數位性別暴力之防制——以網路跟蹤騷擾為中心

張維容

壹、前言

隨著數位科技發展迅速及運用普及，利用或透過網路或數位方式之性別暴力層出不窮，態樣更趨多元，其類型包括人肉搜索、性勒索、網路跟蹤騷擾（以下簡稱網路跟騷）、未經同意散布性私密影像（Nonconsensual Pornography, 簡稱NCP）及人口販運等（行政院性別平等處，2021a）。這些針對性別而施加他人的暴力或不成比例地影響他人，包括身體、心理或性之傷害、痛苦、施加威脅、壓制和剝奪其他行動自由等（《消除對婦女一切形式歧視公約》〔1979〕；行政院性別平等處，2020）。尤有甚者，該類型的犯罪並非性別中立之犯罪，而是以婦女為主，例如，以未經同意散布性私密影像的案件，就有高達九成的受害者為女性（Cyber Civil Rights Initiative, n.d.）。

我國為防制這些針對性別的網路暴力，陸續制定或修正相關法律，以強化相關處罰規定。包括2023年1月立法院三讀通過《刑法》修正草案（2023年2月8日總統修正公布），增訂「妨害性隱私及不實性影像罪章」，將偷拍、強拍等攝錄或散布性私密影像等犯罪行為明確入刑（註1）。此外，2022年6月1日我國施行之《跟蹤騷擾防制法》（2021）（以下簡稱《跟騷法》）中，將網路跟騷行為納入規範。該法規定行為人以電話、傳真、電子通訊、網際網路或其他設備，對特定人進行干擾，反覆或持續為違反其意願且與性或性別有關之行為，使之心生畏怖，足以影響其日常生活或社會活動者，即成立跟蹤騷擾罪，亦即網路跟騷係屬該法所列舉八種行為態樣之一。此外，該法規定於被害人報案後，警察機關應依法調查，如認有犯罪嫌疑者，得對行為人實施書面告誡；行為人如於受告誡後二年內再有跟騷

行為，被害人、警察機關、檢察官得聲請保護令。再者，由於跟騷行為具有高發生率、高恐懼性、高危險性及高傷害性等特徵，為能周全被害人之保護，該法亦規定於符合一定要件下，法官得對行為人採取預防性羈押，以及時保護被害人之安全。

我國《跟騷法》中之刑事制裁及相關保護措施，均屬案件「發生後」或警察機關受理「報案後」始啟動之防制作為。以刑事制裁為例，就該法一般跟騷罪、加重跟騷罪或是違反保護令罪之論處，司法機關必須依據法律構成要件，判斷案件事實，以定奪行為人之罪責，在刑事訴訟法就證據採取嚴格證明法則下，如欲達成「事後懲制」行為人之目的，不僅耗時費日，且緩不濟急。故本文關注之重點在於，如何於跟騷事件「發生前」或警察受理「報案前」，運用其他可能的措施或作為，以防制網路跟騷行為。從而，本文研究重心如下：首先，先釐清數位性別暴力、網路跟蹤騷擾之意涵及嚴重性。其次，探索被害人遭遇網路跟騷行為，於其未向警察機關報案前，或是未被執法人員（亦或被害人本身）認定是違法行為前，被害人會採取哪些模式以因應網路跟騷？最後，本文欲了解，除法律就違法行為採取事後制裁外，針對網路跟騷行為，哪些主體有共同防制之責？包括執法機關、刑事司法機關、網路平臺業者、被害人保護組織及被害人本身等，渠等又得採取哪些措施及具體作為防制網路跟騷行為？

貳、數位性別暴力與網路跟蹤騷擾

一、數位性別暴力之意涵及嚴重性

2018年聯合國人權理事會於其研究報告中，基於《消除對婦女一切形式歧視公約》（*The Convention on the Elimination of All Forms of Discrimination Against Women*, CEDAW）及相關人權文書，將「數位性別暴力」（Online and ICT-facilitated violence against women）予以概念性定義，並擴展其意涵如下：

> 部分或全部透過資通訊技術（如手機、網路、社群媒體、或電子郵件等）所施加或輔助於婦女的任何性別暴力行為，且該行為係針對婦女的性別而實施，對婦女構成嚴重影響。（United Nations, 2018）

有鑑於數位科技發展迅速，網路及其他數位環境之性別暴力叢生，對隱私權與人身安全造成諸多實害，我國行政院性別平等處（2021b）參酌CEDAW第35號一般性建議、第三次國家報告審查委員會結論性意見與建議第28點、第29點之意見，於2020年10月會議後公布《數位／網路性別暴力之定義、類型及其內涵說明》之文件，作為各部會未來政策制定及法令修正（制定）之參考。上開文件列舉十種為數

