J Multidisciplinary Scientific Journal

MDPI

Article

The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)

Martin Ebers [1,*], Veronica R. S. Hoch [2], Frank Rosenkranz [2], Hannah Ruschemeier [3] and Björn Steinrötter [4]

[1] Robotics & AI Law Society (RAILS), 12203 Berlin, Germany
[2] Faculty of Law, Ruhr-University Bochum, 44801 Bochum, Germany; veronica.hoch@rub.de (V.R.S.H.); frank.rosenkranz@rub.de (F.R.)
[3] Center for Advanced Internet Studies (CAIS), 44799 Bochum, Germany; hannah.ruschemeier@cais.nrw
[4] Faculty of Law, University of Potsdam, 14469 Potsdam, Germany; steinroetter@uni-potsdam.de
* Correspondence: ebers@ai-laws.org

Abstract: On 21 April 2021, the European Commission presented its long-awaited proposal for a Regulation "laying down harmonized rules on Artificial Intelligence", the so-called "Artificial Intelligence Act" (AIA). This article takes a critical look at the proposed regulation. After an introduction (1), the paper analyzes the unclear preemptive effect of the AIA and EU competences (2), the scope of application (3), the prohibited uses of Artificial Intelligence (AI) (4), the provisions on high-risk AI systems (5), the obligations of providers and users (6), the requirements for AI systems with limited risks (7), the enforcement system (8), the relationship of the AIA with the existing legal framework (9), and the regulatory gaps (10). The last section draws some final conclusions (11).

Keywords: artificial intelligence (AI); machine learning; European Union (EU); regulation; harmonization; Artificial Intelligence Act

Citation: Ebers, M.; Hoch, V.R.S.; Rosenkranz, F.; Ruschemeier, H.; Steinrötter, B. The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J* **2021**, *4*, 589–603. https://doi.org/10.3390/j4040043

Academic Editors: Ugo Pagallo and Massimo Durante

Received: 15 September 2021
Accepted: 28 September 2021
Published: 8 October 2021

1. Introduction

Artificial intelligence (AI) systems based on machine learning (ML) and other techniques have the potential to improve our lives as well as the overall economic and societal welfare. They can contribute to better healthcare services, safer and cleaner transport systems, better working conditions, higher productivity, and new innovative products, services, and supply chains. AI systems can also benefit the public sector in a number of ways, for example, by automating repetitive and time-consuming tasks, or by providing public agencies with more accurate and detailed information, forecasts, and predictions, which in turn, might lead to personalized public services tailored to individual circumstances. AI-powered systems may even help to respond to key global challenges, such as climate change and the novel coronavirus pandemic.

However, as with every disruptive technology, AI systems come not only with benefits but also with substantial risks, raising a broad variety of legal and ethical challenges. AI systems have the potential to unpredictably harm people's life, health, and property. They can also affect fundamental values on which western societies are founded, leading to breaches of fundamental rights of people, including the rights to human dignity and self-determination, privacy and personal data protection, freedom of expression and of assembly, non-discrimination, or the right to an effective judicial remedy and a fair trial, as well as consumer protection [1–3].

Against this backdrop, we welcome that the European Commission presented on 21 April 2021, the proposal for a Regulation "laying down harmonized rules on Artificial Intelligence", the so-called "Artificial Intelligence Act (hereinafter: AIA) [4]. We particularly appreciate that the AIA follows a risk-based approach by imposing regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety.

However, a closer analysis shows that the proposed AIA may need improvement in many areas. This position paper is to be understood as a preliminary assessment of the AIA in order to provide a meaningful basis for further discussion.

2. Unclear Preemptive Effect of the AIA and EU Competences

The AIA does not clearly state as to what extent the Member States may deviate from the substantive requirements contained therein, i.e., whether it establishes a framework of full harmonization or whether it is one of minimum harmonization that allows Member States to maintain or introduce provisions diverging from those laid down in the AIA, including more stringent provisions to ensure a different level of protection (on the difference between full/maximum harmonization and minimum harmonization: [5] (pp. 269–270), [6] (pp. 47–83), [7], [8] (pp. 133–134)). For example, do Member States still have the competence to ban certain AI systems beyond the prohibitions of Art. 5 AIA, e.g., biometric systems or social scoring by private companies?

Regarding the legislative competences, the proposed regulation follows the European Commission's tendency to use Art. 114 TFEU as a general competence for the regulation of commercial law. Whether this legal basis can be used for the AIA is doubtful in light of the Tobacco Advertising case-law [9,10], especially regarding the prohibition of certain systems used by state authorities (cf. Art. 5(1)(c) and (d) AIA). How does the prohibition of certain AI systems used by public authorities contribute to removing barriers to trade in the internal market? Likewise, it is questionable whether these prohibitions can be based on Art. 16(2) TFEU, since these bans do not directly aim at the protection of personal data but at other fundamental rights and democratic values. Additionally, the exceptions in Art. 5(1)(d)(iii) AIA address detailed requirements for administrative procedural rules including certain groups of cases and the requirement of prior authorization by a judicial or independent administrative authority. These kinds of procedural obligations concerning state security, risk prevention, and prosecution are usually part of the administrative police law or the criminal procedure code of the Member States [11] (p. 143).

3. Scope of Application

3.1. Overly Broad Definition of "AI Systems"

The proposal regulates "AI systems". Besides the question of what should be the difference between "AI" [4] (p. 11; recitals (28), (38), (39) (40), and (47) AIA) and "AI systems", the overly broad substantive scope of the AIA seems problematic [12] (pp. 215–216). Art. 3(1) AIA in conjunction with Annex I covers almost every computer program. Such a broad approach may lead to legal uncertainty for developers, operators, and users of AI systems [13] (p. 280). Many associate the term "artificial intelligence" primarily with machine learning, and not with simple automation processes in which pre-programmed rules are executed according to logic-based reasoning.

The AIA also goes beyond the necessary degree of regulation, at least in some cases. On the one hand, a wide definition of "AI systems" may be justified in light of the prohibited AI practices delineated in Art. 5 AIA to offset the threats posed by different kinds of software to the fundamental rights of individuals. Indeed, it seems to make little difference to the rights of affected citizens whether the banned practices (subliminal manipulation, exploitation of vulnerabilities, social scoring, or remote biometric identification) are enabled by machine learning or logic-based reasoning. On the other hand, such a broad definition is too wide when it comes to high-risk AI systems. The mandatory requirements envisaged for these systems in Title III, Chapter 2 are based on the observation that a number of fundamental rights are adversely affected, in particular, by the special characteristics of ML, such as opacity, complexity, dependency on data, autonomous behavior [14] (p. 11 at 3.5.). Since these characteristics are either not or only partly present in simple (logic based) algorithms, the broad definition of AI potentially leads to an overregulation.

