COMPARATIVE LAW REVIEW

Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

Edited by Federica Giovanella

AFFECTIVE COMPUTING-BASED ATTENTION MONITORING IN AI EDUCATION: A COMPARATIVE ANALYSIS OF CHILDREN'S BIOMETRIC DATA PROTECTION IN CHINA AND THE EU

Xiaotong Bing – Anne Oloo[*]

TABLE OF CONTENTS

The classroom has become a hub of AI technologies, with affective computing and attention monitoring systems processing sensitive biometric data. This paper examines how the European Union (EU) and China are grappling with the data protection challenges posed by these emerging technologies, particularly when it comes to safeguarding children's rights. We argue that while the legal frameworks in both the EU and China are shaped by different regulatory logics reflecting distinct social, political, and economic contexts, both jurisdictions share some similarities in their approaches. In both jurisdictions, children are singled out as requiring heightened protection, yet both regulatory frameworks struggle to define the bounds of such protection. Our research shows that the use of affective computing and attention-monitoring systems in educational settings reveals fault lines in the current data protection framework, underscoring the need for tailored, child-centric regulations that balance technological innovation and fundamental rights protection.

Keywords: Affective computing, biometric data, AI education, GDPR, AI Act, Civil Code, PIPL, fundamental rights, Brussels Effect, comparative law, China, EU.

I. INTRODUCTION

The rapid development of affective computing technology, a branch of AI that detects and responds to human emotions and cognitive states, is beginning to reshape educational environments by enabling more emotionally responsive and personalised learning.[1] Affective computing aims to enable machines to recognise and respond to human emotions through techniques such as facial analysis, speech processing, and physiological monitoring.[2] Attention-monitoring is often considered a subset of affective computing,

---

[*] The authors' contributions are described based on the Contributor Roles Taxonomy (CRediT). Both authors were involved in the conceptualisation of the paper. The authors jointly defined the main structure and argument and jointly drafted the introduction and concluding sections. Anne Oloo drafted the sections on the EU Legal Framework and Comparative Insights. The sections on Description of Affective Computing and Attention Monitoring and the Chinese Legal Framework were drafted by Xiaotong Bing. Both authors take responsibility for the final text. We are grateful for the comments received at the European Law and Digital Technologies workshop at the University of Udine, Italy, on the 5th of September 2025. Thank you also to Prof Wouter Vandenhole and the anonymous reviewers for their comments and feedback. Xiaotong Bing is funded by the scholarship programme of the China Scholarship Council [Grant No.202409370002]

[1] A. O. R. Vistorte et al., *Integrating Artificial Intelligence to Assess Emotions in Learning Environments: A Systematic Literature Review*, 15 Frontiers in Psychology 1387089, 9 (2024).

[2] Y. Wang et al., *A Systematic Review on Affective Computing: Emotion Models, Databases, and Recent Advances*, 83–84 Information Fusion 19, 19 (2022).

focusing specifically on tracking students' focus and engagement in real time.[3] This aligns with the connection between one's affective state and ability to focus.[4]

However, their integration has raised urgent questions concerning privacy, ethics, and the governance of sensitive biometric data, especially when applied to minors.[5] In China, the deployment of such technologies in classrooms has often outpaced the development of corresponding legal safeguards, leading to significant regulatory gaps in the protection of minors' biometric data. This approach reflects China's emphasis on a policy-driven and technology-enabled approach to digitizing education, but it has sparked concerns about individual privacy and data protection. In contrast, the European Union (EU) has adopted a more cautious regulatory stance, enacting data protection frameworks that impose limitations on biometric data processing in educational settings, such as the General Data Protection Regulation (GDPR)[6] and the Artificial Intelligence Act (AI Act) [7].

This paper examines the emergence of affective computing and attention monitoring technologies in China's basic education system, focusing on the regulatory implications for children's biometric data protection in China and the EU. Whilst these technologies are far more widely deployed in classrooms in China than in Europe, where uptake is still limited but policy relevant, China's large-scale implementations offer a valuable use case for legal analysis. In anticipating cross-border market and vendor behaviour and considering the EU's role as a normative trendsetter in AI regulation, an EU-China comparison becomes pertinent for assessing the potency of EU rules. The analysis is principally legal; however, the authors acknowledge that affective computing and attention monitoring technologies also give rise to wider social, epistemological and ethical questions[8], such as children's autonomy[9], bias characterised in these systems[10], the validity of inferred mental states[11], as well as shifts in pedagogical authority[12], issues that cannot be fully addressed within the scope of this paper. Accordingly, the paper limits itself to a

[3] Vistorte et al., *supra* note 1 at 10.

[4] Y. Liu, Q. Fu & X. Fu, *The Interaction between Cognition and Emotion*, 54 Chinese Science Bulletin 4102, 4103 (2009); Nesreen Mejbri et al., *Trends in the Use of Affective Computing in E-Learning Environments*, 27 Education and Information Technologies 3867, 3868 (2022).

[5] R. Yuvaraj et al., *Affective Computing for Learning in Education: A Systematic Review and Bibliometric Analysis*, 15 Education Sciences 65 (2025); C. S. Montero & J. Suhonen, *Emotion Analysis Meets Learning Analytics: Online Learner Profiling beyond Numerical Data*, *in* Proceedings of the 14th Koli Calling International Conference on Computing Education Research 165 (2014), https://dl.acm.org/doi/10.1145/2674683.2674699; P. Ceres, *Kids Are Back in Classrooms and Laptops Are Still Spying on Them*, Wired, https://www.wired.com/story/student-monitoring-software-privacy-in-schools/ (last visited Oct. 14, 2025).

[6] 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 (General Data Protection Regulation) (GDPR) of 2016, OJ L 119.

[7] 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) (AI Act) of 2024, OJ L 2024/1689, 12.7.2024.

[8] Montero and Suhonen, *supra* note 5 at 168–169.

[9] Yuvaraj et al., *supra* note 5 at 35.

[10] A. Katirai, *Ethical Considerations in Emotion Recognition Technologies: A Review of the Literature*, 4 AI and Ethics 927, 931 (2024).

[11] G. Mobilio, *When the Kids Aren't Alright: The Use of Facial Recognition Technologies at School*, *in* Digital Governance: Confronting the Challenges Posed by Artificial Intelligence 41 (K. Prifti et al. eds., 2024), https://doi.org/10.1007/978-94-6265-639-0_3.

[12] C. Vidal, *The Convergence of Neurotechnology and Digital Technology in Education: Ethical and Societal Issues*, Inserm, 21 (2024).

legal and regulatory examination while seeking to contribute to and stimulate the broader interdisciplinary discourse on the interplay between technological innovation, regulatory frameworks, and human rights.

I. FROM POLICY TO PRACTICE: ATTENTION- MONITORING IN CHINA'S SMART CLASS

I.1. *Affective Computing, Attention Monitoring, and Biometric Data*

Understanding the regulatory implications of attention-monitoring technologies requires clarity about their conceptual and technical underpinnings. AI is a highly interdisciplinary field that integrates computer science, cognitive science, linguistics, psychology, and more. As defined by Russell and Norvig in their authoritative textbook *Artificial Intelligence: A Modern Approach*, AI is "the study of agents that receive precepts from the environment and perform actions," aiming to reproduce intelligent behaviour with a rational basis.[13] Within this broad framework, affective computing has emerged as a distinctive subdomain. Affective computing refers to technologies that enable computers to recognise, interpret, and respond to human emotions.[14] It focuses on systems that can detect emotional states through expressions and behavioural cues, allowing machines to simulate or adapt to emotional intelligence in human–computer interaction.[15]

Affective processes involve the psychological and physiological mechanisms through which an organism evaluates stimuli and generates adaptive responses.[16] Emotion represents a fundamental affective process, manifesting as a short-lived, multi-dimensional reaction to internal or external events relevant to an individual's important concerns.[17] It is dynamic, involving coordinated changes in the body, behaviour, subjective experience, and action tendencies, enabling effective adaptation to environmental challenges.[18] Unlike a simple feeling, which reflects only the conscious experience, emotion encompasses the entire multi-modal, evolving process, combining internal states and outward expressions into a coherent episode.[19]

Attention, in turn, a core cognitive function, regulates the processing of sensory information and plays a central role in controlled processes, ensuring that the pursuit of a goal is protected from interference.[20] Cognitive functions, in general, such as memory, language, problem-solving, and planning, are traditionally contrasted with affective functions, highlighting their reliance on rational, controlled processing rather than emotional evaluation.[21] However, attention is closely linked to affective processes[22]: its dynamics reflect an organism's evaluation of environmental events, prioritisation of salient stimuli, and associated physiological and behavioural responses, as well as subjective

---

[13] S. J. Russell & P. Norvig, *Artificial Intelligence: A Modern Approach*, 1 (Third edition, Global edition ed. 2016).
[14] K. R. Scherer, T. Bänziger, and E. Roesch, *A Blueprint for Affective Computing: A Sourcebook and Manual*, 1 (2010).
[15] H.-C. K. Lin, C.-H. Wu, and Y.-P. Hsueh, *The Influence of Using Affective Tutoring System in Accounting Remedial Instruction on Learning Performance and Usability*, 41 Computers in Human Behavior 514, 515 (2014).
[16] L. Pessoa, *On the Relationship between Emotion and Cognition*, 9 Nature Reviews Neuroscience 148, 148 (2008).
[17] K. R. Scherer, *What Are Emotions? And How Can They Be Measured?*, 44 Social Science Information 695, 697 (2005).
[18] *Id.* at 698.
[19] *Id.* at 699.
[20] Pessoa, *supra* note 16 at 149.
[21] *Id.* at 148.
[22] *Id.* at 158.

experiences such as focus, alertness, and engagement.[23] From this perspective, while attention remains fundamentally a cognitive function, its observable manifestations overlap with emotion, making computational detection of attention a concrete application of affective computing in educational contexts.