位性別暴力之類型及意涵，包括網路跟蹤、惡意或未經同意散布與性／性別有關個人私密影像或資料、網路性騷擾、透過數位方式發表、散播性別貶抑或仇恨之言論或行為、性勒索、人肉搜索、基於性別偏見所為之強暴與死亡威脅、招募引誘、非法侵入、竊取他人資料以及偽造或冒用身分。

依據我國行政院性別平等處（2023）公布之性別圖像統計，2021年依《性騷擾防治法》受理性騷擾申訴調查結果「成立」，且發生場所係在「虛擬環境－科技設備（如：網際網路、手機簡訊等）」者計291件（占所有場所22.7%），件數較前兩年（2020年172件、2019年122件）呈增加趨勢。另利用或透過網路或其他數位方式，直接或間接實施校園性騷擾且調查屬實者為487件（占25%），件數較2020年161件增加。

數位性別暴力造成受害婦女身體、心理乃至於經濟生活遭到傷害，其隱私權、人格權及名譽等亦遭受嚴重侵害。更甚者，由於網路匿名、快速廣泛傳播、反覆重製與存取，以及永久留存等特性，倘若被害人遭受性別暴力的影片或言詞一經公布，將難以完全移除下架，久而久之，受害婦女被迫退出不友善的數位空間，與社會漸行漸遠，其公共參與的意願及可能性受到壓抑，渠等獲取資通訊技術上亦產生不平等（王伊軒，2020）。

二、網路跟蹤騷擾之意涵及嚴重性

（一）網路跟騷之意涵

「網路跟騷」一詞用於指涉重複使用網路、電子郵件或其他電子通信設備跟蹤、騷擾、警告或威脅特定的個人或個別群體（D'Ovidio & Doyle, 2003），例如，美國司法部將網路跟騷定義為「使用網路、電子郵件或其他電子通訊，向其他用戶發送騷擾或威脅電子郵件」（U. S. Department of Justice, 1999; U. S. Department of Justice, 2005）。

我國行政院性別平等處（2021b）對於網路跟蹤騷擾之意涵如下：（1）對於他人反覆實施跟蹤騷擾行為，致令他人感到不安或畏懼，例如，傳送攻擊或恐嚇性電子郵件或訊息；對於他人網路留言，發表攻擊性言論等；（2）跟蹤或監視他人活動，例如，透過手機GPS定位或電腦、網路使用紀錄等方法為之；（3）監視或蒐集他人網路活動或資訊，進而違反他人意願與之接觸等。至於網路跟蹤騷擾之法規定義，依據我國《跟騷法》（2021）第三條，行為人以電話、傳真、電子通訊、網際網路或其他設備，對特定人進行干擾，反覆或持續為違反其意願且與性或性別有關之行為，使之心生畏怖，足以影響其日常生活或社會活動者。

（二）網路跟蹤騷擾之嚴重性

網路跟蹤騷擾之嚴重性，可由以下國內、外調查得知。首先，2012年美國司法部的一項調查中發現，被害人遭遇最多的兩種跟騷行為如下：（1）不受歡迎的電話及簡訊（占30.7%）；（2）不受歡迎的信件與電子郵件（占66.7%）（Catalano, 2012）。另Smith等人（2018）的《全國親密伴侶及性暴力調查總結報告》（*National Intimate Partner and Sexual Violence Survey*, 簡稱NISVS）顯示，跟蹤騷擾的受害者中有約有1／4的人表示，其曾被以電子郵件（83%）、即時訊息（35%）等網路方式騷擾，網路跟騷又以年輕族群較廣泛，年輕族群的生活明顯較為數位化，對相關數位工具也較具可近性（Dhillon et al., 2016）。

國內非政府組織現代婦女基金會於2019年公布一份針對18歲以上民眾所進行的「科技跟蹤線上大調查」（楊綿傑，2019），於397份有效問卷中，受訪者表示曾遭科技跟蹤（網路跟騷）的有24.2%，顯示每四位就有一位曾遭到科技跟蹤，而其中女性占78.4%。年齡分布則以18至25歲占35.4%最多，其次為31至35歲占15.6%，臺灣現況與國際趨勢相同。調查中指出，曾受騷擾民眾中有78.1%遭到臉書、LINE、IG等社群媒體騷擾跟蹤，其次是以手機或電話騷擾占26%；懷疑遭間諜監控軟體跟蹤排名第三，占14.5%。

再者，我國《跟騷法》自2022年6月1日施行至今已滿一週年，業管機關警政署指出統計至今（2023）年4月30日止，各警察機關共受（處）理2,724件跟蹤騷擾案件，其中90%被害人是女性、男性加害人占84.9%。這些案件中，又以利用通訊設備／手段進行騷擾行為（即通訊騷擾）占最多數，例如，GPS定位追蹤、觀察被害人IG打卡以尾隨製造巧遇等，共計1,698次，占所有案件24.42%，通訊騷擾位居八種跟騷類型的第一名，足見當代數位通訊普及，不法人士將之濫用於跟騷行為之嚴重性（內政部警政署公共關係室，2023）。

