「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

委託機關：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 111 年 10 月

「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

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

計畫期程：中華民國 111 年 7 月至 111 年 10 月

國家發展委員會 委託研究

中華民國 111 年 10 月

摘要

人臉辨識技術是近年來廣受矚目之新興技術之一，也因其對民眾資訊隱私及其他基本權利之複雜影響而引發諸多爭議。因應人臉辨識技術對民眾權益之衝擊，個人資料保護法制扮演著重要角色。對此，國際間除檢討個人資料保護法相關規定外，並由主管機關提出針對性指引，提示執行面之最佳實務做法與建議，為相關單位提供法規適用與遵循之參考。

我國人臉辨識技術在海關出入境、執法、戶政、教育等場域之運用實例逐漸增多。鑑於人臉辨識技術對民眾權益之影響，本研究受國家發展委員會委託，將國際間同類指引作比較分析，並提出公務機關使用人臉辨識技術時，落實個人資料保護之重點考量要素及最佳實務作法。

Abstract

Facial recognition is an emerging technology that has attacked much attention and interest in recent years. In the meantime, the technology has also given rise to a great deal of controversies due to the complicated effects on privacy and other fundamental rights. Personal data protection law plays an essential role in mitigating the impacts brought about by facial recognition on people's rights and interests. In this regard, countries have, in addition to efforts on the review and revision of their legislation, produced specific regulatory guidelines that contain operational-level best practices and recommendations, for the reference of relevant actors in their application of and compliance with the law.

Applications of facial recognition technology are on the increase in areas such as border control, law enforcement, household registration and education. In light of the impacts of facial recognition technology on people's rights and interests, and upon commission by the National Development Council, this research conducts a comparative study on similar guidelines from other countries, and produces recommendations on the key considerations and best practices for government agencies in ensuring personal data protection during their use of facial recognition technology.

目錄

表目錄

第一章　研究目的

人臉辨識(facial recognition)是近年來廣受矚目之新興技術之一。在國際層面，諸多執法機關採購並使用商業性人臉辨識技術，引發侵害隱私之廣泛憂慮[1]，並由此催生出禁用特定人臉辨識技術之立法提案[2]。在我國國內，人臉辨識技術之使用也逐漸增多，在海關出入境、執法、戶政、教育等場域皆有其事例。

人臉辨識之所以引發爭議，對民眾權益之複雜影響是原因之一。人臉辨識是一種人工智慧（Artificial Intelligence）技術，蒐集具有高度個人特徵性質的人臉影像畫面，以演算法加以運算後，可能推知當事人之身分，顯著衝擊社會通念上的隱私期待。若大規模蒐集和比對人臉影像畫面，則可實現演算法對當事人行為與人格特徵之剖析，甚至可能造成對當事人之歧視。更進一步，人臉辨識技術可能用於識別抗議遊行等活動之參加者身分，從而導致民眾不敢發聲之寒蟬效應，妨礙民主社會中自由權利之行使。

因應人臉辨識技術對民眾權益之衝擊，個人資料保護法制扮演著重要角色。對此，國際間除檢討該國之個人資料保護法相關規定外，並由主管機關提出針對性指引，說明最佳實務做法與建議，從執行面為相關單位提供法規適用與遵循參考。我國人臉辨識技術在海關出入境、執法、戶政、教育等場域之運用實例逐漸增多。鑑於人臉辨識技

[1] 例如，人臉辨識服務供應商 Clearview AI 因其服務違反個資法規，曾遭多國主管機關裁罰，例如 Information Commissioner's Office, Monetary Penalty Notice, https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf (accessed 30 September 2022); Office of the Privacy Commissioner, Clearview AI ordered to comply with recommendations to stop collecting, sharing images, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/ (accessed 30 September 2022).

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (21.4.2021) (hereinafter the "AI Act Proposal"), COM(2021) 206 final.

術對民眾權益之影響，本研究受國家發展委員會委託，將國際間同類指引作比較分析，並提出公務機關使用人臉辨識技術時，評估個人資料保護作為之重點考量要素及最佳實務作法。

第二章　研究方法

本研究將以文獻分析法為原則，就特定國家主管機關於運用人臉辨識技術提出之指引作重點摘要，比較該等指引關於個資保護重點議題之內容差異，並就我國公務機關使用人臉辨識技術時，評估個人資料保護措施可借鏡之處提出建議。此外，本研究亦將以法規比較法，整理研究特定國家個人資料或隱私保護法規與我國個人資料保護法（以下稱個資法）等法規之差異，以此作為本研究所提建議之參考。

本研究所比較之文獻如下：

（一）歐盟個人資料保護委員會（European Data Protection Board, EDPB）2022 年 5 月 12 日通過之《執法領域人臉辨識技術運用指引 05/2022（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)）[3]，以下稱歐盟 EDPB 指引。

（二）英國警務學院（College of Policing）2022 年 3 月 21 日發布之《即時人臉識別警務專業指引》（Live facial recognition- Authorised Professional Practice (APP)）[4]，以下稱英國警務學院指引。

（三）加拿大隱私監察人辦公室（Office of the Privacy Commissioner, OPC）聯合加拿大各省隱私監察部門，於 2022 年 5 月 2 日發布之《警用人臉辨識技術隱私指引》（Privacy Guidance on Facial Recognition for Police Agencies）[5]，以下稱加拿大 OPC 指引。

---

[3] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en (accessed 30 September 2022).

[4] College of Policing, Live facial recognition- Authorised Professional Practice, https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition (accessed 30 September 2022).

[5] OPC, Privacy Guidance on Facial Recognition for Police Agencies, https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/ (accessed 30 September 2022).

第三章　外國指引研析

第一節 歐盟 EDPB 執法領域人臉辨識技術運用指引

一、指引內容要點

EDPB 認為，由於人臉辨識技術的效率和可擴展性（scalability）係其受到關注的重要原因，然而，在技術獲得大規模應用的同時，技術固有的負面影響亦隨之大範圍發生。執法機關對人臉辨識技術的應用，可能對個人和群體造成重大影響，包括影響民眾之生活方式、以及社會民主穩定。人臉辨識技術的應用可能對多種基本權造成干預，其中，資料保護權利乃保障其他基本權的前提要件。EDPB 據此提出本指引，以期從歐盟執法指令（Law Enforcement Directive, LED）等法規範之角度，為歐盟及會員國立法機關、以及使用人臉辨識技術的執法機關提供參考資訊及實務指引。本指引正文分析人臉辨識之技術面向和法律適用框架，另包含三項附件：附件 1 為人臉辨識技術之情境描述模板，以協助評估人臉辨識技術對基本權影響之面向與程度；附件 2 為人臉辨識技術專案管理實務指引，供執法機關在採購和應用人臉辨識系統過程之參考；附件 3 為對特定實務案例之分析。以下將分述其重點。

（一）技術面向

人臉辨識技術為生物特徵（biometric）辨識技術之一類，係一種機率性(probabilistic)技術，能夠透過人臉圖像自動辨識某一自然人。其作用原理分為兩個步驟：其一為將照片或影片中之人臉畫面(即「樣本」）轉化為數位化之人臉特徵數值（即「模板（template）」），其二為將該模板與一個或多個其他模板相比對，以辨識該模板所代表的人臉。

人臉辨識技術能夠提供驗證(authentication)與識別(identification)兩種不同功能：

1. 驗證又稱一對一（1:1）比對，即透過將某一自然人之人臉與預先儲存模板或樣本進行比對，確認該自然人是否為其所宣稱之身分。人臉識別驗證可用於查驗線上公共服務使用者的身分，亦可用於特定實體場域之進入管控（例如邊境查驗）。
2. 識別又稱一對多（1:N）比對，即透過將某一自然人之人臉模板與儲存於資料庫中的多個模板或樣本進行比對，以從某一群體、某一區域、某一資料庫中，識別出特定個人。人臉辨識識別的應用情境更為廣泛，例如透過檢索照片資料庫，確定某人（例如受害人或嫌疑人）身分，監測某人在公共場所之行動軌跡及所接觸人員，在公共場所中辨識受通緝人員等。

無論是驗證或識別功能，人臉辨識技術都是機率性的，即透過對人臉模板之比對，推算所辨識的個人確係驗證或識別目標的機率。若該機率超過系統使用者或開發者設定之門檻，則系統將認定構成匹配。

人臉辨識技術涉及生物辨識資料屬特種個資，因此構成特種個資運用[6]活動。但並非任何涉及人臉之影像畫面處理技術皆屬人臉辨識。例如，數位相機單純「偵測」人臉之功能，若非以獨特性識別特定個人為目的，且不涉及運用特種個資，則不屬人臉辨識技術。另一方面，人臉辨識係一軟體功能，因而可與既有系統（例如攝影機或影像資料庫）整合。因人臉辨識技術零摩擦（frictionless）[7]、易隱藏之特性，這種整合存在固有風險。

---

[6] 我國個資法將個資之使用分為蒐集 (collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而 GDPR 對個資之蒐集、處理、利用任一行為，皆統稱為 processing。 為與我國個資法中之「處理」有所區隔，本報告因此將 GDPR 中的 processing 譯為「運用」，processor 譯為「受託運用者」。

[7] 在資訊科技領域，零摩擦（frictionless）並無明確定義，但通常是指軟體、系統等之設計、部署協調、配合、符合使用者直覺，從而降低數位應用與使用者所處物理環境的「摩擦」，令使用體驗更加流暢、便利。See, Vivek Agarwal, The Frictionless Enterprise (26 December 2018), Forbes, https://www.forbes.com/sites/forbestechcouncil/2018/12/26/the-frictionless-enterprise/?sh=51386d183ba0 (accessed 25 October 2022); 李宗翰, 不只是要零接觸，更要做到零摩擦（2021.07.02），iTHome, https://www.ithome.com.tw/voice/145419（最後瀏覽日：2022 年 10 月 25 日）。

人臉辨識技術有廣泛應用可能性，其對個資當事人之風險，可從以下幾個方面評估：個資當事人對其個人資料享有之管控程度，個資當事人施以管控的有效方式及啟用辨識技術之權利，辨識結果對個資當事人之影響，以及辨識所涉個資運用之規模。

人臉辨識技術的施用可能面臨可靠性和效力、資料品質、準確性和來源等方面的挑戰。這些挑戰可能對個資當事人造成風險。尤其，人臉辨識系統可能被偽造的面部圖像欺騙（spoofing），且人臉辨識技術系統演算法計算匹配之概率（信心值 (confidence score)），而演算法自身可能因原始資料品質、訓練資料庫等而帶有偏見。EDPB 強調，人為介入本身未必能夠為個人權利提供充分保障，重點是人為介入須批判性檢視人臉辨識結果。除強調高品質的資料外，資料控管者須對演算法處理活動定期進行系統性評估，以確保個人資料運用結果之準確性、公平性和可靠性。

（二）一般法律框架

人臉辨識技術運用之一般法律框架包括歐盟基本權利憲章（EU Charter of Fundamental Rights，以下稱憲章)和歐洲人權公約(European Convention on Human Rights, ECHR）。人臉辨識技術與個人資料（包括特種個資）運用間存在固有關聯，且能夠直接或間接影響歐盟基本權利憲章（EU Charter of Fundamental Rights）所載的多種權利。

1. 憲章之適用

歐盟機構和歐盟會員國執行歐盟法時，皆應遵循憲章。為刑事執法目的而運用生物特徵資料，無可避免地涉及基本權利保護問題，特別是對憲章第 7 條規定之私人生活及通訊受尊重之權利、第 8 條規定之個人資料受保護權利之干預。這是因為，自然人錄影畫面之蒐集和分析（包括其臉部畫面），意味著個人資料之運用；而以人臉辨識技術處理該資料時，基於人臉畫面以及錄影的時間和地點，可推知相關自然人私人生活之資訊，例如種族和民族、健康狀況、宗教信仰、日常習慣、永久或暫時住址、社會關係等。

2. 對憲章所載基本權利之干預

在一切情形下，生物特徵資料之運用本身即構成對基本權利之嚴重干預。辨識結果是否為「匹配」，與其對基本權的干預程度無關。即使在辨識結果為「非匹配」後，生物辨識模板隨即刪除，辨識所涉之資料運用仍構成對基本權之干預。

人臉辨識技術所能揭露之資訊範圍相當廣泛，不僅可能干預憲章第 8 條之資料保護權利，也可能影響憲章第 7 條之隱私權。此外，人臉辨識技術之運用可能引發寒蟬效應，從而干預憲章所保護之思想、良心與宗教自由、表意與資訊自由、集會與結社自由等基本權利。人臉辨識技術將高度個人化之面部特徵用於計算轉化為機器可讀之資訊並計算其匹配概率，有物化人臉之風險，從而可能干預憲章第 1 條所保護之人性尊嚴。

人臉辨識技術運用之背景事實不同，對基本權利所造成之風險也有相應差異。然而，因人臉辨識技術所涉之個人資料（例如人臉或虹膜）具有獨特且不可變更之特性，人臉辨識技術之運用具固有風險。例如，若生物辨識資料遭意外洩漏，可能影響以該等資料作為密碼或密鑰之安全性，該等資料亦可能被用於對個資當事人未經授權之監控。

3. 干預之正當性基礎

依據憲章第 52(1)條，對基本權利與自由之限制須以法律為之，且尊重該等權利與自由之本旨。該等限制亦須符合比例原則。

於刑事執法過程中，為獨特性識別個人而運用之生物特種資料，屬執法指令第 10 條所稱之特種個資。因此，大多數情形下，人臉辨識技術之各項應用，將須以專門性法律規定應用之方式及條件。

該法律並須尊重其所限制的基本權利與自由之本旨。就限制憲章第 8 條資料保護權利之法律而言，如有下列情事，可能違反基本權利與自由之本旨：

- 廣泛蒐集通訊之詮釋資料（meta-data），且獲知電子通訊之內容；

- 要求線上公共通訊存取服務提供者和資訊儲存（hosting）服務提供者完整留存服務提供所涉資訊，包括個人資料。
- 缺乏資料保護和資料安全之基本原則。

該法律須通過比例原則之檢驗，包括具備正當目的、手段必要，且手段與目的相當。依據歐盟法院之實務見解，對資料保護權利之克減（derogation）或限制應限於絕對必要範圍內。限制基本權利與自由之法律應依其目的（例如打擊嚴重犯罪），就不同適用對象作出不同規範。該法律之規定亦應與特定情境相符，例如所運用之資料數量、資料之性質、資料被非法存取之風險等。該法律不得允許資料之受託運用者僅考量經濟性因素。此外，該法律並應確立公務機關存取及利用資料之實體及程序性條件與客觀標準。就刑事執法而言，所涉犯罪之嚴重性須足以作為對基本權利之干預提供正當性理由。

資料之運用須確保歐盟資料保護規則之適用，特別是憲章第 8 條關於獨立監管機關之要求。在資料運用之各個步驟，應就所涉資料對所追求目的之效用、或所涉個資當事人之身分，對各類資料區分不同運用條件，且該條件（例如保存期限）須基於客觀標準，以確保干預限於絕對必要範圍。

評估必要性與合比例性時，須識別並考量對一切基本權利之影響，包括人格尊嚴、思想、良心與宗教自由、表意自由、集會與結社自由等。此外，還應慎重考量，若在個資當事人不知情之情況下系統性處理個人資料，可能構成持續監控。為協助評估立法措施之必要性與合比例性，立法者宜使用歐洲個人資料保護監察人（EDPS）提供之必要性與合比例性工具組[8]。

[8] European Data Protection Supervisor: Assessing the necessity of measures that limit the fundament al right to the protection of personal data: A toolkit (11.4.2017)，https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf (accessed 30 September 2022); European Data Protection Supervisor: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019): https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf (accessed 30 September 2022).

