第五章　焦點議題分析
國外使用社群媒體進行詐欺犯罪預測之現況與反思

葉珈瑜、鄭元皓

壹、前言：網路詐欺預測的可能性

國立中正大學犯罪防治學系戴伸峰教授曾在 podcast 節目[5]上提到：「犯罪是遏制犯罪最好的工具」，許多犯罪行為是從「小嘗試」帶來的正面增強（positive reinforcement）與認知扭曲開始，此觀點可用於解釋特定犯罪問題。如酒駕者初次以機車醉態駕駛且順利到家，便會覺得「行為無傷大雅」，進而轉至汽車、或載人、或煽動周遭親友仿效犯行，直到「撞到人且被逮捕」才可能中止行為。詐欺犯罪亦是如此，在理性選擇下，若個案被刑事司法制裁的機率遠低於犯罪成功機率，就可能助長其持續犯罪。而前述情況便使人好奇，「犯罪預防」作為刑事政策的核心關懷之一，就我國盛行的詐欺犯罪態樣，在實務上有無事前預測且預防之可能？若有，又是如何做到控管？臺灣是否可借鏡他山之石？

在資料科學的發展過程中，相較於問題驅動（problem driven）的方法，資料驅動（data-driven）的決策輔助流程，因不同的機構各自保管資料，運用上缺乏整合/共享、傳統數據倉儲系統過時、資料結構不一致等技術限制，使得龐雜的資料量在萃取（extract）與變

5 曾博恩（2025 年 7 月 7 日）。犯罪心理學教授：某些基因可能讓你更趨向犯罪（EP182）[音訊 podcast 集]。收錄於博音。https://open.firstory.me/story/cmclj8u1h0cuy01w6frgi4v3l

換（transform）上不易進行串接[6]。再者，分析開始前的資料清洗（data cleaning），如未將雜訊（誤導性內容、操弄性內容、虛構性內容等）確實清理，則會受 GIGO（Garbage-in-Garbage-out）問題而使分析品質受到質疑。然而，鑑於資訊科技領域的迅速發展，圍繞著資料驅動的一系列技術與研究正持續精進，例如人工神經網路、聚類分析、案例推理等，都讓資料庫知識探索（Knowledge Discovery in Databases, KDD）的概念，提供了更成熟的實踐環境[7]。

在討論犯罪預測時，應可從「預測技術」、「犯罪屬性」、「資料來源」三個面向建構。首先，預測技術早已普及於現代社會，如 Web Cookies 或《Meta 服務條款》，讓企業於商用目的上，多使用「數據驅動營運」、「商業智能」等決策輔助系統，透過精準分眾並挖掘偏好，以及個人化演算「你可能喜歡…（商品推播）」、「為您推薦最適合您的內容…（新聞推播）」，達到營利目的；於刑事司法運用上，各縣市警察局透過「犯罪熱點地圖」掌握特定時空的高風險區域，並據此集中配置資源（如巡邏人力、即時影像監控與預防策略），藉使潛在受害者提高警惕，並提高潛在加害者之行為成本，以達預防效果。然而不同於傳統犯罪型態，網路詐欺（Internet fraud/cyber

6 SAS.（n.d.）。Digital audit and investigation: Keys to success for government oversight [White paper]。檢自 2025 年 8 月 25 日，取自 https://www.sas.com/en/whitepapers/digital-audit-investigations-112570.html#formsuccess。

7 Zhyber, T., Pyslytsya, A., Zavystovska, H., Tymchenko, O., & Shchur, R. (2024). Data-Driven Public Budgeting: Business Management Approach and Analytics Methods Algorithmization. In A. Semenov, I. Yepifanova, & J. Kajanová (Eds.), Data-Centric Business and Applications: Modern Trends in Financial and Innovation Data Processes 2023. Volume 2 (pp. 89-124). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-53984-8_5

fraud）的特徵之一，便是犯罪時間和空間上的分離型態（Fisher & Lab, 2010；引自賴擁連等人，2023）[8]。因此監測或通報技術的應對就成為防治網路詐欺之重點。

