僅供委員問政所需參考
不代表本院意見或立場

編號：2558

議題研析

一、 題目：從歐盟立法例探討我國人臉辨識相關法制問題

二、 議題所涉法規

個人資料保護法

三、 背景說明

據報導[1]，近期有娛樂活動主辦單位於入口處設置人臉辨識機台，針對持該活動雙日票入場之民眾，要求使用人臉辨識掃描入場，以確保隔日仍為同一人入場，雖主辦單位表示，該入場民眾肖像資料僅儲存於現場機台主機，並於活動結束後立即銷毀，惟仍引發侵害個資之疑慮。生物特徵具有人各不同之特性，而臉部影像之擷取則因較具便利性，人臉辨識成為除指紋辨識外最常使用之生物特徵資料[2]，實務上除常見於手機解鎖、門禁管制、簽到等應用外，我國於入出境管制、警察執法、戶政業務及教育場域等皆有採取相關技術之實例[3]，然查監察院於110[4]年3月18日公告之調查報告，針對交通部鐵道局試辦之「智慧型影像監控系統」及內政部警政署之「M-police」所涉及之人臉辨識技術使用，咸認現行法規範尚有待強化[5]；而國際人權專家於我國兩公約第3次國家報告國際審查會結

[1] 詹湘淇，S2O Taiwan音樂節爆用人臉辨識恐個資外洩，113年7月23日自由時報電子報，網址：https://news.ltn.com.tw/news/life/paper/1658007，最後瀏覽日期：113年8月6日。

[2] 許慧瑩，瑞典高中因測試刷臉點名成瑞典個資保護機關開鍘首例，中研院法律所資訊法中心，網址：https://infolaw.iias.sinica.edu.tw/?p=2279，最後瀏覽日期：113年8月7日。

[3] 國家發展委員會，歐盟、英國及加拿大對警察機關或執法機關運用人臉辨識技術之指引或其他相關文獻探討」委託研究計畫結案報告，111年10月，頁1。

[4] 本報告有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[5] 監察院，110內調字第0010號調查報告，110年3月18日，頁55-56，網址：https://www.cy.gov.tw/CyBsBoxContent2.aspx?n=718&s=17440，最後瀏覽日期：113年8月7日。

論性意見第 85 點指出:「審查委員會建議政府提高使用臉部辨識技術的透明度，包括其法律依據、目的及儲存方法。應訂定及落實防止機關及第三方濫用的保障措施。」[6]。觀察歐盟於 2016 年 5 月公布之一般資料保護規則（General Data Protection Regulation, GDPR），已將生物辨識資料（biometric data）列為特種個人資料，原則禁止處理[7]，爰擬從歐盟立法例探討我國人臉辨識相關法制規範問題。

四、 探討研析

（一）人臉辨識與指紋辨識具相同特性，應依司法院釋字第 603 號解釋標準予以相同程度保護

我國個人資料保護法（下稱個資法）第 2 條第 1 款規定略以：「本法用詞，定義如下：一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、.....及其他得以直接或間接方式識別該個人之資料。」，同法第 6 條第 1 項本文規定略以：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。.....」，爰「特徵」非屬我國個資法上原則「不得」蒐集、處理或利用之特種個人資料而為一般個人資料。惟依司法院釋字第 603 號解釋理由書略以：「指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。.....國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控個人之敏感性資訊。.....」，該號解釋標的雖為「指紋」，惟人臉辨識亦同樣具有人各不同、終身不變之特性，應與指紋辨識為相同程

[6] 對中華民國（臺灣）政府關於落實國際人權公約第三次報告之審查國際審查委員會通過的結論性意見與建議，111 年 5 月 13 日，頁 13。人權大步走，網址：https://www.humanrights.moj.gov.tw/17725/17733/17735/17740/37227/37228/37234/post，最後瀏覽日期：113 年 8 月 7 日。

[7] GDPR Article 9, paragraph 1.

度之保護，以避免個人隱私權之侵害[8]。

（二）歐盟涉及人臉辨識相關法規主要包括一般資料保護規則、執法領域使用人臉辨識技術指引及人工智慧法

1、歐盟一般資料保護規則於 2018 年 5 月正式施行，依該規則第 4 條第 14 款規定：「生物辨識資料（biometric data）係指透過特定技術處理自然人之有關之身體、生理或行為特徵，而得以或確認該自然人之獨有識別性之個人資料，如臉部圖像或指紋資料。」[9]，同規則第 9 條第 1 項規定：「禁止處理有關揭露種族或血統、政治觀點、宗教或哲學信仰或工會身分之個人資料，及基因資料、為識別特定自然人之生物識別資料、健康資料或自然人性生活或性傾向有關之個人資料。」[10]，依上開規定，歐盟已明確將臉部圖像及指紋列為生物識別資料，且該資料屬特種個人資料，原則禁止處理。

2、歐盟個人資料保護委員會（European Data Protection Board, EDPB）2022 年 5 月提出執法領域使用人臉辨識技術指引（公眾諮詢版）（Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement（version for public consultation））[11]，並於 2023 年 4 月正式公布。該指引主要係從歐盟執法指令（Law Enforcement Directive, LED）角度說明執法機關使用人臉辨識技術時應遵循之事項與實務操作程序，依

[8] 王德瀛，【極憲解析】「刷臉」行不行？淺談臉部辨識的隱私議題，107 年 11 月 21 日，網址：http://www.conlawfocus.com/face_recognition_and_privacy/，最後瀏覽日期：113 年 8 月 8 日。

[9] 該款原文：”‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.”

