論新興科技衍生之資訊倫理議題及防制挑戰

葉琨焯*

壹、前言

隨著物聯網、大數據和人工智慧等新興科技的快速發展，不僅改變了我們的生活方式，也引發了諸多資訊倫理議題。這些議題涉及個人隱私保護、資訊透明度、數據安全以及資訊公平性等方面。在這些變革中，我們需要重新審視新興科技對於資訊倫理所造成之衝擊，確保新興科技的發展不損害人類的基本權益和社會價值。

本文試由調查機關之角度出發，援引實務案例，探討物聯網、大數據和人工智慧等新興科技對資訊倫理造成之衝擊及當前面臨之防制挑戰。

貳、資訊倫理框架

美國管理信息科學專家Mason於1986年提出之PAPA理論（PAPA model）[1]是資訊倫理領域中一個重要的框架，提出了四個關鍵議題：隱私（Privacy）、準確性（Accuracy）、所有權（Property）和可存取性（Accessibility）。這四個議題在新興科技的發展下值得重新檢視，因為科技的進步正深刻影響著這些資訊倫理領域中的核心問題。

一、隱私權

在隱私（Privacy）方面，其核心內涵在於每個人均有自主決定個資是否公開，或為他人蒐集、利用之資訊隱私權，該權利包含於憲法隱私權，受憲法第22條之保障，為歷來大法官解釋及憲法法庭判決所肯認[2]。資訊隱私權的保障範圍包含當事人個資於受利用之前，有同意與否之「事前控制權」，以及受利用中、後之「事後控制權」。隨著物聯網、大數據和人工智慧等新興科技之發展下，個人數據的收集和分析已經成為普遍現象。舉例來說，隨處可見的物聯網設備（如穿戴式裝置、智慧型手機、監視器等），透

*本文作者係法務部調查局臺北市調查處調查官，國立臺灣大學電子工程研究所博士，律師高考及格。

註1：Mason, Richard O. “Four Ethical Issues of the Information Age.” MIS Quarterly, vol. 10, no. 1, 1986, pp. 5 – 12. JSTOR, https://doi.org/10.2307/248873. Accessed 10 Sept. 2024.

註2：司法院釋字第603號、111年憲判字第13號判決【健保資料庫案】。

過持續地蒐集個人行為及活動資料，進行大數據及人工智慧分析，利用分析結果優化使用者之生活體驗，雖帶來生活上之便利，也帶來了前所未有的隱私挑戰。由於物聯網設備可透過網際網路（Internet）相互溝通及分享資料，有心人士即有機會透過不安全的物聯網設備竊取個人資料，著名網站「http://www.insecam.org/」蒐集全世界未加以防護的網路攝影機供人觀看隱私影像，即為適例。

二、準確性

在準確性（Accuracy）方面，可分為兩大面向：其一，係資訊使用者有權利獲取正確的資訊。其二，資訊提供者有義務提供正確之資訊，避免生損害於公眾或他人。在大數據的時代，決策越來越仰賴大數據及機器學習之分析結果，當數據資料不正確或扭曲時，即可能產生錯誤之決策結果（Garbage in, garbage out），因此在使用數據進行決策時，必須確保數據的正確性，並對演算法進行嚴格檢驗，以防止因數據錯誤而產生的不公正結果。近年來，假訊息之氾濫不僅損害了資訊的準確性，並對社會造成深遠的負面影響，導致公眾之誤解及恐慌。例如：於疫情期間，關於病毒來源、治療方法及疫苗成效方面之假訊息層出不窮，加深了民眾對於疫病之恐慌，導致了部分群體對疫苗的抵制，進而影響了公共衛生政策的執行。此外，假訊息被利用來操控選舉結果或煽動社會動亂，這些行為不僅破壞了民主制度的公平性，也加劇了社會的分裂和對立。由於社交媒體平臺的普及，假訊息之傳播速度已遠遠超過傳統之口耳相傳，另外在新興科技之發展下，使用生成式AI等人工智慧技術產出之假訊息、假圖片及假語音更加難辨真偽，加深了假訊息之負面影響。

