華岡法粹／*Hwa Kang Law Review*
Vol. 76 (2024), pp. 147-202
DOI10.6868/HKLR.202406_(76).05

有效運用人工智慧打擊洗錢犯罪之研究

Research on the Effective Use of Artificial Intelligence to Combat Money Laundering Crimes

楊　暹　黼*
Hsuan-Fu Yang

摘　要

洗錢防制，在洗錢手段日益複雜、資恐金源五花八門，以及科技洗錢手段遍地開花之年代，逐漸成為法律上、政策上之顯學。本文首先地毯式介紹當代洗錢手段之複雜性，並討論晚近透過虛擬貨幣等科技手段，進行不法交易或洗錢之具體情形，從而導引至當代反洗錢法制發展與整合之脈絡。其次，基於洗錢日漸複雜之趨勢，以及人力反洗錢稽核程序之效率低落，論述引進人工智慧防制洗錢之實益，並介紹晚近反洗錢演算法之發展趨勢，以及市面上人工智慧反洗錢方案之推陳出新。再者，新科技之應用絕非一帆風順，本文接續討論人工智慧反洗錢方案可能面臨之困難，其中包括各國尚在發展階段之人工智慧政策差異、資料在地化趨勢對反洗錢系統資料庫整合帶來之障礙，以及數位主權爭議對反洗錢演算法可能帶來之衝擊。

投稿日期：113.02.29　　接受刊登日期：113.04.12　　最後修訂日期：113.04.20
*　國立臺灣大學法律學系碩士生，國立臺灣大學法學士。
Master Student, College of Law, National Taiwan University; LL. B. National Taiwan University.

關鍵詞：洗錢；洗錢防制；科技管制；人工智慧；資料在地化；數位主權

目　次

壹、緒論
貳、洗錢、資恐與防制
　一、洗錢複雜性之各種面向
　二、金融科技時代之洗錢、資恐手段
　三、當代反洗錢行動之開展
參、人工智慧打擊洗錢之潛力
　一、人工智慧之特性與潛能
　二、人工智慧 vs.工人智慧
　三、人工智慧反洗錢技術之現況
肆、國際人工智慧反洗錢方案之挑戰
　一、人工智慧固有爭議與各國政策落差難題
　二、資料在地化政策之負面影響
　三、數位主權、正當法律程序與反洗錢演算法之困境
伍、結論

壹、緒論

根據路透社（Reuters）報導[1]，義大利警方近期破獲一起大規模洗錢案，共逮捕 33 人，其中包括 7 名中國公民。該案中，犯罪者涉及為義大利之黑手黨、毒販等犯罪團體提供洗錢服務，涉案金流高達 5,250 萬歐元。此外，亦從錢騾（money mule）處查獲 1,000 萬歐元之現金，該等人涉及運送非法現金出國。然而，根據羅馬當局之執法單位表示，真正涉案金額絕不僅如此，檯面上可見的數目約僅 20 %。此即典型用以掩飾犯罪所得之洗錢行為樣態。

另根據 CNN 報導[2]，2023 年以巴戰爭中主導巴勒斯坦一方之哈瑪斯（Hamas）政府，涉以加密貨幣為其重要資產來源。以色列執法單位於 2020-23 年間查獲之眾多加密貨幣地址，總價值約達 4,100 萬美元。專家表示，這些軍事激進組織常利用「一次性地址（one-time-use crypto addresses）」收取捐獻，接著再以非法方式轉化為現金，並避免留下交易紀錄。截至目前為止，比特幣（Bitcoin）、以太幣（Ether）、瑞波幣（XRP）、泰達幣（Tether）等加密貨幣，均曾落入前述之資恐用途。此即典型之資助恐怖份子（terrorist financing，下稱資恐）行為樣態。

犯罪者透過掩飾犯罪所得財產之來源，進一步將該等沾染不法之財產重新復歸合法外觀，或使提供非法用途之資金來源無從查知，終焉使合法、非法之財產難以明確區隔，即通常所理解之洗錢（money laundering）行為[3]。洗錢防制最早與美國試圖處理國際銀行之逃漏稅有

1 Emilio Parodi, *Italy police take down Chinese shadow network laundering mafia cash*, *available at* https://www.reuters.com/world/italy-police-take-down-chinese-shadow-network-laundering-mafia-cash-2023-10-04/ (last visited December 12, 2023).

2 Scott Glover, Curt Devine, Majlie de Puy Kamp & Scott Bronstein, '*They*'*re opportunistic and adaptive*'*: How Hamas is using cryptocurrency to raise funds*, *available at* https://edition.cnn.com/2023/10/12/us/hamas-funding-crypto-invs/index.html (last visited December 12, 2023).

3 Michael Levi & Peter Reuter, *Money Laundering*, 34 CRIME & JUST. 289, 290 (2006).

關，其後更成為打擊毒品、走私、賄賂，或抑制資恐之關鍵[4]。此後，反洗錢（anti-money laundering, AML）更延伸到金融機構以外之領域，包括賭場、珠寶交易、車商、保險公司、餐旅業，甚至私營小型店面等[5]，顯見用以漂白不法資金之管道，日漸多元，也使洗錢防制之難度不斷提升。

慮及洗錢逐漸成為橫跨全球之難題，七大工業國組織（Group of 7, G7）於 1989 年峰會發布經濟宣言（Economic Declaration），其中在毒品問題（Drug Issues）段落，宣布召集防制洗錢金融行動工作組織（Financial Action Task Force, FATF），以強化國際協力、評估合作成效，並促進各種洗錢相關預防工作[6]。1990 年，FATF 隨即發布 40 項建議，囊括眾多洗錢防制重要政策建議，其後並不斷更新其建議內容，以因應不斷變化之洗錢手段[7]。

臺灣雖非 FATF 之會員國，惟已在 1997 年加入亞太洗錢防制組織（Asia /Pacific Group on Money Laundering, APG）[8]，並應定期執行會員國間之同儕審查（mutual peer review system）[9]，檢視是否如實遵守 FATF

4 *Id.*

5 舉例而言，瑞士係世界知名之旅遊勝地，同時也因其金融機構安全可信，被視作理想的洗錢王國之一。在反洗錢行動興起時，瑞士甚至要求旅館提供換匯服務者，應留存客戶交易紀錄。*Id.* at 290-291.

6 其提及之方案，包括法律與監管措施之強化、多邊（multilateral）司法互助措施之建立等。*See* G7 Summits, *Economic Declaration*, *available at* http://www.g8.utoronto.ca/summit/1989paris/communique/index.html (last visited December 12, 2023).

7 舉例而言，2019 年之更新版本囊括關於虛擬資產相關之議題，而最近期 2022 年之版本，則與透過秘密的公司結構藏匿非法所得有關。*See* FATF, *History of the FATF*, *available at* https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html (last visited December 12, 2023).

8 邵之雋、李怡萱，人壽保險公司所受洗錢及資恐風險與相應抵減風險措施研究，交大法學評論，第 13 期，頁 126，2023 年 9 月。

9 APG, *FAQ: Mutual Evaluations*, *available at* https://apgml.org/about-us/page.aspx?p=ac38f87e-2341-43e6-84b2-4dbd6346f6c3 (last visited December 12, 2023).

之 40 項建議內容[10]。同儕審查之報告，均公開於 APG 之公開網頁，對各會員國內國政策與法律之決定，具有相當之警惕效果[11]，也具有國際法律整合之事實上作用。

FATF 於 2012 年修正之 40 項建議明確採取風險基礎方法（risk-based approach）後，除傳統以刑事責任加諸洗錢犯罪者外[12]，防範（prevent）與減緩（mitigate）洗錢發生之措施，亦形重要[13]。2016 年著名的兆豐案中，兆豐銀行紐約分行因內控制度不善、客戶身分確認措施（know your customers, KYC）執行不力、其他海外分行之可疑金融行為等故，面臨 1.8 億美元之天價罰則[14]，加以臺灣自 2007 年之 APG 同儕審查中持續得到欠佳成績，一度冷凍在立法院的洗錢防制法，終獲各界重視。2016 年修正理由明確提及，我國向來偏重洗錢之事後刑事制裁，卻忽略事前防範措施[15]，故修法除擴大並明確化洗錢定義外，更強化相關之事前防範措施與主管機關之查核權限，以銜接國際標準[16]。

金管會為貫徹洗錢防制作業，更依據洗錢防制法制定諸多「洗錢防制及打擊資恐辦法」之法規命令，其執行內容包括應執行客戶身分確認

10 至於 APG 與 FATF 之關係，前者為後者之準會員（associate member），得參與後者之各大重要集會，並據此影響相關政策之討論與制定。APG, *Relationship to the FATF*, *available at* https://apgml.org/about-us/page.aspx?p=52e840ea-0599-4c85-9424-1abd272ba9f3 (last visited December 12, 2023).

11 以我國為例，近期關於洗錢防制法之各項修正，與 APG 相互評鑑之結果有相當之關聯性，可見評鑑機制之警惕作用。請參見林鈺雄，普通洗錢罪之行為類型－評析洗防法第 2 條，月旦法學教室，第 224 期，頁 36-37，2021 年 6 月。

12 FATF, 40 RECOMMENDATIONS 3-4 (2003).

13 FATF, FATF RECOMMENDATIONS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 11 (2012).

14 參見林志潔，兆豐案天價罰款的啟示－美國反洗錢法的重點與金融業應有的作為，月旦法學雜誌，第 259 期，頁 36，2016 年 11 月。

15 請參見張明偉，論洗錢防制，軍法專刊，第 68 卷，第 4 期，頁 12，2022 年 8 月。

16 不過，洗錢防制法第 2 條關於洗錢行為之定義，向來受到刑法學者不少批評，例如單純移植國際文件而未充分進行理論思辨、對國際文件之理解有誤等。請參見林鈺雄，同註 11，頁 37；同前註，頁 12。

措施、拒絕與符合特定條件客戶之交易往來、持續風險審查機制、實質受益人之確認、可疑交易之紀錄等[17]。固然，在積極的法制建構下，我國終擺脫陰霾，在 2019 年在 APG 第三輪評鑑中躍升「一般追蹤」等級，成為亞太國家中成效最佳者[18]，惟實務上繁瑣之洗錢防制確認程序、日益困難之開戶作業，實際上卻經常招致民眾反感情緒[19]。箇中原因，往往出在洗錢手法日漸複雜，而風險基礎方法確實有造成偽陽性（false positive）回報之可能[20]，勢必使遭受「關切」的客戶感到莫名奇妙。

然而，偽陽性之問題不僅出在客戶觀感之下降，銀行防制洗錢資源分配欠佳係更嚴重之隱憂。反洗錢業務在各大金融行業開展後，銀行莫不挹注大量資源因應潛在犯罪，惟若因偽陽性回報而耗費勞力、時間、費用，調查無辜的低風險帳戶，不啻為防範資源之浪費。此外，資料搜集之不完善、回報標準不一、作業流程之缺失，均可能導致銀行莫名浪費大量資源，卻無從奈何洗錢犯罪[21]。

近年來，人工智慧（Artificial Intelligence）的快速進展，已使其足以擔綱不少人類能力無法企及之工作，特別在涉及大量資料之搜集、基

17 例如：金融機構防制洗錢辦法各條之規範。近期最受矚目之行政法規，則如領先國際標準之「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」。簡要介紹，請參見楊岳平，虛擬通貨的洗錢防制監管疆域與國際標準－評我國「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」，法律扶助與社會，第 9 期，頁 100-104，2022 年 9 月。

18 請參見行政院，第 3 輪洗錢防制評鑑　台灣獲佳績－金流透明　世界好評，https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/bdf44d9a-f4f0-43aa-99f2-771f612983ac（最後瀏覽日期：2023 年 12 月 4 日）。

19 請參見法務部，洗錢防制不是在擾民，https://www.moj.gov.tw/media/14695/1651812311852055e8.pdf?mediaDL=true（最後瀏覽日期：2023 年 12 月 4 日）。*See also* Levi & Reuter, *supra* note 3, at 293.

20 *See* Stuart Breslow, Mikael Hagstroem, Daniel Mikkelsen & Kate Robu, *The new frontier in anti-money laundering*, *McKinsey & Company*, *available at* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-new-frontier-in-anti-money-laundering (last visited December 8, 2023).

21 *Id.*

於既存資料之精確判斷等領域，其工作效能具有不少過人之處[22]。進而，業界已開始嘗試使用人工智慧從事洗錢或資恐防制偵測工作，力主其強大之洞察力與事件分類能力，足資判斷極為複雜之交易，進而揪出背後藏鏡之人[23]。

本文認為，基於洗錢或資恐行為之複雜性日益增長，傳統以人力層層把關的防制手段，已經不合時宜。又適逢金融科技崛起之時代，許多交易轉往線上、虛擬環境，加深洗錢或資恐防制之困難性，更屬人力防制所難以跟進之領域。據此，本文擬從洗錢行為之複雜性及其晚近之演變出發，討論人工智慧介入之實益，同時盤點現實上可能遭遇之阻力。本文論述架構如下：第貳部分，詳論洗錢之發展、執法之困難與法律上因應；第參部分，探討人工智慧具體運作、能夠解決之問題，以及當代技術之進展；第肆部分，提出當前運用人工智慧防制洗錢之困境所在，第伍部分則為結論。

貳、洗錢、資恐與防制

一、洗錢複雜性之各種面向

洗錢，通常認為係緣起於犯罪的果實－不法所得[24]。其植基於各種類型之前置犯罪[25]，如販毒集團（drug cartel），透過出售在多數國家均屬違禁物之毒品，獲取高額利潤。另者，緒論所介紹之資恐行為，係指發起恐怖攻擊之組織，透過各種合法或非法之管道，獲取金錢或其他財

22 *See generally* Karni A. Chagal-Feferkorn, *How Can I Tell if My Algorithm Was Reasonable?*, 27 MICH.TECH. L. REV. 213, 250-259 (2021).

