

不實影像之刑事規制

張明偉*

壹、前言

俗話說：「眼見為憑。」對於一般人來說，相信自己眼睛看到的事，特別在照相與錄影等影像技術開始被廣泛應用在日常生活以來，這是再正常不過的一件事。然而，隨著人工智慧的發展，特別是在深度偽造（deepfake）¹不實影像技術逐漸普及之今日，早已為普遍認知的眼見為憑，卻面臨前所未有的挑戰，蓋依深度偽造之技術，看似真正的影像，可能是由人工智慧創造或修改而成；在影片中呈現出某種意思表示的紀錄，不僅可能不是那個人所說，其內容亦可能係虛構而成。這個世界的表象，真真假假、假假真真，而受深度偽造高度影響的世

界，似乎越來越有金剛經所稱「如夢幻泡影、如露亦如電」的意境。

面對影像技術的發展，刑事法制亦受到衝擊。傳統的刑法規範是否足以因應深度偽造技術發展所造成的侵害與影響，亦受到來自各方面的檢討，特別在深度偽造技術被用來編輯或捏造性影像時²，是否有必要制定特別法來回應³，引起許多爭論。依2023年1月增訂刑法第28章之1「妨害性隱私及不實性影像罪章」之刑法第319條之4立法理由：「二、因網路資訊科技及人工智慧技術之運用快速發展，以電腦合成或其他科技方法而製作關於他人不實之性影像，可能真假難辨，易於流傳，如有意圖散布、播送、交付、公然陳列，或以他法供人觀覽而製作，或散布、播送、交付、公然陳列，或以他法供人觀覽他人

* 本文作者係輔仁大學法律學院教授

註1：按深度偽造（Deepfake）一詞，源自深度學習（Deep learning）與偽造（Fake）的組合，包含AI換臉與語音複製等技術，主要乃指利用深度學習技術訓練大規模的數據，包括人臉圖像、語音，以及視頻等將已有的圖像或影片疊加至目標圖像或影片上之人工智慧運用。「這些數據用於模仿和學習不同人的特征、動作和聲音。然後，再利用人工智能（AI）技術創建虛假內容，包括假的圖像、聲音和影片，從而實現AI換臉或者語音複製等功能。…深度偽造最廣為人知的用途卻是製作虛假的名人視頻或音頻，以傳播虛假或誤導性訊息。除此之外，人們也可能濫用這項技術來製作色情影像或進行詐騙。」香港網路安全事故協調中心，〈深度偽造：有圖未必有真相〉，2024年03月11日，<https://www.hkcert.org/tc/blog/deepfake-where-images-don-t-always-speak-truth>

註2：例如：YouTuber小玉（朱玉宸）與團隊利用Deepfake技術製作出AI換臉之不雅造假色情影片，並販售牟取暴利，造成許多女性網紅、藝人、政治人物聲譽受到侵害，此一數位性暴力事件引起社會關注。呂志明（2023），〈小玉條款！換臉A片修法重懲〉，壹蘋新聞網，<https://tw.nextapple.com/local/20230210/1930B66D3671F4B2D36DB19FC2318116>

註3：許恒達（2022），〈深度偽造影音及其刑法規制〉，《法學叢刊》，第265期，第3頁。

不實之性影像，對被害人造成難堪與恐懼等身心創傷，而有處罰必要」說明，不實性影像之處罰，其目的在於保護個人之隱私權及人格權。又為避免以深度偽造之方式透過視訊或電話假冒身分進行詐騙獲取不法利益⁴，於同年5月增訂之刑法第339條之4第1項第4款之加重處罰規定，即在防止民眾因分不清深偽影像真假而受騙上當⁵。

由於現行立法已明文處罰「意圖散布、播送、交付、公然陳列，或以他法供人觀覽而製作，或散布、播送、交付、公然陳列，或以他法供人觀覽他人不實之性影像」與「以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法犯詐欺罪」等行為，故對此等行為在實體法上之評價，以及其於程序法上之適用，將出現何種問題，均有進行探究之必要，以期正確適用此等新制定之刑法規範，落實立法者懲治數位性暴力與深偽詐欺之立法初衷。

貳、有關深度偽造之法制修正

一、修正前法制規範不足

伴隨網際網路與不實影像技術之發展，網路世界所流通的資訊，常常讓接收者難辨真偽。依國際電信聯盟（International Telecommunication Union：ITU）發布的 Measuring Digital Development Facts and Figures 調查報告，在2022年底，全球已有近七成的人口透過網際網路進行相關活動⁶；另依2022年初DATAREPORTAL全球報導，全球已有約50億人在使用網際網路⁷。因此，可以想像在網際網路與不實影音相互結合下，非物理性暴力之復仇式色情⁸與不實影音對被害人所可能造成的傷害，不僅超出加害者之掌握與預期，簡直是無遠弗屆。依婦女救援基金會2021年度執行報告專刊報導，在2021年，其所接獲有關數位性暴力的通報人數即已達577人⁹，可見此問題已具相當嚴重性，

註4：按英國曾出現以深度偽造模仿母公司來電命令其轉帳24萬美元之詐騙案例。Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case: Scams using artificial intelligence are a new challenge for companies*, Wall Street Journal, <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

