National Chengchi University
國立政治大學

moda 數位發展部
Ministry of Digital Affairs

政府機關臉部辨識運用研析
-以數位權利與原則為框架

計畫主持人：曾憲立 / 臺南大學行政管理學系 副教授

協同主持人：戴豪君 / 世新大學法律學院法律學系 副教授

許慧瑩 / 中原大學法學院財經法律學系 助理教授

顧　　問：朱斌妤 / 政治大學公共行政學系 特聘教授

本研究成果不代表委託單位立場

National Chengchi University
國立政治大學

moda 數位發展部
Ministry of Digital Affairs

目錄
Content

01

研究背景

- 研究背景及目標
- 文獻回顧

研究背景

- 因應落實推動「公民與政治權利國際公約」及「經濟社會文化權利國際公約」相關工作，政府機關運用人工智慧臉部辨識技術（Facial Recognition Technology）之個資隱私保護議題，引發各界的高度關注與討論。

- 歐盟「數位權利和原則」（Digital Rights and Principles），以民眾的數位轉型為目標，涵蓋以民眾權益為數位轉型的核心、團結與涵容、確保選擇自由、鼓勵數位參與、個人賦權與增進安全、永續環境。

研究目標

- 以政府機關對於臉部辨識技術運用為例，研擬個資隱私保護相關規範建議。
- 蒐整歐洲數位權利和原則之內容，了解其數位權利和原則的發展與落實，並為我國數位權利和原則之建議參考。

人工智慧風險與治理

- 2023年9月13日歐盟執委會主席von der Leyen發表國情咨文，將人工智慧對社會帶來的滅絕風險，與大規模流行病和核子戰爭並列為相同規模之風險

AI三大支柱	主要目標	實施與應用範例
安全門檻（Guardrails）	確保AI以以人為本、透明和負責任的方式發展	提出歐盟人工智慧法草案—全球首個全面支持創新的AI法律
治理（Governance）	建立單一治理系統，與全球合作夥伴合作，並以全球性方式理解AI在社會中的影響	建議建立一個類似IPCC（氣候變化政府間專門委員會）之全球小組，專門研究AI的風險和益處
引導創新（Guiding Innovation）	在負責任的方式下引導創新，並與開發和部署AI的人進行開放對話	歐洲已成為超級運算的領導者，將開放高性能運算資源給AI初創公司，藉以訓練其人工智慧模型

資料來源： https://ec.europa.eu/commission/presscorner/detail/ov/speech_23_4426

臉部生物特徵技術運用

種類	處理模式	應用
辨識 (identification)	一對多的比對處理模式	指以辨識特定自然人身分為目的，透過系統將生物特徵資料轉特徵值，進而與資料庫中之生物特徵值相互比對，從而辨識特定自然人之身分
確認與驗證 (verification/authentication)	一對一的比對處理模式	指將個人的生物特徵資料轉特徵值與先前提供的生物特徵值，透過系統進行一對一驗證（包括鑑別），驗證自然人的身分
區別與分類 (categorization/segregation)	非以辨識或確認個人為目的，只要區分與分類	指依據自然人的生物特徵資料（例如：性別、年齡等），將其歸納分屬特定類別
情緒認知 (emotional recognition)		指用於識別或根據自然人的生物特徵資料推論其情緒或意圖

我國臉部辨識運用案例

機關	用途	種類
彰化縣政府	員工考勤	為一對多的比對
新北市地政局 板橋地政事務所	土地登記申請之身分核符	為一對一的比對
勞動部桃竹苗分署	訓練學員之出缺席紀錄	為一對多的比對
新北市立圖書館	用於借還書	為一對一的比對
高雄捷運	廣告推播	區別與分類 不涉及識別

我國臉部辨識判決案例

- **宜蘭地方法院110年度簡字第749號刑事判決（偽造文書）**
  被告假冒他人身分至戶政補辦身分證，嗣因查驗身分經戶籍員提供之同意書下簽章同意由電腦輔助人臉辨識，而後發現被告偽造他人身分。

