Berytus Review | Year 1- Vol. 1 – Issue 1 – June 2026

Legal Challenges of Protecting Students' Privacy in Online Learning: A European Data Protection Law Analysis

Author: **Dr. Firas El Harake – Lebanon**
ORCID: 0000-0003-3183-9653

Reviewed by: **Prof. Asser Harb**, **Egypt**

Paper received	Peer review report	Received amended	Published
11 May, 2026	16 May, 2026	19 May, 2026	1 June, 2026

Abstract

The rapid expansion of online learning technologies across Europe has significantly transformed the collection, processing, and governance of students' personal data within digital educational environments. Educational institutions and educational technology providers increasingly rely upon remote learning platforms, artificial intelligence systems, learning analytics tools, biometric monitoring technologies, and cloud-based infrastructures to facilitate educational delivery and administrative management. While these technologies provide substantial educational benefits, they also generate serious legal challenges concerning privacy, surveillance, automated decision-making, cross-border data transfers, and institutional accountability.

This article examines the adequacy of European legal frameworks governing the protection of students' privacy in online learning environments. The study adopts a doctrinal legal methodology supported by analytical and descriptive approaches in order to evaluate the application of the General Data Protection Regulation (GDPR), the European Union Artificial Intelligence Act, Convention 108+, and relevant European jurisprudence to digital education practices.

The article argues that although European data protection law establishes an advanced framework for safeguarding students' personal data, significant doctrinal and enforcement gaps remain in relation to AI-driven educational technologies, remote proctoring systems, and algorithmic profiling practices. Particular legal concerns arise regarding proportionality, lawful processing, biometric surveillance, automated decision-making, and fragmented enforcement across European member states.

The study further analyses the role of the Court of Justice of the European Union (CJEU), the European Data Protection Board (EDPB), and selected national legal frameworks in Germany and France. It concludes that stronger regulatory harmonisation, enhanced institutional accountability, stricter proportionality assessments, and clearer safeguards governing educational AI systems are necessary to ensure effective protection of students' privacy within the evolving European digital education environment.

Keywords

Student Privacy; Online Learning; GDPR; European Union; Educational Technology; Artificial Intelligence; Remote Proctoring; Learning Analytics; Data Protection; Digital Education.

1. Introduction

The expansion of digital education has fundamentally transformed the collection, processing, and governance of students' personal data across Europe. Online learning platforms, videoconferencing systems, cloud-based educational services, remote assessment technologies, and artificial intelligence-driven learning tools now constitute central components of modern educational environments. Although the rapid transition toward online learning accelerated significantly during the COVID-19 pandemic, digital educational technologies continue to shape higher education and school systems throughout Europe beyond the immediate public health context.[1]

Educational institutions increasingly depend upon extensive forms of personal data processing in order to facilitate remote instruction, monitor attendance, evaluate academic performance, prevent academic misconduct, and optimise learning outcomes. As a result, students are now subject to unprecedented forms of digital monitoring within educational settings. Online learning systems routinely collect and process names, identification numbers, academic records,

[1] European Commission, *Digital Education Action Plan 2021–2027* (European Commission 2020).

behavioural data, IP addresses, geolocation information, biometric identifiers, audiovisual recordings, and predictive learning analytics generated through educational platforms.[2]

The increasing integration of artificial intelligence systems into educational technologies has intensified concerns regarding surveillance, algorithmic profiling, automated decision-making, and behavioural prediction within digital learning environments. AI-driven educational systems are increasingly capable of evaluating student engagement, predicting academic performance, detecting behavioural anomalies, and generating automated recommendations concerning educational interventions.[3] While these technologies may improve administrative efficiency and educational personalisation, they also create substantial risks relating to privacy, transparency, discrimination, and informational autonomy.

Within the European legal order, the protection of personal data constitutes a fundamental right recognised under Article 8 of the Charter of Fundamental Rights of the European Union and reinforced through the General Data Protection Regulation (GDPR). [4]The GDPR establishes a comprehensive legal framework regulating the lawful processing of personal data and imposes obligations relating to transparency, accountability, proportionality, data minimisation, storage limitation, and automated decision-making. Nevertheless, the practical implementation of these principles within online learning environments remains legally contested.

