新興法律問題學術研討會（第一場）
數位證據之取證及證據能力

■ 林育賢 *

▪▪▪目次▪▪▪

壹、前言

刑事偵查的數位化，早在人類步入網路時代後，已是不可逆的過程，隨著人類活動軌跡涉入網路世界，變更原先社交、行動模式，另外個人活動軌跡也透過資料形式儲存或暫存於終端設備或個人電腦當中，數位證據（digital evidence），其意義隨著人類社會活動高度仰賴網路世界而更形重要，這不單只侷限於傳統國家透過刑事程序干預個人生活領域的視角切入，或侷限於電腦

* 現職為臺灣花蓮地方法院法官—投稿時為司法官班第 59 期學員。臺灣大學法律研究所碩士、臺灣大學法律研究所博士生。感謝劉建志檢察官、與會 59 期學習司法官及與談人王士帆教授的提問、指教及修改意見，惟文責仍由筆者自負。

網路的犯罪，進而衍生對於證據取得、評價的基本議題，更關切到國家在這一過程中所產生的社會控制與監控手段的擴張，從而影響並參與網路時代形塑公民生活方式。固然這已經不是嶄新的議題，但隨著科技技術發展上快速變遷，法律系統調控能力應對高度複雜化的現狀，在自我變遷上顯有不足，目前所有國內文獻均係以此一前提意識下展開論述[1]。

以下將從三個角度來分析這一問題，首先，以下先從數位證據的概念範圍進行界定（貳、），接著，由於數位證據以不同形式存儲在電子載體或網路空間，因而衍生取證手段的差異，由此也衍生不同層次的基本權干預問題，基此，藉以區別討論取證形式的合法性（參、），並論及由此取證形式衍生的證據評價（肆、）。在上述討論中，會一併將近期法務部公告《科技偵查法》列為檢討範圍[2]。

貳、數位證據之定義

一、定義

數位證據，文獻將之定義為透過電腦或相似裝置儲存、傳輸，用以認定（或否證）被訴犯罪存在的資料，這些資料是透過二元方式儲存，亦即 0 即 1[3]，並透過電腦設備轉換成人類可以理解的內容，包含文字檔、圖像檔、音檔或影像檔[4]，不過，即便是屬性檔案（metadata），可以顯示資料何時或如何遭到更動修改[5]，亦有可能有證明待證事實存在的效果。依照羅卡定律，凡兩個物體接觸，必會產生轉移現象，

1 國內關於網路偵查及取證等相關先行研究，參見王銘勇（2003），網路犯罪之搜索與扣押，法學叢刊，191 期，頁 45-62；法思齊（2011），美國法上數位證據之取得與保存，東吳法律學報，22 卷 3 期，頁 95-147；何賴傑（2012），論德國刑事程序「線上搜索」與涉及電子郵件之強制處分，月旦法學雜誌，208 期，頁 230-244；吳秋宏（2012），照相錄影與刑事程序，臺北：承法；劉芳伶（2015），論「對情報扣押」之可能性－一個法益論的新展開，刑事法雜誌，59 卷 3 期，頁 99-126；施育傑（2017），數位證據的載體、雲端與線上取證－搜索扣押與類型化的觀點，月旦裁判時報，64 期，頁 55-71；李榮耕（2018），初探遠端電腦搜索，東吳法律學報，29 卷 3 期，頁 49-87；王士帆（2017），網路之刑事追訴－科技與法律的較勁，政大法學評論，145 期，頁 339-390；王士帆（2019），當科技偵查駭入語音助理——刑事訴訟準備好了嗎？，臺北大學法學論叢，112 期，頁 191-242。

2 本次科技偵查法草案涵蓋眾多科技偵查手法，本文以下無法一一敘及，僅能擇其要而論述，其餘部分有待日後另外為文說明。

3 Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 538（2005）.

4 Casey, in, Casey el.（ed.）, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 7（2011）.

5 Kerr, *supra* note 3, at 542.

數位證據形成過程雖然並未經過實體物理空間中的活動交換或殘留生物跡證，同樣的觀點一樣可以演繹至數位證據的形成：只要是利用 IT 系統變更資料，無可避免仍會留下數位蹤跡，即便並未複製資料，仍有可能留下使用者的資訊[6]。例如 A 以電子郵件寄信給 B 恐嚇、A 透過 FaceTime 來聯絡共犯，同時手機 GPS 定位系統留下 A 在犯罪現場的位置資訊，準備押 B 取款，上述兩個事例都有電腦設備或網路作為中介，甚且連結進一步與衛星系統產生定位資訊，藉此留下足以證明 A 犯罪（恐嚇信、犯罪計畫或在場證明）的證據[7]，而數位資料所得勾勒的人際社會網絡[8]，往往也成為犯罪偵查的著力點。基於上述理解，如何取得數位證據，仰賴對使用者資料存取、變更、傳輸等資訊傳輸與使用方式的釐清。

二、數位資料的產生及傳輸途徑

進一步來說，數位資料的產生，粗略可以區分成（1）資料產生方式、（2）資料狀態來架構可能的干預模式。資料產生方式，如是否在①通訊中產生，例如發送電子郵件即屬之，反之，在電腦中製作帳冊或者撰寫日記，並且上傳到雲端硬碟，並無他人參與通訊或跟他人溝通的特徵，因此無法歸屬於通訊所產生的資料。其次，②是否為人的陳述內容也是區別方式[9]，例如電腦儲存紀錄（computer-stored records），可能是通訊內容，因涉及人基於自我思想所為陳述及表達，但通訊過程中附隨產生的資訊如通聯紀錄，則並未涉及人的特定思想表達，如電腦產生紀錄（computer-generated records）[10]。另外，可從③使用者製造或變更資料與否來確認，例如使用者自行拍攝照片即屬此類，相較於此，地方政府裝置於路口的監視器錄影設備所攝得的影像，即不屬此類[11]。資料狀態是另一種思考面向，資料是在傳輸中取得

---

6 Heinson, IT-Forensik: Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen, 2015, S. 21.

7 Casey, *supra* note 4, at 16.

8 Momsen, Zum Umgang mit digitalen Beweismitteln im Strafprozess, in: Ein menschengerechtes Strafrecht als Lebensaufgabe : Festschrift für Werner Beulke zum 70. Geburtstag（2015）, S. 874.

9 李榮耕（2014），刑事審判程序中數位證據的證據能力－以傳聞法則及驗真程序為主，臺北大學法學論叢，91 期，頁 176。

10 李榮耕，同前註 9，頁 176-177。

11 有認為此涉及資訊自主決定權的主體與射程，見劉芳伶，同前註 1，頁 119-121。

或者儲存在特定位置、儲存於個人電腦硬碟、行動攜帶裝置或者第三者所提供儲存空間，如雲端服務提供者所提供的雲端硬碟，即是差異所在。

參、取證方式及合法性

一、基本權干預類型化及適法的干預手段

基於上述理解，刑事偵查上對數位資料的取得，若干不同的蒐證方式，現行法下較無爭議的是搜索、扣押電磁紀錄及透過通訊監察或調取通聯紀錄而取證，然而以下主要檢討現行法存有疑義或尚未授權、授權不足等取證形式。

（一）搜索、扣押

1. 現行法下客體取得界限

刑事訴訟法第 122 條，分別對被告、第三人的電磁紀錄搜索有所規範。傳統的進行方式，是將搜索電磁紀錄的載體並將之扣押，例如現場搜得可能與案件相關的電腦設備、硬碟、光碟或其他儲存裝置等載體，將之扣押後並帶回進行鑑識處理，進行數位鑑識後（關於數位鑑識，則見下述（五）），再將載體儲存的電磁紀錄加以存取、保全，學說又稱為二階段搜索扣押模式[12]，上述流程當中，必須透過占有載體為作為取得數位資料的中介[13]。儘管現行法的文字用語，係以搜索「電磁紀錄」，且扣押「得為證據或得沒收」之物，而非電磁紀錄之載體，不過目前偵查實務，基於後續數位鑑識的必要性，均須藉由這一方式上述二階段搜索扣押模式來達成[14]。

現行法雖然同時規範第三人電磁紀錄搜索、扣押，但當扣得被告占有電磁紀錄載體後，能否透過連線方式存取並取得數位資料？通常會有這種問題，主要是因為偵查機關發現資料已上傳至雲端儲存空間，遇此情形，能否透過被告所使用載體業已登入存取的狀態，從雲端儲存空間將資料下載？學說即有認為，縱使是與空間分離的雲端儲存空間，也在檢閱範圍內[15]，此時被告並未透過載體占有資料，仍可透過被告的資料存取權限加以檢閱、複製，此一情形下，認已上傳的資料屬於現行法所容許的扣押客體[16]，應屬合理的看法。相較

---

[12] 李榮耕（2012），電磁紀錄搜索和扣押，臺大法學論叢，41 卷 3 期，頁 1060。

[13] 施育傑，同前註 1，頁 59。

[14] 李榮耕，同前註 12，頁 1062-1063。

[15] 王士帆（2017），同前註 1，頁 373-375。

[16] 施育傑，同前註 1，頁 62。

於此，當無法透過被告或者第三人所支配的載體直接登入[17]，例如被告拒絕提供解除加密機制，此際已上傳的資料或者過去已結束的通訊紀錄[18]，只能透過第三人搜索、扣押的方式來達成扣押上述資料的目的。不過，對第三人搜索扣押之難題，在於目前雲端服務提供者或者通訊服務提供者，其公司多半設置國外，非我國司法主權所及，無法直接搜索、扣押公司所持載體或資料來達成訴追犯罪之目的，即便能從截獲封包資訊也無法解密，有技術上的難題，此外，現行法下尚涉及到司法權競合的問題[19]。除透過正式司法互助管道解決，只能透過事前與第三國公司協議如何執行搜索、扣押。例如，手機通訊軟體 LINE 有其加密技術的資料封包，在一定時間內保存的通訊內容，如有向 LINE 公司調取所通訊資料的必要，須向經由臺灣高等檢察署提出調取聲請書，與 LINE 公司洽妥時間，並向法院聲請核發搜索票，始得向境外日本 LINE 總公司，持搜索票讓 LINE 公司交付該資料，才能扣得特定時段的通話紀錄。

2. 無載體中介的搜索、扣押？

線上搜索（Online-Durchsuchung），係國家透過以資訊科技侵入私人資訊系統，取得特定資料的一種干預手段[20]，這種不透過電腦等資訊載體作為中介，性質上無法類比通訊監察或一般搜索，一方面，線上搜索客體並非通訊內容，而是針對資料串流，相較於在實體世界的搜索，偵查官員通常無法當下確認搜索對象是否存在於電腦[21]，另一方面，由於採取突襲性的刺探手段，以獲取資料串流，無法如一般搜索保障被告在場權[22]。關於線上搜索所干預的權利，有認為係干預仍為受搜索人的合理隱私期待[23]，亦有強調此係干預擔保資訊系統完整性及可靠性的基本權（Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informations-

---

17 當使用者不願提供，能否直接破解密碼或得共同權限人同意而進入是另一問題，就此相關討論，參見王銘勇，同前註 1，頁 53-54；法思齊，同前註 1，頁 110-114。