依憲章第 52(3)條和第 53 條，憲章所保障權利之範圍與解釋，應與歐洲人權公約（ECHR）中對應權利相同。憲章第 7 條「私人生活受尊重之權利」與 ECHR 第 8 條「私人和家庭生活、住家和通訊受尊重之權利」相對應，而憲章第 8 條「個人資料受保護之權利」於 ECHR 中並無對應權利。但憲章第 52(3)條並未限制歐盟法對基本權利提供更廣泛的保護。

依 ECHR 第 8 條，對該權利之干預，僅得以法律為之，且應出於民主社會中維護國家安全、公共安全或國家的經濟福祉，防範動亂或犯罪，保護健康或道德，或保護他人權利與自由之必須。此外，ECHR 亦確立權利限制措施之要件，其中，除法治要求外，「可預見性」亦屬基本要求。為滿足明確性要求，限制基本權利之法律，其內容應足夠明確，以使民眾能夠清楚認知公務機關得援用該法律之條件。

此外，就 ECHR 第 8 條之權利而言，亦應充分尊重自動化處理個人資料保護公約（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）。且該公約應被認為僅屬當前歐盟法對權利保護之最低要求。

（三）具體法律框架

執法領域人臉辨識技術運用之具體法律框架為執法指令（LED 指令）。首先，LED 指令第 3(13)條對「生物辨識資料」作了定義。其次，該指令第 8(2)條明文要求，該指令適用範圍內之個資運用活動須以法律規範，且該法律至少應明確規定適用對象（objectives）、所涉個人資料之範圍，以及處理之目的。此外，LED 指令第 10 條（應與第 8 條共同適用）和第 11 條規定亦與生物辨識資料相關。人臉辨識技術所涉之生物辨識資料運用應始終遵守該指令第 4 條規定之資料運用原則。

1. 為執法目的運用個人資料

依 LED 指令第 10 條，為執法目的運用生物辨識資料等特種個資，僅得於絕對必要範圍內為之，且須為個資當事人權利與資料採取適當安全維護措施。此外，特種個資之運用，須符合下列要件之一：

- 依歐盟法或會員國法授權為之；
- 為保護個資當事人或其他自然人之重大利益而為之；或
- 該運用係涉及個資當事人顯已公開之個人資料。

此一條款表明運用特種個人資料之敏感性。

(1)依歐盟法或會員國法授權為之

關於立法措施之類別，LED 指令前言第 33 點敘明，該指令所稱之法律，依會員國之國內憲法秩序為之，不以議會制定之法律為必要。

該指令前言第 33 點並指出，「然而，該法律依據或立法措施應明確具體，且其適用應可為受規範者所預見」；且規範該指令適用範圍內個資運用活動之會員國法規，應至少明確規定適用對象、所涉個人資料之範圍，以及處理之目的，以充分防範濫用和任意獨斷之風險。

依 LED 指令規範和歐盟法院（CJEU）、歐洲人權法院（ECtHR）之見解，人臉辨識措施之法律依據對個資當事人之可預見性至關重要。

若一項立法措施僅將 LED 指令第 10 條之文句內容轉化為國內法，則其將缺乏足夠具體性與明確性，從而不足以作為以人臉辨識技術運用生物辨識資料之授權法律。

(2)絕對必要

「絕對必要」之文句，表明運用特種個資之條件，應比「必要」更為嚴格。其應解釋為達到不可或缺（indispensable）之程度，且其將執法機關之裁量邊際（margin of appreciation）限於最小範圍。

(3)顯已公開

顯已公開之照片通常並不構成生物特徵資料。因此，個資當事人公開照片，並不意味著能從照片中提取之生物特徵資料亦屬「顯已公開」。

生物特徵資料之顯已公開，須由個資當事人故意公開生物特徵模板（而非僅臉部照片），供民眾由公開管道自由存取。若生物特徵資料係由第三方公開，則不構成已由個資當事人顯已公開。

此外，不得藉由解釋當事人之行為，認為生物特徵資料已屬顯已公開。例如，社群網路平台上，個資當事人未進行某項隱私設定，並不構成將生物特徵資料公開。服務之默認設定（例如公開生物特徵模板）或缺乏選擇（例如當事人無法選擇不公開其生物特徵模板），皆不得被解釋所涉生物特徵資料構成顯已公開。

2. 自動化個人決策，包括剖析

LED 指令第 11(1)條規定，會員國應原則禁止僅依據自動化運用（包括剖析），進行對個資當事人有不利法律效果或重大影響之決策。作為此一禁止之例外，僅得於符合下列條件時進行此等運用：

- 經適用於控管者之歐盟法或會員國法授權；且
- 該歐盟法或會員國法規定對當事人權利與自由之適當安全維護措施，且至少包括控管者方面的人為介入。

前述標準係針對一般個人資料而設。針對特種個人資料，LED 指令第 11(2)條確立了更嚴格之標準，要求同條第 1 項之決策不得基於特種個人資料為之。此項禁止僅有一項例外，亦即已就個資當事人之權利和自由以及正當利益採取適當安全維護措施。

依 LED 指令第 11(3)條，基於特種個人資料而造成對個人歧視之剖析應依歐盟法規範加以禁止。依 LED 指令第 4(3)條，「剖析」係指對利用個人資料評估自然人個人特徵之任何形式的個人資料自動化處理，特別是用來分析或預測該自然人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或移動等特徵。判斷是否

已採取措施維護個資當事人權利和自由以及正當利益時，須考量人臉辨識技術依其使用方式和目的，可能導致剖析。而依 LED 指令第 11(3)條，禁止基於特種個人資料而導致歧視之剖析。

3. 個資當事人之類別

依 LED 指令第 6 條，不同類別之個資當事人應盡可能區別對待。個人資料之運用方式須呈現此等區別對待。依第 6 條所舉例示可知，對於不同類別之個資當事人，運用其個人資料亦須符合必要性和比例原則之要求。從該條規範亦可進一步推知，若無證據表明個資當事人之行為與 LED 指令規範之正當目的有關（即使是間接或微弱關聯），則很可能並無干預其權利之正當性理由。

基於前述要求，並考量偽陽性或偽陰性匹配結果之可能性，及其對個資當事人及偵查活動之重大影響，對於人臉辨識所涉個人資料運用而言，區分不同類別之個資當事人係一核心要求。

4. 個資當事人權利

LED 指令規定個資當事人享有之權利，且第 29 條個資保護工作小組（WP29）已對此提供一般性指引，並為 EDPB 所採認。以人臉辨識技術運用個人資料時，LED 指令第三章所規範之當事人權利皆有其適用。但本指引僅就其中重點事項提供指引。且本指引當事人權利一節之前提，係人臉辨識技術之個人資料運用已滿足前述章節所述之合法性要件。

考量以人臉辨識技術運用個人資料之性質（運用特種個人資料，且通常與個資當事人並無明顯互動），控管者在啟動人臉辨識技術之運用作業前，須仔細考量如何（以及是否能夠）遵循 LED 指令之要求。控管者尤應仔細分析：

- 所涉個資當事人之身分（通常涉及運用目標以外之其他人）；
- 個資當事人如何得知人臉辨識技術之個資運用；

- 個資當事人如何行使其權利（除 1 對 1 驗證外，其他形式之人臉辨識技術在資訊提供、近用權、更正權、限制運用權方面都將面臨挑戰）。

(1)向當事人告知權利和資訊

人臉辨識技術將為資訊告知帶來挑戰。特別是當執法機關使用第三方提供之影像時，幾乎沒有在蒐集資料時向當事人告知之現實可能性。

在部署生物特徵資料運用前，與偵查無關之影像內容應予以移除或匿名化（例如，將相關內容以不可逆之方式作模糊化處理），以遵循 LED 指令第 4(1)(e)條之資料最小化要求，以及指令第 13(2)條之資訊提供要求。

LED 指令 13(1)條規定向個資當事人提供資訊之最低要求。此等資訊得透過控管者網站、紙本（例如可供取閱之宣傳頁）等個資當事人易於取得之管道提供。控管者須確保所提供之資訊包含下列內容：

- 控管者之身分與聯絡方式，包括個資保護長（DPO）；
- 運用之目的，以及運用係透過人臉辨識技術執行；
- 向監管機關提前申訴之權利，以及該監管機關之聯絡方式；
- 近用權、更正權、刪除權與限制運用權。

此外，在國內法依 LED 指令第 13(2)條規定之特定情形下（例如人臉辨識運用），應向個資當事人提供下列資訊：

- 運用之法律依據；
- 個人資料於何處在個資當事人不知情時蒐集；
- 個人資料之儲存期限，或在儲存期限未知時，確定儲存期限之標準；
- 個人資料接收者之類別（包括第三國和國際組織）（如適用）。

LED 指令第 13(1)條之資訊係向全體民眾揭露，而第 13(2)條之資訊係於特定情形下，項特定個資當事人揭露，例如直接向當事人蒐集

資料時、或於當事人不知情之背景下間接蒐集。LED 指令第 13(2)條對「特定情形」並無明確定義。然而，其係指個資當事人需要知悉涉及該當事人之運用活動，且獲取相關資料，以利有效行使當事人權利。確定「特定情形」之考量要素包括資料是否在當事人不知情之背景下蒐集（此時，告知資訊乃當事人當以行使其權利之唯一方式）。

個人資料若被進階運用（例如用於國際刑事合作程序或國內法規範之秘密行動），亦屬「特定情形」之一。此外，依 LED 指令第 38 條之意旨，若利用人臉辨識技術進行純自動化決策，則應向個資當事人告知自動化決策之相關資料，故此時亦構成「特定情形」。

最後應留意，LED 指令第 13(3)條允許會員國透過立法措施，為特定目的，於特定情形下限制資訊提供義務。但其須為民主社會中為必要且合乎比例、並尊重基本權利和個資當事人正當利益之措施。

(2) 近用權

通常而言，個資當事人有權確認其個人資料是否被運用，且在資料確實被運用時，有權存取其被運用之資料，以及 LED 指令第 14 條所列資訊。

對於人臉辨識技術而言，若生物特徵資料係連結至字母/數字資料，則執法機關在回應個資當事人近用請求時，應可透過搜尋該字母/數字資料為之，而無需進階運用他人的生物特徵資料（即透過人臉辨識技術搜尋資料庫）。須遵守資料最小化要求，超出運用目的必要範圍之資料不得儲存。

(3) 更正權

由於人臉辨識技術並不提供絕對正確性，控管者須格外留意資料更正請求。個資當事人可能被歸入錯誤類別，例如依錄影畫面內容，將個資當事人誤認為嫌疑人。若不正確之資料被納入警用資料庫或分享予他機關分享，則對個資當事人可能造成重大風險。控管者須依 LED 指令前言第 47 點意旨，相應更正所儲存的資料及人臉辨識系統。

(4)刪除權

除 1 對 1 驗證外，人臉辨識技術在大多數情形下將需處理眾多個資當事人的生物特徵資料。因此，控管者須事先考量其目的及必要性之邊界，以及時回應使個資當事人依 LED 指令第 16 條提出之刪除請求。

(5)限制運用權

若個資當事人爭執其個人資料之正確性，且其正確性與否無法被驗證（或該個人資料須作為證據而留存），則控管者有義務依 LED 指令第 16 條限制運用該個人資料。

人臉辨識技術匯集大量資料，且辨識之準確性與品質可能存在差異。因此，限制運用權對於人臉辨識技術十分重要。品質不佳的影像將導致偽陽性風險上升。此外，若觀察名單（watch list）中的臉部畫面未定期更新，則偽陽性與偽陰性之風險皆會升高。

依 LED 指令前言第 47 點意旨，在特定情形下，若有合理理由相信資料之刪除會影響個資當事人之正當利益，則應轉為限制資料運用，且其運用僅限於作為不能刪除原因之目範圍內。

(6)對當事人權利之正當限制

就控管者的資訊提供義務以及個資當事人之近用權而言，其限制僅得以法律為之，且須構民主社會中為必要且合乎比例、並尊重基本權利和個資當事人正當利益之措施(LED 指令第 13(3)條、第 13(4)條、第 15 條和第 16(4)條）。

為執法目的使用人臉辨識技術時，可以預期在某些情形下，若向個資當事人告知資訊或提供存取，將妨礙使用目的之達成（例如犯罪偵測、保護國家安全或公共安全等）。

近用權並不表示可取得一切相關資訊（例如刑事案件）。刑事偵查過程中限制近用權，係權利限制之適當例示。

(7)透過監管機關行使權利

若 LED 指令第 3 章規定之當事人權利受正當限制，則個資當事人得請求資料保護監管機關代其行使權利，確認控管者資料運用之合法性。控管者須依 LED 指令第 17 條和第 46(1)(g)條，向個資當事人告知此一權利。

對於人臉辨識技術，控管者須採取適當措施，確保能夠因應此類請求（例如，在個資當事人提供充分資訊時，能檢索錄影資料，確認個人資料之位置）。

5. 其他法律要求和安全維護措施

(1)個資保護影響評估（DPIA）

因人臉辨識技術係個資運用之新技術，且其運用之性質、範圍、背景和目的可能造成自然人權利與自由之高風險，故在使用人臉辨識技術前，必須執行 DPIA。DPIA 至少應包括：

- 對所預想運用之一般性描述；
- 評估運用作業相對於運用目的之必要性與比例原則；
- 對個資當事人權利與自由之風險；
- 預計採取之風險因應措施、安全維護措施、資料安全措施、確保個資保護並證明遵循之機制。

EDPB 建議公開評估結果（至少公開主要發現和結論），以提升透明度，強化民眾信任。

(2)向監管機關事前諮詢

依 LED 指令第 28 條，控管者或受託處理者於下列情形時，須在運用前諮詢監管機關：

(a) DPIA 顯示，若控管者未採取降低風險之措施，該運用將導致高風險；或

(b)運用之類型對資料主體之權利及自由具有高風險（特別是新技術、機制或程序者）。

EDPB 認為，大部分人臉辨識技術之部署，對個資當事人之權利與自由存在固有之高風險。因此，除執行 DPIA 外，部署人臉辨識技術之機關亦應在系統部署之前，諮詢監管機關。

(3) 運用之安全性

生物特徵資料具有獨特性，在發生侵害事故時，個資當事人無法變更該資料。因此，使用人臉辨識技術之機關應依 LED 指令第 29 條，格外注意運用之安全性。特別地，執法機關應確保其系統符合相關標準並採取生物辨識模板保護措施（例如 ISO/IEC 24745 標準）。當執法機關使用第三方服務（資料受託處理者）時，尤為如此。

(4) 資料保護之設計與預設

依 LED 指令第 20 條，資料保護之設計（by design）和預設（by default）係為確保資料保護原則和安全維護措施在個人資料運用開始前，即已內建於技術中，且將適用於運用之整個生命週期。因此，若執法機關擬使用人臉辨識技術，其應確保（例如透過採購程序）部署符合資料保護設計與預設原則之技術。

(5) 日誌紀錄

LED 指令規定了數種證明運用合法性、確保資料完整性和資料安全性的措施。在此方面，日誌紀錄（logging）對內部和外部而言，都是確認運用合法性之實用工具和重要維護措施。依據 LED 指令第 25 條，自動化運用系統中，至少對於下列運用作業保留日誌：蒐集、變更、查閱（consultation）、揭露（包括傳輸）、合併與刪除。此外，查閱和揭露之日誌，應記載正當性理由、日期和時間，並盡可能紀錄查閱者或揭露者的身分，以及資料接收者的身分。此外，對於人臉辨識系統而言，亦宜對下列運用作業保留日誌（部分超出 LED 指令第 25 條之範圍）：

- 對參考資料庫之變更（新增、刪除或更新內容）。當無法以其他方式確認運用活動之合法性或結果時，日誌並應保留被變更（新增、刪除或更新）之畫面。
- 識別或驗證行為，包括其結果與信心值。日誌應嚴格遵循最小化原則，僅記載相應畫面在參考資料庫的識別碼，而非記載所搜尋之畫面。除必要情形（例如結果匹配時），應避免在日誌中記錄搜尋時輸入之生物特徵資料。
- 發起識別或驗證之使用者 ID。
- 系統日誌中保存的個人資料應嚴格遵循目的限制（例如稽核），且不得用於其他目的（例如將參考資料庫中已刪除的畫面再行用於識別/驗證）。應採取安全措施確保日誌之完整性，高度建議以自動監測系統偵測對日誌之濫用行為。參考資料庫之日誌如包含人臉畫面，則應與參考資料庫自身採同等保護。此外，應採取自動化程序，確保執行日誌資料保存期限之規範。

（四）附件 1：人臉辨識情境描述模板

附件 1 - 人臉辨識情境描述模板

運用之描述：

- 運用之描述，背景（犯罪關聯性），目的

資訊來源：

- 個資當事人類別：☐ 全體公民 ☐ 犯罪人 ☐ 嫌疑人
  ☐ 兒童 ☐ 其他弱勢個資當事人
- 畫面來源： ☐ 公開場所 ☐ 網路
  ☐ 私人實體 ☐ 其他個人 ☐ 其他 .....
- 犯罪關聯性： ☐ 時序直接相關 ☐ 時序非直接相關
  ☐ 地域直接相關 ☐ 地域非直接相關
  ☐ 未必相關
- 資訊取得模式： ☐ 遠端取得 ☐ 在拍照亭或其他受控環境取得
- 背景—對其他基本權利之影響：

☐ 無

是，影響 ☐ 結社自由

☐ 言論自由

☐ 各項權利：.....