Particular controversy surrounds the growing use of remote proctoring technologies and AI-based learning analytics systems within European educational institutions. Remote proctoring software frequently relies upon facial recognition systems, eye-tracking technologies, behavioural monitoring, screen recording, and continuous audiovisual surveillance in order to detect suspected academic misconduct during online examinations[5] These practices may involve the processing of

[2] European Union Agency for Cybersecurity (ENISA), *Data Protection and Privacy in Education* (ENISA Report, 2021).

[3] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' (2019) 2 *Columbia Business Law Review* 494.

[4] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1.

[5] Katarina Lindroos, 'Remote Proctoring, Privacy and Data Protection in Higher Education' (2022) 12 *International Journal of Educational Integrity* 1.

biometric data and intrusive monitoring of students within private domestic environments, thereby raising serious concerns regarding proportionality and human dignity.

In addition, online learning environments often involve complex relationships between educational institutions and private technology companies operating across multiple jurisdictions. Educational platforms frequently depend upon cloud infrastructures and third-party service providers that transfer or store personal data outside the European Economic Area. Following the judgment of the Court of Justice of the European Union (CJEU) in *Schrems II*, questions concerning international data transfers and the adequacy of safeguards protecting European personal data have become increasingly significant within educational contexts[6]

European institutions have also begun to recognise educational AI systems as a potentially high-risk regulatory sector. The adoption of the European Union Artificial Intelligence Act introduces additional legal obligations relating to transparency, human oversight, accountability, risk assessment, and the governance of AI systems used in educational environments.[7] These developments demonstrate that educational technologies now occupy a central position within broader European debates concerning digital rights and algorithmic governance.

Despite the growing regulatory attention devoted to digital education, uncertainty persists regarding whether existing European legal frameworks provide sufficient protection for students' privacy in online learning environments. Divergent enforcement practices among European supervisory authorities, inconsistent institutional compliance mechanisms, and the rapid evolution of educational technologies continue to expose significant legal and doctrinal gaps.

This article argues that although European data protection law establishes an advanced framework for safeguarding students' privacy, substantial deficiencies remain in relation to AI-driven educational technologies, remote proctoring systems, automated profiling practices, and cross-border educational data governance. The article further contends that fragmented enforcement among European member states weakens the effectiveness of privacy protections and creates inconsistent standards for educational institutions operating within the European digital education environment.

---

[6] *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Schrems II) Case C-311/18, EU:C:2020:559.

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L.

The article adopts a doctrinal legal methodology supported by analytical and descriptive approaches in order to evaluate the adequacy of European legal frameworks governing student privacy in online learning. The analysis focuses specifically on the GDPR, the EU Artificial Intelligence Act, Convention 108+, European Data Protection Board guidance, selected national legal frameworks, and relevant jurisprudence of the Court of Justice of the European Union.

2. Research Problem and Objectives

2.1 Research Problem

The rapid expansion of online learning technologies within European educational institutions has fundamentally altered the ways in which students' personal data are collected, processed, analysed, and transferred. Digital education platforms increasingly rely on artificial intelligence systems, cloud-based infrastructures, remote proctoring technologies, and learning analytics tools in order to facilitate educational delivery and monitor student performance. While these technologies provide substantial educational and administrative benefits, they simultaneously generate serious legal challenges relating to privacy, surveillance, transparency, accountability, and automated decision-making.

Within online learning environments, students are frequently subjected to continuous forms of digital monitoring that extend beyond traditional educational supervision. Educational platforms routinely collect sensitive categories of personal information, including biometric identifiers, behavioural data, geolocation information, audiovisual recordings, examination recordings, browsing activity, and predictive analytics concerning student behaviour and academic performance.[8] The scale and intrusiveness of such processing activities raise significant concerns regarding the adequacy of existing European legal safeguards protecting students' fundamental right to privacy.

