中央警察大學法律學研究所

碩士論文

指導教授：吳耀宗 博士

WU,YAO-ZONG

科技定位技術偵查之立法研究

A Legal Study On Using Positioning And Tracking Technology In Criminal Investigation

研究生：李欣儀

LI,HSIN-YI

中華民國 111 年 8 月

謝誌

時光荏苒，回首校園時光，充滿無盡感觸與感恩。在職場工作多年，機械式的處理各種刑事案件和突發狀況，或有經驗傳承，或有瞎子摸象，在實務面臨困境下，總希望能找尋適切的法律基礎與邏輯思維脈絡解決問題，因而進入法律所學習。進入警大後，有幸遇到導師吳耀宗老師，對於不是法律本科出身的我，學習是充滿挫折的，老師總能循循善誘，以幽默口吻給予明確方向和指引，讓我省思也重建僵化的既有的邏輯思考，受益良多，感謝老師辛苦的付出與指導；非常感謝口試委員楊雲驊老師及葉雲虎老師，在撰寫論文過程，不吝指導給我許多實質建議，並且以更深更廣的方向思索，讓論文能夠更加完整。

特別感謝好戰友景嘉、彥嘉的一路相挺，有你們共同學習前行，論文才能完成，還有研究所的好夥伴軒耀、博文、士恆、昭毅、映玎，以及韻慈、小璇，每每在工作與學習兩頭燒，感到疲勞與沮喪時給予陪伴鼓勵。感謝刑事局的長官、三隊同事的包容與幫忙，支持我完成學業並給予我強大後援。

最後，想感謝我親愛的父母，總提醒我要好好認真完成想做的事情，不可以半途而廢。研究所的時光，比想像中的辛苦，也比想像中的快樂，感謝身邊每一份善意與支持，給予我努力前行的勇氣。

李欣儀 謹誌

2022 年 8 月

摘要

隨著科技發展及犯罪型態的改變，偵查人員仰賴各種新型態科技定位技術追蹤調查，在此背景下，引發使用科技定位技術偵查，造成干預隱私權等基本權之疑慮。找人，是犯罪偵查初始，也是刑事案件的基礎。使用科技定位技術偵查不僅是經濟成本考量，更重要的是面臨各種新型態犯罪，是與犯罪者相抗衡的唯一解決之道，在立法上是必須且迫切要面對的課題。

本文臚列我國實務使用之科技定位技術偵查工具，以介紹該項技術之原理、功能及偵查上運用做為開端，進一步討論使用科技定位技術偵查可能干預之基本權，並試圖在我國法尋找可能法源。在科技定位技術偵查探討，其一，是使用該技術涉及的基本權干預，包含獲取資訊的質與量不同，討論何界定合理期待隱私界線，及使用時間長短所造成之圖像效果。其二，是在強制處分令狀原則下，使用該項技術之發動門檻及層級化授權，及實施該項技術的要件、程序及相關法律規範。

在我國，科技定位技術偵查尚無明確之法律授權基礎，109 年 9 月 8 日科技偵查法草案推出後，雖受到重視引發關注討論，惟目前仍在研議。本文以觀察美國法及德國法之文獻作為立法借鏡，於文末提出立法建議，以期能對我國科技定位技術偵查法律規範盡一份心力。在科技發展與保障人權的權衡，立法才能有效保障人權，期盼科技偵查法草案的推出是及時雨而不是曇花一現，能使執法人員執法有據，落實人權保障。

關鍵字：隱私權、科技定位偵查、全球定位系統、M 化偵查、長期監視

Absract

Scientific methods to criminal investigation are inextricably linked to technology development and crime patterns.The lack of awareness raises concerns about the interference of fundamental rights, such as privacy rights, under the use of scientific and technological investigations.We use scientific and technological investigations not only for economic considerations, but also it's the only solution to fend off criminals. It becomes a vital issue in legislation. We eager to find the source of the law, and then comparing the content of the draft law of science and technology investigation of the Ministry of Justice with the German and American documents and current norms, and put forward legislative suggestions.

In the exploration of scientific and technological positioning and investigation, first of all, the fundamental rights intervention involved in the use of technology, including the difference in time, quality and quantity. With the evolution of human rights protection, how to define reasonable expectations of privacy and the image effect caused by the length of time becomes vital.Furthermore, under the principle of criminal pleadings, the threshold and hierarchical authorization for using the technology, as well as the requirements, procedures and relevant legal norms for the implementation of the technology.

This essay argues that only legislation can effectively protect human rights, and looking forward to the introduction of the draft science and technology investigation law to enable law enforcement officers to

enforce the law and protect human rights.

Keywords: privacy right, right to informational self-determination, technology positioning and investigation, global positioning system, Mobility Location Tracking System, long-term surveillance

科技定位技術偵查之立法研究

目錄

第一章　緒論

第一節　研究動機與目的

科技改變生活的型態，這已經不是標語，而是每天在我們生活周遭發生的事實。即將邁入 5G 社會，科技徹底改變我們的生活，以我們有能力消費的方式如影隨形在生活的枝微末節，例如我們的交易方式，從現金變成電子錢包、虛擬貨幣區塊鍊；我們的聯繫方式，從面對面，到社群媒體、網路電話、衛星電話；我們的教育方式，從進入校園，到視訊教學及網路大學，各種例子不勝枚舉。因應科技發展，各種智慧 AI 產品也因應而生，如人臉辨識、空拍機、網路電話、GPS 定位技術、雲端儲存空間等等，應用在各行各業，且藉由不同管道開發創新，社會正在面臨極大的轉變。刑事訴訟法之目的，乃為發現實體真實、恪遵法治程序以及維護法安定性，以職司偵查犯罪的司法警察角度觀之，現下警察工作面對的挑戰更為嚴峻，傳統跟監蒐證及通訊監察之方式，在科技技術不斷更新下，已不敷偵查人員使用且不符執法成本，且在現行刑事訴訟法、通訊保障及監察法及警察職權行使法之範疇，似難有對於附隨於載體之電子訊號或網路連線產生之資訊，給予明確的法律授權依據。

犯罪偵查的目的，在於搜尋、保全利於與不利於被告的證據，以求能發現真實。在偵查過程中，找人，是偵查的基礎工作，偵查人員必須從跟監、靜態資料、物證等蒐集及調查犯罪證據。在科技時代下，傳統偵查手段追蹤位置或蒐集犯罪資訊方法，已不敷應對各種新型態犯罪。為此，執法機關基於武器對等，研發應用科技產品，作為科技定位技術偵查使用，雖解決燃眉之急，惟因欠缺授權基礎，屢遭抨擊濫權。

有關科技定位技術，實務常見有手機基地臺定位、M 化偵查網路系

統定位、全球定位系統定位、WIFI 定位及藍芽定位等。本文首先討論各項技術原理及偵查實務應用現況，以及分別可能干預的基本權範疇。在合憲性討論，科技定位技術偵查所蒐集的資訊，是附隨於載體之訊號，本質上非屬通訊內容，較可能干預的是憲法保障之隱私權、資訊自決權及人格權，惟在我國刑事訴訟法、通訊保障及監察法、警察職權行使法、電信管理法、個人資料保護法等相關法律規範中，並沒有足夠的法律授權基礎。

103 年海巡署王姓士官長為查緝私菸將全球定位系統裝設於車輛底盤，判處妨害祕密罪定讞後（最高法院 106 年度臺上字第 3788 號刑事判決參照[1]），107 年法務部曾嘗試將 GPS 偵查法制化於通訊保障及監察法內，惟因採取檢察官許可，過於側重偵查便利性遭到抨擊。108 年立法院委員爰擬具「刑事訴訟法」增訂部分條文草案，在搜索扣押章節下增訂第十一章之一「全球定位追蹤監察程序」，列為強制處分一種，採法官保留原則，然而法案立法意見未形成共識而石沉大海。106 年臺北市政府警察局偵辦詐欺機房案，使用 M 化偵查網路系統偵測詐騙門號訊號位置，第一審法院判決使用 M 化偵查網路系統無法律授權，直接取得之證據無證據能力（桃園地方法院 106 年度易字第 164 號刑事判決參照）。在第二審法院，高等法院以訊號偵測無顯示隱私內容，且僅為限縮警方已知範圍為由，基於公益的合理權衡，依刑事訴訟法第 158 條之 4，認具有證據能力（高等法院 109 年度上易字第 1683 號刑事判決參照）。接續在 109 年 9 月 8 日，法務部推出科技偵查法草案，惟因發動門檻過低、公告期程僅 5 日、法官保留原則不足等討論聲浪，因此草案目前仍在法

[1] 按民國 111 年 6 月 22 日修正法院組織法第 57-1 條，最高法院於中華民國 107 年 12 月 7 日本法修正施行前依法選編之判例，若無裁判全文可資查考者，應停止適用。未經前項規定停止適用之判例，其效力與未經選編為判例之最高法院裁判相同。

務部研議，懸而未決。科技定位技術偵查並非我國首創，本文以美國及德國文獻及現行規範為例，提出我國科技定位技術偵查立法建議，希冀能在兼顧科技執法及人權保障下，盡一份心力。

第二節　研究方法與範圍

行政院法務部 109 年 9 月 8 日公告「科技偵查法」草案[2]，內容共計 7 章節 28 條，並將「科技定位技術」以非隱私空間(第 3 條)、以空中技術設備為之(第 4 條)、全球定位系統及相類設備(第 5-8 條)，以及隱私空間的非侵入性調查(第 9-13 條)規範。草案公告後引發爭議理由，除制定程序未經討論過於倉促，侵害基本權之規範是否符合層級化之法官保留原則，另者主張對於此種技術應以「功能」會造成何種基本權侵害、時間長短、質與量之區別等，以類型化區分規範之內容，以因應科技變遷之根本之道。雖法務部提出草案後，受到負面評價多於正面，然筆者認為此舉應給予掌聲，其因在於將科技技術應用於犯罪偵查，是時勢所趨、行之有年，甚可說是未來之課題，如不及早充分討論並將科技偵查技術法制化，終究是鴕鳥心態，且無法令規範，便難以避免國家機器，若假藉偵查之名行濫權之實情形發生，亦使執法人員無所適從。

有關「科技定位技術偵查」，應可自手機普及後，偵查機關以基地臺定位功能之「即時定位」功能談起，而後衍生出手機基地臺定位、M 化偵查網路系統定位、全球定位系統定位、WIFI 定位及藍芽定位等技術。值得注意的是，科技定位科技術在文義解釋上雖都是「定位」功能，但在使用之原理、功能、方法、程序等，均有所差異，以致存在法律審查

[2]-法務部全球資訊網官方網站業務公告，2020 年 9 月 8 日， https://www.moj.gov.tw/，(最後瀏覽日：2021 年 1 月 2 日)。

漏洞，亟待立法者補足。

本文討論之「科技定位技術偵查」，係筆者以警察機關偵查犯罪及急難救助之角度論述，然除警察機關外，我國偵查各類犯罪之分工，有國安局、調查局、憲兵隊、海巡署、移民署等機關，因分屬不同執掌及法令規範，且使用之技術不盡相同，故本文未臚列分述討論。本文研究方法以「文獻分析法」及「比較法」，盡可能蒐集我國論文、期刊、專書及研討會等文獻及實務判決案例，提出爭議看法及立法評估，並以美國及德國學說、文獻、判決及法制作為參考，以釐清思路，期能從中探討科技定位技術偵查之發展軌跡，作為我國日後科技定位技術偵查之修法建議。

第二章　科技定位技術偵查

第一節　概論

科技定位技術在生活中應用範圍相當廣泛，在商業領域亦蓬勃發展，例如失智老人照護、山難救助、車隊管理、失竊手機定位、監控犯人電子腳鐐、居家疫情定位，應用功能不計其數，可知定位技術在日常生活之重要性已不容忽視。定位技術應用在犯罪偵查，常見形式的有影像聲音及位置資訊，前者如空拍機、雲龍系統，後者如全球衛星定位系統、基地臺定位等，本文僅以位置資訊為核心討論。科技定位技術應用犯罪偵查起始，可自手機通話之定位功能談起。1993 年美國一位女孩遭綁架後殺害，在過程曾使用行動電話撥打 911 就，但當時 911 中心無法通過行動電話信號確認位置，有鑑於此，1996 年美國聯邦傳播委員會(Federal Communication Commision , FCC)[3]要求移動電信系統業者為行動電話使用者提供緊急救助服務，即提供呼叫者位置以及時救援，此法令被名為 Enhanced 911(E911)。在歐洲，2003 年歐盟執行委員會(EU Commision)通過 Enhanced 112(E112)法令，採行類似 E911 的規定要求每個會員國的行動電話廠商，必須強化緊急救援電話的自動定位功能。自此，各國開始要求移動電信系統業者必須建置設備保留、存儲提供發受話者位置之義務。隨著科演進技發展，智慧型手機的普及，GPS 系統、網路通話及通訊軟體附載成為手機內的標準配備，衛星定位及網路定位偵查技術應運而生，科技定位技術成為犯罪偵查之趨勢。

[3] 美國聯邦通訊委員會(Federal Communications Commission)是聯邦通訊委員會通過廣播、電視、衛星和電纜在所有州、哥倫比亞特區和美國領土內監管州際和國際通訊。該委員會是受國會監督的獨立美國政府機構，是負責實施和執行美國通信法律法規的聯邦機構。

第二節 基地臺定位

第一項 原理

在 1940 年代末期，美國的貝爾實驗室提出蜂巢式(cellular)的觀念，1959 年美國摩托羅拉公司推出世界上第 1 支蜂巢式行動電話(Dyda TAC 8000X)[4]，將服務的範圍分成數個小區域，並在每個區域中使用不同的無線電頻率，蜂巢式行動電話的基地臺電磁波強度範圍會互相重疊，並被設計成以兩個基地臺的電磁波強度範圍的交疊區中線為基準，超過中線的部分將歸另一個基地臺所管轄。於此，若將一個基地臺與其鄰近的基地臺交疊範圍中線進行連接後，該基地臺涵蓋的範圍就會成為六角形，稱為一個細胞(Cell)，若再將所有的基地臺中線交疊起來，則會成為一個跟蜜蜂蜂巢形狀一樣的通訊網路，所以被稱為蜂巢式行動電話(Cellulae Phone 或 Cell Phone)。在分布蜂巢的時候，蜂巢與蜂巢間不能夠有空隙，因為凡是蜂巢沒有覆蓋的區域就沒有基地臺提供服務，代表無法通訊。[5]行動通訊定位，係利用行動電話通訊時，發射的無線電與行動通訊的基地臺而為之定位技術，屬二度空間定位，申言之，行動電話於待機狀態時，每 7 秒會自動搜尋訊號最強之基地臺，以利通訊時能在最佳的品質下進行，而搜尋到能提供最佳訊號之基地臺時，行動電話則會自動傳送使用者門號(即 IMSI， SIM 卡識別碼)與該行動電話獨有的序號(即 IMEI，手機序號)[6]，此時，可以透過基地臺接收之門號或行

---

[4]全球首款手機誕生 45 年，蘋果日報財經新聞，
https://tw.appledaily.com/property/20180402/
TIUSSDJRSCMJD74AH3CISWVBLM/ (最後瀏覽日期：2020 年 12 月 29 日)

[5]曾德文著、呂明都編審，資通科技犯罪偵查通訊篇，初版，2013 年 8 月，頁 33。

[6] IMEI(International Mobile Equipment Identity)是移動設備國際身份碼的縮寫，具有唯一性，是用來標識手機的 15 位數字，其中前 6 位數(TAC，Type Approval Code)是「型號核准號

動電話序號，又依此分為兩類[7]：一為利用基地臺記錄「行動電話門號」，知悉該「門號」的使用位置，稱為行動電話基地臺分析；二為以「行動電話序號分析」知悉並鎖定使用該行動電話之位置，稱為行動電話序號清查，如該使用者使用到某個基地臺，即可觀察行動電話與多個基地臺的訊號強度，推估與行動電話的距離。行動電話定位技術泛指利用相關訊號的量測來估測手機用戶之空間坐標位置，透過無線基地臺的相關量測資訊來進行手機定位的方法有多種，例如：細胞識別法（Cell-ID）、訊號到達時間法（TOA）、訊號到達時間差法（TDOA）、增強型觀測時間差法（E-OTD）、時間提前法（TA）、訊號到達角度法（AOA）、資料庫相關法（DCM）、訊號接收強度法（RSS）以及混合法（Hybrid）[8]。

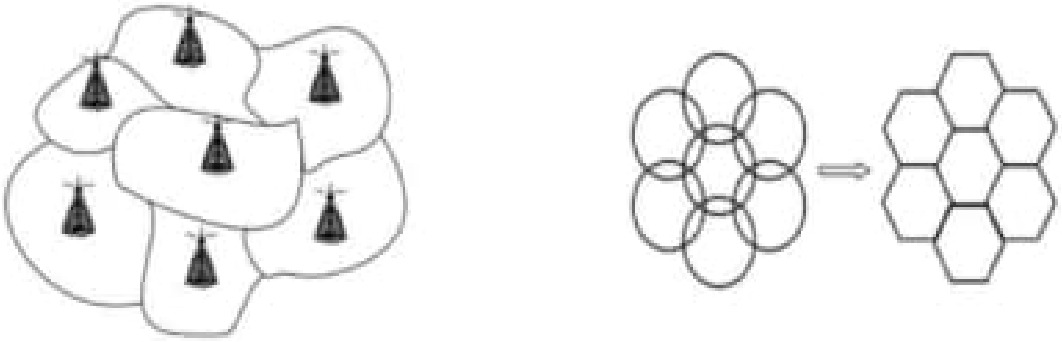


圖 1　實際上涵蓋範圍與理論上蜂巢式基地臺[9]

碼」，一般代表機型。接著的 2 位數(FAC，Final Assembly Code)是「最後裝配號」，一般代表產地。之後的 6 位數(SNR)是「串號」，一般代表生產順序號。最後 1 位數通常是 0，為檢驗碼。IMSI（International Mobile SubscriberIdentification Number）是國際移動用戶識別碼，區別移動用戶的標誌，儲存在 SIM 卡中，是為了在移動通信網上正確地識別某個移動用戶，就必須給用戶分配一個特定的識別碼。

[7]黃清德，科技定位追蹤監視與基本人權保障，初版，2011 年 11 月，頁 91-92。

[8]吳世琳、張自強、葉禹良、許冠傑，無線網路定位技術應用於即時救援，臺灣職能治療研究與實務雜誌，4 卷 2 期，2008 年 12 月，頁 140；朱翊雯，結合 TOA 及 AOA 混合式定位技術於地面無線定位之應用，成功大學電機工程學系碩士論文，2015 年 1 月，頁 139-140。

[9] 引自蜂巢式網路概念，https://images.app.goo.gl/yWCtPnudySi46zBc6 (最後瀏覽日期：2021

第二項　功能及偵查上運用

行動通訊定位在犯罪偵查的應用上有「通信紀錄」[10]和「即時定位」，分別被規範於通訊保障及監察法和電信法，以時間軸區分，前者係指已發生過去之發受話之通信紀錄，後者是對於特定單一對象之未來位置資訊。通信紀錄調取法源依據為通訊保障及監察法，依循重罪原則及相對法官保留原則有不同的聲請調取層級，在犯罪偵查的所得內容，有單向通聯、雙向通聯、通話時間秒數、基地臺位置、使用手機序號等，偵查機關可用以研判犯罪者共犯身分、作息活動及接觸對象軌跡等資訊，亦為提交法院判決之重要證據。但通信紀錄在網際網路及通訊軟體盛行後，犯罪者亦知悉使用語音通話會暴露行蹤，故轉而使用網路電話(VOIP)功能，傳統通信紀錄調閱及定位在犯罪偵查應用已漸不敷使用。

即時基地臺位置資訊(CSLI)是行動電話在蜂巢式網路運作過程中所可能產生之各種手機定位資訊[11]，依據電信法第 25 條作為法源基礎，僅能針對天然災害、急難救助、國家安全或公共利益，始得為之，也就是說犯罪偵查並不屬於容許調閱手機「即時定位」之範疇。於實務上常見使用即時定位需求，大多以通報自殺、緊急危難或重大災害等緊急案件。2019 年全球爆發 COVID-19 疫情，為避免疫情擴大傳染，各國開始追蹤居家隔離民眾之活動軌跡，並蒐集染疫民眾之接觸史，我國「染疫者足跡通報」即為細胞臺定位之應用，一旦出現確診者，與確診者在一定期間內基地臺收發訊號重疊之手機門號持用者，便會收到通知有重疊

年 1 月 1 日)

[10]電話通聯紀錄係電信業者為了核算客戶帳務，而對客戶電話發、受話的紀錄。詹明華、邱紹洲、易序忠，通聯紀錄在犯罪偵查上之應用－行動電話持機人之動態與靜態分析，警學叢刊第 33 卷第 2 期，2002 年 1 月，頁 111-131。

[11]黃政龍，新型態科技偵查作為之法規範研究，中央警察大學警察政策所博士論文，頁 265。

足跡之相關健康提醒指引。在我國，疫情爆發後返臺民眾須遵守居家檢疫，為避免民眾不遵守居家隔離造成防疫破口，政府提供防疫手機要求居家隔離民眾攜帶防疫手機，一旦監控者離開居家隔離範圍疾病管制署便會發出警報，通報警政單位及鄰里長前往民眾家中查訪，之後隨著防疫手機數量不足，便納入一般居家隔離民眾之手機號碼做為監控，電子圍籬系統防疫追蹤系統因應而生，利用原有的基地臺的細胞識別法（Cell-ID）定位技術，築一道電子防疫城牆。[12]疫情期間另有發布疫情足跡之細胞簡訊功能，原理與此相同。[13]

然而，即時定位調閱必須要有法律授權，此種監控基於傳染病防治法及個人資料保護法授權依據，雖經疾病管制署聲明蒐集之資料僅有手機號碼及活動範圍警示，沒有持有手機者之個人資料，但因缺乏外部監督及審查機制，是否有侵害隱私權之虞，亦引發討論。[14]

第三項　干預基本權及現行法源依據

按司法院釋字第 631 號解釋：「憲法第 12 條規定，人民有秘密通訊之自由」，旨在確保人民就通訊之有無、對象、時間、方式及內容等

---

[12]黃彥棻，科技抗疫實例電子圍籬系統有助落實居家檢疫，https://www.ithome.com.tw/news/137939(最後瀏覽日期：2020 年 12 月 25 日)；鍾張涵，以色列稱讚、美國想合作揭密台灣科技防疫國家隊。https://www.cw.com.tw/article/5099449?template=transformers。細胞台技術即手機插入 SIM 卡開機後，會主動搜索周圍數個基地台，選出距離最近、信號最強的基地台作為通信基地台。因此，透過三個基地台連線距離手機的距離，就能三角定位，算出你手機的位置。在防疫期間，被列管者的手機已被登記只能出現在哪些基地台範圍內（電子圍籬），一離開相關區域，警方、疾管署都會收到電信基地台自動發的通知，就像出國時會自動跳出該國漫遊簡訊一樣。可視為手機追蹤定位與電子圍籬示警之結合應用。(最後瀏覽日期：2021 年 1 月 1 日)

[13]簡宏偉、吳麗芬、洪振耀、劉倢旻、吳卓葳、林瑜，大數據運用與隱私保護－手機定位資訊於防疫應用之法律問題研析，國土及治理季刊，第八卷第三期，109 年 9 月，頁 64-75。

[14]邱文聰，科技防疫與個人資料保護，「法治國之科技偵查與科技防」研討會，2020 年 10 月 23 日。

事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利」。由此可知，秘密通訊自由涉及憲法人格權、隱私權、資料自決權等重要基本權。

又按最高法院 106 年度台非字第 259 號判決理由書：「通訊隱私權保護之主要緣由，乃通訊涉及兩個以上參與人，意欲以秘密之方式或狀態，透過介質或媒體，傳遞或交換不欲為他人所得知之訊息。因其已脫離參與人得控制之範圍，特別容易受國家或他人之干預與侵擾，有特別保護之必要，故其保障重在通訊之過程。」意即，通訊本質乃「兩人以上之特定人間的意思交換」，若非兩個以上參與人意思交換，雖非「通訊隱私權」，亦能主張一般隱私權所保障之對象。換言之，不論是通信紀錄或是即時定位，都並非「通訊」，但涉及的仍有人格權、隱私權、資料自決權之問題。另依個人資料保護法第 2 條第 1 款：「個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」法條雖未直接規範手機號碼或位置資訊，然從法院見解[15]及函釋[16]意旨，手機號碼應認為是可直接或間接識別之個人

