From data subjects to data suspects: challenging e-proctoring systems as a university practice

by **Alexandra Giannopoulou, Rossana Ducato, Chiara Angiolini, and Giulia Schneider ***

Abstract: E-proctoring is a set of software and tools to monitor students' behaviour during online examinations. Many universities have implemented this type of invigilation in response to the lockdowns during the pandemic to guarantee the validity and the integrity of exams. However, the intrusiveness of such technology into the students' personal environment along with major accuracy problems (e.g., in authenticating black students) has attracted the scrutiny of various European data protection authorities and, more recently, equality bodies.

In this paper, we critically approach the European normative framework available in countering the risks and situations of harms generated by e-proctoring through the lenses of data protection and anti-discrimination law. This work, in particular, is one of the first to systematise and analyse the corpus of online proctoring-related decisions that have emerged in the EU over the past three years.

After an overview of the technical aspects of such technology and an outline of the legal issues debated in the literature, the paper will reconstruct and discuss the convergences and divergences in how courts and independent authorities have assessed the lawfulness of online invigilation tools. In our analysis, we observe that such instruments were evaluated differently depending on the concrete features implemented. However, with some notable exceptions, the General Data Protection Regulation and the anti-discrimination framework have largely proven helpful to combat the most intrusive forms of e-proctoring deployment or to mitigate their risks. Nevertheless, to ensure a safer and fairer educational environment, we conclude that a few crucial issues—including the effectiveness of the collective enforcement of rights, discriminatory effects for people not covered by a protected ground, and the governance of edTech within the university—should be further taken into account.

Keywords: e-proctoring, data protection, GDPR, anti-discrimination, pandemic

© 2023 Alexandra Giannopoulou, Rossana Ducato, Chiara Angiolini, and Giulia Schneider

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8.

Recommended citation: Alexandra Giannopoulou, Rossana Ducato, Chiara Angiolini, and Giulia Schneider, From data subjects to data suspects: challenging e-proctoring systems as a university practice, 14 (2023) JIPITEC 278 para 1.

A. Introduction

1 Lately, teaching has had to adapt to fundamental and urgent shifts. After more than two years into a global pandemic and several COVID-19 variants, life is progressively returning to normal. The majority of governments have lifted several, if not all, restrictions. This trend is valid for academic life as well. With Higher Education Institutions (HEIs) shut down for a large part of 2020 and 2021 and engaged with dual delivery and gradual return to in-person teaching in 2022, the academic year 2022/2023 is seeing a general resumption of on-campus activities. However, it is unlikely that things will return to exactly as they were before the COVID-19 pandemic. Firstly, as public health experts warn, COVID-19 is still "a global health threat".[1] Hence, we might

* Alexandra Giannopoulou: Postdoctoral researcher, Institute for Information Law (IViR), University of Amsterdam (a.giannopoulou@uva.nl). Rossana Ducato: Senior Lecturer in IT Law and Regulation, School of Law, University of Aberdeen; Lecturer at UCLouvain (rossana.ducato@abdn.ac.uk). Chiara Angiolini: Research Fellow, Law Department, University of Siena (chiara.angiolini@unisi.it). Giulia Schneider: Research Fellow, Department of Banking Sciences, Catholic University of Milan (giulia.

need to remain flexible and be prepared to face future emergencies.[2] Secondly, education has seen a paradigmatic digital shift over the past three years. Several investments have been made, new service providers have entered the market and offered additional services, staff have been trained on these services, further teaching methodologies have been developed, and several have proven pedagogically helpful or simply more efficient in addressing some issues (e.g., the lack of teaching spaces). Hence, some tools introduced during the pandemic are likely to remain.

2 This might be the case with e-proctoring systems. These are technologies designed to monitor student behaviour during online exams. Their function is to replicate in-person invigilation and guarantee the integrity of exams.[3] However, the extensive intrusion into the private sphere of students and numerous publicised cases of discriminatory outcomes[4] have raised several questions about these tools.

3 Used for many years now in some parts of the world, online proctoring software entered European HEIs during the first COVID-19-related lockdowns. Faced with urgent rules, HEIs were forcedto reflect on how to guarantee the integrity of online exams, opting in some cases for e-proctoring solutions. This brought the conversation on the credibility, necessity, and reliability of e-proctored assessment methods to the forefront of academic discourse.

4 The growing use of e-proctoring tools in European HEIs during the pandemic is confirmed in an explorative study the authors conducted between April and July of 2021.[5] The research targeted 38 HEIs in the United Kingdom, Italy, and the Netherlands, collecting 194 responses to a 32-question survey. It resulted that 13.10% of educators have been using e-proctoring systems during the pandemic, and 8.70% were offered the possibility to opt-out and choose a non-e-proctored alternative.[6] These results cannot be generalised, but they signal the emergence of e-proctoring usage among traditionally non-distant education providers. At the same time, they show that e-proctoring was not the only means to guarantee the integrity and validity of exams, as a large part of the respondents organised online exams without remote invigilation.

5 By now, most universities are back to on-site exams. However, the possibility of yet another upsurge of the coronavirus has led a few HEIs to ensure that formal rules for reinstalling online proctoring processes are in place for when the circumstances might make it necessary. These rules, incorporated, for example, as Examination Board rules and responsibilities, describe the framework for organising distance (written) exams with online fraud prevention measures. While almost lifted everywhere, pandemic-related restrictions have left long-standing traces in the functioning of HEIs and the performance of educational activities. This

schneider@unicatt.it). This paper and the related research are the results of a joint and collaborative work. However, Sections D.I, E, and F can be attributed to Alexandra Giannopoulou; Sections B, D.II.1, D.II.2, D.III, and G to Rossana Ducato; Sections A, C, and D.II.3 to Chiara Angiolini; Section D.IV to Giulia Schneider.

1 On the 5th of May 2023, the WHO Director-General declared that "It is therefore with great hope that I declare COVID-19 over as a global health emergency. However, that does not mean COVID-19 is over as a global health threat." (WHO Director-General's opening remarks at the media briefing, 5 May 2023, <https://www.who.int/news-room/speeches/item/who-director-general-s-opening-remarks-at-the-media-briefing---5-may-2023> accessed 6 May 2023.

2 Such emergencies, unfortunately, are not limited to public health matters. After the Russian invasion, many Ukrainian students were forced to return to remote teaching. Alexandra S Levine, 'Online Learning Resumes In Ukraine, But With New Wartime Challenges' (*Forbes*, 31 March 2022) <https://www.forbes.com/sites/alexandralevine/2022/03/31/ukraine-schools-use-tech-to-bring-classes-to-students-wherever-they-may-be/> accessed 1 November 2022.

3 For an overview of these tools see Section B.

4 More recently, see Naomi Appelman, 'Racist Technology in Action: Proctoring Software Disadvantaging Students of Colour in the Netherlands' (*Racism and Technology Center,* 10 July 2021) <https://racismandtechnology.center/2021/07/10/racist-technology-in-action-proctoring-software-disadvantaging-students-of-colour-in-the-netherlands/> accessed 1 November 2022.

5 This result stems from research conducted within the project 'Zooming in on Privacy and Copyright Issues in Remote Teaching' (https://www.stir.ac.uk/research/hub/contract/1660502). The project investigated the data protection and copyright implications of platforms' adoption in the field of education. The full description of the empirical study and results, including the analysis of the copyright issues, are published in Bernd J Jütte, Guido Noto La Diega, Giulia Priora, Guido Salza, 'Zooming in on education: An empirical study on digital platforms and copyright in the United Kingdom, Italy, and the Netherlands', (2022) 13(2) European Journal of Law and Technology. The present paper explores the data protection implications of those results.

6 At the same time, concerns about these systems were particularly deep, as the use of data by platforms and the deployment of e-proctoring technologies featured prominently among the most pressing issues posed by distance education: "how data are used by the platform", was stressed by 22% of the respondents, followed by "privatisation of educational means" (20.2%), "lack of choice about the platform to use" (16.8%), "e-proctoring technologies" (12.7%), "lack of digital materials at my University library" (9.2%), "uncertainty about online uses of materials" (6.9%).

legacy makes the critical evaluation of e-proctoring systems a necessary exercise for the determination of academic education imaginaries in a hybrid future.

6 The paper aims to map the legal landscape of e-proctoring in the EU. To this end, this contribution provides a brief overview of the technical aspects of e-proctoring systems (Section B) and existing literature (Section C) to map the state of the art of the debate. Section D critically discusses the case law consolidated over the past two years around e-proctoring systems, identifying points of convergence and divergence between the decisions. Section E reflects on the role of collective actions to enforce data protection rights and on the limited role it played in the e-proctoring controversies. After the submission of this contribution for review, a preliminary decision in the field of anti-discrimination law was issued for the first time in the Netherlands. Section F includes this relevant update and focuses on the legal means beyond data protection law for countering the discriminatory effects caused by the adoption of some e-proctoring tools. Section G sums up the results of the research.

B. E-proctoring systems: a brief technical overview

7 E-proctoring systems include a set of methods, software, and devices to monitor students at distance during an online test or exam. Online proctoring systems were already developed and used before the pandemic.[7] This was not only the case for massive open online courses ("MOOCs") and online HEIs but, in some circumstances, also traditionally non-distant learning institutions were relying on them (e.g., to organise computer-based tests at universities for a large cohort of examinees or to introduce more flexibility for some categories of students, such as athletes).[8] However, during the pandemic, their use has become much more widespread as, in some cases, it was considered the only available solution to perform exams and ensure their integrity.

8 Nowadays, various third-party commercial options are specifically designed to manage online exams and remote student invigilation. In principle, such tools enable HEIs and staff members to verify the student's identity at the beginning of the exam, monitor their activity, set up technical restrictions on their computer (e.g., block browsing during the exam or disable copy-paste shortcuts), remotely control and manage the exam and generate a report out of the monitoring activity.[9]

9 With reference to the invigilation modalities, Hussein *et al* classify e-proctoring tools into three main categories: live proctoring, recorded proctoring, and automated proctoring.[10]

10 The first solution, live proctoring, essentially replicates the physical surveillance but via webcams and microphones. Here, a physical proctor remotely verifies the student's identity at the beginning of the exam and monitors their video and audio during the whole duration of the session. In some cases, the invigilator can require a video scan of the workspace to verify that the student does not have any forbidden material at hand.

11 The second category, recorded monitoring, involves capturing and storing students' video, audio, computer desktop, and activity log for a subsequent human check.

12 Finally, automated proctoring relies on artificial intelligence systems to verify, for example, students' identities via a biometric recognition system and/or to automatically detect suspicious behaviours. In this latter case, the algorithm processes students' data (e.g., eye or facial movements, voice, keystroke loggings) and environmental data (such as background noise and the presence of other people in the room) to spot signs of cheating.[11]

7 Chris Rose, 'Virtual Proctoring In Distance Education: An Open-Source Solution' (2009) 2 American Journal of Business Education 81; Brian Bergstein, 'Online Exams: Big Brother Is Watching You: How Can You Tell If an Online Student Has Done the Work? That's Where Webcam Proctoring Comes In' (2012) 116 MIT Technology Review 68; Kenrie Hylton, Yair Levy and Laurie P Dringus, 'Utilising Webcam-Based Proctoring to Deter Misconduct in Online Exams' (2016) 92–93 Computers and Education 53; Kelwyn A D'Souza and Denise V Siegfeldt, 'A Conceptual Framework for Detecting Cheating in Online and Take-Home Exams' (2017) 15 Decision Sciences Journal of Innovative Education 370; Gianni Fenu, Mirko Marras, and Ludovico Boratto, 'A Multi-Biometric System for Continuous Student Authentication in e-Learning Platforms' (2018) 113 Pattern Recognition Letters 83; Silvester Draaijer, Amanda Jefferies, and Gwendoline Somers, 'Online Proctoring for Remote Examination: A State of Play in Higher Education in the EU', *Technology Enhanced Assessment* (Springer International Publishing 2018); Rohit Kumar, Viral Prakash Shah, and Nawaz Mohammed Shaikh, 'Methods and Systems for Monitoring Exams' (2013) <https://worldwide.espacenet.com/publicationDetails/biblio?FT=D&date=20190109&DB=EPODOC&CC=EP&NR=2750063B1> accessed 6 July 2022.

8 D'Souza and Siegfeldt (n 7) 374.

9 Mohammed Juned Hussein and others, 'An Evaluation of Online Proctoring Tools' (2020) 12 Open Praxis 509.

10 ibid.

11 See Liane Colonna, 'Legal Implications of Using AI as an Exam Invigilator' in Liane Colonna and Stanley Greenstein (eds), *2020-2021 Nordic Yearbook: Law in the Era of Artificial Intelligence* (The Swedish Law and Informatics Research

In case of anomalies, the system flags the issue for human review—usually the professor or the trained proctor—or can automatically terminate the assessment.

13 Many e-proctoring services usually offer a combination of the features mentioned above. As this brief overview suggests, there are various levels of intrusiveness in the students' personal sphere depending on the proctoring modalities or the adopted settings. In any case, they all process personal data (relating to the examinees, the examiners, and potentially third parties entering the room), thus triggering the application of data protection law. In the next Section, we will outline the risks and legal issues raised by e-proctoring as emerging from the literature.

C. Legal issues of e-proctoring

14 The increased use of e-proctoring systems has raised several concerns, including from a legal perspective. In the literature, many authors have stressed the potential clash between the use of such tools and fundamental rights and freedoms, particularly regarding the right to privacy, data protection, and non-discrimination.

15 For instance, it has been emphasised that the use of e-proctoring tools is likely to create or foster inequalities, e.g., for disabled people (who can be penalised by the anti-fraud system because they need to use screen readers or dictation software),[12] people with caring responsibilities (whose exam can be disrupted if the person they care for requires their immediate attention), or low income students who might not be able to afford suitable technical equipment, a reliable internet connection, or a room of their own.[13]

16 Moreover, the risk for ethnic minority groups is particularly high when using facial recognition technologies. Several studies have shown that such software is often trained on biased datasets and is systematically better at recognising white people, and particularly white men.[14] Hence, negative consequences for certain groups may occur due to the error rates of such tools or their deployment in a particular context.

17 Concerning privacy, the tracking of students' activity increases the risks of surveillance.[15] In this respect, scholars have warned against the chilling effect that pervasive monitoring can have on "students' intellectual freedom"[16] and their educational privacy.[17]

Institute 2022).

