

MODA-DODS -112-001（委託研析報告）

**政府機關臉部辨識運用研析-以數位
權利與原則為框架
（成果報告）**

**數位發展部編印
中華民國 113 年 7 月**

MODA-DODS -112-001（委託研析報告）

**政府機關臉部辨識運用研析-以數位
權利與原則為框架
（成果報告）**

受委託單位：數位治理研究中心

計畫主持人：曾憲立

協同主持人：戴豪君、許慧瑩

研究顧問：朱斌妤

研究助理：李奐澐、許皓婷、吳潔琳、李柏均

數位發展部編印

中華民國 113 年 7 月

目次

目次.....	I
表次.....	III
圖次.....	V
摘要.....	VII
Abstract.....	IX
第一章 緒論.....	1
第一節 研究背景.....	1
第二節 研究目的.....	2
第二章 文獻回顧.....	3
第一節 歐盟相關研究與調查.....	3
第二節 臉部辨識的法律規制與應用現況.....	10
第三章 調查分析方法.....	31
第一節 研究設計.....	31
第二節 臉部辨識利害關係人訪談.....	32
第三節 數位權利與原則問卷調查.....	35
第四章 調查分析發現.....	37
第一節 臉部辨識技術部分之指引建議.....	37
第二節 臉部辨識利害關係人訪談.....	38
第三節 數位權利與原則問卷調查.....	41
第五章 結論與政策建議	55
第一節 研究結論.....	55
第二節 政策建議.....	56
參考文獻.....	59
附錄.....	65
附錄一、歐盟數位十年問卷摘錄.....	65
附錄二、PEW 研究中心 AI 問卷摘錄	67
附錄三、本計畫數位權利與原則問卷.....	69
附錄四、數位權利與原則問卷調查結果.....	75

表次

表 1：歐盟《AI Act》生物特徵技術應用風險分級與因應措施對應表	14
表 2：臉部辨識應用於公共服務一覽	17
表 3：臺灣臉部辨識技術相關的判例	19
表 4：研究設計摘要.....	31
表 5：訪談對象.....	32
表 6：訪問成功樣本之代表性檢定-性別	42
表 7：訪問成功樣本之代表性檢定-年齡	42
表 8：訪問成功樣本之代表性檢定-教育程度	43
表 9：訪問成功樣本之代表性檢定-戶籍縣市	44
表 10：電話接觸狀況統計表	45
表 11：受訪者戶籍地與居住地分布.....	46
表 12：受訪者學歷與職業分布	47
表 13：受訪者年齡分布.....	48
表 14：數位權利項目同意-落實平均數與差分	49
表 15：受訪者對人工智慧管制的看法	50
表 16：受訪者對人工智慧應用的看法	51
表 17：受訪者對人工智慧應用影響的看法	52

圖次

圖 1：歐洲數位權利和原則項目	4
圖 2：數位十年調查問卷架構	6
圖 3：歐盟人工智慧法風險級別結構	13

摘要

政府應用資通訊科技提供各類數位服務已是近年國際上的趨勢，然而在服務提供的時候，如何以民眾的權益為數位轉型的核心，是各國政府的關鍵議題，對此，歐盟提出「數位權利和原則」(Digital Rights and Principles)，提供兼顧個人賦權與增進數位使用安全的六大目標。我國自 2021 年起執行「服務型智慧政府 2.0 推動計畫」(2021-2024 年)，隨資通訊科技的快速發展，以及國際社會對個人隱私的重視，部分資通訊科技，如臉部辨識 (Facial Recognition)、人工智慧 (Artificial Intelligence)，觸及個人資料保護等多個議題，更需要政府重視。

本計畫整理歐盟對「數位權利和原則」及數位經濟與社會指標 (Digital Economy and Society Index, DESI) 的調查研究，進行我國民眾數位權利與原則和人工智慧意見態度的電話調查；並對臉部辨識如何應用在公共服務做應用單位的訪談；最終透過專家座談收攏意見，研究結果發現：(1) 民眾在數位權利與原則的觀念與歐盟相近，而對我國數位權利與原則的落實有高度期待；(2) 近八成民眾認為人工智慧「雖然有些風險，整體來說仍對社會有利」及「整體來說一定對社會有利」，但若細究人工智慧對社會、經濟等層面的影響，民眾對人工智慧可能造成錯誤或虛假消息的氾濫、詐騙高度擔心。(3) 公部門應用臉部辨識以差勤應用為主，職員影像拍照後轉存特徵值進行辨識，特徵值無法反向重現人臉，且伺服器保存地端，不以遠端操作方式維護，應可有效保護資料不外洩；(4) 若非差勤使用，而將辨識應用於身形、人數、性別等，亦為影像辨識之應用，但對於商業模式的應用情境較差，多為公部門特定機關的應用，如高鐵對月台候車人數的估計。

本計畫認為中期來說應建立公部門臉部辨識使用原則和例外排除的指引，並發展臉部辨識使用稽核與行政處理流程；而對於數位權利與原則的長期目標，應建立我國相關規範，並與現行政策做連結，以進一步落實，其中又因人工智慧的快速發展，需要深化民眾數位素養教育與公部門應用，最後，應持續精進對數位權利和原則的調查方式與擴大調查對象。

關鍵字：臉部辨識、數位權利與原則、數位政府、智慧服務

Abstract

In recent years, the application of information and communication technologies (ICTs) by governments to provide various digital services has become an international trend. However, when offering these services, how to prioritize citizens' rights as the core of digital transformation has become a critical issue for governments worldwide. In response, the European Union introduced the "Digital Rights and Principles," outlining six key goals that balance individual empowerment and the enhancement of digital safety. Since 2021, our country has been implementing the "Service-Oriented Smart Government 2.0 Promotion Plan" (2021-2024) . With the rapid development of ICT and the international community's emphasis on personal privacy, some ICTs, such as facial recognition and Artificial Intelligence (AI), involve multiple issues related to personal data protection, which require heightened government attention.

This project compiles research from the European Union on "Digital Rights and Principles" and the Digital Economy and Society Index (DESI). It conducts telephone surveys to measure public opinion on digital rights and principles, and artificial intelligence in our country. Additionally, it includes interviews with units applying facial recognition in public services. Finally, expert discussions are held to consolidate opinions. The research findings reveal:

1. Public awareness of digital rights and principles is similar to that of the EU, and there are high expectations for the implementation of these rights and principles in our country.
2. Nearly 80% of the public believes that artificial intelligence, despite some risks, is overall beneficial to society, or certainly beneficial. However, when examining the impact of AI on social and economic aspects, the public is highly concerned about the potential proliferation of errors, fake news, and fraud.
3. In the public sector, facial recognition is primarily used for attendance purposes. After capturing employee images, feature values are extracted for recognition. These feature values cannot be reverse-engineered to reconstruct the face, and the server is maintained locally, not remotely, effectively protecting the data from leakage.
4. Besides attendance, facial recognition can also be applied to body shape, number of people, and gender identification. However, its commercial application scenarios are limited, mainly used by specific public sector agencies, such as high-speed rail for estimating the number of people waiting on platforms.

This project suggests that in the medium-term, principles and guidelines for the use of facial recognition by public sectors, including exceptions, should be established. Additionally, it recommends developing audit and administrative procedures for the use of facial recognition. For the long-term goals, digital rights and principles, relevant regulations should be established in our country and linked with existing policies for further implementation. Given the rapid development of artificial intelligence, it is necessary to enhance public digital literacy education and public sector applications. Finally, the methods for investigating digital rights and principles should be continuously refined and the scope of the survey should be expanded.

Keywords: facial recognition, Digital Rights and Principles, digital government, smart services

第一章 緒論

第一節 研究背景

歐盟提出「歐洲數位權利和原則」(European 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、團結與包容、確保選擇自由、鼓勵數位參與、個人賦權與增進安全、永續環境等六大面向。該原則同時闡述政府、企業和其他組織在數位環境中應遵守的責任，進而保護數位環境中的資訊安全和隱私，並確保數位技術的公平和公正使用。經濟合作暨發展組織(Organisation for Economic Cooperation and Development, OECD)也於《Embracing Innovation in Government: Global Trends 2023》報告中，明確指出世界各國政府面對環境不確定性的多重考驗，例如氣候變遷(Climate Change)、數位顛覆(Digital Disruption)以及信任低落(Low Levels of Trust)等問題，亟需思考創新方式，以面對各個面向的轉型需求。

我國自2021年起執行「服務型智慧政府2.0推動計畫」(2021-2024年)，以民眾需求為出發點，深化智慧政府各項作為，在多個領域導入政府創新數位服務，包含發展跨域一站式整合服務(如MyData、公司登記一站式線上申辦等)、並打造多元協作環境(如精進政府入口網使用流程、落實公民網路意見多元參與管道等)。近年在強調數位政府服務上，除持續精進提供兼顧效率和品質的重要效益，及增進透明和開放的施政目標外。隨資通訊科技的快速發展，以及國際社會對個人隱私的重視，部分資通訊科技，如臉部辨識(Facial Recognition)，觸及個人資料保護的法律議題，更需要政府重視。我國有必要以「數位權利和原則」等國際重要發展方向，檢視政府以創新方式提供公共服務、增進民眾福祉、發展資訊及產業生態系、推動數位轉型、及兼顧永續環境等多元目標的執行與落實情形。

同時，因應我國落實推動「公民與政治權利國際公約」及「經濟社會文化權利國際公約」(兩公約)相關工作。2022年度第三次國家報告國際審查結論性意見第85點(人權公約施行監督聯盟，2022)，提出「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，應訂定及落實防止政府機關及第三方濫用的保障措施」，建議我國政府機關應注意運用臉部辨識技術之相關隱私議題。綜合上述，本計畫依據國際發展與國內需求，對下一階段服務型智慧政府重點計畫議題中，有關新興科技應用在數位權利的落實與保護，提供政府推動數位治理政策評估與推展參考，協助周延與落實我國數位治理政策，引領數位政府推展優質且創新的公共服務。

第二節 研究目的

延續前述研究背景，本計畫名稱為「政府機關臉部辨識運用研析-以數位權利與原則為框架」，研究目的有下列三點：

1. 了解歐盟數位權利與原則及國際相關規範，對新興科技涉及民眾隱私、資料利用等議題之影響。
2. 以文獻回顧與訪談方式了解我國機關單位使用臉部辨識提供公共服務之情形，並研擬臉部辨識技術之指引建議。
3. 以文獻回顧與家戶電話調查方式，了解數位權利和原則在我國的落實情形，並提出相應之政策建議。

具體來說，本計畫參考歐盟數位權利與原則、聯合國公民與政治權利國際公約（第 17 條有關隱私權之保障）、歐盟人工智慧法（**Artificial Intelligence Act**，以下簡稱《**AI Act**》）等，對新興科技（臉部辨識與人工智慧）涉及民眾隱私、資料利用等議題，藉由文獻回顧、深度訪談、電話調查、專家座談等方式，產出可供我國數位權利原則之建議方向，以了解並供後續追蹤我國數位權利和原則的推動及落實情形，並據此與國際接軌及相互對照，以供政府單位導入新興科技與研擬下一階段數位政府計畫時參考。

第二章 文獻回顧

第一節 歐盟相關研究與調查

一、數位權利和原則（European Digital Rights and Principles）

歐盟提出「歐洲數位權利和原則」（European Digital Rights and Principles）以民眾的數位轉型為目標，涵蓋六大面向，並闡述政府、企業和其他組織在數位環境中應遵守的責任，進而保護數位環境中的資訊安全和隱私，並確保數位技術的公平和公正使用（參見圖 1），以下分別敘述六個面向的重點。

（一）以民眾權益為數位轉型的核心（People at the Centre）

根據 European Commission（2022）發布的數位權利與原則資訊手冊指出約有四成歐洲人並不知悉如言論自由、隱私或非歧視等自身權利在線上參與時也必須受到重視。因此數位轉型服務除了造福並改善歐盟生活的所有人，使參與者能夠追求自身理想，該服務同時須保護人民的基本權利，確保數位參與者的使用安全，使線上和線下的權利行使皆受到尊重與保障。

（二）支持團結與包容（Solidarity and Inclusion）

對於使用者不應有所限縮，無論是何等條件，民眾應都能在服務中享有自身權利，強調科技應促進團結而非製造衝突。主要針對網路連接能力、數位教育培訓和技能、公平的工作條件及數位公共服務等做為本面向的行動方針。

（三）確保線上選擇自由（Freedom of Choice Online）

每個人在參與線上環境的過程中都該被賦予應有的權利，包含與人工智慧、演算法互動在內，透過行使權利，要求提高透明度並盡可能確保系統符合倫理規範，線上參與者應得到授權與賦能，才能免於非法以及不利於自身數位能力條件的威脅。此外，選擇的自由亦包含參與者得以根據客觀、透明和具有根據的訊息，選擇服務內容、選擇的同時也應確保人人具備競爭和創新的能力。

（四）鼓勵數位公共空間參與（Participation）

使用社群媒體的多數人希望了解自身的資料在使用過程中如何被應用與處理。故數位技術得以做為激發參與的方式，藉由參與各個層級的過程，了解自身使用之服務用途和途徑，掌控自身的資料將有助於多元的公共辯論和民主參與，反映文化和語言的多樣性。在上述條件下，則應建立起能夠保護參與者並免於有害且不實資訊的數位環境。

(五) 個人賦權與增進安全 (Safety and Security)

根據 European Commission (2022) 發布的數位權利與原則資訊手冊指出，2019 年一半的網路使用者會因為安全性的問題而限縮了在網路上的活動。而數位環境之建立應具備安全性與可靠性，表示所有年齡層的用戶，都應該被賦權並受到保障，數位原則在此基礎上將承諾人民、企業和公共服務皆為保護範圍，對於試圖破壞線上環境之安全性與完整性等行為亦須採取抵制行動。

(六) 增進數位未來之永續 (Sustainability)

European Commission (2022) 發布的數位權利與原則資訊手冊中指出八成歐洲人期望強制數位設備製造商對數位設備之修繕更容易。數位轉型的同時也應將綠色轉型納入考量，當數位產品提供對應服務，在設計、生產和處理過程中須避免能源消耗等負面效果，減少環境與社會影響。

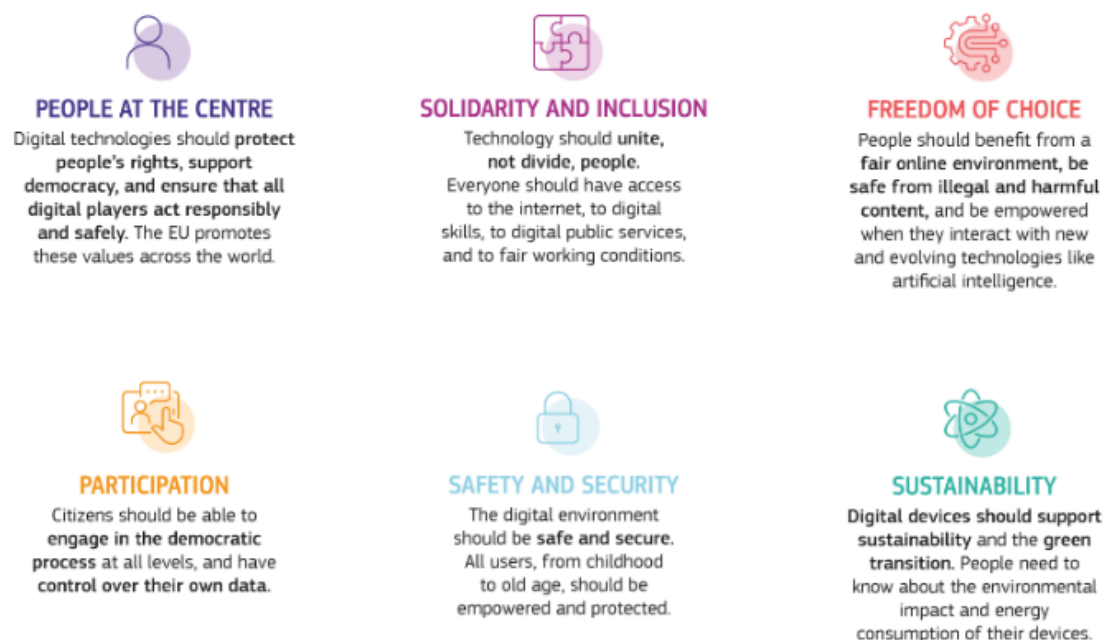


圖 1：歐洲數位權利和原則項目

圖片來源：<https://digital-strategy.ec.europa.eu/en/policies/digital-principles>。

二、 數位經濟與社會指標 (Digital Economy and Society Index, DESI)

歐盟在「數位經濟與社會指標」(Digital Economy and Society Index) 2022 年的報告中對人力資本 (Human Capital)、數位基礎建設 (Digital Infrastructures)、數位技術集合 (Integration of Digital Technology)、數位公共服務 (Digital Public Services) 等四大面向加以調查，以了解歐盟會員國在各面向的表現，據以檢視各會員國在數位權利和原則的落實情形。

(一) 人力資本面向

詢問包含數位技能指標、使用網際網路、內容創作技能、辨別不實資訊等項目。數位經濟與社會指標報告認為數位技能現階段對於各項機構依賴性和重要性提升，因此做為勞動力來源的員工亦需具備適應不同技能變化並持續發展技能創新與保持競爭力。其調查內容又以數位技能衡量、數位內容創作技能、資訊通訊科技專業人員、資訊通訊科技培訓、和資訊通訊科技畢業生為主。

(二) 數位基礎建設面向

詢問包含寬頻連接與半導體等項目。數位經濟與社會指標報告認為：為了使數位服務能夠充分的應用於日常生活，該服務須具備一定性能、安全性和可持續性的數位連接基礎設施，並結合光纖技術連接固網與無線系統，穩定點對點的連接設施。調查指標又以寬頻相關連接與使用、半導體技術為主。

(三) 數位採行面向

詢問包含數位化程度、科技採行程度、雲端運算、大數據、人工智慧、電子商務等項目。數位經濟與社會指標報告認為：數位技術能夠讓企業在競爭市場中獲得優勢，透過先進技術與電子商務之整合，改善該服務和產品，進而達到擴展市場的目標。除了對於資料須具備處理能力外，亦得滿足安全與保障基本權利，透過基礎設施以及創新數位技術的運用延伸至各項服務項目。調查指標又以中小型企業的數位化程度、電子資訊分享 (Electronic Information Sharing)、社群媒體、大數據、雲端運算、人工智慧、電子發票、電子商務營業額、線上跨區域銷售等項目為主。

(四) 數位公共服務面向

詢問包括數位政府使用者、數位服務項目、開放資料、數位身分認證、透明等項目。數位經濟與社會指標報告認為：富有效能的數位政府在處理政府與政府之間 (G2G) 和政府與企業之間 (G2B) 的服務上，能提供兼顧效率及降低成本的重要效益，以及增進透明和開放的施政目標。換句話說，政府以創新方式提供公共服務、增進民眾福祉、發展資訊及產業生態系、推動數位轉型，及兼顧環境永續已是全球共識。

數位公共服務項目的調查結果發現：各項評估項目分數與排名和數位經濟與社會指數 (DESI) 指標呈正相關，愛沙尼亞、芬蘭、馬爾他、荷蘭等，在各項服務項目皆具有較高的得分與領先地位，數位經濟和數位社會發展程度亦優於其他歐洲國家；反之羅馬尼亞、希臘、保加利亞和斯洛伐克等國家各項評估得分較低，數位發展程度較落後於其他歐洲國家。

三、 數位十年調查（Digital Decade）

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，共分三個層面，有 41 道題目，如圖 2，其中有 15 題和數位權利與原則相關，例如：（1）讓歐盟每個人都能負擔得起的高速網路連接、（2）獲得基本和進階數位教育、培訓和技能、（3）在數位環境中獲得公平且健康的工作條件，包含工作和生活平衡、（4）輕鬆獲取歐盟內所有線上關鍵公共服務、（5）獲得有效的自主線上選擇，包含人工智慧互動（如聊天機器人、數位助手）等，本計畫另摘錄部分題目於附錄一。

