Legal Implications of Using AI as an Exam Invigilator*

LIANE COLONNA

The Covid-19 pandemic has taken the world by surprise, forcing many countries to adopt shelter-in-place directives, as well as partial or total lockdown and social distancing orders in order to contain the spread of the virus. Universities around the globe have been profoundly affected by stay-at-home orders, which have required them to close their doors and shift to online education. Despite long-standing skepticism to online teaching and learning, at least compared to active and in-person education, it has become the main platform for education during the pandemic, creating colossal pedagogical changes. One of the biggest challenges that universities have had to confront due to the unexpected and sudden shift to online education concerns what kind of assessment techniques are appropriate in an online environment.

In an effort to avoid delaying or postponing examinations amid the Covid-19 outbreak, many universities have turned to online proctoring tools, raising complex questions about how they can ensure the integrity of online assessments while at the same time respect ethical and legal constraints, especially regarding students' fundamental rights to privacy, data protection and non-discrimination.[1] While institutions insist that these tools are necessary in

* 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.

1 *See* Neil Selwyn et al., *A Necessary Evil? The Rise of Online Exam Proctoring in Australian Universities*, Media Int'l Australia (2021).

order to fulfil the requirements of distance education and to ensure the integrity of the exams, students raise legitimate concerns about whether universities have lawful grounds to process their personal data, particularly when their consent is not provided. They also raise questions about the surveillance effect of online proctoring, which can increase testing anxiety as well as diminish trust and cooperation between students and institutions. Students are further concerned about the technical and social biases that can be embedded into the algorithms that fuel the technology, leading to marginalized students disproportionately and unfairly having to pay the price of these technologies, based on potentially racist, sexist, ableist, and hetero-centrist norms being reflected in the systems.

This article considers the legal implications of the use of remote proctoring using artificial intelligence (AI) to monitor online exams and, in particular, to validate students' identities and to flag suspicious activities during the exam to discourage academic misconduct like plagiarism, unauthorized collaboration and sharing of test questions or answers. The emphasis is on AI-based facial recognition technologies (FRT) that can be used during the authentication process for remote users during the online exam process as well as to identify dubious behavior throughout the examination. The central question explored is whether remote proctoring systems are necessary and lawful based on European human rights law.

The first part of the paper explores the use of AI-based remote proctoring technologies in higher education (HE), both from the institutional perspective as well as from the student perspective. It emphasizes how universities are shifting from a reliance on systems that include human oversight, like proctors overseeing the examinations from remote locations, towards more algorithmically driven practices that rely on processing biometric data. The second part of the paper examines how the use of AI-based remote proctoring technologies in HE impacts the fundamental rights of students, focusing on the fundamental rights to privacy, data protection, and non-discrimination. Next, it provides a brief overview of the legal frameworks that exists to limit the use of this technology. Finally, the paper closely examines the issue of legality of processing in an effort to unpack and understand the complex legal and ethical issues that arise in this context.

Online proctoring tools

In a conventional classroom, exams are proctored by a human being who monitors the students and the physical environment during the exam. In the context of online exams, there is likewise a need for reliable and inexpensive monitoring abilities in order to authenticate test takers' identities, observe the test taker's behavior to preserve academic integrity, and secure test content.[2] Currently, there exist different methods for online proctoring. The focus herein is on live proctored testing and AI proctored testing.

The first group of methods rely on human proctors watching the test takers through a webcam from a remote location.[3] Sometimes this approach is referred to as "online human monitoring."[4] Typically, the online proctoring process starts with a verification of the exam-taker's identity.[5] This may happen by, for example, presenting an identity card like a student card, a driving license or passport to the proctor via the student's webcam.[6] Next, the proctor may ask each test-taker to move his or her webcam around to scan their physical testing environment in order to make sure the student does not have access to unpermitted items like phones or books.[7] It is also important to note that key functionalities from the test-taker's computer may be disabled, like copying, pasting, printing, taking a screen shot or accessing other applications.[8] During the exam, the proctors watch and listen for any unusual behaviors of the test taker, such as unusual eye movements or removing oneself from the field of view, and can alert the test taker or even stop the test in the event

2 Thomas Langenfeld, *Internet-Based Proctored Assessment: Security and Fairness Issues*, 39 Educational Measurement: Issues & Practice 24 (2020).

3 Yousef Atoum et al., *Automated Online Exam Proctoring*, 19 IEEE Transactions on Multimedia 1609 (2017).

4 *Id.*

5 Aiman A. Turani, Jawad H. Alkhateeb & AbdulRahman A. Alsewari, *Students Online Exam Proctoring: A Case Study Using 360 Degree Security Cameras*, 2020 Emerging Technology in Computing, Communication and Electronics (ETCCE), 1–5 (2020).

6 *Id.*

7 *Id.*

8 *Id.*

of suspicious behavior.[9] These types of proctoring exams can take place in real time or, for a more flexible model, can be pre-recorded and played back to a proctor at a later point in time.[10] They can be given at local testing centers but due to the increased ownership of laptops and tablet computers, and, of course, the pandemic situation, they have been increasingly administered in students' homes.[11]

Drawbacks to this approach include labor intensiveness and cost as it often takes many human proctors to monitor the test-takers.[12] Additionally, the proctor might have limited vision and may not be able to observe all cheating strategies, such as notes laying on a test taker's desk.[13] As noted, it may be possible for the remote proctor to ask the test-taker to sweep the room using his or her webcam, but this may create undue pressure and stress for the test taker, as well as reveal intimate information about the student's private life to the remote, human proctor.[14] Furthermore, remote proctored exams require well-established infrastructure, on both the student and institutional sides, including software, hardware and a stable internet connection.[15]

Because of these drawbacks, vendors have begun to supplement live proctoring with AI proctoring, which can automatically detect indications of possible fraud. Since AI is an umbrella term, denoting the use of many different types of technologies, it is important to clarify at the outset that this article is focused on the use of FRT, an application of computer vision. FRT is a "touchless" form of biometric that makes it possible to track an individual based on, for example, iris recognition and facial recognition.[16] More specifically, an algorithm is used to recognize a human face through the use

9 Atoum et al., *supra* note 3.

10 Turani, Alkhateeb & Alsewari, *supra* note 5.

11 Selwyn, *supra* note 1.

12 Atoum et al., *supra* note 3.

13 *Id.*

14 *Id.*

15 Fiseha M. Guangul et al., *Challenges of Remote Assessment in Higher Education in the Context of COVID-19: A Case Study of Middle East College*, 32 Educational Assessment, Evaluation and Accountability 519 (2020).

16 Jeff D. Neuburger, *Will the Role of Facial Recognition Grow In a Post-COVID-19 World?* 25 Cyberspace Lawyer 4 (2020).

of biometrics, which track facial features from a photo or video.[17] These facial features often include the distance between a person's eyes, the distance from their forehead to their chin, and other "facial landmarks."[18]

FRT can be used to support (or replace) human proctors in a number of different ways. First, it can be used to recognize students' in-test (mis)behavior by checking room conditions and analyzing behavior that might indicate cheating.[19] Furthermore, FRT can identify additional faces in a given testing environment that may be assisting the student in an inappropriate manner.[20] It can also recognize unauthorized objects in a testing environment.[21] Furthermore, it can track eye movements which may indicate misconduct, like looking away from the screen.[22]

Besides helping to ensure academic integrity, FRT has a key role to play regarding authentication in advancing proctoring methods.[23] Biometric authentication methodologies rely on intrinsic physical and behavioral traits rather than things like username/passwords or access card/PINs.[24] For example, in biometric verification, discussed more below, FRT might be used to match a student's photographed ID with the student's facial features.[25] Thereafter, biometric data can be captured continuously from the user during an exam session in

17 Steve Symanovich, *How Does Facial Recognition Work?*, Norton (February 8, 2019) http://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html (last accessed Apr. 27, 2021).

