立法院法制局專題研究報告　　編號：1872

本報告僅供委員參考

人工智慧犯罪防制之相關法制問題研究

法制局 林智勝 撰

中華民國 115 年 11 月

人工智慧犯罪防制之相關法制問題研究

目　次

摘要

壹、前言 1

貳、我國犯罪防制法制與 AI 技術運用概況 1

一、我國人工智慧基本法及風險分類框架 2

二、我國犯罪防制相關法令和 AI 技術運用 3

參、AI 之外國法制 4

一、歐盟 AI 法風險等級及禁止使用之簡介 5

二、美國 AI 權利法案藍圖與 AI 框架之簡介 7

肆、問題研析與建議 9

一、AI 促成恐怖組織進化，建議警察法刪除未符時宜之任務界限 9

二、檢討人臉辨識設立人為介入審查機制，避免歧視或偏見情事 12

三、生物特徵識別指紋自動查驗通關，應以法律明定錄存目的 14

四、強化無人載具應用行為，研議訂定適當防範措施與倫理權衡 17

五、明確區分 AI 風險分類框架，強化隱私數據保護之必要性 19

六、建立預測性警務犯罪防制，允宜遵守法律保留原則 22

伍、結論 25

參考文獻 26
附錄：「人工智慧犯罪防制之相關法制問題研究」專題報告(初稿)座談會紀錄及參採情形……30

摘　　要

推動我國成為「人工智慧之島」為政府重要政策。人工智慧同時驅動犯罪與防制，具有正負雙面性，正在同時改變犯罪手段，公務機關亦開始導入犯罪防制應用。其中又以人臉、指紋、生物辨識、無人載具，使用人工智慧技術或方法辨識異常訊息與犯罪節點、預測等應用，也因此面臨新的法制上問題。

本報告爰就人工智慧相關應用與規定、司法院解釋與相關函釋及警察執法實務予以說明，並簡介歐盟、美國等先進國家相關法制，進而研提我國法制之因應與調適建議，俾供本院委員問政之參考。

人工智慧犯罪防制之相關法制問題研究

壹、前言

人工智慧（Artificial Intelligence，下稱AI）逐漸用於各類犯罪防制，惟因涉及高度隱私侵害及國安與人權衡平問題，建構適法AI技術與應用之良善運作環境，為政府刻不容緩之責任。本報告爰聚焦於AI科技應用於犯罪偵查與預防時，在提升執法效率與保障基本人權（特別是隱私權與個資保護）間之衡平。查立法院於民國[1]（下同）114年12月23日三讀通過人工智慧基本法，確認政府推動AI研發與應用的七大基本原則[2]，永續發展與福祉、人類自主、隱私保護與資料治理、資安與安全、透明與可解釋、公平與不歧視，以及問責，作為引導我國各機關發展與促進AI應用之原則。

本報告爰就AI相關應用與規定、司法院解釋與相關函釋及警察執法實務予以說明，並簡介歐盟、美國等先進國家相關法制，進而分析相關生物辨識與如何納管或授權AI工具，研提我國法制之因應與調適建議，俾供本院委員問政之參考。

貳、我國犯罪防制法制與AI技術運用概況

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

[2] 人工智慧基本法第4條規定：「政府推動人工智慧之研發與應用，應在兼顧社會公益、數位平權、促進創新研發與強化國家競爭力之前提下，發展良善治理與基礎建設，並遵循下列原則：一、永續發展與福祉：應兼顧社會公平及環境永續。提供適當之教育及培訓，降低可能之數位落差，使國民適應人工智慧帶來之變革。二、人類自主：應以支持人類自主權、尊重人格權等人類基本權利與文化價值，並允許人類監督，落實以人為本並尊重法治及民主價值觀。三、隱私保護與資料治理：應妥善保護個人資料隱私，尊重企業營業秘密，避免資料外洩風險，並採用資料最小化原則；同時在符合憲法隱私權保障之前提下，促進非敏感資料之開放及再利用。四、資安與安全：人工智慧研發與應用過程，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性與安全性。五、透明與可解釋：人工智慧之產出應做適當資訊揭露或標記，以利評估可能風險，並瞭解對相關權益之影響，進而提升人工智慧可信任度。六、公平與不歧視：人工智慧研發與應用過程中，應盡可能避免演算法產生偏差及歧視等風險，不應對特定群體造成歧視之結果。七、問責：應確保承擔相應之責任，包含內部治理責任及外部社會責任。」

隨著資訊科技日新月異，AI、雲端運算、大數據分析等新技術的應用越來越貼近日常生活，擴展了與以往截然不同的社交模式與經濟發展。這些新技術的應用係為創造人類更好的生活，然若遭濫用，影響政策與安全，甚至成為迫害他人或國家社會的工具，則將造成對全體國民、社會、國家公共利益的危害。以下分述我國對 AI 規範及犯罪防制之應用概況：

一、我國人工智慧基本法及風險分類框架

根據國際資料公司（International Data Corporation,IDC）釋出的 2024 全球政府單位趨勢預測，預計截至 2027 年底，全球將有 50%政府機關透過 AI 技術加速決策支援，藉此提升 10%市民回應速度與 15%人民公僕的生產力，也因如此，全球司法警政機構積極提升對 AI 技術掌握度。我國為促進 AI 產業發展有「產業創新條例」研發支出投資抵減等優惠措施；為推動 AI 自動駕駛有「無人載具創新實驗條例」實驗沙盒規定。惟上述規定無法取代人工智慧基本法的涵蓋內容[3]。為揭示政府整體目標與推動原則[4]，經評估宜採基本法之立法模式，訂定人工智慧基本法[5]，乃對 AI 此特定重要事務之原則性、綱領性、方針性之立法。該法於 115 年 1 月 14 日正式公布施行，數位發展部配合人工智慧基本法推動，於 115 年 7 月公布人工智慧風險分類

[3] 我國針對 AI 及其相關之應用，已陸續提出針對特定領域之若干行政指引、自律規範與部門性規範，例如 107 年立法院通過無人載具科技創新實驗條例、108 年行政院提出科技部人工智慧科研發展指引、110 年立法院通過數位發展部組織三法、111 年行政院提出行政院及所屬機關(構)使用生成式 AI 參考指引、金融監督管理委員會於 113 年提出金管會金融業運用人工智慧（AI）指引、行政院於 114 年 10 月函頒國家關鍵基礎設施應用人工智慧參考指引，要求能源、水資源等設施提供者在導入 AI 時，須嚴格串接個人資料保護法、資通安全管理法與著作權法等現行法規。

[4] 人工智慧研發及應用場域在氣候變遷、環境、醫療、金融、交通、內政、農業、公共服務等多元領域具廣泛影響力，以及對許多製造業與服務業關係密切。對於政府機關而言更涉及行政院消費者保護處、國家科學及技術委員會、內政部、教育部、法務部、經濟部、交通部、勞動部、衛生福利部、文化部、數位發展部、國家發展委員會、金融監督管理委員會、公平交易委員會、國家通訊傳播委員會、個人資料保護委員會籌備處等部會。

[5] 立法院第 11 屆第 4 會期第 2 次會議議案關係文書，院總第 20 號，政府提案第 11015829 號，114 年 9 月 24 日印發，政 1-10。

框架，將 AI 系統面臨的風險細分為 3 大類、20 項子類別等[6]。前述風險分類框架係依據人工智慧基本法第 16 條所訂定[7]，作為各目的事業主管機關訂定以風險為基礎之管理規範。

二、我國犯罪防制相關法律和 AI 技術運用

查我國犯罪防制相關法律，以「恐怖活動」、「恐怖組織」為關鍵字，搜尋相關規定，共計八部法律，包括:資恐防制法[8]、入出國及移民法[9]、財團法人法[10]、國際金融業務條例[11]、通訊保障及監察法[12]、外

[6] 人工智慧基本法推，將 AI 系統細分為 3 大類、20 項子類別分為：第一類風險：AI 系統本身之技術設計缺陷，共 8 項。涵蓋：AI 系統的安全漏洞與攻擊、缺乏透明性或可解釋性、AI 行為偏離人類意圖與社會價值、AI 具有危險的能力、影響隱私與違反個人資料保護法規、侵害智慧財產權疑慮、不公平的歧視或偏見、錯誤或誤導訊息。第二類風險：部署後操作及人機互動問題，共 6 項。涵蓋：過度依賴與不安全使用、喪失人類自主性、生成違法內容、詐欺與深偽技術濫用、用於網路攻擊、AI Agent 自主代理之授權外行為。第三類風險：社會結構與環境衝擊，共 6 項。涵蓋：企業及國家間競爭秩序失衡、權力集中與利益分配不公平、不平等加劇與就業品質下降、人類在經濟與文化上之創作價值受損、環境傷害、認知作戰與資訊主權。

[7] 人工智慧基本法第 16 條規定：「數位發展部應參考國際標準或規範，推動與國際介接之人工智慧風險分類框架，並應協助各目的事業主管機關訂定以風險為基礎之管理規範（第 1 項）。各目的事業主管機關應視人工智慧應用風險管理之需要，循前項風險分類框架，訂定以風險為基礎之管理規範，並應協助相關產業自行訂定產業指引及行為規範。有第五條第一項所列之情事者，應依法令限制或禁止之（第 2 項）。」

[8] 資恐防制法第 1 條規定：「為防止並遏止對恐怖活動、組織、分子之資助行為(以下簡稱資恐)，維護國家安全，保障基本人權，強化資恐防制國際合作，特制定本法。」、同法第第 9 條：「明知為下列個人、法人或團體，而仍直接或間接為其收集或提供財物或財產上利益者，處六月以上五年以下有期徒刑，得併科新臺幣五百萬元以下罰金：一、依第四條第一項或第五條第一項指定制裁之個人、法人或團體（第 1 項）。二、以犯前條第一項各款之罪，而恐嚇公眾或脅迫政府、外國政府、機構或國際組織為其設立目的之團體。三、以犯前條第一項各款之罪，而達恐嚇公眾或脅迫政府、外國政府、機構或國際組織之目的或計畫之個人、法人或團體（第 2 項）。明知為前項各款所列之個人、法人或團體訓練所需之相關費用，而直接或間接提供財物或財產上利益之資助者，亦同（第 3 項）。前二項所列犯罪之成立，不以證明該財物或財產上利益為供特定恐怖活動為必要。第一項及第二項之未遂犯罰之（第 4 項）。」

[9] 入出國及移民法第 7 條第 1 項規定：「臺灣地區無戶籍國民有下列情形之一者，移民署應不予許可或禁止入國：一、參加暴力或恐怖組織或其活動。二、涉及內亂罪、外患罪重大嫌疑。三、涉嫌重大犯罪或有犯罪習慣。四、護照或入國許可證件係不法取得、偽造、變造或冒用。」、同法第 18 條第 1 項第 15 款規定：「有從事恐怖活動之虞。」、同法第 24 條第 1 項第 2 款規定：「二、有從事恐怖活動之虞。」、同法第 36 條第 4 項第 4 款規定：「有危害我國利益、公共安全或從事恐怖活動之虞，且情況急迫應即時處分。」