23 胡　林，AI 超譯資料：Ayasdi、SAS 防洗錢揪出金融詐欺師，能力雜誌，第 767 期，頁 52-55，2020 年 1 月。

24 Levi & Reuter, *supra* note 3, at 311; Peter Alldridge, *Money Laundering and Globalization*, 35 J.L. & SOC'Y 437, 437 (2008).

25 Levi & Reuter, *supra* note 3, at 311.

產[26]，以支應其運作、宣傳、購買武器等基本開銷[27]，並轉化為具體之恐怖攻擊風險[28]。

傳統上，經常採取三階段理論觀察與解釋洗錢行為：即處置（placement）、分層（layering）、整合（integration）。處置，係將系爭財產引入金融體系中，其媒介可能為現金，亦可能透過其他更複雜之財產佈局。分層，係將系爭財產與其犯罪之來源隔絕，例如在不同銀行間連續轉帳。整合，則係將該不法財產再度引入日常金融或商業交易體系，與其真實來源分道揚鑣[29]，如設立境外公司，或使用國際金融體系多層移轉財產，均屬常見[30]。

固然，三階段之觀察法具有簡化討論之實益，惟當代洗錢手法愈趨複雜，許多洗錢手段或具備更多階段之構造，或不必然兼具前述三個階段中每一階段[31]。此外，資恐行為係傳統洗錢定義之變體，蓋其財產之來源未必不法，惟財產之用途卻多有違法之嫌，與傳統之「黑錢漂白」有所不同。有鑒於當代背景物換星移，洗錢之複雜性，尚有進一步剖析之必要。

（一）洗錢手段之多元性

洗錢之核心目的，在於掩蓋系爭財產之來源。能夠達成此一目標之

---

26 FATF, TERRORIST FINANCING RISK ASSESSMENT GUIDANCE 9 (2019).

27 關於恐怖組織之資金如何運用，*See generally* FATF, EMERGING TERRORIST FINANCING RISKS 9-10 (2015).

28 FATF, *supra* note 26, at 9.

29 Levi & Reuter, *supra* note 3, at 311; Jack A. Blum, Michael Levi, R. T. Naylor & Phil Williams, *Financial Havens, Banking Secrecy and Money Laundering*, 4 TRENDS ORG. CRIME 68, 69 (1999).

30 早期有學說認為，洗錢表面看似複雜，但背後多係基於類似的結構（structure）。*See* Blum, Levi, Naylor & Williams, *Id.* 不過，此見解不一定適用於當代之洗錢，請參本文後述。

31 Levi & Reuter, *supra* note 3, at 311-312. 國內則有從犯罪學與刑法理論之角度，檢討三階理論之合理性者。請參見林鈺雄，同註 11，頁 41-42。

手段，不勝枚舉。舉凡境外資產之管轄限制、商業組織可匿名之性質、律師之秘匿特權、銀行之保密義務等[32]，均屬法律上可利用之工具。具體掩飾手段，諸如購買易攜帶之高單價物品（珠寶、藝術品等[33]）、保險、不動產交易、複雜的金融交易，皆有可能[34]。直接僱請專人將大量現金運送出國，在有陸地接壤之國界之間，亦時有所見，緒論提及之錢騾即是。此外，即便是稀鬆平常之生活交易，如頻繁購買價值極小之物品以獲取找零、向蔬果商買取食材等，背後亦相當機率藏有洗錢行為[35]。

商業上常見手法，即試圖利用前述商業組織之可匿名特性，設立空殼公司（shell companies），以脫免法律對受益所有人（beneficial owner）之控制責任追訴，並巧妙規避針對前置犯罪或洗錢行為之法律執行[36]。據研究，空殼公司多半雖係為合法用途而設（如：控股公司），惟亦有顯著之案例涉及嚴重犯罪行為[37]。其成功掩飾金錢來源之關鍵，其一在

32 Blum, Levi, Naylor & Williams, *supra* note 29, at 442.

33 關於藝術品之非法交易可能涉及洗錢之問題，近期受到國內外學者之關注。藝術品交易市場通常具有相當程度之隱密性，蓋其收藏價值通常極為高昂，收藏者多不願公開自己身分，否則或可能莫名受到大眾關注。*See generally* Derek Fincham, *Art, Antiquities, and Money Laundering*, 111 KY. L.J. 309, 314-322 (2022). 作者之理解亦相同，蓋作者曾涉獵國際古董樂器交易市場，發現真正有名之收藏品不見得會在公開之拍賣會上出現，交易更可能係在檯面下完成，而知名收藏標的物現時之所有人，經常不得而知。此情形下，相關交易人員之背景、金流來源、藝術品是否為贓物等，均可能處於保密狀態，或難免成為洗錢者之老巢。國內文獻，請參見蔣念祖，藝術品拍賣業該管了－如何填補洗錢防制漏洞之探討，當代法律，第 9 期，頁 140 以下，2022 年 9 月。此外，該文並提及關於 NFT 虛擬收藏品之問題。

34 Levi & Reuter, *supra* note 3, at 312-314.

35 *Id*. at 317.

36 MICHAEL FINDLEY, DANIEL NIELSON & JASON SHARMAN, GLOBAL SHELL GAMES: TESTING MONEY LAUNDERERS' AND TERRORIST FINANCIERS' ACCESS TO SHELL COMPANIES 5 (2012).

37 舉例而言，有透過在紐西蘭之空殼公司出租飛機予軍火商，並運送軍火至北韓者。亦有幾內亞之政治人物，透過在美國之空殼公司洗清其貪污所得。伊朗政府曾運用在德國、馬爾他等國之空殼公司，規避國際石油禁運。美國公民不時

內國警力受管轄權之限制，一旦公司位於海外，或受益所有人非本國居民，執法即生障礙。其二，各國公司註冊之文件所能揭露之資訊有限，多無法輕易追溯至受益所有人之階層，使執法對象之特定更顯困難[38]。

透過專業人士協助洗錢，亦具相當顯著性。傳統上，洗錢行為人透過金融機構之內部人裡應外合，忒為簡潔有力，其通常以脅迫、利誘或欺騙手段，達成控制內部人之目標。某些情形，協助洗錢之人甚或對自己淪為滲透端點一事，毫無所悉。此外，律師或會計師，亦係幫助洗錢之絕佳人選。透過專業人士，行為人能更順暢地設置空殼公司或商業組織、設置信託、執行特殊交易等。面臨執法單位調查時，律師則可能透過秘匿特權之主張，協助洗錢之人掩飾罪行[39]。

由技術角度以觀，洗錢手段模型可略分類為數類：1. 路徑式（path），透過多個洗錢中介（money laundering agent）串連交易，掩蓋金錢來源。2. 迴圈式（cycle），由單一洗錢中介製造極大量之交易，惟該等交易可能回流於同一洗錢中介本身。3. 拆分式（smurf），將一筆金額細分為不易引發注意的小單位，並存入多家不同金融機構[40]。此外，尚有 4. 動態模式（dynamic scheme），即隨時、隨機組合、替換各種洗錢模式，且併用多種金融工具[41]，造成追查門檻之提升。

透過設立境外空殼公司，以逃避政府稅收。甚至，有俄羅斯軍火商利用美國之空殼公司從事資恐活動。*Id.* at 7-8.

38 *Id.* at 9.

39 以臺灣法為例，釋憲實務即基於辯護人之溝通權、被告之防禦權等重要角度，肯認刑事搜索程序應將涉及辯護人之情形區別規定，以保障律師之工作權與被告之訴訟權。請參見憲法法庭 112 年憲判字第 9 號判決。

40 Olmer Garcia-Bedoya, Oscar Granados & José Cardozo Burgos, *AI against Money Laundering Networks: The Colombian Case*, 24 J. MONEY LAUNDERING CONTROL. 49, 54-55 (2021).

41 *Id.* at 55.

（二）資恐金源之分散性

資恐為洗錢之變體，已如前述。然此型態之下，尚得再粗略分為多種金錢取得管道，顯見恐怖組織之金源正在開枝散葉。根據 FATF 2015 年之資料，在美國進入法律程序之洗錢案件，約 33 %之金流來自個人捐獻，極為顯著。其次，利用非營利組織（non-profit organizations, NPOs）募集資金[42]，並濫用監管漏洞實際取得財產，亦非罕見。再者，參與犯罪活動得利，例如走私違禁物、搶劫銀行、稅務不法行為、詐領保險金、勒索企業、擄人勒贖，均曾發生。當然，資恐金源亦可能完全合法，例如設立公司並經營合法業務之收入[43]。

至於獲利後之財產移轉過程（相當於分層化、整合），多仍利用金融系統之複雜換匯、設立空殼公司等手段，隱匿確切資產來源。亦有透過掮客跨國運送現金者，另有結合金融系統與物理方法者，如在某國開戶存款後，再由他國車手提領之[44]。簡言之，除金錢交換過程如同傳統洗錢般複雜以外，資恐另有特殊之處－財產用途集中，惟來源廣泛，此與傳統洗錢近乎相反。其斂財管道遍佈全球，資恐行為之複雜性有增無減。

（三）前置犯罪之複雜性及其與洗錢樣態之關聯

除洗錢本身手段外，前置犯罪之複雜性，亦與洗錢環環相扣，可能增添執法之困難度。據研究，前置犯罪中有超過 70 %之行為包括販毒、

42 關於濫用非營利組織之最新報告文件，*See* FATF, BEST PRACTICES ON COMBATING THE ABUSE OF NON-PROFIT ORGANISATIONS 6 (2023). 學術研究，*See also* Charanjit Singh & Wangwei Lin, *Can Artificial Intelligence, RegTech and CharityTech Provide Effective Solutions for Anti-Money Laundering and Counter-Terror Financing Initiatives in Charitable Fundraising*, 24 J. MONEY LAUNDERING CONTROL. 464, 472 (2021).

43 FATF, *supra* note 27, at 13-19.

44 *Id.* at 20-23.

詐欺、走私[45]。除此之外，亦囊括人口販運、貪污、逃漏稅、賄賂等[46]。當然，恐怖攻擊亦屬洗錢相關之犯罪，只不過概念上非屬「前置」。

舉例而言，毒販通常由其下線層層轉賣毒品，因此毒品交易中常出現極大額現金，且在毒品市場持續存有需求之前提下，入帳源源不絕。相形之下，人口販運涉及之金流明顯較少，一方面在工業革命後客觀人力需求已下降，另方面人口販運或中介商之獲利模式通常係「抽成」，故涉及洗錢之帳目原則上僅包括淨利（net revenue），而非如毒品市場之總收入（gross revenue）[47]。執法層面以觀，不合理大額交易之風險回報模式，雖可能對毒販有效，卻無法完全抑制人口販運。相同邏輯，資恐通常積少成多，單筆捐獻數額或許微小，卻能匯聚足以發動恐攻之金額，惟此等小額捐獻，或不見得會被認定為高風險交易。

其他特色類型，又如白領犯罪（white-collar crimes，可能包括貪污、詐欺、逃稅等類型）中，洗錢多直接內化為前置犯罪之一部。例如設立空殼公司逃稅，其逃稅過程本身，已經與洗錢行為近乎合一[48]。又如詐欺犯罪，或在行為人使被害人陷入錯誤給付財產時，所指定之給付對象已為安排好之人頭帳戶[49]，則前置犯罪與洗錢行為亦生部分重疊。這類情形，洗錢與前置犯罪之重疊性，可能迫使洗錢行為人從事更進一步之財產安置，否則易成執法機構之目標。研究指出，在貪腐類型之前置犯罪後，行為人通常更傾向將資產移轉出國[50]，增添跨境屏障，此與特定之政治性考量有關。

綜合而言，固然在晚近學說中，洗錢已被肯認係前置犯罪以外之別

45 Levi & Reuter, *supra* note 3, at 314.
46 *Id.* at 323.
47 *Id.* at 323-324.
48 *Id.* at 324-325.
49 關於提供人頭帳戶可能涉犯洗錢罪之介紹，請參見吳俊志，洗錢防制法修法對人頭帳戶的影響，月旦財稅法令，第 46 卷，第 18 期，頁 9-11，2023 年 9 月。
50 Levi & Reuter, *supra* note 3, at 325.

一犯罪[51]，且本身亦發展出眾多類型，惟實際上不僅與前置犯罪之類型有所牽連，甚因前置犯罪本身特性使然，直接或間接影響後續洗錢之手段，從而為反洗錢行動再添變數。

二、金融科技時代之洗錢、資恐手段

（一）虛擬貨幣與犯罪－以絲綢之路爲例

絲綢之路（Silk Road）係日前惡名昭彰之購物網站，以販賣違禁物為主要業務。其首腦 Ross William Ulbricht 在 2013 年以公眾責任（public liability）為由遭加州警方逮捕，嗣聯邦調查局（Federal Bureau of Investigation, FBI）扣押其個人電腦，並查獲其在絲綢之路上擁有之帳號“Dread Pirate Roberts”，及其為該網站擁有者等事實[52]，其後接連扣押相關伺服器主機，並關閉網頁。

絲綢之路主要建構在 Tor 網路上（即俗稱之暗網，dark web），基於該種通訊協定，使用者享有極高匿名性，蓋 Tor 之技術能使資訊傳送、接收者之 IP 位址不易為他人查知[53]。該非法購物網頁介面與 eBay 極為相似，惟依聯邦政府之調查，其不僅販賣冰毒、迷幻藥（LSD）等禁藥，甚提供盜取信用卡之教學、兒童色情、付費委任謀殺等不法服務[54]。

於絲綢之路購買商品或服務者，須以比特幣交易。比特幣用戶一旦自兌幣器（exchanger）獲致虛擬貨幣後，可將之存放於匿名錢包中。一個比特幣錢包可擁有超過一個地址（address），各別發揮類同銀行帳戶之作用。有權存取錢包內之比特幣並進行轉帳交易者，僅限擁有私鑰

51 傳統爭議，*See Id.* at 291.

