

《專題報告》

金融監理科技與司法實務：AI 生成證據於金融犯罪偵查之法律應用

第一章 導論

第一節 研究動機與目的

隨著國際間貿易往來愈發頻繁以及近年生成式 AI 快速發展，以及各類型金融工具層出不窮，消費者在現今資訊量爆炸世代難以辨別投資陷阱，各類型的新型投資在高獲利的誘惑下，使受害者數量及犯罪金額不斷攀升，自內政部警政署統計 113 年第 4 季被害人財損金額新臺幣 500 萬元以上高額財損詐欺案件總計發生 1,677 件，佔總發生數 5 萬 4,113 件的 3.1%、損失金額 211 億 6,167 萬餘元，佔總財損金額 371 億 9,099 萬餘元的 56.9%，以「假投資詐騙」最為嚴重¹

傳統偵查方法對金融犯罪的追緝效果有限，尤其在涉及跨境、匿名化或高技術性操作之案件中，偵查難度更為加劇，在此背景下，因檢警機關難以追查新型的投資詐騙或跨境洗錢，是以，立法院於

¹ 內政部警政署，113 年第 4 季高額詐欺財損趨勢剖析 3%詐騙案造成逾 57%財損！內政部籲民眾投資務必審慎小心以免被騙，114 年 1 月 16 日，

https://www.moi.gov.tw/News_Content.aspx?n=4&sms=9009&s=324961

2024 年七月三讀通過增訂刑事訴訟法十一章之一特殊處分專章，允許新型的科技偵查²，是以可觀察到立法者認為在有相關監督配套措施之情況下，科技偵查能平衡對於被告隱私權、人格權之影響以及犯罪偵查之需要，肯認使用科技手段。

除了一般刑事犯罪，金融監理因相關金融科技（FinTech）如電子支付、線上借貸、區塊鏈技術蓬勃發展，且長涉及多節點的跨境交易，所產生的資安問題與防治詐騙需求，對於金融監理亦須引進科技監理，如如自動化交易異常偵測、跨錢包交易路徑分析、智能合約行為監控等，在檢警機關之偵查方法包括使用外部 AI 軟體輔助調查與分析以釐清交易網絡與犯罪路徑，惟我國實務上對其證據能力仍有爭論，以及是否對於人民的資訊隱私權侵害過大，仍具高度爭議性，亦為學者所討論研究之對象。

從兆豐銀行紐約分行因洗錢內控等疏失遭美國紐約州金融服務署（New York Department of Financial Services, DFS）裁罰 1.8 億美金之案件³，可見金融監理（如反洗錢 AML）之合規性重要性日漸重要，

² 司法院，立法院三讀通過刑事訴訟法部分條文修正草案 增訂特殊強制處分規範、確立偵查中辯護權範圍，113 年 7 月 6 日，<https://www.judicial.gov.tw/tw/cp-1887-1127612-cc4fc-1.html>

³ 高等檢察署，兆豐銀行洗錢案新聞稿，109 年 4 月 17 日，<https://www.tph.moj.gov.tw/4421/4447/757204/757251/post>。

生成式 AI、深偽技術（Deepfake）與自動社交工程等工具亦成為不法分子從事金融詐騙的新利器，這些 AI 技術不僅提升詐騙效率，更增加監管機關在即時偵測與風險控管方面的挑戰。

國外針對金融監理科技工具因發展歷史較為深遠，已有相關法制為規範，本文亦以比較法研究進行討論，將以新型科技方法於法庭上之可用性為核心，尤其是以 AI 證據之使用為論述核心，兼論其與金融業使用 AI 工具防治金融犯罪的法律風險與限制，並以幣流分析軟體或其他 AI 辨識結果為例，討論於金融犯罪偵查中可能引發的證據能力爭議與基本權侵害隱憂，最後以歐美對於 AI 使用的立法趨勢，為我國對於 AI 全面性使用的規範進行借鏡。

第二節 研究問題

人工智慧在金融監理以及犯罪偵查中的應用廣泛，目前已有 61 家金融業者導入生成式 AI，占使用 AI 金融業者之比例達 48%，年增 21 個百分點，未來有 47% 之業者表示會在內部行政作業、智能客服、打擊金融犯罪等領域引進 AI 使用⁴，除了從用戶端如金融業者使用

⁴ 金管會，金管會公布金融業應用人工智慧 AI 調查結果新聞稿，

https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202505200001&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News

（最後瀏覽日：2025 年 9 月 6 日）

AI 來提高作業生產效率、節省人力、提升客戶體驗，而使用的方面據金管會統計，應用 AI 之領域前三名為內部行政作業佔 27%以及智能客服 19%以及認識客戶（KYC）以及防範金融犯罪則佔 14%，可見金融業應用 AI 有逐漸增加的趨勢。