[10] 財團法人法第 11 條第 6 項規定：「申請財團法人設立許可，有下列情形之一者，主管機關應不予許可；已許可者，應撤銷或廢止之：……。六、為恐怖組織、恐怖分子或從事恐怖活動之人，直接或間接收集、提供財物或財產上利益。……。」

[11] 國際金融業務條例第 5 條之 2 第 1 項規定：「為配合聯合國決議或國際合作有必要時，金管會會同中央銀行報請行政院核定後，得對危害國際安全之國家、地區或恐怖組織相關之個人、法人、團體、機關、機構於國際金融業務分行之帳戶、匯款、通貨或其他支付工具，為禁止提款、轉帳、付款、交付、轉讓或其他必要處置。」

[12] 通訊保障及監察法第 8 條第 3 項規定：「前條第一項所稱外國勢力或境外敵對勢力如下：……。

國護照簽證條例[13]、香港澳門關係條例[14]、臺灣地區與大陸地區人民關係條例[15]，上述法律已有將 AI 作為輔助之趨勢。惟我國人工智慧基本法第 18 條規定：「政府應依本法規定，檢討所主管之法規與行政措施；有不符合本法規定或無法規可適用者，應自本法施行後 2 年內，完成法規之制（訂）定、修正或廢止，及行政措施之改進。」基此 115 年 6 月 23 日國家人工智慧戰略特別委員會議決議[16]，要求數位發展部積極協助各目的事業主管機關進行 AI 風險盤查，尤其針對直接涉及民眾重大權益之領域，並協助各級政府完成使用 AI 執行業務之風險評估，建立內控管理機制；另請各目的事業主管機關預先規劃法規調適，協助相關產業訂定指引，針對主管領域之 AI 應用訂定管理規範，落實完善之風險管理。惟因反恐與重大犯罪防制往往涉及大規模監控與生物特徵辨識，爰此前述八部法律後續允宜透過後續配套要求各機關對照人工智慧基本法自我檢視並調整職責與法規。

參、AI 之外國法制

歐盟與美國在 AI 法規的制定上，採取了截然不同的核心路徑，歐盟以「風險等級及禁止使用」為主，美國則以「權利法案藍圖與 AI

三、以從事國際或跨境恐怖活動為宗旨之組織。」、同法第 9 條第 3 項規定：「第七條第一項所稱外國勢力或境外敵對勢力工作人員如下：……。三、擔任外國勢力或境外敵對勢力之官員或受僱人或國際恐怖組織之成員者。」

[13] 外國護照簽證條例第 12 條第 1 項第 11 款規定：「外交部及駐外館處受理簽證申請時，應衡酌國家利益、申請人個別情形及其國家與我國關係決定准駁；其有下列各款情形之一，外交部或駐外館處得拒發簽證：……、十一、有從事恐怖活動之虞者。……。」

[14] 香港澳門關係條例第 14 條第 3 項第 3 館規定：「內政部移民署於強制香港或澳門居民出境前，應給予陳述意見之機會；強制已取得居留或定居許可之香港或澳門居民出境前，並應召開審查會。但當事人有下列情形之一者，得不經審查會審查，逕行強制出境：……。三、有危害國家利益、公共安全、公共秩序或從事恐怖活動之虞，且情況急迫應即時處分。」

[15] 臺灣地區與大陸地區人民關係條例第 18 條第 3 項第 3 款規定：「內政部移民署於強制大陸地區人民出境前，應給予陳述意見之機會；強制已取得居留或定居許可之大陸地區人民出境前，並應召開審查會。但當事人有下列情形之一者，得不經審查會審查，逕行強制出境：……。三、有危害國家利益、公共安全、公共秩序或從事恐怖活動之虞，且情況急迫應即時處分。

[16] 國家人工智慧戰略特別委員會議紀錄，115 年 6 月 23 日。網址：https://naisc.nstc.gov.tw/File/4AED7512DD2CEBAD?A=C，最後瀏覽日期：115 年 10 月 29 日。

框架」為主，分述如下：

一、歐盟AI法風險等級及禁止使用之簡介

歐盟AI法（EU Artificial Intelligence Act）於2024年8月1日生效，其第3條第2款規定，「風險」係指發生損害可能性及該損害嚴重程度之組合[17]，並將AI系統的風險等級分為不可接受的風險（unacceptable risk）、高風險（high risk）、有限風險（limited risk）、極低風險或無風險（minimal to no risk）4個等級[18]，分述如下：

（一）不可接受的風險

所有被認為對人類安全、生存和權利構成明顯威脅的AI系統均應禁止，具體如下：

1、基於AI有目的操縱和欺騙；

2、利用AI對漏洞或錯誤進行攻擊；

3、社會評分；

4、個人犯罪風險評估或預測；

5、無目的地抓取網路或錄影資料，以建立或擴展人臉辨識資料庫：在公共場所進行即時遠端人臉辨識（僅限特定反恐或搜救例外）；

6、工作場所和教育機構中的情緒識別；

[17] EU Artificial Intelligence Act Article 3(2) 'Risk' means the combination of the probability of an occurrence of harm and the severity of that harm.

[18] Artificial Intelligence Act，網址：https://artificialintelligenceact.eu/the-act/，最後瀏覽日期：115年10月12日。

7、利用生物特徵分類推論某些受保護的特徵；

8、在公共場所進行即時遠端生物識別，以用於執法目的；

9、AI 能夠產生未經同意之隱私內容或兒童性虐待影像與散播。

（二）高風險

可能對健康、安全或基本權利構成嚴重風險的 AI 應用案例被歸類為高風險案例。這些高風險案例包括：

1、關鍵基礎設施（例如交通運輸）中的 AI 安全組件，其故障可能會危及公民的生命和健康；

2、教育機構中使用的 AI 解決方案可能會決定一個人接受教育的機會和職業生涯的發展方向；

3、基於 AI 的產品安全組件（例如機器人輔助手術的應用）；

4、用於就業、員工管理和自主創業的 AI 工具；

5、某些 AI 應用案例被用於提供私人和公共服務；

6、用於遠端生物特徵識別和生物特徵分類的 AI 系統；

7、AI 在執法領域的應用可能會干涉人們的基本權利；

8、AI 在移民、庇護和邊境管制管理中的應用案例；

9、用於司法和判決資料庫的 AI 解決方案。

（三）有限風險

這指的是 AI 使用過程中透明度需求所帶來的風險。AI 法案引入具體的揭露義務，以確保在必要時告知公眾，從而維護信任。例如，

在使用聊天機器人等 AI 系統時，應告知公眾他們正在與機器交談，以便他們能夠做出明智的決定。此外，生成式 AI 提供者必須確保 AI 產生的內容可識別。

（四）極低風險或無風險

AI 法並未對被認為風險極低或無風險的 AI 制定規則。目前歐盟使用的絕大多數 AI 系統都屬於此類，包括線上視訊遊戲或垃圾郵件過濾器等應用。

觀諸歐盟 AI 法規範之各類行為態樣，可觀察出立法者對 AI 採取嚴格的禁止要求，倘若使用禁止使用的 AI 系統者，最高可處 3,500 萬歐元，或上一會計年度全球年營業額的 7%；不遵守其他要求者，最高可處 1,500 萬歐元，或上一會計年度全球年營業額的 3%[19]。

二、美國 AI 權利法案藍圖與 AI 框架之簡介

美國在 AI 的監管與治理上，採取由權利法案藍圖與框架構成的漸進式治理網絡。其政策核心從著重公民權利的 AI 權利法案藍圖，走向保障創新與國家競爭力的 AI 國家政策框架，AI 必須與風險管理相輔相成[20]。

（一）AI 權利法案藍圖

美國於 2022 年 10 月發布「AI 權利法案藍圖」(Blueprint for an AI Bill of Rights)[21]，並列出五大應用原則，包括：

1、安全且有效之系統 (Safe and Effective Systems)：民眾應受到

[19] EU Artificial Intelligence Act, Commission Proposal, Article 71(3)、(4).

[20] AI Bill of Rights' must be accompanied by NIST risk，網址：https://fedscoop.com/nist-work-complements-ai-bill-of-rights/，最後瀏覽日期：115 年 10 月 29 日。

[21] Artificial Intelligence Bill of Rights，2022 年 10 月。網址：https://www.managementsolutions.com/en/publications-and-events/regulatory-notes/technical-notes-on-regulations/blueprint-artificial-intelligence-ai-bill-rights，最後瀏覽日期：115 年 10 月 29 日。

保護，避免使用不安全或無效之系統。

2、避免使用有缺陷之演算法（Algorithmic Discrimination Protections）：民眾不應被迫接受使用有缺陷之演算法，系統設計需完善且可被使用。

3、資料隱私（Data Privacy）：應透過內部管制機制，防止民眾資料遭不當利用，並有專責窗口監管各項資料使用情形。

4、理解自動化系統運作原理（Notice and Explanation）：民眾於使用自動化系統時，應先理解其運作原理，以及影響系統運算與判斷之因素，以利協助釐清最終所獲得之結果。自動化系統應提供技術上有效、有意義與有用之解釋，並根據上下文校準風險級別。

5、人員之替代方案、考慮及後備（Human Alternatives, Consideration and Fallback）：於適當情況下，民眾應能選擇退出自動化系統，並得到人工協助。適當性應根據給定背景下之合理期望來確定，重點是確保廣泛之可及性與保護民眾免受特別有害之影響。

（二）AI 風險管理框架

美國白宮於2026年3月20日發布「AI 風險管理框架」（National AI Legislative Framework）」，力求以單一的聯邦法規取代散見各州的監管制度，並重點保護兒童、智慧財產權、與社區免受 AI 潛在危害。七大核心目標與建議方向如下[22]：

1、保護兒童並強化家長權能：推動強化未成年人數位安全、賦予家長更多管理孩子數位環境的權力。

2、保障及強化美國社區：透過經濟成長與能源主導地位，支持小企

[22] President Donald J. Trump Unveils National AI Legislative Framework，2026年3月20日。網址：https://www.whitehouse.gov/releases/2026/03/president-donald-j-trump-unveils-national-ai-legislative-framework/i，最後瀏覽日期：115年10月12日。

業與地方社群發展。

3、尊重智慧財產權與支持創作者：處理 AI 訓練與版權爭議，同時研議允許版權持有人進行集體授權談判的、具反壟斷豁免機制的框架。

4、防止言論審查與保護言論自由：限制聯邦政府出於黨派或意識形態理由強迫 AI 提供商限制或更改內容。

5、推動創新與確保美國 AI 領導地位：建立「監管沙盒」(Regulatory sandboxes）並加速資料中心等基礎建設。

6、教育美國人並培養 AI 準備就緒的勞動力：協助美國勞工適應 AI 時代的培訓與教育。

7、建立聯邦政策框架：統合標準並對抗各地繁瑣的州法限制。

美國 AI 框架主張透過現有機構依其專業領域彈性管理，同時亦要求建立聯邦層級之 AI 法規，制定全國一致之標準。強調監管鬆綁，並欲降低對 AI 之嚴格管制，促進創新及強化美國競爭力[23]。