三、所有權

在所有權（Property）方面，其核心內涵在於尊重他人之資訊所有權，避免侵害他人之智慧財產權。隨著物聯網、大數據和人工智慧等技術的普及，資訊的生成、儲存、傳遞和使用方式發生了巨大變化，這使得資訊所有權的界定變得更加複雜，例如：企業透過大數據分析消費行為所生成之分析結果應歸屬於企業或是消費者，即屬爭議問題。此外，人工智慧系統所生成之創作作品，也存在智慧財產權歸屬不明之問題，依我國著作權法第3條第1項第2款之定義，著作人係指創作著作之人，並依照同法第10條本文之規定，著作人於著作完成時享有著作權。依照文義解釋，僅自然人或法人得為權利主體，當自然人或法人將人工智慧系統做為輔助工具進行創作，而有人類精神力參與其中，所產生具備原創性之作品仍應受著作權之保護。惟由於人工智慧系統並非著作權法之權利主體，故若係人工智慧「自主」創作作品，而無人類精神力投注其中時，原則上仍無法享有著作權[3]，然而隨著人工智慧之持續發展，有朝一日當人工智慧發展至具備類似

註3：熊全迪（2024），〈淺談當前人工智慧發展的若干重要法律議題及法制展望〉，《全國律師聯合會月刊》，第46-54頁。

人類智能及獨立思考能力時，其能否被賦予特殊之人格，而成為著作權法上的權利主體，值得未來持續關注。

四、可存取性

在可存取性（Accessibility）方面，其核心內涵在於確保獲取資訊之公平性，隨著數位化之發展，獲取資訊的途徑變得更加多樣化，但同時也出現了資訊鴻溝，導致不同群體之間的資訊獲取不平等。Mason強調，資訊之獲取不應該因經濟、地理或社會地位的不同而受到限制。這一點在現代社會尤為重要，特別是在教育和醫療等關鍵領域，資訊的不平等可能會加劇社會不公，造成貧者愈貧、富者愈富之現象。隨著物聯網、大數據和人工智慧等技術的快速發展，資訊的不對等益加嚴重，大企業利用自身的數據優勢，並利用這些數據進行深度分析，掌握用戶私人生活、消費習慣和社會關係之同時，可能導致隱私侵害和個人資料的濫用。相較於大型企業，中小企業及個人難以獲取對等的資訊，因為他們無法獲得或負擔與大企業相媲美的數據資源和分析能力。面對大企業資訊壟斷之現象，我國公平交易法雖並未就數據壟斷進行規範，但其一般條款仍然可能適用於涉及數據壟斷的行為。例如：依照公平交易法第9條第1款之規定，獨占之事業不得以不公平之方法，直接或間接阻礙他事業參與競爭，如果獨占事業不當利用數據資源之優勢以不公平之競爭方式壓制其競爭對手時，這樣的行為可能被認定違反公平交易法。此外，大陸地區於2022年修正反壟斷法[4]，新法規定經營者不得利用數據和算法等從事壟斷行為，顯示數據壟斷行為已逐漸受到重視及監管。

參、案例分析

一、網紅小玉利用深偽不雅影片牟利案

本案發生於2020年至2021年間，綽號為「小玉」之網路名人利用深偽技術（Deepfake）換臉軟體，將成人片女演員的臉部替換為知名女性人物，合成製作色情影片，以此招攬會員付費觀看，僅數月間不法獲利已達千萬元[5]。所謂深偽技術，係指利用人工智慧中的深度學習（Deep learning）進行偽造，相較傳統的人工修圖，深度偽造技術所生成之假圖片及假影片幾可亂真，難以透過肉眼進行辨認，更令人擔憂的是，製作深偽影片之門檻相當低，不僅深偽APP工具之價格低廉，縱然是人工智慧的門外漢，也能利用深偽APP製作出Deepfake圖片或影片。深偽技術對於資訊倫理之不利影響，主要在兩大方面：首先，是對資訊準確性之破壞，深偽技術生成之虛假內容因極為逼真，難以透過肉眼及一般方式辨別，尤其當偽造的內容被傳至網際網路之社交平臺時，透過廣泛的分享轉發，對公眾的認知造成誤導，使其難以

註4：中華人民共和國反滲透法第9條：「經營者不得利用數據和算法、技術、資本優勢以及平臺規則等從事本法禁止的壟斷行為。」

註5：維基百科，https://zh.wikipedia.org/zh-tw/小玉Deepfake換臉事件，最後瀏覽日：2024年9月10日。

辨認資訊之真偽。2023年8月我國甚至出現疑似以深偽技術合成政治人物聲音之造假錄音檔[6]，意圖帶動輿論風向及影響後續選舉走向；另一方面，深偽技術之出現導致公眾對於所見所聞之信任度下降，可能使真實資訊反而遭受質疑，而不利真實資訊之流通，顯示深偽技術之濫用已對資訊準確性造成前所未有的挑戰。其次，深偽技術除了破壞資訊準確性外，亦可能侵害個人之資訊隱私權，原因在於偽造者如未通知當事人獲得其書面同意前，即將被害人之個人資料用於訓練深偽模型及生成深偽影音檔，即屬侵害被害人對於個人資料之資訊隱私權。例如：本案中網紅小玉未經女性被害人事前書面同意，利用女性臉部特徵製作深偽影片，破壞被害人對於臉部特徵資料之事前自主控制權，即為違反資訊隱私權的行為。

