de lege

Law, AI and Digitalisation

Editors: Katja de Vries and Mattias Dahlberg

JURIDISKA FAKULTETEN
I UPPSALA

De lege

Juridiska Fakulteten i Uppsala

Årsbok 2021

Redaktör för skriftserien
Mattias Dahlberg

Law, AI and Digitalisation

Eds. Katja de Vries
and Mattias Dahlberg

iUSTUS
FÖRLAG

The Emil Heijne's Foundation for Research in Legal Science (Emil Heijnes Stiftelse för rättsvetenskaplig forskning) has generously provided financial support for the printing of this yearbook.

Upplaga 1:1
ISSN 1102-3317
ISBN 978-91-7737-167-0
Produktion: eddy.se ab, Visby 2022
Omslag: John Persson
Förlagets adress: Box 1994, 751 49 Uppsala
Telefon: 018-65 03 30
Webbadress: www.iustus.se, e-post: kundtjanst@iustus.se

Printed by Dimograf, Poland 2022

Contents

Liane Colonna

The AI Regulation and Higher Education: Preliminary Observations and Critical Perspectives

1 Introduction[1]

The introduction of Artificial Intelligence (AI) into educational contexts may be traced to the 1970s, when researchers were interested in understanding how computers could substitute one-to-one human tutoring.[2] While the development of AI-powered teaching and learning tools has steadily progressed, Higher Education (HE) institutions have been slow to adopt them. However, the Covid-19 pandemic, has drastically changed the landscape, forcing universities to rely on technology for virtual learning. Long gone are the days of clunky desktop computers sitting in lonely student computer labs. These are the days of virtual and

[1] The support of The Wallenberg AI, Autonomous Systems and Software Program – Humanities and Society (WASP-HS), Ethical and Legal Challenges in Relationship to AI-driven Practices in Higher Education (MMW2020.0138), is gratefully acknowledged. Additionally, I would like to express my gratitude to Professor Teresa Cerratto-Pargman, Associate Professor Cormac McGrath and Professor Cecilia Magnusson Sjöberg who have provided helpful comments on the manuscript, or parts thereof, at various stages in its development. An additional thanks goes to the editors of this volume, Assistant Professor Katja de Vries and Professor Mattias Dahlberg for their very constructive feedback. As far as shortcomings are concerned, they are all attributable to the author.

[2] B.S. Bloom, *The 2 Sigma Problem: The Search for Methods of Group Instruction as Effective as One-to-One Tutoring*, 13 Educational Researcher 4 (1984).

augmented realities, remote-based proctoring, Ed Tech robots, predictive learning analytics, and more.[3]

While AI may present incredible opportunities to improve teaching and learning and could have a huge impact on the future of education[4], it poses new and far-reaching ethical, legal, and social challenges.[5] Until recently, the rapid development of technology in this context has generally outpaced policy debates and regulatory frameworks about how best to develop and use AI in HE in ways that are not just equitable, ethical, and effective but also just, fair, and caring.[6] That said, on 21 April 2021, the European Commission published a legislative proposal for a "Regulation on a European Approach for Artificial intelligence" (the AI Regulation) which expressly addresses the use of AI in the educational context.

This paper investigates the proposal from the perspective of HE. More specifically, it seeks to make some preliminary observations as well as offer some critical perspectives concerning the way the proposed AI Regulation addresses the educational context, particularly in HE. It explores whether the proposal is old wine in new bottles or representative of a fundamental shift in approach towards the more ethical use of AI in the HE.

2 Background to the AI Regulation

The proposal was the result of a broad consultation process and many years of investigating whether AI requires specific regulation, and if so, how normative assumptions and ethical principles should be reflected

[3] R. Huang, J.M. Spector, Junfeng Yan, *Introduction to Educational Technology*, In: Educational Technology: Lecture Notes in Educational Technology (eds. Ronghuai Huang, Kinshuk, Mohmed Jemni, Nian-Shing Chen, J. Michael Spector) (Singapore, Springer 2019).

[4] *But see* Cerratto Pargman T. and Cormac McGrath, *Be Careful What You Wish For! Learning Analytics and the Emergence of Data-Driven Practices in Higher Education*, In: Digital Human Sciences (ed. S. Petersson)(Stockholm, Stockholm University Press 2021) (discussing the "techno-romanticism" and hype surrounding learning analytics), https://www.stockholmuniversitypress.se/site/chapters/e/10.16993/bbk.i/#disqus_thread.

[5] Cerratto Pargman T. and Cormac McGrath, *Be Careful What You Wish For! Learning Analytics and the Emergence of Data-Driven Practices in Higher Education*, In: Digital Human Sciences (ed. S. Petersson)(Stockholm, Stockholm University Press 2021), https://www.stockholmuniversitypress.se/site/chapters/e/10.16993/bbk.i/#disqus_thread.

[6] P. Prinsloo and S. Slade, *Big data, Higher Education and Learning Analytics: Beyond Justice, Towards an Ethics of Care*, In: Big Data and Learning Analytics in Higher Education, (Springer 2017), 109–124.

in the law. It builds on key documents such as the AI HLEG, Ethics Guidelines[7] which sets forth ethical imperatives in the context of AI and the Commission's White Paper on Artificial Intelligence[8] which proposes a risk-based regulation for AI with sector and application-specific risk assessments and requirements as opposed to blanket requirements or bans. The aim of the initiative is to establish a comprehensive, "futureproof" legal framework regulating AI in all sectors, including education, to foster economic growth, to ensure that there is harmonization of approaches between all 27 of the EU Member States, to offer safety and legal certainty to both consumers and industry and to create responsible[9] and trustworthy[10] AI.

As a legislative proposal, a debate and an approval process will follow, which might last until 2022. It will likely be amended by members of the EU Parliament as well as by governments of each EU Member State. Even after its publication in the Official Journal of the European Union, its implementation is likely to be incremental with full application after 24 months.[11]

3 The regulatory challenge

In a recent report by the European Parliament on AI in education, culture and the audiovisual sector, released after the AI Regulation in May 2021, it was noted: "Whilst it is easy to understand the potential effects of AI on sectors such telecommunications, transportation, traffic management, health care, evaluating its long-term effects on education" is "considera-

[7] Independent High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI 15 (Apr. 8, 2019), at https://ec-europa-eu.ezp.sub.su.se/newsroom/dae/document.cfm?doc_id=60419.