肆、問題研析與建議

一、AI 促成恐怖組織進化，建議警察法刪除未符時宜之任務界限

論者認[24]，科技技術的發展恐怖主義組織相比過往掌握更多科技

[23] 美國在聯邦層面至今未能通過一部全面性的 AI 監管法律。1.雖然藍圖本身不是法律，但它對接了美國憲法、聯邦法律及各項現行法規範（如反歧視法、消費者保護法等），讓執法機構能依據現有法律來約束不當的 AI 應用。在此背景下，各州紛紛以自身的立法。例如 3.1 Colorado AI Act（SB 24-205），適用於在科羅拉多州營運或向其居民提供服務的「高風險 AI 系統」開發者（Developer）與部署者（Deployer）。「高風險 AI 系統」被定義為在教育、就業、金融服務、醫療保健、保險、住房或法律服務等領域做出或實質性地輔助「consequential decisions」（重大決策）的 AI 系統。法案另規定，自 2026 年 2 月 1 日起，高風險系統的部署者必須採取合理措施，保護消費者免受高風險系統中任何已知或可合理預見的演算法歧視風險的影響。SB24-205 Consumer Protections for Artificial Intelligence，2024 年 5 月 17 日。網址：https://leg.colorado.gov/bills/sb24-205，最後瀏覽日期：115 年 10 月 12 日。

[24] 郭承諭、蔡震榮，〈國土安全與反恐〉，《中央警察大學國土安全與國境管理學報》，第 40 期，

化、效率化的大規模殺傷性武器或高危險性和生化基因武器，並且透過網際網路的快速傳播性大量招募組織人員，使得恐怖主義組織能夠更加隱蔽且高效率地執行恐怖行動和招募。恐怖主義顯著改變了警察之角色，為確保公眾安全並打擊恐怖行為，各國加強警察之執行力，（包括新興 AI 辨識人類面部與虹膜、運用衛星偵蒐能力強化全天候聯合情監偵能力）並建立強大的監控系統，包括運用先進技術，與情報機構合作，密切監控潛在威脅。警方還必須加強預防措施，加大對治安力量脆弱地區巡護量能，並在關鍵地點實施嚴格的安檢措施，專門的培訓裝備警察人員，有效應對和減輕恐怖襲擊，方為當務之急。

依 106 年 8 月 12 日舉行之總統府司法改革國是會議總結會議，針對「維護社會安全的司法分組（第五分組）」就智慧科技時代「警察犯罪預防策略」[25]，要求提升警察專業與執法效能。查我國警察法於 42 年制定公布迄今歷經 4 次修正，皆因組織變革，如新設警察專科學校或精省等所作之修正，於警察任務、組織、權限、中央地方分權等重要事項均未變更。加上政府組織改造後，現行警察法規定已有與現況不相符之情形。例如第 5 條第 3 款，明定警政署所掌理警察業務中，關於管理出入國境之國境警察業務，業已改由內政部移民署主政；同條第 5 款，關於防護連跨數省河湖及警衛領海之水上警察業務亦改由海洋委員會海巡署主政。第 9 條第 7 款仍維持傳統行政警察概念，將「有關警察業務之保安、正俗、交通、衛生、消防、救災、營業建築、市容整理、戶口查察、外事處理等事項。」列為警察之法定職權，迄未修正。然實際上前開事項 早已由相關專責機關掌理，足見現行規定已與現況脫節而亟待修正。另依司法院釋字第 570 號解釋理

112 年 12 月，頁 7。

[25] 106 年 8 月 12 日總統府司法改革國是會議成果報告，網址：https://www.president.gov.tw/File/Doc/8ca89cf6-00e2-4c35-9fe3-d6e54bb90e89，頁 84，最後瀏覽日期：112 年 10 月 24 日。

由書意旨，警察法第 9 條第 1 款規定，警察有發布警察命令之職權，僅具組織法之劃定職權與管轄事務之性質，欠缺行為法之功能，不足以作為發布限制人民自由及權利之警察命令之授權依據，故關於警察任務及職權等規定，亦有修正之必要。釐清警察與其他行政機關間防止危害任務之界限及職務協助關係，避免造成主從不分、權責不明。

為因應上述總統府司法改革國是會議智慧科技需求，行政院於 107 年 6 月核定「108-111 年警察執法設備及效能提升方案」，運用科技協助偵辦案件[26]。後續於 115 年 6 月 23 最新核定「警察科技與執法設備提升計畫（116 年至 119 年）」，面對新一代 AI 科技浪潮，未來警政體系應整合 AI 技術應用，例如擴大無人機運用、推動科技執法與人本安全並重的治安與交通治理模式。行政院亦於立法院第 11 屆第 1 會期施政方針報告提出，政府將首重「五打七安」，不遺餘力的打擊黑、金、槍、毒、詐，保障治安、食安、道安、工安、校安、居安及資安，守護安定公義的社會[27]。

綜上，現行法規更新速度落後 AI 科技變遷，配合人工智慧基本法 2 年內的通盤法規檢討期[28]，現行的警察法及相關警察職權行使法、偵查規範等，預期將逐步納入 AI 決策說明權、風險評估及、救濟

[26] 行政院 107 年 6 月 7 日院臺法字第 1070019109 號函核定「108-111 年警察執法設備及效能提升方案」，分 4 年辦理，總經費新臺幣 13 億 9,901 萬 8 千元，包含「涉案車輛行車紀錄雲端創新應用發展計畫」、「強化數位跡證鑑析能力計畫」、「通訊監察系統建置計畫」、「鑑識及防爆效能推升計畫」、「警通網路效能提升計畫」及「精實警用車輛計畫」等 6 項子計畫。內政部警政署，108-111 年警察執法設備及效能提升方案，111 年 5 月，頁 4。

[27] 行政院 115 年 6 月 23 日院臺法字第 1151054505 號函核定「警察科技與執法設備提升計畫成本效益分析報告」，本計畫包含「鑑識及防爆效能精進計畫」、「強化刑案偵查情資調閱平臺計畫」、「通訊監察核心韌性躍升計畫」、「預防山林盜伐之精進作為計畫」、「強化警用通訊網路韌性計畫」及「汰換警用車輛計畫」等 6 項子計畫，計畫期程為 116 年至 119 年，總經費新臺幣（以下同）31 億 1,113 萬 2,000 元。規劃以「政府挺警察，警察守治安」為核心，透過「精進鑑識及防爆效能」、「強化刑案偵查情資調閱」、「更新通訊監察設備」、「擴大山林科偵量能」、「提升警用通訊網路韌性」及「汰換老舊警用車輛」6 大策略，達到「設備有用」、「警察有為」、「人民有感」3 大願景。。內政部警政署，警察科技與執法設備提升計畫（116 年至 119 年），115 年 8 月，頁 1。

[28] 人工智慧基本法第 18 條規定：「政府應依本法規定，檢討所主管之法規與行政措施；有不符合本法規定或無法規可適用者，應自本法施行後 2 年內，完成法規之制（訂）定、修正或廢止，及行政措施之改進。」

機制及司法院相關 AI 責任認定[29]。爰建議研修警察法，刪除未符時宜之警察業務[30]，並參考數位發展部人工智慧風險分類框架[31]，以符現代社會治安維護需求現況。

二、檢討人臉辨識設立人為介入審查機制，避免歧視或偏見情事

查 111 年第三次兩公約國家人權報告，國際審查委員結論性意見第 85 點建議：「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。」現行我國人臉辨識（Facial Recognition）技術在海關出入境、執法、戶政、教育等場域之運用實例逐漸增多。美國國家標準與技術院（National Institute of Standards and Technology, NIST）2019 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。論者認[32]，因個人資料而導致對自然人歧視的分析建檔應予禁止。為求合法，資料蒐集、建檔不能單純僅有與資料當事人種族、民族或宗教信仰相關的資料，且如果其使用會導致不客觀且不合理證明的歧視。爰此，人臉辨識演算法若人口族群代表性不足，則可能導致不同族群匹配結果之準確率不同，從而造成歧視。歐盟

---

[29] 司法院於 115 年 4 月 22 日頒布了司法院及所屬各機關使用人工智慧系統參考指引，明定 AI 在審判體系中僅能作為「輔助工具」，事實認定、法律適用與裁判核心仍須由法官親自為之。針對訴訟當事人使用 AI 撰寫書狀，近期法院實務（如臺北地院 115 年度聲再字第 13 號裁定、最高法院相關裁判）也指出：當事人不因使用 AI 而免除訴訟行為的責任，書狀內容的真意與法律效果仍由具名的當事人或代理人承擔，法院不會直接承認 AI 為表意人。

[30] 隨著科技迅速發展，利用虛擬資產、暗網交易、Deepfake（深偽技術）等新興工具，對我國現有法律體系帶來嚴峻挑戰。儘管政府持續修正刑法及相關特別法，仍存在法規更新速度落後於科技變遷之問題，導致對新型態詐欺行為之界定與處罰尚有不足。以虛擬資產（如加密貨幣）為例，常被用於吸金詐欺、洗錢等犯罪，但我國對虛擬資產之全面性認識與監管尚不成熟，執法人員在偵查過程中對虛擬資產追蹤和扣押面臨技術及程序上之困難許鈺媜，財團法人民間司法改革基金會（2025），座談側記｜虛擬資產犯罪實務解析之司法實務的挑戰篇，網址：https://www.jrf.org.tw/articles/2500，最後瀏覽日期：115 年 10 月 7 日。

[31] 針對人工智慧基本法第 18 條所定之 2 年法規檢討期，數位發展部已於 115 年 7 月 7 日依同法第 16 條正式發布人工智慧風險分類框架。該框架所建立之「盤點應用情境、識別風險、評估風險、應對風險」四步驟操作流程。

[32] 吳瑛珠，〈運用人工智慧進行預測性警務的人為干預要求－以歐盟與德國法制為例〉，《中央警察大學法學論集》，第 50 期，115 年 4 月，頁 290。

一般資料保護規則（General Data Protection Regulation,GDPR）第 9 條第 1 項規定[33]：「禁止處理有關揭露種族或血統、政治觀點、宗教或哲學信仰或工會身分之個人資料，及基因資料、為識別特定自然人之生物識別資料、健康資料或自然人性生活或性傾向有關之個人資料。」另有研究報告認[34]，資料正確性方面，人臉辨識系統如統計上的準確性不足，可能導致歧視與偏見，對個資當事人權益影響甚鉅。我國個資法雖未明文要求防範對個資當事人之偏見，但要求保有個人資料之機關維護個人資料正確性，且個人資料之蒐集、處理或利用應以尊重當事人權益之方式為之。

依國家發展委員會 110 年 4 月 16 日發法字第 1100005839 號有關戶政事務所使用「輔助人員辨識確認系統」是否符合《個資法》規定一節，函釋略以：「……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，……。」論者認[35]，AI 機器學習具有「內在不可預測性」（inherently unpredictable）使支持者所宣稱優於人類道德判斷的程式設計，可能只是一種技術性的「希望軟體」（technological hopeware）。查我國關於人臉辨識係散見於入出國及移民法第 68 條[36]、第 91 條[37]以監獄及看守所科技設備設置與使用

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

[34] 達文西個資暨高科技法律事務所，《歐盟、英國及加拿大對警察機關或執法機關運用人臉辨識技術之指引或其他相關文獻探討（計畫編號：NDC0111019）》，國家發展委員會 111 年度委託研究計畫，111 年 10 月，頁 68。

