



# 眼見不為憑？ 瞭解 Deepfake 的應用

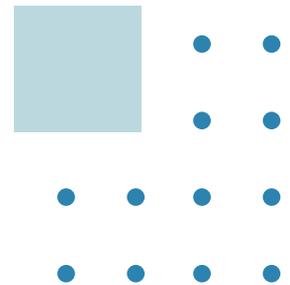


國中學生版

# 目錄

---

一、Deepfake是什麼?	2
二、Deepfake的犯罪類型	3
(一)類型一：造謠影片	3
(二)類型二：詐騙取財	3
(三)類型三：數位/網路性別暴力	3
三、防範Deepfake犯罪行為的方式	4
(一)如何避免成為Deepfake的主角	4
(二)瞭解相關的法律責任	4
(三)成為Deepfake的主角，該怎麼辦？	5



## 一、Deepfake是什麼？

深偽技術（Deepfake）是深度學習（deep learning）和偽造（fake）的混合詞，泛指各種藉由人工智慧達成的幾可亂真的偽造圖片、聲音或影片的技术，也就是透過蒐集同一個人的大量人臉相片，找出人臉的特徵跟結構，類似於人皮面具，直接把某個人的臉置換到另一個臉上。

在Deepfake技術的軟體工具開始開放給大眾下載，任何人只要準備好素材影片並學會如何使用該軟體工具，都能製作出類似的換臉影片。所以，網路上的影片是否真實成為了一個值得懷疑的問題，在識讀五花八門的網路資訊時，你會不會也陷入何者為真？何者為假的困惑呢？

### 深偽技術（Deepfake）的發展一開始是為了正向的用途！

#### 影視領域：重製逝世者的影像

在電影中重現已故人物或角色年輕模樣，或是透過人臉合成電影中很多難以表現的特效。

#### 醫療領域：為聾啞病人重製聲音

在醫療上為聾啞病人進行聲音重製，讓他們將來用原聲與人溝通。

#### 教育領域：翻生歷史人物

學校也可「翻生」歷史人物，將人物帶進課堂或作為教育工具，增加與學生的互動性，讓課程更具趣味性。

但是當這項技術發展得越來越成熟後，一些不法分子運用它做了不良的示範，進而對社會安定與國家安全產生深遠的危害。



## 二、Deepfake的犯罪類型

Deepfake的不適當應用除了可能侵害他人的隱私與名譽外，也可能讓社會大眾難以辨識電腦網路資訊的可靠性與真實性，動搖人與人之間的信任關係，例如可能會有不法分子散布造謠影片，運用Deepfake影像詐騙取財，或是合成色情影片造成他人的傷害。

### (一)類型一：造謠影片

雖然Deepfake能製造出逼真的虛假影像和聲音，導致網路上可能會出現各種造謠影片、虛假的言論或話題，但是很多人都有自己習慣的用語、手勢或是表情，所以知名人物出現與日常言行不一致的影片，就有必要進行查證。

### (二)類型二：詐騙取財

歹徒可能利用合成影片與語音，誘騙被害人聽從指示，例如民眾若會遇到親友或陌生人以影片或電話請求借錢、威脅匯款或要求您提供身分證件，你可以運用Deepfake技術的破綻，要求對方轉轉頭、在臉前揮揮手，辨識對方是否使用變臉，或是你也可以與親友互相約定「通關密語」，所以面對來路不明的電話、影像，必須隨時保持警覺跟存疑，以避免受騙。



### (三)類型三：數位/網路性別暴力

網路上就有透過Deepfake合成某人的色情照片或影片，製作不實的性影像，或是對外散布，甚至營利，但是就算成品的製作拙劣或破綻百出，基本上也不會有人相信影中人是受害者本尊，但是這樣的行為已經對受害者的隱私安全與人格尊嚴造成無法彌補的傷害，而在資訊快速流通的社會中，加害者的照片取得容易，也讓傷害形成的更快速，所以無論性別、年齡都可能受到傷害。

針對深偽影像的專法-刑法「妨害性隱私及不實性影像罪」已經於112年2月10日上路，同時，以Deepfake造謠影片、詐騙取財、製作不實的性影像等等的行為就侵害當事人的肖像權以及素材影片原創者的著作權，可能已經觸犯多項法律，如隱私權、肖像權和倫理議題，而 Facebook和X (Twitter) 社群平臺也會自律地主動下架這些Deepfake色情影片。

