

校園 AI 治理紅線——從歐盟標準看兩岸隱私法制

許慧儀

國立臺北教育大學教育經營與管理博士生

摘要

隨著生成式人工智慧與大數據技術全面滲透教育場域，智慧校園中的數位監控與演算法黑箱對學生隱私造成前所未有的威脅。學生在師生權力不對等中處於弱勢，若缺乏嚴格的監管，極易淪為數據剝削客體。本文旨在探討並劃定校園 AI 應用的「治理紅線」，檢視歐盟規範與海峽兩岸隱私法制之發展脈絡。本文首先確立歐盟標準人權底線，梳理聯合國兒童最佳利益原則以及歐盟《一般資料保護規則》與《人工智慧法案》中資料最小化、高風險分級與絕對禁止情緒辨識的規範。其次，探討中國大陸校園 AI 從不可控生長到以《個人信息保護法》等法規收攏監管之法制與實務演進；並檢視台灣現行法制困境，指出《個人資料保護法》面對 AI 資料最大化時之法理侷限，及政府過度依賴行政指導所造成之法律真空。本文透過比較歐盟規範與海峽兩岸之校園人工智慧法制，期能在促進教育科技創新與保障學生數位人權間，理清完善之法制衡平框架。

關鍵字：校園 AI 治理、數位隱私、歐盟人工智慧法案、個人資料保護法、風險分級

Red Lines in Campus AI Governance: Examining Cross-Strait Privacy Legal Frameworks under EU Standards

Hsu, Hui-Yi

Ph.D. Student in Educational Management, National Taipei University of Education

Abstract

As generative AI and big data technologies increasingly permeate educational settings, digital surveillance and algorithmic black boxes on smart campuses pose unprecedented threats to student privacy. Given the inherent power asymmetry between educators and students, students are highly vulnerable and, without strict regulation, can easily become the subjects of data exploitation. This paper aims to explore and delineate the "governance red lines" for AI applications on campus. Through the lens of comparative law, it provides an in-depth examination of the developmental trajectories of European Union standards and cross-strait privacy legal frameworks.

First, this study establishes the human rights baseline set by EU frameworks, specifically reviewing the European Union's General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). Specifically, it highlights their provisions on data minimization, high-risk classification, and the absolute prohibition of emotion recognition systems. Second, the paper explores the legal evolution and practical tensions in mainland China, tracing the shift from unfettered proliferation to the tightening of regulations through hard laws such as the Personal Information Protection Law (PIPL). Additionally, it examines the current legal predicaments in Taiwan, pointing out the jurisprudential limitations of the Personal Data Protection Act (PDPA) in the face of AI-driven data maximization, as well as the legal vacuum created by the government's over-reliance on soft-law administrative guidelines.

Keywords: Campus AI Governance, Digital Privacy, EU Artificial Intelligence Act (EU AI Act), Personal Data Protection Act, Risk Classification

壹、前言

隨著生成式人工智慧（Generative AI）、機器學習與大數據分析技術的前瞻性發展，智慧校園已從未來願景迅速轉變為當前的現實。AI 技術正全面滲透教育場域，然而，教育資料的規模化蒐集與演算法的不透明作業，也讓校園成為隱私風險的重災區。學生作為心智尚未完全成熟、且在校園及師生權力關係中處於絕對弱勢的群體，其個人資料若缺乏嚴格的保護與監管，將面對被商業濫用、歧視性標籤化及全面監控的巨大危機。因此，劃定校園 AI 應用的「治理紅線」，已成為全球教育與法學界亟待解決的議題。

歐洲聯盟（EU）在數位人權領域的探索一直走在世界前列。從2018年全面生效的《歐盟一般資料保護規則（GDPR）》確立「資料最小化」與「特殊類別個資原則上禁止處理」的基調¹；到2024年8月1日正式生效的《歐盟人工智慧法案（EU AI Act）》，更明確將相關類別列為「高風險」級別，要求開發者與部署者實施嚴格的風險管理、資料治理與人為監督，並明令禁止在教育與工作場所使用 AI 推斷個人情緒，此一禁制條款已於2025年全面落實²。與此同時，聯合國教科文組織（UNESCO）發布的《人工智慧倫理建議書》³以及聯合國兒童基金會（UNICEF）發布的《AI 與兒童政策指引》⁴，皆呼籲在設計與部署教育 AI 時，須以『兒童最佳利益』為考量。這些國際標準共同形塑不可逾越的人權紅線，科技便利絕不能以犧牲學生隱私與發展自主權為代價。

回到兩岸，在中國大陸，AI 與大數據技術在校園應用曾一度呈現高速且難以控制生長的態勢，例如透過「AI 頭環」監測學生注意力⁵、無處不在的人臉辨識打卡與行為分析系統等，引發社會對「圓形監獄」式校園的強烈擔憂。為回應科技反噬現象，中國大陸近年來加快法制收攏腳步。2021年實施的《中華人民共和國個人信息保護法（PIPL）》特別針對不滿14周歲未成年人的個人信息設專章保護，並嚴格限縮公共場所圖像採集設備的設置條件⁶。隨後，2024年施行的《未成年人網絡保護條例》進一步限制利用演算法對未成年人進行畫像與自動化推播。此外，《生成式人工智能服務管理暫行辦法》亦強調

¹ 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), Official Journal of the European Union, L 119, May 4, 2016, p. 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> (last visited July 10, 2026).

² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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), Official Journal of the European Union, L, 2024/1689, July 12, 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (last visited July 10, 2026).

³ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, UNESCO, <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> (last visited July 10, 2026).

⁴ UNICEF, *Policy Guidance on AI for Children*, UNICEF GLOBAL INSIGHT, <https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children> (last visited July 10, 2026).

