DOI: 10.6482/ECPCR.201910.0009

AI與人臉辨識技術運用於犯罪偵防之問題分析

王正嘉*

目　次

摘　要

近年來世界各國莫不致力於人工智慧（AI）的發展，不僅帶給人們更方面，美好的生活，也帶來運用到犯罪偵防的可能性。就目前的應用現狀來看，新的科技帶入刑事司法，必然帶來新的法制上問題，其中又以人臉辨識近來成爲討論話題。

本文的主要目的即在探討此問題，特別從人臉辨識系統運用到在犯罪偵防，在我國可能產生的問題分析，同時借用美國與日本的經驗，來提供給我國法制上的建議。

關鍵字：人工智慧、AI、人臉辨識、法律奇異、犯罪偵防

* 王正嘉，國立中正大學法律學系教授，國立臺灣大學法學博士，Email: ooseika@ccu.edu.tw。

An analysis of applicating AI and facial recognition system on criminal justice

Jiang-Jia Wang*

Abstract

All major nations are engaging on developing Artificial Intelligent (AI) technology in these recent year. It brings not only a better life for human but also the possibility to applicating on criminal justice. In current situation, using new technologies to criminal justice would cause some legal problems consequently. Facial recognition system has become a hot topic especially.

The main purpose of this article aims at these problems. It particularly focuses on facial recognition system, analyzes the experience of U.S. and Japan and gives some suggestions.

Key Words: Artificial intelligence, AI, facial recognition, legal singularity, criminal investigation and prevention

* Professor of Law, Department of Law, National Chung-Cheng University. E-mail: ooseika@ccu.edu.tw

壹、前言

近幾年來，世界各先進國家無不在人工智慧，傾入國家整體力量開展。美國2016年10月公布《國家人工智慧研發策略規劃》（National Artificial Intelligence Research and Development Strategic Plan）[1]，國家科技會議下的網路與資訊科技研究發展委員會，為未來人工智慧提出發展願景，為透過對人工智慧相關技術的投資，促進經濟繁榮、提升生活品質並強化美國國家安全；日本也在2016年1月內閣通過的《第5期科學技術基本計畫》中[2]，雖然沒有特別強調AI，但所提出的未來科學技術的四個重要支柱，特別強調透過科技創新來服務人類社會與生活提升，尤其要求各部會須共同合作進行AI等關鍵技術的研究開發和推動，強化基礎技術和人才，以實現超智慧社會，德國提出工業4.0的方向後，同時也開展相關行動方案與研發計畫，2016年再提出數位策略（Digital Strategy 2025）做為強化工業4.0發展的主要策略[3]，同時亦成立人工智慧研究中心（German Research Centre for Artificial Intelligence, DFKI），致力於人工智慧研究與發展，範疇涵蓋數據及知識管理、影像和語言處理、人機互動、機器人等。2017年7月中國的國務院公布《新一代人工智能發展規劃》[4]，重點任務包含布局前沿基礎理論研究、推動基礎學科的跨領域融合、發展關鍵性共通技術，同時透過創新平台進行協作與工具共享，以及利用「千人計畫」加強人才延攬及培育人工智慧高階人才。中國大陸發展規劃明確訂出各階段發展目標，至2030年在理論、技術和應用都能具全球領先地位，成為全球AI創新中心以及人才培育的基地。即使我國也不落人後，科技部所頒布的《人工智慧推動策略》，也提到機器模仿人類認知能力，在近年來開始廣泛地運用在各個領域，將成為推動科技發展的主要基礎技術，對於產業經濟、社會發展與人類生活都產生極大影響，也是台灣未來必須積極推動的科技。

而這樣的技術有無可能成為犯罪偵查的利器，或者用來預測法院判決，甚至取代人類法官，在我國之前實務研究中，就曾彙整以往的判決書，對於量刑資料庫曾作出一些成果，但隨著人工智慧技術的發展，進一步將AI應

[1] 參閱：https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf（最後瀏覽日：2019/05/25）。

[2] 參閱：http://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf（最後瀏覽日：2018/12/25）。

[3] 參閱：https://www.de.digital/DIGITAL/Redaktion/EN/Publikation/digital-strategy-2025.pdf?__blob=publicationFile&v=8（最後瀏覽日：2019/07/25）。

[4] 參閱：http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm（最後瀏覽日：2019/07/25）。

用在法官判決輔助時，由 AI 法官作出簡單判決，或透過 AI 演算法的運用，判斷被告的再犯與行為危險性，都不再是遙遠的想像。這一點在中國大陸《新一代人工智能發展規劃》構想中，也特別提到智慧法庭，運用人工智慧來建設安全便捷的智能社會項目下，預期建設集合審判、人員、數據應用與司法公開和動態監控於一體的智慧法庭數據平臺，促進人工智慧應用在證據收集，案件分析與法律文件閱讀與分析上，甚至用在於判斷被告的再犯之虞，其中包括：再犯的危險性與犯罪危險性等，最近也有新的進展。但上述的新技術發展，也可以作為犯罪偵防用途，其中尤以人臉辨識技術（Facial Recognition System）是一個受到重視的利器，但近年來這類技術的應用，是否毫無限制，有無憲法或法律的問題，也逐漸受到重視。本文先探討人工智慧對於法律與刑事司法的一般影響與問題（貳），再以人臉辨識作為深入探討對象（參），參酌我國與國外的發展狀況，來分析相關法規制問題（肆），最後是結論（伍）。