[15] 高等法院臺南分院 105 年度上易字第 393 號刑事判決，於網路聊天室公布他人電話致網友取得後撥打騷擾相約其性交案，判決認為行動電話號碼當下，該號碼乍看之下僅為一連串之數字，然該特定人自得藉由行動電話號碼由群體中予以區別，是該資料在群體中顯然對於某特定人具有專屬性、獨特性，換言之，於取得號碼之人撥打該號碼之時，即得直接與行動電話號碼之持有人相聯繫，除非持有人將行動電話關機或變更號碼，否則倘若陌生人持續不間斷地撥打該號碼，該號碼之使用人勢將遭受無止盡之騷擾，其隱私權無疑受有侵害。

[16] 國家發展委員會 107 年 11 月 7 日發法字第 1072002039 號函釋，有關擬將 Google Android 作業系統手機之緊急定位服務（Emergency Location Service, ELS ）之定位資訊與 119 勤務指揮派遣系統介接，涉及個人資料保護法之適法性，認為定位資訊系屬個人資料保護法第 15 條規定第 1 款，公務機關對個人資料之蒐集或處理，依法定執行職務。

資料。因此，手機定位之位置資訊，應屬於個人資料保護法所昭示保障人格權之範疇。

依現行法令，手機即時基地臺定位，不能作為犯罪偵查使用，僅能在電信管理法中尋得法律授權基礎，在重大災變或緊急危難使用，以致於許多重大犯罪(如擄人勒贖、兒少案件)，需要立刻找到犯罪者以保障生命財產安全之案件，卻無法使用該項技術，極其弔詭。即時定位之取得的是手機持有人的現在位置發射訊號，可用以蒐集手機持有人的所在位置基地臺，潛藏干預人民隱私權之可能。公權力運用科技定位措施追蹤監視，即是透過位置資訊的蒐集與處理而追蹤監視特定對象，必然構成侵害個人資訊隱私之疑慮及一般行為自由將受到限制，在處理相關問題上須更為謹慎。[17]然此類附著於科技設備載體之「數位識別碼」訊號，在主觀上是否具備真實隱私期待或保護意識，學說上各持看法。有學者提出修正門檻理論認為，為兼顧現代科技及偵查活動之形成性、多樣性的特性，應承認司法警察(官)之一般調查權限，作為無強制力且質量輕微之資訊干預基礎。論證在於，以刑事訴訟上對自己言語的人格權或資訊自決權為例，已經具體轉化為緘默權、拒絕證言權，並且由於連結了不自證己罪、特殊信賴關係的保護等重要的法治國原則，而與一般人格權及資訊自決權產生了加重的關連性，因此其干預必須具備特別的法律授權基礎。具體的運用結果是，如果警方利用隱性偵查的手法(如線民或臥底警探)，處心積慮刺探被告本身對己之不利陳述，或者有拒絕證言者對被告不利之證詞，屬於實體併合程序基本權的干預，據此，如果欠缺特別的法律授權基礎，構成違法的基本權干預，反之，如果具備特別的法律授權基礎，接下來就是比例原則的檢驗，包括授權基礎本身是

[17]羅翊庭，隱私權與個人位址資訊關係之研究，東海大學公共事務碩士學程在職進修專班碩士論文，2008 年。

否違反比例原則的問題。[18]換言之，如為干預基本權嚴重的偵查作為，應有特別授權依據，但在輕微干預作為，應可以比例原則作為判斷基準即可。也就是說，除已經立法特別授權之干預性偵查措施以外，僅涉及一般人格權或資訊自決權的非強制性干預措施，原則上可以援引一般調查權限作為干預基礎，僅生比例原則之問題。在法律保留原則基礎下，認為應承認司法警察(官)之一般調查權限，作為無強制力且質量輕微之資訊干預基礎。[19]

我國通信紀錄規範於通訊保障及監察法，在 2014 年修法前，犯罪偵查中調閱通信紀錄系依據「電信事業處理有關機關查詢電信通信紀錄實施辦法」，僅須由偵查機關自行審酌通信紀錄之調閱是否符合比例原則即可。在 2014 年修法後，對通信紀錄調閱改採較嚴格的重罪、關聯性原則及令狀原則規定。[20]2014 年修法公布後，在學界中引了批評聲浪，認為通聯紀錄調取的規定，「非輕罪」的案件限制理由不明，且較取通信紀錄干預人民基本權更強烈的羈押、拘提、搜索等強制處分未限定案類限制，何以干預程度較輕微的通信紀錄調取有罪刑責門檻？通信紀錄提升到法官保留的原因及例外的標準不明，何以耗費偵查資源極小、侵害隱私程度極微、但對於事實釐清之功能極大的通信紀調取而須由法官進行審查？[21]在通保法修法後，調閱通信紀錄造成執法機關付出相當大的時間成本，且限定案類及刑度為調閱門檻，使得許多案件在追查和保

[18] 林鈺雄，干預保留與門檻理論－司法警察（官）一般調查權限之理論檢討，政大法學評論第 96 期，2007 年 4 月，頁 189-232。

[19]林鈺雄，干預保留與門檻理論－司法警察（官）一般調查權限之理論檢討，政大法學評論第 96 期，2007 年 4 月，頁 189-232。

[20] 李榮耕，簡評二〇一四新修正的通訊保障及監察法──一次不知所謂何來的修法，月旦法學雜誌第 227 期，2014 年 4 月，頁 165。

[21] 陳重言,刑事追訴目的之通信(通聯)紀錄調取與使用－兼評 2014 年初通保修法,檢察新論第 16 期，2014 年 7 月，頁 50-55。

存證據的程序，造成無法可依據。

綜上，基地臺定位可區分為「通信紀錄」及「即時定位」，前者有授權於通保法，但有限定案類及微罪需法官保留之門檻；後者則不允許使用於犯罪偵查。對比於刑事訴訟法更強烈的羈押、拘提、搜索等強制處分，取得位置資訊，僅是發動強制處分前置必要作為，實質上並無強制力、物理性干預，如此嚴格的規範，令人匪夷所思

第三節　M化偵查網路系統定位

第一項 原理

M化偵查網路系統(Mobility Location Tracking System)[22]，原理是使功率可達範圍內之手機將其視為一虛擬基地臺，藉此令手機向其註冊，並於此同時截取IMEI（手機序號）、IMSI（國際標準識別碼）等資訊後再釋放回正常基地臺，惟該截取資訊僅為系統自行識別使用，並無可供查詢之門號資訊，亦無法連結辨識第三人資料。而運用「M化車」辦案，係將「M化偵查網路系統」裝設於車輛上，由偵查人員將已知之手機識別資訊（如IMSI及IMEI）輸入系統內建立名單，開車繞行於已知之偵蒐範圍內，由系統於偵搜範圍內比對過濾已知目標手機，經由目標手機與系統連線，依連線訊號強弱判定手機位置。另於偵蒐範圍內，無可避免蒐集到第三人註冊於系統內之識別資訊，於系統關閉後即自動清除。[23]我國採購之M化偵查網路系統，係由頻譜分析儀與指向性天線

[22] 依據內政部警政署刑事警察局107年3月20日公告招標標案英譯名稱，廠商名稱怡德視訊股份有限公司(ADE Corporation)、產地以色列、得標金額新臺幣5600萬。

[23]臺灣桃園地方法院 106 年度易字第164號刑事判決，函請內政部警政署刑事警察局說明「M化車」之功能，內政部警政署刑事警察局108年12月13日刑通字第108023155號函覆內容。

所組成，可偽裝成基地臺，蒐集在偽基地臺範圍內的行動電話訊號與資料，再以頻譜分析儀偵測訊號強度，推估與行動電話之距離，再以指向性天線尋找方位，據媒體報導其誤差範圍甚至可縮小至 1 公尺[24]，甚至可以鎖定至特定大樓之房間[25]，以利偵查埋伏與逮捕作業。

使用 M 化偵查網路系統必須要先知悉目標手機的 IMEI（手機序號）與 IMSI（國際標準識別碼）。IMEI 與 IMSI 具有專一性，分別是手機與門號 SIM 卡的身分證，兩者都是 15 碼且為全球通用的專屬對應號碼(倘如雙卡機，則有 2 個 IMEI 碼，若雙卡機插卡 2 張 SIM 卡就會有 2 個 IMSI 碼)。行動虛擬基地臺定位設備，最初是為軍事和情報界開發，而後應用於犯罪偵查，在 2016 年加拿大多倫多大學蒙克國際研究中心研究報告指出，相類似設備有 IMSI catchers、Cell-site Simulators、Digital Analyzers、Cell grabbers、Mobile device identifiers 或 Stingrays[26]，但在廠商與政府簽訂保密合約情況，多難以得知該項科技之全貌。美國聯邦地區法院法官 Smith 曾於一則裁定提到，Cell-site Simulators（有時另稱 Stingrays）利用基地臺資料轉儲之間得差異。雖然兩者均得以在特定地區發掘未知之行動電話號碼及其他識別號碼，但相異處在於：一、行動電話虛擬基地臺是偵查機關自有設備，而不是業者所有。二、行動電話虛擬基的臺所取得者為即時且直接傳送給偵查機關之資訊，而不是溯及既往的調取電信業者之歷史通聯記錄。三、行動電話虛擬基

[24]蘋果日報編輯部，M 化車裝基地臺定位找到藏身地，https://tw.appledaily.com/headline/daily/20150125/36349616(最後瀏覽日：2021 年 12 月 11 日)。

[25]詹明華、陳弘斌、宋奕賢，定位技術在犯罪偵查上之應用，刑事科學，第 80 期，2016 年 3 月，頁 5。

[26]Tamir Israel、Christopher Parsons，加拿大多倫多大學蒙克國際研究中心研究報告，http://www.emsec.rub.de/media/crypto/attachments/files//2011/04/imsi_catcher.pdf.(最後瀏覽日：2021 年 12 月 11 日)。

地臺可以持續地即時追蹤行動電話之移動。[27]

另美國司法部政策說明亦指出，Cell-site Simulators 設備運作如同虛擬基地臺，僅能提供目標電話訊號強度和方向，功能與 GPS 不相同，也不能獲得或下載目標設備的資訊(例如電子郵件、通訊內容、帳號、簡訊、電話等)。在政策內容說明，規範操作此設備專業設備必須受過專業訓練之專責人員，且應聲請核發法院令狀[28]，除司法部例示之緊急情況除外：一、保護生命安全或防止重大傷害必要；二、防止證據行將滅失；三、對逃跑重罪犯為熱追緝 (hot pursuit)[29]；四、防止犯罪嫌疑人或判決有罪確定之逃犯逃逸有重大執法需要之情形。[30] 2001 年 911 事件後，德國為預防恐怖攻擊事件開始將 IMSI Catcher 法制化，在 2002 年德國刑事訴訟法 100i 修訂使用此類設備之法源依據[31]。

第二項 功能及偵查上運用

在功能的理解上，M 化車為一個虛擬基地臺，偵查人員必須事先鎖定對象(犯嫌或被害人)之門號資訊，經偵查人員先依法調閱通聯記錄研

---

[27]黃政龍，新型態科技偵查作為之法規範研究，中央警察大學警察政策所博士論文，頁 297。

[28]美國司法部政策說明，Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators，2015 年 9 月 3 日，https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators。(最後瀏覽日期：2021 年 1 月 2 日)。

[29]王兆鵬，美國刑事訴訟法，2007 年 9 月，頁 231。
熱追緝理論(hot pursuit doctrine)，係指警方所追緝被告或犯罪嫌疑人,在追緝的過程中嫌犯跑進了民宅裡況緊急，警方此時可以無令狀進入住宅內逮捕嫌犯。不受到令狀原則之拘束。換言之,美國聯邦最高法院認為在案發不久於公共場所追被告或犯罪嫌疑人,在追緝的過程中嫌犯跑進了民宅裡，此時符合「即時」追緝嫌犯，客觀上構成情況急迫的要求，可以無令狀進入住宅內逮捕嫌犯。

[30]有關美國 Cell-Site Simulators 介紹，參黃政龍新型態科技偵查作為之法規範研究，中央警察大學警察政策所博士論文，頁 298。

[31]Tamir Israel、Christopher Parsons，加拿大多倫多大學蒙克國際研究中心研究報告，http://www.emsec.rub.de/media/crypto/attachments/files//2011/04/imsi_catcher.pdf. (最後瀏覽日：2021 年 12 月 11 日)。

判分析，確認可能區域後，再與「M 化車」操作人員前往現地周邊勘查，在偵蒐範圍內比對過濾，當比對出現已知目標手機後，使系統和目標手機連線，藉訊號強弱判斷手機位置，相關使用規範則依警政署「執行 M 化定位勤務作業流程」辦理。以偵辦詐欺集團為例，詐欺集團會使用不同的人頭門號撥打詐騙被害人，在詐欺人頭門號撥打給被害人時，需連接鄰近的蜂巢基地臺收發訊號以取得電信服務。因此，偵查機關在知悉犯罪門號後，會先依據通保法調取通信紀錄比對分析蜂巢基地台涵蓋範圍追蹤犯罪者,但實際上各地區的基地臺稠密程度不同(在都市較密集，在鄉野或山上則較為稀缺),因此影響基地臺提供服務的半徑範圍不同，如在偏鄉蜂巢基地臺涵蓋範圍可達 300 公尺至 1 公里，也就是說較難限縮實際犯罪者位置，使用 M 化車偵查即可解決此地理侷限性。在經過分析通信紀錄後，偵查機關會鎖定一定區域半徑，駕駛 M 化車繞行(或背負器材徒步行走)。此時 M 化設備如同虛擬基地臺，因此當越接近目標門號，目標門號誤以為該設備(偽基地臺)是最為接近之基地臺(訊號最強)連結註冊，在偵查人員比對完畢後，則會將偵測目標門號釋放回真正的基地臺。

德國文獻對於設備 IMSI Catcher 的解釋，「為了確保手機用戶隨時享受電信服務，任何手機無論在通訊使用中、處於待機狀態或行動上網時，每隔短暫時間內(大約 2.4 秒)，會反覆向其所在行動電信網路蜂巢區的所屬電信業者基地臺註冊」[32](即 M 化設備操作原理)、「實際上，從 IMSI Catcher 扮演虛擬的行動基地臺開始，無論是否屬於追訴機關的中意目標，所有處於 IMSI Catcher 訊號區域內待機中的手機，都會落入偽基地臺圈套，自動將 IMEI 與 IMSI 資料發送到 IMSI Catcher。至

[32]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 70。

於 IMSI Catcher 偵測期間正在通話的手機，則不會被 IMSI Catcher 截收 IMEI 與 IMSI」[33](使用 M 化設備可能蒐集到第三人資訊)。

虛擬基地臺使用上的疑慮，常討論的有「是否能作為監聽門號工具」、「蒐集到範圍內第三人資料內容」、「虛擬基地臺註冊時的干擾」等問題。德國文獻指出，某些功能模組的 IMSI Catcher 加裝監聽軟體後，可以截收模式切換成監聽模式，一旦知悉目標手機的 IMEI 或 IMSI 時，即可就地同步監聽目標手機撥出的通話。[34]在我國，M 化設備並無監聽功能，如果加裝監聽軟體在技術層面也許可行，但比起使用加裝監聽技術，偵查人員聲請通訊監察，更能完整擷取通訊內容及網路封包，且無須冒著風險靠近目標門號之所在位置。換言之，偵查人員應更傾向依照通保法聲請通訊監察更為實際，且通訊軟體之通訊內容為加密設備端通訊，M 化設備亦無法解譯，即 M 化設備即便加裝監聽軟體也無法取代通訊監察功能。

又，在虛擬基地臺覆蓋區域內之所有手機 IMEI 及 IMSI 遭到蒐集及干擾，是否會造成第三人個人資料曝露或訊號斷訊之問題，在蒐集資料部分，虛擬基地臺誘捕範圍內之手機 IMEI 及 IMSI，無可避免也可能會向偽基地臺註冊，因而蒐集到第三人的 IMEI 及 IMSI，但如前述說明，M 化設備要直接或間接識別個人資訊，仍需依通保法調閱使用者資料，也就是說即便偽基地臺蒐集到第三人註冊資訊，若沒有調閱相關資料，仍為一串無意義數字，惟仍需注意應規範蒐集資料後需銷毀所有數據紀錄。至於斷訊現象之時間長度有不同說法，德國聯邦政府 2001 年在答

[33]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 72。
[34]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 77。

覆國會質詢時，表示該設備可能會「暫時影響(最多 10 秒)」，但德國電信業者根據德國 IMSI Catcher 製造商羅德史瓦茲公司的資訊，認為可長達 5 至 10 分鐘。[35]斷訊現象雖可能導致電信干擾，但本文認為虛擬基地臺偵測時並不會長時間開啟，實際上真的會造成斷訊時間極為短暫，且造成基地臺訊號斷訊或訊號不穩定之因素，在一般電信服務業者基地臺系統轉換或更新修復網路連線時更常發生，反觀使用 M 化設備[36]造成無訊號情形寥寥可數，在法益權衡下應為可忍受之範圍。

在我國，因科技定位技術偵查未法制化，難有相關統計數據可供深入探究，也因為 M 化設備所費不貲，目前我國也僅有調查局、海巡署、刑事警察局及臺北市政府警察局、桃園市政府警察局有購置(高檢署於 2022 年 2 月評估導入檢察機關可能性)[37]，多使用於偵辦重大刑案、找尋藏匿重罪犯、兒少或生命安全緊急案件。事實上，M 化設備以現行專責人員不足且購置數量甚少之限制下，多數案件偵辦並未使用 M 化設備，而是選擇採用其他科技定位技術偵查手段。德國有文獻表示，「IMSI Catcher 對於實務之重要性，或許不如以往。這是因為 IMSI Catcher 除了價格昂貴外，更有以下的技術限制，前置的準備作業是必須先知悉目標手機的 IMEI 或 IMSI，然後初步限縮目標手機所在區域大約在幾公里內，也就是偵查人員必須要目標手機現身的數公里內附近區域持續移動測點，測點實目標手機還必須是待機狀態而未使用電話通訊，或必須處於連接電信業者行動上網的狀態，這些技術限制過於被動且勞師動眾，

[35]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 78。

[36] 黃有容，網路卡卡、時常沒訊號…建設 5G 影響 4G 收訊？中華電信吐真相，聯合報，2020 年 8 月 17 日，https://www.businesstoday.com.tw/article/category/80392/post/202008170008/ (最後瀏覽日：2021 年 12 月 3 日)。

[37]陳志賢，辦機敏案件防洩密 高檢署擬建「M 化車」團隊，中國時報，2022 年 2 月 8 日，https://www.chinatimes.com/realtimenews/20220208001131-260402?chdtv。(最後瀏覽日：2022 年 3 月 10 日)

對於偵查人員較無吸引力。」[38]在有其他科技定位技術偵查手段選擇下，M化設備並非首選，但確實具有高度重要性。

在我國，M化設備的使用最早出現在2012年新聞報導，前行政院秘書長林益世索賄案，該案檢舉人陳啟祥向媒體爆料後即不見蹤跡，最高法院檢察署特別偵查組檢察官以證人身分傳喚陳啟祥後，發現陳啟祥隱匿行蹤，不斷變換居處，拒不到案說明，該案承辦檢察官請求刑事局出動「M化定位車」，順利在某國際級酒店內將證人陳啟祥拘提到案。2015年更因緝捕峨嵋停車場雙屍案槍擊要犯陳福祥、香港富商黃煜坤遭綁架案，被譽為破案神器。2016年10月，臺北市政府警察局添購第二臺M化車，即遭媒體擴大報導並質疑依據法源，直到2017年桃園地方法院因警方使用M化車首度作出違法判決，更加確立M化車使用的法制化之路。

第三項　干預基本權及現行法源依據

M化車之功能為虛擬基地臺，可蒐集某特定區域之IMEI(手機序號)、IMSI（國際標準識別碼）佐以訊號強弱判斷距離，如單純就後者判定連線訊號強弱技術而言(例如獵狐槍)[39]，因沒有個化識別資訊，且干涉程度較輕，普遍被認為是刑事訴訟法所規範之一般調查權限。然M化車之功能係除訊號強弱技術，還能蒐集範圍內之手機識別資訊，故有涉及個人

[38]王士帆，M化車法制出路-德國IMSI-Catcher科技偵查借鏡，2022年3月，臺北大學法學論叢，第121期，頁75-76。

[39]吳坤龍、刑事局通訊監察中心，刑事雙月刊第31期，從神秘的獵狐到M化的宿命，頁44。無線電測向儀（俗稱「獵狐槍」）能針對一般無線電波進行發射源方位偵測。在歐美國家，業餘無線電測向（Amateur Radio DirectionFinding；ARDF）協會舉辦一種業餘比賽。這項運動比賽一般係在山丘叢林或公園草叢中，事先巧妙的藏好數個小型無線電波發射器（俗稱「小狐狸」），而參賽玩家（俗稱「獵手」）手持無線電測向儀（俗稱「獵狐槍」；一般由頻譜分析儀與手持式指向性天線組合而成）進行搜尋狡猾的「小狐狸」。比賽時，先搜尋確認「小狐狸」的方位，然後以徒步方式進行地毯式的偵搜，並以在規定的時間內，找到最多「小狐狸」者為優勝者，這就是無線電測向運動被稱為「獵狐」（Fox Hunting）運動的原因。實務常用於偵測考場舞弊、地下電台等偵蒐勤務。

資料保護之「直接或間接可識別之資料」之疑慮。

在我國，最早購置 M 化設備的是臺北市政府警察局，使用程序係依據臺北市政府警察局制定之「M 化偵查系統勤務執行規定」，須向管轄之地檢署(法院)聲請調取通信紀錄聲請書。在內政部警政署刑事警察局採購 M 化車後，警政署遂訂定「執行 M 化定位勤務作業流程」，據此規範，須依照通保法向法院聲請通訊監察書，始可為之。然而，不論是調取通信紀錄聲請書或通訊監察書，都會面臨到部分犯罪類型不能使用該偵查器材之窘境，且通信紀錄指的是「過去已發生」之資料，通訊監察書則是保障「通訊內容」之隱私權，由定義窺知，M 化車既屬於「未來尚未發生」之附著於載體之可識別資訊，亦無通訊之本質，並不符合通保法之意旨。

104 年員警偵辦詐騙集團機房，辯護人在第一審法院提出認為使用 M 化車，系侵害合理期待隱私之偵查作為，且現行法未明文規範使用，違反法律保留原則，故後續因使用 M 化車取得用以聲請搜索票所取得之證據，應依「毒樹果實原則」均應予排除使用。桃園地方法院在第一審判決，依據司法院釋字第 689 號，認為憲法保障人民行為自由、生活私密領域不受侵擾及個人資料之自主、隱私等權利，均屬憲法第 22 條保障個人人格自由發展之基本權保護範圍，使用 M 化車系干預人民基本權且無法律授權，違反法律保留原則，因排除 M 化車取得資訊的證據能力，[40]引發一陣譁然。

而後緊接在 109 年，高等法院作出截然不同的判決。高等法院認為，法的闡述與適用，不能僅有人權保障的廣度，也須同時把握憲法的高度。

[40]桃園地方法院 106 年度易字第 164 號刑事判決

隱私權之保護並非絕對，仍須與憲法保護之其他權利、所欲追求的價值與公益要求等等，綜合判斷，合理權衡。合議庭進一步指出，司法院釋字第 689 號闡述，新聞採訪者於有事實足認特定事件報導具有一定公益性，而屬大眾關切並具有新聞價值者，如須以跟追方式進行採訪，且跟追行為依社會通念非屬不能容忍，該跟追行為即具有正當理由而不在規定處罰之列。此號解釋正足以正當化治安機關對於有事實足認有特定犯罪嫌疑之犯罪行為，因偵查犯罪之需要，而採用現代科技設備，如對隱私權並未構成重大、不合比例之侵害，也未逾越依社會通念所認不能容忍的界限，符合憲法第 23 條之比例權衡原則。又查獲過程，M 化車的訊號定位系統只是將警方已知的犯罪地點加以限縮，M 化車定位並不會顯示與隱私有關的內容。新聞報導尚且得因特定事件報導、揭發犯罪行為，具有一定公益性，屬於大眾關切並具有新聞價值，即認具有正當理由；何況，警方使用 M 化車是為偵查已經發現的犯罪行為，保護公共利益，基於公益的合理權衡，依刑事訴訟法第 158 條之 4，應認 M 化車的偵查作為，具有證據能力並改判有罪。[41]

綜上，M 化車在犯罪偵查應用目前是沒有法律授權基礎的，且並未明確界定干預程度是否為一般調查權，而直接進入比例原則之討論。本案法院雖然以依刑事訴訟法第 158 條之 4 認為基於保護公共利益、公益的合理權衡，認定有證據能力，然而「位置資訊」干預每一個人的隱私權、人格權、資訊自決權，若不予以規範，則可能無限制擴張國家機器的權限。如同桃園地方法院第一審判決之結論，本院相當理解「科技偵查」在資訊科技時代的重要性，這不僅是本案問題，也是法治國的基本原則。綜上，包括本案「M 化車」在內的科技偵查方式，其犯罪追訴與