[8] *White Paper on Artificial Intelligence - A European Approach to Excellence and Trust* 16, European Commission (February 19, 2020), http://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[9] For more on responsible AI, see Virginia Dignum, *Responsibility and Artificial Intelligence*, In: (Eds. Markus D. Dubber, Frank Pasquale, and Sunit Das) The Oxford Handbook of Ethics of AI (Oxford, 2020).

[10] For more on trustworthy AI see Luciano Floridi, *Establishing the Rules for Building Trustworthy AI*, 1 Nature – Machine Intelligence 261 (2019).

[11] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final) (hereafter 'AI Regulation'), Article 85(2).

bly more challenging."[12] It further noted: "The potential impact of AI on education, culture and the audiovisual sector" is "rarely discussed and is mostly unknown. Yet this question is of utmost importance because AI is already being used to teach curricula…"[13] Here, it is interesting to note that the EU has decided to introduce the explicit regulation of AI in the educational sector without a full understanding of how AI impacts the sector. This, of course, highlights the regulatory challenge at hand.

There is a lack of confidence when it concerns the application of AI with cries from across almost all segments of society regarding the potential for the use of AI to lead to erroneous, opaque, brittle, and biased decisions. There is a fear that the use of AI can put safety, health and fundamental rights to privacy, data protection, free expression and assembly, non-discrimination, dignity at risk. For example, in the educational sector, students are concerned that marginalized students such as those with special needs and those from low-income families may disproportionately and unfairly have to pay the price of AI-based teaching and learning technologies, based on potentially racist, sexist, ableist, and hetero-centrist norms being reflected in the systems.[14] They are also deeply concerned about the role of automated individual decision making in HE, including profiling, where there is no human involvement such as where AI flags a student of color for cheating when the behavior is not actionable.[15] This could, for example, occur when an AI-based proctoring system identifies that a student is "cheating" but in reality all that has happened is that the student's child has entered the test-taker's environment to ask for a snack, causing the student to look away from the screen towards a second person.[16]

[12] European Parliament, Report on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)), https://www.europarl.europa.eu/doceo/document/A-9-2021-0127_EN.html.

[13] European Parliament, Report on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)), https://www.europarl.europa.eu/doceo/document/A-9-2021-0127_EN.html.

[14] Forthcoming, Liane Colonna, *Legal Implications of Using AI as an Exam Invigilator*, In: 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (eds. Liane Colonna and Stanley Greenstein)(Stockholm, The Swedish Law and Informatics Research Institute (IRI)).

[15] Id.

[16] Id.

On one hand, there is a need to intervene before the application of AI within society acquires even greater momentum and AI-based products and services grow larger, more complex, and, naturally, more resistant to regulatory prodding.[17] However, if intervention comes to early than the EU may regulate without fully understanding the technology's likely impact. This dilemma is sometimes referred to as the Collingridge Dilemma[18], or more colloquially as the problem of "chasing a moving target." To put it differently, when it comes to the regulation of AI in the education sector, regulators face an "uncertainty paradox"[19], "where they must make decisions in the absence of reliable risk information or foreknowledge of technological developments."[20]

Basically, the EU's goal is to get ahead of the broad, unregulated use of AI and ensure that society knows that high-risk AI has gone through an extensive vetting process so that individuals can trust it. On the other hand, there is a visceral concern that if the EU starts to introduce cumbersome legislation, then it will fall behind countries like China and the United States. As Eric Schmidt, the former CEO of Google, has said: "The EU should be an "innovation partner to the US," in order to be able to compete with China."[21] Instead, "the EU did regulation first and I think that's a mistake."[22] Sometimes this debate is framed as "regulation

[17] Lyria Bennett Moses, *How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target*, 5 Law, Innovation and Technology 1 (2013).

[18] Anna Butenko and Pierre Larouche, *Regulation for Innovativeness of Regulation of Innovation?*, 7 Law, Innovation and Technology 52 (2015), 70. (According to the Collingridge dilemma, "if regulators want to achieve results, they should act early, but then the full range of risks and benefits is unknown, and if they wait until the risks and benefits are clear, the situation solidifies in a manner that makes it difficult and expensive to introduce regulatory changes." However, in the "early stages of technological development, there is insufficient information regarding potential harms and benefits.").

[19] Marjolein van Asselt, Ellen Voss and Tessa Fox, *Regulating Technologies and the Uncertainty Paradox*, In: Dimensions of Technology Regulation (eds. M. Goodwin, B. J. Koops, & R. Leener)(Wolf Legal Publishers 2010), 259–284.

[20] Lyria Bennett Moses, *How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target*, 5 Law, Innovation and Technology 1 (2013).

[21] Pieter Haeck, *Ex-Google Boss Slams Transparency Rules in Europe's AI Bill, Politico* (31 May 2021) https://www.politico.eu/article/ex-google-boss-eu-risks-setback-by-demanding-transparent-ai/.

[22] Id.

versus innovation" or "upstream governance versus permissionless innovation."[23]

The AI Regulation addresses the pacing problem as well as the need to balance the relationship between innovation and regulation with its risk-based approach. This approach entails that the regulation differentiates between uses of AI that create (i) an unacceptable risk (Title II), (ii) a high risk (Title III) (iii) a limited risk (Title IV) and (iv) a low or minimal risk (Title IX). The first category is generally prohibited, the second category is subject to compulsory regulation such as ex-ante conformity assessment, the third category is permitted but subject to transparency obligations, and the last category is only regulated by voluntary codes of conduct.[24] Thus, the EU takes the position that it is possible to update the law of the analog age (as well as the legacy of today's ICT applications that are already up and running within the digital information society, including HE!), without hindering innovation by focusing on high-risk AI and maintaining that the vast number of use cases are not subject to the regulation. It can be argued that this approach provides legal certainty: once the proposal is finalized, businesses will know the rules of the games so they can invest properly. The rules are based on globally acceptable principles, e.g., data quality, transparency, human oversight etc. so that any great shock to the business community should be avoided. The main difference is that it is no longer enough to just sign up for a list of principles – now AI providers must prove that they abide by them, at least for those systems that present risks to health, safety and fundamental rights.

