最高檢察署
Supreme Prosecutors Office

2026
1月 月刊
E-paper

20220921創刊（歡迎公益推廣）
ISSN：2958-0315
EISSN：2958-0323
GPN：2011100016

No. 41
2026年1月第41期
最高檢察署全球資訊網
https://www.tps.moj.gov.tw/
發行：最高檢察署／編輯：蔡偉玉、柳瑞宗

➢ 檢察機關強化系統性偵辦，遏止劣質防彈背心流入市面
函請相關機關依法核實管制風險，確保社會與國家安全

一、多年來軍警用防彈背心採購涉弊案件一再發生，計畫性的犯罪手法，有集團化、組織化、綁標化傾向，嚴重影響軍、警人身安全及國家安全

多年來不肖業者介入軍警用防彈背心之政府採購案，交付不符合採購案規格或安全性要求之防彈背心或相關產品(如：吸震片、抗彈纖維布)予國防部、法務部調查局、矯正署及警政署等採購機關，嚴重影響第一線軍、警、矯正機關執勤同仁之人身安全與國家安全。

最高檢察署蒐集相關資料，爬梳、分析是類案件，發現：弊案範圍遍及全國各機關；被告利用案件偵審程序及採購法刊登公報前之空窗期，投機違法舞弊，甚至彼此合作，圍標後再分潤之犯罪手法；有集團化、組織化、綁標化傾向。

二、檢察機關強化系統性偵辦，最高檢察署邀集高雄高分檢、臺北地檢、桃園地檢及橋頭地檢共同協力辦理防彈背心採購案，避免因檢察署各自偵辦，讓犯罪組織利用程序間漏洞，趁機牟取暴利

最高檢察署邀集高雄高分檢、臺北地檢、桃園地檢、橋頭地檢等偵辦此類案件之檢察署召開「偵辦軍警用防彈背心採購案策進會議」，各檢察署就具體個案中被告之犯案手法、主要答辯及法院量刑妥適性等面向充分交流意見，並將強化系統性偵辦，避免因案源、偵辦單位與移送時間不同，致各檢察署分別偵查，因偵查步驟不一及資訊盲點，致衍生集團性、組織性犯罪，對國家安全造成嚴重危害。

★會中就檢察機關偵辦是類案件作出決議：

（一）偵查中案件，情節嚴重者，應從速從嚴偵辦，查扣不法所得，必要時應對被告進行科技設備監控。

（二）審理中案件，如個案情節重大者，應從重具體求刑。

（三）判決確定案件，應儘速執行。

（四）個案應審核有無國家安全法第 11、12 條(違法履約交付或提供陸製軍品罪)之適用。

另就不同檢察署之個案，如被告涉及多起案件，將由地檢署對一再涉案之特定被告進行科技設備監控，避免被告逃匿影響後續偵、審或執行程序。

三、各檢察機關依前述決議，已分別做出具體處置，有效防止不肖之徒利用程序間漏洞，趁機犯罪牟取暴利

（一）高雄高分檢

被告楊○勛、李○勳 2 人　共犯案件，未扣案之不法所得高　達新臺

幣 1 億 3 千餘萬元，一審對被告 2 人分別判決 5 年 6 月、2 年且未宣告併科罰金，量刑過輕，該案現於高雄高分院審理中，請高雄高分檢向法院具體從重求刑。

（二）臺北地檢

1. 被告林O哲偵查中案件，請承辦檢察官從速從嚴偵辦，並查扣不法所得；林O哲因同類案件，前經法院判決有罪確定並宣告緩刑，如後案再經判決有罪確定，請執行科檢察官對前案聲請撤銷緩刑。
2. 被告李O勳因同類案件，前經法院判決有罪確定並宣告緩刑，如後案再經判決有罪確定，請執行科檢察官對前案聲請撤銷緩刑。

（三）桃園地檢

被告楊O勛、李O勳 2 人偵查中案件，請承辦檢察官從速從嚴偵辦，並查扣不法所得；鑒於被告楊O勛逃匿目前遭通緝，已於會議中請高雄高分檢提供相關資料，由桃園地檢對李O勳完成適當之科技設備監控。

（四）橋頭地檢

1. 被告李O勳將「未得標之戰鬥背心內蕊」轉賣得利案件，一審判決有期徒刑 6 月量刑過輕，橋頭地檢已依會議決議，提起上訴，請法院從重量刑。
2. 被告楊O勛前已判決確定應執行 5 年 6 月之案件，因被告逃匿目前遭通緝，已請橋頭地檢儘速督導所屬將被告緝捕歸案執行。

四、最高檢察署業已函請國防相關單位進行系統性之風險管理預防，辦理國家安全法第 11 條之採購案時，招標文件應載明「本採購案應依國家安全法管制」，一經載明，如有違反，依國家安全法，最重可處 10 年有期徒刑，確保國防軍品設施及提供服務之安全

112 年 12 月 1 日施行之國家安全法第 11、12 條(違法履約交付或提供陸製軍品罪)，明定「對用於軍事工程、財物或勞務採購之產製品或服務，知悉原產地、國籍或登記地係來自大陸地區、香港、澳門或境外敵對勢力」及「知悉係不實之軍用武器、彈藥、作戰物資」，而為交付或提供之違法履約交付或提供陸製軍品行為之刑責，違者最重可處 10 年有期徒刑，併科新臺幣 5 千萬元罰金。

五、最高檢察署並呼籲：國防單位以外之司法、行政機關，例如調查局、海巡署、警政署、矯正署等，亦應注意避免業者以違反政府採購法或偽造文書之方式，進口大陸、港澳地區或境外敵對勢力之產品，以維護執勤同仁人身安全。

【扣案之劣質品戰鬥背心】

➢ 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

* 前司法官學院
林輝煌院長

壹、前言

台灣素以先進科技為傲，贏得科技島美名，尤以人工智慧(Artificial Intelligence, 以下簡稱 AI）之高度發展為最。繼許多國家紛紛制定人工智慧法規範[1]，監理人工智慧之持續發展，我國亦不落人後，經由立法院於 2025 年 12 月 23 日三讀通過《人工智慧基本法》，作為回應人工智慧發展風險與治理需求的核心立法選擇。該法共計 17 條，揭示政府推動人工智慧研發與應用應遵循「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」、「問責」等七大原則，明定其立法旨在促進以人為本之人工智慧研發與人工智慧產業發展，建構人工智慧安全應用環境，落實數位平權並保障人民基本權利。綜觀該法內容，宣示確保技術應用符合社會倫理，維護國家文化價值及提升國際競爭力，奠立法制基礎[2]。

此一立法模式在價值宣示與政策整合上誠然具有一定意義，然而，對於科技治理仍屬「新進國家」之我國而言，若僅止於制定《人工智慧基本法》，而未同步建構可操作之專法與既有法制之結構性調整，將使 AI 治理流於象徵性，甚至引發刑事程序失衡、行政裁量失控與憲法審查空洞化之制度風險。

有鑒及此，本文爰以「台灣人工智慧基本法之制度性侷限與法治落實之道」為題，分從刑事訴訟程序、行政法治與憲法審查三個面向，對「僅有 AI 基本法」之治理模式，進行粗淺的制度性檢視評議，進而提出建構三層式法制建議，作為我國實現 AI 法制化與永續治理之可行路徑，期能拋磚引玉，盼有司及有識之士，群策群力，再接再厲，進一步全面深入探討，進而付諸行動，共同實現建構我國完備 AI 法制的理想。

---

* 作者，現任東吳大學講座，曾任法務部政務次長、司法官學院院長。

[1] 截至 2025 年，約有 33 個國家或地區已制定具約束力的 AI 相關法律（含專門法律或系統性規範）。約 90 多個國家有國家 AI 戰略或治理框架（含政策性文件、行動計劃等）。其中較為矚目者殆有： 2024 年通過，自 2024 年 8 月 1 日起開始分階段實施的歐洲聯盟 Artificial Intelligence Act(建立 AI 系統風險分級管理與合規要求，涵蓋高風險系統的義務與透明性規範；禁止不可接受的 AI 用例)；2025 年 9 月實施的日本 Act on Promotion of Research, Development and Utilization of AI-Related Technologies (建立 AI 國家發展框架、策略規劃與跨部會機制，強調技術促進與責任治理並重)；預計 2026 年 1 月起實施的南韓 Basic Act on AI Advancement and Trust (強調安全性、透明性與信任機制)；美國目前仍未有統一的聯邦 AI 專門法律，但有多項行政命令、政策與準則，包括拜登政府的 AI 政策框架與安全指引（Executive Orders & NIST AI Risk Management Framework），但在州方面，則有 Colorado 州的 Consumer Protections for Artificial Intelligence (Colorado AI Act)(規範歧視性 AI、就業、醫療等高風險領域)、加州 Transparency in Frontier Artificial Intelligence Act (要求公開 AI 模型安全與風險評估等信息)；加拿大 AI and Data Act (已提交、等待立法通過，規範重點：聯邦層級 AI 法擬訂框架，覆蓋 AI 系統責任、消費者與數據保護義務等；英國以政策與標準為主，無單一 AI 專法，目前多靠行業分類與自願準則；中國大陸設有多項 AI/生成式 AI 管理舉措，例如《生成式人工智能服務管理暫行辦法》等（屬部門規範）。

