, a specific configuration of data could meet the requirements of trade secret protection, even though just the sum of the information, i.e. a collection of information, might not meet the requirements when the information is derived from publicly available sources. Nordberg (2020), pp. 204–205.

[88] Mylly (2021b), p. 1326. However, copyright rules allow reverse engineering only for specific purposes. Ibid.

The AIA envisages that, to comply with its substantive obligations, AI systems must be implemented in a manner that complies with the technical standards applying in specific fields. For example, when standards are applied, the AI system is assumed to comply with the AIA's technical requirements.[89] One may therefore assume that AI systems within EU markets will contain many elements that borrow from standards. What is important here is that standards are open. In essence, the information on how to implement a technology in accordance with a standard's technical teaching must be available to all.[90] Therefore, insofar as an AI system applies a publicly available standard, such implementation details cannot qualify as trade secrets.[91] This reduces the extent of trade secrets in these systems.

What Sandeen and Aplin further emphasize is that, even though some information could be considered as actually being secret or might be treated as secret by the AI developer, it still might not meet the other requirements under the TSD. What needs to be borne in mind is that trade secret criteria are cumulative. This is clear from the definition in Art. 2(1) of the TSD, which stipulates that all the requirements must be met. For the commercial value requirement, one can assume that the criterion is typically easy to fulfill, as AI systems, including the underlying software elements, normally do have some commercial value.[92] Likewise, collected datasets, which are used, for example, in the training of AI and are to be documented under AIA rules, can be considered to have commercial value, as there are markets for such data. These views about commercial value stem from the fact that the TSD's definition of commercial value is inherently quite broad, for example covering both actual and potential commercial value.[93] However, the definition in Art. 2(1) of the TSD could be interpreted as meaning that, to have commercial value, information must give the holder of the information some competitive advantage. Most importantly, commercial value needs to be derived from the parts of the AI system that satisfy the other two trade secret requirements as well. Article 2(1)(b) of the TSD explicitly stipulates that, to qualify for trade secret protection,

[89] Standards are put in place to ensure uniformity, for example, for safety purposes. Ullrich (2017), p. 13. As the objective of the AIA is to have trustworthy and safe AI, reference to and the relevance of standards in high-risk AI implementations is understandable. This is exactly why standards are often adopted.

[90] Ullrich (2017), p. 14.

[91] This does not mean that AI systems would not be subject to IP protection. Standards often contain patented inventions. Therefore, even though the information on how to implement a standard is available to all, one might not be able to implement it without paying licensing fees or royalties for use of the underlying patented technology. The licensing of patented technology essential for a standard is subject to FRAND terms, meaning that terms must be fair, reasonable, and non-discriminatory. Contreras (2017). In addition, software implementation can also be protected through copyright. However, if technical requirements, for example standards, limit copyright creativity, copyright does not protect such parts of the implementation. In the *BSA* case, which was about the protection of a program's graphic user interface, the CJEU held that components of the graphic user interface that were differentiated only by their technical function could not be protected as the author's own original creation. Where the expression of those components was dictated by their technical function, the criterion of originality had not been met, since the different methods of implementing an idea were so limited that the idea and the expression became indissociable. C-393/09, *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury*, ECLI:EU:C:2010:816 paras. 48–50.

[92] Mylly (2021b), p. 1326.

[93] *See* Aplin (2017), pp. 59–72.

information must "have commercial value *because it is secret"* (emphasis added). As the TSD is quite a recent legislative instrument, there is not yet any EU case law on how this requirement should be interpreted.[94] However, it becomes clear from the phrases used that this criterion further narrows down the information that can qualify as a trade secret. In essence, it is not just the general commercial value of the AI system overall that is decisive here.

The last requirement under the TSD is that the person lawfully in control of the information take reasonable steps under the circumstances to keep it secret. This requirement has been identified as serving the "notice" function for trade secret information, whereby a holder of information informs third parties about the existence of a trade secret. It has been suggested that, under the TSD, the activities that qualify as reasonable steps depend on how the context is evaluated, with the value of the trade secret also having an impact. This is similar to the US doctrine, but it is most likely that there will also be some minimum objective requirements to be met.[95] There are various ways of fulfilling the reasonable steps requirement, including technical protection measures, physical safe-keeping, contractual clauses[96] and managerial procedures dealing with the internal processes vis-à-vis employees of an enterprise.[97] For data-driven networked environments, technical encryption measures have been considered to play a particularly important role.[98] It is clear that some activity is required and that measures need to be such that third parties are made clearly aware of the existence of trade secrets.[99] It is also noteworthy that, even though contractual arrangements play an important role in creating reasonable steps, one cannot use contracts to create trade secret protection for information that cannot otherwise be protected.[100] This is clear from the definition of "trade secret", which confirms that all of the requirements have to be met.