調查結果顯示：受訪者對於基本權利，如言論自由、隱私和非歧視等面向，在不同環境中皆需受同等尊重的意識權利，凸顯了提高數位權利意識的重要性，以及確保透過多元管道讓民眾理解他們的基本權利適用於線上和線下的必要性，調查也發現超過半數（57%）的歐洲人知悉在線上與線下皆適用之權利。

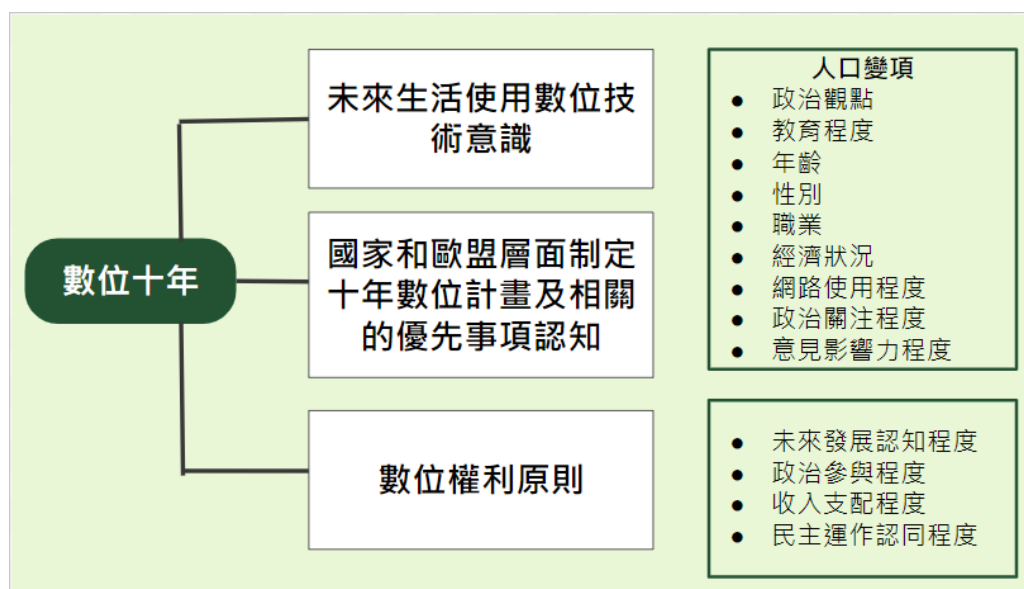


圖 2：數位十年調查問卷架構

資料來源：本計畫繪製。

值得注意的是，僅有一半（50%）的歐洲人認為數位權利在歐洲得到了良好的保護，而超過三分之一（36%）的人認為歐盟在數位環境中未能充分保護他們的權利，且仍有超過十分之一（11%）的受訪者表示並不知道歐洲做了什麼數位權利保護的相關措施（問卷答項：不知情）。調查同樣發現在國家層面上存在明顯的差異，在 16 個歐盟成員國中，超過一半的受訪者認可歐盟在線上環境中保護他們的權利，包含愛爾蘭（69%）、芬蘭（67%）、馬爾他（65%）以及丹麥、盧森堡、波蘭（三國都是 64%），而希臘（32%）、法國（39%）以及西班牙、保加利亞、斯洛伐克（三國都是 42%）等國家則反之。

在數位環境中獲得集會和結社自由的數位權利與原則，及線上表達和資訊自由方面等權利、數位教育培訓與技能、安全和尊重隱私的數位技術、獲取關鍵公共服務、高速網路連接、可信賴和多元的數位環境、公平和健康的工作條件、線上隱私與環境影響和能源消耗的正確資訊等 10 個面向當中，皆有超過半數的受訪者認為在上述情境中權利得以實施並獲得保障。但對於確保兒童和年輕人的安全數位環境、保護個人資料及減少數位技術對環境和社會的負面影響等方面則低於半數表示滿意，以下以分別說明愛沙尼亞與芬蘭兩個會員國為例分別說明調查結果。

(一) 愛沙尼亞

1、數位技能 (Digital Skills)

愛沙尼亞截至 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%，而歐盟平均水準為 54%，資料顯示愛沙尼亞略高於歐盟平均水準，對於發展資訊與通信科技 (Information and Communication Technology, 以下簡稱為 ICT) 的目標有顯著貢獻，在總就業人數中，擁有 ICT 專業技能的比例為 6.6%，遠高於歐盟平均水準 4.6%。再者 ICT 專家中的女性比例為 24.5%，相比歐盟平均水準 18.9%，為歐盟各國家比例最高，顯示愛沙尼亞的女性在 ICT 專業領域占比較高。此外，鑑於愛沙尼亞的 ICT 畢業生比例較高 (2021 年為 10.1%)，在未來可能逐年成長，但提供 ICT 培訓的企業比例卻低於歐盟平均水準，對此近五年該國提供 ICT 培訓的企業比例和歐盟平均水準之間的差距有所縮減。結合上述結果該國主要仍需加強改善基本數位技能的措施，例如鼓勵雇主在工作時間內幫助員工提升技能和進行再培訓等方式強化整體基礎。

2、數位基礎設施 (Digital Infrastructure)

在網路設備相關連接方面，愛沙尼亞較為不足，主要原因為 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。而超高容量網路 (Very High Capacity Network 以下簡稱為 VHCN) 和光纖到戶 (Fiber To The Premises, 以下簡稱為 FTTP) 涵蓋率則持續穩定增長，兩者皆達到 79%，遠高於歐盟平均水準 (VHCN 為 73%，FTTP 為 56%)。因此該國將繼續投資於在鄉村地區建設 VHCN 網路，並得到了歐盟資金的支持。

同時，愛沙尼亞還是歐洲量子通信基礎設施 (The European Quantum Communication Infrastructure Initiative to Build a Pan-European Quantum Infrastructure) 倡議的一員，致力於構建泛歐洲的量子基礎設施，並參與北歐 - 愛沙尼亞量子運算電子基礎設施探索計畫 (NordIQEst)，對歐盟實現數位十年目標做出了重要貢獻。該國應特別採取措施以促進高速網路規格 (Gigabit) 與 5G 連接性的擴展，並繼續進行關於量子運算的發展，加強協調和合作，促進整個歐盟內的量子社區建設。

3、企業數位化 (Digitization of Business)

2021 年，愛沙尼亞使用雲端運算的企業比例為 51%，明顯高於歐盟平均水準（34%），而使用人工智慧和大數據的企業比例在 2021 年和 2020 年分別卻低於歐盟平均水準。至 2022 年，至少具有基本數位化程度的中小企業比例為 67%，也略低於歐盟平均水準。該國目前的商業生態系統包含許多創新和快速增長的初創企業以及規模較大的企業，個別推動著該國的現代化發展。應加快在企業數數位化領域的拓展，尤其是增加企業對先進數位技術的應用與持續支持中小企業使用數位技術，提高競爭力和持續性。

4、公共服務的數位化（Digitalization of Public Services）

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。愛沙尼亞也在電子治理學院（Estonian E-Governance Academy）的國際發展合作計畫中，與其他國家分享了其經驗和方法，在愛沙尼亞的國家數位 2020 年議程下，進一步推進數位公共服務仍是首要目標之一。該國持續實施其政策，特別為投資創新數位解決方案，加速創新數位解決方案在所有公共服務中的應用；此外也解決查閱健康資料的普及性，使所有人（包括殘障人士）都能檢視前述資料，並確保所有相關入口網站能夠從行動通訊設備中使用。

（二）芬蘭

1、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（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（54%）。在全體就業人口中，ICT 專業領域在總就業人口中的比例（2022 年為 7.6%）遠高於歐盟數位十年目標和 2022 年的歐盟平均水準（4.6%）。此外，在 ICT 專家中，女性的比例為 23.8%，遠高於歐盟平均水準（18.9%）。而在教育方面，ICT 畢業生的比例為 7.6%，有 40%的公司為員工提供 ICT 培訓。近年來，新識字計畫 2020-2023（The New Literacies Programme）和 LUMA 中心推動了 ICT、媒體素養和程式設計等方面的能力發展，推動對象亦包含兒童在內。綜合上述發展，應持續在數位技能領域實施其政策，不斷優化與實施已宣布的政策，並進一步促進 ICT 專業領域和人數。

2、數位基礎設施（Digital Infrastructure）

該國在整體 5G 涵蓋率方面表現出色，人口密集區的涵蓋率 95%，且高品質的 3.4-3.8 GHz 頻段涵蓋率為 84%。然而，固網寬頻的普及率略低於歐盟平均水準，有 49%的家庭擁有 100 Mbps 的固網寬頻，只有 3.1%的家庭擁有 1 Gbps 的固網寬頻，遠低於歐盟平均水準的 13.8%。而芬蘭的超高容量網路（VHCN）網路涵蓋率為 71%，稍低於歐盟平均水準的 73%。由於人口密度低，該國的鄉村地區經常存在涵蓋盲點。

芬蘭為歐洲高效能運算聯合協會（European High-Performance Computing Joint Undertaking, EuroHPC JU）的成員之一，位於芬蘭的 EuroHPC 中心正在開發三臺預先規模（Pre-Exascale）的超級電腦之一 Lumi。而該國位在歐洲量子運算和半導體的領先地位，IQM 量子運算公司在芬蘭投資建設了歐洲首座專門用於量子運算的半導體生產設施，並且量子電腦 HELMI 已經連接到了超級電腦 Lumi。此外，亦參與了關於微電子和通信技術的歐洲共同利益重要項目（Important Projects of Common European Interest, IPCEI），著重關注電信和晶圓基板（Wafer Substrates）。綜合上述發展，該國應持續實施其政策，並拓展超高容量網路涵蓋率，將固網寬頻提供到鄉村地區，包括在全國範圍內部署光纖到戶的網際網路；而在半導體和量子運算領域則需協助歐盟發展與革新。

3、企業數位化（Digitization of Business）

芬蘭的中小企業在 2022 年已達到至少基礎數位化程度的比例為 89.5%，略低於數位十年目標（90%），但遠高於歐盟平均水準（69%）。先進技術推動為芬蘭企業的核心，截至 2021 年 66% 的企業使用雲端運算技術，16% 的企業將人工智慧技術整合到其營運工作中，而在 2020 年已有 22% 的企業使用大數據。而至 2022 年，芬蘭仍持續資助支持企業，特別是中小企業，該國特別著重發展新創企業以及規模擴大的企業系統，且將數位技能整合到經濟體系中，即為大學、專門的政府機構和企業之間的合作，如目前所推動的 6G Bridge 計畫。綜合上述發展，該國應持續提供投資和激勵，擴大企業使用如人工智慧和大數據領域等先進的數位技術。

4、公共服務的數位化（Digitalization of Public Services）

芬蘭在政府機構與公眾之間的線上互動方面表現突出，資料顯示有 97% 的芬蘭網路使用者使用電子化的政府服務。而該國在提供線上服務方面也表現得非常出色，2022 年便在前幾年開展的計畫中持續進展，並逐漸升級電子政府服務，將其服務納入數位與人口資料服務機構的管理中。在電子健康領域，芬蘭的得分為 90，高於歐盟平均水準 72，且朝著達成數位十年目標 100 的方向前進。領域發展突出的其中一項原因為 My Kanta 電子醫療記錄服務，民眾可以查詢自身的線上電子文件；此外，該國目前也正完成一個新的數位身分系統，該系統也將做為電子身分認證與信賴服務規則（Electronic IDentification, Authentication and Trust Services, eIDAS）中所指出的身分認證工具。而該國的政府資料開放網站（National Open Data Portal）則繼續以開放形式為企業和公眾提供資料，故芬蘭在網路安全方面亦持續提高其應對能力，並計畫在 2022 年至 2026 年間投入 2.3 億歐元的資金。

第二節 臉部辨識的法律規制與應用現況

隨著具攝錄影功能之裝置或設備被大量廣泛的使用，得以隨時蒐集影像資料並做後續的利用。部分國家的司法偵查與維安利用影像裝置，採用臉部辨識技術掃描人群，以辨識可能的威脅。科技公司亦使用臉部辨識技術提供新型態的服務，例如 Facebook 利用臉部辨識技術，將用戶同意之檔案照片與新照片中的臉孔進行自動掃描與比對，用以標註照片中的人物；Apple 使用臉部辨識技術進行智慧裝置解鎖。

近期，人們開始注意到攝錄影功能對隱私可能造成衝擊與威脅外，當影像結合影像辨識技術可能更具侵犯性（例如：生物辨識技術），如何使影像技術維持於匿名狀態與保護隱私，越顯困難。影像除可能被用來做為資料當事人無合理期待的其他用途，多媒體與科技技術結合影像裝置的使用，可能引發影像資料目的外利用或是誤用的風險。Scott 等人（2019）指出影像與臉部辨識技術除對隱私可能造成威脅之外，因臉部辨識、比對、分析等軟體可能因為年齡、性別、種族等而有運作上的差異或因影像裝置故障等，還可能引起偏差歧見（Biased）等問題，以及基於不同人口資料的演算法，臉部辨識的偏差，可能因此更深化社會的偏見。

（一）我國法律對臉部辨識技術的規制

我國對於臉部生物特徵識別資料的規制，大抵可分為個人資料保護法制及個人資料法制以外之其他規制。我國個人資料法制主要參酌 1995 年《歐盟資料保護指令》（Data Protection Directive），其並未特別將生物特徵識別資料而另為規範，而是將之歸類於非特種個資的範疇。依第四條就個人資料的定義，未將生物特徵識別資料特別提出，而僅是例示為個人資料之一。從我國個人資料保護法的歷史沿革觀之，其實臺灣早於在 1995 年的《電腦處理個人資料保護法》，即將生物特徵識別資料納入個人資料的保護範疇。按 1995 年《電腦處理個人資料保護法》第三條所規定之個人資料的定義，係指足資識別個人之資料即為個人資料；並將特徵、指紋等做為個人資料的例示。雖然法條並無明文生物特徵資料為所指之個人資料，但從定義與例示中可以推導出，指紋屬生物特徵識別資料之一，因此，生物特徵識別資料實已屬個人資料保護的範疇。

在 1995 年後《個人資料保護法》經兩次修訂，2010 年《個人資料保護法》的修訂，將適用主體從公務機關與特定行業之非公務機關擴展至所有實體一體適用，並將個人資料分為敏感性個人資料（或稱為特種個資），及非敏感性個人資料（或稱一般個資）。此次修法對於個人資料的定義，繼續沿用 1995 年《電腦處理個人資料保護法》的規定，僅將個人資料做更加詳細的規範，說明個人資料指得以直接或間接方式識別該個人之資料，並無太大的改變。是以，生物特徵識別資料在我國仍屬於一般個資，適用一般個資蒐集、處理、利用之相關規定。《個人資料保護法》如前所述主要參酌 1995 年《歐盟資料保護指令》，對於個人資料

的定義與生物特徵識別資料的屬性，並未改變；2023 年《個人資料保護法》的修訂，亦僅增修個人資料保護機關與加強對於非公務機關的罰則，對於個人資料的定義與生物特徵識別資料的屬性，仍同 2010 年《個人資料保護法》之相關規定。

即便如此，我國於個人資料法制以外，尚有其他對於生物特徵識別資料的規制。原則上，基於《個人資料保護法》相對於其他法律屬於普通法，若其他法律對於生物特徵識別資料另有規範，將基於特別法優於普通法之法理優先適用。惟目前臺灣生物特徵識別資料的規制，在公務機關面向，多以命令或指引方式為之，例：「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」、及「勞動基準法施行細則」等；或「校園使用生物特徵辨識技術個人資料保護指引」。前述作法因多落於法規命令層級，對於資料當事人的保障不足，恐有違反法律保留原則之虞。

此外，另就生物特徵識別資料的蒐集、處理及利用，若法條並未直接提及生物特徵識別技術或資料的使用，但有「核符」二字，是否授權公務機關得以使用生物特徵識別技術或資料的使用，學者間有不同看法。有部分學者認為，若法律文字已提及確認身分之意，已有某程度的法律授權；另有部分學者認為，必須法律有明文規定才可。另有學者提出應該盤點哪些為公務機關已經據以應用臉部辨識技術的法條用語，並指出與應用臉部辨識技術時，可能蒐集、處理、利用臉部生物特徵資料的差異。

不過，本計畫認為，討論政府公共服務應用臉部辨識技術時，不同場域或機關，會有不同的使用情境，故應考量行政行為的性質及手段是否有強制性的問題。隨著情境的不同，法律授權的強度也可能不同。至於，行政處分的性質，亦將進一步影響當事人後續提起救濟之訴訟途徑的選擇，及處分合法性跟適當性的判斷的問題，仍需做進一步考量。

（二）歐盟法律對於臉部辨識技術的規制

雖然歐盟於 2016 年前並未特別將生物特徵資料另行規範，隨著科技技術的進步與生物特徵資料的使用，個資保護第 29 條工作小組注意到此類技術與資料的使用，對於資料當事人可能產生莫大的影響。原因有二，生物特徵資料本身既為識別因子，又與個資當事人間具有緊密連結與不可否認的特性。個資保護第 29 條工作小組陸續於 2016 年前對於生物特徵資料的蒐集、處理及利用，僅能透過發布意見書之方式，做為法規遵循之參考。

歐盟規制生物特徵資料的方式，在 2016 年歐盟修訂個人資料保護法有了重大的改變。歐盟於 2016 年推出之《一般資料保護規則》（General Data Protection Regulations，以下簡稱為《GDPR》），將生物特徵資料列為敏感性/特種個資，依第九條規定敏感性/特種個資原則上不得蒐集、處理及利用，除非有第二項規定之各款之一。鑑於近期影像與影像辨識技術的發展，歐盟個人資料保護委員會（European Data Protection Board，以下簡稱為 EDPB）先行於 2020 年發布《歐

盟使用影像裝置處理（Process）個人資料指引》（Guidelines 3/2019 on Processing of Personal Data Through Video Device, Version 2.0），提供各界遵循；隨後因為人工智慧技術的崛起，與執法單位使用臉部辨識技術可能帶來的爭議，遂於 2022 年再行發布《執法領域臉部辨識技術運用指引》（Guidelines 05/2022 On The Use of Facial Recognition Technology in the Area of Law Enforcement）。

除此之外，近期歐盟人工智慧法（《AI Act》）對人工智慧技術結合生物特徵資料的應用給予非常多的關注。該法於今年（2024 年）3 月 13 日於歐洲議會以壓倒性多數通過，主要係對人工智慧提出以用途的風險做為監管分級的基礎理論與法律規範。通過的法案版本以人工智慧的用途可能對於個人或群體的自主、自由與安全可能造成的風險加以分類，並要求利害關係者（含研發產製的企業、使用者—含公私部門）依 AI 的使用目的與風險層級，額外採取因應風險的配套措施及技術面的要求，或其他例外的規範。《AI Act》為全球第一部規範人工智慧的法律，並做為透過透明、問責與人類監督，做為實現「歐洲數位權利和原則」的實例。

有關使用生物特徵資料的人工智慧技術的用途，一直為《AI Act》歐盟會員國熱烈討論的重要項目之一，因為各國對於什麼人、基於何種目的、於什麼情境、使用用途等，是否應該允許使用之看法不一，尤其以臉部生物特徵之應用具多元與價值性，不應全面禁止，而是透過談判討論後形成共識，依據該使用者之使用依據、用途與風險層級加以分類，並要求使用者應按照風險檢視技術應用之合法性與必要性，以及採取與風險層級相對應之因應措施，以透明、問責與人類監管與監督應用臉部辨識技術。

《AI Act》將 AI 可能的風險分為無法接受的風險、高風險、有限風險、微小風險或無風險四個層級（如圖 3），並對於各該風險所應採取的因應措施具相關規定。涉及使用生物特徵資料之相關技術（含應用人工智慧的臉部辨識技術），大多被歸類於無法接受的風險層級而禁止使用，或落於高風險層級，法規進而要求系統建置者與使用者必須於系統之全生命週期，進行評估、註冊與受監管。

《AI Act》將涉及「生物特徵資料」，指與自然人的身體、生理或行為特徵有關的由特定技術處理所產生的個人資料，如臉部影像或指紋和掌紋資料等之生物特徵資料的應用，進一步區分如下：

- 生物特徵辨識（Biometric Identification）¹

係指以辨識特定個人身分為目的，透過自動辨識系統將個人之身體、生理、行為和心理特徵等生物特徵資料，與已儲存於生物特徵資料庫中之個人生物特徵資料相互比對，從而辨識特定個人之身分。

- 生物特徵驗證（Biometric Verification）²

¹ EU, AI Act, Article 3 (35).