Attention monitoring refers to the use of technological means to detect and assess learners' focus levels in real time during classroom or learning activities.[24] Collecting and analysing learners' physiological or behavioural data helps educators understand the distribution and fluctuations of students' attention, enabling timely adjustments to teaching content and methods to enhance instructional effectiveness.[25] The computational feasibility of attention monitoring, like emotion recognition, rests on the collection and analysis of biometric data.[26] Biometric data forms a key technical foundation of affective computing and attention monitoring. Both rely on the analysis of multimodal biometric signals[27] including facial expressions, eye movements, posture, and, in some cases, brainwave activity, to infer internal mental states that are not directly observable.

These data serve as proxies for internal mental states that are not directly observable. They can be broadly categorised into behavioural and physiological signals.[28] Behavioural signals encompass observable characteristics such as facial expressions, speech, body posture, and eye movements that can be captured through cameras or microphones without physical contact.[29] Their non-intrusive nature and relatively low cost make them the dominant mode of data collection in classroom-based emotion recognition.[30] Physiological signals, by contrast, require dedicated sensors to monitor indicators such as electroencephalography (EEG), galvanic skin response, and heart rate variability.[31] These signals tend to reflect more accurately since individuals have limited conscious control over physiological changes.[32] However, the collection of physiological signals is complex, costly, and often requires direct contact with the subject, which may interfere with the learning process.[33] Moreover, emotional and attentional states are inferred probabilistically from these proxy signals, whose quality can vary due to differences in EEG devices, sampling rates, and channel configurations, and are further affected by individual and

[23] A. Ohman, A. Flykt, and F. Esteves, *Emotion Drives Attention: Detecting the Snake in the Grass*, Journal of Experimental Psychology: General, 466 (2001)

[24] Z. Trabelsi et al., *Real-Time Attention Monitoring System for Classroom: A Deep Learning Approach for Student's Behavior Recognition*, 7 Big Data and Cognitive Computing 48, 2 (2023).

[25] D. Durães et al., *Monitoring Level Attention Approach in Learning Activities*, 478 *in* Methodologies and Intelligent Systems for Technology Enhanced Learning, 6th International Conference 33 (M. Caporuscio et al. eds., 2016), http://link.springer.com/10.1007/978-3-319-40165-2_4.

[26] Y. Wang et al., *A Systematic Review on Affective Computing: Emotion Models, Databases, and Recent Advances*, 83–84 Information Fusion 19, 19 (2022).

[27] Multimodal biometric signals refer to the combined use of two or more types of biometric data such as facial expressions, voice, eye movements, or physiological signals like EEG and heart rate to infer an individual's emotional, cognitive, or identity-related states. Compared to unimodal systems, multimodal approaches are more robust, accurate, and resistant to spoofing, as they integrate information from multiple sources to reduce uncertainty and improve system performance. *See* P. S. Sanjekar and J. B. Patil, *An Overview of Multimodal Biometrics*, 4 Signal & Image Processing: An International Journal 57, 58 (2013).

[28] Wang et al., *supra* note 26 at 19.

[29] R. A. Calvo & S. D'Mello, *Affect Detection: An Interdisciplinary Review of Models, Methods, and Their Applications*, 1 IEEE Transactions On Affective Computing 18, 23–25 (2010).

[30] Y. Xu *et al.*, *Learning Affective Computing Research: A Systematic Literature Review Based on International Studies*, Featured Article Digital Education 1, 4.

[31] Wang et al., *supra* note 26 at 20.

[32] H. Liu et al., *Review on Emotion Recognition Based on Electroencephalography*, 15 Front. Comput. Neurosci. (2021), https://www.frontiersin.org/journals/computational-neuroscience/articles/10.3389/fncom.2021.758212/full.

[33] Xu et al., *supra* note 30.

contextual variability.[34] Consequently, even technically feasible systems may produce misclassifications or erroneous assessments in real-world classroom environments, which can have ethical and legal implications when used to guide instructional decisions.[35]

China's deployment of an EEG-based attention-monitoring device illustrates these contrasts. In one notable case, several elementary schools adopted the *Focus headband*,[36] a device that measured students' brainwave activity and displayed colour-coded indicators of attentiveness: red for focused, blue for distracted. It also sent real-time attention scores to teachers and parents.[37] The project was soon suspended following public backlash over potential harm to children's well-being: concerns included the potential inaccuracy of the attention measurements, intrusive student surveillance, potential manipulation of emotional states, and risks to children's privacy and data protection regarding the processing of their biometric data.[38]

To ground the subsequent legal and comparative analysis, the following section turns to the Chinese context, where affective computing and attention monitoring systems have been deployed most visibly in educational settings. It traces their policy foundations, practical implications, and public controversies to illustrate how China's broader AI strategy translates into the classroom.

I.2. *Affective Computing and Attention Monitoring in Chinese Classrooms*

AI is increasingly shaping the education sector worldwide. According to the 2025 *AI Index Report*, two-thirds of countries now offer or plan to offer K–12 computer science education, twice as many as in 2019.[39] China has prioritised AI education on the national agenda. The latest *Blue Book on AI-Powered Applications in Basic Education*[40] reports that by early 2025, AI technologies had entered the initial stages of integration into China's basic education system through a pilot project spanning teaching, learning, assessment, student development, educational research, and governance. These initiatives aim to build a data-driven smart education ecosystem, featuring tools such as intelligent lesson preparation, personalised learning assistance, multimodal performance evaluation, and automated education management.

Behind these applications lies the growing use of affective computing to assess students' emotional and cognitive engagement. The so-called 'Attention Index' has emerged as a key indicator of instructional quality.[41] Yet because these systems rely on processing highly

---

[34] N. Babu et al., *Emotion Recognition in Virtual and Non-Virtual Environments Using EEG Signals: Dataset and Evaluation*, 106 Biomedical Signal Processing and Control 107674, 2 (2025).

[35] A. McStay, *Emotional AI and EdTech: Serving the Public Good?*, 45 Learn Media Technol. 270 (2020).

[36] The Focus headband is a product of BrainCo, a company founded in 2015 and incubated at the Harvard Innovation Lab. A FOCUS Headband consists of three parts: hardware, algorithm, and software. By using its proprietary sensors to detect brain signals and deploying an AI algorithm to translate signals into focus levels in real time, the Headband provides insights into the engagement levels of users and tracks whether a user is focused or distracted. *See* BrainCo company website: https://brainco.tech/technology/

[37] *AI Headbands Tracking Student Attention Levels Suspended amidst Online Controversy* - People's Daily Online, https://en.people.cn/n3/2019/1101/c90000-9628768.html (last visited Jan. 28, 2026).

[38] *Headbands Monitoring Elementary Students' Focus Likened to 'Tightening Curse': What Fuels the Backlash against Smart Education Devices?*, Xinhua Net, http://www.xinhuanet.com/politics/2019-11/10/c_1125214619.htm (last visited July 19, 2025).

[39] N. Maslej *et al.*, *Artificial Intelligence Index Report 2025*, Artificial Intelligence, 367 (2025).

[40] Engineering Research Center for Smart Technology and Education, Ministry of Education; Beijing Digital Education Center (Beijing Educational Technology Center), Blue Book on AI-Enabled Applications in Basic Education (2025) (2025).

[41] A. Al-Nafjan & M. Aldayel, *Predict Students' Attention in Online Learning Using EEG Data*, 14 Sustainability 6553, 1 (2022); *See also* A. Becerra, R. Cobos & C. Lang, *Enhancing Online Learning by Integrating Biosensors and*

sensitive biometric and emotional data, their use has sparked public controversy. The diffusion of these attention monitoring systems has followed a phased diffusion trajectory, moving from initial pilot projects through intense public debate to a relatively stable, though still contested, stage.