An analysis of the definition of "trade secret" makes it clear that the way the reference in Art. 70 of the AIA to the source code is written is confusing, as it gives the impression that source code would invariably qualify as a trade secret. This kind of general assumption cannot be made. Firstly, as discussed, many design elements underlying AI systems form part of common knowledge, or else AI implementation is based on information derived from publicly available sources, including standards. Therefore, these parts of the source code cannot qualify as trade secrets. In addition, an AI supplier might have also relied on an open-source model when

[94] Radauer, Bader, Aplin, Konopka, Searle, Altenburger and Bachner (2022), pp. 76–77. For the US *see* for example Hrdy, (2021). However, the definition in the US is slightly different than the EU TSD definition. In the United States, the UTSA stipulates that the information must ''[derive] *independent economic value*, actual or potential, from not being generally known or readily ascertainable by other persons *who can obtain economic value* from its disclosure or use'' (emphasis added) UTSA Sec. 1(4)(i).

[95] Radauer, Bader, Aplin, Konopka, Searle, Altenburger and Bachner (2022), p. 80.

[96] Knaak, Kur and Hilty (2014), p. 957. For managerial measures *see* Radauer, Bader, Aplin, Konopka, Searle, Altenburger and Bachner (2022), pp. 38–39.

[97] Radauer, Bader, Aplin, Konopka, Searle, Altenburger and Bachner (2022), pp. 38–39.

[98] Wiebe and Schur (2019), p. 8019.

[99] Mylly (2021b), p. 1330.

[100] This interpretation has been adopted in the US at least. *See* Sandeen (2020), p. 49.

implementing an AI system. Or at least some parts of the system may depend on open-source modules.[101] Even though in situations where AI implementation is based on an open-source model, it is unlikely that the developer would seek confidentiality, it is still important to highlight here that this is one of many instances where source code cannot be assumed to be a trade secret. Other technical documentation required under AIA rules might likewise lack trade secret protection.[102]

Consequently, it is important for various institutions, both within the context of the AIA and beyond, to understand the concept of the trade secret in order to be able to make correct decisions on the scope of confidentiality required. This cannot be based on the putative trade secret holders' own evaluation and demands for confidentiality. Therefore, the notified bodies and public authorities that conduct the compliance assessment under the provisions of the AIA need to be equipped to evaluate the TSD's criteria for trade secret protection, as this is what essentially defines the scope of their confidentiality obligation. In addition, even when there are trade secrets, there are exceptions to trade secret protection that need to be taken into consideration. These will be examined in the next section.

5 Exceptions to Trade Secrets Owing to Freedom of Expression and Whistleblowing

Interestingly, the AIA refers not only to the trade secret protection available under the TSD but explicitly also to the exceptions applicable thereunder. Article 70(1)(a) of the AIA requires that trade secrets be protected except in the cases referred to in Art. 5 of the TSD. This section elaborates on the two most important exceptions under Art. 5 of the TSD. According to that Article, the measures, procedures and remedies provided for in the TSD should be dismissed "where the alleged acquisition, use or disclosure of the trade secret was carried out […]: (a) for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media; [or] (b) for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest".[103]

In order to appreciate the scope of Art. 5 of the TSD, we need to understand the scope of freedom of expression as a right under the Charter. Article 11(1) of the Charter provides that "[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and

[101] *See also* Sandeen and Aplin (2022), p. 11. Likewise, datasets can be part of open data movements. *See* Aplin (2017), p. 66.

[102] Copyright and patent law may protect actual implementation even when there is no trade secret protection. The scope of these forms of protection is not analyzed in this article.

[103] Freedom of expression as a fundamental Charter right is as such an exception to trade secret protection. It has been recognized as a very particular way of bringing a fundamental right into the heart of trade secret rules. *See* Mylly (2021a), p. 196. The wording of this provision has made academics question whether it can even be understood as an exception or whether it is rather a rule that requires the balancing of various interests. Aplin (2021), p. 188.

ideas without interference by public authority and regardless of frontiers". Article 52(3) of the Charter links the interpretation of the Charter to the ECHR by providing that "[i]nsofar as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and the scope of those rights shall be the same as those laid down by the said Convention". Consequently, the notion of freedom of expression expressed in the ECHR and the relevant case law give some guidance for interpreting the Charter's provision on freedom of expression.

Firstly, the scope of freedom of expression is broad, covering a wide array of forms of expression.[104] Therefore, information related to the AIA, i.e. commercially relevant technical information, would be covered by this freedom.[105] The right to freedom of expression covers not only the right to impart information but also the right to receive it. The European Court of Human Rights (ECtHR) did not previously recognise a separate right to access information but has since broadened its interpretation so that the right to receive information as part of the fundamental right of freedom of expression now also includes the right to seek and access information and government documents. It is noteworthy, however, that this access right covers only state-held information and documents. Another restriction is that, under ECtHR case law, the right of access is mainly limited to representatives of the media and NGOs, which play a watchdog role in society.[106] This limited approach has been subject to criticism.[107]

In contrast with the ECtHR, the EU has adopted a broader approach to access to information. In addition to contributing to the fundamental right of freedom of expression, the Charter provides, in Art. 42, for the related fundamental right of access to *EU Parliament, Council and Commission documents*. This right is enjoyed by EU citizens and residents, including legal entities that have a registered office in any EU Member State. It broadens the scope of access to information beyond the media and NGOs. Account must be taken of the right to access documents under the TSD too. Recital 34 thereof provides that "[t]his Directive respects the fundamental rights and observes the principles recognised in particular by the Charter". One of the fundamental rights listed in recital 34 refers to access to files. The Charter's right of access to documents serves as an important complement to the fundamental right of freedom of expression.