在犯罪屬性上，調查局《111 年經濟犯罪防制工作年報》[9]指出日益猖獗的電信網路詐欺，如投資詐欺、戀愛詐欺、購物詐欺等新型態網路詐欺犯罪，乃係以簡訊、LINE、Telegram、Facebook、山寨網站、金融交易平臺等方式進行。其中又有五大慣用手法：網路購物詐騙、假投資詐騙、假交友詐騙、騙取金融帳戶詐騙、色情應召詐財詐騙。再根據 165 反詐儀表板的詐騙話術解析[10]，其共通點則以「急迫感」、「高報酬低風險」、「要求匯款或個資」、「語氣樂觀，卻未具體說明產品或服務細節」等，誘騙手法看似持續更新，但大多只是更換標的與敘述方式，手法上仍不脫離：「養、套、殺」與「小額出金」等投資龐氏騙局，或混合數種手法之方式。由此可見，詐欺應有一定的徵兆以得預測。

若進一步將社群媒體（social media）視為資料來源，除因詐欺經常發生於此，又係因其不同於 111 年憲判字第 13 號釋憲案所提

8 賴擁連、蔡田木、陳玉書（2023）。我國網路詐欺被害調查與防制研究（研究成果報告，研究計畫編號：PG112-A-002）。法務部司法官學院委託研究。取自：https://www.cprc.moj.gov.tw/media/20213323/112%E5%B9%B4%E5%A7%94%E8%A8%97%E7%A0%94%E7%A9%B6%E6%A1%88-%E8%B3%B4%E6%93%81%E9%80%A3%E7%AD%89-%E6%88%91%E5%9C%8B%E7%B6%B2%E8%B7%AF%E8%A9%90%E6%AC%BA%E8%A2%AB%E5%AE%B3%E8%AA%BF%E6%9F%A5%E8%88%87%E9%98%B2%E5%88%B6%E7%A0%94%E7%A9%B6.pdf?mediaDL=true

9 法務部調查局（2020）。經濟犯罪防制工作年報。法務部調查局。

10 內政部警政署，165 打詐儀表板，引用日期 2025/08/25，取自：https://165dashboard.tw/

之衛福部「健保資料庫」爭議，超出原始蒐集目的外之利用違反《個人資料保護法》，因此民眾被賦予退出權，且可書面申請個人醫療資料不提供予任何單位二次利用。原因在於，名義上的社群媒體分析資料，多取用於公開來源情資(Open-Source Intelligence, OSINT)，或已事先於社群媒體註冊、使用即授權同意之內容，因此常見資料（如用戶即時位置、搜尋記錄、圖像與影音、消費紀錄、網頁 cookie 等）往往不受被「超出原始蒐集目的」之約束。

正因如此，以社群媒體做為資料來源以進行詐欺案件之犯罪預測，既可能整合當前詐欺犯罪屬性與科技發展趨勢，又具備可分析、試驗的資料來源，在犯罪偵測的應用上值得關注。舉例來說，詐欺案例往往結合時事議題，例如川普就任初期即出現較多川普幣（加密貨幣）的相關詐欺事件，透過偵查社群媒體上詐欺案例的詞彙、議題、手法，乃至事件頻發前的時間差，都可能成為此種預測技術的發展方向。

貳、我國詐欺偵測的應用現況：法規與技術的整合

在臺灣，有關詐欺之規範載於刑法第 339、340 條（詐欺背信及重利罪章），其中，第 339 條第 1 項規定「詐欺取財罪」，通說認為，除主觀上應具不法所有之意圖及犯罪故意外，客觀上則必須行使詐術，使被害人陷於錯誤，並因此交付財物予行為人或第三人始能構成[11]。另外因網路犯罪之行為人係透過廣播電視、電子通訊、網際網路或其他媒介等散布於公眾，則適用刑法第 339 條之 4（加

11 2025，臺灣屏東地方法院 113 年度易字第 866 號刑事判決。

重詐欺罪）。從犯罪預測的角度觀察，在上述構成要件未齊備前，國家能否且如何及早介入，值得關注。

換言之，當施用詐術的行為已現跡象，但尚未有人因此陷於錯誤並受財產損害時，刑法往往難以啟動。此時，「犯罪預測」的意義，即在於行為尚未進入著手階段前，便透過偵測與排除機制，遏止其發展為既（未）遂之詐欺。而政府介入的手段主要有二：其一是刑法介入，待可能被害者出現，若行為人已著手施用詐術，即使尚未造成被害人陷於錯誤與交付財物，仍可依未遂評價而處理（林山田，第 444 頁；引自李進榮，2006）[12]。但若仍屬準備階段、只看見異常徵兆（如可疑帳號、異常投放樣態），而尚未有具體對象施用詐術時，由於因果關係難以舉證，刑法便難以啟動；其二是行政法介入，例如訂定平臺責任、事後廣告審查、通報檢舉與下架機制等，使電信業者、網路平臺業者等，得以在「尚未施用詐術」的準備階段進行預防性管理（李侑宸，2023，頁 47-54）[13]。