In addition to the risk approach, the proposed AI Regulation also relies on techniques to monitor and update the legislation which may prove helpful to address the pacing problem. By avoiding the creation of a law that becomes stringently fixed and difficult to change, the AI Regulation allows for incremental adjustments in governance as needs arise.[25] One example is the provisions in Article 7, for the addition of new applications to the list of high-risk uses. This approach provides flexibility and

[23] *See e.g.*, Andrew McCafee, *EU Proposals to Regulate AI Are Only Going to Hinder Innovation*, Financial Times (25 July 2021), https://www.ft.com/content/a5970b6c-e731-45a7-b75b-721e90e32e1c.

[24] For more on the risk-based approach see Stefan Larson and Jonas Ledendal, "AI i offentlig sektor: Från etiska riktlinjer till lagstiftning" in this volume.

[25] Gregory N Mandel, *Regulating Emerging Technologies*, 1 Law, Innovation and Technology 75, 89 (2009).

adaptability as well as mentally prepares industry that the list of high-risk AI is not set in stone.[26]

4 The AI Regulation and Education[27]

Referring explicitly to the educational sector, Annex III of the AI Regulation states that AI systems used for "assessing students in educational training" constitutes high-risk AI.[28] It also refers to "AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions."[29] Recital 35 underlines that "AI systems used in education or vocational training[30], notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood."[31]

First, it is unclear whether the use of AI to predict (possibly falsely) the potential success of a student and then suggest to the student not to pursue a particular line of training would fall under the category of AI systems intended to be used for the purpose of determining access to educational institutions.[32] In other words, what if a student decides, based on a prediction made by AI, to drop out of an educational program,

[26] Id.

[27] Part of this section is based on previous work: Forthcoming, Liane Colonna, *Legal Implications of Using AI as an Exam Invigilator*, In 2020–2021 Nordic Yearbook - Law in the Era of Artificial Intelligence (eds. Liane Colonna and Stanley Greenstein)(Stockholm, The Swedish Law and Informatics Research Institute (IRI)).

[28] AI Regulation, Annex III(3)(b).

[29] AI Regulation, Annex III(3)(a).

[30] Vocational training is not defined in the law but generally it can be defined as "comprising education, training and skills development relating to a wide range of occupational fields, production, services and livelihoods." See Glossary, UNESCO, International Centre for Technical and Vocational education and Training, https://unevoc.unesco.org/home/TVETipedia+Glossary/filt=all/id=474.

[31] AI Regulation, Recital 35.

[32] *See e.g.* the case known as "Drown the Bunnies … put a Glock on their heads" where the president of Mount Saint Mary's University proposed using the results of a student survey to flag students likely to fail and urge them to drop out. As he put it, "You just have to drown the bunnies … put a Glock to their heads." *For more, see* R. Schisler and R. Golden, Mount President's Attempt to Improve Retention Rate Included Seeking Dismissal of 20–25 First- Year Students, The Mountain Echo (2016).

rather than the HE institution, relying on AI, deciding to limit access of the student to the university. It is also unclear whether Annex III's reference to "assessing students in educational training" refers to using AI to facilitate remote proctoring systems used to provide online assessments of students or whether it refers to using AI to literally assess – or score – students, through for example, some kind of grading software. Regardless, remote proctoring systems may fall under high-risk AI to the extent that they involve biometric identification, discussed more below.[33]

Where an AI system is deemed to be high-risk, then providers will have an extensive range of obligations.[34] Obligations for providers of high-risk AI systems include the adoption of risk management systems[35], data governance,[36] technical documentation[37], record-keeping[38], transparency[39], human oversight[40] and accuracy of outputs and security.[41] Additionally, providers of high-risk AI systems must put in place a quality management system.[42] Many of these requirements must be performed *ex ante* before getting access to the EU market, which will ostensibly support a legal by design approach. Users of AI systems, like universities, also have explicit obligations like monitoring the operation of the high-risk AI system on the basis of the instructions of use[43] as well as storing of logs automatically generated by the AI system.[44] Users of high-risk AI systems also need to comply with user-based rules and restrictions regarding AI system monitoring, the use of input data and the storing of logs automatically generated by the AI system. Like the General Data

[33] For a discussion on the state of the art on remote proctoring exams see forthcoming, Liane Colonna, *Legal Implications of Using AI as an Exam Invigilator*, In 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (eds. Liane Colonna and Stanley Greenstein)(Stockholm, The Swedish Law and Informatics Research Institute (IRI)).
[34] See AI Regulation, Chapter II.
[35] AI Regulation, Article 9.
[36] AI Regulation, Article 10.
[37] AI Regulation, Article 11.
[38] AI Regulation, Article 12.
[39] AI Regulation, Article 13.
[40] AI Regulation, Article 14.
[41] AI Regulation, Article 15.
[42] AI Regulation, Article 17.
[43] AI Regulation, Article 29(4).
[44] AI Regulation, Article 29(5).

Protection Regulation (GDPR)[45], the proposed Regulation provides for severe penalties for non-compliance. That is regulators will be able to fine non-compliant actors up to €30m, or 6% of their worldwide turnover.[46]

The proposed Regulation provides definitions of AI "providers"[47] and AI "users"[48], referring to "public authorities" in both definitions. Here, it may be difficult to understand whether Ed Tech companies that supply products and services to HE institutions will qualify as "providers" or whether it will be the HE institutes that are given this title, and the attendant greater weight of obligations under the law. It may be particularly challenging to define public authorities as providers or users where they rely on external actors for the development of a certain AI system but put it into service under their own name. In other words, it can be very hard to distinguish between a university that makes an AI system available (through procuring an entity to build a system for it or developing it internally) ("provider") or uses an AI system ("user"). In many situations, the university is likely to be both the provider and the user. Here, the university must declare the system on the new, central database, managed by the Commission, for the registration of standalone high-risk AI systems as well as upload instructions there.[49]

As already noted, "real-time" and "post" remote biometric identification of natural persons has also been named in the proposed AI Regulation as high-risk which includes not just facial recognition, but also voice or gait recognition for identification purposes.[50] While the Commission considered a five-year moratorium on the use of such technologies in public places when initially drafting its February 2020 white paper, it ultimately decided to heavily regulate remote biometric identification sys-

[45] 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), 2016 O.J. (L 119) art. 4(5) (hereinafter GDPR), Article 9.