Although the General Data Protection Regulation (GDPR) establishes a comprehensive legal framework governing personal data protection within the European Union, uncertainty persists regarding the practical application of its principles to online learning environments. Questions remain concerning the lawfulness of remote proctoring technologies, the proportionality of continuous behavioural monitoring, the legality of automated educational profiling, and the responsibilities of educational institutions when cooperating with third-party educational technology providers.

The growing integration of artificial intelligence into educational technologies has further intensified these concerns. AI-driven systems increasingly influence academic assessment, behavioural prediction, student engagement analysis, and educational decision-making processes. Such systems may produce discriminatory outcomes, inaccurate predictions, or opaque forms of automated profiling that directly affect students' educational opportunities and academic

[8] European Union Agency for Cybersecurity (ENISA), *Data Protection and Privacy in Education* (ENISA Report, 2021).

autonomy. These developments raise important legal questions under European data protection law, particularly regarding transparency, accountability, human oversight, and automated decision-making safeguards.[9]

Moreover, European enforcement practices concerning educational data protection remain fragmented across member states. While the GDPR aims to establish harmonised standards throughout the European Union, supervisory authorities have adopted inconsistent approaches toward educational technologies, remote surveillance systems, and AI-driven learning tools. This fragmentation creates legal uncertainty for educational institutions and weakens the effectiveness of privacy protections available to students across Europe.

Accordingly, the central problem addressed by this research concerns whether existing European legal frameworks provide sufficient protection for students' privacy within online learning environments and whether current regulatory mechanisms adequately address the legal risks generated by AI-driven educational technologies, remote monitoring systems, and cross-border educational data processing.

2.2 Research Objectives

This research seeks to achieve the following objectives:

1. To analyse the effectiveness of the General Data Protection Regulation (GDPR) in protecting students' personal data within online learning environments.
2. To examine the legal implications of remote proctoring technologies, learning analytics systems, and AI-driven educational platforms under European data protection law.
3. To evaluate the extent to which current European legal frameworks address issues relating to proportionality, automated decision-making, biometric surveillance, and institutional accountability.
4. To assess the role of the Court of Justice of the European Union (CJEU), the European Data Protection Board (EDPB), and national supervisory authorities in regulating educational data processing.
5. To analyse selected European national legal approaches, particularly within Germany and France, concerning student privacy and educational data governance.
6. To identify doctrinal and enforcement gaps within existing European data protection frameworks governing online learning.
7. To propose legal and regulatory recommendations aimed at strengthening the protection of students' privacy within the European digital education environment.

2.3 Research Questions

[9] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' (2019) 2 *Columbia Business Law Review* 494.

This article addresses the following research questions:

1. To what extent does the GDPR provide adequate legal protection for students' privacy in online learning environments?
2. Do remote proctoring systems and AI-driven educational technologies comply with the principles of proportionality, transparency, and lawful processing under European data protection law?
3. How do European legal frameworks regulate automated decision-making and behavioural profiling within digital educational environments?
4. What legal responsibilities do educational institutions and third-party educational technology providers bear under the GDPR?
5. How have European courts and supervisory authorities approached privacy challenges arising from educational technologies?
6. What doctrinal and regulatory reforms are necessary to strengthen students' privacy protections within the European digital education environment?

3. Methodology

This study adopts a doctrinal legal methodology supported by analytical and descriptive approaches in order to evaluate the adequacy of European legal frameworks governing the protection of students' privacy in online learning environments. The doctrinal methodology is employed to analyse the interpretation, scope, and application of European legal instruments regulating educational data processing, with particular emphasis on the General Data Protection Regulation (GDPR), the European Union Artificial Intelligence Act, Convention 108+, and relevant European regulatory guidance.[10]

The analytical approach is used to examine the legal implications of remote proctoring systems, AI-driven learning analytics, behavioural monitoring technologies, and cross-border educational data transfers within the European digital education environment. Particular attention is devoted to the interpretation of GDPR provisions relating to lawful processing, proportionality, automated decision-making, accountability, joint controllership, and data protection impact assessments.