⁵ 關於「智慧頭環」爭議事件，參見 BBC 中文網，〈中國小學「監控頭環」引發爭議：科技發展與隱私保護的博弈〉，2019 年 11 月 1 日，<https://www.bbc.com/zhongwen/trad/chinese-news-50262174>（最後瀏覽日：2026 年 7 月 10 日）。

⁶ 中華人民共和國全國人民代表大會常務委員會，《中華人民共和國個人信息保護法》（2021 年 8 月 20 日第十三屆全國人民代表大會常務委員會第三十次會議通過），中國國家互聯網信息辦公室，https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm（最後瀏覽日：2026 年 7 月 10 日）。

科技倫理與隱私保護⁷。而在社會治理的需求下，中國大陸校園隱私保護在「學校管理效率」與「學生個體權利」間的拉扯，仍是充滿張力的實務難題。

視角轉向台灣，台灣在校園資訊化建設上同樣積極，但在 AI 技術導入的監管上，目前仍依賴既有的《個人資料保護法》⁸框架。雖然該法對於個人資料的蒐集與處理設有「告知後同意」及「比例原則」等基本要求，但面對 AI 自動化決策、深度學習與無感式的生物特徵蒐集，傳統法制顯力有未逮。近年來，教育部雖陸續發布《中小學人工智慧教育與應用參考指引》⁹以及針對生成式 AI 的校園使用指引等軟性行政指導，試圖在創新與倫理間取得平衡；但因缺乏針對校園 AI 應用的具體法律禁制，令實務上往往面臨「無法可管」或「各校自行其是」的窘境。但隨著《人工智慧基本法》的立法推進與施行，雖確立風險分級與人權保障的大原則，但如何在保障學生數位隱私的前提下，由教育主管機關進一步確立符合國際人權趨勢的校園 AI 治理具體規範，已是台灣法制現代化不可迴避的挑戰。

貳、 歐盟規範的數位人權與校園 AI 治理紅線

在探討校園人工智慧的治理框架時，國際規範提供最為核心的價值定錨。面對演算法不透明與數據資本主義的擴張，傳統國內法往往難以迅速回應新興科技帶來的隱私衝擊。因此，本章從聯合國體系對「兒童最佳利益」的延伸，及歐盟極具前瞻性的《一般資料保護規則》（GDPR）與《歐盟人工智慧法案》（EU AI Act），探討國際社會如何為校園 AI 應用劃定人權與隱私治理紅線。

一、 學生數位隱私與兒童最佳利益原則

隨著教育場域全面數位化，擴展至數位人權領域。學生作為心智尚未完全成熟且極易受外在環境影響群體，在面對校園 AI 系統資料蒐集與演算法時，處於絕對弱勢地位。因此，國際組織陸續發布指引，試圖將原則具體化為 AI 治理的實體規範。

聯合國教科文組織於2021年通過的《人工智慧倫理建議書》（Recommendation on the Ethics of Artificial Intelligence）¹⁰，是全球首份針對 AI 倫理的全球性規範框架。在教育與學習的專章中，明確指出 AI 技術在教育領域的應用應以「支持學習過程」與「增進人類能力」為目的，而非取代人類教師的引導，更不能將學生客體化為純粹的「數據產出者」。

從學生數位隱私角度出發，UNESCO 建議書帶來兩項重要啟示。首先是「人類能動性與監督」的堅持。強調在涉及學生評量、行為預測等教育決策時，不能全交由自動化系統進行，須保留人類最終決定權，以防止演算法偏見對學生造成不可逆的傷害。其次是「公

⁷ 中國國家互聯網信息辦公室，〈生成式人工智能服務管理暫行辦法〉，2023 年 7 月 13 日，https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm（最後瀏覽日：2026 年 7 月 10 日）。

⁸ 立法院，〈個人資料保護法〉，全國法規資料庫，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021>（最後瀏覽日：2026 年 7 月 10 日）。

⁹ 教育部，〈中小學人工智慧教育與應用參考指引〉，AI 人才方舟計畫，<https://pads.moe.edu.tw/download.php>（最後瀏覽日：2026 年 7 月 10 日）。

¹⁰ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, UNESCO, <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> (last visited July 10, 2026).

平與不歧視」原則。校園 AI 系統訓練資料若隱含社會既有的偏見（如性別、種族或社經地位），AI 將會放大這些歧視。因此，建議書呼籲教育機構在導入 AI 時，須對演算法公平性進行事前評估，確保數位科技引入不會加劇教育資源分配不均，實質保障學生受教權益。

聯合國兒童基金會（UNICEF）發布的《AI 與兒童政策指引》（Policy Guidance on AI for Children）¹¹則更聚焦未成年人的數位脆弱性。宣告 AI 政策制定須以「兒童為中心」，並提出九大原則，其中最核心為「保護兒童的資料與隱私」。UNICEF 強烈建議，各國政府與學校應嚴格限制對兒童進行畫像，特別是禁止將學習資料用於商業行銷或轉售第三方。此外，該指引主張應賦予兒童及其監護人對個人數據的「刪除權」與「被遺忘權」，確保學生在校園內產生的數位足跡，具體轉為對抗資料剝削的權利武裝。

二、 歐盟資料保護法制與教育場域之適用

2018年全面生效的《一般資料保護規則》（GDPR）¹²，是全球隱私保護之高標準，其規範影響全球教育領域的資料治理。

在教育場域中，學校基於行政管理與教學目的，蒐集學生個人資料。然而，GDPR 第5條所確立「資料最小化原則」¹³，要求資料蒐集與處理須「適當、相關且以達成處理目的所必要者為限」。意指學校引入 AI 系統時，須證明其所蒐集的資料與數量，是達成教育目的之「最小必要範圍」。若僅為提升少許管理便利性，大規模蒐集學生的無關數據，即構成對資料最小化原則的違反。

更為關鍵的是，GDPR 對於「同意」機制嚴格界定。在師生權力嚴重不對等的校園結構中，學生或家長往往迫於學校壓力或為獲取教育資源，而須點選「同意」條款。歐洲資料保護委員會（EDPB）實務指引明確指出，在此種權力失衡狀態下，當事人的「同意」缺乏真實自由意志，因此學校不能僅憑一紙同意書，合法化所有 AI 系統資料蒐集行為¹⁴。

GDPR 第9條針對「特殊類別之個人資料」¹⁵，設定「原則禁止、例外允許」的高強度門檻。其中，用於唯一識別自然人的「生物特徵資料」（如人臉、指紋、虹膜）被列為高敏感個資。在校園情境中，此規範產生強大禁制力。例如自 2019 年起，歐洲部分學校曾試圖在校園內裝設人臉辨識點名系統。瑞典資料保護局（IMY）在 Skellefteå 高中試辦人臉辨識考勤的裁決中指出¹⁶，基於校方與學生間的權力不對等，學生的「同意」不

¹¹ UNICEF, *Policy Guidance on AI for Children*, UNICEF GLOBAL INSIGHT, <https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children> (last visited July 10, 2026).