12 Lydia XZ Brown, 'How Automated Test Proctoring Software Discriminates Against Disabled Students' (*Center for Democracy and Technology*, 16 November 2020) <https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/> accessed 6 July 2022; Lydia XZ Brown, Ridhi Shetty, Matt Scherer, Andrew Crawford, 'Ableism And Disability Discrimination In New Surveillance Technologies: How new surveillance technologies in education, policing, health care, and the workplace disproportionately harm disabled people', (*Center for Democracy and Technology*, 24 May 2022, <https://cdt.org/wp-content/uploads/2022/05/2022-05-23-CDT-Ableism-and-Disability-Discrimination-in-New-Surveillance-Technologies-report-plain-language-final.pdf> accessed 31 October 2022.

13 Teresa Scassa, 'The Surveillant University: Remote Proctoring, AI, and Human Rights' (2022) 8 The Canadian Journal of Comparative and Contemporary Law 271; Lindsey Barrett, 'Rejecting Test Surveillance in Higher Education' (2021) Available at SSRN 3871423.

14 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' in Sorelle A Friedler and Christo Wilson (eds), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR* (2018); Jacob Snow, 'Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots', (*American Civil Liberties Union*, 26 July 2018) <https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28> accessed 31 October 2022.

15 Scassa (n 13); Barrett (n 13); Colonna (n 11). On surveillance in education institutions, see: Torin Monahan and Rodolfo D Torres, *Schools under Surveillance Cultures of Control in Public Education* (Rutgers University Press 2010); Barbara Fedders, 'The constant and expanding classroom: surveillance in K-12 public schools' (2019) 97 North Carolina Law Review 1673; Jason Pridmore and others, 'Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households' (2019) 17 Surveillance & Society 125; Maya Weinstein, 'School of Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 Public School Security' (2020) 98 North Carolina Law Review 438; Sara Collins and others, 'The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools' (*Future of Privacy Forum*, September 2021) <https://studentprivacycompass.org/resource/self-harm-monitoring/>, accessed 31 October 2022.

16 Barrett (n 13); Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934.

17 Education privacy has been defined as a specific right "that safeguards the ability for a student to safely explore ideas and knowledge, to develop their intellectual selves and their personal selves, as well as the ability for educators and researchers to facilitate and participate in intellectual endeavours in the education context". Tiffany C Li, 'Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis' (2021) 52 Loyola University of Chicago Law Journal 767. The author affirmed that "this educational privacy right should be linked to the essential purpose for

18 Scholars have also expressed serious concerns about e-proctoring from a data protection perspective. The automated decision-making process performed by such software can impact examinees in a significant way (i.e., the suspected behaviour can be reported wrongly, or the exam can be automatically terminated), and it remains unclear to what extent the ex-post human review is an appropriate guarantee in practice.[18]

19 Moreover, unlike its analogic counterpart, e-proctoring technologies inevitably generate new data and favour their collection and storage. The retention of such amounts of data increases, as a consequence, the risks of the re-purposing and sharing of information without the data subject's awareness.[19] Such risks might range from situations where the HEI has an obligation to disclose such information to the commercial uses performed by the e-proctoring tools or to data breaches.[20]

20 Data security is, indeed, another critical point highlighted in the literature. Security concerns are even more worrisome considering the intimate nature of the data processed via e-proctoring (e.g., exam results, biometric data).[21]

21 Furthermore, the potential threat to fundamental rights caused by e-proctoring is directly recognised in the AI Act proposal,[22] where AI systems intended to assess students or determine their access to educational programs are classified as high-risk (hence, subject to stricter rules for their authorisation).[23]

22 Lastly, the choices that dictate the use of e-proctoring systems contribute to shaping our modern educational infrastructures, with a potential effect on education itself. This means that the existing risks for privacy, data protection as well as the discriminatory effects of these systems all become particularly salient beyond the individual, on a broader societal level.

23 Some of the legal issues just outlined in this paragraph have been challenged before European courts and supervisory authorities over the past few years, mainly from a data protection perspective. Very recently, the discriminatory effect posed by these systems has been raised in the Netherlands.

24 In the following Sections, the decisions concerning e-proctoring will be critically analysed to understand the state of play of this evaluation of practice within the EU legal framework. Section D will focus on data protection, assessing the main arguments used in the decision to see to what extent the GDPR can protect against the risks raised by monitored online exams. Section F will discuss the anti-discrimination case and the possible remedies available under the equality framework.

D. E-proctoring cases and data protection: a critical analysis

25 The data protection implications of e-proctoring tools have been assessed in a few European legal systems so far and with different outcomes. We counted one pre-pandemic decision[24] and eight decisions from 2020 onwards.[25] In terms of Data

education to provide social space for students to learn and grow through learning, for educators to impart knowledge and foster intellectual growth, and for researchers to produce and disseminate knowledge", ibid 791. The notion of "education privacy" recalls the one of "intellectual privacy", defined by Richards as the "ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others"; Neil M Richards, 'Intellectual Privacy' (2008) 87 Texas Law Review 387.

18 Scassa (n 13) 306. See also Colonna (n 11), referring to Christopher O'Neill and others, 'Online Exam Monitoring Is Now Common in Australian Universities — but Is It Here to Stay?' (*The Conversation*, 18 April 2021) <http://theconversation.com/online-exam-monitoring-is-now-common-in-australian-universities-but-is-it-here-to-stay-159074> accessed 21 September 2022. The author reported that, in some cases, the human revision is outsourced to people outside the HEIs context, who are often poorly paid.

19 Barrett (n 13). On the possible negative effects of massive data collection on educational practices, see Pridmore and others (n 15).

20 Colonna (n 11).

21 Barrett (n 13); Colonna (n 11).

22 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. On the 6th of December 2022, the Council of the European Union approved its version of the proposal as a general approach. On the 11th of May 2023, the European Parliament's Internal Market Committee and the Civil Liberties Committee agreed on the compromise text of the AI Act, which is expected to be voted by the plenary in June 2023.

23 See, Annex III of the Commission Proposal for an AI Act. In the literature, see Liane Colonna, 'The AI Regulation and Higher Education: Preliminary Observations and Critical Perspectives' in Katja de Vries and Mattias Dahlberg (eds), *Law, AI and Digitalisation* (Iustus, 2022).

24 Datatilsynet (DK) - 2018-432-0015.

25 Datatilsynet (DK) - 2020-432-0034; Persónuvernd - 2020112830; OVG Nordrhein-Westfalen, Beschluss vom 04.03.2021 - 14 B 278/21.NE; Garante privacy - Ordinanza 9703988 - 16 Sep 2021 (for a commentary in English, see

Protection Authorities ("DPA") guidance, the French *Commission Nationale Informatique & Libertés* ("CNIL") has issued a note with recommendations on surveillance and online exams in 2020.[26]

26 The e-proctoring systems examined in the court decisions varied, ranging from recorded to automated proctoring.[27] Such systems were partly customisable, and the HEIs adopted different features and retention policies. None of these cases reported the use of a facial recognition system to authenticate the examinees, nor the adoption of a fully automated decision-making process (i.e., there is no automated termination of the exam, but the recorded video/audio and the score for the deviant behaviour are reviewed ex-post and the final decision is made by the examiner or the examination board).[28]

27 The table on the right (Table 1) includes the list of decisions summarising their main outcome.

28 In terms of general outcomes, the DPA decisions (with the only exception of Denmark 2) found at least one, but usually numerous, GDPR violations in the application of e-proctoring systems, notably with regard to transparency rules (Denmark 1, Iceland, Italy) or the safeguards on extra-EU transfer (Italy, Portugal). On the contrary, Dutch courts reached an opposing conclusion.

29 Hence, in order to have a clearer understanding of the state of the art of the case law concerning e-proctoring tools and data protection, it becomes relevant to comprehend the different points raised in the decisions, the arguments used, and the friction within the legal framework.

30 In the following subsections, we will focus on the four main points that emerge from the cross-analysis of the decisions on e-proctoring, notably: 1) the actors involved in processing for e-proctoring purposes and the allocation of responsibility between them; 2) the lawfulness of the processing; 3) the respect of the right to information towards the data subject when deploying the e-proctoring system; 4) the challenges of cross-border data transfer.

Table 1. List of the e-proctoring cases with data protection claims and summary of the main outcome of the decisions

Abbreviations	Decision	Type of invigilation	Outcome of the decision	Notes
Denmark 1	Datatilsynet - 2018-432-0015	Automated e-proctoring system	Violation of Arts. 5(1)(c), 9, and 13 GDPR	Pre-pandemic case Use of e-proctoring in a high school
Denmark 2	Datatilsynet - 2020-432-0034	Recorded e-proctoring	Processing in line with data protection rules	Pandemic case Use of the software at a HEI
Germany	OVG Nordrhein-Westfalen, Beschluss vom 04.03.2021 - 14 B 278/21.NE	Recorded e-proctoring	Claim dismissed for procedural reasons	Pandemic case Use of the software at a HEI
Iceland	Persónuvernd - 2020112830	Recorded e-proctoring	Violation of Arts. 5(1)(a) and 13 GDPR	Pandemic case Use of the software at a HEI
Italy	Garante privacy - Ordinanza 9703988 - 16 Sep 2021	Automated e-proctoring system with flagging feature to spot cheating behaviours	Violation of Arts 5(1)(a), (c), (e). 6, 9, 13, 25, 35, 44 and 46 GDPR Violation of Art. 2-sexies of the Italian Data Protection Code (concerning the processing of special category data necessary for the performance of a task carried out in the public interest)	Pandemic case Use of the software at a HEI
The Netherlands 1	Rb. Amsterdam - C/13/684665 / KG ZA 20-481	Automated e-proctoring system with flagging feature to spot cheating behaviours	Claim dismissed	Pandemic case Use of the software at a HEI Judge for the preliminary injunction
The Netherlands 2	Gerechtshof Amsterdam - 200.280.852/01	Same as in *The Netherlands 1*	Decision confirms the outcome of *The Netherlands 1*	Pandemic case Use of the software at a HEI Appeal of *The Netherlands 1* decision
Portugal	CNPD - Deliberação/2021/622	Automated e-proctoring system with flagging feature to spot cheating behaviours	Violation of Art. 5(1)(a), (b), (c) GDPR	Pandemic case Use of the software at a HEI

I. Accountable actors

31 The responsibility of universities has seen an undoubtedly horizontal consensus across all decisions from either courts or national DPAs. HEIs that have used e-proctoring systems for exam invigilation are all considered data controllers, with the e-proctoring system providers qualified as data processors. Such conclusions align with what has already been noticed regarding the relationship between the education provider and the third-party platform used for e-learning purposes.[29]

Giorgia Bincoletto, 'Italy - E-Proctoring During Students' Exams: Emergency Remote Teaching at Stake' (2021) 7(4) European Data Protection Law Review 586); Rb. Amsterdam - C/13/684665 / KG ZA 20-481; Gerechtshof Amsterdam - 200.280.852/01; CNPD - Deliberação/2021/622.

26 CNIL, *Surveillance des examens en ligne : les rappels et conseils de la CNIL*, (20 May 2020), <https://www.cnil.fr/en/node/119918>, accessed 1 June 2022.

27 Following the categorisation made by Hussein and others (n 9).

28 This overview only concerns cases with data protection claims. As will be shown later on, the Netherlands Institute for Human Rights examined a discrimination claim concerning an e-proctoring system with facial recognition implemented for authenticating students.

29 As outlined, for example, by the Italian Data Protection Authority, Act of 26th March 2020, n. 9300784 – "Didattica a distanza: prime indicazioni" (26 March 2020), <https://www.garanteprivacy.it/home/docweb/-/docweb-display/

32 Remarkably, the Portuguese DPA articulated in greater detail the role, responsibility, and liability of the HEI and those of the e-proctoring provider, highlighting that the latter shall be seen as a data controller for the data they process for their own purposes (e.g., for the improvement of the service or for research).[30]

33 All the examined decisions look at the relationship between two actors: the HEI, on the one hand, and the e-proctoring platform, on the other. Even if not dealing with an e-proctoring case specifically, it is worth mentioning a Greek DPA's decision that goes a step further in analysing the responsible and liable actors in providing distance learning in schools.[31] The decision remarked that commercial e-learning service providers usually process data for purposes other than those set out by the HEI. This personal data collection and processing for their own distinct purposes qualifies these providers as data controllers for this function. Following this rationale, the Ministry of Education is the institution enabling and creating the conditions for this additional collection of personal data. Hence, in light of CJEU case law,[32] the Greek Ministry shall be considered a joint controller for the processing of personal data by the service provider.[33] While the reasoning is relatively succinct, and in reality, inconsequential for the Ministry itself as no further conclusions are put forward following this qualification, the recognition of the Ministry as a joint data controller for the data processing operations performed at the initiative of the private service provider, reveals the elevated responsibility of the State when favouring the implementation of distance learning tools.

34 Finally, all reviewed decisions and relevant opinions share the recognition of the responsibility of institutions in the decisions related to e-proctoring and remote teaching more generally. The recognition of a joint controllership between (private) service providers and (public) educational institutions, stressed by the Portuguese and Greek DPA, highlights the dependencies created between these two actors during the decision-making processes that lead to putting in place online education or e-proctoring systems. This "responsibilisation" of educational institutions shows the strong role of HEIs in enabling processing, making it possible for service providers to reuse educational data for autonomous purposes.[34] Moreover, it acknowledges the power dynamics at play throughout the establishment of big data-driven infrastructures.[35]

II. The lawfulness of the processing

35 The principle of lawfulness is a fundamental data protection pillar that protects data subjects, by requiring the processing to be compliant with the law, and necessary and proportionate to pursue a legitimate aim.[36] While there is a general agreement in all the analysed decisions towards the existence of a ground that can potentially legitimise the processing of personal data for e-proctoring purposes, the outcomes of the processing of sensitive data and the assessment of the necessity and proportionality of the means for ensuring the integrity of the exam diverge substantially.

1. Lawful ground(s) of e-proctoring processing

36 The first legal requirement that each HEI, as data controller for e-proctoring purposes, shall respect is the reliance on a lawful basis.[37] The majority of

docweb/9300784>, accessed 11 November 2020.

30 CNPD - Deliberação/2021/622, paras 56-57. In that case, the processing for the improvement of the service or research performed by the e-proctoring provider was deemed invalid for the lack of a lawful basis (specifically, the company was relying on the consent of students who were forced to accept all the terms, which included the conditions for data processing, when they had to take the exam online).

31 Greek DPA, 50/2021, 16th November 2021. A summary of the decision is contained in Annex I of this paper.

32 Case 40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629.

33 According to the DPA's decision, "although the Ministry has no influence on the way Cisco uses this data, it is aware that by choosing to use the Webex Meetings application, it allows the transfer of users' personal data to Cisco for corporate purposes. Therefore, this activity should at least be considered a joint controllership with Cisco". Greek DPA, 50/2021.