本文對於 AI 應用之範圍限定於金融領域在 KYC 客戶調查、反洗錢(AML)偵測、高風險交易示警系統等應用，聚焦在具備機器學習及機器訓練過程並可獨立提出判定或預測結果的技術類型，並專注於在刑事案件發生時，由 AI 軟體所生成的資訊報告、可疑交易現金流統計之報告，成為刑事偵查與審判中的關鍵「證據」時，現行刑事訴訟法與證據法應如何判斷其合法性、證據能力與證明力，以虛擬貨幣之幣流分析作為例子，是否可作為證據使用。

再與歐盟及美國對於 AI 生成之證據之認定與實際於法庭上使用時，如何平衡科技應用與程序正義，為後續的修法建議提供參考依據。

第三節 研究方法

本文主要透過文獻分析，搜集我國及外國司法實務對於 AI 證據之證據能力判斷與證據法之研究，以我國法治為核心另外使用比較法之方式整理歐盟與美國對於金融機構使用 AI 之相關規範與行政準則，與我國對金融業使用 AI 之指引為比較，以期尋找未來合規機制

可增進之方向。

第二章 金融犯罪之特徵及 AI 在我國金融業之應用

第一節 金融犯罪的特徵

金融犯罪（亦稱）大概可以分成以下三種類型，一是以金融體系為犯罪工具的犯罪行為；二是攻擊金融體系的犯罪；三是發生在金融體系內部的犯罪，金融犯罪因實際上時常不會有實際受害之相對人，而係對整體性金融秩序的破壞行為⁵，而在現今網路發達的時代，金融犯罪亦延伸到來自外部的駭客攻擊，竊取客戶資訊造成資安風險，以及新型金融商品例如虛擬貨幣，因其交易的特性而難以追溯犯罪，又因人工智慧快速發展，投資詐欺受害者與受害金額逐漸擴大，須先定義金融犯罪的特徵，再說明為何金融犯罪於刑事案件的追溯難題。

一、 金融犯罪的特徵⁶

1. 缺乏犯罪現場且蒐證困難

⁵ 詹德恩，我國金融犯罪特性與抗制問題，中正財經法學，第7期，頁165，2013年07月。

⁶ 同前註，頁167。

金融犯罪往往有其複雜性、專業性與巨額性，通常金流為全線上且不公開，進行交易有時亦難以重現犯罪現場，對於會計賬簿、虛擬貨幣金流追查等，蒐證方式不同於傳統的搜索扣押，必須仰賴鑑識會計（forensic accounting）等專業職能，才能取得有證明力的證據，法院欠缺財經專業背景致需仰賴，於審理時僅依不明確之法律規範，常導致無法認定事實及取捨證據，故需特定蒐證之偵查程序及鑑定證據辦法，始可解決金融犯罪相關之爭議，另因其犯罪時間可能長達數年持續進行⁷，相關事證可能早已灰飛煙滅，致蒐證相對困難。

2. 被害人不明顯但損害高

金融犯罪有時是對於整體金融市場之影響，例如內線交易、操縱市場，而於投資詐騙的情況，加害人與受害人之界線往往模糊，例如提供人頭帳戶，但同時也是受害者，因有時係貪圖一己私念，對於被害者社會責難性較一般傳統強盜、殺人刑事案件高；另外被害人數往往為多數或涉案金額較高，行政規範亦有定義重大之金融犯罪之範圍：「檢察機關辦理重大經濟犯罪案件注意事項」第二條，將犯特定犯罪所得或被害金額修訂

⁷ 呂倩茹，我國經濟犯罪調查偵查陷入困境之論證，法令月刊，第 67 卷第 7 期，頁 129，2016 年 07 月。

達 5,000 萬以上，或被害人數達 50 人以上者，足以危害社會經濟秩序者，定義為重大經濟犯罪，作為量刑上之考量。

3. 被告社經地位高且屬共犯結構

所謂金融犯罪之型態在我國實務上，大多可分為證券交易市場類，包括操縱股價、內線交易；證券發行市場掏空公司資產類，例如利用子母公司為虛假現金週轉最終掏空公司；證券發行市場財報或資訊不實，常見為依法申報之財務報表或公開說明書之不實隱匿，或會計師為重大虛偽不實或錯誤記載或意見；銀行授信不法，例如不合規的違法超貸；最後還有違法經營金融業，例如銀行法 29 條，非銀行經營收受存款受託經理信託基金、公眾財產或辦理國內外匯兌事務⁸。

根據這些金融犯罪型態，可見其通常公司或機構型態，有上命下從之關係，另外在重大經融犯罪時常被告為公司高階經理人或董事，甚至有時亦有媒體或民意代表影響力，對檢警偵辦有一定之輿論影響。

4. 犯罪手法具高技術性且複雜

⁸ 莊正，金管會如何協助偵辦金融犯罪及現金經融犯罪的重要課題，日新司法，2008 年 7 月，頁 249-250。

因被告多具財務會計金融專業，故時常以多節點的、多層次 (layering) 型態隱藏金流，或是以多頭公司為虛假交易進行洗錢，對犯罪偵查增添難度。

5. 被告容易串供並滅證

如前述，金融犯罪之特徵係多以公司型態為犯罪，具共犯結構，容易互相包庇之情況，另因金融、報表、會議記錄，通常係以電磁紀錄的形式存在，證據不易搜索且滅證可能性高。

6. 容易影響資本市場造成投資人權益受損

例如證券交易法 159 條之一內線交易的立法目的為健全與保護交易市場公平，不許利用未公開重大消息為交易，同常此種情況損及整體市場，傷害不特定投資人權益受損，通常涉案金額較高。