參、被害人回應網路跟蹤騷擾之模式

Tokunaga與Aune（2017）為了解網路跟騷被害人如何回應不受歡迎的追求，針對51位被害人完成調查研究（14位男性及37位女性）。調查結果顯示，被害人使用了七種一般管理風險的策略，其中最常見的是：忽略／迴避（Ignorance／Avoidance）、主動技術分離（Active technological disassociation）及尋求幫助（Help seeking）。此外，結果另顯示，被害者反應的模式與其所經

歷的行為類型有關。這項調查的實際用途在於實務工作者得以推薦以前使用過並獲致一定成功的具體行動予被害人，作為其管理特定類型網絡跟騷行為風險之參考。上述七種被害人回應網路跟騷行為的風險管理模式，依其使用頻繁度，依序為：策略一忽略／迴避（Ignore／Avoidance）、策略二主動技術分離（Active technological disassociation）、策略三尋求幫助（Help seeking）、策略四談判／威脅（Negotiation／Threat）、策略五順從／藉口（Compliance／Excuses）、策略六技術隱私維護（Technological privacy maintenance）、策略七減損（Derogation），具體方法詳如表1。

為了解上述七種策略中，何者最有效？何者較無幫助？Tokunaga與Aune（2017）進一步檢視每個人的感知並對之進行分級。其發現技術隱私維護（策略六）或將資訊設為保密並僅提供特定朋友（Available to negotiated contacts），是管理不受歡迎的線上追蹤（Online pursuit）最有效策略。其次，主動技術分離（策略二）是第二個最成功的風險管理行為；第三，則是忽略／迴避（策略一）。其餘依序為尋求幫助、談判／威脅、順從／藉口及減損。

綜上所述，前揭調查的主要結果依賴於風險管理中使用的行為及其感知有效性的自我報告數據。然Tokunaga與Aune（2017）亦不諱言指出，該研究招募的大學和線上樣本提供了用於解決大量網路跟騷行為更完整的管理策略，然而，這些響應招募資訊的人極有可能存在自我選擇偏見，未來的調查必須更關注用於收集涉及被害的敏感問題資料的抽樣程序。其次，用於評估管理策略有效性的回應效度量表是基於以下假設：被害人必然知道導致網路跟騷行為停止的原因。然而，在許多情況下被害人永遠不知道網路追騷行為結束的真正原因。未來的調查應更關注行為人對被害人所採取哪些行為的反思，以及這些行為如何成功地控制這些不受歡迎的線上追求。

肆、網路跟蹤騷擾的防制措施

Dhillon等人（2016）的研究中，調查一百多名受訪者對於網路跟騷問題的看法，並歸納分析出以下五個主要基本防制目標（即價值觀）：保護在線互動、建立網路跟騷的安全程序、確保技術安全、發展強大的價值體系（被害後之家庭支持）及定義中介盡量減少網路跟騷（註2）。該五大目標之達成，除被害人外，涉及相關公、私部門資源的有效分配。

由於網路跟騷被害人第一時間接觸行為人，其採取各種因應模式下之具體作法，大多涉及其他組織、執法機關或網路業者的配合及協力，以下參考國內

表 1　網路跟蹤騷擾被害人管理風險策略一覽表

策略	具體作法
策略一　忽略／迴避（Ignore/Avoidance）	1. 忽視 2. 避免追求者藉以接觸的網站或程式 3. 改變目標 4. 直接刪除訊息、不讀取 5. 表現出不受影響的樣子
策略二　主動技術分離（Active technological disassociation）	1. 刪除舊帳號，建立新帳號 2. 刪除／拒絕追隨者成為好友 3. 將資訊設為私密，只有接受的「朋友」才能瀏覽 4. 封鎖追隨者的訊息
策略三　尋求幫助（Help seeking）	1. 聯繫當地執法機構／提出告訴 2. 保留所有書面證據的硬碟 3. 聘請私家偵探 4. 要求第三方回應追隨者 5. 透過支持網站獲得幫助 6. 向網路所有人／互聯網服務提供商（Internet Service Provider, ISP）申訴追隨者的行為
策略四　談判／威脅（Negotiation/Threat）	1. 威脅追隨者 2. 與追隨者爭論 3. 告訴追隨者停止其行為或是被害人對其不感興趣
策略五　順從／藉口（Compliance/Excuses）	1. 一起玩 2. 假裝揭露自己的資訊 3. 為不能或不想建立關係找藉口
策略六　技術隱私維護（Technological privacy maintenance）	1. 更改頭像 2. 更改用戶名及／或密碼 3. 更改電子郵件地址 4. 下載防毒軟體
策略七　減損（Derogation）	1. 視追隨者為騙子，正面對抗之 2. 直接侮辱追隨者 3. 向追隨者發表公開議論