針對本案之刑事處罰，實務見解[7]認為網紅小玉製作深偽影片牟取私人不法利益之行為，實係指摘或傳述被害人拍攝色情影片之不實事項，已足貶損被害人之外在名譽，對於被害人之人格、社會評價及名聲產生負面影響，此部分應構成刑法第310條第2項之加重誹謗罪；另就利用網路瀏覽之方式傳送猥褻影像供會員觀看之部分應構成刑法235第1項之販賣猥褻影像罪；末就被害人人臉特徵、姓名及藝名等資訊，法院認為屬個人資料保護法（下稱：個資法）第2條足以直接或間接識別本人之個人資料，屬個資法應受保護之客體。網紅小玉利用被害人個資製作深偽影片販賣，顯已逸脫蒐集個人資料之必要範圍，屬不當利用蒐集他人個資，且主觀上具備為自己不法利益之意圖，應構成個資法第41條非公務機關不當蒐集利用個人資料罪。以上3罪，法院認為屬一行為觸犯數罪名之想像競合，從一重論以個資法第41條非公務機關不當蒐集利用個人資料罪，惟本案製作數個被害人之深偽影片，係分別起意，屬數行為，且受侵害之法益（資訊隱私權）個數，應以受侵害主體人數各別認定，進行數罪併罰，合計119罪，定應執行刑5年。

二、房仲神器「小白機」濫用個資牟利案

本案被告蘇〇〇曾任職不動產仲介從業人員，深諳房仲業者亟思取得不動產登記名義人基本資料，藉以尋找潛在買家、賣家，拓展仲介業務，遂與販售個資集團合作，針對房仲客戶需求開發名為「小白機」之個資查詢系統，系統資料庫中包含全國自然人姓名、國民身分證統一編號、住址、手機門號等個人資訊[8]。我國為顧及個人資訊隱私，於

註6：中央社（2023），〈音檔疑柯文哲批賴清德訪美調查局：深偽可能性高〉，https://www.cna.com.tw/news/asoc/202308250165.aspx，最後瀏覽日：2024年9月10日。

註7：臺灣新北地方檢察署110年度偵字第39192號起訴書、臺灣新北地方法院111年度審訴字第356號判決、臺灣高等法院111年度上訴字第3787號判決及最高法院113年度台上字第1728號判決。

註8：Yahoo新聞（2021），〈房仲神器「小白機」驚傳總統個資也外洩〉，https://tw.news.yahoo.com/房仲神器-小白機-驚傳總統個資也外洩-051503008.html，最後瀏覽日：2024年9月10日。

2015年修正「土地登記規則」第24條之1等條文[9]，自2015年2月2日起，任何人皆能申請的第二類土地登記謄本，將隱匿登記名義人之部分姓名及部分身份證字號等資訊，不公開登記名義人的完整個人資料[10]。然而房仲業者透過「小白機」，可將第二類土地登記謄本所得之部分姓名、部分身份證字號及住址做為查詢條件，輸入「小白機」進行模糊比對，即可列示符合條件之所有可能自然人資料，稍加勾稽比對即可推測出登記名義人之真實身分，甚至透過數據分析可關聯出居住於同住址之其他自然人以及該登記名義人名下之其他不動產，完全背離「土地登記規則」保護登記名義人資訊隱私的立法意旨。本案對於資訊倫理之破壞有二：首先，是對資訊隱私權之破壞，原因在於「小白機」資料庫中的個人資料，未經被利用人書面事前同意利用，已侵害被利用人自主資料控制權；其次，「小白機」讓房仲業者快速取得房地產登記名義人資訊及相關數據分析結果，具有壓倒性的資訊優勢，可能在市場中獲得不公平的競爭優勢，限制了其他房仲從業者和消費者獲取相同資訊的機會，從而破壞了市場競爭的公平性，屬於對資訊公平性之破壞。