3.2. Unclear Scope with Regard to AI Components

The AIA also does not clarify as to how various components of AI systems should be treated which could include either pre-trained AI systems from different manufacturers forming part of the same AI system or components of one and the very system that are not released independently. Therefore, it should be clarified whether separate components of AI systems would be individually required to conform to the AIA and what would be the implications for responsibilities when these components are not compliant.

3.3. Unclear Scope with Regard to Academic Research and Open-Source Software (OSS)

Another regulatory flaw of the AIA is that, unlike Art. 89 GDPR [15], it does not provide for any exception for research purposes. Therefore, in situations where the researchers collaborate with the industry and publish their model for academic purposes, they may run the risk of being regarded as providers who "develop an AI system" with a view of "putting it into service" (Art. 3(2) AIA), i.e., supplying the system "for first use directly to the user or for own use" (Art. 3(11) AIA) [16] (p. 16).

This risk is magnified owing to the fact that open-source software (OSS) is an important part of the research ecosystem. Classifying any release of an OSS as "putting into the market/into service" and imposing conformity assessment requirements on it will simply be detrimental to the entire scientific research ecosystem.

3.4. Territorial Scope

We welcome the broad territorial scope aiming to prevent the migration of innovation to non-European countries. However, a clarification of the term "located" referenced in Art. 2(1)(b) AIA is of utmost importance. From our point of view, "located" refers to—or at least should refer to—the user's or provider's location and not the location of the AI system [13] (p. 278) because such an interpretation would make it increasingly difficult to determine the specific location of the AI system, especially with the increase in the use of cloud computing technologies. Moreover, relocations to third countries would be very easy. Although recital (11) AIA clearly supports the position taken here, a clarification in the binding part of the regulation would be preferable.

Furthermore, limiting the geographical scope of the AIA to only the "use" of AI systems within the European Union (EU) (Art. 2(1)(c) AIA) excludes cases where the development, sale or export of high-risk AI systems or even prohibited AI systems takes place within the EU but are used outside of the EU. This provision creates serious legal and ethical concerns for the users of AI systems located outside of the EU. However, taking into account that the AIA is based on the internal market clause (Art. 114 TFEU), the provision seems justified, because it is difficult to imagine how the AIA could contribute to the internal market if an AI system is only developed in the EU, but never put into operation there.

4. Prohibited Uses of AI (Art. 5 AIA)

The AIA follows the right approach to prohibit certain especially intrusive forms of AI. However, there are still many loopholes that the legislators may need to plug.

4.1. Manipulative AI Systems (Art. 5(1)(a) and (b) AIA)

Art 5(1)(a) and (b) AIA contain two prohibited practices that claim to regulate manipulation.

However, neither the said article nor recital (16) AIA defines what constitutes a "subliminal technique" or what is "materially distorting" a person's behavior. Many user experience (UX) features influence a user's behavior in subtle ways that may go unnoticed by the user. Art. 5(1)(a) AIA covers only AI practices which directly intend to harm other people. It seems likely that most of these kinds of systems are already illegal under criminal law in most of the Member States. Influencing and nudging users into commercial services they potentially do not want is not covered by Art. 5 AIA. Admittedly, a general ban of these kinds of advertisement techniques would be overreaching. Moreover, the Unfair

Commercial Practices Directive (UCPD) [17] prohibits commercial practices which distort human behavior under certain conditions (as to the question whether so-called "dark patterns" and algorithmic nudging/manipulation is prohibited by the UCPD: [18] (paras. 28, 29), [19] (pp. 109–135) [20,21]). Therefore, clarifying the terms of recital (16) or Art. 3 AIA would be useful to ascertain the scope of AI systems using such techniques in light of Art. 5 AIA. The AIA should take into special consideration "collective harms" emanating from the use of manipulative AI systems since the same cannot be effectively identified, proved, or resolved by way of private law remedies [22] (pp. 4–5).

Under Art. 5 AIA, it is sufficient that the distorted behavior of a person is likely to cause physical or psychological harm, but not that the AI system is likely to manipulate behavior. Even when the prohibitions under Art. 5 AIA are not applicable to such manipulative AI systems, as, for example, the AI system is manipulative but lacks causality for causing harm, the system is not per se covered as a high-risk system under the AI.

The AIA did not follow the demands for a general prohibition of deep fakes, which could be defined as manipulative AI systems addressed in Art. 5(1) AIA, but usually do not raise a direct risk of physical or psychological harm rather than individual defamation or reputation damage and systemic problems of fake news and manipulation. Deep fakes are explicitly mentioned in Art. 52(3) AIA and require the disclosure that the content is artificially generated or manipulated.

4.2. Social Scoring (Art. 5(1)(c) AIA)

The ban on AI systems used for social scoring purposes is limited in Art. 5(1)(c) AIA to those deployed by public authorities. It is indefinite when a system is "leading" to a specific outcome, and this allows the possibility that the authority using the social scoring system may claim that the scoring was not a determinative factor [22] (p. 7). Moreover, Art. 5 AIA does not clarify to what extent "the use of an AI system" takes place on behalf of public authorities, especially given that the development of digital technologies is mostly performed by the private sector and deployed by public administration or other public authorities. Whether the citizen scoring, commonly built with broad private sector datasets augmenting administrative data, falls within the scope of Art. 5, remains unclear [22] (p. 6). Therefore, the AIA should clarify the meaning of the phrase "on their behalf" as contained in Art. 5(1)(c) AIA accordingly.

By limiting the ban of social scoring to public authorities, the AIA ignores the use of such systems by private entities, even in high-risk areas which could likely affect the fundamental rights of people via an indirect third-party effect. Accordingly, the Commission should re-evaluate whether the risk of broadly cross-context implemented private social scoring applications, within sensitive areas of public concern like credit scoring, housing or public employment, are properly addressed by the AIA. In addition, limiting the ban of social scoring to situations where the social score leads to treatment of persons that is "disproportionate to their social behavior" creates legal uncertainty [23] (p. 365).