A landmark pilot was the 'Intelligent Classroom Behaviour Management System' installed in 2018 at Hangzhou No. 11 High School.[42] Using facial-recognition technology, the system classified and recorded students' classroom behaviours (e.g., hand-raising, reading, distraction) as well as their emotional states (e.g., happiness, anger, fear) in real time.[43] Developed jointly with Hikvision[44], the project drew extensive domestic and international media attention for its intrusive monitoring capabilities and sparked vigorous debate over student privacy, informed consent, and the ethics of emotion surveillance.[45]

Despite continuing concerns, similar technologies have proliferated across 'smart classroom' initiatives. Corporate materials from Zhizhou AI[46] describe systems that generate individualised student profiles integrating behavioural, emotional, and cognitive data, using indicators such as an Attention Index to monitor engagement and support pedagogical adjustment. In these systems, computer vision technologies analyse students' facial expressions, body postures, and gaze direction to infer levels of attention and participation. Real-time dashboards present visualised data such as emotional distribution charts (e.g., neutral, active, serious), heatmaps of classroom engagement, and time-series graphs showing fluctuations in collective attention throughout a lesson.[47] These analytics are further used to generate diagnostic reports for teachers, detailing behavioural frequencies and engagement patterns, thereby providing data-driven insights for instructional design and learning adjustment.[48]

China's national AI strategy strongly emphasises integrating intelligent technologies into basic education as part of a broader shift towards evidence-based teaching. Affective computing, particularly attention monitoring systems, now sits at the core of this shift. However, their continuous collection of sensitive data, particularly biometric data, has triggered significant ethical and legal concerns.

This controversy highlights a broader regulatory dilemma: how to safeguard children's data protection and privacy rights in the digital classroom when affective and attention

Multimodal Learning Analytics for Detecting and Predicting Student Behaviour: A Review, Behaviour & Information Technology 1 (2025).

[42] *Chinese School Uses Facial Recognition to Make Kids Pay Attention*, Engadget (May 17, 2018), https://www.engadget.com/2018-05-17-chinese-school-facial-recognition-kids-attention.html. (last visited 11 Oct. 2025).

[43] ARTICLE 19, Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights 29 (2021).

[44] Hikvision is a leading provider of AI-driven video surveillance technologies, headquartered in Hangzhou, China. Hikvision, *Smart Classroom Solution*, http://www.hikvision.com/en/solutions/solutions-by-industry/education/smart-classroom/ (last visited June 23, 2025).

[45] GETChina Insights, *Schools Using Facial Recognition System Sparks Privacy Concerns in China*, Medium (Sept. 9, 2019), https://edtechchina.medium.com/schools-using-facial-recognition-system-sparks-privacy-concerns-in-china-d4f706e5cfd0 (last visited June 23, 2025); M. Standaert, *Chinese Primary School Halts Trial of Device That Monitors Pupils' Brainwaves*, The Guardian, Nov. 1, 2019, https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves (last visited Oct. 13, 2025).

[46] Zhizhou AI is a product developed by Beijing Zhizhou Technology Co., Ltd., a Chinese educational technology company focused on smart classroom solutions. https://mp.weixin.qq.com/s/03lXymFqUSaXYE3sfEC2AQ (last visited 16 July 2025.)

[47] Zhizhou AI, *AI Smart Teaching System: Six Core Technologies for In-Depth Learning Analytics.* (June 3, 2024), https://mp.weixin.qq.com/s/03lXymFqUSaXYE3sfEC2AQ (last visited July 16, 2025).

[48] *Id.*

monitoring systems are deployed in learning environments, a question to which the following sections will turn.

II. LEGAL FOUNDATIONS AND REGULATORY FRAMEWORKS

The preceding discussion has shown that affective computing and attention-monitoring technologies introduce unprecedented forms of observation and inference in the classroom. Their capacity to capture or predict children's emotional and cognitive states exposes deep tensions between educational innovation and the protection of privacy and children's data. These tensions underscore the urgent need for a coherent legal framework capable of addressing the direct risks of biometric processing and the subtler harms arising from constant behavioural surveillance.

Children are particularly vulnerable in this context, as they are often less aware of the risks, consequences, and their rights regarding data processing.[49] Any breach of their data, therefore, poses a greater risk to their fundamental right to data protection.[50]

The legal framework governing children's data protection in Europe and China has its antecedents in the international human rights law, specifically in the United Nations Convention on the Rights of the Child[51] (CRC), which lays down nearly universally recognised rights for Children. Whereas data protection is not explicitly mentioned as one of those rights[52], various UN reports[53] and the 2021 General Comment No. 25 (GC 25)[54] have affirmed that children have a fundamental right to data protection.

The UNCRC lays down four essential principles that underpin children's data protection[55]:

1. Non-discrimination: Guaranteeing the same rights to all children without discrimination (Article 2).
2. Best interests of the child: Ensuring that the interests of children are given paramount consideration above those of others (state, parents, and community) (Article 3).
3. The right to survival and development: Recognising children's right to the full extent of their development (Article 6).
4. Participation and inclusion: Ensuring that children's views are taken into account throughout their different stages of development (Article 12).

These principles are reflected, to varying extents, in the legal frameworks of the EU and China. The next section will examine the law governing children's data protection in the

---

[49] GDPR r 38.

[50] K. Faisal, *Certain Legal Aspects of Children's Right to Protect Personal Data in the Context of AI under the European Union Data Protection Laws*, Vapaita Sanoja. Viestintäoikeuden Vuosikirja 106, 109 (2022).

[51] Convention on the Rights of Child (adopted 20 november 1989, entered into force 2 september 1990), UNTS 1577.

[52] V. Verdoodt, Y. Zhang & E. Lievens, *Safeguarding the Child's Right to Privacy and Data Protection in the European Union and China: A Tale of State Duties and Business Responsibilities*, 28 International Journal of Human Rights 125, 5 (2024).

[53] United Nations General Assembly, The Right to Privacy in the Digital Age: Resolution Adopted by the General Assembly on 17 December 2018 [on the Report of the Third Committee (A/73/589/Add. 2)] 73/179. The Right to Privacy in the Digital Age (2019), http://digitallibrary.un.org/record/1661346; Human Rights Council, Artificial Intelligence and Privacy, and Children's Privacy: Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci (2021), https://documents.un.org/doc/undoc/gen/g21/015/65/pdf/g2101565.pdf.

[54] UN Committee on the Rights of the Child, 'General Comment No. 25 on Children's Rights in Relation to the Digital Environment' (2021) UN Doc CRC/C/GC/25.

[55] C. Caglar, *Children's Right To Privacy And Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?*, 12 European Journal of Law and Technology 11 (2021), https://ejlt.org/index.php/ejlt/article/view/828.

context of attention monitoring and affective computing systems in the European Union. The focus will be on the key provisions within the GDPR and the recently enacted AI Act that address the protection of children's personal data in these emerging technological applications. The aim is to explore how these EU regulations seek to uphold the core principles of children's rights within the specific context of AI-driven educational technologies that monitor students' emotional and cognitive states.

III.1 *The EU's Legal Framework for Children's Data Protection*

The EU's legal framework for protecting children's data rights in the context of affective computing and attention monitoring systems is firmly rooted in its fundamental legal instruments. Article 8 of the Charter of Fundamental Rights of the European Union explicitly safeguards the right to data protection for 'everyone,' which has been interpreted to include children.[56] This provision establishes data protection as a fundamental human right that applies to all individuals, regardless of age.[57]

Furthermore, the legal foundation for children's data protection can be traced back to the founding treaties of the EU. The Treaty on European Union establishes data protection as a fundamental human right that underpins the Union's values and objectives.[58] Article 16 of the Treaty on the Functioning of the European Union[59] further enshrines the right of all individuals to the protection of their personal data, requiring the European Parliament and Council to enact legislation to this end.

It is on this basis that the GDPR was adopted and is now applicable. The AI Act, on the other hand, was enacted in response to the growing prominence of AI systems and aims to regulate them, including those used in the education sector. Together, the GDPR and AI Act lay down the law on the use of biometric data which are characteristic of attention monitoring systems.

III.1.1. *Key Definitions and Legal Scope in the AI Act and GDPR*

Affective computing and attention monitoring systems in educational settings often rely on biometric data such as facial expressions, voice, and physiological signals to detect and respond to students' emotional and cognitive states. However, other attention monitoring systems also employ non-biometric data, such as on-screen activity[60], test completion rates[61] or keyboard stroke[62] tracking to determine the attentiveness of students. Under

[56] Council of Europe, 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, 12–22 (2018), https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.

[57] Article 29 Data Protection Working Party, Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) 3 (2009), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf.

[58] Consolidated Version of the Treaty on European Union of 2016, 202 OJ C 202/17.

[59] Consolidated Version of the Treaty on European Union of 2016, 202 OJ C 202/55.

[60] M. Dorge et al., *Screen Activity Monitoring Using Federated Learning*, in 2025 International Conference in Advances in Power, Signal, and Information Technology (APSIT) 1 (2025), https://ieeexplore.ieee.org/abstract/document/11086241.