¹² 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), O.J. 2016 L 119/1.

¹³ GDPR, Art. 5(1)(c) (Data minimization).

¹⁴ 歐洲資料保護委員會（European Data Protection Board, EDPB）發布之指引指出，在公權力機關或雇主與員工（法理上可類推適用於學校與學生）之間存在明顯的權力不平衡（Imbalance of power），當事人難以在不受不利益威脅下拒絕同意，故其「同意」通常不被視為符合 GDPR 下「自由給予（Freely given）」之合法要件。參見 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, para. 16-24.

¹⁵ GDPR, Art. 9(1) (Processing of special categories of personal data).

¹⁶ 瑞典資料保護局（現為 IMY，原為 Datatilsynen）於 2019 年 8 月針對 Skellefteå 學校委員會開出瑞典首張 GDPR 罰單。參見 Swedish Authority for Privacy Protection (IMY), *Facial recognition in school renders Sweden's first GDPR fine*, August 21, 2019.

具備合法性；且僅為單純點名行政目的而處理敏感的生物特徵，嚴重違反「資料最小化原則」與利益權衡。法國國家資訊自由委員會（CNIL）與馬賽行政法院亦在類似的高中人臉辨識鬧門案中，做出違反比例原則的相同認定¹⁷。這為校園生物特徵的大規模濫用，劃下堅實的法律紅線。

三、《歐盟人工智慧法案》的風險分級與禁制

隨著 AI 技術從單純資料處理演進為具備推論、預測與自主決策能力的系統，傳統以「個人資料」為核心的 GDPR 已不足以應對演算法帶來的全方位風險。為此，歐盟於2024年正式生效的《歐盟人工智慧法案》（EU AI Act）¹⁸，象徵數位監管從「資料保護」邁向「演算法治理」。該法案首創「風險基礎途徑」，依據 AI 系統可能對人類基本權益造成的危害程度，劃分為不可接受風險、高風險、有限風險與極小風險四個等級，對校園 AI 應用產生決定性的影響。

《歐盟人工智慧法案》對校園隱私法制最具突破且象徵意義的規範，在其第5條關於「禁止性 AI 實踐」規定¹⁹。法案明確將「在工作場所與教育機構中使用 AI 系統推斷自然人的情緒」列為不可接受風險，予以全面禁止。此禁令已於2025年初在歐盟境內全面生效。

綜上所述，從聯合國的「兒童最佳利益」原則，到 GDPR 的「資料最小化」，再到《歐盟人工智慧法案》全面封殺校園情緒辨識，這些國際標準顯示其正在共同構築嚴密的防護網，無論技術如何進步，保障學生主體性、尊嚴與內在自由，始終是校園 AI 應用不可逾越的治理紅線。

參、中國大陸校園 AI 應用之法制演進與實務張力

中國大陸作為全球 AI 技術發展最猛烈的國家之一，其教育體系曾是各類前沿演算法與監控技術的絕佳試驗場。然而，隨著科技狂飆帶來的隱私反噬引發強烈民怨，中國大陸近年來迅速啟動法制收攏的步伐。本章將從中國大陸校園 AI 應用從擴張到依法合規的演進軌跡，探討在國家治理、學校管理效率與學生個體權利之間，那些仍充滿張力的實務困境。

一、科技狂飆與校園監控之爭議案例

在2015年至2020年間，伴隨智慧教育政策大力推動及充沛的商業資本挹注，中國大陸校園內的 AI 應用呈現野蠻生長態勢。教育科技業者與學校管理者為追求教學效率與絕對安全，將大量帶有強烈監控性質的技術引入校園，對學生數位隱私造成巨大衝擊。

¹⁷ 法國案例參見法國國家資訊自由委員會（CNIL）對蔚藍海岸大區（Région PACA）高中建置人臉辨識系統之警告，以及馬賽行政法院（Administrative Court of Marseille）於 2020 年 2 月之判決。參見 CNIL, Facial recognition in high schools: the CNIL underlines that the planned systems are contrary to the GDPR, October 29, 2019.

¹⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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), O.J. 2024 L 1689.

¹⁹ EU AI Act, Art. 5(1)(f). 該條文禁止將 AI 系統用於工作場所與教育機構推斷自然人之情緒（the placing on the market, putting into service for this specific purpose, or use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions），除非基於醫療或安全理由。

最為著名的為2019年浙江省金華市某小學的「AI頭環」事件²⁰。該設備透過讀取學生腦電波量化注意力集中程度，並將數據實時傳送給教師與家長。這種將學生大腦活動直接數據化、並作為評分依據的作法，引發輿論對「思想監控」強烈撻伐，最終迫使當地教育局下令暫停使用。

「人臉辨識」技術在中國大陸校園的泛濫亦達到高峰。從校門禁、宿舍打卡、圖書館借書到食堂支付，學生生物特徵成為校園通行證。部分科技公司亦推出「課堂行為分析系統」，透過架設在黑板上方的AI攝影機，實時捕捉並分類每位學生的微表情與肢體動作（如聽講、閱讀、舉手、趴桌睡覺等），生成學生的「專注度報表」²¹。