[41]高等法院 109 年度上易字第 1683 號刑事判決

權利保障的平衡點，有賴立法機關的睿智考量，盡速衡酌、決定。

第四節 GPS 全球定位系統

第一項 原理

GPS 全球定位系統（Global Positioning System、正式名稱為 NAVigation Satellite with Time and Ranging Global Positioning System），亦稱為全球衛星定位系統，其發展脈絡與網際網路相似，皆濫觴於軍事部門的需求而建立；最早的衛星定位系統即 GPS 全球定位系統之前身，係美國海軍所建立之 TRANSIT 衛星星系，即經緯儀系統[42]或子午儀衛星定位系統，此系統透過都卜勒頻移原理(Doppler Frequency Shift)，由人造衛星發射無線電波傳達至地面接受臺，透過都卜勒頻移量度來推算接收者位置，而接收方如有運動(移動)，則亦會影響都卜勒偏移量[43]，由上述原理可知，整個 GPS 全球定位系統的組成，勢必需要衛星與接收端，事實上，除接收端與衛星外，還需地面控制端監控衛星於太空的運作情形，方能確保整個 GPS 全球定位系統正常運作。[44] GPS 全球定位系統建置之濫觴係軍事需求[45]，最著名的即是 1991 的波斯灣戰爭與 2003 年伊拉克戰爭，利用 GPS 間接定位，迅速掌握敵方資訊精準轟炸，並提高地面飛彈的命中率，使平民傷亡人數下降，

[42]陳詩經，衛星定位系統，船舶科技，9 期，1992 年 4 月，頁 93。

[43]安守中，GPS 與都卜勒勒偏移量的基礎介紹，2005 年 10 月，頁 2-85；黃正中，漫談全球定位系統，國研科技，7 期，2005 年 7 月，頁 53。

[44]林誠澤，GPS 科技定位偵查與刑事訴訟法的搜索概念，國立政治大學法律學系碩士班碩士學位論文，頁 7。

[45]黃俊麟，中共衛星航太科技與反衛星系統發展，國防雜誌，22 卷 4 期，2007 年 8 月，頁 40-52；林明武、林輝龍，導航衛星於電子戰作為之研究，國防雜誌，25 卷 5 期，2010 年 10 月，頁 75-87；羅春秋，中共「北斗」導航衛星發展及其軍事戰略意涵，國防雜誌，29 卷 6 期，2014 年 11 月，頁 63-79。

使 GPS 全球定位系統於現代軍事中成為不可或缺的角色。[46]目前聯合國衛星導航委員會認定的全球衛星導航系統四大核心供應商有美國全球定位系統（GPS）、俄羅斯的格洛納斯衛星系統（GLONASS）、中國的北斗衛星系統（BDS）和歐盟的伽利略衛星系統（Galileo）。

第二項　功能及偵查上運用

GPS 最廣為人知的應用，不外乎就是導航的功能，初期建置之 GPS 全球定位系統亦用於軍事導航，流用於民間後，結合 GIS 地理資訊系統與電子地圖， 構成汽車導航系統的基礎，是類導航系統主要功能為定位與方向確認[47]，然智慧型手機的興起、Google 地圖日益完善，再加上行動網路技術成熟，以智慧型手機內建 GPS 定位已是常識，事實上，透過行動網路定位可分 GPS、A-GPS、Wi-Fi 與行動通訊四種方式[48]。因 GPS 全球定位系統的導入，在產業管理上亦有相當的助益，例如，建置「GPS 車隊管理系統」使現行物流、計程車隊、大眾運輸業等，透過該系統管理車隊調度與運送時間，進而降低管理成本、提高運輸效率，而歐美國家進一步研究「智慧型運輸系統」(Intelligent Transportation System，簡稱：ITS)，其由 GSM 系統、電子地圖、電腦網路、監控系統與控制系統組成，亦係利用 GPS 全球定位系統調度大眾運輸工具[49]，除運輸產業外，農工礦業亦有利用 GPS 全球定位系統，農業部分，例如

---

[46]林誠澤，GPS 科技定位偵查與刑事訴訟法的搜索概念，國立政治大學法律學系碩士班碩士學位論文，頁 9。

[47]賴進貴，導航系統發展與地圖問題之探討，中華民國地圖學會會刊，7 期，1996 年 12 月，頁 29。

[48]崔文、殷志揚、陳昭男，行動網路定位技術概觀，電腦與通訊 115 期，2006 年 3 月，頁 54-60。

[49]相關介紹可參見交通部，101 年運輸政策白皮書，101 年 8 月 22 日，https://www.iot.gov.tw/cp-78-11391-115bb-1.html(最後瀏覽日：2021 年 1 月 10 日)。

用 GPS 結合 GIS 地理資訊系統，進行農業蟲害防治分布的分析，礦業則是用於探勘礦脈，提高發現機率，節省昂貴的機械使用，另外，亦可利用差分全球定位系統（Differential Global Positioning System，簡稱：DGPS）於原油管線埋設規劃，使用公分級的精確定位，利於事後的維修保養。[50]GPS 全球定位系統，可以即時、正確地顯示所在位置，搭配路線紀錄器後，更可以記錄其行經路線，更有應用於人身保全系統之上，而在日本，因高齡化社會而老人失智人口亦隨之上升，為解決老人走失問題，如日本有將 GPS 全球定位系統之接收器，配戴於失智老人身上或鞋子中，以防其走失，而走失問題不僅於老人才有，幼童走失亦屢見不鮮，同樣在日本亦有人研發 GPS 電子書包，將 GPS 追蹤器安裝於書包中，防止走失與綁架時，能立即知悉兒童位置；另外，於美國則有研發盲人用的 GPS 導航手杖，亦是應用於社福的例子。[51]自從 GPS 接收器趨於迷你化後，攜帶更加方便外，其隱蔽性亦隨之提升，因此，各國偵查、警察機關看上 GPS 全球定位系統的追蹤功能與日益優越的隱蔽性，具有秘密、即時、精確及廉價特性，以 GPS 追蹤、接收器預防犯罪，亦非不能想像之事，而將其應用於犯罪預防[52]與犯罪處遇[53]之上，有手機、汽機車等較昂貴的商品，業者即推出內建 GPS 全球定位系統之商品，如 iPhone 即內建「尋找我的 iPhone」功能，使該商品被竊時，透過內建的 GPS 全球定位系統予以尋回，減少失竊率，亦有文獻[54]

---

[50]安守中，GPS 與都卜勒勒偏移量的基礎介紹，全華科技圖書股份有限公司，2005 年 10 月，頁 68-80。

[51]林誠澤，GPS 科技定位偵查與刑事訴訟法的搜索概念，國立政治大學法律學系碩士班碩士學位論文，頁 11。

[52]詹明華、李文章，全球衛星定位系統在犯罪偵防上之應用，刑事科學，第 59 期，2005 年 9 月，頁 11-15。

[53]許福生，科技設備監控在性侵害犯之運用，月旦法學雜誌，166 期，2009 年 3 月，頁 92-110。

[54]詹明華、李文章，全球衛星定位系統在犯罪偵防上之應用，刑事科學，第 59 期，2005 年

建議可運用於運鈔車,防止運鈔車被搶事件,或放置於擄人勒贖贖款內,或運用在警車上以利警力之布署與攔截圍捕作業。

總體而言，GPS 在犯罪偵查之應用，為輔助跟監及取得目標軌跡，以克服無法知悉行為人後續動向的困擾，縮小偵查範圍，於實務走私毒品案件中，以漁船方式走私者可謂相當常見，然縱算有情資顯示有走私毒品情形，偵查人員於海上亦難以跟蹤接應之漁船，經常無法知悉接應毒品之漁船的上岸地點，查緝毒品走私相當困難，如於接收情資時，鎖定接應之漁船並裝置 GPS 接收器，即可知悉其泊錨地點、上岸地點等，降低查緝的困難程度，是以，就 GPS 全球定位系統於偵查應用上，有監控對象活動之功能。[55]此外，在我國查緝森林法案件，亦會使用 GPS 裝設在林木上，如珍貴林木遭山老鼠砍伐或將林木順流而下假借漂流木撿拾，便能立即發報前往查緝。另有私人運用 GPS 全球定位系統，來進行監控活動並蒐證者，最常見的就是─配偶外遇(即俗稱的抓姦)。[56]惟此係私人運用，非國家偵查行為，不在本文討論範圍。

第三項　干預基本權及現行法源依據

GPS 系統因成本下降且應用廣泛，很早便使用於犯罪偵查之輔助設備，但也因為沒有明確法律授權，而被喻為「能做不能說」的偵查設備。2014 年海巡士官長因查緝私菸在營業用自小貨車上裝設 GPS 設備，經

9 月，頁 11。

[55]林誠澤，GPS 科技定位偵查與刑事訴訟法的搜索概念，國立政治大學法律學系碩士班碩士學位論文，頁 13。

[56]許恒達，GPS 抓姦與行動隱私的保護界限——評臺灣高等法院一〇〇年度上易字第二四〇七號刑事判決，月旦裁判時報，24 期，2013 年 12 月，頁 59-78；薛智仁，衛星定位追蹤之刑責－評臺灣高等法院 100 年度上易字第 2407 號判決，科技法學評論，11 卷 1 期，2014 年 6 月，頁 119-154。

審理，判處妨害秘密罪，提出最高法院上訴駁回。最高法院判決理由[57]，闡述司法院釋字第 603 號、689 號解釋意旨，認為維護人性尊嚴與尊重人格自由發展，是自由民主憲政秩序的核心價值。隱私權雖非憲法明文列舉的權利，不過，基於人性尊嚴與個人主體性的維護及人格發展的完整，並且為了保障個人生活私密領域免於他人侵擾及個人資料的自主控制，隱私權乃為不可或缺的基本權利，受憲法第 22 條所保障。又對個人前述隱私權的保護，並不因其身處公共場域，而失其必要性。亦即他人的私密領域及個人資料自主，在公共場域也有可能受到干擾，而超出可容忍的範圍，尤以現今資訊科技高度發展及相關設備的方便取得，個人的私人活動受注視、監看、監聽或公開揭露等侵擾的可能大為增加，個人的私人活動及隱私受保護的需要，也隨之提升。所以個人縱然在公共場域中，也應享有依社會通念得以不受他人持續注視、監看、監聽、接近等侵擾的私人活動領域及個人資料自主，而受法律所保護[58]。又進一步說明以行為人駕駛小貨車行駛於公共道路上為例，就該行駛於道路上的車輛本體外觀而言，因車體本身無任何隔絕，固然是公開的活動；但是從小貨車須由駕駛人操作，該車始得移動，且經由車輛移動的信息，即得掌握車輛使用人的所在及其活動狀況，足見車輛移動及其位置的信息，應評價為等同車輛使用人的行動信息，故如就「車內的人物及其言行舉止」而言，因車輛使用人經由車體的隔絕，得以確保不欲人知的隱私，即難謂不屬於「非公開的活動」。

[57]最高法院 106 年度台上字第 3788 號刑事判決

[58] 1967 年 Katz v.United States 案警察於被告慣常使用的公共電話亭外，在電話亭外的電話線上安裝竊聽器材，因而取得被害跨洲賭博的通話內容。隱私權的判斷角度從美國聯邦憲法增修條文第 4 條理解之財產權基準，改認隱私權保護對象是「人」，而不是「處所」。Harlan 大法官協同意見書，合理期待隱私的雙叉法則，即「當事人主觀上必須具備真實隱私期待，在客觀上，該真實隱私期待為一般社會大眾所認為合理」，以及後續判決實務發展出「第三人法則」(自願揭露法則)，影響甚鉅。

最高法院指出，由於使用 GPS 追蹤器，偵查機關可以連續多日、全天候持續而精確地掌握該車輛及其使用人的位置、移動方向、速度及停留時間等活動行蹤，且追蹤範圍不受時空限制，也不侷限於公共道路上，即使車輛進入私人場域，仍能取得車輛及其使用人的位置資訊，且經由所蒐集長期而大量的位置資訊進行分析比對[59]，即可窺知車輛使用人的日常作息及行為模式，難謂對於車輛使用者隱私權的毫無侵害。

在日本平成 29 年 3 月 15 日最高裁判所，曾對公共場域之定位科技做出裁判，認為檢索與掌握對向車輛隨時(無時無刻)的位置資訊所為之 GPS 偵查，可能逐一掌握對向車輛以及其使用者之所在與移動狀況；必然伴隨無所不包(網羅)的、繼續不斷地掌握個人行動，可能會侵害到個人的隱私權；另外，GPS 機器祕密的安裝於個人攜帶物品上所進行的行為，應該是公權力對於私領域的侵害。[60]

值得一提的是，在我國，GPS 追蹤器在法定義務揭露之情形，並不少見，例如在環保法規內規範廢棄物清運機具應裝置即時追蹤系統、漁業法規規範裝設漁船監控系統、交通法規規範遊覽車裝設全球衛星定位系統。依據廢棄物清理法第 31 條第 1 項第 3 款規定：「中央主管機關指定公告之事業廢棄物清運機具，應依中央主管機關所定之規格，裝置即時追蹤系統並維持正常運作」。又 102 年 6 月 10 日行政院環境保護署環署廢字第 1020047198 號修正「應裝置即時追蹤系統之清運機具及其規定」，係指領有交通部監理單位核發之行車執照之清運機具(車輛)，

[59] 馬賽克理論（Mosaic theory），係指以 GPS 定位追蹤器可連續多日、全天候不間斷追蹤他人車輛行駛路徑及停止地點，將可鉅細靡遺長期掌握他人行蹤，此等看似瑣碎、微不足道之活動資訊，經由此種「拖網式監控」大量地蒐集、比對定位資料，個別活動 之積累集合將產生內在關連，使以此等方式取得之資料呈現寬廣的視角場景，私人行蹤將因此被迫揭露其不為人知之私人生活圖像。

[60]黃朝義，刑事訴訟法程序基礎理論，2020 年 1 月，頁 343。

如水肥車、大貨車、特種車(載送化學有毒物質)、曳引車或油罐車。另依據漁業法第五十四條第五款，規定「二十噸以上未滿一百噸延繩釣漁船及一百噸以上拖網漁船裝設漁船監控系統應遵守及注意事項」，應依本注意事項規定裝設漁船監控系統，始得出海作業。另依據交通部公路總局汽車運輸業管理規則第十九條之四，規定「遊覽車客運業車輛裝置全球衛星定位設備及營運監控系統管理要點」遊覽車客運業所屬遊覽車應依規定裝置 GPS，並應維持正常運作，其車輛 GPS 資訊並應由受委託營運系統業者依規定介接至遊覽車動態資訊系統。可知為了強化管理之實際需求，在法律上明訂有法定義務揭露之規範。在各地方自治條例，已有部分縣市修訂自治條例，規範垃圾車、計程車、砂石車等行業，需要裝設 GPS 追蹤器，配合主管機關管理。據此，GPS 即時追蹤系統並非新創設且多有規範在法令之中，原因在於便利且有效乃時勢所趨。由此可見，應該討論的並非 GPS 追蹤器是否使用，而是如何具體務實的探討 GPS 在犯罪偵查使用之授權基礎、設規範備、報告義務及救濟，才是根本解決之道。

第五節 其他科技定位技術

第一項 WIFI 定位

Wi-Fi，係為 Wi-Fi 聯盟所創之產品品牌認證，為建立於 IEEE 802.11 標準的無線區域網路技術，現今都市中，不論室內或室外，幾乎有分布 Wi-Fi 訊號，正因其訊號分布廣泛的特性，用於定位上自然是可以想像的事，關於 Wi-Fi 定位之原理與技術，分為時間測距(Time-to-distance)、角度測距(Angle-to- distance)與訊號強度測距

(Signal strength)三種[61]，應用層面各有不同，本文不多加詳述，而大多的技術方法於室內、室外均可為定位，然須注意，既然是以無線電傳送訊號，對於不同的物體就會有不同的反應，進而影響其反射率、折射率等，其訊號強度亦容易受環境因素、布建方式、位置而有不同[62]，影響 Wi-Fi 定位技術的主要因素有訊號的存取地點、基地臺分布與接收端移動速度等。Wi-Fi 定位係仰賴 Wi-Fi 基地臺而為定位，而 Wi-Fi 基地臺所在位置的資訊就相當重要，現關於 Wi-Fi 基地臺位置資料(即 MAC 位址，Media Access Control)[63]，例如 Google 地圖街景車應用所建置的資料庫，即為 Wi-F 基地台定位所得資訊的應用。申言之，Google 地圖的街景車除蒐集街道的景物外，還蒐集所經路線 Wi-Fi 基地臺位置資料，再透過 Android 用戶或 Google 地圖之使用者，更新 Wi-Fi 基地臺位置資料，實際上，縱算以行動網路定位而使用 Google 地圖時，Google 地圖通常會建議打開 Wi-Fi 接收選項，以提供更準確的定位[64]，可見 Wi-Fi 定位的存在已經是相當成熟的技術，然 Google 畢竟是私人企業，其資料庫亦為私人所有，而我國國家機關此一資料庫之建置仍在發展階段，尚無成功以此定位方式偵查之例[65]。MAC 識別碼的定位技術以漸臻發展成熟，且具有可單一識別化的特性，如有朝一日開放應用大

[61]吳世琳、張自強、葉禹良、許冠傑，無線網路定位技術應用於即時救援，臺灣職能治療研究與實務雜誌，4 卷 2 期，2008 年 12 月，頁 140-143。

[62]詹明華、陳弘斌、宋奕賢，定位技術在犯罪偵查上之應用，刑事科學，第 80 期，2016 年 3 月，頁 8。

[63] MAC（Media Access Control）位址是由六組 16 進位數字組成的物理位置，這個位址分為兩個部分，前三組數字是廠商 ID；後三組數字則是網路卡的卡號，理論上全世界沒有網路卡的 MAC 位址是相同的。

[64]林老生、郭清智，整合 Wi-Fi 與 GPS 技術於室外定位之研究，臺灣土地研究，18 卷 1 期，2015 年 5 月，頁 7。

[65]詹明華、陳弘斌、宋奕賢，定位技術在犯罪偵查上之應用，刑事科學，第 80 期，2016 年 3 月，頁 8。

數據，必定會成為科技定位技術偵查之工具。

第二項　IP 位址定位

IP 位址（Internet Protocol Address）是指網際網路協議地址，經協議提供的一種統一的地址格式，網際網路上的每一個網路和每一臺主機分配一個邏輯地址，可視為網路傳輸間的門牌號碼。IP 位址又可區分為固定位址和動態(浮動)位址，設定上可分為公開位址和私人位址。由於在網路每一次的重新登入後，IP 位址會被重新配發，且在同一時段可能會有不同使用者共用的問題，除了固定位址外，僅能在特定時段限縮犯罪者的身分，在實務犯罪偵查並不能作為追蹤定位功能，且在虛擬私有網路（Virtual Private Network, VPN）遠端連線服務[66]盛行後，經過 VPN 跳板設定，可將使用者之電腦或手機 IP 位址顯示於其他國家，IP 位址目前在犯罪偵查上多為一般調查權之基礎資料調閱分析。

第三項　藍芽定位

藍牙是一種無線傳輸技術，1994 年電信業者愛利信（Ericsson）發展出這個技術，理論上能夠在最遠 100 公尺左右的裝置之間進行短距離連線，但實際使用時大約只有 10 公尺。其最大特色在於能讓輕易攜帶的行動通訊裝置和電腦，在不借助電纜的情況下聯網，並傳輸資料和訊息，目前普遍被應用在智慧手機和智慧穿戴裝置的連結以及智慧家庭、車用物聯網等領域中。[67]目前藍芽定位技術尚未使用於犯罪偵查，而是首要被關注使用在防疫工作，在 2019 年為新冠肺炎疫情爆發，兼顧人權保障及公衛疫調，衛

[66] VPN 即虛擬私人網路（Virtual Private Network, VPN），是一種常用於連接兩地之間的私人網路的通訊方法，在連線設備與 VPN 伺服器之間使用隧道協定（Tunneling Protocol）以建立加密的連線通道，達到傳送端認證、訊息加密與準確性等功能。

[67]程正孚，藍芽的演進，台灣電信月刊，108 年 3-4 月號，頁 13-14。

生福利部疾病管制署與行政院資安處、臺灣人工智慧實驗室(Taiwan AI Labs)進一步合作開發「臺灣社交距離 App」[68]，利用手機的藍牙定位，以訊號強度偵測使用者間接觸的距離與時間，以科技輔助記錄其過去 14 天內的接觸史。「臺灣社交距離 App」原理，係當你下載接觸通知系統的 App，你的裝置就會得到一組隨機產生的 ID(去識別化)。為了確保你的身分或位置不會因為這些隨機 ID 而外洩，系統每 10 到 20 分鐘就會變更一次隨機 ID。手機會定期比對本身的記錄清單與所有 COVID-19 陽性確診病例的隨機 ID，如果發現有符合，代表你曾經在某個地方接觸過患者。此種利用「藍芽定位」方式僅限約 3 公尺內，比起基地臺定位方式(100 至 500 公尺)範圍更限縮且侵害更小[69]。為更有效率及準確判別是否與確診者近距離接觸，也因藍芽定位具備去識別化之特性，且偵測距離較短，在疫情期間被廣泛運用。

[68]衛生福利部疾管署新聞稿，2021 年 5 月 14 日，https://www.cdc.gov.tw/Bulletin/Detail/4tvSn4wPDjJe42YTuS8LjA?typeid=9(最後瀏覽日：2021 年 5 月 15 日)。
「臺灣社交距離 App」無須註冊，也不會上傳任何個人資料；功能主要是利用藍牙技術，記錄接觸對象去識別化資料，不包括地點定位資訊，相關接觸資料僅儲存於個人手持裝置端 14 天，不會上傳到任何雲端服務。當使用者接獲通知為確診者時，經衛生單位徵得確診者同意後可上傳資料，App 將主動通知過去 14 天曾接觸過的對象並出現警示畫面。

[69]吳哲宜，中時新聞網，科技防疫！台南首創群聚警示系統，戶外 10 人以上群聚警方馬上知， https://www.ctwant.com/article/120143(最後瀏覽日：2021 年 5 月 30 日)。
臺南市政府擇定 10 處試辦場所，群聚監測警示系統是利用 NB-IoT 技術之晶片裝置，會偵測藍芽訊號，以估算人數，如果出現 10 人以上群聚狀況，系統將會立即通報警察局的 LINE 群組，為了顧及民眾隱私權，系統不會紀錄民眾資訊與行蹤，僅會在監測到群聚現象時通知警方。

第三章 我國科技定位技術偵查之可能法源

第一節　刑事訴訟法

刑事訴訟法之目的在於發現實體真實，藉由刑事訴訟程序實踐刑罰權之有無及範圍。犯罪偵查目的在於尋找罪犯、保全證據，以求發現真實，或指蒐集保全有利與不利於被告證據，以確保被告受審判之權利。因此，犯罪偵查即是指「偵查機關及其偵查人員，基於告訴、告發、自首或其他原因，知有犯罪嫌疑時，立即行使偵查職權，逕行調查犯罪嫌疑人犯罪情形及蒐集證據，藉以證明犯罪及確定犯人，並依法定程序檢舉犯罪，以供檢察官提起公訴與法院決定刑罰之依據，期能達到維護社會治安的最終目的。[70] 犯罪偵查依據之強制處分，因可能侵害人民權益，在積極意義上必須遵守避免類推、不利益變更禁止等準則。強制處分之具體訴訟法律效果，應探究實定法規而非不明確之「正當法律程序」(司法院釋字第 384 號參照)。然而，就刑法而言，詮釋時原則上不能超出法條文字範圍，亦即以條文的「可能文義」作為詮釋刑法的最大界限。[71]刑事訴訟法為犯罪偵查最重要之法律授權基礎，惟目前我國未將科技偵查手段法制化，而以逐案檢視科技偵查手段與人權保障之衡量，如此終將使偵查人員無所適從，亦無法有效保障人民權益。

[70]鄭厚堃，警察百科全書，2000 年 1 月，頁 3。
[71]林山田，刑法通論(上)，2008 年 1 月，頁 157。

定位方式	鎖定目標	精準度	通訊內容	第三人資料	資料來源
基地臺	電信門號	視基地臺密集度，約 100 公尺到 500 公尺	X	X	原有載體資訊
M 化	電信門號、IMSI、IMEI	約 3 公尺內	X	V	原有載體資訊
GPS	網路	約 3 公尺內	X	X	物理附加設備
WIFI	網路、MAC 位址	約 5 公尺內	X	X	原有載體資訊
IP	網路、IP 位址	約 5 公尺內	X	V	原有載體資訊
藍芽	網路、無線電波協定	約 3 公尺內	X	X	原有載體資訊