- **臺北高等行政法院109年度訴字第912號判決（戶政）**
  抗告人因認戶籍法並未賦予主管機關得強制人民換發具有數位身分識別功能之eID權限，但若不換發將使其權利受損。

- **臺南地方法院109年度交字第200號判決（交通裁決）**
  即使外貌屬於公開可見的個人生物特徵資訊，亦非不屬於隱私權保障範圍 。

我國對臉部生物特徵識別資料之規制

個資法

- 1995年《電腦處理個人資料保護法》
  將特徵、指紋等做為個人資料的例示
- 2010年修訂《個人資料保護法》
  將生物特徵識別資料仍屬一般個資
- 2023年修訂《個人資料保護法》
  生物特徵識別資料仍同2010年之規定未做修正

個資法以外之命令或指引

- 個人生物特徵識別資料蒐集管理及運用辦法
- 執行外來人口入出國(境)辨識個人生物特徵作業要點
- 勞動基準法施行細則
- 校園使用生物特徵辨識技術個人資料保護指引

歐盟對臉部生物特徵識別資料之規制

1995年《個人資料保護指令》

生物特徵資料
屬於一般個人資料

第29條工作小組意見書

2003年第80號
《有關生物特徵的工作文件》

2012年第192號
《有關於線上或連網服務應用臉部辨識技術意見書》

2012年第193號
《有關生物特徵技術發展意見書》

2016年《一般資料保護規則》(GDPR)

將生物特徵資料列為敏感性特種個資

原則上不得蒐集、處理及利用，除非有第9(2)條之規定

歐洲個人資料保護委員會指引(EDPB)