[2] 參見我國《人工智慧法》第一條規定：為促進以人為本之人工智慧研發與應用，保障國民人格尊嚴及權利，提升國民生活福祉、維護國家主權、安全及文化價值，增進永續發展及國家競爭力，特制定本法。

貳、問題意識：AI 基本法係作為治理起點，抑或治理終點？

近年來，台灣立法政策中頻繁出現以「基本法」作為回應新興風險與結構性挑戰的立法選擇，從弱勢族群、環境生態、科技發展到人權保障，皆可見其蹤影[3]。然而，基本法究竟是否真能承載制度建構之重任，抑或僅成為政治上可快速交代的「宣示型立法」，始終有待嚴肅檢證。AI 作為高度技術密集、風險外溢性強，且影響層面橫跨刑事司法、行政管制與憲法權利保障的科技領域，若僅以一部「人工智慧基本法」作為回應，是否足以形成可運作的法治框架，洵有高度疑問性[4]。

從比較法觀點，基本法的本質，大都被理解為「政策方向與立法原則之宣示」，而非直接可適用的行為規範[5]。倘若立法者誤將基本法視為治理完成的終點，而非制度工程的起點，則極可能導致規範密度不足、權責配置模糊，甚至使法治要求在實務運作中落空[6]。此一問題，在人工智慧領域尤為明顯。

人工智慧對於社會秩序之影響，並非僅止於產業創新或行政效率提升，而是深刻介入人民基本權利、國家公權力行使方式，以及司法判斷結構本身。我國目前選擇以《人工智慧基本法》作為整體回應，形式上雖與國際趨勢相符，實則隱含一項關鍵風險：將高度複雜、風險導向，且需即時應對的科技治理問題，過度簡化為價值宣示與政策原則的立法工程。

拙見認為，若我國 AI 基本法未被清楚定位為「制度起點」，則在實務運作中被視為「治理完成」，恐將產生結構性法治缺陷，尤以刑事程序、行政裁量與憲法控制三個面向最為顯著。

參、制度面分析與評議

以下分別刑事程序、行政裁量與憲法控制三個制度面向，簡析如次：

一、 刑事程序觀點：演算法介入下的程序正義真空

人工智慧技術已實質介入刑事司法流程，包括犯罪預測、風險評估、臉部辨識、證據分析等面向。此類技術一旦被引入刑事程序，其影響不僅止於效率提升，更直接牽動被告之防禦權、對質詰問權與法院心證形成之透明性。然而，人工智慧基本法多僅止於抽象原則宣示，對於刑事程序中何種情形得以使用

---

[3] 我國現有八個以「基本法」為名之法律：《教育基本法》、《科學技術基本法》、《環境基本法》、《原住民族基本法》、《文化基本法》、《客家基本法》、《海洋基本法》及甫通過的《人工智慧基本法》。這些「基本法」並非憲法層級，而是「政策統攝法」，多數基本法具備：宣示性條款多、授權行政機關規劃政策、作為下位法與行政計畫的正當性基礎，真正具有「憲法補充規範效果」者僅有《環境基本法》及《原住民族基本法》。

[4] 關於基本法作為政策憲章（policy charter）之性質，參見：Peter Häberle, Verfassungslehre als Kulturwissenschaft, 2. Aufl., 1998, S. 620–635；並可對照台灣《環境基本法》、《文化基本法》之立法理由。

[5] 比較法上所稱之「基本法」（framework law / loi-cadre / Grundsatzgesetz），多被定位為具有政策指導性與立法綱領性之規範，其功能在於確立國家政策方向、價值選擇及未來立法之原則，而非直接對人民或行政機關產生具體、可裁判之權利義務關係。此一理解可見於德國法上「綱要性立法」（Rahmengesetzgebung）之理論、日本對於「基本法」之通說見解，以及歐盟法制中「框架性規範」之制度設計，均強調其對後續具體立法與行政措施之引導功能，而非作為直接適用之行為規範。

[6] 歐盟人工智慧治理所採之風險導向立法模式，參見：Regulation (EU) 2024/1689 (Artificial Intelligence Act), Recitals 1–12, 26–48。

AI，並未提供具體規範[7]。其結果是否具證據能力[8]、如何確保被告得以有效爭執與檢驗[9]，也未有明確規定。

在欠缺刑事訴訟法層級的明確規定下，AI 生成或輔助形成的資料，極可能在實務中被視為「中立、客觀」的技術結果而未經嚴格審查，反而弱化法院對證據可靠性之實質審酌。此一現象，將使正當法律程序流於形式，形成所謂「技術黑箱取代司法心證」的風險[10]。基本法若未能引導並要求部門法完成相應修正，即難以避免刑事程序保障被科技理性侵蝕。

茲舉其犖犖大者，簡述如下：

（一）AI 對刑事程序的實質衝擊

在偵查、羈押、量刑乃至假釋評估等階段，AI 已可能被用於風險評估、模式分析或決策輔助[11]。此類技術的引入，直接影響被告之人身自由、訴訟防禦權與正當法律程序保障。然而，人工智慧基本法多僅停留於「人本原則」或「可解釋性」的抽象宣示，並未建立任何可直接適用於刑事程序的具體規範。

（二）程序法未調整所生之違憲風險

若刑事程序仍以傳統「人類裁量」模型為預設，而實際上卻大量引入演算法輔助，恐將產生規範與現實的斷裂。例如：

---

[7] 關於演算法風險評估工具於刑事司法中之運用與爭議，參見：State v. Loomis, 881 N.W.2d 749 (Wis. 2016)；並可比較美國學界對 COMPAS 系統之廣泛批判。

[8] 刑事程序中正當法律程序保障與科技輔助決策可能產生之衝突，參見：Danielle Keats Citron, "Technological Due Process," Washington University Law Review, Vol. 85 (2008), pp. 1249–1313。

[9] 人工智慧介入刑事程序所涉及之正當法律程序問題，參見 Andrew Selbst et al., "Fairness and Abstraction in Sociotechnical Systems," Proceedings of the Conference on Fairness, Accountability, and Transparency, 2019, pp. 59–68。

[10] 關於「技術黑箱取代司法心證」之風險，參見 Frank Pasquale, The Black Box Society, Harvard University Press, 2015, pp. 135–160。

[11] 此之所謂在偵查、羈押、量刑乃至假釋評估等階段運用 AI，係指司法實務中引入以演算法或資料分析模型為基礎之工具，協助評估被告之再犯風險、逃亡可能性、犯罪模式或量刑參考區間。比較法上，美國刑事司法實務最早且最廣泛採用此類風險評估系統（risk assessment instruments），例如 COMPAS（Correctional Offender Management Profiling for Alternative Sanctions），曾被用於保釋、量刑及假釋決策之輔助。然學界與實務普遍指出，此類系統可能涉及演算法之偏誤、不透明性及對正當法律程序之衝擊，故多數法制仍將 AI 定位為「決策輔助工具」，而非取代司法機關之裁量與判斷；歐盟並進一步於 AI Act 中，將刑事司法領域之風險評估系統列為高風險 AI 系統，要求更嚴格之治理與監督。參閱 Danielle Kehl et al., Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing, Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard University (2017)；Julia Angwin et al., Machine Bias, ProPublica (2016) 揭露 COMPAS 風險評估在實務運作中可能產生之偏誤問題，為後續學術討論之重要起點）；Sonja B. Starr, Evidence-Based Sentencing and the Scientific Rationalization of Discrimination, 66 Stanford Law Review 803 (2014)；Mireille Hildebrandt, Law as Computation in the Era of Artificial Legal Intelligence, 68 University of Toronto Law Journal 12 (2018)；European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final（將刑事司法風險評估系統定位為高風險 AI）。

1. 被告是否有權請求揭露演算法模型[12]？

2. 法官是否理解演算法結論之不確定性[13]？

3. 若錯誤評估導致羈押或量刑不當，責任如何歸屬[14]？

在缺乏專門程序規範下，現行 AI 基本法恐無法作為有效救濟依據，反而可能掩護制度性侵害基本權之發生。

二、 行政法觀點：基本法治理下的裁量擴張與責任稀釋

就行政法而言，人工智慧的治理高度依賴行政機關之管制、監理與裁量[15]。然而，行政權之行使，依憲法法律保留原則，必須有明確法律授權作為基礎。人工智慧基本法多採原則性規定，未清楚界定主管

[12] 關於被告是否得請求揭露用於其案件之演算法模型或評估邏輯，涉及刑事正當法律程序中之防禦權、對質詰問權與程序透明性。比較法上，美國實務對此問題高度分歧，例如 State v. Loomis 一案中，法院雖允許使用 COMPAS 風險評估工具，惟否認被告有權要求完整揭露其演算法模型，理由在於營業秘密保護；然而，學界普遍批評此一立場可能侵蝕被告有效防禦權。相對而言，歐洲法制更強調「可理解性」與「可受質疑性」，並逐步要求對自動化或半自動化決策提供足以使當事人理解與爭執之說明。參閱：State v. Loomis, 881 N.W.2d 749 (Wis. 2016)；Sandra G. Mayson, Bias In, Bias Out, 128 Yale Law Journal 2218 (2019)；Frank Pasquale, The Black Box Society, Harvard University Press (2015), ch. 3; Mireille Hildebrandt, Smart Technologies and the End(s) of Law, Edward Elgar (2015)。

[13] 演算法風險評估工具所產生之結論，本質上係基於統計相關性與機率推估，而非個案事實之確定判斷。然而，實證研究顯示，司法決策者可能傾向過度信賴演算法所呈現之量化結果，產生「自動化偏誤」（automation bias），而未充分理解其誤差範圍、假設前提與適用限制。此一問題不僅涉及法官專業理解能力，更關係到裁量權是否被技術性結論事實上架空，從而引發審判獨立性與責任歸屬之憲法疑慮。參閱：Aziz Z. Huq, Racial Equity in Algorithmic Criminal Justice, 68 Duke Law Journal 1043 (2019); Danielle Kehl et al., Algorithms in the Criminal Justice System, Berkman Klein Center, Harvard University (2017); Cary Coglianese & David Lehr, Regulating by Robot, 105 Georgetown Law Journal 1147 (2017); Chris J. L. Miller, Automation Bias in Judicial Decision-Making, 20 Law, Probability & Risk 1 (2021).