隨著《詐欺犯罪危害防制條例》第 31 條第 1 項第 2 款修訂後，規定平臺業者應揭露委託刊播者與出資者之資訊，若平臺業者之廣告服務管理系統出現缺失，則須接受行政處分。可見我國偏向「預防與管理」，而非逕以刑事偵查上之應用。而 2023 年 3 月起，數位

12 李進榮（2006）。論數人參與犯罪之中止（下）。日新法律半年刊，(6)，p115，註 26。https://www.airitilibrary.com/Article/Detail?DocID=P20200604001-200601-202006100011-202006100011-115-127。

13 李侑宸（2023）。後真相時代之假訊息管制結構－以刑法規範為中心。載於法務部司法官學院（主編），刑事政策與犯罪研究論文集（頁 29-60）。法務部司法官學院。https://doi.org/10.6482/ECPCR.202305.0002。

發展部數位產業署運行「詐騙分析與 AI 防詐雷達工具」，其結合人工智慧技術，針對數位平臺（如 Facebook、Instagram、LINE、Google 等）上之資訊進行巨量掃描、比對與詐騙樣態分析，以建立預警模型。該系統可依據近期熱門商品與詐騙常用手法（如短期內大量湧現的虛假商品評價）設定關鍵字，進一步觸發即時自動化通報機制[14]。此一流程涵蓋通報（由民眾、公眾人物與 AI 掃描舉報疑似詐騙訊息）、分案（通報於「網路詐騙通報查詢網」後，自動化分案）、確認（比對既有資料庫）、通知下架（由平臺業者進行預防性下架）」等四個步驟[15]。而社群媒體業者在防制詐欺廣告、下架違法內容、設立法律代表人等義務，性質上主要屬行政規範，行政機關多以罰鍰、限期改善或限制服務等手段進行規範與管理，不涉及刑事範疇。然而本章認為，其中仍可能有部分疑義亟待改善：

一、 分案標準未明、權責不清

目前「網路詐騙通報查詢網」對於受理有詐欺疑義案件之分案標準尚不明確，民眾檢舉相似之可疑貼文，卻出現一案通知金管會，另一案卻通知數發部之情形（圖 4-5-1）。

14 數位發展部. (2024, 3 月 14 日). 數位部開發詐騙分析與 AI 防詐雷達工具 每日找出逾千筆詐騙廣告與電商商品. [新聞稿]. https://moda.gov.tw/press/press-releases/11602。

15 數位發展部數位產業署. (2025, 6 月 12 日). 網路詐騙通報查詢網成效報告. 取用日期：2025/08/25，取自網址：https://www.ocac.gov.tw/OCAC/File/Attach/76669441/File_532270.pdf。

圖 4-5-1　網路詐騙通報查詢網頁頁面

二、 重複審核以致效率低落與判斷不一致

同一日內數個假帳號散布「布蘭特大叔的投資筆記」資訊，縱使審查單位查核了百餘則貼文，但事實上，其內容仍屬同一來源。此情形使得審查單位的檢核資訊效益未必與事務量相當。再者，針對相似的貼文內容，不同部會對於詐騙訊息的認定標準似乎也未一致，因此出現金管會認定「不是詐騙訊息」，而數發部認為「是詐騙訊息」的矛盾（圖 4-5-2）。

圖 4-5-2 「投資粉絲專頁」假帳號頁面

三、 檢測限於表徵，且行政部門鑑別力有限

此問題與第二點相似但仍不同之處在於，所謂施用詐術，係指傳遞與事實不符資訊之行為，包括虛構事實、歪曲或掩飾事實等手段[16]，先前被認為是「詐欺前兆」，如：過度誇大或空洞的承諾[17]、誘導點擊外部連結或加入群組[18]、刻意模糊或缺乏透明資訊