註5：蔡智銘（2023），〈別再亂搞『換臉』了！立院修法加重電腦合成不實影像及聲音刑責〉，yamNews，<https://n.yam.com/Article/20230516857818>

註6：ITU, *Measuring digital development: Facts and Figures 2022*, <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>

註7：DATAREPORTAL, *DIGITAL 2022: GLOBAL OVERVIEW REPORT*, Jan. 26, 2022, <https://datareportal.com/reports/digital-2022-global-overview-report>

註8：關於復仇式色情（Revenge Porn），一般係以違反本人意願散布性隱私內容為特徵，並未涉及不實影像，被害人因性隱私內容意外曝光，不僅名譽權和隱私權受到侵害，其學業、職涯和社交生活更可能莫名充斥無數的威脅、誹謗、性勒索（Sextortion）、以及跟蹤，對其影響甚大，惟非本文討論範圍。相關說明，蕭郁澹（2017），〈參閱日本情色報復受害防治法之評估〉，《科技法律透析》，第29卷第2期，第21-28頁。

註9：婦女救援基金會，〈2021年度執行報告專刊〉，<https://www.twrf.org.tw/info/download/1230>，<https://www.twrf.org.tw/info/download/1230>

值得各界關注。

關於製作他人不實性影像並予以散布之行為，在修法前並無直接可適用的處罰規範，雖然散布不實性影像之行為可該當刑法第310條誹謗罪與第235條散布猥褻物品罪等規定，惟如刑法第319條之4立法理由所述：「以電腦合成或其他科技方法而製作關於他人不實之性影像，可能真假難辨，易於流傳」，此種製作他人不實性影像並予以散布之行為，因其作用與另一種侵犯性隱私之行為態樣（將錄製的私密影片外流之復仇式色情）相近，並具高度流通性，因刑法第235條：「（第1項）散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處二年以下有期徒刑、拘役或科或併科九萬元以下罰金。（第2項）意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。（第3項）前二項之文字、圖畫、聲音或影像之附著物及物品，不問屬於犯人與否，沒收之。」與第310條：「（第1項）意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或一萬五千元以下罰金。（第2項）散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或三萬元以下罰金。（第3項）對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。」等規定並不足以反應此行為

為之不法內涵，故為提高處罰製作他人不實性影像並予以散布之行為，乃特別制定刑法第319條之4之規定¹⁰，以為適用。

二、新增立法規範

於2023年2月10日生效之刑法修正中，有關深度偽造行為之處罰，計有刑法第10條第8項：「稱性影像者，謂內容有下列各款之一之影像或電磁紀錄：一、第五項第一款或第二款之行為。二、性器或客觀上足以引起性慾或羞恥之身體隱私部位。三、以身體或器物接觸前款部位，而客觀上足以引起性慾或羞恥之行為。四、其他與性相關而客觀上足以引起性慾或羞恥之行為。」與第319條之4：「（第1項）意圖散布、播送、交付、公然陳列，或以他法供人觀覽，以電腦合成或其他科技方法製作關於他人不實之性影像，足以生損害於他人者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。（第2項）散布、播送、交付、公然陳列，或以他法供人觀覽前項性影像，足以生損害於他人者，亦同。（第3項）意圖營利而犯前二項之罪者，處七年以下有期徒刑，得併科七十萬元以下罰金。販賣前二項性影像者，亦同。」等規定。然而，就其文義來說，其僅適用於不實之性影像，如係其他「與性無關」之不實影像，即不在修法之適用範圍內。至於如何判斷「足以生損害於他人」之要件，尚待實務具體補充。

註10：按於刑法第319條之4尚未增訂前，實務上有依個資法及刑法加重誹謗、妨害風化等罪論處、並以想像競合犯從一重罪（個資法）論罪之案例。雖實務肯認對「換臉」營利之不法行為予以刑事處罰，但也引發討論此種Deepfake換臉行為究竟侵害何種法益、現行個資法或刑法規定是否適合或足以規範此一行為的討論。蔡碧玉（2024），〈利用深度偽造（Deepfake）犯罪在我國的刑事規制〉，《裁判時報》，第144期，第78頁。

關於以立法規範深度偽造性影像之考量，如以性影像之定義來說，依刑法第10條第8項立法理由：「一、為明確規範性影像之定義，爰增訂第八項規定，說明如下：（一）第一款性影像，係指含有『以性器進入他人之性器、肛門或口腔，或使之接合之行為』、『以性器以外之其他身體部位或器物進入他人之性器、肛門，或使之接合之行為』之內容者。（二）第二款所稱『客觀上足以引起性慾或羞恥之身體隱私部位』，指該身體隱私部位，依一般通常社會觀念足以引起性慾或羞恥而言，例如臀部、肛門等。（三）第三款所定『以身體或器物接觸前款部位』，例如以親吻、撫摸等方式或以器物接觸前開部位之內容，不論自己或他人所為者均屬之。（四）第四款規定『其他與性相關而客觀上足以引起性慾或羞恥之行為』，例如其影像內容未如第一款或第三款行為清楚呈現『性器』或『足以引起性慾或羞恥之身體隱私部位』，而係對該等部位以打馬賽克等方式遮掩、迴避，或因攝錄角度未能呈現，而客觀上足以引起性慾或羞恥之行為。」說明，性影像除包含有關同條第5款性交之影像或電磁紀錄外，其內容尚及於其他涵蓋類似猥褻物（與性相關而客觀上足以引起性慾或羞恥行為）之影像或電磁紀錄。