² EU, AI Act, Article 3 (36).

係指將個人的生物特徵資料與先前提供的生物特徵資料，透過自動系統進行一對一驗證（包括鑑別），自動驗證自然人的身分。

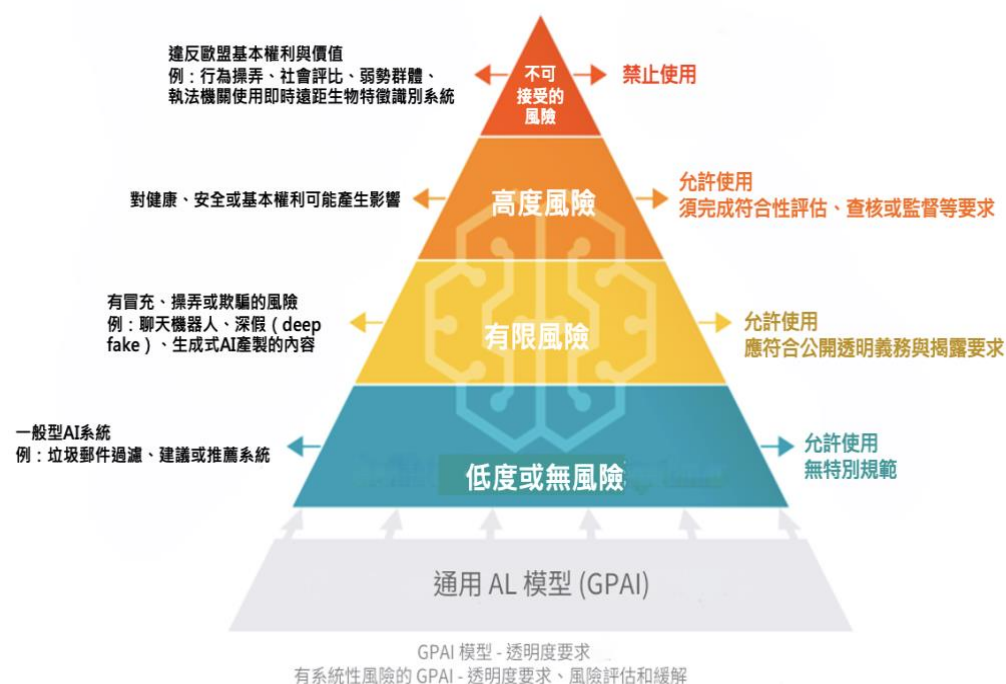


圖 3：歐盟人工智慧法風險級別結構

資料來源：本計畫翻譯整理自 European Parliament, Artificial intelligence act Briefing³。

另外，《AI Act》同時規範以下涉及生物特徵資料的應用，但非以確認或驗證特定個人為目的之人工智慧系統，亦在《AI Act》的規範範疇之內。

- 情緒辨識或推論系統（Emotion Recognition System）⁴

係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的人工智慧系統。

- 生物特徵分類系統（Biometric Categorisation System）⁵

係指依據自然人的生物特徵資料，將其歸納分屬特定類別的人工智慧系統。若系統為附屬於另一項商業服務，且因客觀技術原因而嚴格必要者，不屬之。

³ European Parliament, Artificial intelligence act Briefing, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).

⁴ EU, AI Act, Article 3 (39).

⁵ EU, AI Act, Article 3 (40).

表 1：歐盟《AI Act》生物特徵技術應用風險分級與因應措施對應表

風險層級	原因	允許使用/ 因應措施	使用事例
無法接受的風險	對安全、生命、權利具明顯威脅	禁止使用 ⁶	♦ 以提供產品或服務進入市場之特定目的或其他使用生物特徵用以推斷或推論其種族、政治意向、貿易公會所屬會員、宗教、哲學信仰、性生活或性傾向) (基於合法取得之生物特徵資料之資料集所進行之標註或篩選過濾除外，例如：執法單位之影像、生物特徵資料，或以基於生物特徵資料所為之分類) ♦ 以提供產品或服務進入市場之特定目的或其他使用為臉部辨識資料庫之建置或擴展，於網際網路或 CCTV 錄影無差別任意地蒐集影像 ♦ 以提供產品或服務進入市場之特定目的或其他使用情緒辨識或推論系統於工作或教育機構環境(基於醫療或安全者除外) ♦ 僅做為剖繪或評估之預測性警務使用(具客觀確認特並犯罪活動者除外) ♦ 原則禁止執法單位使用遠距生物特徵辨識系統，除非符合第五條規定之禁止事例之例外情況。只

⁶ EU, AI Act, Article 5.

風險層級	原因	允許使用/ 因應措施	使用事例
			有在滿足相對應的保障 措施，才得以使用。於取 得司法授權，進行重罪追 訴與偵查等，始得為之。
高度風險	對健康、安全、基 本權利或環境可 能具有負面影響	允許使用，但 系統建置公司 與系統使用者 須於系統部署 前及系統生命 週期採取各項 符合性評估、 技術面與查核 面要求、受監 督的要求等	除禁止事例外，其他涉及生物 特徵資料用以即時或事後遠距 識別或區別自然人之各式應用 事例 AI Act 第五條禁止事例之例外
有限度的 風險		系統建置公司 與系統使用者 應符合公開透 明與揭露要 求，使民眾得 以決定是否使 用	具有特定透明度義務的人工智 慧系統，例如聊天機器人
低度風險 或無風險		系統建置公司 與系統使用者 應自行盤點與 紀錄，以確認 系統是否受限 於 AI Act 之規 定	允許免費使用支持人工智慧的 影片遊戲，或垃圾郵件過濾器 等應用程式

資料來源：本計畫自行整理。

《AI Act》除了將 AI 系統依其使用進行風險分類，要求高風險 AI 系統使用前製造商與使用者所應採取的各項配套措施，同時，《AI Act》進一步規範，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。《AI Act》還特別規定，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。

1. 風險控管制度的建置與落實。
2. 訓練、驗證與測試資料與資料治理。
3. 系統上市或使用前技術文件之整備。
4. 系統運行紀錄之自動保存。
5. 系統資訊之透明與提供。
6. 人類行為的監督與介入。
7. 系統運行的準確性、穩定性及資訊安全。

儘管歐盟會員國肯認生物特徵的應用，占有極重要的規範必要，《AI Act》於經過多輪的談判與討論後，對於應用生物特徵資料之人工智慧技術可能的用途，含生物特徵辨識與驗證、情緒辨識與推論、生物特徵分類等，訂立可能危及人權的禁止使用與高風險應用的事例，例如，預測性警務、社會評比，以及可能會影響人類行為的應用等。然而，該法並未更進一步討論與規範人工智慧技術結合生物特徵資料之其他使用，例如於公共場所使用情緒辨識與推論系統，與即時/事後遠端生物特徵識別技術。《AI Act》過於狹窄的規範禁止使用的用途及開放使用的例外，是否可能使大多數的使用將落於高風險的類型，這樣對於基本權利的保障是否足夠，令許多關切該技術應用可能侵犯人權的公民社會與團體感到十分失望與憂心。此外，《AI Act》過度聚焦於透過技術與標準，用以確認人工智慧技術的安全性，也飽受批評。雖然，人工智慧技術的安全性有助於保障權利，但若於科技研發前端未能把人權保障的概念納入考量，產品與服務上市後對於人權的保障，需要各方利益關係者花費更多心力做評估、監督、調適與校正。即便如此，《AI Act》將由各會員國接續加以執行，針對前述應用生物特徵資料之人工智慧技術可能的用途的落實情況與障礙，相關經驗應可提供我國對參考。

（三）臉部辨識技術實際應用案例

臉部辨識技術應用領域廣泛並且不斷持續發展中，包括門禁管制、安控保全、身分辨識、人員監控、員工考勤等。相關的應用目的是希望透過臉部辨識技術可以確保身分的真實性、並提高安全性、效率，減少工作量和時間，同時也可以減少使用者的負擔，增加便利性及易用性。**表 2** 整理臺灣應用案例，供構思公務機關應用臉部辨識技術提供公共服務（不含司法調查、犯罪偵查及警察執法等）時，於個人資料蒐集、處理、利用時參考。

表 2：臉部辨識應用於公共服務一覽

機關	用途	辨識流程
彰化縣政府	員工考勤	1. 多人同時比對辨識 2. 非觸控式平板，辨識客體經過即可辨識
新北市地政局板橋地政事務所	身分核符	1. 研勤科技「人臉辨識 E 拍即合」系統，使用 1 對 1 比對技術，臉部比對後會留存臉部特徵值 15 年 2. 進行臉部辨識前： (1) 承辦人員請民眾出示身分證，確認身分與身分證真偽 (2) 承辦人員向民眾解釋權益，說明臉部辨識之使用，並告知民眾還有其他不使用臉部辨識之選項，例如印鑑證明、內政部線上聲明、簽證、公證程序 (3) 詢問民眾是否同意使用臉部辨識方式確認其身分別 (4) 申辦同意簽請民眾同意書 3. 進行臉部辨識後：保存影像、特徵值、比對結果書面報告，僅司法機關、偵查機關、辦理地政相關業務才可調閱相關資料
勞動部勞動力發展署桃竹苗分署	學員出缺席紀錄	1. 學員註冊機制 2. 指定課程學員於劃定區域內暫停即可辨識
2017 年臺北世大運	確保選手和民眾安全	靠近臉部辨識系統 2 公尺範圍內，事前被加入臉部辨識的模組，即可於後端分析影像中的人臉，並在 2 秒內發

機關	用途	辨識流程
		出嗶嗶響聲，搭配 X 光檢驗入場者攜帶物品及金屬探測儀器
新北市立圖書館	借還書	專人審核身分後協助讀者註冊
科學教育博物館	廣告推播	1. 與廣告機結合 2. 系統會判定性別、年齡層，判別推送那些廣告給被辨識者
國家兩廳院	防疫測溫	防疫溫測系統有零接觸的自動化偵測配戴口罩、測量體溫，和消毒手部設備
臺灣高鐵	員工考勤、門禁	嚴格型雙模系統，意指除出示員工證，還需員工臉部辨識才能通過門禁認證
高雄捷運	廣告推播	透過高科技分析，在捷運站內觀看多媒體看板者的性別、年齡、喜好
桃園市立木藝博物館	志工打卡	寬鬆型雙模系統，意指掃描員工卡上的 QR Code 或臉部辨識擇一即可打卡

資料來源：本計畫整理。

(四) 臉部辨識技術爭議案例

然而，在臉部辨識技術應用，仍存在許多爭議。因臺灣目前對於臉部辨識技術的應用尚未有規範運用生物特徵資料之專法，各界對於應用臉部辨識技術提供公共服務爭議案例不多，表 3 呈現我國臉部辨識技術相關判例，及臉部辨識技術相關函釋之重點，並整理國外臉部辨識技術的爭議案例於後。

表 3：臺灣臉部辨識技術相關的判例

判決	案由	重點摘要整理
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 ⁷ 。
臺北高等行政法院 109 年度訴字第 912 號判決	戶政事件	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 的權限，但若不換發將使其權利受損 ⁸ 。
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 ⁹ 。

函釋	重點摘要整理
法矯署安字第 11204001710 號	為戒護安全目的，各矯正機關得於必要範圍內，運用科技設備蒐集、處理、利用收容人或進出人員之個人資料（含生物特徵識別資料）。 一、按監獄行刑法第 21 條第 3 項及羈押法第 16 條第 3 項規定，為戒護安全目的，機關得於必要範圍內，運用科技設備蒐集、處理、利用收容人或進出人員之個人資料。 二、按監獄及看守所科技設備設置與使用及管理辦法（以下簡稱管理辦法）第 8 條至第 10 條、第 12 條第 2 項及第 13 條第 2 項規定，各機關得設置採集、辨識或門禁設備之處所及運用、蒐集收容人以外人員之個人生物特徵識別資料（以下簡稱識別資料）前應告知事項及各類人員識別資料之銷燬或刪除期限。 三、各機關蒐集收容人以外人員之識別資料，以輔助門禁管制或依法處理、利用，應於採集處所張貼設置依據、蒐集範圍、使用目的、保存期限，並告知需配合使用設備並附帶輸入個人資料等程序事項，俾利進出人員知*

⁷ 宜蘭地方法院 110 年度簡字第 749 號刑事判決。

⁸ 臺北高等行政法院 109 年度訴字第 912 號判決。

⁹ 臺南地方法院 109 年度交字第 200 號判決。

函釋	重點摘要整理
	四、設置科技設備進行門禁管制之機關，原則以設備管制進出，惟如有特別事由，進出人員無法配合採集或未能使用設備進行辨識（管制）時，得由機關人員確認身分，並以登錄簿冊之方式管制進出。 五、進出人員如對於旨揭設備之使用及留存資料有疑義時，應按上開規定及相關辦理程序妥予說明；如進出人員結束與機關業務關係後，要求立即刪除留存之識別資料時，則應依個人資料保護法第 11 條第 3 項規定，於個人資料蒐集之特定目的消失時，依當事人之請求，刪除該個人資料，以臻周延。 六、未按管理辦法第 17 條規定，機關設置各類科技設備時，應分別訂定內部科技設備操作及管理之規定¹⁰。
發法字第 1100005839 號	貴部函詢戶政事務所使用「輔助人員辨識確認系統」拍攝 14 歲以上之未成年人臉部影像所涉個人資料保護法（下稱個資法）問題一事 一、中央法規標準法第 16 條第 1 項前段規定： 「法規對其他法規所規定之同一事項而為特別之規定者，應優先適用之。」個資法之性質為普通法，其他特別法有關個人資料蒐集、處理或利用之規定，依特別法優於普通法之法理，自應優先適用各該特別規定。是有關戶政事務所蒐集、處理或利用個人資料，若無其他法令（例如戶籍法）之特別規定應予優先適用者外，始適用個資法之相關規定，合先敘明。 二、次按個資法第 15 條規定「公務機關對個人資料之蒐集或處理，…應有特定目的，並符合下列情形之一者：…二、經當事人同意…。」、同法第 7 條第 1 項規定「第 15 條第 2 款…所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。」、第 8 條第 1 項規定「公務機關…依第 15 條…規定向當事人蒐集個人資料時，應

¹⁰ 法矯署安字第 11204001710 號。

函釋	重點摘要整理
	明確告知當事人下列事項：…。」、「同法施行細則第 16 條規定「依本法第 8 條…所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」以及同法第 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。」 三、查本案戶政事務所蒐集當事人之臉部影像並透過「輔助人員辨識確認系統」辨識當事人身分，以防範民眾假冒身分、冒辦（領）戶籍資料或國民身分證等情事一節，鑒於「臉部影像」具有人各不同、終身不變之生物特徵特質，屬具備高度人別辨識之個人資料，一旦外洩可能對資料當事人造成難以彌補之損害，故倘公務機關基於「戶政」（代號 015）之特定目的蒐集該等資料，並以當事人同意做為其合法事由時，除應尊重當事人權益，注意蒐集臉部影像是否為辨識當事人身分之唯一或最小侵害方式、有無其他方式供當事人選擇等；並應注意踐行法定應告知事項，以符合當事人年齡、生活經驗及理解能力，且容易理解、清楚簡單之語言或文字為之，使當事人得充分瞭解個人資料之後續利用，始符合上開個資法及其施行細則等規定。 四、至有關戶政事務所經當事人同意蒐集 14 歲以上之未成年人臉部影像，得否由該當事人自行同意而無須取得法定代理人之同意一節，由於個資法就未成年人權利行使之年齡並無特別規定，故關於未成年人同意權之行使，應回歸適用民法有關行為能力之一般性規定，併此敘明¹¹。
法律字第 1000015826 號	為釐清民眾疑慮，內政部為強化國境入出管控所函報之「個人生物特徵識別資料蒐集管理及運用

¹¹ 摘自 發法字第 1100005839 號。

函釋	重點摘要整理
	建置計畫書（草案）」，應就生物辨識應用對象之不同，分別敘明蒐集個人資料之特定目的及法律依據。 一、查本案計畫書草案（下稱本草案）內容，係內政部入出國及移民署為執行入出國及移民法第 4 條及第 91 條規定，擬就個人生物特徵識別資料之蒐集、管理及運用為系統建置，因本案涉及層面廣泛，本部謹就與電腦處理個人資料保護法部分提供意見，先予敘明。 二、本草案之目的除強化國境入出境管控，以保障國家安全，復有建立民眾信任，消除侵害人權之疑慮，建請考量在適當章節增列「合法性說明」，以釐清民眾疑慮，故應就生物辨識應用對象之不同，分別敘明蒐集個人資料之特定目的及法律依據，此參本草案「壹、計劃緣起」「三、未來環境預測」之「（四）我國實施生物特徵概況，表 1-3 我國實施生物特徵辨識法規依據及執行情形」中，在應用對象為國民部分，國際機場旅客自動查驗快速通關系統，並未說明法規依據；就國民之晶片護照部分，亦未敘明護照條例修正草案方向及大致內容，宜增加相關說明，以期明確。 三、另建請於適當章節（如：參、三（三）系統安全措施及隱私權保護；伍、四（七）維護及監控作業需求）增加存取紀錄及資料稽核等內部控制稽核措施之程序，以強化個人資料安全之維護，且於系統建置過程，應確實遵守法令規定，以維護個人資料之安全性¹²。

資料來源：本計畫自行整理。

¹² 摘自 法律字第 1000015826 號。

- 西班牙個資保護機關（Agencia Española Protección Datos 以下簡稱為，AEPD）¹³發現連鎖超市 Mercadona 使用臉部辨識的影像監視系統做為證據保全，或偵測並阻止具犯罪前科或入境禁令者進入超市。由於臉部辨識系統的運作方式即為大規模蒐集、處理與利用生物辨識資料，受影響的資料主體眾多，所以應遵守《GDPR》第 5 條，最小化和目的限制原則，以加強對於資料當事人的保障。超市處理所有潛在客戶和員工的資料只為了控制少數被定罪者，係已違反《GDPR》第 5（1）（c）條最小化原則。超市主張的使用系統係為公共利益，實則二者間不具真正關聯，僅涉及控管者的私人利益。AEPD 以該超市未有資料保護評估（Data Protection Impact Assessment 以下簡稱為，DPIA）、使用該系統之行為不符比例原則、違法（資料保護法第 28 條第 2 項）處理兒童與弱勢人群資料、違反透明原則、資料主體無法履行刪除權和反對權等理由對該超市開罰 315 萬歐元。
- 美國勞工部監察長辦公室提出警告：各州使用的臉部辨識演算法監控失業補助金的發放存在偏見，其指出，使用臉部辨識系統做為審查失業補助金的輔助，可能造成失業補助金發放的歧視，且演算法的偏見，可能讓女性和少數族裔處於較不利地位。美國國家標準與技術研究院（National Institute of Standards and Technology 以下簡稱為，NIST）¹⁴2019 年的報告指出，臉部辨識系統演算法在分析女性或少數族裔時錯誤率較高，且失業補助金申請的批准率，非裔申請者的通過率僅為白人申請者的一半。警告後，負責制定失業制度政策的就業和培訓管理局，已對公務機關提供「最低限度的指導文件」。勞工部長布倫特·帕頓（Brent Parton）表示，部門將為各州失業補助計畫制定指引，並要求提供至少一種不包括臉部辨識的身分驗證形式。
- 與上一則案例類似，係美國勞動部警告各州就業和培訓局需要確保臉部辨識系統須能公平地提供失業補助並保護生物辨識資料。由於疫情影響，失業保險補助計畫發生大量冒名頂替者盜領之情形，故州勞動力機構（State Workforce Agencies 以下簡稱為，SWA）¹⁵與臉部辨識系統之承包商合作，此一合作下會使申請人須使用承包商網站並提供臉部影像進行身分驗證，再行後續申請程序。此一做法下迫使申請人必須提交生物辨識資料，以獲得州和聯邦法律規定的失業補助金。勞動部監察長辦公室指出，從過去 NIST 報告發現臉部辨識系統對某些人口群體存在明顯偏見。隱私安全保護風險必須由 ETA（Employment and Training.