16 2022，臺灣士林地方法院 111 年度易字第 248 號刑事判決。

17 婦幼警察隊。(2024 年 6 月 9 日)。高報酬、零風險、保證獲利。新北市政府警察局婦幼警察隊反詐騙專區。引用日期 2025.09.08，引自網址：https://www.wpb.police.ntpc.gov.tw/cp-3522-116216-30.html](https://www.wpb.police.ntpc.gov.tw/cp-3522-116216-30.html。

18 打擊詐欺指揮中心。(2025 年 6 月 12 日)。打擊數位詐騙訊息 防詐成效卓越。行政院網站。引用日期 2025.09.08。取自網址：https://www.ey.gov.tw/Page/448DE008087A1971/5696578e-0c1f-447d-82b6-d7f1056ba071

[19]，然而社群媒體上的詐術行為，其意圖雖可是以騙取錢財為主，但也涵蓋報復、偏見或仇恨行為等動機[20]。在法條適用上，為避免桎梏言論與表意自由，除非具備相當確信才會進行下架，否則多以「缺乏資訊應對」或「高風險」註記。由於此種標註未必直接影響使用者的瀏覽體驗，故其實際預防效果往往不如通報數量所呈現般顯著（圖 4-5-3、4-5-4）。

圖 4-5-3　詐騙資訊檢測情形一

19 內政部。(2025.01.08)。優惠簡訊是詐騙？！這些訊息要小心！內政部 Facebook。引用日期 2025/09/08，取自網址：https://www.facebook.com/moi.gov.tw/posts/1021063276727372/

20 Apte, M., Palshikar, G. K., & Baskaran, S. (2019). Frauds in Online Social Networks: A Review. In T. Özyer, S. Bakshi, & R. Alhajj (Eds.), Social Networks and Surveillance for Society (pp. 1-18). Springer International Publishing.

圖 4-5-4　詐騙資訊檢測情形二

最後，目前我國之詐欺犯罪預測主要以 Facebook、Instagram、Line、Google、TikTok 等與部分詐騙網站為主。然而，根據社群媒體流量調查[21]，臺灣民眾社群媒體使用習慣依序為 Facebook、Instagram、PTT、Line、Dcard、thread、X，可見現行工具尚未涵蓋部分高度使用平臺。因此如何整合多平臺資訊、同步更新並建立聯防機制，仍是未來亟待精進之處。

參、國外社群媒體犯罪預測之借鏡

如前所述，臺灣詐欺犯罪預測之應用正逐步成形，但仍受限於「技術」（如重複檢索、鑑識能力不齊）及「制度」（如分案標準不清、跨平臺檢核緩慢）種種限制。有鑑於近年許多民主國家強化對社群平臺、電信與支付業者的「預防與移除」義務，以下將從「懲

21 參考 SimilarWeb 近 3 個月對社群媒體網路網站流量統計，引用日期：2025/08/25，取自網址：https://www.similarweb.com/zh-tw/top-websites/computers-electronics-and-technology/social-networks-and-online-communities。

罰密度」、「跨部門聯防」及「資訊同步」三個視角，簡介英國、澳洲及美國如何以治理框架輔助詐欺犯罪預測：

一、懲罰密度

過去許多網路科技巨擘多主張自己僅為資訊中介者，不願介入內容審查。然而英國《網路安全法》（Online Safety Act）引入「看管義務」（duty of care）[22]後，要求平臺對非法內容採取積極措施，包括明確界定並移除不法資訊、打擊網路暴露（cyber-flashing），並針對誤導性資訊進行風險評估與管理。若違反，平臺可能被處以全球年營業額 10%的罰款，甚至勒令停用[23]。雖然英國並未以刑法上「幫助犯」或「共同正犯」追究平臺責任，但依《2023 年金融服務與市場法》（Financial Services and Markets Act 2023），業者對應用程式詐欺須負賠償責任。此種高密度的行政與民事責任，迫使平臺一改被動態度，開始主動投入偵測技術並轉向「積極防範」，此舉顯示了懲罰密度的效果。

澳洲政府則於 2025 年推出全國性的「詐騙預防框架」（Scams Prevention Framework, SPF），旨在強化銀行、電信業者與社群平臺在「預防、偵測與阻斷」[24]詐騙行為上的法律責任。該框架要求金

22 財團法人國防安全研究院. (2022 年 4 月 14 日). 英國新版《網路安全法》強化對網路平台監管權力引發爭議. 取自：https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1601。