4.3. Biometric AI Systems (Art. 5(1)(d) AIA)

The approach in Art. 5(1)(d) AIA to prohibit only biometric identification systems (BIS) used for law enforcement is too narrow. Especially private companies pursue their own interests and are not bound by the common good. This means it is even more imperative to prohibit practices which pursue commercial, private interests of companies. Therefore, the prohibition should be applicable to all uses of biometric AI systems—public or private and hence, should be extended to all AI systems used by other public authorities and by private actors.

Moreover, the exceptions for BIS are too broad since the proposal establishes exceptions not only for the time-sensitive search for crime victims and prevention of terrorist attacks, but also for the detection of criminal suspects concerned by a custodial sentence of three years and above referred to in Council Framework Decision 2002/584/JHA [24]. These exceptions will be regularly met in the practical work of law enforcement.

All in all, there should be a general ban on BIS in publicly available spaces which should be extended to all kinds of biometric, behavioral, or emotional signs in any context, e.g., DNA, movement analysis, and post remote biometric identification, as the same could enable indiscriminate mass surveillance. Already the anticipation of being identified in public accessible places can cause chilling effects on exercising fundamental rights [25] (pp. 125–126), [26].

It is also interesting to note that Art. 5(1)(d) AIA prohibits the use of BIS, which is different from "biometric categorization systems" (BCS). In contrast to the definition contained in Art 3(35) AIA, some categories may also be much more sophisticated, such as relating to the concrete regional background, a particular risk group, or certain personality traits, in which case biometric categorization is usually combined with detection techniques [27] (p. 56). While a BIS identifies natural persons on the basis of their biometric data, a BCS is able to assign a natural person to specific categories, such as sex, age, ethnic origin, or sexual or political orientation [28] (p. 288). This difference is acknowledged in Annex III of AIA which explicitly uses the term "biometric identification and categorization". Moreover, an emotion recognition system (ERS) tries to detect different emotions through the integration of information from facial expressions, body movement, gestures, and speech. However, the automated recognition of characteristics like gender, sexuality, or ethnicity as well as emotions caused by BCS and ERS is not prohibited under the AIA. All these features were repeatedly the cause for biased automated decisions in the past. AI systems like BCS and ERS which are categorizing individuals from biometrics and emotion detection into clusters according to grounds for discrimination prohibited under Art. 21 Charter of Fundamental Rights of the European Union should be prohibited under Art. 5 AIA [16] (pp. 25–28) (see also [29] (pp. 56–59)).

4.4. Possibility of the European Commission to Add Prohibited AI Practices?

Whereas Art. 7 AIA gives the European Commission the possibility to amend the list of stand-alone high-risk AI systems, the AIA does not confer the same power when it comes to prohibited practices. According to the proposal, Art. 5 AIA cannot be amended by the European Commission. Since some problematic features of AI practices can only be determined ex post, the legislators could consider allowing the European Commission to have the option to amend the prohibited practices under Art. 5 AIA. However, given the far-reaching consequences of total bans, such a delegation of power would go too far. Therefore, in our view, it is justified that the power to adopt delegated acts is conferred on the European Commission only with regard to high-risk AI systems.

5. High-Risk AI Systems

5.1. Classification of High-Risk AI Systems

While we appreciate the risk-based approach adopted by the European Commission, we strongly believe that a more detailed classification of risk could be necessary for the industry to perform the self-assessment of risks associated with their products. Currently, the AIA prescribes a broad definition for "AI" and generalizes the risk levels for various AI applications, which may not identify specific risks of AI systems, leading to insufficient compliance. A more granular classification of risk will also be conducive in ensuring the safety of high-risk AI systems developed outside the EU. Therefore, the AIA should reflect flexibility and adaptability in its risk classification and should allow for modifications to the areas listed in Annex III and not just specific uses within the existing categories, along with the possibility to add entire new categories of risk, including ones that may not be currently contemplated. In doing so, the European Commission should initiate risk assessments following transparent mechanisms in order to enable companies to anticipate possible expansions as early as possible. During this process of revising the list of high-risk AI systems, the public should also be provided with consultation and participation rights. It is also observed that for the classification of risks to be pari materia with the continuous innovation, the risk assessment should be based on continuously updated standards, based on ongoing research.

In particular, the AIA omits several relevant contexts of use of high-risk AI systems which can pose significant risks, such as AI systems used for determining the insurance premium, health-related AI systems that are not already covered under Annex II, AI systems deployed for housing purposes, to name a few [30]. It is also questionable as to why Annex III.6. narrowly focuses on the use of AI systems by law enforcement authorities regarding "individual risk assessments for natural persons", detection of "the emotional state of a natural person," and "profiling of natural persons". In doing so, the AIA limits its scope to only individual natural persons, excluding AI practices which are directed at groups or areas, such as for example "predictive policing" which uses geospatial data to determine future crimes. Since these systems may contribute to over-policing and systemic discrimination, we are of the opinion that predictive policing should also be included under Annex III.6.

A problem of duplication of conformity assessment may arise in case of AI systems that are products or safety components covered by the New Legislative Framework (NLF) under Annex II. Such AI systems may undergo conformity assessment once under the NLF (Annex II) and the second time when integrated into a machine, according to Annex III. Therefore, there is a need for clear provisions that avoid duplicate tests for such AI systems which would otherwise cause inconsistency in the legal framework with contradictory assessments, accompanied with additional expenditure for companies.

5.2. High-Risk AI Systems Already Placed on the Market

Furthermore, we observe that under the AIA, high-risk AI systems are mandated to undergo a new conformity assessment procedure whenever they are "substantially modified" (Art 43(4) AIA), whereby recital (66) AIA creates a low threshold for any such "substantial modification". In contrast, the proposal creates a significantly higher threshold for high-risk AI systems already placed on the market or put into service. According to Art. 83(2) AIA, the Regulation applies to these systems only if they are "subject to significant changes in their design or intended purpose". By focusing only on the design and purpose, the proposal fails to take into account all external security risks posed to the AI systems from the purview of a "significant change", thereby creating a higher threshold for any changes or modifications in the AI systems [31] (p. 13).

5.3. Standardization as Non-Justified Delegation of Rule-Making Power

Title III, Chapter 2 AIA contains an extensive list of essential requirements which must be observed before a high-risk AI system is put on the market. In line with the NLF, all of these requirements are worded in a rather broad way. Instead of formulating the requirements for high-risk AI systems itself, the AIA defines only the essential requirements, whereas the details are left to standards elaborated by the European Standardization Organizations (ESOs). Standardization has many positive aspects. Standards can promote the rapid transfer of technologies, ensure the interoperability of systems, and pave the way to establish uniform requirements that support the implementation of legal requirements and ethical values [32] (pp. 3–4).