貳、人工智慧、未來法律與刑事司法

在 2016 年初，人工智慧機器在圍棋比賽中擊敗棋聖李世乭。對於那些曾經誇耀電腦不可能去掌握這種獨特的人類比賽的學者與圍棋粉絲來說，機械獲得勝利彷彿是一件不可思議的事。因為圍棋比賽向來被認為過於巧妙及優美，而不適合於機械，因為成功的選手是仰賴人類的直覺及判斷力，而不是強大的計算能力。但這場圍棋比賽，並非單一例子，IBM 的華生人工智慧程式曾在電視智力遊戲危險邊緣中擊敗節目中的西洋棋大師，超級電腦也在國際西洋棋比賽中擊敗大師 Garry Kasparov。這都是十幾年前根本難以想像的事，但這只是人工智慧革命的開端，未來也有可能運用到法律各個層面（Alarie, Niblett, & Yoon, 2016），乃至於刑事司法。

一、未來法律的圖像

上述人工智慧在人類圍棋比賽及西洋棋比賽擊敗人類的經驗，引導出關於人工智慧的開發，不侷限在比賽還能運用在各個領域方面，尤其是法律。按照專家預測，人工智慧將會一直不斷發展，直到這個趨勢的極盛時期，就是所謂的法律奇異（legal singularity）點。在這個法律奇異點，排除法律的不確定性和普遍性，出現馬上可以即時普遍可觸及的法律秩序。在法律奇異上，對於事實與法律獨特性的爭議也將很罕見，因為即使存在事實的爭議，但一旦發現爭議，事實將直接映射到明確的法律結果（Alarie, 2016, p.

447）。這種未來的法律想像，可以透過三個觀點，來討論大數據及人工智慧將如何影響法律（Alarie et al., 2016, pp. 423-428）：1）法律制定的改變：當數據及人工智慧運用在法律制定上，我們將可能會發展出微指令（micro-directive），將會比法規更加具體，也會比規範更加的精確。2）改變個人對法律的理解：我們將能更輕而易舉且以低成本的方式獲取資訊，並理解我們在法律上的權利及義務。3）法律服務業的改變：隨著技術發展及人工智慧的應用，律師事務所可以透過電腦去分析，以減少時間和成本。而法律的電子搜尋工具也促進更快速且經濟的法律搜尋。

對於人工智慧應用到刑事司法，也並不那麼遙遠，2016年美國Wisconsin州最高法院，審理法官使用危險評估系統COMPAS，顯示被告Eric Loomis對社群有高度危險，因此駁回其假釋聲請（Joh, 2017, p. 288），這是將大數據運算法預測法運用到量刑的首例，未來的運用更加地廣泛。但若要將人工智慧技術運用到刑事司法的預測上，在現階段還有一段路要走。然而目前的研究方向來看，關於刑事司法的常態活動，可以準確適用既有的刑事規則來判斷，依據本身具有穩定屬性的既有規則屬性者，似乎可以交給人工智慧，另一方面，若是是牽涉動態規則適用面向，實際決策核心部分，人工智慧可以涉入多深，取代人類到何種地步，都還會是問題，也就是作為輔助系統的弱人工智慧，已經水到渠成，但完全取代人腦判斷的強人工智慧，則仍在發展途上。

二、犯罪的預測判斷運用

但近年來，隨著幾個關鍵的技術的成熟，人工智慧開始得以真正地稱得上相似於人腦的智慧：首先電腦運算能力技術的大幅提昇，得以同步、即時且正確地處理大量資訊；再者類神經網路（quasi-neural network）技術發展，可以仿照人的大腦神經元進行函數演算，接收到資訊後，根據其性質及內容的不同，產出反應，或是調整內部函數的結構。每一次的資料輸入，都可以產出需要修正的參數，回饋給原有的函數，以為調校，讓機器學習（machine learning）或深度學習（deep learning），成為可能（Harry, 2014, pp. 89-）。

在犯罪預測與刑事司法的運用，更顯著的則在警政系統。相較於犯罪的偵查，警方熱衷於預測接下來犯罪，會在何處發生，誰是可能的犯罪人，可能的被害人，過去的傳統警察，透過經驗、直覺與訓練的累積來達到這個目的，但隨科技的發展，警方也轉向分析大數據與演算法的各種工具，來達成這項工作。（Joh, 2017, p. 287）美國加州大學法學院教授Elizabeth E. Joh

在其著作中，就曾經描寫過不遠的將來，警察部門將具備科技能力的情節（（Joh, 2016, p. 1）：

> 在犯罪分析局，警官登錄網路查看社交媒體軟體發佈了哪些警報，旨在發現每日數十億條線上推特中，釘選、按讚和貼文中潛在的威脅。在街上，一名警官用他戴在身上的相機掃描人群；迴響資訊即時發送回人臉識別和動作分析軟體，提醒巡警是否發現了鬼祟的行動或觀察名單上的人。警方密切關注這些警報，以確定應該立即調查的人。其他人會因為沒有立即構成威脅而被解除，但會被記錄在觀察名單上，以供鬼祟行為的參考。

這些看起來，不久就可能實現的事情，其實現有警政模式中，運用在犯罪防治上，透過大數據與人工智慧，早已發展多年。結合地區資訊系統GIS，來建置犯罪地圖（crime mapping）與高度犯罪熱點（hotspot of crime），期待能夠從過去犯罪的犯罪數據分析，預測未來犯罪的空間與時間，進而導引出一個可靠的預測模式，來確認獨特犯罪模式，警方得以進一步確認犯罪趨向，並重新配置警力（Andrew Guthrie, 2011, p. 197）。美國芝加哥早就這樣做，警察當局特別注意到一些熱門名單（heat list）人選，以風險分析軟體確定出未來可能的暴力犯罪人；北卡州的Charlotte市，警察整理出先期揭露資料，指定出可能發生犯罪高危險區的地圖；紐約市警局則與微軟合作，發展出地區認知系統（Domain Awareness system）用來從街頭攝影機（CCTV）收集資訊，並連結到車牌辨識系統、感應器與資訊資料庫，可以說已進入到數位警政時代（Joh, 2014, p. 35）。