針對本案之刑事處罰，實務見解[11]認為被告蘇○○意圖為自己不法利益，非法蒐集及利用他人個資開發並販售「小白機」之行為，已構成個資法第41條非公務機關不當蒐集利用個人資料罪。此外，向被告蘇○○購買「小白機」之買家均另經檢察官為緩起訴處分、聲請簡易判決處刑或提起公訴，顯示實務上無論買方或賣方均應負個資法之刑事責任。

肆、新興科技濫用之防制及挑戰

一、濫用深偽技術之防制及挑戰

濫用深偽技術之防制可從法律及技術面著手，首先就法律面，針對營利型深偽不實性影像之行為，參照前述網紅小玉的案例，主要以加重誹謗罪、販賣猥褻影像罪及個資法第41條進行處罰；惟有疑問者，針對非營利型深偽不實性影像之行為，例如：行為人不

註9：土地登記規則第24-1條第1項：「申請提供土地登記及地價資料，其資料分類及內容如下：一、第一類：顯示登記名義人全部登記資料。二、第二類：隱匿登記名義人之出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿之資料。但限制登記、非自然人之姓名及統一編號，不在此限。三、第三類：隱匿登記名義人之統一編號、出生日期之資料。」同條第2項：「前項第二款資料，得依登記名義人之請求，隱匿部分住址資料。但為權利人之管理人及非自然人，不適用之。」同條第3項：「登記名義人或其他依法令得申請者，得申請第一項第一款資料；任何人得申請第一項第二款資料；登記名義人、具有法律上通知義務或權利義務得喪變更關係之利害關係人得申請第一項第三款資料。」其中，土地登記規則第24-1條第1項第2款即為俗稱之第二類土地登記謄本，並依照同條第3項中段，任何人均得調閱。

註10：全國地政電子謄本系統，https://ep.land.nat.gov.tw/Home/SNEpaperKind，最後瀏覽日：2024年9月10日。

註11：臺灣新北地方檢察署110年度偵字第44042號起訴書及臺灣新北地方法院111年度原訴字第69號判決。

具營利意圖，僅係為了自娛而製作深偽影片分享給朋友，是否仍構成個資法第41條之罪？最高法院刑事大法庭針對此爭議曾作成裁定[12]，認為個資法第41條之主觀要件可區分為「意圖為自己或第三人不法之利益」（營利意圖）及「意圖損害他人之利益」2種意圖型態，且「意圖損害他人之利益」中的「利益」不限於財產上利益，而包含人格權利益，因此行為人縱不具有營利意圖，惟如意圖損害他人人格權者，仍有個資法第41條之適用。綜上所述，無論是營利型或非營利型深偽不實性影像之行為均得依照個資法第41條進行處罰，且受侵害主體人數為複數時論以數罪併罰之情形下，似乎已達到有效嚇阻及矯治之成效，惟實際上製作關於他人之不實性影像加以散布、流傳，對被害人造成之難堪及身心創傷等法益侵害，恐非加重誹謗罪、販賣猥褻影像罪及個資法第41條等罪所能充分評價，而屬無法可管之數位性暴力[13]。法務部因而推動修法，立法院於2023年1月7日三讀通過刑法增訂[14]第28章之1「妨害性隱私及不實性影像罪章」，新增刑法319-4條，其中第1項處罰意圖散布而以電腦合成或其他科技方法製作關於他人不實之性影像之行為、第2項處罰散布他人不實之性影像之行為以及第3項加重處罰意圖營利之行為，藉以嚇阻深偽技術之濫用。本次修法應值得肯定，惟仍有幾點可惜之處，首先就規範客體部分，刑法319-4條之處罰客體為「性影像」，文義上是否能包含靜態圖片及聲音容有疑問，恐造成未來適用上的爭議，無論是性影像、靜態圖片或聲音，均可能對被害人造成不同程度上之難堪及身心創傷，如僅以性影像為處罰範圍，對被害人之性個人法益無法為充分保護，宜修法解決之。另外本次刑法修正雖已針對性深偽犯罪加以處罰，惟並未就其他非涉及性之其他深偽犯罪進行立法，恐無法全面有效打擊深偽犯罪。例如：製作深偽影音對他人進行不實指摘，而損害他人名譽之行為，如該深偽影音非性影像，自不構成刑法319-4之性深偽犯罪，僅能退而論以加重誹謗罪。鑒於以深度偽造之聲音、影像犯加重誹謗罪，因相關內容真偽難辨，對一般社會大眾造成之認知混淆及被害人之名譽侵害，其危害程度較傳統文字、修圖方式更為嚴重，如僅論以現行法之加重誹謗罪刑責，本文認為實難以遏止深偽犯罪及充分評價對被害人之名譽權侵害。所幸立法者已逐漸意識深偽技術所帶來之危害，推動相關修法，有鑑於詐騙犯罪氾濫，邇來更從單純財產犯罪，質變朝向科技化發展，以製作深偽影像及聲音方式行詐，有加重處罰之必要，