18 已結束之通訊內容資料，並不適用通訊監察及保障法，就此可見最高法院 106 年度台非字第 259 號判決。

19 王士帆（2017），同前註 1，頁 375。

20 何賴傑，同前註 1，頁 232；王士帆（2019），同前註 1，頁 196-197。

21 Kerr, *supra* note 3, at 540.

22 王士帆（2017），同前註 1，頁 378-379。

23 李榮耕，同前註 1，頁 60。

technischer Systeme）[24]。另一種近似情形，則是來源端電信監察（Quellen Telekommunikationsüberwachung, Quellen-TKÜ），不過干涉範圍限縮在通訊中電磁紀錄，如將間諜程式裝置在使用者的資訊設備或所攜帶數位裝置中，藉此擷取加密前或加密後的即時通訊內容，解決無法有效應對通訊軟體加密技術的障礙，除高度涉及使用者的資訊安全外，由於是透過間諜程式介入進行中的通訊，如網路電話這種非傳統固網通訊方式，藉以解決資訊封包的加密問題，係具有通訊干涉效果而侵害秘密通訊自由[25]，另外，對於已儲存之電信通訊及資料狀態，亦屬於獲取範圍，但此時則不具有秘密通訊的侵害效果，而近似於線上搜索[26]，故來源端通訊監察又被稱為小線上搜索（kleinen Online-Durchsuchung）。

上述手段均係透過國家藉由私密植入間諜程式，在現行法下並無明確授權依據。首先關於線上搜索，固然學說有主張透過合理隱私期待界定搜索範圍，只要構成隱私權侵害，即屬搜索行為[27]。然而，這一見解顯然不合理，因為搜索在現行法的體系地位中，均無從私密為之，同時現行法也要求賦予被搜索人在場權的保障（刑事訴訟法第148、150條），難以透過合理隱私期待的概念來證成線上搜索為現行搜索規定所允許的一種偵查手段。其次，通訊保障及監察法第3條第1款固然規範「利用電信設備儲存符號、文字、影像、聲音或其他信息之有線及無線電信」，不過通保法的儲存訊息只能涵蓋儲存於中繼端的訊息，這種情形通常是指電子郵件這類準即時性的通訊內容，必須透過帳號登入控管機制，讀取或閱覽中繼端的通訊內容，至於儲存於個人載體的訊息，則不應包含在內[28]，實務見解近期亦支持這一看法[29]，由此可進一步推論，線上搜索所獲取的資料狀態，既然

---

[24] Vgl. Großmann, Zur repressiven Online-Durchsuchung, GA 2018, S. 440f. 中文文獻亦有略稱為「IT基本權」（王士帆，同前註1，頁346）或「資安基本權」（施育傑（2019），「資安基本權」之研究－以「線上搜索」為核心，世新法學，12卷2號，頁355），下文均略稱資安基本權。

[25] 王士帆（2019），同前註1，頁224；施育傑，同前註24，頁351-352。

[26] 王士帆（2019），同前註1，頁228-229。

[27] 王兆鵬（2003），重新定義高科技時代下的搜索，月旦法學雜誌，93期，頁179-182；李榮耕，同前註12，頁1067；李榮耕，同前註1，頁61。

[28] 許恒達（2010），通訊隱私與刑法規制—論「通訊保障及監察法」的刑事責任，東吳法律學報，21卷3期，頁133。

[29] 最高法院106年度台非字第259號判決：「通保法所規範之通訊監察，重在過程，應限於「現時或未來發生」之通訊內容，不包含「過去已結束」之通訊內容，偵查機關如欲取得「過去已結束」之通訊內容，應回歸適用刑事訴訟法，依刑事訴訟法搜索扣押相關規定為之。」

並非處於類似通訊的狀態，也不在通保法範圍，並非立法者所授權干預的基本權範圍。

至於來源端電信監察，其手段除干預資訊自主權及隱私外，同時伴隨對資訊安全系統的干擾效果，有必要檢討其干預對象為何？德國學說基本上認為來源端電信監察同時干預彼邦秘密通訊自由及一般人格權所推導出的資安基本權[30]。目前我國學說對於資安基本權，憲法第 22 條可以導出資安基本權，其保障範圍係以處理資訊科技系統的機密性、完整性及可用性，藉此保障人格權及資訊自主權的提前、無漏洞保護[31]，就此來看，通保法第 13 條第 1 項雖然規定：「以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法」作為通訊監察的手段，不過，對於有加密措施的通訊內容，現行法所列舉的手段，均無從擔保資訊安全，其他必要方法也難以涵蓋使用間諜程式等有高度資安疑慮的方式，顯然不足作為授權依據。

日前科技偵查法草案於第 3 章設有來源端通訊監察之偵查方式，並名之為「設備端通訊監察」，主要規範緣由便是針對上述網路電話或通訊軟體視訊等通信內容進行通訊監察而設（參見草案第 3 章立法理由），由草案第 14 條至第 16 條觀之，大部分的規定均係準用通保法，並適用法官保留原則[32]，同時第 17 條強調應確保使用上的資訊系統安全[33]。

（二）科技定位監控設備

科技定位設備有至今相當可觀的發展，目前實務常見的是全球衛星定位系　統（Global Positioning System），又稱為 GPS 定位，其機制是透過三維空間資訊而測量並計算所定位的地方，並回傳位置資訊，當偵查機關透過這

---

30 Bantlin, Grundrechtsschutz bei Telekommunikationsüberwachung und Online-Durchsuchung, JuS 2019, S. 669f

31 施育傑，同前註 24，頁 395-396。

32 草案第 14 條第 2 3 項:「(第 2 項)前項情形 , 應由檢察官或由司法警察官報請檢察官同意後，以書面聲請該管法院核發設備端通訊監察書。(第 3 項) 有事實足認被告或犯罪嫌疑人涉有通訊保障及監察法第六條第一項所列罪嫌，為防止他人生命、身體、財產之急迫危險；或有事實足認有其他通訊作為第一項所列罪嫌之連絡而情形急迫者，得由檢察官或司法警察官報請檢察官許可後，通知執行機關先予實施設備端通訊監察，並於二十四小時內，由檢察官或由司法警察官報請檢察官同意後，聲請該管法院核發設備端通訊監察書。」

33 實施設備端通訊監察，應依相關科技 , 於技術可達成之範圍內，確保下列事項：一、不得監察或取得通訊以外之資訊。二、對受監察人之資訊系統或設備僅進行為取得監察資料所必須之變更。三、監察結束時，曾進行之變更應即時回復，曾植入之軟體應即時除。四、所採用之監察方法應防止第三人利用而入侵受監察人所使用之資訊系統或設備。

一方式取得被告的位置資訊，是否於現行法下受到允許？多數見解均持反對看法，由於 GPS 定位系統對於被告資訊自主權及隱私權干預不亞於其他強制處分措施，此一干預侵害不因被告身處公共場域而欠缺對於資訊自主及隱私的侵害[34]，且現行刑事訴訟法並無任何授權依據，刑事訴訟法第 228 條、第 230 條、第 231 條等規定，或認為只能授權司法警察進行較低度基本權的干預措施[35]，或認為僅為任務分配規定，並無任何干預基本權的授權[36]，通保法雖然同樣涵蓋合理隱私期待的保護，不過 GPS 定位位置資料無涉於任何人際意思內容交換[37]，自非立法者所授權干預的通訊隱私，同時 GPS 定位資訊，也與通訊附隨產生的通信紀錄或使用者資料無涉[38]，此外，警察職權行使法也僅止於授權危險預防，而不及於犯罪偵查[39]，最高法院 106 年度台上字第 3788 號判決亦同此見解。另有認為，現行法下可以類推適用搜索規定，由法院核發令狀進行 GPS 定位[40]，不過這一前提也值得商榷，理由在於，搜索規定於現行法下必須於受搜索人、物以保全被告或者保全犯罪證據，但 GPS 定位技術係透過將定位位置資料回傳到偵查人員手中的接受器，並且透過將這些資料建構出行動剖繪，干預項目、內涵已經不同於搜索規範所授權，在美國，依照憲法增修條文第 4 條，規範人民有不受不合理搜索扣押之權利（the right ... against unreasonable searches and seizures, shall not be violated），是否要令狀必須出於合理性，這也決定了令狀適用範圍，不過現行法的搜索跟美國法關注合理性與否無關，而美國法在近年對於令狀適用範圍的界定，採取採取

34 陳運財（2016），GPS 監控位置資訊的法定程序，台灣法學雜誌，293 期，頁 73。

35 關於上開條文是否賦予司法警察一般調查權限的討論，參見林鈺雄（2007），干預保留與門檻理論 ——司法警察（官）一般調查權限，政大法學評論 96 期，頁 214-216；薛智仁（2014），司法警察之偵查概括條款？－評最高法院一〇二年度台上字第三五二二號判決，月旦法學雜誌，235 期，頁 241-254。

36 薛智仁（2018），刑事程序法定原則，月旦刑事法評論，11 期，頁 28-29。

37 關於通訊之定義，參見許恒達，同前註 28，頁 119-120。

38 李榮耕（2015），科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展，臺大法學論叢，44 卷 3 期，頁 932-935；范耕維（2019），現行法下 GPS 追蹤定位偵查行為之合法性與立法方向——比較法觀點與最高法院 106 年度臺上字第 3788 號判決之考察，政大法學評論，157 期，頁 181。

39 李榮耕，同前註 38，頁 935-937；范耕維，同前註 38，頁 179。

40 吳燦（2020），科技偵查蒐證之授權依據及證據能力——以警察裝置 GPS 偵查為例，檢察新論，27 期，頁 162-164。

合理隱私期待作為上位標準[41]，然而觀諸現行搜索規定，則非如此，合理隱私期待概念既非現行法事前取得令狀之前提，遑論主張有合理隱私期待干預，繼而推論搜索令狀有適用餘地，縱使出現高度的犯罪偵查需求，亦難以為這一偵查手法開法律保留原則的後門而容許通關。再者，GPS 定位追蹤干預內容，尚且包含對於受偵查者資訊自主權的干預，由此亦無法與現行法的搜索相互類比，也欠缺類推適用的基礎。

另一種較為折衷的看法是依照 GPS 設置時間的長短來決定是否構成強制處分。其中一種支持看法源自於強制處分的區分問題，該說源自於任意偵查與強制處分的二元區分，認為被定位者在公共場所內短時間的裝設，其資訊總量不多，並未達到實質侵害隱私，未達強制處分的程度，僅為任意偵查，而長時間的裝置則已到達強制處分之程度，因此，GPS 定位是否構成強制處分，取決於時間因素及場所因素[42]。這組區分於日本法，是來自彼邦刑事訴訟法第 197 條規定「偵查，得為達其目的而為必要之調查。但強制處分如無法律特別規定者，不得為之。」由是區分出任意偵查及強制處分，向來日本即有有形力施用為強制處分與否之認定，則有意思壓制說或個人權利或法益侵害說[43]，而認定是否為強制處分的依據，不過，強制處分與否的界限，在於國家能否干預被告或第三人基本權或私人領域而取得證據[44]，如已干預則應有授權規範，欠缺授權規範則不得為之[45]。科技偵查法草案第 5 條目前區分時間長短來界定檢察官保留及法官保留的範圍[46]，固非不妥[47]，但鎖定期間依照第 3 項，檢察官保留可長達 2 個月，如繼續實施始須

41 李榮耕，同前註 38，頁 884-886。

42 陳運財，同前註 34，頁 68。

43 相關討論，參見井上正仁（2014），強制捜査と任意捜査，頁 4、10-11。

44 井上正仁，同前註 43，頁 28-29。

45 如果用重要基本權來理解強制處分在我國法上的地位，恐怕會與大法官過往對於法律保留原則概念的闡釋相互衝突，因此，在我國行政、立法均享有獨自的民主正當性，而非源自於國會的議會內閣制，行政權基本權干預的授權密度，仍要仰仗立法者的形成，或許才是問題所在。

