

Chapter 3

When the Kids Aren't Alright: The Use of Facial Recognition Technologies at School



Giuseppe Mobilio

Contents

3.1	Introduction	42
3.2	The Applications of FRTs in the School Environment	43
3.3	Ethical Concerns	45
3.4	The Answer of Data Protection Legislation	46
3.4.1	The Defence Based on the Principle of Proportionality	47
3.4.2	The Best Interests of the Child, between Empowerment and Protection	48
3.5	FRTs in the New AIA	54
3.6	Conclusions	58
	References	58

Abstract The use of artificial intelligence in the field of education has great potential. However, applications need to be approached with caution, as in the case of those for surveillance purposes and the use of biometrics. In particular, facial recognition technologies (FRTs) are highly controversial and problematic due to the ethical issues they raise, their intrusiveness on fundamental rights and the technical problems of accuracy. This Chapter looks at the specific use of FRTs on minors in schools as a paradigmatic case to address these concerns.

The analysis will provide a reasoned overview with selected use cases of the application of this AI-based technology in the school environment for different purposes. Considering the ethical implications for the development of children and adolescents, attention will be focused on the legislation applicable to this particular use of FRTs for the protection of children, namely data protection legislation. The legal regime will be assessed through the lens of the principle of proportionality and the principle of the best interests of the child in order to determine whether or not the data protection legislation fails to balance the protection of the fundamental rights and other interests of minors at stake with the actual benefits of the use of FRTs. The Chapter concludes with a look at the recent AIA and how the two pieces of legislation are expected to interact in this specific domain of application.

G. Mobilio (✉)

Department of Juridical Science, University of Florence, Pandette Street, 35, 50127 Florence, Italy
e-mail: giuseppe.mobilio@unifi.it

Keywords Education · Facial recognition · Surveillance · Schools · Proportionality · Best interests of the child · Data protection · AIA

3.1 Introduction

Artificial intelligence in education (AIED) is creating new opportunities for designing and developing learning environments.¹ Algorithmic technologies are transforming the educational landscape, by increasing understanding of students' needs, enhancing teaching performance and personalising learning experience.² As a consequence of these kinds of digital innovations, children are more and more 'datafied',³ i.e. they are becoming objects of a multitude of monitoring devices that generate data about them. Biometrics is an advanced technique for monitoring students, as it allows the automatic recognition of individuals based on their biological and behavioural characteristics.⁴ Among such biological characteristics, facial features deserve specific attention, as AI-based technology can exploit them for the purpose of recognising students, surveilling them, inferring information and, more generally, opening up a wide range of practical benefits for institutions and school communities.

Broadly speaking, facial recognition technologies (FRTs) work by automatically extracting facial features captured on a digital image of a face (so-called biometric template), and then comparing these data with previously analysed facial images already stored in a database (so-called watchlist). These databases contain large numbers of images with associated names and other personal information. FRTs are subtle instruments of surveillance, as they allow a child to be recognised from a distance, without contact, whether they are standing still or moving, and also without their awareness.⁵ Moreover, FRTs can be easily deployed on a large scale around educational systems, because school infrastructures are already prepared to be equipped with these technologies, especially where extensive video monitoring and CCTVs have been widely implemented.⁶ In addition, schools are institutions with relatively stable populations, and FRTs can leverage existing name-and-face photographic databases of school registers as watchlists to recognise children.⁷

However, good educational outcomes do not occur simply by virtue of the use of advanced technologies.⁸ These innovations are going to affect the whole educational community, from schools to educators, parents and—above all—students.

¹ Hwang et al. 2020.

² Seldon and Abidoye 2018.

³ Lupton and Williamson 2017.

⁴ Jasserand 2015, pp. 68–70.

⁵ Berle 2020, p. 5.

⁶ Taylor 2013.

⁷ Andrejevic and Selwyn 2020, p. 120.

⁸ Castañeda and Selwyn 2018.

Careful consideration must be given to the pedagogical, ethical and legal implications deriving from the deployment of these surveillance means, which have not yet been fully addressed. This gap calls for an analysis of whether and how the regulatory framework provides for the protection of children's fundamental rights when dealing with much debated AI systems such as those deploying facial recognition.

This Chapter will focus on the use of FRTs in schools and their impact on students. Sect. 3.2 will describe the most widespread uses of these biometric technologies, mentioning some of the concerns that have been raised so far. In the light of this overview, Sect. 3.3 will analyse the resulting consequences at the ethical level. From Sect. 3.4 onwards the analysis will shift to the legal level and, in particular, will focus on the EU legal system. The objective is to delve into the regulatory response to these issues through data protection legislation, namely the EU General Data Protection Regulation (GDPR).⁹ In particular, the protection of students' rights will be analysed through the lens of the principle of proportionality and the principle of the best interests of the child. In Sect. 3.5, the analysis will focus on the EU Artificial Intelligence Act (AIA),¹⁰ to examine whether this regulation addresses the limitations of the existing legislation. In fact, the GDPR only regulates personal data processed by FRTs, with rules that have been directly enforced by courts and national supervisory authorities to ensure the protection of minors. By contrast, the AIA aims to directly regulate technologies such as facial recognition technology, but risks being less careful about the protection of minors. Section 3.6 will provide some brief concluding remarks.

3.2 The Applications of FRTs in the School Environment

In general FRTs can pursue three main objectives¹¹: *verification*, when the biometric template extracted from the facial image is compared with an existing image (e.g., from the class register) of the individual child; *identification*, when the extracted biometric template is compared with a watchlist of many images (e.g., students of a class); *categorisation*, which is aimed not strictly at identifying a child, but rather at inferring several characteristics from the facial image (such as age or personality traits) and classifying the student into one or more categories. On the basis of these three objectives, it is possible to give an overview of the most widespread uses of FRTs in educational systems.

⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

¹⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), in OJEU of 12.7.2024.

¹¹ Article 29 Data Protection Working Party 2012.

First, FRTs are used for *security control*, i.e. to secure access points, as an alternative to or in addition to locking or monitoring gates, or to monitor movements within school areas. These automated biometric systems make checks cheaper, faster, and possible on a large scale. By means of identification, FRTs will detect if there is someone on school grounds who is not supposed to be there and those people will be denied entry to particular classrooms or the school building. These systems have been used in the USA since the mid-2010s, particularly given the rise of school shootings.¹² In Russia as well, since 2020, thousands of schools have been testing a system named ‘Orwell’ to ensure children’s safety.¹³

A similar application is for school *attendance* checks, where FRTs allow for saving time when it comes to this kind of routine activity. A significative example is offered by India, where in 2020 the Uttar Pradesh government started implementing such AI systems to tackle the issue of fraudulent attendance, both in regard to teachers’ use of proxies and ghost students.¹⁴ But more generally, as education switched online during the pandemic, many schools around the world have adopted attendance systems capable of recording online class participation.¹⁵

FRTs are also used for contactless lunch *payments*, with the aim of reducing administrative burdens for families and school institutions. By means of a combination of identification and verification, the system first confirms the pupil’s identity and then accesses and deducts money from an online account, under the supervision of a catering staff member. In 2019, several schools in North Ayrshire, Scotland, launched a pilot project to enable schoolchildren to make payments of this kind.¹⁶

Another discussed use of FRTs, instead, is the assessment of student *engagement*. CCTVs installed in classrooms are embedded with facial recognition software, and the systems, through categorisation, are able to measure the level of involvement based on facial and nonverbal micro-expressions. The aim is to motivate students to stay focused and keep their minds from wandering and to personalise learning activities that consider students’ emotions and moods, as well as to provide teachers with valuable feedback.¹⁷ Schools in China have recently reported a massive use of FRTs in this way.¹⁸

In the face of this diversity of applications, many voices have been raised calling for caution. Not only in academia,¹⁹ but also among regulators. For example, in October 2021, the UK Information Commissioner’s Office (ICO) stepped in to probe into the use of FRTs in school lunch queues²⁰ and, in light of the investigation, North Ayrshire

¹² Harwell 2018.