即使在我國，早有研究說明大數據結合到犯罪預測與預防日益深化，分析台灣社會犯罪事件發生現狀，即時發現高風險犯罪人口特徵、犯罪模式，提供防治對策等（許華孚; 吳吉裕, 2015, p. 11），而實際上警方也逐步建置的「M-POLICE」警用行動載具系統，並廣泛使用中，第一線執勤警員可即時查詢治安整合資訊，提高警察行政效率，在協尋失蹤老人、查詢贓車及嫌疑犯中有所成效，甚至建置起警政大數據分析平台，透過人工智慧的演算法，結合原本既有的犯罪資料庫分析比對[5]。

當然刑事司法的數據資料運用，並非現在才有，傳統上，已經犯罪人前科資料、指紋與DNA等資料蒐集，並透過比對來確認人資，但是隨著資訊整合與AI技術的發展，資料運用規模的質與量都前所未有成長，因此上述運用也引發若干疑慮。

[5] 參閱：警政署力推智慧警政，打造大數據分析平臺以提高網路犯罪偵查率，Available at: https://www.ithome.com.tw/news/126521（最後瀏覽日：2019/07/26）

三、使用的疑慮

AI技術結合大數據與演算法，來進行犯罪預測，就以目前的犯罪嫌疑自動演算法（Automated suspicion algorithms；ASA）系統為例，實際上有二個步驟：一方面蒐集政府或民間關於個人資訊，另一方面透過機器學習等AI技術，來分析這些技術（Rich, 2016, p. 873），前者包含來自於公部門與私部門的龐大資訊，就產生了使用的界限問題；至於後者的演算技術，仍是由程式設計人員製作出來，就不容忽視可能的演算法歧視（Algorithmic bias）[6]。這個系統是否毫無限制地，可以取用任何資料庫？計算上是否會比人類公平？公平可以用演算法計算嗎？演算法應考量因素為何？再者，當資料趨勢（data-driven）的刑事司法形成之後，與舊有的問題相同，必定可能遭逢到資料錯誤，所運用的犯罪相關資料庫，維護正確性與可靠性，都需要大量經費，並縮小錯誤可能（Wayne & Andrew Guthrie, 2016），如果能夠做到？都成為亟待關注的焦點。

基本上，新的技術發展，有時也將既有犯罪偵防技術延伸運用，而更加速警察發現犯罪和識別嫌疑人的能力，但這樣的運用也非全無問題。例如自動車牌閱讀器（ALPR），相對過去的肉眼或照相機，到街頭攝影機拍攝，而ALPR科技，則是其變得便宜、高級，而且越來越普及，安裝在巡邏車上或固定位置的監視器及資料分析，每秒可讀取多達50個車牌與識別，記錄每個掃描車牌的日期、時間和GPS位置，然後將其與熱門清單進行比較，這些清單包含被盜車輛、違規停車和恐怖分子監視清單等資訊的相關車牌數據，同時通過一組特定的時空參數，也可以用來調查刑案中，通過某些地點的車輛，成為潛在嫌疑人的判斷，或與其他工具結合使用，調查已經發生的犯罪。再如美國警方曾利用過的手機基地台模擬器，又被稱為IMSI捕捉器或黃貂魚（stingrays），是以虛假的移動基地塔來欺騙附近的手機提供數據，後來被公民自由組織和記者發現，美國司法部於2015年9月宣布適用於司法部使用手機監控技術包括令狀要求的新規則[7]。

但是，這二個偵防犯罪的新技術都產生疑慮，例如ALPR如何減少犯罪的作用，其實知之甚少，以致於無法評估投資的效益；後者則受制於開發民間公司的保密義務，禁止透露該技術的任何資訊，而無法獲知該技術的詳細資料，這就產生透明度問題。相關的法制問題，則在於這些利用電腦程式

[6] 騰訊研究所，人工智能：國家人工智能戰略行動抓手，中國人民大學出版社，2017年11月，頁240。

[7] 參　閱：https://www.wsj.com/articles/justice-department-changes-policy-on-cellphone-surveillance-1441314839。

生成的警報及大量資訊篩選可疑活動等的科技大數據，大量增加警察監視的自由裁量權（surveillance discretion），引發有關警察監督的權力與責任之重要法律和政策關鍵問題（Joh, 2016, p. 18）。美國林肯紀念大學大學法學院Reid教授，也認為在這個超級電腦、人工智慧與機器人的時代下，同時運用多種執法工具，配備有IBM超級電腦Watson的人工智慧機器警察，也應該重新思考美國憲法第四修正案（Reid, 2017）。這是因為在傳統的警察調查模式中，聯邦最高法院解釋的美國憲法《第四修正案》，是允許警察經過初步調查，來決定針對特定的人的進一步調查，美國最高法院判決清楚地表明，對此自由裁量權利幾乎沒有監管權，而且不同於逮捕或竊聽，就算證據不多，警察將注意力集中在某些個人身上的決定，也不太可能被視為第四修正案事件。在這種情況下，警方不需要證明可能的原因或合理的懷疑（或懷疑的通常標準）來決定是否對個人進行監視。但在大數據的資訊時代，這樣傳統的見解是否仍然妥當，則有待爭議，人工智慧直接運用在刑事司法系統上，大幅度擴大警察權力，是否應該有所界限？界限為何？正是值得探討的問題。