這些技術的應用，實質上將校園轉化為一座高科技的「圓形監獄」。在全天候、無死角的監控下，學生不僅喪失隱私，其行為更被異化為迎合演算法評分標準的表演。過度數據化不僅無法提升真實教育品質，反而剝奪學生自由發展人格的空間，這種科技對教育本質的嚴重反噬，成為推動後續法制重塑的導火線。

二、《個人信息保護法》之規範重塑

面對社會對無底線科技監控的反彈，中國大陸於2021年實施《中華人民共和國個人信息保護法》（以下簡稱PIPL）²²。該法作為中國大陸數據保護領域的基本法，大幅借鑒歐盟GDPR的立法精神，對校園AI資料蒐集劃定嚴格的法律界線，使教育科技應用進入規範重塑的新階段。

依據PIPL第28條與第31條之規定，法律將「不滿14周歲未成年人的個人信息」定性為「敏感個人信息」²³。代表學校或相關單位若要處理國中及小學學生的學習數據、行為軌跡或生物特徵，應符合更嚴苛的條件：必須具備「特定的目的和充分的必要性」，採取嚴格的保護措施，亦須取得未成年人父母或其他監護人「單獨同意」，且應當制定專門個人信息處理規則。

2024年1月1日施行的《未成年人網絡保護條例》²⁴進一步鞏固這道防線，條例嚴格限制

²⁰ 關於「智慧頭環」爭議事件，參見BBC中文網，〈中國小學「監控頭環」引發爭議：科技發展與隱私保護的博弈〉，2019年11月1日，<https://www.bbc.com/zhongwen/trad/chinese-news-50262174>（最後瀏覽日：2026年7月10日）。

²¹ 曠視科技（Megvii）曾於2019年展示其「AI課堂行為分析」概念系統，該系統能即時辨識學生聽講、玩手機、睡覺等行為並給予評分，引發輿論對隱私權與教育倫理之強烈抨擊。相關探討參見：新京報，〈教室裝監控抓學生小動作？曠視科技回應：僅為技術場景概念演示〉，2019年9月2日，<https://www.c114.com.cn/ai/5339/a1099705.html>（最後瀏覽日：2026年7月10日）。

²² 中華人民共和國全國人民代表大會常務委員會，《中華人民共和國個人信息保護法》（2021年8月20日第十三屆全國人民代表大會常務委員會第三十次會議通過），中華人民共和國國家互聯網信息辦公室中央網絡安全和信息化委員會辦公室，https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm（最後瀏覽日：2026年7月10日）。

²³ 《中華人民共和國個人信息保護法》第28條規定：「敏感個人信息是一旦洩露或者非法使用，容易導致自然人的的人格尊嚴受到侵害或者人身、財產安全受到危害的個人信息，包括生物識別、宗教信仰、特定身份、醫療健康、金融賬戶、行蹤軌跡等信息，以及不滿十四周歲未成年人的個人信息。」

²⁴ 中華人民共和國國務院，〈未成年人網絡保護條例〉，中國政府網，2023年10月24日公布，2024年1月1日施行，http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/content/202310/content_6911288.htm（最後瀏覽日：2026年7月10日）。

網路服務提供者利用演算法對未成年人進行「畫像」與自動化推播。這些法規相互交織，使得過去「預設開啟、無感蒐集」的校園 AI 系統在法律上失去正當性。

另外，PIPL 對校園 AI 監控最具殺傷力的條文，莫過於第26條針對圖像採集與個人身份識別設備的限制。其規定在公共場所安裝此類設備，必須「為維護公共安全所必需」，且應當設置顯著的提示標識；所收集的影像與特徵，只能用於維護公共安全的目的，不得用於其他用途²⁵。

此條款在實務界引發激烈「校園適用爭議」。教室與校園走廊是否屬於法律定義的「公共場所」？若是，則學校基於「考勤管理」或「課堂專注度分析」等行政或教學目的而使用人臉辨識與 AI 攝影機，顯然逾越「維護公共安全」的法定紅線。對此，中國大陸教育部等主管機關近年來態度逐漸明朗，多次發布指導意見，要求校園內慎用人臉辨識技術。並於2025年6月1日起施行《人臉識別技術應用安全管理辦法》²⁶明確人臉辨識資訊處理，例如規則處理須具特定目的與充分必要性，採侵害最小方式並嚴格保護；同時須履行告知義務，並取得當事人充分知情之「單獨同意」(未滿14歲者須經監護人同意)。此外，除法定或另獲同意外，人臉資訊限存於設備本機端且禁止外傳，保存期須降至最短，且事前必須完成個資保護影響評估並留存紀錄等，相關解釋及規範已著實收緊。

三、 演算法與生成式 AI 服務之合規挑戰

中國大陸於2023年率先全球發布《生成式人工智能服務管理暫行辦法》(以下簡稱《暫行辦法》)²⁷目前亦正積極推進綜合性的《人工智能法(草案)》²⁸。該辦法對投入教育場域的生成式 AI 服務施加沉重的合規義務，徹底改變教育科技產業遊戲規則。

首先是「演算法偏見與歧視」的防範。《暫行辦法》第4條要求，在演算法設計、訓練資料選擇與模型生成過程中，須採取有效措施防止產生性別、年齡、職業等歧視。意味自動評分系統或學習路徑推薦演算法，不能因學生社經背景或過往成績而給予歧視性評價或差別待遇。

其次是「防沉迷與未成年人保護」。《暫行辦法》第10條明定，提供者應採取有效措施防範未成年人過度依賴或沉迷生成式 AI 服務。要求教育科技業者在開發 AI 輔導工具時，須內建工時限制與內容過濾機制，避免 AI 為學生直接提供作業答案，或生成違反公序良俗的有害內容。

²⁵ 《中華人民共和國個人信息保護法》第 26 條規定：「在公共場所安裝圖像採集、個人身份識別設備，應當為維護公共安全所必需，遵守國家有關規定，並設置顯著的提示標識。所收集的個人圖像、身份識別信息只能用於維護公共安全的目的，不得用於其他目的；取得個人單獨同意的除外。」