¹³ AEPD – PS/00120/2021, from [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-PS/00120/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-PS/00120/2021).

¹⁴ States warned about facial recognition for unemployment claims, from <https://statescoop.com/labor-dept-inspector-general-warns-states-facial-recognition-unemployment/>.

¹⁵ U.S. Department of Labor Office of Inspector General Washington, DC 20210, from <https://www.oig.dol.gov/public/reports/oa/2023/19-23-005-03-315>.

Administration) 提供適當監督和指導加以解決，SWA 還需要為無法完成身分驗證流程的申請人提供替代方案。

- 西班牙個人資料保護機關對管轄內酒店因為違反《GDPR》開罰¹⁶，荷蘭旅客向個人資料保護機關投訴，西班牙酒店未經旅客同意，逕掃描旅客護照蒐集資料與影像，主張其為辦理住宿手續必要程序之一。酒店主張其因警方要求而掃描護照，透過光學字元辨識生成文字資訊導入酒店管理軟體以驗證旅客身分，避免第三方消費詐欺。西班牙個人資料保護機關於調查時，起初認為酒店具備資料蒐集處理與利用的合法利益與法律義務，原決定駁回此案。但經調查後，酒店確實為確認旅客身分防止消費詐欺，且利用資料協助旅客辦理入住之手續，係具備歐盟《GDPR》第 6 (1) (b) 條及第 6 (1) (c) 條處理資料及遵守法律規定住宿機構之法律義務做為法律依據，具合法性；雖經掃描護照時僅使用文字辨識技術獲得所需欄位及影像，酒店並未保留護照頁面副本，酒店行亦應符合比例原則與《GDPR》第 5 (1) (c) 條之資料最小化原則。個人資料保護機關認為酒店未遵循《GDPR》之處，在於酒店隱私政策未說明將掃描護照資料係用於驗證身分目的，且無說明其個資蒐集處理與利用之法律依據及合法利益。基此，西班牙個人資料保護機關以違反《GDPR》第 6 條對該酒店處以 3 萬歐元罰款，並令其採取必要措施，確保個人資料之處理符合《GDPR》之規定。
- 義大利個人資料保護機關日前因博洛尼亞市政府的 D'Accursio「ShareArt」的專案，因違反《GDPR》的規定處理臉部影像提出警告。該事件起因於義大利新技術能源和可持續經濟發展局（European Network of Environmental Authorities 以下簡稱為 ENEA）與博洛尼亞博物館合作，透過「ShareArt」系統利用鏡頭自動偵測參觀者的臉部影像，同步獲取觀察參觀者與藝術品間之互動資料做為藝術專案。雖然參觀者於通過售票處時，確實告示有該系統存在，但該告示明確表示系統並不涉及臉部辨識。經義大利個人資料保護機關之調查，認為儘管系統處理個人資料的時間相當短暫，該系統仍處理參觀者臉部影像的個人資料。另外，該市政府與 D'Accursio 博物館二者除未符合蒐集、處理、利用合作應遵守之聯繫方式、資料保護員之資訊、未定義處理之法律依據、資料保留期限、資料當事人之權利，更重要的是，ShareArt 系統並未具備處理個人資料之法律依據，已經違反《GDPR》第 5 (1) (a) 條，不符於合法性、公正性及透明原則，及 ShareArt 系統的通知未包含《GDPR》第 13 條要求

¹⁶ AEPD (Spain) - PS/00078/2021, from [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-PS/00078/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-PS/00078/2021).

的所有要件。最終，義大利個人資料保護機關認定市政府違反了《GDPR》第 5 (1) (a)、12 和 13 條給予警告¹⁷。

- 加泰羅尼亞大學於 Covid-19 疫情期間，為驗證線上考試的學生身分，在考試前使用臉部辨識系統捕捉學生臉部影像，與身分證照片進行比較，比對準確者允許參加考試，拒絕辨識的學生視同缺考。該大學表示，根據 WP29 第 3/2012 號意見，其所蒐集的資料並非敏感性資料，且蒐集、處理與利用為大學入學考試所必要，係基於防止學術詐欺之合法利益。經機關調查，共計 31,501 名學生經使用臉部辨識技術才參加考試。調查後，加泰羅尼亞個人資料保護機關認為，臉部辨識系統所使用之生物特徵資料已規定於《GDPR》，該法第 4 (14) 條將生物辨識資料定義為「與自然人的身體、生理或行為特徵有關的特定技術處理所產生的個人資料，允許或確認該自然人的唯一識別，如臉部影像或指紋等」。該定義已排除 WP29 第 3/2012 號意見的適用，且該意見在《GDPR》之前，已過時。加泰羅尼亞個人資料保護機關認為，臉部生物特徵資料是《GDPR》第 9 (1) 條所規定之敏感性資料，原則禁止蒐集處理利用，除非符合規定情況下才能用於辨識或認證目的。然而，該校未能舉證具備《GDPR》第 9 (2) 條所規定的例外情況。此外，學校也未提供給學生不使用臉部辨識系統之其他替代方案，故即便獲得學生同意進行臉部辨識，任何同意皆為無效同意。雖加泰羅尼亞個人資料保護機關對於臉部辨識技術可能是防止學術詐欺的有效手段表示認可，但還有其他侵入性較小的有效措施可達成目的，故該校採取措施不符比例原則。綜上所述，個人資料保護機關認定該大學違反《GDPR》第 5 (1) (a) 條和第 9 條，處以 20,000 歐元罰款¹⁸。
- 另一個線上考試的案例。哥本哈根 IT 大學¹⁹於 Covid-19 疫情期間，為確保考試完整性與防弊，在線上授課與考試期間，對於每場考試進行監督，若考生不同意即不可參與考試。經丹麥個人資料保護機關調查，國際電信聯盟線上監督工具（Proctor Exam）之監督包括：學生向鏡頭出示身分證件或學生證、錄製影片（含聲音）及學生螢幕、網路瀏覽歷史紀錄（不包括處理生物識別資料及臉部辨識技術）。錄音採用加密傳輸，僅保存 21 日，國際電聯使用 Chrome，無需考生電腦的相關額外授權，該線上監督工具亦易於安裝和卸載。本案爭議在於，國際電信聯盟是否有要求學生參加線上考試時接受線上監督的法律依據。經丹麥個人資料

¹⁷ Garante per la protezione dei dati personali (Italy) –9896808, from [https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-9896808](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-9896808).

¹⁸ APDCAT (Catalonia) - PS 49/2019, from [https://gdprhub.eu/index.php?title=APDCAT_\(Catalonia\)_-PS_49/2019](https://gdprhub.eu/index.php?title=APDCAT_(Catalonia)_-PS_49/2019).

¹⁹ Datatilsynet (Denmark) - 2020-432-0034, from [https://gdprhub.eu/index.php?title=Datatilsynet_\(Denmark\)_-2020-432-0034](https://gdprhub.eu/index.php?title=Datatilsynet_(Denmark)_-2020-432-0034).

保護機關調查，認定國際電信聯盟符合《GDPR》，原因如下：（一）對考試進行記錄使用監督工具的必要性評估、（二）監督工具的選擇，於學生線上考試而言是侵害性最小的、（三）國際電信聯盟以簡潔、透明、易懂和易於理解的方式通知學生，並向學生提供一般隱私聲明、（四）國際電信聯盟進行了風險評估，包括考慮了技術和組織安全措施，儘量減少相關處理（例如傳輸和靜態加密、位於歐洲經濟區的安全伺服器、存取控制）。

- 「數位健康」公司 Consciously Digital²⁰的 Anastasia Dedyukhina 博士對於 Global System for Mobile communications Association（以下簡稱為 GSMA）要求她上傳護照資料以便參加 2021 年世界行動通訊大會活動感到震驚。於是她向西班牙資料保護機構（AEPD）提出投訴。該大會使用與 BREEZ 臉部辨識結合之技術，使用該技術下得以實現無接觸式存取（Mobile World Congress，以下簡稱為 MWC）活動。當初，MWC 活動舉辦者主張已完成《GDPR》第 35 條所規定之資料保護影響評估，但後來發現，該組織並未真正審視或完成風險評估，而僅完成系統實施的比例原則。主辦者在對參與者權利的影響及相關的自由及保障，並未做進一步的規劃。個人資料保護機關認為，MWC 活動舉辦者對於《GDPR》的法規遵循非常草率，尤其涉及生物辨識資料和臉部辨識技術方面。該錯誤雖非最嚴重的違規行為，但因數位足跡越來越不容易被消除，故此涉及廣泛的資料隱私問題。爾後，個人資料保護機關認 MWC 活動舉辦者 GSMA 侵犯近 20,000 名與會者的隱私，並處以 20 萬歐元的罰款。
- 2019 年法國政府通過一項允許可跨政府機關和公共服務網站之「行動身分驗證個人資料自動處理系統」（Alicem）的法令，該系統可簽發電子身分，提供民眾以電子方式認證，用以向公共或私人機構證明身分，俾以非接觸式讀取電子元件的終端設備。不過，設立使用 Alicem 系統需先開設帳戶，使用者須同意通過臉部辨識系統蒐集其的生物識別資料，同時須錄製一段短影片，以提供臉部辨識演算法進行驗證，通過驗證後即可完成註冊。如使用者不同意臉部辨識處理個人資料，將無法設立帳戶與無法應用程式。法國促進數位權利和捍衛公民自由組織 La Quadrature du Net（LQDN）²¹ 對該法令的合法性提出質疑並宣稱，該法令不符合《GDPR》第 4（11）條和第 7（4）條所規定之合法同意，也不是基於第 9（2）（a）條敏感性個資的規定。對於是否具有同意，依歐洲議會和理事會《GDPR》第 4（11）條，將同意定義為，資料當事人

²⁰ GSMA fined €200,000 for MWC facial recognition GDPR infringement, from <https://www.telecoms.com/virtualization/gsma-fined-200-000-for-mwc-facial-recognition-gdpr-infringement>.

²¹ CE – 432656 , from https://gdprhub.eu/index.php?title=CE_-_N%C2%B0_432656.

通過聲明或明確的行動同意處理與其有關的個人資料下任何自由、具體、知情和明確的意願。此外，同法第 7 條規定，判斷同意是否為自由給予時，必須最大限度地考慮了解，是否具其他執行合約（包括提供服務）的問題，且須同意該個人資料處理對於履行合約而言，並非必需的個人資料。該規定的第 42 條規定，如果未給予資料當事人真正的選擇自由、無法拒絕或撤回同意，則不應視為同意。

- 資料當事人向義大利個人資料保護機關投訴，Clearview AI 公司在未經其同意的情況下處理其個人資料。此外，兩個致力於捍衛個人隱私和基本權利的組織，向義大利個人資料保護機關提交有關德國和瑞典對於 Clearview AI 公司活動的報告。對於 Clearview AI 公司透過網路蒐集臉部影像訓練演算法，以供客戶使用系統，透過臉部辨識特定個人。雖 Clearview AI 公司宣稱該服務不對外開放，僅向特定類別的客戶（即執法單位）使用。義大利個人資料保護機關仍認為，Clearview AI 公司不僅蒐集個人資料，還進一步處理將照片轉換為生物辨識資料，已經違反《GDPR》第 5（1）（a）條所規定之個人資料處理須遵循之合法、公平和透明原則的要求；更進一步指出，Clearview AI 公司違法行為非常嚴重，因為該行為已類似大規模監視，而且該事件並不是獨立的事件。即便 Clearview AI 公司不再向歐盟境內私人客戶提供服務，這些行為仍持續進行²²。
- Clearview AI 公司亦受到法國個人資料保護機關²³的關注，認為雖然 Clearview AI 為美國公司，在歐盟未有據點，但 Clearview AI 公司已涉及處理歐盟資料當事人之個人資料，包括未成年人。有關管轄權與《GDPR》是否適用之議題，法國個人資料保護機關認為，根據《GDPR》第 3（2）條規定，本案有《GDPR》之適用。由於 Clearview AI 未於歐盟設立公司，還應先行確認兩點：其一，是否處理歐盟轄內資料當事人之個人資料；其二，此種處理是否與監視資料當事人之行為有關。最終，法國個人資料保護機關指出，Clearview AI 公司根據其隱私政策蒐集了三類個資，包括網路上可公開近用的照片、從照片中提取的資料（如地理位置資料）及照片中臉部外觀的資料。依歐洲法院判例法（CJEU Case Law），當個人可被辨識時，被拍攝的個人影像構成個人資料。而且本案，Clearview AI 公司也處理了生物辨識資料，並確認收集之照片也涉及歐盟的資料當事人；其次，法國個人資料保護機關認為 Clearview AI 公司的個資處理與監視行為有關，只要個資處理與監視相關，是否將行為監視做為處理的主要目的，在所不問。另外，監視亦可包括分析（Profiling）。

²² Garante per la protezione dei dati personali (Italy) – 9751362, from [https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9751362](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9751362).

²³ CNIL (France) - SAN-2022-019, from [https://gdprhub.eu/index.php?title=CNIL_\(France\)_-_SAN-2022-019](https://gdprhub.eu/index.php?title=CNIL_(France)_-_SAN-2022-019).

本案與照片相關的搜尋結果是資料當事人的行為概況，Clearview AI 公司使用其資料庫中蒐集的所有資料當事人圖片建立行為檔案，包括網路上影像原始來源的連結—這導致蒐集不同資料間產生連結的可能性。或是，透過分析資料當事人決定放在網上的內容，使在網路上辨識資料當事人的行為，產生連結的可能性。(1) Clearview AI 公司的個資處理，構成監視—辨識資料當事人並蒐集個人資料、第三方可以多次搜尋，得以分析資料當事人行為的變化。(2) 一站式機制的適用性，法國個人資料保護機關認為，一站式機制不適用於此種跨境處理情形，並認為歐盟的每個監督機構皆有權處理其境內案。本案 Clearview AI 公司位於美國，且在歐盟內未有主要或唯一機構。(3) 缺乏處理的法律依據，法國個人資料保護機關認為，Clearview AI 公司違反《GDPR》第 6 條—缺少個資處理的法律依據。法國個人資料保護機關認為，儘管執法機關也可能使用該服務，但 Clearview AI 公司的個資蒐集處理利用僅出於商業目的處理資料，其隱私政策並未明列相關法律依據，同時，《GDPR》其他依據不適用本案。另外，即使個資蒐集處理利用具有經濟利益，也不能主張具《GDPR》具有合法利益為依據，進行個資的蒐集處理與利用。法國個人資料保護機關最終裁定，為衡平控制者的利益及資料當事人的利益，由於該處理具侵入性，故偏向應保護資料當事人的利益。(4) 侵犯近用權，個人資料保護機關認為，Clearview AI 公司的隱私政策提及，其資料庫中只包含搜尋結果。法國個人資料保護機關認為，Clearview AI 公司限制資料當事人近用權（每年兩次）並無依據，因隱私政策並未規定個人資料的保留期間。(5) 侵犯刪除權，法國個人資料保護機關認為，Clearview AI 公司未回覆資料當事人個資刪除請求權，且 Clearview AI 公司並無處理個人資料的法律依據，(6) 未與法國個人資料保護機關合作，僅部分回答資料請求，且忽略法國個人資料保護機關遵守《GDPR》的命令。

- 2021 年 8 月，北艾爾郡議會在其網站公布²⁴，表示將從隔年 10 月開始使用 iPayimpact 系統，允許學生用餐時以臉部辨識之非接觸式支付餐費，同時提供選擇退出該系統或使用 PIN 驗證服務之其他方式支付餐費。英國個人資料保護機關表示，雖臉部辨識技術可能帶來好處與效率，但從個人資料保護的角度來看，仍有相關的法律風險，尤其是涉及兒童之個人資料時，風險將會增加。依英國規定，兒童在個人資料處理時應受到特定保護，因為兒童可能不太了解相關的風險、後果和保障措施，以及他們於個人資料處理相關的權利。隨後，個人資料保護機關更進一步指出，基於確保兒童資料處理須具有有效的合法依據，本案係取得當事人同意透過臉部辨識技術處理生物特徵資料用於用電子支付餐費，所以

²⁴ Council breached GDPR in deploying facial recognition technology in schools – ICO, from <https://techmonitor.ai/policy/privacy-and-data-protection/facial-recognition-technology-school-ico>.

當事人同意應是個資處理的合法基礎。然而，若要透過同意處理兒童生物特徵資料，北艾爾郡議會需要用適合年齡的語言解釋如何蒐集、處利、利用和保存兒童的個人資料，應明確列出與其使用相關的風險。由於本案未滿足取得兒童有效同意的要求，英國個人資料保護機關最後裁定，九所學校違反個人資料保護法，包括透明度、告知同意與當事人權利等條款。有效同意的取得，無論是向學生還是家長或照顧者尋求同意學校必須確保同意是自由給予的、具體的、知情和明確的，如果學生或家長照顧者拒絕同意，學校必須為學生提供不使用臉部辨識技術的替代方案，可能包括刷卡、密碼或現金，且選擇使用其他方式不得對學生造成任何損害，例如，不需等待更長時間才能購買午餐或支付更多費用。

- 英國資訊委員辦公室（ICO）提供安全空間（**Safe Space**）予業者，得在此空間利用個人資料提出創新服務與產品個人資料監理沙盒，為首例英國個人資料監理沙盒制度，由希斯洛機場與航空公司、IT 供應商共同合作，以臉部辨識技術進行驗證乘客身分，使乘客無須提供護照或身分證，即可被驗證為本人之乘客自動化旅程（**Automated Passenger Journey, APJ**）。希斯洛機場因自動化旅程中涉及複雜資料控管者關係，討論歐盟《GDPR》第 26 條之共同控管者間須由何者處理之安排，提供旅客足夠的透明度告知義務。機場須確保採取適當之完整機制，以便蒐集生物特徵識別資料等敏感性資料，並須依《GDPR》第 9 條規定，在取得明確同意前履行對旅客之告知義務²⁵。

²⁵ Regulatory Sandbox Final Report: Heathrow Airport Ltd, from <https://ico.org.uk/media/for-organisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf>.