[46] AI Regulation, Article 71.

[47] AI Regulation, Article 3(2)('provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge).

[48] AI Regulation, Article (3)(4) ('user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity).

[49] AI Regulation, Article 60.

[50] AI Regulation, Annex III (1)(a).

tems without going for an outright prohibition. Building on an existing legal framework with respect to biometric identification like the GDPR and the Law Enforcement Directive[51], the AI Regulation proposes to regulate all biometric identification systems yet making a controversial distinction between private and state actors as well as between uses, subjecting law enforcement's real-time use of biometric identification in publicly accessible spaces to the unacceptable risk category.

Where it concerns education, the use of biometric identification, for example, for exam invigilation or roll call[52], must comply with the high-risk systems requirements discussed above. Additionally, the compliance assessment process that is required for the producer of such a system is more stringent than the one required for any other stand-alone AI system. More specifically, the use of a system that uses AI for exam invigilation must go through a third-party conformity assessment or comply with harmonized European standards.[53] These systems will also be subject to ex-post surveillance requirements.

Finally, while the AI Regulation makes special note of the use of AI in the educational sector, it is certainly clear that not every single type of AI used in education and vocational training will be considered high-risk. For example, the use of an AI algorithm to match lecture halls and lecturers and student's course to make sure they do not clash would likely be classified as minimal or no risk. If an educational technology is classified as non-high risk, then they are not required to comply with the above requirements. Nevertheless, the provider of such a technology is encouraged to create codes of conduct.[54] Here, the idea is that the voluntary application of the above requirements would help lead to a larger uptake of trustworthy artificial intelligence in the EU.

[51] Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 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. OJ L 119, 4.5.2016, Article 10.

[52] Carly Kind, *Containing the Canary in the AI Coalmine – the EU's Efforts to Regulate Biometrics*, Ada Lovelace Institute Blog (30 April 2021)(Explaining, "A biometric roll-call system would be classified as a high-risk biometrics system, requiring schools to ensure they procured products that had undergone a conformity assessment and received a CE marking.").

[53] AI Regulation, Article 43(1).

[54] AI Regulation, Article 69.

5 Critical perspectives

5.1 How to understand the risk categories and the appropriate level of acceptable risk?

When it comes to understanding the risk categories, many questions emerge: How does one precisely identify a system as high risk? What exactly is the process? Where does the input come from? While the AI Regulation provides a definition of high risk, categories and use cases and directs providers to take into account the likelihood and severity of the impact on health, safety, and fundamental rights there is plenty of room for ambiguity.[55] For example, what happen if low-risk AI turns into high-risk AI?

Technologies are situated in society and interact with people who can use them in ways not yet imagined. Indeed, the multistability of technologies, a concept proposed by Ihde that refers to the unpredictable uses of technology different from the originally intended ones, is well explored.[56] When it comes to Ed Tech, it is not hard to envisage that students or teachers might find unexpected uses for the technology that that neither the university nor the technology provider imagined which may be "high risk." For example, what happens when a teacher uses AI to gain insight into a student's learning habits (probably low risk), and that information, either consciously or unconsciously, impacts a student's final grade (probably high risk)? Will the software, perhaps first classified as minimal or no risk, be subjected to high-risk scrutiny by authorities considering this new application?

Another ambiguity concerns the level of acceptable risk. A provider must estimate and evaluate known and foreseeable risks that may emerge before putting an AI system on the market.[57] Even after the AI has received its CE mark and is on the market, there needs to be a continuous evaluation of risk and the provider must take measures to eliminate or

[55] *See e.g.* AI Regulation Article 6 and Article 65 (referring to Article 3(19) 'product presenting a risk' in Regulation (EU) 2019/1020 of the European Parliament and the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.

[56] D. Ihde, *Technology and the Lifeworld. From Garden to Earth* (Bloomington and Indianapolis: Indiana University Press 1993); Mireille Hildebrandt, *Technology and the End of Law*, In: Facing the Limits of the Law (Springer 2008), 1–22.

[57] AI Regulation, Article 9.

mitigate identified risks.[58] It appears that there will always be some residual risk if the provider cannot eliminate all known and foreseeable risks and that this risk must be acceptable but who determines what level of risk is acceptable and how much discretion should it have? Also, what happens when there are unexpected benefits from the use of a technology, and should they factor into the risk analysis?

In the context of HE, understanding what constitutes a risk for health, safety, and fundamental rights, whether it can be eliminated, what adequate measures needs to be adopted to mitigate the risks and what constitutes an acceptable risk takes place in a very complex institutional setting with a distinct organizational, political, and bureaucratic culture. Is it appropriate that Ed Tech providers will largely oversee risk calculations? What happens when one Ed Tech provider or HE institution (in the event it is found to be the provider) have a larger risk appetite than another? Is it appropriate that students and teachers are not required to be consulted in the determination of what constitutes an acceptable risk?[59]

Finally, it is worth mentioning that the proposal almost exclusively focuses on risks to individuals and not risks to society. Societal risks transcend individual harm and include uses of AI systems that might harm the democratic process, the rule of law, or in this case, public education.[60] Here, a question arises concerning whether, and if so how, to consider societal risks in this already complex risk assessment. Here, a question arises whether the proposal sufficiently requires Ed Tech providers and/or HE institutions to consider the long-term societal risks and harms associated with practices like the technological surveillance of students with AI.[61]

[58] AI Regulation, Article 61.