[35] 巫穎翰，〈致命自主武器系統規範爭議的探討與展望〉，《安全與情報研究》，第 9 卷第 2 期，115 年 7 月，頁 111。

[36] 入出國及移民法第 68 條第 4 項規定：「以電子設備進行個人生物特徵識別資料之辨識。」

[37] 入出國及移民法第 91 條第 1 項規定：「外國人、臺灣地區無戶籍國民、大陸地區人民、香港及澳門居民於入出國（境）接受證照查驗或申請居留、永久居留時，移民署得運用生物特徵辨識科

及管理辦法等。

綜上，資料正確性方面，人臉辨識系統如統計上的準確性不足，可能導致歧視與偏見，對個資當事人權益影響甚鉅。主管機關宜參考歐盟立法例，公務機關宜在人臉辨識技術設計和採購階段，即可採取降低歧視風險之措施，設立人為介入審查之機制，避免歧視或偏見之情事。

三、生物特徵識別指紋自動查驗通關，應以法律明定錄存目的

隨著航空業的持續發展，飛航安全始終是各方關注的核心議題。AI 影像辨識技術應用範圍相當廣泛，不僅包含基本人臉和車牌辨識，還擴展至入侵偵測、醫療行為、互動遊戲、農業生產、商場行為分析、運動教學輔助、跌倒偵測以及產線公共安全等[38]。這些技術能夠自動進行安全分析和異常事件的檢測與通報，進而大幅減少人力監控監視器之需求和時間。透過 AI 技術，飛行數據可以快速進行分析與處理，及時發現潛在風險並改善，避免事故發生[39]。各國海關與移民局（如美國等）在入境檢查時，會透過掃描指紋來核對旅客身份，防止恐怖分子或危險分子冒名頂替或持假護照入境。指紋辨識技術在反恐與

技，蒐集個人識別資料後錄存。」

[38] 智慧機場（Smart Airport）係指機場導入智慧化科技，整合機場資通訊服務所需各項應用功能，如大數據(Big Data)、人工智慧(Artificial Intelligence， AI)、邊緣雲(Edge Cloud)、數位分身(Digital Twin)、生物辨識(Biometric)及機場協調整合決策(Airport Collaborative Decision Making，A-CDM）系統等，實現一鍵式線上服務，並同時擴充、改善、整合資料庫，將機場所有利益相關者進行充分連結，實現不同領域資訊共享，使資訊系統與作業流程均能協同合作，方便即時調度人力與設備，以即時回應及處理營運及旅客需求，俾達到機場資源配置最佳化，為旅客提供最佳服務品質與旅遊體驗，同時降低機場成本及增加收入，交通部運輸研究所編印，《國際推動機場智慧化趨勢及我國發展課題探討》，113 年 2 月，頁 2。

[39] 目前桃園機場、臺北松山機場的 One ID，在短期內只能做到讓旅客於登機證、護照檢查時，透過生物辨識方式通行；但涉及政府不同機關業務，如移民審查作業時，仍無法整合使用；此外若要在登機門也使用 One ID 通行，也需要與航空公司、地勤的旅客系統進行整合、資料串接，這些都需要在法規調適、系統與資料介接上進一步溝通、整合，並評估優化民航資訊交換機制之可行性。不同利害關係人（如航空公司、地勤、服務營運商、貨運業者等）使用各自的系統，標準不一，導致數據難以即時整合，影響智慧化營運成效。機場單位雖已著手建立跨系統標準協議，但仍期待由交通部統籌制定標準，並協助跨機關協調，以利促進不同系統間的無縫對接，交通部運輸研究所編印，《國際推動機場智慧化趨勢及我國發展課題探討》，113 年 2 月，頁 34-35。

邊境安全中被廣泛應用，主要用來追蹤、過濾與識別潛在的威脅分子。民航業對恐怖份子一直是非常具有吸引力的目標，民用航空具有高度國際性及經濟性的特色，加上部分國家的航空公司屬屬國營事業，因此攻擊該航空公司，同時象徵攻擊該國家[40]。

查我國機場自動查驗通關係依入出國及移民法第 4 條規定：「入出國者，應經移民署查驗；未經查驗者，不得入出國（第 1 項）。移民署於查驗時，得以電腦或其他科技設備，蒐集及利用入出國者之入出國紀錄（第 2 項）。前二項查驗時，受查驗者應備文件、查驗程序、資料蒐集與利用應遵行事項之辦法，由主管機關定之（第 3 項）。」另同法第 91 條第 1 項規定：「外國人、臺灣地區無戶籍國民、大陸地區人民、香港及澳門居民於入出國（境）接受證照查驗或申請居留、永久居留時，移民署得運用生物特徵辨識科技，蒐集個人識別資料後錄存。」而這些個人的生物特徵係以個人資料作連結，藉此識別個人的身分，以作為通關之用，與資訊隱私權息息相關[41]。

觀諸現行外國人（外來人口）與本國國民，在入出國及移民法及申請及使用入出國自動查驗通關系統作業要點等相關邊境管理實務中之生物特徵錄存規範，核心差別如下[42]：

---

[40] 交通部民用航空局編印，《航空運輸專論》，101 年 4 月，頁 86。

[41] 依據內政部移民署 113 年 12 月 23 日移署境字第 1130155260 號函：（一）為擴大 e-Gate 使用對象，自 114 年 1 月 1 日起，調降申請使用年齡至 10 歲且身高下修為 120 公分；無戶籍國民持中華民國有效晶片護照，免事先申請入國許可，亦得申請使用 e-Gate。（二）該署新世代 e-Gate 具閘道內註冊及通關二合一功能，於進入閘道前選擇錄存臉部影像，或選擇錄存臉部影像及指紋，即可同步完成註冊及通關。另所有外來人口符合使用年齡且已完成入境生物特徵擷取者，均得於出境時使用 e-Gate，提供旅客更便利及快速的通關服務。（三）我國與他國推動互惠使用 e-Gate 之國家有美國(全球入境計畫 Global Entry)、韓國、澳洲、義大利、德國、新加坡及馬來西亞等 7 國，持效期 6 個月以上晶片護照之國民得申請使用 e-Gate。前述國家國民以旅遊或商務等事由來臺短期停留者，經人工註冊櫃完成註冊後（現尚未開放閘道自助註冊功能），每次通關前應完成電子 A 卡填繳且簽證種類勾選「免簽證」欄位者，入境時即可使用 e-Gate。

[42] 內政部移民署網站，本國國民申辦自動查驗通關及使用說明。網址：https://www.immigration.gov.tw/5385/7445/7889/7892/50760/，最後瀏覽日期：115 年 10 月 11 日。

（1）外國人（外來人口）：指紋為「法定強制錄存」：依據入出國及移民法第 91 條規定，外國人等外來人口在「入出國境接受證照查驗」或「申請居留、永久居留」時，移民署得運用生物特徵辨識科技，蒐集並錄存個人識別資料。未配合者，移民署得不予許可其入國、居留或永久居留。

（2）本國國民：指紋為「自願錄存」：並不適用上述第 91 條的強制錄存規定。有戶籍國民不論是出國或入國，只要持有有效護照即可通關。

國際旅客來臺觀光人數逐漸升高，每年入出境人次急速攀升，運用生物特徵辨識科技已成為國境安全管理之重要核心。然針對臺灣地區有戶籍國民自動查驗通關自願錄存指紋部分，似尚無法律明定其蒐集之目的。按司法院釋字第 603 號解釋之意旨[43]：「國家基於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。」指紋等生物特徵，因具有人各不同、終身不變之特質，一旦與個人身分連結，即屬具備高度人別辨識功能之個人資料。

綜上，有研究報告認[44]，生物特徵資料之保護應與其敏感性相當，而不宜僅以一般個人資料性質看待。查入出國及移民法第 91 條「規範對象」，並未包括臺灣地區有戶籍國民，申請及使用入出國自動查驗通關系統作業要點，法位階亦不足。國家若基於特定重大公益之

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

[44] 達文西個資暨高科技法律事務所，同註 34，頁 67-68。

目的，有大規模蒐集、錄存人民指紋並建立資料庫之必要，即便是本國國民自願錄存指紋，建議仍應以法律明定錄存目的。

四、強化無人載具應用行為，研議訂定適當防範措施與倫理權衡

查我國無人載具科技創新實驗條例第 3 條第 1 項第 1 款規定：「無人載具：指車輛、航空器、船舶或其結合之無人駕駛交通運輸工具，透過遠端控制或自動操作而運行，且具備以下技術……。」，亦即指的是透過遠端駕駛或自動操作而運行，且可用於載運客貨之無人駕駛交通運輸工具，其範疇涵蓋陸（如自駕車）、海（如自動化船舶）、空（如無人機）等不同領域的載具。論者認[45]，AI 改變了訊息傳播模式並加速了訊息擴散的效益，一旦遭到不當的利用則容易變成惡意行為者製造和傳播爭議訊息及操縱目標受眾感知的不法工具；例如透過深偽技術進行換臉、鍵入特定提示詞生成特定圖像、影片或運用演算公式媒介特定言論訊息，藉情感化互動模式影響受眾思想情緒；於群眾間挑撥分化、製造矛盾對立，進而鼓譟目標受眾從事破壞公共秩序甚或改變社會價值觀；因此對於 AI 發展與應用行為制訂適當的防範措施暨法律規範，是目前各國政府在於 AI 研發上應高度關切議題 。

一般認為，無人機在所謂「反恐」戰爭的應用上，只會針對極少數特定的對象，而且造成的平民傷亡很少。但事實上，在世界各地的戰場上，無人機已經造成數千人死亡，其中有許多都是平民。即使是搭乘在戰場上近距離盤旋的直升機，都已經不容易判斷現場的狀況[46]。有論者認[47]，無人機的使用，特別是在非戰鬥區域，提出了重大的

[45] 趙萃文，〈科技創新下的法律挑戰－以人工智慧為中心〉，《軍法專刊》，第 70 卷第 2 期，113 年 5 月，頁 94。

[46] 林宗德，機器人倫理學專題報導（一）：無人機的警示，科技大觀園，網址：https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=6f786f6b-e4ab-4e2e-918c-3aa3d70d1254，最後瀏覽日期：115 年 10 月 12 日。

[47] 洪澤顥、周傑泰，〈運用 SWOT 分析探討導入無人機空軍軍機維保作業調整策略〉，《空軍學術雙月刊》，第 707 期，114 年 8 月，頁 126。

倫理和法律問題，問題包括無人機攻擊在主權領土上的合法性、平民傷亡和附帶損害、無人機操作中的責任制和透明度，都是值得重視的問題。AI 兼具軍民兩用與高度資料驅動特性，其發展脈絡牽涉敏感的安全與道德議題。若缺乏充分的法制規範與倫理評估，AI 技術在武器化運用或隱私侵害中可能對全球安全構成潛在威脅，也可能在醫療、交通和金融等領域引發系統性風險。因此，AI 的推廣與部署不僅須兼顧技術創新與經濟效益，也必須考量監管與社會衝擊，確保技術落實於軍民兩用場合時，能平衡國際安全、人類福祉與可持續發展等核心價值。倫理上，機器是否應在缺乏即時人類判斷下行使致命武力；法律上，則涉及法律能否符合國際法對區分、比例、必要性與責任之要求；政治經濟上，國家追求戰略優勢可能加速 AI 軍事化，並透過國防採購、研發合作與安全需求，促使大型科技企業調整既有的倫理限制。換言之，國家可能為技術優勢淡化倫理與法律考量，企業亦可能受資金、技術、政府市場與競爭誘因吸引而向軍事應用靠攏[48]。