綜上所述，人工智慧運用到刑事司法，主要目的在於讓決策更為正確，以提高社會治安效能，但同時也要避免人民隱私等權利受到過度的破壞。當然中立的科技技術本身並無所謂好壞，重點在於使用者與如何使用。隨著科技技術日新月異的發展，相關監督管理機制亦須跟上腳步，防止國家過度監控造成的人權侵害，才能享受科技帶來的便捷及效率，並合理維護個人公民權利，下一個章節就針對目前被廣泛利用的人臉辨識系統為例子，進一步深入說明這個問題。

參、人臉辨識系統於犯罪偵查運用與問題

一、人臉辨識的技術概說

所謂的人臉辨識，是透過數位圖像來辨識人的應用，尤其當街頭監視攝影機盛行，從監視攝像機的圖像中，自動識別人的身分，並結合到資料庫進行比對的整體硬體而言。計算機應用程序，人臉辨識大致分為兩個過程：「臉部檢測」和「臉部匹配」。在「臉部檢測」處理中，先根據圖像確定臉部區域，然後檢測臉部特徵點以找到臉部的特徵點位置，例如眼睛、鼻子和嘴部邊緣。然後，在使用特徵點位置對臉部區域的位置和大小進行整合後，再執行「臉部匹配」處理。因此人臉辨識可以說是判別人的身分，最容易方

便實現的認證系統，因為不需專用裝置，就可以作到，發展已久日本企業宣稱辨識度達到99.2%，且已有廣泛應用[8]。

但實際上要達到犯罪偵防的境界，人臉辨識還要跟AI技術相配合，因此廣義的人臉辨識，包括構建人臉識別系統的一系列相關技術：人臉圖像採集、人臉定位、人臉識別預處理、身份確認以及身份查找等，透過大數據建構的人臉資料庫，才能透過人臉進行身份確認或者身份查找，成為可能。

此時人臉辨識系統之演算法可大致分為兩種類型，即直接將幾何特徵與外觀特徵進行比較的方法，以及統計量化圖像並將其數值與模板進行比較的方法。人臉辨識可以由一個照片組成的數據資料庫，將每個臉部分析並轉化為代表其測量結果的數位，用戶將要搜尋的照片輸入到系統中，生成與數百萬其他人進行比較，產生候選列表，用以比對身分之同一性。

二、人臉辨識的廣泛應用

由於人臉辨識不須像指紋認證一樣觸摸感應器，或像虹膜認證一樣須直視感應器，被攝像者無任何受侵害的身體感知，沒有任何入侵動作，人臉辨識技術即能以臉部來確認人別，現今早已在各種場景以及智能手機中使用。例如，許多國家將這種人臉辨識用於入出境管理，自動通關系統方便國民入出境，或入境審查蒐集入境外國人的臉部認證資料，辨識危險份子，以維護國境安全；亦有公司舉辦演唱會，以人臉辨識做為入場使用，避免黃牛票的買賣或防止危險人物進入；更有甚者，便利商店播放廣告看板，能就播放廣告板前的人臉，感知年齡及臉部表情，以為顧客是否喜愛廣告商品之販售參考。

而在公共領域中，如何提供安全環境與便民服務，並避免犯罪、打擊犯罪，為政府、警務單位與民眾所關切的議題，人臉辨識技術帶來便捷及效率，有助於警方治安維護，加速調查及提高公共安全性。因此人臉辨識系統在犯罪偵防上運用，開始廣泛於世界各國，不僅提高警察的行政效能，有效維護社會治安，配合其他資料庫及社群媒體，並能達成有效偵查，乃至於預防犯罪之效果。

我國警政署從2007年起開始建置M-Police行動平台，原來是透過以小型的行動裝置搭載M-Police，後來擴充為行動電腦，整合9個機關超過30個資料庫，供基層員警在執勤查詢各式資料使用。而M-Police更導入人臉辨識系統，整合內政部的戶政資料，利用照片比對，理論上幾乎涵蓋全國

[8] 參閱：日本NEC公司網站資料，available at : https://jpn.nec.com/solution/face-recognition/index.htm（最後瀏覽日：2019/0730）。

二千三百萬百萬人民的資料。

至於將人臉辨識系統應用到監控人民最受到矚目的，莫過於中國大陸「天網」監控系統，近年來新聞多次顯示，透過人臉辨識，在演唱會或街頭，迅速尋獲在逃通緝犯，但同時也可以在街頭迅速確認每個行人，並連結到社會信用評估以及前科資料，然而同時也引發監控人民的隱憂。

當人臉辨識系統逐漸進入到犯罪偵防場域時，使用此利器同時，也產生過度侵犯人民隱私的隱憂，因此若干國家，已經開始注意到這個問題，並透過法規範來加以對應，避免國家過度的侵害，形成監控社會。據此，如何在犯罪偵防與侵害人權，尋得國家社會安全維護的平衡，是接下來要探討的問題。

三、運用到犯罪偵防的問題

（一）比對資料庫蒐集與儲存問題

人臉辨識系統是由照片組成的數據資料庫，將每個臉部分析並轉化為代表其測量結果的數字，用戶將要搜尋的照片輸入到系統中，與數百萬其他人進行比較，然後系統產生可能吻合的列表。因此除攝影機外，還需要比對的資料庫，否則人臉辨識系統無法達到犯罪偵防效果，這就涉及到臉部特徵是否屬於人體特徵，以及建檔的合法性問題。

關於人體資料庫建檔的相關爭議，在司法院釋字第 603 號中，大法官認為國家大規模蒐集、錄存人民指紋、建立資料庫儲存，應以法律明定蒐集目的，且蒐集手段應與重大公益目的達成有密切必要與關聯，並應依法明文禁止法定目的外使用。基本上建立起法律保留原則。而解釋文並揭示：「人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」