[14] 當演算法風險評估之錯誤導致不當羈押或過重量刑時，其責任歸屬涉及多層次法理問題，包括司法裁量責任、行政機關採用工具之制度責任，以及技術提供者之產品或專業責任。多數法制目前仍傾向將最終責任歸屬於作成裁判之司法機關，並以「AI 僅屬輔助工具」作為責任切割依據；惟學界已指出，若制度性、結構性地依賴高風險 AI 系統，卻未設計相應之審查、校正與救濟機制，國家可能需承擔公法上之違法責任，甚至引發國家賠償或人權侵害之問題。參閱：Karen Yeung, Algorithmic Regulation, Oxford University Press (2018)；Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 UC Davis Law Review 399 (2017)；European Union Agency for Fundamental Rights (FRA), Bias in Algorithms – Artificial Intelligence and Discrimination (2022)；European Commission, Artificial Intelligence Act, COM(2021) 206 final（關於高風險 AI 系統之責任與治理架構）。

[15] 就行政法觀點而言，人工智慧之治理並非主要透過個案裁判或私法自治，而係嵌入於行政機關之事前管制、持續監理與裁量運作之中，呈現典型之「行政國家」（administrative state）或「管制國家」（regulatory state）特徵。由於 AI 系統具有高度技術性、不確定性與跨領域風險，其風險評估、合規要求、資料治理及事後監督，均仰賴行政機關透過命令、指引、許可與裁量判斷加以實現；歐盟 AI Act 即明確採取以行政監理為核心之治理模式，賦予主管機關對高風險 AI 系統之審查、監督與裁量權限，顯示 AI 治理在制度設計上高度行政法化。參閱：Giandomenico Majone, The Rise of the Regulatory State in Europe, 17 West European Politics 77 (1994); Cary Coglianese & David Lehr, Regulating by Robot, 105 Georgetown Law Journal 1147 (2017); Karen Yeung, Algorithmic Regulation, Oxford University Press (2018);European Commission, Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final.

機關之權限範圍[16]、介入時點[17]與程序要求[18]，規範密度顯有不足（principle-based regulation），容易導致兩種極端結果：其一，行政機關因欠缺明確授權而消極不作為；其二，行政機關以概括條款為由，擴張裁量空間，反而侵害人民權利。

更值得注意的是 AI 系統往往由私人企業開發與運作，但其決策效果卻直接影響公共利益。若僅依基本法宣示「促進創新」[19]與「兼顧人權」[20]，卻未在行政法制中具體化為監理義務[21]、資訊揭露責任[22]與

[16]多數人工智慧基本法或框架性立法，僅概括宣示政府對 AI 發展與風險治理之責任，未明確劃分主管機關之具體權限範圍、管制手段與裁量界線。此種高度原則化之設計，雖保留行政彈性，卻可能導致權限競合、責任不清，並弱化國會對行政權行使之事前授權與事後監督。學界因此指出，若未透過具體授權條款界定行政權限，AI 治理恐流於政策宣示，而非可受法律拘束之管制體系。參閱：Karen Yeung, Algorithmic Regulation, Oxford University Press (2018).; Cary Coglianese, Optimizing Regulation for an Optimizing Algorithm, 4 Columbia Law Review Forum 1 (2019); Giandomenico Majone, The Rise of the Regulatory State in Europe, 17 West European Politics 77 (1994)。

[17]人工智慧基本法多未明確規範行政機關應於 AI 系統之設計、訓練、部署或實際運作之何一階段介入，致使行政監理在事前預防與事後糾正之間擺盪。相較之下，風險導向治理理論主張，對高風險 AI 系統，行政介入應前移至開發與部署前階段，以避免損害發生後僅能採取補救性措施。介入時點之模糊，亦可能削弱比例原則與風險控管之實質效果。參閱：European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final; OECD, Artificial Intelligence and Risk Management (2020); Brent Mittelstadt et al., The Ethics of Algorithms, 3 Big Data & Society 1 (2016).

[18]多數 AI 基本法僅原則性要求「透明」、「可問責」或「人為監督」，卻未具體規範行政機關在作成監理或介入決定時，是否應踐行聽證、說明理由、資訊揭露或救濟程序。此種程序規範之缺位，使 AI 治理難以有效銜接行政法上之正當程序與法律保留原則，亦增加行政裁量恣意行使之風險。學界因此主張，若 AI 治理高度行政法化，則相應之程序法制亦應同步具體化。參閱：Mireille Hildebrandt, Law as Computation in the Era of Artificial Legal Intelligence, 68 University of Toronto Law Journal 12 (2018); Jerry L. Mashaw, Due Process in the Administrative State, Yale University Press (1985); Cary Coglianese & David Lehr, Regulating by Robot, 105 Georgetown Law Journal 1147 (2017).

[19]關於人工智慧系統由私人主體開發，卻對公共決策產生實質影響所引發之責任歸屬與監理困境，參見 Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press, 2019, pp. 215–230。

[20]多數人工智慧基本法或政策性立法，係以促進科技創新與經濟發展，同時宣示尊重人權、倫理與社會價值作為核心目標，惟其規範內容多停留於價值宣言或政策指引層次，而未直接創設可執行之義務或權利。此類「原則導向」（principle-based）的立法模式，雖有助於避免過度抑制技術發展，卻也導致人權保障在規範密度上顯著不足，須仰賴後續行政法制或部門法加以具體化。參閱：OECD, Recommendation of the Council on Artificial Intelligence (2019): Karen Yeung, A Study of AI Governance, in The Oxford Handbook of AI Governance (2022).

[21]在 AI 系統主要由私人企業開發、部署與營運之情形下，若基本法未進一步明定行政機關對其風險評估、合規審查、持續監督與介入更正之具體監理義務，則行政權對於實質影響公共利益之技術決策，僅能消極依賴一般授權或事後救濟。學界指出，此種監理義務之空缺，將使 AI 治理流於「政策協調」而非「法律管制」。參閱：Giandomenico Majone, The Rise of the Regulatory State in Europe, 17 West European Politics 77 (1994); Cary Coglianese & David Lehr, Regulating by Robot, 105 Georgetown Law Journal 1147 (2017); European Commission, Artificial Intelligence Act, COM(2021) 206 final（高風險 AI 之行政監理設計）。

[22]AI 系統雖由私人主體運作，然其決策結果往往影響個人權利或公共資源分配，若法律未課予相應之資訊揭露、可解釋性或說明理由義務，將使受影響者無從理解、質疑或挑戰相關決策。此種「黑箱化」不僅侵蝕程序正義，亦使行政監理與司法審查失去實質基礎。參閱：Frank Pasquale, The Black Box Society, Harvard University Press (2015); Mireille Hildebrandt, Law as Computation in the Era of Artificial Legal Intelligence, 68 University of Toronto Law Journal 12 (2018); Sandra Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist, 7 International Data Privacy Law 76 (2017)。

救濟機制[23]，則極易形成「權力影響存在、責任主體缺席」的制度斷裂。此種責任真空，並非基本法所能單獨填補。

特舉以下兩點說明之：

（一）AI 基本法與行政裁量的結構性張力

行政機關是 AI 應用最廣泛的場域之一，從補助審查、稅務風險評估到社會福利分配，均可能導入自動化決策。然而，基本法高度原則化的規範設計，實際上恐將「如何用 AI」的決定權，全面交由行政機關內部技術與政策判斷，形成裁量高度集中卻責任模糊的治理結構。

（二）法律保留原則的空洞化

依行政法理論，凡涉及人民權利重大影響者，應有明確法律授權。然而，若僅以 AI 基本法作為總括依據，而未就高風險 AI 使用設計專法與程序，將使法律保留原則流於形式，馴至行政法治將退化為「技術信任治理」，而非法治治理。

三、 憲法審查觀點：缺乏可審查性的準憲法困境

從憲法層次觀察，人工智慧對隱私權、平等權、人格權乃至人身自由之潛在侵害，已屬可預見之科技風險[24]。依大法官解釋所揭示之意旨，國家對於此類結構性風險，負有預防與制度建構之積極義務[25]。倘若立法者僅止於制定一部缺乏可操作性的基本法，而未同步完善相關部門法制，恐難通過憲法比例原則與實質法律保留之檢驗。尤其在人工智慧被用於高度侵害性場域（如刑事追訴、重大行政處分）時，若缺乏明確法律規範作為依據，未來一旦進入憲法訴訟審查，基本法本身反而可能被視為立法怠惰的象徵，而非合憲性的支撐理由。

茲析述如下：

（一）基本法的準憲法地位與其限度

基本法常被視為憲法價值在特定領域的延伸，理論上應能作為憲法審查的中介規範。然而，若條文僅

[23] 當 AI 系統之錯誤或偏誤造成權利侵害時，若法制未明確設計行政救濟、司法審查或責任歸屬機制，受害者往往難以確認應向何一主體主張權利，形成責任真空。學界將此現象形容為「權力效果存在，但責任主體缺席」，顯示 AI 治理若未同步建立救濟制度，將與法治國原則產生結構性衝突。參閱：Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 UC Davis Law Review 399 (2017); Karen Yeung, Algorithmic Regulation, Oxford University Press (2018); European Union Agency for Fundamental Rights (FRA), Bias in Algorithms (2022).