綜上，爰建議設立跨部會 AI 倫理審查委員會，由法律、科技、社會學等領域專家組成，對重大 AI 研發項目進行事前倫理風險評估和事中監督。另外，修訂相關法規為 AI 測試提供空間，例如沙盒機制（Sandbox）讓某些新技術在監管下試用，同時完善保密法規以便利與民間技術交流[49]。無人載具應用行為，研議訂定適當防範措施與倫理權衡，透過制度化的審查與規範，為 AI 安裝「安全欄杆」，在追求創新的同時守住道德與法律底線[50]。

[48] 巫穎翰，同註 35，頁 94。

[49] 于子揆，〈人工智慧於軍事應用之發展與管制：國際趨勢與我國政策建議〉，《國會季刊》，第 53 卷第 4 期，114 年 12 月，頁 104。

[50] 林玉書，數位創新實驗法規沙盒制度研析，資訊工業策進會科技法律研究所，112 年 1 月 17 日，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8966，最後瀏覽日期：115 年 10 月 7 日

五、明確區分 AI 風險分類框架，強化隱私數據保護之必要性

依人工智慧基本法第5條第2項規定：「政府應以兒少最佳利益為原則，AI 產品或系統經中央目的事業主管機關會商數位發展部認定為高風險應用者，應明確標示注意事項或警語。」、同法第16條第1項規定：「數位發展部應參考國際標準或規範，推動與國際介接之人工智慧風險分類框架，並應協助各目的事業主管機關訂定以風險為基礎之管理規範。」亦即，高風險 AI 係由各目的事業主管機關依「風險分類框架」之風險評估原則認定；依第5條第2項規定，人工智慧產品或系統經中央目的事業主管機關會商數位發展部認定為高風險應用者，應明確標示注意事項或警語。惟論者認[51]，目前我國公部門風險管理主要依行政院及所屬各機關風險管理及危機處理作業手冊執行，該手冊已整合內部控制、風險管理與績效管理三大機制，並明確規範風險管理（含內部控制）步驟六大步驟:首先，建立背景資料，並界定內外部風險因素;其次，運用歷史資料、SWOT、腦力激盪等方法辨識風險;再來透過可能性與影響程度分析評估風險，並建立分級標準;接著採取接受、規避、抑減、移轉等策略，並制定處理計畫，以處理風險;然後進行自主與外部監督及滾動檢討;最後，藉由傳遞資訊、溝通及諮詢，強化內外部溝通，並提升透明度。其中，風險評估階段特別強調風險分級與風險可容忍度的設定，透過風險值等於可能性乘以影響程度進行計算。

論者亦認[52]，我國人工智慧基本法第19條[53]雖已對公部門使用使AI課予風險評估與內控管理機制之法定義務，在尚未建立一致的細部程序與標準前，易致治理落差與形式化評估。為縮短 AI 技術快速演進

[51] 潘俊良，〈公部門人工智慧應用之風險評估與內控治理—以歐盟人工智慧法及相關 ISO 國際標準為借鏡之法制建構〉，《科技法律透析》，第 38 卷第 2 期，115 年 7 月，頁 122。

[52] 同前註，頁 125。

[53] 人工智慧基本法第 19 條規定：「政府使用人工智慧執行業務或提供服務，應進行風險評估，規劃風險因應措施。 政府應依使用人工智慧之業務性質，訂定使用規範或內控管理機制。」

與現行制度間的落差，可在「行政院及所屬各機關風險管理及危機處理作業手冊」核心結構下，將 AI 專屬風險及應變嵌入現有流程節點與表單:例如，參照歐盟 AI 法對高風險 AI 之基本權利影響評估、人為監督與可解釋、資料與紀錄保存、以及透明度義務等要求，於「風險辨識、評估（分析及評量）、處理、監督、資訊傳遞與溝通」各步驟建立相應作法、審查清單與記錄保存週期，將「行政營運風險管理」升級為「專業 AI 應用風險管理」，並得以與國際規範接軌[54]。

論者肯認[55]，隱私數據的保障係為現今 AI 應用上相當矚目的議題，AI 的運用須以數據資料作為演算的基礎，但其數據資料多半與個人隱私資料息息相關，因此在於該數據的應用及保障上即會產生矛盾。具有特定個人識別性之符號，如顏面辨識、虹膜辨識資料為個人生理、身體特徵經數位化後之個人識別符號，或由提供資通訊服務事業所分配給利用人之身分辨別號碼，個人使用網路所被長期蒐集之瀏覽履歷（life log）、位置資料等，如被長期大量蒐集或跨業界領域共用時，一經網路串聯比對，往往可描繪出個人生活動向行動履歷、或推知個人消費傾向、興趣嗜好等，使當事人隱私權受到極大威脅，實有必要將個人識別符號納入個資法領域中，以規範其蒐集、處理及利用。

續從憲法層次觀察，人工智慧系統因其高度仰賴大規模資料蒐集、交叉分析與自動化決策，對個人隱私權與資訊自主權構成結構性壓力[56]。人工智慧基本法在第5條第2項及第17條中賦予「高風險應用」

[54] 各目的事業主管機關執行 AI 風險管理之主要遵循流程，依序包含以下四步驟：一、盤點應用情境：整理所管產業 AI 應用之基本資訊，作為風險評估準備。二、識別風險：對照風險類型表，識別潛在風險類型。三、評估風險：評估風險影響程度，判定是否為高風險 AI 應用。四、應對風險：依風險情形規劃促進發展措施或管理措施，並應定期檢視法令規範。數位發展部編印，《人工智慧風險分類框架》，115 年 7 月，頁 iii。

[55] 范姜真媺，〈大數據時代下個人資料範圍之再檢討—以日本為借鏡〉，《東吳法律學報》，第 29 卷第 2 期，106 年 10 月，頁 1。

[56] 林輝煌，〈我國人工智慧基本法之制度性侷限與法治落實之道——從刑事程序、行政法與憲法審查觀點出發〉，《最高檢察署月刊》，第 41 期，115 年 1 月，頁 8。

特定法律效果。至於真正具有等級化設計者，仍由各目的事業主管機關訂定。換言之，人工智慧基本法的重點，是先確認某一 AI 應用是否進入「高風險」類型，若一旦進入，即應依第17條啟動責任歸屬、歸責條件以及救濟、補償或保險等制度[57]。又若 AI 應用經評估，有發生人工智慧基本法第5條第1項所列之情事（如侵害人民生命、國家安全等），且評估依現行技術手段，仍無法有效管理或降低該應用風險者，目的事業主管機關應依同法第16條第2項規定，依其主管法令（包括既有作用法或後續配合 AI 應用訂定之法令），予以限制或禁止其應用。若目的事業主管機關評估其所管領域的 AI 應用為高風險時，依據人工智慧基本法第5條第2項規定，應要求所管業者明確標示注意事項或警語；並依同法 17條第1項規定，明確其責任歸屬及歸責條件，並建立其救濟、補償或保險機制。

綜上，依人工智慧基本法第16條第2項規定[58]，各目的事業主管機關基於人工智慧應用風險管理之需要，得對轄管產業制定管理規範。因而，目的事業主管機關在盤點轄管產業的高風險 AI 應用情境時，可依產業領域的專業特性和需求參考國際經驗或相關規範協助其風險判定，故[59]參考前述歐盟外國立法例，目前針對 AI 的治理，皆普遍採用「風險導向」，要藉由 AI 風險分類框架來識別風險，以強化隱私數據保護。我國由數位發展部負責建立 AI 風險分類框架，警察機關所採購或開發的執法 AI 系統（如車牌辨識、犯罪大數據分析、深偽

[57] 張麗卿，〈AI 基本法下高風險智慧醫療之治理〉，《當代法律》，第 54 期，115 年 6 月，頁 109。

[58] 人工智慧基本法第 16 條第 2 項規定：「各目的事業主管機關應視人工智慧應用風險管理之需要，循前項風險分類框架，訂定以風險為基礎之管理規範，並應協助相關產業自行訂定產業指引及行為規範。有第五條第一項所列之情事者，應依法令限制或禁止之。」

[59] 人工智慧基本法第 4 條第 3 款規定：「隱私保護與資料治理：應妥善保護個人資料隱私，尊重企業營業秘密，避免資料外洩風險，並採用資料最小化原則；同時在符合憲法隱私權保障之前提下，促進非敏感資料之開放及再利用。」第 4 款規定：「資安與安全：人工智慧研發與應用過程，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性與安全性。」第 14 條規定：「各目的事業主管機關會商個人資料保護主管機關，在人工智慧研發及應用過程，避免不必要之個人資料蒐集、處理或利用，並應促進個人資料保護納入預設及設計相關措施或機制，以維護當事人權益。」

偵測等），必須依其風險等級進行分類與列管。透過法律、科技等多面向同步深化，明確區分 AI 風險分類框架，強化隱私數據保護之必要性，方能從根本面保障民眾權益。

六、建立預測性警務犯罪防制，允宜遵守法律保留原則

有論者認[60]，隨大數據的持續增長，擁有大量資料存取權限的執法機關，長期存在專業知識、經驗與能力的學習落差，須掌握快速發展的技術能力，了解最新進展的潛在影響，方能強化 AI，協助打擊或預防犯罪。AI 技術雖能滿足執法機關的某些需求，也須審慎檢查、評估和調校 AI 技術的運用方式，作為執法機關判斷模式和分析方法。AI 技術的導入對公部門而言，實為機遇與挑戰並存之雙重局面[61]，其對於公共行政的助益，包括行政流程簡化、強化效率及創新品質、決策制定優化、參與透明提升等。我國107年起著手規劃推動「警政科技躍升計畫」，已開始全面 AI 化，並整合現有各項系統、連結部會的資料庫，建置「AI 決策支援系統」，該系統主要運用巨量計算分析，將所有監視系統（含車辨系統）、影像及治安數據的資料庫工具整合，從最基層的執勤端末到重大刑案的偵辦都在 AI 支援輔助下，即時提供所有執法上、勤務上或案件偵破上最關鍵的資訊（料），減少資料檢索分析與人力成本的消耗，並極大化增強案件處理能力與刑案偵查的效率，完全不同於傳統警務運作模式[62]。

有關預測性警務（predictive policing）係利用數據分析和運算法來預測犯罪地點或個人犯罪風險的技術，透過分析歷史治安數據，預測潛在犯罪者（被害者）、犯罪熱點及行為，有效部署警力，更有

[60] 高大宇，〈評析智慧警務的前瞻執法應用〉，《執法新知論衡》，第 16 卷第 1 期，109 年 6 月，頁 78。

[61] 林子倫，〈AI 提升公共治理能力-培養特定領域非資訊人員的 AI 素養〉，《科技與人力教育季刊》，第 11 卷，第 2 期，113 年 12 月，頁 5。