46 第 5 條：「（第 1 項）偵查中檢察官認有必要時，得使用全球定位系統或其他具有追蹤位置功能之科技設備或技術實施調查。（第 2 項）檢察事務官、司法警察官或司法警察因調查犯罪情形及蒐集證據，必要時得報請檢察官許可後，實施前項調查。（第 3 項）檢察官、檢察事務官、司法警察官或司法警察實施前二項調查之累計期間，不得逾二個月。有繼續實施之必要者，至遲應於期間屆滿之五日前，以書面記載具體理由，由檢察官或由司法警察官報請檢察官同意後，聲請該管法院許可。」

47 對於此種容許短期監控為程序例外的立法模式疑慮，已見於李榮耕，同前註 38，頁 958。

得法院同意，如此立法模式，恐怕對於隱私權的侵害干預程度過高，且欠缺事前監督機制介入，GPS 定位的運用，亦非所有情況均係遲延危險（且如有遲延危險，檢察事務官、司法警察官、司法警察依草案第 7 條，可逕行實施），上述做法實值商榷[48]。

科技定位技術近期浮現的問題是 M 化車的使用。M 化車為 M 化偵查網路行動電話定位系統簡稱，M 化車如同虛擬基地台，偵查人員首先確認目標對象的 IMSI（SIM 卡識別碼）、IMEI（手機序號），以及目標即時位置之基地台地址及編號（Cell ID），並確認目標是否開機，藉 M 化車與目標設備之間的訊號連結，進而定位目標設備，藉此定位所欲偵查之對象。由上述作用機制可知，M 化車除了能確認通聯對象外，尚能針對目標裝置訊號強弱而產生即時定位效果，對於個人資訊自主權的干預及隱私權干預非輕。桃園地方法院一則具指標性的判決，強調上述即時定位效果，亦未向電信業者調取通聯紀錄，顯非通訊法第 11 條之 1 所授權的範圍，故牴觸偵查法定原則[49]。首先，上述定位資訊內容，並非通保法第 3 條所謂的通訊，因為並非有人類意思傳達，所蒐集的資訊僅為位置資訊，並無干涉使用者的秘密通訊自由，因此與通訊監察的規定不合。其次，依照通保法第 3 條之 1 之通信紀錄，固然包含行動電話基地台位置資訊（CSLI）[50]，但

---

48 另一種支持 2 分式的看法則是從令狀原則及 GPS 如未採取令狀原則可能的弊害何在，據以推論 GPS 定位追蹤可能帶來的問題在於資料分析跟使用階段要有更強的監督機制，而非針對短期 GPS 定位均採取令狀原則而失去了 GPS 於偵查技術使用上的便利，參見稻谷龍彥（2017）刑事手続におけるプライバシー保護－熟議による適正手続の実現を目指して－，東京：弘文堂，頁 336-338。

49 桃園地方法院 106 年度易字第 164 號判決。

50 附帶一提，106 年度易字第 164 號判決中，檢察官曾提出 M 化車應類比通信紀錄處理，並且依照美國法上的第三人原則（third party doctrine），應認所取得的定位資訊，是可適法取得的。然而這一論點值得商榷，理由在於：依照美國最高法院過往見解，當事人自願揭露給第三人的資訊內容，並無合理隱私期待可言，因此第三人將資訊內容轉交給國家使用，應自負風險，不過近期美國聯邦最高法院反而認為，如果一概適用第三人原則，將導致任何資訊取得均不受司法事前審查，仍認為有第三人控制持有之資訊，個人具有合理隱私期待，這意味著並非所有資訊轉交給非國家的第三人，均應自我承擔風險，而且當代科技技術服務已經將個人所有可能的資料及科技足跡均涵括於多家或一家公司所持有，倘若毫不保留適用第三人原則，對於個人隱私及資訊自主的保障顯然是過度侵害的選項，顯不足採，就此相關討論，參見溫祖德（2020），調取歷史性行動電話基地台位置資訊之令狀原則——自美國 Carpenter 案之觀察，月旦法學雜誌，297 期，頁 133-135；李榮耕（2020），與談意見（一）：科技偵查法立法之可行性評估及建議方向，檢察新論，27 期，頁 183；深入批評此原則亦請見稻谷龍彥，同前註 48，頁 263-269。其次，M 化車所取得的資訊，既非通信紀錄，亦非使用者所自願提供，因此適用第三人原則之前提顯然也不存在。

偵查人員透過上述機制，行動裝置位置訊號將被截取、接收，並非使用者自願將資訊傳送至電信服務提供者，因此作用機制確實與電信業者所持有的通信紀錄調取不同。德國法上為了擷取類似資訊，在彼邦刑事訴訟法第 100i 條第 1 項的授權下，允許使用國際移動用戶識別碼擷取器（IMSI Catcher），用以掌握行動裝置卡號（Kartennummer）及行動裝置的位置（Standort eines Mobilfunkendgerätes），因此這一定位偵查手法，仍需透過立法者預先授權干預資訊自主權及一般行為自由，始得為之[51]。警職法固然規範運用科技設備進行危險預防，然而考察警職法相關規定，並無授權偵查人員得於個案運用科技刺探被告資訊自主權來進行犯罪偵查，加上干預基本權的程度非輕，顯然不是現行法的適法的取證手段，故上開桃園地院判決見解值得贊同。

（三）監視器照相錄影

實務上最為龐大的數位證據來源，則係源自於各種形式的照相錄影畫面，除直接當場拍照攝影外，另如閉路電視監控系統（Closed-Circuit Television，CCTV），即俗稱監視器，此可分為私人或國家裝置。私人設置監視攝影，如私人所裝設行車紀錄器或者住家設置的防盜監視器，原則上透過扣押錄影紀錄即可，私人並非刑事訴訟法所禁止的取證主體（至於證據能力與否，涉及私人不法取證的議題，見下述肆、二、（二））。相較於此，現行法下的國家裝置監視器或使用科技設備錄影，可分成一般行政目的與預防犯罪目的。目前在現行刑事訴訟法及相關法規，並未授權偵查機關可因「犯罪偵查」而進行監視錄影[52]。不過，除了監視器外，依照警察職權行使法第 10 條，警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，為維護治安之必要時，得協調相關機關（構）裝設監視器，或以現有之攝影或其他科技工具蒐集資料，同時亦授權使用目的及資料保存期限。上述規定除授權裝設監視器，實務上亦常見於執法過程中警員使用密錄器紀錄案發過程，最高法院亦曾認為，類此處理方式，可透過警職法第 10 條第 1 項獲得授權依據[53]，不過「維護治安之必

---

51 Vgl. Beulke/Swoboda, Strafprozessrecht, 14 Aufl., 2018, Rn. 254c.

52 德國法則在刑訴法第 100h 條第 1 項規定，得於當事人住家外採取攝影措施，但限於調查對象為重罪（Straftat von erheblicher Bedeutung）。目前科技偵查法草案第 9 條也有相似的設計。

53 最高法院 99 年度台上字第 4546 號判決：「第十條第一項規定：「警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，為維護治安之必要時，得協調相關機關（構）裝設監視器，或以現有之攝影或其他科技工具蒐集資料。」足認警察人員為調查

要」在要件上過於抽象，執法員警亦可能以隱藏身分查訪時透過密錄器加以拍攝。然而，事涉犯罪偵查，且錄影拍照亦有侵害肖像權或是造成表現自由的限制[54]（如集會遊行場所架設執法員警攝影機），上述警職法的規範，至多僅授權為治安維持等犯罪預防目的所用，再者，刑事訴訟法第 205 條之 2，僅授權檢察事務官、司法警察官或司法警察「因調查犯罪情形及蒐集證據之必要，對於經拘提或逮捕到案之犯罪嫌疑人或被告，得違反犯罪嫌疑人或被告之意思，採取其指紋、掌紋、腳印，予以照相、測量身高或類似之行為」，學說即有認為，必須考慮：1. 客觀上有無保全證據之公共利益與必要性，此際偵查輔助機關依於集會遊行或其他公共活動參與者之行為，得透過攝影、錄音或以其他科技工具蒐集證據，然此時則以警職法第 9 條第 1 項為依據；2. 如有涉犯重罪或參與職業性、習慣性、集團性或組織性犯罪之虞者，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動，此時則以警職法第 11 條第 1 項為依據[55]。最高法院直接以警職法第 10 條第 1 項為依據，將此規定之授權目的及範圍，擴及於刑事偵查，乃至於為危險預防的裝設依據[56]，仍有過於曖昧之嫌。

這是否意味監視錄影器設置或者使用密錄器一概違反偵查法定原則？德國學說普遍認為，監視器裝置用於刑事程序之犯罪偵查，應有相應的授權規定[57]，而預防性警用錄影監視（Präventiv polizeiliche Videoüberwachung）依照彼邦學說可透過一般偵查條款取得授權。不過，即便採取一般偵查條款的見

犯罪，在犯罪現場以自備影音器材或其他科技工具進行蒐集現場外觀情狀之證據資料，乃法律賦予警察職權之正當行使，此與通訊保障及監察法第一條所定「為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維持社會秩序，特制定本法。」之旨，係執行通訊監察之公務員以公權力介入他人間之秘密通訊為通訊監察對象者迥異，自無所謂依通訊保障及監察法第二十九條第三款：「監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者，不罰。」規定之適用。倘警察人員因調查犯罪，為蒐集犯罪證據，對犯罪現場外觀呈現情狀而為錄音、錄影，過程又無違法或不當之情形，其蒐證取得之證據資料，即難謂並無證據能力。」

54 吳秋宏，同前註 1，頁 220。

55 吳秋宏，同前註 1，頁 222-223；類似以遲延危險為切入視角的見解，亦可參見大野正博（2001），現代型捜査とその規制，東京：成文堂，頁 120-121。

56 參見劉靜怡（2016），監視科技設備與交通違規執法，月旦法學雜誌，248 期，頁 75。

57 Singelnstein, Bildaufnahmen, Orten, Abhören – Entwicklungen und Streitfragen beim Einsatz technischer Mittel zur Strafverfolgung, NStZ 2014, S. 306.

解，並不意味可以均可廣泛使用警察監視錄影所得，其中如監視攝影時間過長，干預隱私及資訊自主亦非輕微，如此即非學說所稱一般偵查條款可正當化[58]。我國學說則認為，依照警職法第 10 條第 1 項的規範，事前設置必須符合法定原則及比例原則，並非可以無差別在任何地點、時間裝置監視器，至少應以有防範保全證據之必要、緊急性及手段相當性；至於依照警職法第 11 條第 1 項所設置監視錄影器，該規定所設定要件為重罪原則且經警察局長書面同意，此事前限制門檻固然相對嚴格，然並無額外的監督機制，亦有不妥，學說認為此時干預隱私及表現自由的侵害危險程度極高，有必要考慮納入令狀原則[59]，由法官保留機制加以監督，此一看法應屬較為合理的看法。對此，科技偵查法草案第 3 條完全放棄法官保留的立法模式，是否在所有情形均屬妥當合適[60]，便有檢討空間。

另外基於行政目的而來的監視器錄影設置，如自動測速照相設備裝置，當被告有違規超速繼而有過失致死傷的疑慮時，即有可能將行政調查之成果轉換成刑事證據使用，關此合法授權依據何在，有認為道路交通管理處罰條例第 7 條之 2 第 1 項關於經科學儀器取得證據資料證明其行為違規等文字即已有充分授權[61]，亦有認為，現行法就此目的範圍應有限制，縱使經科學儀器取得，仍應考慮是否有當場不能或不宜攔截製單舉發之情形[62]。上述爭議癥結在於，立法者透過道交條例所授權的監視器允許的範圍，如違規停車的情形，可能透過科學儀器攝得被告當時有違規停止於紅線，繼而導致車禍發生，除非符合當場不能或不宜攔截之要件，否則顯然難以援引此規定作為合法拍攝道路行車畫面的合理依據。基此，在現行法下，若要使用此類非偵查機關所蒐集的個人資料或者影像，原則上應以合法蒐集為其