[61] T. C. Papadopoulos et al., *Assessment of Attention in School Children: Teachers' Ratings Related to Tests of Attention*, 17 European Journal of Special Needs Education, 15 (2002).

[62] V. Kuvar et al., *Partner Keystrokes Can Predict Attentional States during Chat-Based Conversations*, *in* Proceedings of the 16th International Conference on Educational Data Mining 217 (M. Feng, T. Käser, & P. Talukdar eds., 2023), https://zenodo.org/record/8115697.

both the AI Act and GDPR, these affective computing technologies intersect with key legal concepts and definitions.

Biometric data under GDPR

Biometric data is defined in the GDPR as 'personal data resulting from specific technical processing relating to a natural person's physical, physiological or behavioural characteristics, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.'[63] Personal data, more broadly, refers to 'any information relating to an identified or identifiable natural person ('data subject').'[64] Facial recognition, gaze tracking, and other physiological signals processed by attention monitoring systems fall under these definitions.[65]

The GDPR categorises biometric data as a 'special category' (or 'sensitive data') of personal data.[66] Special categories of data include data revealing one's racial, ethnic, political, religious or philosophical beliefs as well as data concerning one's health, sex life or sexual orientation.[67] These data are considered sensitive because of their significant risk to 'fundamental rights and freedoms'[68] and therefore trigger heightened protections. Consequently, the processing of such data is generally prohibited, unless specific conditions are met, such as explicit consent, substantial public interest, or necessity for preventive/occupational health.[69] These exceptions to the general prohibition of processing of special categories of data are interpreted strictly.[70]

However, the GDPR's scope is limited in certain respects when it comes to affective computing technologies.[71] The regulation does not apply to anonymous information, and its definition of biometric data is confined to information that allows or confirms unique identification.[72] Thus, biometric data processing that does not identify or render the data subject identifiable falls outside its material scope.[73] For example, a system that analyses aggregated or anonymised emotional responses for non-individualised purposes may not qualify as personal data processing under the GDPR.[74] In practice, however, anonymisation in educational settings is rare, as such systems are usually tied to named students and used for evaluative purposes.[75]

Moreover, emotion data is not automatically classified as 'special category' personal data under Article 9 GDPR. This special category designation only applies if the emotion data is derived from physiological sources that enable unique identification, such as facial images or fingerprints. This distinction means that visual approaches relying solely on

63 GDPR art 4(14).
64 *Id.* at art. 4(1).
65 AI Act r 15.
66 GDPR art 9, r 51.
67 *Id.* at art. 9(1).
68 *Meta Platforms Inc and Others v Bundeskartellamt* 66 (ECJ 2023).
69 GDPR art 9(1) (a-j); *Meta Platforms Inc and Others v Bundeskartellamt*, *supra* note 68, paras 74–85.
70 *Meta Platforms Inc and Others v Bundeskartellamt*, *supra* note 68, para 76.
71 A. Häuselmann et al., *EU Law and Emotion Data*, *in* 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII) 1, 3 (2023), https://ieeexplore.ieee.org/document/10388181/.
72 GDPR r 26, art 4(14), 9.
73 L. Menges & E. Weber-Guskar, *Digital Emotion Detection, Privacy, and the Law*, 38 Philosophy & Technology 77, 84 (2025).
74 *Id.* at 85.
75 *See* A. P. Carvalho et al., *Big Data, Anonymisation and Governance to Personal Data Protection*, in The 21st Annual International Conference on Digital Government Research 185 (2020), https://dl.acm.org/doi/10.1145/3396956.3398253.

facial expressions may escape enhanced protections, whilst physiological approaches processing data like heartbeat or electrodermal activity generally fall within them. This differential treatment reflects the GDPR's focus on identifiability and biometric identification as the key criteria for heightened protection. Yet even when not classified as special category data, emotion and attention inferences remain personal data, subject to GDPR principles of lawfulness, fairness, necessity, and proportionality. This creates a regulatory gap: certain attention monitoring systems may escape the strictest safeguards despite producing highly sensitive inferences about students' emotional states.

Biometric data under the AI Act

The AI Act and its follow-up commission guidelines[76] *attempt* to address some of these gaps by including specific provisions related to 'emotion recognition systems' (ERS)[77], and other affective computing technologies.

The keyword here is *attempt,* since the current definition of emotion recognition systems suffers from two key limitations. First, the Act defines an ERS system as 'an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data'[78]. Biometric data under the Act reproduces the exact wording of the GDPR[79], tying its scope to data that enable or confirm the unique identification of an individual.

This definitional choice has a narrowing effect: only systems that rely on biometric signals such as facial images, voice, or physiological patterns are captured. Emotion or attention inference based on non-biometric indicators, such as on-screen activity[80], time spent on task[81], or log-in patterns[82], thus falls outside the prohibition on ERS in educational settings, even though such systems may generate comparably sensitive inferences. However, such systems may still qualify as personal data processing under the GDPR, insofar as the inferences are linked to identifiable students, and may be categorised as high-risk under the AI Act where they play a role in assessment or progression decisions. Their definitional status is therefore one of partial exclusion: they escape the strictest categorical safeguards of EU law but remain potentially subject to general obligations depending on their deployment.

Second, the inclusion of both 'emotions' and 'intentions', even though they are intertwined, produces an overbroad and conceptually ambiguous category. Emotions, though difficult to standardise, refer to recognisable affective states.[83] Intentions, by contrast, imply predictions about future behaviour, such as whether a student is likely to

[76] European Commission, Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act) (2025).

[77] The term 'emotion recognition system' is used in the Act to refer to the broader concept of affective computing. *See* D. Iren, L. P.J.J. Noldus, & A. M. Brouwer, AI Act & Guidelines on Prohibited Artificial Intelligence (AI) Practices: An Analysis for the Emotion Recognition Field 1 (2025), https://www.aigl.blog/content/files/2025/04/AI-Act---Guidelines-on-Prohibited-Artificial-Intelligence--AI--Practices--An-Analysis-for-the-Emotion-Recognition-Field.pdf.

[78] AI Act art 3(39).

[79] *Id.* at art. 3(34); GDPR art 4(14).

[80] P. Krieter & A. Breiter, *Track Every Move of Your Students: Log Files for Learning Analytics from Mobile Screen Recordings*, *in* Die 16. E-Learning Fachtagung Informatik (DELFI) (2018).

[81] D. Mistry et al., *Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning*, 11 IEEE Access 79315 (2023).

[82] V. Mandalapu et al., *Student-Centric Model of Login Patterns: A Case Study with Learning Management Systems* (International Educational Data Mining Society 2021) https://eric.ed.gov/?id=ED615654 (last visited Oct. 15, 2025).

[83] K. Mulligan & K. R. Scherer, *Toward a Working Definition of Emotion*, 4 Emotion Review 345, 346 (2012).

disengage, cheat, or drop out.[84] By conflating these distinct forms of inference, the Act risks sweeping together fundamentally different technologies while at the same time failing to provide clear boundaries for what counts as ERS. The conflation of these categories makes it difficult to establish clear boundaries for what counts as ERS, reducing legal certainty.

III.1.2. *EU Legal Implications for Attention Monitoring Systems*

The definitional analysis above shows where (non) biometric attention monitoring systems sit within the GDPR and the AI Act. What matters next is not only the regulatory categories themselves, but how the obligations that follow from them interact with the rights of children. Against this backdrop, the obligations set out in the GDPR, and the AI Act must be read through a child-centred lens: one that rests on the CRC principles and recognises the long-term consequences of profiling in educational settings.

Compliance with the GDPR

The GDPR's primary aim is to protect all individuals' fundamental right to data protection, with children explicitly recognised as the only group[85] in the GDPR requiring 'specific protection' in data processing.[86] This protection extends in particular to collecting their data for marketing or services offered directly to them.[87] To this end, data controllers processing children's data are required to provide information regarding such processing in clear and plain language 'that [a] child can easily understand'[88].

Additionally, the GDPR imposes strict obligations on all data controllers to comply cumulatively with the principles in Article 5, namely fairness, lawfulness, transparency, purpose limitation, proportionality, data minimisation, accuracy, storage limitation, confidentiality, and accountability. Compliance with one principle does not excuse non-compliance with another.[89] Children are also afforded individual data subject rights, including the right to erasure[90], data portability[91] and the right to be informed[92]. Relatedly, all processing must be grounded in on one of the legal bases listed under article 6, among which consent, contract and legitimate interest of the controller are the most relevant for children's data processing.

It is doubtful that data processing in attention monitoring systems can meet these cumulative obligations. Whilst this paper does not analyse every principle and right in detail, it focuses on consent as a legal basis for data processing and the proportionality and

---

[84] V. G. Morwitz & K. P. Munz, *Intentions*, 4 Consumer Psychology Review 26, 27 (2021).