At the same time, however, standards create concerns surrounding excessive delegation of regulatory power to private ESOs. Such a delegation of power is problematic, above all, due to the lack of democratic oversight, the missing possibilities of relevant stakeholders (civil society organizations, consumer associations) to influence the development of standards, and the lack of judicial means to control them once they have been adopted. The standardization of AI systems is not a matter of purely technical decisions. Rather, a series of legal and ethical decisions must be made, which should not be outsourced to private ESOs, but which require a political debate involving society as a whole. The European standardization process must reflect European values and fundamental rights, including consumer protection by granting European stakeholder organizations effective participation rights [33].

Therefore, the European Commission should reconsider its approach. Instead of delegating fundamental decisions to ESOs, the AIA should establish legally binding provisions for the essential requirements of high-risk AI systems, including questions relating to but not limited to which forms of algorithmic discriminations should be prohibited; how algorithmic biases should be mitigated; what type and degree of transparency AI systems should have; how AI-driven decisions and predictions should be explained in a comprehensible way. These legally binding obligations could then, in turn, be further specified by harmonized standards for specific applications by the ESOs. Since such harmonized standards can still have far-reaching social and legal consequences, European policymakers should at the same time take the necessary steps to improve the overall process of standardization, including the structural and organizational framework of ESOs like CEN and CENELEC to facilitate an inclusive standardization system which provides for democratic input on the development of technical standards [33].

5.4. Ex Ante Conformity Assessment

We welcome that AI systems posing a high-risk must be subject to a prior conformity assessment before they can be placed on the market or otherwise put into operation in the EU.

What is concerning, however, is that the so-called "stand-alone" AI systems (Annex III) only need an internal control according to Art. 43(2) AIA. The involvement of a notified body according to Art. 43(1) AIA is only necessary for a very limited number of AI systems, e.g., certain biometric systems. With this approach, the proposal gives AI providers an unduly broad margin of discretion regarding the application and enforcement of the AIA, especially regarding the questions: (i) Whether the used software is an AI system; (ii) whether the system may likely cause harm; and (iii) how to comply with the mandatory requirements of Title III, Chapter 2 AIA, which are not laid down in detail in the proposal. Taking into account that the CE marking system failed in other sectors to protect human health and safety—such as in the medical sector, where 400.000 defective breast implants where certified by TÜV Rheinland as being safe [34] (pp. 13–27)—the European Commission should explore whether at least certain high-risk AI systems should be subject to an independent ex ante control.

5.5. Essential Requirements for High-Risk AI Systems

We appreciate that the AIA intends to introduce mandatory requirements for high-risk AI systems. Yet, as already mentioned under Section 5.3., most of the requirements are formulated in a rather broad way, giving too much discretion to AI providers. In addition, some of the mandatory requirements are not convincing for the following reasons.

5.5.1. Data and Data Governance (Art. 10 AIA)

Regarding data and data governance, Art. 10 AIA refers mainly to training, validation, and testing data sets. With the limitation to training, validation, and testing data sets, the AIA disregards other stages of ML that should also be subject to data quality criteria and data governance practices (We notice that Art. 10 AIA can also have an impact on data licenses, which are increasingly relevant in practice, and which have as their object access to data (usually for remuneration). Consequently, the "data quality" can be a reference point for contractual conformity: [35]).

On the other hand, the requirement in Art. 10(3) AIA regarding the training, validation, and testing data sets to be, inter alia, free of errors, is quite impossible to meet [13] (p. 280). Such a level of perfection is technically not feasible and might also hamper innovation. Consequently, the AIA should rather require that providers take appropriate measures to ensure that data sets are free of errors.

In addition thereto, several privacy enhancing techniques such as differential privacy [36] intentionally introduce noise into datasets in order to prevent the unintentional disclosure of sensitive data. This renders the data not free of "errors," although it helps in protecting the sensitive data which is also in consonance with the principle of data

protection by default as provided under Art. 25 GDPR. Accordingly, Art. 10 AIA should be amended to allow the use of privacy-enhancing techniques in data governance practices of high-risk AI systems.

While mandating that the training, validation, and testing data sets should be free of errors and complete, the AIA fails to define the criteria for measuring the quality of data sets (e.g., predictive accuracy, robustness, fairness of trained machine learning models).

Although the AIA requires AI providers to use data governance practices that shall concern in particular "examination in view of possible biases" (Art. 10(2)(f) AIA), the proposal fails to clarify the notion of "bias." This is problematic for various reasons. First, there is no common understanding or generally accepted definition of "bias" [37]. Second, recital (44) AIA states that AI systems should not become "the source of discrimination prohibited by Union law". However, the AIA does not indicate what forms of biases are prohibited under the existing framework and how algorithmic bias should be mitigated. Having said that, it is argued that existing EU non-discrimination law "displays a number of inconsistencies, ambiguities, and shortcomings that limit its ability to capture algorithmic discrimination in its various forms" [38]. What is also concerning is that there are different notions of fairness which are incompatible with each other (e.g., individual vs. group fairness) [39]. This leads to the problem of deciding which fairness standards are desirable. All in all, an unclear understanding of "bias" will only cause confusion among AI providers as they would not be able to apply appropriate measures to prevent or minimize bias or discrimination.

5.5.2. Transparency and Provision of Information to Users (Art. 13 AIA)

The requirements for transparency of high-risk AI systems laid down in Art. 13 AIA are certainly a step in the right direction. However, it is rather problematic that this norm only formulates general requirements without specifying them [40]. Art. 13 AIA focuses on the interpretability of AI systems' output by its users without clarifying the concept of interpretability and its correlation with explainability. While all policy documents preceding the AIA focused on explainability, the AIA refers only to interpretability (as to the various terms cf. [40]). Thus, the AIA is silent on the specific measures that need to be taken to ensure that AI systems are sufficiently transparent. Instead, this issue is largely left to the self-assessment of the provider, who must ensure that the system undergoes an appropriate conformity assessment procedure before it is placed on the market or put into service (Art. 16(a) and (e) AIA). While it is true that, according to Art. 16(j) AIA and Art. 23 AIA, providers must demonstrate, upon request of a national competent authority, that their AI system complies with the transparency requirements set out in Art. 13 AIA, the question of how to make AI systems interpretable is left to the discretion of the AI system provider.