Another specific feature of freedom of expression under the Charter is that the Charter explicitly recognizes the freedom of the media.[108] This aspect of the Charter's right also forms an explicit part of the provisions on freedom of expression in Art. 5 of the TSD by stipulating "including respect for the freedom

[104] However, the scope of the protection afforded to freedom of expression may still depend on the form of expression e.g. whether it is political, commercial or artistic. Bychawska-Siniarska (2017), p. 12.

[105] For example, work-related speech has been given protection under the case law of the ECtHR *Herbai v. Hungary*, 2019 EctHR Appeal No. 11608/15, paras. 41–43.

[106] *Youth Initiative for Human Rights v. Serbia*, 2013 EctHR Appeal No. 48135/06; Erhaltung v. Austria, 2013 EctHR Appeal No. 39534/07.

[107] Woods (2017), p. 397.

[108] *Ibid*.

and pluralism of the media". Moreover, recital 19 of the TSD highlights the role of investigative journalism. One may assume that, in the context of the AIA, the media will play a special role in bringing to light any problems regarding, for example, safety or risks to fundamental rights associated with high-risk AI systems operating on the EU markets. The media will play an important role both in imparting and seeking information.

In this regard, one specific issue under the AIA is the role of private entities that assess *ex ante* compliance, whether this involves self-assessment by AI suppliers or third-party assessment by notified bodies. The media has no right of access to the information held by these private entities.[109] Nor is this right granted to private citizens or legal entities under Art. 42 of the Charter. But the EU database for high-risk AIs might provide some information for the purposes of detecting who holds the relevant information.

When it comes to *ex post* evaluation under the AIA, information will be in the hands of the national public authorities and, in specific situations, also the EU Commission. As explained earlier in Sect. 3, public authorities conduct the assessment in the event of serious incidents. The EU Commission then becomes part of the procedure when the risks relate to the territory of more than one Member State. Serious incidents are by their very nature of public concern. Consequently, it is likely that debate will be generated about these issues, and freedom of expression including media freedom will be important for providing access to information to enable that debate. Exceptions under the TSD that recognize the freedom of expression are of paramount importance here.

When media access to information is limited so that the media have to seek information held by public authorities, whistleblowers may play a role in delivering information to private entities. Under the TSD, whistleblowers are allowed to reveal misconduct, wrongdoing or illegal activity, provided that they act for the purpose of protecting the general public interest. A Council of Europe Recommendation defines a whistleblower as "any person who reports or discloses information on a threat or harm to the public interest in the context of their work-based relationship, whether *it be in the public or private sector*" (emphasis added).[110] It is noteworthy that whistleblowing activity covers both public and private sectors according also to the TSD, which imposes no limitations in this regard. Nor does the latter limit revelations to those who are in a work-based relationship. It defines what activity is allowed rather than who is allowed to take action. Yet whistleblowers are most likely insider informants and therefore might be employees of an entity in which there is wrongdoing.[111]

[109] One specific aspect, however, is whether the notified bodies that conduct the *ex ante* assessment of AI system compliance under the AIA can be considered as public authorities on account of the functions they have. Such evaluation may vary from country to country, and its analysis is outside the scope of this article.

[110] Recommendation CM/Rec(2014)7 of the Committee of Ministers to Member States on the Protection of Whistleblowers, COUNCIL EUR (30 April 2014).

[111] *See* for more Mylly (2021a).

For example, when reports under the AIA on serious incidents or risks to safety, health and fundamental rights are not made with due diligence, it might be possible for whistleblowers to provide information to media representatives or occasionally even directly to the general public.[112] This is an example of how freedom of expression, including freedom of the media, becomes closely linked with whistleblowing activities. Whistleblowers play an important role in delivering information to representatives of the media and are therefore protected by the fundamental right to freedom of expression.[113] Even though they play a particularly important role when information is held by private entities, they may also serve as important initial information channels when information is in the hands of public authorities.

It is telling that the AIA rules explicitly refer to the exceptions under the TSD as being applicable, even though this would be the case anyway even if there were no such reference. It is also laudable that the TSD clearly mentions freedom of expression and whistleblowing provisions that enable information relating to trade secrets to be disclosed and trade secret claims to be dismissed in specific situations. However, beyond the AIA and the TSD, there are also important principles of openness within administrative laws, as well as more detailed rules to enable access to information and its disclosure. These are applicable when public authorities hold the information in question. These rules will be elaborated on next.