[85] The GDPR refers to children as 'vulnerable' (recital 75). However, academics have criticised such inference and instead argue for a more agency-oriented outlook in children's rights protection. *See* for example L. Lundy, *Vulnerability Should Not Eclipse Agency: Children's Perspectives on Their Own Lives*, *in* Perspectives on Children, Rights, and Vulnerability 31 (2025), https://www.scup.com/doi/10.18261/9788215069500-25-03.

[86] GDPR r 75.

[87] *Id.* at art. 38.

[88] *Id.* at art. 58.

[89] A. Atabey & R. Scarff, *The Fairness Principle: A Tool to Protect Childrens Rights in Their Interaction with Emotional AI in Educational Settings*, 4 Global Privacy Law Review 5, 5 (2023).

[90] GDPR art 17.

[91] *Id.* at art. 20.

[92] *Id.* at art. 13, 14.

fairness principles to illustrate that such systems are unlikely to comply with GDPR's requirements.

At the heart of the GDPR is the requirement for consent to process data. Consent under the GDPR is valid when certain conditions are met: It has to be freely given, specific, informed and unambiguous,[93] taking into account the maturity of the concerned child. Additionally, under Article 8, only children who are at least 16 years old can consent to information services offered to them; otherwise, parental/guardian consent is required[94]. Because of the inherent imbalance of power that exists between educational institutions and children[95], consent is unlikely to be freely given. Children and their guardians often have little practical choice but to accept such technologies if they are integrated into the learning environment, undermining the voluntariness of consent. Furthermore, the complex nature of attention monitoring, which often involves opaque algorithmic inferences and data flows, makes it nearly impossible for data subjects to provide fully informed consent.

Likewise, the proportionality of the use of attention monitoring systems is questionable. Proportionality is closely tied to the purpose limitation and data minimisation principles[96] and requires that any interference with privacy be necessary and not excessive in relation to the aim pursued. Attention monitoring systems involve the continuous and granular collection of data, often in real-time, ostensibly to improve student engagement. While such an objective could be educationally desirable, the scale and sensitivity of data processing in these systems exceed what is necessary to achieve their stated objectives.[97] Moreover, a proportionality assessment requires an account not only of the volume of data collected but also of the potential harms[98], such as the normalisation of surveillance[99], chilling effects on student behaviour[100] or long-term risks of profiling[101].

Finally, the fairness principle, embedded in Article 5(1)(a) GDPR, is also challenged by the use of attention monitoring systems. Fairness operates as a normative safeguard, ensuring that data processing respects individuals' reasonable expectations and does not reproduce unjust outcomes. The opacity that characterises attention monitoring systems makes it difficult for children and parents to understand how their data is processed. Additionally, such systems may also misinterpret attention cues, which are subjective and vary according to one's cultural background[102], behavioural or neurodivergent differences[103]. This lack of fairness and accuracy in the data processing can have significant consequences for children, potentially leading to unfair outcomes that undermine their educational experiences and opportunities.

---

93 *Id.* at art. 4(11).

94 Member states, however, can choose to lower the age, which should not be lower than 13.

95 Atabey and Scarff, *supra* note 89 at 13.

96 M. Finck & A. J. Biega, *Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems*, 2021 Technology and Regulation 44, 57 (2021).

97 D. Lupton & B. Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 New Media & Society 780, 789 (2017).

98 Article 19, Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights 28,30 (2021), https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

99 Lupton and Williamson, *supra* note 97 at 789.

100 Atabey and Scarff, *supra* note 89 at 10.

101 Article 19, *supra* note 98 at 30.

102 *See* L. F. Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, 20 Psychol Sci Public Interest, 1 (2019).

103 N. Ouherrou et al., *Comparative Study on Emotions Analysis from Facial Expressions in Children with and without Learning Disabilities in Virtual Learning Environment*, 24 Education and Information Technologies 1777, 1785 (2019).

These data protection principles, which are central to the various data subject rights enshrined in the GDPR, are enforced by independent Data Protection Authorities (DPAs).[104] DPAs are competent to receive complaints, including those submitted by or on behalf of children, and may issue a variety of administrative procedures, including warnings, fines, and reprimands, when infringements occur.[105]

However, the complex and often opaque nature of attention monitoring systems presents significant challenges for DPAs in effectively supervising and regulating their deployment, particularly in the context of protecting children's rights and interests. This is because, in and of itself, the GDPR is limited in scope, in that it does not effectively account for 'different layers of vulnerabilities of children'.[106] For instance, children with learning difficulties or neurodivergent conditions may face heightened risks when attention monitoring systems process their behavioural data, as the GDPR does not explicitly address how such intersecting vulnerabilities should be integrated into data protection assessments. This regulatory gap finds partial expression in the AI Act's risk-based framework. Nevertheless, as the following section illustrates, the Act's narrowly defined conception of 'risk' leaves important gaps in the protection of children's rights and interests.

Compliance analysis under the AI Act

Building upon the GDPR's data protection framework, the AI Act introduces complementary, risk-based approach to the regulation of AI systems. This tiered model[107] assigns differentiated obligations to deployers and data controllers depending on system's assessed risk profile.[108] However, while the Act refrains from defining the notion of 'risk', it adopts a relatively narrow interpretation, confining its scope to health, safety, and fundamental rights concerns.[109] Notably, the Act does not outline any criteria for categorising the different levels of risk.[110] This limited framing raises questions about whether the Act sufficiently captures the nuanced or context-specific harms, such as those affecting special-interest groups, including children, that arise from the deployment of attention-monitoring systems.

To operationalise this framework, the Act categorises AI systems into five distinct risk levels, each corresponding to a different degree of regulatory intensity; These comprise: (i) prohibited practices posing unacceptable and unmitigable risks; (ii) high-risk systems subject to a variety of obligations; (iii) general-purpose AI models with transparency requirements; (iv) limited-risk AI systems with lighter transparency obligations; and (v) minimal-risk systems, such as chatbots or simple recommendation engines, largely exempt from the Act's transparency rules. Yet, the classification of certain technologies, such as attention monitoring systems, within this hierarchy remains legally and conceptually contested, particularly where their deployment intersects with the protection of children's fundamental rights.

---

104 GDPR r 116–123.

105 *Id.* at art. 58.

106 Atabey and Scarff, *supra* note 89 at 12.

107 G. Makauskaite-Samuole, *Transparency in the Labyrinths of the EU AI Act: Smart or Disbalanced?*, 8 Access to Justice in Eastern Europe, 38, 42 (2025).

108 AI Act r 26.

109 *Id.* at art. 52,53,72; N. A. Smuha & K. Yeung, *The European Union's AI Act: Beyond Motherhood and Apple Pie?*, in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* 228, 236 (N. A. Smuha ed., 2025).

110 M. Ebers, *Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, 16 European Journal of Risk Regulation 684, 692 (2025).

The AI-Act risk-based framework impacts attention monitoring and affective systems to differing degrees. Despite the definitional ambiguity surrounding ERS systems, the Act explicitly bans AI systems used to identify or infer emotions through biometric data processing in educational settings, except for health and safety reasons.[111] Follow-up commission guidelines clarify that whilst article 5(1)(f) does not explicitly mention ERS systems, the prohibition under this article should be interpreted as having the same scope as rules applicable to other ERS systems as provided under Annexe III (1)(c) and Article 50 AI Act.[112] Most importantly, the guidelines confirm the limitations on biometric data discussed above.

Concerns over the limited reliability, generalisability, and cultural variability of these technologies justify the prohibition in Article 5(1)(f)[113] , as well as the recognised imbalance of power in educational (and work) settings[114].
This limited prohibition under Article 5(1)(f) creates two distinct scenarios for attention monitoring systems:

1. AI systems that infer emotions for medical or safety reasons are permitted but classified as high-risk, triggering strict obligations.[115] These include establishing a risk management system[116], implementing a data quality and governance framework[117], producing technical documentation[118], and maintaining human oversight to ensure effective review of automated decisions[119].
2. Non-biometric attention monitoring systems could be classified as either high-risk or low-risk, depending on their functionalities. High-risk systems in educational contexts include those that influence grades, affect progression or access to opportunities, or shape educational pathways.[120] Lower-risk systems, such as those using aggregate analytics (for instance, '10% of the class is disengaged after 20 minutes), are still subject to general AI Act obligations like accuracy, transparency, copyright, and system evaluation requirements.[121]

The transparency obligations for high-risk systems are quite comprehensive. Providers must disclose detailed information to users and affected individuals, such as the purpose and functionality of the system, accuracy rates, and potential biases. In the context of children, this includes explanations comprehensible to minors and their guardians. However, the Act stops short of requiring the disclosure of the specific emotions detected to individuals, a gap that was unaddressed under the GDPR. This increased transparency is vital given these systems' significant impact on the fundamental rights of children.
Regarding enforcement, the Act sets up mechanisms such as market surveillance by authorities[122], conformity assessments[123], and fines for non-compliance[124]. These tools

111 AI Act art 5(1)(f).
112 European Commission, *supra* note 76 at 244–246.
113 AI Act r 44.
114 *Id.*; European Commission, *supra* note 76 at 253.
115 *See* AI Act section 2.
116 *Id.* at art. 9.
117 *Id.* at art. 10.
118 *Id.* at art. 11.
119 *Id.* at art. 14.
120 *Id.* at art. 127 Annex III 3.
121 *Id.* at art. 53(1), 55(1).
122 AI Act r 156.
123 *Id.* r 173; art. 16(f).
124 *Id.* r 168; art. 99.

provide a more proactive approach to ensuring compliance compared to GDPR's mainly reactive, complaint-based system.