第三章 調查分析方法

第一節 研究設計

本計畫綜合上述文獻，回顧國內外文獻及新興科技執行現況，同時探討可能涉及之政府機關運用臉部辨識指引，並進行國內機關在數位權利和原則之實踐調查。

執行方式說明如表 4，具體來說本計畫參考歐盟數位權利與原則，整理芬蘭與愛沙尼亞在數位權利和原則的情形，蒐集西班牙、美國、法國與我國的臉部辨識爭議法律案件；並訪談公部門使用臉部辨識的單位，以及提供服務的廠商，以了解近年我國機關單位使用臉部辨識技術可能的情境與資安管理議題，對新興科技（臉部辨識與人工智慧）涉及民眾隱私、資料利用等議題，藉由文獻回顧、深度訪談、電話調查、專家座談等方式，產出可供我國數位權利原則之建議方向，以了解並供後續追蹤我國數位權利和原則的推動及落實情形，並據此與國際接軌及相互對照，以供政府單位導入新興科技與研擬下一階段數位政府計畫時參考。

表 4：研究設計摘要

研究目的	資料蒐集方法	資料來源
1. 對新興科技（如臉部辨識等）涉及民眾隱私、資料利用等前瞻科技應用之議題，建立政府機關運用臉部辨識指引（如涉及使用情境、使用時機、使用原則等）	文獻蒐集	各國官方網站與文獻、現行措施與相關法規
2. 研析 1 個政府機關在創新數位服務的使用情形	文獻蒐集、訪談	文獻、現行措施與相關法規
3. 蒐集與整理歐盟執委會對歐洲數位權利和原則之內容	文獻蒐集、問卷調查	各國官方網站與文獻

資料來源：本計畫整理。

第二節 臉部辨識利害關係人訪談

本計畫透過專家個別訪談，以了解政府單位在使用臉部辨識技術時，如何兼顧民眾數位權利與服務便利、個資隱私保護等多方權衡。

專家個別訪談的目的是為了解政府單位在使用臉部辨識技術時，流程或技術方面有哪些困難，期望透過訪談，優化機關所提供的公共服務，給予改善建議。專家個別訪談約 60 至 120 分鐘不等，本計畫專家個別訪談會在取得受訪者同意後，以錄音、筆記等方式記錄訪談內容，並於整理訪談摘要與逐字稿後，與受訪者確認訪談內容。本計畫專家個別訪談名單與訪談時間參見表 5。

表 5：訪談對象

訪談時間	機關單位	職稱	對應的訪談大綱	編碼
113/03/29	科技股份有限公司	高階經理人	廠商	A1
	科技股份有限公司	高階經理人	廠商	A2
113/03/29	科技股份有限公司	高階經理人	廠商	A3
	科技股份有限公司	協理	廠商	A4
	科技股份有限公司	協理	廠商	A5
113/05/03	勞動部勞動力發展署	督導	政府單位	A6

資料來源：本計畫繪製。

訪談大綱有兩部分：(1) 詢問機關應用相關；(2) 詢問個資與資安相關；若為廠商，則再詢問臉部辨識技術相關題目，最後會詢問開放題「請問您有什麼可與我們分享，或可提供團隊接續研究的」，各分述訪談大綱如下：

● 政府單位的訪談大綱：

機關應用相關

1. 機關臉部辨識系統除差勤目的外，通常還有哪方面的應用？貴機關未來業務可能結合哪些公共服務呢？請舉例說明。
2. 機關內部對系統的導入與接受度如何？（資料或流程整合度、人員培訓）
3. 機關臉部辨識技術系統應用之閾／閥值及人為介入值是如何設定的？
4. 機關人員是否曾反饋臉部辨識系統使用上之困難、不便，原因為何？

5. 本於臉部辨識技術的敏感性與專業性，機關如何服膺透明公開與民眾可理解的方式說明臉部辨識的應用？
6. 機關內部對系統的導入與接受度如何？（資料或流程整合度、人員培訓）
7. 是否曾有第三人/執法機關向機關索取應用臉部辨識所保存的影像或模板資料？若有，機關如何應對？
8. 請問機關使用臉部辨識系統至今，遇到哪些困難、不便之情形？

個資與資安相關

1. 機關採購系統時，通常有哪些基本共通需求，或其他要求？
2. 機關於採購系統時，是否將個資法法規遵循之流程與介面設計納入規劃，例如：告知同意、儲存期間限制、個資刪除等？
3. 機關採購系統時，是否要求內建合法合規的設計，或具備前述能力之佐證例：個資隱私保護、資安等？
4. 請問機關採用臉部辨識技術有何隱私個資保護的做法（例如：個資管理制度導入、訓練與稽核等）？若有，教育訓練之方向、核心大致為何？
5. 請問機關採用臉部辨識技術有何維護資安的作為，例如：近用存取（Access）權限等？
6. 請問臉部辨識系統建置後由內部人員負責還是委外維護？

● 廠商的訪談大綱：

公部門應用相關

1. 公務機關採購之臉部辨識系統，就資料當事人目的告知及相關目的說明及同意之取得是否有相關設計告知、執行，與留存證據，以及事後有確認和刪除等之權限（及我國個資法當事人可主張之權利）？
2. 就貴公司所知，公務機關採購AI臉部辨識技術系統大多應用於哪些情境？除差勤外，通常會與貴公司的臉部辨識技術做哪方面結合與應用？請舉例說明。
3. 採購AI臉部辨識技術系統時，依各應用情境通常具有不同考量或限制。

請問公務機關通常有何基本共通的需求？或有提出要求或須注意之處？

4. 請問，公部門就已取得與保存的影像或模板資料，就您所知是否曾有第三人/執法機關索取？若有前述機關單位前來索取，貴公司對於影像或模板資料在技術面可有何因應？
5. 本於臉部辨識技術的敏感性，公部門應以透明公開的方式說明臉部辨識的應用。若公部門需向民眾說明臉部辨識技術的應用，包含技術運作、資料類型、資料生命週期等，或資料如何被蒐集、處理、利用、儲存、刪除，貴公司會如何協助？
6. 行政部門對臉部辨識的導入與接受度如何？（資料或流程的整合度、人員的訓練等）

個資與資安保護相關

1. 請問，貴公司臉部辨識系統有何內建合法合規的設計，例如：隱私、個資保護、資訊安全等？或特別符合哪一國的法規之設計？如何向客戶展現已具備前述能力（例如：測試、認證、權限等）？採購機關會有所要求嗎？
2. 貴公司於規劃系統時，是否可能將目的特定、資料最小化、資料儲存限制等，納入設計。產品推出前，對於產品的設計與應用，內部是否具對於民眾權利與自由保護的評估報告。採購機關會特別要求嗎？
3. 請問貴公司臉部辨識系統是否因應機關在資安責任層級，規劃不同的軟、硬體規格、或特別需要注意的事項？（例如：臉部辨識技術演算法之母資料群來源、演算法的學習訓練過程、演算法的研發與整合等）

臉部辨識技術相關

1. 請問，常見臉部生物特徵應用的基礎技術有哪些？可舉例公務機關的臉部辨識技術系統多是基礎於前述哪些技術？各技術間有何主要差異？優缺點？
2. 您認為目前臉部辨識技術發展是否已趨於成熟？或是哪些地方需要改善或強化？目前使用臉部辨識技術之機關有否反饋使用上之困難、不便，原因為何？
3. 請問貴公司臉部辨識技術的準確率大概是多少？是否曾出現無法判

讀的狀況？若有案例，能否舉例說明。相對地，公部門採購臉部辨識系統時會要求準確率？依據機關業務或使用目的不同而有所不同？準確率如何佐證？

4. 就您目前對於無論是生物辨識或是臉部辨識技術之觀察，您認為此一技術最大的優勢及最大的劣勢分別為何？針對劣勢之部分是否有改善調整之可能？
5. 請問貴公司如何取得訓練模型時必須使用之資料庫？在訓練模型時是否有應對不同分析客體而有分開訓練之機制？公務機關在採購時，是否有特別要求？

第三節 數位權利與原則問卷調查

本計畫參考歐盟數位權利與原則調查、PEW 研究中心問卷（參見附錄二）、中研院社會變遷調查，發展適合我國機關單位調查使用之數位權利與原則調查問卷，以臉部辨識服務機關單位為發放對象，以了解機關對於數位權利與原則的知覺程度和落實情形，本計畫的完整問卷請參見附錄三。

問卷題目共計 29 題，第 1-2 題詢問戶籍地與居住地，第 3-13 題詢問關於數位權利的同意程度與受訪者對於在臺灣落實程度的看法，這部分題目修改自歐盟數位十年調查，包含民眾應該有可以負擔（得起）的高速網路、民眾應有接受到基礎與進階的數位教育、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、民眾可以容易地在網路上獲取關鍵公共服務、民眾可以自主決定要不要在網路上與 AI 互動等 11 題；第 14-17 題詢問民眾對人工智慧應用與管制的看法，問卷題目為本計畫自行設計，包含您同不同意，人工智慧服務上線前應該取得合格認證標章與管制網路大型數位平台或社群媒體（如 Facebook、YouTube 等）？；第 18-24 題詢問民眾對人工智慧影響的看法，問卷題目參考中研院社會變遷調查，包含擔不擔心，人工智慧的產出結果可能造成偏見或歧視，不利於特定族群、人工智慧可能造成錯誤或虛假消息的氾濫、人工智慧可能影響您的工作機會等題目；第 25-29 題詢問職業教育程度等題目，問卷題目為本計畫自行設計，並經專家會議與民調公司督導確認詢問方式，以確保問卷之專家效度。

本計畫所使用的問卷調查方法為電話調查，委託民間民調公司以電腦輔助電話調查系統（CATI）進行訪問，以臺灣地區住宅電話號碼簿為抽樣清冊，抽樣方式採兩階段進行：第一階段使用「分層比例系統抽樣（Stratified Systematic Sampling, SSS）」自住宅電話簿抽取樣本局碼，以取得電話號碼局碼組合（Prefix）。由於電話號碼簿並未包含未登錄電話，因此抽出的電話必須進行「隨機撥號法」（Random Digit Dialing, RDD）的處理程序，才能做為訪問使用，而在第二階段時，會將第一階段所抽的電話號碼最後兩碼以隨機亂數方式取代之，俾使原本沒

有登錄在電話號碼簿上的住宅電話，也有機會能夠中選成為電話號碼樣本。接通後戶內採任意成人法選取戶中成員進行訪問，且受訪對象一經確認即不再任意更換。

調查完畢後，資料經審查和複查後，為瞭解調查有效樣本的母體代表性，將分別就性別、年齡、教育程度及居住地區進行卡方檢定。為避免資料分析時造成推論的偏差，本計畫將以「多變數反覆加權（Raking）」方式進行成功樣本統計加權，亦即先調整樣本之性別結構與母體相符，然後依序調整年齡、教育程度及縣市地區等變數結構，直至調查樣本在這些變數的分布與母體一致。

本次電話調查是委託典通公司進行，調查的對象是以臺灣地區（包括臺北市、新北市、臺中市、臺南市、高雄市及臺灣各縣市，共 20 個縣市）中，普通住戶內年滿 16 歲以上成年人為調查對象。調查時段為 2024 年 3 月下旬執行電話調查。平日調查時段為晚上 6 點 30 分至 10 點，例假日調查時段為上午 9 點至晚上 10 點。

第四章 調查分析發現

第一節 臉部辨識技術部分之指引建議

本計畫以《個人資料保護法》為基礎，就政府公共服務應用臉部辨識技術所涉及之個人資料或個人資料檔案時，協助確認申辦民眾身分涉及個資保護事項所參用，並不適用於公務機關基於司法、犯罪偵查或安全維護，於公共場所應用臉部辨識技術以識別特定人或分類之應用情境。另外，有關臉部辨識技術應用所延伸出之其他目的，例如資料分析或自動化決策目的等，亦非本計畫之涵蓋範圍。

本計畫所提議之技術架構規範提要建議書如下：

以下係對應「公務機關使用臉部辨識技術情形調查表」【第三部分：準確率及安全性檢驗】之問題，所提出之技術面規範建議。

- 一、公務機關辦理臉部辨識技術採購時，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。
- 二、公務機關使用臉部辨識技術時，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。
- 三、公務機關使用臉部辨識技術時，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。
- 四、公務機關使用臉部辨識技術時，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。
- 五、公務機關使用臉部辨識技術時，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。
- 六、公務機關使用臉部辨識技術後，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。

第二節 臉部辨識利害關係人訪談

本計畫透過專家個別訪談，以了解政府單位在使用臉部辨識技術時，如何兼顧民眾數位權利與服務便利、個資隱私保護等多方權衡，目的是為了解政府單位在使用臉部辨識技術時，流程或技術方面有哪些困難，期望透過訪談，優化機關所提供的公共服務，給予改善建議，整理如下：

一、公部門

● 機關應用相關訪談結果

勞動部勞動力發展署桃竹苗分署採用臉部辨識系統於學員上下課簽到退使用，因學員人數平均每年至少 110 班約 3,600 人上下，有時因為人數、刷卡機與卡片問題，上、下課尖峰時段學員打卡大排長龍，常有抱怨，另外，依請假曠課時數規定，不符規定可能退訓或要求賠償，若符合規定將給予補助及發給完訓證明，產生學員可能代打卡弊端，為避免此弊端，需額外指派人員監看學員打卡情形，臉部辨識系統可以節省人力與提高簽到退效率（A6）。

機關的以 108 個面部特徵為辨識點，閾／閾值設定值在 0.58，以錯誤辨識率計算約 1 萬人錯誤率為 1 人，目前使用都還算順利，少數會遇到的問題是學員姓名使用冷僻字，會在後台管理系統與臉部辨識系統間造成出缺勤資訊不正確的問題，故擬改以學員學號、身分證取代姓名執行比對，目前尚無以臉部辨識結合其他公共服務應用之規劃（A6）。

● 個資與資安相關訪談結果

由於臉部辨識系統使用生物特徵資料具高度敏感性，機關制定「勞動部勞動力發展署桃竹苗分署學員使用人臉辨識技術差勤作業指引」，提供機關同仁與學員參考（請參考附件一），並於學員入訓第一天，宣導說明臉部辨識系統之使用，告知其所相關之權利及保護措施，並解釋使用該系統之理由，於取得學員同意後簽署「學員使用人臉辨識技術同意書」，由學員自行拍照上傳系統。若學員有操作相關之問題，分署人員將會提供協助（A6）。

另因學員人數眾多，臉部圖像檔案的儲存除會增加系統負擔，後台系統留存數值資料來確認學員受訓時數，該資料留存至就業後 90 天（訓後就業追蹤期）定期執行刪除，防止資訊攻堅的發生（A6）。

另外，機關的資安管理比照 ISO27001 規範要求，符合中級 58 項條件，做到所有的功能最小化的權限（例：新增、刪除、修改、匯入、匯出、查詢）給予，依權限身分分別區分管理班級、學員，而每人每天的登入、登出、進到哪個功能項也同樣會被記錄在系統日誌，僅系統管理員及科室主管有權限於

必要時撈出完整資料，且系統為落地無法遠端維護，由委外廠商一季至少 1 次到現場維護（A6）。

二、 技術單位

● 機關應用相關訪談結果

1. 服務類型

機關使用臉部辨識技術提供公共服務較少，新北地政 E 拍即合與勞動力發展署的使用與機場，是較為明顯的案例，大部分用於基本考勤，例如衛福部、新竹縣政府、苗栗縣政府、移民署等（A1）。

國內公部門大都用於差勤和訪客，另外一塊則是用於國安或執法。臺灣在差勤和訪客以外，曾有疾管署於機場使用生物特徵資料，系統使用目的並非做為人臉辨識之用，而是用來分析來自不同區域的乘客是否配戴口罩與疾病本身是否有關連性，進一步探求是否有領先指標或是落後指標的參考。至於，國外公部門客戶所採購的臉部辨識技術系的用途，則多用於入出境（A3）。

臉部辨識技術若未經受辨識者同意，因為法律未授權，除非執法需求，或者是前述疾管署應用案例，因其應用情境並非人別辨識，亦即非針對特徵、非特定人所進行之資料採集等（A3）。

機關臉部辨識技術系統應用之閾/閥值會依臉部辨識系統在不同情境下會有不同設定的需求，例如機場通關就會高度要求準確度，閾值就會設定的比較高（A1）。又如工廠使用人臉識別系統做進出管制，但因該時段上下班人潮眾多，速度要較快，這種通常會再搭配其他身分認證，人臉就是做紀錄，與一般公務機關 1:1 打卡較不同（A3）。

2. 接受程度

機關導入系統，以差勤為例，公部門原都是紙本簽到，或是感應卡，這會牽涉到有人會代打卡的問題，或是疫情時有接觸的風險。系統導入時剛開始有公務機關的人員不大能接受，但因跟差勤與薪水相關，很快就接受了（A1）。

一開始是會有業務到機關說明，讓機關內部與使用者對技術有一定的了解。因為導入系統時多為接觸到機關的執行單位，倒是較少聽到使用者的聲音，導入對機關來說多少跟之前做法有所變化會有額外的事務需要完成。不過這也是要看機關對於科技的接受度，有些機關會有科技使用程度評比，所以有些機關會是較積極去運用科技（接受度較高）（A3）。

除機關外，可能還要考量到社會的接受度。之前有豐原車站智慧車站的案例，運用臉部辨識系統協助鐵路警察辨識通緝犯。透過影像導入辨識系統做

人臉識別，確實也有比對且抓到通緝犯，但後來因為社會輿論的關係下最後下架。對於執法機關來說，導入臉部辨識抓通緝犯可能是有幫助的，但民眾會擔憂不知該使用之意圖（A3）。

- 個資與資安相關訪談結果

目前活躍於臉部辨識技術的各家廠商，大部分都已不需要訓練新模組，且大部分都有送美國 NIST 送評比，但因為各家評比結果非常接近，現在不太會有人強調 NIST 評比結果（A1）。目前尚未有相關的認證，可能等待歐盟人工智慧法有相關認證機制，會再繼續注意這塊。目前公司在資安認證有 ISO 27001，但這塊主要認證範圍為公司跟機房，與產品本身較無關係（A3）。

有關影像的保存與刪除，只會取得影像轉出的特徵值，也就是由一串數字或符號組成，通常不會保存原始圖像。因為圖像所需的空間比數字或符號大，基於成本考量，不存圖像；其次，就是要符合個資法的要求（A1）。

另外，在臉部辨識系統的運用，即便是同一人，在不同地方，在不同系統裡，系統會給他不同的特徵值，由於我國各系統內是沒有串連的，所以就不會有這樣的風險問題（A1）。

- 技術相關訪談結果

臉部辨識技術系統在人 18 歲以前可能要重練一個模組，但是如果是 18 之後的話，人臉不會有什麼變化了。加上正常有完整露出人臉的情況下少有無法判讀的情形，以現在的臉部辨識技術而言，準確率非常高（A1）。要有準確的臉部辨識結果，通常最開始都是要建檔，效果會比較好，無論是像素、解析度、年份久遠的考量（A1）。

在政府機關提供公共服務，服務對象通常在面前採用 1 比 1 的模式，防偽需求不高，準確度可以確認是本人沒有問題。一般政府機關要用到 1 比 N 非常少，除非是警察機關。在限制下，幾乎是用在路上失智老人。個人猜測，如果在國安偵查針對境外恐怖勢力，才有可能是有在用 1 比 N（A1）。

由於公共服務提供時有會有服務的特定對象，蒐集前會先經過其同意且在其有意識下進行影像蒐集，故人們會將臉正對機器，這種情況蒐集下對於準確率不會有太大的問題（A3）。

臉部辨識系統的準確度會回歸到 NIST 的檢測，因其會含不同之結果可供參考，且資料為公開資料，準確度會與該公司之資料集資料相關，為常見參考之依據。準確率會與考題有關，各家臉部辨識系統的準確率是拿自家用資料集去做檢測。在臉部辨識技術產業，大都會找公信力的組織美國政府 NIST 做 FRTE，做臉部辨識系統相關參考依據（A3）。

另外，實際操作時，可藉由二因子的方式提高人臉的易識別性及準確度，或是人臉+手機 PIN CODE+一次性密碼三重因子下去實施。目前，尚未收到

演算法所產生之問題反映。如果準確率會因受環境影響，則可加入排除之，若是因為人的關係，可多增加該人不同角度之照片，用以提升臉部辨識的準確率（A3）。

- 其他訪談內容分享

回應公部門在資訊素養上是否會有數位落差的提問，各公務機關確實存有落差的，根據工作內容或工作心態不一樣，但是落差不大（A1）。

臉部辨識是否能判斷空間的人數或一群體內男多女的分類，技術上是可以達到的，但問題在於得到這樣的大數據，商轉利益不高。不過，仍有少數案例，像高鐵對於知道月台每一車廂等候區之人數有需求，因為高鐵有自由座機制，但是他們只想要知道人數，像是有演唱會的情況，要知道什麼時候不再放人進去，以避免有人數太多，互相推擠，造成危險的情事發生（A1）。

在民間臉部辨識技術還可用於許多不同的情境，例如可以使用具臉部辨識技術的 ATM，該情境下去偵測戴口罩或安全帽等異常行為；或辨識詐騙集團車手等；或者是銀行辨識 VIP 等服務（A3）。

第三節 數位權利與原則問卷調查

本計畫以臺灣地區（含金馬地區）為調查範圍，包括新北市、臺北市、桃園市、臺中市、臺南市、高雄市、臺灣省各縣市及福建省金門縣、連江縣，調查對象設定年滿 16 歲以上本國籍人口，平日調查時段為晚上 6 點 30 分至 10 點，例假日調查時段為上午 9 點至晚上 10 點，委託民間調查公司，採用電話訪問並使用電腦輔助電話調查系統（CATI 系統）以臺灣地區住宅電話號碼簿為抽樣清冊，抽樣方式採兩階段進行：第一階段使用「分層比例系統抽樣（Stratified Systematic Sampling, SSS）」自住宅電話簿抽取樣本局碼，以取得電話號碼局碼組合（Prefix）。由於電話號碼簿並未包含未登錄電話，因此抽出的電話必須進行「隨機撥號法」（Random Digit Dialing, RDD）的處理程序，才能做為訪問使用，而在第二階段時，會將第一階段所抽的電話號碼最後兩碼以隨機亂數方式取代之，俾使原本沒有登錄在電話號碼簿上的住宅電話，也有機會能夠中選成為電話號碼樣本。接通後戶內採任意成人法選取戶中成員進行訪問，且受訪對象一經確認即不再任意更換。本次調查實際完成有效樣本數為 1,227 份，在 95% 的信心水準下，抽樣誤差為 ± 2.80 個百分點。