6 Doctrine on Access to Documents and the Transparency Obligations of Public Authorities Under Administrative Laws

Firstly, it is noteworthy that the TSD refers not only to the fundamental rights that are relevant for accessing and imparting information, but also explicitly to the administrative rules on transparency. It stipulates in Art. 1(2) that:

> [t]his Directive shall not affect […] (b) the application of Union or national *rules requiring trade secret holders to disclose*, for reasons of public interest, information, including trade secrets, to the public or to administrative or judicial authorities for the performance of the duties of those authorities; (c) the application of Union or national *rules requiring or allowing Union institutions and bodies or national public authorities to disclose information submitted by businesses which those institutions*, bodies or authorities hold pursuant to, and in compliance with, the obligations and prerogatives set out in Union or national law … (emphasis added).

Recital 11 of the TSD refers to the same EU and national rules and explicitly mentions some of the EU rules on transparency, which remain applicable notwithstanding the introduction of the TSD. In essence, this means that rules on

[112] The situations in which whistleblowers are allowed to reveal information directly to the media are regulated in Art. 15 of the Whistleblowing Directive – Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, OJ L 305, 26.11.2019, 17–56. *See* for more discussion on this Mylly (2021a).

[113] Whistleblowers are also protected against retaliation under the Whistleblowing Directive.

the disclosure of information may also cover information relating to information protected as a trade secret. Even though the AIA does not explicitly stipulate specific rules on when the public will have access to information held by public authorities, the EU regulations and directives, as well as national legislation, that govern access to documents and transparency obligations are generally applicable when information is held by public authorities.

In addition to the explicit reference in Art. 1(2) of the TSD, these transparency rules are also arguably within the scope of Arts. 3(2) and 5(d) of the TSD. Article 3(2) provides that "[t[he acquisition, use or disclosure of a trade secret shall be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law". Article 5(d) allows disclosures "for the purpose of protecting a legitimate interest recognised by Union or national law". The scope of this Art. 5(d) exception has been said to be unclear.[114] However, under the context of the GDPR, it has been argued that, for example, the right of data subjects to be informed could be understood as falling within the scope of this exception to trade secrets. Consequently, the right to explanation could not be refused on the grounds of protecting trade secrets.[115] Assuming that transparency legislation falls within the scope of the exception under Art. 5(d) of the TSD, even the AIA would explicitly allow such disclosures, given the reference in Art. 70(1)(a) of the AIA to the exceptions under Art. 5 of the TSD. However, as already indicated, these transparency rules apply in any case when public authorities hold information and the possibility of disclosing information in such situations is recognized under the TSD.

At the EU level, the legislative instrument most relevant for the purposes of AIA is the Transparency Regulation, which allows access to documents held by EU institutions.[116] Even though the Transparency Regulation initially applied only to documents held by the European Parliament, Council and Commission, it is now applied also by EU agencies through specific provisions in their founding acts. Some institutions and bodies have also adopted acts laying down rules on access to their documents that are identical or similar to the Transparency Regulation.[117] For example, recital 11 of the TSD explicitly mentions this Regulation. At the EU level, as already discussed in the previous section, access to documents is also a right under Art. 42 of the Charter, being connected to other fundamental rights.

At the national level, similar rules are in place. For example, in Finland the relevant legislation is the Act on the Openness of Government Activities.[118] That Act stipulates that official documents are in the public domain unless specifically provided otherwise in the Act itself or in another act. Similar to the EU level, the

[114] Aplin (2021), pp. 192–193.

[115] Noto La Diega and Sappa (2020), Sec. IV.

[116] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

[117] Leino-Sandberg and Curtin (2016), p. 4.

[118] Act 21.5.1999/621 (Laki viranomaisten toiminnan julkisuudesta). Link to the unofficial English translation of the Act. https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf (accessed 28 September 2022).

right to access public documents is a constitutionally recognized right in Finland. The Finnish Constitution stipulates that "[d]ocuments and other records in the possession of public authorities shall be public unless their publication has, for compelling reasons, been specifically restricted by Act of Parliament. Everyone shall have the right to obtain information from public documents and records". Finland was one of the first countries to implement the legislation on access to documents. Moreover, the constitutional principle stems from as far back as 1776.[119]

Notwithstanding these rules, which make transparency an important objective, academics have criticized EU agencies' practice of giving private companies too much power to define the scope of access to documents. This has the result that companies rely on the rules on confidentiality, which constitutes an exception to the right to access. One of the EU agencies that has faced criticism is the European Medicines Agency (EMA),[120] which evaluates the safety of medical products before they are put on the market. The EMA's assessment is therefore analogous to the proposed compliance assessment for AI systems before they are put onto the market.

It is noteworthy that the initial idea under the EU White Paper for AI was to introduce a centralized EU agency to evaluate AI systems. This approach would have been in line with the tasking of the EMA and other EU agencies to check product safety. Even though the AIA in its current form does not have a centralized EU agency in place, the EU Commission will in some cases have access to documentation provided by AI suppliers.[121] In such cases, the Transparency Regulation would be applicable. When it comes to the national public authorities, national rules on access to documents or openness that resemble the Transparency Regulation will be applicable. National rules would apply, for example, when market surveillance authorities had checked the compliance of AI systems with AIA requirements *ex post*. Therefore, it is important to look at how such rules are to be interpreted and what the role of trade secrets is under such legislative instruments. This article does not discuss national rules. The analysis will focus on the Transparency Regulation and how access to documents is interpreted under that framework.