The study further evaluates the practical enforcement of European data protection law through analysis of decisions issued by the Court of Justice of the European Union (CJEU), the European Data Protection Board (EDPB), and selected national supervisory authorities, including the French Commission Nationale de l'Informatique et des Libertés (CNIL), German data protection authorities, and the Dutch Data Protection Authority.[11]

In addition, the article incorporates examination of selected national legal frameworks within European member states, particularly Germany and France, in order to assess how domestic

[10] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1; Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L.
[11] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (Version 1.1, 4 May 2020).

legislation supplements and interacts with the GDPR in the educational context. Germany's constitutional principle of informational self-determination and France's data protection framework under the *loi Informatique et Libertés* provide important doctrinal perspectives for evaluating the protection of students' privacy within European educational institutions.[12]

The study does not adopt a comparative legal methodology in the strict sense. Rather than systematically comparing multiple legal systems, the research focuses exclusively on European legal frameworks and institutions governing educational data protection. The analysis is therefore confined geographically and doctrinally to the European legal order.

4. European Legal Framework Governing Student Privacy in Online Learning

4.1 The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) constitutes the primary legal framework governing the protection of students' personal data within the European digital education environment. Since its entry into force in 2018, the GDPR has established a harmonised legal regime regulating the collection, processing, storage, and transfer of personal data across European Union member states.[13] Educational institutions, online learning platforms, and educational technology providers processing student data are therefore subject to extensive legal obligations under the Regulation.

Within online learning environments, educational institutions routinely process significant volumes of personal data, including names, identification numbers, academic records, attendance information, behavioural metrics, IP addresses, biometric identifiers, geolocation information, and audiovisual recordings generated through remote learning systems.[14] In many circumstances, such processing extends beyond ordinary educational administration and enters the realm of continuous behavioural monitoring and automated profiling.

The GDPR attempts to regulate such practices through several foundational principles contained in Article 5, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.[15] These principles are particularly important within educational settings because students frequently occupy structurally

[12] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 15 December 1983, BVerfGE 65, 1 (*Volkszählungsurteil*).

[13] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
[14] European Union Agency for Cybersecurity (ENISA), *Data Protection and Privacy in Education* (ENISA Report, 2021).
[15] GDPR, art 5.

vulnerable positions characterised by unequal bargaining power and limited ability to refuse intrusive forms of monitoring imposed by educational institutions.

The principle of data minimisation is especially significant in online learning environments. Under Article 5(1)(c) GDPR, personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Nevertheless, many educational technologies collect excessive quantities of behavioural and biometric data that may exceed what is strictly necessary for educational purposes.[16] Remote proctoring systems, for example, frequently monitor eye movements, facial expressions, background noises, room activity, and browsing behaviour, despite uncertainty regarding the necessity of such extensive surveillance for maintaining academic integrity.

Similarly, the principle of transparency requires educational institutions to provide students with clear and accessible information concerning the nature, purpose, duration, and legal basis of data processing activities.[17] In practice, however, privacy notices provided by educational platforms are often lengthy, technical, and difficult for students to understand. This creates substantial obstacles to meaningful informational autonomy and informed participation within digital educational environments.

4.2 Lawful Basis for Educational Data Processing under Article 6 GDPR

One of the most significant legal issues within online learning concerns the lawful basis upon which educational institutions process students' personal data under Article 6 GDPR.
Educational institutions often rely on multiple legal bases simultaneously, including performance of a public task, contractual necessity, legal obligation, or consent.[18] However, the application of these legal bases within digital education remains controversial.