52 United States v. Ulbricht, 858 F.3d 71, 82-84 (2d Cir. 2017).

53 Carmine DiPiero, *Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web*, 2017 U. ILL. L. REV. 1267, 1273-1274, 1279 (2017).

54 *See Id.* at 1275.

（private key）之人。比特幣交易，全數記載於區塊鏈（Blockchain）之分散式帳本上，且每筆交易均能在公開網站上查知[55]。不過，帳本僅會顯示移轉金流，並不反映從事交易者之身分[56]，且可能因使用 Tor 瀏覽器再加強身分之隱匿，整體仍有相當程度之匿名性[57]。顧客將比特幣轉入屬於絲綢之路之錢包地址，即能購買商品。簡言之，絲綢之路基於比特幣交易之匿名性，作斂取犯罪所得之用。

在不法交易的世界，絲綢之路僅為冰山一角。透過暗網進行之交易，涉及犯罪行為者不能勝數，而 Tor 瀏覽器、虛擬貨幣恰成為行為人之盾牌。研究指出，暗網交易基本上均能採用比特幣支付[58]，其匿名性為非法交易所重用。即便在絲綢之路遭強制關站後，暗網交易市場仍持續擴大，且包含數量更多、品項愈趨複雜之毒品等違禁物交易[59]。以洗錢行為階段之觀點，前置犯罪與財產取得等行為，於此均已具備。

---

55 Blockchain.com, *available at* https://www.blockchain.com/explorer (last visited December 6, 2023).

56 國內文獻有提及，交易者之 IP 位址請係有可能查知的。參見魏至潔，世界金流新秩序－FATF 虛擬資產規範及我國法制面整體建議，交大法學評論，第 12 期，頁 171，2023 年 3 月。

57 嚴格而言，匿名性仍有一定極限，蓋區塊鏈紀錄非無可能成為逆向追蹤的基礎。其他如網站登入紀錄、網站本身所使用的 Javascript、Adobe Flash 插件，均有可能繞過 Tor 留下足跡。不過，本案執法機關主要是依據 Google 帳號對外部網頁之連結追蹤主嫌，尚非透過鏈上紀錄逆向追蹤，或許此追蹤方法仍有其特別複雜處。*See* Kyle Swan, *Onion Routing and Tor*, 1 GEO. L. TECH. REV. 110, 116-118 (2016).

58 Sophia Dastagir Vogt, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 SANTA CLARA J. INT'L L. 104, 104 (2017).

59 DiPiero, *supra* note 53, at 1278-1282. 有量化研究顯示，暗網上可能有超過半數之交易均屬非法。*See* Rolf van Wegberg, Jan-Jaap Oerlemans & Oskar van Deventer, *Bitcoin Money Laundering: Mixed Results?: An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin*, 25 J. FIN. CRIME 419, 421 (2018).

（二）虛擬貨幣之洗錢手段

早在 2015 年 6 月，FATF 發布之報告中便提及虛擬貨幣可能產生之洗錢與資恐風險[60]。具體而言，其已意識到虛擬貨幣基於區塊鏈運作之去中心化特性，並指出交易者可利用 Tor 隱藏身分，甚提及各種可能涉及洗錢之匿名化措施，例如 Bitmixer, Sharedcoin, Bitlaunder, Easycoin 等混幣器（mixer）服務[61]。該服務可能由獨立之軟體開發商，或由錢包服務商本身所提供[62]。2021 年之報告中，FATF 針對虛擬資產洗錢風險管控提出建議，明確將混幣器等匿名化措施認定為高風險之服務類型，建議主管機關應加強監督[63]，並列入虛擬資產之紅旗指標中（red-flag indicator，象徵高風險交易之指標）[64]。

比特幣係基於去中心化、點對點之交易方法，原則上並不經過類似銀行之中介服務，僅存在於交易兩方之間[65]。透過比特幣進行非法交易、移轉犯罪所得，雖有一定程度之匿名性，惟技術上，透過每筆金流之逆向追蹤，仍可能溯源（link back）查出幕後黑手[66]。混幣器即為打破此一交易連結所由生，其目的在於斷開真實金流來源，使無法查知[67]。洗錢用途上，恰能用以掩飾犯罪所得。

常見之混幣器運作方式，係由服務者對使用者提供一個錢包地址，由使用者先將其虛擬貨幣輸入（input）該地址，再由服務者將不同之虛擬貨幣輸出（output）往該使用者之地址。惟首要弱點在於，一旦服務

60 FATF, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL CURRENCIES 3 (2015).
61 *Id.* at 27-28.
62 *Id.* at 30.
63 FATF, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 72 (2021).
64 *Id.* at 88. 關於數位資產之反洗錢指引，請參本文後述。
65 van Wegberg, Oerlemans & van Deventer, *supra* note 59, at 422.
66 *Id.* at 423.
67 *Id.*

者所提供之地址有所重複，金流可能仍易追溯發現。因此，服務者通常會為每一個使用者生成不同之輸入地址，並允許使用者指定多個輸出地址，使過程更加複雜[68]。

混幣器服務者通常擁有資金池（pool），以混合眾多使用者提供之虛擬貨幣，並確保混合後再輸出之比特幣，與該使用者所輸入者完全迥異[69]，以繞過回溯追蹤。實際混和手段，得由交易量、交易時間等可能被公開查閱之資訊下手。例如，服務者對每一位使用者課以不同數額之使用費（mixing fee），使交易金額混亂化。又如，服務者使輸入、輸出資金池之時間產生延遲（mixing delays），造成交易時間互相交錯，以增加資訊複雜度[70]。這些變數之配置，通常係由服務商隨機安排（randomized），惟亦有部分系統開放使用者客製選擇各種變數[71]。

值得注意者係，晚近已開始有實證研究針對混幣器之匿名實效進行分析[72]。現存之混幣服務中，有成效卓越者，其輸出之金額恰好等於輸入金額減去服務費用，相當於 100 %混合成功。惟亦有效能堪慮者，例如在不同服務中提供了相同地址，使匿名性毀於一旦。此外，使用者之行為本身，仍可能影響匿名措施之成效，例如未使用 Tor 瀏覽器、將同一地址重複使用於不同交易中、不慎向交易對象提供聯絡資訊等[73]，均使功虧一簣。

整體而言，晚近研究指出混幣器不僅有被用以洗錢之風險，甚提供

68 Jaswant Pakki, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao & Adam Doupé, *Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask)*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 25TH INTERNATIONAL CONFERENCE 4 (2021).

69 van Wegberg, Oerlemans & van Deventer, *supra* note 59, at 424.

70 Pakki, Shoshitaishvili, Wang, Bao & Doupé, *supra* note 68, at 4.

71 *Id.*

72 *See e.g.* van Wegberg, Oerlemans & van Deventer, *supra* note 59, at 424-432; Pakki, Shoshitaishvili, Wang, Bao & Doupé, *supra* note 68, at 7-21.

73 van Wegberg, Oerlemans & van Deventer, *supra* note 59, at 430.

了積極降低洗錢之成本之益處，政府應推出相關之執法配套措施，如比特幣錢包之扣押等[74]，以因應未來挑戰。固然另有研究指出，部分混幣器之使用者，本非為洗錢目的，純粹係為提升使用上之匿名性[75]，惟不論如何，FATF 已將使用混幣器視為高風險行為，且實務上虛擬貨幣確實遭用於各種不法交易，此技術勢將構成洗錢防制之當代課題。

三、當代反洗錢行動之開展

（一）國際反洗錢法體系

國際上最早關於洗錢防制之法律，可追溯至 1970 年代之美國法。當時，該國之銀行秘密法案（Bank Secrecy Act, BSA）要求銀行就單筆現金交易價值超過 10,000 美元者，應向聯邦財政部（Department of the Treasury）回報，以避免外國銀行掩飾其逃稅行為[76]。接踵而來者係 1986 年之洗錢防制法（Money Laundering Control Act of 1986），旨在打擊美國國內之販毒團體[77]，此後聯邦政府積極取締未依法回報之銀行，於焉金融界逐漸形成自願回報之慣習[78]。除美國以外，加拿大、澳大利亞等國均開始要求銀行提供更多資料，而奧地利、德國、列支敦士登、瑞士等國則係以可疑交易報告循線調查前置刑事案件，其通常先暫時凍結相關銀行帳號，再決定是否開啟洗錢調查[79]。

國際間正式反洗錢合作之序章，始於 1989 年之 G7 會議。該年度

74 *Id.* at 431.

75 Pakki, Shoshitaishvili, Wang, Bao & Doupé, *supra* note 68, at 21.

76 Levi & Reuter, *supra* note 3, at 296.

77 蓋當時許多毒販試圖攜帶少於 10,000 美元之現金進出銀行，以規避 BSA 之適用。*Id.*

78 *Id.*

79 *Id.* at 304. 美國、英國、澳大利亞、瑞士等國傳統之洗錢管制理由、手段等背景，均有不同，也使其早期原始規範呈現不同風貌。*See Id.* at 304-306.

峰會中發布了一份經濟宣言，並基於打擊國際毒品買賣之初衷，宣布召集 FATF，成為首個國際反洗錢政府間組織。FATF 嗣於 1990 年代開始推出關於反洗錢政策之「40 項建議」，並持續因應時代變化更新內容[80]。該等建議雖無法律上拘束力，事實上卻成為各國政策之重要導引，蓋無論 FATF 之會員國，抑或與之有間接關係的地區性組織（regional bodies，如緒論提及之 APG），均應透過同儕審查制度，彼此檢視內國反洗錢政策與 40 項建議之相容性。評分結果不善之國家將被公開揭露，形成一種公開羞辱（name and shame）之壓力，迫使成效不彰之國家迅速修正內國規範[81]。不僅如此，在國際金融領域具有影響力之組織－如世界銀行（World Bank）、國際貨幣基金（International Monetary Fund, IMF）均開始採用 FATF 之標準[82]，更使影響力無遠弗屆。

2012 年起，FATF 之 40 項建議修訂版正式採納風險基礎方法（risk-based approach, RBA），其核心目標在於透過識別（identify）、評估（assess）、理解（understand）洗錢與資恐之風險，以妥適分配相關防制資源，達到減緩及預防之目標[83]。據此，針對風險較為顯著之情形，內國政府應採取相當程度之管制措施；風險相對較低之情形，則得採用簡化手段[84]。具體而言，事前之客戶身分確認措施（customer due diligence, CDD, or know your customer, KYC）、重要交易資料之留存、特殊類型客戶之風險評估[85]、可疑交易之回報、法人受益所有人之揭露、主管機關之監督、國際法律互助，均屬風險基礎方法之核心實踐。各該義務之主

80 *See* FATF, *supra* note 7.

81 Levi & Reuter, *supra* note 3, at 306.

82 *Id.* at 307.

83 關於風險基礎方法之細部法律解釋，包括風險評估之定義、高風險與低風險之界定、例外情形，*See generally* FATF, *supra* note 13, at 31-33.

84 *Id.* at 11.

85 如重要政治性職務者（politically exposed persons, PEPs）、通匯銀行（correspondent banking）、新科技相關（new technologies）、涉及高風險國家等。*Id.* at 16-19.

要適用對象，包括金融機構與指定之非金融事業或人員（designated non-financial businesses and professions, DNFBPs）。

晚近金融科技興起，前述透過虛擬貨幣及其相關服務洗錢之風險，為 FATF 所關注並採納。具體而言，2023 年 6 月更新版 40 項建議之 15.3 項以下，明確採納虛擬資產（visual assets）概念，並將虛擬資產服務提供者（visual asset service providers, VASPs）納入管制範圍。虛擬資產與提供者適用之措施，包括 1. VASPs 原則上應採核准或註冊制（15.4）、2. 主管機關之監督（15.6）、3. VASPs 未遵守規定之制裁（15.8）、4. 準用第 10-21 項之各項預防措施（15.9）[86]。易言之，虛擬資產基本上適用所有針對傳統金融機構之監管措施。前揭指引，短期內是否再因科技進展而生變動，亦值得觀察。

（二）我國法反洗錢規範之困境、變革與缺憾

我國洗錢防制法最早於 1996 年公布施行，曾為亞洲首部洗錢防制專法[87]，立法過程主要參考美、德、英三國之洗錢防制專法。其後之重要修法，包括 2003 年修正洗錢定義、前置犯罪範圍與刑責規範，以符合 FATF 1996 年修訂版 40 項建議之要求。2007 年之全文修正，則包括更新前置犯罪樣態、落實資恐行為之入罪化、增訂打擊資恐相關刑事程序之規範等[88]。

前述修正多屬漸進式改善，然事實上我國之洗錢防制規範早已漸趨無力。自 2007 年 APG 第二輪評鑑以降，我國洗錢防制表現差強人意，加以 2016 年兆豐案爆發，顯示金融機構之內控內稽制度、CDD 等重要反洗錢事項執行不力，終於促成 2016 年之全面修正。新法不再囿於行