¹³ The Moscow Times 2020.

¹⁴ Business Insider 2022.

¹⁵ Kamil et al. 2023.

¹⁶ Weale 2021.

¹⁷ Bala 2020, p. 250.

¹⁸ Connor 2018.

¹⁹ Barrett 2020; Bala 2020; Andrejevic and Selwyn 2020; Berendt et al. 2020, p. 316.

²⁰ Information Commissioner’s Office 2023.

Council paused the implementation of the above-described practices.²¹ In the US, New York State adopted a law in 2020 placing a moratorium on the use of biometric surveillance in schools, although this law seems to have been circumvented.²² The European Parliament has called for a ban on FRTs used for educational purposes.²³ Given these positions, a more in-depth analysis of some key concerns arising from the aforementioned uses of FRTs seems to be warranted.

3.3 Ethical Concerns

The need to consider the ethical issues arising from AIED has become increasingly urgent in recent years.²⁴ Many concerns stem from the view that children and young people are a vulnerable group who deserves special care and protection, especially when in contact with AI-based technologies, internet and social media. Minors' attitudes to privacy risks and their ability to protect themselves from surveillance intrusions are a very sensitive issue. However, a growing body of research demonstrates that children are not oblivious to the consequences of their behaviour as they interact with digital technologies and online environments.²⁵

The use of FRTs in schools interferes with many ethical values that international guidelines and documents pose as requirements for the deployment of AI in education.²⁶ Furthermore, these technologies have a direct impact on the pedagogical context and the quality of education.²⁷

In this respect, we need to consider the use of FRTs *within classrooms*, such as to assess student engagement. This deployment has many negative implications for students. Firstly, considering their *autonomy*, such surveillance narrows the definition of the 'acceptable student',²⁸ based on the (facial) characteristics that an ideal engaged student is supposed to meet through an automated assessment. Normal behaviours can be stigmatised, and those who fall outside that definition and do not fit within narrow standards of acceptability may be punished. Secondly, considering students' *agency*, this type of assessment pushes students to alter their behaviours in order to appear engaged or to 'game the system' by simply forcing themselves to change their facial appearance. The price of this is a curb on their individuality and chilling of their freedom of expression. Thirdly, considering students' *dignity*, there is a shift from active targeting to passive and generalised recognition, which leads to

²¹ BBC News 2021.

²² Miguel and Schwarz 2022.

²³ European Parliament 2021, para 45.

²⁴ Nguyen et al 2023; Holmes et al. 2021; Reiss 2021.

²⁵ Livingstone et al. 2019, pp. 21–22.

²⁶ UNESCO 2019; UNESCO 2021; European Commission 2022.

²⁷ Holmes et al. 2021.

²⁸ Galligan et al. 2020, pp. 43–46.

the dehumanisation of schools.²⁹ Assessment on the basis of schematic representations of facial features is a very reductive engagement with students. More in general, the attempt to detect emotions is largely unachievable given the technical and scientific failure to achieve such a result with certainty.³⁰ Although to a lesser extent, a similar impact on their dignity may result from attendance checks, where the use of biometric technologies risks objectifying the face of pupils and depersonalising the relationship between school institutions and students.³¹

Other implications arise from the use of FRTs *outside the classroom*, such as for security checks and monitoring of students within schools, or payment systems. Constant monitoring in school areas can have the same impact on students' autonomy, agency or dignity as it does within classrooms. In addition, considering students' *development*, careful attention must be paid to the longer-term individual and social impact of engaging with young people during a formative period. Indeed, the implementation of FRTs in schools will potentially normalise the experience of being under constant surveillance from an early age.³² Moreover, considering students' *exercise of freedoms*, surveillance of children may have a profound effect on their privacy expectations in later life.³³

3.4 The Answer of Data Protection Legislation

Given these ethical implications, there is a need to consider what the legal response should be. Currently, the regulation that protects children's fundamental rights against the use of FRTs in schools is data protection legislation.³⁴ While Directive 95/46/EC did not contain any child-specific provisions, Regulation 2016/679 (GDPR) declares that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data' (Recital 38). This statement is followed up with other specific provisions that regard FRTs.³⁵

When applied to these biometric systems, the GDPR is deemed to protect different domains of the so-called 'institutional privacy' of children, in which personal data control is mediated by schools³⁶: namely pupils' 'physical privacy', which is affected by technologies that track, monitor and broadcast children's live images, behaviour or locations; but also their 'informational privacy', which is at stake when children's

²⁹ Andrejevic and Selwyn 2020, p. 121.

³⁰ Barrett 2020.

³¹ Nakar and Greenbaum 2017, p. 120.

³² Galligan et al. 2020, pp. 38–42.

³³ Bala 2020, p. 250.

³⁴ Mobilio 2023.

³⁵ Lievens and Verdoodt 2018, pp. 270–278.

³⁶ Livingstone et al. 2019, pp. 13–14.

personal data are collected, stored or processed.³⁷ In addition, by protecting personal data, the GDPR indirectly provides protection for other rights, freedoms, interests and ethical values that are at stake when one is dealing with AIED, such as freedom of expression, freedom of assembly or the right to education.³⁸

Considering all the ethical concerns discussed above in Sect. 3.3, the question is whether, and to what extent, this regulation achieves its objective of protection, given that we are talking about biometric technology, special subjects such as children, and a specific context such as schools. In order to attempt an answer, we need to consider that the use of FRTs in schools creates a conflict between interests that translates into the need to balance the protection of fundamental rights and other interests of minors with the achievement of different practical benefits, as seen in Sect. 3.2. In legal terms, the principle of proportionality and the principle of the best interests of the child come to the fore in this balancing assessment. The relationship between these two principles is complex and warrants a more in-depth analysis than can be carried out here.³⁹ For the purposes of this discussion, the two principles will be considered as complementary and will be used to examine whether the GDPR offers sufficient protection to students.