[59] *C.f.* Article 35(9) of the GDPR (stating, "where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.").

[60] Nathalie A. Smuha, Beyond the Individual: Governing AI's Societal Harm, 10 Internet Policy Review 1, 3 (2021).

[61] Alisia LoSardo, *Faceoff: The Fight for Privacy in American Public Schools in the Wake of Facial Recognition Technology*, 44 SETON HALL LEGIS. J. 373, 383–87 (2020); J. William Tucker and Amelia Vance, *School Surveillance: The Consequences for Equity and Privacy*, 2 EDUCATION LEADERS REPORT 4, 8 (2016).

5.2 Why is the focus on developers instead of universities, students, and teachers?

While most entities involved in the AI supply chain are required to comply with certain obligations, there is little doubt that AI providers are particularly burdened by the rules. Indeed, most of the requirements in the proposed AI Regulation rely on AI developers as "providers" under the regime to implement technical and organizational solutions to complex social issues. As hinted above, this may be a misstep given the complexity of the Ed Tech supply chain where many different actors are involved, including hardware and software providers, internet providers, subcontractors, etc. as well as, of course, the HE institutions, teachers and students that ultimately employ and use the tools.[62]

Where the proposed AI Regulation concerns high-risk AI in education, it asks these developers to self-assess their own compliance, at least concerning applications that do not involve biometric identification. While there are mechanisms built into the proposed regulation which encourage compliance with self-assessments like rigorous post-market surveillance, it can be questioned whether more responsibility should be placed on the HE institutions that put the systems to use, particularly as Ed Tech developers have played an increasingly prominent role in the HE in light of the COVID-19 pandemic. In other words, there is a concern that Ed-tech companies, representing private and commercial interests, may exert undue influence in the realm of public education, shifting power from the HE institutions to the providers of Ed Tech.[63] While HE institutions, as data controllers, will be responsible for the processing personal data, they may escape responsibility where, for example, anonymization techniques are applied in an application, therefore making the GDPR inapplicable.

Even where HE institutions are classified as providers and are responsible for the bulk of compliance, it still may be the case the proposal fails to sufficiently address the power imbalances between HE institutions and

[62] Forthcoming, Liane Colonna, *Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?*, Case Western Reserve Journal of Law, Technology & the Internet (JOLTI).

[63] European Trade Union Committee for Education, ETUCE Position on the EU Regulation on Artificial Intelligence (June 2021), European Trade Union Committee for Education, https://www.csee-etuce.org/en/resources/statements/4456-etuce-position-on-the-eu-regulation-on-artificial-intelligence-june-2021:%20Liane%20Case%20Western.

students, particularly historically marginalized and under-represented students. Here, it is worth mentioning that there are no obligations for providers and/or users of high-risk AI to consult with or notify civil society organizations and affected communities.[64] The role of national authorities and standardization bodies can be juxtaposed with the role of civil society and stakeholder engagement which, is much more limited. This is regretful since it is crucial to take a relational ethics approach to algorithmic injustices and involve multiple stakeholders at the institutional or organizational levels, from the public and private sector, to nurture a dialogue on AI practices in HE.[65] The proposal's largely technocratic approach, focusing on technical fixes like data quality, fails to engage the individuals and communities that are disproportionally impacted by the AI practices.[66]

Concerning the specific role of teachers in this context, one question is whether the role of teachers is reduced to the mere providers of instructions of AI-based technologies?[67] As stated by the European Trade Union Committee for Education, "the AI Regulation should ensure that the development of AI in education does not reduce the role of teachers to mere providers of instructions but rather serves as a supporting tool for the teaching profession while preserving the professional and pedagogical autonomy and academic freedom of teachers and academics."[68] Should

[64] Forthcoming, Michael Veale and Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act,* 20 Computer Law Review International (2021)(noting, "It is unclear whether limited existing efforts to include stakeholder representation will enable the deep and meaningful engagement needed from affected communities.").

[65] Johanna Björklund, Teresa Cerratto Pargman, et. al.,WASP-HS. Community Reference Meeting: Life in the Digital World. Report (August 2021), 6–7, https://wasp-hs.org/wp-content/uploads/2021/08/WASP-HS-CRM-Virtual-Worlds-brief_Aug-2021.pdf (further explaining, "A wide range of stakeholders needs to be involved in discussing AI in higher education. Starting with students, we need to include teachers, administration, IT department, university management, trade unions, and the EdTech industry to understand better how relations constituting AI-driven educational practices are configured and shaped."); Abeba Birhane, Algorithmic Injustice: A Relational Ethics Approach, 2 Patterns 1 (2021).

[66] Abeba Birhane, Algorithmic Injustice: *A Relational Ethics Approach*, 2 Patterns 1, 2 (2021).

[67] European Trade Union Committee for Education, ETUCE Position on the EU Regulation on Artificial Intelligence (June 2021), https://www.csee-etuce.org/en/resources/statements/4456-etuce-position-on-the-eu-regulation-on-artificial-intelligence-june-2021:%20Liane%20Case%20Western.

[68] Id.

teachers have an obligation to intervene when AI gives rise to a conclusion that a student could benefit from additional support?[69]

While users of AI in HE (*e.g.* students, teachers, academics and education staff for the education sector) must be adequately informed about the intended purpose, level of accuracy, residual risks of AI tools, there is still a question about whether the AI is sufficiently transparent.[70] Will overworked academics and busy students have time to read information about the AI and, more importantly, will they have the AI literacy skills to interpret it?[71] While the proposed AI Regulation mentions the possibility of providing users with training on AI, it is unclear what this means in practice and in terms of sustainable public funding.[72]

On one hand, the proposal mainly refers to obligations for users and providers of AI systems. Here, it could be argued that there should be clearer rights for students that suffer harms because of the illegal or unethical use of AI. The proposal delegates all enforcement responsibilities to the competent authorities who can impose financial penalties and, potentially demand a noncompliant AI system to be withdrawn from the market.[73] It does not create any specific legal right to bring a claim against a provider or user for failures under the proposed law. Furthermore, the proposal does not enable an individual affected by AI practices to lodge a complaint and seek redress from a court or authority which is an especially relevant enforcement mechanism in an age where regulators have often been reluctant stand up to big technology firms (think: Max Schrems). There are no collective action mechanisms like there are in the GDPR.[74] It is also worth mentioning the proposal does not create the kinds of substantive rights for individuals such as those found in Chapter III of the GDPR ("Rights of the data subject").

