ISSN 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Vol. 1, n. 1/2020

Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education

Chiara Angiolini, Rossana Ducato, Alexandra Giannopoulou, Giulia Schneider

Pacini Giuridica

Articles

Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education

Chiara Angiolini[*], Rossana Ducato[**], Alexandra Giannopoulou[***], Giulia Schneider[****]

Abstract

Due to the spread of Covid-19 in the first months of 2020, almost all Universities across Europe had to close their buildings and migrate online. This rapid shift towards the provision of education online has been characterized by the externalization to and use of third-party service providers, such as Zoom, for ensuring the continuity of learning. The 'platformisation' of education, however,

[*] Chiara Angiolini, PostDoc Researcher, University of Trento.
[**] Rossana Ducato, Lecturer in IT Law & Regulation, University of Aberdeen.
[***] Alexandra Giannopoulou, Researcher, Institute for Information Law (IViR), University of Amsterdam.
[****] Giulia Schneider, PostDoc Researcher, Sant'Anna School of Advanced Studies (Pisa, Italy).

raises several concerns, especially from a privacy and data protection perspective. The aim of this paper is to map the possible data protection risks emerging from the platformisation of education by focusing on the most pressing points of friction with the European data privacy regime: 1) allocation of roles and responsibilities of the actors involved; 2) transparency of the processing and possibility to effectively exercise data subjects' rights; 3) extra-EU data transfers after Schrems II; 4) challenges of e-proctoring systems.

The paper argues that the implementation of the right to privacy and data protection in remote teaching is not merely an issue of compliance, but a substantial measure that Universities shall ensure to guarantee the fundamental rights of our students and colleagues. The paper concludes with recommendations for ensuring a safer and fairer remote teaching experience, also discussing long-term strategies beyond the emergency and beyond the mere compliance with the General Data Protection Regulation.

Keywords

Privacy – Data protection – GDPR – EdTech – Emergency Remote Teaching – digital education – online platforms

Table of contents

Introduction

Due to the spread of Covid-19 in the first months of 2020, schools and higher education institutions (HEIs) were among the first places to experience the lockdown. From Italy to the UK, from Spain to Greece, almost all Universities across Europe had to close their buildings and migrate online[1].

[1] See, the European University Association, *Briefing: European higher education in the Covid-19 crisis* (September 2020) https://eua.eu/downloads/publications/briefing_european%20higher%20education%20in%20the%20covid-19%20crisis.pdf (last

Despite the use of online tools and educational technology ("Edutech" or "EdTech") was nothing entirely new[2], the pandemic dictated a paradigmatic digital turn in education, promptly labelled as Emergency Remote Teaching (ERT)[3]. If compared to pre-pandemic online learning, ERT presents the distinctive and unknown convergence of three main elements:
1) The velocity of the migration. In order to ensure the continuity of education, traditionally non-distance education providers had to switch online in a matter of days. HEIs tended to use third-party services already in their portfolio or to search for popular options available on the market. In either case, there was little time to consider all the possible EdTech options and their consequences, including the legal ones.
2) The volume of activities that had to be transferred online. If the repository hosted on the University servers was enough for sharing teaching materials (such as slides and suggested reading), with ERT the HEIs have started relying on digital means to carry out very diverse aspects of education activities, such as teaching, correcting assignments, holding school meetings, running PhD defences, etc.
3) The variety and combination of tools to be used for synchronous and asynchronous teaching, research, and administrative work. Especially at the beginning of the pandemic, no EdTech online service offered all the features requested for ERT (e.g. videoconferencing tools, hosting space, forums, videomaking, automated captioning, students record systems, etc.). Therefore, many institutions and teachers had to do "patchwork", searching for the right tool, the right add-on, and then checking its compatibility requirements.
As an effect, these "3Vs" (velocity of migration, volume of activities, and variety of tools) have resulted in a general shift towards the 'platformisation' of education, i.e. a major reliance and outsourcing of tasks to third party online platforms. As a matter of fact, the vast majority of Universities did (and still do) not have a technological infrastructure designed to fully support academic life online[4]. Therefore, the recourse to third party providers (from Zoom to Skype, from MS Teams to Whatsapp) was a path followed by many Institutions during the lockdown.
The use of third-party providers is not, by itself, an inherent shortcoming in an educational environment. This situation requires, however, careful scrutiny. Some of the platforms used are not specifically designed for education, the vast majority offer standard services that cannot be customised according to the specific needs of HEIs, and the platforms' business

accessed: 11 November 2020).

[2] There are already several accredited online Universities and also "traditional not-distance education providers" have been delivering part of the academic activity online (e.g., skype sessions with students, online communities for sharing teaching materials, virtual student record systems, etc.).

[3] C. Hodges, S. Moore, B. Lockee, T. Trust, A. Bond, *The Difference between Emergency Remote Teaching and Online Learning* (2020) 27 *Educause Review*, https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning (last accessed: 11 November 2020)..

[4] There are some notable exceptions however. For example, the Italian GARR consortium (https://www.garr.it/en/garr-en) or the portal "Fare" of the Politecnico di Torino (https://fare.polito.it/) Last accessed: 11 November 2020

model is often incompatible with the public interest goals of Universities. Most importantly, the 'platformisation' can affect the level of control that HEIs can exercise over the delivery of education and, as a consequence, over the lawful processing of students' and teachers' data. While much attention has been, rightly, dedicated to the pedagogical challenges, we intend to contribute to the debate on ERT by outlining its legal implications, in particular from a data protection perspective. We argue that the implementation of the right to privacy and data protection in the ERT environment is not merely an issue of compliance, but a substantial measure that Universities shall ensure to guarantee the fundamental rights of our students and colleagues. The right to privacy and data protection are in fact constitutional enablers of other fundamental rights such as the freedom of expression, education, research, and interests, as our digital well-being[5]. To this end, the paper intends to map the possible data protection risks emerging from the platformisation of education, by discussing four topical points of friction with the European data privacy regime.

Firstly, the roles of the entities responsible for the data processing in an ERT context are outlined, showing that data collected for educational purposes are often subject to further processing. The unclear definition of purposes of the processing and allocation of roles and responsibilities between the University and the platform create a situation of opaqueness that can harm students and teachers directly. Therefore, the respect of the transparency principle is examined by highlighting the practical difficulties in exercising data subject rights as described in the GDPR.

Following this analysis, the paper will assess the implications brought by the recent *Schrems II* decision. The latter, invalidates the adequacy decision allowing EU-US data transfers and questions the validity of other transfer mechanisms as well. Thus, such a decision is a serious warning against the platformisation trend in education, considering that cross-border data flow is a common feature of providers' business models in this sector. Later on, we turn our attention to the concerns raised by the use of 'e-proctoring' services, a growing set of information technology tools adopted for ensuring digital invigilation of students during exams. Even though such tools are not prohibited as such and, in a first national decision, have been considered compliant with GDPR principles, we question whether we should seek less intrusive solutions.

Finally, the paper proposes recommendations for ensuring a safer and fairer remote teaching environment: it discusses possible ways forward to support the implementation of edTech in a short, medium, and long-term perspective beyond the emergency and beyond mere compliance with the GDPR.

[5] G. Comandè, *Tortious Privacy 3.0: a Quest for Research*, in J. Potgieter, J. Knobel, R. M. Jansen, *Essays in Honour of Huldigingsbundel vir Johann Neethling* (Lexis Nexis, 2015), pp. 121-131.

1. Data protection roles: Untangling the powers and responsibilities of actors involved in remote teaching

When a University builds its remote teaching infrastructure relying on an external service provider, it must choose how to organise the processing of data concerning students and teachers. This Section will consider one main aspect of this choice: the allocation of the data protection roles among different actors (students, teachers, the University, and the service provider). This issue is of particular importance because that distribution of roles has significant consequences on the attribution of data protection responsibilities and duties.
Considering the processing of data for educational purposes, the allocation of data protection roles should be generally articulated as follows (Fig. 1).