3.4.1 *The Defence Based on the Principle of Proportionality*

When considering the consequences of the use of FRTs in terms of the restriction of fundamental rights, the criterion for assessing the legitimacy of such use is the *principle of proportionality*.⁴⁰ In general, Article 52(1) of the Charter of Fundamental Rights of the European Union (CFREU) refers to the principle of proportionality as the criterion for striking the right balance between the objectives pursued by a particular measure and the sacrifice of rights. According to the Court of Justice of the EU (CJEU), the principle of proportionality requires that legal acts be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.⁴¹ The Council of Europe has also laid down a similar provision with specific regard to children's rights in the digital environment.⁴² However, the principle of proportionality is the criterion not only for assessing the legitimacy of a law that allows a limitation of fundamental rights, but also, according to the GDPR, for assessing *ex ante* the legitimacy of a measure in a specific situation, such as

³⁷ UNICEF 2018, p. 8.

³⁸ Simoncini and Longo 2021, p. 38.

³⁹ Committee on the Rights of the Child 2021, para 69.

⁴⁰ Barak 2012, p. 243; Dalla Corte 2022; Mobilio 2023.

⁴¹ *Ex multis*, CJEU Judgement of 6 October 2020, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*, ECLI:EU:C:2020:791, para 46.

⁴² Council of Europe 2018, para 38

the concrete use of FRTs. Therefore, the actual benefits of using FRTs must be balanced with the sacrifice of fundamental rights of students; hence, ‘personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means’.⁴³ The main tool for carrying out this balancing is the data protection impact assessment (DPIA),⁴⁴ which must include at least ‘an assessment of the necessity and proportionality of the processing operations in relation to the purposes’.⁴⁵

In this respect, the national data protection authorities have provided useful guidelines for better addressing whether the concrete use of FRTs in the school environment can be considered proportionate or not. The French Data Protection Authority (Commission nationale de l’informatique et des libertés—CNIL) reached a decision on FRTs installed at the entrances of two French high schools for security purposes, specifically to assist school officials in preventing intrusions and to reduce the time of checks; measures to which the students had previously consented. The CNIL ruled that such controls were in violation of the principle of proportionality, as there were much ‘less invasive means’ to achieve the same purpose in terms of privacy and individual freedoms, such as the use of badges.⁴⁶ The same conclusions were drawn by the Swedish Data Protection Authority (Integritetsskyddsmyndigheten—IMY) in a case where FRTs were used instead to monitor students’ attendance. The use of these technologies was judged to be too ‘intrusive’ with regard to the personal integrity of students and excessive compared to what was necessary to monitor their attendance.⁴⁷ A similar disproportion can be seen in the different uses of FRTs for functions such as making payments (where, for example, prepaid cards can be used), and even more so where they are used to assess student engagement (rather than, for example, more educators).

In conclusion, to protect children’s rights, data protection legislation, through the principle of proportionality, imposes strict conditions on the use of biometric surveillance that would be very difficult to meet.

3.4.2 The Best Interests of the Child, between Empowerment and Protection

A different criterion for balancing the interests at stake when using FRTs in schools is offered by the *principle of the best interests of the child*. This principle assists both regulators in adopting policies and general rules, and judges in making decisions in specific situations, by requiring an assessment appropriate to the specific context; under this principle, the special value of children is given priority over all other

⁴³ Recital 39 GDPR.

⁴⁴ Demetzou 2019.

⁴⁵ Article 35(7)(b) GDPR

⁴⁶ Commission nationale de l’informatique et des libertés 2019.

⁴⁷ Swedish Data Protection Authority 2019.

compelling interests.⁴⁸ At the same time, the principle has also been criticised for its breadth and open-ended, indeterminate nature, and for its exposure to cultural relativism.⁴⁹

Many legal sources cite the principle of the best interests of the child and a large body of case law has helped to refine it: this principle was first affirmed by the UN Convention on the Rights of the Child (Article 3.1),⁵⁰ and then reaffirmed by the CFREU (Article 24).⁵¹ At EU level, it has been developed in the context of regulation on the internal market and the Area of Freedom, Security and Justice, with a direct impact on family law cases.⁵² But now it can be considered as a general principle to be taken into account when interpreting and assessing the legality of the relevant secondary legislation in order to ensure that the child's best interests are given primary consideration.⁵³

Within this legal framework, the principle seeks to reconcile the dual objectives of ensuring the protection and welfare of children, on the one hand, and their autonomy and agency, on the other.⁵⁴ For its own part, the GDPR tries to address the so-called 'empowerment versus protection dilemma', that is, the need to empower children as digital users able to grasp the opportunities of playing, learning and communicating, while protecting them from privacy violations and harms.⁵⁵

Thus, the analysis will now focus on the provisions of the GDPR that more directly address this dilemma vis-à-vis FRTs, namely the provisions related to the values of awareness (for empowerment) and inclusion (for protection). The aim is to examine whether this regulation adequately considers the best interests of the child in relation to both of these needs, thereby protecting students against the potential harms arising from FRTs.

⁴⁸ Eekelaar 1994; Freeman 1993.

⁴⁹ Alsto and Gilmour-Walsh 1996.

⁵⁰ States 'should have regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied' (Committee on the Rights of the Child 2021, para 13).

⁵¹ Although there is no direct reference to it in the European Convention on Human Rights (ECHR), the European Court of Human Rights (ECtHR) largely uses it as a criterion for interpretation.

⁵² Lamont 2021, pp. 694–703.

⁵³ CJEU Judgement of 6 June 2013, *MA et al. v. Secretary of State for the Home Department*, C-648/11, ECLI:EU:C:2013:367, para 57 ff.

⁵⁴ Verhellen 2015, pp. 50–52; McGlynn 2002, p. 397. According to the UNCRC, the former is reflected in the right to be heard (Article 12), while the second in the right to non-discrimination (Article 2) in relation to the right to education (Articles 28–29) (UN Committee on the Rights of the Child 2013, para 41–43).

⁵⁵ Macenaite 2017.

3.4.2.1 Learner Awareness

The GDPR protects the student's awareness and freedom to choose whether to be subject to FRTs in three main ways. The first one is related to the legal ground. Data processed by FRTs, such as biometric templates, are qualified as 'biometric data'⁵⁶; consequently, the GDPR prohibits the processing of such data unless they are covered by one of the exceptions provided for in Article 9.

Should the use of FRTs fall within the institutional activities of the school, the processing could be considered, according to Article 9(2)(g)GDPR, necessary for reasons of '*substantial public interest*', as long as the use is regulated 'on the basis of Union or Member State law'. In this case, the use of such technologies does not require the student's permission. However, 'reasons of substantial public interest' is a very high standard to meet,⁵⁷ as the Swedish IMY also found in the aforementioned case that the school's monitoring did not fall within this case.