一、樣本代表性檢定及加權

資料經審查和複查後，為瞭解調查有效樣本的母體代表性，分別就性別、年齡、教育程度及戶籍縣市別進行檢定。檢定結果發現成功樣本與母體在性別、年

齡、教育程度等方面有不一致的現象。為避免資料分析時造成推論的偏差，以「多變數反覆加權（Raking）」方式進行成功樣本統計加權，亦即先調整樣本之性別結構與母體相符，然後依序調整性別、年齡、教育程度、戶籍縣市等變數結構，直至調查樣本在這些變數的分布與母體一致。

經過加權處理後，顯示成功樣本在性別、年齡、教育程度及戶籍縣市的分布上，均與母體分布無顯著差異，請見表 6、表 7、表 8、表 9。

表 6：訪問成功樣本之代表性檢定-性別

單位：人；%							
性別	16 歲以上母體結構		調查樣本				卡方檢定 (P 值)
	人數	百分比	加權前		加權後		
			樣本數	百分比	樣本數	百分比	
總計	20,428,315	100.0	1,227	100.0	1,227	100.0	
男性	10,002,345	49.0	595	48.5	601	49.0	1.000
女性	10,425,970	51.0	632	51.5	626	51.0	

資料來源：內政部戶政司，「112 年各縣市鄉鎮市區現住人口數－按性別、單一年齡及教育程度分」。

表 7：訪問成功樣本之代表性檢定-年齡

年齡	16 歲以上母體結構		調查樣本				卡方檢定 (P 值)
	人數	百分比	加權前		加權後		
			樣本數	百分比	樣本數	百分比	
總計	20,428,315	100.0	1,227	100.0	1,227	100.0	
16~29 歲	3,697,405	18.1	127	10.4	222	18.1	1.000
30~39 歲	3,241,310	15.9	119	9.7	195	15.9	
40~49 歲	3,895,161	19.1	237	19.3	234	19.1	
50~59 歲	3,542,733	17.3	302	24.6	213	17.3	
60~69 歲	3,295,450	16.1	268	21.8	198	16.1	
70 歲以上	2,756,256	13.5	174	14.2	166	13.5	

資料來源：內政部戶政司，「112 年各縣市鄉鎮市區現住人口數－按性別、單一年齡及教育程度分」。

表 8：訪問成功樣本之代表性檢定-教育程度

單位：人；%							
教育程度	16 歲以上母體結構		調查樣本				卡方檢定 (P 值)
	人數	百分比	加權前		加權後		
			樣本數	百分比	樣本數	百分比	
總計	20,428,315	100.0	1,227	100.0	1,227	100.0	
不識字	154,823	0.8	11	0.9	9	0.7	1.000
小學畢業	1,886,501	9.2	34	2.8	109	8.9	
國、初中畢業	3,010,828	14.7	109	8.9	180	14.7	
高中、職畢業	5,167,402	25.3	323	26.3	310	25.3	
專科畢業	3,477,471	17.0	193	15.7	209	17.0	
大學畢業	5,293,949	25.9	416	33.9	323	26.3	
碩士畢業	1,328,691	6.5	134	10.9	81	6.6	
博士畢業	108,650	0.5	7	0.6	6	0.5	

資料來源：內政部戶政司，「112 年各縣市鄉鎮市區現住人口數－按性別、單一年齡及教育程度分」。

表 9：訪問成功樣本之代表性檢定-戶籍縣市

單位：人；%							
戶籍縣市	16 歲以上母體結構		調查樣本				卡方檢定 (P 值)
	人數	百分比	加權前		加權後		
			樣本數	百分比	樣本數	百分比	
總計	20,428,315	100.0	1,227	100.0	1,227	100.0	
新北市	3,551,295	17.4	210	17.1	213	17.4	1.000
臺北市	2,181,376	10.7	135	11.0	131	10.7	
桃園市	1,976,908	9.7	116	9.5	119	9.7	
臺中市	2,441,939	12.0	144	11.7	147	12.0	
臺南市	1,632,829	8.0	103	8.4	98	8.0	
高雄市	2,409,888	11.8	141	11.5	145	11.8	
宜蘭縣	395,455	1.9	23	1.9	24	2.0	
新竹縣	491,923	2.4	29	2.4	30	2.4	
苗栗縣	468,593	2.3	28	2.3	28	2.3	
彰化縣	1,080,601	5.3	66	5.4	65	5.3	
南投縣	424,631	2.1	31	2.5	25	2.0	
雲林縣	585,183	2.9	34	2.8	35	2.9	
嘉義縣	439,983	2.2	26	2.1	26	2.1	
屏東縣	709,205	3.5	43	3.5	43	3.5	
臺東縣	186,539	0.9	12	1.0	11	0.9	
花蓮縣	279,348	1.4	16	1.3	17	1.4	
澎湖縣	96,564	0.5	6	0.5	6	0.5	
基隆市	324,634	1.6	19	1.5	20	1.6	
新竹市	379,090	1.9	22	1.8	23	1.9	
嘉義市	228,261	1.1	14	1.1	14	1.1	
金馬地區	144,070	0.7	9	0.7	9	0.7	

資料來源：內政部戶政司，「112 年各縣市鄉鎮市區現住人口數－按性別、單一年齡及教育程度分」。

二、電話撥號接觸狀況

本次市話調查共使用 49,803 個電話號碼（含傳真機、電話故障、非住宅電話、空號及無人接聽），成功訪問有效樣本數為 1,227 份，訪問成功率（Cooperation Rate）為 22.0%、拒訪率（Refusal Rate）為 15.5%、接觸率（Contact Rate）為 24.2%，如表 10。而 1,227 份有效樣本數，在信心水準 95% 的情況下，抽樣誤差介於±2.80% 之間，請見表 10。

表 10：電話接觸狀況統計表

接觸狀況	撥號數	百分比 (%)	有效撥號 (%)
總計	*66	100.0	100.0
合格樣本			
I.成功訪問	1,227	2.5	5.3
P.約訪	703	1.4	3.1
R.中途拒答與拒訪	3,568	7.2	15.5
NC.無法聯繫（如無人接聽、答錄機等）	12,430	25.0	53.9
O.其他類型（如生理或心理因素無法接受訪問）	71	0.1	0.3
UH.無法判定是否為合格電話數住戶數（如忙線）	5,037	10.1	21.9
UO.其他種類未知類型	4	0.0	0.0
非合格樣本			
公司行號	1,780	3.6	
傳真	1,710	3.4	
空號	23,196	46.6	
暫停使用	49	0.1	
非合格受訪對象（或外國人）	12	0.0	
配額已滿	16	0.0	

資料來源：本計畫自行整理。

註：成功率= $I / (I+P+R+O)$

拒訪率= $R / (I+P+R+O+NC+UH+UO)$

接觸率= $(I+P+R+O) / (I+P+R+O+NC+UH+UO)$

三、 調查結果

為與母體進行比較，本調查結果一律使用加權後之統計結果進行敘述統計與推論統計的結果分析報告，在受訪者的戶籍地址部分，以新北市最多，占 17.4%、其次為臺中市，占 12.0%、第三為高雄市，占 11.8%。居住地部分和戶籍地雖有差異，約 9.6%，但差異不大，請見表 11。

表 11：受訪者戶籍地與居住地分布

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
AREA	戶籍縣市（合併 Q1、Q27、Q28）	新北市	197	16.1	213	17.4
		臺北市	152	12.4	131	10.7
		桃園市	112	9.1	119	9.7
		臺中市	142	11.6	147	12.0
		臺南市	102	8.3	98	8.0
		高雄市	139	11.3	145	11.8
		宜蘭縣	22	1.8	24	1.9
		新竹縣	30	2.4	30	2.4
		苗栗縣	28	2.3	28	2.3
		彰化縣	66	5.4	65	5.3
		南投縣	33	2.7	25	2.1
		雲林縣	34	2.8	35	2.9
		嘉義縣	26	2.1	26	2.2
		屏東縣	47	3.8	43	3.5
		臺東縣	8	0.7	11	0.9
		花蓮縣	18	1.5	17	1.4
		澎湖縣	7	0.6	6	0.5
		基隆市	18	1.5	20	1.6
		新竹市	21	1.7	23	1.9
		嘉義市	14	1.1	14	1.1
		金馬地區	11	0.9	9	0.7
		總數	1,227	100.0	1,227	100.0
Q1	請問您住在哪個縣市？哪個鄉鎮市區？（居住地）	新北市	210	17.1	228	18.6
		臺北市	135	11.0	115	9.4
		桃園市	116	9.5	122	10.0
		臺中市	144	11.7	146	11.9
		臺南市	103	8.4	96	7.8

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
		高雄市	141	11.5	149	12.1
		宜蘭縣	23	1.9	25	2.0
		新竹縣	29	2.4	27	2.2
		苗栗縣	28	2.3	28	2.3
		彰化縣	66	5.4	67	5.5
		南投縣	31	2.5	25	2.0
		雲林縣	34	2.8	34	2.8
		嘉義縣	26	2.1	28	2.3
		屏東縣	43	3.5	39	3.2
		臺東縣	12	1.0	14	1.1
		花蓮縣	16	1.3	15	1.2
		澎湖縣	6	0.5	5	0.4
		基隆市	19	1.5	20	1.7
		新竹市	22	1.8	23	1.8
		嘉義市	14	1.1	13	1.1
		金馬地區	9	0.7	7	0.5
		總數	1,227	100.0	1,227	100.0
Q27	請問您目前居住的地方是您的戶籍所在地嗎？	是【跳問第 29 題】	1,104	90.0	1,110	90.4
		不是	123	10.0	117	9.6
		總數	1,227	100.0	1,227	100.0

受訪者的學歷部分，以大學畢業最多，占 26.3%、其次為高中、職畢業，占 25.3%、第三為專科畢業，占 17.0%。職業部分，以退休最多，占 14.7%、其次技術員及助理專業人員，占 12.2%、第三為事務支援人員，占 11.7%，見表 12。

表 12：受訪者學歷與職業分布

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
Q25	請問您畢業的最高學歷？	不識字	11	0.9	9	0.7
		小學畢業	34	2.8	109	8.9
		國、初中畢業	109	8.9	180	14.7
		高中、職畢業	323	26.3	310	25.3
		專科畢業	193	15.7	209	17.0
		大學畢業	416	33.9	323	26.3

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
		碩士畢業	134	10.9	81	6.6
		博士畢業	7	0.6	6	0.5
		總數	1,227	100.0	1,227	100.0
Q26	請問您的職業？	軍人	2	0.2	2	0.2
		民意代表、主管及經理人員	69	5.6	47	3.9
		專業人員	140	11.4	101	8.2
		技術員及助理專業人員	153	12.5	149	12.2
		事務支援人員	146	11.9	144	11.7
		服務及銷售工作人員	115	9.4	124	10.1
		農、林、漁、牧業生產人員	35	2.9	38	3.1
		技藝有關工作人員	42	3.4	42	3.5
		機械設備操作及組裝人員	60	4.9	72	5.9
		基層技術工及勞力工	26	2.1	34	2.8
		家管	113	9.2	116	9.4
		學生	60	4.9	141	11.5
		在找尋工作或等待恢復工作而無報酬者	17	1.4	16	1.3
		退休	231	18.8	180	14.7
		無業	15	1.2	18	1.4
		拒答/不知道	3	0.2	3	0.3
		總數	1,227	100.0	1,227	100.0

在受訪者的年齡部分，以 40-49 歲最多，占 19.1%、其次為 16~29 歲，占 18.1%、第三為 50~59 歲，占 16.1%，見表 13。

表 13：受訪者年齡分布

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
Q2	請問您是民國幾年出生的？（須年滿 16 歲）	民國 97~84 年（16~29 歲）	127	10.4	222	18.1
		民國 83~74 年（30~39 歲）	119	9.7	195	15.9
		民國 73~64 年（40~49 歲）	237	19.3	234	19.1
		民國 63~54 年（50~59 歲）	302	24.6	213	17.3

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
		民國 53~44 年 (60~69 歲)	268	21.8	198	16.1
		民國 43 年以前%-%- (70 歲以上)	174	14.2	166	13.5
		總數	1,227	100.0	1,227	100.0

本計畫先詢問民眾對該項數位權利與原則是否同意，再詢問就他的理解，認為臺灣在該項數位權利與原則落實的程度。**表 14** 呈現各組數位權利與原則的平均數、標準差以及兩者差分，數位權利與原則同意分數前三高為：「應該要保障兒童和年輕人安全的數位環境和內容」，4.70 分、「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 分、「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 分；落實分數前三高為：「民眾可以在線上論壇、社群媒體獲得更多言論和資訊自由」，3.51 分、「民眾可以容易地在網路上獲取關鍵公共服務」3.36，分、「民眾應該有可以負擔（得起）的高速網路」，3.31 分；差分最大的前三為：「應該要保障兒童和年輕人安全的數位環境和內容」，2.09 分、「民眾在線上的通訊（文字及語音）保密，資料不被外洩」，1.95 分、「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」，1.68 分。請見**表 14**。

表 14：數位權利項目同意-落實平均數與差分

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

項次	題目	同意分數/ 標準差	落實分數/ 標準差	差分
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

本計畫另針對人工智慧議題進行詢問，題目參考中研院社會變遷調查與本計畫自行設計，結果說明如下，對於立法管制人工智慧高達八成民眾同意或非常同意，對於人工智慧服務上線前應該取得合格認證標章更高達九成民眾同意或非常同意，面對管制網路大型數位平台或社群媒體，如 Facebook、YouTube 等，也有七成四的民眾同意或非常同意，這反映對國內加速相關科技立法或修法的需求與期待，請見表 15。

表 15：受訪者對人工智慧管制的看法

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
Q14	請問您同不同意，人工智慧應該立法管制？	非常不同意	12	1.0	12	0.9
		不同意	46	3.7	48	3.9
		普通	4	0.3	8	0.6
		同意	350	28.5	387	31.6
		非常同意	787	64.1	738	60.2
		拒答/不知道	28	2.3	34	2.8
		總數	1,227	100.0	1,227	100.0
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？	非常不同意	12	1.0	13	1.0
		不同意	31	2.5	24	2.0
		普通	3	0.2	6	0.5
		同意	327	26.7	346	28.2
		非常同意	839	68.4	824	67.1
		拒答/不知道	15	1.2	15	1.2
		總數	1,227	100.0	1,227	100.0
Q16	請問您同不同意，（應該要）管制網路大型數位	非常不同意	81	6.6	88	7.2
		不同意	159	13.0	169	13.8
		普通	12	1.0	14	1.2

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
	平台或社群媒體，如 Facebook、YouTube 等？	同意	420	34.2	423	34.5
		非常同意	529	43.1	493	40.2
		拒答/不知道	26	2.1	40	3.3
		總數	1,227	100.0	1,227	100.0

科技執法做為人工智慧應用的一種形式，也有超過六成五的民眾同意或非常同意，當問到有關人工智慧對社會可能的影響，有近七成的民眾認為「雖然有些風險，整體來說仍對社會有利」，代表未來人工智慧的應用應強調風險控制，民眾整體接受意願應該算高，請見表 16。

表 16：受訪者對人工智慧應用的看法

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
Q17	請問您同不同意，使用科技執法？	非常不同意	200	16.3	198	16.2
		不同意	176	14.3	177	14.5
		普通	14	1.1	17	1.4
		同意	505	41.2	503	41.0
		非常同意	316	25.8	315	25.6
		拒答/不知道	16	1.3	17	1.4
		總數	1,227	100.0	1,227	100.0
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	25	2.0	26	2.1
		雖然有些好處，整體來說仍對社會不利	166	13.5	160	13.0
		雖然有些風險，整體來說仍對社會有利	864	70.4	851	69.4
		整體來說一定對社會有利	134	10.9	146	11.9
		拒答/不知道	38	3.1	45	3.6
		總數	1,227	100.0	1,227	100.0

當進一步問到哪些影響，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，擔心的受訪者有 65%；造成錯誤或虛假消息的氾濫，擔心的受訪者有 89%；影響工作機會，擔心的受訪者有 53%；做為犯罪工具，例如詐騙、駭

客攻擊，擔心的受訪者有 95%；被少數人掌控而成為特權工具，擔心的受訪者有 87%；使社會不平等現象更嚴重，例如貧富不均，擔心的受訪者有 73%，見表 17。

表 17：受訪者對人工智慧應用影響的看法

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
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？	非常擔心	287	23.4	267	21.8
		擔心	553	45.1	547	44.6
		無所謂擔不擔心	14	1.1	17	1.4
		不擔心	290	23.6	312	25.4
		非常不擔心	56	4.6	53	4.4
		拒答/不知道	27	2.2	31	2.6
		總數	1,227	100.0	1,227	100.0
Q20	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？	非常擔心	611	49.8	584	47.6
		擔心	504	41.1	510	41.6
		無所謂擔不擔心	8	0.7	11	0.9
		不擔心	72	5.9	87	7.1
		非常不擔心	22	1.8	25	2.0
		拒答/不知道	10	0.8	10	0.8
		總數	1,227	100.0	1,227	100.0
Q21	請問您擔不擔心，人工智慧可能影響您的工作機會？	非常擔心	304	24.8	318	26.0
		擔心	318	25.9	333	27.1
		無所謂擔不擔心	23	1.9	19	1.5
		不擔心	402	32.8	387	31.6
		非常不擔心	167	13.6	158	12.9
		拒答/不知道	13	1.1	12	1.0
		總數	1,227	100.0	1,227	100.0
Q22	請問您擔不擔心，人工智慧可能做為犯罪工具，例如詐騙、駭客攻擊？	非常擔心	912	74.3	891	72.7
		擔心	266	21.7	282	23.0
		無所謂擔不擔心	3	0.2	4	0.3
		不擔心	33	2.7	36	2.9
		非常不擔心	10	0.8	12	0.9
		拒答/不知道	3	0.2	2	0.2
		總數	1,227	100.0	1,227	100.0
Q23	請問您擔不擔心，人工智慧可	非常擔心	732	59.7	705	57.4
		擔心	354	28.9	370	30.1

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
	能被少數人掌控而成為特權工具？	無所謂擔不擔心	5	0.4	6	0.5
		不擔心	98	8.0	108	8.8
		非常不擔心	25	2.0	26	2.1
		拒答/不知道	13	1.1	13	1.0
		總數	1,227	100.0	1,227	100.0
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？	非常不同意	470	38.3	441	36.0
		不同意	443	36.1	457	37.3
		普通	13	1.1	14	1.1
		同意	241	19.6	243	19.8
		非常同意	41	3.3	47	3.8
		拒答/不知道	19	1.5	24	2.0
		總數	1,227	100.0	1,227	100.0

第五章 結論與政策建議

本計畫透過文獻回顧，蒐集西班牙、美國、法國與我國的臉部辨識爭議法律案件；並訪談公部門使用臉部辨識的單位，以及提供服務的廠商，以了解近年我國機關單位使用臉部辨識技術可能的情境與資安管理議題；針對數位權利與原則議題，參考歐盟數位十年調查，與中研院社會變遷調查，以家戶電話訪問的調查方式，對數位權利與原則的認知與落實情形之落差加以調查，並於 2024 年 4 月 8 日召開專家會議，邀集產官學民各界專家²⁶，解讀民眾對數位權利與原則的意見態度，據此提供政策建議和後續研析建議。計畫結果發現：政府應持續加強對各項數位權利與原則的保障與提升，特別是新興科技（如人工智慧）；公務單位若將臉部辨識使用於門禁差勤，對數位權利的侵害與影響較小，彙整本計畫各結論與政策建議如後。