當然人類的臉部資訊，與指紋相比，使用非接觸型生物辨識技術，有著被測個體不易察覺的特點。而且辨識作業也在大眾不知情下進行，來做成臉部畫面保存紀錄，但如同指紋一般，具有其生物特徵性，有不易改變之特性，取用應有限制，人民也應該享有個人自主控制個人資料的「資訊隱私權」。

據此來說，用來作為臉部與指紋認證的資料庫建檔，仍然需要一定的法律授權，人民對於這些資訊隱私權，要能決定是否揭露及何種方式揭露，並有知悉與控制權及更正權。臉部資訊之保存，是否應該有法律明文依據？應該保存多久？被攝像者是否應受告知？是否能有影像刪除權？我國現有的警

察職權執行條例，雖對預防的街頭攝影機有法律上授權，但其明確性仍難謂充足。

（二）辨識可能發生錯誤

人臉辨識系統技術雖然日益成熟，從2D邁向3D，有效提升辨識率，但是仍難達到百分之百正確。運用人臉辨識最有名的錯誤例子，是已被幾家美國警察機構使用亞馬遜臉部辨識系統（Amazon Rekognition），所引發的爭議話題[9]。

美國公民自由聯盟（American Civil Liberties Union；ACLU）曾經測試這個系統，將535位美國國會議員（100位參議員及435位眾議員）的照片，跟一個被捕罪犯大頭照資料庫的25,000張照片作對比，結果發現有28人的頭像被Rekognition系統判定為「吻合」。進一步分析，甚至發現相對整個國會中，有色人種的議員只佔20%，被錯誤配對的28位議員當中，竟然有高達39%為有色人種。這項研究顯示，臉部識別技術用在成年白人男性最準確，但如果用在其他膚色、性別及年齡的人身上，錯誤比率就會明顯增加。

據此來說，亞馬遜的系統用來偵測攝影機前之人臉，與犯罪資料庫照片比對，在幾分鐘內能找出潛在可能的犯罪嫌疑人，大幅提昇警察犯罪偵查之效率；但因為光線、拍攝角度，都會影響人臉辨識的正確率，且系統出錯引致的偏見問題亦受關注，特別是演算法面對不同膚色的人時出錯機率有別，不成比例地使少數族群受到影響，在美國引發可能侵害人權及人種歧視的疑問。

（三）資料交錯比對的隱私保護

雖然臉部辨識系統的準確性逐漸提高達到99.2%，但即使正確率達到百分之百，不會有識別錯誤風險，但人臉辨識技術大規模地運用，增加執法部門監控民眾的能力，即使沒有涉嫌犯罪的人，亦會受到政府大規模的監控，尤其資料交錯比對，數據資料愈多而相互連結，使人無法維持匿名，隱私愈無所遁行。

其實在所有新科技運用，都會遇到的這個問題。人臉辨識的取用、攝像，若在公共場合，民眾看似難有隱私合理期待，對人臉被攝像根本也不知不覺，看似人權並未受到侵害，但被攝像者的照片可能從此存在於警方資料庫內，並與各式資料庫之連結比對，更甚者，與多年資料、各大路口之監視

[9] 參　閱：Michael Kan，Amazon's Facial Recognition Mistakes Lawmakers for Criminals，available at：https://www.pcmag.com/news/362740/amazons-facial-recognition-mistakes-lawmakers-for-criminals（最後瀏覽日：2019/7/31）。

影像中人臉影像資料交互比對，層層堆疊可以勾勒出一個人生活態貌，如過往經歷、行車路徑、生活喜好及偏向等，對個人隱私造成具大損害。

司法院釋字第 689 號解釋，對於新聞媒體的跟拍問題，認為在公共場所亦得享有隱私權，並以得合理期待於他人者為限，解釋理由書中闡釋：「蓋個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者。」

而運用 GPS 產生的問題，最高法院 106 年台上字第 3788 號判決的「海巡緝私案」。本案被告為海巡署士官長，為了查緝私菸而在犯罪嫌疑人使用的汽車底盤裝設 GPS 追蹤器，透過行動電話取得犯嫌的行蹤，經原審判決成立刑法第 315 條之 1 無故竊錄罪。檢察官上訴主張 GPS 跟監有法律根據，故不該當「無故」竊錄，本判決駁回其上訴，維持原審有罪判決。

本案乃針對司法警察身分之公務員（海巡署）使用 GPS 追蹤器進行跟監追蹤成立無故竊錄罪，對於前開的非公開活動的隱私秘密，進一步闡述：「在參與社會生活時，個人之行動自由，難免受他人行動自由之干擾，於合理範圍內，須相互容忍，乃屬當然。如行使行動自由，逾越合理範圍侵擾他人行動自由時，自得依法予以限制。在身體權或行動自由受到侵害之情形，該侵害行為固應受限制，即他人之私密領域及個人資料自主，在公共場域亦有可能受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要。」據此來說法院認為，經由科技設備對他人進行長期且密集之資訊監視與紀錄，他人身體在形式上雖為獨處狀態，但心理上保有隱私之獨處狀態已遭破壞殆盡，自屬侵害他人欲保有隱私權之非公開活動。