III.1.3. *Analysis EU law: Children's rights and data protection*

An examination of the GDPR and AI Act shows that both pieces of legislation recognise that affective and attention-monitoring systems in education are high-stakes, high-risk, and require unique, children's rights-centred legal attention. Both regulations attempt to translate CRC principles (*non-discrimination*, the *best interests of the child*, a *child's right to survival and development*, and the *participation and inclusion* principles) into technical and procedural safeguards for children exposed to affective and attention-monitoring technologies.

The CRC mandates that all children enjoy their rights without discrimination.[125] The AI Act and GDPR embody this principle by emphasising the need to protect children from discriminatory outcomes arising from the use of AI-driven affective computing systems. Recital 28 of the AI Act highlights concerns over manipulative and exploitative practices enabled by AI, stating such practices are 'particularly harmful and abusive and should be prohibited because they contradict Union values. including the right to non-discrimination, to data protection and to privacy and the rights of the child'. Within the GDPR, recital 75 specifically flags risk of discrimination as a key reason for affording special protection to children. Similarly, *Non-discrimination* is reflected in the GDPR's fairness, purpose, and accuracy obligations[126], and in the AI Act's requirement to test for bias, ensure data quality, and monitor discriminatory outcomes[127], which together force developers and deployers of attention-monitoring technologies to consider the disparate impact on children.

Article 3 requires that the *best interests of the child* be a primary consideration in all actions concerning children. This principle is given effect by GDPR's special protection for minors[128], i.e., high-threshold consent requirements and tailoring information for children, and by the AI Act's specific prohibition of ERSs in education settings, except for narrowly defined safety or medical uses[129]. This precaution privileges children's welfare over unfettered deployment.

Similarly, the child's right to *survival and development*[130] is advanced through GDPR's data minimisation, purpose limitation, and restrictions on profiling[131], which limits harmful inferences that could stigmatise or channel a child's educational trajectory. The AI Act complements this with mandatory risk-management and corrective action duties for high-risk systems.[132]

Finally, *participation and inclusion* are supported by heightened transparency and information obligations: the GDPR requires clear, age-appropriate notices and parental/guardian consent where relevant[133], and the AI Act imposes disclosure obligations for systems that

[125] CRC art 2.
[126] GDPR art 5(1) (a), 5(1) (c), 25.
[127] AI Act arts 10, 15, Annexe III.
[128] GDPR art 5(1) (a), 5(1) (c), 25.
[129] AI Act art 5(1) (f), Annexe III.
[130] CRC art 6.
[131] GDPR art 5,9,22.
[132] AI Act art 9,20,27.
[133] GDPR art 6,8,12.

interact with or infer states of natural persons[134] and human-oversight safeguards[135] to preserve meaningful agency.

However, some gaps persist, notably a definitional and scope ambiguity within EU law. The GDPR and AI Act do not entirely align on how biometric data and ERSs are defined and when they fall within heightened protection or prohibition. As discussed above, this produces uncertain coverage for some attention-monitoring tools (e.g. systems that infer affect based without uniquely identifying pupils or those using non-biometric proxies), and hence uneven legal obligations for providers and schools. Placing this internal EU ambiguity beside China's comparatively permissive approach where attention monitoring systems have been widely deployed under a different mix of state oversight, parental authority and education policy, brings to focus the contrast and similarities in approaches in the two jurisdictions. It also provides a vantage point for examining the potential and limits of the Brussels Effect: the capacity of EU law to influence regulatory practices beyond its borders. Whereas both jurisdictions recognise that children merit particular protection in the digital sphere, they operationalise this recognition in markedly different ways. The following section analyses Chinese law relevant to attention monitoring systems. Thereafter, a comparative assessment of both legal frameworks will be proffered.

III.2 *China's Legal Framework on Children's Biometric Data Protection*

The establishment of Chinese privacy and data protection law came later than in Europe.[136] In terms of legislative approach, it initially drew on EU-style techniques by centring regulation on the processing of personal information, while distinguishing between privacy protection and the regulation of information processing.[137] The 2020 Civil Code systematised personality rights, explicitly including privacy as one category and framing its protection in the context of interpersonal relationships.[138] The 2021 Personal Information Protection Law (PIPL)[139], China's first dedicated data protection law, establishes the rights of data subjects and sets out principles for lawful processing, framing its protection in the context of information processing activities.[140] Together, these two laws form a complementary *dual-track system*, in which the Civil Code safeguards individual autonomy and dignity, while the PIPL governs personal data processing and compliance obligations, reflecting both EU-inspired principles and China's distinct focus on balancing individual rights, security, and digital sovereignty.

Against the backdrop of the gradual deployment of affective computing and attention monitoring in schools, China has not yet enacted a unified AI law. Current governance relies on sector-specific regulations[141], which provide limited constraints on the use of AI

134 AI Act art 50(3).
135 *Id.* at art. 14.
136 E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 Penn State Journal of Law & International Affairs 49, 53 (2020).
137 X. Ding *The Jurisprudential Relationship between the Protection of Privacy Rights and Personal Information Protection*, 40 Studies in Law and Business 61, 63–64 (2023).
138 Civil Code of the People's Republic of China of 2020.
139 Personal Information Protection Law of the People's Republic of China of 2021.
140 M. He & Y. Chen, *Personal Data Protection in China: Progress, Challenges and Prospects in the Age of Big Data and AI,* Telecommunications Policy 49, 1–28 (2025).
141 The current governance structure relies heavily on sectoral regulations and administrative rules issued by specialised agencies such as the Cyberspace Administration of China (CAC), particularly in relation to algorithmic transparency, data governance, and content moderation. Notable examples include the *Provisions on the Administration of Algorithmic Recommendation for Internet Information Services* (2021) and the *Provisions on the Administration of Deep Synthesis for Internet Information Services* (2022).

in educational settings but remain fragmented and lack systematic operational standards.[142] In addition, regarding biometric information, China has no standalone legislation and instead relies on a fragmented protection framework established through the PIPL and the Civil Code.

III.2.1. *Legal Recognition and Conceptual Uncertainty under the Civil Code*

In the Chinese legal system, 'biometric information' has been recognised as an independent 'civil interest' instead of a 'civil right'[143], mainly reflected in Chapter 6 Protection of Privacy and Personal Information of Part IV Personality Rights of the Civil Code, as well as in Chapter 2 Protection of Sensitive Personal Information of the PIPL.[144] This recognition progresses from the Civil Code, as the general law, to the PIPL, a specialised law. However, issues regarding its legal nature, specific rights and powers, and methods of protection still require further clarification and in-depth study.

Specifically, Article 1034 (2) of the Civil Code enumerates biometric information as a type of personal information; [145] it does not confer an independent right to personal information, which means protection relies on privacy rights and tort remedies, rather than allowing individuals to assert claims solely based on their biometric information. Moreover, its placement under the chapter on privacy and personal information protection should not be misconstrued as equating biometric data with privacy rights. Notably, Paragraph 3 of the same article provides that confidential information within personal information may be governed by the rules on the right to privacy.[146] However, this does not mean that biometric data, by default, constitutes such confidential information. Consequently, the legal characterisation of biometric information remains uncertain.

Therefore, under the Civil Code, it is necessary to determine whether biometric information qualifies as confidential information. The Civil Code does not provide explicit criteria for determining what constitutes confidential or private information. According to judicial practice—for instance, in the *WeChat Reading Case*[147]—the plaintiff argued that their WeChat friend list and reading records should be regarded as private information. However, the court rejected this claim. The judge reasoned that privacy refers to information that an individual does not wish others to know, emphasising the element of subjective intent. Nonetheless, such intent cannot be determined solely by the individual's personal will; it must also accord with the general standard of reasonableness recognised by society. This general perception of what is considered private may vary depending on factors such as region, cultural tradition, legal tradition, and social custom. Therefore, the determination of privacy must be made on a case-by-case basis, taking into account the specific context and its broader social implications.