18 *Id.*

19 Evan Selinger, *Abolish A.I. Proctoring*, https://onezero.medium.com/abolish-a-i-proctoring-c9e017dd764f (last accessed April 27, 2021); Selwyn, *supra* note 1.

20 Aileen Scott, *Artificial Intelligence Is Making Online Proctoring Safe and Secure*, Medium (March 14, 2019), http://medium.com/@aileenscott604/artificial-intelligence-is-making-online-proctoring-safe-and-secure-9b03845602da (last accessed April 27, 2021).

21 *Id.*

22 Selinger, *supra* note 19; Scott, *supra* note 20.

23 Atoum et al., *supra* note 3.

24 Corey Ashby, Amit Bhatia, Francesco Tenore, Jacob Vogelstein, *Low-cost Electroencephalogram (EEG) Based Authentication*, 5th International IEEE/EMBS Conference on Neural Engineering 442–445 (2011).

25 Selwyn, *supra* note 1.

order to verify the exam taker throughout the session.[26] This might be accomplished through, for example, the use of eye tracking and facial detection.[27]

Fundamental rights implications of proctoring exams

Privacy and data protection

Privacy and data protection have long been leading concerns with eLearning, and when it comes to online proctoring systems the issues only multiply.[28] A first concern is that of the legality of processing, especially concerning the processing of biometric data like student' faces as well as student's living spaces.[29] This issue will be explored in detail below.

A related, and equally complex, concern involves the role of automated individual decision making, including profiling, where there is no human involvement. Here, concerns arise where AI flags a student for cheating when the behavior is not actionable; for example, where a student's child enters the test-taker's environment to ask for a snack, causing the student to look away from the screen towards a second person. Other scenarios can easily be imagined such as where a student urgently needs to get up to urinate or change a sanitary pad.[30] While many software providers insist that their proctoring systems are trustworthy to the extent that humans can review the computer-generated results before sanctions are imposed, it is not clear that ex post human review is capable of mitigating the risks of

26 Hadian S. G. Asep & Y. Bandung, *A Design of Continuous User Verification for Online Exam Proctoring on M-Learning*, 2019 International Conference on Electrical Engineering and Informatics 284–289 (2019).

27 Selwyn, *supra* note 1.

28 Faten F. Kharbat & Ajayeb S. Abu Daabes, *E-proctored Exams During the COVID-19 Pandemic: A Close Understanding*, Education and Information Technologies (2021).

29 Anandi Barker, *Big Brother is Proctoring You*, The Daily Texan (September 23, 2020), http://thedailytexan.com/2020/09/23/big-brother-is-proctoring-you/ (last accessed April 27, 2021).

30 Heather Murphy, *She Was Going Into Labor. But She Had a Bar Exam to Finish*. The New York Times (September 13, 2020)(last accessed May 3, 2021)(explaining how students have urinated in their seats in order to avoid being flagged for cheating and how one woman even gave birth during a remote exam).

harms created by these systems, particularly as the exam review process can be expensive, complex and outsourced to actors far removed from the local context.[31]

It is also important to mention the surveillance effect that may arise when students feel as though they are being watched under a constant microscope as they take online exams in their homes, traditionally an area designated with a very high level of privacy protection.[32] Not only can intensely personal information about a student, such as their lifestyle choices and socio-economic status, be revealed in the home setting, but online assessment tools may also make students feel like cheaters, even before submitting any work.[33] The surveillance capabilities of AI-based proctoring tools may create a lack of trust and cooperation between the students and the institution by causing them to feel that they are in a "less nurturing, comfortable learning environment."[34] It may also exacerbate existing test anxiety[35] causing some students to refrain from taking certain exams out of fear that they would be accused of cheating for accidentally moving

31 Michael Dodge, *Online Exam Monitoring is Now Common in Australian Universities — But Is It Here to Stay?* The Conversation (April 18, 2021), http://theconversation.com/online-exam-monitoring-is-now-common-in-australian-universities-but-is-it-here-to-stay-159074 (last accessed April 26, 2021)(explaining that suspicious behaviour can be reviewed by a "live" remote proctor. This work is often outsourced to developing nations such as India and the Philippines, where remote proctors are reportedly paid around $3.50 per hour.)

32 Beverly Balos, *A Man's Home Is His Castle: How the Law Shelters Domestic Violence and Sexual Harassment*, 23 St. Louis U. Pub. L. Rev. 77, 90 (2004)("The home and non-interference with the sanctity of home is well established. It is not just a physical place but is imbued with idealized characteristics. It is a place of respite from the commercial marketplace. It fosters intimate relationships and allows family life to flourish. It is also a place of safety and physical comfort. Beyond relational intimacy, the home also functions as a symbol for a feeling of belonging and a place where one can realize one's potential.")

33 Jessica Wong, *Post-secondary Students Call for Changes to Online Exam Rules as Cheating Concerns Rise*, CBC News (October 25, 2020), http://www.cbc.ca/news/canada/post-secondary-assessment-integrity-proctoring-1.5767953 (last accessed April 27, 2021).

34 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 & Amelia Vance, *School Surveillance: The Consequences for Equity and Privacy*, 2 Education Leaders Report 4, 8 (2016).

35 Barker, *supra* note 29.

too much or going off screen, particularly those with disabilities who do not want to (or have the means to) go through the "grueling, exposing and expensive process" of requesting accommodations.[36] Essentially, students are required to show their private homes, be in an interruption-free space with sufficient lighting, have a computer and stable internet connection, maintain consistent eye contact with a webcam — in addition to knowing the course content, which understandably can seriously increase their anxiety and break down trust.[37]

Some experts argue that FRT will breed a "generation that will be comfortable with and fully accepting of total government surveillance."[38] In other words, FRT might "normalize invasive means of surveillance in the eyes of students."[39] One commentator notes: "When professors rely on proctoring services, they devalue their students' privacy and mental ease while forcing them to demonstrate their comprehension of class material in almost dystopian conditions."[40] In short, there is a genuine concern that "surveillance pedagogy" is becoming entrenched in contemporary education.[41]

Relatedly, the use of FRT may create a threat to intellectual privacy, understood as "a much-needed protection for learning, reading and communicating" that helps students develop their free thoughts, creativity, risk-taking and overall inquisitiveness.[42] Tucker and Vance explain: "If students feel as though they cannot step outside of the mainstream for fear of ridicule or are afraid to ask a question because their ignorance might be captured forever in the virtual cloud, then surveillance has gone too far."[43] Hartzog and Selinger suggest that

36 Heather Murphy, *She Was Going Into Labor. But She Had a Bar Exam to Finish*. The New York Times (September 13, 2020)(last accessed May 3, 2021)(also describing how students have resorted to wearing diapers or urinating in their seats).

37 Wong, *supra* note 33.

38 Brian Heaton, *State Legislatures Grapple with Biometrics Use in Schools*, Govtech Today (April 16, 2014), http://www.govtech.com/data/state-legislatures-grappling-with-biometrics-use-in-schools.html (last visited April 27, 2021).

39 LoSardo, *supra* note 34.

40 Barker, *supra* note 29.

41 Selwyn, *supra* note 1.

42 Tucker & Vance, *supra* note 34; *see also* LoSardo, *supra* note 34.

43 Tucker & Vance, *supra* note 34.

facial recognition invariably results in "impeding crucial opportunities for human flourishing."[44]

Additional concerns relate to the way that FRT and biometric technology make private information widely available in ways that were simply not possible in recent memory, eliminating the "practical obscurity" that used to exist when information was kept written down on sheets of paper and neatly stored in filing cabinets.[45] The way that, for example, faceprints and videos are compiled, structured, and stored in databases raises serious privacy and data protection concerns, not least because FRT often requires accessing material through a multimedia database.[46] While many systems will encrypt users' data and store it on their own data centers, on secured networks, or on the devices themselves, there is a genuine concern that data can be easily searched, repurposed and shared with third parties.[47] For example, it is possible that student data is unknowingly shared with third parties and then used as a virtual tracking device.[48] There is also a concern that public institutions like universities can be forced to turn over these data on public access grounds, especially in Nordic countries where the right to access public information is very strong.[49]

Data security is an urgent matter when it comes to online examination systems, which rely on highly sensitive biometric data as well as confidential data concerning exam material.[50] The reliance

44 Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 Loy. L. Rev. 33, 50 (2020).