[62] 許城銘、黃宗仁、高哲翰，〈警察人員強制力運用策略初探〉，《臺灣警察專科學校警專學報》，第 7 卷第 4 期，109 年 12 月，頁 83。

效率維持社會治安秩序[63]。運用 AI 演算法與大數據分析，預測高風險之犯罪時間、地點及潛在對象，進而引導巡邏路線規劃與警力資源配置。此類技術常與情報主導警政模式結合，形成以數據驅動為核心之決策架構，提升資源運用之精准性與效率[64]。有關預防犯罪，警察勤務條例第11條第2款規定：「警察勤務方式如下：……二、巡邏：劃分巡邏區（線），由服勤人員循指定區（線）巡視，以查察奸宄，防止危害為主；並執行檢查、取締、盤詰及其他一般警察勤務。」、刑事訴訟法第88條之1第1項第3款前段規定「有事實足認為犯罪嫌疑重大，經被盤查而逃逸者。」，亦即必須符合盤查執行前的犯罪之虞預測[65]。再者處理毒品成癮者、性侵害犯罪者等潛在高風險者，需有個人資料的法律依據，以滿足合法性要件的主張。

然預測性警務，查司法院釋字第535號解釋曾針對警察勤務條例中「臨檢」之規範做出該條例兼具組織法與行為法性質，但並未授權警察得任意或隨機實施臨檢與盤查認定。預測性警務往往奠基於「統計機率」或「群體特徵」，若僅因演算法指出某地為熱點或某人具高風險即進行盤查，極易落入「無合理懷疑之恣意盤查」窘境。復依司法院釋字第689號解釋指出：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、探聽或公開揭露之私人活動領域及個人資料自主，而受憲法第22條隱私權之保障。論者認[66]，在

[63] 鄭勝天，〈淺論人工智慧與預測性警政發展〉，《中央警察大學警察行政管理學報》，第 21 期，114 年 5 月，頁 89。

[64] 洪文玲、黃富源，〈探討人工智慧在偏遠地區警察勤務應用之挑戰與接受度——以科技接受模式（TAM）為例〉，《臺灣期刊法律警專學報》，第 8:6 期，114 年 12 月，頁 5。

[65] 警察職權行使法第 11 條規定：「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動：一、有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。二、有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。前項之期間每次不得逾一年，如有必要得延長之，並以一次為限。已無蒐集必要者，應即停止之。依第一項蒐集之資料，於達成目的後，除為調查犯罪行為，而有保存之必要者外，應即銷毀之。」

[66] 孟維德，〈智慧警政的意涵、架構與標準〉，《外執法與政策學報》，第 15 期，114 年 5 月，頁 89。

實施一項新式智慧刑事司法措施或相關應用程式之前，有必要先處理好該項創新方案的法律基礎和完整合法性。例如，我國警察機關先前曾使用M化偵查網路行動電話定位系統，調查詐欺嫌犯的手機發話處及定位詐騙集團機房，進而搜索並逮捕犯罪嫌疑人，移送檢察機關起訴後，法院判決警察機關使用M化車是干預人民基本權的處分，違反法律保留原則。後於113年7月16日，立法院三讀通過刑事訴訟法修正案，增訂「特殊強制處分」，規範為調查犯罪情形或蒐集證據認有必要時，得使用全球衛星定位系統等科技方法追蹤被告或犯罪嫌疑人位置，警察機關的科技偵查行為得以正當化。

綜上，歐盟AI法，針對個人的預測性警務已被列入「不可接受的風險」的禁止項目[67]（非完全禁止但有嚴格限制，例如預防真實存在或可預見的威脅以及搜捕涉嫌犯有最嚴重罪行的人員等情形）。惟個人犯罪風險評估或預測，若無限使用預測性演算法將淡化刑事法上既有的各種犯罪嫌疑標準，例如：合理懷疑標準，相當理由等。長久以往，若過度依賴算法模型，在數據、模型任一者出錯都可能產生嚴重且長久的影響[68]。爰此，建立預測性警務犯罪防制，允宜遵守法律保留原則，並在防止犯罪與個人不受侵擾自由間進行權衡。

---

[67] 歐盟AI法第5條規定：「僅依據剖析或人格特質來預測某人未來是否會實施刑事犯罪的 AI系統遭到全面禁止。」、Law enforcement exceptions，Moreover, as regards the use of real-time remote biometric identification systems in publicly accessible spaces, the provisional agreement clarifies the objectives where such use is strictly necessary for law enforcement purposes and for which law enforcement authorities should therefore be exceptionally allowed to use such systems. The compromise agreement provides for additional safeguards and limits these exceptions to cases of victims of certain crimes, prevention of genuine, present, or foreseeable threats, such as terrorist attacks, and searches for people suspected of the most serious crimes.，Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world，網址：https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/，最後瀏覽日期：115年10月12日。

[68] 王正嘉，〈預測性警察活動在犯罪偵防運用與問題〉，《刑事政策與犯罪防治研究專刊》，第25期，109年8月，頁42。

伍、結論

自人工智慧基本法制定以降，凡事涉為建設智慧國家，促進以人為本之 AI 研發與 AI 產業發展，建構 AI 安全應用環境，落實數位平權，保障人民基本權利，增進社會福祉，提升國人生活品質，促進社會國家之永續發展，維護國家文化價值及提升國際競爭力，並確保技術應用符合社會倫理，皆須依據人工智慧基本法之規定辦理。世界各地的城市都在其政府和民間活動中實施 AI 解決方案，以改善公共安全並減少犯罪，然 AI 在供犯罪防制領域也面臨挑戰。爰參考美國及歐盟等先進國家相關法制，針對上開爭議問題研提相關建議如下，俾供委員問政參考：

一、AI 促成恐怖組織進化，建議警察法刪除未符時宜之任務界限。

二、檢討人臉辨識設立人為介入審查機制，避免歧視或偏見情事。

三、生物特徵識別指紋自動查驗通關，應以法律明定錄存目的。

四、強化無人載具應用行為，研議訂定適當防範措施與倫理權衡。

五、明確區分 AI 風險分類框架，強化隱私數據保護之必要性。

六、建立預測性警務犯罪防制，允宜遵守法律保留原則。

參考文獻

一、政府出版品

1、立法院第 11 屆第 4 會期第 2 次會議議案關係文書，院總第 20 號，政府提案第 11015829 號，114 年 9 月 24 日印發。

2、交通部運輸研究所編印，《國際推動機場智慧化趨勢及我國發展課題探討》，113 年 2 月。

3、數位發展部編印，《人工智慧風險分類框架》，115 年 7 月。

4、鄭文亭，《新北市政 110 年度自行研究報告，臉部辨識與個資保護之探討》，新北市政府地政局地政資料科，110 年 10 月。

三、期刊論文

1、于子揆，〈人工智慧於軍事應用之發展與管制：國際趨勢與我國政策建議〉，《國會季刊》，第 53 卷第 4 期，114 年 12 月，頁 82-114。

2、王正嘉，〈預測性警察活動在犯罪偵防運用與問題〉，《刑事政策與犯罪防治研究專刊》，第 25 期，109 年 8 月，頁 1-47。

3、林輝煌，〈我國人工智慧基本法之制度性侷限與法治落實之道—從刑事程序、行政法與憲法審查觀點出發〉，《最高檢察署月刊》，第 41 期，115 年 1 月，頁 3-10。

4、林子倫，〈AI 提升公共治理能力-培養特定領域非資訊人員的 AI 素養〉，《科技與人力教育季刊》，第 11 卷，第 2 期，113 年 12 月，頁 7-23。

5、巫穎翰，〈致命自主武器系統規範爭議的探討與展望〉，《安全與情報研究》，第 9 卷第 2 期，115 年 7 月，頁 83-152。

6、洪澤顥、周傑泰，〈運用 SWOT 分析探討導入無人機空軍軍機維保作業調整策略〉，《空軍學術雙月刊》，第 707 期，114 年 8 月，頁 118-142。

7、洪文玲、黃富源，〈探討人工智慧在偏遠地區警察勤務應用之挑戰與接受度—以科技接受模式（TAM）為例〉，《臺灣期刊法律警專學報》，第 8:6 期，114 年 12 月，頁 1-27。

8、高大宇，〈評析智慧警務的前瞻執法應用〉，《執法新知論衡》，第 16 卷第 1 期，109 年 6 月，頁 75-88。

9、吳瑛珠，〈運用人工智慧進行預測性警務的人為干預要求－以歐盟與德國法制為例〉，《中央警察大學法學論集》，第 50 期，115 年 4 月，頁 241-311。

10、達文西個資暨高科技法律事務所，《歐盟、英國及加拿大對警察機關或執法機關運用人臉辨識技術之指引或其他相關文獻探討(計畫編號：NDC0111019)》，國家發展委員會 111 年度委託研究計畫，111 年 10 月。

11、孟維德，〈智慧警政的意涵、架構與標準〉，《外執法與政策學報》，第 15 期，114 年 5 月，頁 55-76。

12、趙萃文，〈科技創新下的法律挑戰－以人工智慧為中心〉，《軍法專刊》，第 70 卷第 2 期，113 年 5 月，頁 91-128。

13、潘俊良，〈公部門人工智慧應用之風險評估與內控治理—以歐盟人工智慧法及相關 ISO 國際標準為借鏡之法制建構〉，《科技法律透析》，第 38 卷第 2 期，115 年 7 月，頁 111-130。

14、范姜真媺，〈大數據時代下個人資料範圍之再檢討—以日本為借鏡〉，《東吳法律學報》，第 29 卷第 2 期，106 年 10 月，頁 1-

38。

15、張麗卿，〈AI 基本法下高風險智慧醫療之治理〉，《當代法律》，第 54 期，115 年 6 月，頁 106-112。

16、許城銘、黃宗仁、高哲翰，〈警察人員強制力運用策略初探〉，《臺灣警察專科學校警專學報》，第 7 卷第 4 期，109 年 12 月，頁 65-86。

17、郭承諭、蔡震榮，〈國土安全與反恐〉，《中央警察大學國土安全與國境管理學報》，第 40 期，112 年 12 月，頁 1-46。

18、鄭勝天，〈淺論人工智慧與預測性警政發展〉，《中央警察大學警察行政管理學報》，第 21 期，114 年 5 月，頁 85-94。

四、網路資源

1、Artificial Intelligence Act，網址：https://artificialintelligenceact.eu/the-act/，最後瀏覽日期：115 年 10 月 12 日。

2、Artificial Intelligence Bill of Rights，2022 年 10 月。網址：https://www.managementsolutions.com/en/publications-and-events/regulatory-notes/technical-notes-oregulations/blueprint-artificial-intelligence-ai-bill-rights，最後瀏覽日期：115 年 10 月 29 日。

3、President Donald J.Trump Unveils National AILegislative Framework，2026 年 3 月 20 日。網址：https://www.whitehouse.gov/releases/2026/03/president-donald-j-trump-unveils-national-ai-legislative-framework/i，最後瀏覽日期：115 年 10 月 12 日。