第一項 搜索

依據刑事訴訟法中第 228 條第 1 項前段、第 230 條第 2 項、第 231 條第 2 項之規定，僅係有關偵查之發動及巡防機關人員執行犯罪調查職務時視同刑事訴訟法第 231 條司法警察（官）之規定，惟長期追蹤取得大量資訊，足以揭露其不為人知之私人生活圖像，應屬超越合理隱私期待之侵害，構成強制處分。[72]本條在犯罪偵查的概括授權干預，認為只能授權司法警察進行較低度基本權的干預措施[73]，或認為僅為任務分配規定，並無任何干預基本權的授權。[74]在我國刑事訴訟法第 122 條規定有相當理由，得搜索相對人之身體、物件、電磁紀錄及住宅或及其他處所，「搜索」概念是否可適用於「偵測、攔截載體訊號」，通說是否定的。在最高法院 97 年度台上字第 1509 號判決闡述，搜索之目的在搜索以及其後所為

[72]吳巡龍，檢察官傳訊方式及任意偵查，2009 年 2 月，刑事法雜誌，頁 3。
[73]薛智仁，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。
[74]薛智仁，刑事程序法定原則，月旦刑事法評論，2018 年 11 期，頁 28-29。

之拘捕或扣押等處分，係對於被搜索人之身體、住宅或財產等基本權之強制干預，故而發動實施搜索處分時應謹守法律設定之要件限制。故推知，搜索仍相當侷限於物理性侵入有形空間，藉以發現有形體之物件，並取得佔有，並未涵蓋無形體之資訊。

另有學者認為，我國刑事訴訟搜索扣押的執行圖像並不具有秘密性，偵查人員現身搜索扣押地點，且應讓受干預人知悉或在場，受干預人請求搜索證明書，以藉此獲得審查搜索扣押合法性的救濟機會[75]，然科技定位技術偵查實施多為隱密性，受干預人當場防禦知悉可能性甚低。科技定位工具，是以掌握特定對象於公共空間的動態或所在位置，取得對象一定資訊，且，因此，不符合刑事訴訟法搜索之概念。[76]由此可知，刑事訴訟法之「搜索」，侷限於有形物體，且應為物理性之有形侵入強制處分，與科技定位偵查「偵測、攔截」之概念不相符。

第二項 電磁紀錄

刑法第 10 條第 6 項稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。而電磁紀錄的特性，係可透過電腦設備予以編輯、處理、傳輸、顯示或儲存，本質上具備一定之可再現性，且因電腦科技的創新與進步，在重複讀取、傳輸電磁紀錄的過程中，原有電磁紀錄的檔案內容，可以隨時複製而不致減損，屬電磁紀錄與一般動產的差異所在。[77]另刑法第 359 條之破壞電磁紀錄罪，立法理由係因「電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性

[75]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，臺北大學法學論叢，第 121 期，2022 年 3 月，頁 92。
[76]李榮耕，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，國立臺灣大學法學論叢，2015 年 9 月，44 期，頁 875-886。
[77] 司法院公報，第 60 卷 第 7 期， 2018 年 7 月，頁 164。

與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害」，爰參考世界先進國家立法例，予以增設、規範。而電腦資料，皆係經由電磁紀錄之方式呈現，此電磁紀錄，具有足以表徵特定事項之作用（諸如身分或財產紀錄），一旦對電磁紀錄侵害，亦可能同時造成身分或財產上之損害，嚴重影響在網路之電腦使用的社會信賴及民眾日常生活安全。可見，本罪所欲保護之法益，即為維持網路電腦使用之社會安全秩序，並避免對公眾或他人產生具體之侵害。(最高法院 108 年度台上字第 4114 號刑事判決參照)，由此推知，電磁紀錄必須要有「表徵特定事項」(直接實質內容)且著重於網路電腦使用保障，與科技定位偵查手段利用「附隨載體之訊號」(非直接實質內容)，且非專屬以電腦網路之技術，兩者並不完全相同。

第三項 交付命令

刑事訴訟法第 133 條，可為證據或得沒收之物，得扣押之。係指對於「應扣押物」之所有人、持有人、保管人，要求提出或交付應扣押物之命令者。交付命令的性質，本身不具強制效力，僅於受命令人無正當理由拒絕提出時，得強制扣押，故屬「間接強制處分」。交付命令，為偵查階段中對當事人侵害較小之手段，對當事人之名譽或隱私權等損害較低，如函調戶政機關有關被告之戶籍口卡，或金融銀行有關被告資金往來明細等。而命令則隱含後續之強制處分，受處分人如無正當理由拒絕提出或交付時，通常伴隨著後續之不利處分，即得用強制力扣押之，此無須事先由法院審查，且無其他要件限制(最高法院 106 年度台非字第 259 號刑事判決參照)。

在最高法院106年度台非字第259號刑事判決，員警為偵辦賭博案，

經檢察官向法院聲請核發之「調取票」，向中華電信調取犯罪嫌疑人所使用「Hibox」網路傳真服務所接收賭客傳真簽單影像之列印資料，法院認為該傳真資訊非屬通訊或通信紀錄之範疇，而應屬資訊隱私權，回歸適用刑事訴訟法，依刑事訴訟法搜索、扣押相關規定。又，有主張（如本案非常上訴理由書）既屬於本案證據，且為應扣押之物，即可依手段比例原則，分別命扣押物之所有人、持有人或保管人提出或交付，甚而進一步依非附隨搜索之扣押程序，逕以實行扣押之方式取得即可，均無庸向法院聲請扣押裁定。惟，法院則認為，此對人民一般隱私權之保障實有未足，蓋以現今資訊世界，大量仰賴通訊軟體，通訊服務，有大量之隱私儲存於此，如容許偵查機關未經法院之介入，逕行調閱，其侵害隱私至深且鉅，顯違比例原則。準此，「應扣押物」及「得為證據之物」之扣押客體，基於維護人民一般隱私權、保障其訴訟權益及實現公平法院之憲法精神，應依目的性限縮。是以，檢察官對於「過去已結束」之通訊內容之非附隨搜索之扣押，原則上應向法院聲請核發扣押裁定，不得逕以提出或交付命令之函調方式取得，方符上開保障人民一般隱私權之旨。由此推知，交付命令並不足以作為科技定位技術偵查之依據。

第四項 羈押替代處分之科技設備監控

科技設備在我國刑訴法中，並非完全沒有討論，第 116 條之 2 第 1 項第 4 款及第 117 條之 1 第 1 項：「法院許可停止羈押時，經審酌人權保障及公共利益之均衡維護，認有必要者，得定相當期間，命被告接受適當之科技設備監控。」，據此訂定刑事被告科技設備監控執行辦法。依上開辦法第 3 條，科技設備監控，係指運用一切適當之科技工具或設備系統，輔助查證受監控人於監控期間內是否遵守法院或檢察官所命事項，及記錄其於監控期間內之行蹤或活動，並藉由信息之傳送，通報法

院、檢察署或其指定之人員。同辦法第 5 條，科技設備監控之實施，偵查中由檢察官、審判中由審判長或受命法官指揮執行之。第 6 條法院及檢察署為辦理科技設備監控業務，應備置信息接收及其他必要之科技監控相關設備與器材，並得視需要以監控中心辦理。第 8 條審判長、受命法官或檢察官依第五條指揮執行時，應核發記載下列事項之執行科技設備監控命令書：一、受監控人之姓名、性別、出生年月日、住所或居所、身分證明文件編號。二、實施科技設備監控之法令依據。三、配戴監控設備之身體部位或裝置監控設備之處所或物品。四、實施科技設備監控之期間及時間。五、應遵守之事項。六、違反命令之法律效果。七、不服指揮執行之救濟方法。由刑訴法作為起始之依據，訂定法條架構與通保法十分相似，如「執行科技設備監控命令書」(通訊監察書)、「監控中心」(通訊監察中心)且有規範使用設備、執行期間義務及救濟等規定。

雖本條文係為防止未經羈押或停止羈押之被告，在偵查或審判中逃匿藉以規避刑責，所訂定之替代處分，顯非偵查所使用之手段。但在立法理由，闡明本條文係因科技設備技術日新月異，為因應未來科技之進步，自有命對被告施以適當科技設備監控之必要，爰增訂以利彈性運用。由此可見，在科技定位技術法制化之路，也許可效仿此立法模式參照。

第五項 現行可能之授權基礎

科技定位技術偵查不論是在刑事案件或非刑事案件，實務應用相當廣泛，以發動的態樣而言，前者常見為拘提搜索的前置摸索偵查作為，後者則有如基於犯罪預防目的，事先將 GPS 設備裝設在易生犯罪之物體

上，例如裝設 GPS 在保護區林木上，用以查緝盜伐山老鼠，或在竊盜熱區之車輛裝上 GPS，以追蹤竊車集團。在前述討論，我國似無法尋得科技定位技術偵查之直接授權之法源授權基礎，然而，在探討科技定位技術偵查之使用方式可發現，仍有可能存在不須特別之法律授權之情形，例如附隨於強制處分之前置偵查作為。此為實務上常見之樣態，即在實施干預性更大且已有獲得授權基礎之強制處分前，將科技定位技術作為前置輔助使用，在此情形下並無超出使用目的及範圍，應推論為已給予授權基礎。例如依法執行拘提、搜索，或緝捕通緝犯，依據刑事訴訟法已取得搜索票或可執行逕行搜索之情狀，在前置偵查摸索作為，使用科技定位技術以確保執行目標之處所，因在已先行取得法官保留之門檻，而後使用相較強制力較低的定位技術之情形，本文認為應視為強制處分整體執行而論，無需畫蛇添足另尋求法官令狀之授權。

另在行政法令與刑事案件之界線，有可能產生無需特別授權基礎之樣態，如在依法有揭露位置資訊義務之客體私自裝設 GPS。在實務上，尤以漁船走私毒品或砂石車傾倒廢棄物案件，犯罪者為滅證會在犯罪時關閉 GPS 之定位裝置，以隱匿行蹤。倘偵查人員為偵查犯罪，在此情形私自裝設 GPS 裝置在(行政法規)有揭露位置資訊之物體上，基於發現真實蒐集犯罪事證，且裝設時間、位置均與法定義務相同，事實上並未逾越法規範之本質，亦未超越干預人民之基本權利(因法規範已有義務在前)，而無需特別法律授權。

第二節　通訊保障及監察法

按我國通保法第一條揭示之立法目的，為保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序，特制定本法，似與科技定位技術偵查所需保障之處相同，故實務上會以聲請調

取票或通訊監察書方式，以相對法官保留原則之架構取得犯罪偵查手段之合法性，實屬在法未明文下採取之權衡之計。然通保法所規範之「通信紀錄」及「通訊」，與本文所討論之各種定位科技偵查技術並不相同，對於「現時及未來發生」之「附隨載體之訊號」（甚至設備有可能係由偵查人員裝設），與通保法所規範內容並不相符。

第一項 通訊

通訊監察具有「隱密性」(監聽對象無法察覺被監聽)、「未來性」(監聽的對話並非現在已存在，而是預期未來會發生)、「持續性」(監聽時間較長，也不受有形空間的限制)、「流刺網性」(並非只蒐集監察對象的訊息，第三人使用被監聽的電話或第三者與監察對象的對話均被一網打盡)等特性，其對人民基本權的干預，相較於一般傳統之強制處分有過之而無不及[78]。憲法第十二條規定：「人民有秘密通訊之自由。」旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利。秘密通訊自由即通訊隱私權之保障，在於通訊參與人間之訊息係以秘密之方式往來或遞送，該訊息因已脫離參與人得控制之範圍，特別易受國家或他人之干預及侵擾，而有特別保護之必要，其既重在保障通訊之過程，其保障之範圍，自應隨訊息送達接收方，傳遞過程結束而告終止。(彰化地院 105 年度易字第 867 號刑事判決、臺中高分院 106 年度上易字 180 號刑事判決參照)

由此可知，在國內學說及實務見解認為「通訊」必須含有人的意思或想法，如果只是單純截收訊號，並不屬於通訊。又依通保法第三條，通訊，以

[78]何信慶，從立法審議過程談新修正通訊保障及監察法，司法新聲第 111 期，頁 27。

有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。科技定位技術偵查所「偵測、攔截」訊號，並無實質通訊內容，難謂有合理隱私期待。在國內，通說認為 GPS 設備相類訊號資訊，並非通訊內容。GPS 偵查之隱密偵查方式同於通訊監察，但取得內容有明顯差異。首先，通保法第 5 條「通訊監察」所取得者為同法第 3 條第 1 項第 1 款之「利用電信設備發送、儲存、傳輸或接收符號、文字、影 像、聲音或其他信息之有線及無線電信」，但通訊的意涵為包含通訊者意思或想法在內的溝通。[79]GPS 設備偵查取得之位置資訊僅是透過訊號接收與計算而得到的結果，難謂符合該意涵，故無法適用通訊監察規範之。[80]

第二項 通信紀錄

依通保法第 3-1 條通信紀錄者，謂電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。在保障通訊之過程，其保障之範圍，自應隨訊息送達接收方，傳遞過程結束而告終止，亦即，「過去已結束」之通訊內容，已非秘密通訊自由保護之客體，應僅受一般隱私權即個人資料自主控制之資訊隱私權所保護。依司法院釋字第 631 號解釋理由書之意旨及通保法之規範體系，通保法所規範之通訊監察，係以「監控與過濾」受監察人通訊之方式，蒐集對其有關之紀錄，通訊監察並具有在「特定期間內持續實施」之特性，益徵通訊監察之客體，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。(臺中高分院 106 年度上易字 180 號刑事判決參照)。

[79]許恒達，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，2010 年 1 月，頁 119-120。

[80] 李榮耕，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，國立臺灣大學法學論叢，2015 年 9 月，44 期，頁 905-906。

換言之，通信紀錄在文義解釋上，確實有將「位置資訊」規範在內，但在通保法立法目的，應只涵蓋「過往已發生」儲存的資料，而不包含「未來未發生」的位置資訊。

第三節　電信管理法

電信管理法於 108 年 5 月 31 日經立法院三讀通過，自 109 年 7 月 1 日起正式施行，為健全電信產業發展，鼓勵創新服務，促進市場公平競爭與電信基礎建設，建構安全、可信賴公眾電信網路，確保資源合理使用與效率，增進技術發展與互通應用，保障消費者權益，內容大幅鬆綁傳統電信法之管制架構。電信管理法第 9 條，所稱通信紀錄，指用戶或電信使用人使用電信服務後，公眾電信網路所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄，並以公眾電信網路性能可予提供者為限。電信事業及設置公眾電信網路者有依通訊保障及監察法協助執行通訊監察、調取通信紀錄及通訊使用者資料之義務，為電信事業機構協力義務之法源。

現行調閱手機定位之位置資訊，並未通保法所准許之範圍，僅能依第 8 條電信事業對下列通信應予優先處理：一、於發生天災、事變或其他緊急情況或有發生之虞時，為預防災害、進行救助或維持秩序之通信。二、對於陸、海、空各種交通工具之遇險求救及飛航氣象等交通安全之緊急通信。三、為維護國家安全或公共利益，有緊急進行必要之其他通信。故，依據電信管理法之規範，科技定位技術僅能適用於急難救助，而無法使用於犯罪偵查。

第四節　警察職權行使法

警職法第 11 條，經警察局長同意，基於防止犯罪目的，以目視或

科技工具，針對特定對象進行觀察及蒐集資料，期間為 1 年，必要得延長 1 次為限。「跟監」係指國家機關為防止犯罪或犯罪發生後，以秘密而不伴隨國家公權力之方式，對無隱私或秘密合理期待之行為或生活情形，利用目視或科技工具進行觀察及動態掌握等資料蒐集活動。是所謂「跟監」包括對人民行動為追跡、監視及蒐證等活動。無論係基於調查犯罪之必要所為具司法警察偵查犯罪性質之活動；或係為預防犯罪所為之行政警察活動，對於被跟監者之隱私權、資訊自決權等憲法所保留之基本權固有不當之干預，然偵查犯罪及預防犯罪之發生等均係維持社會秩序及增進公共利益所必要，自得以法律限制之(最高法院 101 年度台上字第 5635 號刑事判決參照)。

刑事訴訟法第 230 第 2 項、第 231 條既規定司法警察官、司法警察知有犯罪嫌疑者，應開始調查。而「跟監」復係調查及蒐集犯罪證據方法任意性偵查活動，不具強制性，苟「跟監」後所為利用行為與其初始之目的相符，自無違法可言。最高法院認為，偵查跟監是任意性偵查活動，且刑事訴訟法第 230 第 2 項、第 231 條即可授權基礎，然而，對於「跟監」是否已嚴重干預人民之基本權利，學說見解相當分歧。肯定說認為上開規定是偵查跟監的授權基礎；否定說認為，偵查跟監侵害人民隱私或資訊自決權，在現行法下欠缺法律根據。折衷說認為在強制處分的個別授權之外，上開規定可構成司法警察的一般調查權限條款，但是適用範圍限於干預強度未達一定門檻、輕微的偵查措施。[81]本文所討論之科技定位技術偵查，具體而言即為傳統跟監之手足延伸(輔助)，因以科技技術之手段可減少偵查人員負荷，且能更精確有效針對犯罪樣態採取合適之監控手段，警職法第 11 條觀文義解釋雖符合科技監控，然目的

[81] 林鈺雄，干預保留與門檻理論－司法警察（官）一般調查權限之理論檢討，政大法學評論第 96 期，2007 年 4 月，頁 222 。

係為預防犯罪，並非為「犯罪偵查」或「蒐集證據」，故警職法之「監控」似不足以作為科技定位監控之法律依據。

然而，在我國，警察之行政與司法身分顯然重疊，且犯罪偵查程序之規範，散見於刑訴法(犯罪調查權限，如拘提搜索)及警職法(發動措施、採取手段，如臥底線民、科技監控)，並未相連一體，造成在判斷係行政犯罪預防或是危害發生前置行為上，產生困難，亦有模糊空間。我國警職法立法雖仿照德國法，但未有類似德國之「前偵查程序」(Vorermittlungsverfahren)。前偵查程序，係指在偵查程序前，調查是否具備「德國刑事訴訟法第一百五十二條第二項之充分的事實根據」，是刑事追訴機關為調查犯罪，於尚未符合偵查法定原則所需前提下，所為的各種資訊蒐集行為[82]。因此，在論定上，警職法是否足以作為可能法源依據，仍須回歸討論警職法所為之蒐集資料與利用，是否能夠做為刑事司法證據，而此部分仍多有爭議。本文認為，雖警職法不宜作為科技定位技術之直接法律授權基礎，惟警察基於預防犯罪目的蒐集之資料，應可轉化成為犯罪偵查之目的使用，例如一般合法執勤所發現之證據與個人資料，當可轉換為犯罪偵查上使用[83]。

第五節　個人資料保護法

依個人資料保護法第 2 條第 1 款規定：「個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」在科技定位技術，多使用手機號碼或網路卡作為訊號

[82] 林永瀚，論前偵查程序，國立政治大學法律學研究所碩士論文，頁 51。
[83]許義寶，警察蒐集與利用個人資料職權之研究—以警察職權行使法第 17 條為中心，高大法學論叢，15 卷 1 期，2019 年 9 月，頁 90-92。

擷取來源，而訊號提供位置資訊供偵查人員跟監或找尋犯罪嫌疑人。此種手機訊號，顯然足以直接或間接識別個人資料，故應屬個人資料保護法之範疇。在實務判決「可間接識別特定個人」之資料，應理解為藉由複數之個資進行「間接連結」後，足以特定個人之「直接識別性」而言(高等法院 104 年度上訴字第 1393 號刑事判決參照)。亦有認為僅傳送電話號碼也會構成個資之侵害(高等法院臺南分院 105 年度上易字第 393 號刑事判決參照)。因此，個人資料保護法之內涵，可能是目前最符合「位置資訊」之定義，與個資法保障人格權與隱私權之目的相符。

又，依個人資料保護法第 15 條規定：「公務機關對個人資料之蒐集或處理，除第 6 條第 1 項(法律有明文規定)所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」第 16 條，公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安全或增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。・・・七、經當事人同意。」意即公務機關執行法定職務(犯罪偵查)，於法定職務必要範圍(跟監、監控、逮捕拘提)，為了增進公共利益或免除生命、身體、自由或財產之危險，即可蒐集、利用個人資料。

然，概括性的蒐集資料規範，是否足以作為法律授權基礎，最為引發爭議的，是將科技定位技術應用在防疫工作上。在疫情爆發後，各國為了避免人傳人之疫情擴大，須立即隔離染疫者及相關接觸史民眾，染疫者足跡也必須立即消毒靜置空間，因此掌握行蹤變成防疫首要工作之

一。依傳染病防治法第 48 條，「主管機關對於曾與傳染病病人接觸或疑似被傳染者，得予以留驗；必要時，並得令遷入指定之處所檢查、施行預防接種、投藥、指定特定區域實施管制或隔離等必要之處置。中央主管機關得就傳染病之危險群及特定對象實施防疫措施；其實施對象、範圍及其他應遵行事項之辦法，由中央主管機關定之。」據此，中央流行疫情指揮中心聲明疫調「電子圍籬」乃依法明定之必要措施，符合個人資料保護法蒐集、利用資料之範圍，要求民眾出入場所皆必須「實聯制」，電信業者則需蒐集、提供資料，並配合相關措施。由於電信業者提交給政府的實質內容、法律依據以及告知義務均無公開透明，且遭質疑有使用於防疫以外偵查使用[84]，引發譁然。值得注意的是，同時在各國亦面臨相同窘境，如新加坡針對防疫推行之「合力追蹤」(Trace together App)，因使用在犯罪偵查卻法無明文，引發抨擊。據此，新加坡國會隨即召開修法，修訂七大案類可將疫調資料作為犯罪偵查。[85]

在我國，個人資料保護法之規範，雖符合位置資訊定位之定義，然司法之犯罪偵查如以行政法令作為法律依據，將架空刑事訴訟法，實不宜本末倒置。

---

[84]警用「實聯制簡訊」資料辦案抓人？NCC 駁斥：僅供防疫用途，鏡周刊，2021 年 6 月 21 日，https://www.mirrormedia.mg/story/20210621edi026/ (最後瀏覽日：2021 年 8 月 23 日)。
台中地方法院法官投書刑警使用１９２２簡訊資訊聲請搜索票，經ＮＣＣ澄警方的辦案方式是依據《通訊保障及監察法》規定，經向法官申請後許可的合法調查行為，指揮中心並未提供任何資料。
會產生此種歧異，源自於疫調簡訊系統並未分流，雖事後核准通訊監察書會附註不可使用實聯制之內容作為犯罪偵查，然仍非解決之道。

[85]星立法通過 警方取用追蹤接觸者資料僅限重罪，中央社，2021 年 2 月 3 日
https://udn.com/news/story/6809/5227568(最後瀏覽日：2021 年 8 月 23 日)
新加坡政府頒訂新冠病毒暫行措施專法(COVID-19 (TEMPORARY MEASURES) ACT 2020)，並採行各項防疫措施。其中，包括鼓勵人民將手機下載「合力追蹤 App(Trace together App)」並領用「合力追蹤器(Trace together token)」於出入公共場所時，採行實聯制登錄紀錄，便於政府掌控染疫者行蹤等。然而，於此措施實施後，遭質疑稱有執法者可將追蹤資料做為偵查犯罪使用的顧慮，引起人權組織對個人私隱的關注，而新加坡國會也因此緊急將 2020 新冠病毒暫行措施專法提列增修法案。增修法條明文規定合力追蹤應用數據和追蹤器，可以用在七大類嚴重犯罪案件的調查工作和法庭程序上，同時也明確限制警方及執法部門的使用權限，只有符合調查謀殺、綁架、恐怖主義等 7 種嚴重罪案時，才可索取「合力追蹤」資料。此外，濫用資料公務員以及拒絕提交資料者均須面對刑罰。

第四章 美國與德國法制之觀察

第一節 美國法

在美國，關於利用行動電話訊號所進行的追蹤紀錄，涉及到了警察機關取得該訊號資訊的程序規定，其中包括了「聯邦收發話記錄監察法」(the Pen Register/Trap Act、中文有譯為電話撥號紀錄器法)、「聯邦通訊服務提供業者協助執法條例」(CELLA)，以及「聯邦儲存中通訊監察法」(the Stored Communication Act , SCA、有譯為存儲通訊法)。依據聯邦收發話記錄監察法，在獲得法院授權後，警察機關可以藉由裝設收發話訊號紀錄器即時地取得電話通信裡的收受(incoming impulse)、撥號(dialing)、路徑(routing)、位址(asdressing)及訊號(signaling)資訊。[86]「聯邦收發話記錄監察法」主要規範的是向未來之非內容性通訊，「聯邦儲存中通訊監察法」(SCA)規範的是過去的通訊內容。