45 Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 B.U. L. Rev. 2179, 2247 (2020)("FRT and biometric technology nullify … practical obscurity with searchable databases. New private technology is rapidly eliminating anonymity even further.").

46 Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 616–23 (2019).

47 Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 Stan. Tech. L. Rev. 1, 24–34 (2020).

48 LoSardo, *supra* note 34.

49 Rowe, *supra* note 47.

50 Abdul Wahid, Yasushi Sengoku & Masahiro Mambo, *Toward Constructing a Secure Online Examination System,* IMCOM '15: Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication (2015).

on public networks amplifies security concerns.[51] Biometric data can be the target of hacking or identity theft schemes.[52] When breaches occur in databases that contain large amounts of biometric data, the potential intrusion into the life of the individual is massive since it is extremely difficult to alter physiological characteristics.[53] Unlike a password or social security number which can be changed and replaced after a breach, there is almost no way to replace or remedy a breach involving biometric data.[54] It may be the case that stolen facial data can be used by a person with malicious intent to impersonate an individual.[55] Alarmingly, there have been notorious examples of breaches of large-scale biometric databases, for example, the fingerprint database maintained by the United States Office of Personnel Management.[56] Last year, there was also a data breach last that affected more than 440,000 individuals using the exam proctoring program ProctorU.[57]

Finally, it is important to mention concerns about the accuracy of proctoring systems that rely on the collection of biometric data. Unlike DNA or fingerprints, a person's face changes over time, and incorrect results can arise from the use of FRT: if a person gets a

51 *Id.*

52 Wright, *supra* note 46.

53 Wright, *supra* note 46.

54 Elizabeth McClellan, *Facial Recognition Technology: Balancing the Benefits and Concerns*, 15 J. Bus. & Tech. L. 363, 371–76 (2020); Fiona Q. Nguyen, *The Standard for Biometric Data Protection*, 7 J.L. & Cyber Warfare 61, 84 (2018); *see also*, Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. Rev. 349, 355–56 (2019) (explaining, "The value of biometric data lies in the data's unique and unchangeable nature, which provides much greater security than easily-hacked passwords.").

55 Wright, *supra* note 46; Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737, 757–58 (2018)(explaining,"Biometric data such as fingerprints or eye scans, health information, and genetic data cannot be exchanged. A criminal may obtain a victim's personal data and use it months or years later; the data will still be useful for committing fraud.").

56 Wright, *supra* note 46.

57 Brandon Paykamian, *Anti-Cheating Software Drawing Criticism at Universities*, Government Technology (April 09, 2021), http://www.govtech.com/education/higher-ed/anti-cheating-software-drawing-criticism-at-universities.html (last accessed April 27, 2021).

new hairstyle, grows some facial hair or gains some weight, then the technology may misidentify them.[58] In other words, false positives can arise when an individual makes even minor aesthetic changes.[59]

Non-discrimination

There is a substantial body of research that demonstrates that the use of FRT technologies threatens marginalized communities.[60] 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.[61] This, of course, raises concerns that women or students of color will disproportionately and unfairly bear the consequences of these technologies.[62] Other groups at risk for discrimination by proctoring systems include: students with accessibility needs; students with learning disabilities, neurodivergence, and anxiety; low-income and rural students; and transgender students.[63]

58 Rowe, *supra* note 47; *see further*, Umar Toseeb, David R. T. Keeble & Eleanor J. Bryant, *The Significance of Hair for Face Recognition*, 7 PLoS ONE 1 (March 26, 2012), http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0034144 (last accessed April 27, 2021).

59 Marcus Smith, Monique Mann & Gregor Urbas, Biometrics, Crime & Security 64 (2018).

60 *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); *see also* 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 (Apr. 21, 2021) (hereinafter "AI Regulation").

61 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.*

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

63 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).

Bias can arise both because of technical and social aspects. 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.[64] Selection bias is also an issue. For example, an FRT algorithm worked better on white people than on people of color because the images used for training the algorithm were collected by white developers.[65]

An additional problem is that AI is often seen as neutral and not subject to the biases of human beings.[66] Here, it is possible for an algorithm to be highly accurate yet be biased from a social point of view.[67] To put it differently, societal biases that exist in society can be reproduced in an algorithm.[68] From an ethical and legal point of view, it can be argued that AI should not just be "bias preserving" but also capable of improving the status quo.[69]

Current laws and regulations in Europe

This section will briefly explore existing and emerging laws that regulate the use of FRT in HE. As it currently stands, the legislative landscape in the EU associated with FRT in the HE context is highly complex and constantly evolving. Legal and ethical obligations are reflected in a number of binding legal instruments as well as in soft law and proposed legislation. There is no direct specific legal regime applicable to biometric data, other than the General Data Protection Regulation (GDPR). That said, there is a highly

64 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).

65 *Algorithms: Please Mind the Bias!* Institut Montaigne (March 2020), http://www.institutmontaigne.org/ressources/pdfs/publications/algorithms-please-mind-bias.pdf.

66 Bala, *supra* note 62.

67 Institut Montaigne, *supra* note 65.

68 Institut Montaigne, *supra* note 65.

69 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.

developed human-rights framework as well as an emerging regime which will govern high-risk AI like the use of FRT in the higher-education context.

Legal framework governing AI

Since the EU's working group on legal questions related to the development of AI and robotics was launched in 2015[70], the regulation of AI has become a hotly debated policy and academic subject. There have been intense discussions about whether AI needs specific regulation and, if so, what this regulation should look like. For example, some have argued that existing legal frameworks are sufficient to safeguard individuals from potential adverse effects of AI systems while others have contended that regulation is necessary but that it should take place at the Member State level instead of at the regional or international level.

A first step towards the regulation of AI occurred in April 2019 when the High-Level Expert Group on Artificial Intelligence (AI HLEG)[71] released its Ethics Guidelines on AI, setting forth four ethical imperatives in the context of AI: respect for human autonomy, prevention of harm, fairness and explicability.[72] From those four principles, seven principles to design trustworthy AI based on fundamental rights are derived which include: (1) human agency and oversight; (2) robustness and safety; (3) privacy and data governance; (4) transparency; (5) diversity, non-discrimination, and fairness; (6) societal and environmental well-being; and (7) accountability. Basically, in the guidelines the AI HLEG translated broad, normative assumptions and discussions into specific requirements which were reflected in soft law.

70 *See e.g.* Committee on Legal Affairs Working Group on Legal Questions related to the Development of Robotics and Artificial Intelligence, *Meeting of 22 October 2015 (Minutes)*, European Parliament, http://www.europarl.europa.eu/cmsdata/94927/Minutes_WG_Robotics_Oct.pdf.

71 The High-Level Expert Group on Artificial Intelligence (AI HLEG) was established as the flagship group for the European AI Alliance and tasked to provide guidelines on AI Ethics as well as AI policy and investment recommendations; for more *see* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, OJ 237 C 25.4.2018.