2020年《歐盟使用影像裝置處理（process）個人資料指引》

2022年《執法領域臉部辨識技術運用指引》

人工智慧法

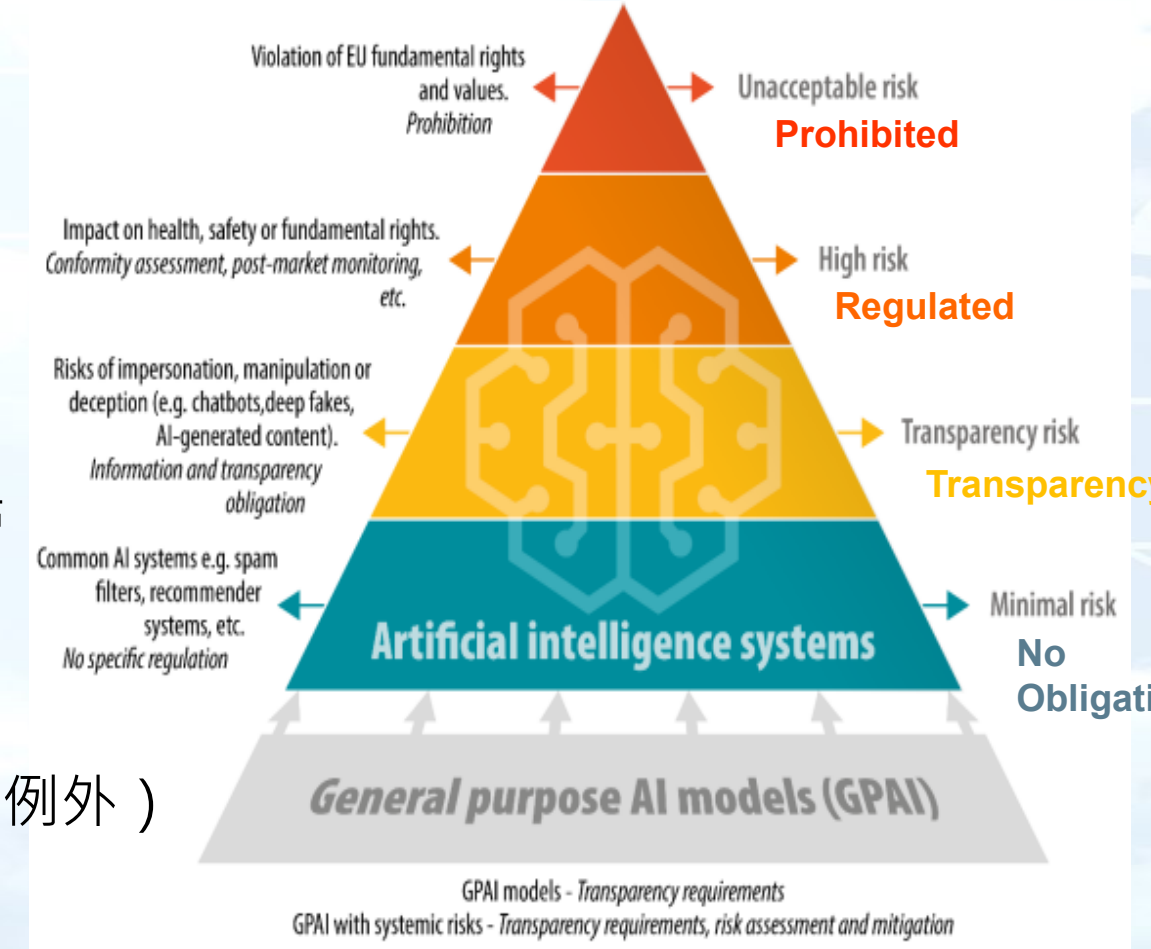
將運用生物特徵資料的人工智慧系統那管

從使用者與情境及例外可使用之用途分類，進一步做風險分級

要求依風險檢視技術應用之合法性、必要性，及與風險層級相對應之措施

歐盟人工智慧法 (AI Act)

- 為全球第一部規範人工智慧的法律
- 透過透明、問責與人類監督作為實現「歐洲數位權利和原則」的實例
- 以用途可能涉及的風險層級作為監管分級的理論基礎
  - 臉部生物特徵依使用者與情境
    - 不被接受的風險（原則禁止使用除具例外）
    - 高風險層級



資料來源：European Parliament, Artificial intelligence act Briefing, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

歐盟人工智慧法 (AI Act)