34 See Chiara Angiolini and others, 'Remote Teaching During the Pandemic and Beyond: Four Open Privacy and Data Protection Issues of "Platformised" Education' (2020) Opinio Juris in Comparatione 45.

35 On this aspect, see Roberto Caso and Maria Chiara Pievatolo, A liberal infrastructure in a neoliberal world: the Italian case of GARR, 14 (2023) JIPITEC 349 para 1.

36 Cécile de Terwangne, 'Article 5 Principles Relating to Processing of Personal Data' in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020).

37 Art. 6 GDPR establishes the grounds on which each processing must be based to ensure its lawfulness. These are alternatively: the consent of individuals (Art. 6(1)(a) GDPR), the necessity of the processing for performing or entering into a contract (Art. (6)(1)(b) GDPR), compliance with a legal obligation (Art. 6(1)(c) GDPR), protection of the vital interests of the data subject or of any third party (Art. 6(1)(d) GDPR), performance of a task carried out in the

the cases found that the e-proctoring processing (whether live, recorded or automated) can fall within the umbrella of Article 6(1)(e) GDPR which qualifies data processing as lawful when "necessary for the performance of a task carried out in the public interest".[38] Whether the HEI is a public or a private entity, according to DPAs and judicial decisions, putting in place monitored online exams can be qualified as "necessary to fulfil a task in the public interest", i.e., to provide education, organise exams, and issue valid academic qualifications.[39]

37 The Italian DPA and the Dutch judge focused on the aspects of the processing that the law must regulate when Article 6(1)(e) GDPR is used.[40] In this respect, according to the Dutch judge of the first instance, it is not necessary "that the public task or data processing is exhaustively regulated in a law in a formal sense, it is sufficient that the main features are known in the law".[41] Hence, the use of the automated e-proctoring tool was considered compatible with the Dutch legal framework. A more restrictive stance is taken by the Italian DPA, which stresses that the flagging system monitoring students' behaviour during the exam entails profiling. This processing creates specific risks for students (e.g., the exam can be invalidated) in violation of the principle of non-discrimination.[42] According to the DPA, when the relies on the lawful basis provided for by art. 6(1)(e) GDPR, such risks shall be properly assessed in a specific legislative provision.[43] The latter, however, was found missing in the Italian system, leading the DPA to invalidate the processing.

38 Contrary to the other decisions, the Icelandic DPA found the lawfulness of the processing in the legitimate interest of the HEI to ensure the integrity of exams and the quality of studies.[44] In the opinion of the DPA, such interests were not overridden by the students' fundamental rights and freedoms, *a fortiori* because the students who did not have facilities at home were offered to take the online exam in the HEI buildings. However, the decision did not thoroughly discuss the feasibility of such an alternative. For instance, it emerges from the complaint that the student could not accept this option due to the health conditions of his spouse (who was a suspected COVID-19 contact). Such a situation then leaves more than a doubt concerning the actual chance of the person accessing the exam without the use of the e-proctoring system proposed by the university.

39 Finally, the Italian DPA also contemplates the possibility that e-proctoring might be grounded in Article 6(1)(c) GDPR, i.e., the necessity of the HEI to comply with a legal obligation.[45] However, this point is not further elaborated by the Authority.

40 A substantial agreement instead can be found in the express refusal of consent as a basis that can legitimise the processing of personal data when deployed by a HEI for e-proctoring purposes. This result is not surprising as it applies a consolidated interpretation of the consent requirements. In particular, the manifestation of will shall be "freely given", i.e. the data subject shall have a real choice whether to accept the processing for e-proctoring purposes, and, in this context, such a choice might be impaired by the imbalance of power between the students and the HEI, the lack of equivalent alternative modalities for the exam, or the inability to take the exam without agreeing to the further processing performed by the platform. For example, the Icelandic DPA stated that consent may not be a lawful legal basis for processing due to the nature of the relationship between the university and the students. For the Portuguese Authority, the consent was de facto imposed if students wanted to do the exam (hence, it was not freely given).

public interest or in the exercise of official authority (Art. 6.1.e GDPR) or, the pursuit of a legitimate interest of the controller or any third party (Art. 6(1)(f) GDPR).

38 Confirmed also in CNIL (n 26).

39 On the application of Art. 6(1)(e) GDPR to private Universities, see Garante privacy - Ordinanza 9703988 - 16th September 2021 and CNPD - Deliberação/2021/622.

40 According to Art. 6(3) GDPR, the legal basis referred to in (e) of paragraph 1 must be laid down by Union law or Member State law to which the controller is subject. The processing purpose must be i) determined on that legal basis or ii) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The legislation, at EU or national level, must meet an objective of public interest and be proportionate to the legitimate aim pursued. Art. 6(3) GDPR states also that the legal basis provided for by law may contain specific provisions to adapt the application of the GDPR (*e.g.*, the general conditions governing the lawfulness of processing by the controller; the category of data that can be processed; the data subjects concerned; the purpose limitation; and storage periods).

41 Rb. Amsterdam - C/13/684665 / KG ZA 20-481, para 4.9.

42 Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.5.

43 Such a conclusion echoes the considerations made by the former Article 29 Working Party, which, in relation to the forthcoming Art. 6(1)(e) GDPR, stated that: "when the processing implies an invasion of privacy or if this is otherwise required under national law to ensure the protection of the individuals concerned, the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed". WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, adopted on 9th April 2014, 22.

44 Persónuvernd - 2020112830, para 2.2. On the contrary, the reliance on the legitimate interest was expressly excluded by Rb. Amsterdam - C/13/684665 / KG ZA 20-481 (para 4.9) and CNPD - Deliberação/2021/622 (paras 47-50).

45 Garante privacy - Ordinanza 9703988 - 16 Sep 2021.

2. Processing of sensitive data

41 During the invigilation activity, the video recording can capture images or sounds revealing the ethnic or racial origin of the examinee, and the flagging system relies on the elaboration of the student's movements to identify suspicious behaviours. Whether such activities qualify as the processing of sensitive data, including biometric information, is a question that was answered quite differently in the analysed decisions.[46]

42 The first divergence concerns the classification of the information collected for detecting signs of cheating as biometric data. As known, biometric data are defined as those "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".[47] The definition reflects that biometric data are generated through the use of specific technologies that elaborate individuals' features to identify (1:n biometric identification) or confirm (1:1 biometric verification) the data subject's identity.[48]

43 In *Denmark 2*, the lawfulness of the processing of biometric data was raised but dismissed because it was proven that the system was not adopting any facial recognition technologies. Student IDs were checked randomly by the staff instead. In the Dutch cases, the judge of the injunction affirmed that the e-proctoring system was used for authentication purposes,[49] but it seems to emerge from the decision that the staff manually verified students' identity at the end of the exam. With regard to the use of the flagging system to analyse students' behaviour, the same decision quickly concluded that it did not entail any processing of biometric data.[50]

44 Different from the Dutch court, the Portuguese and Italian DPAs affirmed that the automated analysis of the students' behaviour was processing of a "particularly sensitive nature".[51] Both decisions stressed that such data were not used to identify or confirm the student's identity.[52] Nevertheless, they were used to profile students.[53] Without entering into the assessment of the legal nature of such data, the Portuguese authority stated that the processing was disproportionate.[54] On the contrary, the Italian decision specifically recognised that the e-proctoring system was generating, through automated means, a biometric template, i.e., a digital representation of the biometric characteristics of the students extracted from the video recording, and, as a consequence, the university was processing biometric data to verify the presence of the student during the exam and to spot anomalies in their behaviours.[55] Given the classification of the students' facial images as biometric data, the Italian Authority applied the stricter regime established for special categories of data.[56] It concluded that, since there

46 Sensitive data or special categories of data are listed in Art. 9(1) GDPR and include "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". The processing of such data is prohibited by default unless the controller respects one of the conditions set in Art. 9(2) GDPR.

47 Art. 4(14) GDPR.

48 Lee A Bygrave and Luca Tosoni, 'Article 4(14). Biometric Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 213.

49 Rb. Amsterdam - C/13/684665 / KG ZA 20-481, para 4.16

50 ibid.

51 CNPD - Deliberação/2021/622, para 54.

52 See, Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.4 and CNPD - Deliberação/2021/622, para 52.

53 See, in particular, Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.5 and CNPD - Deliberação/2021/622, para 52.

54 See infra Section D.II.3.

55 Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.4. On the notion of biometric data under the GDPR and the distinction between identification and verification, see Els J Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013); Catherine Jasserand, 'Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data' (2016) 2 Eur Data Prot L Rev 297; Catherine A Jasserand, 'Avoiding Terminological Confusion between the Notions of "biometrics" and "Biometric Data": An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective' (2016) 6 International Data Privacy Law 63; Rossana Ducato, 'I dati biometrici' in Vincenzo Ricciuto, Vincenzo Cuffaro, Roberto D'Orazio (eds), *I dati personali nel diritto europeo* (Giappichelli 2019).

56 Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.4. There has been some debate concerning the classification of biometric data as sensitive data. It has been noticed in the literature that the list of special categories of data at Art. 9 GDPR does not include all biometric data, but only those meant to "uniquely identifying a natural person". This narrow reading might exclude from the more stringent discipline of sensitive data biometric information used, for example, for verification purposes (Jasserand, 'Avoiding Terminological Confusion between the Notions of "biometrics" and "Biometric Data": An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective' (n 55)). However, this difference is not specifically marked in the Italian legal system. The national law regulates biometric data *tout court* as a special category of data together with genetic and health-related

was no national provision to date that authorised the processing of such sensitive data for ensuring the integrity of exams, the processing was unlawful.

45 The second point of divergence in the decisions analysed concerns the classification of the information contained in the video recording, able to reveal the ethnic or racial origin, as sensitive data.

46 The Court of Appeal of Amsterdam (*Netherland 2*) is again very restrictive in its interpretation, excluding that the facial images—e.g., those contained in the student ID card—can trigger the protection reserved in the GDPR for special categories of data.[57] First, because the processing is not meant to process the sensitive characteristics;[58] and, second, because it is unlikely that the lecturers will discriminate against students based on those attributes.[59]

47 Similarly, the Danish DPA (*Denmark 2*) affirms that although "it cannot be ruled out that personal data covered by Art. 9 GDPR may be processed in connection with the monitoring of examinees' computers"[60], the processing of such information is, in principle, unintentional. Hence, it dismisses the point of the university, which was declaring to rely on Article 9(2)(g) GDPR (i.e., the necessity of the processing for reasons of substantial public interest). Instead, the Authority recommended the controller to encourage students to avoid the sharing of sensitive data during the examination.[61] In a 2018 decision (*Denmark 1*), the DPA excluded as well the applicability of Article 9(2)(g) GDPR, considering its narrow scope (i.e., "which is namely assumed to be used, e.g., for processing of personal data for the purpose of health security, monitoring and alerting, prevention or control of communicable diseases and other serious threats to health"[62]). However, on that occasion it clearly stated that the controller should have identified another suitable lawful basis for the processing of sensitive data that can be accidentally recorded during an online exam.

48 The legal status of pictures and videos is not unproblematic.[63] There are only two direct references in the GDPR (Recital 51 and Article 4(14)) to them, and they are both related to biometric data. However, this is not the only special category of data that can be inferred from a picture. In its 'Advice Paper on special categories of data'[64], the Article 29 Working Party admitted the possibility that images of persons, like those captured by surveillance cameras, can reveal information about the ethnic origin or the health status of an individual and, as a consequence, can be classified as sensitive data. This initial interpretation, however, was not confirmed in the following Guidelines 3/2019 where the European Data Protection Board affirmed that video footage could be covered by Article 9 only if the processing is aimed at inferring special categories of data.[65] This ambivalence reflects the two main approaches that have emerged in the literature so far: a first approach (context-based) considers information in terms of special category of data and whether it is possible to derive the sensitive attribute from the circumstances of the processing; a second approach (purpose-based) retains that information can be considered under the umbrella of Article 9 when the controller aims to infer and use the sensitive characteristic.[66] The *Netherlands* and *Denmark 2* cases seem to align with this latter approach.

49 However, the recent CJEU decision in *OT* offers some elements to reconsider the above mentioned assessment.[67] In this case, the EU Court went for a context-based interpretation, affirming that the publication of the spouse's name on the controller's website can indirectly reveal the sexual orientation of the data subject and shall be classified as a processing of sensitive data.[68] The Court, in particular, stated that the notion of special category of data shall be interpreted broadly to guarantee a high level of protection of fundamental rights, especially in cases where the data's sensitivity can seriously interfere with privacy and data protection.[69]

50 If the rationale is to ensure an enhanced level of protection for those data that can reveal sensitive information through an intellectual operation of deduction or comparison, we might assume that the e-proctoring activity consisting of the recording of a video that is automatically elaborated for

data, establishing enhanced safeguards for it (see Section 2-f, Personal Data Protection Code).

57 *Contra,* Hoge Raad [Netherlands Supreme Court], [23rd March 2010] LJN BK6331. As reported in Kindt (n 55) 135-136.

58 Gerechtshof Amsterdam - 200.280.852/01, para 3.3.10.

59 ibid.

60 Datatilsynet - 2020-432-0034, para 3.1.3.

61 ibid. See, also ibid. para. 3.2.

62 Datatilsynet - 2018-432-0015, para 3.3.

63 Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Colum Bus L Rev 494; Paul Quinn and Gianclaudio Malgieri, 'The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22 German Law Journal 1583.

64 WP29, *Advice paper on special categories of data*, 20th April 2011, para 3.2.1

65 EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, 29th January 2020.

66 Quinn and Malgieri (n 63).

67 Case 184/20 *Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601.

68 ibid para 128.

69 ibid paras 125-127.

spotting signs of fraud and that can be assessed by the lecturer, should be considered as a processing of sensitive data. Especially in this case, the intention to rely on the sensitive characteristics should be considered irrelevant: both humans and machines can be affected by biases and give rise to disadvantageous treatment in practice.[70] That is why, for example, written assignments are usually marked anonymously.[71] On the contrary, recommendations on the measures to avoid the unintentional sharing of sensitive data, as suggested in *Denmark 2*, might eventually be considered a minimisation strategy, which presupposes a processing of sensitive data and the need to be covered by one of the conditions under Article 9(2) GDPR. Indeed, even if some elements are easy to hide from a camera (and we should question whether such a request is legitimate in terms of freedom of expression), others are impossible to (e.g., physical characteristics revealing our ethnic origin).