72 Nathalie A. Smuha, *The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence*, Computer L. Rev. Int'l 97 (2019).

The next important step towards regulation occurred when the Commission released its White Paper on Artificial Intelligence. While the White Paper recognized the requirements set forth by the AI HLEG in its Ethics Guidelines, it expressly pointed to the need for regulation beyond soft law and provided guidance on how legislation should be developed to ensure legal certainty. More precisely, it proposed a risk-based regulation for AI with sector- and application-specific risk assessments and requirements as opposed to blanket requirements or bans.[73]

The White Paper explained that AI risks include risks for fundamental rights, including personal data and privacy protection and non-discrimination as well as risks for safety and the effective functioning of the liability regime.[74] It further stated that AI should be considered high risk when it is applied in a critical sector, and it is used in a manner in which significant risks are likely to arise.[75] Biometric identification was explicitly recognized as a high-risk application that should only be used "where such use is duly justified, proportionate and subject to adequate safeguards."[76]

In April 2021, the Commission put forward a legislative proposal maintaining the risk-based approach adopted in the White Paper, which broadly groups AI practices into four groups: unacceptable, high risk, limited risk and minimal risk. FRT is a central concern of the proposed AI regulation as it expressly prohibits the use of "real time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement unless certain limited exceptions apply.[77] Outside of being used for law enforcement

73 *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. (For high-risk AI applications the White Paper identifies six key requirements that could be included in upcoming AI legislation: (1) training data, (2) data and record-keeping, (3) information provision, (4) robustness and accuracy, (5) human oversight, and (6) specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification.).

74 *Id.*

75 *Id.*

76 *Id.* at 65, stating, "The gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights").

77 AI Regulation, *supra* note 60, Article 5(1)(d) and Explanatory Memorandum at 3.

purposes in publicly accessible spaces, Recital 33 and Annex III(1)(a) explain that "real-time" and "post" remote biometric identification systems should be classified as high-risk.[78] Consistent with the GDPR's definition, discussed in detail below, the regulation makes a sharp distinction between identification and verification techniques, placing stricter rules on the former[79], and essentially placing AI used for verification purposes outside the scope of high-risk AI all together.

Referring explicitly to the educational sector, Annex III states that AI systems used for "assessing students in educational training" constitutes high-risk AI.[80] 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."[81] Recital (35) clarifies that the reason for this is that they "may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood."[82] It is 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.

Where an AI system is deemed to be high-risk, then providers will have an extensive range of obligations.[83] Obligations for providers of AI systems include the adoption of risk management systems[84], data governance,[85] technical documentation[86], record-keep-

78 *Id.,* Recital 33.

79 *Id.*, Article 3(33); *see further* Recital 7 stating the definition in the AI Regulation should be interpreted consistently with Article 4(4) of the GDPR.

80 *Id.*, Annex III(3)(b).

81 *Id.,* Annex III(3)(a).

82 *Id.*, Recital 35.

83 See *Id.*, Chapter II.

84 *Id.*, Article 9.

85 *Id.*, Article 10.

86 *Id.*, Article 11.

ing[87], transparency[88], human oversight[89] and accuracy of outputs and security.[90] Additionally, there are a number of express obligations for providers of high-risk AI systems like putting in place a quality management system.[91] 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.[92] Regulators will be able to fine non-compliant actors up to €30m, or 6% of their worldwide turnover.[93]

Legal framework for privacy and data protection

Article 8 of the European Charter of Human Rights (ECHR) sets forth a right to respect for private life. It covers four distinct areas: private life, family life, home, and correspondence.[94] Importantly, Article 8 imposes two types of obligations on the State. First, Article 8 obliges States to avoid interference with an individual's private life, family life, home and correspondence.[95] Second, there is a positive obligation to actively secure respect for private and family life, home and correspondence, between the state and the individual.[96] The positive obligation under Article 8 is derived from Article 1 ECHR,

87 *Id.*, Article 12.

88 *Id.*, Article 13.

89 *Id.*, Article 14.

90 *Id.*, Article 15.

91 *Id.*, Article 17.

92 *Id.*, Article 29(4).

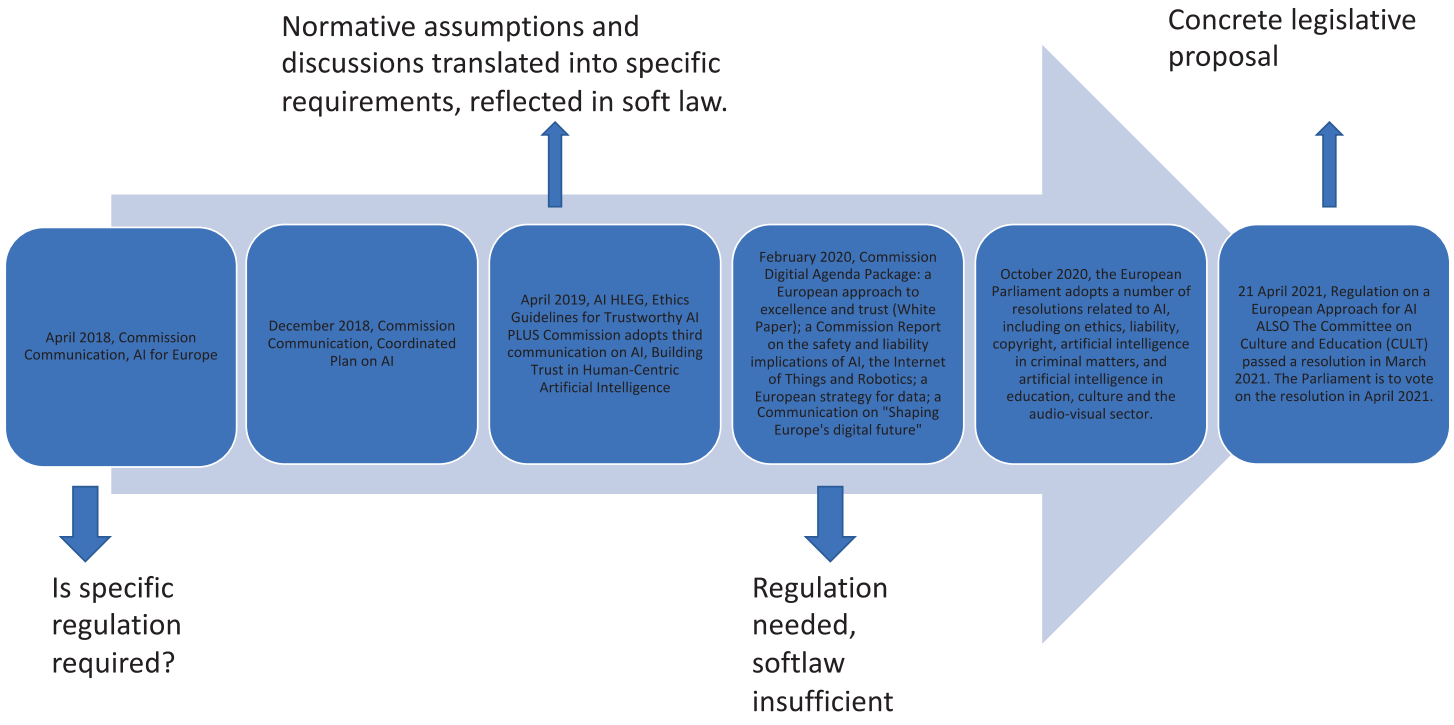
93 *Id.*, Article 71.

94 Ivana Roagna, *Protecting the Right to Respect For Private and Family Life Under the European Convention on Human Rights,* Council of Europe (2012), https://rm.coe.int/16806f1554.

95 *See e.g.* Leander v. Sweden, no. 9248/81, European Commission on Human Rights decision of 3 March 1987.

96 *See e.g.* I v. Finland, 2008 Eur. Ct. H.R., http://hudoc.echr.coe.int/eng?i=001-87510.