58 Singelnstein,（Fn. 57）, S. 307.

59 吳秋宏，同前註 1，頁 238-239。

60 草案第 3 條第 1 項:「偵查中檢察官認有必要時,得位在非隱私 空間之人或物,秘密實施監看、與聞、測量、辨識、拍照、錄音、錄影之調查。檢察事務官、司法警察官或司法警察 因調查犯罪情形及蒐集證據之必要,亦同。」; 草案第 4 條第 1 項:「檢察事務官、司法警察官或司法警察依前條規定，以科技設備或技術於空中實施前條調查者，應予立案，自立案之日起，實施之累計其間不得逾三十日。有繼續實施之必要者，至遲應於期間屆滿之五日前，檢附調查所得資料，敘述理由報請檢察官許可後續行之」。

61 吳秋宏，同前註 1，頁 244。

62 劉靜怡，同前註 56，頁 77。

使用前提[63]。

相較於本文上述所提及情況，實務上目前使用警用攝影器材的最大疑慮，在於透過密錄攝影機去私下蒐證。常見的狀況是員警以私人身分或者以非刑事偵查的外觀，去查訪私人住宅內從事的性交易或者賭博，由於這兩類犯罪類型均不容易由外觀上探知，如無現場影像確難判斷有相關犯罪正在進行。然而，依照上述說明可知，警職法第 9 條至第 11 條並無相應授權從事隱密性偵查的授權目的，且目前臥底偵查法仍未通過，相關授權隱密偵查的規定均未臻完備，於現行法下應認係不適法的取證手段。

（四）數位鑑識

最後便要討論數位鑑識（Digital Forensics; IT-Forensik）。數位鑑識主要聯結到前端其他數位取證手段，同樣可能有與針對以載體為中介所取得資訊及針對無載體中介的兩種主要情況，而鑑識流程則包含保存備份（Sicherung）、分析及呈現[64]。關於保存備份階段，必須準備（取得授權進行必要支援措施及具體計畫）、驗證（確認何種資料係要受到保存備份，涉及對於資料是否為證據之評估）、備份，可分成即時保存備份（Live-Sicherung）及事後保存備份（Post-Mortem-Sicherung），是蒐集與取得的過程[65]，除透過實務上常見透過電腦鑑識軟體將載體內的資訊加以複製並存取副本外，前已提到的線上搜索，在此意義下亦係複製並備份被告的個人電腦或使用裝置中的資訊的備份手段，線上搜索所運用的間諜程式或者國家木馬，也都是遠端鑑識軟體[66]。分析則是涵蓋蒐集及評估的過程，針對特定資料屬性、來源、製作者、內容加以解析，具體而言，透過鑑識軟體透過線上分析處理（OLAP）、資料探勘（Data Mining）等主要方式進行分析，而資料倉儲（Data Warehousing），即資料分析、整理於資料庫系統中，有利於上述分析方式的進行[67]，透過上述數位鑑識過程，將載體內龐大的資訊內容轉化成容

---

[63] Vgl. Singelnstein, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 604.

[64] Heinson,（Fn. 6）, S.26f.

[65] Casey/Schatz, in, Casey el.（ed.）, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 189（2011）.

[66] Heinson,（Fn. 6）, S.40; 施育傑，同前註 1，頁 64。

[67] Heinson,（Fn. 6）, S.60.

易理解的形式，並進行有系統的分類，於此同時，由於資料儲存特性，仍有可能透過數位鑑識將系統內資料（即便被格式化）予以還原[68]，乃證據蒐集及保全不可或缺的新技術形式。實務上目前主要透過檢察事務官、刑事警察局來進行相關數位鑑識，民間公司亦有提供數位鑑識的服務。

此外，由於雲端運算的進展，所謂雲端鑑識（Cloud-Forensik）也應運而生，鑑定方式除將鑑識能力透過雲端運算加以強化，亦可由雲端環境取得資訊，例如從 Dropbox 等雲端空間儲存位置取得資料，並且還原、重建雲端服務使用者使用情況，可能從雲端服務提供者或租用者手中取得資訊或經由使用者的登入帳號機制取得資訊，前者涉及到第三人持有資料的扣押問題，且因多半服務提供者並未位於我國領域，同樣可能會跨越國境取得的難題[69]。雲端鑑識在概念上亦同時包含了資料取得面向及資料分析面向。

由上述簡略說明可知，數位鑑識的過程中，可能會將載體內或者鑑識標的龐大的資料全部解析出來並進行有系統的歸類方式，由此也衍生過度蒐集資料的疑慮。學說即有認為，合理隱私期待侵害的角度，數位鑑識可將所有被告得以掌握或不能掌握的資訊（如機器自動記錄的檔案），均一網打盡，實質意義上已經等同於搜索，且其干預隱私之程度，可能更甚於對於實體物理空間搜索[70]；亦有認為，數位鑑識報告係透過具有專業知識經驗之人對於電腦設備或者網路設備的資料，應係鑑定[71]。

上述爭論多半聚焦在取得載體後對於載體內的資料如何進行數位鑑識的問題，如果綜合本文先前界定可能運用數位鑑識的範圍，可以發現數位鑑識這一觀念本身涵蓋多元的取證手段，其中由脈絡資料將載體資料予以重建、還原的驗真程序，必須遵循一定的科學鑑識規範，如道伯法則（Daubert-Crtieria），性質上是鑑定[72]，但將資料最大可能從載體中解析出來，相較於單純對於載體的占有，進一步加深對於

---

68 Momsen,（Fn. 8）, S. 877.

69 Heinson,（Fn. 6）, S. 49. 縱使沒有這跨越境外的問題，服務提供者的資料提供義務固然有可能透過立法實現（如美國法，參見法思齊，同前註 1，頁 122-124），然實際上是否願意配合，考慮到企業的商業利益及企業與客戶間的信賴關係，顯然不能期待。

70 李榮耕，同前註 12，頁 1068-1069。

71 王勁力（2010），論我國高科技犯罪與偵查－數位證據鑑識相關法制問題探究，科技法律透析，3 期，頁 24。

72 Momsen,（Fn. 8）, S. 878ff.

被告資訊自主權及隱私的干預，故無法單純侷限於特定強制處分或特定法定證據調查方法，來理解數位鑑識的法律性質。故本文認為，數位鑑識應區分其階段來確認其法律性質，而上述學說性質爭論主要是針對分析階段所為，從分析階段來看，現行法的鑑定確實無法明確涵蓋數位鑑識額外對於資訊自主權的干預[73]，數位鑑識過程中所進行的資料檢閱、還原，而且現行法下欠缺任何有效的救濟手段，包含拒絕還原鑑識特定資訊，是否會擴大資訊自主的侵害，只能仰賴鑑識人員與檢警機關的自律，並無相應的監督機制及權限範圍的限制[74]，除此之外，鑑識過程中可能會也會帶來資料毀損或影響載體運作的風險，例如運用鑑識軟體或者鑑識過程可能觸發載體自動銷毀資料等情況，刑事訴訟法第 204 條固然授予鑑定人經法官、檢察官許可，得毀壞物體之權限，常見如將扣案子彈擊發消耗以測試殺傷力，然數位鑑識情況下，如進一步影響到載體運作效能，亦非無過度干預之疑慮。再者，目前行動裝置利用生物特徵進行加密的情況亦非罕見，如指紋辨識或虹膜辨識，數位鑑識過程中如果要取得被告生物特徵破解數位裝置的加密措施，至少要分成兩個階段，第一階段是讓被告將手指或者眼睛湊近裝置解鎖，第二階段則是藉此動作解鎖[75]，仍有疑義。詳言之，進行鑑定時，鑑定人固得依照刑事訴訟法第 205 條之 1 而採取指紋，然進行數位鑑識時，鑑識客體自始與被告身體特徵無關；司法警察（官）因調查犯罪情形及蒐集證據之必要時固得採取指紋，然而這是為了建構被告身體特徵與現場犯罪蹤跡的關係或本案事證的關聯性，藉以澄清事實，僅干預身體完整性，並未進一步授權可以用來解除特定加密裝置的防護，進而容許被告的資訊自主權及資訊安全受到干預[76]，倘認為現行法身體檢查處分可支撐鑑定人或者

---

73 就此劉芳伶（2016），遠距搜索扣押與令狀之明示特定，東海大學法學研究，49 期，頁 83-84 註 77 認為，電腦鑑識雖不應被理解為搜索，然藉由扣押載體進行遠端檢索、查找或下載檔案，仍非現行法勘鑑定本身所授權，而係因鑑定所為必要處分，應另由立法者授權。

74 李榮耕，同前註 12，頁 1086-1089。

75 Vgl. Rottmeier/Eckel, Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren, NStZ 2020, S. 195.

76 值得反思的議題至少有二，第一，是強制處分是否一律容許附隨權限（Annexkompetenz）干預被告，相關討論，就此參見 Ziemann, Strafprozessualer Eingriff und Gesetzesbindung. Ein Beitrag zur Lehre von der Annexkompetenz im Strafverfahrensrecht, ZStW 130（2018）, S. 762ff.；第二，立法者可否課與被告容忍義務去揭露自己的身體資訊，破解相關的加密機制？有無違反不自證己罪原則？相關討論，Vgl. Rottmeier/Eckel,（Fn. 75）, S.199f.

司法警察（官）逕自解鎖加密裝置，例如使用鑑識軟體植入間諜程式開後門，藉以擷取資料，或是違反被告意願開啟加密裝置的內容，即有商榷空間。儘管學說苦心孤詣透過類比搜索將電腦鑑識納入搜索、扣押的適用範圍，但數位鑑識與現行法搜索扣押的機制有若干扞格之處，例如是否應交付扣押物名目[77]、能否事前特定搜索範圍[78]及執行時間[79]等規範，均有疑問，自有另外修法的必要性。對此，科技偵查法就第一階段所涉及的載體內容電磁紀錄保全問題，為避免資料內容遭竄改或湮滅，另外創設了授權條款[80]，以及針對分析時可能要進行的破解、資料擷取、儲存或還原，以及資料取得後之分析比對，均進行了授權，同時也擔保了數位證據在採證上應維持其同一性[81]，固值贊同。然而在本案使用之外，建置資料庫將所取得的資料供他案比對，是否妥當？是否過於廣泛？而且似乎欠缺監督機制？上述諸多問題，容有檢討餘地[82]。

（五）小結

由上述討論可知，現行法關於科技偵查方式的強制處分及手段，均無法有效證成其使用，也令偵查機關面對利用科技技術的犯罪或者數位化的人類生活軌跡不免於規範面上捉襟見肘，甚且有違反刑法之疑慮。然而，資安基本權、資訊自主權、隱私權乃至於個人生

---

77 李榮耕，同前註 12，頁 1083。

78 李榮耕，同前註 12，頁 1097-1099。

79 李榮耕，同前註 12，頁 1100-1101。

80 草案第 20 條：「電磁紀錄之搜索或扣押開始執行前及執行完畢前，得對於行動裝置、儲存設備、電腦或其他相類之設備及其內之電磁紀錄為必要之處分。對於被告、犯罪嫌疑人、前述設備或電磁紀錄之所有人、持有人、保管人或其他相關之人，亦同。前項之人無正當理由拒絕或抗拒前項之處分者，得以強制力為之，但不得逾必要之程度。」