- 個資當事人相關資訊之其他來源：

☐ 身分文件 ☐ 公共電話使用狀況 ☐ 車牌

☐ 其他 .....

參考資料庫（用於與拍攝之資訊相比對）：

- 特定性： ☐ 通用目的資料庫 ☐ 犯罪相關之特定資料庫
- 參考資料庫之組成結構描述（以及法律依據）
- 資料庫目的變更（例如，此前以私有財產安全為主要目的）： ☐ 是

☐ 否

演算法：

- 運用類別： ☐1對1驗證 ☐1對多識別
- 準確性考量
- 技術性防護措施

結果：

- 影響 ☐ 直接影響（例如，個資當事人可能被逮捕、訊問或受歧視性對待）

☐ 非直接（用於統計模型，不致對個資當事人採取重大法律行動）

- 自動化決策： ☐ 是 ☐ 否
- 儲存期限

法律分析：

- 必要性與比例原則分析 — 目的/犯罪嚴重性/受運用影響之無關人員數量
- 向個資當事人提前提供資訊之類別：

☐ 進入特定區域時提供

☐ 在執法機關網站提供一般性資訊

☐ 在執法機關網站提供具體運用之資訊

☐ 其他 .....

- 可適用之法律框架：
  - ☐ 將LED指令文句轉化為國內法
  - ☐ 關於執法機關利用生物特徵資料之國內普通法
  - ☐ 關於該執法機關利用生物特徵資料之國內特別法
  - ☐ 關於該運用之國內特別法（自動化決策）

結論：

關於該運用是否符合歐盟法之一般性意見（並論及法律要件）

（五）附件 2：人臉辨識技術專案管理實務指引

本附件就人臉辨識技術部署過程中的組織性措施和技術性措施提供相關資訊，但並未對所應採取措施作完全列舉。

本附件為執法機關採購人臉辨識技術成品（無客製）提供指引。若執法機關擬開發（進階訓練）人臉辨識技術，則在選擇開發所需之訓練資料集、驗證（validation）資料集和測試資料集，以及開發環境之角色/措施方面，需遵守額外要求。此外，若執法機關依使用目的對人臉辨識技術作進一步調適，亦應在選擇訓練資料集、驗證資料集和測試資料集方面遵守前述額外要求。

為特定執法目的、依據特定法律而蒐集之生物特徵資料，若無用於其他執法目的之適當法律依據，不得用於其他執法目的（LED 指令第 4(2)條）。此外，開發/訓練人臉辨識工具係依其他目的，且對此應參酌運用之初始目的，進行下列評估：為防範低效能對個資當事人產生不良之影響，而利用生物特徵資料評測成效/訓練技術，是否確有必要且符合比例？

1. 角色與責任

執法機關使用人臉辨識技術執行 LED 指令範圍內之職務時，係該人臉辨識技術之控管者。但執法機關內部之不同部門都會參與該運用。在涉及人臉辨識技術之專案中，可能需要執法部門內部下列部門之參與：

- 最高管理階層：衡量風險與成效後，核可該專案。
- 執法機關之 DPO 和/或法務部門：協助評估人臉辨識專案之適法性；協助執行 DPIA；確保尊重個資當事人權利並滿足其行使。
- 運用作業所有者（Process Owner）：負責該專案之發展，確定其細節（包括系統成效要求）；確定公平性指標；確定信心值；確定偏見之可接受標準；識別該專案對個人權利與自由之潛在風險（同時諮詢 DPO 和 IT AI 和/或資料科學部門）並將其向最高管理階層報告。該所有者在確定人臉辨識專案細節前，應諮詢參考資料庫之管理者，以理解參考資料庫之使用目的和技術細節。若對所採購的人臉辨識技術執行重新訓練，則該所有者亦負責選擇訓練資料集。該所有者亦負責執行 DPIA。
- IT AI 和/或資料科學部門：協助執行 DPIA；對評量系統成效、公平性與偏見之指標加以解釋；執行技術性安全維護措施。若對所採購的人臉辨識技術執行重新訓練，則該部門亦負責與運用作業所有者共同識別風險，並採取措施因應該等風險（例如模型推論攻擊 (model inference attack)）。
- 最終使用者（例如外勤警員或鑑識人員）：執行與資料庫的比對；參酌已有證據審查比對結果，並向運用作業所有者通報偽陽性結果和可能存在之歧視。
- 參考資料庫管理者：負責構建和管理參考資料庫（即用作比對對象之資料庫），包括在儲存期限屆滿後刪除人臉畫面。該資料庫可能是專為人臉辨識專案而構建，也可是用於相容目的之現有資料庫。參考資料庫管理者負責確定人臉畫面之儲存於資料庫之時點和條件，以及儲存期限要求（依時間或其他標準確定）。

大部分人臉辨識技術之部署與使用，對個資當事人之權利與自由存在固有之高風險。因此，應依 LED 指令第 28 條，向個資保護監管機關進行事前諮詢。

2. 採購前措施

運用作業所有者應首先清楚理解人臉辨識技術之使用流程（用例 (use case)），並確保該用例有適當法律依據。因此，其需要：

- 正式描述該用例。描述擬解決之問題，人臉辨識技術如何提供解決方案，並概述該技術之應用流程。在此方面，應至少以書面記錄：
  - 該流程所涉之個人資料類別。
  - 人臉辨識技術之適用對象和具體目標，包括匹配吻合對個資當事人之後果。
  - 蒐集人臉畫面之時點與方法，包括蒐集之背景（例如機場安檢門、犯罪現場監視錄影等），以及所運用生物特徵資料之個資當事人。
  - 參考資料庫，及其設立方式、規模以及所含生物特徵資料之品質。
  - 有權限使用人臉辨識系統並據此採取執法行動之執法機關人員（運用作業所有者須確定其帳號內容 (profile) 及使用權限）。
  - 輸入資料之保存期限，或保存期限之終點（例如蒐集該資料之刑事訴訟程序終結時），以及後續作為（刪除資料、匿名化處理後用於科學研究目的等）。
  - 系統運作日誌，以及所留存日誌和紀錄之可用性。
  - 表現指標（例如準確率、精確率 (precision)、召回率 (recall)，F1 分值 (F1-score)），以及可接受之最低標準。
  - 預估在何種時段內/場合下，將對多少人使用人臉辨識技術。

- 執行必要性與比例原則評估。運用作業所有者應首先評估所設想之運用是否有法律依據，此時應諮詢 DPO 和法務部門。部署人臉辨識技術之原因，應係其為執法部門具體問題之必要且符合比例之解決方案。這需要評估其目的、犯罪嚴重性、受人臉辨識系統影響之無關人員數量。評估合法性時，應考量 LED 指令、GDPR、AI 相關法規框架，以及個資保護監管機關之指引[9]，並配合其國內法（特別是刑事訴訟法）適用。比例原則之評估，應識別個資當事人可能受影響之基本權利（隱私和資料保護權利以外的其他權利），並描述及檢視該用例的人臉辨識系統之限制（例如，該系統是持續性或臨時性運作、是否限於特定地域等）。
- 執行 DPIA。在執法領域使用人臉辨識技術可能造成個人權利與自由之高風險，因此應執行 DPIA。DPIA 內容應包括：對所預想運用之一般性描述；對個資當事人權利與自由之風險的評估[10]；預計採取之風險因應措施、安全維護措施、資料安全措施、確保個資保護並證明遵循之機制。DPIA 為持續性過程，因此應針對專案之不同階段更新風險評估。
- 取得最高管理階層之核可。向最高管理階層說明對該用例及該技術對個資當事人權利與自由之風險，以及風險因應計畫，並取得最高管理階層之核可。

3. 採購啟動至部署前措施

- 確定選擇人臉辨識技術（演算法）之標準。運用作業所有者應（在 IT AI 和/或資料科學部門協助下）確定選擇演算法之標準。此等標準應包括用例描述中的公平性和成效指標。並應包括演算法訓練資料之相關要求。對於作為該人臉辨識技術使

[9] 例如 EDPB Guidelines 3/2019 on processing of personal data through video devices.

[10] 對當事人風險之評估，應包括下列方面：與人臉資料庫儲存位置（本地/遠端）相關之風險；受託/複受託運用者相關之風險、所使用之機器學習技術之專有風險（例如資料汙染(data poisoning)）等。

用對象的個資當事人，訓練資料集、測試資料集和驗證資料集應充分納入該等個資當事人各項特徵之樣本（例如年齡、性別、種族等），以降低偏見。人臉辨識技術之供應廠商應提供其訓練資料集、驗證資料集和測試資料集之相關資訊和指標，並描述評量和因應潛在歧視和偏見之措施。運用作業所有者應依廠商提供之資訊，盡可能確認廠商將資料集用於訓練演算法是否有法律依據。此外，運用作業所有者應確保廠商採行生物特徵資料相關之安全標準，例如 ISO/IEC 24745。

- 重新訓練演算法（如有必要）。運用作業所有者應確保所採購之技術已為實現更高準確率進行調適。如需對所採購之人臉辨識系統進行額外訓練，以使其達到準確率指標，運用作業所有者應（在 IT AI 和/或資料科學部門協助下）確保所使用之資料集之充分性與代表性，並檢核資料利用之適法性。
- 設定安全、偏見與低效風險之適當因應措施。該等措施包括確立人臉辨識技術投入使用後的監測機制（日誌紀錄，結果準確率和公平性的反饋機制）。此外，確保識別、評量並因應機器學習和人臉辨識系統特有之風險（例如資料汙染 (data poisoning)、對抗例 (adversarial examples)[11]、模型逆推 (model inversion)、白箱推論 (white-box inference)[12] 等）。運用作業所有者並應採取措施，確保再次訓練所用資料集中的生物辨識資料遵守保存期限。
- 保存人臉辨識系統之紀錄。該紀錄包括對人臉辨識系統之概述，對人臉辨識系統各組成部分及其設立過程之詳細描述，人臉辨識技術監測、運作及控管機制之詳細描述，以及對其所涉

[11] 對抗例（adversarial examples）係指有意對輸入資料增加難以認為察覺之細微干擾（perturbation），使模型以高信心度（confident level）得出錯誤的輸出結果。See, Szegedy et al., Intriguing Properties of Neural Network (2013, revised2014), https://arxiv.org/pdf/1312.6199.pdf (accessed 25 October 2022).

[12] 白箱推論（white-box inference）係指在已知模型細部資訊的背景下，推論其訓練資料之成員身分。See, Nasr et al., Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning (2018, revised 2020). https://arxiv.org/pdf/1812.00910.pdf (accessed 25 October 2022).

風險及因應措施之詳細描述。該紀錄將隨著人臉辨識系統之監測和變更（例如版本更新和/或重新訓練）而不斷發展。

- 製作使用者手冊，清楚說明人臉辨識技術及其用例，以及使用該技術之一切情境與要件。
- 舉辦最終使用者教育訓練。說明人臉辨識技術之能力和限制，以利使用者瞭解何時可使用該技術、何種情境下該技術可能不準確。
- 依 LED 指令第 28 條，向個資保護監管機關進行事前諮詢。依 LED 指令第 13 條向個資當事人告知運用相關資訊及當事人權利。對個資當事人之告知內容應使用適當語言，以使其理解資料如何運用、瞭解技術之基本要素（包括準確率、訓練資料集、已採取何種措施防範歧視和低準確率）。

4. 部署後建議

- 確保對結果之人為介入和監督。不得僅基於人臉辨識之結果而對特定個人採取行動（此將違反 LED 指令第 11 條）。確保執法人員審核人臉辨識之結果。並應確保使用者檢視相反資訊，批判性評估人臉辨識之結果，以避免自動化偏見（automation bias）。為實現此一目的，對最終使用者進行持續教育訓練十分重要，而最高管理階層亦應確保有足夠人力實施監督，使每名工作人員能有足夠時間檢視人臉辨識之結果。記錄、評量並評估人為監督在何種程度上改變人臉辨識之原始結論。
- 監測並因應人臉辨識技術之模型漂移（model drift）。
- 建立風險和安全措施複評機制，定期執行複評，且在人臉辨識技術或用例發生變化時執行複評。
- 記錄人臉辨識系統生命週期內的一切變化（例如更新、重新訓練等）。

- 建立個資當事人權利行使請求回應機制，並確保在技術面能夠提取所涉資料，回應個資當事人請求。
- 確保建立資料侵害因應程序。發生涉及生物特徵資料之資料侵害事故時，可能引發高風險。此時，須遵守因應程序，立即通知 DPO，並通知個資當事人。

（六）附件 3：實務應用案例

人臉辨識技術之實務應用多種多樣，包括在出入境過程中驗證身分、與警用資料庫交作比對、利用公開資料作比對、以即時錄影畫面作比對等。各應用之方式和目的不同，對個人資料保護及其他權利與自由之風險亦有顯著差異。本指引於附件 3 提供執法領域人臉辨識技術之實務應用案例，以協助執法機關在決定部署該技術前，評估其應用之必要性與合比例性。對於所列每個應用案例，本附件之必要性與合比例性評估，分為如下四個步驟：

- 利用附件 1 之「情境描述模板」描述其人臉辨識用例；
- 概述可適用之法規框架；
- 從部署之目的、所涉犯罪之嚴重性、受運用影響之無關人員數量等方面，具體分析該部署之必要性與合比例性；
- 就該部署是否合於必要性與合比例性得出結論。