A timeline for the EU's AI Strategy



which requires states to secure Convention rights to everyone within their jurisdiction.[97]

In 2000, the EU proclaimed the Charter of Fundamental Rights of the European Union ("Charter") which became legally binding as EU primary law, pursuant to Article 6(1) of the TEU, when the Lisbon Treaty came into force on 1 December 2009.[98] Article 7 of the Charter reiterates the definition of privacy given by the ECHR.[99] Unlike the ECHR, however, the EU Charter defines the right to data protection as an autonomous right, instead of a simple dimension of the right to privacy.[100] It is important to emphasize that Article 8 not only explicitly mentions a right to data protection, but also refers to key data protection principles. It is further worth highlighting that the Charter requires that an independent authority will ensure compliance with the principles set forth in Article 8.

In 2016, the GDPR was adopted, modernizing EU data protection legislation and making it suitable for protecting fundamental rights in the digital age. The GDPR applies to partly or fully automatic AI systems that process personal data. It contains several core principles for the collection and processing of personal data such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security) and accountability. It also affords the data subject numerous rights over their own personal data, such as the right to be informed of the collection and use of their personal data, the right to access their personal data and the right to have inaccurate or incomplete information corrected. As discussed in detail below, personal data must be processed lawfully in accordance with one of the six lawful grounds specified Article 6.[101]

97 Council of Europe (1952). European Convention for the Protection of Human Rights and Fundamental Freedoms, Europ.T.S. No. 5; 213 U.N.T.S. 221 (November 4, 1950), Article 1.

98 *See* consolidated versions of the European Communities (2012), Treaty on European Union, OJ 2012 C 326; and of European Communities (2012), TFEU, OJ 2012 C 326.

99 European Charter of Fundamental Rights, 2000 O.J. (C364), 18 December 2000, Article 7.

100 *Id.*, Article 8.

101 For all six legal bases see further European Union, Council Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

Importantly, from the perspective of the use of proctoring in HE, Article 22 of the GDPR states that a data subject should not be subject to a decision based *solely* on automated processing, including profiling, which produces *legal effects* concerning him or her or *similarly significantly* affects him or her.[102] If an automated decision is likely to have a significant impact on the life of an individual, then special protection is necessary to avoid negative consequences. Automated decision-making includes profiling, which is defined in Article 4(4).[103]

Under the GDPR, a data controller has the responsibility to "implement appropriate technical and organizational measures", taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."[104] Article 32 explicitly refers to pseudonymizing and encrypting personal data as appropriate technical measures.[105] A legal definition of "pseudonymization" is set forth in the GDPR[106], which basically explains that pseudonymizing data means replacing the attributes in personal data – which make it possible to identify the data subject – with a pseudonym, and ensuring that the additional data necessary for reidentification are kept safely inaccessible for the users of "pseudonymized data."[107] This process can be juxtaposed with anonymization which requires all links to identifying the data subject to be broken.[108] Regularly testing

---

natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119/1 [*hereinafter* General Data Protection Regulation], Art. 6.

102 *Id.* Article 22.

103 *Id.* Article 4(4).

104 *Id.* Article 32.

105 *Id.* Article 32(1).

106 *Id.* Article 4(5).

107 *Handbook on European Data Protection Law*, European Union Agency for Fundamental Rights 131, (2018); Waltraut Kotschy & Ludwig Boltzmann, *The New General Data Protection Regulation—Is There Sufficient Pay-Off for Taking the Trouble to Anonymize or Pseudonymize Data?* (November 2016), https://fpf.org/wp-content/uploads/2016/11/Kotschy-paper-on-pseudonymisation.pdf.

108 Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymization Techniques* (2014) WP 216, 3, 10 (http://www.pdpjournals.com/docs/88197.pdf (stating

and evaluating the effectiveness of the technical and organizational measures in place is also recommended.[109]

Legal framework for non-discrimination laws

While there is currently no AI specific equality legislation within European law, the EU has a well-developed *acquis communautaire*[110] of equality law. The EU has approved two major equality Directives[111] as well as adopted the Charter which includes anti-discrimination provisions set out in Chapter III. Furthermore, the Court of Justice (CJEU) has stated that equal treatment is a general or fundamental principle on which the EU is founded.[112] This body of law also draws on the jurisprudence of the European Court of Human Rights based on Article 14 of the ECHR.[113] Furthermore, by making a request for transparency pursuant to Article 15 of the GDPR, individuals may be able to identify that discrimination is occurring to the extent that a data controller must explain the categories of personal data being processed and the existence of automated decision-making, including profiling.

---

pseudonymization is "not a method of anonymization" but "merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure.").

109 GDPR, Article 32(1)

110 *Glossary of Summaries*, EUR-Lex, http://eur-lex.europa.eu/summary/glossary.html (last accessed April 27, 2021) (defining "acquis" as the "body of common rights and obligations that are binding on all EU countries, as EU Members.").

111 Council Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000, and Council Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation, OJ L 303 2.12.2000. Council Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), OJ L 204, 26.7.2006.

112 Case C-144/04, *Werner Mangold v. Rüdiger Helm* [2005] ECR I-09981; Case C-555/07, *Seda Kücükdeveci v. Swedex GmbH & Co. KG* [2010] ECR I-00365 at 20-22; and Case C-441/14 *Dansk Industri* (*DI*), *acting on behalf of Ajos A*/*S v Estate of Karsten Eigil Rasmussen,* OJ C 211 13.6.2016.

113 Robin Allen & Dee Masters, *Artificial Intelligence: The Right to Protection From Discrimination Caused by Algorithms, Machine Learning and Automated Decision-Making*, ERA Forum 585–598 (2020).

Legality case study

Personal data or sensitive data?

When personal data is gathered by a proctoring system it is subject to the GDPR, which defines personal data as "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his 5 physical, physiological, mental, economic, cultural or social identity."[114] To put it differently, if any information can be related to an identified or identifiable natural person then it is "personal." This is a broad definition and biometric data, like raw images of students, would clearly fall into this category, as they are inherently linked to a specific individual.

The EU also makes a distinction between personal data and sensitive personal data with the later receiving a higher level of protection under EU data protection. Sensitive data is information that relates to health, sex life, racial or ethnic origin, political opinions, religious or philosophical beliefs, and even trade-union membership. Under the GDPR, biometric data is explicitly covered under "special categories of personal data" and consequently, the processing of this data for the purpose of uniquely identifying a natural person is strictly forbidden, at least as a general principle.[115] That said, there are number of enumerated exceptions including, for example, obtaining explicit consent, specified public interest considerations, and certain exemptions in the fields of employment and social protection law.

The GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person which allow or confirm the unique identification of that natural person."[116] The reason for the general prohibition against processing biometric data is because biometrics, by their very nature, are "unlike other unique identifiers" since they are "biologically unique to the individual" and

114 GDPR, *supra* note 101, Article 4(1).

115 *Id.* Article 9(1).

116 *Id.* Article 4(14).

cannot be changed.[117] This means, as described above, if the data is compromised the risks of harm are very serious.

The classification of data used by proctoring exams as merely personal and subject to one of the Article 6 grounds for lawful processing or as sensitive and subject to one the Article 9(2) exceptions is of critical relevance. When understanding whether data falls under the definition of biometric data in the GDPR, it is first important to consider the source of biometric data. Here, it is important to understand that the GDPR protects two separate categories of biometric data.[118] First, it protects information connected to a person's physical or physiological trait like iris features or face patterns.[119] The second category concerns any behavioral information that can be used to uniquely identify someone, like the hand with which a person holds their phone.[120] Monajemi explains that it is unclear how the GDPR will regulate measures of a person's physical being based upon behavioral characteristics as "it has no nexus to the 'normal' definition of biometrics as it relates to body information."[121]

Second, in order to constitute sensitive data, the processing "needs to be carried out through specific technical means and measurements."[122] Recital 51 explains that the processing of digital photographs which may contain raw data relating to the physical characteristics of a person does not constitute biometric data unless it is "processed through a specific technical means allowing the unique identification or authentication of a natural person."[123] In other words, the image data might be used to create an individ-

117 Fiona Q. Nguyen, *The Standard for Biometric Data Protection*, 7 J.L. & Cyber Warfare 61, 84 (2018), citing 740 Ill. Comp. Stat. Ann. 14/5(c) (2008).

