苗栗縣政府政風處

廉政宣導

2020.08

Contents

1、公務員涉犯貪污治罪條例案例

2、公務員服務法

-公務員兼職禁忌多，當社區管委也不行

3、消費者保護篇

-Deepfake模擬人聲太真實！

一通電話騙走CEO近千萬

PART 1

公務員涉犯貪污治罪條例案例

案例1、

聯合報2020/08/06

涉採購洩密圖利廠商 南部某鄉公所4公務人員遭起訴

南部某地檢署偵辦某鄉公所，有公務員涉嫌洩漏相關採購資訊以圖利特定廠商與違反政府採購法等不法情事，經廉政署南調組調查發現，某鄉公所鄭姓主秘與公所張姓、余姓、劉姓課長與6名廠商，共10人，檢方依貪汙罪起訴，考量在偵查中坦承，廠商以繳回不法得利約45萬元，建請法官減輕量刑。

某鄉公所第二納骨堂興建及第一座納骨堂整修補強統包工程之公共藝術設置的勞務採購標案，公所在2018年8月20日開標，得標廠商承諾回饋方案包括在工程範圍的綠地，某國小旁公園內，以45萬元建置「紅豆地景藝術作品」。檢方發現，鄭姓主秘有意將該工程給黃姓廠商施作，事前將徵選委員名單的秘密事項洩漏給黃姓廠商。從中獲得第一序位與優先參加議價會議的權利。

案例1、

(續前頁)

聯合報2020/08/06

另外，2019台灣燈會某鄉鎮市點亮計畫-OO鄉公所特色花燈車勞務採購標案中，鄭姓主秘為讓黃姓廠商取得該標案承作，將該標案採評選方式以參考最有利標精神的決標方式辦理，也為讓黃姓廠商得標，由公所余姓人員配合將標案相關訊息應保密事項洩漏給黃姓廠商，讓黃姓廠商可以事先規畫設計與預先備標。

檢方查出，2018、 2019年的紅豆牛奶節相關活動，鄭姓主秘也都事前洩漏相關採購需求的內容給黃姓廠商。

檢方指出，公所鄭姓主秘、張姓、余姓與劉姓課長，黃姓廠商等人，在偵查中自白，其中黃姓廠商等人已繳回不法所得，44萬8000多元，建請法官減輕其刑。

案例2、

TVBS NEWS 2020/07/15

護航KTV業者
某市建管處人員涉收賄遭搜索

檢調獲報，曾姓、周姓公務員任職北部某市政府，負責建築物升降設備委外抽驗標案，2人互為職務代理人，並同時聘請劉男作為私人助理。

北部某市錢櫃KTV4月間發生火警後，某市府嚴查電梯安全。曾男5月間發現一家連鎖KTV的5部菜梯並無使用許可證，輾轉向業者浮報申請竣工檢查費用，每部菜梯溢價2000元，共收取1萬元，事後菜梯獲核發許可證。

此外，曾男發現某市一家賣場的升降設備檢查照片有異，暗示電梯公司與受託檢查的民間協會「要處理一下」，藉此收受電梯公司與協會的8萬元賄款。

案例2、(續前頁)

TVBS NEWS 2020/07/15

檢調還查出，曾姓、周姓公務員對外宣稱檢查量太大，必須聘請私人助理，曾男向3家得標的廠商按月收取4萬5000元，周男則向2家廠商按月收取9000元。曾、周向廠商取款後，部分款項交給劉姓私人助理，其餘朋分花用。

地檢署蒐證多時，今天上午指揮調查局某市調查處兵分27路搜索，預計約談39名犯罪嫌疑人、證人，全案朝貪污治罪條行受賄等罪嫌偵辦。

PART 2

公務員服務法
-公務員兼職禁忌多，當社區管委也不行

公務員
服務法

公務員兼職禁忌多，當社區管理委員也不行

自由時報2020/05/21

圖片來源：台中市政府警察局

某市交警石oo2010年起開始上電視當球評，雖屢遭檢舉，但交通大隊始終認定查無違法兼職，直到今年再度被檢舉，才移請公懲會懲戒。一名曾任公懲會委員的法官指出，公務員的兼職禁忌非常多，只要未報備核准，全部屬於違法，依照實務見解，一般可處記過，並視情節追加罰款。

銓敘部對違法兼職的態樣多所函釋，最離奇的是，連擔任社區管理委員會委員，都屬於兼職，應報請機關首長簽核，公務員宜特別注意。

該名法官指出，石oo2010年及2015年任職某市A、B分隊期間，各被調查過一次，惟報告結論是「查無違法兼職」，有兩種可能，第一種可能是石oo上電視評論足球前，有依規定向所屬機關報備並獲准，第二種可能是調查嚴謹度不足，未先函詢銓敘部意見。