以下將對各實務應用案例之必要性與合比例性評估作重點摘要。

1. 應用 1

出入境程序中，海關設置人臉辨識技術裝置，將出入境人員之人臉畫面與儲存在旅行證件中的資料相比對，以供出入境人員自助通關。若出入境人員無法通過辨識，則由邊境執法人員查驗其身分，確定其能否通關。

該應用在歐盟法下有明確之法規依據。邊境管控是歐盟確保邊境安全之重要措施。自助通關可提升通關效率，降低人為查驗錯誤之風險。且該措施干預基本權利之範圍及程度皆相當有限。因此，應認其符合必要性與比例原則，但執行機關仍應採取風險防免措施。

2. 應用 2

警方對於通報失蹤、疑似被綁架之兒童，建立失蹤兒童資料庫，內含失蹤兒童姓名、生日、家庭資訊、照片等。執法過程中，警方如遇到疑似被綁架之兒童，以人臉辨識技術搜尋失蹤兒童資料庫，以確認該名兒童是否在資料庫內。如系統提示匹配結果，須由警官綜合考量此前已獲知之證據，判斷該兒童是否為失蹤兒童。

相關會員國國內法對該失蹤兒童資料庫之建置、存取與使用提供明確法律依據。該資料庫係為重大公益目的而設立，其利用僅限於失蹤兒童案件之刑事調查，警員僅能依授權使用，且使用前須具備懷疑該兒童遭綁架之合理事由，對於辨識結果，須綜合證據加以判斷。因此，應認該應用符合必要性與比例原則。

3. 應用 3

一場示威遊行發生暴亂，在暴亂管控與調查過程中，警方廣泛蒐集彙整民眾提供、公務機關監控錄影、媒體報導等相關影像畫面，建立遊行相關者之人臉資料庫，並將暴亂嫌疑人與資料庫中人臉作比對。

相關會員國雖將 LED 指令第 10 條轉化為國內法，提供為執法目的運用生物辨識資料等特種個資之一般性規範，但對於建置人臉辨識資料庫之條件等，並無具體規範，故該應用並無法律依據。

此外，該應用所涉人臉資料庫內人員，並不以涉及嚴重範圍為必要。且因該資料庫對時間、地點及來源之要求相當寬鬆，當地人口之相當部分皆可能在不知情之背景下，被納入資料庫中，且該資料庫可能包含民眾社會生活與政治立場之資訊，從而抵觸資料保護之基本原則，並對集會自由等其他基本權利造成不利影響。因此，應認該應用不符必要性與比例原則。

4. 應用 4

嚴重犯罪調查過程中，警方蒐集犯罪當時之監控錄影畫面，並將嫌疑人影像提交鑑識部門，由鑑識人員將該影像與警用資料庫作比對。

鑑識人員僅將辨識結果提供予負責調查之警員，而不提供人臉模板等生物特徵資料。

該應用以國內法中將生物特徵資料用於刑事鑑識調查之法律為依據。該應用以打擊嚴重犯罪為目的，依法定程序，由適當授權之人員於事後對人為挑選之特定畫面執行辨識，辨識結果須經人為審核，且辨識完成後，生物特徵模板自身不會被用於刑事調查。因此，該應用對當事人權益之影響較為有限，應認其符合必要性與比例原則。

5. 應用 5

警方就特定公共場所執行遠距即時人臉識別。由警方事前建立犯罪嫌疑人之觀察名單（watch list），並依據情報得知名單上嫌疑人可能出現在特定地點。警方據此在特定時間於該地點部署遠距即時人臉識別，由攝影機採集路過該地點者之人臉畫面，並自動傳輸至觀察名單資料庫作比對。如比對發現匹配結果，則由行動指揮警官告知現場警員，由警員決定現場行動。

相關會員國雖將 LED 指令第 10 條轉化為國內法，提供為執法目的運用生物辨識資料等特種個資之一般性規範，但對於即時人臉識別之條件等，並無具體規範，故該應用並無法律依據。

此外，人臉辨識應用對基本權利之干預程度越深，其必要性及合比例性之標準越高。該應用對基本權利有多方面影響。其監控公共場所每名路過者之行為，從而嚴重影響民眾在公共場所身分隱密性之期待，並進而對民主社會中言論自由、集會自由等權利之行使造成限制。民眾可能於單純從事日常活動過程中，即被採集人臉畫面並與警用資料庫相比對。此不僅不符比例原則，亦有大規模監控之風險。即時警用人臉識別實質是將每個人都作為嫌疑犯對待，從而與法治社會中之無罪推定原則相抵觸。若民眾知悉即時人臉識別之存在，可能會因此改變其行為，這不僅影響其自由權利之正常行使，並可能造成人性尊嚴之損害。此外，該應用可能影響個人資料受保護之權利核心，導致民眾依其種族、性別、宗教等被歸類，且因辨識結果準確性不足而遭

受歧視。因此，該應用將難以衡平個人權益與公共利益，應認其不符必要性與比例原則。

6. 應用 6

一家私有公司蒐集網路上公開資料，建成人臉資料庫，並對外提供人臉辨識服務。服務使用者可上傳人臉畫面，將其與該公司之人臉資料庫相比對。警方在案件調查過程中，取得嫌疑人之錄影，但無法透過警用資料庫確認其身分。警方決定使用該公司提供之服務，以識別嫌疑人身分。

私人公司運用個人資料提供前述服務，須具備法律依據。執法機關使用該公司之服務運用個人資料，亦須具備法律依據。該服務需在當事人不知情之背景下，大規模蒐集個人資料，此僅會在極度例外之情形下方屬適法。執法機關使用該服務，將使用該資料庫。而該資料庫資料之蒐集，與執法目的並無關聯。且警務機關將資料揭露予該公司，將難以控制該公司如何運用該資料，且該揭露行為亦可能違反 LED 指令第 39 條關於資料跨境傳輸之規範。因此，應認該應用不符必要性與比例原則。

二、指引簡析

歐盟對於個人資料保護高度重視，於歐盟基本權利憲章中，將「個人資料受保護之權利」規定為一項獨立權利，並要求以「獨立機關」監督個人資料保護法規之遵循。此外，歐盟對於刑事執法領域之外的個人資料運用，以「規則（Regulation）」方式訂定具有全面拘束力、在會員國內可直接適用之法律（即 GDPR），統一歐盟境內之個資保護要求。對於刑事執法領域之個人資料運用，則以「指令（Directive）」方式劃定各會員國個資保護之最低標準，由各會員國依此訂定國內法，並予以遵循。

本指引即為 EDPB 就執法領域人臉辨識技術之使用議題，對於憲章及 LED 指令規範之適用指引。EDPB 強調，為執法目的使用人臉

辨識技術，除干預憲章第 7 條、第 8 條所保護之隱私權及個人資料保護權外，並可能對人格尊嚴，思想、良心與宗教自由，表意自由，集會與結社自由等多種基本權利造成不利影響。因此，為執法目的執行人臉辨識，須以法律作為依據，且該法律須尊重其所限制之權利與自由之本旨，使民眾可明確預見其適用條件，干預程度應限於絕對必要範圍內，並通過比例原則之檢驗。

為執法目的使用人臉辨識技術，將涉 LED 指令第 3(13)條所稱之生物特徵資料之運用。本指引從運用之法律依據、自動化決策、區分當事人類別之義務、當事人權利、資料保護安全維護措施 5 大面向分析 LED 指令之規範要求。EDPB 並提供人臉辨識情境描述模板，協助控管者識別其人臉辨識用例之風險；以及人臉辨識技術採購指引，協助執法機關與人臉辨識系統之採購決策、採購前準備、採購及系統部署、部署後運作 4 個階段，落實個人資料保護。

為執法目的使用人臉辨識技術具有高度敏感性。EDPB 於本指引中說明，其已與 EDPS 聯合作出聲明，呼籲以法律明文禁止對公共場所實施遠距人臉辨識等行為[13]。在歐盟執委會於 2021 年 4 月提出之人工智慧法草案（Proposal on the Artificial Intelligence Act）中，亦主張將「公共場所為執法目的執行即時遠距生物特徵辨識」列為「造成不可接受之風險之 AI」，僅允許在特定例外情形下，依嚴格限制條件使用[14]。因此，未來歐盟法制下，為執法目的執行人臉辨識，除個資保護義務外，並可能面臨 AI 法之監理規範。

[13] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf (accessed 30 September 2022).

[14] European Commission, AI Act Proposal, Article 5.

第二節 英國警務學院即時人臉識別指引

一、指引內容要點

英國警務學院針對警察機關為確定觀察名單（watchlist）上人員之位置，公開設置（overt）之即時人臉識別（live facial recognition, LFR）應用之條件、程序、運作等，提出本《即時人臉識別指引》。因此，本指引為一專門性指引。

本指引除引言外，包括適用範圍、法律框架、公部門平等責任（public sector equality duty, PSED）、警務政策文件、輔助性政策文件、執行面治理和監督等六個章節，另包含兩項附件：附件 A 為即時人臉識別法律與倫理治理框架；附件 B 為即時人臉識別部署步驟圖。

英國警務學院並提出「觀察名單指引」、「部署位置指引」、「關鍵績效指標指引」，與本指引形成完整系列。下文將摘錄本指引重點內容，並以同系列其他指引作為參考。

（一）適用範圍與背景

1. 適用範圍

本指引所稱之即時人臉識別應用，係指對人臉辨識技術之下列應用：為確定相關人員之位置，預先確定其觀察名單，並由系統將攝影機拍攝之即時影像畫面中的人臉與該觀察名單自動進行即時比對，如比對結果為匹配，則將由系統作出提示。本指引僅適用於警務機關為正當警務目的對即時人臉識別應用之部署、使用和管理，而不適用於如下情形：

- 人為地事後在資料庫中搜尋及比對人臉畫面之「事後人臉識別」（retrospective facial recognition, RFR）。
- 人為地以行動裝置上傳畫面以供比對的「類即時人臉搜尋」（near-real-time facial searching）。
- 透過數個彼此串聯之監視錄影系統，以人臉識別方式追蹤特定個人之行動軌跡。

- 私人公司或其他公務機關在警務執法範圍外使用即時人臉識別系統，或為協助警方使用即時人臉識別系統而向警方提供資料。
- 非公開（covert）使用即時人臉識別系統。

2. 適用背景

即時人臉識別應用可用於多種警務相關目的，包括：協助查找和逮捕刑事犯罪通緝對象、防範特定人員進入限制區域、協助查找可能面臨危險或對他人造成危險之人員(例如失蹤人員、恐怖活動人員等)。

技術面向觀察，即時人臉識別應用之運作包含如下六個步驟：

- 構建影像資料庫或使用既有資料庫。即時人臉識別應用首先要求存在觀察對象之「參考畫面」（reference image），用以與「即時畫面」進行比對。參考畫面須經處理，提取觀察對象之人臉特徵並轉化為數值形式。
- 獲取人臉畫面。設置攝影機，當自然人經過攝影機錄影範圍時，即時拍攝該自然人的影像。
- 人臉偵測。對於攝影機拍攝所得的影像，即時人臉識別軟體偵測其所包含的人臉畫面。
- 人臉特徵提取。對於所偵測到的人臉畫面，即時人臉識別軟體自動提取其人臉特徵，形成生物辨識模板。
- 人臉比對。即時人臉識別軟體將提取所得的生物辨識模板與觀察名單相比對。
- 匹配。即時人臉識別系統來自兩張不同畫面的人臉特徵相比對，並產出相似度值（similarity score），此一數值越大，表示相似度越高。如該相似度值超過預定閾值（threshold value），即時人臉識別軟體將提示發現可能匹配結果。經訓練的警務人員將確認匹配結果，並決定是否採取進一步行動。因此，即時人臉識別系統僅協助警務人員進行辨識，而非獨立判斷辨識。

（二）法律框架

1. 相關法規

即時人臉識別系統部署和使用應遵循相關法規。警方對即時人臉識別系統之使用方式依其用例（use case）、犯罪調查需求、警務優先事項而定。警務首長應就即時人臉識別系統制定警務政策，且其內容應符合本指引所述法遵要點，並特別留意即時人臉識別系統實務運作對下列領域法律之遵循：普通法上的警務職責、刑事證據法律[15]、人權保護法律[16]、個人資料保護法律[17]、監視錄影監管法律[18]、平等權保護法律[19]。

本指引之適用係配合監視錄影委員（Surveillance Camera Commissioner, SCC）[20]和資訊委員（Information Commissioner）之其他見解與指引。

2. 人權考量要素

對於即時人臉識別系統拍攝之人及觀察名單上人員，即時人臉識別系統可能影響其依《1998 年人權法（Human Rights Act 1998）》第 8 條享有之隱私權。此外，即時人臉識別系統可能對基本人權有更廣泛的影響，包括《1998 年人權法》第 2 條之生命權，第 3 條之不受酷刑、不人道或有辱人格待遇之權利，第 9 條之思想、良心與宗教自由，第 10 條之表現自由，第 11 條之集會與結社自由[21]，以及第 14 條之平等權[22]。警務首長於制定即時人臉識別系統部署計畫及使用政策時，

[15] Police and Criminal Evidence Act 1984 Code D.
[16] Human Rights Act 1998.
[17] Data Protection Act (DPA) 2018, UK General Data Protection Regulation (GDPR).
[18] Protection of Freedoms Act 2012.
[19] Equality Act 2010.
[20] SCC 係依英國《2012 年自由保護法（Protection of Freedoms Act 2012）》設立之獨立監管機關，負責促進《監視錄影實務守則（Surveillance Camera Code of Practice）》之遵循。
[21] 警方如擬在集會或示威場合使即時人臉識別技術協助執法，須尤其審慎評估，包括徵求法務部門意見，以確保所採取執法措施之必要性與合比例性，將對民眾權利之影響降至最小。
[22] 人臉辨識演算法若人口族群代表性不足，則可能導致不同族群匹配結果之準確率不同，從而造成歧視。

應參酌警務機關內法律單位之建議，考量即時人臉識別系統對人權之影響。

（三）公部門平等責任（PSED）

警務機關對即時人臉識別系統之使用，應遵循公部門平等責任（PSED）之要求。PSED 源於《2010 年平等法（Equality Act 2010）》第 149 條，依該條規定，公務機關於執行法定職務過程中，須適當注意消除歧視、騷擾等該法所禁止之行為，促進因年齡、身心障礙、種族、性別、宗教等因素而形成之不同族群間之平等，培育不同族群間之友善關係[23]。

研究顯示，人臉辨識演算法可能存在偏見，而對不同族群（demographic group）之辨識效果有所不同。然而，不同演算法之準確度不同。因此，在採購即時人臉識別系統之過程中，須評估演算法之整體準確度，以及其對不同族群的辨識效果。人臉辨識演算法的準確度受訓練資料集影響。雖然廠商訓練資料集之具體性質與組成內容可能難以確認，但警務機關應要求廠商提供其演算法對不同族群辨識效果之書面實證證據。

PSED 之遵循不僅限於即時人臉識別技術和攝影機本身，亦適用於人臉辨識技術運用方案之各個方面，包括決策警官之角色。警務機關應從如下方面遵循 PSED：

- 完成並持續維護平等影響評估（equality impact assessment）。
- 採取一切合理可行措施確保即時人臉識別軟體不存在不可接受之偏見，包括因種族、性別、宗教信仰或觀念而生之偏見。但沒有任何系統是完全無偏見的，警務機關應瞭解偏見之程度並採取因應措施。

[23] Equality Act 2010, Section 149(1) (Public sector equality duty): A public authority must, in the exercise of its functions, have due regard to the need to— (a)eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act; (b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; (c)foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