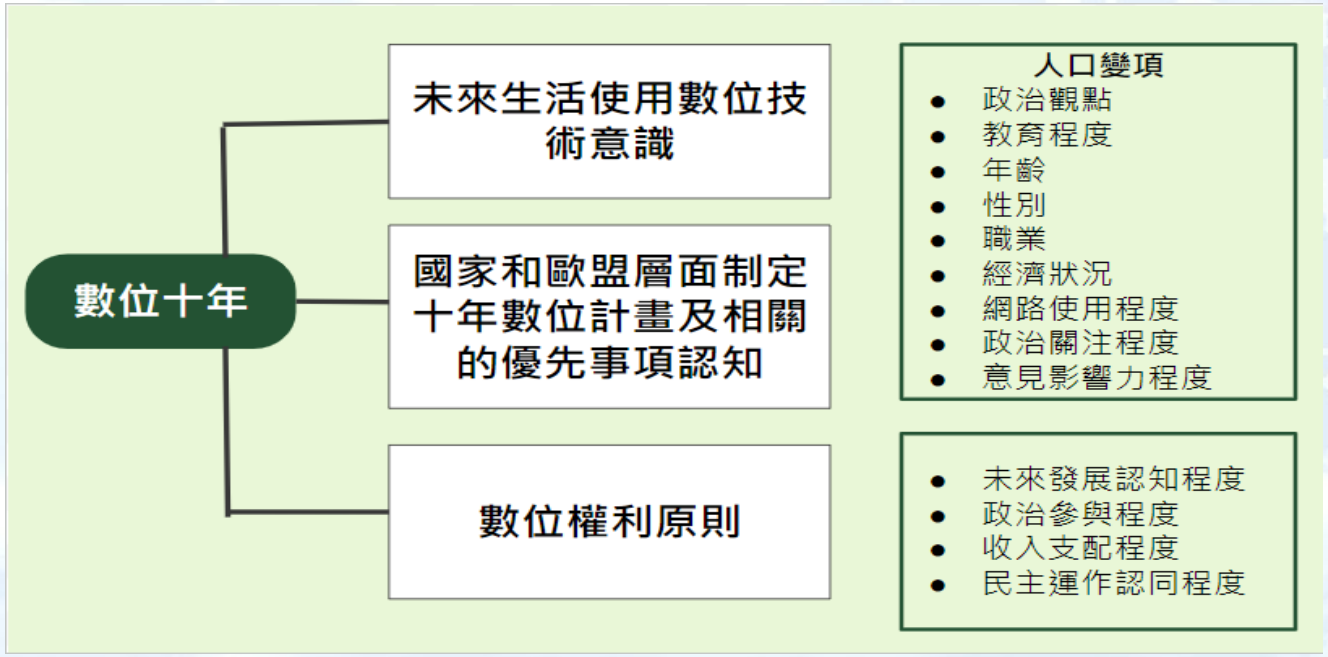
- 依風險檢視技術應用之合法性、必要性，及與風險層級相對應之因應措施
- 製造商與使用者對應前述要求的義務，製造者與使用者還要在系統採用後，持續進行上市後的監督，在特殊嚴重事件的資訊分享，與市場監控
- 要求公務機關（排除司法調查與犯罪偵查、邊境控管、移民難民或其他機關）使用高風險的AI系統，應先行至歐盟資料庫登錄
  - 風險控管制度的建置與落實
  - 訓練、驗證與測試資料與資料治理
  - 系統上市或使用前技術文件之整備
  - 系統運行紀錄之自動保存
  - 系統資訊之透明與提供
  - 人類行為的監督與介入
  - 系統運行的準確性、穩定性及資訊安全

National Chengchi University
國立政治大學

政府機關臉部辨識運用研析
—以數位權利與原則為框架

- 數位經濟與社會指標（Digital Economy and Society Index, DESI）
  - 人力資本面向
  - 數位基礎建設面向
  - 數位採行面向
  - 數位公共服務面向

- 數位十年調查（Digital Decade）



政府機關臉部辨識運用研析
—以數位權利與原則為框架

愛沙尼亞

- 人力資本 - 數位技能（Digital Skills）
  - 截至2021年為止，年齡在16-74歲之間的人至少有基本數位技能的比例為56%，略高於歐盟平均水準（歐盟平均水準為54% ）
- 數位基礎設施
  - 5G涵蓋率低以及固網寬頻速度（Fixed Broadband of Speed）超過100 Mbps的普及率低。
- 數位採行 - 企業數位化（Digitization of Business）
  - 使用雲端運算的企業比例為51%，明顯高於歐盟平均水準（34%）
- 數位公共服務
  - 愛沙尼亞在這一領域為全球領先國家，具有顯著貢獻，使其數位公共服務對使用者帳戶更加友善和便利，便於公民和企業使用。

National Chengchi University
國立政治大學

政府機關臉部辨識運用研析
—以數位權利與原則為框架

芬蘭

- 人力資本 - 數位技能（Digital Skills）
  - 在2021年，芬蘭16-74歲人口中至少具備基本數位技能的比例為79%，非常接近歐盟數位十年目標80%的水準，遠高於歐盟平均水準（歐盟平均水準為54% ）
- 數位基礎設施
  - 該國整體5G涵蓋率表現出色，但固網寬頻普及率略低於歐盟平均水準，VHCN網路涵蓋率稍低於歐盟平均水準的73%
- 數位採行 - 企業數位化（Digitization of Business）
  - 使用雲端運算的企業比例為66% ，明顯高於歐盟平均水準（34%）
- 數位公共服務
  - 在政府機構與公眾間的線上互動表現突出，97%網路使用者使用電子化政府服務。在電子健康領域90分，高於歐盟平均水準72分，並有My Kanta電子醫療記錄服務、正完成的新數位身分系統。