²⁶ 中國國家互聯網信息辦公室，〈人臉識別技術應用安全管理辦法〉，2025 年 3 月 21 日，https://www.moj.gov.cn/pub/sfbgw/lfyjzj/lflfyjzj/202308/t20230808_484167.html (最後瀏覽日：2026 年 7 月 11 日)。

²⁷ 中國國家互聯網信息辦公室，〈生成式人工智能服務管理暫行辦法〉，2023 年 7 月 13 日，https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (最後瀏覽日：2026 年 7 月 10 日)。

²⁸ 中國大陸《人工智能法》之立法推進，已正式列入官方年度立法計畫。參見中華人民共和國國務院辦公廳，〈國務院 2023 年度立法工作計劃〉(國辦發〔2023〕14 號)，中華人民共和國生態環境部，2023 年 6 月 7 日，https://www.mee.gov.cn/zcwj/gwywj/202306/t20230607_1033044.shtml (最後瀏覽日：2026 年 7 月 11 日)。

最後是「數據訓練的合法性」。《暫行辦法》第7條要求用於訓練模型的數據須來源合法，若涉及個人信息，必須取得當事人同意。這切斷過去業者將千萬學生的過往作業、考試卷或線上問答紀錄直接免費餵給大模型進行訓練的灰色產業鏈。業者必須進行嚴格的資料去識別化或重新獲取家長明確授權。若系統具有輿論屬性或社會動員能力，業者在產品上線前還須完成安全評估與演算法備案。這些嚴苛的合規要求，雖大幅提高教育 AI 的安全性，但也無形中拉高技術創新門檻，重塑中國大陸教育科技產業生態。

肆、台灣校園 AI 隱私法制現況與規範挑戰

在全球教育數位轉型的浪潮中，台灣憑藉著深厚的資通訊（ICT）產業底蘊，積極推動「智慧校園」建設。然而，相較於歐盟以強勢法規劃定人權紅線，或中國大陸以密集立法收攏科技監管，台灣在校園 AI 的隱私法制上，呈現出「法律滯後、規則乏力」的困境。本章將從台灣智慧校園的發展現況檢視現行《個人資料保護法》在面對 AI 技術時的法理侷限，探討現階段依賴行政指導所造成的法律真空。

一、智慧校園發展與 AI 應用現況

自2022年起，教育部全面啟動「推動中小學數位學習精進方案（班班有網路、生生用平板）」²⁹，為校園 AI 落地鋪平硬體基礎。隨後，各類基於大數據與機器學習技術的教育科技產品大規模進入校園。

目前台灣校園 AI 應用主要集中於兩大領域：其一為「適性化學習平台」，如官方推動的「因材施教」或民間教育平台等。這些平台透過演算法記錄學生答題正確率、觀看教學影片的停留時間與行為軌跡，進而自動生成個人化的學習路徑推薦。然而，隨著教育科技的擴張，資料蒐集逐漸走向無感式與極端化。除常規的學習歷程外，部分民間教育科技業者已開始推廣具備前置鏡頭捕捉臉部表情變化以分析專注度的「AI 專注力分析」系統，並試圖透過產學合作或實驗計畫導入教學場域。其二為「校園安全與行政管理系統」，近年台灣部分高中與大學陸續試辦具備人臉辨識功能的智慧門禁與圖書館借閱系統，此舉引發民間人權團體對於校園生物特徵過度蒐集的強烈質疑，批評學校不應淪為監控科技的實驗場³⁰。

隨著生成式 AI 的普及，校園 AI 應用更從「被動數據分析」轉向「主動內容生成」，AI 助教、自動作文批改系統逐漸成為師生日常工具。然而，這些立意良善的教育科技背後，卻伴隨海量學生個資常態性蒐集。在缺乏針對 AI 特性量身打造的隱私法規，這些資料流向、演算法演算邏輯，及資料是否被教育科技業者二次用於商業模型訓練，皆成為校園隱私隱憂³¹。以故，則須思考是否應建議教育部規定各級學校在採購 AI 系統前，強制業者提交「演算法與隱私影響評估」，從資金與市場端阻斷違規 AI 進入校園以維護學

²⁹ 教育部，〈推動中小學數位學習精進方案〉，教育部全球資訊網，2021 年 12 月，<https://pads.moe.edu.tw/>（最後瀏覽日：2026 年 7 月 10 日）。

³⁰ 台灣人權促進會，〈給教育部長的公開信：有關校園人臉辨識技術的使用〉，台灣人權促進會網站，<https://www.tahr.org.tw/news/2539/>（最後瀏覽日：2026 年 7 月 13 日）。

³¹ 學理上稱此現象為「教育數據資本主義（Educational Data Capitalism）」，指教育科技業者透過免費或低價提供平台服務，換取海量學生行為數據，並將其轉化為訓練商業 AI 模型或精準推播之資本。關於教育平台化與資料二次利用之隱私風險，詳細探討請參見 Williamson, B., *Big Data in Education: The Digital Future of Learning, Policy and Practice*, SAGE PUBLICATIONS, 2017, pp. 85-110.

生基本人權。

二、《個人資料保護法》在 AI 時代的局限

台灣目前對於校園個資保護，仰賴2010年大幅修正，雖於2015年、2023年及2025年陸續進行修法，但核心框架仍屬『前 AI 時代』的《個人資料保護法》（以下簡稱個資法）³²。這套制定於「前 AI 時代」的法律框架，以傳統靜態資料建檔與人工處理為預設情境，面對 AI 大數據分析「動態預測」與「自動化決策」，顯力有未逮。

《個資法》的核心正當性基礎在於「告知後同意」機制。依據該法第7條規定，同意必須是當事人經充分告知後所為「出於自由意志」表示。然在校園場域中，此一機制面臨著結構性的崩解。

首先，師生間存在天然「權力不對等」。當學校或教師基於教學管理目的，要求全班學生使用特定設備或系統，學生或家長實質上不具備說「不」的權利。若拒絕同意，學生可能面臨無法繳交作業、無法參與課堂測驗，甚至被邊緣化的不利益。在此「被迫自願」情境下，家長勾選的同意書，在法理上無法滿足「自由意志」要件，使《個資法》同意防線形同虛設。