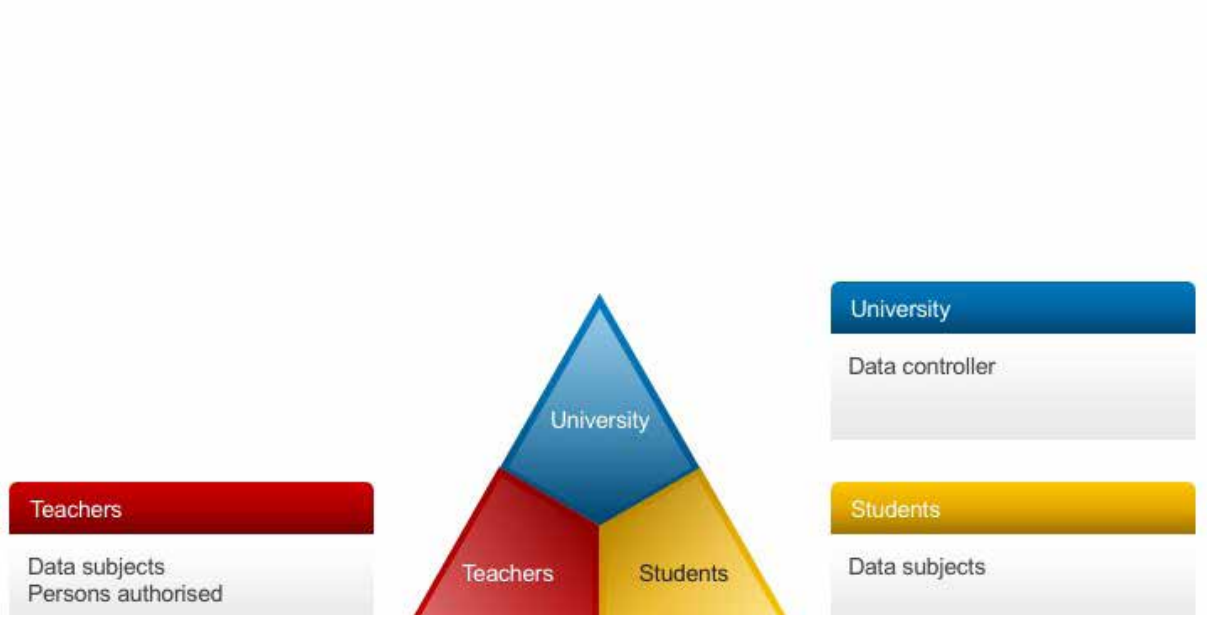

Figure 1. Basic scheme of data protection roles in the processing for education purposes.

Universities are data controllers, i.e. the entity determining the purposes and the means of the processing, while students are data subjects. Teachers can be considered data subjects vis-à-vis the University, when the latter processes data concerning them (e.g. their email address for sending communications, their workload, their pay slip, etc.). They can also vest another data protection role, as 'persons authorised' under Art. 29 GDPR. In other terms, when teachers have access to students data (e.g. for grading and assessment, teaching, tutoring, etc.), they do so on

instructions from the University-controller[6]. However, the shift toward ERT and the reliance on platforms affects this general scheme by altering the role of teachers and that of Universities.
With regard to the first aspect, teachers could be considered data controllers in certain circumstances. For example, at the beginning of the lockdown, lacking sufficient (or any) instruction by Universities on the tools to use for remote teaching, many teachers decided to act autonomously, searching for solutions that would allow them to ensure delivery of their courses. By choosing the means and the purposes of processing, they became *de facto* controllers[7]. In this way, they have assumed, often unaware, the corresponding responsibilities established at Art. 28 GDPR.
The introduction of the platform in the educational cycle also affects the University's position. When HEI partially or entirely outsources the processing of data to a third-party provider, the latter should be appointed as data processor (see, Fig. 2)[8].

Figure 2. Data controller and data processor roles when the purpose of the processing is the provision of educational services.

[6] The definitions of data protection roles are provided by Art. 4 Regulation EU 2016/679/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC of 4 May 2016, General Data Protection Regulation (hereafter GDPR) [2016] OJ L 119/1.

[7] The recent European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_it) adopted in the version for public consultation on 2 September 2020, may result particularly useful for determining, in each specific case, data protection roles.

[8] Processor is defined at Art. 4(1)(8) GDPR as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Within this context, Universities must ensure that the platform offers appropriate safeguards for the protection of data and, in general, guarantees GDPR compliance[9]. Nowadays, the importance of this duty is becoming particularly pressing. Several security issues have been uncovered from the extended use of EdTech for ERT, such as hackers intruding meetings, a phenomenon known as "zoombombing"[10].

The controller shall provide the processor with instructions about processing, through an agreement or another act. However, in the definition of the data processing agreement the platform may play the most active and powerful role, with the consequence that the University formally determines purposes and means of processing, but the platform exercises a substantial power in planning data processing and its limits.

The schema according to which the University is a controller and the platform a processor (as in Fig. 2) is only one possible configuration and not necessarily the most common one. If we consider the business model of many of the digital providers (education-native or repurposed by users for education), we will find that online platforms usually perform further processing on the data collected within an ERT context for their own purposes[11]. Not entering into the lawfulness of such a processing for the moment, but only considering the data protection roles, in such a case the platform may be classified as controller for the processing of data for its own purposes, as it determines the means and purposes of this specific processing. Meanwhile, the University can act as a joint controller for certain processing operations.

In this respect, the recent European Data Protection Board (EDPB) guidelines 7/2020 on the concepts of controller and processor in the GDPR are of particular interest[12], jointly with the CJEU's case law[13]. As to the Guidelines, the EDPB stated that joint controllership exists not only in cases of common decisions taken by two or more entities concerning the means and the purposes of processing, but also where those decisions are the result of *converging decisions* by two or more entities[14]. According to the EDPB, an important element of joint controllership is that the processing would not be possible without both parties' participation in the sense that the processing by each party is "inextricably linked"[15]. The CJEU *Fashion ID* case is worth mentioning to this end. In that case, the Court stated

[9] As established by Art. 28 GDPR.

[10] On Zoom's privacy issues is of particular interest the message published by the CEO of Zoom, available at: https://blog.zoom.us/a-message-to-our-users/ (last accessed: 24 August 2020).

[11] In that regard, for analysis of some of data protection policies of some of the most popular online platforms see R. Ducato et al., 'Emergency Remote Teaching: A Study of Copyright and Data Protection Policies of Online Services (Part. II)', (*CopyRightBlog*, 4 June 2020) http://copyrightblog.kluweriplaw.com/2020/06/04/emergency-remote-teaching-a-study-of-copyright-and-data-protection-policies-of-popular-online-services-part-ii/ (last accessed: 11 November 2020).

[12] See European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, cit.

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

[14] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', cit., p. 3.

[15] *Ibid.*, p. 3. See, with specific regard to service providers, paras 79-82.

that the operator of a website that embeds on that website a social plugin transmitting to Facebook personal data of the visitor shall be considered a controller for the operations consisting of the collection and transmission of visitor's data[16].

Thus, in light of *Fashion ID* and of the EDPB Guidelines, if the platform processes data collected within educational activities for further purposes, the University might be classified as a joint controller for the transmission of that information, because without the processing of data for educational purposes, where the University is a controller, the platform may not have access to data, and may not process them for other purposes. Therefore, the processing by each party may be defined as "inextricably linked". This conclusion is supported also by the fact that the University complies with some of the criteria elaborated by the EDPB in order to affirm that an entity is a controller: the University participates in the definition of what kind of personal data is collected and further processed and the categories of data subjects[17].

In case of joint controllership, it is necessary to contractually establish the allocation of responsibilities between the controller and the processor and towards the data subjects. This (contractual) agreement "would provide certainty and could be used to evidence transparency and accountability"[18]. In cases where multiple actors are engaged in data processing, it is recommended that transparency and accountability would be better served if the joint controllers "organise and agree on how and by whom the information will be provided and how and by whom the answers to the data subject's requests will be provided. Irrespective of the content of the arrangement on this specific point, the data subject may contact either of the joint controllers to exercise his or her rights in accordance with Article 26(3)"[19]. In that regard, according to the EDPB, "requiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject, that would be contrary to the objective of facilitating the exercise of their rights under the GDPR"[20].

Nevertheless, as the "assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing"[21], in each case a concrete assessment must be done, taking into account all relevant factual circumstances in order to determine if the two entities are determining both and jointly the means and/or the purposes of processing.