The use of consent as a lawful basis is particularly problematic in educational environments because consent under the GDPR must be freely given, specific, informed, and unambiguous.[19] Due to the imbalance of power between educational institutions and students, especially within compulsory educational settings, students may not possess a genuine ability to refuse consent without suffering academic disadvantages. Consequently, the European Data Protection Board (EDPB) has repeatedly emphasised that consent should not be relied upon where a clear imbalance exists between the data subject and the controller.[20]

For this reason, many educational institutions instead rely upon Article 6(1)(e), which permits processing necessary for the performance of a task carried out in the public interest. However,

[16] European Digital Rights (EDRi), *Remote Proctoring and Fundamental Rights in Europe*

[17] GDPR, arts 12–14.
[18] GDPR, art 6.
[19] GDPR, art 4(11).
[20] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (Version 1.1, 4 May 2020).

reliance on the public task basis does not eliminate the obligation to comply with proportionality, necessity, and transparency requirements. Educational institutions must therefore demonstrate that intrusive forms of educational monitoring are strictly necessary and proportionate to legitimate educational objectives.

The proportionality principle occupies a central position within European constitutional and data protection law. Measures interfering with privacy rights must be suitable, necessary, and proportionate in relation to legitimate objectives pursued.[21] Consequently, educational institutions cannot justify unlimited surveillance merely by invoking concerns relating to academic integrity or institutional efficiency. The legality of remote monitoring technologies therefore depends upon whether less intrusive alternatives are available and whether the educational benefits outweigh the risks imposed upon students' privacy and dignity.

4.3 Special Categories of Data and Biometric Monitoring under Article 9 GDPR

The increasing use of remote proctoring technologies has generated substantial legal concerns regarding the processing of special categories of personal data under Article 9 GDPR. Remote proctoring systems frequently utilise facial recognition technologies, eye-tracking software, voice recognition systems, keystroke analysis, and behavioural monitoring mechanisms designed to detect suspected academic misconduct during online examinations.[22]

Such practices may involve the processing of biometric data for the purpose of uniquely identifying students, thereby triggering heightened protections under Article 9 GDPR[23] Under the Regulation, processing of biometric data is generally prohibited unless a specific legal exception applies. The legal justification for widespread biometric monitoring within educational environments therefore remains uncertain and contested.

Critics argue that remote proctoring technologies may violate the principle of proportionality because they subject students to extensive surveillance within private domestic environments.[24] Unlike traditional examination settings, remote proctoring systems often require continuous audiovisual monitoring of students' homes, family members, and personal surroundings. This level of intrusion raises significant concerns regarding dignity, autonomy, and informational self-determination.

The principle of informational self-determination, originally developed by the German Federal Constitutional Court in the Census Act Case (*Volkszählungsurteil*) of 1983, remains foundational

[21] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* EU:C:2020:559.
[22] Katarina Lindroos, 'Remote Proctoring, Privacy and Data Protection in Higher Education' (2022) 12 *International Journal of Educational Integrity* 1.
[23] Katarina Lindroos, 'Remote Proctoring, Privacy and Data Protection in Higher Education' (2022) 12 *International Journal of Educational Integrity* 1.
[24] European Digital Rights (EDRi), *Remote Proctoring and Fundamental Rights in Europe* (Policy Brief, 2021).

to European understandings of privacy and data protection.[25] According to this principle, individuals must retain meaningful control over the disclosure and use of their personal information. Continuous algorithmic surveillance within educational settings may therefore conflict with core European constitutional values concerning personal autonomy and democratic participation.

Moreover, remote proctoring technologies may disproportionately affect vulnerable students, including students with disabilities, students lacking adequate private learning spaces, and students from socioeconomically disadvantaged backgrounds. Such technologies may therefore generate indirect forms of discrimination contrary to broader European equality and human rights principles[26]

4.4 Automated Decision-Making and Learning Analytics under Article 22 GDPR

Educational institutions increasingly employ artificial intelligence-driven learning analytics systems capable of monitoring student engagement, predicting academic performance, identifying behavioural risks, and generating automated educational recommendations. These technologies rely upon extensive data aggregation and algorithmic profiling in order to evaluate student behaviour and optimise educational outcomes.[27]

The deployment of such systems raises important legal questions under Article 22 GDPR, which grants individuals the right not to be subject to decisions based solely on automated processing where such decisions produce legal or similarly significant effects.[28] Although educational institutions frequently argue that learning analytics merely support human decision-making, the practical influence of algorithmic systems on academic evaluations, disciplinary interventions, scholarship opportunities, and educational access may nonetheless generate significant consequences for students.