- 確保對所用即時人臉識別演算法之統計準確性及族群間辨識表現進行確實監督。須對廠商說辭進行驗證，以確保所採購之演算法符合警務機關用例之需求及 PSED 責任之要求。
- 確保對即時人臉識別技術、演算法之表現、因應措施之效果進行持續監督。

（四）警務政策文件

應由警務首長擔任即時人臉識別之「高級負責警官」（senior responsible owner, SRO），負責即時人臉識別技術之策略管理，並針對即時人臉識別技術之使用訂定總體政策文件。該文件應規定：

- 即時人臉識別技術之使用，應以負責任、透明、公平且符合倫理之方式為之，遵循各項法令規範，且僅限於無法依其他干預較小之方式實現所追求之正當警務目的時方可為之。
- 強化並持續發展即時人臉識別技術之準確度和功能。
- 遵循即時人臉識別溝通計畫，向民眾說明即時人臉識別之使用如何確保隱私、平等及透明性，以取得民眾對即時人臉識別技術之信任。
- 與社區保持持續溝通，增進即時人臉識別使用之認知，回應民眾之疑慮。
- 發展警務首長之策略面治理（strategic governance），盡可能與執行面之決策相區分，以確保對即時人臉識別使用行為之獨立、確實監督。
- 對於即時人臉識別之部署，將執行單位和技術單位主管納入指揮體系，實施良好執行面治理。部署即時人臉識別之決策應僅限一定層級以上之警官作出，且應作成書面紀錄。作出部署決策者稱為「授權警官」（authorising officer, AO）。
- 以透明方式識別、管理和因應警務機關因即時人臉識別而面臨的名譽與組織風險，從每項部署中學習經驗。
- 管理即時人臉識別系統及其內含資料之安全性。

- 與獨立監管機關保持適當溝通。
- 確定部署成效之評估指標，包括確定虛警率（false alert rate）目標，並持續評估所部署系統之成效。
- 若被拍攝人員經比對不符觀察名單，確保該人員之生物辨識模板自動即時刪除。錯誤匹配示警應儘速確認，至遲不得超過31日。

該政策文件得規定，在緊急情形下，得適當放寬即時人臉識別部署授權之人員位階要求。緊急情形可能包括：

- 對生命、人身或財產之急迫威脅；
- 具時效性之情蒐或調查機會，且依其所涉威脅之嚴重性和所獲成效判斷，有必要採取緊急行動。

前述緊急狀況下授權應保留紀錄，包括授權所依據之資訊與理由。且警務政策文件應要求緊急授權警官儘速將授權決定及其理由通報有部署決策權之上級警官，由該上級警官決定是否維持、變更或終止部署。

（五）輔助性政策文件

警務首長應主責訂定輔助性文件，包括：

- 即時人臉識別授權流程指引，明確規範決定使用即時人臉識別之各個步驟。
- 即時人臉識別標準作業程序（SOP），且應包括下列內容：
    - 即時人臉識別相關警務用例和警務優先事項之考量要素。
    - 觀察名單和影像來源之標準。
    - 接獲示警後之處置指引，示警後應採取之行動，因應示警之資源部署，以及相關警務職權。
    - 確定部署地點和攝影機位置之考量要素。
    - 確保部署公開性之措施，包括事前通知、張貼提示標誌等。

- 參與部署人員之職責。
- 保存期限。

- 就警務首長授權使用之各類部署，依英國《2018 年資料保護法（Data Protection Act 2018）》第 64 條（對應歐盟執法指令第 27 條）執行個資保護影響評估。
- 就警務機關擬實施之各類部署，執行平等影響評估（equality impact assessment, EIA）。
- 社區影響評估（community impact assessment, CIA）。
- 即時人臉識別教育訓練資料，以確保機關內即時人臉識別技術使用者充分瞭解：
  - 如何回應示警；
  - 即時人臉識別之技術特性；
  - 即時人臉識別之技術對所涉生物辨識個資當事人之影響；
  - 核心人權原則、資料保護和平等權法規，以及前述規範與即時人臉識別之關聯；
  - 對個資當事人之干預程度及其潛在影響。
- 依英國《2018 年資料保護法》第 35(5)(c)條（對應歐盟執法指令第 10 條），關於即時人臉識別所涉特種個資運用之適當政策文件（appropriate policy document）。依英國《2018 年資料保護法》第 42 條，該文件應包含下列內容，且應依要求提供予英國個資保護主管機關「資訊委員辦公室（Information Commissioner's Office, ICO）：
  - 該運用如何遵循資料保護原則之說明；
  - 控管者資料保存與刪除政策之說明，包括資料可能之保存期限。

警務文件並應確定即時人臉識別執行面之指揮架構，並區分三種不同角色：

- 警務即時人臉識別部署之策略指揮官，即「高級負責警官」（SRO）。
- 部署行動之授權者，即「授權警官」（AO）。
- 即時人臉識別「實地執行」之指揮者，即執行指揮。

（六）執行面治理和監督

各項部署皆應經適當評估與授權，並作成紀錄。若 AO 無法立即對部署申請以書面作出授權決定，可口頭作出授權，但應於事後儘速作成書面紀錄。除有緊急情形外，授權應於即時人臉識別部署前作成紀錄。

即時人臉識別技術之部署應符合警務政策要求及用例，且應符合下列條件：

- 具針對性；
- 依情資作出；
- 具適當時限和地理範圍限制。

即時人臉識別部署前，AO 應確保申請者須完成該表 1 所列評估項目，並基於該等評估決定是否提出部署申請。AO 依據申請書及評估結果，以書面方式決定是否授權部署。

即時人臉識別部署申請書和部署授權書應包含下列內容：

- 敘明部署之正當目的、所涉法定職權，以及個人權利與即時人臉識別技術使用成效間之均衡。
- 依《1998 年人權法》，說明：
    - 該部署之必要性（而非僅便利性）；
    - 與擬達成之正當目的間符合比例。
- 依《2018 年資料保護法》，說明所涉個資運用活動屬執法目的之絕對必要，包括：
    - 所涉「迫切社會需求」（pressing social need）為何；
    - 為達成該目的，為何須要運用敏感個資；

- 運用所援用之《2018 年資料保護法》附錄 8 中所列依據；
- 為何干預性較低之方式無法實現該目的。

表 1　英國警務學院 LFR 部署文件和記錄表

評估	評估內容包括社區影響評估（CIA）、平等影響評估（EIA）、個資保護影響評估（DPIA）和 SCC 之自評[24]。 AO 授權決策過程中，應參酌上述文件，以確保部署所涉風險可獲有效因應。AO 應使個資保護長（DPO）參與撰寫 DPIA 以及管理個資運用活動。 AO 應確保上述評估適當識別、記錄並因應風險，以確保部署為警務目的所必要且合於比例。 DPIA、EIA 等評估文件可適用於多項部署。雖該等評估文件須持續檢視其充分性，但未必需要針對每項部署分別調整其內容。
作業風險評估	評估該即時人臉識別部署之具體作業風險，包括因應風險之相關決策。
即時人臉識別部署申請書	申請書說明擬部署之即時人臉識別應用與情蒐事例（intelligence case）之管理，並詳述部署之細部安排，包括： - 位置； - 時間；

[24] SCC 自評詳見：https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool (accessed 30 September 2022)。

	- 正當目的； - 法律依據； - 必要性； - 合比例性； - 安全維護措施； - 觀察名單之組成； - 相關資源。 AO 應依據所涉警務目的和情資，基於必要性和比例原則，事前同意部署之地點、日期、時間和時長。部署之地點與時間應符合對目標人員出沒之地點與時間之合理懷疑，且相關原因之紀錄應足以使客觀第三人理解。
成效評量指標	說明用以評量部署成效之指標。該等指標亦可在部署申請書和/或即時人臉識別政策中列明
部署授權書	AO 之部署授權書提供決策之審計軌跡，並表明 AO 認為部署申請書符合下列條件之理由： - 部署符合課責性、合法性、嚴格必要性和比例原則； - 執行適當安全維護措施； - 替代措施不足以實現警務政策目的。 - 該部署授權書將載明落實下列事項之方法： - 依進入拍攝範圍之路徑，設置明確且適當之標誌； - 於部署地點和警方網站揭露個資運用相關資訊； - 回應個資當事人之權利行使請求；

	- 因部署即時人臉識別技術所取得個資之保存和/或刪除。 部署授權書應依法保存，並依要求提供獨立查核。
即時人臉識別部署終止報告	記載下列事項： - 部署之執行地點和時間； - 終止部署之事由； - 所使用之資源； - 相關統計資料； - 部署之結果； - 事後審查所發現問題之摘要。
部署日誌	即時人臉識別部署規劃與執行之日誌，例如 AO、執行指揮和實際執行者之日誌。
部署清冊	警務機關應建立全部即時人臉識別部署之清冊，且該清冊應予以公開。

二、指引簡析

英國雖已正式脫離歐盟，但其個資保護法制，仍沿用脫歐前訂定之 2018 年資料保護法。該法除併入 GDPR 之全文（形成 UK GDPR）外，並於第 3 編（Part 3）將歐盟 LED 指令轉化為英國國內法。

本指引係英國警務學院所發布之警務專業指引（APP）之一，英國警務學院係英國內政部下設之獨立機構，負責支援警務機關之專業技能發展，為關鍵警務領域訂定標準與指引，以及分享知識與最佳實務等[25]。而警用人臉辨識所涉之法令遵循議題，在英國分屬資訊委員、監視錄影委員等之主管範圍。因此，本指引聚焦於「即時人臉識別」此一對民眾基本權利風險較高之人臉辨識應用態樣，以警方之實務作

[25] College of Policing, About Us, https://www.college.police.uk/about (accessed 30 September 2022).

業為導向，對相關法規遵循、管理制度建置、執行面管理等事項提供具操作性之指引。

對於警用人臉辨識技術而言，英國和歐盟之法規框架整體一致，故前述 EDPB 之執法領域人臉辨識技術運用指引之諸多要求，例如使用人臉辨識技術運用個資之絕對必要性和法律依據、事前執行 DPIA 等，在本指引中亦有要求。此外，本指引亦對警務機關即時人臉識別應用之決策、申請、部署與執行各個階段之職責分工、作業流程、文件要求等有詳細說明。

第三節 加拿大 OPC 警用人臉辨識技術隱私指引

一、指引內容要點

人臉辨識技術可能對隱私造成高風險，然而，加拿大聯邦及各省隱私保護委員皆認為，加拿大現行法律框架並不足以充分因應人臉辨識帶來的隱私侵害風險。且在缺乏統一法制的背景下，警務機關使用人臉辨識技術的適法性有時並不明確。因此，加拿大隱私保護委員聯合各省級隱私保護委員，發布警用人臉辨識技術隱私指引，以期呈現警用人臉辨識技術之最佳實務，協助警務機關管理不當使用人臉辨識技術可能帶來之高風險。

本指引除引言外，主要包括人臉辨識技術、隱私框架、結論和建議摘要四大部分。其中，「隱私框架」部分為人臉辨識技術隱私保護之重點說明，包括法律依據、隱私保護影響評估、準確性、課責性等面向。本指引重點內容摘要如下：

（一）人臉辨識技術

人臉辨識技術係一種軟體，其透過複雜圖像處理方法，偵測並分析人臉的生物辨識特徵，並用以識別（identification）或驗證（verification/authentication）特定個人之身分。人臉辨識技術使用經「深度學習（deep learning）」方式訓練之演算法，能基於平面的影像畫面，生成包含近百個生物辨識特徵的立體臉紋（faceprint）。

人臉辨識的功能包括「識別」和「驗證」兩種。「識別」過程中，系統接收之畫面（即「標的畫面」 (probe image)）將與資料庫中預存之畫面相比對，以確定標的畫面中個人之身分。識別又稱一對多（1:N）比對。「驗證」過程中，標的畫面已附有身分資訊。系統將驗證畫面與資料庫中該身分之對應畫面相比對，以證明標的畫面中個人之身分。驗證又稱一對一（1:1）比對。因警用人臉辨識多涉及「識別」功能，故本指引主要以「識別」為功能說明對象。

人臉辨識系統之主要組成部分如下：

1. 訓練資料

人臉辨識軟體之演算法需以機器學習（machine learning）方法，以大量已加註標籤（labelled）的人臉畫面加以訓練。機器學習過程中，演算法不斷調整其模型，以達到符合訓練資料結構之效果。使用訓練資料「訓練」演算法，一方面可實現演算法之自動「學習」，無需特別調整其程式，另一方面，訓練資料如有不足或缺陷，亦會被演算法「學習」，並進而反應在後續運作中。

2. 演算法

人臉辨識之演算法提供四項核心功能：

- 人臉偵測：掃描特定畫面，並偵測其中人臉。
- 臉紋生成：基於人臉畫面，生成臉紋。
- 臉紋比對：比對兩項臉紋，生成相似度值（similarity score）。
- 臉紋匹配：搜尋人臉資料庫，並藉由臉紋比對功能，產出相似度值不低於閾值（threshold）之結果清單。

3. 標的畫面

輸入系統中，用以識別或驗證其身分之畫面為「標的畫面」。依標的畫面之提交方式，可分為：

- 事後人臉辨識：標的畫面之蒐集與比對間相隔一段時間。
- 即時人臉辨識；標的畫面蒐集後立即用於比對。

4. 人臉資料庫

為識別或驗證標的畫面中個人之身分，人臉辨識系統將其與資料庫中已知身分之畫面相比對。人臉資料庫通常由最終使用者提供。例如，警方資料庫通常是嫌犯照片資料庫或失蹤人員照片資料庫。然而，部分人臉識別系統廠商自身亦提供資料庫。廠商資料庫通常是蒐集網路公開可得畫面，其法律依據相當不明確。

5. 臉紋

人臉辨識系統將所偵測的人臉各項特徵加以測量，並將測量結果生成人臉特徵數值之模板（template），即「臉紋」。臉紋中記載特定個人不易改變之人臉特徵，例如：

- 兩眼間距；
- 鼻子寬度；
- 人中長度；
- 眼窩深度；
- 顴骨形狀；
- 下顎長度。

6. 相似度值

人臉的變化性很高。不同人臉可能在某些方面極為相似，但在其他方面完全不同。即使是同一張人臉，也可能因光線、角度等因素而看起來不同。人臉辨識系統以「相似度值」（又稱信心值 (confidence score)）表示兩項臉紋間生物特徵之相似程度。相似度值越高，相似度越高。

7. 閾值

相似度值達到或超過預設閾值時，兩項臉紋才會構成「匹配」。閾值之設定直接影響搜尋可得之結果數量，並間接影響人臉辨識演算法之準確率。

除前述七項組成部分外，人臉辨識系統亦可能包含品質評估、偽冒偵測（impersonation detection）等功能。

（二）合法授權

警務機關對人臉辨識技術之使用須經依法授權，且須保障人民隱私。警務機關應就其是否有權部署或執行人臉辨識計畫、該計畫是否適足保障個人權利，取得法律意見。如不符前述條件，則不得執行人臉辨識計畫。

1. 授權之來源

目前除魁北克省外，加拿大並無規範人臉辨識技術之專門性法規。人臉辨識之法規框架，包括各隱私保護、警察職權、人權保障相關成文法、普通法等。

人臉辨識運作的各個階段，例如演算法之訓練、人臉資料庫之設立、標的畫面之獲取與比對等，都需蒐集和利用個人資料。涉及個人資料之各個階段，均須具備合法授權。此外，若警務機關使用外部人臉辨識服務，須確保其外部廠商有權蒐集和利用其服務所涉之個人資料。