[69] Teresa Cerratto Pargman, Cormac McGrath, *Mapping the Ethics of Learning Analytics in Higher Education: A Systematic Literature Review of Empirical Research*, 1 Journal of Learning Analytics 17 (2021).

[70] European Trade Union Committee for Education, ETUCE Position on the EU Regulation on Artificial Intelligence (June 2021), https://www.csee-etuce.org/en/resources/statements/4456-etuce-position-on-the-eu-regulation-on-artificial-intelligence-june-2021:%20Liane%20Case%20Western.

[71] Id.

[72] Id.

[73] AI Regulation Article 65(2), Article 71.

[74] GDPR, Article 80.

On the other hand, there exists many other laws where students can enforce their rights and complain against AI practices such as under non-discrimination laws, the GDPR, product legislation, tort law. Furthermore, the European Commission is expected to publish a draft liability framework for AI systems which could potentially strengthen the rights of individuals who are adversely impacted by AI systems. As such, it may be that the core idea behind the proposal is to enforce existing remedies rather than create new ones. This proposition is supported by reference to Article 64 which provides detailed rules for access to data and documentation by national public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights.

5.3 When it comes to governance and oversight, who is doing what (when, and at what level?)

When it comes to governance and oversight, questions arise concerning who is doing what (when, and at what level?). The governance structure of the proposed AI Regulation involves a European as well as a national level. At the European level, with the European Commission acting as Secretariat, there exists the European Artificial Intelligence Board (EAIB), as well as the Expert Group (in planning).[75] The EAIB is tasked with collecting and sharing expertise and best practices among Member States; contributing to uniform administrative practices in the Member States; and issuing opinions, recommendations or written contributions on matters related to the implementation of the Regulation.[76]

At the national level, Member States have an important role in the application and enforcement of the proposal. Importantly, Member States must designate National Competent Authorities (NCA) to ensure the application of the law. Under the ambit of NCA is the National Supervisory Authority, Notifying Authority, and the Market Surveillance Authority (MSA).[77] The National Supervisory Authority is the authority to which a Member State assigns the responsibility for the implementation and application of the Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point

[75] AI Regulation, Article 56–58.
[76] AI Regulation, Article 58.
[77] AI Regulation, Article 3(43).

for the Commission, and for representing the Member State at the European Artificial Intelligence Board.[78] Notifying authorities are responsible for setting up and carrying out the necessary procedures for the assessment, designation, and notification of conformity assessment bodies and for their monitoring.[79] The MSA is tasked with monitoring market activities, informing national authorities of breach of obligations, and performing activities and taking measures pursuant to Regulation (EU) 2019/1020.[80] Additionally, there are the Conformity Assessment Bodies that apply for notification and as a result become a notified body tasked with performing conformity assessments, testing, certification and inspection.[81]

These national competent authorities will have a key role for embedded AI as well as AI that relies on biometric data like Facial Recognition Technology (FRT) since these types of AI require third-party conformity assessments as well as conduct post market surveillance. It appears that the Commission would like to rely on supervisory bodies that have already been designated in accordance with other relevant Union harmonization legislation wherever possible. For example, most Member States have a body that regulates automobiles: now that body would be tasked with checking the AI in a car before giving a CE mark for the entire product. It will be harder to locate notified bodies for the new self-standing AI[82] categories like those that exist in the Ed Tech sector. Here, it appears that a Member State can opt for a sectoral approach (e.g., have its labor agency review AI tools for human resources or have its financial authority review AI tools for finance). Alternatively, it could take a more omnibus, "one stop shop" approach, delegating most tasks to a body like the Member State's DPA. It is unclear which national authority will represent each Member State in the European Artificial Intelligence Board (if the Member State takes a sectoral approach), although European Data Protection Board and European Data Protection Supervisor are already calling for

[78] AI Regulation, Article 3(42).
[79] AI Regulation, Article 3(19).
[80] AI Regulation, Article 3(26).
[81] AI Regulation, Article 33.
[82] Self-standing AI systems can be contrasted with systems that are implemented into other products like AI embedded into autonomous cars or smart toys.

DPAs to be designated as national supervisory authorities pursuant to Article 59 of the Proposal.[83]

Most Ed Tech will fall outside of high-risk AI and therefore not be subject to oversight under the Regulation. However, Ed Tech that utilizes biometric data will constitute high risk AI and therefore be subject to third party conformity assessment, at least where harmonised standards or common specifications have not been applied. It is unclear what Member State agency will be tasked with conducting the conformity assessment, but it is likely to be the DPA. Ed Tech that is used to assess students[84] or determine access to education[85] will be able to rely on conformity assessment procedure based on internal control (detailed in Annex VI), which does not require any involvement from a notified body but is nevertheless subject to post-market surveillance by the national competent authority(s).

With many different actors in the space working in different locations, times frames and with possibly different information, it is easy to imagine a lack of coordination, particularly where it concerns the monitoring of risk. This is especially true given the fact the supply chain of AI products and services is increasingly complex, distributed, and diverse.[86] The increased complexity of the supply of AI-based Ed Tech may make it harder not only for those participants acting within the supply chain to manage responsibility, as well as risk, more broadly, but also for external parties with monitoring and oversight duties.[87]

There is also a question about whether there is sufficient expertise and resources for monitoring and assessing at the national level. If expertise and resources are lacking, this may prohibit the adoption of swift qualification procedures which could have a major impact on the development

[83] European Data Protection Board, *EDPB & EDPS Call for Ban on Use of AI for Automated Recognition of Human Features in Publicly Accessible Spaces, and Some Other Uses of AI that Can Lead to Unfair Discrimination* (21 June 2021), https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

[84] AI Regulation, Annex III(3)(b).