此外，在無感式資料蒐集對比例原則部分，《個資法》第5條明定「比例原則」，要求個人資料之蒐集、處理或利用「不得逾越特定目的之必要範圍」³³。此即歐盟 GDPR 所稱「資料最小化」原則。然而，AI 技術的運作邏輯恰好相反，其仰賴的是「資料最大化」，透過餵養海量數據來提升模型精準度。

現代智慧校園中，資料蒐集是無感式的。學生在使用平板電腦時，系統不僅記錄其答題對錯，更可能默默記錄其滑鼠游標移動軌跡、停留秒數、打字習慣，甚至透過前置鏡頭捕捉臉部表情變化。學校與業者往往以優化教學體驗為名，將蒐集目的無限擴張。在此情況下，《個資法》第5條的「必要範圍」變得難以界定。若無具體法規加以限縮，學校極易以追求管理效率，合理化對學生實施全面且過度數據採控，對比例原則構成嚴重挑戰。

三、教育部行政指導之軟性規範與不足

為回應 AI 應用浪潮，教育部於2023年正式發布《中小學人工智慧教育與應用參考指引》³⁴，隨後因應生成式 AI 的普及，陸續頒布相關使用參考指引³⁵。這些指引確實在開篇提及「隱私保護」、「資料安全」與「避免演算法偏見」等重要 AI 倫理原則，並提醒教師在引導學生使用 AI 工具時應注意個資不可外洩。

然而，從行政法學角度觀之，「參考指引」屬《行政程序法》第165條所稱之「行政指導」

³² 立法院，《個人資料保護法》，全國法規資料庫，2025 年 11 月 11 日公布，

<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021>（最後瀏覽日：2026 年 7 月 10 日）。

³³ 《個人資料保護法》第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」

³⁴ 教育部，〈中小學人工智慧教育與應用參考指引〉，AI 人才方舟計畫，

<https://pads.moe.edu.tw/download.php>（最後瀏覽日：2026 年 7 月 10 日）。

³⁵ 同前註 33。

³⁶，其性質不具備法律強制力的建議或勸導。這種政策定位導致三個致命的實務落差：

第一，缺乏法律禁制力與罰則。指引僅能鼓勵學校注意隱私，但若某學校執意在教室內安裝大規模情緒辨識攝影機，或要求學生提供人臉特徵，指引本身並無法直接禁制，亦無對應罰則。

第二，規範對象的侷限性。教育部指引主要約束對象為學校與教師，但真正掌握核心演算法與資料庫的，是背後的「教育科技業者」。在台灣過去《個資法》採分業管轄的體制下，教育部門難以跨界直接開罰民間科技公司。儘管「個人資料保護委員會籌備處」已成立，但面對此一法制真空，當前行政指導仍無法越過學校，實質監管業者商業模式與資料流向。

第三，各地學校自行其是亂象。由於缺乏統一硬性法規，是否導入具爭議性的 AI 設備，往往取決於各校校長或資訊組長個人認知。使得學生隱私保障程度因校而異，無法形成全國一致基本人權底線。此種法制真空，凸顯台灣在推進《人工智慧基本法》與完善專項法規上新增之迫切性。

伍、兩岸校園隱私法制比較與治理紅線

經過前述章節對國際標準的確立、中國大陸法制收攏的觀察，以及台灣現行法制侷限探討，本章將透過比較海峽兩岸的法制演進軌跡，釐清雙方在治理紅線上的優勢與侷限，藉此作為未來重塑學校、業者與學生三方權利義務關係的探討基礎。

海峽兩岸在應對校園 AI 浪潮時，基於不同的社會脈絡與政治體制，展現截然不同的法制演進軌跡。首先，在立法精神與規範上，中國大陸呈現「先狂飆、後重管」特徵。在國家治理宏觀需求驅動下，AI 技術在校園的落地極為迅速，但也引發嚴重的隱私反噬。為此，中國大陸迅速提出《個人信息保護法》（PIPL）與《生成式人工智能服務管理暫行辦法》，以強勢的法規介入市場，展現極高的立法效率；然而，其法制仍難以完全擺脫「國家監控」與「個體權利」之間深層矛盾。相對而言，台灣的立法精神建立在自由民主與人權保障基礎上，但在面對新興科技時，立法節奏明顯「滯後」。台灣長期依賴《個資法》的既有框架與教育部的「軟性行政指導」，雖給予科技創新較大彈性，卻也讓校園成為缺乏法律明確禁制的真空地帶。

其次，在保護客體細緻度上，兩岸對「未成年人數位隱私」法制設計存在顯著落差。中國大陸的 PIPL 第28條明確將「不滿14周歲未成年人的個人信息」列為「敏感個人信息」，賦予最高級別保護，並要求取得監護人的單獨同意³⁷。反觀台灣，現行《個資法》並未針對未成年人或學生設定獨立的年齡分級保護標準。雖然台灣《民法》對限制行為能力人設有保護，但將民法財產與身分行為邏輯，直接套用於 AI 時代動態且無感的資料授

³⁶ 《行政程序法》第 165 條規定：「本法所稱行政指導，謂行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為。」

³⁷ 中華人民共和國全國人民代表大會常務委員會，《中華人民共和國個人信息保護法》（2021 年 8 月 20 日第十三屆全國人民代表大會常務委員會第三十次會議通過），中國國家互聯網信息辦公室，https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm（最後瀏覽日：2026 年 7 月 10 日）。