81 草案第 21 條：「檢察官、檢察事務官、司法警察官或司法警察對於行動裝置、儲存設備、電腦或其他相類之設備或其內之電磁紀錄實施搜索或扣押時，得為下列處置，對於已經合法扣押或經自願性交付之前述設備或其內之電磁紀錄，亦同：一、實施使用、操作、檢查、必要之變更或其他相類之處置。二、破解相關帳號、密碼或保護措施。三、以擷取、複製、鏡像或相類似之方式將全部或一部之電磁紀錄另行儲存。四、復原已遭變更、刪除、覆蓋、格式化、損壞或其他相類情形之電磁紀錄。五、對於電磁紀錄進行分析、比對及其他必要之處置。六、將電磁紀錄內之犯罪資訊建置於自願性交付之行動裝置、儲存設備、資料庫，供本案或他案分析使用。七、其他關於蒐集、保全數位證據之必要處置。實施前項處置時，應依相關科技技術可達成之範圍內，確保實施標的與實施前之完整性及同一性。」

82 關於犯罪資料庫建置與資料比對的議題，以及授權密度，須另行為文討論，但初步認為，目前草案規範模式缺乏法官保留等外部監督機制，容有不妥。目前關於犯罪偵查方面的資料庫建置均集中於 DNA 的採集，相關討論，參見劉靜怡（2009），DNA 採樣、犯罪預防和人權保障，台灣法學雜誌，124 期，頁 119-123；涂俊偉（2012），建構刑事 DNA 資料庫之合理界限，法學新論，35 期，頁 157-182。

活私密領域，均係重要的基本權利，倘若上開手段，現行法若無規範，固然不能加以干預，其立法原則之形成，則必須嚴守法律保留原則、基本權保護[83]、事後權利救濟機會的賦予及通知義務等基本要求[84]，同時由法院進行合法性控制亦屬必要，無論係事前或事後，然不宜由單獨檢察官保留，至少應有相對法官保留，如於個案中有遲延危險之情形，始由檢察官先行發動[85]，於執行後再向法院報告。此外，縱使予以規範並授權偵查機關得以搜索、扣押、檢閱、鑑識這些數位資訊與資料[86]，這種資訊安全缺口仍難以受到有效填補及保障[87]，其射程範圍也應審慎為之[88]。目前科技偵查法的草案，雖然試圖填補規範缺口，但其規範密度及合法性調控、監督機制是否合宜妥當，值得我們進一步檢討。

二、令狀原則及特定明確原則

除了授權依據外，令狀原則或法官保留也是必須加以檢討的部分，特別是對於數位取證的令狀內容要求。令狀原則是授權規範或程序干預規範的具體化[89]。通常最常見的問題是搜索扣押範圍的界定，於此處不得僅記載載體，如手機、光碟片等，否則無異於容許概括搜索，就現行法而言，得為沒收及得為證據之物均得扣押，惟仍應限定在與本案有關者[90]。就令狀範圍外的扣押，傳統搜索雖依照一目瞭然法則，針對搜索所不及的另案扣押，僅就偵查官員目光所及之處，得一併予以扣押。而這一問題在數位取證上有特別的難處，就當場扣押的情形，單純瀏覽檔案名稱，無法判斷與本案是否有關連性[91]，從而扣押

---

83 施育傑，同前註 24，頁 401-402。

84 Vgl. Zöller, Heimliche und verdeckte Ermittlungsmaßnahmen im Strafverfahren, ZStW 2012, S. 420ff.

85 Vgl. Zöller,（Fn.84）, S. 434ff.

86 另外現行實務還有網路巡邏或加入聊天（已見於王士帆（2017），同前註 1，頁 366-370）、司法警察網路釣魚等一些偵查技巧，或者是跨政府資料庫的資料調取及比對，礙於篇幅關係無法詳細討論，只能暫時擱置不論，但本文初步認為現行法並無合理的偵查一般授權條款之依據，由於上述偵查手段有一定程度的基本權干預效果，如必須採取此類偵查手段，有立法加以明確規範的必要性。

87 Großmann,（Fn. 24）, S. 454f.

88 特別是干預基本權重大或者已經嚴重涉入私人生活形成核心領域時，應係國家不能涉入市民生活的界線，vgl. Zöller,（Fn.84）, S. 430f.

89 Heinson,（Fn. 6）, S. 206; Ziemann,（Fn. 76）, S. 791f.

90 李榮耕，同前註 12，頁 1093。

91 法思齊，同前註 1，頁 116。

時勢必會將所有相關的檔案一併複製，另一方面，在電腦鑑識也有相同的情況，在檢閱檔案過程中，同樣可能發現作為證明他案所用證據，文獻上亦有主張應限於另案為重罪的情況，始得加以使用[92]，此外，由於電腦鑑識過程過於不確定，文獻當中認為事前限制無法有效控管，應以事後管制始妥[93]。

從避免過度干涉無關於犯罪的資訊自主權，學說認為數位鑑識的分析過程有令狀原則適用的必要，確實值得傾聽。然而，數位鑑識結果，導致偵查機關取得無關於本案的資料，也並不表示鑑識本身違法。再者，鑑識人員對於從載體內擷取的資料，並無承辦案件的偵查官員對於案件相關理解，如此要判斷何種資料屬於本案有關，何者與本案無關，已屬困難，更何況偵查機關人員多半只能在鑑識結果出來後，才能進一步篩選可能的證據，難以事前特定證據特徵跟性質[94]，如欲令偵查官員釋明欲扣押資料性質特徵，確實強人所難。或許可以考慮於聲請搜索前，註明將鑑識所扣押本案相關電磁紀錄，並於執行搜索時，告知被告本案進行鑑識與鑑識過程可能的風險；如鑑識過程中如有必要採取更進一步的破解措施，若會伴隨物體的破壞，應考慮取得檢察官或法官的許可；於鑑識執行後，應容許被告對於鑑識結果有救濟之機會；如確認所蒐集的非本案資料，無法形成犯罪嫌疑，應課予偵查機關資料刪除義務。

另外必須強調，重罪原則本身不宜作為解除令狀原則的理由，而僅能構成急迫情形與否的衡量因素，特別是重罪定義易隨著立法者加重法定刑而擴大[95]，如此將使法官保留的機制無法起到有效的監督功能，縱使有一定訴追利益，也不能替國家監控手段逕行大開其門，仍須有相應的程序調控機制。

肆、數位證據之證據評價

一、證據同一性

因數位證據因其容易複製，同時因其資料狀態或內容容易變更，無法擔保資料形式及完整性與原件相符，有遭竄改的風險[96]，實務上不乏被告爭執數

92 李榮耕，同前註 12，頁 1108-1109。

93 李榮耕，同前註 12，頁 1099；Kerr, *supra* note 3, at 572.

94 See Kerr, *supra* note 3, at 569.

95 已指出這一點，見李榮耕，同前註 38，頁 957。

96 Casey, *supra* note 4, at 26.; Momsen,（Fn. 8）, S. 876.

位證據同一性，因此不惟數位鑑識過程應確保同一性[97]，確保數位證據與原件具有同一性厥屬必要，就此而言，驗真（authentication）即屬必要的程序[98]。同一性問題涉及到訴訟上要證明如何證明數位證據與原件具有同一性，放在民事訴訟法的脈絡則是文書真正性與否的問題，證明同一性才能繼而證明：特定資訊是否透過行為人活動產生，包含有意識地使用行動裝置或電腦設備進行溝通，或是無意識地透過行動裝置所產生的紀錄，可藉此證明特定犯罪事實的構成或者建構行為人的行動軌跡。不過由於數位證據可以複製的特性，因此相較於實體物證如有爭議則須提示實物提示外[99]，其調查並不以原件檔案為必要，可能是原件複製而來的複本，亦有可能是硬碟內的暫存（Cache）[100]。

近期最高法院對於這一問題進行闡釋，其事實關係為：被告 A 對證明其犯罪的行車紀錄器 SD 卡數位錄音影檔案是否遭到影像處理軟體為工具，竄改、偽造行車紀錄檔案內容及屬性，而不具同一性而有所爭執，就此進行如下闡釋：「數位證據具無限複製性、複製具無差異性、增刪修改具無痕跡性、製作人具不易確定性、內容非屬人類感官可直接理解（即須透過電腦設備呈現內容）。因有上開特性，數位證據之複製品與原件具真實性及同一性，有相同之效果，惟複製過程仍屬人為操作，且因複製之無差異性與無痕跡性，不能免於作偽、變造，原則上欲以之證明某待證事項，須提出原件供調查，或雖提出複製品，當事人不爭執或經與原件核對證明相符者，得作為證據。然如原件滅失或提出困難，當事人對複製品之真實性有爭執時，非當然排除其證據能力。此時法院應審查證據取得之過程是否合法（即通過「證據使用禁止」之要求），及勘驗或鑑定複製品，苟未經過人為作偽、變造，該複製品即係原件內容之重現，並未摻雜任何人之作用，致影響內容所顯現之真實性，如經合法調查，自有證據能力。至於能否藉由該複製品，證明確有與其具備同一性之原件存在，並作為被告有無犯罪事實之判斷依據，則屬證據證明力之問題。」[101] 據此，首先，該檔案是由另案被告 B 電腦中查扣。檔案內錄音有 A 被 B 交付 20 萬

---

97 Heinson,（Fn. 6）, S. 49.

98 李榮耕，同前註 9，頁 183；Heinson,（Fn. 6）, S. 146ff.

99 最高法院 97 年度台上字第 1355 號判決。

100 Momsen,（Fn. 8）, S. 881.

101 最高法院 107 年度台上字第 3724 號判決。

元，該錄音最後作為 A 職務上機會詐取財物罪之證據。而錄音有部分遺失，該遺失部分，則上傳至 B 的雲端硬碟中，因檢察官於勘驗前係即將①「所有上傳」的錄音檔案下載，②上傳原因係出於 B 自我保護意識、③檔案經撥放候連續、無中斷、雲端硬碟檔案目錄、④ A 於被偵辦時，上開檔案目錄雖然「上次修改時間」早於案發期間，但該修改時間係在 A、B 第一次見面前，因此檔案目錄時間跟檔案內容製造或修改日期並無關係。根據①至④點，認為原審認定該行車紀錄器錄音檔跟原件具同一性，並無違誤。

最高法院上開闡釋，認為原件滅失時，確認有無證據能力，有兩項審查標準：（1）複製品取得合法性、（2）複製品並未作偽變造[102]，如通過（1）、（2）則應認有證據能力。首先，認為真實性[103]與同一性為證據能力問題，應可贊同[104]。就複製品與原本間的關係，學說即參考美國法的見解，如果數位證據屬於電腦儲存紀錄時，可以由對該電腦記錄有其個人認知之人證明該紀錄為真，如銀行消費借貸部門經理可以證明與借貸相關的電腦資料為真，亦可以由審判者或專家證人與其他經驗真的資料加以比對，確認是否為真，如檢察官可藉由經驗真的電子郵件，來比對其他電子郵件是否也由被告所撰寫或寄出[105]；另外，如果電腦儲存紀錄有著獨一無二的特徵，輔以情狀證據，也可以透過驗真要求，如被告電子郵件中有特殊的簽名檔[106]；如果數位證據是電腦產生證據時，得以證明該電腦系統是使用於日常性營運，來驗真其所產生的紀錄為真，例如電信公司就電話通聯設備所記錄的用戶撥打電話號碼、秒數、開始時間或結束時間等資訊，也可以透過對電腦程式具有特別知識經驗之人，來證明該程序或設備所產生的紀錄為真[107]，作類型化的區隔。另外針對上述最高法院見解，學說認為此一見解似乎採取英美法上最佳證據原則（the Best Evidence Principle），似乎與過往最高法院認為影本亦有證