[85] AI Regulation, Annex III(3)(a).

[86] Petri Helo, Yuqiuge Hao, *Artificial Intelligence in Operations Management and Supply Chain Management: An Exploratory Case Study*, Production Planning & Control (2021).

[87] Slinger Jansen, Sjaak Brinkkemper, Anthony Finkelstein, *Providing Transparency in the Business of Software: A Modeling Technique for Software Supply Networks*, In: Establishing the Foundation of Collaborative Networks (Camarinha-Matos L.M., Afsarmanesh H., Novais P., Analide C. (eds)) (Springer, Boston, MA. 2007).

of AI within the EU. The possibly overlapping nature of these new AI regulatory bodies with DPAs may also cause confusion, and potentially undermine the authority of these bodies. Where it concerns the HE, the role of educational trade unions is unclear.[88] It is also unclear whether there will be boards similar to institutional review boards (IRB) that have an oversight role where it concerns the use of AI in HE.

5.4 Do the restrictions on biometric data go far enough?[89]

There is a question concerning whether the EU's proposal is sufficient to mitigate the potential abuse caused by technologies like FRT. There is a substantial body of research that demonstrates that the use of FRT technologies threatens marginalized communities.[90] Study after study demonstrates that FRT is typically better at detecting light-skinned people than dark-skinned people, and better at detecting men than women.[91] This, of course, raises concerns that women or students of color will disproportionately and unfairly bear the consequences of these technologies.[92] Other groups at risk for discrimination by FRT technologies include: students with accessibility needs; students with learning disabil-

[88] European Trade Union Committee for Education, ETUCE Position on the EU Regulation on Artificial Intelligence (June 2021), https://www.csee-etuce.org/en/resources/statements/4456-etuce-position-on-the-eu-regulation-on-artificial-intelligence-june-2021:%20Liane%20Case%20Western (explaining, "Education trade unions have a crucial role to play to addressing the risks of Artificial Intelligence in education and bring the perspective of AI users on the implementation of the regulation.".

[89] Part of this section is based on previous work: Forthcoming, Liane Colonna, Legal Implications of Using AI as an Exam Invigilator, In 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (eds. Liane Colonna and Stanley Greenstein)(Stockholm, The Swedish Law and Informatics Research Institute (IRI)).

[90] *See e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research (2018), http://proceedings.mlr.press/v81/buolamwini18a.html (last accessed April 27, 2021).

[91] Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT News (February 11, 2018), http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 (last accessed April 27, 2021); Meredith Whittaker et al., *AI Now Report 2018*, AI NOW Institute, at 16 (December 2018) *citing* Buolamwini & Gebru, *id.*

[92] Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, Duke L. & Tech. Rev. 249, 250–58 (2020).

ities, neurodivergence, and anxiety; low-income and rural students; and transgender students.[93]

Bias can arise both because of technical and social aspects. Technical biases arise from the way in which both hardware and software systems are designed[94] and "reduce the performance of the algorithm, hindering the achievement of its objective."[95] A core technical reason for why FRT technologies fail to identify people correctly is the use of training data sets that, for example, do not include people of African descent.[96]

An additional problem is that AI is often seen as neutral and not subject to the biases of human beings.[97] It is also the case that education is seen as neutral instead of acknowledging that is related to the changing socio-cultural and political-economic context.[98] Here, it is possible for an algorithm to be highly accurate yet be biased from a social point of view.[99] To put it differently, societal biases can be reproduced in an algorithm.[100] From an ethical and legal point of view, it can be argued that

[93] Tyler Sonnemaker, *Tech Companies Promised Schools an Easy Way to Detect Cheaters During the Pandemic. Students Responded by Demanding Schools Stop Policing Them Like Criminals in the First Place*, Insider (November 1, 2020), http://www.businessinsider.com/proctorio-silencing-critics-fueling-student-protests-against-surveilalnce-edtech-schools-2020-10?r=US&IR=T (last accessed April 27, 2021).

[94] The Institute of Technological Ethics, Three Kinds of Bias in Computer Systems, https://www.technologicalethics.org/three-kinds-of-bias (providing examples of technical bias such as "designers and programmers have a strong preference for one tool more than other tools, even though some other tools may be better or more appropriate for developing a product that will work better for achieving the purpose or end-goal as held by the product owner.")

[95] Institut Montaigne, Algorithms: Please Mind the Bias! Report March 2020, http://www.institutmontaigne.org/ressources/pdfs/publications/algorithms-please-mind-bias.pdf.

[96] Jay D. Aronson, *Computer Vision and Machine Learning for Human Rights Video Analysis: Case Studies, Possibilities, Concerns, and Limitations*, 43 Law & Soc. Inquiry 1188, 1194–95 (2018).

[97] Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, Duke L. & Tech. Rev. 249, 250–58 (2020).

[98] G. Biesta, *Good Education in an Age of Measurement: On the Need to Reconnect with the Question of Purpose in Education*, 21 Educational Assessment, Evaluation and Accountability 33 (2009).

[99] Institut Montaigne, Algorithms: Please Mind the Bias! Report March 2020, http://www.institutmontaigne.org/ressources/pdfs/publications/algorithms-please-mind-bias.pdf.

[100] Id.

AI should not just be "bias preserving" but also capable of improving the status quo.[101]

Where it concerns HE, universities are increasingly relying on AI-based FRT. For example, many universities have used FRT to authenticate remote users that connect from offsite the campus as well as to identify cheating and other dubious behavior throughout the online exam process during the Covid 19 pandemic.[102] The proposed AI Regulation makes a sharp distinction between identification and verification techniques, placing stricter rules on the former, and essentially placing AI used for verification purposes outside the scope of high-risk AI all together.[103] In other words, if biometric data is processed for the purpose of verification, which does not aim to uniquely identify a natural person, the processing would not fall within the categorization of high-risk AI in Annex III. While the Council of Europe has explained that biometric verification contains less risk than biometric identification because the utilization of a database is not required, it certainly contains risk such as those to fundamental rights described above.[104] Here, there is a question with the AI Regulation goes far enough to address such concerns which will no doubt be subject to great debate before the proposal becomes law.