PTC Therapeutics International Ltd v. European Medicines Agency is a fairly recent decision by the Court of Justice of the European Union (CJEU) on the conflict between the right to access documents and exceptions thereto based on harm to commercial interests. In this case, it seems that the EMA no longer follows the practice criticized earlier of over-relying on companies' claims to confidentiality. However, this new approach was the subject of a complaint by a pharmaceutical company whose clinical test data documentation was given to a competitor on the basis of a request for access to documents. The documents contained information submitted by the appellant within the scope of an application for a marketing authorization of a medicinal product for human use. The EMA had redacted some

[119] Mäenpää and Fenger, p. 172.

[120] *See* Korkea-aho and Leino (2017).

[121] Article 65 of the AIA is relevant for information exchange between national authorities and the EU Commission.

information from the documents, but the pharmaceutical company claimed that the documentation relating to clinical test data submitted in the course of its application for a marketing authorization should have been kept secret in its entirety. The decision clarifies the core issue of interpretation under the Transparency Regulation, namely the extent to which access to information should be denied because of claims of commercial interest, including confidentiality. The CJEU highlighted that an important objective of the Transparency Regulation was to ensure that decisions were taken as openly as possible and as closely as possible to the citizen. Moreover, the CJEU emphasized the connection of this objective of the Regulation to Charter rights and TFEU principles. It also emphasized that recital 2 of the Regulation connected the principle of openness to the greater legitimacy of EU institutions and how those could be held accountable by EU citizens. And that the objective of the Regulation was to provide as broad access to the documents as possible.[122] Importantly, the CJEU in this case held in favor of access to the documents.

The exception to the right to access that was relevant in this case is laid down in Art. 4 of the Transparency Regulation. The specific part subject to interpretation was as follows: "The institutions shall refuse access to a document where disclosure would undermine the protection of: commercial interests of a natural or legal person, including intellectual property". Firstly, the CJEU held that exceptions to the right to access should be construed narrowly. It highlighted that, whenever an EU institution made a decision that denied access to a document, it was obliged to explain how access thereto could specifically and actually undermine the interest protected by the relevant exception. Moreover, the risk of the interest being undermined must be reasonably foreseeable and not purely hypothetical.[123] The appellant had not specifically and precisely identified before the EMA (or before the General Court) which of the passages (in the disclosed document), if disclosed, could harm its commercial interests.[124] A mere unsubstantiated claim relating to a general risk of misuse cannot lead to data being regarded as falling within the scope of the exception.[125]

The appellant also argued that the EMA should have relied on its presumption of confidentiality. However, the CJEU held that the purpose of such presumptions was to simplify the process for the institutions when there were vast quantities of similar types of document subject to access requests.[126] Moreover, the institutions are always entitled to carry out an individual examination to check whether the information in question actually qualifies as confidential. In this case, the EMA had carried out such an evaluation and decided on the basis thereof that most of the

[122] Case C-175/18 *PTC Therapeutics International Ltd v. European Medicines Agency (EMA)*; ECLI:EU:C:2020:23, paras. 51–54.

[123] *Ibid*. paras. 56–57.

[124] *Ibid*. para. 82.

[125] *Ibid*. para. 96.

[126] In fact, the option open to the institutions to rely on presumptions of confidentiality has been subject to criticism also because such presumptions are at odds with the principles of widest possible openness and narrow interpretation of the exceptions. Leino-Sandberg and Curtin (2016), pp. 10–11.

information was not confidential.[127] In that case, the applicant was unable to identify how disclosing the information would be harmful. Therefore, access was allowed after the EMA had redacted some of the information.

In cases where an exception would be applicable, the institutions are required, under the principles of established case law, to weigh confidential commercial interests against the overriding public interest in transparency. In the case in question, because the exception was not applicable, there was no need to conduct this balancing exercise.[128]

What one learns from *PTC Therapeutics International Ltd* is, firstly, that not all information claimed to be confidential can be treated as such. This is the important notion that was already emphasized in Sect. 4 when discussing the definition of trade secrets under the TSD. Moreover, under the Transparency Regulation, the protection of commercial interests is an exception that needs to be construed narrowly. From the case discussed here, it also becomes apparent that claims for confidentiality and harm to commercial interests must be real rather than purely hypothetical, and that specific information must be identified. In addition, EU institutions are obliged to explain why access to a document has been denied. Importantly, the default rule is to provide access to documents.