By contrast, when the use of FRTs does not fall under this exception, the legal ground is offered by the *explicit consent*⁵⁸ of students for the automated processing of their facial images in relation to the defined purposes.⁵⁹ In this way, greater awareness should be guaranteed. Indeed, the GDPR specifies that consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes.⁶⁰ However, in the case of students, the freedom of consent is generally undermined by an imbalance of power.⁶¹ A decision of the Bulgarian Commission for Personal Data Protection (CPDP) in 2020 explicitly underlined this aspect.⁶² When asked to rule on an access control system with FRTs and body temperature monitoring for COVID-19 installed by a school, the CPDP declared that the only basis for processing personal data that could apply is consent. However, it stressed that consent in a hierarchical relationship between a principal and a student is an inappropriate ground, because of doubts that it is not freely given. Consent will also not be free in cases where there are no alternatives to the use of FRTs that are easy to implement.⁶³

The use of consent as a legal ground for data processing by public authorities is not totally excluded, as long as students are not denied education or services and can refuse the use of these technologies without any detriment.⁶⁴ However, there is still a risk that consent does not indicate actual awareness. FRTs, in fact, accentuate the crisis of the traditional principle of 'notice and consent': as it is well known, limited

⁵⁶ Article 4(1)(14) GDPR.

⁵⁷ Raposo 2022, p. 11.

⁵⁸ Article 9(2)(a) GDPR.

⁵⁹ No parental consent is strictly required, because the provisions of Article 8 GDPR regarding conditions for a child's consent applies only for information society services (as per Article. 4(25) GDPR, which refers to Directive EU 2015/1535), and therefore not for FRTs.

⁶⁰ Article 4(1)(11) GDPR.

⁶¹ European Data Protection Board 2020, para 16–24.

⁶² Bulgarian Commission for Personal Data Protection 2020.

⁶³ Consultative Committee of the Convention 108 2021, p. 7.

⁶⁴ European Data Protection Board 2020, para 20.

understanding, lack of available time, and information asymmetries are all elements that result in consent being given automatically, and without full awareness.⁶⁵

The second way of ensuring student awareness is related to *information*. Regardless of whether or not they have actually given their consent, students have the right to receive certain information about the use of FRTs, as a corollary of the principle of transparency.⁶⁶ They must be able to exercise this right before recognition takes place, or in any case at the time facial images are collected, in order to avoid students being subjected to FRTs without their awareness. In particular, schools must make available various types of information about the use of FRTs, such as the legal basis, the purposes of the processing, the data retention period, the right to withdraw consent, and at least 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.⁶⁷

However, as the UK ICO emphasised in its opinion on the use of FRTs for payments, the provision of this type of information does not necessarily mean greater awareness; therefore, there is an issue of effectiveness here too. Technical terms may be unfamiliar not only to children, but also to parents. Hence, these individuals may benefit from an explicit explanation, in age-appropriate language, of how children's data will be collected, used, stored and retained.⁶⁸ This is the proper application of the GDPR, which states that information must be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'.⁶⁹

The third way of ensuring student awareness is related to *human supervision*. The intervention of a human being prevents machines from taking autonomous decisions that have a negative impact on people and provide him or her with a higher level of awareness.⁷⁰ According to the GDPR, students 'have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.⁷¹

Typically, the use of FRTs in schools does not involve a decision 'based solely on automated processing', because the intervention of a person, such as a school security official, or a teacher in the case of engagement assessment, is expected in any case. However, this supervision remains crucial because, from the educator's standpoints, machines could never replace human judgement, but at most support it,

⁶⁵ Custers et al. 2022, pp. 466–469.

⁶⁶ Article 5(1)(a) GDPR.

⁶⁷ Article 13 GDPR.

⁶⁸ Information Commissioner's Office 2023.

⁶⁹ Article 12(1) GDPR. See also Recital 58.

⁷⁰ European Commission 2019, p. 4.

⁷¹ Article 22(1) GDPR. This regime does not apply where the legal ground – as mentioned above – is 'substantial public interest' (Article 22(2) GDPR), or 'explicit consent' (Article 22(3) GDPR). Nevertheless, invoking these exceptions should be avoided, as the same GDPR states in Recital 71 that such measures 'should not concern a child'.

since algorithms and AI systems lack self-reflection and social abilities.⁷² At the same time, as far as students are concerned, exposure to purely automated surveillance would create a sense of resignation and internalisation of authority which could be detrimental to their educational process.⁷³

However, the danger of uncritically relying on intelligent machines always lurks.⁷⁴ In this case there is a risk of overlooking the need for greater awareness on the part of both students and teachers. But more importantly, in the case of facial recognition errors—as will be clarified in the next Section—the consequence is that humans will be prompted to follow the machine’s suggestions, which could lead to mistakes. This could be to the detriment of individual students or certain categories of students, leading to a misplaced focus of control on them or a negative evaluation of their engagement.

3.4.2.2 Equity and School Inclusiveness

The second need that the GDPR seeks to address, in accordance with the principle of the best interests of the child, is the protection of students, notwithstanding the other benefits that may arise from the use of FRTs. This need, in the perspective discussed here, is met through the construction of a more equitable and inclusive school.⁷⁵ Equity and inclusiveness in a school environment where algorithmic technologies are deployed depend mostly on how reliably the technologies operate, i.e. they should not produce harmful errors and should likewise not cause discrimination.⁷⁶

The use of FRTs in schools is motivated by the assumption that they enable more efficient and equal supervision or assessments of pupils. However, there is a growing body of literature that directly correlates the accuracy of FRTs with the quality of the algorithmic training datasets, i.e. the absence of *bias*.⁷⁷ The more biased the datasets are—because they do not contain enough high-quality facial images of people of a certain gender, age or ethnic origin—the less accurate the recognition of the misrepresented people will be, leading to discrimination.⁷⁸

Tests carried out on datasets and facial recognition algorithms show that recognition errors increase exponentially according to the age of the person they are trying to recognise.⁷⁹ From a technical point of view, it is clear that the images of young people generate a higher number of false negatives than those of adults, due to the rapid growth and changes in facial physiognomy that occur during their development. In this case, it is sufficient to compare a facial image taken in youth with images of

⁷² Xu and Ouyang 2021.

⁷³ Andrejevic and Selwyn 2020, p. 123.

⁷⁴ Article 29 Data Protection Working Party 2017, p. 10.

⁷⁵ UNESCO 2019, para 22–24.

⁷⁶ Nguyen et al., 2023, pp. 4232–4233.

⁷⁷ Zuiderveen Borgesius 2018, p. 17.

⁷⁸ Leslie 2020.

⁷⁹ Grother et al. 2019, p. 2.

the same individual after only five years have passed and the accuracy of recognition will be compromised. In general, therefore, it has been demonstrated that the current state of technology makes the analysis of images of children under the age of thirteen less reliable.⁸⁰ This is why children need to be overrepresented in the construction of training datasets⁸¹, while in the construction of watchlists facial images should be refreshed continuously.