118 GDPR, *supra* note 101, Article 4(13).

119 *Id.* Article 4(1).

120 *Id.* Article 4(1); Michael Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with A New World Order of Information*, 25 U. Miami Int'l & Comp. L. Rev. 371, 383 (2018).

121 *Id.*

122 GDPR, *supra* note 101, Article 4(14).

123 GDPR, *supra* note 101, Recital 51 (stating, "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person…").

ual digital template or profile, which in turn is used for automated image matching and identification.[124] The key to a finding of biometric data is the existence of biometric processing, and not just the existence of a database with facial images or fingerprints.[125] Kindt explains: "Facial images only become biometric data … if they are used for biometric comparison, and more precisely, if they are the result of 'specific technical processing'."[126]

Third, the purpose of the processing must be identified insofar as the GDPR distinguishes between processing biometric data for identification purposes and verification purposes. Here, Article 9(1) GDPR only includes "biometric data for the purpose of uniquely *identifying* a natural person." 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 prohibition provided for in Article 9(1) GDPR.

Biometric identification can be described as "using an individual's biometric identifier to match the identifier with that specific individual within a database of biometric identifiers compiled from multiple individuals."[127] Essentially, it seeks to answer the question: who is this student? In the education context, this process would permit the unique identification of a student from a database containing data on all students in a given population, confirming his or

124 *What is Special Category Data?*, Information Commissioner's Office, http://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4 (last accessed April 27, 2021).

125 Els J. Kindt, *Having Yes, Using No? About the New Legal Regime for Biometric Data*, 34 Computer L. & Security Rev. 523 (2018).

126 *Id.* (providing the example, "Photographs, for example of children at schools, if collected and disclosed on websites of the school, or registered in an internal database of the school, are according to the new definition in the GDPR not biometric data as long as they are not processed by a biometric system.").

127 Kelly A. Wong, *The Face-Id Revolution: The Balance Between Pro-Market and Pro-Consumer Biometric Privacy Regulation*, 20 J. High Tech. L. 229, 232 (2020); *see also* J. Valera, J. Valera and Y. Gelogo, *A Review on Facial Recognition for Online Learning Authentication*, 8th International Conference on Bio-Science and Bio-Technology 16-19 (2015) ("…user identification determines the person based on exhaustive verification where the actual biometric features is compared to all registered references and determined of which has the greatest similarity.").

her identity (positive identification).[128] It might also identify that a student's information is not present in a certain database, preventing him or her from having multiple identities in the system (negative identification).[129] Sometimes this approach is referred to as a one-to-n matching process, where "n" is the total number of biometrics in the database.[130] Ankerman explains: "Both positive and negative identification serve the same goal: to authenticate each individual based on a single, non-transferable identity."[131] Importantly from a data-protection standpoint, for identification to function, it is always necessary to utilize a database of stored biometric data, as compared to just the storage of a single biometric characteristic.[132]

On the other hand, in biometric verification, an individual's biometric trait is scanned and compared to the existing template that has been formed for that specific individual to verify that the individual is who he or she claims to be.[133] Essentially, it seeks to answer the question: "Is the student who they claim to be?" Sometimes this approach is referred to as a one-to-one matching process.[134] With biometric verification, it is only necessary to store a single biometric characteristic.[135] This data may be stored in a database or stored locally, on an identification card, for example.[136] The Council of Europe has explained that biometric verification contains less risk

128 Stefan P. Schropp, *Biometric Data Collection and Rfid Tracking in Schools: A Reasoned Approach to Reasonable Expectations of Privacy*, 94 N.C. L. Rev. 1068, 1071–72 (2016); James Wayman et al., Biometric Systems 5 (2005).

129 Alexa N. Acquista, *Biometrics Takes Off – Fight Between Privacy and Aviation Security Wages On*, 85 J. Air L. & Com. 475, 480 (2020).; Wayman, *id.*

130 Kindt, *supra* note 125; Margaret Hu, *Biometric Id Cybersurveillance*, 88 Ind. L.J. 1475, 1491 (2013).

131 Chantelle D. Ankerman, *A Closer Look: Iris Recognition, Forensics, and the Future of Privacy*, 49 Conn. L. Rev. 1357, 1379 (2017).

132 Acquista, *supra* note 129.

133 Clifford S. Fishman & Anne T. McKenna, Biometrics: A General Overview of Biometric Technology in Wiretapping and Eavesdropping (2019).

134 Kindt, *supra* note 125 ("The processing for verification purposes is a one-to-one (1:1) comparison and is used to verify and to confirm by biometric comparison whether an individual is the same personas the one from whom the biometric data originates.").

135 Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis 18, 38-39 (2013).

136 *Id.*

than biometric identification because the utilization of a database is not required.[137]

In the context of proctoring exams, it may be possible that emotional data like the facial expressions of students (without the retention of facial image characteristics) would constitute mere personal data if it is insufficiently distinctive to allow or confirm identification of the student.[138] Furthermore, behavioral data that is insufficiently distinctive to allow or confirm identification would also fall in this category.[139] Personal data that relates to a student's physical, physiological or behavioral characteristics, which allows for unique identification or confirmation of an identity, but are not used in a biometric comparison, also fall within the scope of personal data.[140] Furthermore, biometric data like iris features and face patterns captured by a proctoring system will not constitute biometric data if they are used in biometric verification systems whereby only a one-to-one comparison is made based on biometric data. However, using biometric data in a proctoring system that involves identification in a one-to-many matching process is in principle forbidden, unless exempted.

Finally, the intersectionality that exists between facial image data and special categories of data must be highlighted. That is, data collected by proctoring systems, particularly, facial image data, may reveal information about racial or ethnic origin, religious orientation, health related information and even sexual orientation. This information may be shared, consciously or unconsciously. The legal significance of this that certain data collected by these systems may nevertheless be classified as sensitive data even through it falls outside the technical definition of "biometric data" in the GDPR.[141]

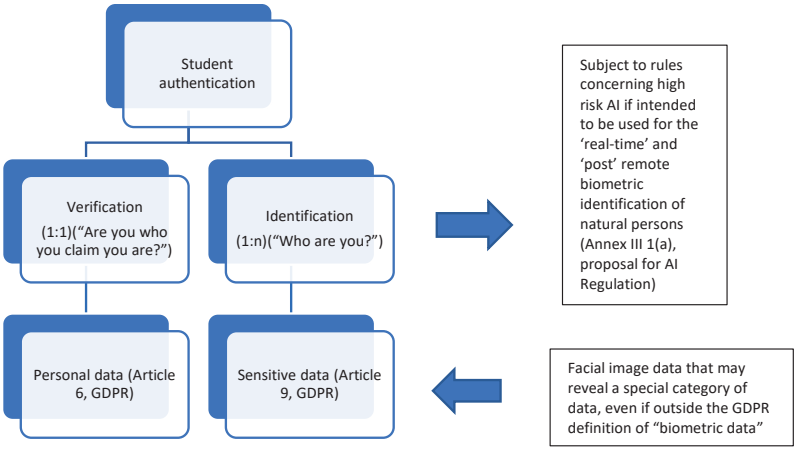
137 *See Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*, Council of Europe (2005), and the updated Progress Report of 2013, T-PD(2013)06, https://rm.coe.int/progress-report-on-the-application-of-the-principlesof-convention-108/1680744d81 (last accessed April 27, 2021); *see also* Kindt, *supra* note 125 (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.")