資料來源：作者參考Tokunaga與Aune（2017，頁1461）繪製。

文相關研究之成果（吳聖琪，2016；黃翠紋，2019；D'Ovidio & Doyle, 2003; Dhillon et al., 2016; Livingstone & Bober, 2005; MacKenzie & James, 2011; Petrocelli, 2005; U. S. Department of Justice, 1999; U. S. Department of Justice, 2005），歸納各個不同主體得採取哪些措施或作為，以有效防制網路跟騷行為。

一、執法及刑事司法人員

（一）建立認知及意識（Recognition and awareness）

執法機關及刑事司法體系人員應加強教育，以認識網路跟騷之類型及其嚴重性，包括離線與線上跟騷之間的密切關聯性。

（二）加強教育訓練（Training and education）

執法機關應就網路跟騷問題之本質及程度（nature and extent）加強教育訓練，包括可用於解決該問題的法律工具（Legal tools）、執法機關迅速採取行動之有效性及必要性、調查及起訴該犯罪最有效之技術、跟騷被害人可運用的資源等。透過適當的培訓及指導，執法調查人員通常可以準確地追蹤到網路跟騷行為人留下的電子痕跡，回溯至最初的起點（initial point of origin）。

（三）將網路跟騷防制納入執法任務（Including cyberstalking as unit's mission）

設有跟騷或網路犯罪部門之執法機關，應考慮擴大該單位之任務，將網路跟騷之防制納入工作範圍；未有該特定單位的執法機關，則應考慮加強其解決該犯罪的能力。

（四）情報共享機制（Information sharing mechanism）

由於跟騷行為的形式非常多樣化，加害人使用各種方法和技巧與被害人互動，使之形成恐懼感。要有效對應跟騷行為，需要跨網絡合作，以社區為導向的方法，相關部門需要共享訊息、合作解決問題（黃翠紋，2019）。跨網絡合作方式可以在資源有限的情況下，讓最合適的提供者做出更快的回應，主要執法機關應與其他執法機關建立機制，以共享及傳送網路跟騷事件的資訊，從而降低行為人繼續威脅被害人之可能性。

（五）加強與專業人員網絡之聯繫與協調（Coordinate with expertise）

檢察機關應與各執法機關會商，檢視可運用的資源，及加強與偵查人員及檢察官共同處理跟騷案件的專家網絡，包括暴力犯罪專家、電腦犯罪偵查人員及檢察

官、電子鑑識專家及被害之證人等。

（六）與被害人團體密切合作（Work closely with the victim group）

執法機構應與被害人團體更密切地合作，以確認網路跟騷模式及被害人經歷，並鼓勵被害人向執法機關報案。

二、網路業者

任何網路跟騷訊息的傳達，均必須透過網路服務提供者（Internet Service Provider, ISP），才能由行為人傳達給被害人，因此在防制措施上，若能課予網路業者一定的責任，將能有效防制網路跟騷行為，相關具體作法如下。

（一）提升社群網路的責任（Increase responsibility of social media sites）

負責建立、維護、監管及實施社交媒體網站的組織，應負起一定之企業社會責任（Corporate social responsibility），承擔起確保其網站安全之共同義務，努力制定企業社會責任政策，以防止網路跟騷事件（Dhillon et al., 2016）。

（二）建立業者支援網站（Creation of industry-support website）

建立業者支援網站，並將以下資訊置於該網站上，包括網路跟騷資訊、遭遇該問題時應採取之措施、主要ISP的聯繫資訊、客戶投訴電子專用信箱，以利網路用戶在該資源集中的網站上即能簡易聯絡業者，並報告其所遭遇的網路跟騷案件。

（三）開發並授權使用者得以運用於保護自身安全的網路選項（Empower individuals to protect themselves）

提高用戶管控個人資訊的能力，使其知悉其個人資訊如何在網路上被共享、儲存及轉傳。網路業者應開發額外的方法，使個人能夠保護自己，以免受到網路跟騷。例如，使用上更方便且有效的過濾及攔阻選項（Filtering and blocking options），包括業者就網路聊天室提供使用者自行封鎖（Block）、抑制（Squelch）或忽略（Ignore）等功能，以回應訊息或他人的呼叫（Paging），避免受到網路干擾或威脅。若用戶選擇於社交媒體網站分享資訊，業者應增加隱私設定或私人網路瀏覽方法等工具，以保護用戶安全地分享資訊（Safe information sharing）（Dhillon et al., 2016）。

（四）與執法機關充分配合（Cooperate fully with law enforcement）

業者與執法機關有共同之目標，即消除線上騷擾，因此，業者於執法機關調查網路跟騷投訴案件時，應與執法機關充分合作，例如，立即凍結及保存資料，以供執法機關調查任何潛在的網路跟騷案件中得以使用。