Another problem is that under the AIA, neither providers nor users are required to provide transparency to the person affected by an AI-based prediction or decision. According to Art. 13 AIA, the provider must ensure transparency only vis-à-vis the user of the system. In this regard, we recommend that the AIA should be amended to include an obligation to explain AI-based predictions or decisions to the affected persons in order to safeguard the rights and freedoms of individuals.

5.5.3. Human Oversight (Art. 14 AIA)

In our opinion, the provision for human oversight (Art. 14 AIA) is rife with many impracticalities. First, the requirement for a human to fully understand the capacities and limitations of a high-risk AI system (Art. 14(4)(a) AIA) is currently not feasible for some AI systems and could, accordingly, lead to an indirect ban of such systems. If this is the intention of the proposal, the text of the AIA should at least point out that AI providers must not use opaque high-risk AI systems.

Second, Art. 14 AIA nowhere specifies as to when, how, and at what stage human oversight is required. Strangely enough, it is also silent on any obligation of the users to ensure human oversight. A comprehensive human oversight must entail supervision of

the AI system during its entire lifecycle by ensuring mandatory transparency measures about the use of AI applications, including public statistics on deployments, aims, scope, and developers.

The measures stipulated to ensure human oversight under Art. 14(3) AIA and the corresponding provision Art. 14(4) AIA are also silent on aspects such as non-discrimination and fairness. In that regard, it would be prudent to involve National Centers of Expertise on AI with strong engagement and involvement with civil society, equality bodies and human rights to provide qualitative inputs to the measures stipulated to ensure human oversight under Art. 14(3) AIA and propose guidelines to assess bias in AI systems.

5.5.4. EU Database (Art. 60 and Annex VIII AIA)

The AIA proposes a new central database, managed by the European Commission, for the registration of "stand-alone" high-risk AI systems. While the purpose of an EU database is to facilitate societal scrutiny for greater transparency, we raise concern over why the same should be only limited to stand-alone high-risk AI systems. The database should also encompass AI systems used by public authorities irrespective of their assigned risk level, as well as those used by private entities whenever their use has a significant impact on an individual, a specific group, or society at large.

Moreover, the information required by Annex VIII does not seem to be sufficiently comprehensive, as the data listed under the said Annex omits a number of substantial information such as the intended purpose of the system, explanation of the model or type of ML involved, actors involved in developing and deploying the system, results of any algorithmic impact assessment/human rights impact assessment carried out.

6. Obligations of Providers and Users

6.1. Misaligned Obligations

Since many AI systems operate on processing of large-scale data, there is an inherent need for it to be aligned with the existing legal framework. In this context, it seems conspicuous that the AIA requires the providers (developers) of an AI system to perform a risk assessment, whereas under the GDPR, the user (as defined under the AIA) acts as the "data controller" who takes on the task of risk assessment. This shift of roles has the effect of removing "users" from any responsibility for risk assessment under the AIA. Consequently, the AIA should provide for an obligation of high-risk AI system users to carry out an AI impact assessment similar to the one carried out under Art. 35 GDPR, Art. 39 EUDPR [41] or under Art. 27 LED [31] (p. 9), [42].

Moreover, the concept of user needs to be clarified in multi-stakeholder environments, where more than one actor is "using" the system. This is the case, for example, in the healthcare context, where a multitude of actors is involved (healthcare organization, nurses, physicians, etc.,). Since the AIA does not clarify who should be regarded as a "user" in situations where more than one person has the authority to decide about how to use the AI system, there is the risk of improper compliance with the obligations of the AIA [43] (p. 12).

6.2. General-Use AI Systems

In situations where AI systems can be used for many different purposes (general-use AI systems), there may be circumstances where such an AI technology gets integrated into a high-risk system, without the provider having any or only limited influence over the compliance obligations of high-risk AI systems. This aspect assumes major relevance since Art. 3(2) AIA presumes that the provider or developer of an AI system is also the one deploying it in a high-risk application. Therefore, we strongly suggest that the European Commission clarifies the responsibilities of providers of general-use AI systems.

6.3. AI as a Service (AIaaS)

Moreover, the AIA should clarify and delineate the responsibilities of providers and users with regard to AIaaS. Providers of AIaaS may develop either off-the-shelf software

solutions or industry specific customized software. This means that their customers often have no insight into the technology. Still, it is unclear whether customers of AIaaS qualify as "providers" or "users". If customers are regarded as "providers", they might not be in the position to satisfy the mandatory requirements set out in Title III, Chapter 2, due to their lack of knowledge. Accordingly, it is important that the AIA maps the responsibilities of providers and customers of AIaaS.

6.4. Post-Market Monitoring by Providers

We particularly welcome the provision allowing for the post marketing plan to be at the discretion of the providers and users (Art. 61 AIA), facilitated by provisions obliging providers to maintain logs automatically generated by their high-risk AI systems by virtue of a contractual arrangement with the user or otherwise by law (Art. 20 AIA). With that said, the provision obliging the provider to evaluate the continuous compliance of AI systems (Art. 61(2) AIA) appears to be counter-intuitive since complex ML techniques render continuous evaluation to become an uphill task. For this reason, we believe that owing to the complexities posed by software systems as opposed to hardware components, where detection of any anomaly is easier, the short window of 15 days provided under Art. 62(1) AIA for reporting any serious incidents and/or malfunctions to the market surveillance authorities of the Member States would be unreasonable. Therefore, we suggest that the legislators should extend the short deadline of 15 days.

Furthermore, we are of the opinion that requiring full access to training, validation, and testing datasets to the market surveillance authorities (Art. 64(1) AIA) should be omitted, as it is a highly unworkable provision. The legislators need to acknowledge that some AI systems or legacy software could be built using datasets which do not exist anymore or do not use centralized datasets. For example, Federated Learning (FL) is a technique used by AI developers to train ML models without centralized data collection. FL leaves the data where it is, distributed across numerous devices and servers on the edge. This means that it may not always be possible for these AI systems to demonstrate compliance with dataset requirements under Art. 10 AIA, generate centralized logs as outlined in Art. 12 AIA, or provide direct access to datasets per Art. 64 AIA.

Furthermore, the requirement to grant access should take into account relevant EU legislations such as the GDPR imposing data retention obligation following the data minimization principle, strict data transfer mechanisms, safeguards for security of personal data. The obligation to share source code of high-risk AI systems upon a reasoned request to the market surveillance authorities (Art. 64(2) AIA) is further problematic as source code may be protected by the EU Trade Secrets Directive [44] and the Computer Programs Directive [45]. The confidentiality provision of Art. 70 AIA seems insufficient to protect providers' intellectual property rights. Instead of stipulating full access and disclosure of data and documents, the AIA should be modified to enable the market surveillance authorities to carry out robust testing.