第一節 研究結論

（1）民眾對數位權利與原則之觀念與歐盟相近，但對我國數位權利與原則之落實不滿。

11 項數位權利與原則的平均分數為 4.31 分，顯示民眾對各項目均高度認同，但各項目的落實平均分數僅 2.93，應有可提升的空間。肯定分數最高的三項分別為：「應該要保障兒童和年輕人安全的數位環境和內容」、「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」、「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」。

第二項「個人資料的控制權」恰與數位部近年推動之「隱私強化技術應用指引」、「個人資料自主應用」(MyData)、「電子簽章法」有關，加上我國持續推動個人資料保護法修法，以及個人資料保護委員會，對此項數位權利與原則之保障應可有效落實。

至於第一與第三項，本計畫認為業務主管機關涉及跨部會業務，如 NCC、衛福部、勞動部，值得注意的是：「應該要保障兒童和年輕人安全的數位環境和內容」與「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」，是落實滿意度最差的兩項，應有賴相關單位的推動。

（2）民眾對新興科技的使用（人工智慧）的看法認為「雖然有些風險，整體來說仍對社會有利」與「整體來說一定對社會有利」有 80%，但若細究其影響，對造成錯誤或虛假消息的氾濫、詐騙等仍高度擔心。

²⁶ 與會專家名單：朱景鵬 / 東華大學公共行政學系 歐盟莫內講座教授兼副校長、李欣穎 / 開放文化基金會 執行長、陳正然 / 數位經濟暨產業發展協會 理事長、陳恭 / 政治大學資訊管理學系 教授、蕭乃沂 / 政治大學公共行政學系 副教授兼系主任。

逾九成民眾同意或非常同意，人工智慧服務上線前應該取得合格認證標章，以及應立法管制，反映對國內加速相關科技立法或修法的需求與期待，例如歐盟近年推動人工智慧法，美國也有 AI 單一入口網整理聯邦政府的 AI 應用。

AI 風險部分，本計畫參考中研院社會變遷調查，詢問了 6 題與民眾切身相關的影響，包含「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」、「造成錯誤或虛假消息的氾濫」、「影響工作機會」、「做為犯罪工具，例如詐騙、駭客攻擊」、「被少數人掌控而成為特權工具」、「使社會不平等現象更嚴重，例如貧富不均」，最多人擔心的項目是：做為犯罪工具，例如詐騙、駭客攻擊，高達 95%，顯示民眾仍最關心政府打詐，防詐以及相關措施，數位部推動政府簡訊「111」、運用「詐騙樣態分析」技術自動掃描網路廣告進行樣態分類、風險評級與詐騙行為分析、通報數位平臺核對處理，或 TWNIC 啟動 DNS RPZ 停止解析網域等措施，未來可能也需因應 AI 樣態的詐騙進行技術或與機關單位聯防等措施。

(3) 臉部辨識在公部門以差勤應用為主，職員影像拍照後轉存特徵值進行辨識，特徵值無法反向重現人臉，且伺服器保存地端，不以遠端操作方式維護，應可有效保護資料不外洩。

本計畫建議「公務機關使用臉部辨識技術時，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」，經訪談發現：目前公務機關之應用多以差勤應用為主，受訪單位表示同仁照片一經轉存為特徵值後即刪除，特徵值無法反向重現人臉，若同仁離職，系統也會於七日刪除檔案，若辨識不易或系統出現異常，廠商需到現場維護，無法以遠端操作，故應可有效保護資料不外洩。

(4) 若非差勤使用，而將辨識應用於身形、人數、性別等，亦為影像辨識之可能應用，業界對於此商業模式較不看好，目前多為特定機關的應用，如高鐵對月台候車人數的估計。

第二節 政策建議

(1) 建立公部門臉部辨識使用原則和例外排除的指引

透過對現行中央與地方政府使用臉部辨識於差勤打卡，或其他使用方式（如治安維護）之盤點，完善臉部辨識使用指引，中長期或可建立共同供應契約之規格與資安要求。對於導入新興科技之機關單位，也要有除錯機制的建立，以免機關單位因不了解或誤解法令，而投入儀器設備的建置與應用，但之後又無法利用。

(2) 發展臉部辨識使用稽核與行政處理流程

機關單位若有違反個人資料蒐集、處理與利用之規範，除應遵循個人資料保護法之規範，對於請求停止蒐集、處理或利用，機關單位應有清楚流程，舉例來說，若為差勤打卡使用，則人事室應需有相關作業規範，且應有臉部辨識使用稽核措施，以落實資料保護與資安規範。

（3）應重視數位權利與原則，建立我國規範與政策連結

依本計畫調查結果，民眾對歐盟數位權利與原則項目有高度認同，不過考量國情不同，建議我國應有符合我國情與政策方向之數位權利與原則，並和各部會未來施政方向連結，以落實數位權利與原則的保障，特別是針對民眾覺得落實程度不高的項目，宜納入政策之優先考量。

（4）考量科技發展，深化民眾數位素養教育與公部門應用

由於科技發展快速，亦須加強民眾數位素養教育，以充分賦能民眾，才有可能應變真假訊息，或 AI 自動化決策的應用（如金融產品）。本計畫報告完成之時正遇上 2024 年 4 月 3 日強震，應持續推動公部門導入新興科技與人工智慧，應用於防救災、民生議題、國土安全、淨零等領域，對於數位轉型優異之單位，可參考「政府服務獎」數位創新加值的敘獎鼓勵。

（5）持續精進調查方式與擴大調查對象

本計畫以電話調查方式，以 16 歲以上民眾為調查對象，完成 1,227 份有效樣本，為國內首次進行之數位權利與原則調查，考量數位部現行之「111 年數位發展調查報告」採市話及手機雙底冊隨機抽樣調查，完成 15,142 份有效樣本，未來數位權利與原則調查應可獨立或納入辦理，同時依照需要針對不同對象與族群擴大辦理（如兒少、原住民、新住民、或高齡長者等），此外，亦可增加數位能力或科技使用經驗等題目，以了解不同數位素養民眾對數位權利與原則落實情形的看法。

參考文獻

一、 中文文獻

人權公約施行監督聯盟（2022）。兩公約第二次審查。2023 年 11 月 01 日，
<https://covenantwatch.org.tw/2021-third-review-on-iccpr-and-icescr/>。

FaceMe（2023）。人臉辨識應用最新趨勢，6 大產業領域一次了解！2023 年 6 月 16 日，
取自：https://tw.cyberlink.com/faceme/insights/articles/236/how_is_facial_recognition_used_in_2021。

司法院（2021）。宜蘭地方法院 110 年度簡字第 749 號刑事判決，2021 年 11 月，取自：<https://judgment.judicial.gov.tw/FJUD/default.aspx>。

司法院（2020）。臺北高等行政法院 109 年度訴字第 912 號判決，2020 年 5 月，
取自：<https://judgment.judicial.gov.tw/FJUD/default.aspx>。

司法院（2020）。臺南地方法院 109 年度交字第 200 號判決，2020 年 01 月，取自：<https://judgment.judicial.gov.tw/FJUD/default.aspx>。

法務部（2020）。法矯署安字 1120400171 號，2020 年 03 月，取自：
<https://mojlaw.moj.gov.tw/LawContentExShow.aspx?id=FE367325&type=E&kw=%E7%94%9F%E7%89%A9%E7%89%B9%E5%BE%B5&etype=etype5>。

法務部（2017）。法律字第 1000015826 號，2017 年 07 月，取自：
<https://mojlaw.moj.gov.tw/LawContentExShow.aspx?id=FE241587&type=E&kw=&etype=etype5>。

柯皓仁（2019）。圖書館資訊科技與應用。中華民國圖書館年鑑。108。211-213。

桃園國際機場（2022）。刷臉走遍機場，One ID 試辦計畫開跑。桃園國際機場季刊，3，4-5。

許慧瑩、張鐙文（2022）。政府公共服務應用臉部辨識技術之規範架構研究。數位發展部委託研究（編號：MODA-DODS-111-003），未出版）。

國家發展委員會（2021）。發法字第 1100005839 號，2021 年 04 月，取自：
<https://theme.ndc.gov.tw/lawout/LawContent.aspx?media=print&id=GL000382>。

張忠義（2017）。大數據拼商機，人臉辨識系統進駐高雄捷運。自由時報，2017 年 12 月 1 日，<https://news.ltn.com.tw/news/life/breakingnews/2270884>。

黃靜萍（2018）。新北圖書館人臉辨識，首創刷臉入館借還書，2018 年 8 月 1 日，
<https://www.cardu.com.tw/news/detail.php?36262>。

萬容均（2020）。地政業務應用人臉辨識系統研析－以核對身分為例。宜蘭縣政府暨所屬機關自行研究報告。

新北縣政府（2017）。竹警運用工研院人臉辨識技術，協助維護 2017 臺北世大運入場安全，2017 年 8 月 17 日，
https://www.hsinchu.gov.tw/News_Content.aspx?n=153&s=98250。

二、 英文文獻

- AEPD (Spain) (2019). AEPD (Spain)-PS/00078/2021, GDPRhub.08.01.2019, from [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-PS/00078/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-PS/00078/2021).
- AEPD (Spain) (2021). AEPD (Spain)-PS/00120/2021, GDPRhub. 26.07.2021, from [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-PS/00120/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-PS/00120/2021).
- APDCAT(Catalonia) (2019). APDCAT(Catalonia)-PS/49/2019, GDPRhub. 03.31.2019, from [https://gdprhub.eu/index.php?title=APDCAT_\(Catalonia\)_-PS_49/2019](https://gdprhub.eu/index.php?title=APDCAT_(Catalonia)_-PS_49/2019).
- BIG BROTHER WATCH (2023). BIOMETRIC BRITAIN: The Expansion of Facial Recognition Surveillance, from https://bigbrotherwatch.org.uk/wp_content/uploads/2023/05/Biometric-Britain.pdf.
- CE(France) (2020). CEN°432656, GDPRhub, 04.11.2020, from https://gdprhub.eu/index.php?title=CE_-N%C2%B0_432656.
- CNIL(France) (2022). CNIL - Délibération SAN-2022-019, GDPRhub, 17.10.2022, from [https://gdprhub.eu/index.php?title=CNIL_\(France\)_-SAN-2022-019](https://gdprhub.eu/index.php?title=CNIL_(France)_-SAN-2022-019).
- Council of the European Union (2022). 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. Retrieved November 25, 2022, from <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.
- Sophia Waterfield (2023). Council breached GDPR in deploying facial recognition technology in schools – ICO. Techmonito, February 1, 2023, from <https://techmonito.r.ai/policy/privacy-and-data-protection/facial-recognition-technology-school-ico>.
- Datatilsynet(Denmark) (2020). Datatilsynet (Denmark), GDPRhub, 04.23.2020, from [https://gdprhub.eu/index.php?title=Datatilsynet_\(Denmark\)_-2020-432-0034](https://gdprhub.eu/index.php?title=Datatilsynet_(Denmark)_-2020-432-0034).
- DLA PIPER (2019). EDPB Issues Guidelines on Processing of Personal Data Through Video Devices, Retrieved July 23, 2019, from <https://privacymatters.dlapiper.com>.
- European Commission (2023). European Digital Rights and Principles. Retrieved September 01, 2023, from <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>.
- European Parliament (2023). Artificial Intelligence Act. Retrieved June 14, 2023, from https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

European Council (2022). Artificial Intelligence Act. Council Calls for Promoting Safe AI That Respects Fundamental Rights. Retrieved December 6, 2022, from <https://www.consilium.europa.eu/en/press/press->.

EU AI Act (2023). European Parliament, First Regulation on Artificial Intelligence. Retrieved August 6, 2023, from <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.

European-American Chamber of Commerce (2022). Digital Rights and Principles: Presidents of the Commission, the European Parliament and the Council Sign European Declaration. Retrieved December 16, 2022, from <https://eaccny.com/news/chapters/digital-rights-and-principles-presidents-of-the-commission-the-european-parliament-and-the-council-sign-european-declaration/>.

European Commission (2022). Digital Economy and Society Index (DESI) 2022. Retrieved July 28, 2022, from <https://digitalstrategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>.

European Parliament (2023). DRAFT Compromise Amendments. Retrieved May 9, 2023, from https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/Committee/ES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf.

European Commission (2023). Special Eurobarometer SP532 : The Digital Decade. Retrieved June 14, 2023, from https://data.europa.eu/data/datasets/s2959_99_1_sp532_eng?locale=en.

European Commission (2023). The Digital Decade. Retrieved June. From <https://europa.eu/eurobarometer/surveys/detail/2959>.

European Commission (2023). Report on the State of the Digital Decade. Retrieved September 27, 2023, from <https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade>.

European Commission (2023). European Digital Rights and Principles. Retrieved June 19, 2023, from <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>.

Garante per la protezione dei dati personali (Italy) (2023). Garante per la protezione dei dati personali – 9896808, Retrieve March 31, 2024, from [https://GDPRhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9896808](https://GDPRhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9896808).

Garante per la protezione dei dati personali (Italy) (2023). Garante per la protezione dei dati personali, Retrieved March 31, 2024, from [https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9751362](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9751362).

GDPR HUB (2021). AEPD (Spain) - PS/00120/2021. Retrieved August 5, 2021, from [https://gdprhub.eu/index.php?title=AEPD \(Spain\)-_PS/00120/2021](https://gdprhub.eu/index.php?title=AEPD%20(Spain)-_PS/00120/2021).

Scott Bicheno (2023). GSMA fined €200,000 for MWC facial recognition GDPR infringement, Retrieved March 31, 2024, from <https://www.telecoms.com/virtualization/gsma-fined-200-000-for-mwc-facial-recognition-gdpr-infringement>.

Regulatory Sandbox Final Report: Heathrow Airport Ltd (2020), ICO, Retrieved April 01,2024, from <https://ico.org.uk/media/fororganisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf>.

Scott, M., Cerulus, L., & Vinocur, N. (2019). Europe eyes stricter rules on facial recognition. Retrieved July 9, 2019, from <https://www.politico.eu/article/europe-facial-recognition-facebook-privacy-data-protection/>.

STATESCOOP (2023). States warned about facial recognition for unemployment claims. Retrieved April 6, 2023, from <https://statescoop.com/labor-dept-inspector-general-warns-states-facial-recognition-unemployment/>.

Takhar, J. (2023). EU AI Act: Top 10 Changes in the Latest Draft. Connect On Tech. Retrieved May 5, 2023, from <https://www.connectontech.com/eu-ai-act-top-10-changes-in-the-latest-draft/>.

U.S. Department of Labor (2023). Office of inspector General Washington, DC 20210. Retrieved March 31, 2023, from <https://www.oig.dol.gov/public/reports/oa/2023/19-23-005-03-315.pdf>.

附錄

附錄一、歐盟數位十年問卷摘錄

問題	選項
1. 您的最高學歷是？（D8c）	
2. 性別（D10）	
3. 您幾歲？（D11）	
1. 您目前的職業是什麼？（D15a）	
2. 請問您是否在家中使用網際網路？（D62.1）	☐ 是 ☐ 否
3. 您是否在工作場所使用網際網路？（D62.2）	☐ 是 ☐ 否
4. 您是否在您的行動裝置上使用網際網路（筆記型電腦、智能手機、平板電腦等）？（D62.3）	☐ 是 ☐ 否
5. 您是否在其他地方使用網際網路（學校、大學、網咖等）？（D62.4）	☐ 是 ☐ 否
6. 當您和朋友或親戚聚在一起時，您對於國內政治事務討論頻率為何？（D71.1）	☐ 經常 ☐ 偶爾 ☐ 從不討論
7. 當您和朋友或親戚聚在一起時，您對於地方政治事務討論頻率為何？（D71.2）	☐ 經常 ☐ 偶爾 ☐ 從不討論
8. 在這次訪問之前，您是否知道那些線下適用的權利也應該在線上受到尊重？（QB6.）	☐ 是 ☐ 否 ☐ 不知道
9. 您認為歐盟在數位環境中保護您的權利做得有多好？（QB7.）	☐ 是 ☐ 否 ☐ 不知道
10. 您認為在我們的國家，數位權利和原則在以下方面得到了多大程度的應用...？	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(1) 讓歐盟每個人都能獲得負擔得起的高速網路連接（QB8.1.）	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(2) 獲得基本和進階數位教育、培訓和技能（QB8.2.）	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道

問題	選項
(3) 在數位環境中獲得公平且健康的工作條件，包含工作和生活平衡 (QB8.3.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(4) 輕鬆在歐盟內線上獲取所有關鍵公共服務 (QB8.4.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(5) 獲得有效的自主線上選擇，包含與人工智慧互動（如聊天機器人、數位助手） (QB8.5.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(6) 獲得可信賴、多元且多語言的數位環境，包括更多元的內容、較少虛假訊息以及較少非法內容 (QB8.6.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(7) 於線上獲得更多言論和資訊自由，例如透過線上平臺、社交網路和搜尋引擎 (QB8.7.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(8) 在數位環境中獲得集會和結社自由 (QB8.8.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(9) 獲得安全和尊重隱私的數位技術的使用權 (QB8.9.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(10) 獲得線上隱私，即尊重通訊和設備上訊息的保密性 (QB8.10.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(11) 獲得對自己的資料的控制權，即資料在線上如何使用以及與誰分享 (QB8.11.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(12) 掌控自己的數位遺產，例如在自己離世後決定個人帳戶和訊息的處理方式 (QB8.12.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(13) 確保為兒童和年輕人提供安全的數位環境和內容 (QB8.13.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(14) 獲得對環境和社會造成最小化損害的數位產品和服務（如可修復或回收的產品和服務，不牽涉強迫勞動） (QB8.14.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道
(15) 獲得有關數位技術對環境影響和能源消耗的正確資訊 (QB8.15.)	☐ 非常好 ☐ 相當好 ☐ 不太好 ☐ 一點也不好 ☐ 不知道

附錄二、PEW 研究中心 AI 問卷摘錄

問題	選項
1. 人工智慧電腦程式旨在學習人類通常執行的任務，例如識別語音或圖片。總體來說，您是否認為日常生活中人工智慧電腦程式的使用增加讓您感覺...	☐ 興奮大於擔心 ☐ 擔心大於興奮 ☐ 既擔心又興奮 ☐ 沒答案
2. 如果人工智慧電腦程式能夠執行以下各項操作，您會感到興奮或擔心？	☐ 很興奮 ☐ 有些興奮 ☐ 既擔心又興奮 ☐ 有些擔心 ☐ 非常擔心 ☐ 沒答案
3. 對於日常生活中人工智慧電腦程式的使用增加，您更擔心而不是興奮的主要原因是什麼？	開放式回答
4. 對於日常生活中人工智慧電腦程式的使用增加，您更興奮而不是擔心的主要原因是什麼？	開放式回答
5. 您認為警察廣泛使用臉部辨識技術會是...	☐ 對社會來說是好主意 ☐ 對社會來說是壞主意 ☐ 不確定 ☐ 沒答案
6. 您是否認為社交媒體公司廣泛使用電腦程式在其網站上尋找虛假資訊是...	☐ 對社會來說是好主意 ☐ 對社會來說是壞主意 ☐ 不確定 ☐ 沒答案
7. 您認為無人駕駛汽車的廣泛使用會是...	☐ 對社會來說是好主意 ☐ 對社會來說是壞主意 ☐ 不確定 ☐ 沒答案
8. 想想設計人工智慧電腦程式的人，您認為他們對以下每個人的經驗和觀點的考慮程度如何？	☐ 很好 ☐ 還不錯 ☐ 不太好 ☐ 一點都不好 ☐ 不確定 ☐ 沒答案

附錄三、本計畫數位權利與原則問卷

政府機關臉部辨識運用研析 - 以數位權利與原則為框架

家戶電訪調查問卷

您好：

我們是政治大學數位治理研究中心，接受數位發展部的委託，希望瞭解民眾對於新興科技（如人工智慧 AI）與其相關數位權利的看法。打擾您幾分鐘的時間（約 10 分鐘），詢問您對於一些關於新興科技的看法，您的回答對未來我國推動相關政策將有相當大的幫助。