86 FATF, FATF METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS 53-55 (2023).

87 王志誠，洗錢防制法之發展趨勢－金融機構執行洗錢防制之實務問題，月旦法學雜誌，第 267 期，頁 7，2017 年 8 月。

88 請參見張明偉，同註 15，頁 4-10。

為後階段之刑事追訴，而係同步落實前階段之預防措施[89]。

依現行法律，洗錢之定義（洗防法第 2 條）基本呈現三階理論之構造，即－第 1 款處置、第 2 款分層、第 3 款整合[90]。所謂之犯罪所得（洗防法第 4 條第 1 項）係指前置犯罪（洗防法第 3 條）所變得之財物、財產上利益或孳息，且犯罪所得之認定不以經有罪判決為必要。各種金融機構、辦理融資性租賃者、虛擬通貨業者，原則上均適用洗錢防制法（第 5 條第 1、2 項）。金融機構以外之專業人員經列舉者（第 5 條第 3 項），亦適用之。適用本法之各該主體應採取之預防措施，包括內控內稽制度之建立（第 6 條）、風險基礎方法之 CDD 與特殊類型客戶之審查（第 7 條）、大額交易之申報（第 9 條）、紅旗行為之申報（第 10 條）、針對高風險國家之特別措施（第 11 條）、海關措施（第 12 條）、凍結帳戶（第 13 條），同法並設有罰則（第 14 條以下）。

根據本法各條之授權規定訂定之法規命令，屬於金融類者包括「金融機構、銀行業、農業金融機構、保險公司、金融科技創新實驗、特定財團法人、虛擬通貨平台及交易業務事業等」防制洗錢及資恐之辦法，指定之非金融事業專業人員則包括「律師、會計師、公證人、地政士與不動產經紀業者、記帳士及報稅代理人等」防制洗錢及資恐之辦法。此等行政命令，加以各界自律組織（如銀行業、信託業、信用合作社業、保險業、期貨業公會）自訂之注意事項範本，實務上應能更加細緻處理洗錢問題在各業之特殊面向，並作為未來監管科技施展之基石。

整體而言，我國洗錢防制規範逐漸跟上國際趨勢，其成果並反映在 2019 年終於「校正回歸」之評鑑結果上[91]，值得肯定。不過，自洗錢手

89 相關介紹，請參考本文壹、緒論之討論。

90 依我國學界觀察，實務見解即有採行此種解釋者。惟學說對此有所批判，認為此種「一個蘿蔔一個坑」的解釋方法，可能產生不少漏洞。請參見林鈺雄，同註 11，頁 41-50。

91 關於 2019 年之評鑑結果，請參見本文壹、緒論之討論。

段科技化、線上化趨勢以觀，可預期虛擬資產之洗錢議題，或將造就新一波衝擊[92]。學說指出，晚近始納入我國洗錢防制體系之虛擬通貨事業，雖泰半承襲 FATF 之最新指引，惟現行虛擬通貨事業洗錢防制辦法之部分用語，非但可能有損法律之技術中立性原則，甚因法條要件上之安排，導致新興如穩定幣、非同質化代幣（non-fungible token, NFT）、遊戲點數等邊界案例逸脫潛在之納管範圍[93]。諷刺者係，愈趨複雜之新興科技洗錢手段，恰為後述科技洗錢防制技術之應用重心之一，若欠執法之相關法律授權，其勢無從發揮所長，形成「英雄而無用武之地」之窘境，頗值留意。

參、人工智慧打擊洗錢之潛力

洗錢或資恐行為之複雜性，在當代成為各界關注之核心，特別在洗錢手段日新月異，甚至高科技洗錢手段興起之際，其預防工作有如警匪大戰，惟已非純然人與人之交鋒，而係人類與洗錢科技之大戰。解鈴還須繫鈴人，人類創造科技卻落入歹徒手中，則透過科技與之抗衡，頗有

92 關此議題，晚近國內基礎面或介紹性之討論甚多，均有助於建立基本理解，如李怡萱，重新思考虛擬資產與洗錢犯罪之可罰性關係，檢察新論，第 32 期，頁 234 以下，2023 年 5 月；魏至潔，論非同質化代幣法律定位及我國相關法規適用－以洗錢防制為例，檢察新論，第 31 期，頁 196 以下，2022 年 11 月；蔡佩玲，虛擬貨幣與洗錢防制－未知之金流世界交易規則，月旦法學雜誌，第 324 期，頁 132 以下，2022 年 5 月；曹維傑、黃亞森，虛擬通貨反洗錢辦法及打擊資恐辦法之立法及虛擬通貨產業查核實務，會計師季刊，第 293 期，頁 49 以下，2022 年 12 月。

93 用語問題，如虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法第 2 條第 1 項第 2 款「虛擬通貨」指涉對象，限於「運用密碼學、分散式帳本或其他相類技術」者，準此若系爭虛擬資產之技術未落入前揭要件（如：使用了中心式技術），則非辦法適用範疇，可能造成不正當差別管制之疑義。此外，同款並限於「用於支付或投資目的者」，則穩定幣、NFT、遊戲點數等新興案例能否合致此一要件，亦不明確，同樣容易引發監管套利之弊。更細緻之討論，請參見楊岳平，同註 17，頁 118-125。

理據。適逢人工智慧興起之時代，其用途多端，且在特定事務處理能力上，遠勝人類，其能否擔綱未來反洗錢之先鋒部隊，非無討論空間。本章首先簡介人工智慧之能力與潛在之強項，第二部分凸顯人工智慧反洗錢之優勢，最後則回顧人工智慧反洗錢技術之晚近發展與實務應用。

一、人工智慧之特性與潛能

人工智慧最簡明的定義，或謂「將機器變聰明的科學」。細繹之，其定義寬狹不一，或認為必須達到與人類近似之社會上（甚或物理行為上）存在[94]，亦可能認只要足以接收人類指令，並根據所處情境產出回應之演算法，即屬之[95]。惟無論採取何種定義，至少務實觀察而言，晚近人工智慧已逐漸脫離「由人類事先撰寫演算法並交給電腦執行」之階段[96]，進入機器學習（machine learning）之新紀元。簡言之，人類僅須告知演算法「待完成之目標」，但不要求其執行固有的、人類撰寫之手段。人類主要負責給予其相當回饋，並交由演算法自行尋找更佳解方[97]。

---

94 在部分學者之視角下，人工智慧可以與機器人（robot）相互代換稱之，或更精確言之，其差異僅在於是否已經具體化（embodied），但二者均能表現出智能行為（intelligent behavior）。Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1311, 1321 (2019). 若建立在這種概念上，其實如 Calo 教授之「機器人定義」，也可能被理解為人工智慧定義的一種類型，此處沿用之嚴格定義亦主要發想自其對機器人之理解。*See* Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CAL L REV 513, 529-530 (2015). 晚近研究有彙整各方對 AI 定義之描述，引述了歐盟、OECD、Open AI、HM Government 等各方說法，*See* Simon McDougall, *More Speed, less Haste: Finding an Approach to AI Regulation That Works for the UK*, 5:1 AMICUS CURIAE 104, 108 (2023).

95 European Commission (EC), *Proposal of a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final, 39 (Art. 3.1) (2021).

96 此階段又稱為“Good Old-Fashioned A.I, GOFAI”. Lemley & Casey, *supra* note 94, at 1322.

97 故事實上，學者認為在此階段中，演算法本身亦成為自己之程式設計師。*Id.* at

基於此種運作模式，晚近人工智慧開始具備可訓練、可持續進步之性質[98]。

從人工智慧進行決策之流程以觀，某程度上實與人類類似，即OODA決策流程－觀察（observe）、調整定位（orient）、決定（decide）、行動（act）[99]。各流程中，人類與人工智慧之能力，各有千秋。以觀察階段為例，人工智慧能夠透過網路，或甚至裝設在機器上之大量感應裝置，瞬間取得為數龐大之資料，且由於資料本身無邊無際，演算法可能藉此梳理出人類無從發現之關聯性，並將之精確以數據化呈現[100]。又如決定階段，演算法之決定能夠權衡一切已知資料，並在短時間內作出決策。相形而言，人類面臨極為大量之資訊，且需短時間作出回應時（如：遭遇生命危險），通常仰賴直覺－某程度上可能極不精準[101]。

然而，二者亦存在若干差異。調整定位階段，人類與人工智慧之決策權重，存有本質上不同，如人類在某些情境下容易感情用事，這可能是基於人際互動為基礎之「人性」；人工智慧則依演算法設定數值，自由調整不同認知之權重，惟執行設定之流程基本上與人類性質之感情無關，僅依靠其自身運作之穩定邏輯[102]。決定階段，人類直覺尚有另一面

1324-1325.

98 Chagal-Feferkorn, *supra* note 22, at 233.

99 *Id.* at 236.

100 *Id.* at 240-244.

101 *Id.* at 246-247.

102 此種性質，學者認為人工智慧之決策流程是「客觀的」。*Id.* at 244-245. 不過，所謂「客觀」或許不甚精準，本文認為描述為「方向穩定的」更好，蓋邏輯上若先認為人類與人工智慧之思考途經類似，卻只因人類看待事物所帶眼光（相當於演算法之參數）含有人之主體性，便又認為是「主觀的」而與機器相左，似乎有些矛盾。此外，亦不能排除人類思想被植入演算法之情形，例如某間未來醫院院長很愛賺錢，便將旗下所有的人工智慧診療儀器設定為以「盈利」為優先目標，此際是否仍能謂該人工智慧很客觀？社會意義上，我們是否會說偏袒一方的人很客觀？益見，主觀與客觀的區分，極可能非絕對之對立，尤其在討論人類與「類人類實體」之區別時，尤其如此，故本文不擬將人工智慧之決策形容為

向之優勢在於「創意」，而演算法相對更重視基於資料之運算邏輯，也或許因此較依賴過往訓練資料之內容[103]。行動層面，人類可能具有較強之共情能力，並在行動上展現體恤他人之禮節；相對而言，人工智慧則較難掌握非理性之社會脈絡[104]。

建立於上述理解，人工智慧與人類適合從事之活動，即有差距。以洗錢防制為例，當今國際金融交易頻繁，單以 2022 年全球每日平均之外匯場外交易量為例，即高達 7.5 兆美元[105]。又如虛擬貨幣交易，研究顯示日均比特幣交易量約達 30 萬枚[106]，加以單枚比特幣得分割至小數點後 8 位數之性質[107]，其實際交易次數或許更為驚人。試想，各類交易均可能涉及洗錢行為，若欲採行符合法定預防流程之風險基礎回報模式，資訊基數極為龐大，交易間之關係如蛛網般密麻，人工智慧之資料搜集與決策特性，及其發現潛在關聯性之能力，似有實用空間。又為維繫銀行之運作順暢，篩選可疑客戶或行為之機制，勢應高效運作[108]，並維持穩定之判斷標準，此正屬人工智慧之優勢領域[109]。

「客觀的」。

103 *Id.* at 242-243.

104 *Id.* at 247.

105 BANK FOR INTERNATIONAL SETTLEMENTS, TRIENNIAL CENTRAL BANK SURVEY: OTC FOREIGN EXCHANGE TURNOVER IN APRIL 2022, 3 (2022).

106 Pakki, Shoshitaishvili, Wang, Bao & Doupé, *supra* note 68, at 4.

107 參見魏至潔，同註 56，頁 171。

108 Georgios Pavlidis, *Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of Anewera*, 24 J. MONEY LAUNDERING CONTROL. 155, 156 (2023).

109 固然，我們亦可能認為洗錢之調查需要一點「創意」，或者一種「直覺」，又或是理解人際關係之「人性」，惟洗錢調查勢應先齊備基礎分析資料，始能進入更高層次之判斷。在此層面上，至少可以主張「基礎調查」之層次，人類不具特別優勢。

二、人工智慧 vs.工人智慧

當代反洗錢相關法令蓬勃發展，各國亦透過跨政府組織之通力合作，建立反洗錢法制之堡壘。然而，立法容易執行難，蓋如前述，國際金融交易之數目與日俱增，洗錢之手段又漸趨複雜，據研究，金融機構每年可能至多需耗費總收益之 4 %執行反洗錢相關程序[110]。如此沉重之法遵壓力，在在使得金融機構試圖建立新的資源分配模式，甚至轉而尋求新科技之協助。

（一）「工人智慧」反洗錢之困境

洗錢逐漸國際化、複雜化，對於反洗錢程序之人類查核員（human auditors）而言，係一嚴峻挑戰。傳統之洗錢查核程序，大致可分為四個階段：1. 資料搜集（data layer）、2. 篩選與監控（screening and monitoring layer）、3. 事件警示（alert and event layer）、4. 執行（operational layer）[111]。

1. 資料搜集階段，金融機構能自內部直接取得客戶資訊、帳戶與實時（real time）交易資訊等項目，另可能對外搜集資訊，其來源包括主管機關、國際標準、地方法令、監視名單、社群媒體等[112]。由於資料異質性（heterogeneity）相當顯著，猶須經標準化程序，始具分析價值[113]。

---

110 Pavlidis, *supra* note 108, at 156.

111 Jingguang Han, Yuyun Huang, Sha Liu & Kieran Towey, *Artificial intelligence for anti-money laundering: a review and extension*, 2 DIGIT FINANCE 211, 211 (2020).

112 用以搜集資料之軟體，包括能平行處理與資料搜集之 Hadoop、能搜尋之 Solr、能建立模型與分析之 Mahout 集 Spark。*Id.*

113 *Id.* 關於資料異質性之觀察，*See also* Pavlidis, *supra* note 108, at 158. 該文指出，可能之料來源包括收據（invoices）、提單（bills of landing）、電子郵件、管制資料（regulatory data）以及其他外部資料（external data）。亦觀察到類似現象者，*See* Garcia-Bedoya, Granados & Burgos, *supra* note 40, at 58.