又以意圖散布、播送、交付、公然陳列，或以他法供人觀覽而製作，或散布、播送、交付、公然陳列，或以他法供人觀覽他人不實性影像等行為來說，因刑法第319條之4立

法理由：「三、製作他人不實性影像之行為手段包括以電腦合成、加工、編輯或其他科技方法，例如以深度偽造技術，將被害人之臉部移接於他人之性影像即屬之。」明確列舉製作他人不實性影像之非法手段行為類型，且使用深度偽造技術已為立法例示之一種手段，故如稱本條為立法者為回應小玉事件而增訂，應不為過。另依刑法第319條之6：「第三百十九條之一第一項及其未遂犯、第三百十九條之三第一項及其未遂犯之罪，須告訴乃論。」之規定，刑法第319條之4為非告訴乃論之罪，不以臉部遭移接於他人性影像之被害人提出告訴，為進行刑事追訴、審判之訴訟條件。

除前述有關不實性影像罪之修正外，於2023年6月2日生效之刑法第339條之4第1項第4款：「犯第三百三十九條詐欺罪而有下列情形之一者，處一年以上七年以下有期徒刑，得併科一百萬元以下罰金：四、以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法犯之。」規定，亦新增以製作他人不實影像、聲音或電磁紀錄等深度偽造手段作為施用詐術方法之加重詐欺罪；查此次修正主要係「考量網路資訊科技及人工智慧技術的運用快速發展，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，可能真假難辨，易於流傳，如果詐騙集團用這些方法詐騙，易使被害人陷於錯誤，其侵害社會法益程度及影響層面均較普通詐欺行為嚴重¹¹」，因此，

註11：胡晴美（2023），「《刑法修正三讀》私刑拘禁凌虐、製作不實影音詐欺最高可處7年有期徒刑」，信傳媒，

https://www.cmmedia.com.tw/home/articles/40099?utm_source=YH

法制上乃將製作他人不實影像、聲音或電磁紀錄等深度偽造手段，明文為加重處罰要件。

此外，為防止深度偽造影響選舉及民主制度¹²，於2023年6月9日施行之公職人員選舉罷免法第104條第2項：「以散布、播送或以他法供人觀覽候選人、被罷免人、罷免案提議人之領銜人本人之深度偽造聲音、影像、電磁紀錄之方法，犯前項之罪者，處七年以下有期徒刑。」與總統副總統選舉罷免法第90條第2項：「以散布、播送或以他法供人觀覽候選人、被罷免人、罷免案提議人之領銜人本人之深度偽造聲音、影像、電磁紀錄之方法，犯前項之罪者，處七年以下有期徒刑。」等規定，均將深度偽造列為散布謠言或傳播不實事項之行為態樣，並納為刑事處罰對象。

參、刑法修正之檢討

前述修法雖在回應社會上有關對製作、散佈或利用深偽不實影音之人予以刑事懲罰之

主張，惟其內容是否妥適，卻非沒有進一步檢討之餘地。按就2023年之修法來說，有關深偽不實影音之刑事處罰，僅限於「不實性影音」與「加重詐欺」等罪，故於深度偽造「非屬」性影音之情形中，如未將其作為施用詐術之手段，似乎並不構成犯罪。然而，此種程度之管制，是否足以防杜源自於不實影音之法益侵害，並保護社會大眾不受深偽不實影音之誤導與影響，應有另予檢討之必要。

又如參照釋字第407號解釋：「猥褻出版品，乃指一切在客觀上，足以刺激或滿足性慾，並引起普通一般人羞恥或厭惡感而侵害性的道德感情，有礙於社會風化之出版品而言。猥褻出版品與藝術性、醫學性、教育性等出版品之區別，應就出版品整體之特性及其目的而為觀察，並依當時之社會一般觀念定之。又有關風化之觀念，常隨社會發展、風俗變異而有所不同，主管機關所為釋示，自不能一成不變，應基於尊重憲法保障人民言論出版自由之本旨，兼顧善良風俗及青少年身心健康之維護，隨時檢討改進。」說明¹³，刑法第10條第8項所謂性影像之內涵，其本質並未

註12：按選罷法之深度偽造定義與刑法第319條之4、第339條之4第1項第4款深度偽造之犯罪構成要件並不完全一致，在選罷法及刑法第339條之4第1項第4款的深偽客體包含聲音及影像，而刑法第319條之4之深偽客體則只有「性影像」，可知選罷法及刑法第339條之4第1項第4款規範的深偽範圍較廣。蔡碧玉（2024），〈利用深度偽造（Deepfake）犯罪在我國的刑事規制〉，《裁判時報》，第144期，第82頁。