（五）建立最佳商業實踐（Establish best business practices）

建立最佳商業實踐，終止持有人之詐欺帳戶，以解決非法活動。業者應贊助由ISP所組成之網路安全與執法委員會，以及其他網路社群成員，發展並促進與安全及執法議題相關（包括網路跟騷）的業者最佳商業實踐（Industry best business practices），建立並發送資料給負責調查、起訴網路犯罪的執法機關，促進業者與執法機關之間更有效的溝通及合作，共同打擊網路犯罪。

（六）建立並執行明確的網站使用規範（Establish and enforce clear policies of using website）

業者應建立明確的網站使用政策或線上使用條款（服務協議）中，明確規定禁止濫用或利用其網路服務實施跟騷及相關行為，違者將終止帳戶之使用。

（七）建立明確簡單的投訴程序（Establish clear and understandable procedures of complaint）

業者應建立明確且易於理解的投訴程序，於客戶或非客戶使用其公司服務而有網路跟騷的情形發生時，能簡便地反應給業者。

（八）加強教育民眾網路保護機制（Educate customers how to protect themselves online）

建立並廣泛發送教育資料給客戶或其他人，教導他們網路保護觀念及措施，尤其是兒童及少年。相關調查指出，當父母試圖管理孩子使用網路時，由於雙方間意見分歧，大多數孩子不希望受到父母的限制，會採取一些措施向父母隱藏其線上活動，因此，欲達成監控兒童線上活動及行為，存有相當難度，建議可嘗試將兒童及少年引導至有價值的內容，或是與年輕人開發線上諮詢資源（Livingstone & Bober, 2005）。

三、立法機關

在立法機關方面，根據相關資料顯示，應該要發揮其立法的功能性，將以下作為納入立法考量，進一步具體說明如下。

（一）檢視相關法規範是否已將網路跟騷行為列入管制

運用懲罰之方式，增加對行為人之威懾力（Deterrence），能有效阻止行為人參與網路跟騷犯罪。為達到促使人民遵從法律及阻止犯罪之目的，社區應該採取提高犯罪代價的政策，以明確的法律及更嚴格執法，防制網路跟騷事件（Dhillon et al., 2016）。

主管部門應檢視現行相關法律是否足以規制透過網路及其他電子通信進行之跟蹤騷擾行為。當今社會技術的快速發展，立法者應採取漸進的方法來定義電子通信設備和傳輸系統（D'Ovidio & Doyle, 2003），並應隨時進行法律評估，以確保科技技術在法律管制之列，並應及時因應快速發展的技術，適時修改或制定法律。

（二）跨國或跨境網路跟騷應納入法規範

為避免管轄權之漏洞，政府應將跨國或跨境網路跟騷行為納入規範，亦即法律亦應禁止跨國或跨境傳送任何意圖威脅或騷擾他人的訊息，若此類通訊造成一般合理之人擔心其被殺害或人身傷害。另被害人如係未成年人，行為人則應加重處罰之。

四、被害人協助組織（Victim service providers and advocates）

為正確且有效地提供相關服務及資源予網路跟騷之被害人，被害人協助組織得採取以下具體作為。

（一）提供直接服務或轉介可用資源（Provide direct services and referrals to available resources）

提供直接服務給被害人及轉介專為協助網路跟騷所設計的可用資源給被害人，被害人協助組織應努力確保並擴展網路跟騷服務，以符被害人之需求，周全其人身安全之保護。

（二）加強被害人服務組織之教育訓練（Train victims providers）

加強家庭暴力及其他被害服務組織有關網路科技、網路跟騷行為人所運用之技術等知識的教育訓練，以及教導應如何回應網路跟騷被害人的特定需求。

（三）協助被害人確認網路跟騷行為（Name behavior as cyberstalking and validate the crime）

與個別被害人工作時，協助確認其所遭受之經歷係屬網路跟騷行為，並確認犯罪正發生。

（四）致力與其他社區盟友建立夥伴關係（Efforts to form partnerships among community allies）

作為社區盟友間之催化劑，致力於執法、檢察、司法、醫學界及其他社區盟友之間建立夥伴關係，以達到網路跟騷被害者的特定安全需求，並使犯罪者為其行為負責。

（五）提高公眾對網路跟騷之認識（Raise public awareness on cyberstalking）

網路用戶在登錄社交網站時，應謹

慎發布資訊。使用者（被害人）無意中張貼的訊息，均可能被用來追蹤其本人或是家人的行蹤，網路安全意識的提升，已成為各個社會中不容忽視的課題之一（吳聖琪，2016）。公、私部門均應共同加強教育社會大眾，使其認識網路跟騷對被害人及社會所造成之傷害與負面效應，以及得以採取哪些措施加以防制。

五、被害人

網路跟騷被害人於事件發生前、後，亦得採取相關作為，以減少被害的可能性、降低所受損害或是協助司法機關提高緝獲加害人的機會，以下分述之。

（一）網路使用安全觀念

為避免成為被害者，應選擇性別和年齡不明確的帳戶名稱，不在線上發布個人資訊、不共享密碼，並下載反間諜軟體等，這些都可以減少成為受害者的可能性（Petrocelli, 2005）。此外，網路貼文應盡量減少酸民言論（Minimize trolling），以避免引起他人反感、進而騷擾之。減少被追蹤之可能性，確保使用位置不會被所不希望的人所知悉（Dhillon et al., 2016）。