註12：最高法院109年度台上大字第1869號刑事大法庭裁定。

註13：Youtube（2021）〈打擊不法"換臉"高嘉瑜.黃捷提告｜華視新聞20211025〉，https://www.youtube.com/watch?v=tXcf0_7iAbM&t=131s，最後瀏覽日：2024年9月10日。

註14：法務部（2023）〈強化打擊網路性暴力犯罪，完善犯罪被害人權益保障，立法院今（7）日三讀通過刑法增訂第28章之1「妨害性隱私及不實性影像罪章」及「犯罪被害人權益保障法」，建構性暴力防護網絡，全面保障弱勢群體！〉，https://www.moj.gov.tw/2204/2795/2796/161048/post，最後瀏覽日：2024年9月10日。

立法院因而於2023年5月16日三讀通過增訂[15]以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄為詐欺罪之加重事由。此外，為遏止深度偽造影音影響選舉，公職人員選舉罷免法於2023年6月9日修正公布第104條，增訂第2項，以散布、播送候選人深偽影音為方法犯同法第1項意圖使候選人當選或不當選罪者，予以加重處罰。該項立法理由[16]亦明示以散布候選人深度偽造聲音、影像之方法犯第一項選舉罷免誹謗罪，因相關內容真偽難辨，影響一般社會大眾判斷能力並易產生認知偏差及混淆，其危害程度較傳統以第三者角度散布謠言或傳播不實情事之方式更為嚴重，故有加重處罰必要。

深偽犯罪之技術面防制主要可透過以下2種技術：第一種方式係以人工智慧偵測深偽技術，其核心概念係以「AI對抗AI」，目前多種著名的深偽辨識軟體和工具利用AI技術來檢測和識別深偽內容，其原理為檢測影音檔或圖片是否由深偽技術所生成，此方式為目前偵測深偽技術的主流，國內司法調查機關多仰賴此種深偽辨識軟體及工具進行深偽檢測[17]，惟使用深偽辨識軟體仍有許多限制。首先，深偽辨識軟體無法給出確定性的結果，僅能提供概率性之評估；其次，因深偽辨識軟體本質上即為AI結果之產出，而可能出現偽陽性（誤判真實內容為深偽）及偽陰性（未能檢測出深偽）之誤判情況，因此，僅憑藉深偽辨識軟體的檢測結果難以得出確定性之結論，通常需要搭配人工審查或使用多種不同辨識軟體工具以提升準確性及可信度。此外，使用深偽辨識軟體之另一限制在於無法辨別真人模仿之行為，原因在於模仿者的語音並非經過AI所生成，而是自然產生的，因此深偽檢測工具可能難以偵測出異常，此時得嘗試透過其他技術，例如：模仿語音之行為可透過聲紋識別技術，分析語音的聲學特徵，從而區分不同的說話者。由於網路平臺假訊息、假圖片氾濫，數個網路引擎業者及資訊服務提供者分別提出AI深偽檢測服務工具，其中，Google公司於2020年提出名為「Google Assembler」的圖片及視頻檢測工具，惟於2023年即停止服務，關鍵原因可能在於檢測工具難以跟上不斷演進更新之深偽工具、改進檢測工具所需付出之龐大研發及訓練成本以及工具判斷錯誤所招致之抗議及批評，顯示單以AI檢測工具進行深偽技術之防制仍面臨極大的挑戰。

第二種防制深偽技術之方式係使用數位簽章技術，對於文字、聲音、圖片、影像、符號等電子文件進行數位簽名，以確認電子文件之來源。依照我國電子簽章法第2條第1項

註15：法務部（2023），〈擴大處罰加重刑責強力打詐立法院於今（16）日三讀通過刑法第302條之1、第303條及第339條之4修正草案〉，https://www.moj.gov.tw/2204/2795/2796/170834/post，最後瀏覽日：2024年9月10日。

註16：內政部（2023），〈公職人員選舉罷免法部分條文修正草案總說明〉，https://glrs.moi.gov.tw/Download.ashx?FileID=22609&id=FL001996&type=LAW，最後瀏覽日：2024年9月10日。

註17：法務部調查局（2023），〈法務部調查局針對「二合一選舉」深度偽造假訊息之因應措施〉，https://www.mjib.gov.tw/news/Details/1/916，最後瀏覽日：2024年9月10日。