In cases where an exception to the right of access applies because of commercial harm, for example owing to trade secrets, EU institutions need to apply a "balancing of interests" test. They are obliged to assess the public interest in the disclosure of the information and weigh it against a party's interest in keeping the information confidential. These principles of interpretation for the exceptions are part of the established case law of the CJEU.[129] It is noteworthy that these principles might lead to a situation in which the public interest in accessing information prevails over the commercial harm, meaning that even trade secrets may need to be revealed in the public interest.[130]

Importantly, under the AIA rules, technical documentation of AI systems will be in the hands of public authorities, whether national authorities or the EU Commission, when serious incidents have occurred, or if national public authorities have reason to believe that AI systems pose a risk to safety, health or fundamental rights (Arts. 62 and 65 of the AIA). Such situations are naturally of public concern. It can be assumed that, in these instances, investigative journalists at least will be able to claim access to the documentation in question, as there will be a demand for public discussion and oversight of such matters.[131] Here the rules on access to

[127] Case C-175/18 *PTC Therapeutics International Ltd v. European Medicines Agency (EMA)*; ECLI:EU:C:2020:23 paras. 62–64.

[128] *Ibid*, paras. 84–86.

[129] Graig (2018), pp. 395–396.

[130] One might think that such information might not be particularly useful for competitors, because it relates to situations where an AI system is not performing in accordance with the expectations but contains errors. However, it has been recognized that information on what does not work provides an important competitive advantage. This is because negative information saves development costs. Nordberg (2019), p. 200.

[131] However, whether public interest would ensure access after the balancing exercise referred to is another question. In previous case law it seems that the public interest did not in the end play such an

documents can clearly be seen as a component of freedom of expression, and in particular the freedom of the media, as discussed above.

As elaborated on in Sect. 2, the right to such access to documents is an important element in democratic societies as it gives the general public some oversight of public administration. Importantly, this right of access to administrative documents is given to citizens and not only to the media. It enables society to tackle various threats. In the context of the AIA, these are the threats posed to safety, health or fundamental rights by the application of AI systems.

7 Concluding Remarks

This article has analyzed AIA rules, which aim inter alia to reduce the opacity of AI systems and tackle the threats posed by AI systems. Through controls established under the AIA, the EU aims to ensure that AI systems placed on EU markets are safe, trustworthy, and ethical. The rules set up a system of compliance assessment based on technical documentation. This detailed documentation aims to provide all the information required on the AI system and its purpose, in order that the authorities can assess its compliance with the AIA's requirements. AI systems are to become more human-centric through human oversight, and transparency will be ensured through a series of checks and controls. The objective is to create trust in the AI systems that operate on EU markets by reducing opacity and increasing transparency. The impression is that the objectives aim to set in place useful control based on meaningful information/documentation and its disclosures.

However, the disclosure of information is limited to some extent when the information in question is protected as a trade secret. The AIA provisions explicitly refer to confidentiality obligations. However, the article has shown that, owing to the scope of trade secret protection, trade secrets actually play a more limited role under the provisions of the AIA than some might have assumed. What has been elaborated on here is that technical documentation under the AIA contains vast amounts of information that does not qualify for trade secret protection. But even when there are trade secrets, there are still relevant exceptions to trade secret protection. Furthermore, other legislative instruments enable access to information in specific situations notwithstanding the trade secret status of the information. This might occasionally lead to a situation in which information will become available for public scrutiny and oversight by EU citizens. In those cases, the information might lose its trade secret status, and other parties would be free to use such information, unless, for example, any other IP protection over the features of the AI were to restrict such use. All in all, increasing public transparency and oversight is an important element of the provisions of the AIA. Therefore, the outcomes of this

Footnote 131 continued
important role in providing access. This has been subject to criticism. *See* Leino-Sandberg and Curtin (2016), p. 6.

article, elaborating on the rules enabling public oversight and access to information, and the limited role of trade secrets, may not come as such a surprise.

Funding Open Access funding provided by Hanken School of Economics.

References

Abbott R (2016) I think, therefore I invent: creative computers and the future of patent law. Boston Coll Law Rev 57:1079–1126

Alì GS, Yu R (2021) Artificial intelligence between transparency and secrecy: from the EC whitepaper to the AIA and beyond. Eur J Law Technol 12

Aplin T (2017) Trading data in the digital economy: trade secrets perspective. In: Lohsse S, Schulze R, Staudenmayer D (eds) Trading data in the digital economy: legal concepts and tools. Baden-Baden, Nomos, pp 59–72

Aplin T (2021) The limits of trade secret protection in the EU. In: Sandeen S, Rademacher C, Ohly A (eds) Research handbook on information law and governance. Edward Elgar, Cheltenham, pp 174–194

Burrell J (2016) How the machine 'thinks': understanding opacity in machine learning algorithms. Big Data Soc. https://doi.org/10.1177/2053951715622512

Burri T (2017) International law and artificial intelligence (October 27, 2017). German Yearbook of International Law 2017 (vol. 60). Duncker & Humblot, Berlin, pp. 91–108, Available at SSRN: https://ssrn.com/abstract=3060191 or https://doi.org/10.2139/ssrn.3060191

Bychawska-Siniarska D (2017) Protecting the right to freedom of expression under the European Convention on Human Rights – a handbook for legal practioners. Council of Europe

Contreras J (2017) Origins of FRAND licensing commitments in the United States and Europe. In: Contreras J (ed) The Cambridge handbook of technical standardization law: competition, antitrust, and patents. Cambridge University Press, Cambridge, pp 149–169. https://doi.org/10.1017/9781316416723.012