The concern when it comes to minors is also linked to the fact that, more generally, black people and females are grossly underrepresented in training datasets.⁸² As a result, FRTs will be less accurate for dark-skinned women than for light-skinned men of Caucasian origin, especially if the facial image is not captured under optimal conditions (lighting, posture, etc.).⁸³

As a result, the inaccuracy of FRTs can undermine the hypothetical benefits of their use, paradoxically leading to less personalised education, less effective checks and less accessible services. Data protection legislation tackles bias and accuracy where it states that personal data, also when used to train FRTs or to create watchlists, should be 'accurate and, where necessary, kept up to date'; for this reason, schools wishing to employ FRTs must take every 'reasonable step' to ensure that 'personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.⁸⁴ Accordingly, schools should implement appropriate 'technical and organisational measures' in order to prevent 'discriminatory effects'.⁸⁵ The UK ICO also stressed that 'to ascertain whether the algorithm is sufficiently accurate [the authority using FRTs] should seek information and assurances from the supplier about how the algorithm was trained (is the training data sufficiently representative?) and what kind of bias testing has been conducted'.⁸⁶

However, this objective is not easily achievable, mainly because the search for bias or discrimination is not an explicitly mentioned justification for processing biometric data.⁸⁷ As a result, it may be difficult for someone other than the providers who develop FRTs to test a training dataset in search of bias, due to the lack of a legal ground. Furthermore, it will be difficult to replace or correct systems currently in use due to the widespread use of FRTs trained on non-representative data.⁸⁸

⁸⁰ European Union Agency for Fundamental Rights 2018, p. 90.

⁸¹ Han and Jain 2014.

⁸² Cook et al. 2019; Merler et al. 2019.

⁸³ Buolamwini and Gebru, 2018.

⁸⁴ Article 5(1)(d) GDPR.

⁸⁵ Recital 71 GDPR.

⁸⁶ Information Commissioner's Office 2023.

⁸⁷ European Union Agency for Fundamental Rights 2022, p. 26.

⁸⁸ Hacker 2018, p. 1150.

3.5 FRTs in the New AIA

Data protection legislation offers different levels of protection against the use of FRTs in schools: more pronounced in the application of the proportionality principle, while it risks being less effective in meeting the best interests principle. However, the regulation of AI-based technologies is moving forward, as the EU institutions have just approved a new Regulation ‘laying down harmonised rules on artificial intelligence’ (so-called *AIA*).

The AIA reflects the EU’s effort to develop a coordinated approach to the human and ethical implications of AI through a legal framework that addresses the risks associated with certain uses of AI. The aim is, on the one hand, to implement a trustworthy AI and, on the other, to foster the development of a Digital Single Market in the EU.⁸⁹

The new regulation employs a risk-based approach,⁹⁰ distinguishing between “Prohibited AI practices”, “high-risk AI systems” and AI systems associated with ‘transparency obligations’, each associated with different conditions. Therefore, we must first examine the conditions under which it will be possible to use FRTs in schools according to this regulation.

Within the first category, since Commission’s proposal, the regulation bans ‘the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for law enforcement purposes’, except under specific conditions therein provided for.⁹¹ However, the final version of the regulation also prohibits the scraping of facial images from the internet or CCTV and, more relevant here, the use of AI systems ‘to infer emotions of a natural person in the areas of [...] education institutions’.

Within the second category of ‘high risk’ systems, the AIA distinguishes between ‘Biometrics’ and ‘Education and vocational training’.⁹² In the first case, the regulation considers: biometric identification of natural persons outside the prohibited uses; AI systems used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics (evidently outside the school environment). In the second case, the regulation considers: AI systems used for determining access or admission or assigning natural persons to educational and vocational training institutions; AI systems used for evaluating learning outcomes; AI systems used for assessing the appropriate level of education that individual will receive or will be able to access; AI systems used for monitoring and detecting prohibited behaviour of students during tests. Significantly, the regulation does not consider as ‘high-risk’ AI systems intended to be used for ‘biometric verification the sole purpose of which is to confirm that a specific natural

⁸⁹ Laux et al. 2024.

⁹⁰ De Gregorio and Dunn, 2022.

⁹¹ Article 5 AIA.

⁹² Annex III AIA. Article 26(10) also explicitly considers, with some exceptions, AI systems for post-remote biometric identification for law enforcement purposes to be ‘high risk’ and sets out further conditions for this specific use.

person is the person he or she claims to be'. The regime for 'high risk' systems is inspired by that of the New Legislative Framework and imposes numerous burdens on all value chain participants, especially providers before they can place technology on the market.⁹³ Providers must demonstrate compliance with such obligations by undergoing a 'conformity assessment' as an internal control check that, once passed, allows the CE mark to be affixed to high-risk AI systems.⁹⁴

In the last category of AI systems, the regulation states that 'emotion recognition systems' and 'biometric categorisation systems' (which are also classified as high-risk) are also subject to 'transparency obligations', in the sense of an obligation to inform the persons exposed thereto.⁹⁵

In sum, based on the examples in Sect. 3.2, the use of FRTs in schools is not generally prohibited,⁹⁶ while in others it is considered as 'high risk'.⁹⁷ FRTs are 'high risk' AI systems when they are used:

to perform security checks in 'real time' (i.e., where the capturing of the biometric data, the comparison and the identification occur all instantaneously or without a significant delay)⁹⁸ and/or 'ex post' (i.e., where the biometric data have already been captured, and the comparison and identification occur only after a significant delay)⁹⁹, other than by law enforcement authorities; in relation to payments or attendance verification, if there is a 'live' identification coupled with verification; to assess student engagement, without inferring emotions, e.g. when analysing only facial micro-expressions (but it would be very hard to argue that there is no inference of emotion, such as satisfaction, in this case). In this case, schools must comply with 'transparency obligations'.

The new regulation will coexist with the current data protection legislation. However, we need to ask how the two pieces of regulation will coexist. In general, it has been observed that the AIA is to be implemented without prejudice to the EU data protection acquis, so that the applicability of the latter in its entirety will not in any way be affected by the AIA.¹⁰⁰ Nevertheless, there may be tensions between the two regulatory frameworks that affect the protection of fundamental rights, even if they are not explicit.

In some aspects, the two regulations are expressly related, such as for the processing of biometric data in the case of remote biometric identification for purposes other than law enforcement.¹⁰¹ In other aspects, the two regulations do

⁹³ European Parliamentary Research Service 2021.

⁹⁴ Article 43 AIA.

⁹⁵ Article 50(3) AIA.

⁹⁶ Despite the Commission's proposal, categorisation or emotion recognition is now prohibited in schools; see Kind 2021.

⁹⁷ Kind 2021.

⁹⁸ Recital 8 AIA.

⁹⁹ Recital 8 AIA.

¹⁰⁰ Mazzini and Scalzo, 2023, p. 14.

¹⁰¹ Recital 39 AIA.

not overlap and are in fact complementary. This is the case with the consent rules, which will continue to apply to allow the use of FRTs and the processing of personal and biometric data.

Moreover, through this complementarity, the AIA sometimes creates the conditions to facilitate the enforcement of the GDPR. This is the case of the rules on ‘transparency and provision of information to deployers’,¹⁰² which impose on the provider (who develops FRTs) the obligation to provide the user or the deployer (in our case schools) with several items of information.¹⁰³ The information will allow the schools to better comply with their own obligation to provide information to the students who are subjected to FRTs, in accordance with the GDPR and the best interests principle. Another case is the risk management system, which must be applied throughout the entire lifecycle of a high-risk AI system.¹⁰⁴ The aim is to identify, analyse, mitigate or eliminate the most likely risks to fundamental rights, with specific consideration given to the impact on children.¹⁰⁵ This type of assessment could be a useful basis for subjecting FRTs to the proportionality test.