註13：釋字第617號解釋：「為維持男女生活中之性道德感情與社會風化，立法機關如制定法律加以規範，則釋憲者就立法者關於社會多數共通價值所為之判斷，原則上應予尊重。惟為貫徹憲法第十一條保障人民言論及出版自由之本旨，除為維護社會多數共通之性價值秩序所必要而得以法律加以限制者外，仍應對少數性文化族群依其性道德感情與對社會風化之認知而形諸為性言論表現或性資訊流通者，予以保障。刑法第二百三十五條第一項規定所謂散布、播送、販賣、公然陳列猥褻之資訊或物品，或以他法供人觀覽、聽聞之行為，係指對含有暴力、性虐待或人獸性交等而無藝術性、醫學性或教育性價值之猥褻資訊或物品為傳布，或對其他客觀上足以刺激或滿足性慾，而令一般人感覺不堪

與刑法第235條「猥褻物」存在太大差異¹⁴；從而，倘如性影像與猥褻物二者之本質並無實質差異，是否有必要標新立異、大張旗鼓地在立法上另行將一個原已慣用之法概念（猥褻物），冠以新名稱（性影像），就另為立法定義必要性與用語單純化來說¹⁵，是否應將二者用語統一，非無檢討之餘地。

此外，如就處罰刑度來看，相較於刑法第318條之1：「無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處二年以下有期徒刑、拘役或一萬五千元以下罰金。」洩漏他人秘密之刑度，刑法第319條之3第1項：「未經他人同意，無故重製、散布、播送、交付、公然陳列，或以他法供人觀覽其性影像者，處五年以下有期徒刑，得併科五十萬元以下罰金。」與刑法第319條之4第2項：「散布、播送、交付、公然陳列，或以他法供人觀覽前項性影像，足以生損害於他人者，亦同¹⁶。」等規定，將類似洩漏性影像行為之處罰提高到最重本刑5年有期徒

刑，其間刑罰輕重是否失衡，不無檢討之餘地；蓋刑法第318條之1所稱之秘密，其內容非不可能近似於性影像，惟於此情形中，二者之最高刑度間存在超過一倍之差距，是否符合比例原則？非無疑義。

又如比較刑法第315條之1：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」與第319條之4第1項：「意圖散布、播送、交付、公然陳列，或以他法供人觀覽，以電腦合成或其他科技方法製作關於他人不實之性影像，足以生損害於他人者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。」、第2項：「散布、播送、交付、公然陳列，或以他法供人觀覽前項性影像，足以生損害於他人者，亦同。」等規定，亦可發現立法上之

呈現於眾或不能忍受而排拒之猥褻資訊或物品，未採取適當之安全隔絕措施而傳布，使一般人得以見聞之行為；同條第二項規定所謂意圖散布、播送、販賣而製造、持有猥褻資訊、物品之行為，亦僅指意圖傳布含有暴力、性虐待或人獸性交等而無藝術性、醫學性或教育性價值之猥褻資訊或物品而製造、持有之行為，或對其他客觀上足以刺激或滿足性慾，而令一般人感覺不堪呈現於眾或不能忍受而排拒之猥褻資訊或物品，意圖不採取適當安全隔絕措施之傳布，使一般人得以見聞而製造或持有該等猥褻資訊、物品之情形，至對於製造、持有等原屬散布、播送及販賣等之預備行為，擬制為與散布、播送及販賣等傳布性資訊或物品之構成要件行為具有相同之不法程度，乃屬立法之形成自由；同條第三項規定針對猥褻之文字、圖畫、聲音或影像之附著物及物品，不問屬於犯人與否，一概沒收，亦僅限於違反前二項規定之猥褻資訊附著物及物品。依本解釋意旨，上開規定對性言論之表現與性資訊之流通，並未為過度之封鎖與歧視，對人民言論及出版自由之限制尚屬合理，與憲法第二十三條之比例原則要無不符，並未違背憲法第十一條保障人民言論及出版自由之本旨。」亦同此旨。

註14：律師談吉他（2023），〈小玉條款通過，正義就會來了嗎？〉，

<https://www.facebook.com/LawyerGuitar/posts/pfbid0f99FNZ4MoRU2uhBfS264KL2Q4XuaPit6mtACFVnAvFgxAaotgTz6G9GTXjdvPGKDI>

註15：林明鏘（2020），〈立法學之概念、範疇界定及功能〉，《政大法學評論》，第161期，第92頁。

註16：其刑度為：五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。

另一瑕疵，蓋於所製作者係真正之身體隱私部位影像時，其最重刑度僅為3年有期徒刑，然於所製作者係不實的（虛偽的）身體隱私部位影像時，卻應適用更加重度之刑罰，雖因真偽之不同可致刑度差異，惟造成「實際侵害」之處罰強度低於「虛擬侵害」之理由為何？不免令人質疑其間差異之妥當性。

肆、程序法之疑義

一、深偽影音對審判程序造成衝擊

伴隨著深偽不實影音技術的普及與相關刑事犯罪處罰規定之實施，刑事審判也不可避免地將在證據法上面對源自深偽不實影音之挑戰，蓋於過去司法實務中，一旦能夠提出有關爭議事實之影像或照片，由於大眾皆不致對影像或照片之真實性有所懷疑，相關事實爭議大多能迎刃而解。然而，在深偽不實影音技術發展與普及後，關於審判中之影像或照片證據，因原本大眾對其所持之真實性推定已有動搖，導致此類證據之證據能力與證明力都受相當程度影響。