Diakopoulos N (2020) Transparency. In: Dubber MD, Pasquale F, Das S (eds) The Oxford handbook of ethics of AI. Oxford University Press, pp 197–213. https://doi.org/10.1093/oxfordhb/9780190067397.013.11

Drexl J (2017) Designing competitive markets for industrial data – between propertisation and access. JIPITEC 8:257–292

Ebers M (2022) Standardizing AI: the case of the European Commission's Proposal for an 'Artificial Intelligence Act.' In: DiMatteo L, Poncibò C, Cannarsa M (eds) The Cambridge handbook of artificial intelligence: global perspectives on law and ethics. Cambridge University Press, Cambridge, pp 321–344. https://doi.org/10.1017/9781009072168.030

Ebers M, Hoch VRS, Rosenkranz F, Ruschemeier H, Steinrötter B (2021) The European Commission's Proposal for an Artificial Intelligence Act—a critical assessment by members of the robotics and AI Law Society (RAILS). Journal 4:589–603. https://doi.org/10.3390/j4040043

Graig P (2018) EU administrative law. Oxford University Press, Oxford

Graves T, Macgillivray A (2004) Combination trade secrets and the logic of intellectual property. 20 Santa Clara High Tech. L.J. 20:261–292

Grozdanovski L (2021) In search of effectiveness and fairness in proving algorithmic discrimination in EU law. Common Market Law Review 58:99–136
Hacker P (2018) Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law. Common Market Law Review 55:1143–1186
Hakkarainen JM, Koulu R & Markkanen KA (2020) Läpinäkyvät algoritmit? Lähdekoodin julkisuus ja laillisuuskontrolli hallinnon digitalisaatiossa. In: Edilex. 2020/18 https://www.edilex.fi/artikkelit/21042.pdf
Hildebrandt M (2008) Legal and technological normativity: more (and less) than twin sisters. Techné 12:169–183
Hrdy CA (2021) The value in secrecy. Fordham L Rev 91:557–607
Hugenholtz PB, Quintais JP (2021) Copyright and artificial creation: does EU copyright law protect AI-assisted output? IIC 52:1190–1216. https://doi.org/10.1007/s40319-021-01115-0
Keller P (2019) Participatory accountability at the dawn of artificial intelligence. Dickson Poon School of Law Legal Studies Research Paper Series.https://doi.org/10.2139/ssrn.3448315
Keller P, Drake A (2021) Exclusivity and paternalism in the public governance of explainable AI. Comput Law Secur Rev 40:1–4
Knaak R, Kur A, Hilty RM (2014) Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for the Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure of 28 November 2013, COM (2013) 813 Final. IIC 45:953–967. https://doi.org/10.1007/s40319-014-0270-3
Korkea-aho E, Leino P (2017) Who owns the information held by EU agencies? Weed killers, commercially sensitive information and transparent and participatory governance. Common Market Law Rev 54:1059–1092
Koulu R (2020) Human control over automation: EU Policy and AI Ethics. Eur J Legal Stud 12:9–46. https://doi.org/10.2924/EJLS.2019.019
Koulu R (2021) Crafting digital transparency: implementing legal values into algorithmic design. Crit Anal Law 8:81–100
Leino-Sandberg PSM, Curtin D (2016) Openness, transparency and the right of access to documents in the EU: In-depth analysis. European Parliament, Brussels http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/556973/IPOL_IDA(2016)556973_EN.pdf
Lemley MA, Cohen JE (2001) Patent scope and innovation in the software industry. Calif Law Rev 89:1–57
Lawrence L (2006) Code version 2.0. Basic Books, New York
Mäenpää O (2020) Julkisuusperiaate. Alma Talent, Helsinki
Mäenpää O, Fenger N (2019) Public administration and good governance. In: Letto-Vanamo P, Tamm D, Gram Mortensen BO (eds) Nordic law in European context. Ius Gentium: comparative perspectives on Law and Justice. Springer, Cham, pp 163–178. https://doi.org/10.1007/978-3-030-03006-3_10
Mahler T (2022) Between risk management and proportionality: the risk-based approach in the EU's Artificial Intelligence Act Proposal. Nordic Yearbook of Law and Informatics 2020–2021: Law in the Era of Artificial Intelligence, pp. 247–270 https://doi.org/10.53292/208f5901.38a67238
Matulionyte R, Aranovich T (2022) Trade secrets versus the AI explainability principle. In: Abott R (ed) Research handbook on intellectual property and artificial intelligence. Edward Elgar, Cheltenham, pp 404–421
Mökander J, Axente M, Casolari F, Floridi L (2022) Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. Mind Mach 32:241–268
Mylly UM (2011) What ever happened to patent bargain? Prospect theory and software patentability. NIR, Nordisk Immateriellt Rättsskydd 5(2011):444–470
Mylly UM (2021a) Freedom of the media and trade secrets in Europe. In: Sandeen SK, Rademacher C, Ohly A (eds) Research handbook on information law and governance. Edward Elgar, Cheltenham, pp 193–216
Mylly UM (2021b) Preserving the public domain: limits on overlapping copyright and trade secret protection of software. IIC 52:1314–1337. https://doi.org/10.1007/s40319-021-01120-3
Nordberg A (2020) Trade secrets, big data and artificial intelligence innovation: a legal oxymoron? In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive. Edward Elgar, Cheltenham, pp 192–218