102 蘇凱平（2020），數位證據在刑事訴訟中性質與應用，月旦裁判時報，93 期，頁 67。

103 就真實性部分，先前判決持相同見解者，如最高法院 101 年度台上字第 878 號判決。

104 亦見吳冠霆（2011），由嚴格證明法則論數位證據及影音證據於刑事訴訟法上之處理，司法新聲，101 期，頁 79。

105 李榮耕，同前註 9，頁 187-188。

106 李榮耕，同前註 9，頁 188-189。

107 李榮耕，同前註 9，頁 189-190。

據能力見解相左[108]，且原則上仍要提出原本，與原本滅失後與複製品提出並不喪失證據能力，其說理前後不無矛盾之處[109]。

日本實務則認為判斷複本證據能否作為證據之標準在於：（1）原本證據仍然存在。複本證據能與原本證據確認並無不同之時點，該原本證據仍然存在即為已足、（2）本證據係忠實重現原本證據之內容，並不以完全複製原本證據為必要，只要就待證事項有關聯，且就該必要之情狀得予以真實重現即可。（3）複本證據無法顯現出來之原本證據性質、狀況（例如材質、凹凸、有無透明紋路、重量等），並不能作為待證事項[110]。

由上述比較法概況觀之，如何判斷數位證據的真實性及同一性，再度凸顯出取證階段證據保管的重要性，且若當原件（錄音或原始檔案）佚失時，透過製作者、能確認內容之人或其他間接證據加以證明，或證明特定記錄的產生機制並無虛偽的可能性，並區別資訊產生方式來決定證明同一性的方式，屬合理的做法。於訴訟上，若被告或辯護人有所爭執，可就爭執數位證據的真實性說明其所認為不實的理由，檢察官再就此指出證明方法並聲請法院調查該數位證據是否與原件具同一性，例如監聽譯文是否具有同一性有所爭議，得就所爭執的監聽錄音部分勘驗以解決爭議[111]。

二、證據使用禁止

（一）依附性證據使用禁止

依照前述說明，現行法對於多數科技偵查手段取得方式均未授權，因此，在無其他特殊證據禁止規定的情況下（如通保法第 18 條之 1），偵查機關所取得的證據，均落入刑事訴訟法第 158 條之 4 的射程範圍。不過，這不必然均導出無證據能力的結論，例如現行法並未授權員警跟監拍照，但由於干涉被告資訊自主利益不深、影響被告防禦可能性不高且犯罪所生危害或實害非低，個案中仍有可能得出所拍攝的照片，不排除證據能力的結論[112]。另外，現行法下的 GPS 偵查所得結果，其所得證據及派生證據應適用證據排除法則，並無證據能力，至衍生證據是否有證據能力，依照是否與違法取得之證據或係獨立偵查作為來判斷是

108 蘇凱平，同前註 102，頁 64。
109 蘇凱平，同前註 102，頁 68。
110 吳冠霆，同前註 104，頁 79。
111 吳秋宏，同前註 1，頁 263。
112 薛智仁，同前註 35，頁 253-254。

否併予排除[113]。

（二）自主性證據使用禁止

比較關鍵的問題是自主性證據使用禁止的問題，自主性證據使用禁止主要涉及的常見問題有二，第一是所取得的證據如用於訴訟上將造成加深被告其他相關基本權的干預，此時是否仍得調查、使用，第二則是私人不法取證的問題。由於審判程序中調查證據，仍有可能干預被告基本權利，因此第一個問題並非證據取得合法即可忽視不論；至於私人不法取證，於數位證據當中亦非少見，常見者如違法裝置 GPS 系統；私人盜取公司資料；以手機錄音擅自錄取他人聲音、影像；於公司進行內部控制的情況，公司為查緝舞弊，亦有可能對委託民間公司進行數位鑑識，過程是否均係合法取證，亦有檢討必要。

先從實務學說常見的私人不法取證問題，為數不少的見解，均試圖透過依附性證據使用禁止的角度，建構後續證據取證的違法性，例如基於法秩序一體的推論，認為刑事訴訟法亦不約束私人取證，但因私人竊錄、竊聽他人非公開活動受刑法第 315 條之 1 之刑事制裁，應以此為根據加以排除[114]。或係類推適用刑事訴訟法第 156 條第 1 項之任意性法則，但認為於供述性證據，例外得適用刑事訴訟法第 156 條，但應區別情況，於詐欺利誘之情形，限制在私人使用之方法違背社會良心或誘發虛偽陳述之危險，否則仍得為證據使用；於使用強暴脅迫方法，避免鼓勵任意侵害人身自由外，已破壞法律核心價值，且可能因為終止暴力脅迫而被動供述虛偽不實之內容，依此，如有上述情形，則應類推適用第 156 條第 1 項，排除所取得之供述性證據之證據能力[115]。亦有類推適用刑事訴訟法第 158 條之 4 之審查要件，此說認為刑事訴訟法第 158 條之 4 雖規範實行刑事程序之公務員，然如有嚇阻私人違法取證之必要，且考慮到基本權之保障、擔保司法的正潔性及比例原則，審酌其違法情節、違法與證據取得之關聯性、案件重大性、使用證據之必要性，是否會另行侵害關係人隱私權益等因素，衡量是否有違反審判之公正[116]。

然而，上述見解均無法妥適說明其排除證據使用之合理依據；此外，依

113 關此，無論是否採取援用搜索令狀，結論均同於吳燦，同前註 40，頁 167-168。

114 王兆鵬（1999），證據排除法則的相關問題，刑事法雜誌，43 卷 3 期，頁 40。

115 吳巡龍（2004），私人不法取得證據應否證據排除－兼評最高法院九十二年度台上字第二六七七號判決，月旦法學雜誌，108 期，頁 228-235。

116 陳運財（2004），違法證據排除法則之回顧與展望，月旦法學雜誌，113 期，頁 46-47。

附性證據使用禁止的規定，如刑事訴訟法第 156 條第 1 項或第 158 條之 4，均係規範實施刑事偵查之公務員，並無規範漏洞可言，無類推適用之空間[117]，從而如類推適用，將牴觸立法及司法間的權力分立[118]。不過，持自主性證據使用禁止論者，認為評價重點在於將私人不法所取得證據加以調查，而理由及評家標準則有不同見解。第一種看法是國家怠惰其釐清證據之義務，因私人不可期待國家在特定案件中先為蒐證，故可歸責於國家，第二種看法則是避免鼓勵私人違法取證及深化對於先前所干涉的個人權利之侵害，禁止國家收贓，第三種看法則是基於人性尊嚴及個人權利的尊重，關於第三種看法，究竟是國家取得證據會牴觸基本權之保障（如被告遭被害人家屬刑求而坦承犯罪）[119]，或者法院於審判程序中進一步調查證據，會導致基本權及人性尊嚴的侵害，容有不同意見[120]。從禁止法院調查時過度干預基本權的角度來定調自主性證據使用禁止的合理性，應屬合理的看法，因為法院證據調查時，仍有可能進一步在公開審理的情形下，因調查而加深當事人資訊自主權或隱私權的侵害，從而有必要在合乎比例原則的限度內進行審理程序。這套基本權保護導向的思考模式，即是目前持自主性證據使用禁止見解的理論依據[121]，另外，德國學說實務除就隱私領域之侵害外，對於牴觸法治國原則或牴觸公正程序踐行基本權[122]之證據使用，亦認有適用自主性證據使用禁止餘地。

關於隱私侵害的問題，德國實務學說主要係以三階層理論或稱領域理論作為論證基礎[123]，第一階層是私密領域（Intimsphäre），乃基本權絕對保護之核心領域，即便是高度公益事項如個案具高度刑事追訴利益

117 文獻上亦有支持牴觸人性尊嚴的情況，可以類推適用刑訴法關於自白任意性之規定，排除私人不法取供的證據能力，vgl. Beulke/Swoboda,（Fn. 51）, Rn. 478.

118 薛智仁（2014），刑事程序上私人取證之證據能力－評析最高法院判決的新發展，台灣法學雜誌，260 期，頁 52-54。

119 楊雲驊（2002），賠了夫人又折兵？－私人違法取得證據在刑事訴訟的證據能力處理，台灣本土法學雜誌，41 期，頁 14 以下。

120 薛智仁（2011），禁止國家使用私人違法取得證據之理論基礎，政大法學評論，121 期，頁 90-96。

121 Vgl. Eisenberg, Beweisrecht der StPO, 10. Aufl., 2017, Rn. 385.

122 Vgl. Eisenberg,（Fn. 121）, Rn. 386.

123 Vgl. Eisenberg,（Fn. 121）, Rn. 387f.

者，亦無法透過比例原則權衡而正當化國家對於證據的使用，因此屬於絕對證據使用禁止之範疇；第二階層則是私人領域（Privatbereich），個人在此領域會作為社群成員，仍與社會有一定接觸，僅當國家訴追利益大於個人利益的情況下，才能符合比例原則之要求[124]，具體衡量因素可能包括①犯行可非難性的程度、②調查證據之必要性（Unverzichtbarkeit des Beweismittels）、③對於取證對象的基本權具體侵害的嚴重程度[125]；第三階層則是一般社會接觸領域（Bereich allgemeiner sozialer Kontakte），此情形下無明顯保護之必要，所取得證據原則上均有證據能力。

實務見解近期亦可見到在私人不法取證的情形，透過上述基本權保護視角予以證據排除的觀點，如最高法院 107 年度台上字第 1165 號判決：「私人就其因被追訴犯罪而蒐集有利證據，除得依刑事訴訟法第 219 條之 1 至第 219 條之 8 規定，聲請國家機關以強制處分措施取證保全外，其自行從事類似任意偵查之錄音、錄影等取證行為，既不涉及國家是否違法問題，所取得之錄音、錄影等證物，如內容具備任意性，自可為證據。私人將蒐取之證據交給國家作為追訴犯罪之證據使用，國家機關只是被動接收或記錄所通報已然形成之犯罪活動，並未涉及挑唆、參與支配犯罪，該私人顯非國家機關手足延伸，國家機關據此進行之後續偵查作為，自具有正當性與必要性。利用電話通話或兩人對（面）談因非屬於秘密通訊自由與隱私權等基本權利核心領域，國家就探知談話內容所發生干預基本權利之手段（即檢察官或法院實施之勘驗）與所欲達成實現國家刑罰權公益目的（即追訴、證明犯罪）兩相權衡，國家公權力之干預，尚無違比例原則，法院自得利用勘驗結果（筆錄），作為證據資料使用。」明確強調私人取證不受刑事訴訟法規制及對私人取證的調查涉及基本權干預，上述自主性證據使用禁止是可以支持的看法。而最高法院 108 年度台上字第 4094 號判決則強調：「刑事訴訟法上證據排除法則等相關規定，係為防止國家機關以違法侵害人民基本權方式取得證據，故其規範對象係以國家機

[124] 依照德國實務見解，不同情況的衡量因素及判斷則有差異，如錄製他人自我對話的情況，係基本法所保障的人格權核心重要內涵，聯邦憲法法院要求極度優越的公共利益（überwiegende Interessen der Allgemeinheit）始有使用該錄音內容之必要，vgl. BVerfGE 34, 238（249f.）.

[125] Beulke/Swoboda,（Fn. 51117）, Rn. 471.