51 Finally, it shall be mentioned that the Icelandic claimant was trying to introduce a point about the recording of another subject's sensitive data, potentially captured during the videocall. In that case, while the student was taking the exam, his spouse was having a remote medical consultation, and the claimant was worried that the conversation could have been recorded. The issue was dismissed for procedural reasons (although the DPA noticed that, considering the circumstances of the exam, the recording of the data subject's wife would have been unlikely).[72] It is, however, another sign that shows how the deployment of an e-proctoring process can be intrusive, breaking the boundaries between the public and private spheres, revealing students' private life and personal circumstances.

3. The necessity and proportionality of the e-proctoring processing

52 Overall, with the clarifications mentioned in Section D.II.1, the examined decisions recognise that Universities can use e-proctoring systems to pursue the legitimate aim of ensuring the organisation and integrity of exams during the pandemic. However, for the processing to be legitimate, its operations shall be necessary and proportionate in relation to its purpose.

53 With regard to this issue, the French DPA adopted some general guidelines in the document "*Surveillance des examens en ligne : les rappels et conseils de la CNIL*"[73], outlining a few case scenarios and examples. The DPA considered that real-time video surveillance or snapshots of audio/video during examinations do not appear *prima facie* disproportionate. On the contrary, tools that allow the remote control of students' computers or the use of facial recognition systems might not be proportionate to the purpose of online examination.

54 All the decisions acknowledged that the pandemic forced universities to consider alternative assessment methods to traditional ones due to the impossibility of organising exams in person.[74]

55 The Icelandic DPA recognised that the e-proctoring processing was necessary to prevent exam fraud and ensure the reliability of evaluations and, thus, the quality of studies during the pandemic.[75] A similar conclusion was reached in *Denmark 2*. The Danish Authority acknowledged the assessment of the need for examination supervision performed by the HEI in relation to its courses, finding that the university adopted the e-proctoring tool only for one exam where it was crucial to ensure that students did not receive any external help (since there was only one correct identical answer and students did not have to explain how they reached that solution),[76] chose the least intrusive e-proctoring program, and had a proportionate storage period (21 days).[77]

56 The Dutch judge considered the potential interference of the use of e-proctoring tools with the right to data protection as necessary in a democratic society according to Article 8(2) ECHR because of the restrictions adopted during the COVID-19 period and the need to ensure the provision of education (which was considered in its economic relevance as well).[78] Moreover, the Court affirmed that the interference with Article 8 ECHR was proportionate due to the absence of alternative e-proctoring tools which were equally efficient at preventing fraud as the one adopted by the university in its case.

57 The rest of the decisions came to an opposite outcome.[79] The Italian and Portuguese Authorities recognised that the necessity and proportionality

70 See more on this point in Section E.

71 John M Malouff and others, 'Preventing halo bias in grading the work of university students' (2014) 1 Cogent Psychology 988937.

72 Persónuvernd – 2020112830, II.1.

73 CNIL (n 26).

74 This consideration does not apply to *Denmark 1*, as it occurred before 2020. On the use of alternative means, see Barrett (n 13).

75 Persónuvernd – 2020112830, para 2.2.

76 Datatilsynet - 2020-432-0034, para 3.1.1.

77 ibid para 3.1.2.

78 Gerechtshof Amsterdam - 200.280.852/01, paras 3.3.2 and 3.4.2.

79 In *Denmark 1* (pre-covid), the DPA found that the education institution failed to demonstrate how their processing met the necessity and proportionality test.

of the means were not properly considered in the HEIs' Data Protection Impact Assessment ("DPIA").

58 The Italian DPA, in particular, noticed the excessiveness of: 1) the data collection (the system did not simply inhibit some functions on the student's computer, but it also generated information based on their behaviour which was not considered strictly necessary for ensuring the validity of the exam), and 2) the retention policy (initially five years, reduced to one during the proceeding).[80] These elements led the Authority to declare the violation of the principles of minimisation, storage limitation, and data protection by design and default.

59 Reaching a similar conclusion, the Portuguese DPA started from the consideration that the processing involved a massive collection of data for the purposes of profiling and monitoring students. However, there was no assessment of the appropriateness, necessity, and proportionality of such a processing in relation to the general objective of ensuring the integrity of the exams. Furthermore, the scoring system assessing deviant behaviours was considered fairly opaque, making it impossible to evaluate the necessity and proportionality of the collection. Thus, the DPA concluded that the data minimisation principle was not respected.[81]

60 All in all, the examined decisions investigated the necessity and proportionality of the processing's means, with different outcomes. This is not surprising, considering that this assessment should entail a case-by-case evaluation.

61 While the break of the pandemic was, in principle, considered a reason for the necessity of the interference with the right to privacy and data protection, the concrete implementation modalities of the e-proctoring tools led DPAs to sanction the most intrusive e-proctoring processing, i.e., those entailing students' profiling or the calculation of the "cheating score". The only exception is the Dutch case, where the automated e-proctoring was indeed admitted. Here, however, the decision seems to derive from a procedural reason rather than a substantive one, i.e., the lack of adequate evidence provided by the claimants. The Dutch judges considered, in fact, that the students did not furnish suitable and less intrusive alternatives, able to overturn the university's assessment.

62 On a more general level, the DPIA proved to be a crucial document that was extensively used by the majority of DPAs to evaluate the legitimacy of the controllers' choices critically and, in particular, the necessity and proportionality of the measures adopted. For instance, even if the case was not focusing on e-proctoring but on distance education more generally, the Hellenic DPA consistently highlighted that the provision of proof in support of the necessity and proportionality of the COVID-related measures taken by the Ministry of Education should be evaluated on a case-by-case basis, especially due to the diverse ways in which these measures have the potential to impact different educational tiers. The evaluation on this case-by-case basis is expected to be performed (and subsequently proven) in the DPIA document. The engagement with this document is less evident in the Icelandic and Dutch decisions, where the Authority and the judges checked the performance of the DPIA but without an extensive engagement with the merit of the assessment.

III. The transparency of the processing

63 One critical factor that led to the invalidation of the majority of e-proctoring processing was the implementation of the principle of transparency. Such a principle, enshrined at Article 5 GDPR, requires the data controller to inform the data subject about the key aspects of the processing—including its risks—in a clear and timely manner (not only at the beginning of the processing operations but also after a data subject's request or in the case of data breach affecting data subjects rights).[82] The analysis of the cases reveals that universities largely failed in their duty to inform students about the processing occurring during e-proctoring.

64 The Danish (in *Denmark 1*), Italian, and Icelandic DPAs highlighted serious deficiencies in the content of the privacy policies provided to students. In particular, such cases pointed out the lack of adequate information about crucial aspects of the processing, such as the modalities of the monitoring,[83] data subjects' rights,[84] and profiling.[85]

65 The Portuguese and Icelandic DPA also emphasised the lack of clear instructions for teachers on the conditions and features of the respective e-proctoring tool. The Icelandic Authority considered that the training and education about the system was a complementary aspect of the duty to inform the student under Article 13 GDPR.[86]

80 ibid para 3.6.

81 CNPD - Deliberação/2021/622, paras 53-54.

82 See Arts. 5(1)(a), 12-14, and recitals 39, 58-61, and 71 GDPR.

83 Persónuvernd – 2020112830, para 2.4.

84 ibid.

85 Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.3.

86 Art. 13 GDPR requires the data controller to provide the data subject with a series of information (e.g. identity of the controller, purpose of the processing, the recipients of the

Meanwhile, the Portuguese Authority stated that the lack of instructions to lecturers introduced an excessive margin of discretion on staff, denoting a scarce delimitation of the purpose of the processing and a lack of data minimisation by the controller.[87]

66 The Italian DPA noted further violations of the principle of transparency, following the guidelines of the WP29.[88] First, noticing that the privacy policy used general formulas in relation to data storage, the DPA admonished the need to detail the specific storage period for the different categories of data processed. Second, in relation to the lack of relevant information concerning the transfer of data extra EU, the DPA affirmed the need to inform the data subjects about the country where the data were exported, the lawful ground for such a processing, and the specific safeguards for them.[89] Third, even though the DPA recognised that the e-proctoring system was not fully automated (hence, excluding the application of Article 22 GDPR)[90], it recalled the importance of informing data subjects about the risks of the processing in a meaningful way, avoiding situations where they are taken by surprise. In practice, this means that the controller shall make the individual aware of the logic of the e-proctoring algorithm and its consequences.[91]

67 Interestingly, the Portuguese case takes a different stance on the application of Article 22. The Lusitanian Authority, examining an e-proctoring tool similar to the Italian one, doubted that the intervention of a member of the staff, in case of a notification of anomalies in the student's conduct, could be considered a genuine human intervention. Given the lack of instructions to teachers and the lack of transparent information about the parameters used by the algorithm to signal deviant behaviours, the staff would have little elements to draw their own conclusions.[92] It did not elaborate further on Article 22 GDPR (for instance, about the existence of the conditions under Article 22(2) GDPR), but it alluded to the lack of remedies for the students to contest the decision.[93]

68 While both the Italian and Portuguese Authorities confirmed the need to inform data subjects about the logic and parameters of the e-proctoring algorithm, the Court of Appeal of Amsterdam quickly dismissed the possibility that the university should provide full insights into how the suspected behaviour is detected. In the opinion of the Court, such information could actually conflict with effective fraud prevention.[94]

69 Finally, with reference to the form of communication, the Italian DPA provided additional indications. It condemned the adoption of vague formulas (e.g., 'by way of example but not exhaustive') in the text of the privacy policy, the use of hyperlinks that do not lead to the relevant page, and the use of layered notices not accompanied by the full privacy policy. Moreover, the DPA had the occasion to specify that the mandatory disclosures required under Article 13 GDPR cannot be fulfilled by providing information to the students' representatives. Each and every data subject should be targeted instead.

70 In *Denmark 2* the information provided by the university to the students was overall positively evaluated. According to the DPA, the specific target was reached with a letter describing the e-proctoring processing in a "concise, transparent, easy to understand, easily accessible form, and in a clear and simple language"[95], and the letter was in addition to the general information notice that individuals receive at the beginning of their studies (which remains accessible on the university communication platform).[96] However, the Danish DPA pointed out that the university should have specified that the system records the browsing activity during the exam and that it is able to capture sensitive information, encouraging the HEI to fix such issues.

IV. Extra-EU data transfer

71 Many European DPAs have expressed their concerns

data, etc.) when the data are collected directly from them.

87 CNPD - Deliberação/2021/622, 43-44.

88 WP29, *Guidelines on Transparency under Regulation 2016/679*, adopted on 29th November 2017 as last revised and adopted on 11th April 2018 (wp260rev.01).

89 On this point, see *infra* Section D.IV.

90 Art. 22 GDPR prohibits automated decision making systems that can produce legal effects on data subjects or similarly significantly affect them. The provision, however, works when the processing is solely automated, i.e. if there is no meaningful human oversight. See WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, adopted on 3rd October 2017 As last Revised and Adopted on 6th February 2018 (wp251rev.01).

91 As recently stated by the Italian Supreme Court in a case concerning the creation of "reputational ratings" for the accreditation of physical and legal persons by a not-for-profit association, the controller shall disclose the "executive scheme of the algorithm and the elements of which it is composed". See, Cass civ (1) 25 May 2021, 14381.

92 CNPD - Deliberação/2021/622, 54. According to WP29, a "fabricated human intervention" falls within the scope of the "solely automated" decision under Art. 22 GDPR. WP29 (n 90).

93 CNPD - Deliberação/2021/622, 55.

94 Gerechtshof Amsterdam - 200.280.852/01, para 3.3.7.

95 Datatilsynet - 2020-432-0034, para 3.2.

96 ibid.

and issued decisions regarding the legitimacy of occurred data transfers outside of the EU in the context of e-proctoring.

72 The Italian DPA has underlined that many transfers to the US of data collected during remote teaching activities lacked an adequate lawful basis.[97] This trend was confirmed in the e-proctoring decision at stake. The DPA ascertained that the transfer was based on standard contractual clauses ("SCCs"). However, the technical and organisational measures were not sufficiently described in the contract by the importer and, as a consequence, were not in line with the requirements established by the same SCCs, as data subjects may not rely on such measures.[98] Similarly, the Portuguese DPA underlined the lack of an appropriate transfer mechanism with respect to two e-proctoring applications used by the university. According to the national supervisor, the university did not adopt the additional safeguarding measures to protect data in line with the *Schrems II* principles.[99]

73 Remarkably, the Dutch courts in *Netherlands 2* rejected the claim made by the plaintiffs with regard to the extra-EU data transfer and highlighted that they did not plausibly demonstrate that anyone not authorised by the university to view the video and audio, such as the service provider itself or US intelligence agencies, could gain access.[100] This appears to be quite a peculiar perspective, since the GDPR requires—in first stance—proof of the establishment of adequate safeguards for the protection of transferred personal data. The GDPR's approach is that of minimising the risk of access, by preventing access episodes through enacted safeguards. Along these lines, the Dutch Court appears to postpone the focus of the analysis to a secondary and pathological moment that the GDPR intends to approach through anticipatory protection tools. Hence, in line with the GDPR's objectives, the Court should have rather focused on the proof of safeguards instead on the proof of access. This is the approach taken in the Italian decision instead.

74 The cases mentioned above illustrate the concrete challenges for transferring data outside of the EU after the invalidation of the Privacy Shield. The DPA decisions are not isolated cases but follow a series of other important interventions in the sector of edTech. The Austrian DPA, for example, found that Google analytics services used for educational monitoring purposes were violating Article 44 GDPR, for they did not ground outside EU data transfer in one of the legal bases envisaged by the GDPR.[101] Similarly, the CNIL deemed the SCCs relied on by Google to be ineffective in so far as these did not "prevent access possibilities of US intelligence services or render these accesses ineffective"[102]. The transfers enacted by Google were thus considered to undermine "the level of personal data protection of data subjects as guaranteed in Art. 44 of the GDPR".[103] The Danish government has announced a ban on Google Workspace and Chromebooks in Danish schools, noting that data processed from online education activities could be accessed by non-EU authorities in manners inconsistent with EU data protection law.[104] More recently, a data governance study in UK schools showed that little has changed since the invalidation of the EU-US Privacy Shield, and many companies continue to transfer education data to the US.[105]

75 It is yet to be seen how the new draft US-EU adequacy decision "Data Privacy Framework", under discussion within the EU institutions, will address the concerns that have emerged so far.[106] In this respect, the EDPB raised several concerns in its Opinion 5/2023, restating the presence in the draft of existing issues related to "the rights of data subjects (e.g. some exceptions to the right of access and the timing and modalities for the right to object), the absence of key definitions, the lack of clarity in

97 Garante per la protezione dei dati personali, Memoria del Presidente del Garante per la protezione dei dati personali, Pasquale Stanzione - Affare assegnato n. 621 (impatto della didattica digitale integrata (DDI) sui processi di apprendimento e sul benessere psicofisico degli studenti), <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9581498>, 27 April 2021 (Italian only).