[24] 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；同時，演算法訓練資料之偏差與模型設計假設，亦可能導致對特定群體之差別待遇，進而侵害平等權。另就人格權而言，當個人被簡化為可計算之風險分數、信用評等或行為預測標籤時，易造成對人格尊嚴與自我決定之貶抑。至於人身自由，若 AI 被運用於刑事司法、治安維護或行政管制領域，其錯誤或偏誤判斷即可能導致不當羈押、監控或行動限制。此等侵害雖未必在個案中即時顯現，但在制度設計階段即已具高度可預見性，故屬憲法層次上應提前回應之科技風險。參閱：
Mireille Hildebrandt, Privacy as Protection of the Incomputable Self, in Privacy, Due Process and the Computational Turn, Routledge (2013); Julie E. Cohen, What Privacy Is For, 126 Harvard Law Review 1904 (2013); Sandra G. Mayson, Bias In, Bias Out, 128 Yale Law Journal 2218 (2019); Aziz Z. Huq, Racial Equity in Algorithmic Criminal Justice, 68 Duke Law Journal 1043 (2019); Bundesverfassungsgericht, Judgment of 27 February 2008, 1 BvR 370/07, 1 BvR 595/07（德國聯邦憲法法院關於資訊自主權與科技監控之里程碑判決）。

[25] 大法官釋字第 603 號、第 689 號（關於隱私權、人格權及國家監控之憲法界限）。

止於宣示性原則，則在具體個案中難以形成違憲審查的可操作標準。

（二）AI 案件中的違憲審查真空

當人民因 AI 系統決策而主張基本權受侵害時，憲法法院若僅能援引抽象基本法原則，將難以進行實質比例原則、必要性或最小侵害審查。結果可能會產生：

1. 對行政與立法過度尊重[26]
2. 對技術判斷不敢介入[27]
3. 形成「技術例外狀態」[28]

此一後果，恐與憲法作為最高權利保障規範之功能背道而馳[29]。

四、 檢視後小結：象徵性治理的三重風險

綜上分析，若僅以人工智慧基本法作為治理核心，至少可能產生三重制度風險：

1. 刑事程序中正當法律程序的實質弱化
2. 行政法上裁量膨脹與法律保留空洞化
3. 憲法審查中可審查性與規範密度不足

這些風險並非立法技術瑕疵所致，而是治理策略選擇所致的結構性後果。

肆、建構對策：邁向可審查、可執行、可調整的 AI 法治

基此，拙文主張，我國 AI 法制應採下列三層式之建構：

一、 第一層：AI 基本法（價值與治理架構）

將該基本法功能限縮於價值原則、風險分類與後續立法義務之明確設定，是「命令後續立法的法律」，而不是「自我滿足的宣言」。質言之：

（一）明確宣示人本原則、民主、可解釋性、比例原則

（二）界定 AI 風險分類（低 / 中 / 高風險）

---

[26] 當法院面對高度技術性或政策性問題，而欠缺具體法律授權與審查基準時，往往傾向採取高度自制立場，對立法形成與行政裁量給予廣泛尊重。於 AI 治理情境下，若僅存在抽象基本法原則而無可操作之實質規範，憲法法院即難以具體檢驗行政措施是否符合比例原則與必要性要求，致使司法審查流於形式，實質上轉化為對行政與立法之過度尊重。參閱：Aharon Barak, Proportionality: Constitutional Rights and Their Limitations, Cambridge University Press (2012); Mark Tushnet, Taking the Constitution Away from the Courts, Princeton University Press (1999).

[27] 面對 AI 演算法與資料模型所涉及之高度專業與不透明性，司法機關若欠缺法律明文要求行政機關說明、揭露或可受質疑之技術標準，易將相關爭議視為「專業判斷」而避免實質審查。此種態度不僅強化行政機關對技術決策之壟斷，亦可能導致技術性理由成為規避憲法審查之屏障。參閱：Cary Coglianese & David Lehr, Regulating by Robot, 105 Georgetown Law Journal 1147 (2017); Frank Pasquale, The Black Box Society, Harvard University Press (2015).

[28] 所謂「技術例外狀態」，係指在以科技風險、不確定性或效率需求為由之情境下，國家權力運作實際脫離既有憲法審查與基本權保障架構，形成事實上的例外領域。若 AI 系統之使用被視為不可或缺且不可理解，司法機關即可能默許其運作不受充分比例與必要性檢驗，從而使科技治理成為憲法控制之外的灰色地帶。參閱：Giorgio Agamben, State of Exception, University of Chicago Press (2005); Mireille Hildebrandt, Law as Computation in the Era of Artificial Legal Intelligence, 68 University of Toronto Law Journal 12 (2018); David Lyon, Surveillance Society, Open University Press (2001).

[29] 大法官釋字第 499 號、第 585 號（關於立法形成自由與司法審查密度）、釋字第 603 號、第 689 號（關於隱私權、人格權及國家監控之憲法界限）。

（三）建立跨部會治理機制（如 AI 治理委員會）

（四）明確規定「後續專法義務與期限」

二、 第二層：高風險 AI 專法

此一層次乃為操作核心，應優先建立：

（一）高風險 AI 管理專法，定義高風險系統係指司法、醫療、金融、就業、選舉等；評估強制影響（AI Impact Assessment）；採上線前審查或登錄制度、緊急停用與撤回機制。

（二）自動化決策與人民權利保障法，賦予人民知情權、拒絕權、人工覆核權；可解釋性最低標準；行政機關使用 AI 的程序法制。

三、 第三層：既有法律的「AI 化修正」

此之所謂「修正」，非指全部另立新法，而是修正部分現行法。例如：

（一）《刑事訴訟法》、《行政程序法》與相關實體法做系統性調整

（二）《個資法》：補強演算法剖析、再識別風險

（三）《公平交易法》：演算法共謀、平台歧視

（四）《選罷法》：深偽政治廣告

（五）《行政程序法》：AI 輔助決策規範

這一層次乃是永續關鍵核心，因為它才能使 AI 治理內建於既有法治結構中。

唯有採此三層法制結構，人工智慧治理方能從政治正確的立法姿態，轉化為真正可運作、可監督且可永續的法治工程。

伍、結論

總結而言，《人工智慧基本法》並非全然無用，只是其真正意義在於揭示政策方向、凝聚社會共識，並作為後續立法與修法的起點。然而，若立法政策停留於基本法層次，而未落實於刑事程序、行政管制、權利救濟等具體制度設計，則不僅無法有效治理 AI 風險，反而可能稀釋法治國原則之要求。基本法的作用，不是用來「把事情做完」，而是用來「把方向定準」。若沒有後續補充立法的基本法，它只是價值宣言；唯有系統性配套的基本法，才是真正的制度工程。

對於以科技立國自許的我國而言，真正的挑戰不在於是否制定更多「看得見的法律名稱」，而在於是否有能力完成繁瑣而必要的制度工程。人工智慧治理的永續發展，終究必須回到部門法的細緻修正與憲法價值的具體落實，基本法只能是起點，而不應是終點。甫訂定的《人工智慧基本法》若缺乏制度縱深，恐將成為一部「不會違憲，卻無法保護權利」的法律。直言之，對我國而言，真正的挑戰不在於是否制定基本法，而在於是否有勇氣承認：科技治理不能只靠宣言，而必須承擔制度細化的政治與法律成本。

➢ 有關德國電子通訊領域偵查措施實務介紹（下）

最高檢察署
林麗瑩檢察官

【總目錄】

（二）行動通訊裝置定位資料(Standortdaten)，依第 100i 條蒐集

第 100i 條主要明定偵查機關可運用科技設備調查行動通訊裝置之識別碼或該裝置所使用的卡片卡號(第 1 項第 1 款)，亦可調查該設備所在位置(第 1 項第 2 款)。

1. 掌握行動通訊號碼 [§100i I (1)] 及虛擬基地台(M 化車)定位 [§100i I (2)]

從規定的脈絡可知，本條授權不單純只有位置資訊，而是透過可蒐集行動通訊過程中相關識別資訊，而獲知位置資訊。本條項授權要件既然載明運用「科技設備」，顯然並非透過業者調取資料，目前常見的運用是所謂虛擬基地台(IMSI-Catcher)即國內俗稱 M 化車的使用。虛擬基地台的原理，正是利用行動通訊設備須不斷與最近的基地台訊號區取得聯繫，以準備隨時進行通訊，而架設模擬基地台發射訊號，即在誘取就位於附近的對象行動通訊設備與之聯繫，而取得其 IMSI 資訊，並因此查知位置資訊，此較一般調取基地台位置更為精準，實務運用上，通常會先透過調取通聯流量資料中的基地台位置資訊縮小範圍後，再運用虛擬基地台確認精確位置。