7. 產生巨額犯罪所得進行洗錢與潛逃出境之虞

因涉案金額甚鉅，且因海外追查不易，被告通常在境外成立公司為虛偽循環交易，或將資金匯往國外再轉匯回國內，造成全盤犯罪事實不易建構；且因其在海外如有置產或提前轉移，極高機率會潛逃海外，此時為了限制被告出境，需要各部門之整合，包括警察及調查機關以「入出國及移民法」第六條第一項第六款⁹限制出境、檢察官則依刑事訴訟法 93 條、228 條第四

⁹ 第 6 條 國民有下列情形之一者，移民署應禁止其出國：

項，傳喚被告或限制住居嚴格限制被告，已達日後犯罪追溯效果。

上述七款金融案件之特徵，使金融案件具有其特殊性，不僅有追溯之困難，亦有發現之困難，本部分凸顯，金融監理之必要，以及主管機關與檢警機關的資源整合的重要性。

二、 金融刑事案件之追溯難題

金融犯罪難以追查主要係於是否進行追溯及移送相關證據階段。在是否進行追查主要之難點在於因金融犯罪往往沒有現場，且用層層合法行為掩飾非法，且通常證據有高度專業性或為電磁紀錄，需有專門的勘驗設備以及專業知識背景之人，另外因其共犯結構，往往難以透過證人之證詞搜集有力資訊¹⁰，另外現行檢警可使用之金融

一、經判處有期徒刑以上之刑確定，尚未執行或執行未畢。但經宣告六月以下有期徒刑或緩刑者，不在此限。

二、通緝中。

三、因案經司法或軍法機關限制出境。

四、有事實足認有妨害國家安全或社會安定之重大嫌疑。

五、涉及內亂罪、外患罪重大嫌疑。

六、涉及重大經濟犯罪或重大刑事案件嫌疑。

七、役男或尚未完成兵役義務者。但依法令得准其出國者，不在此限。

八、護照、航員證、船員服務手冊或入國許可證件係不法取得、偽造、變造或冒用。

九、護照、航員證、船員服務手冊或入國許可證件未依第四條規定查驗。

十、依其他法律限制或禁止出國。

¹⁰ 同註 7，頁 141。

監管手段法規範不足，無權限為事前或長時間的監控，故在搜集事證至足矣起訴之階段具有困難性。

是以經濟犯罪難以追溯的原因係因事證搜集難，犯罪事實時常難以呈現，以及難以沒收不法所得，因此日常的金融監理（Sub Tech）、法律遵循（Reg Tech）更為重要，需透過日常申報以及高風險交易偵測，藉由機器學習(Machine Learning)及人工智慧(Artificial Intelligence)，來大量搜集、分析並訓練來監測高風險交易，以利監管機關及早介入，避免損害繼續發生。

第二節 AI 在金融監理之應用概況

所謂金融監理可分為法遵科技（Regulatory Technology ,RegTech）以及金融監督（Supervisory Technology ,Suptech），而目前因應人工智慧的發展階段，再改之能理方面可分為初級、中極、高級，初級算力主要係協助大量的資料處理，提供重複性且制式的自動回答，中期則更能解讀資訊並主動解讀示警，或是為客戶制定財富管理計畫（如：理財機器人）¹¹等可以透過深度學習採取更靈活之相應行為，而高級則係指人工智慧具備原生認知能力或自我意識，我國目前在 AI 上應用處於感知能力中期¹²，主要為資訊處理、內控機制監

¹¹ 蕭俊傑，人工智慧與金融應用，財金資訊季刊，95 期，2019 年 7 月，頁 26。

¹² 杜研禎，〈金融業人工智慧應用之金融監理規範研究〉，國立成功大學法律學系碩士班碩士論

理以及透過事先設定之資料學習為客服主動式問答等。

目前 AI 於金融業之應用除了為提供客戶服務與內部企業行政作業外，亦應用於企業法律遵循，特別是 KYC 認證以及洗錢防制（反洗錢 AML）上之應用，首先在 KYC 認證上，係在符合個資法與歐盟《一般資料保護規範》（GDPR）下對於客戶之背景資料為識別並驗證客戶身分，對於受 AML（反洗錢）法規約束的公司尤其重要，因此 KYC 程序允許在建立業務關係之前檢索客戶資料來建立客戶的風險概況，通常是在數位開戶或交易過程中透過收集客戶的個人資料和身分證件，故需要由於相關資訊龐雜且不可能僅憑人腦記憶足以處理，因此必須依靠大數據基礎，並由人工智慧技術進行精確分析，人工智能所能提供的便利性具體包括：整合內部客戶資料以建立完整的帳戶資料庫並進行影像識別；清理帳目涵蓋多個報表系統所產生的重複資料；從外部相關資料來源收集與資訊以檢驗客戶所提供資訊的正確性¹³。