When biometric information is recognised as *confidential*, three protective pathways become available for invocation. First, rely on Article 1033, which strictly prohibits acts

142 X. Fu, *The unified legislation on artificial intelligence should proceed with caution*, Oriental Law 17, 20 (2025).

143 Ding, *supra* note 137 at 65.

144 L. Cui, *Legal Characterization and Regulatory Approaches to Personal Biometric Information: An Analysis Based on Article 1034 of the Chinese Civil Code*, 313 Study & Exploration 73, 73 (2021).

145 Civil Code of the People's Republic of China 2020, art 1034(2).

146 *Id.* at art. 1034(3). 'Private information within personal information is subject to the provisions on the right to privacy; where there are no such provisions, the rules on personal information protection shall apply.'

147 *Xunxun Technology (Shenzhen) Co., Ltd. et al., Online Infringement Liability Case* (China) [2020] Beijing Internet Court (2019) Jin 0491 Min Chu No. 16142.

that infringe upon an individual's peace of private life, private space, private activities, or confidential information, unless otherwise provided by law or explicitly consented to by the right holder.[148] Second, regarding remedies, the specific provisions on the protection of personality rights may be applied. These include the general clause on personality rights (Article 990)[149], the right to claim relief for infringements on personality rights (Article 995)[150], and the injunction provision (Article 997)[151]. Third, one may invoke the general tort provisions as a fallback remedy, specifically Articles 1165 and 1166,[152] in the Part on Torts, which provide general protection against infringements. If biometric information is not recognised as private information, the data subject may find it difficult to obtain effective remedies under the Civil Code's provisions on personality rights or tort liability. In such cases, they must instead rely on the administrative or compliance mechanisms provided by the PIPL, rather than asserting a civil claim in the tort law sense. This *dual-track* structure results in significantly different levels of protection for the biometric data of children.

III.2.2. *Regulatory Framework and Compliance Obligations under the PIPL*

Under Article 28 of the PIPL, biometric data is explicitly classified as 'sensitive personal information', defined as data that, if leaked or illegally used, may infringe upon a natural person's dignity or endanger their personal or property safety.[153] Article 29 requires obtaining separate consent for processing sensitive personal information, and Article 30 further mandates that data controllers clearly justify the necessity of processing and explain its potential impact on individual rights.[154] Article 26 further regulates the use of image-capture and identity-recognition devices in public spaces, limiting such use to the necessity of maintaining public safety and requiring prominent notification. The collected data for such purposes may not be repurposed without separate consent.[155] Moreover, Article 31 introduces additional obligations for handling 'minors' personal information'. When processing the personal data of children under the age of fourteen, controllers must obtain the consent of their parents or other guardians and establish dedicated processing rules specifically designed for minors' data.[156]

148 Civil Code of the People's Republic of China art 1033.
149 *Id.* at art. 990. 'Personality rights are the rights enjoyed by civil subjects, including the right to privacy and other related rights.'
150 *Id.* at art. 995. 'Where personality rights are infringed, the victim has the right to request the infringer to bear civil liability in accordance with this Law and other applicable laws...'
151 *Id.* at art. 997. 'Where a civil subject has evidence proving that another party is committing or is about to commit an unlawful act that infringes upon their personality rights, and failure to stop such an act in time would cause irreparable harm to their legitimate rights and interests, the civil subject has the right to apply to the People's Court for an order requiring the other party to cease the relevant act in accordance with the law.'
152 *Id.* at art. 1165,1166. Article 1165: 'A person who infringes upon the civil rights and interests of others due to his fault shall bear tort liability. If it is presumed by law that the person is at fault, and the person cannot prove that he is not at fault, he shall bear tort liability.' Article 1166: 'If the law stipulates that a person shall bear tort liability for damaging the civil rights and interests of others, regardless of whether the person is at fault, such provisions shall apply.'
153 Personal Information Protection Law of the People's Republic of China (adopted 20 august 2021, effective 1 november 2021) of 2021.
154 *Id.* at art. 29, 30.
155 *Id.* at art. 26.
156 PIPL art. 31.

However, these provisions are largely principled and abstract, lacking specific standards for implementation and enforcement.[157] Violations involving biometric data often involve procedural breaches, such as failure to inform or failure to obtain clear consent, but it remains difficult in practice to determine whether such infringements of the right to be informed and the right to autonomous decision-making constitute legally remediable harm, thereby creating barriers to individual redress.[158] Moreover, under Article 26, the installation of image and identity recognition devices is permitted in public spaces solely for the purpose of maintaining public safety. However, educational environments such as classrooms serve pedagogical or administrative purposes rather than public safety functions. Therefore, their regulation should not be analogised to public-space surveillance but should instead be subject to stricter consent and transparency requirements, particularly when minors' biometric data are involved.

III.2.3. *Practical Limitations of the Civil Code and PIPL: Insights from Judicial Cases*

Civil remedies under the Civil Code are only available when personal information is simultaneously recognised as private. In such cases, individuals may initiate a tort action based on the infringement of privacy rights. Nevertheless, this remedy often proves ineffective in practice because plaintiffs must bear the burden of proving the defendant's fault under tort law. For example, in *Luo v Company X, Privacy and Personal Information Protection Dispute*[159], the plaintiff was required to provide evidence demonstrating that the defendant had unlawfully collected his mobile phone number, which in practice entailed preserving and submitting all relevant communications and transaction records.

Similar evidentiary difficulties are further magnified in AI-enabled educational settings. The collection and processing of children's educational data is often continuous, opaque, and embedded within complex technological systems, making it difficult for children and their guardians to identify specific unlawful acts or attribute responsibility to particular data controllers.[160] Coupled with the structural power imbalance between educational institutions and children,[161] these characteristics significantly undermine the data subjects' practical ability to gather evidence and effectively pursue civil remedies. Consequently, rendering tort-based relief pathways largely ineffective in addressing data protection risks in AI-powered educational environments.

A significant legislative advancement in the PIPL is the introduction of the presumption of fault under Article 69(1), which shifts the burden of proof to the data controller. If the controller cannot prove that they are not at fault for the infringement, they must bear liability for damages.[162] This theoretically alleviates the evidentiary burden on minors and their guardians. However, under Article 69(2), which stipulates that compensation is determined by the losses suffered by the individual or the benefits obtained by the

[157] H. Zhu, *Definition of Sensitive Personal Information and Improvement of the Path of Handling*, Data Governance, 53.

[158] W. Fu, *A Legal Protection Model for Personal Biometric Data and China's Regulatory Approach*, Journal of East China University of Political Science and Law, 84 (2019).

[159] *Luo v Company X, Privacy and Personal Information Protection Dispute* (China) [2021] Beijing Internet Court (2021) Jing 0491 Min Chu No 5094.

[160] R. Taylor, *New Approaches to Data Stewardship in Education*, *in* Education Data Futures: Critical, Regulatory and Practical Reflections (2022).

[161] E. Day et al., *Who Controls Children's Education Data? A Socio-Legal Analysis of the UK Governance Regimes for Schools and EdTech*, 49 Learning, Media and Technology 356 (2024).

[162] PIPL art 69(1)

controller, and where both are difficult to determine, the court shall decide the amount based on actual circumstances.[163] In judicial practice, this valuation mechanism often results in nominal rather than substantial relief. The *Guo Bing v. Hangzhou Safari Park*[164] case vividly illustrates the difficulty of quantifying losses in biometric processing. Despite the unauthorized unilateral shift from fingerprinting to facial recognition, the court only awarded compensation for the plaintiff's direct out-of-pocket expenses (such as travel costs), while dismissing claims regarding the inherent value of facial data or the risk of its misuse.

This precedent suggests that under the PIPL, the actual circumstances clause may be interpreted restrictively. For children in educational settings, the loss of biometric privacy is an intangible and long-term risk rather than an immediate financial injury. If the judiciary continues to rely on a *tangible loss* standard, Article 69(2) effectively renders the presumption of fault a right without a remedy, as the cost of litigation for guardians far outweighs the meager compensation typical of such cases.