2. 人權保障

警務機關對人臉辨識技術之使用除須具備合法授權外，並應確保遵循人權保護法規。

《加拿大權利與自由憲章（Canadian Charter of Rights and Freedoms）》保障人民不受不當搜索（unreasonable search）和逮捕之權利。其所稱之「搜索」，視是否違反人民之合理隱私期待（reasonable expectations of privacy, REP）而定。而適當之搜索，須經適當法律授權，且以適當方式為之。

就警用人臉辨識技術而言，是否涉及人民之合理隱私期待，須依個案事實綜合判斷。考量因素包括個人對原始畫面之隱私利益、蒐集之方式、背景與目的、警方是否使用額外資料等。合理隱私期待之判斷可能涉及個人之主觀期待，以及客觀合理之期待。

雖然合理隱私期待須依個案判斷，然人臉辨識確實將個人難以改變之敏感個人資料用於身分辨識。且個人在公開場所亦維持一定程度之合理隱私期待，並不因其臉部公開可見而被自動否定合理隱私期待。縱使個人知悉使用人臉辨識系統之可能性，亦不意味社會因技術進步而接受更高程度之隱私干預。

3. 隱私保護

人臉辨識技術將涉個人資料之蒐集與利用，故須遵守隱私法規關於個人資料蒐集、利用、揭露和保存之規範。雖聯邦和各省之隱私法規內容不同，但通常允許公務機關為正當目的蒐集個人資料。例如，依聯邦隱私法規，聯邦機關之個人資料蒐集行為須與該機關之職權活動直接相關。除另經授權外，所蒐集之個人資料僅得用於蒐集目的或與蒐集目的相容之用途。

4. 必要性與比例原則

必要性與比例原則確保隱私干預活動係出於足夠重要之目的，且符合嚴格限縮（narrowly tailored）於該目的之必要範圍。執法活動顯然具有確保公共安全之公共利益，然保障個人隱私權亦屬公共利益之要求。隱私保護雖非絕對，然亦不得以公共安全為由任意干預。對於人臉辨識技術之使用而言，必要性與比例原則要求：

- 為達成特定目的所必要：

  人臉辨識計畫之目的須明確界定，不得僅以一般公共安全作為實施之理由。警務機關應證明該特定目的之迫切性（pressing）與重大性（substantive）。所蒐集之個人資料範圍不得過於廣泛，而應限於實現該特定目的之必要範圍。

- 有效性：

  警務機關應證明個人資料之蒐集有助於該特定目的之達成。有效性之證明，亦應考量該特定目的之準確率要求。

- 最小損害：

  人臉辨識計畫應限於最小範圍。警務機關應證明並無隱私干預較小之其他手段可合理實現該特定目的。

- 合比例性：

  合比例性要求人臉辨識計畫所造成之隱私干預與所獲成效相均衡。人臉辨識計畫之合比例性判斷分為兩個步驟：

- 首先，警務機關應確認其人臉辨識計畫對個人隱私干預，包括人臉辨識對隱私之一般影響，以及該特定利用之具體影響。
- 其次，警務機關應評估該人臉辨識計畫所獲成效是否足以作為該等隱私干預之正當性理由。不同目的之正當性論證力度不同。例如，打擊恐怖活動可支持較強之隱私干預，而偵辦一般毀損犯罪則不然。在自由與民主的社會中，某些高強度隱私干預（例如大規模監控）可能無法獲得正當性支持。若人臉辨識計畫之隱私干預程度較高，警務機關應採取明確、全面之安全維護措施，保障民眾隱私與人權。

（三）隱私保護之設計

警務機關在開始使用人臉辨識技術之前，應正式將隱私保護措施納入人臉辨識計畫。且隱私保護措施應覆蓋該計畫所涉之全部個人資料，包括訓練資料、臉紋、原始畫面、人臉資料庫、因人臉辨識搜尋而推知之情資等。

1. 隱私影響評估

隱私影響評估（privacy impact assessment, PIA）為落實隱私保護設計、分析並因應隱私保護影響之有效方式。警務機關應於人臉辨識計畫開始執行（包括試行）前、重大變更前，執行 PIA。

為有效執行 PIA，警務機關應：

- 以 PIA 報告記錄 PIA 之執行過程；
- 遵循隱私委員所發布之 PIA 相關指引；
- 採取措施降低 PIA 所識別之風險；
- 指派專人負責管理剩餘風險；
- 若該計畫之個人資料蒐集、利用、揭露或保存發生重大變化，重新執行 PIA（或適當修正已執行之 PIA）。

PIA 執行過程之初始階段，警務機關應諮詢隱私保護專家和利害關係人，包括：

- 相關隱私委員辦公室；
- 相關人權委員辦公室；
- 弱勢群體之代表，包括原住民族等。
- 受影響民眾之其他代表。

PIA 應識別並評估對下列各項之影響：

- 個人；
- 作為人臉辨識系統部署對象之社區；
- 可能因隱私干預而受不當損害之群體；
- 民眾對警方個人資料蒐集和利用之信任；
- 人權和民主權利，包括隱私權、平等權、和平集會權、表現自由等。

針對所識別之影響，警務機關應說明：

- 為何所規劃之人臉辨識應用為實現迫切或重大公共目標所必須；
- 該計畫之預期成效為何，以及該成效為何與所涉風險間符合比例；
- 為何其他干預性較低之措施不足以實現所追求之目的；
- 該計畫執行過程中如何將風險降至最低。

2. 監測與複評

警務機關應持續監測並重新評估隱私風險及隱私保護措施之有效性。相關最佳實務包括：

- 年度遵循狀況稽核：由內部或外部人員就下列遵循事項執行年度稽核：
    - 法令要求之持續遵循；

- 該計畫整體隱私管理制度之持續遵循，包括課責性、透明性、資料安全、資料揭露、資料保存、目的限制等方面之政策、程序和規程（protocol）；
- 該計畫之資料儲存與汰除機制，確保個人資料依資料保存程序儲存和汰除；
- 第三方對該計畫隱私義務之遵循，包括遵循採購要求、資料分享協議等。

- 計畫年度審查：每年評估該計畫目標之達成狀況。評估應使用可展示（demonstrable）之標準，例如因使用人臉辨識而完成之逮捕、起訴和判決有罪之案件數量。

警務機關應持續諮詢利害關係人意見，包括因使用人臉辨識技術而受影響之群體代表。

警務機關並應依稽核發現、審查結果、安全事故、法規變更、技術發展等因素，及時更新政策、程序、相關協議等。該等更新並應記錄於 PIA 中。

（四）準確性

警務機關須確保人臉辨識計畫所蒐集和利用之個人資料之正確性。由於不正確資料之蒐集和利用可能對個人權利造成嚴重風險，不得想當然地認為人臉辨識系統具有準確性。

1. 影響人臉辨識各組成部分之準確性

人臉辨識系統之準確性應整體評估。只有人臉辨識系統各組成部分皆能準確、公平地處理個人資料時，系統整體方具準確性。

(1) 訓練資料：

訓練資料可能加劇人臉辨識系統之偏見。若訓練資料中特定族群（demographic）之代表性不足，則所訓練之演算法對不同族群之辨識準確度可能存在差異。

(2) 演算法：

演算法之準確性應從以下三個面向考量：

- 首先是統計上之準確性。人臉辨識系統產出之結果為兩張畫面同屬一人之推測機率（probabilistic inference）。因此，其準確性並非是/否之二元判斷，而是需觀察其搜尋結果之錯誤率。應考量如下兩類錯誤：
    - 偽陽性錯誤（第 I 型錯誤），即演算法返回之匹配結果與標的畫面並非屬同一人；
    - 偽陰性錯誤（第 II 型錯誤），即演算法未得出匹配結果，但資料庫中包含匹配對象。
- 其次，偽陽性錯誤與偽陰性錯誤間通常具交替（trade-off）關係，且與所設定之閾值相關。較高閾值將降低偽陽性錯誤，但可能致使偽陰性錯誤增加。
- 第三，閾值之設定應考量人臉辨識技術的性質、範圍、背景與目的，以及對個人權利與自由之影響，以利優先降低對個人風險較高之錯誤，同時確保人臉辨識系統有效性。

(3) 人臉資料庫與標的畫面

資料庫中畫面及標的畫面的品質、新舊將影響人臉辨識系統的準確性。此外，不同族群在人臉資料庫中之代表性也將影響準確率。

(4) 人為審核

人為審查是降低錯誤或偏見的重要措施，但也可能無意間帶來錯誤或偏見。為降低人為風險，應確保：

- 審核人員經人臉比對鑑識訓練，並瞭解人臉辨識系統之運作方式；
- 審核人員有合理時間進行判斷；
- 審核人員避免「自動化偏見」（automation bias）或過分依賴自動化系統進行決策。

2. 提升準確性、降低偏見之最佳實務

警務機關應要求提供人臉辨識技術之廠商：

- 將其演算法交予外部獨立測試，測試範圍應包括對不同社會族群（例如不同種族、性別或年齡層）之準確性。
- 在人臉辨識搜尋結果中，列明相似度值（例如，以百分比形式呈現）。

警務機關還應：

- 設定適當閾值，以利優先降低對個人風險較高之錯誤，同時確保人臉辨識系統有效性。
- 在人臉辨識系統部署前，內部測試其整體偏見性和準確率，並在部署後定期重複測試。
- 確保測試由適格人員執行。
- 確保測試遵循通行標準和技術規範，包括成效指標、測試數據紀錄、測試結果報告、測試程序和方法、族群變化等。
- 在記錄和揭露匹配結果時，列明搜尋結果所示之相似度值。
- 僅使用高畫質且較新的影像作為資料庫畫面和標的畫面。
- 考慮使用畫質評估演算法，協助確定輸入人臉辨識系統之畫面品質。
- 依演算法之改善，及時更新其人臉辨識系統。
- 如內部或外部測試發現如下情形，停止使用該人臉辨識系統：
    - 人臉辨識系統統計上之準確性不足；或
    - 不同社會族群間的錯誤率有實質差異。

警務機關應避免：

- 完全依人臉辨識結果進行決策。
    - 換言之，影響法律權利或利益之決定，應由人類作出。
- 對未經適當人為審核之匹配結果採取行動。
    - 此外，審核人員應不同於案件調查人員，以避免偏見。

（五）課責性

警務機關應對其所管控之個人資料負責，並能夠證明其遵循法律要求。

1. 隱私管理制度

警務機關應訂定隱私管理制度（privacy management program, PMP），該制度之主要內容應包括：

- 載明人臉辨識計畫所涉個人資料蒐集、利用、保存、揭露條件和方法之政策和程序。
- 載明人臉辨識搜尋執行條件之規程。
- 使用人臉辨識系統之標準作業程序（SOP），包括人臉辨識搜尋之操作說明。
- 人臉辨識搜尋之紀錄制度，包括搜尋之正當性理由。
- 人臉辨識系統使用授權制度。
- 人臉辨識計畫遵循監督作業辦法，包括違反行為之偵測與處理方式。
- 定期教育訓練制度。

警務機關並應：

- 明確內部權責，指定專人負責隱私制度管理與執行（包括核發權限）。
- 建立通報制度，提供事故和問題通報至管理高層之管道。
- 建立人臉辨識軟體使用日誌，以軟體自動記錄每次搜尋及執行人員登入帳密。
- 建立個人資料揭露狀況紀錄，包括揭露之依據（包括具體指明所涉契約），揭露對象、揭露方式、揭露所附條件、授權揭露之人員。揭露狀況紀錄應依要求提供監督機關檢視。
- 採取管理上、技術上或實體管控措施，確保相關人員僅於人臉辨識計畫目的範圍內存取和使用人臉辨識系統。

2. 採購

警務機關應於採購過程中，透過契約確保提供人臉辨識軟體和服務之廠商遵守人臉辨識計畫之要求。採購相關要求通常至少包括：

- 廠商之活動—包括訓練所用個人資料之蒐集和利用，符合隱私法規。
- 充分說明廠商之訓練資料來源。
- 確保訓練資料對不同族群之代表性。
- 以獨立測試（例如美國 NIST 測試評分）評估廠商是否達到效果要求。
- 以警方內部測試評估廠商是否達到效果要求。
- 禁止留存、揭露警方提供之個人資料，或把該等資料作二次利用。
- 就廠商之遵循狀況執行稽核。

警務機關亦可利用採購過程協助確保對內部政策和程序之遵循。例如，警務機關得要求採購產品符合下列規格：

- 包含嚴格驗證程序（strong authentication procedure）；
- 自動留存軟體使用紀錄；
- 發動搜尋須經主管授權；
- 發動搜尋須提供輔助資訊（例如案件編號）。

3. 教育訓練

警務機關應對人臉辨識技術訂定專門教育訓練方案。且相關人員須經教育訓練方可使用人臉辨識系統。教育訓練應確保參加者充分理解下列內容，且其教育訓練資料應及時更新：

- 存取、使用、揭露和保存個人資料以及人臉辨識系統之政策和程序。
- 依人臉辨識計畫處理個人資料之法律責任。
- 人為審核程序和人臉比對鑑識技巧。
- 人臉辨識之技術原理，包括系統產出之結果。

- 人臉辨識比對程序可能因種族、性別等族群特徵而存在偏見。
- 因標的畫面之畫質較低或人臉資料庫中的既存錯誤，導致錯誤結果之可能性。

（六）資料最小化

警務機關應將其所蒐集之資料，限於與人臉辨識計畫之具體目的直接相關且必要之範圍內。

警務機關應就臉紋及相關資料之蒐集、利用、保存和揭露訂定並執行規程。對於人臉資料庫應由哪些畫面組成，該規程應自計畫開始時，即訂定明確、具體且客觀之標準，且其範圍應足夠限縮，以確保人臉辨識計畫符合必要性和比例原則。

警務機關並應採取其他必要措施，將人臉辨識計畫所蒐集和利用之資料限於最小範圍。例如：

- 對標的畫面進行裁切，確保其不含搜尋對象以外之其他自然人。
- 除依法執行人臉辨識計畫所必須外，不得將人臉辨識計畫之個人資料與其他資料庫相連結。
- 人臉資料庫之資料應盡可能單獨儲存，且與其他網路系統相區隔。

（七）目的限制

警務機關必須確保個人資料僅用於其蒐集目的（或與蒐集目的相符之其他目的），且個人資料之各項利用皆屬於該計畫合法授權之範圍內。為滿足前述要求，警務機關應採行一系列管理上、技術上或實體管控措施，且須確保受委託之第三方不致將個人資料用於其他目的。例如，若警務機關將畫面提供予第三方軟體廠商作辨識用途，則須確保廠商不會將該畫面用作訓練資料、納入人臉資料庫或作其他利用。警務機關應以合約明確約定廠商對人臉辨識相關資料（畫面、資料庫、人臉辨識搜尋結果等）之利用條件和保護措施。

警務機關如向其他執法機關或公務機關揭露個人資料，則應與接收機關訂定資料分享協議。資料分享協議應至少約定下列事項：

- 資料揭露之合法授權依據；
- 所揭露個人資料之具體內容；
- 揭露之具體目的；
- 利用和再行傳輸（onward transfer）限制；
- 具體安全維護措施；
- 資料本地化儲存要求（如有）；
- 資料侵害應變程序；
- 保存期限和資料銷毀要求；
- 課責性措施，包括遵循狀況監測。

（八）資料保存

警務機關不得超出計畫目的之必要範圍保存個人資料。因此，警務機關應訂定並執行資料保存規程，針對人臉辨識系統之各組成部分作出規定。

1. 人臉資料庫

人臉資料庫應就其畫面入選標準作出明確規定。人臉辨識資料庫內畫面不符入選標準後，應立即從人臉資料庫中移除並銷毀。若其他計畫仍需保留該畫面，則應將該計畫之資料庫與人臉辨識系統相區隔。