按深度學習與偽造之程式，乃利用人工智慧技術從事影像或照片之偽造或變造，並使觀看者誤以為影像遭偽造或變造後之人做過或是說過其未曾做過的事與說過的話¹⁷。由於許多具深度偽造功能之影音軟體已可免費

在網路中取得，而ChatGPT亦已成為普遍可使用之人工智慧工具，可以想見目前我們所接觸的影音檔案，已有相當比例係經深度偽造；除一般人因此也更加無法辨識其所接觸影音檔案之真偽外，在審判中（不論民事或刑事）面對深度偽造影音證據之機會，也因此大大提升。此種轉變也勢必將在證據法與律師倫理等領域中，對傳統規範產生相當程度之衝擊。

又如使用人工智慧模擬他人臉部動作，製造他人說話或動作的不實影音，並散布於網路上，利用一般人誤會進而從中謀取政治或財產利益，亦常為深度偽造技術所衍生出來的議題，例如在2020年美國總統大選時，即有有心人士利用深度偽造技術，製造出美國前總統Obama及時任總統Trump變臉、並在影音中說出不符其理念的虛偽言論¹⁸，企圖獲取不當政治利益。因此，關於如何預防、緩和與處罰濫用惡意使用深度偽造技術之人¹⁹，已成為這幾年來法學界所關注之議題。美國紐約州眾議員伊薇特·克拉克（Yvette Clarke）曾於2019年6月提出了「深度偽造究責法案（Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019, DEEP FAKES Accountability Act.）」草案²⁰，雖因深度偽造定義範圍過廣且無助於防止惡意深度

註17：Riana Pfefferkorn, Deepfakes in the Courtroom, 29 B.U. Pub. Int. L. J. 245, 247(2020).

註18：許恆達，前揭註3，第3頁。

註19：Kirsten Korosec, 'Deepfake' revenge porn is now illegal in Virginia, TechCrunch, March 17, 2023, available at:

<https://uk.news.yahoo.com/deepfake-revenge-porn-now-illegal-223137643.html>

註20：有指出，「本草案令人關注之處除配合現今科技發展特性為規定外，另針對實務上曾衍生的爭議問題，特別將外國勢力或其代理人（foreign power or an agent thereof）介入美國國內政治行為，如

偽造行為而未通過²¹，卻也突顯此一問題之重要性。

除了引發前述實體法之爭議外，深度偽造之影音檔案在審判（不論刑事、民事或行政訴訟）上，將對證據法則之適用產生重大影響；蓋除了當事人會爭執其證據能力外，關於法官如何判斷影音檔案之證據能力，也將成為一個問題。此外，當所提出之影音證據存在是否經深度偽造之爭議時，證人（含鑑定人）如何對深偽影音作證、與陪審員（國民法官）如何評價該影音證據，均會是判斷影音證據是否屬深偽影音之重要議題²²。而在製作或散佈深偽影音檔案罪之審理過程中，如該深偽影音檔案已經加密時，類此舉證或取證等問題將變得更加複雜。

二、驗真或釋明程序之重要性

又深偽影音之普及，亦將對真正影音之舉證產生衝擊，蓋縱當事人所舉之證據為真實

影音檔案，在深偽影音無所不在的影響下，一般人難免會對所接觸影音檔案之真實性，產生質疑，因此，深偽影音的出現，亦將變相地加重舉證者之證明義務，亦即，舉證者必須證明其所提影音證據為真正影音（authentic video），而非深偽影音（deepfake video）。而其對造即可在藉由對所提影音是否屬於深偽影音之質疑，挑戰該影音檔案之證據能力與可信性，並降低該影音檔案於訴訟上可能產生對其不利影響²³。而因法官與陪審員亦將期待影音檔案之舉證者，使用複雜之科技證明該檔案之真實性，此亦加重舉證之負擔。而如法官與陪審員均對影音檔案之真實性以過於嚴格之高標準，課予舉證者高度之證明義務，導致證明手段越來越困難；因此，持此種高度之懷疑論，將對整體司法制度之功能造成負面之影響²⁴。

為能初步確認所舉證據之真實性，聯邦證據規則Rule 901(a)乃要求舉證者提出支持該證

意圖影響美國國內公共政策辯論(domestic public policy debate)、選舉或其他不得合法從事的行為等納入規範。依該草案之內容，其所規範者包含視聽紀錄、視覺紀錄及錄音紀錄；意即任何人使用任何技術或設備製作假冒他人名義(false personation)的紀錄，並於網路或其他知識傳播管道發布者，應有浮水印、口頭陳述或是於文本中有簡要說明等揭露，以使他人得清楚知悉該紀錄並非真實，如行為人有違反該揭露規定並利用深度偽造1.意圖羞辱或騷擾(包含性內容)；2.意圖造成暴力、身體傷害、煽動暴亂、外交衝突或干預選舉；3.詐欺犯罪等，將可處5年以下有期徒刑，或科或併科罰金。另若行為人修改或刪除他人揭露之資訊而有上述意圖或犯罪行為者，亦可處以同等罰責。」莊貫勤(2020)，〈美國眾議院提出「深度偽造究責法案」〉，資策會科技法律研究所，available at:

<https://stli.iii.org.tw/article-detail.aspx?no=0&tp=1&d=8373>

註21：Zachary Schapiro, DEEP FAKES Accountability Act: Overbroad and Ineffective, B.C. INTELL. PROP. & TECH. F. (Apr. 27, 2020),

<http://bciprf.org/2020/04/deepfakes-accountability-act/>

註22：Riana Pfefferkorn, Deepfakes in the Courtroom, 29 B.U. Pub. Int. L. J. 245, 254(2020).