權³⁸，顯得捉襟見肘，致學生在校園中面臨極高隱私剝削風險。

最後，在執法機制上，中國大陸由國家網信辦主導，依據相關法規具備強大的行政處罰權限，甚至掌握責令停業與下架違規 app 的實質生殺大權。台灣過去在《個資法》下採「各目的事業主管機關（如教育部）」分業管轄，導致缺乏具備科技審查專業與獨立調查權的機構。所幸，隨著台灣推動設立獨立的「個人資料保護委員會籌備處（PDPC）」³⁹，未來在面對跨越教育與科技領域的 AI 業者時，應思考是否應由 PDPC 針對「校園情境」發布具強制力的裁罰基準，以解決過去由各目的事業主管機關分業管轄所導致的「多頭馬車、專業不足」困境，方能具備實質穿透並落實執法監管量能。

綜上所述，為具體呈現三地在立法精神、保護客體、授權機制與執法量能上的差異，將其核心指標彙整如下所示，凸顯台灣法制現代化之迫切性：

歐盟、中國大陸與台灣校園 AI 隱私法制比較表⁴⁰

比較維度	歐盟 (EU)	中國大陸 (PRC)	台灣 (ROC/Taiwan)
核心法規與監管模式	《一般資料保護規則》(GDPR)、《歐盟人工智慧法案》(EU AI Act)。採「風險分級」與嚴格人權防線。	《個人信息保護法》(PIPL)、《生成式人工智能服務管理暫行辦法》。法規強勢介入，立法效率高。	舊有《個人資料保護法》與教育部軟性行政指導。法規滯後，缺乏強制禁制力。
未成年人保護層級	延伸聯合國「兒童最佳利益原則」，全面禁止教育機構使用 AI 推斷情緒（不可接受風險），對生物特徵採高強度限制。	最高級別保護。將不滿 14 周歲未成年人個資明定為「敏感個人信息」，須符合特定目的與充分必要性。	缺乏獨立分級。未針對未成年人設定數位隱私專門標準，僅依賴傳統《民法》對限制行為能力人的財產與身分邏輯。
同意機制有效性	實質無效。官方指引明示師生間具明顯權力不對等，學生「同意」缺乏真實自由意志，無法合法化所有 AI 資料蒐集。	須取得監護人「單獨同意」。但實務上常面臨以「維護公共安全」（如校園監控）為由擴張例外適用。	形同虛設。在「被迫自願」的校園結構下，家長或學生告知後同意無法滿足自由意志，致防線崩解。

³⁸ 台灣現行《民法》第 77 條與第 79 條對於限制行為能力人之意思表示，主要立基於「財產行為」與「身分行為」之規範邏輯（如純獲法律上利益或日常生活所必需）。然而，面對數位環境下牽涉人格權與資訊自主權之「個人資料處理同意」，其授權客體具有高度動態性與難以預測的演算法風險，傳統民法法定代理人同意機制往往難以涵蓋數位隱私剝削之全貌。

³⁹ 行政院於 2023 年底成立「個人資料保護委員會籌備處」，並推動相關組織法與《個人資料保護法》之修法，旨在打破過去各目的事業主管機關「多頭馬車、專業不足」的執法困境，建立具備獨立調查權與裁罰權之國家級個資監管機關。

⁴⁰ 作者自行繪製。

最高監管機構與執法機制	歐洲資料保護委員會 (EDPB) 及各國資料保護局 (如瑞典 IMY、法國 CNIL)，具備實際裁罰案例與高額罰款權力。	國家互聯網信息辦公室 (網信辦) 等機關主導，具備強大行政處罰、責令停業與下架違規服務之權限。	過去採各目的事業主管機關 (如教育部) 分業管轄，現正籌設獨立的「個人資料保護委員會 (PDPC)」以統籌監管量能
-------------	--	---	---

陸、 小結

當數位浪潮席捲教育場域，AI 的大規模應用凸顯校園隱私治理的迫切性。綜觀全球，國際及歐盟標準已明確劃定人權底線：聯合國強調「兒童最佳利益」，歐盟 GDPR 嚴格限縮師生不對等下的同意機制，《歐盟人工智慧法案》更以「風險分級」全面禁止教育機構的情緒辨識，確立保障學生尊嚴凌駕於技術創新的普世共識。

兩岸法制軌跡則截然不同。中國大陸經歷科技野蠻生長的隱私反噬後，迅速祭出《個人信息保護法》等法規收攏監管，但在國家監控與學校管理效率的雙重需求下，實務運作仍充滿張力；而台灣現行法制則陷入「法規滯後、規則乏力」的困境——舊有《個資法》難以應對 AI 的無感資料蒐集，師生權力不對等的「告知後同意」淪為形式，教育部缺乏強制力的軟性指引，更讓學生的數位隱私暴露於高度風險中。

為構築契合國際趨勢的人權防線，台灣應揚棄單純依賴軟性指引的模式，以《人工智慧基本法》為授權母法制定具強制力與罰則的校園 AI 應用專法，且導入風險分級，明令禁止非公安目的之情緒辨識與無差別生物特徵採集，並對影響升學評量的 AI 強制人為監督與演算法透明度；同時，須跳脫僅憑形式上家長同意之盲點，以教育法定義務之必要性為前提，賦予學生免受歧視之「拒絕權」與畢業後之「被遺忘權」落實資訊自決；在源頭監管上，應嚴格要求業者落實隱私設計、禁止校園數據二次利用，並強制學校在採購前完成演算法與隱私影響評估。劃定上述治理紅線並非阻擋科技，而是在演算法之冰冷邏輯與教育人文溫度間築起防火牆，確保創新不以犧牲下一代隱私與尊嚴為代價，打造出真正自由、安全且受尊重之智慧學習殿堂。

一、中文文獻與註釋參考

(一) 官方文件與法規

1. 立法院，《個人資料保護法》，全國法規資料庫，2025 年 11 月 11 日公布，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021>
2. 教育部，〈中小學人工智慧教育與應用參考指引〉，AI 人才方舟計畫，<https://pads.moe.edu.tw/download.php>
3. 中華人民共和國全國人民代表大會常務委員會，《中華人民共和國個人信息保護法》（2021 年 8 月 20 日第十三屆全國人民代表大會常務委員會第三十次會議通過），中國國家互聯網信息辦公室，https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm。
4. 中華人民共和國國務院，〈未成年人網絡保護條例〉，中國政府網，2023 年 10 月 24 日公布，2024 年 1 月 1 日施行，http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/content/202310/content_6911288.htm
5. 中國國家互聯網信息辦公室，《生成式人工智能服務管理暫行辦法》，2023 年 7 月 13 日，https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
6. 中國國家互聯網信息辦公室，〈人臉識別技術應用安全管理辦法〉，2025 年 3 月 21 日，https://www.moj.gov.cn/pub/sfbgw/lfyjzj/lflfyjzj/202308/t20230808_484167.html