（二）減少被害的機會

例如，自行購買軟體並安裝以阻止、過濾或忽略不受歡迎的電子通信。使用網路時，於安全瀏覽模式下進行（註3）、留意線上言行，避免引發他人侵犯性的行為，亦可減少成為網路跟騷被害人的機會。另外，如欲與在網上認識的人會面時，應格外小心，儘量選擇公共場所，並應有朋友一同前往，不可單獨行事。

（三）加強對網路跟騷之認識

相關研究指出，被害人可能不會尋求幫助，因為其認為某些被跟騷的行為不夠嚴重，無法向執法機關報案，或是認為警方不會認真對待此事（U. S. Department of Justice, 1999），因此跟騷事件有被低估的可能性。此外，由於各種原因，例如，不知道其所遭受的行為是非法的、害怕被指責、害怕行為人可能會轉向其家人和朋友進行騷擾、行為人的威脅以及認為對事件無能為力等（MacKenzie & James, 2011），故被害人未向警方報案，因此應加強大眾對網路跟騷行為之認識、造成的影響及得採取之防制作為。

（四）保全證據，並協助調查

被害人應通知行為人其通信是不必要的，而且不受歡迎的，要求其應立即停止。另為協助調查，被害人應記錄來自行為人任何電子郵件、電話和信件等通信證據，這些證據必須是未被更改及未被編輯過的，並主動聯繫執法機關或被害人協助單位。另為避免再次被害，應更改電子郵件地址及電話號碼。

（五）聯繫網路服務業者

主動聯繫網路服務業者，告知其遭受網路跟騷，使業者能依據線上協議，就違反者終止提供服務。

（六）諮詢被害者服務團體

諮詢被害者服務團體，尋求有關協助、支持及建議。

伍、結論與建議

綜合前揭論述，本文提出以下四項結論與建議，提供相關機關（構）於立（修）法與執行面之參考，或作為個人於生活面之建議，分述如下。

一、數位性別暴力隨著資通訊技術發展呈現多樣化，主管機關應確保各種科技技術在法律管制範圍內

本文綜合學理及實際已發生類型，認為數位性別暴力之主要要素如下：（一）行為對象：針對性別為之，尤其是婦女；（二）媒介：透過網路及數位技術，包括各種電子裝置（手機、平板、電腦）、網路、社群平臺、電子郵件等；（三）行為類型：人肉搜索、性勒索、網路跟蹤騷擾、未經同意散布性私密影像及人口販運等；（四）人權侵害及造成影響：侵害他人隱私權（性隱私權）、人格權及名譽權等權利，並造成他人身體、心理或性之傷害、痛苦、施加威脅、壓制和剝奪其他行動自由，而影響其經濟生活、人際關係受阻、公共參與意願降低以及獲取資通訊技術之不平等。

由於網路科技發展日新月異，甚至一日千里，各種數位技術手法不斷推陳出新，加上網路社群生態變幻莫測，以致於數位性別暴力之意涵或態樣亦呈現多樣化。為有效防制數位性別暴力，相關政府機關應採取漸進式的方法加以定義網路及數位技術，而且應隨時進行法律評估，以確保科技技術在法律管制的範圍內，並且應及時因應快速發展的技術，適時修改法律（張維容，2021）。

二、交互運用被害人網路跟蹤騷擾回應模式，能提升防制效果

依據研究，被害反應的模式與其所經歷的行為類型有關，在七種策略模式中，以忽略／迴避、主動技術分離及尋求幫助最為常見，但若以有效程度，依序為：技術隱私維護、主動技術分離及忽略／迴避。

本文認為，由於網路跟騷必須透過手機簡訊、電子郵件及網際網路等電子通訊系統，對特定人進行騷擾及威脅的行為，一般人遭遇此情況，消極地忽略或迴避，是當下立即的反應策略，惟若被害人具備一定的電腦網路知識，則應主動積極地運

用技術分離及技術隱私維護之策略，以因應更具威脅性或更嚴重性的行為，惟有各種模式交互運用，才能達到最佳的防制成效，歸納以下之具體作為供參：（一）刪除舊帳號，建立新帳號；（二）刪除／拒絕追隨者成為好友；（三）將資訊設為私密，只有接受的「朋友」才能瀏覽；（四）封鎖追隨者的訊息；（五）更改個人資料：帳戶頭像、更改用戶名、密碼、電子郵件地址；（六）下載防毒軟體。被害人若能熟悉這些網路電腦知識，善用網站平臺功能、提升用戶隱私設定及安裝必要的防毒軟體，以達到忽略或迴避行為人干擾之目的。