[101] Sandra Wachter, Brent Mittelstadt & Chris Russell, *Bias Preservation in Machine Learning: The Legality of Fairness Metrics Under EU Non-Discrimination Law*, W. Va. L. Rev. (forthcoming 2021), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792772.

[102] Forthcoming, Liane Colonna, *Legal Implications of Using AI as an Exam Invigilator*, In: 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (eds. Liane Colonna and Stanley Greenstein)(Stockholm, The Swedish Law and Informatics Research Institute (IRI)).

[103] Id.

[104] *See* Council of Europe, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data (Strasbourg: 2005), and the updated Progress Report of 2013, T-PD(2013)06, https://rm.coe.int/progress-report-on-the-application-of-the-principlesof-convention-108/1680744d81; *see also* E.J. Kindt, *Having Yes, Using No? About the New Legal Regime for Biometric Data*, 34 Computer Law and Security Review 523 (2018)(explaining, "The distinction between these two functionalities, whereby identification requires a data-base with one or more data records, is of key importance in the discussion and regulation of biometric data processing.").

5.5 Interoperability – how is this regulation going to deal with the global nature of Ed Tech?

The proposed AI Regulation is so far the most comprehensive and large-scale legislative initiative to regulate AI that has been taken and it means that the world is particularly focused on Brussels and the negotiations taking place there. Certainly, the EU sees itself as a regulatory leader where it concerns personal data protection, and it is no doubt following along the same path where it concerns the regulation of AI.[105] That said, it is unclear whether the proposed AI Regulation will have the same global impact with this proposal as the GDPR, especially given the proliferation of actors in the field already issuing soft law, hard law, and self-regulatory initiatives. It is also unclear what the proposal will mean for transatlantic AI partnerships and cooperation.

Many of the biggest AI firms are in the US and it remains to be seen whether they will be willing to adapt to the new rules to enter the EU market. While there is greater alignment in values between the democratic regimes of the US and the EU, than China, for example, and certainly some convergence where it concerns the regulation of AI (e.g., some US cities have already banned the use of FRT)[106], the US tends to prefer a more sectoral, self-regulatory approach to technology regulation with a consumer protection model of enforcement over the omnibus approach exemplified in the EU. It is likely that big tech firms that want to sell their product or service in Europe will need to adjust their systems to meet the regulatory burden, but smaller companies may simply decide to the avoid the market all together.

Broadly, the term interoperability is "the ability of diverse systems and organizations to work together."[107] The meaning of interoperability has expanded beyond its technical origins to include a diverse range of social,

[105] See Lee A.Bygrave, The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, 40 Computer Law and Security Review 105460 (2021)(providing a detailed and critical overview of the "Brussels Effect" of EU data protection law).

[106] See Blake Montgomery, *Facial Recognition Bans: Coming Soon to a City Near You*, The Daily Beast (July 31, 2019), http://www.thedailybeast.com/facial-recognition-bans-coming-soon-to-a-city-near-you (last accessed April 27, 2021).

[107] Hunton Privacy Blog, *Interoperability: Facilitating the Global Flow of Data* (14 June 2012) https://www.huntonprivacyblog.com/2012/06/articles/interoperability-facilitating-global-flow-data/.

political, and legal frameworks.[108] In other words, while the development of AI requires interoperability of information systems (e.g., codes and architecture), it also requires the interoperability of legal systems. Interoperability can be seen as a tool to assist the growth of the digital economy, promote innovation, facilitate compliance for multinational firms and strengthen fundamental rights protections for individuals around the world.[109] Svantesson has suggested that interoperability should be a policy aim of lawmakers "to the greatest degree possible."[110]

Where it concerns Ed Tech, there is a need for both sides of the Atlantic to come together both on the development of the technology as well as to create a shared market. This is, of course, easier said than done. The 27 EU member states have a hard time creating a single market so adding the US to the mix most certainly adds complexity. On one hand, making transnational entities choose between conflicting regulatory frameworks is regretful at a time when promoting legal interoperability is critical to support the development of AI applications in key sectors like education. On the other hand, it is possible, in the long run, that the proposal will lead to interoperability through the creation of a common legal, ethical, and technical standards.

6 Conclusion

This paper has made some preliminary observations as well as offered some critical perspectives concerning the way the proposed AI Regulation addresses the educational context, particularly HE. It concludes that the proposal represents a fundamental shift in approach towards the more ethical use of AI in the HE, albeit one that suffers from certain defects

[108] *What is Interoperability?*, Network Centric Operations Industry Consortium, https://www.ncoic.org/technology/what_is_interoperability.

[109] Hunton Privacy Blog, *Interoperability: Facilitating the Global Flow of Data* (14 June 2012) https://www.huntonprivacyblog.com/2012/06/articles/interoperability-facilitating-global-flow-data/.

[110] Dan Jerker B Svantesson, *The Holy Trinity of Legal Fictions Undermining the Application of Law to the Global Internet*, 23 International Journal of Law and Information Technology 219, 234 (2015)(stating, "(o)ur aim should be to create jurisdictional interoperability between the different domestic legal systems to the greatest degree possible… by identifying any uniting features (of which there are many), and in seeking to iron out inconsistencies and clashes, between domestic legal systems, both in substantive and procedural rules, much can be achieved.").

that may undermine its ultimate effectiveness as a mechanism to ensure accountable, transparent, and responsible AI. These defects include the difficulty of understanding high-risk applications of AI in the Ed Tech sector as well as a lack of focus on universities, students, and teachers who ultimately employ and use the tools. When it comes to governance and oversight, there are a multiplicity of actors at both the national and EU level that possess different competences, interests, and capabilities. This introduces complexity and possibly a lack of coordination that may undermine effective governance. There is also a question about whether there is sufficient expertise and resources for monitoring and assessment at the national level. Furthermore, there is an issue concerning whether the EU's proposal is sufficient to mitigate the potential abuse caused by technologies like FRT in the HE context. Finally, it is unclear how this regulation will deal with the global nature of AI-based Ed Tech and promote legal interoperability in the realm of AI.