---

[16] See, Case C-40/17. For an overview of the most important aspects of that judgment, see: J. Globocnik, *On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID* (2019) 50 IIC 1033.

[17] *Ibid.*, pp. 46-48.

[18] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, cit., p. 43.

[19] *Ibid.*, p. 44.

[20] *Ibid.*, p. 45.

[21] *Ibid.*, p. 49.

Figure 3. Data protection roles when the processing is jointly determined.

2. Setting the boundaries of processing: Determining the legal basis and purposes and enforcing data subjects' rights

The attribution of data protection roles to the actors involved in remote teaching implies the mutual acknowledgement of power and responsibility in setting boundaries to data processing. Thus, it is essential that the legal basis and purposes for processing be determined according to GDPR imperatives. Furthermore, these same actors would be liable to ensure that data subjects rights are respected[22].

Universities, as controllers or joint controllers, determine both the purposes and the legal basis for processing. Beyond compliance, that planning is informed by and constitutes a political and cultural choice for the University. Consequently, when Universities rely solely on an external online platform, they need to perform an adequate assessment not only of the suitability of the tool for educational purposes, but also of the guarantees that the platform offers in terms of data protection. An overview of the processing activities is usually contained in the privacy policies of such platforms. However, as previously explained[23], these policies and overall applied business models do not always align with the Universities' objectives.

[22] As highlighted by the CJEU, the concept of 'controller' is defined broadly in order to ensure "effective and complete protection of data subjects": Case C-131/12 *Google Spain and Google* [2014] ECLI:EU:C:2014:317, para 34; Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, [2018] ECLI:EU:C:2018:388, para 28; Case C-40/17, *cit.*, para 70.

[23] R. Ducato et al. (n. 11).

As for the purposes pursued by Universities with the ERT processing, educational purposes are the obvious candidate. For those purposes, as the Italian Data Protection Authority has stated[24], consent does not appear to be the appropriate legal basis for processing. Therefore, the relevant lawful bases for the processing would be the public interest or, depending on the jurisdiction, contractual necessity.
Conversely, when processing of data is performed also for secondary purposes, such as promotional ones, it would need to be anchored to the lawful basis of legitimate interests[25]. In any case, personal data can only be processed for the specified, explicit lawful purposes for which they were collected, and cannot be further processed in a manner incompatible with those purposes (see Articles 5 and 6 GDPR).
This also applies when Universities use external services for providing remote teaching. Specifically, HEIs would have to carefully consider if these platforms process students' or teachers' personal data for independent purposes (e.g. marketing), and if those purposes are compatible with the purposes of data collection. Beyond compliance and considering the importance of the definition of the data processing purposes for the cultural and institutional policies, it should be highlighted that the choice of the platform becomes crucial especially when Universities and platforms are considered autonomous or joint controllers, because Universities will not be considered as having any power or direction over these platforms[26]. Moreover, when the University is classified as a controller which engages the platform as a processor, the question arises as to whether these processors could lawfully pursue autonomous purposes without prior controller authorisation[27].
Any institutional choice for the determination of data processing other than the educational purpose should take into consideration the impact that these choices will have on student and teacher activities. In that regard, transparency plays a crucial role in determining how data subjects can interrogate the platforms on which they (as students and teachers) progressively rely to study and to work. The principle of transparency, as enunciated in Art. 5 and Recital 58 GDPR, is a fundamental enabler of data protection. It is an obligation that data controllers are required to take into consideration when building their data

[24] Italian Data protection Authority, act of 26th March 2020, n. 9300784 – "Didattica a distanza: prime indicazioni", https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9300784 (last accessed: 11 November 2020).

[25] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", (9 April 2020) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (last accessed: 24 August 2020). See also I. Kamara, P. De Hert *Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach* (2018) 4, 12 Brussels Privacy Hub.

[26] The lack of legal clarity in the allocation of liability and responsibility between joint controllers does not facilitate this choice for Universities.

[27] As pointed out by the Italian Ministry of Education, where a school decides to rely on an external platform, it will be necessary to appoint the platform as data processor and verify with the Data Protection Officer that only the services related to the remote teaching will be activated. These general indications seems to exclude the possibility that platforms act as controllers. See, Italian Ministry of Education, *Didattica Digitale Integrata e tutela della privacy: indicazioni generali* (4 September 2020) https://www.istruzione.it/rientriamoascuola/allegati/Didattica-Digitale-Integrata-e-tutela-della-privacy-Indicazioni-generali.pdf (last accessed: 11 November 2020).

processing systems, but also it constitutes the foundation based on which data subjects are entitled to exercise their rights, as prescribed in the GDPR.

It has already been highlighted in our previous work[28] that platforms used in ERT have manifested significant shortcomings in fulfilling their transparency obligations. For instance, there is considerable lack of clarity in the personal data collected and the respective lawful grounds of processing that data within the platforms that were part of the study. As a consequence, transparency, as a pillar in facilitating the exercise of data subjects' rights, is effectively hindered. Unclear phrasing, simple mentions of data subjects' rights without further support, all point to a rather superficial approach towards ensuring the respect of these rights. These practices chip away from the available tools that data subjects possess to keep data processing powers in check[29].

Admittedly, the examined platforms differ in their focus and business plan. Some are designed and specialized in the educational infrastructure field, and others are generalistic platforms, with education being remotely linked to their group video functionalities and capabilities. The discrepancy in business goals has undoubtedly impacted the types of personal data collected and the purposes for collecting them.

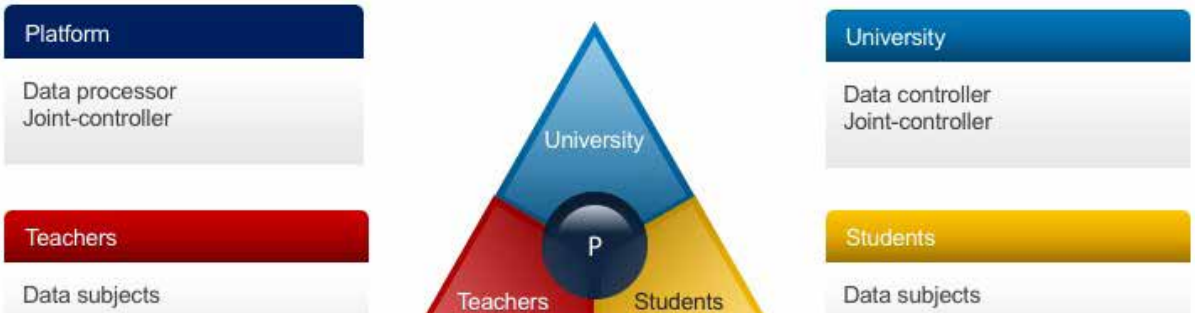

Figure 4. Overview of various data protection roles of actors involved in ERT.

[28] R. Ducato et al. (n. 11).

[29] For a detailed analysis of data subjects' rights, see: J. Ausloos, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection* (Oxford University Press 2020). See also, J. Ausloos, M. Veale, R. Mahieu, *Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance* (2019) 10(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 283.

Keeping accountability within the remote teaching agenda is key in creating a safe environment for data subjects to be able to exercise their rights. Take for instance, the right of access (Art. 15 GDPR). It is difficult to imagine how a data subject would be able to convey the access request focused solely on their remote teaching or learning activity on a given platform. The response from a generalistic platform like Facebook to that data access request appears, for instance, quite challenging. Specifically, the parsing of the data to focus solely on all data collected via the educational/teaching platform activity of the data subject, could likely become cumbersome. Even if that distinction is not relevant to some, it is essential in helping all interested parties hold the platforms accountable for their data processing practices happening during the ERT-provision services. Education-oriented platforms do not appear to provide the level of information required for the exercise of data subjects' rights, at least on an individual level[30]. More focus is placed on deferring to a relevant representative body (often with misleading information), rather than ensuring that the rights demand in question can be effectively responded to[31].