第1款之定義，數位簽章屬於電子簽章之一種，係將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，得以公開金鑰加以驗證，並具憑證機構簽發之憑證者。簽署人之私密金鑰由個人私有，具有秘密性，故以私密金鑰所為之數位簽章具有不可否認性，意即簽署人無法否認其數位簽章。由於數位簽章之不可否認性，以數位簽章簽署電子文件，於符合一定條件下[18]，即得推定為本人親自簽名或蓋章；從另一個面向理解，除私密金鑰遭外流之情況外，由於私密金鑰僅簽署人知悉，故數位簽章無法被他人偽造。數位簽章係以公開金鑰進行驗證，所謂公開金鑰，係簽署人所持有之另一把金鑰，該把金鑰不具有秘密性，主要提供給外界使用，其中一個主要用途即於驗證數位簽章。簽署人需提供公開金鑰向憑證機構申請憑證，所謂憑證，依照電子簽章法第2條第1項第6款之定義，指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。簡言之，公眾可透過憑證中的公開金鑰驗證簽署人之數位簽章，並確認簽署人之身分。另為確保憑證真實性及公正性，我國憑證發放機構採許可制，需向數位發展部申請許可始得提供簽發憑證服務，目前國內業者已有中華電信股份有限公司及臺灣網路認證股份有限公司獲得許可[19]。當前數位簽章已廣泛應用於各領域，例如：政府機構及民間業者使用數位簽章來簽署電子公文，以確認簽署者之身分；民間軟體業者亦會使用數位簽章來簽署他們的軟體和更新包，確保用戶下載和安裝的軟體來自可信任的來源，避免用戶下載到偽冒惡意軟體。針對深偽犯罪，數位簽章能提供驗證電子文件來源之功能，防止深偽者冒充合法來源發布不實影音。近期詐騙集團假冒投資名人、政府官員及金融機構重要人士，深偽合成不實語音之案例頻傳[20]，倘若我國能由政府機關、金融機構或其他重要民間企業開始，全面推動電子文件之數位簽章，即能提供一般社會大眾驗證電子文件來源之管道，如發現電子文件並無數位簽章時，一般社會大眾即應審慎評估其可信性，並輔以其他管道（例如：臺灣事實查核中心）查證電子文件內容之真實性。惟數位簽章仍有其限制及缺點：首先，數位簽章無法協助判定電子文件內容是否經過深偽技術變造，僅能驗證電子文件之來源；其次，數位簽章需要電子文件創建者主動採取該技術，創建電子文件之程序較為繁瑣，且可能需負擔申請憑證之費用。此外，因實際上難以期待一般社會大眾自行驗證數位簽章，故

註18：電子簽章法第6條：「以數位簽章簽署電子文件，符合下列各款規定者，推定為本人親自簽名或蓋章：一、使用經主管機關依第十二條或第十五條許可之憑證機構簽發之憑證。二、憑證未逾有效期間及其使用範圍。」

註19：數位發展部（2024），〈依電子簽章法第12條第3項公告憑證實務作業基準經許可之憑證機構名單與其憑證實務作業基準版次及許可文號〉，https://moda.gov.tw/ADI/news/bulletin-board/11802，最後瀏覽日：2024年9月10日。

註20：聯合新聞網（2024），〈碳交所總經理遭AI深偽科技製作仿真影片詐財民眾切勿輕信受騙〉，https://udn.com/news/story/7239/8192654，最後瀏覽日：2024年9月10日。