23 同前註 22。

24 Treasury. (2025 年 1 月). Scams Prevention Framework – Protecting Australians from scams. 取自：https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf

融服務業需遵守「Scam-Safe Accord」行業守則[25]，實施即時交易警示與收款人身份驗證等措施；電信業者必須封鎖或標註來自未註冊發送者的詐騙簡訊，並參與建立 SMS Sender ID 註冊系統；社群平臺則需驗證廣告主身份並移除假冒廣告。在制度設計上，SPF 違規多以第一、二級民事處罰處理，並輔以其他非懲罰性命令處置[26]（如「立即撤銷」，其被認為是指導而非行政處分）。其特色在強調「一站式協處原則」（No Wrong Door Principle）[27]，指消費者可向任一相關單位提出詐騙申訴，所有涉案方均須共同處理。若業者違反防詐義務導致消費者蒙受損失，消費者可先透過內部申訴程序（Internal Dispute Resolution, IDR）處理。若無法解決，則可轉向澳洲金融申訴管理局（Australian Financial Complaints Authority, AFCA），進入外部爭議處理程序（External Dispute Resolution, EDR），由 AFCA 統一審理並依責任比例裁定賠償。對於未遵守 SPF 規定之業者，最高可處 5,000 萬澳元之罰款。

與英、澳不同，美國在詐欺課責上，傾向於提高詐欺行為的定罪機率，而非直接強制社群平臺承擔法律責任。近年美國實務肯認「欺詐誘導理論」（fraud inducement theory）[28]，即當被告的欺騙行

25 Australian Payments Plus. (2025 年 7 月 2 日). Australian banks launch new defence in battle against scammers. 引用日期 2025/09/03，取自：https://www.auspayplus.com.au/australian-banks-launch-new-defence-in-battle-against-scammers

26 Gibson, J. (2025 年 1 月 24 日). Bills Digest No. 33, 2024-25: Scams Prevention Framework Bill 2024. 取自：https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd033

27 同前註 25。

28 Kousisis v. United States, 82 F.4th 230 (2025). Supreme Court of the United States.

為導致受害者進行原本不會進行的交易時，即構成詐欺，此舉大幅降低了詐欺的舉證門檻。而美國的社群媒體預測詐欺是由聯邦調查局（FBI）轄下之網絡犯罪投訴中心（Internet Crime Complaint Center, IC3）主導，其不主動進行網路偵察（技術監控），而是透過被害者於官網（www.ic3.gov）提交的投訴，進一步進行資料分析與詐欺趨勢識別（如加密貨幣投資詐騙、盜用帳戶詐騙親友，利用虛擬會議與深度偽造技術的商務電子郵件詐欺等）[29]，並將分析報告與其他執法部門共享。此外，IC3 的國家技術團隊，亦引進工程、設計、使用者經驗、數據科學、產品、策略與營運等領域之私部門專業人才[30]，推廣以使用者為中心、迭代式（iterative）、數據驅動（data-driven）的數位技術開發方法[31]，以此強化聯邦機構取得與整合數位證據的能力和執法支援[32]。在責任面上，意圖詐欺者不僅可能面臨民事處罰，美國司法部（DOJ）亦可對其提出刑事訴訟。此模式與臺灣 165 檢舉專線及資策會之 AI 掃描模式最為接近，不過在如灣，雖然詐欺犯罪防制條例已對網路廣告平臺業者的付費廣告設下移除、限制、停權等義務，但對於社群媒體用戶所發佈的非付費平臺原生內容，仍缺乏如英、美等國之明確可操作的刑事標準及規範。

29 Federal Bureau of Investigation. (2022 年 3 月 22 日). 2021 Internet Crime Report. 取自： https://www.ic3.gov/AnnualReport/Reports/2021_ic3report.pdf

30 Sloane, M., Chowdhury, R., Havens, J. C., Lazovich, T., & Rincon Alba, L. C. (2021). AI and Procurement: A Primer. New York University. 取自:https://doi.org/10.17609/bxzf-df18

31 Smith, C., & Soka, S. (2020 年 10 月). Technology, Data, and Design-Enabled Approaches for a More Responsive, Effective Social Safety Net. Beeck Center for Social Impact + Innovation, Georgetown University.