There are also cases in which the AIA and the GDPR do not overlap, but one limits the scope of the other. This is the case where the AIA directly regulates FRTs, imposing some conditions on their legitimate use and, consequently, setting limits on the application of the GDPR. We are referring to the prohibited uses set out in the regulation, as well as the many voices that have demanded an extension of the list of prohibited uses. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces and for categorising individuals into clusters according to any grounds for discrimination under Article 21 CFREU.¹⁰⁶ Civil society organisations¹⁰⁷ and academics¹⁰⁸ have also called for a ban on FRTs for non-law enforcement agencies, such as schools, given the evidence that they engage in mass biometric surveillance. The EU Parliament pushed (unsuccessfully) to include in the list of prohibited AI practices some uses of FRTs relevant here, such as ‘real-time’ remote biometric identification systems in publicly accessible spaces.¹⁰⁹ Here we see a shift in regulatory policy: from a general regulation of AI-based technologies to the regulation of a specific type of technology. It is the AIA in itself that balances the different freedoms and interests at stake, on the assumption that, in the case of FRTs and education or minors, there can be an absolute presumption of disproportionality and an excessive sacrifice of the child’s

¹⁰² Article 13 AIA.

¹⁰³ Such as the level of accuracy, robustness and cybersecurity; risks to fundamental rights; performance as regards the persons or groups of persons on which the system is intended to be used; relevant information in terms of the training, validation and testing data sets.

¹⁰⁴ Article 9(2) AIA.

¹⁰⁵ Article 9(8) AIA.

¹⁰⁶ EDPB and EDPS 2021.

¹⁰⁷ EDRi 2021.

¹⁰⁸ Smuha et al. 2021.

¹⁰⁹ European Parliament 2023.

interests. However, the legislator should be aware of the risk that the regulation may soon become obsolete, given the rapid development of biometric technologies in recent years.

Finally, we must consider the cases in which the AIA and GDPR overlap. Here the problem lies, first and foremost, in the difficulties of interpretation that arise from the possible lack of connection. Just think of the different definition of 'biometric data', which the GDPR defines as data resulting from (i) specific technical processing of (ii) personal data relating to the physical, physiological or behavioural characteristics, with the aim of (iii) uniquely identifying a person, while the AIA omits the purpose of identification.¹¹⁰ However, such a lack of connection risks, above all, weakening the protection of students against FRTs. For example, there is an increase in protection where the AIA provides for the requirement of human oversight,¹¹¹ specifically where it states that two individuals must verify and confirm facial recognition matching, having been enabled by the measures adopted to correctly interpret the system's output and decide whether to disregard, override or reverse it: here the AIA establishes a framework that lends substance to the meaningful human involvement required by the GDPR,¹¹² again in accordance with the best interests principle.

In other parts of the regulation, the enhancement of the protection of fundamental rights risks being more apparent than effective, as in the case of data quality and bias. The AIA recognises that the technical inaccuracies of FRTs can lead to biased results and entail discriminatory effects due to the age of people.¹¹³ Therefore, training, validation and testing data sets should be subject to appropriate data governance and management practices, to ensure that they are relevant, representative, free of errors and complete.¹¹⁴ Datasets will consider the specific geographical, behavioural or functional setting within which FRTs will be used.¹¹⁵ Bias monitoring, detection and correction will be separate justifications for the processing of sensitive categories of personal data as part of the measures taken to ensure compliance with the quality standards for 'high-risk' AI systems.¹¹⁶

Compared with the generic provisions of the GDPR, the requirements set forth by the AIA are more precise. However, we should not forget that the enforcement of the new rules is left up to providers, leaving them too much discretion in the assessment of 'adequacy'.¹¹⁷ In addition, requirements such as 'error-free' or 'complete' can almost never be fully met in a large-scale AI training dataset without setting a qualitative threshold.¹¹⁸ This threshold is particularly problematic if it is to be parametrised for minors, because of the difficulties outlined in Sect. 3.4.2.

¹¹⁰ Article 4(1)(14) GDPR and Article 3(1)(34) AIA.

¹¹¹ Article 14(5) AIA.

¹¹² Mazzini and Scalzo, 2023, p. 15.

¹¹³ Recital 32 AIA.

¹¹⁴ Article 10(3) AIA.

¹¹⁵ Article 10(4) AIA.

¹¹⁶ Article 10(5) AIA.

¹¹⁷ Smuha et al. 2021, p. 24.

¹¹⁸ Hacker 2021, p. 298.

The last example suggests that the AIA could include more specific provisions for minors—such as those found in the GDPR—consistently with Recital 48 of the regulation, which recalls children’s rights according to Article 24 CFREU and the UN Convention on the Rights of the Child, ‘both of which require consideration of the children’s vulnerabilities and provision of such protection and care as necessary for their well-being’.

3.6 Conclusions

AI-based technologies are becoming increasingly widespread in education. FRTs, in particular, deserve special consideration. The many uses that these biometric technologies can find are accompanied by just as many significant concerns. This type of surveillance can have a direct impact both on the construction of the educational system and on the development of the school-age children. The protection of the fundamental rights of minors is supposed to be guaranteed by data protection legislation. The analysis has attempted to show how this legislation offers a very high threshold of protection, if the principle of proportionality is applied, in that it is designed to prevent the use of FRTs in schools for purposes that could well be achieved by other means. On the other hand, this legislation runs the risk of not really meeting the requirements underlying the principle of the best interests of the child, namely to ensure greater awareness among pupils and equity in the school system. In the light of these considerations, attention needs to be shifted to the AIA, to assess whether this regulation not only seeks to maintain the level of protection of personal data legislation, but also helps to remedy some of its limitations, in the event that FRTs find their way into schools. In the near future, therefore, it will be crucial to read the two regulations in an integrated way.

Funding The research is supported by the project ‘SE.CO.R.E. TECH: Self- and Co-Regulation for Emerging Technologies: Towards a Technological Rule of Law’, funded by the Italian Ministry for University and Research’s (MUR’s) ‘Progetti di Ricerca di Rilevante Interesse Nazionale’ (PRIN; Bando 2017—grant prot. no. 2017SW48EB).

References

- Alston P, Gilmour-Walsh B (1996) The Best Interests of the Child Towards a synthesis of children’s rights and cultural values. Innocenti Studies, https://www.unicef-irc.org/publications/pdf/is_best_interest_eng.pdf Accessed 30 January 2024.
- Andrejevic M, Selwyn N (2020) Facial Recognition Technology in Schools: Critical Questions and Concerns. *Learning, Media and Technology* 2(45): 115–128, <https://doi.org/10.1080/17439884.2020.1686014>.
- Article 29 Data Protection Working Party (2012) Opinion 02/2012 on facial recognition in online and mobile services, WP 192, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf Accessed 30 January 2024.