調查行動通訊裝置識別資訊，實務運用另有功能。例如虛擬基地台設備不僅可截取 IMSI，亦同時可截取 IMEI，除了定位外，實務上也可透過已確認的 IMEI，而掌握對象當下使用的 SIM 卡，這對於為逃避追緝經常更換 SIM 卡通訊的犯罪者，無疑是掌握其通訊的利器。

2. 本條之實體與程序要件

本條運用科技設備調查行動通訊裝置號碼、卡號及定位的實體要件規定在第 1 項，須為個案係重大之犯罪，特別是指第 100a 條第 2 項所列舉得通訊監察之案件，並係為查明事實或被告所在而有必要者；程序要件依本條第 3 項之規定準用第 100e 條相關部分規定，主要係法官保留，原則由檢察官向法院聲請令狀，例外檢察官有緊急權限。

3. 其他定位資訊仍回歸依§100g 或 §100k 向業者調取

不過所謂的定位資料，在這裡要進一步說明區分，如依照 TKG 第 3 條第 56 款規定指的是在電子通訊網絡中或由電信業者或由數位服務業者所處理的，而可指出使用者之終端設備（如手機、平板、GPS 裝置等）所處位置的資料。特別是手機的定位資料，有所謂的「基於位置的服務」（Location Based Services），例如交通資訊、查詢附近的趣點（Point of interest POI）、路線規劃、查詢所在位置（我在哪裡？）或查詢親屬（例如父母對子女）或朋友的所在地（「定位」功能）等功能，這也使得追蹤服務（Tracking-Dienste）成為可能。進一步透過這些服務，可以確認裝有相關系統的車輛所在位置，甚至可以自動傳送位置資訊。這類資料原則上係由電信業者或數位服務業者處理蒐集的資料，而非透過科技設備，因此如果要蒐集此類定位資料，仍要回到通聯流量資料(第 100g 條)或使用資料(第 100k 條)之調取。

（三）「用戶存檔資料」(Bestandsdaten)，即「使用者資料」之調取（§100j）

第 100j 條授權調取所謂用戶存檔資料，相當於國內所稱之使用者資料。如同前述，用戶存檔資料之相關定義與範圍分別依照德國電信法 (TKG)或電信與數位服務資料保護法(TDDDG)規定。犯罪偵查機關得調取之要件則依刑訴法第 100j 條第 1 項第 1 句之規定。至於同條項第 2,3 句則特別將電信業者及數位服務業者存有的用戶登入權限資料區分出來，另定其干預門檻且有第 3 項法官保留的程序要件；第 2 項則明

定調取浮動 IP 的用戶存檔資料要件，同樣依照第 1 項第 1 句。以下分別說明之：

1. 區分向電信業調取用戶存檔資料與向數位服務業調取存檔資料(§100j Ⅰ)

本條第 1 項第 1 句第 1 款所定向電信業者調取之用戶存檔資料，係指向 TKG 第 3 條第 6 款及第 172 條電信業者所保有之資料，第 3 條第 6 款為一般性定義，指電信服務契約關係之建立、內容之設計、修改或終止所必要的用戶檔案資料，第 172 條第 1 項則具體列舉 7 款項目：1.電話號碼、2.其他由業者分配的連線識別符號、3.該線路使用者的姓名、住址、4.使用者為自然人時，其出生日期、5.在固網線路時，其線路之地址、6.在行動通訊情況，除行動通訊號碼，尚包括使用之終端行動設備識別碼，以及 7.該行動電話號碼分配使用或使用契約的起始日期等，相當於我國通訊保障及監察法第 3-1 條第 2 項所規定之通訊使用者資料。

本條項第 1 句第 2 款則為向網路數位服務業者調取之用戶存檔資料，依 TDDDG 第 2 條第 2 項第 2 款之定義與範圍，內容大致與 TKG 上述規定相同。

如上所述，本條用戶存檔資料即相當我國使用者資料，具體而言，除用戶姓名、地址外，還可包括基於契約而設定的銀行轉帳帳戶資料、在網路通訊上則包括網路使用者之固定 IP 位址(feste IP-Adressen)、電子郵件使用者之真實姓名，在行動電話則包括 IMSI 或 IMEI 等資料(§172 Ⅰ TKG；§ 2 ⅡNr. 2 TDDDG)。

本條第 1 項第 1 句作為調取使用資料之授權規定，其明文之實體要件為須因調查事實或被告所在而有必要者，並未另有程序要件要求法官令狀，檢察官或警方得依職權調取之。

2. 浮動 IP 的用戶資料之調取 (§100jⅡ)

按照用戶存檔資料的定義，IP 位址也係用戶存檔資料(連線時分配的識別符號)，但其性質上也屬於連線時產生的通聯流量資料(在通訊過程中產生的資訊)，惟所謂固定 IP 位址並不會變動，每次網路連線均透過相同 IP 位址，與電話號碼具有類似性，被歸類為用戶存檔資料尚無爭議，且目前僅有公司企業或機關等網路大用戶使用固定 IP，數量不多且在網路上已可公開查詢，屬於本條第 1 項第 1 句可調取之範圍。至於浮動 IP 位址，通常為個人上網使用，每次連線均會分配到不同的 IP 位址，與通訊密切相關，如前所述屬於依第 100g 條第 1 項或第 2 項調取通聯流量資料之規定調取之，並不在本條第 1 項所謂用戶存檔資料範圍內。惟取得浮動 IP 後，要確認該 IP 實際使用者，是否即得依本條調取用戶存檔資料，則有很大爭議。聯邦憲法法院定調浮動 IP 包括浮動 IP 使用者的身分資料均屬於基本法第 10 條秘密通訊自由保障之範圍內(BVerfG 02.03.2010 – 1 BvR 256/08)，理由在於其與固定 IP 不同，浮動 IP 係伴隨在個別的通訊過程中產生，每次均不相同，而與具體通訊之進行密切關連，縱使已知浮動 IP 位址，其使用者身分的確認尚必須透過分析通聯流量資料，方得以調取用戶存檔資料，因此仍將其歸屬於秘密通訊自由保障之範圍。雖然如此，聯邦憲法法院認為縱然確認浮動 IP 使用者需透過通聯流量分析，才能取得用戶存檔資料，但偵查機關並不是調取通聯流量資料，而是藉由分析流量資料確認特定用戶後調取其用戶存檔資料，目的僅在確認使用者身分，因此不須法官保留。不過調取浮動 IP 之用戶存檔資料畢竟與一般調取電話號碼或固定 IP 位址用戶存檔資料有別，立法上乃另立第 100j 條第 2 項針對浮動 IP 使用者資料的調取授權，要件仍同第 1 項第 1 句，並無須

法官令狀，僅須為調查事實或被告所在有必要時，檢警即得依職權為之，但必須將有滿足第 1 項第 1 句之要件明確記載於案卷內。本項規定隨著 2021 年修正後，除得向電信業者調取外，也包括得向數位服務業調取浮動 IP 之用戶存檔資料。

3. 登入權限資料(Zugangsdaten)之調取(§100j Ⅰ S.2,3 + §100jⅢ)

依照上述 TKG、TDDDG 法律定義的用戶存檔資料，實際包含所謂使用特定設備或特定服務的登入權限。但用戶使用相關服務之登入權限設定，例如密碼、金鑰等，形式上雖屬用戶存檔資料，但其功能又與所謂內容(可能是通訊內容或隱私內容)緊密相關，本條規定也將其特別區分出來，另定其干預門檻。實體要件區分向電信業者調取者依照本條第 1 項第 2 句；向數位服務業者調取使用其服務之登入權限資料者，依該項第 3 句。至於程序要件則依本條第 3 項規定，原則需要法官令狀，但檢察官、司法警察均有緊急調取權限。

第 1 項第 2 句規定向電信業者調取登入權限資料，必須依照相關得調取此種資料之授權規定。亦即如所欲調取之資料係用於保護進入終端設備，或用於保護置於該等終端設備內或與其在空間上分離使用之儲存裝置者（TKG 第 174 條第 1 項第 2 句），必須依照可取得隱私或干預通訊秘密的法定授權為之，例如取得對終端設備內容的扣押命令或搜索票，即得向業者調取登入該設備之密碼。但如果不是基於搜索或扣押命令，例如非透過被告之電腦，而是從他處網路在被告不知情狀況下，登入其使用之雲端服務系統，則須依照第 100a 條取得通訊監察許可，因使用雲端，係透過上網連線，即落入通訊秘密保護的範疇。

此處尚需一提的是，就現實狀況，所謂終端設備密碼，可區分為一般 PIN 碼，或所謂 Super-PIN 碼，即 PUK，前者用戶自己可以隨時變換，電信業者並無法掌握，而後者則是用於 PIN 碼忘記丟失、輸入三次以上錯誤鎖住無法登入時，由業者提供的解鎖密碼，這方屬於業者存有且固定不變的登入權限資料，因此現實中，就終端設備能向業者調取到的登入權限資料，即僅有 PUK 碼。