註23：United States v. Dhinsa, 243 F. 3d 635, 658 (2d Cir. 2001); United States v. Tin Yat Chin, 371 F. 3d 31, 38 (2d Cir. 2004).

註24：Riana Pfefferkorn, Deepfakes in the Courtroom, 29 B.U. Pub. Int. L. J. 245, 255 (2020).

據具其所指證據價值之證明²⁵，此即一般所稱之證據驗真或釋明 (Authenticating or Identifying Evidence) 程序；任何未能通過此程序之證據，原則上即無證據能力。其實早在1860年代，當新興的照相技術方興未艾之際，即曾有人利用幾可亂真的靈異照片 (spirit photograph) 進行詐騙，後經專業攝影師揭露照片造假疑點，方使真相大白²⁶。或許在完備的驗真或釋明程序之要求下，對於有意利用深度偽造影音技術在網路上造成特定侵害或侵擾之人來說，深偽影音對審判程序所造成之威脅，將會如同過去相片、影片、電子影像發展初期亦曾對司法程序造成相當影響般，終將逐漸消退²⁷。

三、驗真標準及其難題

按證據能力的基本前提在於滿足驗真之要求，舉證者必須提出支持該證據具其所指證據價值之相關證明，亦即透過表面證據 (prima facie) 使理性陪審員相信舉證者之證據主張為真正²⁸。只有在滿足驗真要求後，陪審團才可以自由心證之標準，認定事實存

否之爭議²⁹。一般來說，法院在影音檔案之驗真程序，其要求與相片之驗真程序相同，均要求舉證者證明影片或相片即能真實地代替其所描述之事實經過³⁰。證明者可以是拍攝之人，也可以是在場目擊之其他證人，或是其他可以證明該影片或照片係於何時、何地、或在何種情況下拍攝之人³¹；換言之，證人不一定是要對證明事項有第一手資訊之人，任何對影像或照片中所描述之人、事、時、地、物有認識之人，均可在驗真程序中提供有關影音檔案為真正之證明³²。

然而，由於實際上沒有人對經深度偽造之影音檔案握有第一手資料，因此，只要對影音檔案中所描述之人有相當程度之熟識，均得以辨識容貌或聲音之方式，提出影音是否遭偽造之證明。不過，當影音內容不含聲音時，真偽之辨識工作即有困難。特別當某則影音檔案原係存放在某新聞媒體之檔案室（不論係媒體工作者自行拍攝或是由民眾提供手機影音檔案）、或是存放在政府資料庫中之時，誤判之風險將高度提升，蓋因在此種情況中，通常只要求檔案保管者提供者保

註25：It provides: “(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.”

註26：Jennifer L. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 *Yale J. L. & Humanities* 1, 38 (1998).

註27：Russell Brandom, *Deepfake propaganda is not a real problem*, *The Verge*, Mar 6, 2019, available at: <https://www.theverge.com/2019/3/5/18251736/deepfake-propaganda-misinformation-troll-video-hoax>

註28：United States v. Workinger, 90 F. 3d 1409, 1415 (9th Cir. 1996).

註29：United States v. Tin Yat Chin, 371 F. 3d 31, 38 (2d Cir. 2004).

註30：People v. Goldsmith, 326 P. 3d 239, 245 (Cal. 2014).

註31：State v. Newman, 484 P. 2d 473, 477 (Wash Ct. App. 1971).

註32：State v. Sapp, 332 P. 3d 1058, 1061 (Wash Ct. App. 2014).

管及複製證明，即完成驗真程序³³，甚至在政府資料庫中保存之情形中，還可能因聯邦證據規則Rule 902(4)(A)自我驗真之規定，而免除驗真程序³⁴。此種自我驗真或免除驗真程序之規定，在駭客猖獗、資料遭不當使用之案件頻傳之現實環境中，如不能確保網路安全，亦可能成為誤判影音檔案真實性之重要因素。特別在警方隨身攜帶之街頭攝影機可能被遠端操控、其所錄製電子檔案可能遭人為竄改並上傳的風險中，如果不能肯認該街頭攝影機能自動地以加密技術確保所錄影像之真實性，其於雲端所同步儲存之影音紀錄檔案，即無從以證人或其他方法確認影像中之連續畫面未經變造³⁵。

另在前述第三人資料庫可能遭遠端竄改之情形中，因影音紀錄之連續性及可能遭質疑，舉證者勢必要付出更大的心力去證明該

影音檔案之真實性，以擔保影音檔案未經竄改；故除舉證之對造會主張排除該可能遭偽造之影音證據外³⁶，審判法官於作出證據能力之判斷前，亦必須考量該影音證據遭竄到改之可能性³⁷。而因深偽影音之證據爭議在於如何證明其經偽造，甚至反過頭來影響真正影音之證據能力判斷，不過，隨著人工智慧技術的發展，越來越多設計用來偵測深度偽造之工具與數位鑑識專家，均將在電子證據之驗真程序中扮演重要的角色³⁸，並在訴訟程序中協助法院排除虛假影音證據³⁹。惟如科技發展導致影音證據之真偽難以區分，似乎只能藉由製作真正影音檔案時附加確認真實標記之技術，才能作為證據能力之判斷依據。換句話說，如果於技術上無法或難以辨別影音證據之真偽，似乎只能在影音檔案作成時就同步進行驗真之程序⁴⁰，此觀聯邦

註33：Riana Pfefferkorn, Deepfakes in the Courtroom, 29 B.U. Pub. Int. L. J. 245, 260 (2020).