138 Kindt, *supra* note 125.

139 Kindt, *supra* note 125.

140 Kindt, *supra* note 125.

141 Kindt, *supra* note 125.



Lawful grounds

Article 6, personal data

As explained above, processing personal data requires a lawful basis. The lawful bases for processing personal data in the context of online proctoring are namely: (1) consent, (2) the need to process personal data in order to perform a task that is in the public interest or under public authority, and (3) the need to process personal data in the context of a legitimate interest.

Consent

Relying on consent as a valid ground to process personal data in connection with online proctoring is generally not possible because of the power imbalances and the hierarchical relationship that exists between the students and the teachers representing the university.[142] Students might feel coerced to give consent because they fear they will get a bad grade. This is particularly true when they are under exam pressure, exacerbated by a pandemic as well as the surveillance capabilities of the exam software itself. Furthermore, in a lock-down situation, it is not clear that students can freely offer consent to

142 *See* GDPR, *supra* note 101, Article 4(11)(defining consent).

the extent that no practical alternatives may be available for taking tests.[143]

While the requirements for consent to be freely given, informed, specific and unambiguous are difficult to meet in the university context, it may be used in certain, limited situations, for example, for students who wish to take exams from abroad.[144] It is also possible that the consent grounds to process personal data takes on a bigger role when alternative legal grounds like legitimate interest and public interest, discussed more below, are not strictly required by the exigencies of the pandemic situation. In the post-pandemic context, for example, the consent grounds might be used for students who have indicated that they prefer to take their exams at home, because of noise that exists in an exam hall or because they want to skip the commute to the university.[145] If consent is relied upon then it is important to remember that students may revoke their consent at any time, and the university has an obligation to keep a record of the consent.

Legitimate interest

When considering the interests of online proctoring, it is first required to consider the legitimate interest of the institution. Second, the extent to which the processing is necessary to defend the legitimate interest must be analyzed with references to the concepts of proportionality and subsidiarity. Basically, a balance between the institutions interests and the students' rights to privacy and data protection must be struck which must be well documented.

According to the GDPR, the legitimate interest basis may not apply to processing carried out by public authorities as part of their tasks.[146] As such, an institution that classifies itself as a government organization does not have the option to use legitimate interest as a basis. That said, in the context of the coronavirus crisis, VU Amster-

143 *Student Proctoring Software Gets First Test Under EU Privacy Law*, Bloomberg Law (July 29, 2020), http://news.bloomberglaw.com/tech-and-telecom-law/student-proctoring-software-gets-first-test-under-eu-privacy-law (last accessed April 27, 2021).

144 *Whitepaper Online Proctoring: Questions and Answers At Remote Surveillance*, SURF (April 2020), http://www.surf.nl/files/2020-06/surf-whitepaper-online-proctoring_en_mei-2020.pdf.

145 *Id.*

146 GDPR, *supra* note 101, Article 6 ("Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.").

dam first argued that it is not a government agency due to private funding, and second, asserted that it had a legitimate interest to process personal data for online proctoring.[147] Furthermore, even some clearly public universities have argued that a public authority performing activities that are not part of a public task may do so on the basis of legitimate interests.[148]

Legitimate interests include things like the need "to organize exams and avoid postponement of exams as much as possible, as this leads to study delay for students, accumulation of work for teachers and a shortage of spaces for taking exams at a later stage" as well as needed to fulfil the requirements of distance education by securely organizing remote exams.[149] However, online proctoring will likely be found to be disproportionate after universities open and exams can be held in halls again. This is because a less privacy intrusive alternative to online proctoring would exist.[150]

Task of public interest

A university may invoke as a legal basis the argument that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.[151] The GDPR requires that the underlying task, function or power of the public body must have a clear basis in law. The "law" in question, however, does not have be a legislative act adopted by

147 *Guide to Reference Framework For Alternative Forms of Assessment*, Vrije University Amsterdam (March 26, 2020)("B. The use of online surveillance by means of video images VU Amsterdam can use online surveillance without the student's permission, provided that: 1. a case can be made that remote monitoring of the assessment in question is needed to: check the identity of the individual taking the assessment; establish that no academic misconduct has been committed during the assessment; and to establish that the assessment was completed within the allotted time frame… In such cases, VU Amsterdam can be said to have a necessary, legitimate interest that outweighs the rights and freedoms of those involved (Art. 6.1 f GDPR).")

148 Rechtbank Amsterdam 11 June 2020 rolnr. C/13/684665; *Court Decision on Remote Proctoring in the Netherlands*, Association of Test Publishers, https://www.testpublishers.org/amsterdam-court-case (last accessed April 27, 2021).

149 Meike Davids, *Data Protection Impact Assessment (DPIA),* U. of Twente (December 17, 2020), http://www.utwente.nl/remote-exams/students/proctoring/dpia-proctoring.pdf.

150 SURF, *supra* note 144.

151 GDPR, *supra* note 101, Article 6(1)(f).

parliament but can, for example, include a university charter.[152] Therefore, things like advancing education, learning and research to be a public task can be considered part of the "public tasks" of a university. Here, there can be little doubt that universities have legal obligations to administer exams, award degrees and make efforts to prevent fraud/ensure the quality of the education in doing so.[153]

The principles of proportionality and subsidiarity are key issues when it comes to online proctoring exams. First, the processing of personal data must be necessary and in proportion to the ends (proportionality). Second, if the university could reasonably perform its tasks or exercise its powers in a less intrusive way, this lawful basis does not apply. As discussed above, online proctoring has the potential to intrude deeply into the private lives of students through, for example, AI that monitors the student's computer, home, and facial images. The essential question becomes where to draw the line, and whether the use of FRT in the educational context in order to ensure academic integrity and to verify the student's identity are necessary and proportionate.

In a pre-Covid 19 case, the Danish Data Protection Agency found that a high school's reliance on an online proctoring system (Examcookie), did not sufficiently explain that the processing of the collected information about all examinees had been sufficient, relevant and limited to what is necessary in relation to the purpose of detecting and preventing fraud.[154] It found that the high school, Fredericia Gymnasium, only explained that there was a need to prevent exam cheating, but that the monitoring of the students' private computers through the proctoring system intruded too deeply into the private

152 *Id.* Recital 41 (clarifying that a "legal basis" does not have to be an explicit statutory provision, as long as the application of the law is clear, precise and foreseeable.).

153 Selwyn, *supra* note 1; see for an example, Rechtbank Amsterdam, *supra* note 148 ("In this case, the public task of the UvA is regulated by, or can be traced back to, a statutory task, namely its task to provide education, to conduct exams and to issue diplomas, while maintaining the quality of that education and of the diplomas is guaranteed. This task is detailed in the WHW, and the authority to process data in the context of exams is further detailed in the OER and in the Rules and Guidelines of the Examination Board.").

154 *Fredericia Gymnasiums behandling af personoplysninger ved brug af programmet Examcookie*, Datatilsynet (May 16, 2019), https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/maj/fredericia-gymnasiums-behandling-af-personoplysninger-ved-brug-af-programmet-examcookie (last accessed April 27, 2021).

lives of the students.[155] The Danish Data Protection Agency emphasized that Fredericia Gymnasium did not account for all the personal information collected being necessary to fulfill Fredericia Gymnasium's purpose of detecting and preventing fraud.[156]

In another more recent case, however, the Danish Data Protection Agency found that the use of an online proctoring system (ProctorExam) to control cheating during exams was necessary and proportionate.[157] The Danish DPA emphasized the COVID-19 situation and the fact that the IT University (ITU) was physically closed and forced to conduct all teaching and all examinations online.[158] It also emphasized that ITU reportedly made an assessment of the need for examination supervision for different subject areas and found that in the subject in question ("Algorithms and Data Structures"), it was particularly necessary to utilize online proctoring.[159] In other words, ITU only used ProctorExam for exams where it was specifically deemed necessary. This case demonstrates that what is necessary for the performance of a public task may vary over time to the extent that a university may come to the conclusion that it is required to process video images of students in specific situations in order to carry out the public tasks laid down by their charters during a pandemic, unlike in normal times.