三、社會相關主體有責共同介入及預防網路跟蹤騷擾

針對網路跟騷之防制作為，Pittaro（2007）之研究中，將法律干預及其他主體之防制作為，包括業者、被害人協助組織、執法機關及被害人本身，統稱為社會介入及預防（Societal intervention and prevention）。

此外，由於跟騷行為之成因相當多元，除因愛戀、恨意外，也可能是病態或精神方面的問題，如僅以警察機關之公權力介入，恐怕僅能治標、而無法治本。有關跟騷加害人後續處遇與教育及被害人相關援助服務等，必須整合衛生醫療、勞政、社政及教育等機關之力量及專業，才能共同防制（張維容，2020）。

再者，無論組織和個人，均應善盡線上社會責任（Online social responsibility），兩者在防止網路跟騷方面具有重大利害關係，組織及個人應遵循基本行為規範，主動承擔責任，使線上經驗具有積極性（Dhillon et al., 2016）。另外，課責或問責制度（Accountability）可以保護公眾健康及安全、促進執法及加強國家安全。每個人或每個部門，包括私人業者、公共行政人員及司法體系每一環節，都有責任採取相應的措施以防制網路跟騷。

四、持續加強情感教育及正確使用網路觀念

許多跟騷事件之產生，源自於情感關係（包含愛情、友情及親情）之過與不及，因此加強公民情感教育，將能幫助個人澄清對於情感的需求，建立良好的情感態度，並學習在面對挫折與衝突時，如何判斷、如何處理、如何作決定，以及如何從不同角度來思考問題的因應作法，提升問題解決能力，同時幫助個人在面對問題時可以調適自己、紓解壓力與情緒。此外，心理健康與否，會對一個人在網路上正確行事的能力及判斷力產生不利影響。一項針對371名英國學生的調查研究表明，18.3%的樣本被認為是病態的網路用戶，由於其過度使用網路而產生學業、社交和人際關係方面的問題。因此，人們

認為網路使用、網路跟騷及心理健康是相互關聯且值得關注的重要領域（Dhillon et al., 2016）。為建立正確使用網路觀念，網路使用者除了具備上網能力外，如何在網路上保障自己和他人的安全，建立健康、合理與合法的資訊科技使用態度與習慣，已然是當代每位公民應擁有的基本素養。

陸、結語

筆者曾於警察實務機關工作將近20年，期間曾承辦各項婦幼保護業務及擔任家庭暴力防治官，深覺人身安全之保護，「預防勝於治療」為其重點所在。亦即，如何在事件尚未發生前或未惡化前，即建立被害人預防被害之意識與觀念，並教導其各種防制作為與因應措施，才能保護個人身心安全、行動自由、生活私密領域及資訊隱私，免於受到網路跟蹤騷擾行為之侵擾並維護個人人格尊嚴（參照《跟騷法》〔2021〕第一條）。因此，在網路時代下，持續整合並精進公、私部門所建構起之防制網絡，且務必使每個環節善盡職責，才能真正落實被害人保護之精神，並有效防止數位性別暴力之發生。

（本文作者為中央警察大學外事警察學系副教授兼系主任）

關鍵詞：數位性別暴力、網路跟蹤騷擾、網路犯罪、資通訊、未經同意散布性私密影像

註　釋

註1：俗稱「復仇式色情」的「未經同意散布性私密影像」，指的是「沒有經過當事人同意，而故意散布、播送、張貼或以任何方式讓第三人觀覽當事人為性交、裸露性器官等性私密之照片、影像，或以這些性私密影像作為威脅」（張凱強，2016）。

註2：定義中介盡量減少網路跟騷（Defining intermediaries to minimize cyberstalking）之目的，某種程度上與確保安全程序之基本目標有關。亦即，業者購買網路責任保險（也稱為網路安全保險）以降低網路威脅所造成的財務損失。

註3：Safe Browsing會提供瀏覽器以及網路服務商一系列含有惡意軟體或網絡釣魚內容的網址（URL），當用戶將進入之網頁可能含有惡意內容時，就會看到畫面彈出的警告提示，代表可能有網絡釣魚或惡意軟體出現，接著就會被Chrome、Firefox、Safari這些瀏覽器阻擋下來（高敬原，2017）。

參考文獻

《消除對婦女一切形式歧視公約》（1979）。https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=Y0000042

《跟蹤騷擾防制法》（2021）。https://law.moj.gov.tw/LawClass/LawHistory.aspx?pcode=D0080211

內政部警政署公共關係室（2023年6月1日）。〈跟蹤騷擾防制法施行周年初見成效 超過8成跟蹤騷擾行為經告誡未再犯〉。中華民國內政部警政署全球資訊網。https://www.npa.gov.tw/ch/app/news/view?module=headnews&id=2136&serno=14739de7-5f68-4cc6-ae33-e39a48644ff5