98 Garante privacy - Ordinanza 9703988 - 16 Sep 2021, para 3.7.

99 CNPD - Deliberação/2021/622, paras 60-62.

100 Gerechtshof Amsterdam - 200.280.852/01, para 3.3.8.

101 Datenschutz behorde - 2021-0.586.257 (D155.027)).

102 CNIL, 'Google Analytics et Transferts de Données : Comment Mettre Son Outil de Mesure d'audience En Conformité Avec Le RGPD ?' (7 June 2022) <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/google-analytics-et-transferts-de-donnees-comment-mettre-son-outil-de-mesure-daudience-en-conformite> accessed 1 November 2022.

103 ibid.

104 Paul Sawers, 'Denmark Bans Chromebooks and Google Workspace in Schools over Data Transfer Risks' (*TechCrunch*, 18 July 2022) <https://techcrunch.com/2022/07/18/denmark-bans-chromebooks-and-google-workspace-in-schools-over-gdpr/> accessed 1 November 2022.

105 Louise Hooper, Sonia Livingstone, Kruakae Pothong, *Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo* (Digital Futures Commission and 5Rights Foundation, 2022).

106 Commission, 'Joint Statement on Trans-Atlantic Data Privacy Framework' <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087> accessed 1 November 2022. On the 13th of December 2022, the Commission has presented the draft of the adequacy decision for the EU-US data transfer, available at: <https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf> accessed 21 February 2023.

relation to the application of the DPF Principles to processors, and the broad exemption for publicly available information".[107] Similar concerns were expressed by the Committee on Civil Liberties, Justice and Home Affairs ("LIBE") in a draft motion for a resolution on the proposed adequacy decision, pointing out that, despite the changes introduced in the US legal order, the US system does not still grant an equivalent level of data protection.[108] Hence, the LIBE called on the Commission to continue the negotiations and urged not to adopt the draft of the adequacy decision presented on the 13th of December 2022. The European Parliament confirmed this view in its Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, urging the Commission "not to adopt the adequacy finding until all the recommendations made in this resolution and the EDPB opinion are fully implemented".[109]

76 This situation concerning the EU draft transfer inevitably highlights the technological dependence of HEIs on third-party providers subject to foreign law and the risks associated with such a choice.[110] Therefore, it is crucial to reflect on the possibility that edTech tools could be developed by European public players, who shall take into account—by design—the needs of the institutions and the EU values embedded in the Charter of fundamental rights and CJEU case law.

107 EDPB, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework,* adopted on 28 February 2023.

108 See LIBE 'Draft motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))', <https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.html> accessed 21 February 2023.

109 European Parliament, *Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework*, P9_TA(2023)0204, para 20.

110 In the case of public authorities using cloud computing services, see the recent EDPB, *2022 Coordinated Enforcement Action 'Use of cloud-based services by the public sector',* Adopted on 17 January 2023, <https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf> accessed 21 February 2023 (see, in particular, paras 3.5 and 3.6).

Table 2. Summary of the key points emerging from the analysis of data protection cases discussed in Section D.
All decisions concern data processing carried out using-e-proctoring tools, except the Greek decision which examines e-learning tools (*).
All decisions describe cases which occurred during the pandemic, except *Denmark 1*(**).

	Accountable actors	Lawful ground(s) of processing	Processing of sensitive data	The necessity and proportionality of data processing means		Transparency of the processing	Extra-EU data transfer	Type of action
Denmark 2	Data protection roles: HEIs: data controllers e-proctoring system provider: data processor In addition:	Art. 6(1)(e) GDPR (necessity to perform a task in the public interest)	The processing of sensitive data is in principle unintentional	The decisions acknowledged that the pandemic forced universities to adopt alternative assessment methods to traditional ones due to the impossibility of organising exams in person	Necessity of e-proctoring to prevent exam fraud and ensure the reliability of evaluations during the pandemic	Overall, the information provided was concise, timely, and transparent. Additional information should have been given regarding certain aspects of processing (e.g., recording of the browsing history during the exam and how to avoid the sharing of sensitive data)	-	DPA investigation after a phone inquiry
Iceland		Art. 6(1)(f) GDPR (legitimate interest)	The claim concerning the potential processing of sensitive data of third-party during the recording (health data of the data subject's wife) was dismissed for procedural reasons		The education institution failed to demonstrate how their processing met the necessity and proportionality test	Serious deficiencies in the privacy policies provided to students. Lack of clear instructions to teachers on the e-proctoring tool	-	DPA investigation following a student's complaint
Italy		In principle, Art. 6(1)(e) GDPR. However: i) according to the Italian DPA the performance of a task in the public interest shall be regulated in the law or a regulation (lacking in the Italian system with reference to the necessity of the specific e-proctoring tool); ii) in *Netherlands 1* the Court stated that it is not	The processing involves biometric data. No existing provision in Italian law authorises the processing of such data for e-proctoring purposes		The necessity and proportionality of the means were not properly assessed in the DPIA	Serious deficiencies in the privacy policies provided to students	Block of the transfer towards the US Lack of proof that the transfer of personal data to the US (including biometric data) complied with the GDPR	DPA investigation following a student complaint
Netherlands 1			No processing of biometric or sensitive data found by the judge		The alternatives (e.g., essays) to e-proctoring were considered not suitable by the judge	-	The plaintiff did not prove that the transfer occurred in violation of the	Lawsuit initiated by the representative body of students

Netherlands 2	- the Portuguese DPA stated that the e-proctoring system provider is a data controller for the data they process for their own purposes - According to the Greek DPA the Greek Ministry is a joint controller for any personal data processed by the e-learning platform	necessary that the public task or data processing is exhaustively regulated - According to the Italian DPA Art. 6(1)(c) GDPR (compliance with a legal obligation) could be another potential lawful basis - The Portuguese DPA questioned whether processing could be based on Art. 6(1)(f) GDPR (legitimate interest)	The processing of students' facial images was not regarded as sensitive data		The need for the delivery of educational services made the interference with the right to data protection necessary in a democratic society under Art. 8 ECHR	-	GDPR principles.	against their university
Portugal			-		The necessity and proportionality of the means were not properly assessed in the DPIA	Lack of clear instructions to teachers on the e-proctoring tool	Block of the transfer towards the US. Lack of additional measures preventing access to the transferred personal data by the US authorities	DPA investigation, following a complaint
Greece*			-		The provision of distance education is necessary for the educational process to be effective in periods when live education is impossible	Serious deficiencies in the information provided. The role of information is also to ensure proper understanding of the risks. It must be ensured that the information addressed to different data subjects is concise, transparent, understandable, and easily accessible, with simple wording especially with regard to children	The Greek Ministry of Education breached the obligations of Art. 46 GDPR, as no evaluation of the extra-EU data transfer had been carried out for the legality of the found data transfers	DPA investigation after a teachers' union complaint
Denmark 1**			Sensitive data might be captured during the recording, and the controller did not provide a suitable lawful basis for it	The education institution failed to demonstrate how their processing met the necessity and proportionality test		Lack of specific information about the e-proctoring processing	-	DPA investigation

E. Countering e-proctoring systems with GDPR collective action

77 GDPR enforcement processes—either through the exercise of data rights before the data controller, or through recourse to a DPA or courts—are key in understanding how e-proctoring systems can be inspected, challenged, and lawfully restrained. Whether at a university or an e-proctoring service provider level, personal data processing left unchecked risks, principally, harming students' fundamental rights. It is thus important to inspect the degree to which students and other (collective) entities are empowered to challenge e-proctoring systems bringing claims in front of the relevant authorities to contest the exclusionary and intrusive effects of online invigilation.

78 As our above analysis shows, e-proctoring systems can and have been challenged in both national courts and data protection authorities with relative success. It is interesting to note that on many occasions, universities were ordered to stop using specific e-proctoring software due to the GDPR violations observed by the DPAs. To this day, national courts have not delivered similar decisions.

79 Student complaints vis-a-vis the national DPAs is what instigated the decisions against the use of e-proctoring systems in Italy, Portugal, and Iceland. As we briefly presented above and as summarised in the Annex, students were able to raise arguments ranging from GDPR violations (unlawful consent to the processing of personal data, etc.) to violations of fundamental rights such as privacy and data protection.[111] These cases stayed well within the realm of individual direct action that aims to counter harms experienced by students in the deployment of e-proctoring systems.

80 Personal data protection normative frameworks tend to centre around the individual. This perspective is an important dimension of the way in which data protection law ensures (levels of) control over personal data. Yet, there are different ways in which data protection law—and the GDPR in particular—enables collective empowerment beyond the individual. While understudied in scholarship and underused by policymakers, judges, and authorities, it is vital to explore GDPR collective action as a tool to challenge e-proctoring systems, especially as it has become widely accepted that data-driven technologies often provoke harm beyond the

111 This was particularly discussed in the Dutch cases.

individual level.

81 The GDPR creates the procedural framework within which individuals can claim redress of individualharms incurred to each data subject respectively, but through acting collectively.[112] The recent *Ola/Uber* cases[113] show how these types of processes can empower groups of individuals when they exercise their rights in a coordinated manner. The *Oracle/Salesforce* case[114] is another stellar example of this understanding of collective action because its reasoning goes well beyond the limited number of individual claimants. This procedural framework requires a representative organisation or simply the coordination of numerous individuals, who bring one single procedure forward. Collective action can also refer to a single action on behalf of a group of individual data subjects operating to obtain a collective gain.

82 In the case of e-proctoring, we believe that GDPR collective action can be viewed as one available tool to tackle and counter harms suffered by specific groups of students or even by the student body as a whole. However, their (limited) exercise has not been particularly successful.

83 Collective student action has been a key instrument for ensuring the broader impact of the desired outcome. In Germany, for example, a complaint contesting the use of e-proctoring software was filed jointly by a university student and a digital rights non-profit organisation (*the Gesellschaft für Freiheitsrechte* ("GFF")).[115] The complaint regarded the storage and processing of video and screen-recorded data by the e-proctoring software that the university chose for conducting student exams during the lockdown. The requested injunction failed to produce the desired outcome of restricting the storing of exam video recordings, as the motion was denied by the Court on the basis of procedural elements, preventing the examination of substantive aspects.[116] In particular, the Court stated that it could not address the lawfulness of the processing in the emergency proceeding. An overview of the injunction reveals that the urgent procedure which was chosen due to the student circumstances was not the appropriate juridical forum, especially when the objective was to produce an impactful decision that would contribute to counter surveillance and e-proctoring system normalisation in HEIs. This case is a representative example of litigation efforts to ensure a strategic outcome against the use of e-proctoring software.

84 When thinking about the effects upon individuals of powerful systems mediated through data-driven technologies, strength in numbers is critical. For this reason, GFF is decidedly attempting to create the necessary conditions for introducing collective action representing multiple students. Namely, the

112 The GDPR gives data subjects the ability to have specific types of organisations represent them to obtain remedies for GDPR violations if such representation is recognised in Member State law. In *Meta Platforms Ireland Limited*, the CJEU recently clarified that Art. 80(2) GDPR does not preclude national legislation that allows a consumer protection association to bring legal proceedings in the absence of a mandate conferred on it for that purpose (and independently of the infringement of specific rights of a data subject), by alleging infringement of the prohibition of unfair commercial practices, consumer protection legislation or the prohibition of the use of invalid general terms and conditions (Case C-319/20 *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV*. [2022] ECLI:EU:C:2022:322). Art. 80 GDPR designates a particular type of third party that can be mandated by data subjects to exercise a number of remedial rights. It enables pre-specified entities to exercise a subset of procedural rights attached to the data subjects (i.e. Arts. 77-79). Similarly, Art. 82 GDPR shows promise in empowering (groups of) individuals who have suffered damage by data processing infrastructures to seek compensation. So far, however, the exact scope and extent of this provision in practice is murky.

113 Rb. Amsterdam - C/13/692003/HA RK 20-302. The Court of Amsterdam ruled in a case brought by the UK drivers that were using Ola Driver App to provide services. The case concerned the right to access personal data and the right to data portability. While the Court rejected the request to order Ola to provide all personal data that falls within the scope of Art. 20 GDPR as insufficiently determined, it ruled that a driver collective action to seek access to their data did not amount to an abuse of data protection rights. It also confirmed the right of third parties to establish a gig workers data trust.

114 Rechtbank Amsterdam, C/13/688682 / HA ZA 20-863. The Privacy Collective (TPC) started a class action on behalf of ten million individuals against Oracle and Salesforce. It claimed that Oracle and Salesforce unlawfully processed personal data, and played a crucial role in the Real Time Bidding (RTB) process. The Court rejected the claim on grounds of representativeness of the TPC, but not before providing valuable insight in the concept of collective action. According to the decision, simply clicking on the support button does not mean that a statement of support has been obtained as intended within the representativeness requirement. The Court elaborated that the following information would have been necessary: information about the nature and deployment of the procedure; parties the action is directed at; and a description of the victims for whom TPC stands up for.

115 Gesellschaft für Freiheitsrechte e.V. - GFF, 'Monitoring of Online Examinations' <https://freiheitsrechte.org/en/themen/digitale-grundrechte/proctoring> accessed 1 November 2022.

116 OVG Nordrhein-Westfalen, Beschluss vom 04.03.2021 - 14 B 278/21.NE.

NGO has launched a public call looking for affected students. According to the call, GFF "want(s) to win fundamental decisions against excessive surveillance through online proctoring - and the best way to do that is with several cases that illustrate the problem".[117]

85 Similarly, in *Netherlands 1 and 2*, rather than individually instigated student complaints, it was the representative body of students who launched a lawsuit against their university challenging the decision and the conditions of use of e-proctoring systems for online invigilation. The representative student council body contested the unlawfulness of the personal data processing, the discriminatory effects of the software, and the lack of student participation in the decision-making process regarding the use of e-proctoring systems for exam invigilation. This case is among the few that were brought forward by students on the basis of multiple GDPR violation claims.