Considering teachers as both data subjects and possible data controllers, their level of engagement towards responding to a data access request will probably be quite limited. This *de facto* controllership puts teachers in a position to carry considerable responsibilities towards their students, a responsibility which the University would traditionally carry. Furthermore, the elements that guided the teacher in choosing a specific platform would most probably have little to do with privacy protection and more with opportunity, usability, prevalence among students and teachers alike, cost of maintenance, inclusivity, etc. Should the remote teaching infrastructure remain unchecked, the dissonance between offline and online education will keep growing. The choice of ERT is fundamental in that regard. With little decision making in the hands of data subjects, they remain subject to terms and policies that risk disempowering them.

In this respect, in order to foster a substantial role of the University as a controller *vis-à-vis* the platforms, associations which represent groups of Universities, at the national or European level, could support HEIs in negotiations with platforms, for example providing guidelines or technical assistance with regard to institutional choices concerning the legal basis for processing and purposes of the latter. Moreover, a debate can be opened on the possibility that a collective entity representing Universities, or a group formed by members (e.g. DPOs) of several Universities would offer guidelines on these agreements, enhancing the role of Universities in shaping the legal architecture of EdTech platforms. While

[30] R. Ducato et al. (n. 11).

[31] Noyb, *Interrupted transmission. Zooming in on video conferencing privacy policies* (02 April 2020) https://noyb.eu/en/interrupted-transmission (last accessed: 11 November 2020).

this solution would enhance Universities' bargaining power, it would have to be balanced against the principle of autonomy of each University[32].

Following the trend of collective engagement in personal data, it would not sound far-fetched to envisage a possibility of a collective agreement, or ensuring the representation through a data subjects' administrative body, that would claim a seat at the negotiating table with regard to the ERT choice or infrastructure design principles. This collective engagement is not in contrast with the GDPR, which recognizes the need for collective means of safeguarding data subjects' rights in Article 80 GDPR. More generally, the nascent calls for collective empowerment of individual data subjects are highlighted in some jurisdictions which envisage data trusts and other forms of intermediaries representing data subject collectives (e.g., data cooperatives, data commons, data collaboratives)[33].

Finally, the importance of teachers' and students' engagement in data protection issues related to ERT platforms cannot be overstated. Their involvement in the negotiations and decision-making processes would ensure *ex ante* empowerment of them as data subjects. This collective data protection exercise would preserve transparency, accountability, and it would ultimately promote the educational and teaching values of each institution.

3. The Platformisation of Education: Life after Schrems II

The majority of platforms employed in ERT expressly relies on cross-border data flows as a fundamental element of their digital service model, in particular for storage and maintenance purposes. As the analysis of the privacy policies of some of the most employed service providers shows[34], until recently, most of these platforms' privacy policies were re-

[32] An example in that regard is the initiative of the Conference of Rectors of Italian Universities, which launched a survey within Universities, in order to negotiate at a collective level with Microsoft, for changing certain (only technical) aspects of Microsoft Teams. See EUA, 'Survey on Digitally Enhanced Learning in European Higher Education Institutions' https://www.fondazionecrui.it/wp-content/uploads/2020/05/Survey_03-04-2020_.pdf (last accessed: 11 November 2020).

[33] On the topic, see S. Delacroix, N. D. Lawrence, 'Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance' (2019) 9, 4, *International Data Privacy Law* 326. These intermediaries are also mentioned under the umbrella term data cooperatives. According to the European Commission, "Data cooperatives seek to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use or potentially solving disputes between members of a group on how data can be used when such data pertain to several data subjects within that group". See European Commission, Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM (2020) 767 final, para. 24.

[34] R. Ducato et al. (n. 11) where the authors have examined the privacy policies of Discord, Facebook, G-Suite for Education, Jitsi Meet, MoodleCloud, Microsoft Teams, Youtube, Skype, Zoom.

ferring to the Commission adequacy decision allowing EU-US data flows, generally known as the *Privacy Shield*[35], as the legal basis for these transfers[36].

However, in the recent *Schrems II* decision[37], the Court of Justice of the European Union invalidated the Privacy Shield and stated that any transfer shall be subject to a specific risk assessment. By ruling so, the Court has discarded the legal basis for the transatlantic data flow, retaining that US law (and in particular the surveillance programs for security purposes) did not grant an equivalent level of protection to the EU.

This decision has two important consequences in the ERT context (and beyond): 1) if the processing relies on the Privacy Shield, it is no longer lawful; 2) if it is done under an alternative legal basis, the HEI, as the controller, must perform the necessary risk assessment considering the law of the "data importer" and the appropriate safeguards that might be implemented to ensure the importer is up to the European standards[38]. Therefore, ERT providers using the Privacy Shield shall now find an alternative legal basis if they have to transfer data extra-EU. For the sake of the discussion, we will try to investigate the possible alternatives and to what extent these can be used in the short-term period. The European Data Protection Board's recently enacted recommendations are just a first step towards the establishment of a very much needed clearer framework regarding extra-EU data transfers[39].

A first option, already proposed by some platforms, is to use SCCs[40]. The latter have been formally upheld by the Court. However, reading carefully the decision of the Court one can reasonably doubt the ability of SCCs to support the extra-EU data transfer of data col-

[35] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L 207 (no longer in force).

[36] This is the case of Moodle, Zoom, Teams, Jitsi, Youtube, Skype, Facebook, Discord. Other Platforms, as Google Meets do not mention the case of extra EU data transfers.

[37] Case C–311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems* [2020] ECLI:EU:C:2020:559, para 201. For a comment see C. Kuner, 'The Schrems II Judgment of the Court of Justice and the future of data transfer regulation' (*European Law Blog*, 17 July 2020) https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ (last accessed: 11 November 2020).

[38] The reference is to the "essential equivalence" standard related to European Union law and in particular to the rights established in the EU Charter of Fundamental Rights. See recital 104 GDPR and Case C–311/18, para 99. See also European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI:EU:C:2020:559, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[39] European Data Protection Board, *Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (10 November 2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[40] SCCs are referred to in the privacy policies of Moodle, Zoom, Teams, Youtube, Google Meet, Facebook. See, here, the list of responses received by Noyb after inquiring the platforms directly. Noyb, 'Opening Pandora's Box: How Companies Addressed Our Questions About Their International Data Transfers After the CJEU's Ruling in C-311/18- Schrems II (25 September 2020) https://noyb.eu/files/web/Replies_from_controllers_on_EU-US_transfers.pdf (last accessed: 11 November 2020).

lected during digital education activities, at least toward the US[41]. First, SCCs are contracts, this means that they only bind the parties. Contractual measures do not prevent third parties, as public authorities, to access transferred data and do not establish effective remedies for data subjects *vis à vis* those third parties[42]. That is why the Court of Justice concluded that it might be necessary for controllers, especially in the case of transfers towards the US, to provide supplementary guarantees to ensure that data subjects will enjoy an equivalent level of protection[43]. What these supplementary guarantees should be is a question that was left open by the CJEU. The EDPB's Recommendations advise controllers to define the relevant technical, organisational and contractual measures, on the basis of careful evaluation of the *length and complexity* of the data processing workflow; the *number* of actors involved and their respective relationships; as well as the possibility of *onward transfers*[44]. What is certain is that Universities choosing an ERT provider relying on SCCs for the transfer will have to perform their own evaluation considering all the concrete circumstances of the transfer, including the possible legal, technical and organisational safeguards that they or their providers can put in place. This is a task that inevitably requires investments of time, effort, and money (most probably beyond the limited resources available to Universities DPOs).

Among the conditions that can legitimise the transfer, the GDPR includes Binding Corporate Rules (BCRs)[45]. These rules provide a framework specifically designed on the basis of the specificities of a given sector and are approved by the supervisory authority[46]. However, this option raises some doubts. Firstly, BCRs usually take into account the reality of large companies. In the ERT scene, to the contrary, there are also smaller providers (and previously largely unknown, such as Jitsi and Discord) that have become widely used. One might then reasonably doubt that BCRs shaped upon the features of the bigger players in the ERT sector could encompass the varied design of the businesses that are active in the field. In addition to this, the effective implementation of BCRs could take a very long time. Most importantly, BRCs might experience the same fate of SCCs, as, given the current

[41] As retained by Solove D., 'Schrems II: Reflections on Decision and Next Steps' (*TeachPrivacy*, 23 July 2020) https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/ (last accessed: 11 November 2020).

[42] As it is possible to read in Court of Justice of the European Union, Case C-311/18, cit., paras 126-127

[43] *Ibid.*, para 133.