在法案的規範，可分為程序及實質要件兩方面，程序要件的部分，法案採取令狀原則，亦即，除非有法定的例外情形，偵查機關在電信業者處裝設收發號碼紀錄器前，必須要事先取得法院所核發的命令。實質要件部分，偵查機關在聲請法院命令時，必須要敘明紀錄器所可能取得的資訊與所要進行的犯罪偵查間有其關聯性審查，監察期間不得超過 60 日。偵查機關欲延長者，必須依上述的聲請程序為之，延長的其間也不得逾 60 日。[87]

美國警察機關調閱行動通訊位址依據「聯邦收發話記錄監察法」及「聯邦儲存中通訊監察法」(SCA)，並主張，依 SCA 的§2703(C)(1)可以命行動電話服務業者提出行動電話用戶在通話時所使用的基地臺位址等資料(cell-

[86] 李榮耕，數位時代的搜索扣押，2020 年 4 月，初版，頁 111。
[87] 李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，第 115 期，2010 年 6 月，頁 127-129。

site data)，以及(一)行動電話訊號位址資訊屬於聯邦收發話記錄監察法中所定義的「訊號」；(二)CELLA 僅規定，不能單憑聯邦收發話記錄監察法的授權取得行動電話訊號位址資料，該條例並未禁止警察機關依其他法規授權後可以取得之[88]；(三)若取得同時和於這兩個法案的法院命令，就可以合法地利用行動電話訊號位址技術追蹤特定人的活動路徑及位置。[89]在早期，實務認為若分別向法院取得法院命令，即可查詢行動電話訊號(未來)位置資訊，然晚近判決可見，多數法院傾向仍需符合令狀原則。

以科技定位技術偵查之 GPS 追蹤偵查為例，在聯邦收發話記錄監察法 18U.S.C§3117 規範「從追蹤器發出之通訊」規範中，其內容稱「追蹤器」是一種允許追蹤人或物體移動的電子或機械裝置，截取進入之電子或其他脈衝以識別起始號碼或其他撥號、路徑選擇、定址及訊號發射資訊，而以合理可能得識別有線或電子通訊之來源的一種裝置或程序，惟不得包含任何通訊內容，且命令授權在法院管轄內使用追蹤器，而當追蹤器在法院轄區內安裝後，亦得在管轄範圍外使用之[90]，然，現今在合理隱私期待流變下，美國聯邦最高法院作出判決，認為裝設 GPS 追蹤器屬搜索之一環，須遵循令狀原則。

	名稱	規範項目	我國法制
A	聯邦收發話記錄監察法(the Pen Register/Trap Act)	電話通信裡的收受、撥號、路徑、位址及訊號資訊	GPS
B	聯邦通訊服務提供業者協助執法條例(CELLA)	電信業者協力義務	

[88] CELLA 規定，當政府取得法院令狀或其他合法授權時，電信業者應協助政府取得電話識別資訊。但如單獨使用電話撥號紀錄器或追蹤器時，電信業者提供之電話識別資訊，不得包含任何會顯露用戶所在位置之資訊。

[89]李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，2010 年 6 月，第 115 期，頁 112

[90]黃政龍，美國行動電話定位追蹤法規範研究、警大法學論集，第 18 期，99 年 4 月，頁 171-172。

C	聯邦儲存中通訊監察法 (SCA)	過去結束的通訊內容	調取票：使用者資料、通信紀錄；搜索票：電子郵件、伺服器內容
D	聯邦通訊監察法 (The Wiretap Act)	未來的通訊內容	通保法、通訊監察書：通訊內容
位置資訊：早期 A+C ；晚近，A+第四條修正案令狀原則			

第一項 合理隱私期待

無論是法律的條文或是傳統學理上，我國刑訴法對於搜索的界定，與美國聯邦最高法院早年的判決極為相仿。依刑訴法，搜索的客體雖然包括「電磁紀錄」，但仍是以「身體」、「物件」、「住宅」或「處所」為主，限於物理性地侵入有形的空間(physical instruction)，藉以發現有形體之物件或人(tangible objects)，並取得其佔有或為拘捕。[91]此外，傳統學者也多將「搜索」理解為「搜查檢索」[92]。由於在傳統概念下，隱私權界線各有主，在美國判斷標準的流變，從財產權(Property-based Approach)到隱私權基準(Privacy-based Approach)及第三人原則(Third-Party Doctrine、自願揭露法則)，近年發展出各項判斷法則，與科技定位技術偵查所應有之法律授權基礎，息息相關。

從財產權到隱私權基準發展，明顯從 Katz v. United States[93]案開始，在本案美國聯邦探員在公共電話亭上方外安裝電子監聽設備而取得通話內容證據，已侵害了公共電話亭使用者的隱私權[94]。在 kazs 案，Harlan 大法官協同意見書內闡述了「合理隱私期待」，依據美國憲法第四條修正案[95]，人民

[91]李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，2010 年 6 月，第 115 期，頁 96。
[92] 陳樸生，刑事訴訟法實務，1999 年，頁 208。
[93] 王兆鵬，重新定義高科技時代下的搜索，月旦法學雜誌，2003 年 2 月，第 93 期，頁 166-182。
[94] Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967)。
[95]人人具有保障人身、住所、文件及財物的安全，不受無理之搜索和拘捕的權利；此項權利，不得侵犯；除非有可成立的理由，加上宣誓或誓願保證，並具體指明必須搜索的地點，必須拘捕的人，或必須扣押的物品，否則一概不得頒發搜捕狀。

不受無理之搜索和拘捕的權利，除非有相當理由(probable cause)並具體指明必須搜索的地點，並聲請搜捕狀(the warrant requirement、令狀原則)。在隱私權的判斷，必須具有真實主觀隱私期待(主觀條件)及符合一般客觀大眾期待(客觀條件)。又如 oliver 案[96]，住宅旁之開放空地，雖屬於被告財產，也標示了禁止進入之看板，但在任何經過的人都可以目視可見，被告不得主張有隱私合理期待(客觀條件)，故不符合搜索。對比早期在 Olmstea 案[97]，警察監聽被告辦公室(公共空間非個人財產物品)，認定為侵犯個人財產權而符合第四條修正案之觀點，有相當大的調整。在此判斷標準，我們尋求的是主觀及客觀綜合判斷之隱私權，而不因物理空間限制(實際上以科技發展的速度，用傳統物理空間區分解釋是否有隱私權，已不足以涵蓋所有事實行為)。

第二項　第三方原則

根據第三方原則（Third-Party Doctrine），在個人自願揭露向第三方提供信息，不具有「合理隱私期待」，即不屬於憲法第四條修正案之適用。在 United States v. Miller[98]案，法院認為警方調取銀行紀錄(如信用卡)，是個人已同意向銀行提供之訊息，沒有合理隱私期待；Couch v. United States 案[99]，法院認為金融稅務資料，亦屬於個人自願揭露之訊息；Smith v. Maryland 案[100]中，最高法院裁定警方向電信公司調取通聯記錄等訊息，是個人為了取得電信公司的服務，自願提供之資料，故無需聲請搜查令。

然後，在 Carpenter 案[101]，法官開始對於第三方法則，產生歧異。法院在本案認為，警方向電信公司調取基地臺位置資訊中，應遵循令狀原則。

---

[96] Oliver v. US , 466 US 170, 104 S.Ct. 1735 (1984)
[97] Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564 (1928)
[98] United States v. Miller, 425 U.S. 435, 443 (1976)。
[99] Couch v. United States, 409 U.S. 322, 335 (1973)。
[100] Smith v. Maryland, 442 U.S. 735, 743－44 (1979)。
[101] Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018)。

Carpenter 案中，Gorsuch 法官表示支持使用第四條修正案，係因根據普通法，委託是財產的非所有權轉移，委託人將個人財產的實際佔有轉移給受託人一段時間，但保留所有權。受託人以信託方式持有個人財產，並在一定時間將財產交還給委託人。因此，受託人負有法律義務，即應保護財產。Gorsuch 法官認為，將財產託付給他人，並不代表能讓他們全權使用它，不論出於任何目的。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，也因此，當第三人將資訊內容轉交給國家使用，當事人應自負風險。

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。[102]

第三項 基地臺定位判決

Carpenter v. United States[103]案，2011 年警察逮捕 4 名涉嫌搶劫商店的男子，涉案人並坦承在密西西根州和俄亥俄州搶劫了 9 家商店，經過指認其他共犯，並提供涉案相關之手機號碼，檢察官依據此，依據「聯邦儲存中通訊監察法」(SCA)申請法院命令，獲取 Carpenter 及部分犯罪嫌疑人之手機紀錄，依據該法，允許執法機關在「提供具體可闡明的事實」及「表明有合理理由相信」對於「刑事調查相關且重要」，強制電信業者披露某些電信紀錄。經法院命令核准，電信業者共提供 Carpenter 四個月內共 12,898 個

[102]溫祖德，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，2020 年，第 297 期，頁 133-135。

[103] Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018)。

位置資訊，平均每天 101 個數據。在審判時 Carpenter 主張這些資訊之搜查應遵循美國憲法第四條修正案，必須有相當理由向法院申請搜查令。但在第六巡迴上訴法院維持原判認為 Carpenter 與電信業者共享位置訊息，鑒於手機用戶自願將位置資訊傳給營運商以達到通信手段，對於該位置資訊缺乏合理隱私期待，無權獲得第四修正案的保護。

2018 年 Carpenter 上訴最高法院判決獲得反轉，最高法院首席法官 Roberts 闡述多數意見，認為位置資訊仍屬合理期待隱私範圍，並揭示第四條修正案精神認為應聲請搜查令。其中提及了 Jones 案中在車輛裝設 GPS 相比，雖然人們經常離開他們的車輛，但總是強迫性地隨身攜帶手機，人們隨身帶著手機，穿過公共街道，進入私人住宅和其他可能暴露的地方，並引用 Riley v. California 案[104]的社會調查，認為有近四分之三的智能手機用戶表示大部分時間都在距離手機 5 英尺以內，另有近 12%的人承認，甚至在淋浴時都會使用手機，因此認為當跟蹤手機的位置時，可能會實現近乎完美的監控，就像是將電子監控設備連接手機用戶身上。[105]在 SOTOMAYOR, J.法官意見書，提及「儘管此類記錄是出於商業目的而生成的，但這種區別並不否定 Carpenter 對其物理位置隱私的預期。」在該判決可知，雖然手機用戶為了使用電信服務，必須同意電信業者記錄位置資訊，用以計算費率、紀錄統計等，但基於商業目的同意揭露個人隱私，不若調閱銀行資料，已構成合理隱私期待，須法官保留聲請搜查令。

[104] Riley v. California, 573 U.S. 373 (2014)。

[105] 判決原文節錄 "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. Accordingly, when the Government tracks the location of a cell phone, it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user. "

第四項 「Cell-site Simulators」判決

在本文第二章，對於我國使用之「M 化偵查網路系統」(Mobility Location Tracking System)之原理設備已有介紹，而在美國，使用此類設備多稱為「Stingray」、「cell-site simulators (CSS)」、「IMSI catchers」[106]。根據統計，此類設備至少在美國其中的 27 個州及哥倫比亞特區，有聯邦調查局(FBI)、緝毒局管理局(DEA)，國家安全局(NSA)、國土安全部（DHS）、移民和海關執法局(ICE) 正在使用這些設備。雖然，執法機關聲稱僅有攔截 IMSI，仍有部分證據顯示此種設備有攔截信息、欺騙來電者身分之可能性。[107]在全球，執法人員目前已在使用基地臺模擬器蒐集資料，調查大大小小的犯罪案件與民事侵權案件。除了刑事案件，聯邦移民及海關執法局（ICE），在底特律(Detroit)也使用基地臺模擬器來逮捕非法移民，邁阿密(Miami)警方亦在 2003 年首次購入基地臺模擬器，用以監控會議外的示威者。[108]另，因虛擬基地臺有攔截訊號功能，可能導致緊急情況時第三人之通訊障礙等問題，因此，在各州重視下，開始立法相關科技定位技術偵查之法案。

第一款 State v. Andrews[109]

犯嫌 Kerron Andrews 涉嫌在巴爾的摩市斯塔福德街街區購買毒品時，向三人開槍，被指控犯有與槍擊、謀殺未遂等罪行。2014 年 5 月 5 日，巴爾的摩市警察局 (BPD) 在沒有搜查令的情況下，使用名為

[106] 電子前鋒基金會(EFF)，美國人權團體針對政府使用，Cell-Site Simulators/IMSI Catchers 相類設備報導、https://www.eff.org/pages/cell-site-simulatorsimsi-catchers(最後瀏覽日 2021 年 11 月 5 日)。

[107]美國公民自由聯盟(ACLU)，Stingray Tracking Devices: Who's Got Them? https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingraytracking-devices-whos-got-them(最後瀏覽日 2021 年 10 月 17 日)。

[108]電子前鋒基金會(EFF)、翻譯沈威宏(最後瀏覽日期:2021 年 11 月 21 日)。https://lab.ocf.tw/2021/05/24/street-level-surveillance/

[109]State v. Andrews, 227 Md.App.350,(2016)。

「Hailstorm」基地臺模擬器，追查 Andrews 的手機傳輸信號，因而警方鎖定位於巴爾的摩市克利夫頓大道 5032 號的住宅內的精確位置。經由「Hailstorm」基地臺模擬器，警方進入鎖定位址，發現 Andrews 正坐在客廳的沙發上，並根據有效的逮捕令逮捕了他，並在 Andrews 褲子口袋內發現鎖定之手機，以及在沙發坐墊上發現了一把槍。

在本案，法院認為以定位和跟蹤手機及其用戶在公共和私人空間的移動，這項技術將使政府能夠發現任何用戶的私人和個人習慣，屬於美國憲法第四條修正案保障，必須要有搜查令。故本案搜查中獲得的證據依據毒樹果實理論排除。

第二款 United States v. Lambis[110]

2015 年，緝毒局（DEA）偵辦國際販毒組織案件，在針對目標犯嫌之手機註冊訊息及位置信息(通信紀錄)調閱後,確定目標位於「華盛頓高地 177 街及百老匯附近」，但無法至別特定的建築物或樓層。為了尋求更精確的位置，緝毒局使用了 Cell-site Simulator 模擬基地臺（有時稱為 StingRay、Hailstorm 或 TriggerFish)透過強制手機的設備將訊號傳輸到模擬基地臺，經過設備計算訊號強度，直到確定目標手機。由操作 Cell-site Simulator 技術人員進入目標建築物後，在大廳走動偵測，直到找到信號最強的特定地點，鎖定位置，在偵查人員經 Lambis 父親同意進入住宅後，現場發現了毒品、磅秤、空拉鍊袋及吸毒工具。

本案法院判決，使用 Cell-site Simulator 模擬基地臺，屬於美國憲法第四條修正案保障，必須要有搜查令。判決主要論述，依據 Kyllo v. United States 案[111]，該案認為當執法機關使用熱成像設備檢測住宅發出的紅外輻射時，屬於美國憲法第四條修正案的搜索。在 Kyllo 案法院認為，隔

[110] United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016)。
[111] Kyllo v. United States , 533 US 27 (2001)。

牆觀察將使被觀察人受制於先進技術，其中包括可以識別家中所有人類活動的成像技術，例如可能偵測到女屋主是否在洗澡。法院進一步說明，政府使用一種不常用於公共用途的設備，來探索在沒有物理侵入的情況下不可知的房屋細節，監視就是一種「搜查」，在沒有搜查令的情況下推定是不合理的。雖然執法機關提出爭執，認為法院擔心政府可能會使用諸如熱成像設備之類的設備來了解有關房屋內部的更多私密細節，但模擬基地臺並不會獲得住宅內的任何私密細節，但未獲法院採納。又，法院引用 Thomas 案[112]中，利用訓練有素犬類嗅聞住宅內的毒品，執法機關可以獲得無法通過使用自己的感官獲得的訊息。法院認為，被告享有合理的期望，即住宅有保持私密的期待，意即從門外無法「感知」到這些內容的期待，但若是在公共場所，如機場嗅聞，則不可主張合理隱私之期待。因此，法院判決本案應有搜查令狀，後續取得之證據始具有證據能力。

第三款 State v. Tate[113]

2009 年 6 月 9 日，威斯康辛州密爾沃基的超市發生一起兇殺案，抵達後，警察發現一名受害者躺在路邊和人行道之間，頭部中槍致命。第二名受害者因左腳踝的槍傷被送往醫院接受治療。目擊者將槍手描述為一名身穿條紋馬球衫的黑人男性。警方在超市監視器影像畫面發現，一名與目擊者描述相符的犯罪嫌疑人在店內購買了一部預付卡手機，然後離開店面，朝受害者的後腦勺開槍。將手機賣給犯罪嫌疑人的店員告訴警方，嫌疑人自稱「Bobby」並稱自己當天剛出獄。警方隨即根據店員提供嫌疑人購買的電話的信息，使用數據庫確認手機的服務提供商，並依據這些事實，向地方檢察官 Grant Huebner 申請批准以下命令： 1、安裝和使用釣魚及追蹤裝置或程序；2、記錄裝置使用的過程；3、偵測包括基地臺活動和位置以及可以識

[112] United States v. Thomas , 757 F.2d 1359, 1366－67 (2d Cir.1985)
[113] State v. Tate, 849 N.W.2d 798, 2014 WI 89 (Wis. 2014)。

別目標手機物理位置的全球定位系統 (GPS) 信息[114]，並獲得法官核准命令。

據此，警方使用「StingRay」在西漢普頓大道 5700 街區鎖定一間公寓大樓，並逐戶訪查，查訪中一名住戶指稱「Bobby」現正在臥室睡覺。警方經同意進入公寓，後發現犯嫌正睡在臥室，身上還有一件條紋馬球衫和一隻似乎有血跡的網球鞋和手機，當場以一級故意殺人罪逮捕了自稱「Bobby」的 Tate。

在這個案子 Tate 不爭執殺人罪之事實，但針對警方使用「StingRay」設備僅有法官核准命令，而法官的命令並不等同於搜查令，沒有法官核准的搜查令，不符合美國憲法第四條修正案。巡迴法院在評估後，法官 Jeffrey Wagner 認為該執法追蹤，屬於搜查，因此需要有搜查令狀。但本案警方不需要特定的法定授權來發布授權用於跟蹤 Tate 手機的程序的命令，因為該命令得到了法院核准之命令，且核發之命令確實符合州法 Wis. Stat[115]的精神。依據該州法令之搜查令和刑事傳票法規，其中已表達了有關使用搜查令和刑事傳票程序的立法選擇。巡迴法院最終推論，在本案法院命令目的及精神，已符合手機追蹤授權基礎，故駁回 Tate 上訴。

第五項 GPS 判決

在早起，GPS 判決在法院見解，並不屬於第四條修正案之範圍，也就是無需聲請搜查令。如 United States v. Garcia 案[116]，警方偵辦毒品案件在嫌犯車上裝設 GPS，法院判決警方只是使用 GPS 定位追蹤器取代跟監，不構

[114] 搜查令狀聲請原文摘錄 Assistant District Attorney Grant Huebner applied for an order approving the following: (1) installation and use of a trap and trace device or process; (2) installation and use of a pen register device or process; and (3) the release of subscriber information, including cell tower activity and location and global positioning system (GPS) information that could identify the physical location of the target phone.

[115] 威斯康辛州搜查令法案。

[116] United States v. Garcia, 906 F.3d 1255 (11th Cir. 2007)。

成美國憲法增修條文第四條所規定之搜索；在 United States v. Marquez 案[117]，聯邦第八巡迴上訴法院裁決，警方在公共場所時在車上安裝非侵入性的 GPS 定位追蹤器，並且監控只持續合理期間，使用 GPS 定位追蹤器持續監控在公共道路上的車輛行踪無須取得搜索令；在 United States v. Knotts 案[118]，警方在經由藥品商同意，在嫌犯所訂購之三氯甲烷原料桶內，裝置 GPS 並目視跟追監視，據以找到毒品工廠據點，經過蒐證後查獲製毒工具及毒品成品，經法院判決認為警方在公共場所使用 GPS，只不過是輔助肉眼跟蹤之不足，並不構成搜索，從而無庸有法院令狀之事先許可[119]。一直到了 United States v. Jones[120]案，法院見解開始發生了轉變。

2004 年，哥倫比亞特區夜店經營者 Antoine Jones，因涉嫌販賣毒品而成為聯邦調查局調查目標。警方採取了目視監控、在夜店前門安裝錄影器材，及監聽犯嫌手機等偵查手段。基於蒐集的證據，在 2005 年，調查人員向美國哥倫比亞特區地方法院申請授權令，授權在 10 天內向犯嫌車輛，在哥倫比亞特區內的範圍安裝 GPS 設備。然而，調查人員在第 11 天(並且不是在哥倫比亞特區，而是在隔壁的馬里蘭州)，在車輛停在公共停車場時安裝了 GPS 設備，並在接下來的 28 天裡，政府使用該設備來跟蹤車輛的行動軌跡。通過 GPS 信號，設備在 4 週內轉發了 2,000 多頁數據。在調查人員查獲毒品後，根據 GPS 設備蒐集資訊顯示，Jones 經常出入共謀者藏匿 85 萬美元現金與 97 公斤的古柯鹼以及 1 公斤古柯鹼原料的犯罪處所，因而陪審團做出有罪裁定，聯邦地方法院判處 Jones 終身監禁。

本案在 Jones 上訴後，聯邦上訴法院採 United States v. Maynard 案

[117] United States v. Marquez, Case No.: 3:19-cr-4626-BTM-1 (S.D. Cal. Nov. 25, 2010)。
[118] United States v. Knotts, CASE NUMBER 6:20-CR-00086-JDK (1983)。
[119]林利芝，從美國最高法院 United States v. Jones 案分析美國政府運用 GPS 定位追蹤器探知個人位置資訊之適法性，月旦法學雜誌，2018 年 1 月，頁 180-183。
[120] United States v. Jones, 132 S. Ct. 945 (2012)。

提出之「馬賽克理論」(the Mosaic Theory)[121]，認為長期監控一個人，個人資訊被一點一滴地蒐集起來，就像拼一片一片的馬賽克一樣，最後會拼湊出對這個人的完整圖像，「量變」產生「質變」[122]侵害這個人的隱私權。法院亦引用了 Katz 案的「合理隱私期待法則」， 認為，侵犯了 Jones 對其整體行蹤的合理隱私期待，構成非法搜索。雖然法官一致同意使用 GPS 構成憲法第四修正案之搜索，但理由不全相同。Scalia 大法官代表多數意見，主張 GPS 裝置安裝於私人座車以獲取犯罪資訊之行為，應屬對私人財產之物理侵入。Alito 及 Sotomayor 等大法官雖肯認多數意見書之結論，惟其並不同意多數意見援用「物理侵入」判斷標準，主張應採用「合理隱私期待」標準。Sotomayor 大法官認為，有鑑於「第三人法則」對於現今數位時代的民眾消費服務產生必然不可忽視之隱私風險，民眾不應基於有限目的主動向公眾一些成員提供個人資訊，即喪失那些資訊的隱私保護。據此，Sotomayor 大法官表示要重新思索「第三人法則」在先進科技下保護個人隱私的可行性及適法性。[123]在 Jones 案後，美國各州針對 GPS 判決發生反轉，確立了使用該類設備與隱私權密不可分，使用前應聲請法院令狀，始符合憲法第四條修正案之精神。

現今在美國，GPS 設備的使用，系依據聯邦刑事訴訟規則第 41 條(a)(2)(E)之規定。追蹤裝置之定義，則規定於美國聯邦法典第 18 章第 3117 條(b)，該法典明文「本條中所指『追蹤設備』一語係只允許追蹤人或物活動的電子或機械設備。」而安裝與使用追蹤設備，依聯邦刑事訴訟規則第 41

[121]或譯為「鑲嵌理論」，即如馬賽克拼圖一般，乍看之下微不足道、瑣碎的圖案，但拼聚在一起後就會呈現一個寬廣、全面的圖像。個人對於零碎的資訊或許主觀上並沒有隱私權遭受侵害之感受，但大量的資訊累積仍會對個人隱私權產生嚴重危害。

[122] 部分學者認為此說會有爭議，無法推論蒐集多少的「量」會產生質變，如裝設 GPS 達 7 天，亦會構成侵害隱私權。

[123]林利芝，從美國最高法院 United States v. Jones 案分析美國政府運用 GPS 定位追蹤器探知個人位置資訊之適法性，月旦法學雜誌，2018 年 1 月，頁 185。