86 Interestingly, among all the cases examined, the student council was the only one challenging the institutional decision-making processes that led to the introduction of the e-proctoring systems. These processes did not involve the input and feedback from the student council, characterised by the university as "unsolicited advice" on the use of online proctoring.[118] The Amsterdam Court in *Netherlands 2* rejected the student council's claims invoking the internal regulations that permit such 'emergency' decisions to be taken unilaterally by the administrative body of the university without having to necessarily consider the input of student representative bodies. Remarkably, but not surprisingly since this was a civil litigation, the Court put the responsibility to determine, describe, and explain all available alternatives to all types of invigilation processes that are occurring in the context of student exams on the claimants, i.e., student council.[119] In sum, this means that the Court conceded that the student council's input was not necessary in the decision-making process regarding e-proctoring systems; at the same time, the Court decided to put the burden of explanation (and proof) on the advantages of alternative solutions to that same student council.

87 Finally, the Dutch Court in *Netherlands 2* recognised the admissibility of the student council as a claimant in this case. However, it did not justify the decision based on the GDPR procedural standing rules nor clarified whether the claimants represented the university's students in their collective interests vis-a-vis the GDPR violations in question. This lack of clarity is but one example illustrating the need for legal and procedural certainty in collective action cases with GDPR-based claims.

88 Similarly, in Greece, following a complaint filed by the association of teachers and even though the decision addresses remote teaching in general and not e-proctoring specifically, the DPA delivered its opinion highlighting the constitutional duty of the state to ensure the provision of education.[120] This duty, according to the DPA, provides the necessary precondition to any decision that is geared towards fulfilling that obligation. As mentioned in Section D.I, the complaint was filed with the Greek DPA by the private schools' teachers' union. It is noteworthy that the DPA found the union to not have the standing to file such a complaint because it did not operate under a specific mandate.[121] The lack of clarity

117 Oberverwaltungsgericht Für Das Land Nordrhein-Westfalen, 'Eilantrag Gegen Videoüberwachte Prüfung Der Fernuniversität Hagen Erfolglos' (*Justiz-online*, 4 March 2021) <https://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/01_archiv/2021/17_210304/index.php> accessed 1 November 2022.

118 Gerechtshof Amsterdam - 200.280.852/01, para 2.8.

119 According to the Court, the student council did not make "it concrete in this way that there is a workable and sufficiently fraud-resistant alternative for every type of examination, which would make the use of Proctorio completely unnecessary. Nor have CSR et al. given concrete examples of exams where an alternative is available and the UvA has nevertheless opted for the application of Proctorio". Gerechtshof Amsterdam - 200.280.852/01, para 3.3.6.

120 See Greek DPA 50/2021, para 11: "During the school year 2020-2021, the Covid-19 coronavirus pandemic continued, while for long periods of time the schools did not function for life, either due to a decision of their universal non-operation for reasons of public health protection, or individual schools or sections, in accordance with the health protocols. In such cases, it is clear that the provision of education, which is an obligation of the state, must be continued at a distance through modern or asynchronous education procedures. The methods of providing distance education can, in general, be distinguished into methods of asynchronous distance education and modern synchronous distance education. As documented by the memorandum of the Ministry of Education and Science and the studies attached to it, **the provision of modern distance education is considered a necessary tool to be effective in the educational process, especially for long periods of non-functioning of lifelong learning for reasons of public health protection**, as the purpose of providing education can not be fulfilled effectively by providing only asynchronous distance learning. As modern distance education can only be done by electronic means which ensure two-way communication between teacher and trainee, which in fact presupposes processing of personal data of the participants in the educational process, such processing is necessary". (Our translation and our emphasis).

121 Art. 80(2) GDPR provides that Member States can allow

about the need for representation mandates with regard to the defence of individual and collective interests and the inconsistencies in collective representation at national levels are creating the space for inefficiencies of GDPR enforcement.[122]

89 Overall, we contend that collective action cases instigated by students and/or represented by student bodies and other similar organisations help (re)shape the public interest objectives of HEIs to a participatory model that includes student voices in determining student interests as a whole. In this context, the GDPR can constitute a solid legal basis for these actions because of its potential to uncover harms and inequalities. This has certainly proven to be true in the *Ola/Uber* cases and can follow similar paths in contesting e-proctoring systems. However, existing disparities in national collective action legal frameworks could limit the full potential of these mechanisms.

90 Beyond the data protection framework, equality law can be distinctly mobilised for the same purposes, as shown in a recent case in the Netherlands. In the next Section, the paper will present the first case contesting the discriminatory effects of the identity recognition feature of an online invigilation software, discussing the remedies available to challenge e-proctoring practices under the EU anti-discrimination legal framework.

F. The right to non-discrimination and e-proctoring

91 The above analysis reflects on the effectiveness of data protection tools as forms of accountability and assessment for e-proctoring systems used by public educational institutions. Despite the potential of the GDPR as a frame of reference and enforcement tool to protect human rights, the above-mentioned decisions did not go beyond data protection concerns. For instance, the discriminatory risks brought by e-proctoring were rarely put forward and discussed. However, such risks have become more and more pressing over the past few years.

92 As mentioned in Section C, many concerns have been raised about the error rates of the e-proctoring's facial recognition systems used for authenticating students leading to discriminatory effects against, such as black examinees.[123] Those students, for instance, have reported trouble logging into the virtual environment or were only able to do so when shining additional light on their faces.[124]

93 An e-proctoring software was used by the California bar for the admission exams organised remotely during the COVID-19 lockdown. Three students with disabilities sued the California bar because it refused to modify its remote proctoring protocols, which were making it impossible for disabled test-takers to efficiently sit the remote exams.[125] In *Gordon v. State Bar of California*,[126] the Court rejected the preliminary injunction because it did not recognise a concrete

collective organisations to lodge a complaint before a DPA or exercise data rights even without the mandate of the data subjects. However, this is not the case for Greece, where the law 4624/2019 requires the presence of an express written mandate for the representation of data subjects in Art. 41(2).

122 For GDPR data rights mandates, see Alexandra Giannopoulou and others, 'Intermediating data rights exercises: the role of legal mandates' (2022) 12(4) International Data Privacy Law 316. In general, and starting from 25 June 2023, the new Collective Redress Directive will be put in place, aiming to ensure that consumers are able to protect their collective interests in the EU via representative actions, the legal actions brought by representative entities. See Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1.

123 Mitchell Clark, 'Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them' (*The Verge*, 9 April 2021) <https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning> accessed 1 November 2022; Nora Caplan-Briker, 'Is Online Test-Monitoring Here to Stay?' (*The New Yorker*, 27 May 2021) <https://www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay> accessed 1 November 2022; NL Times, 'Webcam Exam Software "Discriminatory," Doesn't Recognise Darker Skin Tones, Says Student' (*NL Times,* 15 July 2022) <https://nltimes.nl/2022/07/15/webcam-exam-software-discriminatory-doesnt-recognize-darker-skin-tones-says-student> accessed 1 November 2022.

124 Proctor Ninja, 'Proctorio's Facial Recognition Is Racist' (*Proctor Ninja*, 18 March 2021) <https://proctor.ninja/proctorios-facial-recognition-is-racist> accessed 1 November 2022.

125 Specifically, the e-proctoring system would not accommodate test takers who: were unable to stay in front of the web camera for the entirety of each test section, such as one disabled plaintiff who needed to take unscheduled bathroom breaks; needed a paper version of the exam, such as one disabled plaintiff who cannot use a computer screen for long periods of time; needed scratch paper, such as plaintiffs with ADHD; needed different amounts of extra time per test section; or used screen readers or dictation software. See *Gordon v. State Bar of California* N D Cal (30 Sep 2020). Brown (n 12).

126 *Gordon v. State Bar of California* N D Cal (30 Sep 2020). See Olivia Meadows, 'Gordon v. State Bar of California: Test Takers with Disabilities Sue State Bar of California for Forcing Them to Test In-Person During the COVID-19 Pandemic' (2021) 47(1) American Journal of Law & Medicine 138.

harm in the proctoring processes especially vis-a-vis the broader COVID-19 crisis. These are but some examples of reported exclusion.[127]

94 It is important to note that the discriminatory effects of e-proctoring systems are often linked to the facial recognition software and the room scan features of e-proctoring. Bias in these types of algorithms is not new, leading some academic institutions to reject or cease the use of e-proctoring systems citing accessibility and equality concerns.[128] However, as evidenced by our case law analysis, contesting e-proctoring systems has shown its limitations because the examination of data protection and privacy compliance did not always consider potential harmful, discriminatory effects.[129] For instance, while the plaintiffs did mention discrimination concerns in their litigation in the *Netherlands 2* decision, barely any reference to this was provided. In particular, the students argued the potential for discrimination based on the protected characteristics of students recorded for the purposes of identification and online invigilation that might be revealed such as race or religion. However, the Court remarked that it does not appear to be possible that the material recorded will be used for discriminatory purposes but does not provide further arguments for such reasoning.

95 So, the question remains: what are the tools available to counter the discriminatory effects of e-proctoring systems? In examining this, we should also stress that while anti-discrimination law could constitute a suitable tool for software affecting a protected category, other groups (e.g., people with limited internet access) are not directly covered by this legal instrument.

96 The discriminatory effects caused by the facial recognition system were not specifically discussed in the decisions analysed in the previous Sections (see Table 1) because it was ascertained that students' identities were manually checked by the examiners.

97 However, if a facial recognition system was adopted, the GDPR might have offered some (limited) grip to combat algorithmic discrimination. Article 22 GDPR might apply, but on the condition that the processing was solely automated with no meaningful human oversight. Moreover, the DPIA would offer the chance to assess and address discriminatory effects.[130] However, these sections of the DPIA often remain not sufficiently investigated.

98 Beyond the GDPR, anti-discrimination law is another relevant framework whose impact against e-proctoring systems is soon to be tested for the first time in the Netherlands.[131] During the submission of this paper, the first European case of an anti-discrimination complaint against the facial recognition system of an e-proctoring tool was filed by a student within the *College voor de Rechten van de Mens* (the "Netherlands Institute for Human Rights", hereinafter "NIHR").[132] According to the submitted complaint,[133] the student had difficulties logging into the e-proctoring system because the facial recognition software could only detect her face with the light pointing straight at her. The student claimed that this software's inability to detect black people, especially when a public HEI mandates the use of this software, was discriminatory. The university's initial response to the student was to attempt to decouple the student's skin colour from the factors considered by the facial recognition proctoring algorithm mainly due to the lack of proof of the existence of such a link. The response to the internal complaint was that "they cannot establish an objective link between the student's skin colour and whether or not the digital surveillance system

127 Brown and others (n 12).

128 See the public announcement from the University of Illinois, stating they will not renew their licence to the Proctorio software due to discrimination concerns at <https://emails.illinois.edu/newsletter/1970177238.html> accessed 15 September 2022.

129 Indirectly, the Portuguese and Italian DPA offered some shielding against discrimination when considering the processing of sensitive data.

130 As stressed in Frederik Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) 24(10) The International Journal of Human Rights 1572 and the bibliography therein cited at fn 70. More recently, see also Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic impact assessments under the GDPR: producing multi-layered explanations' (2021) 11(2) International Data Privacy Law 125 and their suggestions for improving the current mechanism into a more effective Algorithmic Impact Assessment.

131 See Hans de Zwart, 'Dutch Student Files Complaint with the Netherlands Institute for Human Rights about the Use of Racist Software by Her University' (*Racism and Technology Center*, 28 July 2022) <https://racismandtechnology.center/2022/07/28/dutch-student-files-complaint-with-the-netherlands-institute-for-human-rights-about-the-use-of-racist-software-by-her-university/> accessed 1 November 2022.

132 The NIHR is the national human rights institution established according to the United Nations General Assembly Resolution A/RES/48/134 of 20 December 1993 on National institutions for the promotion and protection of human rights and Recommendation R (97) 14 of the Committee of Ministers to member states on the establishment of independent national institutions for the promotion and protection of human rights.

133 See the complaint here (in Dutch only): <https://racismandtechnology.center/wp-content/uploads/20220715-klacht-over-proctoring-bij-college-voor-de-rechten-van-de-mens.pdf > accessed 22 February 2023.

is functioning properly".[134] Against the backdrop of this case, it is useful to evaluate anti-discrimination laws as defensive tools against harms caused by e-proctoring algorithmic systems.

99 As explained by the complaint filed by the student, the Dutch anti-discrimination law qualifies indirect discrimination as whenever any apparently neutral provision, standard or practice related to people of a particular religion, belief, political opinion, race, gender, nationality, heterosexual or homosexual orientation or marital status is particularly harmful when compared to its effect on other people.[135]

100 The NIHR published an interim judgement on the 7th of December 2022.[136] It found that the facts presented by the student were sufficient for a presumption of indirect discrimination based on race, because: a) she was disadvantaged by the anti-spying software; and b) there is academic research showing that facial detection software generally performs worse on people with darker skin colours.[137] The NIHR applied existing legislation according to which, when there is a presumption of discrimination (so-called *prima facie discrimination*), the burden of proof shifts to the defendant, who must justify the use of the software.[138] In this respect, the NIHR concluded that the university had not provided sufficient evidence to do so. Hence, it gave ten weeks to the university to further substantiate its defence and reserved its final decision. As some authors have stressed, if the algorithm is a black box, it might be quite challenging to provide evidence of the lack of discrimination.[139]

101 Universities have a duty under anti-discrimination law to ensure that the practices—including e-proctoring features—are not unduly disadvantageous to any students before implementing them. To this end, they should choose a provider who will ensure this condition is satisfied.

102 In GDPR terms, this duty of care can be reflected in the application of the fundamental principles, such as accountability, fairness, and integrity. The principles of proportionality and necessity may play a significant role in assessing the lawfulness of the processing through e-proctoring software, also in relation to the assessment of discrimination risks. Moreover, it would be interesting to see national courts or DPAs assessing the existence of discrimination through the DPIA and the lens of the fairness of processing, a principle affirmed by Article 8 CFREU and Article 5 GDPR. This assessment could take place, for instance, when contesting a biased e-proctoring system that involves biometric authentication to sign in.

G. Final remarks

103 Over the past three years, many concerns have been raised in relation to the risks and situations of harm of e-proctoring implementation at universities during the pandemic.[140] Such concerns have been voiced and examined across Europe in a series of cases that were collected and critically analysed in this paper. In this final Section we summarise the legal takeaways of the analysis and pinpoint the more systemic issues that need to be addressed in relation to e-proctoring, and edTech more broadly.

104 Even if e-proctoring will not generally be needed by traditionally non-distant HEIs anymore (unless new emergencies arise), it might still be considered by those universities which are offering online programs, or which want to keep online assessments as an option. Hence, it is relevant to understand

134 Statement naar aanleiding berichtgeving Volkskrant, 15 July 2022 (in Dutch only): <https://vu.nl/nl/nieuws/2022/statement-naar-aanleiding-berichtgeving-volkskrant> accessed 22 February 2023.