- Article 29 Data Protection Working Party (2017) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251, 3 October 2017, <https://ec.europa.eu/newsroom/article29/redirection/document/49826> Accessed 30 January 2024.
- Bala N (2020) The danger of facial recognition in our children's classrooms. *Duke Law & Technology Review*, 18: 249–267.
- Barak A (2012) Proportionality: Constitutional rights and their limitations. Cambridge University Press, <https://doi.org/10.1017/CBO9781139035293>.
- Barrett L (2020) Ban Facial Recognition Technologies For Children—And For Everyone Else. *Boston University Journal of Science & Technology Law*, 26(2): 223–285.
- BBC News (2021) Schools pause facial recognition lunch plans, 25 October 2021, <https://www.bbc.com/news/technology-59037346> Accessed 30 January 2024.
- Berendt B, Littlejohn A, Blakemore M (2020) AI in education: learner choice and fundamental rights. *Learning Media and Technology*, 45(3): 312–324 <https://doi.org/10.1080/17439884.2020.1786399>.
- Berle I (2020) *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*. Springer International Publishing, <https://doi.org/10.1007/978-3-030-36887-6>
- Buolamwini J, Gebre T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 81: 77–91. <http://proceedings.mlr.press/v81/buolamwini18a.html> Accessed 30 January 2024.
- Business Insider (2022) Uttar Pradesh to start marking school attendance using facial recognition, 11 December 2022, <https://www.businessinsider.in/india/news/uttar-pradesh-to-start-marking-school-attendance-using-facial-recognition/articleshow/96145648.cms> Accessed 30 January 2024.
- Castañeda L, Selwyn N (2018) More than tools? Making sense of the ongoing digitizations of higher education. *International Journal of Educational Technology in Higher Education*, 15(22): 1–10 <https://doi.org/10.1186/s41239-018-0109-y>.
- Christakis T, Becuywe M, AI-Regulation Team (2021) Facial recognition in the draft European AI Regulation: Final report on the high-level workshop held on April 26, 2021. AI-Regulation.com, <https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/> Accessed 30 January 2024.
- Commission nationale de l'informatique et des libertés, Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position, 29 October 2019, <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position> Accessed 30 January 2024.
- Committee on the Rights of the Child (2021) General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation> Accessed 30 January 2024.
- Connor N (2018) Chinese school uses facial recognition to monitor student attention in class. *The Telegraph*, 17 May 2018, <https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/> Accessed 30 January 2024.
- Consultative Committee of the Convention 108 (2021) Guidelines on facial recognition (T-PD(2020)03rev4), <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> Accessed 30 January 2024.
- Cook C M, Howard J J, Sirotin Y B, Tipton J L, Vemury A R (2019) Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1(1): 32–41 <https://doi.org/10.1109/TBIOM.2019.2897801>.

- Council of Europe (2018) Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a> Accessed 30 January 2024.
- Custers B, Fosch-Villaronga E, van der Hof S, Schermer B, Sears A M, Tamò-Larrieux A (2022) The role of consent in an algorithmic society—Its evolution, scope, failings and re-conceptualization. In Kosta E, Leenes E (ed) *Research Handbook on EU Data Protection Law*. Edward Elgar, 455–473.
- D Leslie (2020) Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute, <https://doi.org/10.5281/ZENODO.4050457> Accessed 30 January 2024.
- Dalla Corte L (2022) On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*, 12(4): 259–275, <https://doi.org/10.1093/idpl/ipac014>.
- De Gregorio G, Dunn P (2022) The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, 59(2): 473–500, <https://doi.org/10.54648/COLA2022032>.
- Demetrou K (2019) Data Protection Impact Assessment: A tool for accountability and the unclarified concept of ‘high risk’ in the General Data Protection Regulation. *Computer Law & Security Review*, 35(6): 1–14, <https://doi.org/10.1016/j.clsr.2019.105342>.
- EDRi (2021) EU’s AI law needs major changes to prevent discrimination and mass surveillance, <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/> Accessed 30 January 2024.
- Eekelaar J (1994) The Interest of the Child and the Child’s Wishes: The Role of Dynamic Self-determinism. *International Journal of Law and the Family*, 8: 42–61.
- European Commission (2019) Communication “Building Trust in Human-Centric Artificial Intelligence”, COM(2019) 168 final, 8 April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58496 Accessed 30 January 2024.
- European Commission (2022) Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, <https://op.europa.eu/en/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1/language-en> Accessed 30 January 2024.
- European Data Protection Board (2020) Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1, 4 May 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf Accessed 30 January 2024.
- European Data Protection Board, European Data Protection Supervisor (2021) EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf Accessed 30 January 2024.
- European Parliament (2021) Report on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)), 19 April 2021, https://www.europarl.europa.eu/doceo/document/A-9-2021-0127_EN.html Accessed 30 January 2024.
- European Parliament (2023) Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html Accessed 30 January 2024.
- European Parliamentary Research Service (2021) Regulating facial recognition in the EU, PE 698.021, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf) Accessed 30 January 2024.
- European Union Agency for Fundamental Rights (2018) Under watchful eyes—biometrics, EU IT-systems and fundamental rights, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf Accessed 30 January 2024.

- European Union Agency for Fundamental Rights (2022) Bias in algorithms—Artificial intelligence and discrimination, <https://op.europa.eu/en/publication-detail/-/publication/c5bdd489-7cf4-11ed-9887-01aa75ed71a1> Accessed 30 January 2024.
- Freeman M D A (1993) Laws, conventions and rights. *Children & Society* 7(1): 37–48.
- Galligan C, Rosenfeld H, Kleinman M, Parthasarathy S (2020) Cameras in the Classroom. Facial Recognition Technology in Schools. University of Michigan Technology Assessment Project 2020, https://stpp.fordschool.umich.edu/sites/stpp/files/uploads/file-assets/cameras_in_the_classroom_full_report.pdf Accessed 30 January 2024.
- Grother P, Ngan M, Hanaoka K (2019) Face recognition vendor test part 3: Demographic effects (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology, <https://doi.org/10.6028/NIST.IR.8280> Accessed 30 January 2024.
- Hacker P (2018) Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, 55(4): 1143–1185, <https://doi.org/10.54648/COLA2018095>.
- Hacker P (2021) A legal framework for AI training data—from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, 13(2): 257–301. <https://doi.org/10.1080/17579961.2021.1977219>
- Han H, Jain A (2014) Age, gender and race estimation from unconstrained face images. MSU Technical Report (2014): MSU-CSE-14-5, http://biometrics.cse.msu.edu/Publications/Face/HanJain_UnconstrainedAgeGenderRaceEstimation_MSUTechReport2014.pdf Accessed 30 January 2024.
- Harwell D (2018) Unproven Facial-Recognition Companies Target Schools, Promising an End to Shootings. *The Washington Post*, 7 June 2018, https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html Accessed 30 January 2024.
- Holmes W, Porayska-Pomsta K, Holstein K, Sutherland E, Baker T, Shum S B, Santos O C, Rodrigo M T, Cukurova M, Bittencourt I I, Koedinger K R (2021) Ethics of AI in education: Towards a community-wide framework. *International Journal of Artificial Intelligence in Education*: 1–23 <https://doi.org/10.1007/s40593-021-00239-1>.
- Hwang G J, Xie H, Wah B W, Gašević D (2020) Vision, challenges, roles and research issues of Artificial Intelligence in Education. *Computers and Education: Artificial Intelligence*, 1, 100001: 1–5 <https://doi.org/10.1016/j.caeai.2020.100001>.
- Information Commissioner's Office (2023) North Ayrshire Council's use of Facial Recognition Technology in its schools, 31 January 2023, <https://ico.org.uk/media/action-weve-taken/4023847/ico-letter-to-nac-appendix.pdf> Accessed 30 January 2024.
- Jasserand C A (2015) Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': An investigation into the meanings of the terms from a European data protection and a scientific perspective. *International Data Privacy Law*, 6(1): 63–76, <https://doi.org/10.1093/idpl/ipv020>.
- Kamil M H M, Zaini N, Mazalan L, Ahamad A H (2023) Online attendance system based on facial recognition with face mask detection. *Multimedia Tools and Applications*, 82: 34437–34457, <https://doi.org/10.1007/s11042-023-14842-y>.
- Kind C (2021) Containing the canary in the AI coalmine—the EU's efforts to regulate biometrics. Ada Lovelace Institute, <https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/> Accessed 30 January 2024.
- Lamont R (2021) Art 24. In Peers S, Hervey, T K, Kenner J, Ward A (ed) *The EU Charter of Fundamental Rights. A Commentary*. Hart.
- Laux J, Wachter S, Mittelstadt B (2024) Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance*, 18(1): 3–32. <https://doi.org/10.1111/rego.12512>.
- Lievens E, Verdoodt V (2018) Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation. *Computer Law & Security Review* 34: 269–278, <https://doi.org/10.1016/j.clsr.2017.09.007>.