7. Requirements for AI Systems with Limited Risks (Art. 52 AIA)

Art. 52 AIA refers to transparency in the context of human awareness of communication with AI systems. However, while doing so, it introduces another category of subjects involved in an AI life cycle, namely "natural persons" that interact with AI systems. This causes confusion with the other terms referred to in the AIA such as "user". Thus, it would be appropriate to clarify in the AIA if these categories of subjects are any different from each other.

8. Enforcement

8.1. Lack of Effective Enforcement Structures

As mentioned under Sections 5.3 and 5.4, the AIA fails to establish effective enforcement structures, because it relies primarily on an internal self-assessment by AI providers for high-risk AI systems, combined with harmonized standards to be developed by private

ESOs. Although Member States are empowered to implement rules on sanctions, and market surveillance authorities can require that a non-compliant AI system be withdrawn or recalled from the market, this may not be sufficient to ensure effective enforcement. The experience with the GDPR shows that overreliance on enforcement by national authorities leads to very different levels of protection across the EU due to different resources of authorities, but also due to different views as to when and how (often) to take actions [46]. Moreover, Member State authorities lack the substantive standards to assess whether providers of high-risk AI systems are in breach of the AIA. Since the proposal does not set any precise requirements for high-risk AI systems, but leaves this to the self-assessment of the providers (as well as the standardization organizations), there are no (uniform) standards according to which the AIA could be enforced.

Moreover, individuals affected by AI systems, civil rights organizations, or other interested parties have no right to complain to market surveillance authorities or to sue a provider or user for failures under the AIA. Hence, the proposal also lacks effective means of private enforcement to compensate for the weak public enforcement.

8.2. Competences of the European AI Board (EAIB)

The enforcement deficit described above would also not be overcome by way of the newly created "European Artificial Intelligence Board" (EAIB). Although the EAIB is aimed to facilitate the harmonized implementation of the AIA, the proposal does not confer any powers to the EAIB regarding the enforcement. Instead, the EAIB's main purpose would be to issue opinions and recommendations on the implementation of the AIA, especially on standards and common specifications (Art. 58 AIA).

Further, the ambition of the European Commission to facilitate consistent and harmonized application of the AIA may seem dubious due to certain reasons. First, the functioning of the EAIB does not seem to be entirely independent from any political influence, insofar as the AIA has allotted a predominant role to the European Commission, which not only chairs the EAIB, but also has a right of veto for the adoption of the EAIB rules of procedure [31] (p. 15). Second, the mechanism for cooperation between either the national supervisory authorities and the individuals affected by the AIA; or among different national supervisory authorities, remains unspecified under the AIA. Therefore, there is an apparent need to revise the provisions of the AIA in order to ensure greater autonomy to the EAIB.

9. Relationship of the AIA with the Existing Legal Framework

9.1. New Legislative Framework

The European Commission intends to incorporate the AIA into the NLF of product safety requirements as a horizontal standard. The AIA is to contain specific requirements for AI systems, while the end product may well be subject to further requirements under the NLF. In the proposal, this only follows from an argumentum a contrario to Art. 2(2) AIA, which excludes AI systems that fall into the scope of the old legislative framework as safety components of products or systems, or as products or systems. Against this backdrop, we welcome that the Commission intends to adopt the AIA together with the proposed Machinery Products Regulation [47].

9.2. Civil Liability

As is common in product safety law, the AIA does not contain any provisions on civil liability for damages caused by AI systems. The proposal also lacks integration into European product liability law, currently regulated by the Product Liability Directive 1985/374 [48]. This approach is comprehensible, since the EU plans to address liability issues related to new technologies, including AI systems, in Q4 2021–Q1 2022 [49]. However, we would like to point out that the AIA should at least contain a clarification that it does not affect claims for damages by persons who have been harmed by a breach of the AIA.

Otherwise, it would remain unclear whether affected persons have a claim for damages under national law [50].

9.3. Data Protection Law

EU data protection law is basically not affected by the AIA. However, such a statement is missing in the draft; only occasional references are made to the applicability of certain relevant provisions of the GDPR or the LED. Other provisions contain specific exceptions to the provisions of the GDPR, such as Art. 10(5) or Art. 54 AIA. The provisions on data governance apply alongside the GDPR and regardless of whether the data is personal or not. From our point of view and contrary to the EDPB-EDPS, Joint Opinion 5/2021, Art. 10(5) AIA seems clear enough to create a legal basis for the processing of special categories of data.

Consequently, the GDPR and the AIA follow different approaches. While the GDPR addresses primarily the protection of individual rights, embedding the values of European fundamental rights; the AIA targets product control and systemic risks without directly establishing any individual rights.

Nevertheless, there should be an operative clause explicitly mentioning that the use of AI systems should comply with data protection laws and not just mere recitals clarifying this point. Rather, such a requirement for compliance with data protection laws should be incorporated in Chapter 2 of Title III of the AIA. This requirement must also entail creating provisions for taking into consideration the codes of conduct and certification as provided under Chapter 4 of GDPR under Chapter 2 of Title III of the AIA, as in the current form, the CE marking issued by notified bodies under the AIA simply disregards the GDPR.

Furthermore, data protection authorities (DPA) are already enforcing the GDPR, the EUDPR, and the LED on AI systems involving the use of personal data in the Member States, thus, it would be appropriate if the DPAs were also designated as the national supervisory authority pursuant to Art. 59 AIA owing to the major intersection of the scope of their work under both AIA and data protection laws in the EU [31] (p. 14).

9.4. Proposal for a Digital Services Act (DSA)

The AIA also does not clarify how it relates to the proposed Digital Services Act (DSA) [51] which is intended to update the EU's horizontal rules on online providers, amending at the same time, the E-Commerce Directive 2000/31. The explanatory memorandum of the AIA [14] only briefly states that the two legal acts are consistent with each other. Since online platforms often use AI systems to optimize their services [52] (paras. 16,17), it should be made clear, whether the obligations for high-risk systems governed by the AIA apply to platforms in addition to those arising under the DSA. There are strong arguments that the obligations of both EU regulations must be observed cumulatively, but in case of doubt, the liability privilege for platforms will prevail. Nevertheless, a statement from the EU legislator would be important here for reasons of legal certainty.