135 Wet van 2 maart 1994, Artikel 1(c) indirect onderscheid: indien een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze personen met een bepaalde godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat in vergelijking met andere personen bijzonder treft.

136 College voor de Rechten van de Mens (Dutch Human Rights Institute), Decision 2022-146, available online at: <https://oordelen.mensenrechten.nl/oordeel/2022-146>.

137 On this issue, see Buolamwini and Gebru (n 14); Hanna F Menezes and others, 'Bias and Fairness in Face Detection' (2021 34th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI)) 247.

138 To prove algorithm *prima facie* discrimination is not often an easy task: the way some systems operate makes it difficult for an individual to realise whether, and how, they have been discriminated against. Moreover, without knowledge of the logic of the algorithm it will also prove challenging to see how other people might have been treated and, as a consequence, define a legitimate comparator group (people in a similar situation of the victim who were not disadvantaged by the alleged discriminatory practice). See, Sandra Wachter, Brent Mittelstadt, and Chris Russell, 'Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI' (2021) 41 Computer Law & Security Review 105567.

139 See, Jeremias Adams-Prassl, Reuben Binns, and Aislinn Kelly-Lyth, 'Directly discriminatory algorithms' (2023) 86(1) The Modern Law Review 144, referring to the Joint Opinion of Robin Allen QC and Dee Masters in the Matter of Automated Data Processing in Government Decision Making (7 September 2019) <https://perma.cc/M2GU-D8HS> accessed 9 February 2023.

140 See Section C of this paper.

to what extent e-proctoring tools shall be used or implemented by universities in the post pandemic world.

105 The case analysis shows that Courts and Authorities i) took the emergency situation into account in their decisions, ii) identified key problematic issues in the use of e-proctoring tools from a data protection point of view; and iii) non-discrimination issues emerged later, and the litigation is, at the moment, less developed when compared to data protection.

106 With reference to the first aspect, the situations of urgency and emergency faced by HEIs due to the COVID-19 lockdowns entered the balancing exercise to assess the legitimacy of alternative exam measures and, in some circumstances, led to the justification of the adoption of remote proctoring. However, now that COVID-19 is over as a global health emergency it is important that universities review the measures implemented during the past three years and abandon those that are no longer necessary or proportionate.

107 Secondly, data protection authorities found several points of friction between the deployment of remote invigilation and the GDPR, leading, in the majority of cases, to the block of the processing. For instance, the most invasive features, including the profiling of students for flagging suspicious behaviours, were banned by DPAs on a number of grounds, such as the lack of proportionality or lawful basis for the processing of sensitive data or for the extra-EU data transfer.

108 Different lines of reasoning were followed by civil courts. Dutch judges, in *Netherlands 1 and 2*, generally admitted the legality of the use of automated e-proctoring during the pandemic, confirming the assessment performed by the university.

109 When the processing did not involve the controversial flagging feature, all DPAs stressed some issues in the implementation of the transparency measures adopted by the universities to inform students.

110 Indeed, the lack of information provided to students and staff was a critical deficiency highlighted by the supervisory authorities. This situation might be a consequence of the general opaqueness of the system (noticed, for instance, by the Portuguese DPA). The lack of information on the "cheating score" and the way it should be reviewed by examiners raises several questions as to the effective presence of the "human in the loop" in this kind of situation. Hence, where there is no authentic human oversight, Article 22 GDPR should find application and this will cast more than a doubt about the possibility to justify an automated decision, based on profiling, against the students on any grounds of Articles 22(2) or (4) GDPR.

111 DPAs and Courts developed divergent reasonings on two further important issues that can put into question the use of e-proctoring tools: 1) the scope of Article 6(1)(e) GDPR and to what extent the processing performed in the exercise of a public task should be sufficiently specified in a law or regulation; and 2) the assessment of the legal status of pictures and biometric templates collected or generated during e-proctoring operations.

112 With reference to the first point, the Italian DPA convincingly points out that the profiling feature and the flagging system raise new risks for the protection of fundamental rights that should be adequately considered in a specific law or regulation. The necessity to guarantee the integrity of exams and degrees is indeed a task carried out in the public interest by HEI, but the legal framework in place reflects a situation where the exams were supposed to be organised in a more traditional fashion. Hence, unless this specific processing is adequately regulated in a law, detailing the limits and safeguards of it, the feature to monitor the behaviour of students during the online exam might not be grounded on a lawful basis (at least in Italy, the flagging system was declared to be in violation of Article 6 GDPR).

113 On the contrary, the Dutch judges seem to have adopted a lighter interpretation of the requirements needed under Articles 6(1)(e) and (3) GDPR or, at least, they did not consider the e-proctoring data processing particularly intrusive as to justify a more tailored regulation. Hence, given these different interpretations, this point might be contested in a future litigation or investigation before a data protection authority.

114 With regard to the second aspect—the assessment of the legal nature of pictures and videos collected during the exam, the decisions raise some further issues concerning the notion of biometric and special categories of data.

115 All the cases examining the flagging systems excluded that the processing of pictures to assess the students' behaviours was used to identify or verify the identity of individuals. The definition of biometric data and its classification as a special category of data in the GDPR is quite narrow and it might not include situations like the one here, namely biometric categorisation.[141] Nevertheless, as pointed out by the Italian Authority, when the system generates a biometric template, it is performing a processing that is preparatory to the identification and verification of the identity, even if

141 See bibliography mentioned in (n 55).

the data is not used for this purpose in the end.[142] In other words, following the DPA's logic, the attitude of the template to "allow or confirm the unique identification of that natural person" (Article 4(14) GDPR) can meet the definition of biometric data.

116 A different question is whether the processing of biometric data that is not used to uniquely identify an individual will attract the regime designed for the special category of data. As pointed out in Section D.II.2, the reference to biometric data is quite narrowly crafted in Article 9, and the GDPR seems to have drawn a distinction between identification and verification based on the level of risk that these activities pose to individuals.[143] Nevertheless, many scholars have been quite vocal about the pitfalls of this classification, considering that —for whatever purpose a biometric data is used—the characteristics that can be extracted from it still retain a considerable potential to enable the identification of individuals or negatively affect them.[144] Moreover, and as we have already highlighted, biometric data is one of the areas where Member States can intervene to specify further conditions for the processing. Hence, biometric classification performed with some e-proctoring tools could entail the processing of special categories of data (as affirmed, for example, in the Italian case).

117 As for the pictures not transformed into biometric data, but collected and stored during the invigilation procedure, we have seen that these have the potential to reveal sensitive attributes related to ethnic origin, religious beliefs or political opinions. The legal nature of such data has been debated, but the CJEU has recently confirmed a broad understanding of the notion of sensitive data: if it is possible to infer the sensitive characteristics from the context of the processing, data should be treated as a special category and protected accordingly. This interpretation would be able to address most of the discriminatory concerns as data controllers will have to properly assess the disparate impact for students in the DPIA and, if the system is adopted, appropriately justify their choices and safeguards in place (for instance, how to train the examiner who reviews the flagged videos or how to explain how the "cheating score" is calculated).

118 In any case, if an e-proctoring system processes sensitive data, it might be very challenging to ground it on any of the conditions under Article 9(2) GDPR. Indeed, we might consider the goal of ensuring the integrity of exams as being of substantial public interest (Article 9(2)(g) GDPR). However, such interest should be clearly spelled out in the law, which has to be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for appropriate safeguards. As mentioned in *Denmark 1* and *2*, such a threshold is quite high. Alternatively, the data subject could explicitly consent to the processing (Article 9(2)(a) GDPR). However, the imbalance of power between students and the university casts serious doubts about the use of such a ground. Finally, one could argue that sensitive data might be processed because the data subjects made those data manifestly public (Article 9(2)(e) GDPR). This lawful basis is generally interpreted in a restrictive way by DPAs.[145] In particular, it is necessary to verify that the data subject is proactively deciding to share this information and be aware of the consequences.[146] This would imply that the data subject shall have an effective power to choose whether to disclose or hide the sensitive characteristic (which might not always be the case in an e-proctoring processing). Moreover, the "making public" is generally understood as finding application where the individual makes the information available to the public at large, e.g., on a social network or through

142 See also, Els J Kindt, 'Having yes, using no? About the new legal regime for biometric data' (2018) 34(3) Computer Law & Security Review 523, 531.

143 In this sense, the ongoing negotiations on the Draft AI Act should be used to coordinate the definitions of biometric data under data protection and the new framework and to ensure a higher level of protection – beyond the GDPR - when systems, like biometric categorisation or tools intended to assess students, are designed. See, Lydia Belkadi 'The Proposed Artificial Intelligence Act and Biometric Systems: A Peek Into the Conceptual Maze (Part II)' (*KULeuven - Citip Blog*, 3 November 2021) <https://www.law.kuleuven.be/citip/blog/the-proposed-artificial-intelligence-act-and-biometric-systems-part-ii/> accessed 1 February 2023. Both biometric and AI-based systems to assess students are categorised as high-risk AI systems in the Draft AI Act.

144 As stressed, for example, by the European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA 2020), 8. See also, Kindt (n 142).

145 See, Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' (2021) 11(2) International Data Privacy Law 107. For instance, with reference to the specific case of video surveillance, the EDPB clarified that: "the mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data related to him or her". EDPB (n 65) para 69.

146 Interestingly, the General Advocate Rantos has noticed that Art. 9(2)(e) GDPR requires an "explicit act" of making personal data public and that such condition "is very similar to that of the data subject's consent". Case C-255/21 *Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v Bundeskartellam* [2022] ECLI:EU:C:2022:704, Opinion of AG Rantos, fn 50.

mass media.[147] On the contrary, the data acquired by an e-proctoring tool are meant to be processed within a closed environment and usually visualised only by a restricted number of authorised persons.[148] Hence, this lawful basis might not be fitting for the context at stake.

119 Moreover, even if not fully tested in the decisions examined, the principle of fairness (Article 5(1)(a) GDPR) and the tool of the DPIA could be used to address the potential discriminatory effects caused by e-proctoring and not only when the discrimination is based on an existing protected ground under data protection or anti-discrimination law (e.g. race, religion, etc.). For instance, situations of socio-economic discrimination do not fall within the existing boundaries of protection (unless it can be linked with, e.g., a certain ethnic group) but should nevertheless be taken into account by a HEI before deciding to deploy remote invigilation for an exam.

120 In parallel, we have seen that anti-discrimination law could address other serious pitfalls of e-proctoring systems, for instance, the failure of facial recognition tools for authenticating students. Based on the evidence collected and the studies emerging in this field, it was possible to build a case of *prima facie* discrimination before the Equality body in the Netherlands. The claimant showed that the tool used by her university did not let her join the exam unless she shone some powerful light directly at her face. It is yet to be seen how the university will discharge its burden of proof.

121 All in all, the adoption of an e-proctoring system requires the universities to perform a careful assessment of the characteristics of the software, the concrete modalities of deployment in the specific context, and the guarantees offered by the provider. As controllers, they should also evaluate the processing they are enabling when using a commercial third-party platform. The latter often perform further purposes with the data collected that are not necessarily in line with the institutional goals of HEIs. Many of these platforms are also based in the US, and the transfer towards this country is still highly problematic.

122 As we have pointed out in our analysis, some features, or some concrete implementations of such software in the educational environment have been sanctioned by DPAs and challenged by the NIHR, making the adoption of such tool much harder in practice, especially now that the pandemic is over.

123 To a large extent, the current legal framework has proven responsive to counter the unlawful use of e-proctoring tools by universities. The main notable exception is represented by the Dutch saga, where the judges adopted a debatable restrictive interpretation of some GDPR provisions, and the burden of proof carried by the claimants has practically disadvantaged the students.

124 Notably, and from a procedural point of view, we have argued that GDPR collective actions can become a useful tool in contesting e-proctoring systems. We have noted that GDPR has the potential to tackle and counter harms suffered by specific groups of students or even by the student body as a whole. However, as shown in the German and Netherlands cases, while different entities brought forward (admissible) GDPR claims against the HEI's decisions to introduce e-proctoring systems, the cases were ultimately dismissed. The examined case law has also revealed disparities in both collective action processes and rules between different Member States. National procedural rules are coupled with GDPR and implementation laws, which all create a complex matrix of rules to navigate. These disparities are far from creating the necessary clarity needed for representative bodies to ensure the success of their claims.

125 Now that the emergency is over, the questions that remain open are what lessons have been learned and how should universities approach the decision-making process about edTech tools more generally?

126 The comparative analysis of the DPA's decisions and the case law allowed to identify the controversial issues emerging in the different cases. This critical overview is functional to reflect on the reasons why e-proctoring has been contested, and to imagine how to develop edTech tools which are not only lawful but also able to guarantee the full exercise of the right to education and adequately reflect the *ethos* of the university.

127 We contend that while edTech tools may offer a series of advantages in terms of efficiency and productivity, they are rarely neutral instruments: they interact with the environment, people, and institutions. This mutual interplay in turn affects

147 Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of special categories of personal data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020), 378.

148 However, it has to be noted that in a case from 2002, the CJEU touched upon this issue although with reference to Regulation 45/2001 (which establishes data protection rules when the processing is performed by European institutions and bodies), implicitly including a closed group like an organisation in the notion of "public" (see, Case T-320/02 *Monika Esch-Leonhardt and Others v European Central Bank* [2004] ECLI:EU:T:2004:45, commented in Dove and Chan (n 143)).

how these elements interact with each other and, ultimately, how education is provided. Hence, their adoption should involve the consultation of all the affected parties. How to ensure this democratic participation in the governance of institutions in a meaningful way (not just a ticking box exercise) and make sure that minority voices are heard is a crucial aspect that universities should fully embrace.

Acknowledgments

This research was supported by the British and Irish Law Education and Technology Association (BILETA) Research Awards 2021 and the School of Law of the University of Aberdeen. The views expressed in this paper are those of the authors only.

The authors would like to thank all the participants attending the workshop "Law and the Digital Classroom", organised in Lisbon at the NOVA School of Law on the 12th of July 2022, for their comments and suggestions on the draft version of this paper.

A special thanks to Dr Guido Salza for his support in constructing the survey and analysing the e-proctoring questions within the BILETA project 'Zooming in on Privacy and Copyright Issues in Remote Teaching', Dr Maria José Schmidt-Kessen for the helpful discussion on the Danish sources, and Mr Jamie Murphy for the final proofreading of this work.