至於第 1 項第 3 句授權向數位服務業者調取使用其服務之登入權限資料，相關實體要件比向電信業者調取登入權限資料更為嚴格，除了第 2 句相同的要件外，尚必須係為調查第 100b 條第 2 項第 1 款 a,c,e,f,g,h 或 m，或該項第 3 款 b 的第一種，或第 5,6,9,10 款所列之犯罪，主要為偽造貨幣、幫派竊盜、強盜、收賄等特別嚴重之犯罪，因此範圍較得向電信業者調取者更為限縮。

（四）「使用資料」(Nutzungsdaten)：即使用數位服務產生之通聯流量資料之調取（§100k）

調取通聯流量資料的授權依據，早期僅在德刑訴法第 100g 條內加以規定，隨著網路服務越趨多樣化、普遍化，使用網路服務所產生的通聯流量資料已與基本連接網路的通聯流量資料大有不同；另一方面立法政策上也配合前端管理法規區分電信業者與數位服務業者，在調取網路流量資料上，也把使用數位服務所產生的通聯流量資料與電信業處理的通聯流量資料區分開來，另訂授權依據第 100k 條，並稱此類資料為「使用資料」(Nutzungsdaten)。

1. 通聯流量資料與使用資料之區別

依照刑訴法第 100k 條第 1,2 項規定的干預目標是來自使用數位服務的資料。同樣的，本條授權規

定並未具體說明哪些數據屬於此類，也是援引 TDDDG 第 2 條第 2 項第 3 款的法律定義，是指數位服務業為啟用和計費所必要，而處理之用戶個人資料，同款並列出三種具體資料：a) 用於識別用戶的特徵，b) 有關開始使用和結束以及該使用範圍的資訊，c)用戶所使用之服務。其內涵與通聯流量資料似無不同，個案上兩者區別在於：當網路使用者透過電信業者建立網路連線，則此電信流程最初會產生 TDDDG 第 9、12 條和 TKG 第 176 條所定義的流量數據，涉及網路連接的開始和結束以及使用的電話號碼或分配的 IP 位址，偵查機關應分別情況依第 100g 第 1 項或第 2 項調取。而在後續通訊過程中，相關網路服務提供者可能會收集除流量資料之外的其他資訊，這些資訊與特定數位服務的具體使用情況相關，即為本條之「使用資料」，有些與通聯流量資料相當，如浮動 IP 位址以及相關傳輸的網路流量資料，但不僅是網站(Web Seite)，會更進一步具體到用戶實際登上哪個網頁(URL)的資訊，只要是數位服務業者所蒐集處理的流量資料即屬之。

至於所謂的數位服務業，即包括社群網站、電子商務網站(如拍賣網站、商城等)、遊戲平台、搜尋引擎、線上遊戲、線上銀行等，以及透過下載 App 的各項服務(新聞、健康、健身等)，均被歸類為數位服務業，用戶必須上網連線才可以進一步取得其服務，則使用該服務所產生的網路流量即使用資料。至於提供通訊服務的業者，特別指可一對一的通訊，包括所有的電子信箱(E-Mail)、信息(Messenger-Dienste)服務，則仍屬於電信業的範疇。

2. 調取使用資料之權限區分第 1 項、第 2 項與第 3 項不同層級

關於調取使用資料的要件基本與調取通聯流量資料的要件規範類同。實體要件依照本條第 1 項之規定，必須為個案係重大之犯罪，特別是指第 100a 條第 2 項所列舉得通訊監察之案件，並為查明事實所必要，且調取之資料必須與案件的重要性比例適當，其中有關位置之資料，除可因調查事實所必要外，也可為查明被告所在有必要而調取之，但如果要調取的位置資訊是屬於過去的存檔資料，則必須滿足第 100g 條第 2 項所定之要件[參見本文(中)段落貳、三、(一) 2. 中之說明]，惟本條並未如第 100g 條第 2 項授權偵查機關調取法律課予業者有儲存義務之資料。因此得調取過去回溯性的使用資料，僅限於本項第 1 句指向 TDDDG 第 2 條第 2 項第 3 款規定，業者因啟用與計費目的所必要而儲存之使用資料。是以依本條項大部分調取的仍屬於現在與未來的使用資料。

本條第 2 項另規定擴大授權得調取使用資料之案件。主要係針對網路仇恨言論、網路犯罪，縱然不屬於本條第 1 項所定之犯罪，但如有具體事實可認涉有本項所列舉之犯罪，而以其他方式調查事實難期有結果時，亦得調取使用資料，但不包括位置資訊。

調取使用資料之程序要件，係依第 101a 條第 1a 項準用第 100e 條第 1 項，亦如同通聯流量資料之調取程序，須由檢察官向法院聲請，例外檢察官有緊急權限。不過第 100k 條第 3 項針對單純為確定使用者身分之情況，授權檢察官在滿足第 1 項或第 2 項實體要件下，得依職權調取上述 TDDDG 第 2 條第 2 項第 3 款所列 a) 用於識別用戶特徵之資料。屬於這類資料者如用戶的使用者名稱、E-Mail 或 IP 位置等類似用戶存檔資料。

參、結語

本文以上分(上)、(中)、(下)介紹德國在電子通訊領域的偵查措施，包括規範與實務運用，除主要依照德國刑訴法條文先後順序外，也以電子通訊資料分類來加以說明，包括了通訊監察(含來源端通訊監察)、線上搜索、通聯流量資料的調取(即相當於我國通信紀錄與網路流量紀錄之調取)、基地台全區通聯資料之調取、定位資料之蒐集或調取、用戶存檔資料(即相當使用者資料)、登入權限資料之調取，以及較新立法的使用資料之調取等。又因為規範依不同的基本權干預及不同的干預強度而為層級化規定，也特別先就其規範的結構提出四個重點：授權基礎的雙門模型、對過去回溯性資料儲存、調取的限制、電信業與數位服務業之區分，以及依資料種類而設計不同干預門檻等大原則加以提示，以助於瞭解掌握，這四點有關規範結構的原則，也極具比較法上參考的意義與價值。

整體而言，電子通訊偵查措施各國檢警運用的實務不會相差太多，但是就法制面觀察顯然差異甚大。德國法制在電子通訊偵查上干預授權的層級化非常縝密，又基於雙門模型，對於業者提供相關資料的授權規定與資料的分類，也相當細緻，一方面立法者並不吝於給予偵查機關相應的權限，僅在事前、事中及事後設計多層保護權利的機制，本文集中於介紹事前授權的層級化規定與運用，除在本文(上)貳、一、(三)段落提及通訊監察、線上搜索執行過程之保護措施外，並未觸及其他各項措施事中、事後的監督、保護規範。而這部分重要性並不亞於事前的授權規定，限於篇幅無法深入，尚待日後有機會補充。相對於德國，我國法在此部分的法制相對簡陋，甚至於來源端通訊監察或線上搜索，迄今仍無授權之法源，對於已經網路化的現代通訊社會而言，制度與現實顯然嚴重脫節，也遠遠落後國際間的犯罪查緝腳步。

此外，值得一提的是為因應科技持續推陳出新，犯罪手法不斷精進，德國相應的司法實務、行政、立法修法的速度也非常快，每年均有因應新興運用手段而有新的司法實務見解產出，並緊接著有新的修法進度。本文也多次引用到其聯邦憲法法院、最高法院甚或是歐洲法院於審查實務具體措施所表示的意見，並進而引導修法方向，德國不管是刑訴法或相關電信、數位法規，近年的修法頻率確實非常高。目前熱門的話題，正是因應歐洲法院判決指出不得要求業者無差別、一般性的儲存所有用戶的通聯流量資料，德國正研議是否立法採行緊急凍結(Quick-Freeze)的保全措施，但檢警實務則希望能特別針對 IP 位址允許儲存，這也是歐洲法院明白表示可行的方式，否則事後在無資料紀錄可追索的情況下，顯難以有效查緝犯罪。是以可預見短期內，又有一波不小的修法。雖然各國立法、司法有其本土考量，未必可一味參照，但德國司法、立法上因應犯罪新興工具的效率深值我國參考。

➢ 德國檢察官之產生

臺北地檢署
李進榮檢察官

【目　錄】

壹、前言

德國檢察制度之創建始自薩維尼(Friedrich Carl von Savigny)就任普魯士王國部長，並於 1849 年在普魯士刑事訴訟法增設檢察官以承擔追訴犯罪任務。隨著普魯士統一德國，至 1877 年整個帝國終於有統一檢察制度[1]。第二次世界大戰後，德國分裂為東西德，嗣東德於 1990 年併入西德，兩德統一。西德自成立起，即採聯邦制，各邦與聯邦各有獨立行政、立法及司法等機構，檢察體系亦區分為聯邦與邦兩層級:

1. 聯邦層級有聯邦檢察署(Bundesanwaltschaft)，隸屬聯邦司法行政部；
2. 邦層級由下到上有區檢察署(Amtsanwaltschaft)、地方檢察署 (Staatsanwalt-schaft)及高等檢察署(Generalstaatsanwaltschaft)，隸屬各邦司法行政廳。

聯邦檢察署與各邦高檢署間係平等，並無隸屬關係。

德國檢察官依該國刑事訴訟法規定，係偵查階段主體，負責對警察調查結果作出法律評價以終結偵查程序；或中止(第 170 條第 2 項)；或提起公訴(第 170 條第 1 項)；或向法院聲請簡易判決處刑(第 407 條第 1 項)。如認為警察調查結果尚難以作出法律評價，得命警察繼續調查。檢察官提起公訴後，須於法院審判時蒞庭，從朗讀起訴要旨起(第 243 條第 3 項第 1 句)，繼而參與證據調查(第 240 條第 2 項第 1 句)，最後論告(第 258 條第 1 項)，對判決或裁定不服，得為被告利益或不利益提起上訴或抗告(第 296 條第 1 項、第 2 項；第 312 條、第 333 條及第 335 條)。有罪判決確定後，檢察官亦為執行機關，但此項業務通常委由司法事務官(Rechtspfleger)行之。

由前述說明可知，德國檢察官雖因聯邦體制，在組織結構上與我國不甚相同，然職權與任務則幾無二致，是該國檢察官如何產生，已足引人好奇。筆者於德國波昂大學攻讀法學博士期間，曾親身觀察法律系學生準備司法考試，2022 年亦與檢察總長及司法官學院院長至德國考察該國「完全法律人」制度，以下擬簡

[1] Peter Collin, Die Geburt der Staatsanwaltschaft in Preußen(12.03.2001), in forum historiae iuris.