在反洗錢(Anti-Money Laundering,AML)之實際應用，則係因需留存交易紀錄，或是由 AI 提醒，提醒法令遵循部門的人員及法遵長重

文・2023 年 1 月・頁 121。

¹³ 韓其珍，AI 在洗錢防制及打擊資恐業務上的實際運用，中研院，台灣人工智慧行動網，<https://ai.iias.sinica.edu.tw/ai-on-aml-and-cft-in-practice/>（最後瀏覽日：2025 年 8 月 31 日）

視洗錢高風險帳戶的活躍問題，此以 AI 進行提示及警告便是健全洗錢防制及打擊資恐所不可或缺的業務系統。

不論是在 KYC 程序中對於客戶的風險評價與個資搜尋之分析結果，或是 AML 分析報告、高風險交易之示警報告等，如為 AI 所生成，可能涉及資訊安全防護風險、數位歧視風險，因其快速生成與不可解釋性¹⁴，在司法案件提出時，難以說明辨識證據之真偽，以及依何特定交易所為的判斷，因其涉及大量數據分析與黑盒子自動生成，在實務上難以用數位證據的方式為驗真，故學界對於 AI 生成之證據是否承認，仍有待釐清，以下著重於則以我國 AI 生成之證據能力與各國相關實務與規範進行整理介紹。

第三章 AI 證據於我國刑事訴訟法上之適用

第一節 我國是否承認 AI 證據

生成式 AI 在司法上的風險，主要分為兩類，一類為輔助審判程序，是否影響法官心證為核心進行討論，¹⁵另外則是對於 AI 生成內

¹⁴ 王志誠，人工智慧在金融業運用之法律風險及監控，當代法律，第 28 期，頁 17，2024 年 04 月。

¹⁵ 李建良、蘇凱平等，以人工智慧輔佐法院心證——統計證據之觀點，司法院台灣人工智慧行動

容是否具有證據能力之討論，因與數位證據具有本質上之不同，數位證據文獻將之定義為透過電腦或相似裝置儲存、傳輸，用以認定（或否證）被訴犯罪存在的資料，這些資料是透過二元方式儲存，亦即 0 即 1，並透過電腦設備轉換成人類可以理解的内容，包含文字檔、圖像檔、音檔或影像檔，故可用傳統之搜索扣押或監聽之強制處分取得，並經數位驗真，作為法庭上可使用之證據¹⁶；而 AI 證據則係由 AI「生成」的資料，如高風險帳戶示警、或是對違法交易自動申報的判斷，時常為偵查機關開啟調查的前哨，甚或會作為起訴證據之一環，但生成式 AI 因其在生成時具有不可解釋性，不論係作為證據或輔助法官判斷，因其黑盒效應以及因訓練資料常會有不準確或有認知偏差之情況¹⁷，使得生成式 AI 在實務上之應用受到挑戰，因我國刑事訴訟法第 154 條、第 155 條明確規範犯罪事實應依證據認定，且無證據能力或未經合法調查之證據，不得作為判斷依據認定犯罪事實，以下主要針對可否作為我國刑事訴訟法之「證據」進行討論。

網，2020 年 12 月 18 日，<https://ai.iias.sinica.edu.tw/ai-assisted-evaluation-of-evidence/>。

¹⁶ 林育賢，數位證據之取證與證據能力，司法新聲，第 135 期，頁 19，2020 年 11 月。

¹⁷ 張麗卿，生成式 AI 對刑事實務之挑戰（下），月旦法學雜誌，第 351 期，頁 2，2024 年 08 月。

1. AI 證據之屬性

以訓練過程中可獨立提出判斷或偵測結果之生成式 AI 模型為例，生成之過程可分為兩階段，第一階段為搜集資料來訓練模型，此部份因其訓練資料仰賴技術人員篩選資料與校正，故有人證之性質；而在後階段由機器所生成之結果或報告，亦不脫離物證之本質，如認為係人證則需要輔以傳聞法則，進行詰問，惟詰問之對象為使用該資料之當事人，抑或軟體開發商不無疑問；如認為係物證，傾向將此類證據視為一種不具備人類陳述的機器生成資料，因而不考慮適用以人類主張為前提的傳聞法則及詰問權。

如為物證，是否可以用「數位證據」中之電腦紀錄來檢視其屬性，首先美國實務就電腦紀錄又可再分為「電腦存儲紀錄」(computer-stored data)與「電腦生成紀錄」(computer-generated data)¹⁸，前者為單純儲存人為交流之紀錄，因電腦輸出之資料是人類證述內容的直接紀錄時，該紀錄只是人類證述內容轉換至電腦儲存載體而已，因而具有人類於法庭外陳述之性質，適用傳聞法則；後者主要是指完全不經人為介入而由電腦紀錄與產出，例如電腦產出的通聯紀錄，其性質上因無「人」介入，故不適用傳聞法則，惟應

¹⁸ State v. Armstead, 432 So. 2d 837, 840 (La. 1983).