2. 篩選與監控階段，重在觀察客戶行為，具體操作手法如：交易篩選（transaction-screening module）用以偵測受制裁者之交易[114]、姓名篩選（name-screening module）用以比對交易實體之身分與關係[115]、客戶資訊監控（client profile-monitoring module）用以監測客戶潛在之高風險行為等[116]。3. 事件警示階段，即「行為之比對」，多係由人類查核員將個案所悉資料與過往洗錢案例對照，以決定是否進一步回報警示[117]。4. 執行階段，即若決定回報警示，將引發後續之法律行動[118]。

看似操作體系嚴明，惟傳統之查核機制，面臨不少障礙。首先，語言隔閡可能成為資料搜集階段之致命傷，尤在洗錢國際化、集團化之下，更是如此[119]。其次，在篩選與監控階段，單僅繪製交易相關人之關係圖，便可能因涉及過量資訊，對人類調查員產生超載負荷[120]。再者，事件與警示階段之比對與決策過程，相當冗長，易生嚴重之時間延遲，使實時監控難以企及[121]。又傳統決策系統多立基於規則為基礎之方法（rule based system）－即由人類預先決定標準後，再標準化執行，在當今力求配合法遵義務之前提下，機構可能傾向以嚴格且無彈性之標準檢視客戶行為，造成極為嚴重之偽陽性問題[122]，進而又因過量的偽陽性而

114 相關應用程式，如 Actimize、Mantas。Han, Huang, Liu & Towey, *supra* note 111, at 211.

115 相關應用程式，如 Compliance Link of Accuity、Oracle Watchlist Screening of Oracle、LexisNexis Bridger Insight XG。*Id.*

116 *Id.*

117 *Id.*

118 *Id.*

119 關於此問題，*See* Pavlidis, *supra* note 108, at 157.

120 Han, Huang, Liu & Towey, *supra* note 111, at 211.

121 Kamlesh D Rohit & Dharmesh B Patel, *Review on Detection of Suspicious Transaction in Anti-Money Laundering Using Data Mining Framework*, 1 INT. J. INNOV. RES. SCI. TECHNOL. 129, 129 (2015).

122 根據研究，傳統反洗錢流程造成之偽陽性警報率，可能高達 90 %。同時，人類查核員平均浪費 80 %時間在處理本質上合法之交易，僅 20 %時間用於處理真正

衍生警訊疲勞（alert fatigue）[123]，陷入嚴重惡性循環。此外，因人類查核員之間欠缺互動、溝通不良所造成之重複調查、報告內容之不一致或錯誤[124]，均構成嚴重挑戰。

前述內部運作困境，首先直接反映在不成比例的人事開銷上。據統計，在大型公司之反洗錢部門相關支出中，約 52 %係用於人事成本，小型公司之數據更高達 68 %[125]，係名符其實的「人力密集（labor-intensive）」行業[126]。業界相關部門之員工數量，在 2012-2017 年間約成長 10 倍，實為反洗錢業務支出不斷高漲之元兇[127]。其次，洗錢法遵業務造成之外溢效應，亦波及不少無辜存戶。研究顯示，自從反洗錢業務上路以降，日漸提高之開戶門檻、冗長之身分審核程序等，無一不致客戶對銀行服務產生負面觀感[128]。

（二）人工智慧判斷洗錢之實際優勢

將人工智慧引進反洗錢機制中，具有不少顯著優勢。以國際化洗錢造成之語言隔閡為例，在傳統反洗錢機制下，透過大量擁有不同語言背景之員工通力合作，固非無可能，惟人力成本之高昂，不難想見，人員良莠不齊與經驗差距，尤其嚴重。相對而言，訓練人工智慧學習萬國語言，能夠全天候連續進行，排除人力之生理限制。且專責訓練之人員集中精力訓練單一演算法，顯然勝過萬人懸樑刺股之經濟效益－此即規模

高風險之交易。Juan Carlos Estrada, *The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering*, 16 RUTGERS BUS. L.J. 383, 392-393 (2021).

123 Pavlidis, *supra* note 108, at 158.

124 Singh & Lin, *supra* note 42, at 475-476.

125 Estrada, *supra* note 122, at 392.

126 Rohit & Patel, *supra* note 121, at 130.

127 Estrada, *supra* note 122, at 392.

128 Levi & Reuter, *supra* note 3, at 293. 我國政府針對反洗錢業務之相關澄清，請參見法務部，同註 19。

效益（advantage of scale）[129]。又一旦人工智慧學成技能，其成果即能在機構中無限複製使用[130]，弭平向來人員素質差異之通病。

其次，在客戶行為之監控與比對階段，實時監控有其必要，然傳統判斷方式為兼顧決策之品質，往往犧牲效率而造成延遲，已如前述。拜演算法之運算速度所賜，在偵測（detect）、識別（identify）、回報（report）可疑交易之流程中，人工智慧能即時將異質性極高之客戶資訊與快速更新的實時交易資訊結合，並作成動態分析（dynamic analysis），建立高效率產出，同時兼顧決策之穩定性。此等能力之運用極為重要，在經典之高風險行為偵測－如交易價值嚴重偏離常理之情境，相關交易客體之一切歷史價格、交易者身分與特性等資料，均應納入比對，人工智慧演算法能在短時間內完成重複度、複雜度、枯燥度均極高之分析工作[131]。

最核心之貢獻，應係人力資源之配置之優化及預測正確性之大幅提升。反洗錢人力資源成本支出節節高升之問題，早已為金融業者所意識到，並使斬新科技解決方案之尋覓、數位轉型之推動，榮登業界積極投入之排行榜。據國外預測，金融機構投入法遵科技（regulation technology, RegTech）之金額，2023 年約達 1,150 億美元，至 2026 年更將攀升至 2,040 億美元，RegTech 領域之成長幅度，將在琳瑯滿目的法遵項目中一支獨秀[132]，其重要性可見一斑。具體成效上，引進人工智慧演算法判

129 Chagal-Feferkorn, *supra* note 22, at 240.

130 *Id.*

131 *See generally* Pavlidis, *supra* note 108, at 158.

132 *Id.* at 156. 產業角度而言，民間企業經常為 RegTech 發展之領頭羊，扮演開創、引入新技術之關鍵角色。而從監管機構之角度而言，引進科技手段輔助其執法、進一步推動法制完善化，則屬監管科技（supervisory technology, SupTech）之應用。二者本質上雖如一體兩面，惟時間向度而言，前者之發展往往先於後者。先進國家地區如美、歐之 RegTech、SupTech 發展歷程簡述，請參見臺灣集中保管結算所，監理科技與法遵科技最新發展趨勢之探討，2020 年 12 月，頁 49-70，https://m.tdcc.com.tw/TDCCWEB/upload/402897967d841dba017e3226bd08006c.pdf（最後瀏覽日期：2024 年 4 月 18 日）。基此經驗，當前民間多元之人工

斷洗錢，能將原本出錯率高達 90 %之偽陽性警報，有效地壓低至 40 %[133]，搭配前述動態、實時分析與行為預測能力，能更敏捷地掌握未曾出現之洗錢樣態，潛力無窮。

傳統金融機構以外，持續成長中之虛擬資產業務，亦能透過人工智慧預防洗錢。其仰賴區塊鏈運作之性質，雖能透過混幣器、Tor 網路等技術掩飾不法交易，惟如混幣器之時間延遲、金額切分等功能，仍在鏈上留下不可抹滅的紀錄，一旦所有數據綜合觀察，亦非不能拼湊高風險交易之原樣；又如 Tor 瀏覽器隨機安排節點（randomized nodes），以模糊化（blur）使用者與終端伺服器間之連線路徑[134]，惟調查交易主體身分時，若輔以人工智慧逆向追蹤路徑，其實時、動態分析之特性，應能在更短時間內溯源，指向背後藏鏡人。

FATF 之 40 項建議中，第 22、23 項明列之指定之非金融事業或人員（DNFBPs），亦可能輔以人工智慧，開展反洗錢業務。賭場、不動產經紀人、珠寶交易商、律師、會計師、信託，係第 22 項明定之適用對象[135]，並依第 22、23 項準用各項預防與減緩洗錢行為之措施，如 CDD、資料保存、對特殊客戶採取特定措施、留意新科技洗錢手段、對第三方

智慧反洗錢方案，往後亦非無可能轉往 SupTech 領域而受各國政府之青睞。以我國為例，近期金管會發布「金融業運用人工智慧（AI）指引（草案）」，提及治理與問責機制、公平性與以人為本價值、保護隱私、確保系統穩健與安全、透明性與可解釋性等重要原則，請參見金融監督管理委員會，金融業運用人工智慧（AI）指引（草案），頁 14-23，https://www.fsc.gov.tw/uploaddowndoc?file=news/202312281513450.pdf&filedisplay=新聞稿附件 1-金融業運用 AI 指引草案.pdf&flag=doc（最後瀏覽日期：2024 年 4 月 18 日），主要仍聚焦在「金融機構本身」應用人工智慧之視角。主管機關未來是否跟進導入相類技術，並具體用於反洗錢層面，有待時間證明。

133 *Id.* at 158. 另有文獻指出，偽陽性將從 90 %降至 50 %。*See* Estrada, *supra* note 122, at 392.

134 DiPiero, *supra* note 53, at 1273-1274.

135 FATF, *supra* note 86, at 19-21.

交易之措施、調查可疑交易並回報等[136]。該等業者，固可能由經濟實力豐富之人或團體經營，亦可能為個人或小團體自營，惟後者若不具雄厚資力以確實執行反洗錢作業，則非但成為反洗錢之破口，更可能因難以履行其內國法義務而面臨嚴厲法律效果。此際，若以人工智慧輔助業者之反洗錢流程，應能撙節成本、補苴罅漏。

綜合而言，針對劣跡斑斑之傳統反洗錢機制，引進人工智慧判斷不僅降低法遵壓力、節約成本，亦提高運作效率[137]，此無論對於傳統金融機構、虛擬資產服務提供者、指定非金融事業或人員、其他新興可能涉及洗錢之行業（如前述之藝術品買賣行業），甚或監管機構未來之多元手段選擇，均有助益。

三、人工智慧反洗錢技術之現況

（一）從規則爲基礎到動態分析

早期之反洗錢演算法，多呈現「以規則為基礎」之架構。如 2014 年即有學者提出一種嘗試，在系統中寫入某銀行預先制定之反洗錢監測標準，以偵測可疑交易並回報警示。2013 年前後，亦有學者提出植基於本體論（ontology）之模型，藉語意網法則語言（Semantic Web Rule Language, SWRL）及貝葉斯網路（Bayesian network）偵測可疑行為[138]。

然而，以規則為基礎之演算法，同樣招致與傳統人類稽核員標準化審查相似之困境。設想，一旦該演算法參照之規則過於嚴格，同樣造成嚴重之假陽性問題；反之，若規則過於寬鬆，則可能湧現大量漏網之魚。此外，若出現新型態之犯罪，僵化之規則基礎模型與傳統方法一樣無能

136 *Id.* 觀我國針對指定非金融事業或人員之法規命令，如律師、會計師、不動產經紀人等類型之子法，均明定有前揭義務之規定。

137 Pavlidis, *supra* note 108, at 162.

138 Rohit & Patel, *supra* note 121, at 131.

為力。是以學說認為，此類型之演算法，仍非金融機構反洗錢業務之最適解決方案[139]。

近期研究有自「回饋（feedback）機制」著手，試圖強化人類稽核員對人工智慧演算法所提供分析報告之評價機制，加強其辨識新型犯罪之能力[140]。有認為應納入更多不同屬性之資料[141]、擴增非屬金融機構內部之資訊來源[142]。亦有從交易資料之即時性出發，認為應在不同偵測工具之間共享資訊，如建立資訊池（data pool）以強化動態分析交易資料之能力[143]，藉龐大完整之共享資料資料，對人工智慧執行監督式機器學習（supervised machine learning），以滿足動態風險基礎方法（dynamic risk-based）迅速因應新風險之要求[144]。

（二）常見之分析模型

除所謂「過時的」規則基礎方法以外，晚近常見之分析模式如聚類分析（clustering），顧名思義係將類似資料分門別類之技術。具體而言，其分類基礎為「類似性（similarity）」，將類似之客戶或交易歸入相應類別[145]。有意義的分類基礎多與風險因素有關，如客戶之經濟活動性質、

139 Han, Huang, Liu & Towey, *supra* note 111, at 211.

140 *Id.*

141 Rohit & Patel, *supra* note 121, at 130.

142 Alhanouf Abdulrahman Saleh Alsuwailem & Abdul Khader Jilani Saudagar, *Anti-Money Laundering Systems: A Systematic Literature Review*, 23 J. MONEY LAUNDERING CONTROL. 833, 846 (2020).

143 Pavlidis, *supra* note 108, at 158. 應注意者係，該文同時提及，這種資訊分享之措施，應同時注意個資保護之法律問題。

144 動態風險基礎方法強調洗錢風險在當代之變動極快，相關之評估（assessment）方法一旦過時（outdated），可能構成嚴重風險。因此，無論係監督程序本身，抑或主管機關，均應備敏捷的（agile）應變能力，在可能的情況下並得採用科技手段（technology by supervisors, SupTec）。*See* FATF, GUIDANCE ON RISK-BASED SUPERVISION 65 (2021).