02

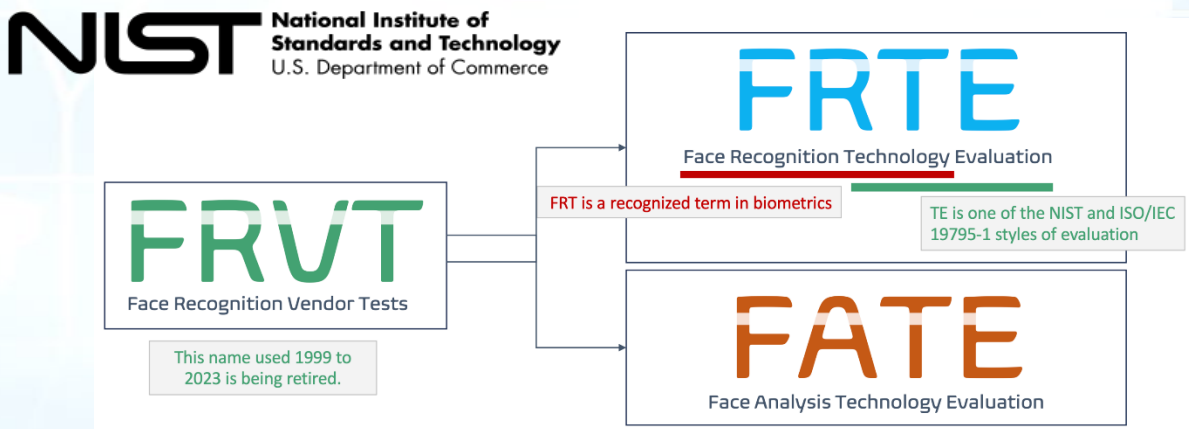
調查分析

- 訪談
- 問卷

機關與技術單位訪談

主要訪談題綱

- 機關採購系統時之共通需求
- 採購系統時之個資法法規遵循流程與介面、合法合規之設計及具備個資隱私保護、資安能力之佐證例
- 維護資安的作為
- 系統建置後之維護



問卷題目來源

- **數位十年調查（Digital Decade）**
  - 數位權利與原則相關之題目

- **臺灣社會變遷基本調查計畫**
  - 2024年第八期第五次調查 -「數位社會」問卷
  - AI影響之題目

問卷問法調整

1. 詢問方式改為兩階段詢問

QB8.1. How well do you think digital rights and principles are applied in (OUR COUNTRY) for…? :-Getting an affordable high-speed internet connection for everyone in the EU

Q3. 請問您**同不同意**，民眾應該有可以負擔(得起)的高速網路？
Q3_1. 就您的理解，請問您認為台灣在「民眾應該有可以負擔的高速網路」方面，**落實的好不好**？