考慮電腦的計算結果，是否屬於證據法定義的科學證據，故須通過科學證據之可信信審查¹⁹。

本文認為考量風險示警或金融交易紀錄分析報告，皆為自動由電腦判斷，人為介入程度少，而軟體開發商所為的設計僅為篩選關鍵字、統計、計算分析結果，為客觀性、機械性判斷，難謂有對於個案行為有所評價而具有人證之性質。故性質上較類似於物證。

2. 證據能力

如認為 AI 生成之報告為物證屬性，那究竟屬於何種類之物證？係屬數位證據或電磁紀錄抑或認為仍有人證之性質，例如專家證人報告、或是鑑定報告等適用人證的證據程序，將影響其補強證據能力之要求，以及證據能力判斷，對於 AI 生成之分析報告國內及國外多有討論。

我國實務上有將虛擬貨幣「幣流分析」說明作為法庭證據的例子，當事人使用 AI 技術產出幣流分析報告作為建構犯罪事實之證據，被法院認為其性質上屬於「鑑定報告」²⁰ 準用刑事訴訟法 206

¹⁹ 曾小蓉、金孟華，AI 在刑事證據法之研究----以美國聯邦證據規則為核心，歐美研究，第 55 卷第一期，2025 年 3 月，頁 21。

²⁰ 臺灣高等法院臺中分院 113 年度金上訴字第 436 號判決、臺灣高等法院臺中分院 113 年度金上訴字第 1361 號

條第 208 條所定「鑑定之經過及其結果」之法定要件，由鑑定人為言詞或書面報告，即屬同法第 159 條第 1 項「法律有規定者」之傳聞例外，惟於眾多判決中，僅查詢到此二判決就採用 AI 技術產出幣流分析報告之證據能力進行論述，其餘 AI 證據相關之判決多依刑事訴訟法第 159 條之 5 經當事人同意作為證據，或因行簡式審判程序而不適用第 159 條第 1 項關於排除傳聞證據規定之限制，而未進一步進行說明涵攝。

本文亦採肯定見解，因刑事訴訟法於 2023 年 12 月 1 日通過修正鑑定章節，從第 206 條之文義解釋，鑑定報告應包括鑑定人之專業能力、足夠之事實或資料基礎，以及可靠原理及方法之適用，應使鑑定人到庭陳述，如陳述為真正得為證據，亦即肯認鑑定報告得為證據，又從立法理由觀察，206 條為促進真實之發現，保障被告之詰問權，故如使用 AI 幣流分析之報告作為證據使用時，如經可驗證之事實或資料（例如公開鏈上的資訊、如何交叉比對之原理解析）且工具本身具有可驗證性與可解釋性，再加上鑑定人之現場陳述，並無一定禁止使用 AI 生成之結果報告之理。

另外就科技發展衍伸之新型證據方法之可信性上並非僅有 AI，隨著科技發展，現代鑑定工作需使用科技之輔助例如 DNA 鑑定

(包括鑑識調查性基因族譜學 Forensic Investigative Genetic Genealogy, FIGG²¹)、毒物氣相層析質譜儀(GC/MS)等，都是經由科學性的解釋，並經法院實務累積，肯認在法院上使用之證據可信性，可見法院對於藉由新型科技之證據方法採開放態度²²，就前述所舉的 AI 幣流分析報告之新型科技方法而言，虛擬資產領域中所使用之幣流分析軟體屬於特定專業領域內之進階分析工具，其所輸出結果，應解釋為鑑定人結合專業知識與科技工具所為之鑑定過程與結論，符合所要求之「鑑定之經過及結果」構成要件，例如臺灣高等法院臺中分院 113 年金上訴字第 436 號判決即指出：「搭配使用幣流分析軟體 Chainalysis.....使用該軟體工具分析所得資料通常具有參考性」是以實務肯認科技工具所輔助之鑑定分析具備相當程度之證據能力。

亦有學說從「證據的生命週期」(the evidentiary cycle) 的概念²³，其係作為面對新型證據時，可概略分析可信度在哪一階段之判斷

²¹ Oliver M. Tuazon et al., Law Enforcement Use of Genetic Genealogy Databases in Criminal Investigations: Nomenclature,

Definition and Scope, 8 FORENSIC SCI. INT' L.: SYNERGY, 2024, at 2. ; 中文文獻亦可參見：吳宜蓁、金孟華，基因族譜學在刑事司法的應用，萬國法律，第 261 期，頁 94，2025 年 06 月。

²² 僅列舉部分實務判決：最高法院 114 年度台上字第 2473 號刑事判決、最高法院 112 年度台上字第 2523 號刑事判決

²³ Sabine Gless, AI In The Courtroom: A Comparative Analysis Of Machine Evidence In Criminal Trials, 2020. https://ius.unibas.ch/fileadmin/user_upload/ius/09_Upload_Personenprofile/01_Professuren/Gless_Sabine/AI_in_the_courtroom_GT-GJIL2020.pdf (Last Visited Sep. 1, 2025)