145 Rohit & Patel, *supra* note 121, at 131.

交易頻率、交易數額、收入、存款數額、產品類型、分銷管道、地理位置等[146]。分類工作後，通常搭配次一階段之比對分析。亦即，第一階段將某客戶之個人資料與歷史交易資訊分類，第二階段則判斷每一項新交易是否偏離該客戶之典型行為[147]，並產生警示回報[148]。前述二階段分析，均能引進機器學習演算法以執行之，包括邏輯回歸（logistic regression）、決策樹（decision tree）、極限梯度提升（XGBoost）、自動編碼器（AutoEncoder）、深度神經網路（Deep Neural Network）等[149]。

探究洗錢交易之複雜網路並予以精要呈現，圖像化（visualizing）之分析技術益顯重要。常見之分析模型包括以中心程度（degree of centrality）判斷結點（nodes）之間關聯性之網路分析（network analysis）、探究結點間聯繫關係之連結分析（link analysis）、將交易背後所隱藏之各種關係圖形化的社會網路分析（social network metrics）、圖像學習（graph learning）等。此種分析模式下，可用之演算法技術包括自然語言處理（natural language processing, NLP）、快速圖形卷積網路（fast graph convolutional networks）等[150]。

此外，風險之分類與評分（risk classifying and scoring）係另一種分析模式。其運作主要基於客戶資訊之大量變數，如職業類型、地點、企業大小、存款數額等，交由演算法將之歸類為不同之風險層級，或給予不同之風險分數，以揪出可疑交易。根據研究，此種分析模式下，決策樹之實際表現最為良好，而其他之機器學習類型，如資料探勘等，亦有相當之發揮空間[151]。

---

146 Garcia-Bedoya, Granados & Burgos, *supra* note 40, at 58.

147 Rohit & Patel, *supra* note 121, at 131; Han, Huang, Liu & Towey, *supra* note 111, at 211.

148 Garcia-Bedoya, Granados & Burgos, *supra* note 40, at 57-58.

149 *Id.*

150 Han, Huang, Liu & Towey, *supra* note 111, at 211.

151 *Id.*

（三）業界實例－Ayadsi、SAS 與 Google

實務上，Ayadsi 係近期頗受關注之反洗錢系統，其強調以「行為」為基礎之智慧區分模式。透過整合用戶之交易歷史數據，並藉「行為洞察力」功能，將用戶每日交易行為之變化趨勢加以分析，與用戶自身過去行為、其他顧客群體之行為互相對照，以找出偏離常態之可疑交易。此外，Ayadsi 系統即時更新交易屬性之相關資訊，如交易數據、地理數據、時間序數據等，使金融機構能及時因應新局面。匯豐銀行即採用此一方案，並造就偽陽性警報約 20 %之減少幅度[152]。

至若 SAS 之技術方案，除偵測用戶行為趨勢與潛在威脅，更能夠整合關聯交易之資訊，透過圖像化儀表顯示，使分析師實時監測交易現況。其強調，不待收到系統之警示回報，分析師即能直接透過其簡明之操作介面，預先關注可疑之交易。以色列之 Ayalon 保險公司即採用此一方案，並曾與 SAS 共同開發此系統[153]。

晚近 Google 亦推出洗錢防制系統，其特色在於摒棄過往之規則基礎方法，以機器學習為主要技術手段。運作上，該系統不僅偵測高風險之交易，亦同時提供該次交易之諸多背景分析，以解釋其獲得高風險分數之原因。據 Google 所述，其方案將能降低 60 %之偽陽性警報，並提高 2-4 倍之準確通報數。不過，此一技術上之革新，亦引起部分懷疑論者質疑，實效有待時間證明。近期，匯豐、Bradesco、Lunar 等銀行已開始採用此方案[154]。

---

152 胡　林，同註 23，頁 53-55。

153 同前註，頁 55。

154 Dylan Tokar, *Google Cloud Launches Anti-Money-Laundering Tool for Banks, Betting on the Power of AI, The Wall Street Journal, available at* https://www.wsj.com/articles/google-cloud-launches-anti-money-laundering-tool-for-banks-betting-on-the-power-of-ai-2512ccce?mod=business_minor_pos4 (last visited December 9, 2023).

肆、國際人工智慧反洗錢方案之挑戰

洗錢行為開枝散葉，科技洗錢手段又加劇其挑戰，人力查核洗錢之措施，似已不合時宜，人工智慧演算法介入反洗錢流程，儼然形成當代趨勢。然而，新科技之運用絕非一帆風順，除其本身技術問題猶待解決以外[155]，其所具跨國應用之本質，使得政策上、法律上之進一步安排，構成嚴肅課題。本章首自人工智慧之固有議題出發，討論各國政策落差可能造成之部署障礙；其次，論述當代資料在地化（data localization）趨勢，對反洗錢資料整合工作之威脅；最後，人工智慧反洗錢措施仰賴線上工具之必要性，可能引發類似晚近針對線上平臺影響資料主權之質疑。此等議題，希自更為宏觀之跨國法律政策角度出發，並期開創未來更多討論。

一、人工智慧固有爭議與各國政策落差難題[156]

（一）二大陣營：歐盟與美國

歐盟之人工智慧政策，在 2020 年之人工智慧白皮書（White Paper on Artificial Intelligence - A European approach to excellence and trust）發布

155 應注意者係，本章非以人工智慧「技術層面」之討論為核心，下文並不包含對現行分析模型、機器學習技術本身應用上之評論，而係聚焦於法律面之問題。關於技術問題之研討，*See generally* Rohit & Patel, *supra* note 121, at 132; Han, Huang, Liu & Towey, *supra* note 111, at 211.

156 需澄清者係，本節檢討之範圍，僅舉現今人工智慧反洗錢方案在國際間應用時，初步可能面臨之困境數端，屬於非常前階段之討論，其中人工智慧管制模型之爭占據其一痛處。至各國內國法（含我國）應如何具體規範或推動此類技術，確實值得展開論述，惟實應先探尋前開人工智慧技術之管制模型之輪廓後，始能進一步建構。此係重大議題，值得專文探討，惜囿於本文研究範圍與篇幅限制，難憑單一章節細緻處理。作者由衷感謝匿名審查人進一步提出此論點，而有待將來各論式之延伸。本文有限能力內，僅能提及當前人工智慧管制模型爭議之梗概，及其與高科技反洗錢方案間可能之互動與衝突，如本節下述。

後，已然確立。開宗明義，其目標係建立可信賴之人工智慧（trustworthy AI），並強調 AI 時代之基本權保護[157]。2021 年版草案即透過風險（risk）高低區分規範之適用情境[158]，原則僅高風險人工智慧應採取加強措施，以符比例原則[159]。規範要素[160]，可大別為 1. 訓練資料之管控[161]、2. 資料保存[162]、3. 資訊提供[163]、4. 穩健性與精確性（robustness and accuracy）[164]、5. 人類監視（human oversight）[165]、6. 遠端生物辨識（remote biometric identification）應用之限制[166]、7. 責任歸屬[167]數端。2024 年上旬，歐盟 AI 法案甫經歐洲議會通過，扮演 AI 法制之先鋒部隊。觀其立法宗旨[168]、

157 EC, *White Paper on Artificial Intelligence: A European approach to excellence and trust*, COM (2020) 65 final, 1-2 (2023).

158 草案具體之風險分類方式，係以系統預期之目的（intended purpose）區分。EC, *supra* note 95, at 13. 實際條文規範，如可能造成身心傷害（Art. 5(a)）、易對特定弱勢者或族群造成傷害（Art. 5(b)）、根據人之行為評量社會分數並據此施加不利措施（unfavorable treatment, Art. 5(c)）、非屬「保護犯罪被害人、緊急救援、執法程序」之實時監控（Art. 5(d)）等，受到直接禁止。EC, *supra* note 95, at 43-45. 至於高風險系統之通案定義及管制手段，規定於法案第 6 條以下。

159 低風險之人工智慧系統，亦能自願採取更嚴格之應對措施。根據歐盟之規劃，自願遵守更高管制密度者將獲得自願標章（voluntary label），將有利於提升人民對人工智慧之信賴。*See Id*. at 24.

160 *See generally*, *Id*. at 18-24.

161 如確保資料多元性、避免基於敏感特徵之歧視、個資保護等。

162 訓練資料選用方法之紀錄、資料使用方式、歧視防範措施等紀錄保存。

163 應明揭人工智慧系統之能力（capabilities）與限制（limits），且須使用戶明瞭其互動對象非人類。

164 應確保系統正確反映其實際性能、結果之可重現性（reproducibility）、系統除錯能力、免受攻擊或操縱之韌性（resilience）。

165 依風險高低區分人類介入程度，貫徹人類中心之人工智慧（human-centric AI）。

166 原則禁止實時監控，惟在合乎比例原則前提下，允許如執法需要等例外。

167 視提供者、散佈者或使用者，何人最適合負責降低風險，並課予相應責任。

168 即可信賴性、穩健性、非歧視性、以人為中心、基本權之充分保護等。European Parliament (EP), *Corrigendum, Artificial Intelligence Act*, P9_TA (2024) 0138, 3-7, 159 (Art. 1.1) (2024).

管制密度分類[169]、高風險 AI 管制手段[170]等骨幹，主要承襲草案架構並加以擴充、細緻化[171]。至其後續之實施與執法，猶待觀察。

往昔，歐盟在諸多法律領域保持領先地位，執法及於主要跨國企業，甚影響各國立法，隱私權法即為典例。歐盟於 2016 年通過一般資料保護規則（General Data Protection Regulation, GDPR），不僅形成以美國為首之大型科技公司實質受歐盟法諸多管制之現象[172]，迄今更已有超過 150 國在其內國資料法領域採行類似 GDPR 之架構[173]。強大之域外影響力，儼然為歐盟法一大特色，通稱布魯塞爾效應（Brussels Effect）[174]。2024 年歐盟 AI 法案通過後，倘若 GDPR 橫掃全球之戲碼再次上演，勢將牽動往後 AI 法制之走向。

美國之規範模式相對繁雜。聯邦立法動作，最早可溯自 2019 年眾議院推動人工智慧倫理發展之指南（Supporting the Development of Guidelines for Ethical Development of Artificial Intelligence），其提出如透明性與可解釋性、資訊隱私與個資保護、問責性與監視下決策、可近用

169 與草案相仿，係基於風險高低區分之。*Id.* at 26-50, 189-195 (Art. 6, 7). 不過，歐洲議會通過版本之條文，更明確揭櫫「風險」之定義。*Id.* at 165 (Art 3(2)).

170 第二章為特定 AI 用途之禁止規範，第三章則為高風險系統之規制措施，包括定義（第一節）、對該種系統之要求（第二節）、對系統提供者及部署者之要求（第三節）、評估機關之設置（第四節）、標準之評估與認證（第五節）。

171 加以擴充處，犖犖大者如「通用人工智慧模型（general-purpose Al models）」之規範。*See generally* EP, *supra* note 168, 90-108, 285-299 (Chapter V). 又如管制客體（第 2 條第 2 項）、特定用途禁止規範及例外（第 5 條）之擴充。再如定義規範（第 3 條）、透明義務（第四章）、創新輔助措施（第六章）、治理機制（第七章），均能觀察到更加細緻之處理。囿於篇幅與主題，本文無從一一介紹。

172 該等公司通常傾向以世界上最嚴格之規範為法遵之基本要求，通常係基於商業習慣之統一（uniform business practice）以及規模經濟（economies of scale）之考量。*See* Anu Bradford, *Europe's Digital Constitution*, 64 VA. J. INY'L L. 1, 6 (2023).

173 *Id.*

174 Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3 (2015).

性與公平性等概念[175]。聯邦或各州並依其需求進行立法，如 2019 年參眾兩院針對高風險自動決策系統（high-risk automated decision systems）提出之演算法課責法案（Algorithmic Accountability Act），或紐澤西州、紐約市、華盛頓州、加州提出之類似法案。臉部辨識（facial recognition）技術使用之規定，參眾兩院、加州、麻州、伊利諾州、德州均有草案。透明性（transparency）義務，加州、伊利諾州有相關法案。其他議題包括反歧視、政府使用等，均有立法嘗試[176]。相形於歐盟之整合，美國 AI 政策雖可由州法窺探其大方向，惟聯邦層級之立法仍欠明顯進展[177]。

拜登（Joe Biden）總統於 2023 年 10 月簽署之行政命令，係美國近期重要之政策表態。其主軸包括：1. 人工智慧之安全可靠性（safe and secure）[178]、2. 負責任之創新、競爭與合作（responsible innovation, competition, and collaboration）[179]、3. 負責任的發展與使用（responsible development and use）[180]、4. 保護公平與公民權利（equity and civil rights）

175 Yoon Chae, *U.S. AI Regulation Guide: Legislative Overview and Practical Considerations*, 3 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (FASTCASE) 17, 20 (2020).

176 *Id.* at 21-29.

177 類似觀察，認為美國 AI 政策仍在各州立法摸索階段者，*see* Srinivas Parinandi et al., *Investigating the Politics and Content of US State Artificial Intelligence Legislation*, 26 BUS. & POL. 240, 240-243 (2024). 關於美國人工智慧政策之走向，白宮科學與科技辦公室（The Office of Science and Technology Policy, OSTP）曾於 2022 年提出具有原則性之報告書，力主五大目標，包括：安全與效率之系統、對抗演算法歧視、資訊隱私、通知與解釋、人類替代方案與決策介入。整體而言，雖未如歐盟明確指出以風險為基礎之分類，惟在規範架構上（如：人類之介入程度），仍明確建議應符合比例原則。*See generally* The White House, BLUEPRINT FOR AN AI BILL OF RIGHTS 8 (2022).