Automated educational profiling creates substantial risks relating to transparency, fairness, and discrimination. AI-driven educational systems frequently operate through opaque algorithmic models that students cannot meaningfully understand or challenge. Consequently, students may become subject to behavioural categorisation or predictive assessments without sufficient awareness regarding how their personal data are processed or how algorithmic conclusions are generated.[29]

[25] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 15 December 1983, BVerfGE 65, 1 (*Volkszählungsurteil*).
[26] Council of Europe, *Artificial Intelligence and Education: Challenges and Opportunities for Human Rights* (Council of Europe Report, 2022).
[27] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' (2019) 2 *Columbia Business Law Review* 494.
[28] GDPR, art 22.
[29] Frank Pasquale, *The Black Box Society* (Harvard University Press 2015).

Furthermore, predictive learning analytics systems may reproduce discriminatory outcomes where algorithms rely upon incomplete, biased, or historically unequal datasets. Students from disadvantaged socioeconomic backgrounds, students with disabilities, or students belonging to minority communities may therefore face disproportionate risks of inaccurate profiling or adverse educational predictions.[30] Such concerns are particularly significant within the European legal order, where the principles of fairness, equality, and human dignity occupy central constitutional positions.

The GDPR attempts to address these risks through obligations relating to transparency, accountability, and meaningful human oversight. Under Articles 13, 14, and 15 GDPR, data subjects possess the right to receive meaningful information concerning the logic involved in automated decision-making processes.[31] In practice, however, educational institutions and private technology providers often provide only limited information regarding the functioning of educational algorithms, thereby weakening students' ability to exercise effective control over their personal data.

The increasing reliance on AI-driven educational systems has also intensified debates regarding the relationship between the GDPR and the European Union Artificial Intelligence Act. The EU AI Act identifies certain educational AI systems as high-risk technologies where they significantly affect students' educational opportunities or assessment outcomes.[32] Consequently, providers and deployers of such systems become subject to additional legal obligations relating to transparency, risk management, data governance, human oversight, accuracy, cybersecurity, and accountability.

The classification of educational AI systems as high-risk technologies represents a significant development within European digital regulation. It reflects growing recognition that algorithmic decision-making within educational environments may substantially affect students' fundamental rights, academic autonomy, and future opportunities. Accordingly, educational institutions deploying AI-based systems must ensure that algorithmic tools remain subject to effective human supervision and that students retain meaningful opportunities to challenge automated outcomes.

4.5 Data Protection Impact Assessments under Article 35 GDPR

Article 35 GDPR requires controllers to conduct Data Protection Impact Assessments (DPIAs) where processing operations are likely to result in high risks to the rights and freedoms of individuals.[33] The use of remote proctoring systems, biometric monitoring technologies, behavioural surveillance mechanisms, and AI-driven learning analytics within educational environments frequently satisfies this threshold due to the scale, sensitivity, and intrusive nature of the processing involved.

[30] Council of Europe, *Artificial Intelligence and Education: Challenges and Opportunities for Human Rights* (Council of Europe Report, 2022).
[31] GDPR, arts 13–15.
[32] Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L.
[33] GDPR, art 35.

DPIAs serve a preventive and risk-management function within European data protection law by requiring organisations to assess necessity, proportionality, security risks, and protective safeguards before implementing high-risk technologies.[34] In educational contexts, DPIAs are particularly important because students frequently possess limited bargaining power and may lack meaningful alternatives to institutional technological requirements.