標準，亦即因為該證據方法太心而被認為不可靠時，需經過檢驗，檢驗過認為大致可靠時而最為證據使用，其通常需要食物之累積以及確保沒有濫用，係指即便此類 AI 之證據目前可能被認為是太新而不可靠的，也不排除 AI 形成的判定結果可能在未來會被普遍地認為可靠，故 AI 判定之證據並非完全禁絕²⁴。

第二節 小結

我國實務肯認由 AI「輔助」生成之證據，而非直接使用 AI 證據，符合刑事訴訟法第 206 條直接審理之要求，是以在金融業使用之 AI 工具，實際上亦為輔助性質，如涉及犯罪構成要件行為，仍是由主管機關與檢警合作，搜集完整的事證資料，AI 證據僅為犯罪基礎事實之一環，若鑑定人確已到庭說明 AI 工具之操作原理、輸入數據、風險評分模型與錯誤率驗證報告，並接受關於數據選擇、參數設定、及結果解讀等方面的交互詰問，已足以落實我國刑事訴訟法第 206 條實質保障當事人之防禦權之立法理由，如使用自動偵測所生成之報告，或是利用 AI 工具輔助大範圍之統計，有利於犯罪事實

²⁴ 參前註 19，頁 22。

之發現，在衡平被告之防禦權與追訴犯罪之社會法益下，應認為 AI 生成之報告可為證據，並已具有證據能力。

第四章 其他國家立法趨勢之比較法分析

第一節各國對於 AI 生成內容立法趨勢

1. 歐盟

歐盟為作為最早對於 AI 建置全面規範之地區，其於 2024 年通過之《AI Act》《人工智慧法案》並於 2024 年 8 月 24 日正式生效，其主要之核心為風險分期以及提供監管建議，《AI Act》第五條針對「不可接受之風險」再增加「受禁止人工智慧指引」對於例如高風險用途如司法決策、犯罪風險評估將被嚴格規管，並強調使用時須確保資料可追溯性與系統可解釋性、強制技術透明度與人為監督機制，以確保在教育、生醫、司法領域不受到 AI 之操縱或剝削²⁵，雖然歐盟對 AI 於「個人犯罪風險評估或預測」持

²⁵ 魏徹，歐盟執委會發布《受禁止人工智慧行為指引》，資工業策進會科法所，2025 年 4 月，<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=9322&no=64>。

排斥態度，但若僅用於輔助事實推論，則合理運用與權衡人權保障於司法仍有接受使用之空間。

另外，雖相關之子法如《人工智慧責任指令》（AI Liability Directive）因仍有疑慮而被撤回，為其可作為我國未來對於釐清 AI，我國也因應《AI Act》的發展，於近日行政院也通過《人工智慧基本法》草案²⁶，可見我國對於全面性之 AI 之發展也順應國際趨勢發展。

2. 美國

美國實務對於法庭上提出之 AI 證據，可先區分為是「已確認的 AI 生成證據」（“acknowledged AI-generated evidence”）亦即雙方承認使用 AI 所生成的證據，作為增強論述，將 AI 作為輔助工具使用，例如前述提到的 AI 幣流分析；以及未確認的 AI 生成證據（“unacknowledged AI-generated evidence”）指一方當事人提出證據，但另一方質疑其真實性，認為是 AI 所偽造的，例如深度偽造（Deepfake）就屬於此類²⁷。

²⁶ 行政院，政院通過「人工智慧基本法」草案 建構 AI 發展與應用良善環境 打造臺灣成為 AI 人工智慧島，2025 年 8 月 28 日，<https://www.ey.gov.tw/Page/9277F759E41CCD91/5d673d1e-f418-47dc-ab35-a06600f77f07>。

²⁷ Grossman, M., & Grimm, P. (2025). Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence. *Science and Technology Law Review*, 26(2).

而美國實務對於 AI 之證據是否可使用之標準，主要是美國聯邦證據法(Federal Rules of Evidence,FRE)，不論物證或人證，皆需要經過原始證據(Originality)、拒絕證言特權(Privileges)、關聯性、驗真以及傳聞證據之檢驗，始具證據能力，而 AI 證據通常於法院所爭執之原因係因缺乏有效性 (valid) 跟可信性 (reliable)，在已確認的 AI 生成的證據，其因雙方未爭執故屬於當事人同意使用之證據時，不再爭執於證據是否真正而重點在科學性以及對於案件的關聯性如何；又未經承認的 AI 生成證據，尤其是深度偽造 (Deepfake) 之證據，其是否得為法院所採則需要證實其真實性，並同時驗證其生成之方式是否可經美國證據法的檢驗，來證實其有效性以及可信性。

不論係已確認或未確認之 AI 證據皆須經檢驗，美國法對於科學技術之可信性的疑慮科學有效性之檢驗部分主要係以美國聯邦最高法院在 *Daubert v. Merrell Dow Pharmaceuticals*²⁸案中依據 FRE 第 702 條所提出的專家科學證詞，初步評估該證詞所依據的推理或方法論是否具備科學有效性，並且能夠恰當地應用於相關事實，但需注意該法條未明文列出 *Daubert* 案提出「可靠方法」