介德國檢察官之養成過程及與我國現制之差異。

貳、法令依據

依德國基本法第 74 條第 1 項第 27 款規定，各邦法官之權利義務，屬於聯邦與邦競合立法(konkurrierende Gesetzgebung)，亦即就特定事項，邦與聯邦均有立法權限，惟就同一事項聯邦與邦均訂有法規範時，應優先適用聯邦法。屬於聯邦法之德國法官法第 122 條第 1 項規定，只有取得法官職務資格者，得被任命為檢察官；同法第 5 條第 1 項規定，修畢大學法律學程、通過第一次考試、完成法律實習、並通過第二次國家考試者，取得法官職務資格。德國傳統法學教育與國家考試以培養法官為目標，然實際上通過考試者大都從事律師或公務員，且學生在校成績與國家考試無關，為此德國於 2002 年 7 月 1 日修改法官法(2003 年 7 月 1 日生效)，將法學教育目標由培養法官轉向律師或能提供適當法律諮詢之法律人，並於前述法官法第 5a 條第 3 項規定課程框架，即從事律師工作所需之談判管理、修辭學、爭端解決、調解、詢問技巧與溝通能力等。新法亦提高大學法學教育對國家考試的影響力，具體作法乃引入「中間考試」與「重點領域課程」，通過「中間考試」，始能修習「重點領域課程」，而該課程之在校成績，占第一次司法考試成績的 30%[2]。

另依聯邦律師條例第 4 條第 1 項第 1 款規定，具德國法官法所定之法官職務資格者，得申請擔任律師。此外聯邦公證人條例第 5 條及聯邦公務員職等辦法第 21 條第 2 項均規定，具法官職務資格者，得申請擔任公證人及非技術性之高等聯邦公務員。

參、養成過程

依德國法官法第 5 條第 1 項規定，擬成為檢察官者須具有法官職務資格，而該資格之取得依序須經歷「修畢大學法律學程」、「通過第一次司法考試」、「完成法律實習」及「通過第二次國家考試[3]」。

一、大學法律學程

德國法官法第 5 條第 2 項規定，法律課程與實習內容應相互協調，該國法學教育主流係「國家考試學程」(Staatsexamen Studiengang)，依同法第 5a 條規定，修業年限 4.5 年，唯有循此學程修業者，方具參與司法考試之資格。學科類別上分為三大領域:民法、刑法及公法，學程安排上區分為「基礎課程」(Grundstudium)、「主要課程」(Hauptstudium)、「重點領域課程」(Schwerpunktbereich)與「考試準備課程」(Examensvorbereitung)等[4]。

（一）「基礎課程」預計於 3 學期完成，學生必須修完公法、民法及刑法三大領域之基礎課程，並通過期末考試(Abschlussklausur)，部分課程須繳交家庭作業(Hausarbeit)。若期末考試不及格，有一次重考機會，若重考仍未通過，則無法繼續註冊，將被退學。完成「基礎課程」並通過「中間

[2] 柯格鐘、葉啟洲，國家菁英季刊，第 16 卷第 2 期(112 年 12 月)，第 7 頁以下。

[3] 以往德國之司法考試劃分為第一次與第二次「國家考試」(Staatsexamen)，但於 2003 年修法後，因於第一次考試採納 30%之在校成績，故第一次考試不再以「國家」考試稱之；惟第二次考試因由各邦舉辦，故依舊稱為國家考試。

[4] 蔡麒亞，初探德國法律專業人員培訓制度，二(一)以大學為起始點之法學訓練，台灣新社會智庫，網址:初探德國法律專業人員培訓制度 | 台灣新社會智庫全球資訊網(最後瀏覽日:114 年 7 月 1 日)。

考試」(Zwischenprüfung)，方得選修「重點領域課程」。「中間考試」並非專指某項特定考試，而係指基礎課程中所有修業條件之集合名詞。

（二）修畢「基礎課程」後，進入「主要課程」階段，此階段之課程目的在於加深三大領域之授課內容，授課範圍大幅擴張至各專門法律領域，包含商事法、勞動法、訴訟法及稅法等進階課程，預計 3 學期可完成。主要課程、重點領域課程與考試準備課程三者間並無必然先後順序，三者可同時進行，惟「主要課程」通常是「重點領域課程」之準備階段。

（三）進入「重點領域課程」階段，會再細分數個子領域，供學生自行選擇。此階段之考試方式視各校規定，有須筆試或口試，或須繳交課堂報告，或數種方式結合，類型不一而足。重點領域課程考試之成績占第一次司法考試 30%，其餘 70%係國家指定科目考試，兩者合併計算出第一次司法考試成績。此二項考試參與時程，並無硬性先後順序，學生得視情況自行安排應考順序。各大學法學院藉由「重點領域課程」而發展自己不同學科特色，以北威邦波昂大學 2023 年為例，即提供下列 12 種重點領域課程:1.基礎課程、2.民事與商事案件之爭端解決、3.家事法及繼承法、4.企業法與資本市場法、5.企業、稅與結算、6.經濟法、競爭法與資訊法、7.勞動法與社會安全法、8.法治比較與國際私法、9.德國與歐洲憲法、10.關於永續發展之公法、11.國際關係法、12.犯罪學[5]。

（四）通常於第 6 學期即開始進入「考試準備課程」，目的在於複習過往教授之法學知識，透過大量案例分析，鍛鍊學生答題技巧與應試能力，並設有模擬考試，使學生預先熟悉國家考試之情境。德國亦有司法考試補習班傳授應考技巧，吸引不少學生前往。

另依德國法官法第 5a 條第 3 項後段規定，學生須在未修習課程期間(即我國所稱寒暑假期間)，完成至少 3 個月的校外實習(praktische Studienzeit)，目的在於使學生了解相關法律行業之實際運作過程。惟校外實習地點，以各邦主管機關所公告者為限，未必限於傳統司法機關或律師事務所，行政機關、公司行號或私人機構均有可能。至於應徵實習地點，則由學生自行規劃投遞[6]。

二、第一次司法考試

第一次司法考試係由各邦之司法考試局(Justizprüfungsamt)依據各邦頒布之相關法令辦理，所以具體考試細節各邦會略有差異，但原則上每年固定舉辦兩次。至於考試資格，依北威邦司法考試及法律實習法第 7 條第 1 項規定，須於德國境內大學修習法學達 4 學期以上、通過中間考試、修習外語課程及完成 5 次閉卷考試、4 次家庭作業與校外實習等條件。

考試內容大別分為筆試或口試。筆試部分民法考 3 次、公法 2 次、刑法 1 次，通常每天考一次，每次 5 個小時，總共需歷時 6 天方能完成所有筆試。筆試時可攜帶經考試委員會許可之資料(如法典)入內。口試於筆試後擇期舉行，部分邦會限制筆試成績合乎一定標準者始得參加。口試亦分民法、刑法及公法，考生進試場後，先取得試題，經過一定準備時間後，再進行口試。口試委員多半為 3 名，至少一位委員

[5] https://www.jura.uni-bonn.de/studium/studieninformationen/schwerpunktbereiche/ueberblick (最後瀏覽日 114 年 7 月 1 日)。

[6] 蔡麒亞，前揭文，二(一)以大學為起始點之法學訓練。

須具學術背景，口試時間大約 30 分鐘，3 名口試委員均應對考生提問。口試成績出爐後，與筆試成績按比例加總後，得出總成績[7]。筆試與口試總成績與大學之重點領域考試依照 70%與 30%之比例加總後，得出第一次司法考試成績，高於 4 分以上者，方屬合格[8]。凡第一次司法考試合格者，始完成「國家考試學程」，可獲得「大學法學文憑」(Diplom-Jurist Univ.)並具有「法學士」頭銜(Jurist)，而成績在前百分之 15%以內者，可攻讀博士。

依德國法官法第 5d 條第 5 項規定，第一次司法考試僅能重考一次，如重考仍未通過，往後不能再參加考試。為鼓勵學生盡速完成大學學業，各邦設有「額外機會」(Freiversuch)，若考生未中斷學程，於法定期限內修畢所有課程後，參加第一次司法考試國家指定科目，卻未通過者，該次考試不列入法官法第 5d 條第 5 項所限次數內，亦即合乎此條件之考生總計可參加 3 次[9]。法律雖規定修業年限 4.5 年，但因德國文獻汗牛充棟，掌握需時，且得考試次數有限，而成績對於未來職業選擇影響重大，所以大部分德國法律系學生非有充分準備，不敢貿然應試，參加第一次司法考試時均已修業多年，遠逾法定年限。