[44] Emphasis added. European Data Protection Board, 'Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', cit., 15-17.

[45] Article 29 Data Protection Working Party, 'Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules' (28 November 2017, modified 6 February 2018) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109, para 6.1.1, which outlines a series of essential elements and data protection principles to which BCRs must comply with.

[46] *Ibidem*.

US surveillance law, it is difficult to identify supplementary measures able to assure the equivalent standard of protection[47].

Ultimately, in accordance with Art. 46 GDPR, international transfers of personal data regarding digital education activities could be grounded in codes of conduct issued under Art. 40 GDPR or in approved certification mechanisms under Art. 42 GDPR[48]. Also, the reliance on these alternative transfer tools compels data controllers or processors to implement "appropriate" safeguards for the protection of the rights and freedoms of involved data subjects. In this case, however, problems of vagueness regarding what safeguards would be appropriate to these ends are likely to impair the achievement of the standard of essential equivalence with European Union law.

Finally, international data transfers could find legitimising grounds in some of the exceptions outlined by Art. 49 GDPR. In the context of ERT the following would be relevant: 1) explicit consent of the data subject and reinforced information obligations of the controller[49]; 2) necessity of the transfers for the conclusion or performance of a contract; 3) necessity of the transfer for important reasons of public interest.

The use of each of the three exceptions is highly questionable in the context at stake. For the purposes of the legal basis of consent, controllers would need to adequately inform data subjects regarding the envisaged transfer of personal data to countries that have a lower standard of protection, exposing themselves to objections or erasure requests. Moreover, in case the consent to the transfer is an outright condition for accessing the service, concerns regarding the free nature of such consent arise[50].

Furthermore, ERT service providers could argue that the transfer is necessary for the performance of the contract having as the object of the contract the digital educational service. In this case, however, according to the EDPB, the transfer needs to be "occasional" and most of all "objectively necessary for the performance of the contract"[51]. Thus, these two requirements will have to be demonstrated by ERT platforms, as they might clash with their business models and the scalability of their solutions.

Finally, also the derogation regarding the achievement of a public interest could be relied on by ERT service providers for conveying their datasets overseas. However, in respect to this possible derogation, substantial restrictions apply. As the EDPB has stated, public

[47] Solove D. (n. 41).

[48] European Commission, *Data Protection Certification Mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679* (February 2019) https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf, which also defines the specific data protection framework relevant for the purposes of certification mechanisms, in particular the principles under Articles 5; 24, 25 and 28 GDPR.

[49] The controller will have to inform the data subject about the possible risks of the transfers due to the absence of an adequacy decision and appropriate safeguards. See, Art. 49(1)(a) GDPR.

[50] This point has been raised by R. Ducato et al. (n 11).

[51] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679* (25 May 2018) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, 9.

interest must be clearly identified by the processing organisations irrespective of their public or private nature[52]. Different from the transfers justified in the performance of a contract, data transfers under public interest grounds do not have to be restricted to occasional transfers. Nonetheless, these transfers cannot occur in a systematic way nor on a large scale.

On a general level, the EDPB has highlighted that these derogations need to be "interpreted strictly so that the exceptions do not become the rule"[53]. This means that these derogations can only be applied in specific circumstances, in strict observance of the necessity test. A restrictive interpretation of such derogations is additionally encouraged by the data protection by design and by default principles[54]. These principles require businesses to arrange themselves in a way that maximises data protection. In this respect, the limitation of data transfers to third countries could be a means for minimizing the risks to data subjects' rights stemming from controllers' activities.

Given the new scenario of international data transfers opened up by the *Schrems II* decision, it is crucial for Universities to revise their ERT practices and implement the CJEU *decisum*. For instance, when universities (controller) outsource the digital delivery of teaching to external services (processor), the question arises as to whether HEIs are able to know that the processor transfers collected personal data outside the European Union, under which legal basis and for which purposes. This is not a trivial task as it might appear to be, as the privacy policies of most of the platforms employed for education purposes[55] remain quite vague about these aspects. Contractual agreements shall then define these issues in more clear terms.

In accordance with Art. 28(1) GDPR, controllers shall choose processors that guarantee technical and organisational measures "in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". This means that HEIs, as controllers, should be sure about the employed platform's organizational structure and the legal bases relied on for extra-EU data transfers. In addition to those aforementioned measures, the authorisation to transfer should be contained in the contract between the university and the service provider, specifying the nature of the transferred data and the location of storage. Such authorization is also needed for the entrustment of sub-processors for extra-EU transfers by the processor, to maintain consistency with the principle of lawfulness. In this respect, it must also be recalled that in case a

[52] European Data Protection Board, 'Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 – *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, cit., 4.

[53] European Data Protection Board, *Initial Legal Assessment of the Impact of the US Cloud Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence* (10 July 2019) https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf.

[54] Art. 24 GDPR.

[55] Again, reference is made to the privacy policies of the platforms analysed in the study by R. Ducato et al. (n 11).

joint controllership relationship under Art. 26 GDPR exists between the university and the platform, the contract among the parties should allocate respective liabilities in regards to the specific case of international data transfers.

With the falling of the Privacy Shield, most universities relying on processors transferring data to the US should act promptly as to stop these unlawful transfers and renegotiate the terms of the processing agreement in order to find a more legally-sound solution. To these ends, a means to contractually empower universities vis à vis ERT platforms could be found in the establishment of outright associations of universities, which could collectively manage and regulate envisaged international transfers that mostly involve sensitive data.

Moreover, HEIs can rely on supervisory authorities to choose the most convenient legal basis for the eventual extra-EU data transfers and for the related adequacy assessments. As the CJEU has highlighted, especially as a result of the falling of the Privacy Shield, these authorities have a central role in the oversight of international transfers: they can also suspend the transfer in the case where no effective equivalence is found and when the controller or processor fails to do so[56]. In this perspective, a stronger collaboration between universities' DPOs and supervisory authorities should be encouraged, so as to tighten the supervision over recurring cross-border flows of educational-related personal data.

The international dimension of digital educational models and the frequency of resulting data flows, should garner greater attention by European regulators due to the need of establishing a clearer normative framework for the extra EU circulation of European citizens' data collected during educational activities. In light of the transnational nature of remote teaching services, it is useful to look at the phenomenon of data flows originating from remote teaching services through the concept of "data space" used by the European Commission in the latest European data strategy for indicating a market zone of free data exchanges[57]. It is interesting to note that in the list of the "data spaces" envisaged by the Commission in various sectors such as health, energy, financial, and agricultural[58], any reference to the field of education is missing.

Nonetheless, the recently released Digital Education Action Plan 2021-2027[59] directly targets objectives related to the "cross-sector collaboration", the establishment of "new models for the exchange of digital learning content", addresses "issues such as common standards, interoperability, accessibility and quality-assurance". In this respect, more defined rules regarding the sharing practices of education-related data, specifically in regards to extra EU flows, are needed in order to meet those objectives more effectively.

[56] Case C-311/18, cit., paras 113 and 135.

[57] European Commission, *A European Strategy for Data* (Communication) COM (2020) 66 final.

[58] *Ibid.*, pp. 22-23.

[59] European Commission, 'Digital Education Action Plan (2021-2027) – Resetting Education and Training for the Digital Age' (Communication) COM (2020) 624 final.

A clearer framework regarding overseas data transfers involving sensitive personal information and adhering to the "essential equivalence" rule is key for shaping of a fundamental rights-oriented European digital education mode to act as a benchmark when interacting with other legal systems and emerging foreign digital education systems that have lower protection standards[60]. It is of note that in accordance with Art. 6 TFEU, as with the health sector, the education sector is also within a Member States' competence. In this field, the European Union thus has only supporting competences aimed at coordinating or complementing Member States' actions.

Nonetheless, it appears that the digitisation of education tools is triggering a "Europeanisation" of the education sector[61]: the set focus of digital education through a European Action Plan suggests that technological developments are attracting the regulation of this traditionally national-based subject matter at the European level. The fact that technologies and related risks are mainly addressed at the European level, is causing a spillover regulatory effect in those areas that are being most affected by technological transformations, such as the health sector[62] and now, under the pressure of the Coronavirus pandemic, the education sector. This is clearly demonstrated by the planned establishment of a European Education Area by 2025[63].