該判決見解同時引用美國聯邦最高法院在 United States v. Jones 針對類似案件所採取之「馬賽克理論（mosaic theory ）」（或譯為「鑲嵌理論」），即如馬賽克拼圖一般，乍看之下微不足道、瑣碎的圖案，但拼聚在一起後就會呈現一個寬廣、全面的圖像。個人對於零碎的資訊或許主觀上並沒有隱私權遭受侵害之感受，但大量的資訊累積仍會對個人隱私權產生嚴重危害。是以車輛使用人對於車輛行跡不被長時間且密集延續的蒐集、紀錄，應認仍具有合理之隱私期待。因此政府長期監控一個人的片段行蹤累積拼湊出一個人

的整體行蹤，由此產生關於一個人的生活全貌是具有受到隱私保護之價值而言。

據此個人在公共領域內，若得知被攝入人臉照片，應可合理期待不被保存而存置於資料庫建檔；若非係基於維護重大公共安全，應有不被比對資料庫資訊的合理期待，而這個期待，在社會通念下會被認為合理，而受到隱私保護的價值。

（四）掃瞄辨識的法律定位

如前所述，在美國此問題涉及到憲法增修條文第四條的爭議問題。該條文規定：「人民有保障其人身、住所、文件、財物，不受不合理搜索及扣押之權利，不得非法侵犯，除非有相當事由，經宣誓或代誓宣言，並詳載搜索之地點、拘捕或扣押之人或物外，不得核發搜索令、拘票或扣押狀」，向來的看法與解釋認為，該法條是保護民眾不受政府「不合理搜索和扣押」，至於政府對人民產生增修條文第四條所述之干預前的調查，除非帶有調查對象之歧視性選擇，否則警察如何決定挑選所關注的人、方式及原因，是警方之自由裁量權。法院普遍接受任何個人都無權免受監控調查的觀點。因此傳統警察調查模式，不需要證明可能的原因或合理的懷疑，來決定是否對個人進行監視，反而因需具備一些法律手段，來發展所必要的美國憲法第四修正案之個人化懷疑標準，供以後進行搜查或扣押，但到達這個臨界點之前的調查活動，只要警察將調查對象限制在非私密區域[10]，即使使用秘密的方法，警察也不需要對於調查對象有任何的個別化懷疑，也不需要搜索令狀。且按照美國最高法院 1972 年 Laird v.Tatum 案的見解，認為若沒有「由於監視或威脅到未來的具體傷害，而造成的具體的目前客觀傷害」、「若僅僅存在政府調查和資料收集活動，沒有更多的活動」，都不能構成聯邦訴訟的依據，依此一標準，法院訴訟上除了侵入性的監視，其他方面合法監視的訴求往往遭到敗訴。

但學者 Joe 教授認為，此過去背景已經改變，公共場所警察監督資訊的累積，也是有可能成為呈現一個人的宗教信仰、健康狀態、政治信念與惡行，雖然個別獨立的蒐集活動，單獨不能被視為搜索，但大量個人公開資料的蒐集卻可能堆積起來，像馬賽克一樣拼成一個完整圖像，形成第四修正案的侵害，主張大數據正在改變警察自由裁量權的結構，對於大數據工具存在類似的問題，應該有相應的責任機制工具來整體控制這些實務作法，責任機制措施應側重於政策結果而非技術具體措施（Joh, 2016, p. 38）。

[10] United States v. Knotts 案發展出「公共場域的行蹤不受美國憲法增修條文第四條之保護」法則。

據此來說，不僅是資料庫的建立，利用人臉辨識的掃描，其透過所建置的街頭攝影機，或是警車警員身上配置的攝影機，來進行掃描，並非無法律疑慮。警政署近年推動「警政雲端運算發展計畫」，「M-Police」導入智慧型手機，透過即時相片比對系統，鎖定人臉 10 秒即可知該對象身分，並能連結戶政系統，雖然提昇警察辦事效率，卻可能侵害民眾個人資料隱私，因為戶政資料庫的蒐集目的，是否得以擴大到人臉辨識上，不無爭議。且按照警察目前運用人臉辨識系統的方式，有現場照相、路口監視器的影像、或從社群媒體尋找照片等。當警察使用臉部辨識系統，在公共場所內任意搜尋、掃瞄辨識人臉，再連結配合戶政資料、車籍資料、犯罪前科等，隨即能描繪出被攝像者之個人生活態貌，這種情況，縱使未達到搜索程度，但也有達到類似於臨檢的干預，甚至比臨檢影響民眾更甚，因為被攝像者難以得知並無從拒絕。

按照司法院釋字第 535 號解釋：「臨檢自屬警察執行勤務方式之一種。臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均屬對人或物之查驗、干預，影響人民行動自由、財產權及隱私權等甚鉅，應恪遵法治國家警察執勤之原則。實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範，方符憲法保障人民自由權利之意旨」據此來說，警察執行勤務，使用人臉辨識系統，若非為了重大犯罪需求，以任意掃瞄人像，進而查知個人身分資料，無異如同臨檢一般，干預人民的個資隱私權，卻能不受任何規範，警察的人臉辨識行為，無異逸脫法律保留原則。

肆、外國法制的參考

一、美國

如前所述，按照傳統見解人臉辨識系統的掃瞄決定對象，在公共場所中執行，是警察的監視自由裁量權，不會構成美國憲法增修條文第四條規定之「搜索」，也不需具備相當理由；使用在公共場合，也符合公共場所的隱私合理期待法則，辨識的過程，也不會對民眾產生客觀傷害，若僅是政府調查和資料收集，沒有更多活動，也不能構成聯邦訴訟的依據。

然而人臉辨識系統所攝入的人像，若與警方所掌握的照片檔及巨大的資料庫連結比對，例如戶政資料、犯罪前科資料、車籍資料、監視錄影資料，如「馬賽克」般，資料庫愈詳盡、整合處理愈全面，愈能累積拼湊出被攝像者的生活整體行蹤及生活全貌，恐有受到隱私保護的價值，引發隱憂。美國