- Livingstone S, Stoilova M, Nandagiri R (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science, https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf Accessed 30 January 2024.
- Lupton D, Williamson B (2017) The Datafied Child: The Dataveillance of Children and Implications for their Rights. *New Media & Society* 19(5): 780–794, <https://doi.org/10.1177/146144481668632>.
- Macenaite M (2017) From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5): 765–780, <https://doi.org/10.1177/1461444816686327>.
- Mazzini G, Scalzo S (2023) The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts, <https://ssrn.com/abstract=4098809> Accessed 30 January 2024.
- McGlynn C (2002) Rights for children: the potential impact of the European Union charter of fundamental rights. *European Public Law* 8(3): 387–400.
- Merler M, Ratha N, Feris R S, Smith J R (2019). Diversity in faces. ArXiv:1901.10436, <https://doi.org/10.48550/arXiv.1901.10436>.
- Miguel J, Schwarz D (2022) NY Is Ignoring The Ban On Facial Recognition In Schools. NYCLU, 28 June 2022, <https://www.nyclu.org/en/news/ny-ignoring-ban-facial-recognition-schools> Accessed 30 January 2024.
- Mobilio G (2023) Your face is not new to me—Regulating the surveillance power of facial recognition technologies. *Internet Policy Review*, 12(1): 1–31, <https://doi.org/10.14763/2023.1.1699>.
- Nakar S, Greenbaum D (2017) Now you see me. Now you still do: facial recognition technology and the growing lack of privacy. *Boston University Journal of Science & Technology Law*, 23(1): 88–123.
- Nguyen A, Ngo H N, Hong Y, Dang B, Nguyen B-P T (2023) Ethical principles for artificial intelligence in education. *Education and Information Technologies*, 28: 4221–4241 <https://doi.org/10.1007/s10639-022-11316-w>.
- Raposo V L (2022) (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation. *Information & Communications Technology Law*: 1–19 <https://doi.org/10.1080/13600834.2022.2054076>.
- Reiss M J (2021) The use of AI in education: Practicalities and ethical considerations. *London Review of Education*, 19(1): 1–14. <https://doi.org/10.14324/LRE.19.1.05>.
- Seldon A, Abidoye O (2018). *The fourth education revolution*. Legend Press Ltd.
- Simoncini A, Longo E (2021) Fundamental Rights and the Rule of Law in the Algorithmic Society. In Micklitz H-W, Pollicino O, Reichman A, Simoncini A, Sartor G, Gregorio G D (ed) *Constitutional Challenges in the Algorithmic Society*. Cambridge University Press, 27–41, <https://doi.org/10.1017/9781108914857.003>.
- Smuha NA, Ahmed-Rengers E, Harkens A, Li W, MacLaren J, Piselli R, Yeung K (2021) How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act, <https://doi.org/10.2139/ssrn.3899991>.
- Swedish Data Protection Authority, Supervision pursuant to the General Data Protection Regulation (EU) 2016/679—facial recognition used to monitor the attendance of students, 20 August 2019, <https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf> Accessed 30 January 2024.
- Taylor E (2013). *Surveillance schools: Security, discipline and control in contemporary education*. Palgrave Pivot.
- The Moscow Times (2020) Russia to Install 'Orwell' Facial Recognition Tech in Every School—Vedomosti, 16 June 2020, <https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585> Accessed 30 January 2024.
- UN Committee on the Rights of the Child (2013) General comment no. 14 (2013) On the right of the child to have his or her best interests taken as a primary consideration (article 3, para. 1), CRC/

- C/GC/14, 29 May 2013, https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf Accessed 30 January 2024.
- UNESCO (2019) Beijing Consensus on artificial intelligence and education, <https://unesdoc.unesco.org/ark:/48223/pf0000368303> Accessed 30 January 2024.
- UNESCO (2021) AI and education: Guidance for policy-makers, <https://unesdoc.unesco.org/ark:/48223/pf0000376709> Accessed 30 January 2024.
- UNICEF (2018) Children's online privacy and freedom of expression: Industry toolkit, [https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf) Accessed 30 January 2024.
- Verhellen E (2015) The Convention on the Rights of the Child Reflections from a historical, social policy and educational perspective. In Vandenhoe W, Desmet E, Reynaert D, Lembrechts S (ed) *Routledge International Handbook of Children's Rights Studies*. Routledge, 43–59.
- Weale S (2021) ICO to step in after schools use facial recognition to speed up lunch queue. *The Guardian*, 18 October 2021, <https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk> Accessed 30 January 2024.
- Xu W, Ouyang F (2021) A systematic review of AI role in the educational system based on a proposed conceptual framework. *Education and Information Technologies*, 27: 4195–4223, <https://doi.org/10.1007/s10639-021-10774-y>.
- Zuiderveen Borgesius F (2018) Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> accessed 30 January 2024.

Giuseppe Mobilio is Assistant Professor at the University of Florence, where he is a researcher in Constitutional Law. He studied law at University of Florence (2009) and later obtained a Ph.D at University of Pisa (2014). His current research interests include biometric surveillance, the regulation of technology and the protection of fundamental rights. His previous work includes constitutional justice, dynamics of forms of governments, sources of law, territorial government and metropolitan authorities.