需仰賴網路廣告平臺或社群媒體支援數位簽章認證功能，協助使用者於網路廣告平臺及社群媒體上瀏覽電子文件時，即自動化驗證電子文件之來源並顯示給使用者參考。然而目前Google、Facebook、Instagram及Twitter等主流廣告平臺或社群媒體均未支援電子文件數位簽章認證功能，縱使電子文件創建者已主動採取數位簽章技術，於一般社會大眾無法自行驗證數位簽章之情形下，恐仍難以遏止深偽訊息於廣告平臺及社群媒體上之散布與氾濫。立法院於2024年7月12日三讀通過「詐欺犯罪危害防制條例」（下稱：詐防條例），針對金融服務、電信產業及數位經濟產業（包含網路廣告平臺業者、第三方支付服務業者、電商業者及網路連線遊戲業者）制定防詐措施[21]。凡利用網際網路於中華民國領域內提供網路廣告服務且達一定規模之網路廣告平臺業者均適用詐防條例之規定，且應依照詐防條例第28條以適當方式公開揭露業者資訊，包含業者及其代表人名稱、事務所或營業所地址、電話或電子郵件等，以增進網路廣告平臺業者之透明度，另鑒於提供我國人民廣告服務者多為境外業者（例如Google, Line及Facebook等），如於中華民國無營業所或住居所，且未設立分公司者，應依詐防條例第29條第1項指派境內法律代表，以落實防詐措施及落實執法。此外，為杜絕網路詐欺訊息的氾濫，防制廣告詐騙，網路廣告平臺業者應依照詐防條例第30條第2項第1款之規定，以數位簽章或其他安全性相當之技術或方式（例如人工查驗）驗證委託刊播者及出資者之身分，以降低偽冒他人名義刊登或推播廣告之潛在風險，落實廣告實名制。此外，為增進網路廣告透明度，以利社會大眾判斷網路廣告可信度，網路廣告平臺業者於刊播廣告時，依照詐防條例第31條第1項第2款應揭露委託刊播者、出資者相關資訊；另如廣告使用深度偽造技術或人工智慧生成個人影像者，依照詐防條例第31條第1項第4款亦應於廣告中揭露，以利公眾判斷真偽。廣告實名制之立法雖值得肯定並有助於追查廣告刊播者之身分，釐清責任歸屬，藉以嚇阻偽冒者，惟廣告實名制僅針對廣告平臺用戶進行實名認證，而不包含一般社群媒體用戶。例如，Facebook同時為社群媒體及網路廣告平臺業者，廣告平臺用戶依照前述規定需實名認證，其他社群媒體用戶則無需實名認證，因此若偽冒者係以社群媒體用戶身分於Facebook發布深偽訊息，公眾即無實名認證之管道。此外，廣告實名制雖可針對廣告用戶進行身分認證，惟無法協助公眾驗證廣告內容所包含之影音檔真偽，用戶仍可能遭受深偽影音之欺騙，尤其網路資源轉載容易，引用他人影音者比比皆是，廣告刊播者亦可能誤引用深偽影音進行廣告，或故意引用深偽影音而推諉不知。因此，為杜絕深偽影音之散布及負面影響，推動電子文件數位簽章仍有其必要性。另針對廣告平臺用戶，本文建議可結合數位簽章及廣告實名制之作法，以數位簽章提供內文影音檔來源驗證，

註21：立法院全球資訊網（2024），
https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=33324&pid=242170，最後瀏覽日：2024年9月10日。

並透過廣告實名制進行刊播者身分追查及責任歸屬。

二、濫用大數據分析之防制及挑戰

於前述房仲神器「小白機」之案例中，「小白機」提供的功能並非單純查詢登記名義人個資，亦透過進一步的數據分析關聯出居住於同住址之其他自然人以及該登記名義人名下之其他不動產，目前雖無證據顯示「小白機」使用大數據分析技術，但無疑問的是，如果將大數據分析技術應用至「小白機」中，將能夠為房仲客戶提供更多的資料加值服務，協助房仲業者更快速、更精確進行市場分析及客源發掘，將造成房仲業者間更大的資訊落差及不公平現象。大數據分析之濫用除了可能發生於房仲業外，亦可能發生於政治圈及其他領域，在2016年美國總統選舉期間，劍橋分析公司利用從Facebook上非法獲取之大量用戶數據，進行精確的選民分析並將分析結果提供給共和黨總統參選人川普做為選戰參考[22]。

由上可知，大數據分析之濫用已成為當前重要課題，為防制大數據分析之濫用，本文認為應釜底抽薪，對數據來源進行管制，減少非法或不當獲取數據的途徑，從而減少數據在分析過程中被濫用的可能性。首先，應落實公務機關及非公務機關對於其保有個人資料檔案進行保護，避免個資外洩或遭駭客竊取。針對公務機關，依照個資法第18條，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏；另針對非公務機關，個資法第27條第1項規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，同條第2項規定，主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。非公務機關違反上開義務者，主管機關得依第48條第2項、第3項[23]處以行政罰鍰並命限期改正。其中，個資法第48條係於2023年5月16日立法院三讀修正通過，其修法意旨在於促使非公務機關投入人力、技術，落實保護民眾個人資料之責任，並提高裁罰額度，以回應各界普遍反應原罰鍰過低之問題[24]。

個資法雖已賦予公務機關及非公務機關妥

註22：維基百科，https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal，最後瀏覽日：2024年9月10日。

註23：個人資料保護法第48條第2項：「非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。」同條第3項：「非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，其情節重大者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。」