的各地方政府，開始要求警方使用人臉辨識的透明度和課責機制，要求在購買擴大監視能力的新技術之前須經地方政府批准。

華盛頓州西雅圖通過的一項監督通知條例，要求市議會在任何市政部門獲得「監視設備」前獲得批准。該條例不僅要求申報計畫購買的任何監視設備，還要求制定「緩和計畫」，說明該部門對這些設備的使用，以保護隱私、匿名性和限制潛在的濫用風險。公眾對新的監視技術採購的批准，還可包括批准員警部門可能與之簽訂此類服務契約的協力廠商[11]。新聞報道也指出，加州舊金山的立法機構（Board of Supervisors）首開先例，決議所有市屬公部門禁止公共場合使用人臉辨識系統[12]，導因於人臉辨識系統執行的錯誤率及歧視性的傷害。使用人臉辨視系統必須向市政監督委員會提交使用準則說明，此後也須每年提報詳細使用狀況，包括數據的保存方式、刪除及曾受提供的單位等。添購任何辨識系統，也都必須先經過監委會的許可。根據此決定，舊金山街道及公共場所，民眾將不用擔心「機器辨臉」的隱私曝露，市政府購買臉部辨識系統，必須事先經過審查。舊金山市政監督委員會官員佩斯金（Aaron Peskin）說：「這在心理上是不健康的，當人們知道他們在公共場所的每一處，都被監看著，不論是在街道上還是公園，這不是我想要居住的城市。」[13] 支持這項決定的人認為人們應該要自由的走在街上，而不是處於科技巨獸、甚至是政府的眼皮底下。除了涉及隱私，人臉辨識技術也被質疑不夠精準，錯誤率高，但鄰近矽谷，眾多 AI 與網路科技產業群聚的舊金山，卻開全美之先，禁止公共場所「機器辨臉」的設備，引發矚目。

二、日本

日本律師聯合會在 2016 年 9 月 15 日針對人臉辨識系統，發出「關於臉部認證系統的法律限制意見書（顔認証システムに対する法的規制に関する意見書）」，並提交給警察廳長官、個人資訊保護委員會委員長、總務大臣、都道府縣知事、以及政令指定都市市長。[14]

---

[11] 參閱：http://clerk.seattle.gov/ ~archives/Ordinances/Ord_124142.pdf（最後瀏覽日：2019/07/30）。

[12] 參閱：科技重鎮禁人臉辨識 舊金山開先例，新新聞，2018 年 6 月 20 日，available at: https://www.new7.com.tw/NewsView.aspx?t=05&i=TXT20190612173926AVZ（最後瀏覽日：2019/7/30）。

[13] 參閱：全美首例！舊金山警政機關禁「人臉辨識」，TVBS 新聞，2018 年 5 月 16 日，available at: https://tw.news.yahoo.com/ 全美首例 - 舊金山警政機關禁 - 人臉辨識 -112104593.html（最後瀏覽日：2019/7/30）。

[14] 參閱：日本辯護士連合會網站資料，https://www.nichibenren.or.jp/activity/document/opinion/year/2016/160915_2.html（最後瀏覽日期：2019/7/30）。

該意見書的主要目的，是針對人臉辨識系統與資料庫而來，建構是將臉部特徵數位化後的人臉辨識資料集合而成，並透過互相對比一致來確定嫌疑犯之身分辨識系統，為促使盡力少侵害人民的隱私權等權利，除了要求各種相關法令修正的適當規制外，也應該肯認犯罪嫌疑人或被告的「近接權（access right）」保障[15]。該意見書認為就法令修正與制度，有幾個方向：

（一）利用人臉辨識的限定條件

1. 令狀主義的要求：

警察為了犯罪搜查，而收集監視攝影機所紀錄的人臉圖像，應該依據法官的令狀而行。（但在許可區域中合法有權設置之店鋪內犯罪的臉部圖像資料除外）。

2. 限於重大組織犯罪：

來自犯罪現場附近的影像之人臉影像資料收集，僅於侵害重大保護法益之組織犯罪的偵查，有必要情況為限，當無偵查犯罪必要時，應立即銷毀。警方所能合法保有的臉部影像資料，只限定於重大組織犯罪前科者。

3. 設定臉部認證資訊的保留期間：

前開資料只能允許設定登錄期間，期間一滿，應立即銷毀。

4. 法律保留原則的要求：

對比於臉部辨識資料庫，限定在對重大組織犯罪偵查有具體必要性情況下，其容許的方法與條件，應以法律明確規定之。

（二）由個人資訊保護委員會監督

個人資訊保護委員會，應就警察的人臉辨識影像資料收集，臉部認證數據的生成、利用、廢棄，臉部認證資料庫的構築，臉部認證資料庫的登記，臉部認證資料庫的利用狀況，臉部認證資料庫的數據刪除等事，確實執行檢查。

（三）公開基本資訊

應定期公布人臉辨識系統執行架構，以及比對的精確度。

（四）嫌疑人、被告人等之權利

人臉辨識系統，同時也可作為與犯罪事實無關者，提供作為不在場證明之主張的手段，因此應該許可因嫌疑人、被告人等的請求，進行人臉辨識系統的比對。另外，對人臉辨識系統中，錯誤登錄之人，應肯認其公開請求權及刪除請求權。

[15] 同前註 11。

日本律師聯合會上開意見書，其實承繼2012年的《監視攝影機意見書》而來，相比於當時對逐漸增加街頭監視攝影機憂心，而且欠缺法律規範的狀況，隨後人臉辨識的技術發展與實用，從人臉的特徵抽出辨識資訊後，比對人臉資料庫，快速地進步，更加可能造成人民隱私權侵害，而再次出據意見書，強調制定相關法令的必要。