條，需有令狀始得為之。在規則第 41 條中規定，核發主體為治安法官，根據聯邦官員或檢察官聲請，對轄區內的人或財產核發令狀，如人或財產有移動至管轄以外之區域，仍得對之核發令狀。在實質規範上，追蹤裝置的令狀須明確表明追蹤的人或財產，並註明令狀返還的法官與使用裝置的合理期間，該合理期間不得超過自核發令狀日起 45 日，但法院得基於正當理由予以延長，每次延長不得超過 45 日，而安裝需在令狀所載期間內，不得超過 10 日內完成，且除非法官有正當理由授權於其他時間安裝，否則應在日間安裝，最後，在執行期間過後，10 日內執行官員應歸還令狀予指定法官，並送達令狀影本予追蹤對象，如追蹤對象之救濟途徑，則是需依規則第 12 條，於本案訴訟中的審前程序，聲請證據排除。[124]

第二節　德國法及判斷標準

就歐洲聯盟（Europäische Union，簡稱歐盟 EU）及其前身的歐洲共同體（Europäische Gemeinschaft，簡稱歐體 EG）而言，很早已經開始注意個資在刑事追訴中的重要性以及刑事偵查與人權保障在個資保護範圍中的緊張關係。就人權而言，例如歐盟綱領（EU）2018/680 於立法理由明文指出，「個人資訊在處理中的保護屬於基本權利。依歐盟人權公約第 8 條第 1 項[125]以及依歐盟運作條約第 16 條第 1 項等，任何人都享有個人資訊保護的權利」。既然個資保護屬於基本權利，限制該基本權利需經過個人同意，或基於明定的法律依據。後者不僅要法律明定，另還

[124]林誠澤，GPS 科技定位偵查與刑事訴訟法的搜索概念，國立政治大學法律學系碩士班碩士論文，頁 30-32。

[125]歐洲人權公約第 8 條所保障之私生活應受尊重之權利。該規定如下：「1. 任何人皆享有其私人生活、家庭生活、居住與通訊受尊重之權利。2. 前項權利之行使，不受公權力之侵犯。但基於民主社會中國家安全、公共安全或國家經濟福祉之利益、為防止失序或犯罪、為保護健康或道德，或為保護他人之權利與自由所必要，且依法為之者，不在此限。」

要符合比例原則，以免發生不當擴充等現象。[126]德國立法者於 1999 年刑事訴訟法之修正中創設了所謂「偵查概括條款」，有鑑於犯罪型態不斷轉變以及偵查手段必須對應地創新，因此有此等所謂偵查概括條款之產生，不過一般認為，對於基本權力干預較深的偵查手段，此等概括條款並無法替代憲法上與刑事訴訟法上之個別干預授權要求，例如對犯罪嫌疑人的長期監視，則不得援引此為根據，而須有個別的授權條款。[127]

在德國沒有訂定科技偵查的專法，而是將科技偵查手段規定在刑事訴訟法（StPO），大致可分為，住宅外監聽（§100f）、住宅外監視科技方法與長期監視（§100h, 163f）、對行動通訊設備之科技偵查（§100i）、秘密偵查措施之通知與救濟（§101）。在德國，電信從「社會互動（soziale Interaktion）的觀點」，是指人與人之間透過電子媒介進行意見交換的過程，國家介入此過程並且知悉交換的內容，被視為是「電（通）信監察」[128]。德國科技偵查條款規定在刑事訴訟法第 100a 條以下。第一個是針對網路電話監聽的 「來源端電信監察」，例如針對 LINE 電話監聽(§ 100a I S. 2, 3 StPO)。德國刑訴本來就有電話監聽條文，網路電話監聽則是 2017 年增訂的，我們法務部草案裡面則稱它是設備端通訊監察。第二個是線上搜索(§ 100b StPO)，也就是使用木馬侵入電磁設備，第三和四個是住宅內或住宅外的非公開談話的監聽 (§ 100f StPO) 。第五個是住宅外監視定位追蹤，是住宅外的監視定位追蹤(§ 100h StPO) ，像無人機。第六個是 IMSI Catcher，指截取國際行動用戶識別碼或國際行動設備識別碼(§ 100i StPO)，例如 M 化車。還有一個是我們目前比較陌生的科技偵查「無聲簡訊」。無聲簡訊偵查

[126]葛祥林，數位化、大數據和人工智慧對刑事訴訟的衝擊，高大法學論叢，2020 年 3 月，第 15 卷第 2 期，頁 54。

[127] 吳耀宗，警察在犯罪偵查程序的角色與權限之再思考，犯罪與法之抗制，2006 年 3 月，頁 207-208。

[128]吳俊毅，德國刑事訴訟上使用衛星定位技術進行監察之研究，中正大學法學期刊， 107 年 4 月 29 日，頁 40。

技術，我國並未使用，與「釣魚連結偵查」亦不相同，無聲簡訊是一種發送特殊簡訊到目標手機，透過基地臺登錄紀錄，再向電信業者調閱手機位置的科技方法。[129]在德國，基於科技偵查是秘密性的手段，因此在規範上都有詳盡的程序配套，包括審核機關、禁止干預取證、事後救濟、通知義務。

第一項 隱私權

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，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，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 3、對於取證對象的基本權具體侵害的嚴重程度；第三階層則是一般社會接觸領域， 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[130]。

基於歐洲人權公約第 8 條所保障之私生活，「任何人皆享有其私人生

[129]王士帆，德國聯邦最高法院刑事裁判 BGHSt 63, 82 —發送「無聲簡訊」的法律基礎—，司法周刊，109 年 12 月 31 日。有關「無聲簡訊」在王士帆老師論著說明詳盡，摘錄部份內容，據德國國會調查，早在 2014 年，德國聯邦刑事警察局（Bundeskriminalamt, BKA）使用無聲簡訊追蹤定位的案件是 58 件、 122 人，高於 IMSI-Catcher 的 24 件。 光是 2017 年下半年，包含聯邦刑事警察局在內的德國聯邦機關，已發送 過 234,835 次無聲簡訊。不只是聯邦層級，各邦警方尤其熱衷無聲簡訊， 例如據統計，在 Schleswig-Holstein 邦，警察在 2019 年發送過 112,354 次，柏林在 2019 年有 336,569 次。被無聲簡訊鎖定的目標手機，必須是開機狀態且未設定拒收簡訊，如果手機關機，無聲簡訊便無法發送到該目標手機。無聲簡訊發送成功後，手機不會發出聲響，螢幕和簡訊匣也不會顯示，手機使用人除非有安裝反制或監控 APP，否則根本不能察覺無聲簡訊的入侵。手機收到無聲簡訊，會如同平常收到一般簡訊，自動回覆數據到其功率最強或距離最近的登錄基地台，然後在各電信服務業者處產生通信紀錄。之後，當偵查機關向電信業者調取目標手機的通信紀錄，即可查明手機接收無聲簡訊時點的大約所在位置。

[130]林育賢，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，司法新聲，法務部司法官學院第 135 期，頁 41。

活、家庭生活、居住與通訊受尊重之權利」。有關公共場所之隱私權保障的辯論，從 1997 年 8 月英國威爾斯王妃戴安娜，於法國巴黎因狗仔記者飛車追逐，不幸車禍喪生後，歐洲各國對於新聞工作者以全天候攝影跟追公眾人物，以作為新聞報導題材的作為（所謂「獵奇攝影者」(paparazzo)），開始了法律規範的反思與討論。

在 2008 年 Mosley v. the United Kingdom 案[131]，衛報集團（Guardian News & Media Ltd）的周日報紙，將 FI 賽車公司老闆參與某個性愛派對者所偷拍的錄影片段截錄成短片和靜態照片上網公開，並予以公開報導，雖經過原告律師提出抗議。世界新聞報在隔天立刻將網站影片下架，原告律師主張衛報集團（Guardian News & Media Ltd）侵害原告的祕密，並且對其隱私造成損害。歐洲人權法院則認為，當新聞報導所揭露的系爭資訊乃屬個人私密資訊，而且其揭露與傳播毫無公共利益可言時，應受隱私權之保障，並首度針對公約平等保障之私人生活與表意自由提出判斷標準，即「公益辯論原則」。

在 Von Hannover v. Germany 案[132]中，摩洛哥公主卡羅琳因在公共場所遭到媒體未經許可偷拍並公佈照片於雜誌，因而向歐洲人權法院提出法院上訴，法官認為公約第 8 條所規定「私人生活」之保障，即非限定於特定空間或場所，而係取決於該私人活動之本質是否為公約所欲保障之範圍而定，再次肯認公共場所應享有隱私權之保障概念。隱私權在現代法律屬較新的概念，在各國案例討論後，確認為憲法層級保障地位。

自 2008 年，當隱私涉及個人資料，歐洲人權法院之標準開始趨於嚴格，歐洲人權法院開始具體的檢視個人資料的紀錄與保存情況、性質、處理與使

[131] 司法院歐洲人權法院裁判選譯（四），Mosley v. The United Kingdom, no.48009/08, §§ 16-25, ECUR, 10 May 2011，劉靜怡節譯。
[132] 司法院歐洲人權法院裁判選譯（一），Von Hannover v. Germany, no.59320/00, § 51, ECHR, 2004-VI.，蔡宗珍節譯。

用方式。歐洲人權法院在 Köpke v. Germany 案，Köpke 為一超級市場之收銀員，其有天被無通知解雇，因其雇主在超級市場內裝設隱藏之攝影機，對 Köpke 負責之收銀臺監視，發現 Köpke 有竊取收銀臺內歐元之行為。Köpke 從德國勞動法院一路敗訴至憲法法院，爾後向歐洲人權法院為申訴。歐洲人權法院認為德國未有違反公約第 8 條情事，理由在於，對於 Köpke 所為之錄影監視並非來自國家，而是其雇主。[133]歐洲人權法院認為國家並無保護義務，但法院也有注意到新興且逐漸複雜的科技，可能導致私人生活之干預。

在 2019 年 Mehmedovic v. Switzerland 案，Mehmedovic 為一對夫妻，Mehmedovic 先生某日在搭乘巴士時發生車禍，其主張因該車禍遭受之傷害造成終身的勞動力減損，從而向保險公司主張保險金 1,777,353 歐元。保險公司對此起疑，在 2006 年，挑選四天聘請私家偵探對 Mehmedovic 先生為跟監攝影，但拍攝與錄影之皆僅該夫妻處於公共場域中。保險公司獲得的資訊顯示，Mehmedovic 先生所受之傷害並沒有如他所稱的嚴重，對此，Mehmedovic 夫妻認為，保險公司這樣的行為已侵害其隱私權，而在瑞士的法院起訴，但一路敗訴後，本案終至歐洲人權法院，法院卻認為瑞士聯邦政府並未違反公約第 8 條，理由在於，本案所涉者為商業保險，被保險人與保險公司是在私法之下。而瑞士內國法院也仔細審酌、分析兩造雙方背後的利益，而認保險公司代表的利益與申訴人 Mehmedovic 先生所稱之隱私權相較，實具壓倒性[134]。

惟到了 2017 年在 Antović and Mirković v. Montenegro 案，蒙特內哥羅的國立蒙特內哥羅大學（University of Montenegro）兩名數學系的教

[133]陳宗奇，合理隱私期待之末路?-近期歐洲人權法院隱私權相關判決概述，律師法學期刊，第 5 期，
109 年 9 月 3 日，頁 93。
[134]陳宗奇，合理隱私期待之末路?-近期歐洲人權法院隱私權相關判決概述，律師法學期刊，第 5 期，
109 年 9 月 3 日，頁 94。

授表示，學校在他們授課的地方裝設了兩支攝影機是侵害隱私權的，人權法院認為則認為，因為其所授課地點為大講堂，為公共場域，其合理的隱私期待相當有限，自然沒有隱私侵害的問題。[135]基於人類社會群居生活之前提，個人生活不可能完全不受他人干擾，本即係參與社會生活所需付出之代價，同時社會生活中也自然產生守望相助、彼此觀察之需求存在。然而與他人過度頻繁、近距離的接觸，勢必將壓縮個人行動、言論自由，從而影響人格之形成。[136]因此，人與人在公共場所是社會群居必然之狀態，如何判斷是否侵害隱私權，仍須衡酌社會通念容忍程度，在公共空間區分個人不受侵擾之範圍，以保障合理界限。

第二項 資訊自決權

德國之資訊自決權，可謂始於「一九八三年人口普查法」判決。在當時，該法規定全國人口統計及社會結構詳盡資料之收集。除人口統計及個人基本資訊之收集外（如姓名、地址、性別、婚姻狀態、宗教信仰等）個人並應填寫詳細之問表答覆所得來源、職業、額外工作、教育背景、工作時間、工作往來之交通方式及其他相關事宜。法條並規定統計資訊移轉於地方政府以從事區域計劃、調查、環境保護與選區之劃分。由於該法涉及對基本權之立即侵害、該院免除須窮盡法律救濟之要件，在超過一百人申請下，該院暫時停止該法之執行、理由為將該等資訊移轉與若干行政單位涉及隱私及人格權之侵害可能。[137]聯邦法院判決理由闡述，個人資訊自決權包括保護資料不受提取、儲存、使用及繼續傳送之權利。在資訊社會中的「隱私權」界線越來越

[135]陳宗奇，合理隱私期待之末路?-近期歐洲人權法院隱私權相關判決概述，律師法學期刊，第 5 期，
109 年 9 月 3 日，頁 95。
[136]司法院釋字第 689 號，大法官林子儀協同意見書
[137]關於「一九八三年人口普查法之判決」，司法院西德聯邦憲法法院裁判選輯（一），109 年 10 月，蕭文生譯。

模糊，此社會形態下應肯定個人對本身資料擁有的自主控制權利，才能有所保護。

然，但「資訊自決權」並非絕對。人在社會中發展，個人資訊無非社會現實之反映，而不能單獨與個人連結。基本法為解決個人與社會之緊張而鋪陳出一個與社群相關並與社群結合之個人。個人原則上應因「重大之公共利益」（Compelling public interest）而接受對其個人資訊自決權之某些限制。如聯邦統計法第六條第一項所承認，基本法第二條第一項要求立法者明確規定所有官方資訊收集過程之目的及條件，使公民明白資訊收集之種類及原因。立法者並應遵守比例原則，使對基本權之限制在公共目的之必要程度內。[138]

歐盟在 1995 年開始就個人資料規範，並發布了 1995 年第 46 號指令(資料保護指令、Data Protection Directive; DPD)，該指令規定成員國在處理個人資料時，有義務保障國民的基本權利，尤其是隱私權。而個人資料的處理，則必須建立在「質的原則」(qualitative principle) 上，包括個人資料的取得就其所欲追求的目的必須符合比例，且原則上必須取得當事人同意。同時，此一指令也禁止成員國處理種族、宗教、政治傾向等敏感資料。[139]。德國憲法法院認為資訊自決權之保護是包含在基本法第 2 條第 1 項一般人格權內，內容包括一個人的人格或行為之自我形成權(Recht auf eignene Gestaltung)，即自我決定權[140]。因此認為資訊自決權是人格權及隱私權所放射出之基本權利。

[138]關於「一九八三年人口普查法之判決」，司法院西德聯邦憲法法院裁判選輯（一），109 年 10 月，蕭文生譯。

[139]劉靜怡，通訊監察與民主監督：歐美爭議發展趨勢之反思，中央研究院歐美研究所《歐美研究》第四十七卷第一期，106 年 3 月，頁 45。

[140]李震山，個人資料保護與警政資訊管理，「資訊管理學術暨警政資訊實務研討會」論文集，中央警察大學，1966 年 3 月，第 4 頁。

在歐洲人權法院 Brother Watch and Others v United Kingdom 案[141]，三個非政府組織，Big Brother Watch、English PEN 和 Open Rights Group，以及來自柏林的學者 Constanze Kurz 向法院提出申請，認為英國政府為防恐訂定之監控法令內，內容為可批量攔截通訊、可從服務商獲取通信數據以及情報之共享接收，三類監視提出質疑。2018 年 9 月 13 日，歐洲人權法院裁定英國以情報及防恐目的，蒐集大量數據收集計劃因未能納入足夠的隱私保護和監督而違反了人權法，但大規模監視和情報共享並未違反國際人權法。這是自 2013 年愛德華·斯諾登 (Edward Snowden) [142]揭露事件以來，首次針對大規模監視計劃作出裁決。在傳統概括授權的思維，認為非私密領域蒐集到之資訊，基於高度公共利益者，即可使用於刑事追訴之證據，然在此判決可知，在資訊社會，因個人自願或非自願(個人可能不知悉)之情況，所揭露資訊量過於龐大，大規模蒐集不特定人之數據資訊，顯然違反人權法。另在德國刑事訴訟法第 100d 對於監聽涉及「私生活核心領域」者，有立即應停監聽、紀錄，需銷毀及禁止使用之各項規定，強調不應損及「私人生活不可侵犯之核心領域」，即便是為了重大公益的需求，亦無法正當化對此一核心領域之侵害。私人住宅是維護人性尊嚴的「最後堡壘」。[143] 個人通訊資訊數據應與監聽所得內容相同，屬於「私人生活不可侵犯之核心領域」同受保障。

---

[141] 作者 Chinmayi Sharma，lawfare 雜誌，Big Brother Watch and Others v. the United Kingdom (application nos. 58170/13, 62322/14 and 24969/15)，https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom，(最後瀏覽日 2021 年 12 月 7 日)。

[142]2013 年史諾登向媒體揭露的是美國名為「稜鏡」（Prism）的監控計畫，該計畫從谷歌、雅虎、微軟、蘋果與其他美國科技公司的主機蒐集通訊資料，甚至與英國政府通訊總部（GCHQ）合作破解密碼與相關技術，也讓美國開發的網路竊密工具、網路攻擊程式，甚至針對外國領導人的竊聽計畫都公諸於世，引發全球嘩然。

[143]楊雲驊，保障「私人生活不可侵犯之核心領域」—德國聯邦憲法法院對於「住宅內監聽」（大監聽）違憲審查判決簡評，司法改革雜誌 62 期，2006 年 6 月 25 日，頁 32-35。
德國基本法第 13 條規定住宅不容侵犯，只有在嚴格的要件下，方可對住宅進行搜索或安置科技設備蒐證。

第三項 資訊科技基本權

德國聯邦憲法法院於 2008 年 2 月 27 日做成的「線上搜索判決」中，在論及線上搜索干預何種基本權時，從德國基本法對於一般人格權的保障(德國基本法第 2 條第 1 項結合第 1 條第 1 項)新發展出「保障資訊科技系統機密性與完整性之基本權」，德國學術文獻簡稱「電腦基本權」。[144]

與「資訊自決權」著重資訊不受提取、儲存、使用及繼續傳送，個人資訊應保有隱私權，是人性尊嚴的保障。而「資訊科技基本權」或稱「電腦基本權」所著重的是資訊的機密性與完整性，起因在於「線上搜索」的判決中，憲法法院在現有的基本權中難以尋得防禦理由，為了填補漏洞而催生此新基本權。以住宅不受侵害基本權觀察(德國基本法第 13 條)，電信秘密自由有時間上之限制，如通訊結束資料進入通訊當事人可支配範圍，電信秘密自由的保障也就跟著一併結束。如國家機關以科技設備侵入電腦設備，保障範圍則有空間上拘束，國家機關對於「人民私領域」的侵犯，必須和「住宅」有空間關聯性，而行動式資訊設備往往會被人民攜出「住宅」外使用，從而欠缺空間關聯性。

至於資訊自決權，在德國聯邦憲法法院在「線上搜索判決」中則認為，其保障範圍侷限在防禦「個別的資料蒐集」，因此對於侵入資訊系統，對於眾多資料進行存取，程度遠比「個別資料蒐集」更為強烈，難以透過「資訊自決權」加以防禦。[145]但對於是否需要此新興基本權，仍不乏反對見解，因憲法法院認為「資訊自決權」僅能限縮為「防禦個人資料蒐集」，並非多數判決的見解，且「資訊自決權」與「電腦基本權」同為人格權所導出，事實

[144]謝碩駿，警察機關的駭客任務——論線上搜索在警察法領域內實施的法律問題，臺北大學法學論叢，2015 年 3 月，頁 21-22。
[145]謝碩駿，警察機關的駭客任務——論線上搜索在警察法領域內實施的法律問題，2015 年 3 月，臺北大學法學論叢，頁 23-24。

上目的及保障範圍並無不同，故此基本權目前仍有質疑聲浪。

第四項 基地臺判決—「預防性電信監察」

在德國，「電子搜尋追緝」[146]最初是於 1970 年代為了對付恐怖活動之領域所發展出來的。在刑事訴訟上之法基礎，是由 1992 年 7 月 15 日防制煙毒販賣法與各類組織犯罪態樣法(OrgKG)，配合刑事訴訟法第 98a 條所創設的，且被視為是預防性之追緝手段。在 2001 年 911 攻擊之前各邦警察法就已經含有此種追緝手段之授權。一開始，在德國電子搜尋追緝，只能用來保護利益且要是當下即時危險。在之後，大部分之其他各邦不僅更是降低了發動門檻以及被危害之保護利益之要求，甚至有些邦立法者整個去除了危險存在之要件，將電子搜尋追緝之授權改為警察法之權限。

2003 年 12 月 11 日之下薩克森邦公共安全及秩序法增列了第 33a 條之規定，如符合重大犯罪行為及集團性或職業性所為之輕罪行為，並符合下開其中一項情形，即可透過電信監察蒐集資料內容：1、為防止個人身體、生命、自由之現時危害，在不能透過其他方法調查事實時或對於事實之調查有必要時。2、有事實足認某人有重大犯罪行為之虞者，在不能透過其他方式對該犯罪之追訴預作準備或防範該犯罪時。3、對犯罪追訴預作準備或防範該犯罪有必要者，亦得對第 2 款所稱之人的「聯繫者及其伴同者」採取電信監察。所實施之資料蒐集，得針對 1、電子通訊之內容，包括在電信網路內儲存於資料庫之內容。2、電子通訊連線資料。3、有效開通之行動通訊終端設備的位置信號。4、資料蒐集僅得及於第 1 項規定之人所為之電信連接。但資料蒐集無法避免涉及第三人者，亦得及於第三人。在聲請的規定，上開

[146]艾明，德國對技術偵查措施的法律規制，https://www.gushiciku.cn/dc_hk/100730582，106 年 6 月 7 日(最後瀏覽日：110 年 12 月 20 日)。電子搜尋追緝(Rasterfahndung)是一種資料自動化比對的偵查措施。透過預先設定某些特徵條件，與其他國家或第三方之資料進行自動化比對，從而發現可能的嫌疑人。

資料蒐集必須由警察機關所在地之地方法院核發命令，期限最長為三個月，情況急迫由警察機關首長決定做成命令後，立即報請法官追認。且基於電信監察命令，電信業者有提供資料協力義務。憲法訴願人主張，此法令已干預基本法第第 5 條第 1 項(自由表意基本權)及第 2 條第 1 項(人格之自由發展)之基本權。2006 年德國憲法法院針對 Nordrhein-Westfalen 邦警察法上之電子搜尋追緝做出裁判，認為大規模蒐集電信監察數據，系干預資訊自決之基本權[147]。

根據 Nordrhein--Westfalen 邦之說法，全國性之電子搜尋追緝標準，是為了發掘潛伏在德國之回教恐怖份子。據司法部說明，為了發掘恐怖份子，有 4,669,222 筆資料由邦內 36 個戶政登記局提出，有 474,517 筆資料被 61 所大學與大專院校所提出，以及有 89,980 筆資料係由外籍人中央登記局所提出，總計有 5,233,721 筆資料。 然後，透過資料自動化之資料對比，來過濾出比對。其中提取使用的共計 11,004 筆資料。其他剩餘之 5,222,717 筆資料一直到 2001 年 12 月 10 日才刪除、銷毀。訴願人主張：「電子搜尋追緝涉及嚴重之基本權干預。雖然電子搜尋追緝不一定觸及敏感之資料，不過光是從該追緝係在未告知當事人底下來進行，就已得出其嚴重性了。國家這種暗中蒐集資料正是會引發人民之不確定性與不安。其對基本權干預之嚴重性尤其來自於其非常高度之散佈規模。」憲法法庭則認為，電子搜尋追緝命令所根據之 1990 年 Nordrhein-Westfalen 邦警察法第 31 條第 1 項，無論在形式上或實質上均合憲。然而，電子搜尋追緝所涉及之資訊皆具有人格關聯性，以及當其與他資訊串連在一起時，可使人們透視該人格關聯性之資訊，以及具有特別人格關聯性的資訊。尤其是涉及被憲法所保護之領域之資訊，比如：種族、血統、政治見解、宗教信仰、健康或性生活，認為有可能