問卷問法調整

2. 調整一題多問的內容

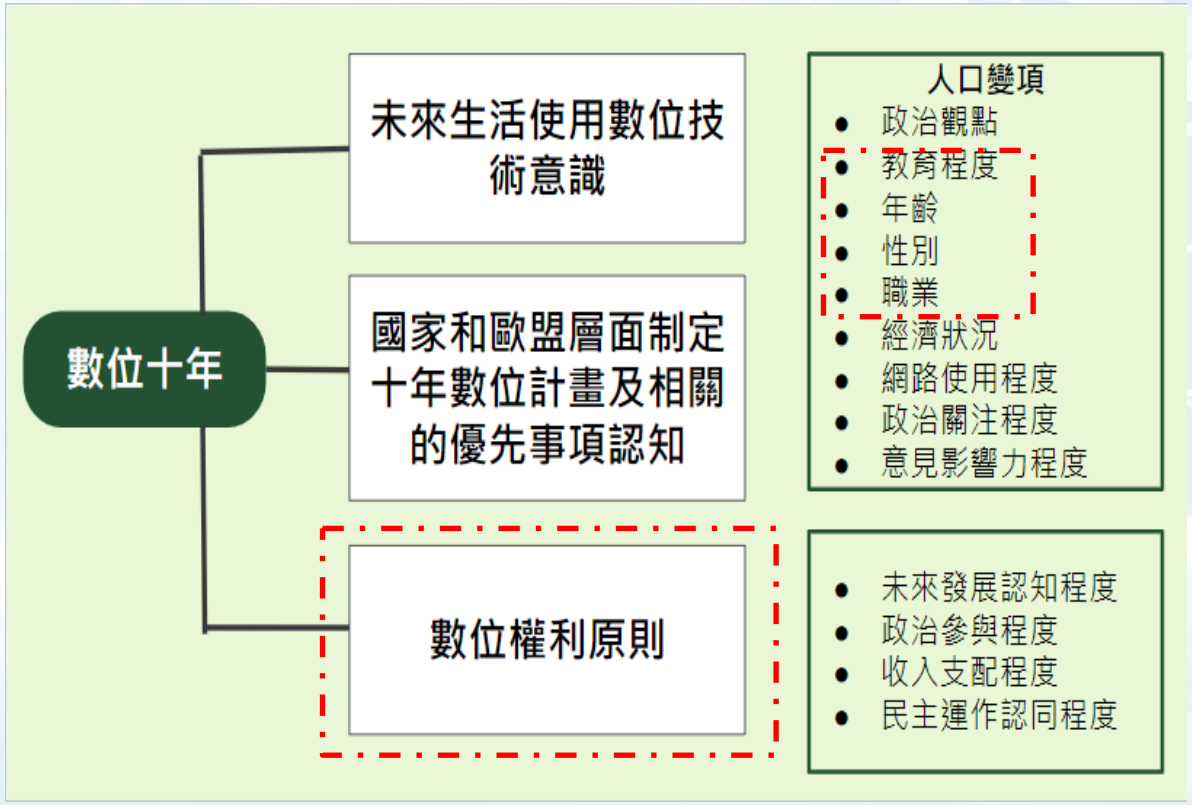
QB 8.2. How well do you think digital rights and principles are applied in (OUR COUNTRY) for…? :-Getting basic and advanced digital education, training and skills

Q4. 請問您同不同意，民眾應有接受到基礎與進階的數位教育的權利？

問卷問法調整

3. 調整調查方法

歐盟於2023年3月間以**面訪**方式進行了數位十年調查（Digital Decade），調查國家共計26國，共分三個構面，有41題目。



調查結果

項次	題目	同意分數/標準差	落實分數/標準差	差分
1	民眾應該有可以負擔(得起)的高速網路	4.23 (0.73)	3.13 (1.16)	1.1
2	民眾應有接受到基礎與進階的數位教育	4.40 (0.66)	2.87 (1.19)	1.53
3	民眾應得到公平且健康的工作環境，包含工作與生活的平衡	4.48 (0.66)	2.80 (1.21)	1.68
4	民眾可以容易地在網路上獲取關鍵公共服務	4.33 (0.79)	3.36 (1.18)	0.97
5	民眾可以自主決定要不要在網路上與AI互動	4.00 (1.06)	2.89 (1.26)	1.11
6	民眾可以獲得可信賴、多元或多語系的數位環境	4.05 (1.01)	2.96 (1.21)	1.09
7	民眾可以在線上論壇、社群媒體獲得更多言論和資訊自由	3.98 (1.14)	3.51 (1.31)	0.47
8	民眾可以獲得安全和尊重個人隱私的數位服務	4.45 (0.89)	2.83 (1.30)	1.62
9	民眾在線上的通訊(文字及語音)保密，資料不被外洩	4.28 (1.13)	2.33 (1.24)	1.95
10	民眾擁有個人資料的控制權，可以決定個人資料的使用方式與分享對象	4.52 (0.73)	3.00 (1.28)	1.52
11	應該要保障兒童和年輕人安全的數位環境和內容	4.70 (0.60)	2.61 (1.26)	2.09
	平均	4.31	2.93	1.37