32 同前註 30。

二、跨公私部門聯防

藉由初探英、澳、美國的政策可以發現，單靠檢、警、調或單一主管機關難以全面應對社群媒體詐欺問題。英國以 DCMS 擔任政策與法規制定者，並透過英國通訊管理局（Office of Communications, Ofcom）負責平臺監管與業者義務之落實[33]。如透過《線上安全法》要求各類平臺(如搜尋、社群、聊天)實施風險評估與應對流程，並由英國通訊管理局 Ofcom 執行督導與裁量權[34]。在跨境案件上，英國亦主辦了首屆 Global Fraud Summit（全球詐騙峰會），聚集 G7、五眼聯盟等政府代表，以及 Google、Apple、Amazon 等科技巨擘[35]，藉此提升跨部門的合作意識與效能。

澳洲則由 ACCC 與澳洲國家反詐騙中心（National Anti-Scam Centre, NASC）擔任協調核心，要求銀行、電信與社群平臺業者將接獲的詐騙情資（帳戶、電話號碼、網站等）通報至 ACCC[36]。NASC 再將情資整合並共享至其他業者與執法單位，必要時亦通報國際組織，以即時攔截詐騙活動[37]。此機制結合通報義務、威脅情報交換（如與金融犯罪交換中心合作）、情資整合與警示發布，建構出跨

33 英國「文化、媒體及體育部」宣布了電信管制機關 Ofcom 的改革，資訊工業策進會科技法律研究所，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=5322（最後瀏覽日：2025/09/03）。

34 Department for Science, Innovation & Technology. (2025). Online Safety Act: explainer. 引用日期 2025/09/01，取自：https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

35 華視新聞網. (2024 年 3 月 11 日). 打詐跨國合作成顯學 英澳政府與社群巨頭聯手反詐. 引用日期 2025/09/01，取自：https://news.cts.com.tw/cna/international/202403/202403112297015.html。

36 STLI. (2019, July 4). 澳洲防詐騙框架 (Scams Prevention Framework, SPF) 簡介. 社會科技法律資訊網. https://stli.iii.org.tw/news2019-detail.aspx?d=714&no=57。

37 同前註 36。

產業、跨機關的防詐聯防體系。

而美國早期多採委外協作進行，其將重大網絡事件的事後分析工作委託民間企業，如安永（EY）、普華永道（PwC）和德勤（Deloitte）等[38]。2014 年後，則透過專門化內部機制：美國數位服務局（USDS）等國家團隊，透過引進技術專才，強化政府取得與整合數位證據的能力。

本章觀察到，政府與平臺業者的合作大致可分為兩種情境：（一）積極配合（以防弊為中心）：業者主動識別並防範詐欺；（二）消極配合（以法遵為中心）：業者僅於政府通報異常後才採取行動。例如，FBI 會與銀行、電信業者和社群媒體平臺保持聯繫，以快速凍結資金或移除假冒帳號來因應詐欺。然而，後者的合作往往在異常金流或帳號活動發生之後才啟動，因此難以達成「防患未然」的詐欺預測效果。也因此，美國的合作模式就顯得較為緩慢。而英國政府與監管機構已引入強制補償機制，要求支付服務供應商（Payment Service Provider, PSP）[39]及平臺業者對 APP 詐欺受害人進行補償。此舉促使金融機構與平臺加強互動與資訊交換，並投入更多資源於詐欺預測技術與內部控制機制。澳洲則如前述之《詐騙防制框架》（SPF），透過要求銀行、電信公司與平臺業者採取「合理措施」防範詐騙，這意味著政府鼓勵建立一套跨部門、產業的反詐防線，以促進利害關係人協力對抗詐騙網絡。

38 WHEELER, T. (2018). IN CYBERWAR, THERE ARE NO RULES. Foreign Policy, 230, 34–41. https://www.jstor.org/stable/26535815.

39 資策會科技法律研究所。(2024 年 9 月 23 日)。英國支付系統監管機構打詐新政策一次看。中央通訊社。引用日期：2025/09/11，取自：https://www.cna.com.tw/postwrite/chi/382133