10. Regulatory Gaps of the AIA

Despite the innovative risk-based structure, the AIA appears to have some remarkable gaps.

10.1. Lack of Individual Rights

The AIA—and this is arguably one of the most crucial points—does not provide for any individual rights. Although the regulation is intended to protect fundamental rights, it lacks remedies by which individuals can seek redress for a breach of the regulation. In particular, the draft does not foresee any mechanism to facilitate individuals' recourse against AI-driven decision-making. This may be in line with the product safety regulatory approach, but it may fundamentally challenge that approach. In any case, individual rights should be well coordinated with existing entitlements.

10.2. Other Gaps

The AIA aims to implement the legal policy goals in consonance with the European values, for example the prohibition of social scoring in Art. 5(2) AIA. However, a European approach toward AI should respect not only human rights and ethical values but also other goals such as climate change and sustainability. In this regard, the AIA does not directly mention "Green AI" or "Sustainable AI" as a concrete goal of a European understanding of futureproof and sustainable AI development, which are also important topics of the European Green Deal [53].

The proposal acknowledges that AI can support socially and environmentally beneficial outcomes and that such action is needed in the high-impact sector of climate change. Recital (28) AIA mentions that the fundamental right to a high level of environmental protection should be considered when assessing the potential harm of AI systems. Nevertheless, there are only scattered provisions addressing environmental protection, e.g., under Art. 62 AIA, if providers of high-risk AI systems report any serious incident, which includes the serious damage to the environment, Art. 3(44)(a) AIA.

11. Conclusions

All in all, despite of some flaws and needed clarification, the European Commission's Proposal for an Artificial Intelligence Act has many innovative elements and is generally well designed. The risk-based regulatory approach is not only appropriate but the most practical. Nevertheless, one main aspect in need of improvement is the definition of the term "AI." The AIA employs a rather broad definition and thus creates the risk of overregulating systems, which typically do not pose any danger resulting from ML and AI techniques. The second major critique concerns the proposed (self-)enforcement structure, which mainly relies on internal controls conducted by the AI provider. In most cases, the AIA requires no external oversight. Additionally, the provisions regarding the conformity standards and criteria often appear to be fragmentary and imprecise. In contrast to the imminent overregulation attributable to the broad AI definition, the self-enforcement approach raises concerns of underregulation.

Regardless, we strongly believe that the AIA is the appropriate measure to create a safe and reliable regulatory environment for AI in Europe and, thus, is a step in the right direction.

Author Contributions: Conceptualization: M.E., V.R.S.H., F.R., H.R. and B.S.; Writing—original draft: M.E., V.R.S.H., F.R., H.R. and B.S.; Writing—review & editing: M.E., V.R.S.H., F.R., H.R. and B.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ebers, M. Regulating AI and Robotics. In *Algorithms and Law*; Ebers, M., Navas Navarro, S., Eds.; Cambridge University Press: Cambridge, UK, 2020; pp. 37–99. ISBN ISBN 9781108347846. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3392379 (accessed on 29 September 2021).
2. Gerke, S.; Minssen, T.; Cohen, G. Ethical and legal challenges of artificial intelligence-driven healthcare. *Artif. Intell. Healthc.* **2020**, 295–336. [CrossRef]
3. Tzimas, T. *Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective*; Springer: Cham, Switzerland, 2021; pp. 9–32. ISBN 978-3-030-78585-7.
4. European Commission. *Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*; COM (2021) 206 final; European Commission: Brussels, Belgium, 2021.
5. Ebers, M. *Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht*; Mohr Siebeck: Tübingen, Germany, 2016; ISBN 978-3-16-154870-3.
6. Micklitz, H.W. The Targeted Full Harmonisation Approach: Looking Behind the Curtain. In *Modernising and Harmonising Consumer Contract Law*; Howells, G., Schulze, R., Eds.; Otto Schmidt/De Gruyter, European Law Publishers: München, Germany, 2009; pp. 47–83. ISBN 9783866538603.
7. Riehm, T. Die überschießende Umsetzung vollharmonisierender EG-Richtlinien im Privatrecht. *JuristenZeitung (JZ)* **2006**, *61*, 1035–1045. [CrossRef]