調查結果

	平均數	標準差
Q14.請問您同不同意，人工智慧應該立法管制？	4.50	0.789
Q15.請問您同不同意，人工智慧服務上線前應該取得合格認證標章？	4.60	0.702
Q16.請問您同不同意，(應該要)管制網路大型數位平台或社群媒體，如Facebook、YouTube等？	3.90	1.287
Q17.請問您同不同意，使用科技執法？	3.46	1.430
Q19.請問您擔不擔心，人工智慧的產出結果可能造成偏見或歧視，例如不利於特定族群？	2.45	1.218
Q20.請問您擔不擔心，人工智慧可能造成錯誤或虛假消息的氾濫？	1.73	0.941
Q21.請問您擔不擔心，人工智慧可能影響您的工作機會？	2.78	1.454
Q22.請問您擔不擔心，人工智慧可能作為犯罪工具，例如詐騙、駭客攻擊？	1.36	0.725
Q23.請問您擔不擔心，人工智慧可能被少數人掌控而成為特權工具？	1.67	1.013
Q24.請問您擔不擔心，人工智慧可能使社會不平等現象更嚴重，例如貧富不均？	2.17	1.230

調查結果

題號	題目	選項	加權後	
			樣本數	百分比
Q18	有關人工智慧對社會可能的影響，您最同意以下哪一個說法？	整體來說一定對社會不利	26	2.1
		雖然有些好處，整體來說仍對社會不利	160	13.0
		雖然有些風險，整體來說仍對社會有利	851	69.4
		整體來說一定對社會有利	146	11.9
		拒答/不知道	45	3.6
		總數	1,227	100.0

03

結論與建議

臉部辨識指引技術面規範建議

採購

- 應要求廠商檢附具臉部辨識技術之第三方測試、認證之證明等。

使用期間

•1. 應提供系統無法運作或民眾選擇不使用臉部辨識技術時之其他選項，並建置相關備援機制。

•2. 應具備防止偏誤發生之資料正確與品質確認機制，及偏誤發生所應採行之因應流程與步驟。

•3. 應依系統運作之目的與設定，建置與落實系統運作之紀錄機制，以監測系統運作之穩定性與準確性，並於超過允許之偏誤率時由人為介入。

•4. 應建置與落實使用臉部辨識技術風險等級對應之安全維護措施、資料外洩侵害應變及通報程序、定期進行符合性評估與稽核，並於必要時採用隱私強化技術，以提高其安全性。

•5. 應要求廠商對系統運行持續進行監測與監督，並定期更新技術之監測、預防或矯正措施，以確保符合當時科技或專業水準可合理期待之安全性。

結論

01

民眾大多同意歐洲數位權利與原則內容；且對國內目前落實情形不甚滿意

02

民眾對科技態度樂觀,69.4%民眾認為新興科技「雖然有些風險，整體來說仍對社會有利」；11.9%認為「整體來說一定對社會有利」

03

公部門臉部辨識技術應用以差勤為主，以影像轉存特徵值進行辨識，無法反向重現臉部影像，系統封閉與落地且不以遠端維護，應可有效保護資料不外洩

04

非差勤之其他用途臉部辨識(分類分群、情緒認知等)之商業模式仍待開發

建議

- 建立公部門臉部辨識使用原則和例外排除的指引
- 發展臉部辨識技術使用稽核與行政處理流程
- 重視數位權利與原則，建立我國規範與政策連結
- 考量科技發展，深化民眾數位素養教育與公部門應用
- 持續精進調查方式與擴大調查對象

簡報結束
感謝聆聽 敬請指教

本研究成果不代表委託單位立場