178 包括風險控管（國家安全、經濟安全、公衛安全、網路安全等）、透明性與複雜度問題、部署前後之測試與監控、人民對與非人類互動之知情權等。

179 包括技術人才訓練、研究量能建立、智慧財產權保護、大小企業兼容之公平競爭環境等。

180 其力主勞權在數位時代之保護。

[181]、5. 美國應引領國際人工智慧管制之發展[182]等。倘若美國能夠成功統合國內政策，或將因循往例，設法對外輸出其管制模型以抗衡歐盟法[183]。眼下一觸即發的管制競賽，不免為國際 AI 法制再添變數。

（二）未解之爭議概念與反洗錢人工智慧部署之困境

人工智慧管制政策面臨之上位問題係，究應個別立法，抑或基於當前法律架構，另闢符合人工智慧時代之法律修正途徑即足。美、歐當前似較傾向建構獨立法律體系，僅其取向有所差異。惟亦可見別一路徑：英國。其 2023 年提出之「有利創新之人工智慧管制手段（A Pro-innovation Approach to AI Regulation）」文件，大致採取維持現有法律架構加以個別修正之模式[184]，往後亦不排除成為立法體例之第二選項。採取不同模式之影響在於，採行專門法制之模型，勢有必要重新劃定法律適用範圍、建構嶄新的法律效果；維持現行管制架構之模型，則應確保各部現行法涉及 AI 面向之修正達成同步化，並留意不同法規間就相同問題口徑不一之危險。對切入國際市場之人工智慧反洗錢方案，各國立法取向之差異，儼然構成 FATF 規範整合以外之第二波法遵挑戰。

實質規範內容，如人工智慧是否、如何採取風險分類，及各該法律

---

181 包括反詐欺、反歧視、保護隱私，並避免在健康（healthcare）、金融服務、教育、住房（housing）、運輸等運用領域可能之傷害等。

182 *See generally* The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/(last visited December 10, 2023).

183 此由第 5 點目標可略窺一二。關於美國過往透過雙邊貿易條約（bilateral trade agreement）繞過 WTO 體系，對特定貿易國家輸出內國管制模型之探討，*See generally* Han-Wei Liu, *Exporting the First Amendment through Trade: The Global "Constitutional Moment" for Online Platform Liability*, 53 GEO. J. INT'L L. 1, 1 (2021).

184 McDougall, *supra* note 94, at 118.

效果之對應，亦可能影響反洗錢演算法之跨國部署。歐盟 AI 法案中，高風險人工智慧對應全面性之義務。依反洗錢系統之運作原理，其似可能該當第 6 條第 2 項、附件三 6(e)所指之「與執法單位調查刑事犯罪相關之自然人資料分析系統」[185]，而以高風險系統之姿納管。相對者，美國 2023 年行政命令中所謂風險因素，包括國家安全（涉及化學、生物、核子武器之使用）、網路安全、易規避人類監督等性質，與歐盟定義不盡相同[186]。至人工智慧權利法案藍圖（Blueprint for an AI Bill of Rights）中，關於安全與效率之實現[187]，以及人類介入程度之決定[188]，係基於對人權之影響或危險性等因素判斷，其展現之比例原則精神，某程度又與歐盟模式雷同。依本文所見，美國聯邦層級立法之變數不少，洗錢防制演算法服務提供者，尤應密切留意其發展趨勢[189]。

除法律架構與規範邏輯之差異外，其他如透明度與可解釋性、個人資料之使用規則[190]、反歧視規範、人類介入（human in loop）之程度、

185 EP, *supra* note 168, 427. 該條並針對所謂「自然人資料分析」之內涵，嫁接至 Directive (EU) 2016/680 關於檔案分析（profiling）之定義，可謂某程度上與反洗錢演算法之性質吻合 [‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;…]。

186 若該當美國之風險定義，將引發一系列風險評估（assessment）、管理（manage）與減緩（mitigate）之義務。The White House, *supra* note 182.

187 The White House, *supra* note 177, at 21.

188 *Id.* at 49, 51.

189 學說有認為，美國當前階段係以州法作為「民主實驗室」，為未來整合性之聯邦法鋪路。依此，州法之立法動向及其影響力之消長，為現階段需關注之重點。*See* Srinivas Parinandi et al. *supra* note 177, 241.

190 舉例而言，美國並無如歐盟 GDPR 般一套完整的個資保護法律，個資相關規範係散落於單行法當中。*See generally* HENRY GAO, DATA SOVEREIGNTY AND TRADE AGREEMENTS: THREE DIGITAL KINGDOMS, HINRICH FOUNDATION 9-10 (2021). 據此，人工智慧演算法如何使用個資之法律安排，仍可預期在兩大陣營間出現一定程度之差異。

人工智慧系統造成傷害之法律責任分配等基本議題之建構，均與反洗錢演算法之設計、部署、實效等層面息息相關[191]。在多方陣營之人工智慧法制藍圖間，反洗錢之全球性科技管制方案既選擇擁抱機器學習等演算法，則除反洗錢法制、金融法制等現行基本規範以外，人工智慧相關法制之走向，勢將同步制肘其拳腳。

二、資料在地化政策之負面影響

人工智慧反洗錢方案重要目標之一，在於避免人類查核員因溝通不良、協調不佳而產生效率、準確性之減損。此外，技術方案中關於資料共享之倡議，亦希冀透過動態風險基礎模式之建構[192]，強化對新威脅之因應能力。綜合以觀，基於演算法之反洗錢系統，藉人工智慧「一次訓練、全體適用」之特質[193]，理論上能克服「人際間」、「國際間」之屏障，實現反洗錢措施之真正整合。此外，前文所介紹之三種反洗錢方案[194]，均有在不同國家同時適用之案例，此類大型線上反洗錢偵測平臺之發展，亦可能事實上強化整合之效能。

然近年關於資料在地化（data localization）之發展趨勢，係反洗錢方案提供者或使用者所應特別留意。理論上，網路資料傳輸路徑之決定，僅取決於最有效率之路徑[195]，不受其他外力干涉[196]。若反洗錢演算

191 關於人工智慧傳統適用問題之討論，與洗錢偵測演算法相關之討論，比較法文獻已可見於 Estrada, *supra* note 122, at 400-408; Pavlidis, *supra* note 108, at 159-162; Han, Huang, Liu & Towey, *supra* note 111, at 211. 本文不擬贅之。

192 此一概念，請參照本文參、三、（一）之介紹。

193 請參照本文參、一、之討論。

194 請參照本文參、三、（二）之討論。

195 Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015).

196 學說提出，網路具備無遠弗屆的可連接性（universal connectivity），且用戶之操作行為原則上不受網路服務提供者所干涉（dumb at the centre and smart at the edges）。John Selby, *Data Localization Laws: Trade Barriers or Legitimate*

法、資料庫等技術欲進行超國界整合，此特徵亦屬必要條件。惟近年許多國家開始在不同程度上要求網路服務提供者（internet service providers，或線上平臺，online platforms）將用戶相關資料（包括金融資料）、其他特定類型之資料儲存於國內，甚或要求平臺業者在境內設置資料中心，或設下對境外傳送特定資料之法定限制[197]，相關規範亦已開始見於一些區域貿易條約[198]。其追求資料在地化之理由，不外乎 1. 對抗外國情報單位之監視（foreign surveillance）、2. 隱私權與安全（privacy and security）、3. 經濟發展、4. 法律執行之強化、5. 自由之追求五端[199]。

可想見者係，無論採取何種程度之資料在地化措施，均阻礙反洗錢人工智慧系統之國際化發展。前述關於特定資料向境外傳送之限制，輕則影響資料共享之可行性，重則阻撓相關演算法之研發工作[200]。強制資料於境內儲存之政策，則可能面臨設置當地資料中心潛在之不經濟因素[201]、資料存儲安全性受到挑戰[202]等疑雲。此均可能影響反洗錢服務提供者進入特定市場之意願，蓋一旦結合反洗錢法規、金融法規、人工智慧法規之嚴苛要求，外加資料在地化所面臨之法律、經濟風險，似非所有服務提供者均能、均願意承擔。

Responses to Cybersecurity Risks, or Both, 25 INT'L J.L. & INFO. TECH. 213, 214 (2017).

197 *See generally* Chander & Le, *supra* note 195, at 708-713.

198 Selby, *supra* note 196, at 220-221.

199 此等論據是否有理，並非當然。相關討論，*See* Chander & Le, *supra* note 195, at 713-739.

200 類似看法，*See* Han, Huang, Liu & Towey, *supra* note 111, at 211.

201 事實上，由於建立新的資料中心耗費極高，對於當地工作機會之貢獻卻不多（蓋資料中心無庸太多員工），同時降低了國內用戶選擇外國尖端技術（cutting-edge technologies）之機會，甚至可能對當地電力基礎設施構成嚴峻挑戰，學界認為並非經濟的選項。*See* Chander & Le, *supra* note 195, at 721-730; Selby, *supra* note 196, at 228-229.

202 學者認為，將資料儲存於特定國境內，形同將網路攻擊之目標集中於一地，反而更加深資安風險之疑慮。*See* Chander & Le, *supra* note 195, at 714-721.

三、數位主權、正當法律程序與反洗錢演算法之困境

資料主權（data sovereignty）最直接之理解，應係對於資料或資料設施有意義之控制、所有權或其他主張[203]。歐盟 GDPR 強調保護資料主體（data subject）對個人資料（personal data）之控制與決定權，與非個人資料（non-personal data）之自由流通政策交相輝映。基於 GDPR 對個資基本權之尊重，學者將其資料主權之模型歸類為「個人主權（individual sovereignty）」，亦即對資料之主權掌握在個人－資料主體手中[204]。相對而言，美國法雖肯認個資保護係消費者權益之一環，在針對不同行業（sector-specific）之單行法中亦有零碎之個資保護規範，惟實際上該國政策向來力主資料之自由流通（free flow of data），且致力於保護大型平臺之商業利益[205]，故學者將其資料主權歸類為「企業主權（firm sovereignty）」，即由企業主宰資料。

細繹美國之資料政策，大型網路平臺獲致之商業利益，影響深遠[206]。最為著名之例子，應係 1996 年通訊端正法案（Communications Decency Act of 1996）第 230 條。該規定原則免除平臺業者之民事責任[207]，使其無論對網路言論採取消極不管，抑或積極管制之策略，均不因

---

203 *See* Gao, *supra* note 190, at 7. 該文引述之論點，係自傳統國際法上對「主權」之理解出發，並延伸至資料的觀點。

204 *Id.* 學界並有觀察，歐盟之資訊政策基本上圍繞在基本權之保護、民主制度之維繫、且重視在資訊市場下之公平性（例如：對中小企業之協助），故將之形容為「權利驅動模型（right-driven model）」，而與中國之「國家驅動模型（state-driven model）、美國「企業驅動模型（firm-driven model）」互相對照。*See generally* ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE THE TECHNOLOGY 1-11 (2023).

205 甚至有過於個人權利之保護，請參見下文之介紹。

206 *See* Selby, *supra* note 196, at 215-217.

207 詳細而言，包括（1）平臺業者不被視作出版者或資訊提供者（盾）、（2）平臺業者以合乎誠信（in good faith）之方法限制不當（如暴力、侮辱性）言論者不負

而招致法律責任[208]。該國同時正透過雙邊貿易條約輸出此種模型[209]，試圖形塑一種全球治理模式。晚近平臺自主管制（self-regulate）之規範模式，造就數位平臺成為當代的新管制者，加以對言論自由之斲傷、使用者難以對平臺究責等問題[210]，已變相剝奪個人權利。以資訊主權之觀點而言，此形同摧毀資訊主體擁有之個人資訊主權。又依本文所見，數位平臺言論管制之問題另一核心在於，從正當法律程序之觀點，應僅法院有權決定涉及個人權利相關爭議，惟平臺之內容稽核（content moderation）形同架空內國法院固有權限，並將權限移轉至「外國公司」，嚴重欠缺正當性。

反洗錢用途之人工智慧一旦進入國際化、資料整合之階段，將面臨類似問題。由反洗錢法制之規定以觀，經過傳統洗錢稽核程序，並遭回報為可疑交易者，接續進入法律程序之調查，重則可能承擔刑事法律效果。今若將傳統人力之洗錢稽核程序替換為以演算法為主之判斷模式，則演算法提出之警示回報，極大程度將與後續之執法流程緊密銜接。反洗錢法制之設計，雖不如前述美國之數位平臺政策般近乎解除司法介入，惟觀人工智慧在反洗錢領域之強大潛力，亦不排除招致公、私反洗錢部門之「自動化依賴」[211]而形同繳械之窘境，難保不會引發將法律適用判斷權限實質移交「外國公司提供之演算法」之質疑。與此同時，在人工智慧之透明性、安全性、課責性等重要爭議未解之際，只會徒增民

民事責任（矛）。*See* Liu, *supra* note 183, at 15-16. 當然，該法尚有不少基於刑事責任、智慧財產權等例外（carve-outs），惟已超出本文論述範圍，茲略而不論。

208 *Id.* at 28.該文並認為，此形同使「言論自由」之決定權，落入大型數位平臺手中。

209 學界主要觀察北美貿易協定（United States-Mexico-Canada Agreement, USMCA）、美日數位貿易協定（U.S.-Japan Digital Trade Agreement）之規範輸出，對加拿大、墨西哥與日本內國政策之影響。*Id.* at 8-11.

210 Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1662-1664 (2018).