Article 9, Sensitive data

If data collected from a proctoring system is classified as biometric data, then it should not be processed unless one of the ten exemptions from the prohibition of processing biometric data found in Article 9(2) apply. This section will explore how these exemptions might apply in the context of proctoring exams. The first exemp-

155 *Id.*

156 *Id.*

157 *Universitets brug af tilsynsprogram ved online eksamen*, Datatilsynet (January 26, 2021), https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen (last accessed April 27, 2021).

158 *Id.*

159 *Id.* (reasoning that "the subject was a basic course where the students had to show their basic skills within the subject area. All correct answers in the exam would be identical, as there was one correct answer without explanation or elaboration, which is why, unlike other subjects, it was crucial to be able to demonstrate that the examinee did not receive help from others.").

tion concerns where the "explicit consent" of the data subject is obtained.[160] For the reasons set forth above, this exemption will, at best, have narrow application. This is particularly true in light of a 2019 decision by the Swedish Data Protection Authority, which rejected consent as a valid ground for a school in Northern Sweden to use FRT to keep track of students' attendance in school based on the relationship of dependence between students and institutions, as well as the substantial power imbalance between the different actors.[161] It is also important to note that Union or Member State law may limit the circumstances where explicit consent can be relied upon as a legal grounds to process biometric data.[162] Kindt notes: "This leaves Member States to carefully think about situations where biometric identification, based on consent, may not be desirable."[163]

Another exemption is found in Article 9(2)(g) where the processing is necessary "for reasons of substantial public interest" so long as there is a Union or Member State law which is (1) proportionate to the aim pursued, (2) respects the essence of the right to data protection and (3) provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[164] When discussing whether this ground applied in the Fredericia Gymnasium case, the Danish DPA rejected that the school had a ground for processing sensitive personal data covered by Article 9 of the GDPR.[165] However, in the ITU case, the DPA found that Article 9(1)(g) was a legal basis for processing sensitive data. The DPA emphasized that the ITU did not rely on image identification at the beginning of the examination. More specifically, it stated "The ITU does not use software-based face recognition or other technical treatment to uniquely

160 GDPR, *supra* note 101, Article 9(2)(a).

161 *Supervision Pursuant to the General Data Protection Regulation (EU) 2016/679 – Facial Recognition Used to Monitor the Attendance of Students, Ref. no. DI-2019-2221*, Swedish Data Protection Authority (August 20, 2019), http://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf.

162 GDPR, *supra* note 101, Article 9(2)(a).

163 Kindt, *supra* note 125.

164 GDPR, *supra* note 101, Article 9(2)(g).

165 Datatilsynet, *supra* note 154.

identify the examinee."[166] Instead, at random checks, staff from the ITU manually checked the identity of the examinee by holding a student card or other photo ID up to the face, which appears on the computer camera.[167] It also emphasized that the ITU "encouraged the examinees to arrange their computers in such a way as not to accidentally process sensitive information in connection with the recordings of video, audio and screen."[168]

If a proctoring system involves the processing of a special category of personal data on a large scale, then a DPIA will be required.[169] Prior consultation with the supervisory authority will also be required in the event that the DPIA indicates that the processing would result in a high risk in the absence of or which the controller cannot mitigate by appropriate measures 'in terms of available technology and costs of implementation'.[170] Consultation with the supervisory authority is also required if national law requires prior authorization for a task carried out in the public interest.[171]

Relevant factors for determining whether the use of AI-based proctoring tools are necessary and proportionate to achieving their aims

The question of which legal basis is appropriate in a specific situation when utilizing online proctoring will always depend on the circumstances, the concrete purpose for the use of the tool, and the type of data being processed. It is of utmost importance that the educational institution is able to justify its choice of a particular legal basis. In addition, the processing of personal data must be necessary and proportionate to achieve the underlying purpose.

166 Datatilsynet, *supra* note 157.

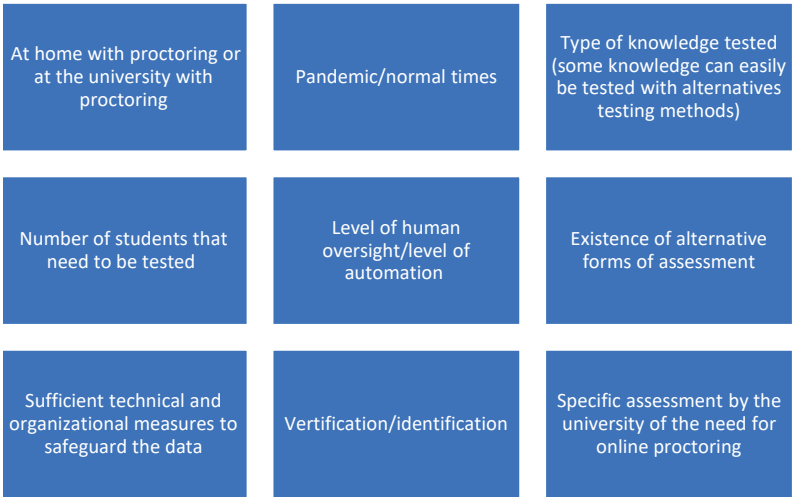
167 *Id.*

168 *Id.*

169 GDPR, *supra* note 101, Article 35.

170 *Id.* Article 36.

171 *Id.* Article 36(5).



Conclusion

In light of the potential harms posed by online proctoring exams, one potential response is to reject them completely. Several prominent groups and privacy experts have made it clear that educational institutions "must proceed with great caution when considering the implementation of FRT, especially to provide safeguards necessary to protect students against its many projected, yet ultimately unknown harms."[172] For example, Hartzog and Selinger call for a wholesale ban on facial recognition, explaining that "when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering."[173] Likewise, Barrett calls for ban of FRT in the school context because of the "vast and far-reaching" harms.[174] Complete bans already exist in some American schools.[175]

172 LoSardo, *supra* note 34.

173 Woodrow Hartzeg & Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (August 2, 2018), http://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 (last accessed April 27, 2021).

174 Lindsey Barrett, *Ban Facial Recognition Technologies for Children-and for Everyone Else*, 26 B.U. J. Sci. & Tech. L. 223, 275–83 (2020).

175 *See* Blake Montgomery, *Facial Recognition Bans: Coming Soon to a City Near You*,

In the EU, many are pushing for a multi-year moratorium on FRT so that the technology's impact can be studied.[176] While it appears that this idea was at least explored in earlier drafts of the AI White Paper[177], no references to a ban or a moratorium were reflected in the final published document nor have any been included in the AI Regulation. Instead, the EU appears to be adopting a risk-based approach regulation to these types of technologies.

Ultimately, future scenarios of online proctoring in a post pandemic world remain unclear. Will it be immediately cut by the institutions themselves in order to implement a clear and consistent policy, in favor of the protection of students' human rights? Will it fade out as regulators make clear that legal grounds to process personal data in these systems do not exist? Will it be continued to be used because of increased demand for digital education, as well as for its potential to cut costs like the maintenance of physical computers, physical exam space and live proctors?

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).

176 *See* Janosch Delcker, *Activists Urge EU to Ban Live Facial Recognition in Public Spaces*, Politico (November 12, 2020), http://www.politico.eu/article/activists-urge-eu-to-ban-live-facial-recognition-in-public-spaces/ (last accessed April 27, 2021).

177 *Facial Recognition: EU Considers Ban of Up to Five Years*, BBC News (January 17, 2020), http://www.bbc.com/news/technology-51148501 (last accessed April 27, 2021).