4、The State of Play and WayForward in Core Government Functions，2025 年 9 月 18 日。網址：https://www.oecd.org/en/publications/governing-with-artificial-intee142-en.html，最後瀏覽日期：115 年 10 月 5 日。
5、林宗德，機器人倫理學專題報導（一）：無人機的警示，，科技大觀園，網址：https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=6f786f6b-e4ab-4e2e-918c-3aa3d70d1254，最後瀏覽日期：115 年 10 月 12 日。
6、林玉書，數位創新實驗法規沙盒制度研析，資訊工業策進會科技法律研究所，112 年 1 月 17 日，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8966，最後瀏覽日期：115 年 10 月 7 日。
7、許鈺淇，財團法人民間司法改革基金會（2025），座談側記-虛擬資產犯罪實務解析之司法實務的挑戰篇，網址：https://www.jrf.org.tw/articles/2500，最後瀏覽日期：115 年 10 月 7 日。

附錄：「人工智慧犯罪防制之相關法制問題研究」專題研究報告（初稿） 座談會紀錄及參採情形

時間：115 年 11 月 6 日（星期五）上午 9 時 30 分

地點：立法院法制局 305 會議室

主席：莊組長弘仔　　紀錄：林智勝

參加人員：

一、學者專家

銘傳大學法律學系　　趙助理教授萃文

二、內政部刑事警察局

科技犯罪防制中心技正　郭有志

三、數位發展部

數位政府司高級分析師　官長治

數位策略司科長　　林姝宜

四、本局出席人員

林研究員鈺琪

陳副研究員育靖

黃副研究員姵瑜

發言要點：

銘傳大學法律學系趙助理教授萃文：

一、本報告就人工智慧相關應用與規定、司法院解釋與相關函釋及警

察執法實務予以研究，值得肯認。目前 AI 已被允許使用，但責任制度卻仍停留在人類操作工具時代。機器生成之意思表示是否為「人之意思」，同時對應出「誰」是表意人的問題，即機器得否作為人的意思表示的主體，亦即 AI 是否具有法人格的法制課題，值得深思。如本報告題目人工智慧犯罪防制，面對犯罪手法升級，若未能建立清楚的責任規則，讓所有參與者明白責任無法轉嫁，風險只會持續向下游移動，最終落在最無力自保的一方。本報告所敘行政單位除執法機關重視外，司法院亦撰有人工智慧系統參考指引，建議撰稿者可再予以補充說明納入補充。當 AI 被部署於金融、醫療、公共服務與自動駕駛等高風險場景，責任不能僅落在最末端使用者身上；行政及立法部門均有責任要求平臺揭露風險、建立補償機制，確實即時修法之必要，避免法制滯後責任缺位。

二、有關本報告建議警察法刪除未符時宜之任務界限。不可否認我國現行相關 AI 法制有明顯缺口，資通安全管理法主要規範政府與關鍵基礎設施，對危害國家資通安全的產品，雖禁止公務機關使用特定中國大陸地區的資通產品，但難以處理民間大規模使用問題。個人資料保護法第 21 條雖可作為跨境限制工具，但其屬個案審查，門檻高且程序繁複，難以應對大規模、持續性之資料流動。在國外立法例方面歐美等國透過嚴格的刑事訴訟專章或特別法，明確規定，例如適用罪名限制（限最輕本刑 3 年以上之重罪）、法官保留原則（使用衛星長期追蹤或即時生物特徵辨識須事前聲請法官核發令狀）、資料銷毀與監督機制（未涉案民眾之生物特徵須立即刪除，並受獨立機關監督）。未來若能透過專法或修正刑事訴訟法及警察職權行使法，解決法院審理時的證據能力質疑，透過強制性法律規範，結合事前預防、事後究責措施，確

保 AI 技術在負責任的監管下成長，形成以科技發展及應用為取向的法秩序，方為正辦。

三、本報告提及明確區分 AI 風險分類框架，強化隱私數據保護之必要性，惟資訊隱私權即個人資料控制權，個人資料保護法第 41 條及第 42 條規範定有主觀意圖，足生損害等規定，並不是只要屬於隱私侵害，即有以刑罰加以處罰之正當性。[69]。AI 的快速發展，遠遠超越法規之制定速度，AI 概念的理解與界定大抵源自科技知識，進入法秩序領域，一時難有全面且周全的定義。導致法條解釋出現模糊空間，引發制度規範和法源適用疑慮；不僅呈現科技正當法律程序與人權保障的衝突，亦迫使傳統規範在面對科技治理時，面臨責任歸屬與風險分級之挑戰。如市場機能在私法自治原則下，對國家社會產生過度不利之影響時，利用立法管制與介入，乃現代國家常用的工具。然而，在使用刑罰管制工具時，不能僅自行政管制的角度予以思維，必須符合刑事法理，才有可能通過憲法比例原則之檢驗，亦即本報告所列舉之司法院解釋的核心初衷。

四、本報告有關建立預測性警務犯罪防制，允宜遵守法律保留原則。要預防人工智慧系統的未知風險，法律有必要根據其不同適用領域調整管制方式。為避免過度箝制人工智慧的科技創新，刑法抽象危險犯作為人工智慧系統的風險管制手段，不能一體適用於 AI

[69] 按不法意識係自然心理主義下的故意概念，本質上涉及普遍性的問題，網路平臺上個人的意思活動，其心理認知程序不會特別注意及存在於客觀環境的行為訊息，如散布猥褻物品罪，行為人於欠缺主觀網路平臺觀覽或轉傳時，是否有能力意識到自身的行為是法所禁止的？若行為人欠缺這種認識狀態者，毋寧形同欠缺了行為的不法意思與刑罰的罪責，難以證立不法行為與罪責非難的一般性要件。刑法中之罪刑法定原則及明確性原則，強調刑事責任之歸責必須基於法律明確的規定，亦即法律構成要件必須清晰明確，讓人民能預測何種行為會構成犯罪；刑法處罰的是客觀的「作為」或「不作為」，而非對個人為心理威嚇、道德約制，甚或是虛擬的「危害可能性」。由於近代刑法的保護法益趨向抽象化與空洞化，不排除行為人有可能是根本未意識到相關規範的存在，或者根本不知行為將對他人造成何種不利益？在此情形下，有必要例外肯認行為人於行為時欠缺所謂的「不法故意」。

的所有適用領域，必須恪守刑法謙抑性，只能點狀地保留給攸關重大生命安全，且風險明確的高風 AI 領域；其餘領域則應交由行政法與市場自律，才能在風險控制與科技創新間取得動態平衡。爰此，引入集體法益領域興起的風險犯，或係必然趨勢。將製造或銷售致命自主武器系統（LAWS）納入刑法處罰，針對製造或使用高風險 AI 系統的行為，設定抽象危險犯的構成要件，不問是否導致法益受侵害，將刑事責任之焦點從後端的「損害結果歸責」，前移至前端的「風險管理義務與法規合規」，毋寧是平衡刑事過失責任與無過失責任之間，用以兼顧科技創新與法律保障的適合手段。這不僅守住了刑法不輕易走向無過失責任的底線，也為受害者提供了前置的制度保障，是當前科技刑法最理想的立法技術，後續值得繼續深入研究。

參採情形：

一、第一點意見，有關司法院人工智慧系統參考指引，已參採補充於報告本文（見頁 12，註 29）。另提及 AI 技術演進速度遠快於法律體制，避免法制滯後責任缺位……，責任不能僅落在最末端使用者身上；行政及立法部門均有責任要求平臺揭露風險、建立補償機制……等，屬立法政策建議，錄供主管機關參考。

二、第二點及第三點意見，與本報告建議方向尚無扞格之處，錄供參考。

三、第四點意見，有關恪守刑法謙抑性，將刑事責任之焦點從後端的「損害結果歸責」，前移至前端的「風險管理義務與法規合規」之科技刑法理想的立法技術建議，錄供主管機關於未來研擬相關法案時併予斟酌參考。

內政部刑事警察局科技犯罪防制中心郭技正有志：

一、有關報告「AI 促成恐怖組織進化，建議警察法刪除未符時宜之任務界限」，本部意見：

（一）針對「因應 AI 促成犯罪進化，研修警察法，刪除未符時宜之警察業務，並檢討修正警察有關 AI 事權之分配」一節，依 92 年 12 月 26 日司法院釋字第 570 號解釋理由書說明，警察法第 9 條關於警察職權之規定，「僅具組織法之劃定職權與管轄事務之性質，欠缺行為法之功能，不足以作為限制人民自由及權利之授權依據」。是以，警察人員針對新興 AI 辨識人類面部與虹膜、運用衛星偵蒐能力強化全天候聯合情監偵能力等，在警察法增訂運用 AI 輔助偵查事權，第一線偵查人員使用時仍缺乏行為法依據，在法院審理時將面臨證據能力的質疑。

（二）檢視當前科技偵查的授權已在刑事訴訟法有明確的立法方向。過去警察使用 M 化車定位詐團機房，法院認定違反法律保留原則。爰在 113 年刑事訴訟法增訂第十一章之一「特殊強制處分」，依干預程度分層規範：如 GPS 追蹤在 24 小時內可由偵查人員自行實施，逾時須法院許可；調查手機位置及門號一律須法院許可；以熱顯像儀等科技方法監看私密空間，限最重本刑 5 年以上之罪並經法院許可。遂 AI 等新興科技偵查工具可以延續「依侵害程度設門檻、法官事前審查」架構，在刑事訴訟法特殊強制處分專章中檢討增訂為宜。

（三）惟警察法第 5 條、第 9 條第 7 款所列保安、正俗、衛生、消防、戶口查察等事項，確實已改由專責機關掌理，且關於警察任務及職權等規定，亦應釐清警察與其他行政機關間防止危害任務之界限及職務協助關係，遂本部贊同警察法確實應全面通盤檢討修正。

二、有關報告「建立預測性警務犯罪防制，允宜遵守法律保留原則」意見：警察機關運用數據分析或演算法預測犯罪地點或個人犯罪風險，據以部署警力或發動偵查作為，本部認同應遵循法律保留原則。AI 演算法分析結果僅得作為參考線索，實際採取盤查、搜索等干預措施時，仍應由執法人員依合理懷疑、相當理由等既有標準進行人為判斷，以兼顧犯罪偵防效能與人民基本權利之保障。

參採情形：

一、第一點意見（一），有關第一線偵查人員使用時仍缺乏行為法依據，參趙助理教授萃文發言要點二，外國立法例方面，歐美等國透過嚴格的刑事訴訟專章或特別法，明確規定。另憲法法庭（如 111 年憲判字第 16 號判決，涉及強制採尿等科技取證，以及近年對 GPS 追蹤器、M 化車之實務爭議）一再重申，凡屬侵害基本權的強制處分，必須遵守「強制處分法定原則」與「法律保留原則」。明定具體的發動門檻、令狀審查機制與救濟途徑，透過專法或配套修正我國刑事訴訟法及警察職權行使法，結合事前預防、事後究責措施，確保 AI 技術在負責任的監管下成長，形成以科技發展及應用為取向的法秩序，方為正辦。