您所填答的資料將僅供學術研究之用，不會有任何不當的引用或個人資料洩露。

如果對本調查有疑問，歡迎來電查詢 06-213-3111 # 931 曾憲立老師

※方便聯繫的時間：周一至周五 中午 12:30-14:00

在調查開始之前想請問：

1	請問您住在哪個縣市？哪個鄉鎮市區？（居住地）
2	請問您是民國幾年出生的？（須年滿 16 歲）

題號	題目
	我國跟許多先進國家一樣，重視人民的基本數位權利，以下有幾項關於數位權利的說法，想詢問您的看法及臺灣的落實（實際執行）情形。
3	請問您同不同意，民眾應該有可以負擔（台語：得起）的高速網路？（QB8.1.） ☐ （01）非常不同意 ☐ （02）不同意 ☐ （03）普通 ☐ （04）同意 ☐ （05）非常同意 ☐ （99）拒答/不知道
3-1	就您的理解，請問您認為臺灣在「民眾應該有可以負擔（台語：得起）的高速網路」方面，落實的好不好？（QB8.1.） ☐ （01）非常不好 ☐ （02）不好 ☐ （03）普通 ☐ （04）好 ☐ （05）非常好 ☐ （99）拒答/不知道

題號	題目
4	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？（QB8.2.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道 【如果受訪者有問再進行說明】 ※數位教育，係指學習者透過網際網的方式來傳遞、學習內容（學習過程中，可能沒有人與人的直接接觸）。 舉例來說：利用公司網路來為員工提供訓練課程。 ※基礎數位教育：基礎使用 ※進階數位教育：程式語言
4-1	就您的理解，請問您認為臺灣在「民眾應有接受到基礎與進階的數位教育的權利」方面，落實的好不好？（QB8.2.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道
5	請問您同不同意，在數位環境下，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？（QB8.3.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道
5-1	就您的理解，請問您認為臺灣在數位環境下「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）」方面，落實的好不好？（QB8.3.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道
6	請問您同不同意，民眾可以容易地（台語：簡單）在網路上獲取關鍵（台語：主要且重要）公共服務？（QB8.4.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道 【如果受訪者有問再進行說明】 ※公共服務，是藉由公共部門，或間接的方式，提供給其轄地的居民，所有人都有資格享受服務。 舉例來說：交通運輸、垃圾處理、教育/文化設施、醫院、消防隊、提供安全保障、社會福利、職業培訓等。
6-1	就您的理解，請問您認為臺灣在「民眾可以容易（台語：簡單）在網路上獲取關鍵（台語：主要且重要）公共服務」方面，落實的好不好？（QB8.4.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道

題號	題目
7	請問您同不同意，民眾可以自主決定要不要在網路上與 AI 互動？（QB8.5.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道 ※如果受訪者不理解，請說明： AI 指的是一套技術，讓電腦執行網路搜尋、理解及翻譯語音和文字、分析資料以及製作圖片。
7-1	就您的理解，請問您認為臺灣在「民眾可以自主決定要不要在網路上與 AI 互動」方面，落實的好不好？（QB8.5.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道
8	請問您同不同意這樣的說法，民眾可以獲得可信賴、多元或多語系的數位環境？（QB8.6.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道 ※如果受訪者不理解可信賴、多元或多語系的數位環境，可以舉例說明：更多元的內容、較少爭議訊息與非法內容。
8-1	就您的理解，請問您認為臺灣在「民眾可以獲得可信賴、多元或多語系的數位環境」方面，落實的好不好？（QB8.6.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道
9	請問您同不同意，民眾可以在線上（台語：網路）論壇、社群媒體獲得更多言論和資訊自由？（QB8.7.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道
9-1	就您的理解，請問您認為臺灣在「民眾可以在線上（台語：網路）論壇、社群媒體獲得更多言論和資訊自由」方面，落實的好不好？（QB8.7.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道
10	請問您同不同意，民眾可以獲得安全和尊重個人隱私的數位服務？（QB8.9.） ☐（01）非常不同意 ☐（02）不同意 ☐（03）普通 ☐（04）同意 ☐（05）非常同意 ☐（99）拒答/不知道
10-1	就您的理解，請問您認為臺灣在「民眾可以獲得安全和尊重個人隱私的數位服務」方面，落實的好不好？（QB8.9.） ☐（01）非常不好 ☐（02）不好 ☐（03）普通 ☐（04）好 ☐（05）非常好 ☐（99）拒答/不知道

題號	題目
	(05) 非常好 ☐ (99) 拒答/不知道
11	請問您同不同意，民眾在線上（台語：網路）的通訊（文字及語音）保密，資料不被外洩？（QB8.10.） ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
11-1	就您的理解，請問您認為臺灣在「民眾在線上（台語：網路）的通訊（文字及語音）保密，資料不被外洩」方面，落實的好不好？（QB8.10.） ☐ (01) 非常不好 ☐ (02) 不好 ☐ (03) 普通 ☐ (04) 好 ☐ (05) 非常好 ☐ (99) 拒答/不知道
12	請問您同不同意，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？（QB8.11.） ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
12-1	就您的理解，請問您認為臺灣在「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」方面，落實的好不好？（QB8.11.） ☐ (01) 非常不好 ☐ (02) 不好 ☐ (03) 普通 ☐ (04) 好 ☐ (05) 非常好 ☐ (99) 拒答/不知道
13	請問您同不同意，應該要保障兒童和年輕人安全的數位環境和內容？（QB8.13.） ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
13-1	就您的理解，請問您認為臺灣在「保障兒童和年輕人安全的數位環境和內容」方面，落實的好不好？（QB8.13.） ☐ (01) 非常不好 ☐ (02) 不好 ☐ (03) 普通 ☐ (04) 好 ☐ (05) 非常好 ☐ (99) 拒答/不知道
14	簡單向您說明一下，【人工智慧】如生成式 AI 指的是一套技術，可讓電腦執行網路搜尋、理解及翻譯語音和文字、分析資料以及製作圖片等。 請問您同不同意，人工智慧應該立法管制？ ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
15	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？ ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
16	請問您同不同意，管制網路大型數位平台或社群媒體？（如

題號	題目
	Facebook、YouTube 等) ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
17	簡單向您說明一下，【科技執法】是使用科技設備取代人力為主的違規舉發（台語：報）方式，例如利用科技設備對全時段（台語：24 小時）或特定時段自動偵測交通違規，並逕行拍照或攝影（台語：錄影）告發。 請問您同不同意，使用科技執法？ ☐ (01) 非常不同意 ☐ (02) 不同意 ☐ (03) 普通 ☐ (04) 同意 ☐ (05) 非常同意 ☐ (99) 拒答/不知道
18	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？ ☐ (01) 整體來說一定對社會不利 ☐ (02) 雖然有些好處，整體來說仍對社會不利 ☐ (03) 雖然有些風險，整體來說仍對社會有利 ☐ (04) 整體來說一定對社會有利 ☐ (99) 拒答/不知道
	有些人認為人工智慧會產生一些負面的影響，想請教您的看法
19	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，不利於特定族群？ ☐ (01) 非常擔心 ☐ (02) 擔心 ☐ (03) 無所謂擔不擔心 ☐ (04) 不擔心 ☐ (05) 非常不擔心 ☐ (99) 拒答/不知道
20	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？ ☐ (01) 非常擔心 ☐ (02) 擔心 ☐ (03) 無所謂擔不擔心 ☐ (04) 不擔心 ☐ (05) 非常不擔心 ☐ (99) 拒答/不知道
21	請問您擔不擔心，人工智慧可能影響您的工作機會？ ☐ (01) 非常擔心 ☐ (02) 擔心 ☐ (03) 無所謂擔不擔心 ☐ (04) 不擔心 ☐ (05) 非常不擔心 ☐ (99) 拒答/不知道
22	請問您擔不擔心，人工智慧可能做為犯罪工具，例如詐騙、駭客攻擊？ ☐ (01) 非常擔心 ☐ (02) 擔心 ☐ (03) 無所謂擔不擔心 ☐ (04) 不擔心 ☐ (05) 非常不擔心 ☐ (99) 拒答/不知道
23	請問您擔不擔心，人工智慧可能被少數人（台語：小部分）掌控（台語：控制）而成為特權工具？ ☐ (01) 非常擔心 ☐ (02) 擔心 ☐ (03) 無所謂擔不擔心 ☐ (04) 不擔心 ☐ (05) 非常不擔心 ☐ (99) 拒答/不知道
24	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？

題號	題目
	☐ (01) 非常擔心 ☐ (02) 擔心 ☐ (03) 無所謂擔不擔心 ☐ (04) 不擔心 ☐ (05) 非常不擔心 ☐ (99) 拒答/不知道
	最後，想請問您幾個基本資料
25	請問您畢業的最高學歷？ ☐ (01) 不識字 ☐ (02) 小學畢業 ☐ (03) 國、初中畢業 ☐ (04) 高中、職畢業 ☐ (05) 專科畢業 ☐ (06) 大學畢業 ☐ (07) 碩士畢業 ☐ (08) 博士畢業 ☐ (09) 其他（請說明） _____ ☐ (99) 拒答/不知道
26	請問您的職業？ ☐ (01) 軍人 ☐ (02) 民意代表、主管及經理人員 ☐ (03) 專業人員 ☐ (04) 技術員及助理專業人員 ☐ (05) 事務支援人員 ☐ (06) 服務及銷售工作人員 ☐ (07) 農、林、漁、牧業生產人員 ☐ (08) 技藝有關工作人員 ☐ (09) 機械設備操作及組裝人員 ☐ (10) 基層技術工及勞力工 ☐ (11) 家管 ☐ (12) 學生 ☐ (13) 在找尋工作或等待恢復工作而無報酬者 ☐ (14) 退休 ☐ (15) 其他（請說明）_____ ☐ (99) 拒答/不知道 ※受訪者年齡：[套受訪者在第二題回答的答案]
27	請問您目前居住的地方是您的戶籍所在地嗎？（同一個鄉鎮市區） ☐ (01) 是【跳問第 29 題】 ☐ (02) 不是 ※如果受訪者回答不出來，可以改問：請問您的戶籍也是在 [套受訪者在第一題回答的答案] 嗎？
28	請問您的戶籍地是在哪個縣市？哪個鄉鎮市區？ ※如果受訪者回答不出來，可以改問：請問您的戶籍也是在 [套受訪者在第一題回答的答案] 嗎？
29	請問您的性別？（訪員判斷不出才問） ☐ (01) 男性 ☐ (02) 女性
	謝謝您協助本計畫的調查 我們保證，您所填答的資料僅提供學術研究之用，遵守個人資料保護法，不會有任何不當的引用。

附錄四、數位權利與原則問卷調查結果

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
Q3	請問您同不同意，民眾應該有可以負擔（得起）的高速網路？（QB8.1.）	非常不同意	12	1.0	8	0.6
		不同意	45	3.7	51	4.2
		普通	6	0.5	8	0.6
		同意	663	54.0	695	56.7
		非常同意	452	36.8	406	33.1
		拒答/不知道	49	4.0	59	4.8
		總數	1,227	100.0	1,227	100.0
Q3_1	就您的理解，請問您認為臺灣在「民眾應該有可以負擔的高速網路」方面，落實的好不好？（QB8.1.）	非常不好	109	8.9	91	7.4
		不好	383	31.2	355	28.9
		普通	64	5.2	66	5.4
		好	509	41.5	550	44.8
		非常好	73	5.9	68	5.5
		拒答/不知道	89	7.3	98	8.0
		總數	1,227	100.0	1,227	100.0
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？（QB8.2.）	非常不同意	6	0.5	6	0.5
		不同意	20	1.6	27	2.2
		普通	4	0.3	4	0.3
		同意	587	47.8	614	50.0
		非常同意	604	49.2	566	46.1
		拒答/不知道	6	0.5	9	0.8
		總數	1,227	100.0	1,227	100.0
Q4_1	就您的理解，請問您認為臺灣在「民眾應有接受到基礎與進階的數位教育的權利」方面，落實的好不好？（QB8.2.）	非常不好	149	12.1	133	10.9
		不好	479	39.0	437	35.6
		普通	77	6.3	75	6.1
		好	373	30.4	429	35.0
		非常好	54	4.4	62	5.1
		拒答/不知道	95	7.7	90	7.4
		總數	1,227	100.0	1,227	100.0
Q5	請問您同不同意，在數位環境下，民眾應得到	非常不同意	6	0.5	6	0.5
		不同意	19	1.5	28	2.3
		普通	-	-	-	-

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
	公平且健康的工作環境，包含工作與生活的平衡？（QB8.3.）	同意	525	42.8	521	42.5
		非常同意	666	54.3	660	53.8
		拒答/不知道	11	0.9	12	1.0
		總數	1,227	100.0	1,227	100.0
Q5_1	就您的理解，請問您認為臺灣在數位環境下「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）」方面，落實的好不好？（QB8.3.）	非常不好	171	13.9	157	12.8
		不好	468	38.1	449	36.6
		普通	63	5.1	54	4.4
		好	385	31.4	418	34.1
		非常好	52	4.2	58	4.7
		拒答/不知道	88	7.2	91	7.5
		總數	1,227	100.0	1,227	100.0
Q6	請問您同不同意，民眾可以容易地在網路上獲取關鍵公共服務？（QB8.4.）	非常不同意	12	1.0	11	0.9
		不同意	53	4.3	58	4.7
		普通	7	0.6	5	0.4
		同意	571	46.5	581	47.4
		非常同意	563	45.9	544	44.3
		拒答/不知道	21	1.7	29	2.3
		總數	1,227	100.0	1,227	100.0
Q6_1	就您的理解，請問您認為臺灣在「民眾可以容易地在網路上獲取關鍵公共服務」方面，落實的好不好？（QB8.4.）	非常不好	95	7.7	78	6.3
		不好	329	26.8	303	24.7
		普通	52	4.2	44	3.6
		好	568	46.3	601	49.0
		非常好	129	10.5	141	11.5
		拒答/不知道	54	4.4	60	4.9
		總數	1,227	100.0	1,227	100.0
Q7	請問您同不同意，民眾可以自主決定要不要在網路上與 AI 互動？（QB8.5.）	非常不同意	50	4.1	49	4.0
		不同意	124	10.1	119	9.7
		普通	6	0.5	10	0.8
		同意	603	49.1	602	49.1
		非常同意	404	32.9	399	32.5
		拒答/不知道	40	3.3	48	3.9
		總數	1,227	100.0	1,227	100.0
Q7_1		非常不好	169	13.8	142	11.6

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
	就您的理解，請問您認為臺灣在「民眾可以自主決定要不要在網路上與 AI 互動」方面，落實的好不好？（QB8.5.）	不好	427	34.8	394	32.1
		普通	56	4.6	53	4.3
		好	332	27.1	378	30.8
		非常好	68	5.5	90	7.4
		拒答/不知道	175	14.3	169	13.8
		總數	1,227	100.0	1,227	100.0
Q8	請問您同不同意這樣的說法，民眾可以獲得可信賴、多元或多語系的數位環境？（QB8.6.）	非常不同意	46	3.7	47	3.9
		不同意	94	7.7	96	7.8
		普通	9	0.7	9	0.7
		同意	628	51.2	636	51.8
		非常同意	417	34.0	403	32.9
		拒答/不知道	33	2.7	35	2.8
		總數	1,227	100.0	1,227	100.0
Q8_1	就您的理解，請問您認為臺灣在「民眾可以獲得可信賴、多元或多語系的數位環境」方面，落實的好不好？（QB8.6.）	非常不好	140	11.4	120	9.8
		不好	450	36.7	422	34.4
		普通	55	4.5	47	3.8
		好	410	33.4	464	37.8
		非常好	72	5.9	79	6.4
		拒答/不知道	100	8.1	95	7.7
		總數	1,227	100.0	1,227	100.0
Q9	請問您同不同意，民眾可以在線上論壇、社群媒體獲得更多言論和資訊自由？（QB8.7.）	非常不同意	62	5.1	51	4.2
		不同意	168	13.7	161	13.1
		普通	14	1.1	13	1.1
		同意	542	44.2	515	41.9
		非常同意	423	34.5	463	37.7
		拒答/不知道	18	1.5	24	2.0
		總數	1,227	100.0	1,227	100.0
Q9_1	就您的理解，請問您認為臺灣在「民眾可以在線上論壇、社群媒體獲得更多言論和資訊自由」方	非常不好	129	10.5	124	10.1
		不好	243	19.8	214	17.4
		普通	39	3.2	38	3.1
		好	520	42.4	511	41.7
		非常好	240	19.6	271	22.1
		拒答/不知道	56	4.6	68	5.6

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
	面，落實的好不好？（QB8.7.）	總數	1,227	100.0	1,227	100.0
Q10	請問您同不同意，民眾可以獲得安全和尊重個人隱私的數位服務？（QB8.9.）	非常不同意	30	2.4	28	2.3
		不同意	59	4.8	54	4.4
		普通	5	0.4	3	0.2
		同意	372	30.3	387	31.6
		非常同意	748	61.0	735	59.9
		拒答/不知道	13	1.1	20	1.7
		總數	1,227	100.0	1,227	100.0
Q10_1	就您的理解，請問您認為臺灣在「民眾可以獲得安全和尊重個人隱私的數位服務」方面，落實的好不好？（QB8.9.）	非常不好	221	18.0	209	17.0
		不好	432	35.2	397	32.3
		普通	55	4.5	49	4.0
		好	397	32.4	432	35.2
		非常好	76	6.2	92	7.5
		拒答/不知道	46	3.7	49	4.0
		總數	1,227	100.0	1,227	100.0
Q11	請問您同不同意，民眾在線上的通訊（文字及語音）保密，資料不被外洩？（QB8.10.）	非常不同意	48	3.9	49	4.0
		不同意	100	8.1	121	9.9
		普通	4	0.3	3	0.2
		同意	313	25.5	316	25.7
		非常同意	755	61.5	730	59.5
		拒答/不知道	7	0.6	9	0.7
		總數	1,227	100.0	1,227	100.0
Q11_1	就您的理解，請問您認為臺灣在「民眾在線上的通訊（文字及語音）保密，資料不被外洩」方面，落實的好不好？（QB8.10.）	非常不好	372	30.3	358	29.2
		不好	454	37.0	444	36.2
		普通	38	3.1	38	3.1
		好	272	22.2	288	23.5
		非常好	35	2.9	43	3.5
		拒答/不知道	56	4.6	57	4.6
		總數	1,227	100.0	1,227	100.0
Q12	請問您同不同意，民眾擁有個人資料的控制權，可以決定個	非常不同意	12	1.0	13	1.1
		不同意	26	2.1	31	2.5
		普通	3	0.2	1	0.1
		同意	422	34.4	430	35.1

題號	題目	選項	加權前		加權後	
			樣本數	百分比	樣本數	百分比
	人資料的使用方式與分享對象？ (QB8.11.)	非常同意	754	61.5	734	59.9
		拒答/不知道	10	0.8	17	1.4
		總數	1,227	100.0	1,227	100.0
Q12_1	就您的理解，請問您認為臺灣在「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」方面，落實的好不好？ (QB8.11.)	非常不好	168	13.7	161	13.1
		不好	370	30.2	346	28.2
		普通	53	4.3	46	3.7
		好	467	38.1	483	39.3
		非常好	83	6.8	95	7.8
		拒答/不知道	86	7.0	95	7.8
		總數	1,227	100.0	1,227	100.0
Q13	請問您同不同意，應該要保障兒童和年輕人安全的數位環境和內容？(QB8.13.)	非常不同意	5	0.4	9	0.7
		不同意	8	0.7	13	1.1
		普通	1	0.1	1	0.1
		同意	264	21.5	283	23.1
		非常同意	945	77.0	915	74.5
		拒答/不知道	4	0.3	6	0.5
		總數	1,227	100.0	1,227	100.0
Q13_1	就您的理解，請問您認為臺灣在「應該要保障兒童和年輕人安全的數位環境和內容」方面，落實的好不好？ (QB8.13.)	非常不好	277	22.6	252	20.6
		不好	461	37.6	428	34.9
		普通	49	4.0	47	3.8
		好	315	25.7	378	30.8
		非常好	47	3.8	50	4.1
		拒答/不知道	78	6.4	72	5.8
		總數	1,227	100.0	1,227	100.0