註34：It provides: “(4) Certified Copies of Public Records. A copy of an official record-or a copy of a document that was recorded or filed in a public office as authorized by law-if the copy is certified as correct by: (A) the custodian or another person authorized to make the certification.”

註35：Lily Hay Newman, Police Bodycams Can Be Hacked to Doctor Footage, Wired, Aug. 11, 2018, available at:

<https://www.wired.com/story/police-body-camera-vulnerabilities/>

註36：State v. Smith, 192 So. 3d 836, 837 (La. Ct. App. 2016).

註37：Kathryn Lehman, Scott Edson and Victoria Smith, 5 Ways to Confront Potential Deepfake Evidence in Court, Jul. 26, 2019, Law360, available at:

<https://www.law360.com/articles/1181306/5-ways-to-confront-potential-deepfake-evidence-in-court>

註38：Jonathan Mraunac, The Future of Authenticating Audio and Video Evidence, Law360, Jul. 26, 2018 available at:

<https://www.law360.com/articles/1067033/the-future-of-authenticating-audio-and-video-evidence>

註39：Mark J. Pescatore, Forensic Video Experts: Fake Videos Not Threat to Courtroom Evidence, PIPELINE COMM, June 24, 2019, available at:

<https://www.pipcomm.com/2019/06/24/forensic-video-experts-fake-videos-not-threat-to-courtroom-evidence/>. 27 People vs Beckley 185 Cal.App.4th 509 (Cal. Ct. App. 2010).

註40：Sam Gregory, Ticks or It Didn't Happen: Confronting Key Dilemmas in Authenticity Infrastructure

證據規則Rule 902(13)(14)有關電子處理系統生成紀錄之自我驗真程序⁴¹，即可明瞭。

伍、律師倫理之挑戰

深偽影音的出現與普及，除衍生前述實體法與程序法的疑義外，亦對律師倫理產生一定程度的衝擊。按依律師法第1條：「（第1項）律師以保障人權、實現社會正義及促進民主法治為使命。（第2項）律師應基於前項使命，本於自律自治之精神，誠正信實執行職務，維護社會公義及改善法律制度。」與第31條：「律師為他人辦理法律事務，應探究案情，蒐集證據。」等規定，為維護被告權益，律師應本於誠信，搜集有利被告之證據，雖依第38條：「律師對於委任人、法院、檢察機關或司法警察機關，不得有矇蔽或欺誘之行為。」與第43條第2項：「律師對於受委任、指定或囑託之事件，不得有不正當之行為或違反其職務上應盡之義務。」等規定，律師不得以欺罔手段執行辯護職務，惟在深偽

影音可為證據之情形中，律師在提出或排除該影音證據時，究竟應遵守何種程序規範，始符合誠信執業之要求，卻有待釐清。

關於前述律師法之誠信執業要求，律師倫理規範⁴²亦有相對應之規範。除律師倫理規範第7條：「律師應體認律師職務為公共職務，於執行職務時，應兼顧當事人合法權益及公共利益。」、第8條：「律師執行職務，應基於誠信、公平、理性及良知。」與第11條：「律師不應拘泥於訴訟勝敗而忽略真實之發現。」等抽象規定外，第16條第2項：「律師不得以威脅、利誘、欺騙或其他不當方法取得證據、要求任何第三人不得向對造當事人提供相關資訊、以提供利益方式誘使證人提供證據，或提出明知為虛偽之證據。」即具體要求律師取得與提出證據之禁止規範。而在證據可能為深偽影音之情形中，律師除不應參與偽造、變造之過程外，亦應具備警覺性，並儘早確認其真實性；倘若律師本身對於當事人提供之證據存在真實性之質疑，即應拒絕在偵查、審判中提出該證據⁴³。事實上，前述具體要求，已為律師

for Multimedia, at 6, Witness, Dec. 2019, available at:
<https://lab.witness.org/ticks-or-it-didnt-happen/>

註41：Rule 902 (13) provides: “(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902 (11) or (12). The proponent must also meet the notice requirements of Rule 902 (11).”

Rule 902 (14) provides: “(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule (902 (11) or (12). The proponent also must meet the notice requirements of Rule 902 (11).”

註42：現行律師倫理規範，乃全國律師聯合會於2022年5月29日、7月3日第1屆第4次及第5次會員代表大會修正通過，全文共55條。

註43：ABA, Model Rules of Professional Conduct Rule 3.3 (a)(3).