關為限，並不及於私人。不可歸責於國家機關之私人違法錄音（影）所取得之證據，既非因國家機關對私人基本權之侵害，自無證據排除法則之適用或類推適用可能，如其內容具備任意性者，自可為證據。且刑事訴訟法與刑事實體法各有不同之功能，因私人違法錄音（影）而受法益侵害之私人，已因刑事實體法之設而受有保護，不能謂法院仍須片面犧牲發見真實之功能，完全不能使用該錄音（影）內容作為證據，始已完全履行國家保護基本權之義務或不致成為私人違法取證之窩贓者。惟為避免法院因調查該證據結果，過度限制他人之隱私權或資訊隱私權，應視該證據內容是否屬於隱私權之核心領域、法院調查該證據之手段造成隱私權或資訊隱私權受侵害之程度，與所欲達成發見真實之公益目的，依適合性、必要性及相當性原則妥為權衡審查。如非隱私權核心領域內容，法院為達成發見真實之公益目的要求，自得使用最小侵害之法定調查方式（例如，以不公開審理方式勘驗，並禁止勘驗結果對外公開，或裁判書遮隱直接或間接足資識別權利人之相關個資或隱私內容），在待證事實之必要範圍內，限制私人之隱私權或資訊隱私權。」上述 108 年判決，較諸於最高法院過往見解更有嶄新意義：其一，明確類型化隱私領域及不同類型隱私所得干預門檻限制，其二，將私人所取得證據，要求法院在進行證據調查階段，一併考慮到何種方式較能減少對於受侵害私人之隱私權或資訊自主權之侵害的加深，意識到法院證據調查本身亦屬基本權干預手段，可謂落實對於國家對基本權保障義務。

另一實務曾出現的問題即前述提及私人不法設置 GPS 定位設備，例如配偶為了捉姦所以在另一半車上裝置 GPS 以定位追蹤，這種擅自裝設的行為，多數見解認為構成刑法第 315 條之 1 第 2 款的無故竊錄他人非公開活動行為。GPS 系統雖然是位置資訊，單純就資訊內容而言，不僅就所得能探知通訊者使用資料及通信紀錄並無太大差異，甚且上述位置資訊所建構的行動剖繪，其精確程度遠勝於調取通信紀錄所能確定的行動軌跡，雖然不涉及自我思想表達或私生活核心領域的保護，但在公共領域當中類此位置資訊仍受隱私及資訊自主權的保護，司法院釋字第 689 號解釋就公共領域的跟追也採取相似看法，此時應取決於有無優越於上述權利保護的公共利益存在，始能認為私人不法取證屬於合法。個案中 GPS 裝置如係長期裝置，對被告隱私權的長期侵害，恐遠甚於通姦罪所要保護法益及國家訴追利益（1 年以下有期徒刑），況且，在司法院釋字第 791 號解釋後，關

於通姦罪已經廢除，其訴追利益已蕩然無存，基於上述說明，應認不得作為證據使用。

剩餘的問題的是，何種情況下於國家合法取得的證據也是自主性證據使用禁止的範圍？在現行法下多數數位取證的情形均未經授權，不過以下可能的案例亦可能檢討其證據使用是否亦應予以禁止，例如於被告遭扣押手機中，裡面儲存日記或者筆記等非對話性質等資訊內容，或是錄下被告自言自語的錄音紀錄，由於個人生活高度仰賴數位裝置及個人電腦設備，各種可能的資訊均會包含在內，如將該等資料運用於訴訟上，將高度侵害個人隱私[126]。德國在彼邦刑事訴訟法第 100d 條，規範禁止監察私人生活形成核心領域，即便取得也負有刪除義務，類似立法模式固然可能迴避上述疑慮[127]。然而現行法之下仍有對證據評價合於基本權保護的解釋，而且這種保障不應因內容陳述涉及犯罪而脫離核心領域的保障[128]。其次，縱使容許使用，如果調查時仍有可能加深被告或被害人等隱私的侵害，宜採取較不侵害隱私的方式，如限制調查結果資料的公開且採取去識別化方式避免對產生對於被害人不利之影響[129]。

三、傳聞法則

另一個問題涉及到傳聞法則。不少數位證據的內容，如錄音或錄影，牽涉到被告以外之人於審判外就被告案件相關內容之陳述，不過並非所有得以文字表示的內容，均屬傳聞證據。此時，取決於所供述內容是否具有人的意思、思想及陳述於其中，即是否具有供述性[130]。如電腦儲存紀錄

126 同樣的問題出現在扣押拒絕證言權人的資訊內容，當對被告以外第三人搜索時，如未能保障拒絕證言權人以數位資料所陳述的內容不受評價，縱使現行法下係合法取得是類證據，如於訴訟上加以調查、使用，仍會終局侵害該第三人與被告間的親密關係或信賴關係，特別是與親屬間可能涉及到私生活核心領域的可能性較高，一概容許扣押文件亦有不妥之處。關於拒絕證言權對於扣押等強制處分之限制效力，參見薛智仁（2020），論拒絕證言權對於取證強制處分之限制：以親屬與業務拒絕證言權為例，臺大法學論叢，49 卷 2 期，頁 726-750。

127 Vgl. Beulke/Swoboda,（Fn. 51）, Rn. 471.

128 參見薛智仁，同前註 118，頁 61；Eisenberg,（Fn. 121）, Rn. 392.

129 就此而言，科技偵查法草案僅於第 27 條規定：「本法施行前，以第五條、第九條之方式所實施之調查，其調查所得有無證據能力，應審酌人權保障及公共利益之均衡維護。」僅對 GPS 定位追蹤及非侵入性科技偵查手法，溯及性的適用刑事訴訟法第 158 條之 4 的權衡判斷方式，似乎並未意識到科技偵查所刺探成果可能往往會涉入高度私人生活核心領域的問題，若參照德國法上的證據使用禁止規定，其內容就將來草案內容增補上，是值得考慮的方向。

130 張明偉（2018）電子證據之傳聞疑義，東吳法律學報，29 卷 3 期，頁 45。

多半具有這種性質，除通訊內容外，包含儲存於電腦的帳冊、公文檔案，均屬常見的傳聞證據形式。

學說有認為，並非所有通訊內容，均係所謂的電腦儲存紀錄，監聽過程所得的通訊錄音本身，係建置機關以程式錄製通訊期間的監察內容，仍屬於電腦產生記錄，故非傳聞[131]。上述說法固然值得傾聽，但這並不表示任何錄音內容均屬無供述性的證據，持供述證據說的論者則認為，影音檔案可能隨著拍攝者之價值判斷與編輯者之取捨，容易使法院對證據證明力有錯誤評價，並因該錯誤評價形成不當偏見[132]，對此仍有必要傳喚製作者到場接受詰問始妥。

至於依照錄音所製作的譯文是否為傳聞證據，即有疑問，最高法院即認為：「偵查犯罪機關依法監聽之錄音，係錄得之聲音為證據，依據監聽錄音結果翻譯而製作之通訊監察譯文，乃該監聽錄音內容之顯示，為學理上所稱之派生證據，屬於文書證據之一種。苟當事人或辯護人對其譯文之真實性發生爭執或有所懷疑時，法院應依刑事訴訟法第165條之1第2項之規定勘驗該監聽之錄音帶踐行調查證據之程序，以確認該錄音帶之語音是否為本人之聲音及其內容與通訊監察譯文之記載是否相符，始得據為判斷之依據。」[133] 不過，監聽譯文仍係經由譯文製作者聽取並轉化成文字內容，錄音內容縱使全文照錄，錄音內容所傳達的情境、音量或說話者的情緒，均可能會經譯文製作者簡化，仍有人的思想表達介入其中[134]，如被告認為證人所述不實，卻僅認為以勘驗錄音即可，顯然剝奪被告就證人對所述不利事項予以對質詰問的機會，因此，上述判決射程應理解為當事人對於監聽錄音譯文真實與否表示爭執，並未於對質詰問的角度脈絡處理。

司法警察所製作監聽譯文或者其他錄音所轉換的文字內容，必須考慮供述性質及所爭執的證據能力項目來決定其證據能力，譯文如為被告不利於己之陳述，仍非傳聞證據；如為證人陳述他人犯罪事實部分，則屬傳聞證據之範疇；如僅爭執譯文內容真實性，僅以勘驗加以確認[135]，反之，如係爭執證人所述未經對質詰問，則應傳該證人到場接受對質。

131 李榮耕（2019），通訊監察所得對話內容及傳聞法則，月旦法學教室，203期，頁23。
132 吳冠霆，同前註104，頁83。
133 最高法院102年度台上字第1842號判決、103年度台上字第2353號判決。
134 吳秋宏，同前註1，頁265。
135 吳燦（2018），勘驗筆錄之證據能力，月旦法學教室，188期，頁28。

至於電子通訊紀錄，如有陳述者自願對於甫察覺事務為記錄，且無其他詐偽目的，仍可綜合判斷陳述客觀情狀後獲得高度特別可信性擔保予以澄清，認定與待證事實有關的該供述有證據能力，文獻有認為可適用刑事訴訟法第 159 條之 4 第 3 款，以特別可信狀況下作成之文書認定有證據能力[136]。就認定電子通訊紀錄作為傳聞證據，固值贊同，然而以甫察覺事務而為記錄作為可信性判斷標準，是否能與「其他特別可信情況」所規範的、與公務員職務上製作之文書及業務文件具有同等程度可信性，而可據以適用該款傳聞例外，恐有商榷餘地[137]。

伍、結論

以下總結本文研究結果：

一、現行法確如學說所指摘，關於對數位證據蒐集的強制處分有所不足（如本文貳、二、(一) 至 (三))，不惟如此，即便現行實務盛行的數位鑑識或監視錄影使用，均有若干的規範授權不足的疑慮（如本文貳、二、(四) 至 (五))。

二、依照令狀原則，固然要明確特定搜索範圍，不過因數位證據蒐證上往往偵查機關要面對過於繁浩的資料數量，難以期待偵查機關聲請時能具體特定，惟不應放任偵查機關就所搜索範圍過於概括而失去令狀限定搜索範圍的合法性控制功能（本文貳、三)。

三、至於就數位證據的證據評價，依照數位證據所涉及的面向，可以分成同一性問題、證據使用禁止問題、傳聞問題。同一性問題有賴於法院透過驗真程序來擔保數位證據與原件具有同一性及真實性、證據使用禁止由於現行法多數證據取得方式均受禁止，然應注意即便合法取得之數位證據，亦可能從過度干預基本權、公正程序請求權或者牴觸法治國原則而應得出證據使用禁止之評價。傳聞證據部分，應區分數位證據與待證事實的關聯性來決定，學說建議以電腦產生記錄及電腦儲存紀錄作為區分方式固然多數情況下可採，然涉及紀錄製作者的思想

136 張明偉，同前註 130，頁 43-44。

137 是否能夠類推適用現行傳聞例外之規定，本文持保留看法，關於傳聞例外得否類推適用之爭議，參見薛智仁，同前註 36，頁 38-40；李佳玟 (2014)，境外或跨境刑事案件中的境外證人供述證據：最高法院近十年來相關判決之評釋，臺大法學論叢 ，43 卷 2 期 ，頁 502-507。

表達時，仍有必要藉由詰問紀錄製作者來擔保被告對質詰問權。

有鑑於現行法確有不足，將來立法時應以基本權干預項目、法律保留密度、法官保留即令狀原則、權利救濟等幾個面向作為切入核心，由於數位偵查手段具有高度干預個人隱私及私人領域的效果，絕對不亞於傳統強制處分，因此進行縝密的授權絕對有其必要，又如新型態的傳聞型態，亦不宜未立法前比附援引現行法規定。另外，上述干預不宜採取概括授權偵查官員進行或判斷是否進行科技偵查作為，應具體規範其發動要件及合法性調控機制。

就此而言，科技偵查法草案固然試圖賦予現行檢警在若干偵查技術上奧援，然而多數的科技偵查手段，如前所述，僅採取檢察官保留或區分其基本權干預強弱而採取弱版本的法官保留的立法設計模式，似乎未能顧及所干預基本權的強度及綜效，以及令狀主義對於偵查權的監督及制衡，仍有必要深入檢討各該草案規定的調控機制。