A legally adequate DPIA should evaluate whether the educational objective pursued could reasonably be achieved through less intrusive means. Educational institutions must therefore consider whether continuous surveillance technologies, behavioural monitoring systems, or biometric verification mechanisms are genuinely necessary to preserve academic integrity or whether less restrictive alternatives could sufficiently achieve the same objective.[35]

Nevertheless, practical implementation of DPIAs within educational institutions remains inconsistent across European member states. Many universities and educational technology providers continue deploying surveillance-based systems without sufficient transparency concerning risk assessments, mitigation measures, or proportionality evaluations. In some cases, institutions have introduced remote proctoring systems rapidly in response to operational pressures without conducting comprehensive privacy impact assessments.[36]

European supervisory authorities have increasingly emphasised the importance of DPIAs in educational settings involving high-risk processing activities. Data protection authorities in several European jurisdictions have warned that educational institutions deploying remote surveillance technologies without adequate risk assessments may violate GDPR obligations concerning accountability and proportionality.[37]

The DPIA requirement therefore represents one of the most important accountability mechanisms available under European data protection law. Properly implemented, it may operate as a safeguard limiting disproportionate surveillance practices and encouraging educational institutions to prioritise privacy-preserving technological alternatives.

4.6 Joint Controllership and Processor Obligations under the GDPR

[34] European Data Protection Board, 'Guidelines on Data Protection Impact Assessment (DPIA)' (WP248 rev.01, 2017).

[35] European Digital Rights (EDRi), *Remote Proctoring and Fundamental Rights in Europe* (Policy Brief, 2021).

[36] Katarina Lindroos, 'Remote Proctoring, Privacy and Data Protection in Higher Education' (2022) 12 *International Journal of Educational Integrity* 1.

[37] French Data Protection Authority (CNIL), 'Educational Technologies and Data Protection Compliance' (CNIL Guidance, 2022).

Online learning environments involve complex legal relationships between educational institutions and third-party technology providers, such as videoconferencing platforms, cloud services, and remote proctoring systems. These relationships raise important legal concerns regarding responsibility and accountability for processing students' personal data.[38]

Under Article 26 GDPR, educational institutions and technology providers may qualify as joint controllers when they jointly determine the purposes and means of data processing. Consequently, universities cannot avoid legal responsibility merely because technical operations are conducted by external companies.[39]

Joint controllership creates shared obligations concerning transparency, lawful processing, protection of students' rights, and data security. However, agreements between institutions and technology providers often lack clarity regarding liability for data breaches or unlawful surveillance practices.[40]

Furthermore, Article 28 GDPR requires educational institutions to ensure that third-party processors comply with European data protection standards and cybersecurity requirements before transferring students' data.[41] These responsibilities become more complex with the increasing use of cloud-based international services, especially following the *Schrems II* judgment concerning international data transfers.[42]

In addition, the GDPR accountability principle under Article 5(2) obliges institutions to demonstrate compliance through internal policies, security procedures, staff training, and documentation practices.[6][43] This accountability obligation has become particularly important with the growing use of artificial intelligence and digital monitoring systems in education.

5. European National Approaches to Student Data Protection

5.1 Germany: Informational Self-Determination and Educational Privacy

Germany has strongly influenced European privacy law through its constitutional protection of informational autonomy and human dignity. The principle of informational self-determination, established by the German Constitutional Court, gives individuals the right to control their personal information. This principle remains important in online learning environments where digital monitoring and remote surveillance may affect students' privacy. Germany also adopts

[38] GDPR, arts 26–28.
[39] GDPR, art 26.
[40] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* EU:C:2018:388.
[41] GDPR, art 28.
[42] *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Schrems II) Case C-311/18, EU:C:2020:559.
[43] GDPR, art 5(2).

strict approaches toward remote proctoring and biometric monitoring technologies, emphasising proportionality and data minimisation.[44]

5.2 France: Data Protection and Educational Technologies

France follows a rights-based approach toward privacy through the *loi Informatique et Libertés* and the role of the CNIL. French authorities stress transparency, proportionality, and cybersecurity when educational institutions use digital learning technologies. The CNIL has also raised concerns regarding intrusive remote surveillance systems used in online education.[45]