倫理規範第24條：「（第1項）律師於執行職務時，不得有故為矇蔽欺罔之行為，亦不得偽造變造證據、教唆偽證或為其他刻意阻礙真實發現之行為。（第2項）律師於案件進行中，經合理判斷為不實之證據，得拒絕提出。但刑事被告之陳述，不在此限。」所規範。不過，在律師確信或懷疑當事人提出之證據為偽造、變造之情形中，律師倫理規範卻無允許律師向律師公會或主管機關諮詢以解免保密義務之規範⁴⁴，尚不足以嚇阻當事人利用律師提出深偽影音作為證據之動機。

此外，即便律師對其當事人負有積極與忠誠之執業義務，在以深偽影音為由排除對造提出證據之情形中，律師應本於促進訴訟之義務，避免提出無根據或瑣碎之反對（異議）⁴⁵，以達其騷擾對造或拖延訴訟之目的；蓋除保障人權外，律師尚擔負著實現社會正義及促進民主法治之使命。如同照相技術一開始對司法系統造成相當程度之衝擊般，影音技術也對當下的事實認定功能產生一定程度之影響，如果基於相片本身具有真實推定之功能，即主張任何出版機構或新聞媒體應拒絕提出明知或懷疑內容經偽造、變造之相片，則基於視聽受眾之信賴保障，進一步要求提出影音證據（包含律師在內）

者，有義務拒絕提出明知或懷疑內容經偽造、變造之深偽影音⁴⁶，應該也是法理之中的倫理要求。

陸、結論

影音技術的發展，在提升生活品質之外，也創造了不少的問題。為了解決源自深偽影音的爭議，立法者雖已於刑法增加相關的犯罪規定，卻未在程序部分，作出相對應的回應。本文除對增訂之實體法規提出檢討外，亦對與深偽影音有關之程序法與律師倫理規範，提出相關建議。期現行法制能正視目前驗真程序與律師倫理規範之缺漏，妥適因應深偽影音對證據法制與律師倫理所造成的衝擊。當然，欲有效處理惡意深度偽造行為，不能僅靠刑事處罰，仍有賴其他行政管制措施與侵權賠償法制的配合⁴⁷，才能讓有害的深偽影音不在網路世界繼續流傳⁴⁸。

不過，前述法制對於移除、下架、禁止散布與再散布等實質補救機制，似乎仍有不足，如此是否將對被害人求助司法的意願造成負面影響，觀諸犯罪被害人權益保障法第35條第2項⁴⁹所採之「介接刑事訴訟法羈押替

註44：ABA, Model Rules of Professional Conduct Rule 1.6 (b)(4).

註45：ABA, Model Rules of Professional Conduct Rule 3.1.

註46：Jeffrey Westling, Deep Fakes: Let's Not Go Off The Deep End, Techdirt, Jan. 30, 2019, <https://www.techdirt.com/2019/01/30/deep-fakes-lets-not-go-off-deep-end/>

註47：Zachary Schapiro, DEEP FAKES Accountability Act: Overbroad and Ineffective, B.C. INTELL. PROP. & TECH. F. (Apr. 27, 2020), <http://bciprf.org/2020/04/deepfakes-accountability-act/>

註48：蔡碧玉，前揭註10，第85頁。

註49：被害人權益保障法第35條第2項：「法院就犯刑法第二十八章之一，或以性影像犯刑法第三百零四條、第三百零五條、第三百四十六條之罪案件之被告許可停止羈押時，經審酌人權保障及公共利益

代處分規定之保護命令」制度，僅將「移除或向網際網路平台提供者、網際網路應用服務提供者或網際網路接取服務提供者申請刪除已上傳之被害人之性影像」作為停止羈押條件等相關法制，是否足以促使未受羈押之被告配合移除境外網站之（深偽）性影音，確實令人質疑；蓋於性私密影像流傳至境外網站時，主管機關難以依性侵害犯罪防治法

第13條第1項⁵⁰與兒童及少年性剝削防制條例第8條第1項⁵¹等規定要求境外網站將其下架或移除，此時，如不能確實要求上傳者移除（深偽）性影像，對被害人來說，其權益保障之意義即屬有限⁵²。因此，宜立法強化加害人移除相關影像之規定，以保障被害人合法權益。

（投稿日期：2024年10月22日）

之均衡維護，認有必要者，得依職權或檢察官之聲請，定二年以內之相當期間，命被告遵守下列事項：一、前項第一款至第三款之事項。二、禁止重製、散布、播送、交付、公然陳列，或以他法供人觀覽被害人之性影像。三、提出或交付被害人之性影像。四、移除或向網際網路平台提供者、網際網路應用服務提供者或網際網路接取服務提供者申請刪除已上傳之被害人之性影像。五、禁止其他危害被害人之事項。」

註50：性侵害犯罪防治法第13條第1項：「網際網路平臺提供者、網際網路應用服務提供者及網際網路接取服務提供者，透過網路內容防護機構、主管機關、警察機關或其他機關，知有性侵害犯罪嫌疑情事，應先行限制瀏覽或移除與犯罪有關之網頁資料。」

註51：兒童及少年性剝削防制條例第8條第1項：「網路業者透過主管機關或其他機關，知有第四章犯罪嫌疑情事，應於二十四小時內限制瀏覽或移除與第四章犯罪有關之網頁資料。」

註52：民間司法改革基金會，〈民間版修法說帖 | 威脅散布性私密影像怎麼辦？〉，2023年1月17日，
<https://www.jrf.org.tw/articles/2417>