三、資訊同步

在資訊同步與處置程序上，英、澳都強調建立「集中或互通情資中心」，主則協調資訊交換、發布警示與督促業者採取行動（例如下架、封鎖惡意帳號）。實務上，已有平臺與金融機構間的跨域合作模式，例如由聯邦銀行（Commonwealth Bank）、西太平洋銀行（Westpac）、國家銀行（National Australia Bank）及澳盛銀行（ANZ）等多家銀行組成之非營利組織「澳洲金融犯罪交換中心」（Australian Financial Crimes Exchange, AFCX），其與電信業者 Optus 及支付業者 Australian Payments Plus (AP+)合作[40]，建立金融界的情資交換模式，齊力協防詐欺，而 ACCC/Scamwatch 則擔任公告與教育角色，將已確認的詐騙手法公開，以便民眾與業者防範[41]。又英國銀行與 Meta 間的「反詐欺情報互惠計畫」（Fraud Intelligence Reciprocal Exchange, FIRE[42]），也使銀行偵測到的詐騙指標能快速回饋至平臺以即時處置。

相較之下，美國更注重事後的多元通報管道，如平臺內部通報、FBI 網路犯罪投訴中心（IC3）等，且有美國數位服務小組（US Digital

40 國家通訊傳播委員會 (NCC). (2023, August 31). 國際通傳產業動態觀測月報，p22，取自：https://intlfocus.ncc.gov.tw/files/file_pool/1/0n299502363793978811/%E5%9C%8B%E9%9A%9B%E9%80%9A%E5%82%B3%E7%94%A2%E6%A5%AD%E5%8B%95%E6%85%8B%E8%A7%80%E6%B8%AC%E6%9C%88%E5%A0%B12023.08.pdf

41 National Anti-Scam Centre. (2025, June 2). National Anti-Scam Centre calls for stronger business role to disrupt scams. 引用日期 2025/09/01，取自：https://www.nasc.gov.au/news/national-anti-scam-centre-calls-for-stronger-business-role-to-disrupt-scams

42 Meta. (2024, October 2). Meta Partners with UK Banks to Combat Scams. 引用日期 2025/09/01，取自：https://about.fb.com/news/2024/10/meta-partners-with-uk-banks-to-combat-scams/

Service, USDS）作為技術支援單位，在政府內部協助整合系統[43]，加速數位證據的採集與偵辦程序。惟美國作法端視法制框架與合作機制而定，業者「在社群平臺內即時主導處置」或「待民眾通報外部專責中心、由部會檢證後接受處置、指導」，其效率取決於合作框架的成熟度，以及責任界定是否清楚。

肆、結論：建構責任分擔與常態化協防的犯罪預測體系

透過國外經驗顯示，社群媒體內容之分析技術推展，係建構在「多方責任分擔」與「常態化（積極）協防」為基礎：藉由法規強化平臺業者的義務與成本、設立專責中心或跨部門協作機制以確保情資即時整合、並透過技術型單位（如美國 USDS）強化政府數位犯罪偵測量能，不僅能避免因分案或職權模糊造成的責任推諉，也能更暢通的提升異常內容識別與處理效率。反觀臺灣，雖然政府已透過修法逐步強化業者責任，但如何在要求平台業者落實法規治理，又賦予其一定免責條款及自律作為間取得平衡，仍待取得共識[44]。總言之，雖然詐欺犯罪難以完全根除，但透過法規制度之設計，並結合相關技術，仍能在事前預測與阻斷上獲得一定成效。因此，本章所提之「責任配置」、「跨部門合作」與「資訊整合」三個層面，對臺灣在建構防詐與犯罪預測體系上，應有重要啟示。

43 United States Digital Service. (2024). Mission. 引用日期 2025/09/01，取自：https://www.usds.gov/mission

44 國家通訊傳播委員會 (NCC). (2024, July 17). 網際網路傳播政策白皮書專區，取自：https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5705&sn_f=50457

中華民國一一三年犯罪狀況及其分析
2024 犯罪趨勢關鍵報告
編　　者：法務部司法官學院
主　　編：蔡宜家
發 行 人：吳巡龍
出 版 者：法務部司法官學院
地　　址：臺北市大安區辛亥路三段 81 號
電　　話：(02)2733-1047
傳　　真：(02)2377-0171
電子郵件：tsaichia@mail.moj.gov.tw
網　　址：https://www.cprc.moj.gov.tw/1563/1590/1592/45180/post
出版年月：2025 年 12 月初版
定　　價：無

GPN 1011401547
ISBN 978-626-7220-87-0 (PDF)
978-626-7220-86-3 (紙本)
DOI 10.978.6267220/863

電子書播放資訊：
作業格式：Windows OS
檔案格式：PDF
播放軟體：PDF Reader
使用載具：PC