<https://doi.org/10.52214/stlr.v26i2.13890>

²⁸ *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993)

之五種標準²⁹，其修正理由指出係為保留於個案中法院判斷之彈性³⁰。

是以在科學有效性之部分此 AI 模型若可提出訓練資料、運算邏輯、驗證紀錄與錯誤率報告，並由專家證人驗證其方法如何應用於本案事實，則符合 FRE 第 702 條之規範，即應有證據能力

在證據的關聯性(Relevant Evidence Evidence) (FRE 第 401-403 條)³¹ 由 FRE 第 401 先解釋何謂關聯性³²，認為有該證據存在，則該事實存在與否之可能性時，較無該證據存在為高時，任何具有此一傾向之證據，且對結果有影響時，即屬具有關聯性之證據，而據有關聯系則必有證據能力³³，FRE 第 402 則係規定原則

²⁹ (1)理論或技術必須要能經過測試、證實；(2)該理論或技術必須經過同儕審查及出版；(3)法院應考量該科學技術之錯誤率；(4)是否存在並維持著該技術操作之標準作業程序；(5)是否為相關科學社群所普遍接受。(詳細標準內涵亦可參見：曾小蓉、金孟華，AI 在刑事證據法之研究----以美國聯邦證據規則為核心，歐美研究，第 55 卷第一期，2025 年 3 月，頁 25)

³⁰ FED. R. EVID. 702. 參見 FRE 第 702 條編纂委員會註解 (FED. R. EVID. 702 Committee Notes on Rules—2000 Amendment)

³¹ 蘇凱平，國民參與刑事審判程序的證據能力判定：兼論鑑定證據證據能力判定標準，國立台灣大學法學論叢，第 50 卷第 4 期，頁 1942，2021 年 12 月。

³² FRE 401. Test for Relevant Evidence Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.

³³ 陳文貴，論被告以外之人於審判中所為陳述之證據能力（六之四），司法週刊，2025 年 1 月 13 日。

上關聯性證據原則上具有證據能力³⁴；FRE 第 403 條則為排除條款³⁵，例如對於具有偏見或是不利影響之證據排除，雖 AI 證據可能有偏見或是誤導之可能而被 FRE 第 403 條排除的可能，為證據能理應審酌一切證據資料相互應證，不一定必排除其證據能力，而在 AI 證據上雖認為可能開發者在設計時，有偏見或歧視，但如經邀請開發商或專家為鑑定意見，法院並審酌 AI 證據（如高風險警示）而可解釋具體的考量條件與時間戳記或金流地圖等，仍有為證據的可能。

最後證據亦須經驗真（FRE 第 901 條）³⁶，以及自我驗真，亦即需具備形式上之真實性，證明其主張與案件相關的某項證據與其提供於法庭上之證據資料是相同的，AI 證據之驗真，則可參考對

³⁴ FRE 402. General Admissibility of Relevant Evidence Relevant evidence is admissible unless any of the following provides otherwise: the United States Constitution; a federal statute; these rules; or other rules prescribed by the Supreme Court. Irrelevant evidence is not admissible.

³⁵ FRE 403. Excluding Relevant Evidence for Prejudice, Confusion, Waste of Time, or Other Reasons The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.

³⁶ FRE 901. Authenticating or Identifying Evidence (a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is. (b) Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement: (1) Testimony of a Witness with Knowledge . (2) Nonexpert Opinion About Handwriting . (3) Comparison by an Expert Witness or the Trier of Fact . (4) Distinctive Characteristics and the Like . (5) Opinion About a Voice . (6) Evidence About a Telephone Conversation . (7) Evidence About Public Records . (8) Evidence About Ancient Documents or Data Compilations . (9) Evidence About a Process or System . (10) Methods Provided by a Statute or Rule . (因篇幅有限有省略部分)

於數位證據之驗真，對於產出的內容未經篡改提出證明，或是由專業人員出具意見等，亦可通過驗真程序。

以上為美國現行對於科學證據的「科學證據可信性」參考標準，原則在美國證據法框架下，AI 證據可為法院採用，須經專家鑑定或說明使該證據通過 FRE 第 403 條排除法則要求，將是否有偏見或誤導的情況加以說明，雖可能專家該發商因其有營業秘密或黑盒子³⁷的因素而無法通過 Daubert 法則而無法通過可信性檢驗，但仍有認為此新興科技隨著新證據之發展週期，仍有成為普遍認可之證據方法之可能，是以美國對新型科技證據採行開放的見解。

3. 英國

英國對於 AI 之使用雖無如歐盟《AI Act》為全面性的 AI 責任風險、監管與透明性要求之法規範，為其仍致力於對於 AI 發展的法規範依據，以行政規範：英國「支持創新的人工智慧監管政策白皮書」(A Pro-innovation Approach to AI Regulation)，於 2024 年 2 月 12 日發布《AI 保證指引》³⁸ (Introduction to AI