二、第一點意見（二），參趙助理教授萃文發言要點三，使用刑罰管制工具時，不能僅自行政管制的角度予以思維，必須符合刑事法理，才有可能通過憲法比例原則之檢驗。

三、第一點意見（三），主管機關表示目前正朝本報告所建議之方向，贊同警察法確實應全面通盤檢討修正。

四、第二點意見，係認同本報告有關建立預測性警務犯罪防制，允宜遵守法律保留原則，錄供參考。

數位發展部數位政府司官高級分析師長治：

一、報告第 4 頁引用戰略委員會議決議，提到本部協助各級政府完成風險評估並建立內控。本部目前確實已依人工智慧基本法第 19 條規定，發布共通的「政府 AI 應用風險評估檢核表」、辦理說明會與諮詢，並研擬了機關內控管理要點範本，供各機關參照調修。惟基本法第 19 條所定風險評估與內控機制的「義務主體」，是使用 AI 的各機關本身。本部的角色是提供通用的治理框架、評估工具與必要協助；至於各項 AI 應用的風險評估結果與內控要點的實質訂定，仍應由各使用機關依其業務性質與實際情境來做專業判斷。

二、報告第 13 頁針對人臉辨識準確性不足恐導致歧視與偏見的疑慮，亦符合基本法第 4 條「人類自主」與「公平不歧視」的原則。警政等機關使用人臉辨識執法，屬於第 19 條使用 AI 執行業務的情形，應落實風險評估與內控管理。報告建議的人為介入審查機制，實務上就可以直接訂定在機關內部的內控要點中。本部修訂中的內控要點範本，針對涉及生物特徵辨識、可能影響人民權益的高風險應用，已明確要求在資料整備期與訓練開發期評估機敏資料防護與模型選用妥適性，並在部署維運階段建立人為監督、決策覆核及紀錄留存機制，主管機關訂定人為審查程序時均可直接參考。另外，因人臉辨識涉及個人資料的蒐集、處理與利用，建議本項併請個人資料保護委員會籌備處表示專業意見。

三、報告第 19 頁提到「人工智慧基本法第 19 條雖已對公部門使用使 AI 課予風險評估與內控管理機制之法定義務.....。」，這部分建議依本部辦理現況予以調整。本部已依第 19 條提供共通的風險評估檢核表，並研擬內控要點範本，依生命週期各階段訂定管

控要求，並融入歐盟 AI 法、美國 NIST 框架及 ISO/IEC 42001 等國際規範，共通工具均已齊備，各機關正依其業務性質訂定執行程序。至於報告建議將 AI 風險嵌入行政院及所屬各機關風險管理及危機處理作業手冊，這與本部範本的設計理念一致，範本本來就是以能銜接機關既有內部控制與風險管理程序為原則。該作業手冊的修訂權責雖屬行政院及國發會職掌，本部很樂意提供 AI 風險態樣與檢核項目供其參考；報告所引歐盟 AI 法的人為監督、紀錄保存與透明度等義務，也均已納入本部範本之中。

參採情形：

一、第一點意見，主管機關說明「政府 AI 應用風險評估檢核表」，業已提供各機關參照調修。至於各項 AI 應用的風險評估結果與內控要點的實質訂定，仍應由各使用機關依其業務性質與實際情境來做專業判斷，錄供參考。

二、第二點意見，係數位發展部表示因人臉辨識涉及個人資料的蒐集、處理與利用，建請個人資料保護委員會籌備處表示專業意見，錄供主管機關參考。

三、第三點意見，數位發展部強調依據人工智慧基本法，已經完成「風險評估檢核表」與「內控要點範本」。另有關將 AI 風險嵌入行政院及所屬各機關風險管理及危機處理作業手冊，可配合提供 AI 風險態樣與檢核項目供主管機關參考。

數位發展部數位策略司林科長姝宜：

一、報告第 3 頁「相關風險分類框架，係依據人工智慧基本法第 16 條所訂定，作為政府跨部會溝通及產業界和社會大眾理解 AI 風險治理體系之參考」，似可微調為「風險分類框架係依據人工智

慧基本法第 16 條所訂定，作為各目的事業主管機關訂定以風險為基礎之管理規範。」與人工智慧基本法呼應。另報告第 11 頁至第 12 頁「配合人工智慧基本法 2 年內的通盤法規檢討期，建議研修警察法……並檢討修正警察有關 AI 事權之分配。」報告所提相關法規之檢討，另可參考「AI 風險分類框架」之流程。

二、報告第 19 頁「高風險 AI 係由『中央目的事業主管機關會商數位發展部』加以認定。」及第 21 頁「目前針對 AI 的治理，皆普遍採用『風險導向』，要藉由 AI 風險分類框架來強化隱私數據保護。」建議敘明納入相關條文規定與文字修正，以為明確。

參採情形：

一、第一點意見前段部分，已參採修正（見頁 3）；後段提及「AI 風險分類框架」之流程，已將相關引註資訊，補充於報告本文（見頁 12，註 31）。

二、第二點意見，有關「風險導向」，要藉由 AI 風險分類框架來強化隱私數據保護之條文與「風險導向」之建議文字修正，均已參採修正（見頁 19、頁 21）。

林研究員鈺琪：

一、AI 技術的快速發展，在簡化行政流程、帶來便利的同時，也無形中降低了犯罪的技術門檻，衍生新的犯罪及資安風險。例如，犯罪者利用生成式 AI 協助編寫惡意程式、自動生成釣魚郵件；或是利用深度偽造(Deepfake) 技術從事詐欺、身分冒用及合成非自願私密影像等不法行為。此類發展不僅改變傳統犯罪手段，也增加犯罪偵查及防制工作的複雜性，實值思考如何適當運用 AI 技術，提升犯罪防制效能，並兼顧人民基本權利之保障。

二、日本東京地方法院於 2024 年 10 月 25 日，針對一起利用生成式 AI 製作勒索軟體之案件作成有罪判決。該案被告透過非官方版本的 ChatGPT 等生成式 AI 工具，成功寫出具有檔案加密、勒索贖金功能的惡意程式，最終被依「製造不正指令電磁紀錄」等罪名，判處有期徒刑 3 年、緩刑 4 年。審理過程中被告供稱，若無生成式 AI 協助，可能無法自行完成該程式[70]。此案例顯示，生成式 AI 可能降低特定犯罪行為所需的技術門檻，使欠缺專業資訊技術的普通人，亦有能力製作惡意程式，凸顯新興科技對犯罪偵查及防制工作所帶來的挑戰。

三、美國近年逐步透過立法因應 AI 遭不法利用所衍生之問題。例如：2025 年制定之「刪除法案」(TAKE IT DOWN Act)，針對未經同意散布私密影像及 AI 生成之偽造私密影像，明文規定刑事責任及網路平台通知移除機制；另有旨在保障個人聲音與視覺形象免遭經授權之數位複製的「禁止造假法案」(NO FAKES Act)立法提案。此外，2026 年提出之「阻嚇美國 AI 模型竊取法案」(Deterring American AI Model Theft Act, DAAMTA)及「AI 終止開關法案」(AI Kill Switch Act)，分別防範境外勢力非法竊取核心 AI 模型技術，並強制要求高風險 AI 系統必須具備安全中斷機制。前揭發展或可作為未來觀察 AI 安全管理、犯罪防制及相關法律責任制度之補充參考。

參採情形：

一、第一點及第二點意見，贊同本報告建議方向，錄供參考。

---

[70] 一宮俊介，生成AIでランサムウェア作成　男性に執行猶予付き懲役3年の判決　東京地裁，弁護士ドットコムニュース，2024 年 10 月 25 日，網址：https://www.bengo4.com/c_18/n_18066/?utm_source=chatgpt.com，最後瀏覽日期：115 年 11 月 5 日。

二、第三點意見，查美國刪除法案，其網路平台通知移除機制已於2026年5月正式全面生效並由聯邦貿易委員會（FTC）執法。禁止造假法案、阻嚇美國AI模型竊取法案，截至目前均為美國國會審議中的立法提案，尚未通過，錄供主管機關參考。

陳副研究員育靖：

一、報告第1頁前言並未列出犯罪防制想要探討的面向，而報告第3頁梳理之我國犯罪防制相關法律，係以涉及「恐怖活動」、「恐怖組織」之法律規定為主，惟報告包括外國立法例及問題研析與建議等整體論述，主要偏向AI之風險層級與隱私權保護，對於「恐怖活動」、「恐怖組織」之犯罪防制觸及反而較少，因犯罪防制之面向甚廣，建議釐清本報告探討之主軸。

二、報告第5頁至第7頁有關歐盟人工智慧法部分，「不可接受的風險」第9項「未成年或兒童性虐待影像的散播」似乎不在歐盟該法規定之風險態樣；又第7頁有關罰則部分，引用資料似並非現行規定，建議再確認。

三、報告第8頁至第9頁有關美國NIST於2023年發布之AI風險管理框架部分，列出七大核心目標與建議方向，惟前6項似是川普總統2026年提出的國家AI立法框架，亦即第8頁註22之參考資料，請再確認。

參採情形：

一、第一點意見，已參採修正並列出進行犯罪預防時，所衍生的基本權侵害與風險控管方向，及點出聚焦於AI科技應用於「犯罪偵查與預防」時，在提升執法效率與保障基本人權（特別是隱私權與個資保護）間之衡平（見頁1，前言）。由於反恐與重大犯罪防

制往往涉及大規模監控與生物特徵辨識，爰特別針對外國法制中之「AI 風險層級」與「隱私權保護」進行深入研析，以作為我國執法界線之參考。

二、第二點意見，已參採修正（見頁 6 及頁 7）。

三、第三點意見，已刪除 2023 年 NIST 之風險管理框架舊有資料，參採修正為 2026 年美國國家 AI 立法框架完整七大核心方向（見頁 8）。

黃副研究員姵瑜：

一、本報告就 AI 於犯罪防制之運用，針對警察職權、人臉辨識、生物特徵資料錄存、無人載具及預測性警務等議題，分別自法律保留、個人資料保護、人為審查及風險管理等面向進行研析，並參考歐盟及美國相關法制，對於釐清 AI 執法之運用界限及人民基本權利保障，具有參考價值。

二、本報告針對人臉辨識之誤判風險，建議設立人為介入審查機制；並就臺灣地區有戶籍國民於自動查驗通關時自願錄存指紋部分，建議以法律明定其錄存目的，實有助於兼顧科技執法效能與資訊隱私權保障，值得主管機關參採。另有關預測性警務仍應遵守法律保留原則之建議，亦有助於避免過度依賴演算法結果，影響人民不受恣意干預之自由。

三、本報告第 7 頁所載歐盟 AI 法罰則部分（含原註 19），仍為 2021 年執委會提案第 71 條第 3 項及第 4 項之內容。查 2024 年 7 月 12 日公布之歐盟 AI 法（Regulation (EU) 2024/1689）第 99 條第 3 項，似已將違反第 5 條禁止行為之行政罰鍰上限定為 3,500 萬歐元；違反者為企業時，則為該金額或前一會計年度全球年營

業額之 7%，原則上以較高者為準，中小企業（包括新創企業）則依同條第 6 項以較低者為準。另同條第 4 項所列其他義務之違反，其罰鍰上限亦已調整為 1,500 萬歐元或企業前一會計年度全球年營業額之 3%，敬請參酌。

參採情形：

一、第一點至第二點意見，贊同本報告建議方向，錄供參考。

二、第三點意見，已參採修正。

散會： 上午 10 時 10 分