Under these premises, the emerging shift of competences of the European Union in the field of digital education may soon reveal that the regulation of the international transfer of European citizens' data for education-related purposes is a fundamental prerequisite for the achievement of the more general goal of strengthening the European leadership in global competition[64] and of consolidating the role of the European Union as a partner in education at the global level[65]. In addition to purely normative responses, technical solutions could speed up the achievement of these ambitious goals: among the available options the establishment of an EU-wide standardised digital learning infrastructure could be useful in order to curb the degree of extra EU flows of data concerning sensitive aspects of European teachers' and students' education activities.

---

[60] Think, for example, of the developing a Chinese digital learning environment, based on the collection of sensitive data through facial recognition technologies, invasive surveillance mechanisms, and a weak cybersecurity coverage, exposing students' to data leakages. See among others, L. Lin, *Thousands of Chinese Students' Data Exposed on Internet – Information Leak From Facial Recognition Databases Raises Questions About School Surveillance and Cybersecurity in China*, *The Wall Street Journal* (18 January 2020) https://www.wsj.com/articles/thousands-of-chinese-students-data-exposed-on-internet-11579283410 (last accessed: 11 November 2020).

[61] For a general overview seeEuropean Parliament, Research for CULT Committee, *The Use of Artificial Intelligence (AI) in Education – Concomitant Expertise for INI Report* (May 2020) https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/629222/IPOL_BRI(2020)629222_EN.pdf (last accessed: 11 November 2020).

[62] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions- A European Strategy for Data*, cit., COM (2020) 66 final, 22.

[63] European Commission, *Achieving the European Education Area by 2025* (Communication) COM (2020) 625 final.

[64] *Ibid.*, p. 8-9.

[65] *Ibid.*, p. 23-24.

4. E-proctoring: Is this the best we can do?

The paradigmatic shift from the physical to the online University environment invested another core area of the students' life: exams. When it was clear that the spread of COVID-19 was going to impact the spring and summer sessions, the whole academic community had to embrace the additional challenge of guaranteeing the legal and pedagogical value of the exam in the online environment, including how to prevent students' fraud. Within this context, many solutions have been proposed and adopted. For example, oral exams have been carried out in synchronous via videoconferencing tools, implementing safeguards to verify the candidate's identity.

However, the majority of concerns focused on written assessments, because of the challenges present in ensuring the integrity and validity of this type of exams. Many institutions decided to rely on e-proctoring systems, which allow the monitoring of students via computer's webcam and microphone. More specifically, depending on the system, the e-proctoring can be "online live" and/or the session can be recorded for later review. In the latter case, the system records both the video and the audio, and analyses the data collected to identify unusual patterns or suspicious behaviours, e.g. the student stands up, takes books or the mobile phone, talks to someone else in the room, surfs online[66], or even looks away from the computer screen. If the software detects any issue, it sends a notification to the examiner. The examiner then has the possibility to verify the portion of the recording in question and makes a decision.

E-proctoring systems aim to replicate the function of in-class invigilation. However, the transplant of an offline concept to an online setting raises additional issues and concerns in this context. If we look at e-proctoring features and use, such tools are likely to be more problematic than their analogue version. The most prominent change is that the exam is not held within the University premises, but it is brought into students' homes[67]. This shift has to be carefully considered as, in principle, it already constitutes an invasion of one of the most intimate spheres of an individual, their home. Second, the inspection of the work station (desk, walls, etc.), which is a preliminary step to be taken before the exam starts, might be frustrating, uncomfortable and humiliating (for the invigilator and) for students in a moment where many of them are already stressed for the exam[68]. Third, we have to consider that, with e-proctoring, the invigilation becomes systematic: an online watchdog examines and records all the movements for the entire duration of the exam. Preliminary

[66] Although some systems block browsing by default.

[67] E-proctoring can be used also in the physical environment of the University (to replace human invigilation) or, in any case, it does not mandate that students stay in their own home. However, considering the lockdown measures during the pandemic, almost all students had to connect from their own room or studio.

[68] Research shows that proctored exams generate more anxiety in test takers if compared to non-proctored exams. M. N. Karim, E. S. Kaminsky, T. S. Behrend, *Cheating, reactions, and performance in remotely proctored testing: An exploratory experimental study* (2014) 29, 4 Journal of Business and Psychology 555.

research underlines that this kind of non-stop monitoring not only is considered upsetting and intrusive, but it is likely to have a negative impact on the performance of those students particularly anxious[69].

Furthermore, a consistent body of literature is showing the lack of accuracy of automated decision-making systems and the problem of algorithmic bias[70]. Thus, there is the risk that these problems will affect the e-proctoring technology as well, leading to inaccurate results and discriminatory outcomes[71]. The issue is not merely hypothetical. Even if what has been reported so far is anecdotal, e-proctoring systems are showing some difficulties in correctly recognising black students[72]. Finally, the negative consequences of such systems on students might be exacerbated if the e-proctoring tool makes automated decisions, e.g. the exam is automatically suspended or failed, without human oversight[73].

In addition to privacy and data protection concerns, this kind of technology does not take into account the difficulties that a student might have in ensuring a stable connection, a computer or other IT device, and a room only for herself during the exam. This logistic issue can become a proxy for bringing out new inequalities or highlighting existing ones. The widespread adoption of e-proctoring has piqued the attention of students and privacy scholars, questioning the intrusiveness of the tool[74]. Some of these concerns have been

---

[69] D. Woldeab, T. Brothen, *21st Century Assessment: Online Proctoring, Test Anxiety, and Student Performance* (2019) 34, 1 *International Journal of E-Learning & Distance Education* 1.

[70] *Ex multis*, F. Pasquale, *The black box society* (Harvard University Press 2015).

[71] See M. Foulkes, *Exams that Use Facial Recognition May be Fair – But They Are Also Intrusive*, *The Guardian*, (London, 22 July 2020) https://www.theguardian.com/law/2020/jul/22/exams-that-use-facial-recognition-are-fair-but-theyre-also-intrusive-and-biased?CMP=Share_iOSApp_Other (last accessed: 11 November 2020).

[72] See S. Swauger, *Software that Monitor Students During Tests Perpetuates Inequality and Violates their Privacy* (*Technology review*, 7 August 2020) https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/ (last accessed: 11 November 2020); and the ongoing discussions on Twitter https://twitter.com/uhreeb/status/1304451031066083331?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1304451031066083331%7Ctwgr%5Eshare_3&ref_url=https%3A%2F%2Fwww.insider.com%2Fviral-tiktok-student-fails-exam-after-ai-software-flags-cheating-2020-10 (last accessed: 11 November 2020). See also S. Swauger, *Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education* (*HybridPedagogy*, 2 April 2020) https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/ (last accessed: 11 November 2020).

[73] It became viral the TikTok's video of a student falsely accused of cheating during a proctored exam. See Swauger, S., *Remote Testing Monitored by AI is Failing the Students Forced to Undergo it* (7 November 2020) https://www.nbcnews.com/think/opinion/remote-testing-monitored-ai-failing-students-forced-undergo-it-ncna1246769 (last accessed: 11 November 2020).

[74] S. Hubler, *Keeping Online Testing Honest? Or an Orwellian Overreach?*, *New York Times* (New York, 10 May 2020) https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html (last accessed: 11 November 2020); M. Chin, *Exam Anxiety: How Remote Test-Proctoring is Creeping Students Out – As Schools go Remote, So Do Tests and So Does Surveillance* (*TheVerge*, 29 April 2020) https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education (last accessed: 11 November 2020); D. Harwell, *Mass School Closures in the Wake of the Coronavirus are Driving a New Wave of Student Surveillance*, *Washington Post* (Washington DC, 1 April 2020) https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/ (last accessed: 11 November 2020). It should be mentioned that privacy concerns were raised even before the pandemic crisis, when e-proctoring was adopted for online testing. See, for example, A. Majeed, S. Baadel, A. Ul Haq, *Global triumph or exploitation of security and privacy concerns in e-learning systems* (2017) *International Conference on Global Security, Safety, and Sustainability*. Springer, pp. 351-363.

brought before the Courts and a first and preliminary decision was issued by the Court of Amsterdam in June 2020[75]. In that case, two student associations and an individual student at the University of Amsterdam complained about the use of the software "Proctorio" adopted by their University, alleging a number of data protection violations. They argued, in particular, the lack of an appropriate legal basis for the specific processing, the violation of the principles of purpose limitation (as the software was collecting more data than necessary for the exam) and proportionality (since there were less privacy-intrusive tools). The judge, however, rejected the complaint, recognizing that the use of the software was done in accordance with the GDPR principles. First, the University was performing a task carried out in the public interest [Art. 6(1)(e) GDPR], namely the provision of education and the issuing of diplomas, which includes the steps to guarantee their quality and validity[76]. Furthermore, according to the Court, the University demonstrated that there were no suitable e-proctoring alternatives and that the chosen system was used only as a last recourse, when it was not possible to convert the exam in essay assignments due to the typology of the assessment or the number of students. In addition, appropriate safeguards were taken, also on the basis of the results of the data protection impact assessment. Hence, the Dutch judge held that the processing was necessary and proportionate given the concrete circumstances[77].