211 請參見李榮耕，刑事程序中人工智慧於風險評估上的應用，政大法學評論，第168期，頁175-177，2022年3月。

眾、各國政府對此技術之質疑。

觀近期反洗錢演算法平臺之發展，即便其終能排除萬難，達成資料、部署、標準統一等國際整合目標，其不當利用個人資料、架空正當法律程序之疑雲，仍不免湧現，前述數位平臺之爭議足以借鑑。固然，洗錢防制之執法正當性、必要性，解釋上似可能認為高於數位平臺對危險言論之管制，惟相關系統開發者、服務提供者，仍應將數位時代資訊政策之演變之討論納入考量，以免招致剝奪個人資訊主權、架空內國正當法律程序等質疑。

伍、結論

洗錢防制，自 20 世紀後半葉以降，已成顯學，理由不外乎洗錢手段之光速演變、資恐風險之急劇上升，以及數位時代下，犯罪者透過先進科技探鑽執法漏洞之種種問題。洗錢行為非當代社會所能容許，蓋一旦給予犯罪者自不法行為獲利之餘地，形同宣示犯罪只要不被執法機關發現，即穩賺不賠。據此，洗錢防制行動旨在宣示－犯罪不僅無從獲取利益，更使人背負洗錢罪名，得不償失[212]，據以降低犯罪誘因。

當代洗錢行為之複雜性、科技性，已非傳統人力防制之手段所能因應。金融機構採取人力洗錢稽核程序者，多為嚴重之偽陽性警報所困，加以人力稽核嚴重之資源浪費、錯誤百出，成為反洗錢執法難有起色之罪魁禍首。基於人工智慧可訓練、快速演化、精準性、穩定性、經濟性等重要優勢，引進人工智慧防制洗錢，不僅有望降低過半之偽陽性警報、實現反洗錢人力資源之妥適分配，更可能借助人工智慧多維度之觀察能力，揪出複雜金融犯罪網背後之藏鏡人。近年發展下，Ayadsi、SAS 與 Google 等反洗錢系統已經上路，未來發展值得期待。

不過，人工智慧反洗錢系統之部署，仍不免遭遇障礙。首先，此類

212 林鈺雄，同註 11，頁 35。

方案既然涉及人工智慧，即不能逃脫當代人工智慧管制競爭之魔掌，相關服務提供者除應符合反洗錢法制之要求外，更應密切關注歐盟法、美國法或其他陣營之發展趨勢，及其對各國人工智慧政策之影響。其次，在數位平臺橫掃全球之當代，許多國家開始轉向要求網路服務提供者將敏感之個人資料儲存於境內，此種資料在地化之趨勢，可能阻礙反洗錢人工智慧相關資料庫之國際整合，並影響相關演算法之開發與運用。最後，數位平臺在近年掌握資料主權所招致之批評，殷鑑不遠。反洗錢演算法既與洗錢之執法流程相輔相成，自不免產生類似資料主權爭議之批評，相關演算法之開發者、部署者，均應留意數位時代之資料政策議題，以建構其輔助洗錢案件執法之最大效益。

參考文獻

中文

一、期刊論文

王志誠，洗錢防制法之發展趨勢－金融機構執行洗錢防制之實務問題，月旦法學雜誌，第 267 期，頁 5-18，2017 年 8 月。

吳俊志，洗錢防制法修法對人頭帳戶的影響，月旦財稅法令，第 46 卷，第 18 期，頁 9-11，2023 年 9 月。

李怡萱，重新思考虛擬資產與洗錢犯罪之可罰性關係，檢察新論，第 32 期，頁 234-255，2023 年 5 月。

李榮耕，刑事程序中人工智慧於風險評估上的應用，政大法學評論，第 168 期，頁 117-186，2022 年 3 月。

林志潔，兆豐案天價罰款的啟示－美國反洗錢法的重點與金融業應有的作為，月旦法學雜誌，第 259 期，頁 34-48，2016 年 11 月。

林鈺雄，普通洗錢罪之行為類型－評析洗防法第 2 條，月旦法學教室，第 224 期，頁 35-51，2021 年 6 月。

邵之雋、李怡萱，人壽保險公司所受洗錢及資恐風險與相應抵減風險措施研究，交大法學評論，第 13 期，頁 123-160，2023 年 9 月。

胡　林，AI 超譯資料：Ayasdi、SAS 防洗錢揪出金融詐欺師，能力雜誌，第 767 期，頁 52-55，2020 年 1 月。

張明偉，論洗錢防制，軍法專刊，第 68 卷，第 4 期，頁 1-30，2022 年 8 月。

曹維傑、黃亞森，虛擬通貨反洗錢辦法及打擊資恐辦法之立法及虛擬通貨產業查核實務，會計師季刊，第 293 期，頁 49-58，2022 年 12 月。

楊岳平，虛擬通貨的洗錢防制監管疆域與國際標準－評我國「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」，法律扶助與社會，第 9 期，頁 93-140，2022 年 9 月。

蔡佩玲，虛擬貨幣與洗錢防制－未知之金流世界交易規則，月旦法學雜誌，第 324 期，頁 132-142，2022 年 5 月。

蔣念祖，藝術品拍賣業該管了－如何填補洗錢防制漏洞之探討，當代法律，第 9 期，頁 140-147，2022 年 9 月。

魏至潔，論非同質化代幣法律定位及我國相關法規適用－以洗錢防制為例，檢察新論，第 31 期，頁 196-205，2022 年 11 月。

魏至潔，世界金流新秩序－FATF 虛擬資產規範及我國法制面整體建議，交大法學評論，第 12 期，頁 163-203，2023 年 3 月。

英文

一、專書

BRADFORD, ANU, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE THE TECHNOLOGY (OXFORD UNIVERSITY PRESS, New York, NY, 2023).

二、期刊論文

Alldridge, Peter, *Money Laundering and Globalization*, 35 J.L. & SOC'Y 437-463 (2008).

Alsuwailem, Alhanouf Abdulrahman Saleh & Saudagar, Abdul Khader Jilani, *Anti-Money Laundering Systems: A Systematic Literature Review*, 23 J. MONEY LAUNDERING CONTROL. 833-848 (2020).

Blum, Jack A., Levi, Michael, Naylor, R. T. & Williams, Phil, *Financial Havens, Banking Secrecy and Money Laundering*, 4 TRENDS ORG. CRIME 68-71 (1999).

Bradford, Anu, *Europe's Digital Constitution*, 64 VA. J. INY'L L. 1-68 (2023).

Bradford, Anu, *The Brussels Effect*, 107 NW. U. L. REV. 1-68 (2015).

Calo, Ryan, *Robotics and the Lessons of Cyberlaw*, 103 CAL. L. REV 513-564 (2015).

Chae, Yoon, *U.S. AI Regulation Guide: Legislative Overview and Practical Considerations*, 3 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (FASTCASE) 17-40 (2020).

Chagal-Feferkorn, Karni A., *How Can I Tell if My Algorithm Was Reasonable?*, 27 MICH.TECH. L. REV. 213-261 (2021).

Chander, Anupam & Le, Uyen P., *Data Nationalism*, 64 EMORY L.J. 677-739 (2015).

DiPiero, Carmine, *Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web*, 2017 U. ILL. L. REV. 1267-1299 (2017).

Estrada, Juan Carlos, *The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering*, 16 RUTGERS BUS. L.J. 383-408 (2021).

Fincham, Derek, *Art, Antiquities, and Money Laundering*, 111 KY. L.J. 309-344 (2022).

Garcia-Bedoya, Olmer, Granados, Oscar & Burgos, José Cardozo, *AI against Moneylaundering Networks: The Colombian Case*, 24 J. MONEY LAUNDERING CONTROL. 49-62 (2021).

Han, J., Huang, Y., Liu, S. et al. *Artificial intelligence for anti-money laundering: a review and extension*, DIGIT FINANCE 211-239 (2020).

Klonick, Kate, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598-1670 (2018).

Lemley, Mark A. & Casey, Bryan, *Remedies for Robots*, 86 U. CHI. L. REV. 1311-1396 (2019).

Levi, Michael & Reuter, Peter, *Money Laundering*, 34 CRIME & JUST. 289-375 (2006).

Liu, Han-Wei, *Exporting the First Amendment through Trade: The Global "Constitutional Moment" for Online Platform Liability*, 53 GEO. J. INT'L L. 1-56 (2021).

McDougall, Simon, *More Speed, less Haste: Finding an Approach to AI Regulation That Works for the UK*, AMICUS CURIAE 104-125 (2023).

Parinandi, Srinivas & Crosson, Jesse & Peterson, Kai, & Nadarevic, Sinan, *Investigating the Politics and Content of US State Artificial Intelligence Legislation*, 26 BUS. & POL. 240-262 (2024).

Pavlidis, Georgios, *Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of Anewer*, 24 J. MONEY LAUNDERING CONTROL. 155-166 (2023).

Rohit, Kamlesh D & Patel, Dharmesh B, *Review on Detection of Suspicious Transaction in Anti-Money Laundering Using Data Mining Framework*, 1 INT. J. INNOV. RES. SCI. TECHNOL. 129-133 (2015).

Selby, John, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both*, 25 INT'L J.L. & INFO. TECH. 213-232 (2017).

Singh, Charanjit & Lin, Wangwei, *Can Artificial Intelligence, RegTech and CharityTech Provide Effective Solutions for Anti-Money Laundering and Counter-Terror Financing Initiatives in Charitable Fundraising*, 24 J. MONEY LAUNDERING CONTROL. 464-482 (2021).

Swan, Kyle, *Onion Routing and Tor*, 1 GEO. L. TECH. REV. 110-118 (2016).

Van Wegberg, Rolf, Oerlemans, Jan-Jaap & Van Deventer, Oskar, *Bitcoin Money Laundering: Mixed Results?: An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin*, 25 J. FIN. CRIME 419-435 (2018).

Vogt, Sophia Dastagir, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 SANTA CLARA J. INT'L L. 104-124 (2017).

三、其他資料

BANK FOR INTERNATIONAL SETTLEMENTS, TRIENNIAL CENTRAL BANK SURVEY: OTC FOREIGN EXCHANGE TURNOVER IN APRIL 2022 (2022).

Breslow, Stuart, Hagstroem, Mikael, Mikkelsen, Daniel & Robu, Kate, *The new frontier in anti-money laundering, McKinsey & Company*, *available at* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-new-frontier-in-anti-money-laundering (last visited December 8, 2023).

FATF, 40 RECOMMENDATIONS (2003).

FATF, BEST PRACTICES ON COMBATING THE ABUSE OF NON-PROFIT ORGANISATIONS (2023).

FATF, EMERGING TERRORIST FINANCING RISKS (2015).

FATF, FATF METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS (2023).

FATF, FATF RECOMMENDATIONS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION (2012).

FATF, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL CURRENCIES (2015).

FATF, GUIDANCE ON RISK-BASED SUPERVISION (2021).

FATF, *History of the FATF*, *available at* https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html (last visited December 12, 2023).

FATF, TERRORIST FINANCING RISK ASSESSMENT GUIDANCE (2019).

FATF, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2021).

FINDLEY, MICHAEL ET AL., GLOBAL SHELL GAMES: TESTING MONEY LAUNDERERS' AND TERRORIST FINANCIERS' ACCESS TO SHELL COMPANIES (2012).

GAO, HENRY, DATA SOVEREIGNTY AND TRADE AGREEMENTS: THREE DIGITAL KINGDOMS, HINRICH FOUNDATION (2021).

Glover, Scott, Devine, Curt, Kamp, Majlie de Puy & Bronstein, Scott, '*They're opportunistic and adaptive': How Hamas is using cryptocurrency to raise funds*, *available at* https://edition.cnn.com/2023/10/12/us/hamas-funding-crypto-invs/index.html (last visited December 12, 2023).

Pakki, Jaswant et al., EVERYTHING YOU EVER WANTED TO KNOW ABOUT BITCOIN MIXERS (BUT WERE AFRAID TO ASK), Financial Cryptography and Data Security: 25th International Conference (2021).

Parodi, Emilio, *Italy police take down Chinese shadow network laundering mafia cash*, *available at* https://www.reuters.com/world/italy-police-take-down-chinese-shadow-network-laundering-mafia-cash-2023-10-04/ (last visited December 12, 2023).

THE WHITE HOUSE, BLUEPRINT FOR AN AI BILL OF RIGHTS (2022).

The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligenc*, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (last visited December 10, 2023).

Tokar, Dylan, *Google Cloud Launches Anti-Money-Laundering Tool for Banks, Betting on the Power of AI*, *The Wall Street Journal*, *available*

at https://www.wsj.com/articles/google-cloud-launches-anti-money-laundering-tool-for-banks-betting-on-the-power-of-ai-2512ccce?mod=business_minor_pos4 (last visited December 9, 2023).

Abstract

Within the realm of countering money laundering, a landscape characterized by progressively intricate methods, diverse sources of terrorism financing, and the widespread proliferation of technology-driven illicit activities, it has undeniably ascended to a pivotal position in legal and policy discourses. This paper embarks on an exhaustive exploration, commencing with a detailed exposition of the intricacies inherent in contemporary money laundering techniques. It meticulously scrutinizes recent instances wherein illicit transactions or money laundering activities have adeptly exploited advanced technological means, such as virtual currencies, prompting an in-depth inquiry into the evolving landscape of contemporary anti-money laundering legal frameworks. In response to the mounting intricacies of money laundering and the palpable inefficiencies associated with manual anti-money laundering audit procedures, this paper ardently advocates for the manifold benefits arising from the strategic integration of artificial intelligence into money laundering prevention methodologies. Beyond introducing recent trends in developing anti-money laundering algorithms, it sheds light on the continuous innovation within artificial intelligence solutions designed explicitly to counteract the multifaceted challenges of evolving money laundering activities. Moreover, the paper strategically pivots towards a nuanced discussion surrounding the potential challenges artificial intelligence anti-money laundering solutions might face shortly. These challenges encompass the variations in artificial intelligence policies among nations still navigating developmental stages and the hindrances arising from the overarching trend towards localized data. Additionally, the paper carefully addresses the potential impacts on

anti-money laundering algorithms stemming from disputes related to digital sovereignty, further complicating the landscape. As the international community grapples with these multifaceted challenges, this paper seeks to enrich the ongoing discourse by providing profound insights into the intricate nature of money laundering prevention in an era characterized by rapid technological advancements and the ever-expanding web of global financial interconnectivity.

Keywords: Money Laundering, Anti-Money Laundering, Technological Regulation, Artificial Intelligence, Data Localization, Digital Sovereignty