註24：國家發展委員會（2023），〈立法院三讀通過個資法修正案將強化企業個資外洩罰責並盡速設置個資保護委員會籌備處〉，https://www.ndc.gov.tw/nc_27_36901，最後瀏覽日：2024年9月10日。

善保管個人資料之相關責任，惟因人為因素及駭客技術之與日俱進，機關遭到駭客入侵或因內部人犯罪導致個資外洩事件仍時有耳聞。由於個資具有高經濟價值，犯罪者經常藉由出售個資牟取不法利益。偵查實務中，犯罪者常透過匿名網站論壇進行販售，因網站論壇常架設於境外，或是架設於暗網，故難以追查販售者之真實身分並將外洩個資下架。惟實務上並非全無查緝機會，2024年4月間名為「Genesis Market」（下稱：創世紀市場）[25]之個資販售市場遭到美國聯邦調查局（FBI）等境外執法機構查封並將與我國有關之註冊用戶資訊交予法務部調查局（下稱：調查局）深入調查，調查局並循線查獲我國虞姓人士等3人於創世紀市場購買多筆國人使用之社群平臺或蝦皮、露天等商用平臺之帳號密碼、手機號碼及身分證統一編號個人資訊，渠等蒐集之帳號權限已嚴重侵害我國民眾資訊及網路隱私安全。為防制及遏止該等不法行為戕害國人權益，調查局表示將持續與國外執法單位保持密切聯繫，透過國際合作共同打擊個資販售論壇，阻斷非法獲取數據之途徑。

伍、結語

新興科技的發展為人類的生活帶來便利，然而伴隨而來的資訊倫理議題亦值得重視，本文從資訊隱私、資訊準確性、資訊所有權及資訊可存取性等4個面向探討新興科技對資訊倫理之衝擊，並援引深偽技術及大數據分析濫用之實務案例進行說明。首先，深偽技術之濫用可從法律面及技術面進行防制，法律面部分，我國刑法針對性深偽犯罪及深偽詐欺罪進行立法防制，並於公職人員選罷法加重處罰深偽候選人、被罷免人等人影音之行為，法律面對於深偽犯罪之防制雖已漸趨完備，惟我國並未就其他利用深偽技術之犯罪類型進行全面立法（例如使用深偽技術之加重誹謗罪），能否全面有效嚇阻深偽相關犯罪仍有待觀察；此外，深偽技術的技術面防制目前多仰賴人工智慧為基礎之深偽辨識軟體，惟其缺點為無法給出確定性的結果，僅能提供概率性之評估，且有誤判之風險，且於深偽技術持續進化下，深偽辨識軟體能否跟上腳步，仍面臨極大的挑戰。鑒於深偽訊息常透過網路廣告平臺進行散布，我國近期制定防詐條例強制網路廣告平臺業者應驗證委託刊播者及出資者之身分，以降低偽冒他人名義刊登或推播廣告之潛在風險，落實廣告實名制。本文認為防詐條例之立法雖有助於嚇阻偽冒者使用廣告平臺發布深偽訊息，惟無法針對一般社群媒體用戶進行管制，且亦無助於公眾對於廣告內文之影音來源進行驗證。對此，本文提倡應推動電子文件數位簽章，所謂電子文件數位簽章係針對影像、聲音等電子文件由生成者進行數位簽名，具有不可否認性，簽署人無法否認其數位簽章，藉以讓公眾驗證影音來源。然而，

註25：法務部調查局（2024），〈調查局與美國聯邦調查局合作，首度偵破創世紀市場不法蒐集國人個資案〉，
https://www.mjib.gov.tw/news/Details/1/1015，最後瀏覽日：2024年9月10日。

雖然數位簽章功能強大，仍需電子文件創建者主動採取該技術，成本較高，且因難以期待一般使用者自行驗證數位簽章，而需網路廣告平臺業者及社群媒體支援簽章驗證功能。我國目前仍缺乏相關配套措施，有待相關政府部門與民間業者共同推動。其次，針對大數據分析之濫用，本文建議可從源頭阻斷非法取得數據之管道。首先，應加強落實公務機關與非公務機關保有之個人資料保護，包含落實個人資料加密以及用畢資料刪除等資安防護機制，減少個資外洩之機會。此外，為徹底阻斷非法取得個資之管道，仰賴我國司法偵查機關持續與境外執法機構國際合作並交流情資，積極查緝透過網路論壇買賣個資之不法行為，亦呼籲社會大眾勿以身試法，尊重他人之個資隱私權。