王伊軒（2020）。〈國際人權視角：新興數位性別暴力與防制〉。《國際性別通訊》，32，11-12。

行政院性別平等處（2020）。〈CEDAW第1號至第38號一般性建議（中文繁體版）〉。行政院性別平等會。https://gec.ey.gov.tw/Page/D704A5B282D840C7/b99bc3b0-800b-4cc5-b3c9-d9b6516bb3ee

行政院性別平等處（2021a）。〈從109年度性別平等議題熱門新聞關鍵字談數位性別暴力〉。性別平等觀測站。https://geo.ey.gov.tw/article?id=8a8a8a22795f4e84017963e1db900019

行政院性別平等處（2021b）。〈數位／網路性別暴力之定義、類型及其內涵說明〉。行政院性別平等會。https://gec.ey.gov.tw/Page/ED8994F4EF5AD73E/2ab74b7e-0bdb-4067-b43a-4a3cfc9e2a1e

行政院性別平等處（2023）。《2023年性別圖像》。https://gec.ey.gov.tw/File/5FCD049ED9E27FDD

吳聖琪（2016）。《臺灣跟蹤騷擾防制法制之實證研究》（博士論文，國立中正大學）。臺灣博碩士論文加值系統。https://hdl.handle.net/11296/y4vw8b

高敬原（2017年9月15日）。〈網頁跳出的安全警告是哪來的？原來Google這項服務，讓全球30億台裝置可以安心上網！〉。風傳媒。https://www.storm.mg/lifestyle/331054

張凱強（2016）。〈論復仇式色情這當代厭女文化下的網路獵巫行動〉。《婦研縱橫》，105，16-21。https://doi.org/10.6256/FWGS.2016.105.16

張維容（2020）。〈我國跟蹤騷擾防制法草案之研究〉。《警學叢刊》，51（2），77-100。

張維容（2021）。〈論兩岸網路跟蹤騷擾與執法挑戰〉。載於蘇志強（編），《警務生態系統發展新思維研討會論文集》（頁291-310）。中華民國刑事偵防協會。

黃翠紋（2019）。〈警察處理跟蹤騷擾案件原則之研析〉。《警政論叢》，19，17-45。

楊綿傑（2019）。〈婦團調查：24％國人曾遭科技跟監 女性占近8成〉。現代婦女基金會。https://www.38.org.tw/news_detail.asp?mem_auto=443&p_kind=%E7%8F%BE%E4%BB%A3%E6%B6%88%E6%81%AF&p_kind2=%E5%AA%92%E9%AB%94%E5%A0%B1%E5%B0%8E&p_kind3=%E7%84%A1

Catalano, S. (2012). *Stalking victims in the united states-revised*. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://bjs.ojp.gov/content/pub/pdf/svus_rev.pdf

Cyber Civil Rights Initiative. (n.d.). *End revenge porn: A campaign of the cyber civil rights initiative, Inc*. https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf

D'Ovidio, R. M. S., & Doyle, J. (2003). Study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, *72*(3), 10-17.

Dhillon, G., Challa, C., & Smith, K. (2016). Defining objectives for preventing cyberstalking. In J. H. Hoepman & S. Katzenbeisser (Eds.), *ICT systems security and privacy protection* (pp. 76-87). Springer. https://doi.org/10.1007/978-3-319-33630-5_6

Livingstone, S., & Bober, M. (2005). *UK children go online: Final report of key project findings*. London School of Economics and Political Science. http://eprints.lse.ac.uk/399/1/UKCGO_Final_report.pdf

MacKenzie, R. D., & James, D. V. (2011). Management and treatment of stalkers: Problems, options, and solutions. *Behavioral Sciences & the Law*, *29*(2), 220-239. https://doi.org/10.1002/bsl.980

Petrocelli, J. (2005). Cyber stalking. *Law & Order*, *53*(12), 56-58.

Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, *1*(2), 180-197. https://doi.org/10.5281/zenodo.18794

Smith, S. G., Zhang, X., Basile, K. C., Merrick, M. T., Wang, J., Kresnow, M., & Chen, J. (2018). *The national intimate partner and sexual violence survey: 2015 data brief – Updated release.* National Center for Injury Prevention and Control, Centers for Disease Control and Prevention. https://www.cdc.gov/violenceprevention/pdf/2015data-brief508.pdf

Tokunaga, R. S., & Aune, K. S. (2017). Cyber-defense: A taxonomy of tactics for managing cyberstalking. *Journal of Interpersonal Violence*, *32*(10), 1451-1475. https://doi.org/10.1177/0886260515589564

U. S. Department of Justice. (1999). *Cyberstalking: A new challenge for law enforcement and industry: A report from the attorney general to the vice president*.

U. S. Department of Justice. (2005). *Prosecutors in state courts*. https://bjs.ojp.gov/redirect-legacy/content/pub/pdf/psc05.pdf

United Nations. (2018). *Report of the special rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*. United Nations Digital Library. https://digitallibrary.un.org/record/1641160