公務員服務法

(續前頁)

自由時報2020/05/21

他解釋，公務員任何的兼職都應向首長報備，否則就是違法，而機關接獲檢舉，應先向「公務員服務法」的主管機關銓敘部詢問，再判定此種兼職是否屬於違法態樣，切勿自行解讀，以免發生疏失，遭到糾正。

而根據銓敘部去年11月25日函釋，只要「經常」、「反覆」實施同一業務，即屬兼職。從過往案例來看，前台大醫師孔OO當部落客並獲取紅利分潤，就被記過一次，石OO是明知且持續、長期領取報酬，除了面臨記過，公懲會若認為兼職所得過高，還可能併為罰款。

PART 3

消費者保護篇
-Deepfake模擬人聲太真實!
一通電話騙走CEO近千萬

數位時代 2020/04/15

Deepfake模擬人聲太真實！一通電話騙走CEO近千萬

新型態網路詐騙到形塑社會矛盾，Deepfake技術出現至今3年間，對「信任」一詞的傷害力，恐怕比想像中還要巨大。

2019年3月，國際間出現了前所未見的網路詐騙行為。一位英國能源公司CEO接到他德國母公司老闆的電話，要求他代墊約730萬新台幣款項，將費用轉給該集團位於匈牙利的一家供應商，並表示之後會再將錢補還給他。

然而，這位CEO不但沒領到錢，反而又一次接到老闆電話，指定他支付另一筆款項。這時他才驚覺，即便老闆德國口音聽上去很正常，實際上卻是由Deepfake模擬出來的人聲。那筆730萬元的款項，也從匈牙利被轉到墨西哥，再匯往多個不同地區，難以追查下落。

資安大廠趨勢科技機器學習研究員張佳彥表示，這是一種進階版「變臉詐騙」（Business Email Compromise，又稱商業電郵詐騙）。他說，隨著Deepfake技術門檻降低，過去在商業郵件中模仿他人文字風格為主的詐騙行為，開始走向影像與聲音應用，彰顯了Deepfake逐漸擴張的威脅性。

圖片來源：品玩

(續前頁)

數位時代 2020/04/15

打假辦法才被提出，一下子就被「突破」

「一旦Deepfake製造時間能壓縮到數分鐘內，Deepfake詐騙就可能愈來愈常見。」張佳彥說。

張佳彥表示，要做出比較擬真的Deepfake，以現有技術來說，影片會需要約數百到數千張人臉素材照片、聲音則需要約20分鐘錄音檔，並讓深度學習的模型演算約一個禮拜時間才可行，時間、技術成本較高。但他也認為，未來Deepfake詐騙的發展性，恐怕難以估量。

令人稍微慶幸的，趨勢科技目前尚未在台灣發現Deepfake網路詐騙行為。「相較於傳統網路釣魚攻擊一次就可以發上萬則電子郵件，用Deepfake做變臉詐騙技術成本還是比較高。」張佳彥說。

我們可以看到，在馬斯克的這段演講影片中，Deepfake的換臉技術幾乎達到人眼無法區別的地步。

值得注意的是，近年來Deepfake的進展速度，正不斷超越現有檢測技術。

2018年時，紐約州立大學奧爾巴尼分校電腦科學系副教授呂思偉曾提交一篇論文，點出Deepfake影片中人物眨眼頻率過低，便建議以此作為檢測標準。

(續前頁)

數位時代 2020/04/15

原來，他發現許多名人Deepfake影音的訓練素材，都來自於公開照片，鮮少有閉眼的圖像數據，導致眨眼動作顯得不流暢。然而，在這則論文公開以後，Deepfake製造者很快就更新了他們的AI訓練模型，克服了眨眼問題。「這是一個持續戰鬥的過程。」呂思偉表示。

就現階段而言，若想防止自身相關影片被有心之人拿來做Deepfake，張佳彥提出一個建議：「你可以試著在影片中用手晃過自己臉上，」他說，「東西晃過去時會切割臉部畫面，就現階段技術而言，很難沒有破綻。」

然而，誰也不知道，這招防禦方法，是否哪天會被持續進步的技術破解。

無論社群平台對抗操弄資訊者，或是資安公司對抗網路詐欺犯，兩者最終都指向一場不斷升級的AI軍備競賽。站在這個看不到盡頭的競賽起跑點，我們將要奔向的未來，或許正是一個「眼見不能為憑」的時代。

苗栗縣政府政風處
關心您

法務部廉政署檢舉服務專線：0800-286-586
苗栗縣政府政風處廉政專線：037-356639