人臉資料庫內畫面因上述原因而移除，原則應主動為之，無須當事人申請。

2. 標的畫面

警務機關應確保人臉辨識資料庫不得自動保存或以其他方式留存人臉辨識搜尋所用之標的畫面。

通常而言，若標的畫面經系統搜尋未見匹配，原則不應繼續留存。但若標的畫面構成證據，則應分開存放。

若標的畫面經系統搜尋發現匹配，則應依證據保存等相關規定保存。

3. 測試資料

為測試人臉辨識系統成效，可能需要將標的畫面保存較久時間。為測試目的保存標的畫面，應限於絕對必要範圍內，且測試完成後應立即將該等畫面刪除。

（九）資料安全

警務機關須依資料之敏感程度，採取適當安全措施保護個人資料安全。考量人臉資料之高度敏感性，其安全維護措施至少應包括：

- 以加密及其他數位保護工具，保護儲存中（in storage）和傳輸中（in transit）資料之安全。
- 確保紀錄和設備，包括伺服器、終端使用者裝置等僅於安全地點使用和儲存。
- 對人臉辨識軟體和資料庫之一切存取和使用行為保留日誌紀錄。
- 定期檢視和更新安全維護措施，以因應最新安全威脅。
- 以契約和資料分享協議確保參與計畫之第三方遵循資料安全之最佳實務。

為維護資料安全，警務機關可能亦須將人臉辨識計畫所蒐集或生成之個資儲存於加拿大境內。

（十）開放性、透明性與當事人近用權

應盡可能向個資當事人和一般民眾揭露個人資料蒐集之目的、資料利用或揭露之方式等。然而，對警務機關而言，並非總是適宜向當事人提供資料蒐集之完整資料（例如刑事偵查程序之偵查對象）。

通常而言，警務機關如將特定人臉畫面納入人臉資料庫，應通知相關個人，但通知將損害該畫面蒐集目的之達成者除外。該通知應說明：

- 將該畫面納入人臉資料庫之正當性標準；
- 該畫面從人臉資料庫中移除之條件；
- 所涉之個人資料銀行（personal information bank）。

同樣地，警務機關如在公共場所使用人臉辨識技術，應張貼公告，但公告將損害該畫面蒐集目的之達成者除外。該公告應：

- 張貼於所涉場所之明顯之處；
- 明確告知該場所使用人臉辨識技術；
- 提供可獲得人臉辨識計畫更多資訊之連結（例如，PIA 摘要之 QR code 或網路連結）。

警務機關應在人臉辨識計畫層面執行透明化措施，以增強民眾對人臉辨識計畫之瞭解與信任。警務機關應透過其官方網站以及其他適當管道，揭露下列資訊：

- 該機關使用人臉辨識之正式政策，包括人臉辨識技術使用情境及個人資料之利用方式。
- 以簡明語言說明該人臉辨識計畫之目的、人臉畫面來源、閾值選擇、預估執行期和一般作業方式等。
- PIA 摘要之連結。
- 該計畫準確性或偏見之測試結果，包括對測試方法之說明。
- 人臉辨識系統採購相關資訊，包括廠商資訊。
- 資料分享協議相關資訊。
- 利害關係人諮詢之結果或摘要。
- 計畫年度摘要，包括：
    - 上一年度執行之搜尋總數；
    - 計畫成效指標（例如：協助逮捕或判罪之使用）；
    - 關於人臉資料庫規模及族群構成之統計數據；
    - 該計畫之重要變更。

通常而言，個人有權存取並更正其個人資料，以及在特定情形下刪除其個人資料。警務機關應建立對該等請求之受理與回應機制，並應確保在法定時限內回應近用請求。

二、指引簡析

加拿大在聯邦層面，對公務機關和非公務機關分別以不同個資保護法律規範。公務機關適用 1985 年訂定的《隱私法（Privacy Act）》，而非公務機關則適用 2000 年訂定之《個人資訊保護和電子文件法（Personal Information Protection and Electronic Documents Act）》。此兩部法律之規範密度遠低於歐盟，且加拿大政府已數度提出修法草案[26]。此外，加拿大各省之隱私保護法規並不一致[27]。在尚無全面性法規框架的背景下，本指引以彙整最佳實務之方式，提供警用人臉辨識技術之隱私保護框架。

[26] 例如，加拿大政府分別於 2020 年和 2022 年提出 Digital Charter Implementation Act 草案，主張修正個人資訊保護和電子文件法，https://www.parl.ca/LegisInfo/en/bill/43-2/c-11 (accessed 30 September 2022)， https://www.parl.ca/legisinfo/en/bill/44-1/c-27 (accessed 30 September 2022)。

[27] 例如，魁北克省於 2021 年 9 月通過 An Act to modernize legislative provisions as regards the protection of personal information, SQ 2021，修正省級隱私保護法規，增訂生物辨識資料之特別規範，http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html (accessed 30 September 2022)。

第四章 各指引比較分析與我國公務機關個人資料保護建議

第一節 各指引比較分析

一、人臉辨識之技術面向

瞭解人臉辨識技術的各個作業步驟如何蒐集、處理和利用個人資料，是落實人臉辨識過程中個資保護之前提。因此，本研究對象之三份外國指引皆在展開具體法遵分析或實務作業指引前，首先以一定篇幅介紹人臉辨識之技術原理。

歐盟 EDPB 指引和加拿大 OPC 指引對人臉辨識技術之說明更加深入。EDPB 指引將「驗證」和「識別」列為人臉辨識之兩種基礎類型，並將「歸類」視為人臉辨識技術之進階運用類型[28]。在此基礎上，EDPB 指引說明人臉辨識技術有多樣化應用潛力，就「驗證」、「識別」兩類人臉辨識技術之實際應用分別舉例，並簡要分析對人臉辨識技術之「可靠性」與「準確性」議題，及其對個資當事人可能造成之風險，以強調人臉辨識技術使用過程中個資保護之重要性。加拿大 OPC 指引亦以「驗證」和「識別」視為人臉辨識之基礎態樣，明確關注「人臉識別」此一警方更為常用之技術類型，並對人臉辨識系統之主要組成部分逐一介紹其要點，以利使用該指引之警務人員能快速對人臉辨識系統有清晰瞭解。

英國警務學院指引聚焦於「以即時人臉識別搜尋觀察名單人員」此一具體使用情景，對其人臉辨識各作業步驟作簡要介紹。

歐盟 EDPB 和加拿大 OPC 指引皆以「強化人臉辨識技術使用過程中之資訊隱私保護」為主旨，是否對人臉辨識之技術面向作深入介紹，應係各指引發布機關依其指引之適用對象、主體範圍、內容深度、文體風格等因素衡酌判斷，並無優劣之分。如國發會未來擬針對人臉辨識相關個資保護議題提供指引或建議，或可以歐盟 EDPB 和加拿大 OPC 之指引為參考。

[28] EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (12 May 2022), para 17.

二、使用人臉辨識技術之適法性

（一） 基本權利保護

本研究對象之三份國外指引皆認同，人臉辨識須蒐集和利用高度人別辨識功能之個人資料，帶來對個人資訊隱私權益侵害之固有風險。三份國外指引並進一步援用憲法或人權相關法律，論及人臉辨識，特別是「人臉識別」作業，可能對人格尊嚴、平等權、言論自由、集會自由等基本權利造成之更深層之影響。

（二） 法律依據

依 LED 指令第 8 條，為執法目的運用個資，須以歐盟或會員國「法律」為依據。因此，EDPB 指引並未論及「當事人同意」等法律依據之適用條件，而是重點分析 LED 指令第 10 條特種個人資料運用之原則禁止及其例外。EDPB 強調，依例外條款運用特種個人資料應限於絕對必要範圍內，並採取適當措施保障個資當事人權利與自由。EDPB 指引附件 2 並就人臉辨識技術之採購，說明評估法律依據時之考量要素。

英國警務學院指引雖屬實務作業指引為重點，仍論及即時人臉識別之個資運用法律依據議題，要求警務機關在輔助警務文件層面和執行面，確認遵循英國 2018 年資料保護法第 35(5)條（對應歐盟 LED 指令第 10 條）之特種個人資料運用限制要求。

加拿大 OPC 指引並未使用「法律依據」之概念，然指出在人臉辨識運作的各個階段，例如演算法之訓練、人臉資料庫之設立、標的畫面之獲取與比對等，均須具備合法授權。且若警務機關使用外部人臉辨識服務，須確保其外部廠商有權蒐集和利用其服務所涉之個人資料。

（三） 資料正確性與人為介入

對於人臉辨識系統而言，資料之正確性有多重含義。一方面，因人臉辨識等人工智慧系統產出結果係對個人之「推測」，而非事實性

資訊，故需考量其「統計上之準確性（statistical accuracy）」[29]。統計上之準確性與人臉辨識系統之歧視和偏見風險密切相關。如不準確之辨識結果作為決策依據，則可能對個資當事人權益影響甚鉅，從而有人為介入之必要。另一方面，人臉辨識系統仍有個人資料保護法制通常意義上之「資料正確性」議題，例如人臉辨識資料庫中人臉畫面所附身分資訊錯誤等。

EDPB 指引於介紹人臉辨識在技術面向可能存在準確率不足及偏見問題後，於附件 2 人臉辨識技術採購實務指引之「部署後建議」部分，明確建議執法部門「確保對結果之人為介入和監督」。

英國警務學院指引將人臉辨識之偏見風險，與警務部門所負之公部門平等責任（PSED）相連結，要求警務機關在採購即時人臉識別系統之過程中，須評估演算法之整體準確度，以及其對不同族群的辨識效果。該指引並要求警務人員就人臉辨識執行平等影響評估（EIA），並持續監測人臉辨識系統及演算法之表現。

加拿大 OPC 指引則就訓練資料、演算法、人臉資料庫、標的畫面、人為審核等人臉辨識各個組成部分或作業步驟，分別分析影響其準確性之因素，並提出提升準確度、降低人臉辨識系統偏見之最佳實務做法。

（四） 目的限制原則

目的限制原則要求個人資料原則僅用於蒐集目的範圍內。對於人臉辨識系統而言，目的限制原則之遵循，可呈現於系統開發和辨識作業的各個階段。例如，人臉資料庫之構建、演算法之訓練，都可能涉及資料之目的外利用適法性。辨識完成後，輸入之畫面之留存及後續利用，亦可能有目的限制原則之適用。

歐盟 EDPB 指引之正文未特別就目的限制原則展開討論，然於附件 2 實務指引之前言中指出，開發/訓練人臉辨識工具係一獨立目的，

[29] UK ICO, Guidance on AI and Data Protection, What do we need to do to ensure lawfulness, fairness, and transparency in AI systems?, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ (accessed 30 September 2022).

如執法機關將其已掌握之個資用於人臉辨識演算法之開發/訓練，須具有適當法律依據，並評估其必要性與合比例性。

英國警務學院指引作為警務機關之實務作業指引，對於人臉辨識系統如何遵循目的限制原則未作特別說明。

加拿大 OPC 指引於「目的限制」一節指出警務機關必須確保個人資料僅用於其蒐集目的，並重點說明警務機關如何確保受委託之第三方不致將個人資料用於其他目的（例如人臉辨識廠商不會將所接收之標的畫面用作訓練資料、納入廠商自己的人臉資料庫等）。

（五） 資料最小化原則與儲存限制

資料最小化原則與儲存限制原則協助將人臉辨識對當事人權益之影響降至最低。

歐盟 EDPB 指引雖未針對此兩項原則作具體說明，然於當事人權利一節，強調人臉辨識之部署應遵循資料最小化要求，回應當事人近用權行使請求時，應落實資料最小化原則，避免不必要地運用更多生物特徵資料。該指引附件 1 將資料之儲存期限列入評估項目，而附件 2 之人臉辨識技術採購實務指引要求由專人負責落實人臉資料庫內資料、系統輸入資料之儲存期限。

英國警務學院指引要求警務機關於人臉辨識專案之「輔助政策文件」中，說明控管者資料保存與刪除政策，包括資料可能之保存期限。

加拿大 OPC 指引指出，警務機關不得超出計畫目的之必要範圍保存個人資料。因此，警務機關應就人臉資料庫內資料、標的畫面、測試資料等，分別訂定資料保存規程並予以執行。

（六） 告知義務與當事人權利

個資當事人對其個人資料享有查閱、更正、請求刪除等多種權利，而資料蒐集機關向個資當事人告知其資料蒐集、處理及利用之法定事項，使當事人知悉資料被利用之事實，乃當事人行使其權利之重要前提。

LED 指令就執法機關之告知義務，區分「至少應告知之資訊」與「特定情形下之進階資訊」。歐盟 EDPB 指引指出，在個資當事人不知情時蒐集其個資、個人資料蒐集後作進階運用、利用人臉辨識技術進行純自動化決策，皆屬須告知進階資訊之「特定情形」。EDPB 指引並認為，執法機關應尊重個資當事人權益，及時回應個資當事人之權利行使請求，且在回應過程中應落實資料最小化原則。

依英國警務學院指引，即時人臉識別之部署授權書中，應載明如何於人臉辨識畫面採集區域適當設置標誌，如何於部署地點和警方網站揭露個資運用相關資訊，以及如何回應個資當事人之權利行使請求等。

加拿大 OPC 指引認為，警務機關如將特定人臉畫面納入人臉資料庫，原則應通知相關個資當事人，如在公共場所使用人臉辨識技術，原則應張貼公告揭露相關資訊。警務機關並應在其官方網站揭露人臉辨識計畫之政策及作業說明，並建立當事人近用個資等請求之受理與回應機制。

三、人臉辨識技術之運作實務

（一） 資料保護之影響評估

全面評估人臉辨識所涉之個資蒐集、處理及利用是否合於法律規範、對個資當事人權益有何衝擊或風險、相關因應措施是否充分等，是落實個資當事人權益保護之有效方法。

歐盟 LED 指令第 27 條明定高風險個資運用作業應執行個資保護影響評估（DPIA）。EDPB 指引認為，因人臉辨識技術之性質、範圍、背景和目的可能造成自然人權利與自由之高風險，故在使用人臉辨識技術前，必須執行 DPIA，且須依 LED 指令第 28 條，就 DPIA 之剩餘風險諮詢主管機關。EDPB 並建議公開評估結果，以提升透明度，強化民眾信任。

英國警務學院之指引，警用即時人臉識別之輔助性政策文件，應包括依英國 2018 年資料保護法執行 DPIA 之要求。在執行面，警務

機關在人臉辨識系統部署前，須先完成 DPIA 等評估，並根據評估結果，判斷是否提出即時人臉識別部署申請。

加拿大 OPC 指引要求警務機關於人臉辨識計畫開始執行（試行）前、重大變更前，執行隱私影響評估（PIA）。執行 PIA 時，警務機關應諮詢隱私保護專家和利害關係人，識別對個資當事人、受影響社區、警務機關公信力等各方面之影響，評估人臉辨識應用之必要性、風險因應措施等。該指引並要求將人臉辨識技術年度稽核之結果記錄於 PIA，並建議公開揭露 PIA 之摘要。

（二） 人臉辨識之個資管理制度

人臉辨識技術實務運作過程中，可透過建置與落實個人資料管理制度，協助實現執行面之個人資料保護。

歐盟 EDPB 指引附件 2 要求執法機關於採購人臉辨識技術前，正式描述人臉辨識技術用例，識別所涉個人資料範圍、確立系統運作各項指標等。在已採購之人臉辨識技術部署前，製作使用者手冊、對使用者執行教育訓練等，以利使用者瞭解並遵循人臉辨識相關個資保護措施。於人臉辨識技術部署後，保留系統運作之日誌紀錄，建立資料侵害因應程序，於生物特徵資料遭侵害時，及時完成通知通報。