(二) 網路資源與新聞報導

7. 台灣人權促進會，〈給教育部長的公開信：有關校園人臉辨識技術的使用〉，台灣人權促進會網站，<https://www.tahr.org.tw/news/2539/>。
8. 新京報，〈教室裝監控抓學生小動作？曠視科技回應：僅為技術場景概念演示〉，新浪科技，<https://www.c114.com.cn/ai/5339/a1099705.html>
9. BBC 中文網，〈中國小學「監控頭環」引發爭議：科技發展與隱私保護的博弈〉，BBC News，<https://www.bbc.com/zhongwen/trad/chinese-news-50262174>

(三) 學理說明與補充性註腳

10. 學理上稱此現象為「教育數據資本主義（Educational Data Capitalism）」，指教育科技業者透過免費或低價提供平台服務，換取海量學生行為數據，並將其轉化為訓練商業 AI 模型或精準推播之資本。關於教育平台化與資料二次利用之隱私風險，詳細探討請參見 Williamson, B., *Big Data in Education: The Digital Future of Learning, Policy and Practice*, SAGE PUBLICATIONS, 2017, pp. 85-110.
11. 中國大陸《人工智能法》之立法推進，已正式列入官方年度立法計畫。參見中華人民共和國國務院辦公廳，〈國務院 2023 年度立法工作計畫〉（國辦發〔2023〕14 號），中華人民共和國生態環境部，2023 年 6 月 7 日，https://www.mee.gov.cn/zcwj/gwywj/202306/t20230607_1033044.shtml

12. 台灣現行《民法》第 77 條與第 79 條對於限制行為能力人之意思表示，主要立基於「財產行為」與「身分行為」之規範邏輯（如純獲法律上利益或日常生活所必需）。然而，面對數位環境下牽涉人格權與資訊自主權之「個人資料處理同意」，其授權客體具有高度動態性與難以預測的演算法風險，傳統民法法定代理人同意機制往往難以涵蓋數位隱私剝削之全貌。
13. 行政院於 2023 年底成立「個人資料保護委員會籌備處」，並推動相關組織法與《個人資料保護法》之修法，旨在打破過去各目的事業主管機關「多頭馬車、專業不足」的執法困境，建立具備獨立調查權與裁罰權之國家級個資監管機關。
14. 歐洲資料保護委員會（European Data Protection Board, EDPB）發布之指引指出，在公權力機關或雇主與員工（法理上可類推適用於學校與學生）之間存在明顯的權力不平衡（Imbalance of power），當事人難以在不受不利益威脅下拒絕同意，故其「同意」通常不被視為符合 GDPR 下「自由給予（Freely given）」之合法要件。參見 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, para. 16-24.
15. 瑞典資料保護局（現為 IMY，原為 Datatinspektionen）於 2019 年 8 月針對 Skellefteå 學校委員會開出瑞典首張 GDPR 罰單。參見 Swedish Authority for Privacy Protection (IMY), *Facial recognition in school renders Sweden's first GDPR fine*, August 21, 2019.
16. 法國案例參見法國國家資訊自由委員會（CNIL）對蔚藍海岸大區（Région PACA）高中建置人臉辨識系統之警告，以及馬賽行政法院（Administrative Court of Marseille）於 2020 年 2 月之判決。參見 CNIL, *Facial recognition in high schools: the CNIL underlines that the planned systems are contrary to the GDPR*, October 29, 2019.
17. EU AI Act, Art. 5(1)(f). 該條文禁止將 AI 系統用於工作場所與教育機構推斷自然人之情緒（the placing on the market, putting into service for this specific purpose, or use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions），除非基於醫療或安全理由。
18. 《個人資料保護法》第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」
19. 《行政程序法》第 165 條規定：「本法所稱行政指導，謂行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為。」
20. 《中華人民共和國個人信息保護法》第 28 條規定：「敏感個人信息是一旦洩露或者非法使用，容易導致自然人的的人格尊嚴受到侵害或者人身、財產安全受到危害的個人信息，包括生物識別、宗教信仰、特定身份、醫療健康、金融賬戶、行蹤軌跡等信息，以及不滿十四周歲未成年人的個人信息。」

21. 《中華人民共和國個人信息保護法》第 26 條規定：「在公共場所安裝圖像採集、個人身份識別設備，應當為維護公共安全所必需，遵守國家有關規定，並設置顯著的提示標識。所收集的個人圖像、身份識別信息只能用於維護公共安全的目的，不得用於其他目的；取得個人單獨同意的除外。」

二、外文文獻與註釋

(一) 書籍(Books)

1. Williamson, Ben, BIG DATA IN EDUCATION: THE DIGITAL FUTURE OF LEARNING, POLICY AND PRACTICE, SAGE Publications (2017).

(二) 官方文件與指引 (Official Documents & Guidelines)

2. CNIL, Facial recognition in high schools: the CNIL underlines that the planned systems are contrary to the GDPR (2019).
3. European Data Protection Board (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679 (2020).
4. Swedish Authority for Privacy Protection (IMY), Facial recognition in school renders Sweden's first GDPR fine (2019).
5. UNESCO, Recommendation on the Ethics of Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> (last visited Jul. 13, 2026).
6. UNICEF, Policy Guidance on AI for Children, UNICEF GLOBAL INSIGHT, <https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children> (last visited Jul. 13, 2026).

(三) 法規 (Legislation)

7. 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), O.J. (L 119) 1 (2016).
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), O.J. (L 1689) (2024).