[147]司法院德國聯邦憲法法院裁判選輯（十三），「Nordrhein-Westfalen 邦警察法上之電子搜尋追緝是否侵犯資訊自決之基本權」裁定(BVerfGE 115, 320)，100 年 5 月，陳怡凱節譯。

侵犯基本法之資訊自決權及人格權。[148]

換言之，本案蒐集資訊雖形式及實質都符合電信監察之法規範，但法院認為，透過蒐集電信數據、戶政、教育等大量資料皆具有人格關聯性，串聯勾勒的結果，仍可能侵犯資訊自決權及人格權。

第五項 IMSI-Catcher 裁判

在德國，IMSI-Catcher 源於德國慕尼黑的羅德史瓦茲(Rohde&Schwarz)電子測量公司開發的科技產品，1996 年 12 月發明之初是作為測量系統，後來研發成探知行動通訊終端設備識別碼的機器。從 1997 年起，德國媒體有了 IMSI-Catcher 的報導，也在同一年 IMSI-Catcher 頭一次被正式列入德國聯邦政府的法案項目。[149]而事實上在此之前，偵查機關已多次使用 IMSI-Catcher 作為犯罪偵查技術設備，只是沒有公開說明而受到關注。在德國 2001 年 10 月 4 日《每日鏡報》一篇標題為「沒有法律基礎的最現代化監聽技術」的新聞報導中，敘述許多犯罪學家視 IMSI-Catcher 為「對抗犯罪的神器」[150]。與本國情形相似，在報導輿論及探討聲浪中，IMSI-Catcher 此種科技偵查技術雖然對於犯罪偵查實務有極大的幫助，但在法令上卻可能干預基本權且無法制可遵循。據統計，德國在 2001 年 11 月以前即動用了 35 次 IMSI-Catcher。惟立法進程德國直到 2002 年 8 月 14 日修正生效的刑事訴訟法修法，才增訂了第 100i 條，納入偵測手機 IMSI 或 IMEI 及手機位置的科技方法，後來 2006 年通過德國聯邦憲法法院的合憲性審查。[151]在德國相類 M 化車

[148]司法院德國聯邦憲法法院裁判選輯（十三），「Nordrhein-Westfalen 邦警察法上之電子搜尋追緝是否侵犯資訊自決之基本權」裁定(BVerfGE 115, 320)，100 年 5 月，陳怡凱節譯。

[149] 王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 63。

[150]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 64。

[151]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論

設備，常見有 IMSI-Catcher 或 Stingrays。

2002 年，德國將 IMSI-Catcher 偵查法制化訂定於德國刑事訴訟法第 100i 條，並經憲法法院合憲性審查，而在 2003 年，由民權組織、律師、自由記者及稅務顧問組成的申訴團體，向憲法法院提出申訴，認為第 100i 條違反基本法第 10 條，因為執法機構採取第 100i 條措施，只要任何手機所有者進入 IMSI-Catcher 捕捉範圍，不涉及的第三方就可能有被該措施捕捉的風險，並且被記錄個人設備或門號標誌加以識別、存儲，違反基本法第 10 條規範「書信秘密、郵件與電訊之秘密不可侵犯。」，且該設備執行時，可能會導致第三人行動電話失去訊號，影響基本權利。[152]在裁判焦點，主要圍繞在秘密通訊自由與資訊自主權，及第三人權利的干預。在 IMSI-Catcher 使用上，少數說主張應使用秘密通訊自由作為第 100i 條違憲審查基準，因為截收待機中的目標手機資訊，其在待機狀態，即表示手機持有人有接收或通訊意願，故應等同於開啟通訊過程，因此屬於秘密通訊自由保護範圍；多數說則認為 IMSI-Catcher 不涉及人為之通訊過程，所以否定其與秘密通訊自由的關聯性。[153]在裁判德國聯邦法院採多數說，指出 IMSI-Catcher 偵查方式僅屬設備之間的連結，欠缺人際之間的訊息交換，因此不在秘密通訊的保護範圍，而僅干預了資訊自決權(定位資訊)[154]。

德國憲法法院論證理由「透過使用 IMSI-Catcher，對於位在虛擬蜂巢區內的行動電話，偵測刑事訴訟法第 100i 條第 1 項第 1 款所稱的設

叢，第 121 期，頁 64。

[152]律師 Thomas Ch. Gramespacher，2006 年 12 月 10 日，Media Internet and Law（縮寫：MIR）網路雜誌，https://medien-internet-und-recht.de/volltext.php?mir_dok_id=480。

[153]王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 81。

[154]施育傑，科技時代的偵查干預處分——兼論我國法方向，月旦法學雜誌，306 期，2020 年 11 月，頁 104。BVerfG, Beschl. v. 22. 08. 2006 – 2 BvR 1345/03 判決。

備序號或卡號，並不以人與人之間發生通訊過程獲至少嘗試發生為必要...截收到的資料，不是在通訊過程中所形成，而是在行動電話待機狀態形成的，待機狀態僅是通訊的技術條件。行動電話單純具有作為通訊工具的科技適合性，以及其為了確保通訊準備就緒所發出的技術訊號，尚不構成通訊...潛在的手機通訊參與人有意通訊時，雖然無法獲得等同於未使用科技媒介的安全，然而具體狀況的通訊隱私，並不會在有通訊意願時就受到危害，除實際通訊過程外，前階段的通訊準備不應給予相同保護，一個『有可能發生』的通訊仍非通訊」[155]在審查不符合秘密通訊自由範疇，德國多數主流見解認為，IMSI-Catcher 影響的是資訊自決權，也就是保護資料不受提取、儲存、使用及繼續傳送之權利。

資訊自決權是人格權及隱私權所放射出之基本權利，與我國大法官釋字第603號闡述意旨相同。值得注意的是，依照德國憲法法院「IMSI-Catcher裁判」見解，因受到 IMSI-Catcher 影響短暫時間無法使用手機對外聯繫，所干預的是一般行為自由，法院見解認為「使用通訊設施時遇到如此輕微的干預，至少就刑事司法需求而言，應予容忍。」[156]。也就是說，第三人所受到的干擾，實屬輕微，在法益衡量下為可容忍範圍。

第六項 Uzun v. Germany

「原告 Uzun 涉嫌參與數起由「反帝國主義組織」所為的左派極端恐怖攻擊行動，以對政府進行武裝暴力攻擊為主要宗旨。自 1993 年起，Nordrhein-Westfalen 邦便開始對原告進行長期性的監控。監控的時間點主要在 1995 年 9 月 30 日起，至 1996 年 2 月 25 日兩人正式被逮捕為

[155] 王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 86。
[156] 王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 80。

止的週末期間。該調查庭法官授權監視原告平時使用之車輛、住處出入口監視錄影器，並對其使用的專業無線電通訊設備進行截聽。1995 年 10 月，聯邦犯罪調查局更進一步在車輛上，裝設了兩個無線電發送器（Peilsender），然而後來被原告 Uzun 與 S 發現，而予以拆除。此後 S 與原告 Uzun 懷疑自己遭到監聽及監視，自此不透過電話進行彼此之間的通訊，也好幾次成功地躲避掉監視人員的跟追。聯邦犯罪調查局在 1995 年 12 月由聯邦檢察總署下令於 S 車上裝設 GPS 接收器。該設備每隔一分鐘便會記錄車輛的即時行蹤。透過數據，可以計算出其車速等相關資訊。但為了避免訊號接收器再次被發現，該接收器所儲存的資料每隔一天才會由聯邦犯罪調查局的人員提取一次。這樣的監控手段一直實施到 1996 年 2 月 25 日，原告與 S 被正式逮捕才告終。」[157]

在本案，法院裁定原告 Uzun 聲請駁回，認為德國刑事訴訟法第 100c 條第 1 項第 1 款授權了系爭個案中對 GPS 系統的使用；因此，以此方式所蒐集到的資料也同樣得以用於訴訟程序中。此外，該院也駁回原告關於使用 GPS 為監控應有法官核發令狀之主張；相反地，法院認為 GPS 監控之使用，得併入其他經合法授權的監控手段，而一併取得合法性。且根據德國刑事訴訟法，相對於其他更深入侵害人民資訊自決權的監控手段，透過 GPS 所為的監控其實無需有法官之令狀授權[158]。又倘若一個監控手段相較於既有的監控措施，其干預程度相對較輕微者， 則理應得將之視為是既有監控措施之附加性措施。原告 Uzun 再次向聯邦最高法院提出抗告，而聯邦最高法院於 2001 年以其論點均無理由而駁回其上訴。法院認為，透過 GPS 等科

[157] 司法院歐洲人權法院裁判選譯（四）2018 年 11 月，Uzun v. Germany 歐洲人權法院第五庭於 2010 年 9 月 2 日之裁判(案號: 35623/05)，蔡宗珍、張君魁節譯。

[158] 此處是指德國刑事訴訟法 2000 年修法前，依照目前德國刑事訴訟法第 163f 條第 4 項的修正後，依該規定，無論是以何種監控技術、實施何種監控手段，只要為監控期間達一個月以上，即有法官保留原則之適用。

技定位裝置進行資料蒐集，並未對本案原告的家宅產生任何侵犯。又原告涉嫌係屬重大犯罪行為，因此以 GPS 監控，對其私生活領域應受尊重的權利以及其資訊自決權，屬合於比例原則的干預。

最終，原告 Uzun 向德國聯邦憲法法院提起憲法訴願。聯邦憲法法院於 2005 年 4 月 12 日駁回原告之訴。法院認為，刑事訴訟法條文中「以監控為目的之特殊技術性方法」等字句規定已足夠明確。本案所雖然是透過科技手段(GPS 追蹤器)，而觀察人員所在處所與動向，但立法者於立法表達監控方法時，並不負有將最新取證技術之使用排除在外的義務。更甚之認為，此類科技產品所為之監控，毋寧避免了更嚴重的侵犯。但有關「預見可能性」之要求，法院重申，於秘密實施監控措施之情形，授權之法律規定應足夠清楚，且應以適當方式使人民得以認知有權機關得採取該等監控措施之條件與情狀，有鑑於秘密性監控所蘊含的濫用危險，此類監控措施之實施應有更精確之法規為依據，特別是考量到持續不斷發展的新型態科技時尤然。

憲法法院說明，”無論於哪一個法領域，包含刑法領域在內，即便法律規定之表達極其清楚，仍存有法官之解釋空間。釐清疑點並因應不斷改變之事態而為法之適用，始終有其必要。事實上，透過法官造法所為之刑法續造，均已為所有締約國法治傳統下已建立且有其必要的部分。人權公約絕非禁止法官透過法律解釋方式，逐漸於個案中精確化刑罰規定內容，只要此等作法之結果最後得以符合犯罪行為之處罰的本旨，並具備合理的預見可能性。”[159]

由此可知，在面對新型態科技監控措施的態度，法院認為是有公約第 7 條適用，但在合理預見性以及防止濫用判斷下，仍須依照整體實施種類、範圍、期間、執行監督、救濟方式，作為判斷標準，已提出明確的方向來檢視

[159]司法院歐洲人權法院裁判選譯（四）2018 年 11 月，Uzun v. Germany 歐洲人權法院第五庭於 2010 年 9 月 2 日之裁判(案號: 35623/05)，蔡宗珍、張君魁節譯。

各種新型態科技監控手段之方式。在判決中，法院進一步說明，因 GPS 監控方式既非視覺性監控、亦非聽覺性監控，特別是該種監控方式是用以「定位出行為人之停留地點」。由於裝設 GPS 本身非屬監視或監聽，而是藉由 GPS 接收器之裝置而對該載體進行定位追蹤，從而也可以對與該載體同行之人進行定位追蹤，亦為刑事訴訟法第 100c 條第 1 項第 1 款之規定所涵蓋的見解，乃屬系爭規定在法官解釋法律方式下之合理可預見的發展。判決中認為本案符合重罪、最後手段、比例原則，且在使用之前竭盡各種可能之方法，但仍無法完全符合法律明確性，是在新型態科技發展時代更是需要面對的課題。

現今，德國刑事訴訟法第 100h 條(使用其他特別為監視目的所設之科技方法)為 GPS 偵查的法源依據，透過一個概括條款作為法源依據。這個條文是從 1992 年就制定（原為第 100c 條第 1 項第 1 款）且不斷的修法，最近修法是在 2019 年，第 100h 條涉及的是核准要件和干預限制，德國通說認為這樣的規定有涵蓋到 GPS 與空拍機。[160]也就是說，在立法上德國考慮科技具有開放性及革新性之巧思，未將條文制定侷限為單一工具，值得效仿學習。另在本條文針對非被告之「相關其他人」亦有適用，在「查清案情或調查被告所在地」採取其他方式可能收效甚微或非常困難可為之，但仍須具備必要性及最後手段性等原則。

第七項　住宅外長期監視錄影

被告 A 涉犯多起竊盜罪。警方為了調查 A 夜晚外出時間、返家攜回之物品，甚或揪出同夥，決定在 A 住家對面暗中架設監視設備，鏡頭對準 A 住家大門區域和前方人行道。此秘密錄影全天候不間斷，持續長達 7 週的

[160]王士帆，刑事法與憲法對話：科技犯罪與偵查會議實錄——科技偵查與令狀原則與談稿，月旦法學月刊第 4 期，2021 年 4 月。

錄影記憶卡，成為法院認定 A 犯竊盜罪之主要證據。A 對判決提起上訴，指摘警察長期監視錄影於刑事訴訟法欠缺授權基礎，干預了被告享有的德國《基本法》第 2 條第 1 項連結第 1 條第 1 項之一般人格權（含資訊自我決定權與肖像權在內），以及《歐洲人權公約》和相同規範宗旨的《公民與政治權利國際公約》所保護的隱私生活權利主張系爭錄影資料不得作為證據使用。[161]長期跟監蒐證在傳統偵查作為行之有年，然因科技發展利用科技工具可取代傳統人力蒐錄且 24 小時無間斷蒐錄，對於此手足感官的延伸，且長期監錄，是否需要給予更高的干預授權基礎，引發質疑。

依德國《刑事訴訟法》現行規定，偵查機關實施「住宅外長期監視錄影」，應同時符合 2 個干預授權基礎：長期監視（§ 163f StPO）與住宅外記錄圖像（§ 100h I S. 1 Nr. 1 StPO）規定。長期監視，德國立法定義指超過 2 日或持續逾 24 小時的計畫性監視，至於未達長期標準的短期監視，德國法則無特別的干預授權規定，立法者認為偵查概括條款（§§161, 163 StPO）即足作為短期監視的實施法源。[162] 在德國刑事訴訟法規範，短期監視、長期監視、利用科技設備錄音(影)監控，是完全不同的干預授權基礎。在德國刑事訴訟法，短期監視的依據是第 161 條（檢察官）或第 163 條（偵查輔助機關），長期監視是第 163f 條，前後規範密度有別；無論短期或長期監視，執行期間未必會記錄影像，若有拍照或錄影這種對肖像權所生、於監視之外的「附加」基本權干預，則另應遵守第 100h 條的干預授權規定。[163]因此，若在長期監視的偵查可能會干預的是隱私權、人格權，在錄影則是產生肖像權的問題，在不同的干預基礎下，則需要給予不同的授權基礎。德國立法者

[161] 王士帆，德國聯邦最高法院刑事裁判 BGHSt 44, 13 ——住宅外長期監視錄影，司法周刊 2054 期，2021 年 5 月 14 日，頁 2。

[162]王士帆，德國聯邦最高法院刑事裁判 BGHSt 44, 13 ——住宅外長期監視錄影，司法周刊 2054 期，2021 年 5 月 14 日，頁 2-3。

[163]王士帆，德國科技偵查規定釋義，法學叢刊，第 66 卷第 2 期，頁 123。

察覺當時短期監視之法規範，並不足以因應現況，於是在 2000 年 8 月，刑事訴訟法增訂第 163f 條長期監視條款。

判決中指出，錄影監視被告住家門口區域和由此取得的資訊，干預被告受《歐洲人權公約》第 8 條保護的隱私領域，以及對應到《基本法》第 2 條第 1 項連結第 1 條第 1 項的一般人格權。理由一是，偵查機關連續數週不間斷監視被告出入其住家，已構成重大干預的偵查措施；二是錄影機不同於人力，後者的觀察能力和記憶能力通常會受到影響，但錄影機則不同，其不受這些限制地製作被拍攝者的照片，又可在時間上幾乎永無期限保存所錄製的影片。準此，對於實施此偵查措施，刑事訴訟的特別法律基礎乃不可或缺」。[164]在德國聯邦最高法院判決說明，科技監視、長期監視，皆與傳統人力監視本質並不相同，應分別需要特別授權基礎。然而，法院在最終判決，卻逕以長期監視之「住宅外記錄圖像」可概括涵蓋科技監視，受到不少批評。

雖然與當時立法風向相違逆，從德國裁判歷史地位來說，該判決卻扮演「過渡裁判」的角色，亦即，當年尚無法預期是否及何時增訂長期監視條款，但為了刑事司法追訴利益，在立法者建構新規範前，充當過渡時期角色，化解干預授權基礎之不足。[165]在我國偵查實務，長期監視例如跟監、埋伏，住宅外紀錄圖像例如裝設照相(錄影)器材，法律授權基礎大多為刑事訴訟法之概括授權條款或有涉及警職法之交錯地帶，然而因應各種科技產品問世，記錄各式資訊之設備如雨後春筍般問世(例如感熱儀、臉部辨識)，因而在實務上發現法律所給予的授權似不足夠。藉此判決，參照我國困境而試圖尋得可能修法方向，能更正面應對科技帶來的影響與變遷。

[164] 王士帆，德國聯邦最高法院刑事裁判 BGHSt 44, 13 ——住宅外長期監視錄影，司法周刊 2054 期，2021 年 5 月 14 日，頁 5。
[165] 王士帆，德國聯邦最高法院刑事裁判 BGHSt 44, 13 ——住宅外長期監視錄影，司法周刊 2054 期，2021 年 5 月 14 日，頁 7。

第三節　我國判斷標準

德國前聯邦司法部長 Barley 女士：「欲實現法治國者，必須對其給予相應裝備。」[166]為平衡犯罪偵查以及人權保障，須遵守正當法律程序之要求，以通保法為例，有 1、重罪原則 2、相關性原則 3、令狀原則 4、一定期間原則 5、事後通知原則 6、監察對象特定原則 7、最後手段性原則 8、最小侵害性原則。另還有法官保留原則及證據排除法則。法官保留原則源自憲法上的「權力分立原則」，依保留的密度分為絕對法官保留原則及相對法官保留原則。現行法例並非所有的強制處分都採取絕對法官保留原則，如刑事訴訟法第 204 條之 1（鑑定許可書。證據排除法則：分為絕對證據排除以及相對證據排除，後者即若無法定強制排除的明文規定，則回歸刑事訴訟法第 158 條之 4 由審判的法官進行權衡。

第一項 基本權

第一款 秘密通訊自由

憲法第十二條規定：「人民有秘密通訊之自由。」旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利（司法院釋字第 631 號解釋參照）。在憲法第十二條明定，國家若採取限制手段，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當，方符憲法保障人民基本權利之意旨，即須符合具體明確性原則、比例原則、令狀原則等，否則違憲。

---

166 „Wer den Rechtsstaat durchsetzen will, muss ihn entsprechend ausstatten“— undesjustizministerin Katarina Barley

第二款 人格權及隱私權

隱私權在我國憲法並無明定，警察職權行使法第 17 條規定：「警察對於一本法規定所蒐集資料之利用，應於法令職掌之必要範圍內為之，並須與蒐集之特定目的相符。但法律有特別規定者，不在此限。」，本條文規定目的主要有：1、警察利用個人資料，需與警察機關之職掌有關。即符合警察機關之法定職掌範圍，並與警察蒐集之特定目的有關，受到關聯性原則之拘束。2、但為了重大公共利益之利用，則不在此限，於此個人資料保護法有相關條文規定。惟隱私權在憲法基本權之地位，觀諸司法院釋字第 603 號、第 689 號解釋意旨自明[167]。為維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（司法院釋字第 585 號解釋參照）[168]。

第三款 資訊自決權

在我國，資訊自決權之意旨，可自司法院釋字第 603 號意旨窺見(爭點為戶籍法第 8 條第 2、3 項須捺指紋始核發身分證違憲案)，所謂「資訊自決權」係指個人有權自行決定，是否將其個人資料交付與提供利用，係基於自決之想法所產生之個人權現，即基本上由個人自己決定，在何時與何種界線內，得以公開其個人生活事實之權利。經過通訊傳送過程而儲存的通訊資料，與其他儲存在資訊科技系統的資料，是否公開以及讓他人加工使用，資料的擁有者對此享有自由決定的利益，因為不違反憲法的價值秩序，也受憲法第 22 條所保障（司法院釋字第 603 號解釋參照）。資訊自決權之概念，

[167]許義寶，警察蒐集與利用個人資料職權之研究——以警察職權行使法第十七條為中心，高雄大學法學院，2019 年 9 月第 15 卷 1 期，頁 77。
[168]司法院釋字第 603 號，解釋爭點為戶籍法第 8 條第 2、3 項捺指紋始核發身分證規定違憲案。

源自於電腦的發明，因為電腦的使用，將個人的意思排除在外，使得本人對於電腦中之資料，毫無置喙之餘地，導致個人對於自己資料之取用及正確性完全失去自主權，並且，電腦資料透過相互引用串連、溝通整合的結果，可能將某一個人塑造的「資料形象」與其本人真實面貌大相逕庭，此種對人格可能造成的重大傷害，所產生的警覺，使得個人應可自決其相關資訊之權力逐漸受到重視[169]。

德國聯邦憲法法院在「一九八三年人口普查案」判決中，以其一貫以來關於「自主性」之理念，進而發展出所謂「資訊資決權」之概念。[170]在德國聯邦憲法法院根據基本法第 2 條與第 1 條將此視為個人資訊自決權並且加以保障。德國聯邦憲法法院在 2008 年 2 月 27 日的判決，更進一步說明，個人資訊自決權的「資訊科技系統的保密性與完整性」（Vertraulichkeit und Integrität informationstechnischer Systeme）基本權的干預。[171]

第四款 合理期待隱私界線

實務與學說見解對於非公開的論述可分為物理性屏障及合理隱私期待兩種觀點，通說採需具有合理隱私期待之雙叉原則，即「當事人主觀上必須具備真實隱私期待，在客觀上，該真實隱私期待為一般社會大眾所認為合理」。在客觀上，有學者指出不應僅以物理性場所做為區別的標準，必須另以「活動之內容」予以限縮，才能對「非公開」之要件做出正確的解釋。

因為在判斷非公開的要件時係以當事人主觀上是否有意隱藏作為根據，若個人有意隱藏，會做出與外界阻隔或者在身體上隔離自己，避免成為

[169]許文義，個人資料保護法論，2001 年，頁 49。
[170]林安邦，德國「資訊自主權」之概念在我國法律上之應用，公民訓育學報 12 期 ，2002 年 7 月，頁 112。
[171]吳俊毅，刑事訴訟上的線上搜索（Online-Durchsuchung） 與源頭通訊監察（Quelle-TKÜ）引進的必要性及實踐上的困境，刑事政策與犯罪研究論文集，頁 469。

大眾的焦點或從焦點抽離出來，於確認主觀隱私期待存在後，再討論該隱私期待是否具備合理性而符合非公開之要件。個人在公共領域所為之行為如果是在沒有隔絕、遮掩的情況下，似不應直接以個人並非有意隱藏而認定為「公開」。[172]學者亦有從活動的場域區分公開與非公開，因為本條保護法亦為隱私，所以應指專屬於個人私密或私人領域中，身體活動不受他人或國家入侵而言；當個人處於公共領域中，例如明星和男友當街十指緊扣、夫妻在深夜大聲咆嘯導致鄰居擔心家暴或噪音過大而加以錄音蒐證、或是選擇不具保密隱密客觀條件之場所[173]導致他人得以偶然侵入或窺視其言論活動(例如在公園或車床族的性愛活動)，則此時被害人不得主張或期待享有在隱私領域中同等的保護。[174] 我國在此判斷，多援引美國之「隱私合理期待」原則，認為在隱私權的判斷，必須具有真實主觀隱私期待(主觀條件)及符合一般客觀大眾期待(客觀條件)，再以「公益原則」判斷隱私權所保障之界線。