英國警務學院指引中，強調即時人臉識別技術部署之制度文件，要求警務首長針對即時人臉識別技術之使用訂定總體政策文件，明定該機關使用人臉辨識技術之各項基本原則。該指引並要求警務首長主責訂定與輔助性政策文件，規定人臉辨識系統作業之 SOP，遵循個資保護法規要求。

加拿大 OPC 指引從課責性角度，要求警務機關就人臉辨識系統訂定隱私管理制度（PMP），載明人臉辨識計畫所涉個人資料蒐集、利用、保存、揭露條件和方法之政策和程序，並要求警務機關指定專人負責隱私制度管理與執行，確實記錄人臉辨識軟體使用和個資利用狀況，建立事故和問題之通報制度，並定期舉行教育訓練。

（三） 資料安全措施

人臉辨識所用之人臉模板等生物特徵資料具高度人別辨識功能，一旦遭到竊取或洩漏等，當事人將難以變更外洩之資料，除可能嚴重影響當事人之隱私權益外，並可能進一步影響以該等生物特徵資料作為密碼或密鑰之安全性。因此，人臉辨識系統之個資安全措施，應較一般個人資料更為謹慎。

歐盟 EDPB 指引要求執法機關於使用人臉辨識技術時，依 LED 指令第 29 條，格外注意個資運用之安全性，包括對生物辨識模板採取保護措施、確保自身及委外廠商之安全性符合 ISO/IEC 24745 等相關國際標準。該指引並提示留意人臉辨識系統特有之安全風險。

英國警務學院指引要求警務首長針對即時人臉識別技術之使用訂定總體政策文件，包括管理即時人臉識別系統及其內含資料之安全性。且人臉辨識部署申請書中，亦應詳述部署之細部安排，包括安全維護措施。

加拿大 OPC 指引要求警務機關依資料之敏感程度，採取適當安全措施保護個人資料安全，對於警用人臉辨識系統，應至少採取資料加密、裝置之實體防護、軟體使用日誌紀錄等安全維護措施。

（四） 人臉辨識技術之採購與委外監督

公務機關部署之人臉辨識系統，可能自外部廠商採購；且系統運作過程中，亦可能由廠商提供協助。因此，確保廠商提供之系統符合當事人權益保護與資料安全標準，監督廠商於提供服務過程中遵守個資蒐集、處理及利用之規範，是人臉辨識技術使用中的重要問題。

歐盟 EDPB 指引指出，若執法機關之人臉辨識系統係委託第三方服務提供者運用個人資料，則更應確保資料運用活動之安全性。附件 2 係針對人臉辨識技術採購之實務指引，要求執法機關於採購人臉辨識系統之前，應執行 DPIA，且其對個資當事人權利與自由風險之評估，應包含受託運用者/複受託運用者相關之風險。

英國警務學院指引聚焦於警務機關內部治理面與執行面之作為，未對人臉辨識技術採購與委外廠商監督議題作針對性說明。

加拿大 OPC 指引認為，警務機關應於採購過程中，透過契約確保提供人臉辨識軟體和服務之廠商遵守人臉辨識計畫之要求，包括訓練資料之適法性、不得將警方提供資料挪作他用、廠商應接受警務機關稽核等。警務機關並應採行管理上、技術上或實體管控措施，確保廠商遵守個人資料之目的限制。

第二節 我國公務機關使用人臉辨識技術之個人資料保護建議

由本章前一節比較分析可知，人臉辨識作業涉及輸入畫面（標的畫面）採集、與人臉資料庫比對、比對結果之利用等不同步驟，且其系統之建置與導入，可能涉及人臉資料庫建置、演算法訓練/調適、系統測試、系統部署、運作監測等不同階段，各個步驟、階段所涉之個資內容與來源，蒐集、處理或利用之法律依據，當事人權益風險等不盡相同，落實個資保護之實務措施亦有差異。因此，我國公務機關於評估人臉辨識技術之個人資料保護措施時，可參酌三份國外指引，採行相關之個資保護最佳實務做法。

（一）臉紋、指紋等生物特徵資料雖非我國個資法所稱之特種個人資料，然如司法院釋字第 603 號解釋所指出，指紋等生物特徵，因具有人各不同、終身不變之特質，一旦與個人身分連結，即屬具備高度人別辨識功能之個人資料。因此，生物特徵資料之保護應與其敏感性相當，而不宜僅以一般個人資料性質看待。

（二）個資蒐集、處理及利用之法律依據方面，生物特徵資料依我國個人資料保護法制尚非特種個人資料，故公務機關透過人臉辨識蒐集、處理或於蒐集目的內利用個資，須判斷是否具備我國個資法第 15 條之合法事由。此外，如公務機關利用現有資料建置人臉辨識技術裝置或資料庫，例如訓練演算法、測試系統成效、構建人臉資料庫等，應檢視是否與資料蒐集之特定目的相

符。如屬蒐集之特定目的外利用，則應遵循我國個資法第 16 條但書之個資目的外利用規範。

（三）資料正確性方面，人臉辨識系統如統計上的準確性不足，可能導致歧視與偏見，對個資當事人權益影響甚鉅。我國個資法雖未明文要求防範對個資當事人之偏見，但要求保有個人資料之機關維護個人資料正確性，且個人資料之蒐集、處理或利用應以尊重當事人權益之方式為之。因此，公務機關宜在人臉辨識技術設計和採購階段，即採取降低歧視風險之措施，並於人臉辨識系統部署後，持續監測歧視或偏見之情事，且定期評估人臉辨識系統或演算法等之準確性。若公務機關使用人臉辨識技術，執行對個人權益有重大影響之作業，宜設立人為介入進行審查之機制。降低人臉辨識演算法偏見風險之相關措施例如：

1. 依所採用技術方案的性質、範圍、背景與目的，以及對個人權利與自由之影響，適當設定認定資料符合之閾值；
2. 使用高品質、較新之原始畫面；
3. 確保演算法訓練資料、人臉資料庫中各類當事人之適當代表性；
4. 對人為介入機制之審查人員執行適當訓練，避免完全依賴系統辨識結果；
5. 建立辨識準確率監測及通報機制。

（四）資料最小化與儲存限制方面，輸入系統用以辨識之資料、人臉資料庫內資料、訓練資料等，皆宜遵守資料最小化及儲存限制要求，以利將人臉辨識對當事人權益之影響降至最低。因此，公務機關宜就用以比對之人臉畫面訂定合理明確之保存期限，並就人臉辨識資料庫內影像畫面等訂定明確、客觀之選擇標準，並建立有效清查機制，主動或依當事人申請，及時將不符標準之影像畫面自資料庫中移除。

（五）資料安全方面，人臉辨識資料之外洩可能對個資當事人權益影響甚鉅，且人臉辨識系統之安全可能受資料之儲存與傳輸、設

備因素、管理因素等多方面影響。公務機關使用人臉辨識技術時，應依個資法及其施行細則規定，指定專人辦理安全維護事項，採取技術上及組織上之安全維護措施。相關安全維護措施例如：

1. 使用人臉辨識系統須經使用者身分驗證並具備適當權限；
2. 建立自動日誌機制，自動記錄系統各項使用、存取、變更等活動；
3. 對所儲存和傳輸之資料予以加密；
4. 確保人臉辨識技術裝置、資料庫等各組成部分之實體安全。

（六）個資保護影響評估方面，個資保護影響評估是識別、分析並因應人臉辨識系統所涉個資保護風險之有效方式，而個資保護影響評估中風險識別之全面性及因應措施之妥適性，將直接影響人臉辨識系統之個資保護效果，公務機關於使用人臉辨識技術之前，宜先行評估擬採用技術必要性及合比例性、對當事人權益之風險等因素，並規劃適當之風險控管或緩解措施；並宜於重大變更前、在人臉辨識技術使用過程中定期繼續評估。公務機關執行該評估時，宜徵詢機關內外關係人（例如個資當事人、員工、受託者）之意見；且宜將評估結果與決策作成紀錄，並適當公開評估之主要發現或結論。個資保護影響評估之相關考量因素例如：

1. 評估人臉辨識技術與欲達成之目的間之必要性及合比例性：
   (1) 所欲達成之目的及其與社會公益之關聯；
   (2) 採用該技術之預期成效及其與對當事人權益影響之均衡性；
   (3) 對當事人權益影響較小之措施為何不足以實現欲達成之目的。
2. 評估人臉辨識技術對當事人之權利及自由可能產生之風險：

(1)所採用之技術方案對當事人資訊隱私權之影響程度及發生侵害事故可能性，包括蒐集、處理及利用資料是否確有必要、當事人對其個人資料使用狀況之知悉與控制、資料安全風險、資料委託第三方蒐集、處理或利用之風險等；

(2)所採用之技術方案對當事人平等權之影響程度及發生侵害事故可能性，包括辨識結果之準確性等；

(3)所採用之技術方案對當事人人格尊嚴、表現自由等基本權之影響程度及發生侵害事故可能性。

（七）委外監督方面，實務中公務機關採購外部廠商之人臉辨識軟體或服務已屬常態，而所採購之軟體或服務品質、外部廠商受託後對個資之作為，皆可能影響個資當事人權益。依我國個資法規定，委託蒐集、處理或利用個人資料者，其行為視同委託機關之行為，個資法施行細則並要求委託機關對受託機關為適當監督。因此，公務機關如委託第三方協助建置或運作人臉辨識技術裝置或資料庫，該第三方因此所為之個資蒐集、處理或利用，將視同公務機關自身之行為，且公務機關應依個資法及其施行細則，對該第三方之行為進行監督。相關監督措施例如：

1. 受託者採取資料安全維護措施與人臉辨識資料之敏感性相當；
2. 受託者不得將人臉辨識資料於委託機關預定目的外利用，例如，所接收用於辨識之人臉影像用作演算法訓練資料、納入受託者自行建置之人臉資料庫等；
3. 受託者如提供人臉辨識軟體或演算法，其開發過程所涉個資蒐集、處理及利用皆應符合法律規範，且採取適當措施降低軟體或演算法之歧視風險。

第五章 結論

綜合前文之比較分析，就人臉辨識技術所涉之重要個資保護議題，考量我國現行個資法之規範，本研究建議我國公務機關於使用人臉辨識技術時，從下列方面落實個人資料保護。

一、 個資蒐集、處理及利用之法律依據方面，公務機關透過人臉辨識蒐集、處理或於蒐集目的內利用個資，須判斷是否具備我國個資法第 15 條之合法事由。此外，如公務機關利用現有資料建置人臉辨識技術裝置或資料庫，應評估是否屬特定目的外利用及是否符合個資法第 16 條但書規範。

二、 資料正確性方面，公務機關宜在人臉辨識技術設計和採購階段，即採取降低歧視風險之措施，並於人臉辨識系統部署後，持續監測歧視或偏見之情事，定期評估人臉辨識系統或演算法等之準確性。若公務機關使用人臉辨識技術，執行對個人權益有重大影響之作業，宜設立人為介入進行審查之機制。

三、 資料最小化與儲存限制方面，輸入系統用以辨識之資料、人臉資料庫內資料、訓練資料等，皆宜遵守資料最小化及儲存限制要求，訂定合理明確之保存期限，並建立有效清查機制，以利將人臉辨識對當事人權益之影響降至最低。

四、 資料安全方面，公務機關使用人臉辨識技術時，宜依個資法及其施行細則規定，依人臉辨識技術之風險程度，採取技術上及組織上之安全維護措施。

五、 個資保護影響評估方面，公務機關於使用人臉辨識技術之前，宜先行評估擬採用技術之適法性、必要性及合比例性、對當事人權益之風險等因素，並規劃適當之風險控管或緩解措施；並宜於重大變更前、在人臉辨識技術使用過程中定期繼續評估。

六、 委外監督方面，公務機關如委託第三方協助建置或運作人臉辨識技術裝置或資料庫，該第三方因此所為之個資蒐集、處理或利用，應視同公務機關自身之行為，且公務機關應依個資法及其施行細則，對該第三方之行為進行監督。

參考文獻

法律和立法草案

1. EU Directive (E 有 U) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
2. EU Charter of Fundamental Rights.
3. European Convention on Human Rights.
4. Quebec, An Act to modernize legislative provisions as regards the protection of personal information, SQ 2021, http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html (accessed 30 September 2022).
5. UK Data Protection Act 2018.
6. UK Protection of Freedoms Act 2012.
7. UK Equality Act 2010.
8. European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (21.4.2021), COM(2021) 206 final.
9. Government of Canada, Digital Charter Implementation Act 2020, https://www.parl.ca/LegisInfo/en/bill/43-2/c-11 (accessed 30 September 2022).

10. Government of Canada, Digital Charter Implementation Act 2022, https://www.parl.ca/legisinfo/en/bill/44-1/c-27 (accessed 30 September 2022).

其他參考資源

11. College of Policing, About Us, https://www.college.police.uk/about (accessed 30 September 2022).

12. European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en (accessed 30 September 2022).

13. European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (accessed 30 September 2022).

14. European Data Protection Board & European Data Protection Supervisor, EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf (accessed 30 September 2022).

15. European Data Protection Supervisor, Assessing the necessity of measures that limit the fundament al right to the protection of personal data: A toolkit (11.4.2017), https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf (accessed 30 September 2022).

16. European Data Protection Supervisor, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019), https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf (accessed 30 September 2022).

17. Nasr et al., Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning (2018, revised 2020). https://arxiv.org/pdf/1812.00910.pdf (accessed 25 October 2022).

18. Office of the Privacy Commissioner of Canada, Clearview AI ordered to comply with recommendations to stop collecting, sharing images, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/ (accessed 30 September 2022).

19. Office of the Privacy Commissioner of Canada, Privacy Guidance on Facial Recognition for Police Agencies, https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/ (accessed 30 September 2022).

20. Szegedy et al., Intriguing Properties of Neural Network (2013, revised2014), https://arxiv.org/pdf/1312.6199.pdf (accessed 25 October 2022).

21. UK Information Commissioner's Office, Monetary Penalty Notice, https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf (accessed 30 September 2022).

22. UK College of Policing, Live facial recognition- Authorised Professional Practice, https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition (accessed 30 September 2022).

23. UK Biometrics and Surveillance Camera Commissioner, Surveillance camera code of practice: self assessment tool, https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool (accessed 30 September 2022).

24. UK Information Commissioner's Office, Guidance on AI and Data Protection, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ (accessed 30 September 2022).

25. Vivek Agarwal, The Frictionless Enterprise (26 December 2018), Forbes, https://www.forbes.com/sites/forbestechcouncil/2018/12/26/the-frictionless-enterprise/?sh=51386d183ba0 (accessed 25 October 2022).

26. 李宗翰, 不只是要零接觸，更要做到零摩擦（2021.07.02），iTHome, https://www.ithome.com.tw/voice/145419（最後瀏覽日：2022 年 10 月 25 日）。

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/葉奇鑫計畫主持 -- 初版.
-- 臺北市 : 國發會, 民 111.10

面：表，公分

編號：(111)010.0901

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

隱私權

575.81

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

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

出版機關：國家發展委員會

電話：02-23165300

地址：臺北市寶慶路 3 號

網址：http://www.ndc.gov.tw/

出版年月：中華民國 111 年 10 月

版次：初版

刷次：第 1 刷

編號：(111) 010.0901 (平裝)