8. Weatherill, S. Maximum or Minimum Harmonisation: What Kind of "Europe" Do We Want? In *The Future of European Contract Law: Essays in Honour of Ewoud Hondius to Commemorate His Retirement as Professor of Civil Law at the University of Utrecht*; Boele-Woelki, K., Grosheide, W., Eds.; Wolters Kluwer: Hürth, Germany, 2020; ISBN 9789041126993.
9. CJEU, C-376/98, ECLI:EU:C:2000:544.
10. CJEU, C-358/14, ECLI:EU:C:2016:323.
11. Valta, M.; Vasel, J. Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz: Mit viel Bürokratie und wenig Risiko zum KI-Standort? *Z. Rechtspolit. (ZRP)* **2021**, *5*, 142–145.
12. Floridi, L. The European Legislation on AI: A Brief Analysis of its Philosophical Approach. *Philos. Technol.* **2021**, *34*, 215–222. [CrossRef] [PubMed]
13. Bomhard, D.; Merkle, M. Europäische KI-Verordnung. Der aktuelle Kommissionsentwurf und praktische Auswirkungen. *Recht Digit.* **2021**, *6*, 276–283.
14. Explanatory Memorandum of the AIA, COM(2021) 206 final.
15. General 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 = GDPR), OJ 2016 L 119/1.
16. Smuha, N.; Ahmed-Rengers, E.; Harkens, A.; Wenlong, L.; MacLaren, J.; Piselli, R.; Yeung, K. How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. Leads Lab@ University of Birmingham. 2021. Available online: https://ssrn.com/abstract=3899991 (accessed on 29 September 2021).
17. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/2/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No7 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149/22, Art 5.
18. Ebers, M. Liability for Artificial Intelligence and EU Consumer Law. *J. Intellect. Prop. Inf. Technol. Electron. Commer. Law (JIPITEC)* **2021**, *12*, 204–221. Available online: https://www.jipitec.eu/issues/jipitec-12-2-2021/5289 (accessed on 29 September 2021).
19. Galli, F. Online Behavioural Advertising and Unfair Manipulation between the GDPR and the UCPD. In *Algorithmic Governance and Governance of Algorithms*; Ebers, M., Cantero, M., Eds.; Springer: Cham, Switzerland, 2020; pp. 109–135. ISBN 978-3-030-50559-2.
20. Helberger, N. Profiling and targeting consumers in the Internet of Things—A new challenge for consumer law. In *Digital Revolution: Challenges for Contract Law in Practice*; Schulze, R., Staudenmayer, D., Eds.; Nomos: Baden-Baden, Germany, 2016; pp. 135–162. ISBN 978-3-8487-2956-2.
21. Mik, E. The Erosion of Autonomy in Online Consumer Transactions. *Law Innov. Technol.* **2016**, *8*, 1–37. [CrossRef]
22. Veale, M.; Zuiderveen Borgesius, F. Demystifying the Draft EU Artificial Intelligence Act. 2021. Available online: https://osf.io/preprints/socarxiv/38p5f/ (accessed on 29 September 2021).
23. Spindler, G. Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). *Comput. Recht* **2021**, *6*, 361–374.
24. 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States—Statements Made by Certain Member States on the Adoption of the Framework Decision, OJ 2002 L 190/1.
25. Bu, Q. The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *Int. Cybersecur. Law Rev.* **2021**, *2*, 113–145. [CrossRef]
26. Büchi, M.; Fosch-Villaronga, E.; Lutz, C.; Tamò-Larrieux, A.; Velidi, S.; Viljoen, S. The chilling effects of algorithmic profiling: Mapping the issues. *Comput. Law Secur. Rev.* **2020**, *36*, 105367. [CrossRef]
27. Wendehorst, C.; Duller, Y. Biometric Recognition and Behavioural Detection. Study Requested by the JURI and PETI Committees of the European Parliament. 2021. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf (accessed on 29 September 2021).
28. van der Ploeg, I. Security in the Danger Zone: Normative Issues of Next Generation Biometrics. In *Second Generation Biometrics: The Ethical, Legal and Social Context*; Mordini, E., Tzovaras, D., Eds.; Springer: Dordrecht, The Netherlands, 2012; ISBN 978-94-007-3891-1.
29. *Biometric Recognition and Behavioural Detection, Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on Their Current and Future Use in Public Spaces*. Study Commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI and PETI Committees. 2021. Available online: http://www.europarl.europa.eu/supporting-analyses (accessed on 29 September 2021).
30. Hildebrandt, M. The Proposal for an EU AI Act of 21 April 2021. *Brief Commentary*. 19 July 2021. Available online: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2662611_en (accessed on 29 September 2021).
31. EDPB-EDPS, Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). June 2021.
32. DIN/DKE. *German Standardization Roadmap on Artificial Intelligence*; 2020; pp. 3–4. Available online: https://www.dke.de/resource/blob/2017010/99bc6d952073ca88f52c0ae4a8c351a8/nr-ki-english---download-data.pdf (accessed on 29 September 2021).
33. Ebers, M. Standardizing Ethical AI—The Case of the European Commission's Proposal for an Artificial Intelligence Act. In *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*; DiMatteo, L.A., Cannarsa, M., Poncibò, C., Eds.; Cambridge University Press: Cambridge, UK, 2022; forthcoming.

34. Kierkegaard, S.; Kierkegaard, P. Danger to public health: Medical devices, toxicity, virus and fraud. *Comput. Law Secur. Rev.* **2013**, *29*, 13–27. [CrossRef]
35. Steinrötter, B. Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts. *Recht Digit.* **2021**, *10*. forthcoming.
36. Dwork, C.; Roth, A. The Algorithmic Foundations of Differential Privacy. *Found. Trends Theor. Comput. Sci.* **2014**, *9*, 211–407. [CrossRef]
37. Goodrum, W. *Statistical & Cognitive Biases in Data Science: What Is Bias?* Elder Research, Homepage. Available online: https://www.elderresearch.com/blog/statistical-cognitive-biases-in-data-science-what-is-bias/ (accessed on 29 September 2021).
38. Gerards, J.; Xenidis, R. *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law, Special Report for the European Commission*; Publications Office of the European Union: Luxembourg, 2021. Available online: https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1 (accessed on 29 September 2021).
39. Dunkelau, J.; Leuschel, M. Fairness-Aware Machine Learning. *Working Paper*. Available online: https://www.phil-fak.uni-duesseldorf.de/fileadmin/Redaktion/Institute/Sozialwissenschaften/Kommunikations-_und_Medienwissenschaft/KMW_I/Working_Paper/Dunkelau___Leuschel__2019__Fairness-Aware_Machine_Learning.pdf (accessed on 29 September 2021).
40. Ebers, M. Regulating Explainable AI in the European Union. An Overview of the Current Legal Framework(s). In *Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence*; Colonna, L., Greenstein, S., Eds.; Forthcoming; Available online: https://ssrn.com/abstract=3901732 (accessed on 29 September 2021).
41. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (EUDPR), OJ 2018 L 295/39.
42. Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive = LED), OJ 2016 L 119/89.
43. Kiseleva, A. AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability? *Eur. Pharm. Law Rev.* **2020**, *4*, 5–16. [CrossRef]
44. 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, OJ 2016 L 157/1.
45. Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, OJ 1991 L 122/42.
46. Massé, E. *Two Years under the EU GDPR: An Implementation Progress Report*; Access Now Homepage; Available online: https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf (accessed on 29 September 2021).
47. European Commission, Proposal for a Regulation of the European Parliament and of the Council on Machinery Products, COM(2021) 202 final.
48. European Parliament and Council Directive 1999/34/EC on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products 1999 OJ L 141/20.
49. European Commission, Commission Staff Working Document, Impact Assessment, Accompanying the Proposal for a Regulation Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), SWD (2021) 84 final, Part 1/2, p. 1.
50. Grützmacher, M. Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO. *Comput. Recht* **2021**, *7*, 433–444.
51. Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.
52. Berberich, M.; Conrad, A. § 30: Plattformen und KI. In *Rechtshandbuch Künstliche Intelligenz und Robotik*; Ebers, M., Heinze, C., Krügel, T., Steinrötter, B., Eds.; C.H. Beck: München, Germany, 2020; ISBN 978-3-406-74897-4.
53. Gailhofer, P.; Herold, A.; Schemmel, J.P.; Scherf, C.-S.; Urrutia, C.; Köhler, A.; Braungardt, S. The Role of Artificial Intelligence in the European Green Deal, Study Requested by the AIDA Committee of the European Parliament, Study requested by the AIDA Committee. 2021. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662906/IPOL_STU(2021)662906_EN.pdf (accessed on 29 September 2021).