Noto La Diega G, Sappa C (2020) The internet of things (IoT) at the intersection of data protection and trade secrets. non-conventional paths to counter data appropriation and empower consumers. Eur J Consum Law/Revue européenne de droit de la consummation 3:419–458
Pasquale F (2011) The troubling consequences of trade secret protection of search engine rankings. In: Dreyfuss RC, Strandburg KJ (eds) The law and theory of trade secrets. Edward Elgar, Cheltenham, pp 381–405
Pasquale F (2016) The Black Box Society the secret algorithms that control money and information. Harvard University Press, Cambridge
Radauer A, Bader M, Aplin T, Konopka U, Searle N, Altenburger R, Bachner C (2022) Final report for the "Study on the legal protection of trade secrets in the context of the data economy" (EASME/2020/OP/0008)
Rowe EA (2022) Procuring algorithmic transparency (February 26, 2022). Alabama Law Review, Vol. 74, No. 2, 303, Available at SSRN: https://ssrn.com/abstract=4044178 or https://doi.org/10.2139/ssrn.4044178
Sandeen SK (2020) Through the looking glass: trade secret harmonization as a reflection of US law. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 38–63
Sandeen SK, Aplin TF (2022) Trade secrecy, factual secrecy and the hype surrounding AI. In: Abott R (ed) Research handbook on intellectual property and artificial intelligence. Edward Elgar, Cheltenham, pp 442–459
Schovsbo J (2020) The Directive on Trade Secrets and its background. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 7–21
Tomkowicz R (2010) Uneasy fit: software patent and the duty of disclosure in patent laws. Can Intellect Prop Rev 25:221–234
Truby J, Brown R, Ibrahim I, Parellada O (2022) A sandbox approach to regulating high-risk artificial intelligence applications. Eur J Risk Regul 13:270–294. https://doi.org/10.1017/err.2021.52
Ullrich H (2017) FRAND access to open standards and the patent exclusivity: restating the principles (February 17, 2017). Concurrences, Issue 2, 2017, Max Planck Institute for Innovation & Competition Research Paper No. 17-04, available at SSRN: https://ssrn.com/abstract=2920660
Veale M, Zuiderveen Borgesius F (2021) Demystifying the Draft EU Artificial Intelligence Act—analysing the good, the bad, and the unclear elements of the proposed approach. Comput Law Rev Int J Inf Law Technol. https://doi.org/10.9785/cri-2021-220402
Wiebe A, Schur N (2019) Protection of trade secrets in a data-driven, networked environment—is the update already out-dated? J Intell Property Law Pract 14:814–821. https://doi.org/10.1093/jiplp/jpz119
Woods L (2017) Digital freedom of expression in the EU. In: Douglas-Scott S, Hatzis N (eds) Research handbook on EU law and human rights. Edward Elgar, Cheltenham, pp 394–417

Official Documents

Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012, pp 391–407
Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1
Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law OJ L 305, 26.11.2019, pp 17–56
EU Commission (2020) White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, Brussels, 19.2.2020 COM (2020) 65 final
European Commission, Impact Assessment Accompanying the 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) (2021) p 57
Finnish Act on the Openness of Government Activities. Act 21.5.1999/621 (Laki viranomaisten toiminnan julkisuudesta). Link to the unofficial English translation of the Act https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf

Opinion of the European Parliament Committee on Legal Affairs (JURI opinion), 12.9.2022 on the AIA proposal
Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final
Proposal for a Regulation laying down harmonised rules on artificial intelligence, 167 final – 84 final – 85 final
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 – General approach (6 December 2022). ST 15698 2022 INIT
Proposal for a directive of the European Parliament and of the Council on liability for defective products. COM(2022) 495
Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence (AI liability directive). (Text with EEA relevance) 344 final – 318 final – 319 final –320. COM(2022) 496
Recommendation of the Committee of Ministers to Member States on the Protection of Whistleblowers, COUNCIL EUR. (Apr. 30, 2014)
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, pp 1–88
Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents OJ L 145, 31.5.2001, pp 43–48
The International Covenant on Civil and Political Rights. Adopted by the General Assembly of the United Nations on 19 December 1966 (ICCPR)
The Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, pp 47–390.
The Treaty on European Union OJ C 326, 26.10.2012, pp 13–390
Uniform Trade Secrets Act 1985 (UTSA)

Case Law

C-393/09, *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury*, ECLI:EU:C:2010:816
C-175/18 *PTC Therapeutics International Ltd v. European Medicines Agency* (EMA), ECLI:EU:C:2020:23
Erhaltung v. Austria, 2013 ECtHR App. No. 39534/07
Youth Initiative for Human Rights v. Serbia, 2013 ECtHR App. No. 48135/06