Despite this first decision, several questions remain open. Of course, there are different types of software available on the market, whose deployment may vary from one University to the other. Therefore, such a decision cannot be generalized. GDPR compliance is and remains a case-by-case evaluation. Nevertheless, we should start asking ourselves what level of interference with the rights to privacy and data protection would we be inclined to accept in our educational environment and, considering the fallibility of such systems, which level of reputational risks Universities might want to take.

As the Amsterdam case shows, during the Covid-19 emergency, e-proctoring has been used for exams based on multiple choice or short answer questions. These are all cases where the teacher tests the general knowledge of the student on a specific topic. Lacking any invigilation, there is a higher risk of cheating, as the *mala fide* student can easily check the response online or in books, notes, group chats, etc. Is then the use of e-proctoring the best option available to ensure the validity of the exam?

We must preliminarily observe that if the purpose of e-proctoring is to prevent or reduce the risk of copying in notional exams, setting up a time limit could be already a solution. Namely, when available time is calibrated in function of the number of questions, precious seconds are less likely to be wasted wandering around in search for the correct answer. We

[75] Rb. Amsterdam - C/13/684665 / KG ZA 20-481 (an unofficial translation in English is available here: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/684665_/_KG_ZA_20-481 (last accessed: 11 November 2020).

[76] See, para 4.10, Rb. Amsterdam – C/13/684665 / KG ZA 20-481.

[77] The decision is currently under appeal.

do not suggest this solution as an ideal way out of the exam dilemma, however, especially considering the potential cognitive diversity in the cohort of students. People with disabilities might be negatively affected by a constrained time limit. Other ways to minimise cheating could consist in the preparation of different versions of the same assessment and their randomised distribution to students. If this solution would reduce the collusion among students, it would not prevent dishonest behaviours *tout court*.

Overall, structuring the exam in a way where pure notions and basic knowledge are not directly evaluated, could offer a better alternative that might solve the copying problem *ab origine*. There are plenty of assessment strategies that can be successfully implemented as a take-home exam (essays, open questions, opinions, reports, interviews) or in the form of continuous evaluation (projects, case studies, group presentations, group works, artifacts, etc.). In these kinds of assessments, the student does not have to demonstrate that she "knows", but that she critically masters the knowledge and uses the skills acquired during the course. Something that is usually the highest desirable learning outcome in all our syllabus. After all, the etymology of assessment comes from the Latin "assidere", that means "to sit with"[78]. As pointed out by Green: "In an assessment, one sits with the learner. It is something we do *with* and *for* the student, not something we do *to* the student"[79].

Such a typology of exam involves a more complex exercise, indeed, not only for the students, but also for the evaluators. It requires more time than a set of multiple choices and it is hard to manage with a huge number of students. Therefore, it cannot always be considered a suitable – although less intrusive – alternative. This was indeed one argument used by the University of Amsterdam to justify the necessity of Proctorio. If such a line of defense is somewhat understandable during the peak of the emergency, it raises the question about whether we should pretend more for the 'postpandemic university'[80].

In other terms, there are less intrusive means than e-proctoring to organise an exam session, but their implementation is going to require systemic changes. First of all, it means to continue/or increase the effort required for the education of our students to the value of academic integrity. The purpose of the University is also to form responsible citizens and accountable future professionals.

Second, non-invigilated exams require setting a reasonable ratio between the number of teachers and students. This will make it possible to structure the exam in a way that would permit testing the analytical and critical thinking of students, so as to render the evaluation manageable for a teacher. Allowing us a "physical" metaphor, the restructuring of the learning experience around the size of the class and not the auditorium will contribute to

[78] As reported in J.M. Green, *Authentic Assessment: Constructing the Way Forward for All Students* (1998) Education Canada 38, 3, 8-12: 11.

[79] *Ibidem*.

[80] As labelled and investigated in the initiative led by Mark Carringan at the Faculty of Education, University of Cambridge. See, https://postpandemicuniversity.net (last accessed: 11 November 2020).

set the main condition for promoting a dialogue and a constructive exchange between all the participants.
The problem of class size, the possibility to have a truly formative experience also during the assessment, and the increasing workload for teachers, are all questions that have been with us for a while. The emergency situation we are experiencing is simply reminding us that those issues remain and that we should no longer postpone looking for an answer.

In lieu of conclusion: Shaping the right to digital education beyond GDPR compliance

Data protection and privacy laws are a first regulatory frame for addressing transformations affecting educational means in (post) pandemic times. They provide a fundamental benchmark upon which the transition to a digital university dimension needs to be measured, and which is useful also for the identification of the deeper socio-legal consequences of the ongoing shift.
During the pandemic, the generalised answer of Universities for coping with remote teaching has been the recourse to third-party digital providers. This 'forced' choice has unveiled a critical weakness of our education systems: the lack of an adequate digital infrastructure to support the provision of education online, not only during an emergency, but, more generally, in a way that makes the most out of EdTech tools.
The trend toward 'platformisation' of education, exacerbated during the COVID crisis, present several challenges for Universities in terms of privacy and data protection. As we have shown in this contribution and in our previous work, there are still serious concerns about the implementation of data protection principles in this context[81]. Each of the identified data protection challenges (concerning purpose limitation, transparency, and extra EU data transfers) suggests that both the platforms and Universities should more effectively embed data protection principles in the design and deployment of their remote teaching policies.
When Universities decide to rely on third-party services (for necessity or convenience), adherence to the data protection framework by them and the platform is a necessary starting point. Privacy and data protection not only deserve protection as such; they are also a precondition of a full protection of other fundamental rights in this context, such as aca-

[81] One concern highlighted in our previous work was related to the reference made, for example, by Facebook and Zoom's privacy policies to legitimate interests as a lawful basis for the processing, without any mention of the balancing between the controller's legitimate interest and the data subjects' interests; furthermore, other platforms as Youtube, Skype, Zoom, Jitsi and Gsuite did not provide sufficient information regarding the purpose for which the categories of collected data mentioned in the privacy policies were processed. Jitsi and Gsuite, for example, generally refer to the purpose of "improvement of the service". See, R. Ducato et al. (n 11).

demic freedom, right to education, freedom of expression, human dignity[82]. The pandemic did not establish any special derogation to the privacy and data protection rights framework under the EU Charter, the European Convention of Human Rights and the GDPR, which therefore must apply. To this end, national data protection authorities should carefully scrutinise the services specifically tailored for education and offered to schools and Universities[83]. The "Sweep days", promoted by the Global Privacy Enforcement Network (GPEN), could be already a first initiative to be launched in the short term[84].

In the medium- and long-term, it will be then relevant to open a channel of collaboration with DPAs for addressing teaching-related personal data collection and processing practices in the educational context when platforms are critically involved. The respect of privacy and data protection are, indeed, a necessary but not sufficient condition. As the case of e-proctoring demonstrates, it might be needed to go beyond mere compliance with the EU data privacy law and consider the broader implications of the tools we are using.

More generally, when Universities outsource whole or part of the processing to platforms, two issues should be carefully considered: 1) who decides what platform to use (hence, what are the characteristics it must have); and 2) how the standardisation of the service is going to impact on the level of (digital) autonomy and independence of Universities in this context.