Annex I - Summary of all the e-proctoring-related decisions mentioned in the paper

Denmark, Datatilsynet (DPA) - 2018-432-0015 ("Denmark 1")

The DPA launched an investigation after learning from the media that various high schools were using an automated e-proctoring system.

The DPA recognised that a high school can, in principle, use the e-proctoring tool to process students' personal data to prevent cheating in online exams. Such processing could be grounded in Art. 6(1)(e) GDPR (necessity to perform a task in the public interest). However, the DPA expressed serious concerns about the lack of an appropriate assessment of the necessity and proportionality of the processing for the declared purpose. Additionally, the investigated school failed to provide an adequate lawful basis for the processing of sensitive data which can be collected by the e-proctoring tool (the necessity for substantive interests' reasons, referred to in Section 7(4) of the Danish Data Protection Act, was not deemed an appropriate ground because it has a narrow scope of application, such as processing for the purpose of a serious threat to health).

Finally, the School did not provide specific information to the students about the e-proctoring processing.

Denmark, Datatilsynet (DPA) - 2020-432-0034 ("Denmark 2")

After receiving a phone inquiry, the DPA launched an investigation concerning the use of a recorded e-proctoring tool by a Danish university in the spring of 2020. The DPA ascertained that the processing involved personal data of approximately 330 examinees in the form of audio and video recording of the students, screenshots of their desktops and browsing history, and IDs. No facial recognition software was used: students' identity was manually checked at the start of the session.

The DPA found that:

- The processing was based on a lawful ground (Art. 6(1)(e) GDPR). E-proctoring was necessary for the performance of a task in the public interest (i.e. to supervise students during exams and prevent cheating) in connection with one specific test assessing the acquisition of basic knowledge and concepts (one answer correct with no space for further elaboration);

- The university performed an assessment about the nature, form, and purpose of the processing, showing that the need to guarantee the integrity of exams and the modalities of the online invigilation were limited to the processing of necessary data, and respected the principles of lawfulness, fairness,

transparency, and data minimisation;

- The DPA considered that the processing of sensitive data during the examination was, in principle, unintentional and that the necessity for substantive interests' reasons did not constitute an appropriate lawful basis for the e-proctoring processing (Section 7(4) Danish Data Protection Act). To prevent the processing of special categories of data, the DPA recommended the university to inform and encourage students taking measures to minimise the unintentional sharing of sensitive information during the session;

- Overall, the university has provided information about the processing in a concise, timely, and transparent way. However, additional information should have been provided on the recording of the browsing history during the exam, the measures to prevent the unintentional sharing of sensitive information and, how to configure the browser in the most privacy-preserving way; and

- The university performed an assessment of the security risks and available e-proctoring options (choosing the least intrusive). The DPA deemed the assessment and the measures adopted (e.g. encryption) to be adequate. After the DPA noted the lack of two-factor authentication for access control, the HEI addressed the issue.

Germany, OVG Nordrhein-Westfalen, Beschluss vom 04.03.2021 - 14 B 278/21.NE

The Gesellschaft für Freiheitsrechte (GFF) filed, together with a student, an emergency application to the Higher Administrative Court of North Rhine-Westphalia claiming several data protection violations. The aim was to ensure that the examination scheduled for shortly after would not be recorded, but, at most, observed by means of video transmission.

The Court rejected the claim on procedural grounds. In particular, it stated that whether the recording and temporary storage of the audio and video connection and thus the processing of personal data by Art. 6(1) GDPR is justified, this cannot be conclusively assessed in interim legal protection proceedings.

Greece, Αρχή προστασίας δεδομένων (DPA) - Decision 50/2021

The Hellenic Ministry of Education and Religions Affairs (the Ministry) decided to promote and implement a method of distance learning by technological means for students in primary and secondary education during the COVID-19 lockdown period. The teachers' union contested the legality of that government decision at the Hellenic DPA. While the DPA considered this method legal, it found that the Ministry had failed to consider a number of factors and risks in relation to the rights and freedoms of the data subjects when conducting a DPIA.

Recognising the need for distance education, the DPA provided an opinion to the Ministry to address the flaws and shortcomings. The DPA noted in its decision multiple GDPR violations, namely of provisions related to the lawfulness of processing and the obligations of the data controllers. It then called on the Ministry to address and remedy these violations in the coming four months. After that period, the Ministry is called to report its updates to the DPA.

Iceland, Persónuvernd (DPA) - 2020112830

After receiving a complaint by a student, the Icelandic DPA assessed the lawfulness of the online monitoring of a remote examination. The Authority dealt with three main legal issues: a) lawful legal basis for processing; b) data security; and c) transparency.

The Icelandic DPA stated that:

- Concerning the lawful ground for processing, consent may not be an adequate basis for processing in the present case due to the nature of the relationship between the university and the students. However, the DPA considered that consent to the online monitoring of the exam was not forced as it was possible to take the examination in person at the university. According to the Authority, the basis for processing should be the legitimate interest of the controller (Art. 6(1)(f) GDPR);

- As to the security of the personal data, the technical and organisational measures implemented by the university were appropriate, taking into account the existing data processing agreement between the service provider and the university; and

- The university violated the principle of transparency, as there was a lack of information duties concerning the legal basis, purposes, security measures, and the student's data protection rights related to this processing.

Italy, Garante privacy (DPA) - Ordinanza 9703988 - 16 Sep 2021

Following a university student's complaint regarding the use of an automated e-proctoring service with flagging features to spot cheating behaviours, the DPA investigated the lawfulness of such processing.

The DPA stated that:

- The processing of personal data for conducting remote exams is lawful if it is necessary "to comply with a legal obligation to which the data controller is subject" or "for the performance of a task carried out in the public interest or in connection with the exercise of official authority" (Art. 6(1)(c) and (e) GDPR. Consent (Art. 6(1)(a)) or contract (Art. 6(1) (b) GDPR) cannot be considered valid legal bases for such processing. Special categories of data could be processed based on Art. 9(2)(g), however, the DPA recognised that the ground for processing biometric data and profiling was lacking;

- The privacy policy did not contain all the information required by the GDPR (e.g., the lack of mention of all the processing, such as tracking the student's behaviour during the test, subsequent profiling based on such data, and audio-video recording of the test). Information on the retention period was too vague, while the information on data transfer to third countries, and the logic of the supervision system, was missing. Moreover, the information available was not transparently presented;

- The principle of data minimisation was not respected. For example, the processing of information concerning the applications running on the student's terminal was not necessary for the purpose of ensuring the proper completion and validity of the test;

- The university transferred personal data, including biometric data, to a third country (the US) without proving that the transfer complied with the GDPR. The transfer in the US was based on SCCs. However, it was considered unlawful as the technical and organisational measures were not sufficiently described in the contract and, as a consequence, were not in line with the requirements established by the same SCCs; and

- The DPIA was not adequately performed, in particular with reference to the evaluation of the necessity and proportionality of the processing and of the risks to the rights and freedoms of the data subjects. Moreover, there was no mention of the appropriate measures to address existing risks, and to mitigate them.

The Netherlands, Rb. Amsterdam - C/13/684665 / KG ZA 20-481 ("Netherlands 1")

The introduction of online proctoring systems to invigilate exams happening remotely was decided due to the COVID-19 lockdown. The software monitored students while they took their exam from home. The software recorded the user's webcam, microphone, internet traffic, and inputs.

The Amsterdam Court of First Instance rejected the request by student representatives and an individual student for a preliminary injunction against the use of the above-mentioned e-proctoring software. The Court ruled that measures against COVID-19 did not allow for a suitable alternative. Also, it examined the GDPR compliance of the software and found the data processing by the university was based on Art. 6(1) (e) GDPR (necessity to perform a task in the public interest or in the exercise of official authority), and that the processing complied with the requirements set by the GDPR.

This being a preliminary injunction, the Court also examined the admissibility of the student council in bringing forward these claims on behalf of the university student body. The Court applied section 3:305a of the Dutch Civil Code, and concluded that only a foundation or association with full legal capacity can institute legal proceedings that protect similar interests of other persons, insofar as they represent these interests under its Articles of Association and these interests are sufficiently safeguarded. In that regard, and according to the court, the student councils are not a foundation or association with full legal capacity.

The Netherlands, Gerechtshof Amsterdam - 200.280.852/01 ("Netherlands 2")

This case is the appeal of the Netherlands 1 preliminary decision. It concerns a civil dispute between the Central Student Council (CSR) at the university, the Student Council at the Faculty of Economics and Business (FSR), and an individual student against the defendant, the university.

The preliminary injunction was filed first, and the District Court of Amsterdam ruled in favour of the university, finding that the government's COVID-19 measures did not allow for suitable alternatives and that the surveillance had a legal basis in Art. 6(1)(e) GDPR. The plaintiffs appealed to the Court of Appeals Amsterdam Court.

The plaintiffs claimed that the introduction of the e-proctoring system chosen by the university breached the GDPR in several respects. They claimed

that it was unnecessary to introduce monitoring software, that more data than necessary was processed, that there was a lack of transparency and security, and that sensitive personal data was processed without a legal basis.

The Court found that the university successfully demonstrated that the use of the software was necessary for the performance of the task of exercising official authority under Art. 6(1)(e) GDPR. It also found that the plaintiffs failed to prove that its use violated the principles of purpose limitation and data minimisation. The plaintiffs had argued that less intrusive alternatives could be used, but the court placed the burden of sufficiently presenting these feasible alternatives to them. The plaintiffs argued that the university had not provided full insight into how the proctoring software detects cheating. However, the Court held that the plaintiffs had not plausibly demonstrated that anyone not authorised by the university to view the video and audio, such as the service provider or US intelligence agencies, could gain access. In addition, the claimants argued that the images collected could be sensitive personal data for which there was no legal basis for collection. The Court ruled that images identifying an individual could not simply be sensitive personal data revealing, for example, religion or race. The court could not foresee that the images would be used by the university to discriminate against test takers based on protected characteristics.

While the Court acknowledged that it was disruptive that students could not go to the bathroom during online exams, it noted that the same was true for on-site exams. The Court therefore held that it could not consider this complaint in assessing the legality of online examinations.

The CSR sent a letter to the university's Executive Board, which was described in the judgement as "unsolicited advice". In this letter, the CSR strongly opposed the use of e-proctoring, recommended against the use of room scanning, and advised that the university provide students who cannot/would not use proctoring with alternative means of taking exams without delaying their studies.

The plaintiffs also argued that e-proctoring violated Art. 8 ECHR. The Court considered whether the interference with privacy by proctoring was justified under Art. 8(2) of the ECHR. To do this, it looked back at the reasoning it had used in assessing the lawfulness of proctoring in relation to the GDPR. It held that it was plausible that the interference with privacy was necessary in a democratic society and could be considered proportionate.

From a procedural side, the plaintiffs alleged that the university had violated the law by changing the so-called Teaching and Examination Regulations (Onderwijs- en Examensregeling, "OER") without following due process. Art. 7.13 of the Higher Education and Scientific Research Act (WHW) requires that every Dutch higher education program adopts an OER. A higher education institution may also adopt a OER for a group of programs. The Court found that the university had not breached any procedural rules in deciding to introduce e-proctoring. Specifically, the Court referred to Art. 7.13(2)(l) WHW which allows the Board of Examiners to depart from OER in special circumstances. The Court found that the COVID-19 restrictions qualified as a special case where the exam board is allowed to deviate from the OER.

The Netherlands, College voor de Rechten van de Mens (Netherlands Institute for Human Rights), Decision 2022-146 ("Netherlands 3")

A university student called on the Netherlands Institute for Human Rights (NIHR) to establish that the use of the e-proctoring software was discriminatory. Specifically, the student argued that she was discriminated against due to her skin colour when she was using the contested software. The student had trouble logging in the exams and was only able to do so when shining a direct light on her face. According to the preliminary decision, the person claiming discrimination has succeeded in this for two reasons. First, the parties agree that the anti-cheat software hindered the woman. Second, there is academic research showing that face detection software generally performs worse on darker skinned individuals. Taken together, these facts are sufficient for a presumption of indirect discrimination on the basis of race.

The NIHR established that the student had provided sufficient facts from which it can be assumed that the university had indirectly discriminated on the grounds of race by using anti-cheat software for the supervision of exams. If there is a suspicion of discrimination, the university must prove that it has not acted in violation of the law. The Board considers that the university has not provided sufficient evidence for this. The intermediate judgement gives a 10-week deadline to the university to provide evidence that there was no discrimination.

Portugal, Comissão Nacional de Proteção de Dados (DPA) - Deliberação/2021/622

The DPA carried out a preventive assessment of the lawfulness of an e-proctoring tool with flagging features to spot cheating behaviours that were

meant to be used by a Portuguese university (the reference was anonymised by the DPA).

The decision focuses on four main aspects: the application of the principles of i) purpose limitation; ii) data minimisation; iii) the legal basis of processing; and iv) the lawfulness of data transfers to the US.

The DPA affirmed that the rectoral order authorising the e-proctoring tool did not provide specific criteria about the cases where such a tool could be used. The lack of such criteria led to the violation of the purpose limitation principle, as the processing purpose was not sufficiently specified, and of the data minimisation principle, as the discretion of the teaching staff concerning the use of such a tool may lead to process data not necessary for the stated purpose.

Furthermore, the Authority doubted that the legitimate interest (Art. 6(1)(f) GDPR) is the correct legal basis for processing. The DPA found that the legitimate interest basis was not used correctly in the present case. In particular, the Authority stated that: i) the data controller did not carry out the balancing test between the legitimate interest at stake and the rights and interests of the data subjects; and ii) the processing at stake was particularly important, as it involved profiling and biometric data.

However, the DPA, taking into account the public interest at stake, stated that Art. 6(1)(e) GDPR should be applied, according to the rules provided for by Art. 6(2) GDPR, concerning national rules on processing for public interest purposes.

In any case, the Authority affirmed that the processing concerning video and audio recordings of students' behaviour, based on consent, was unlawful. The Authority considered that the consent did not meet the requirements set forth by the GDPR, as students are obliged to give their consent if they want to take exams.

As to extra-EU data transfers, the DPA applied the CJEU rationale in C-311/18 Data Protection Commissioner/Maximilian Schrems v. Facebook Ireland, 16 July 2020. It stated that students' personal data must not be transferred to the US, as there was a lack of additional measures preventing the access to the transferred personal data by the US authorities.

Hence, the DPA concluded that the e-proctoring processing at stake violated the principle of lawfulness, purpose limitation, and data minimisation (Art. 5 (1)(a)(b)(c) GDPR) and ordered the e-proctoring provider to destroy the personal data collected through the tool.