[10] 該項原文：”Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.”

[11] 國家發展委員會，同註 3，頁 3。

該指引說明，人臉辨識技術主要分為 2 種模式[12]：

（1）驗證（authentication）：又稱 1 對 1 比對，主要目的係確認某自然人是否其所聲稱之人。辨識系統會將預先記錄的生物辨識範本或樣本與自然人（例如出現在檢查站的人）進行比較，以驗證是否為同一人[13]。例如：門禁管制、簽到退或點名等運用情境皆屬之。

（2）識別（identification）：又稱 1 對 N 比對，主要目的係在特定區域、圖像或資料庫中尋找特定人。因此辨識系統須處理捕獲之所有人臉，產生生物識別模板，並確認是否與系統已知的人相符[14]。例如：於公共場所識別通緝犯[15]。

該指引重申驗證與識別皆係處理生物特徵資料，亦即屬特種個人資料之處理[16]，其各項應用之方式及條件須以專法規定[17]，並強調為避免比對錯誤（wrongly matched）造成對基本權利之侵害，人臉辨識須仰賴高品質資料及演算法，因此資料控管者（data controller）應定期、系統性的評估演算法，以確保準確性、公平性及辨識結果的可靠性[18]；此外，為避免因技術問題造成偏見與歧視，該指引明確建議執法部門「確保對結果之人為介入和監督」，又考量人臉辨識具有侵害基本權利之高度風險，因此於使用前應進行個資保護影響評估（Data Protection Impact Assessment, DPIA），並公開評估結果，以提升透明度及人民之信賴[19]。

3、歐盟於 2024 年 3 月公布人工智慧法（Artificial Intelligence Act,

[12] 國家發展委員會，同註 3，頁 4。
[13] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement version 2.0. Adopted on 26 April 2023. P.9.
[14] EDPB, *Supra* note, P.9-10.
[15] 國家發展委員會，同註 3，頁 5。
[16] EDPB, *Supra* note 13, P.10.
[17] 國家發展委員會，同註 3，頁 7。
[18] EDPB, Supra note 13, P.13.
[19] 國家發展委員會，同註 3，頁 62、64。

AIA），該法第 3 條第 34 款至第 36 款明確定義生物辨識資料、生物辨識識別及生物辨識驗證[20]，同法第 5 條並明文規定，禁止為投入市場之目的，透過網路或監視錄影系統隨機抓取臉部影像以建立或發展人臉辨識資料庫，此外，除非為尋找綁架、人口販運或性剝削被害人或加害人、防止對生命身體立即、嚴重威脅或可預見的恐怖攻擊、為調查、起訴最輕本刑 4 年以上之刑事犯罪嫌疑人或執行該懲罰外，禁止為執法目的在公共場所使用「即時」（real-time）遠端生物識別系統（下稱即時識別系統）。即便為上開目的使用即時識別系統，亦應以法律明文規定或授權、符合適當性及比例原則，且該系統使用應遵循暫時性（temporal）、地域性（geographic）及個別性（personal）之限制，執法機關於使用該系統前並應依第 27 條規定進行基本權影響評估，並依第 49 條規定進行登錄[21]。

（三）研析與建議

我國關於人臉辨識並無一致適用之專法，而係由個別法規規定，如：入出國及移民法第 68 條、第 91 條、刑事訴訟法第 153 條之 1；亦有以授權辦法為相關規定者，如：監獄及看守所科技設備設置與使用及管理辦法等，餘多以管理要點或作業要點為相關規定（如：M-police 之使用係以內政部警政署使用國民身分證相片影像資料管理要點為相關規定）；又依現行個資法規定，人臉辨識資料僅為一般個人資料，有論者認，倘需大規模蒐集、運用人臉辨識資料應與指紋同樣採取司法院釋字第 603 號解釋之標準[22]，應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並

[20] AIA 第 3 條第 36 款規定原文：“'biometric verification' means the automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data;”有關「biometric verification」一詞，雖與「Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement」針對人臉辨識「驗證」類型係採用「authentication」不同，惟依其定義，實則亦係指一對一進行比對之驗證類型，因此此處採取同樣之中譯。

[21] AIA 第 5 條第 1 項(g)款、(h)款及第 2 項。

[22] 王德瀛，同註 8。

應明文禁止法定目的外之使用。考量數位科技快速發展，人臉辨識技術倘遭濫用而無法律明確規範之，將對人民隱私權造成嚴重侵害，主管機關宜參考歐盟立法例，研議將生物特徵資料列為特種個人資料，並明定使用指引及限制、使用前應辦理個資保護影響評估及規範監督管理機制，以落實保障人民基本權益。

撰稿人：陳育靖