為避免成為Deepfake的主角，或是落入不肖人士設下的陷阱，我們每一個人都需要保持警覺心，留意辨識深偽影片，學習尊重他人，切勿散布不實影音。

### 三、防範Deepfake犯罪行為的方式

防範深偽技術的重要性在於保護個人的隱私安全與國家社會的安定。若網路上廣泛出現極為逼真的虛假影片、聲音，就容易誤導公眾並對社會造成嚴重影響，除了避免成為Deepfake的主角，更需要進一步學習辨識Deepfake所產生的內容及人工智慧等相關議題有更深的認識與瞭解，以提升自我的數位素養。

#### (一)如何避免成為Deepfake的主角

盡量避免流傳自己臉部的照片或影片，由於製作Deepfake的軟體工具是開放大眾使用的，為避免成為Deepfake攻擊的受害者，唯一的辦法就是盡量避免流傳自己各種拍攝角度和高解析度的各種照片、影片紀錄等資料。

#### (二)瞭解相關的法律責任

未經當事人授權，無論是製作或是散布Deepfake影片都是侵權或犯法的行為。在臺灣，將他人的臉部移植到某部影片，就已經構成侵害當事人的「肖像權」以及影片原作者的「著作權」，若將影片廣為散布，甚至侵犯當事人的「人格權」。

若將他人的臉部移植到色情影片，基本上散布任何真實或偽造的色情影片就已經觸犯「散布猥褻物品罪」，以及刑法「妨害性隱私及不實性影像罪」，若是針對特定人士偽造影片，可能同時觸犯「公然侮辱罪」或「加重毀謗罪」。

### (三)成為Deepfake的主角，該怎麼辦？

#### 1. 冷靜

先別急著與散布者爭吵，如果激起了加害者或酸民們的情緒，可能會讓影片散布得更廣。

#### 2. 截圖存證

不管是偽造影片本身，發布或散布偽造影片的帳號名稱、時間點、相關留言內容全都截圖保存，以免對方卸責或湮滅證據，這些截圖證據對之後的申訴或訴訟程序非常地有幫助。

#### 3. 申訴

若不幸變成Deepfake影片主角，應該先冷靜地蒐證，再向網路平臺管理員申訴或是向iWIN網路內容防護機構 (<https://i.win.org.tw/>) 申訴。

#### 4. 報警

電信警察也能夠根據電信公司提供的IP使用時間與地點資料，逐步縮小搜查範圍，找出犯罪嫌疑人，警方也會協助要求網路平臺將影像移除。

#### 5. 諮商及輔導

如果學生不慎成為Deepfake的影片主角，並一直處於沮喪及低落的情緒時，教師應該協助學生尋求多元的協助管道，在心理諮商及輔導資源，可撥打衛生福利部安心專線1925、張老師生命專線1980、生命線專線1995，避免學生沉溺於受害者的情境，也可讓學生慢慢恢復原本的生活步調。



Deepfake技術本身並無「好壞」，現今已在影視、醫療以及教育領域等產生正向運用，身處在新興科技與AI發達的時代，人們在網路上辨識各種資訊變得更加具有挑戰性，面對網路資訊，隨時保持警覺心，看到任何奇怪的圖文或影片，盡量求證當事人，對於我們無法即時求證的事，也應當先保留懷疑的態度，不做任何評論或散布訊息，所以我們每個人都應謹慎地思考和評估所見的資訊，培養對於假消息的警惕性，以確保我們獲取的資訊是可信的。

## 參考資料

---

為保護個人隱私，防範深偽技術（Deepfake）淪為犯罪工具，本部研議刑法增訂「散布性私密影音罪」、「製作或散布他人不實性影音罪」、「製作或散布他人不實活動、言論、談話罪」，今日向行政院陳報修正草案（2021年11月17日）。中華民國法務部。

<https://www.moj.gov.tw/2204/2795/2796/123192/post>

Deepfake掀起的新科技犯罪風暴專家教你4招肉眼破解技巧（2023年1月13日）。台灣事實查核中心。

<https://tfc-taiwan.org.tw/articles/8681>