³⁷ 林勤富，歐盟《人工智慧法》之制度設計、規範內涵與治理局限，中研院法學期刊，第 36 期，頁 78，2025 年 3 月。

³⁸ UK Department for Science, Innovation & Technology, Guidance Introduction to AI assurance, Feb. 12, 2024, <https://www.gov.uk/government/publications/introduction-to-ai-assurance/introduction-to-ai-assurance>.

assurance)，其為提供企業使用 AI 之風險評估與判斷依準，主要有五大原則：五項原則³⁹分別為：安全、資安與穩健性（Safety, Security and Robustness）、適當的透明性與可解釋性（Appropriate Transparency and Explainability）、公平性（Fairness）、問責與治理（Accountability and Governance）以及可挑戰性與補救措施（Contestability and Redress），以因應 AI 自動化決策之風險。

金融領域應用 AI 之程度之經統計高於其他行應用的三倍⁴⁰，其中作為大規模統計財務報告、AML 反洗錢合規機制、演算法交易⁴¹等金融工作增加效率之工具，尤其是英國作為金融大國，相應之訴訟亦會產生，該指引特別強調：「若無制度性驗證與透明標準，AI 在司法領域中將無法取得社會信任。」因此，雖該準則並無法律效力，然其內容已逐漸成為英國公部門與法院引入 AI 資料時的依循準則。

³⁹ 劉心妍，英國發布《AI 保證介紹》指引，藉由落實 AI 保證以降低 AI 系統使用風險，資訊科技策進會科技法律研究所，2024 年 3 月 11 日，<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9187>

⁴⁰ KPMG, Artificial Intelligence in finance Artificial intelligence is transforming the future of finance. How does this transformation impact you?, <https://kpmg.com/nl/en/home/topics/future-of-audit/ai-audit.html> (Last visited 7 Sep.,2025)

⁴¹ Amanda McGrath & Amanda Downie, What is artificial intelligence (AI) in finance?, IBM, 24 July, 2025) <https://www.ibm.com/think/topics/artificial-intelligence-finance>.

第二節 小結

首先，歐盟有全面性之規範，其重點在於風險分級，雖歐盟對於高風險 AI 用途（如犯罪風險預測）雖設有限制，惟對於輔助事實發現之 AI 應用（如幣流分析、財務報告等），在符合資料可追溯性與透明度原則下仍予以肯認；美國則是使用美國聯邦證據法 FRE，以現有的法規範架構，檢驗新型科技證據，透過傳統數位證據的可信性、驗真、關聯性等，透過專家證人的到場說明或是傳聞法則、對質詰問法則適用之可能，建構 AI 生成之資料於法庭上之可用性；英國則較偏向於歐盟建構全面性的指引，供企業在使用 AI 時有評估標準，檢驗目前使用 AI 之透明度與資訊安全之保護，尤其是在金融領域因其資料具有高度的敏感性，應加強監管。

我國未來在制度層面上，也期待引進歐盟與美加規範內可學習之處，建立更完整的 AI 證據審查與監督機制，如 AI 證據鑑定人制度、錯誤率與模型評估報告強制附隨、建立可驗證的「AI 證據登錄平台」等，另外不僅在司法領域，在我國金融監管部分亦可參靠英國對於 AI 金融監管的指引，增加民眾對於公、私部門對於適用 AI 的信任

第五章 結論

本研究旨在研究 AI 於金融領域之應用以及使用 AI 對於金融業於發展其業務以及增加效率之益處，另外就 AI 生成之資料於後續面對法律問題例如刑事訴訟法上的數位證據或是 AI 生成資料在法律以及實務上之困境，參考外國法制趨勢，對於我國於 AI 證據使用或金融監理規範提供建議或方向。

面對虛擬貨幣以及金融犯罪日益猖獗，AI 技術在增加效率的同時，例如在使用幣流分析時，可能因為可以大量、大範圍的建構交易網絡而有侵害資訊隱私權之疑慮，故法院在使用相關證據時亦須注意是否對於隱私權有過大侵害，而構成強制處分的疑慮，是以當公、私部門引進 AI 軟體或接納 AI 資料時，須注意是否有偏見或對人權造成侵害，正視其在司法體系中產生的法律挑戰。

本文之重點亦著重於 AI 證據的屬性、證據能力的問題，於國現行實務之案例尚較少對於 AI 生成內容之證據屬性判斷，亦尚未有統一見解，雖部分判決可透過定性為「鑑定報告」透過刑事訴訟法 206 條處理，但在專家證言之部分仍缺少向美國證據法之科學性檢驗、可信性與關聯性之檢驗標準，在事實層面也難以想象可以找到軟體開發商為個案做專家證人，是以 AI 證據在我國實務之定性與檢

驗方式仍待發展。

我國除了可借鑒歐盟為全面性規範作為大架構之指引外，在金融監理上已可如英國以行政規範或指引，作為進入司法前之風險控管，儘早介入避免損害進一步擴大，在司法領域則可考慮以行政規範或是施行細則之方式增加對於科學證據之檢驗會需注意考量之事項，明確建立鑑定之方式或制度，對於科學證據採開放之見解但需多方衡量，在保障人權與打擊犯罪之間取得平衡。