最後，作為生活在網路、數位時代的人，遍布於數位的足跡難以抹去而持續遭到紀錄、監測。在言必大數據（Big Data）的當前，透過雲端運算所建立的人類行為模式與軌跡，早已作為無孔不入的社會監控形式之一[138]，私人企業對於個人資訊蒐集及掌握相較於國家也已不遑多讓，此外，無論是社群媒體、自媒體如刨根式的關注[139]，或者是直截了當、遍布大街小巷的監視錄影，更是稀鬆平常但卻存有未受公眾深入關注的隱私疑慮。當我們想著 Orwell 已經略顯過時的老大哥隱喻或是源於 Foucault 的全景敞視監控（Panoptic Surveilance）[140]，參與網路生活的當下已經決定了日常相互監控（Synopticon）[141]、甚至是浮動且流動的監控（Liquid Surveillance）[142] 的不可逆形勢，如果看著四處攢動的揭弊者及爆料[143]、各種不同電子監控推陳

138 近期關於大數據監控與刑事偵查的關聯性，可參考 Anders, Die Privatsphäre im Zeitalter von Big Data, ZIS. 2/2020, S. 70ff.（2020）.
Zum staatsanwaltschaftlichen Zugriff auf personenbezogene Daten in Speichern privater Dritter

139 BAUMAN &LYON, LIQUID SURVEILLANCE: A CONVERSATION 10-11（2013）

140 BAUMAN &LYON, *supra* note 139, at 15-16.

141 Mathiesen, *The Viewer Society: Michel Foucault's `Panopticon' Revisited*, 1 THEORETICAL CRIMINOLOGY 215, 218-219（1997）

142 BAUMAN/LYON, *supra* note 139, at 17-18.

143 指出如立法創設揭弊者保護法可能產生的日常監控疑慮，參見許恒達（2016），揭弊者保護法的刑事政策省思，收於：貪污犯罪的刑法抗制，頁 310-318。

出新，匿名性已經不是被監控者的護身符，而係監控者得為利用的手段，同時也隨著社群媒體的興起而有湮沒之勢[144]，人們是否還能保留最後一吋不受刺探的場域，便值得懷疑。有鑒於此，那麼國家化身成相互監控者的一員，而參與日常生活，將新型態的基本權干預措施作為干預手段[145]，而鞏固社會控制網路及機制前，縱使對於犯罪追訴、公共安全甚且是防治疫情等重要公共利益，激起人們對於監控機制高度信賴跟讚賞，引頸期盼，沛然莫之能禦，然而除隱私權、資安基本權、私人核心領域乃至於被遺忘權等規範論述外，如何保有人們對監控機制的抵抗工具[146]，值得繼續躊躇、思考及掙扎。

陸、參考文獻

一、中文文獻

王士帆（2017），網路之刑事追訴－科技與法律的較勁，政大法學評論，145 期，頁 339-390。

王士帆（2019），當科技偵查駭入語音助理——刑事訴訟準備好了嗎？，臺北大學法學論叢，112 期，頁 191-242。

王兆鵬（1999），證據排除法則的相關問題，刑事法雜誌，43 卷 3 期，頁 17-48。

王兆鵬（2003），重新定義高科技時代下的搜索，月旦法學雜誌，93 期，頁 166-182。

王勁力（2010），論我國高科技犯罪與偵查——數位證據鑑識相關法制問題探究，科技法律透析，3 期，頁 1-34。

王銘勇（2003），網路犯罪之搜索與扣押，法學叢刊，191 期，頁 45-62。

何賴傑（2012），論德國刑事程序「線上搜索」與涉及電子郵件之強制處分，月旦法學雜誌，208 期，頁 230-244。

吳巡龍（2004），私人不法取得證據應否證據排除——兼評最高法院九十二年度台上字第二六七七號判決，月旦法學雜誌，108 期，頁 223-235。

吳冠霆（2011），由嚴格證明法則論數位證據及影音證據於刑事訴訟法上之處理，司法新聲，101 期，頁 75-86。

---

144 BAUMAN/LYON, *supra* note 139, at 24-25.

145 甚且增訂第三人資料提出義務（Editionspflicht）來取得私人監控所得之資料，相關討論，vgl. Anders,（Fn. 138）, S. 72.

146 相同看法，參見范耕維，同前註 38，頁 188。

吳秋宏（2012），照相錄影與刑事程序，臺北：承法。
吳燦（2018），勘驗筆錄之證據能力，月旦法學教室，188 期，頁 25-28。
吳燦（2020），科技偵查蒐證之授權依據及證據能力——以警察裝置 GPS 偵查為例，檢察新論，27 期，頁 149-168。
李佳玟（2014），境外或跨境刑事案件中的境外證人供述證據：最高法院近十年來相關判決之評釋 ，臺大法學論叢，43 卷 2 期，頁 489-548。
李榮耕（2012），電磁紀錄搜索和扣押，臺大法學論叢，41 卷 3 期，頁 1055-1116。
李榮耕（2014），刑事審判程序中數位證據的證據能力——以傳聞法則及驗真程序為主，臺北大學法學論叢，91 期，頁 169-211。
李榮耕（2015），科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展，臺大法學論叢，44 卷 3 期，頁 871-969。
李榮耕（2018），初探遠端電腦搜索，東吳法律學報，29 卷 3 期，頁 49-87。
李榮耕（2019），通訊監察所得對話內容及傳聞法則，月旦法學教室，203 期，頁 21-23。
李榮耕（2020），與談意見（一）：科技偵查法立法之可行性評估及建議方向，檢察新論，27 期，頁 181-186。
林鈺雄（2007），干預保留與門檻理論——司法警察（官）一般調查權限，政大法學評論，96 期，頁 189-232。
法思齊（2011），美國法上數位證據之取得與保存，東吳法律學報，22 卷 3 期，頁 95-147。
施育傑（2017），數位證據的載體、雲端與線上取證——搜索扣押與類型化的觀點，月旦裁判時報，64 期，頁 55-71。
施育傑（2019），「資安基本權」之研究——以「線上搜索」為核心，世新法學，12 卷 2 號，頁 343-416。
范耕維（2019），現行法下 GPS 追蹤定位偵查行為之合法性與立法方向——比較法觀點與最高法院 106 年度臺上字第 3788 號判決之考察，政大法學評論，157 期，頁 109-197。
涂俊偉（2012），建構刑事 DNA 資料庫之合理界限，法學新論，35 期，頁 157-182。
張明偉（2018）電子證據之傳聞疑義，東吳法律學報，29 卷 3 期，頁 29-48。
許恒達（2010），通訊隱私與刑法規制——論「通訊保障及監察法」的刑事責任，東吳法律學報，21 卷 3 期，頁 109-159。

許恒達（2016），貪污犯罪的刑法抗制，臺北：元照。
陳運財（2004），違法證據排除法則之回顧與展望，月旦法學雜誌，113 期，頁 27-50。
陳運財（2016），GPS 監控位置資訊的法定程序，台灣法學雜誌，293 期，頁 59-74。
溫祖德（2020），調取歷史性行動電話基地台位置資訊之令狀原則 ── 自美國 Carpenter 案之觀察，月旦法學雜誌，297 期，頁 130-147。
劉芳伶（2015），論「對情報扣押」之可能性 ── 一個法益論的新展開，刑事法雜誌，59 卷 3 期，頁 99-126。
劉芳伶（2016），遠距搜索扣押與令狀之明示特定，東海大學法學研究，49 期，頁 45-96。
劉靜怡（2009），DNA 採樣、犯罪預防和人權保障，台灣法學雜誌，124 期，頁 119-123
劉靜怡（2016），監視科技設備與交通違規執法，月旦法學雜誌，248 期，頁 73-84。
薛智仁（2011），禁止國家使用私人違法取得證據之理論基礎，政大法學評論，121 期，頁 53-105。
薛智仁（2014），司法警察之偵查概括條款？ ── 評最高法院一〇二年度台上字第三五二二號判決，月旦法學雜誌，235 期，頁 241-254。
薛智仁（2018），刑事程序法定原則，月旦刑事法評論，11 期，頁 20-44。
薛智仁（2020），論拒絕證言權對於取證強制處分之限制：以親屬與業務拒絕證言權為例，臺大法學論叢，49 卷 2 期，頁 711-778。
蘇凱平（2020），數位證據在刑事訴訟中性質與應用，月旦裁判時報，93 期，頁 61-69。

二、日文文獻

井上正仁（2014），強制捜査と任意捜査，新版，東京：有斐閣。
稲谷龍彦（2017），刑事手続におけるプライバシー保護 – 熟議による適正手続の実現を目指して –，東京：弘文堂。
大野正博（2001），現代型捜査とその規制，東京：成文堂。

三、英文文獻

Bauman, Z. & Lyon, L.（2013）. *Liquid Surveillance: A Conversation*. Malden: Polity Press.
Casey, E.（2011）. *Digital evidence and computer crime: Forensic Science, Computers and the Internet*（3nd ed.）. London: Academic Press.
Kerr, O. S.（2005）. Searches and Seizures in a Digital World. *Harvard Law Review*, 119

（2）, 531-585.

Mathiesen, T.（1997）. The Viewer Society Michel Foucault's `Panopticon' Revisited, *Theoretical Criminology* 1, 215-234.

四、德文文獻

Anders, R.-F.,（2020）. Die Privatsphäre im Zeitalter von Big Data. *Zeitschrift für Internationale Strafrechtsdogmatik. 2/2020*. 70-78.

Bantlin, F.（2019）. Grundrechtsschutz bei Telekommunikationsüberwachung und Online-Durchsuchung, *Juristische Schulung, 2019*, 669-673.

Beulke, W./Swoboda,S.（2018）. *Strafprozessrecht*（14. Aufl.）. Heldelberg: C. F. Müller.

Eisenberg, U.（2017）. *Beweisrecht der StPO*（10. Aufl.）. München: C.H. Beck.

Großmann, S. Zur repressiven Online-Durchsuchung, *Goltdammer´s Archiv für Strafrecht 2018*, 439-456.

Heinson, D.（2015）. *IT-Forensik: Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen.* Tübingen: Mohr Siebeck.

Momsen, C.（2015）. Zum Umgang mit digitalen Beweismitteln im Strafprozess. In: C. Fahl / E. Müller / H. Satzger / S. Swoboda（Hrsg.）, *Ein menschengerechtes Strafrecht als Lebensaufgabe : Festschrift für Werner Beulke zum 70. Geburtstag*（S. 871-887）. Heidelberg: C.F. Müller.

Rottmeier, C./ Eckel, P.（2020）. Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren. *Neue Zeitschrift für Strafrecht, 2020*, 193-200.

Singelnstein, T.（2012）. Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co. *Neue Zeitschrift für Strafrecht, 2012*, 593-606.

Singelnstein, T.（2014）. Bildaufnahmen, Orten, Abhören – Entwicklungen und Streitfragen beim Einsatz technischer Mittel zur Strafverfolgung, *Neue Zeitschrift für Strafrecht, 2014*, 305-311.

Ziemann, S.（2018）. Strafprozessualer Eingriff und Gesetzesbindung. Ein Beitrag zur Lehre von der Annexkompetenz im Strafverfahrensrecht. *Zeitschrift für die gesamte Strafrechtswissenschaft, 124*, 762-803.

Zöller, M.（2012）. Heimliche und verdeckte Ermittlungsmaßnahmen im Strafverfahren. *Zeitschrift für die gesamte Strafrechtswissenschaft, 124*, 411-439.