伍、平衡犯罪偵防與人權侵害 - 代結論

新興的科技犯罪偵防工具，隨著結合到AI與大數據，正在逐漸改變現有的法律架構，造成人權侵害的疑慮，將人臉識別技術用來識別個人，維護國家安全及社會治安，乃至於偵防犯罪，也早已經上路，然而從國外的法制經驗中，正在逐步形成法律框架來進行規制，在我國隨著使用GPS進行偵查，違反妨害秘密罪的最高法院判決出現，相類似的法律規制，似乎已經到箭在弦上，應該一併檢討的時刻了。

為避免技術不斷發展，造成政府對人民的過度侵擾，相應的監督管制措施，也必須跟上，本文藉由人臉辨識系統的問題分析，可以理出人工智慧應用到犯罪偵防，法律規制問題的一些理路。

一、資料使用符合正當性並公開透明

人的臉部資訊所轉化為資料數據，正如同指紋一般，具有生物特徵性，按照司法院釋字第603號見解，應該享有個人自主控制個人資料的「資訊隱私權」，因此人民也應享有知悉的權利，對於人臉攝像使用，存入資料庫，乃至於與其他大資料庫的比對使用，都應該公開透明，非有正當理由，不得任意使用。

二、法律保留原則及法官保留原則

除個別人民具有的資訊隱私權，建立臉部辨識的資料庫，也應該受到法律保留原則適用，正如釋字第603號解釋：「特定重大公益之目的而有大規模蒐集、錄存人民指紋、並有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。主管機關尤應配合當代科技發展，運用足以確保資訊正確及安全之方式為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。」以避免

禁止法定目的外的使用，並對所蒐集的人臉資料檔用採取組織上與程序上必要之防護措施。另外如果為犯罪偵查而進行人臉辨識，除了法律規範外，還需要法官保留的令狀原則，此可參考日本律師聯合會的法規建議。

三、第三方監督機制

隨著人臉辨識技術的應用層面愈來愈廣，應該建立一定監督機制。尤其在政府運用科技技術公權力來擴張犯罪偵防的現狀，日本律師聯合會所建議「個人資訊保護委員會」，透過第三方監督機制的有效率運用，應該更能確保民眾的隱私，避免警察國家或監視社會，更有效維護隱私。

四、採購的事先監督

美國的法制指引了這個方向。透過監督政府機關的民意機構，不論在預算，或是特別的批准制度，可以查知人臉辨識技術等其他新的科技技術，是否被運用於犯罪偵防，得以運用更防止發生秘密侵害人權情形。

五、資料保留期間及刪除錯誤請求權

人民享有個人自主控制個人資料的「資訊隱私權」，除能決定是否揭露及何種方式揭露，並有知悉與控制權及更正權。對於人臉辨識系統的人像資料攝影保存，應設有一定的保留期間，被攝像者對於人臉辨識系統的保存，亦能有刪除請求權，尤其再發現資料錯誤時，可以要求更正或刪除，其實類似的法制，在現行的《個人資料保護法》已經有規範，只要加以擴充即可。

六、人民的近接權

正如日本法制所構想的，人臉辨識系統也有可能成為犯罪嫌疑人或被告的不在場證明，因此必須承認人民也可以具有取得或請求比對人臉辨識系統的權利，俾便可以取得有利於己的證據，辨明自己的犯罪。

參考文獻

許華孚;吳吉裕. (2015). 大數據發展趨勢以及在犯罪防治領域之應用. *刑事政策與犯罪研究論文集, 18期*, 2-19.

Alarie, B. (2016). THE PATH OF THE LAW: TOWARDS LEGAL SINGULARITY. *University of Toronto Law Journal*, 66(4), 443-455. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=119350451&lang=zh-tw&site=ehost-live

Alarie, B., Niblett, A., & Yoon, A. H. (2016). LAW IN THE FUTURE. *University of Toronto Law Journal*, 66(4), 423-428. doi:10.3138/UTLJ.4005

Andrew Guthrie, F. (2011). Crime Mapping and the Fourth Amendment: Redrawing "High-Crime Areas". *Hastings Law Journal*, 63, 179-1645.

Harry, S. (2014). MACHINE LEARNING AND LAW. *Washington Law Review*, 89, 87-1467.

Joh, E. E. (2014). POLICING BY NUMBERS: BIG DATA AND THE FOURTH AMENDMENT. *Washington Law Review*, 89, 35-1467.

Joh, E. E. (2016). The new surveillance discretion: automated suspicion, big data, and policing.(Symposium: Policing in America on the 50th Anniversary of Miranda v. Arizona). *Harvard Law & Policy Review*, 10(1), 15-42.

Joh, E. E. (2017). FEEDING THE MACHINE: POLICING, CRIME DATA, & ALGORITHMS.(Big Data, National Security, and the Fourth Amendment). *The William and Mary Bill of Rights Journal*, 26(2), 287-302.

Reid, M. (2017). Rethinking the Fourth Amendment in the age of supercomputers, artificial intelligence, and robots. *West Virginia Law Review*, 119(3), 889.

Rich, M. L. (2016). Machine learning, automated suspicion algorithms, and the Fourth Amendment. (IV. Including ASAs in the Totality-of-the Circumstances Analysis through Conclusion, with footnotes, p. 901-929). *University of Pennsylvania Law Review*, 164(4), 901.

Wayne, A. L., & Andrew Guthrie, F. (2016). Policing Criminal Justice Data. *Minnesota Law Review*, 101, 541-869.