IV. Comparative Insights

IV.1 *EU regulatory framework vis-à-vis the Chinese regulatory framework*

The Chinese and European children's data protection regimes present both normative similarities and differences in governing attention monitoring systems in education. Both systems recognise the specific needs of children and provide enhanced protection for their data.[165] Standard provisions in both frameworks include consent requirements for processing children's data and the classification of biometric data as sensitive, with additional obligations for data controllers. Notably, under the PIPL, personal data for children under 14 is automatically classified as sensitive personal information.[166] Verdoodt, Zhang, and Lievens argue that the PIPL was inspired by the GDPR, hence the several points of convergence. They illustrate several areas where the EU and Chinese regulatory approaches converge, including these core protective principles.[167] Additionally, two significant differences in the regulatory framework: are noted: the lack of an independent supervisory authority in the Chinese framework, and the application of children-specific protections only to those under 14.[168]

Aspect	European Union (GDPR & AI Act)	China (PIPL & Civil Code)
Definition of Biometric Data	Personal data enabling unique identification from physical, physiological or behavioural traits	Broad personal information, including biometric characteristics; special focus on children's data

[163] *Id.* at art. 69(2).
[164] *Guo Bing v Hangzhou Wild Animal World Co., Ltd, Service Contract Dispute* (China) [2020] Zhejiang Higher People's Court (2020) Zhe 01 Min Zhong No 10940. In this case, the defendant unilaterally upgraded its entry system from fingerprint recognition to facial recognition without obtaining the plaintiff's explicit consent.
[165] Verdoodt, Zhang, and Lievens, *supra* note 52 at 18; GDPR recital 38; PIPL art 28
[166] PIPL art 28.
[167] Verdoodt, Zhang, and Lievens, *supra* note 52 at 18.
[168] *Id.*

Scope of Regulation	Processing of personal data and AI systems use in market/services; risk-based approach	Personal information processing within the territory and extraterritorially; emphasis on data security
Protection of Emotion Data	Not automatically 'special' data unless biometric or physiological data	Classified as sensitive for children; stringent consent for minors under 14
Transparency Requirements	Clear and plain language for children; differential transparency obligations according to risk level of AI system; no requirement to disclose detected emotions	Children not explicitly mentioned, Information to children's guardians should be 'conspicuous and clear' (Art. 9 PIPL)
Consent stipulations	Generally, 16, can be lowered to 13-15 by Member States but only applies to information services (Article 8 GDPR)	14 years, with parental consent requirement for younger children
Supervisory authorities	Independent data protection authorities with enforcement powers, the European Data Protection Board (EDPB) ensures consistent implementation; AI Act establishes and recognises different supervisory and implementation authorities including the AI Office (recital 148), Market surveillance authorities and competent national authorities	Multiple government bodies, no single independent authority

Summary Table: Comparison of EU and Chinese Regulations on Affective Computing-based AI Monitoring Systems and Biometric Data

However, the regulatory logics underpinning the existing frameworks differ. Whereas EU law adopts a right, risk-focused approach that is at least partially responsive to children, Chinese law, characterised by the permissibility of attention monitoring systems in education, approaches it from a perspective of state oversight, parental authority, and educational management. The heightened safeguards in the GDPR and a categorical prohibition of biometric ERSs in schools under the AI Act confirm this European approach. China, by contrast, grounding its approach in data sovereignty and educational management, continues to deploy attention monitoring and affective systems in schools as part of a broader educational management and behavioural evaluation programmes, subject to generalised data protection obligations rather than categorical prohibitions.

Attention monitoring thus provides an important lens through which to test the robustness of the legal frameworks in protecting children's data. In both the EU and China, cracks and gaps remain. Regarding the EU model, the definitional uncertainty around what constitutes biometric data or an ERS, and the risk-based classification of AI systems in the AI Act, pose challenges for classifying attention-monitoring systems, some of which may fall outside the scope of regulation. On the other hand, the Chinese framework largely prioritises administrative oversight and parental consent, potentially leaving children exposed to surveillance and automated evaluation without proper safeguards.

This comparative perspective also raises questions of whether the 'Brussels Effect' may influence Chinese regulation in the future. Unlike the EU, where attention monitoring

systems in educational settings are not yet standard practice, China has rapidly deployed and continues to roll out such technologies nationwide. This rapid expansion of affective computing and attention monitoring in Chinese classrooms starkly contrasts with the more cautious approach in Europe. Whether this already affects the current and future alignment of Chinese law with the European framework is yet to be seen, as discussed in the following section.

IV.2 *Brussels Effect or Independent regulatory approach?*

Both the GDPR and the AI Act exemplify the EU's growing ability to project its regulatory norms globally. This phenomenon, dubbed the 'Brussels Effect', is a term coined by Anu Bradford to describe the EU's unilateral capacity to shape global standards via market mechanisms rather than coercive diplomacy.[169] Companies seeking access to European markets adapt their practices to comply with EU rules, producing a form of *de facto* harmonisation beyond Europe's borders.[170] Elements of this influence can be observed in the evolution of China's data protection framework. The PIPL incorporates GDPR-inspired provisions, such as lawful bases for processing, special protection for minors, and recognisable data subject rights, indicating formal alignment between the two regimes.[171]
Yet, scholarship has increasingly questioned whether the *Brussels Effect* adequately captures the dynamics at play. Bradford describes the phenomenon where global businesses adapt to comply with EU law, but states maintain their domestic frameworks[172]. This leads to bifurcated compliance models where Chinese technological companies operating internationally design products to meet EU requirements while adhering to different state exigencies for their national operations.
In this context, Chinese purported alignment with EU law, such as the GDPR with the PIPL, has been described as a '*gravity assist'*, where the development of a country's privacy law results from internal and external factors (*sources of gravity*).[173] Driven by strategic motivations, a partial alignment of data privacy rules between regimes is viewed as a temporary phenomenon[174], so that the EU's unilateral regulatory influence will diminish once complying with EU standards outweighs the benefits. Thus, EU law functions less as a normative template and more as a reference point used strategically to bolster China's global legitimacy, facilitate data transfers and consolidate state-led governance.
These tensions are illustrated vividly when considering children's data protection in the context of affective computing and attention monitoring. While the AI Act explicitly bans ERS in schools, China still permits experimental use of EEG headbands and gaze-tracking systems, justifying them as educational efficiency and social control tools. The Brussels Effect thus results in only partial convergence: it influences the language and formal structures of Chinese data protection law but not its core commitments. Analysing the evolution of Chinese data protection law through the concept of gravity assists highlights the importance of differentiating between formal similarities and substantive alignment

169 A. BRADFORD, The Brussels Effect: How the European Union Rules the World (2020), https://scholarship.law.columbia.edu/books/232.
170 A. Bradford, *Exporting Standards: The Externalization of the EU's Regulatory Power via Markets*, 42 International Review of Law and Economics 158, 159 (2015).
171 Verdoodt, Zhang, and Lievens, *supra* note 52 at 18; R. Creemers, *China's Emerging Data Protection Framework*, 8 Journal of Cybersecurity 1, 6 (2022); W. Li & J. Chen, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China*, 54 Computer Law & Security Review 1 (2024).
172 Bradford, *supra* note 170 at 160.
173 Li and Chen, *supra* note 171 at 6.
174 *Id.*

when evaluating the global spread of EU standards in children's rights and educational technologies.

Still, the interaction between the EU and Chinese frameworks reveals the potential for reciprocal influence, even in the absence of full convergence. For instance, the PIPL's automatic classification of personal information of children under 14 as sensitive data establishes a higher threshold of protection than that provided under EU law, where no equivalent age-based presumption exists. However, this protection remains limited in scope. Children aged 14 to 18 occupy a legal grey zone: their personal information does not enjoy the same heightened protection, leaving their data in regulatory limbo. While EU law does not provide an explicit statutory definition of a child, the Article 29 Working Party[175] interprets this category consistently with Article 1 CRC, covering all individuals under 18.

Additionally, unlike in the EU, China's Constitution does not explicitly recognise personal information as a fundamental right, while the Civil Code classifies it merely as a type of personal information, with protection largely dependent on privacy rights as a remedy. The EU's rights- and risk-based approach under the GDPR and AI Act could, thus, inform future Chinese reforms by offering a model of rights-based contextualised protection and proactive oversight, particularly relevant to technologies such as attention monitoring systems.

V. CONCLUSION

Attention monitoring and affective computing technologies in educational settings highlight the growing tension between technological innovation and the protection of children's fundamental rights. Because these systems process sensitive data such as emotion and biometric data, their governance warrants the highest level of legal protection.

The comparative analysis of the EU and China frameworks reveals both shared regulatory challenges and normative divergences. In the EU, the definitional ambiguities in the GDPR and AI Act risk leaving some emotion recognition and attention monitoring systems outside the formal scope of biometric data protection. However, the categorical prohibition on biometric-based ERSs in educational settings reflects a precautionary approach consistent with the Union's rights-based legal order. In contrast, China's framework, while demonstrating formal convergence with global data protection norms through the PIPL, continues to emphasise state imperatives alongside data protection and privacy considerations.

These findings also illustrate the global relevance and limits of European regulatory influence. Although European data protection models exert gravitational influence (*gravity assists*), substantive divergence persists where domestic priorities and conceptions of public interest prevail. The diffusion of EU-style data protection norms thus remains partial and value contingent, reflecting distinct regulatory cultures.

In conclusion, protecting children in AI-driven educational environments requires moving beyond narrow definitional boundaries towards a children's rights-centred governance framework. Such a framework, anchored in the CRC principles of non-discrimination, a child's best interests, participation, survival, and development, treats affective and attention monitoring systems with caution. It also ensures that technological innovation in education advances rather than compromises children's rights and dignity.

[175] Guidelines On Transparency Under Regulation 2016/679 (Adopted On 29 November 2017 As Last Revised And Adopted On 11 April 2018) 10 (2017).