6. European Jurisprudence and Regulatory Enforcement

6.1 The Role of the Court of Justice of the European Union (CJEU)

The CJEU has played a major role in strengthening European data protection law. Cases such as *Schrems II* emphasised the protection of personal data transferred outside the European Union, while other decisions expanded the concept of accountability and joint controllership in digital environments.[46]

6.2 European Data Protection Authorities and Regulatory Enforcement

European Data Protection Authorities supervise educational technologies and enforce GDPR obligations. Several authorities have expressed concerns regarding remote proctoring systems, behavioural monitoring, and biometric surveillance in educational settings. However, enforcement practices still differ among European states.[47]

7. Artificial Intelligence and Educational Technologies

7.1 AI-Driven Educational Systems

Artificial intelligence systems are increasingly used in online learning to monitor students, analyse behaviour, and personalise education. While these technologies improve efficiency, they also create risks relating to privacy, discrimination, and automated profiling.[48]

7.2 The EU Artificial Intelligence Act

[44] Bundesverfassungsgericht [BVerfG] 15 December 1983, BVerfGE 65, 1 (*Volkszählungsurteil*).

[45] CNIL, 'Educational Technologies and GDPR Compliance' (2022).

[46] *Schrems II* Case C-311/18, EU:C:2020:559.

[47] European Data Protection Board, 'Guidelines 3/2019 on Video Devices' (2020).

[48] Regulation (EU) 2024/1689 (Artificial Intelligence Act).

The EU Artificial Intelligence Act regulates AI systems through a risk-based approach. Certain educational AI systems may be classified as "high-risk" technologies and therefore become subject to obligations concerning transparency, human oversight, and accountability.[49]

7.3 Remote Proctoring and Educational Surveillance

Remote proctoring technologies use continuous monitoring, facial recognition, and behavioural analysis during online examinations. These systems raise legal concerns regarding proportionality, privacy, and biometric data processing under the GDPR.[50]

8. Institutional Liability and Accountability

Educational institutions and technology providers share responsibility for protecting students' personal data. Universities must ensure that educational platforms comply with GDPR obligations concerning transparency, cybersecurity, and lawful processing.[51]

9. Recommendations

European institutions should establish clearer rules governing educational technologies and AI systems. Educational institutions should prioritise privacy-by-design approaches and conduct proper risk assessments before implementing surveillance-based technologies.

10. Conclusion

European data protection law provides an important framework for protecting students' privacy in online learning environments. However, challenges relating to artificial intelligence, remote surveillance technologies, and accountability mechanisms.

References

- Bundes verfassungs gericht [BVerfG] 15 December 1983, BVerfGE 65, 1 (*Volkszählungsurteil*).
- Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* EU:C:2018:388.
- Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
- CNIL, 'Educational Technologies and GDPR Compliance' (2022).
- Council of Europe, *Artificial Intelligence and Education: Challenges and Opportunities for Human Rights* (2022).
- Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (*Schrems II*) Case C-311/18, EU:C:2020:559.

[49] Artificial Intelligence Act, arts 8–15.
[50] GDPR, arts 5 and 9.
[51] GDPR, arts 24 and 28.

- European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (Version 1.1, 4 May 2020).
- European Data Protection Board, 'Guidelines on Data Protection Impact Assessment (DPIA)' (WP248 rev.01, 2017).
- European Digital Rights (EDRi), *Remote Proctoring and Fundamental Rights in Europe* (2021).
- European Union Agency for Cybersecurity (ENISA), *Data Protection and Privacy in Education* (2021).
- Frank Pasquale, *The Black Box Society* (Harvard University Press 2015).
- GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L119/1.
- German Data Protection Conference (DSK), 'Guidance on Educational Platforms and Remote Examinations' (2021).
- Katarina Lindroos, 'Remote Proctoring, Privacy and Data Protection in Higher Education' (2022) 12 *International Journal of Educational Integrity* 1.
- Paul M Schwartz and Daniel J Solove, *Information Privacy Law* (7th edn, Wolters Kluwer 2021).
- Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L.
- Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' (2019) 2 *Columbia Business Law Review* 494.