三、法律實習

通過第一次司法考試者，原則上得向各邦辦理法律實習之主管機關(通常是邦高等法院)提出申請，若申請時，該邦已無實習職位，主管機關得否准其申請。又通過第一次司法考試後，除圖林根邦限於 4 年內外，其他邦並無規定須何時開始法律實習，當事人得自行決定。獲准參與法律實習者具實習生身分(Rechts-referendar)，屬於公法上關係，每月可獲得生活津貼，具體額度各邦略有差異，大抵在 1000 至 1500 歐元間(巴登符騰堡邦 2022 年是 1353 歐元)[10]。實習生於二年期間是全職參與訓練，除非經主管機關同意，否則不得兼任其他職務。

依德國法官法第 5b 條規定，實習期間為 2 年，期間必須前往地點包括 1.民事法院、2.檢察機關或刑事法院、3.行政機關、4.律師部門以及 5.其他自行選定之實習場所。同條第 4 項規定，於律師部門最少應受訓 9 個月，其他處所至少 3 個月以上。實習目的在使實習生瞭解實務運作態樣。在法院與行政機關階段，須固定聽取課程，參與小組討論，熟悉具體法律事務運作，包含書狀撰寫、法院審理程序及刑事偵查等，結束時尚須通過測驗[11]。依德國法院組織法第 142 條第 3 項規定，法律實習生可履行區檢察官之職權，以及在指導檢察官監督下獨自進行公訴業務。區檢察官並非通過司法考試之檢察官，其職權與我國之檢察事務官相類。公務機關實習結束後，即進入律師部門實習，至何律師事務所受訓係由實習生自行應徵。最後是自選場所階段，選擇之自由程度相當高，不論是國外機構、大型企業或前往 Speyer 的聯邦公共行政學院均可，此階段選擇常與實習生擬從事職業別有關[12]。

---

[7] 法務部司法官學院，赴德考察司法官進用、養成及在職進修制度出國報告(112 年 3 月 3 日)，第 16 頁；蔡麒亞，前揭文，二(二)國家必修科目考試(第一次國家考試)。

[8] 關於評分標準，德國係採 18 分/7 級制：16-18 分係「特優」(sehr gut)、13-15 分「優」(gut)、10-12 分「佳」(vollbefriedigend)、7-9 分「尚可」(befriedigend)、4-6 分「及格」(ausreichend)、1-3 分「差」(mangelhaft)、0 分不及格(ungenügend)。

[9] Jan Ziekow 著, 詹鎮榮譯，德國司法考試制度，國家菁英季刊，第 5 卷第 2 期(2009 年 6 月)， 第 194 頁以下。

[10]法務部司法官學院，赴德考察司法官進用、養成及在職進修制度出國報告(112 年 3 月 3 日)，第 16 頁以下。

[11]法務部司法官學院前揭出國報告第 17 頁以下。

[12]柯格鐘、葉啟洲，前揭文，第 12 頁。

每一階段結束會獲得結訓證書，證書中會針對實習時各項表現、參與程度、專業能力、業務執行力及領導表現予以評價，實習生唯有完整獲得各階段所授予證書，始屬完成實習。

四、第二次國家考試

法律實習結束緊接著第二次國家考試，中間並無間隔，通常至第 19 個月尚在律師部門實習時，邦高等法院就會呈報實習生名單予司法考試局進行考試時程安排，實習生無須另外報名。換言之，第二次國家考試是實習培訓的一環，用以檢驗實習階段成效，一旦開啟實習，即有參與考試義務[13]。

第二次國家考試如同第一次司法考試，分為筆試及口試。筆試仍以公法、民法及刑法三大領域為主，考試次數上，各邦略有不同，少則 7 次(柏林)，多則 11 次(巴伐利亞)，每次考試時間 5 小時，整體筆試時程約半個月至一個月。第二次國家考試題目為相關筆錄證據，考生須像檢察官或法官一樣，綜合事證研判被告是否成立犯罪，構成何罪後，撰成起訴書或判決書，此與第一次司法考試題目為設定之實例題不同，亦即第一次司法考試係以「鑑定書模式」(Gutachtenstil)，而第二次國家考試則為「判決書模式」(Urteilstil)答題。口試則於筆試結束後間隔數個月後舉行，考生多會利用此段期間完成自選場所之實習。口試佔成績比重，各邦略有不同，大抵在 30%至 40%之間。第二次國家考試有二次重考機會[14]。

第二次國家考試通過後，取得「候補司法人員」(Assessor)身分，得依其成績及意願，申請擔任法官、檢察官、律師、公證人等。

五、申請流程

依德國法官法第 9 條規定，擔任法官或檢察官者，除具有「候補司法人員」身分外，尚須係德國基本法第 116 條所稱之德國人，堅決支持基本法意義下之自由民主體制，且具必要社交能力(soziale Kompetenzen)，符合前述資格者得向邦司法行政部申請擔任檢察官，該部會先挑選條件適合者面談，面談目的乃審核申請人個性是否適合檢察官工作，而挑選標準主要是第二次國家考試成績，另年齡不能超過 45 歲，亦須無犯罪紀錄。邦司法行政部再將審核後的名單交邦議會遴選委員會作最後決定，委員由邦議員、法官或檢察官等組成[15]。

經過遴選成為檢察官後，會先分發至檢察署擔任檢察官 2 年，然後轉換成法官亦 2 年後，此 4 年為試用期間(Probezeit)，期滿始能成為終身職檢察官[16]。

肆、半職檢察官

德國有「半職檢察官」之設，得選擇作一半或三分之一工時，薪水則依比例調整。半職檢察官仍屬專職檢察官，而非兼職，只是工時彈性，讓檢察官得以兼顧家庭，特別是許多女性檢察官生產完後，申請成為半職檢察官。以法蘭克福檢察署為例，2018 年有 135 位檢察官，其中 30 位至 35 位是半職檢察官[17]。

---

13 蔡麒亞，前揭文，三、第二次司法國家考試。

14 蔡麒亞，前揭文，三、第二次司法國家考試。

15 法務部司法官學院前揭出國報告，第 13 頁以下。

16 法務部司法官學院前揭出國報告，第 18 頁以下。

17 法務部司法官學院，赴德國考察司法官進用及養成制度、在職進修及監獄矯正制度出國報告 (107 年 8 月 17 日)，第 21 頁。

伍、與我國之差異

一、在德國，僅有修習「國家考試學程」，並通過二次司法考試者，具有「候補司法人員」身分者，始能成為檢察官；我國依法官法第 87 條第 1 項，除司法考試及格者外，曾任公設辯護人、律師、(助理或副)教授、檢察事務官等 6 年以上者，亦得任檢察官。另外，依公務人特種考試司法官考試規則第 3 條規定，在我國除大學法律系外，行政系或政治系畢業生，或經高等考試檢定合格者，亦具應考司法官資格。

二、在德國，檢察官與律師之考訓過程完全相同；在我國，檢察官屬於「公務人員特種考試」，律師則係「專門職業及技術人員高等考試」。二者雖一同筆試，但「前者」尚須口試，且錄取後，須至法務部司法官學院受訓 2 年；「後者」則須接受 6 個月職前訓練，完成後取得律師執業資格。

三、我國的司法官考試，約相當於德國第一次司法考試，錄取後至法務部司法官學院受訓 2 年，即先在學院上課 10 個月，繼而至法院、檢察署、行政機關與矯正機關見習，然後再回司法官學院接受擬判測驗與分科教育，在司法官學院受訓部分，約相當於德國法律實習與第二次國家考試。換言之，德國是「考訓合一」，我國是「先考後訓」[18]。

四、德國大學法律系學生須第一次司法考試合格，始能取得畢業證書，且在校成績佔第一次司法考試成績 30%，法學教育主要目的即在通過國家考試或培養法律工作者；我國則「學考分離」，學生可選擇完成大學法學教育，不參與司法官或律師考試，從事與法律無關的工作；而未完整受過大學法學教育者，只要符合資格，通過司法官考試，亦能擔任檢察官，且司法官考試之通過與否與大學成績無關，使我國大學法學教育對檢察官養成不若德國明顯可見。

五、德國邦層級的法官及檢察官均隸屬邦司法行政廳，所以輪調容易，甚至在試用階段，要強制輪調，藉以熟悉彼此工作內容，且調廳辦事者既有法官，亦有檢察官；我國因法官檢察官隸屬不同體系，雖有輪調制度，但須經嚴格審查及口試，於候補階段並無強制輪調，更無法官及檢察官同調司法院或法務部辦事之可能。

六、我國無德國「半職檢察官」之設，如要照顧家人，得留職停薪。

[18] 柯格鐘、葉啟洲，前揭文，第 16 頁。

臺中高分檢李慶義主任檢察官榮退
邢檢察總長感謝其對司法的貢獻

最高檢察署 1 月份月刊重點內容，聚焦本期核心議題，結合法治專業與數位科技，115 年 2 月 4 日同步透過 AI 主播對談形式播出，帶來嶄新聆聽體驗，邀請您一同收聽！！
（完整資訊請以月刊所載為準）