With reference to the first aspect: the choice of a platform is not a neutral decision. Having an impact on the academic community, the decision-making process for determining the eligible educational infrastructure should be vetted with the inclusion of all the interested persons of that community.

The first point to consider concerns the body within the University making decisions related to data protection (i.e. determining the purposes of processing, and choosing the platform). These decisions undoubtedly affect students and teachers. Therefore, their participation (through representatives or "information champions") in the decision-making process should be considered, especially in view of efforts to establish inclusive educational values. This aspect is particularly relevant because it would shape the governance of data collected and further processed, especially taking into consideration the importance

[82] Analogous considerations hold true for the copyright aspects involved in remote teaching, particularly with reference to the respect of the legitimate uses (so-called exceptions and limitations). On this, see L. Pascault *et al.*, *Copyright and Remote Teaching in the Time of COVID-19: A Study of Contractual Terms and Conditions of Selected Online Services* (2020) 42.9 *European Intellectual Property Review* 548.

[83] As announced by the Italian Data protection Authority, act of 26th March 2020, n. 9300784 – *Didattica a distanza: prime indicazioni*, cit. For a brief analysis of the decision (in English), see R. Ducato *et al.*, *Emergency Remote Teaching and digital data privacy: first instructions from Italy* (*Blog de Droit Europeen*, 16 July 2020), https://blogdroiteuropeen.com/2020/07/16/emergency-remote-teaching-and-digital-data-privacy-first-instructions-from-italy-by-rossana-ducato/ (last accessed: 11 November 2020).

[84] The GPEN is an international network of DPAs for privacy enforcement co-operation, created in 2010 within the OECD. The "Sweep day" is an yearly initiative where data protection authorities, part of the GPEN, investigate practices in the data privacy field and examine specific areas of concern (e.g. transparency of medical apps, privacy communications directed to children, etc.). See, https://www.privacyenforcement.net/ (last accessed: 11 November 2020).

that the recent European Commission proposal for a data governance act has placed in the re-use of (personal) data held by public sector bodies[85].

With regard to the second aspect, the interplay between standardization of the service and Universities autonomy cannot be neglected, as the latter is an essential touchstone for the well-functioning of evolving online institutions[86] HEIs.

Admittedly, standardisation is essential to norm-setting. For instance, it could help smaller institutions to foster lawful requirements, such as data protection and minimum lawful copyright policies. However, the conditions *de facto* imposed by platforms are at odds with the fundamental principle of institutional autonomy of each University. As a constitutional principle in some European countries[87], university autonomy is a foundational value for HEIs. Independence of choice of digital infrastructures is an expression of this autonomy and standardisation could end up rendering aspects of this choice becoming non-negotiable. There is indeed a flagrant asymmetry in bargaining power between platforms, which operate on a global scale, and Universities, which lack sufficient contractual power for affecting the conditions of the service. Collective negotiations could be a possible way out here. Groups of Universities could join forces when negotiating with platforms, proposing their own data protection conditions, shaped according to their cultural mission and educational needs. This collective negotiation may cover several data protection and privacy issues: the data to be collected, the data minimisation safeguards and features[88], the clear distribution of roles and responsibilities vis-à-vis the data subject, the location of the servers, the purposes of the processing, the eventual admissible repurposing, and data sharing.

Considering the input from students and teachers would potentially democratise the drafting of necessary technical and legal conditions that platforms must guarantee.

The shape of these collective negotiations will determine the degree to which institutional values are reflected in the infrastructure choice.

As already stressed, the full reliance on third-party providers has been a general response dictated by the emergency. It does not mean that alternative options might not be considered.

[85] European Commission, Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), cit., COM (2020) 767 final, Chapter II.

[86] The issue of the latent conflict between University autonomy and US-based platforms is not new. It was already raised last year by Dutch Rectors in a public letter, as reported here: https://www.volkskrant.nl/columns-opinie/digitalisering-bedreigt-onze-universiteit-het-is-tijd-om-een-grens-te-trekken~bff87dc9/ (last accessed: 18 December 2020).

[87] See for example, Art. 33(6) of the Italian Constitution.

[88] For instance, how to implement a proper technical feature for allowing the recording of an online seminar, minimising the processing of participants' data at the same time (e.g. impeding to process name and video of attendants which do not want to be recorded or "pinned" during the livestream). Some platforms ask for dubious manifestations of consent to the recording, as stressed here: R. Ducato *et al.* (n. 11).

Thinking on a medium to long-term perspective, it would be worth discussing bringing the digital infrastructure "in-house". New public infrastructures, or the enhancement of existing ones, should be put in place, highly customisable at the local level, in order to ensure a proper balance with the principle of University autonomy.

Institutions could opt to reuse or to create new infrastructures that not only embed fundamental rights from the design stage and throughout the lifecycle of the system, but are also representative of European digital values[89]. This issue is of particular importance if we take into consideration the consequences of EdTech platform standardisation on a global scale for "educational diversity"[90]. The circulation of cultural, educational, learning, and supervision models promoted through the structure of a specific platform could end up hurting the diversity of learning experiences guaranteed in different institutions. This standardization would potentially end up becoming the norm of an educational global monoculture. The conciliation of competing interests could be found in hybrid formulations as well. For instance, some functions could be delegated to the central structure, e.g. storage of data in a secure environment and others would be retained by the single entity. This, from a data protection perspective, might be an example of joint-controllership with clearly set out rules that ensure transparency, accountability, and ultimately, respect of data subjects within the broader institutional and cultural value model.

Seen more broadly, there is still a whole array of unexplored issues related to the implications of the platformisation of education, including possible discriminatory outcomes. For instance, it is critical to consider the divergences in digital skills across different social strata as well as the impact of the considered phenomenon on the access to education by physically or mentally impaired students, whom may not be able to use ordinary digital services. Ultimately, assessments of the quality of digitally provided educational services should be conducted against the backdrop of the fundamental right to education.

With remote teaching having become "an integral part of our future"[91], targeted institutional responses such as the enactment of funding programs and the establishment of specific oversight mechanisms related to EdTech solutions, should move to the top of regulators' agenda. The first institutional moves in this direction are being announced by

[89] European Commission, 'Digital Education Action Plan (2021-2027) – Resetting Education and Training for the Digital Age', cit., COM (2020) 624 final, making reference to the importance of the incorporation of ethical standards in emerging digital education systems.

[90] This notion has been taken into consideration by sociological literature, see Y. Taylor, 'Educational Diversity: the Subject of Difference and Different Subjects', in Y. Taylor, *Educational Diversity: the Subject of Difference and Different Subjects* (Palgrave McMillan, 2012). More recently see V. Harpalani, *Safe Spaces and the Educational Benefits of Diversity* (2017) 13 *Duke Journal of Constitutional Law & Public Policy* 117. Specifically focusing on educational diversity in the remote teaching environment, C.J.K. Sandoval *et al.*, *Legal Education in the Era of Covid-19: Putting Health, Safety and Equity First* (24 July 2020) *Santa Clara Univ. Legal Studies Research Paper* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3660221.

[91] M. Vestager, *Speech by Executive Vice-President Margrethe Vestager on a New Digital Education Action Plan 2021-2027 and a New European Research Area* (30 September 2020) https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1786 (last accessed: 11 November 2020).

the European Commission in its recent Communication on Achieving the European Education Area by 2025[92]. This document envisages training programs to consolidate the digital skills of subjects operating at all levels[93] and, in particular, specialised education programs for advancing digital skills[94]. The objectives currently targeted by the Commission focus on the increase of competences, participation, and inclusiveness of a digitally-fuelled European education system[95], as well as, on the enhancement of connectivity and cooperation of higher education institutions[96]. However, digital infrastructures channelling education efforts are not included among the targets and indicators of the proposed changes. This rapidly changing infrastructural environment deserves more attention, given that in the digital, more than in the physical dimension, the form shapes the matter, and thus, our education.

[92] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Achieving the European Education Area by 2025*, cit., COM (2020) 625 final.

[93] *Ibid.*, p. 9.

[94] *Ibid.*, p. 11, where the lack of experts in the fields of artificial intelligence, cybersecurity and high performance computing is highlighted.

[95] *Ibid.*, pp. 13 ff.

[96] *Ibid.*, p. 20.