[172] 蔡蕙芳，從美國隱私權法論刑法第 315 條之 1 與相關各構成要件(下)，興大法學 7 期，2010 年 6 月，頁 36-37。

[173]臺灣高等法院 98 年上字第 108 號民事判決：「經查，該等照片之拍攝地點為北投湯瀨溫泉餐廳，乃上訴人所自承。該 3 張照片有自餐廳窗戶拍攝、有於餐廳門口拍攝，或於馬路上拍攝，其拍攝地點均為公眾得出入之場合或公眾得共見共聞其行為之地點，要不具備隱密性。上開照片內容雖為上訴人之私人活動，惟不具對隱私之合理期待，縱被上訴人加以拍攝、刊登，不能認係侵害上訴人之隱私權。」。

[174] 王皇玉，刑法對隱私權的保障-以刑法第 315 條之 1 為中心，台灣法學雜誌第 122 期，頁 37。

第二項 國內判決

第一款 最高法院 102 年度臺上字第 3522 號判決(長期監視)

民國 98 年，一統徵信公司與國華徵信公司業務經理為完成委託調查案件，各自多次委託被告，分別侵入他人住宅裝機竊聽、竊錄被害人電話，被告並多次進入各個裝機地點取 出竊錄之錄音帶。警方接獲線報，得知被告涉嫌侵入住宅竊錄他人通訊內容， 派員進行多次跟監、埋伏，獲知被告自上開竊聽地點回到一統與國華徵信公司，並拍攝蒐證照片。同年 8 月底，警方逮捕被告，於其車內扣得竊聽相關設備，復經被告偕警前往裝機地點指認，並自其中一處取出竊聽錄音機。 臺灣高等法院更一審判決被告成立五次違法通訊監察罪（通訊保障及監察法第 24 第 1、3 項），合併定執行刑有期徒刑五年六月。被告提起上訴， 上訴理由之一指摘警方跟監並搭配使用輔助性科技設備，已嚴重干預人民之基本權利，不符合警察職權行使法第 11 條第 1 項之法定程序，故警方跟監中拍攝的蒐證照片係屬違背法定程序所取得之證據，應無證據能力。

復經最高法院駁回上訴，主要理由如下：第一、「跟監」係指國家機關為防止犯罪或犯罪發生後，以秘密而不伴隨國家公權力之方式，對無隱私或秘密合理期待之行為或生活情形，利用目視或科技工具進行觀察及動態掌握等資料蒐集活動（警察職權行使法第十一條規定參照）。是所謂「跟監」包括對人民行動為追跡、監視及蒐證等活動。無論係基於調查犯罪之必要所為具司法警察偵查犯罪性質之活動；或係為預防犯罪所為之行政警察活動，對於被跟監者之隱私權、資訊自決權等憲法所保留之基本權固有不當之干預，然偵查犯罪及預防犯罪之發生均係維持社會秩序及增進公共利益所必要，自得以法律限制之。 第二、刑訴法第 230 條、第 231 條第 2 項既規定司法警

察官、司法警 察知有犯罪嫌疑者，應開始偵查。而 「跟監」復係調查及蒐集犯罪證據方法之任意性偵查活動，不具強制性，苟「跟監」後所為利用行為與其初始之目的相符，自無違法可言。況警察職權行使法第十一條係規定為「防止犯罪」所必要而進行觀察動態、掌握資料等蒐集活動，與本件警方係因已發生違法監察他人通訊之犯罪行為，為進行蒐證，始對被告為跟監，並伺機蒐集證據，不盡相符，本件與警察職權行使法第 11 條規範之目的不同，自不能比附援引。[175]在本案警察跟監期間，被告仍然持續在從事侵入住宅與違法通訊監察，所以警察的跟監並不是單純在追緝已經發生的犯行，而是同時有防止犯罪的性質。此種具有雙重功能的跟監行為，不但應該符合防止犯罪之跟監法定要件，也應該符合追緝犯行之跟監法定要件，依據警職法之「預防犯罪」授權警察在法定程序下實施跟監，並有資料銷毀等義務，但實際案件事實已達到刑事犯罪中追緝犯罪之「偵查跟監」，在刑事訴訟法則無明文，此同一行為具有預防犯罪及偵查跟監並存雙重行為，亦有包含前者的行政救濟即後者的刑事訴訟法證據排除之法律效果問題。[176]

跟監，分為動態的跟監及靜態的監視，且除了以一般目視方法，為了延伸感官能力或儲存所蒐集的資訊，多使用「輔助性科技設備」，例如望遠鏡、夜視鏡、密錄器材。跟監行為蒐集他人在公開場合的活動或位置資訊，有可能因為干預「生活私密領域不受侵擾之自由」及「個人資料之自主權」，而成為干預基本權的國家高權行為。[177] 若以刑事訴訟法第 230 條及第 231 條

[175]林鈺雄，干預保留與門檻理論－司法警察（官）一般調查權限之理論檢討，政大法學評論第 96 期，2007 年 4 月，頁 245-247。

[176]黃榮堅，基礎刑法學，四版，2012 年，頁 675。
德國通說認為，此種雙重功能措施的性質只能在危害防止與犯行追緝之間擇一認定，判斷標準則是根據個案情節衡量，系爭措施的重點在危害防止或犯行追緝，據此認定其法律根據及救濟管道。事實上，此種以措施重點所在來界定其性質的看法，立刻遭遇的問題就是其標準欠缺可操作性。正如同在刑法上一個行為兼具作為與不作為性質時，通說也嘗試以「非難重點」作為界分標準，早已被批評是概念抽象而流於恣意判斷。

[177]吳梓榕，一般偵查措施的合憲控制——從偵查程序之自由形成原則出發，政治大學法律學研究所碩士論文，2008 年，頁 32-77 ；范里，跟監應屬刑事訴訟上之基本權干預——評最高法院

第 2 項作為司法警察之偵查概括條款，在學者主張亦各有不同。持反對立場主張「其僅為組織法上權限之授權而非作用法上之干預權授權」[178]。折衷立場，認為「有無侵害個人之實質或重要之權益」區分「任意處分」與「強制處分」，主張任意處分無庸個別授權規定[179]，又或有學者提出「修正的門檻理論」，認為僅有輕微干預一般人格權（及與此相關之資訊自決權）的非強制性干預措施，始得適用偵查概括條款，至於屬於「立法特別授權之清單」、「憲法古典權利之清單」、「該當刑法構成要件之干預」及「附帶授權之干預」等偵查措施，則必須特別授權。[180]刑事訴訟法之偵查概括條款雖賦予偵查靈活彈性，然而在概括授權和濫權之間，難以有明確之界線。

本文認為，在科技發展下，傳統跟監偵查將面臨甚大的轉變，偵查概括條款將面臨各項無法想像的應用產生解釋困境，給予特別授權是必將面臨的課題，理由有二：其一是檢警工作項目，質與量與日俱增，耗費時間與精力在傳統跟監不符成本效益，且人體器官有其極限，目視、嗅覺及記憶都會隨著時間而模糊，且短期監視甚難達成偵查需求，實務上偵查人員往往需要花費更為長期的監視及配合各種偵查作為，若非以科技工具難以達成。其二是，在資訊爆炸及各類科技設備應用的時代，利用輔助設備監視不僅節省人力，且可以較具隱密性的長期監視，取得之資料具有不可修改、可完整保存等特性。因此，利用科技監視必然會取代傳統跟監蒐證，乃時勢所趨。

---

102 年度台上字第 3522 號判決，刑事法雜誌，58 卷 2 期，2014 年 4 月，頁 75-83。

[178]楊雲驊，「通訊保障及監察法」實施前電話監聽合法性及證 據評價的探討——評最高法院九〇年台上字第八四八號、九一年台上字第二九〇五號及 八七年台上字第四〇二五號判決，台灣本土法學雜誌，57 期，2004 年 4 月，頁 45。

[179]陳運財，偵查之基本原則與任意偵查之界限，東海大學法學研究 1995 年 9 月，9 期，頁 31。

[180]林鈺雄，干預保留與門檻理論－司法警察（官）一般調查權限之理論檢討，政大法學評論第 96 期，2007 年 4 月，頁 217-222。

第二款 M 化偵查網路系統判決

109 年 5 月 8 日我國首見 M 化車判決（臺灣桃園地方法院 106 年易字第 164 號刑事判決）。犯罪事實略已，甲、乙、丙、丁共組詐欺集團，先向某 A 收購行動電話門號 SIM 卡（下稱人頭門號）以 B、C 姐弟居處作為詐騙機房，以收購之人頭門號，撥打電話予被害人，誆稱被害人之子女涉入毒品交易糾紛，遭綁架需交付贖金恐嚇取財，部分被害人陷於錯誤，依指示將所示金額交付款項於指定地點。警方接獲報案後，調取被害人使用門號與犯嫌所用人頭門號之通聯紀錄、門號申登人資料，在分析門號申登人申辦之所有門號、手機序號及通聯紀錄顯示之基地臺位置後，發現人頭門號通聯之基地臺位置均位於特定幾個地址。警方便將上述門號申登人申辦之所有門號及手機序號，鍵入「M 化車」在上述幾個特定基地臺位址周邊測點，其中 X 手機序號當日仍在使用，警局即向電信業者調閱該序號當時搭配之 X 門號，並即時定位特定位置，再搭配「M 化車」鎖定「該門號發話位址」。警方派員於該址埋伏蒐證，經查詢停放門口車輛之車主曾涉及詐騙集團案件經移送偵辦，警方以上述資料報請檢察官指揮偵辦並向原審法院聲請搜索票。 經原審核發搜索票，警方前往該址搜索，扣得本案相關證物。在本案事實，警方根據聲請通信紀錄調取票，調取被告之手機門號發話紀錄，再以 M 化車限縮確認可能基地臺位址，埋伏蒐證機房之犯罪事證，經蒐集事證後向法院聲請搜索票，據以查獲詐欺機房。

第一審法院，被告主張警方使用 M 化車無法律授權，取得證據應依毒樹果實理論，排除證據能力。法院判決結果，認為按大法官釋字 689 號解釋理由，一般行為自由、生活私密領域不受侵擾及個人資料之自主、隱私等權利，均屬憲法第 22 條保障個人人格自由發展之基本權保護範圍；並且因為資訊科技高度發展及相關設備之方便取得，前揭基本權受保護之必要亦隨之

提昇，但此等基本權仍得以法律限制之。惟就M化車而言，其原理係利用「虛擬基地台」的定位科技方法，藉訊號之強弱連結以探知手機位置資訊，其實際發動之時間乃取決於偵查機關，且不分目標係在何處（私人住宅或公開場所）而有異，因而導致目標設備、對象所在之位置資訊，不限時間、地點，均得由偵查機關透過M化車之使用，持續達到定位追蹤以及蒐集、處理與利用該等資料之目的。故M化車使用之結果，已對目標對象的基本權造成並非輕微的干預，但卻欠缺法律授權。基於法治國與法律保留原則，本案因M化車直接取得之證據（資訊）應認無證據能力，不得作為證據使用。

但在證據能力的排除，法院僅將「M 化車」直接取得之證據（資訊）應認無證據能力，不得作為證據使用。於「聲請搜索票後」執行所得之證據，仍「有」證據能力，不因「毒樹果實」原則排除，法院判決內容說明，本案偵查方式是透過卷內的通聯紀錄、使用者資料、基地臺位址、現場埋伏、觀察、目視情狀及相關車輛資訊、車主的前案紀錄等資料，據以聲請本件搜索票，其程序是依循慣例所致，而未刻意違法。另警方客觀上也依據其他的證據資料而縮小偵查範圍、特定搜索標的，並非單純或大部分依據「M 化車」偵查之結果為之，故相關搜索、扣押取得之證據，與「M 化車」之連結已相對薄弱。爰認本案警方因執行搜索所獲之證據，均有證據能力。

第一審判決引發學者及實務界熱議，執法機關科技偵查定位技術之現況浮出檯面，評價兩極。109 年，本案上訴到高等法院(臺灣高等法院 109 年上易字第 1683 號刑事判決)，和第一審法院採不同觀點，法院認為警方使用M化車是為偵查已經發現的犯罪行為，將已知的犯罪地點加以限縮，查獲過程，並非僅只依靠M化車，而是先依被害人報案、提供通訊電話資訊、調閱監視器、進行人臉辨識、查調通聯記錄、分析時間順序、基地臺，然後才聲請調取票，使用M化車配合偵查。並且M化車僅僅是以訊號定位，無法

顯示地址，只是將警方已知的犯罪地點加以限縮，也無精確定位、並無行為人行動影像或對話內容，好比災難生存跡象搜索的訊號顯示，究其實質並無妨害秘密可言。M 化車定位並不會顯示與隱私有關的內容，因此不構成隱私權的侵害。

高等法院認為，第一審法院引用釋字 689 號解釋闡述，新聞採訪者於有事實足認特定事件報導具有一定公益性，而屬大眾關切並具有新聞價值者，如須以跟追方式進行採訪，且跟追行為依社會通念非屬不能容忍，該跟追行為即具有正當理由而不在規定處罰之列，正足以正當化治安機關對於有事實足認有特定犯罪嫌疑之犯罪行為，因偵查犯罪之需要，而採用現代科技設備，如對隱私權並未構成重大、不合比例之侵害，也未逾越依社會通念所認不能容忍的界限，即屬該號解釋意旨所揭示，符合憲法第 23 條之比例權衡原則，基於公益的合理權衡，依刑事訴訟法第 158 條之 4，認 M 化車的偵查作為，具有證據能力。

本案判決後，法院立場雖鼓舞執法者，仍無解決偵查實務面的問題。在執法人員立場，擔憂所使用之科技定位技術偵查作為，將因本案而受到汙名或放大檢視，且若未來使用此類科技設備，均採用權衡法則，偵查人員將產生極大的疑慮。在民眾角度，則擔心執法人員利用科技定位技術偵查，將無死角侵入生活，個人行蹤將無所遁形。本次 M 化車判決爭議，彷如 106 年 GPS 判決重演，有關科技定位技術偵查之爭議與疑慮也逐漸浮出檯面，不如儘早充分討論、立法、納管，才是根本解決之道。

第三款 GPS 全球定位系統判決

在我國實務判決，GPS 設備在十數年前就曾提及，如高等法院 101 上易 2814 判決，警察為偵辦 2 名被告涉嫌竊盜案件而在其駕駛的小客車上裝設 GPS 追蹤器，判決書提及「綜觀全卷，未見警察裝設衛星追蹤器(GPS)之

正當法律程序，檢察官復未舉證證明警察此一行為係依據正當程序所為，則隱私權顯已受此監控行為之侵害……」，認為偵查手段並非依據正當法律程序，而未採用員警關於追蹤器顯示被告曾經到過被害人失竊所在地區的證詞。換言之，此項判決認為若無正當法律程序之依據，警察機關不得以 GPS 定位作為偵查手段，否則其取得的位置資訊，法院得予以排除作為被告犯罪事實的證據使用。在此可看出，法院立場說明認為使用衛星定位追蹤器非屬正當行為，但未直接認定違法，而是以證據排除法則，認定無證據能力。

在早期，部分法院判決亦認為駕車行使於道路上之人自願將自己的行蹤暴露於他人目光之下，不屬於非公開之活動，至 GPS 追蹤器只取得相對人在公共道路上的資訊，與以目視跟追無異，故在他人汽車上裝設 GPS 追蹤器以得知其所在位置的行為，並不構成刑法第 315 條之 1。最高法院 101 年度臺上字第 5635 號刑事判決曾指出，「跟監」係指國家機關為防止犯罪或犯罪發生後，以秘密而不伴隨國家公權力之方式，對無隱私或秘密合理期待之行為或生活情形，利用目視或科技工具進行觀察及動態掌握等資料蒐集活動。是所謂「跟監」包括對人民行動為追跡、監視及蒐證等活動。無論係基於調查犯罪之必要所為具司法警察偵查犯罪性質之活動；或係為預防犯罪所為之行政警察活動，對於被跟監者之隱私權、資訊自決權等憲法所保留之基本權固有不當之干預，然偵查犯罪及預防犯罪之發生等均係維持社會秩序及增進公共利益所必要，自得以法律限制之。刑事訴訟法第 230 條第 2 項、第 231 條既規定司法警察官、司法警察知有犯罪嫌疑者，應開始調查。而「跟監」復係調查及蒐集犯罪證據方法任意性偵查活動，不具強制性，苟「跟監」後所為利用行為與其初始之目的相符，自無違法可言。「跟監」係調查及蒐集犯罪證據方法之任意性偵查活動，不具強制性，苟「跟監」後所為利用行

為與其初始之目的相符，自無違法可言。[181]

歷經使用 GPS 設備不同觀點的流變下，在 106 年海巡署士官長裝設 GPS 追蹤器案(最高法院 106 臺上 3788 號判決)，經過非常上訴駁回後，最終為妨害秘密罪有罪判決，確立了使用 GPS 干預隱私權之立場。節錄判決要旨理由：1、隱私權是憲法保障之基本權。2、公共場所移動車輛評價屬於「非公開之活動」：所謂「非公開之活動」，固指該活動並非處於不特定或多數人得以共見共聞之狀態而言，倘處於不特定或多數人得以共見共聞之狀態，即為公開之活動。惟在認定是否為「非公開」之前，須先行確定究係針對行為人之何種活動而定。以行為人駕駛小貨車行駛於公共道路上為例，就該行駛於道路上之車輛本體外觀言，因車體本身無任何隔絕，固為公開之活動；然由小貨車須由駕駛人操作，該車始得移動，且經由車輛移動之信息，即得掌握車輛使用人之所在及其活動狀況，足見車輛移動及其位置之信息，應評價為等同車輛使用人之行動信息，故如就「車內之人物及其言行舉止」而言，因車輛使用人經由車體之隔絕，得以確保不欲人知之隱私，即難謂不屬於「非公開之活動」。3、此類拖網偵查造成隱私權重大侵害：偵查機關為偵查犯罪而非法在他人車輛下方底盤裝設 GPS 追蹤器，由於使用 GPS 追蹤器，偵查機關可以連續多日、全天候持續而精確地掌握該車輛及其使用人之位置、移動方向、速度及停留時間等活動行蹤，且追蹤範圍不受時空限制，亦不侷限於公共道路上，即使車輛進入私人場域，仍能取得車輛及其使用人之位置資訊，且經由所蒐集長期而大量之位置資訊進行分析比對，自可窺知車輛使用人之日常作息及行為模式，難謂非屬對於車輛使用者隱私權之重大侵害。而使用 GPS 追蹤器較之現實跟監追蹤，除取得之資訊量較多以外，就其取得資料可以長期記錄、保留，且可全面而任意地監控，並無跟丟可能等

[181]陳運財，GPS 監控位置資訊的法定程序，台灣法學雜誌，293 期，2016 年 4 月 14 日，頁 59-74。

情觀之，二者仍有本質上之差異，難謂上述資訊亦可經由跟監方式收集，即謂無隱密性可言。4、強制偵查必須現行法律有明文規定：偵查係指偵查機關知有犯罪嫌疑而開始調查，以發現及確定犯罪嫌疑人，並蒐集及保全犯罪證據之刑事程序。而偵查既屬訴訟程序之一環，即須依照法律規定行之。

又偵查機關所實施之偵查方法，固有「任意偵查」與「強制偵查」之分，其界限在於偵查手段是否有實質侵害或危害個人權利或利益之處分而定。倘有壓制或違反個人之意思，而侵害憲法所保障重要之法律利益時，即屬「強制偵查」，不以使用有形之強制力者為限，亦即縱使無使用有形之強制手段，仍可能實質侵害或危害他人之權利或利益，而屬於強制偵查。又依強制處分法定原則，強制偵查必須現行法律有明文規定者，始得為之，倘若法無明文，自不得假借偵查之名，而行侵權之實。在本案中最高法院認為不論有無「侵入」物理空間，即便在公共場所有車體之隔絕，也應享有不欲人知隱私。最高法院明確指出 GPS 偵查侵害憲法第 22 條保障之隱私權，且參照釋字第 689 號解釋意旨，隱私權保障的對象是「人」而非「地方」。[182]

然在 GPS 偵查性質是任意處分或強制處分頗有爭議，有學者認為，偵查跟監是任意性偵查活動，只要對蒐證資料之利用符合初始目的，刑訴法第 230 條及第 231 條即得成為授權基礎，主張若 GPS 追蹤器只是作為跟監的輔助手段，僅非持續性、片斷地取得位置資訊時，對於隱私難謂構成高度侵害，應屬任意處分；反之若持續性、全面性取得偵查對象之位置資訊時，則應屬強制處分。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。

[182] 劉靜怡，大法官保護了誰？——釋字第 689 號的初步觀察，月旦法學雜誌，197 期，2011 年 10 月，頁 55。

日本刑事訴訟法第 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。[183]在我國 GPS 追蹤器干預基本權，綜合學說及實務見解大概分為：一、資訊總量說，所謂馬賽克理論(或鑲嵌理論)，以取得資訊的總量判斷 GPS 追蹤器監控相對人行動是否已違反了其合理的隱私期待。第二，準物理侵入說，是比較接近於美國聯邦最高法院 Jones 案意見的財產權侵害說，並不著眼於 GPS 偵查所取得的資訊總量，而是重視安裝 GPS 追蹤器及定位的過程中是否伴隨有入侵性的狀況。目前普遍多數見解為前者，認為 GPS 設備雖可能會有財產權侵害，但實質主要干預的基本權，是基於馬賽克理論無差別的被蒐集個人位置資訊，此資訊蒐集造成個人生活圖像拼湊而產生隱私權的侵害。至於取得此類「定位資訊」係屬通保法的通訊監察書(調取票)、刑事訟法的搜索票，定性上仍有爭論。

在早期，曾有以通訊監察書聲請 GPS 追蹤器一說，然「通訊」必須要有意思表示，與單純的「位置」資訊樣態不同，應非屬通保法範疇。又刑訴法之搜索，應係屬物理性的侵入，與資訊概念不甚相符，因此在我國法律難以找到較為符合適用之依據。另一個問題是，使用多長的時間取得「資訊總量」會造成侵害，超過多少總量應視為不可跨越之界線，也就是說法律應給予一個框架界線，准許執法機關僅能在此框架下蒐集必要資訊，且在此界線的蒐集的資訊，應受到監督、救濟、銷毀等保障措施。

本文在上述比較法章節，在美國聯邦刑事訴訟規則便已詳盡地明範了偵查人員使用追蹤器時應遵守：必須經由治安法官審查有無相當理由據以核發令狀，並限定執行追蹤期間原則上 45 日，並課以執行結束後於 10 日內

[183]陳運財，GPS 監控位置資訊的法定程序，台灣法學雜誌，293 期，2016 年 4 月 14 日，頁 68。

以令狀的影本通知受監控之人等等規範。另外，德國刑事訴訟法分別以第100h條第 1 項第2款規範出於監控目的而使用科技設備，調查嫌疑人所在地的依據；同法第163 f條第1項規範較長期的跟監（指持續超過 24 小時或雖有間斷但合計超過2日），因此警察人員使用GPS長期追蹤定位時，應同時具備第100h條第 1 項第2款和第 163f條第1項要件，排除輕罪之適用，且原則上應依偵查法官之命令，遇有急迫情形，得由檢察官命令之，但之後若未於3日內取得法院認可者，失其效力。在此特別注意的是，不論是美國法的「治安法官」或德國法的「偵查法官」，與我國所指的「法官」意義並不相同，在美國法之治安法官負責的是微罪和預審，在德國法之偵查法官，主要之功能則有二，一為對於偵查中強制處分之監督，一為證據保全[184]，與我國強制處分專庭法官較為相似。

[184]劉思妘，論德國偵查法官制度 ─兼論我國引進偵查法官制度之評估，東吳大學法學院法律學系碩士論文，98年6月，頁10-11。
「偵查法官」一詞，乃對於德文「Ermittlungsrichter」之直接翻譯，在德國刑事訴訟法之解釋上，有其獨特之意義，但於我國刑事訴訟程序中，則因為其定義尚未明確，而可能產生兩種不同之解釋方向：就功能面而言，可能指稱職司偵查之法官，亦即於具有偵查權限並負責偵查之法官；但就程序面而言，則可能指稱於偵查程序中之法官，亦即出現於偵查階段僅具有部分權限之法官。

第五章　我國科技定位技術偵查法制化之問題爭議

第一節　我國草案之簡介與評估

犯罪偵查與人權保障並非完全對立的概念，事實上偵查是為了維持治安、公共秩序、保障人權的一環，且科技定位偵查在實務上系基礎且長期使用之偵查方式，如果選擇全然否決使用，真的是我們所想要的結果嗎？遲遲未制定法律干預授權基礎會發生什麼情形？當務之急是一次到位還是先將幾種常使用的方式立法？本文以科技定位偵查技術為核心，探討實務各種定位偵查技術原理、功能及偵查應用、干預授權依據，以及我國判決及外國立法例，進而探討科技偵查法草案及提出未來可能立法建議。

在科技偵查法草案討論聲浪中，除有針對條文規範及發動門檻的疑慮，還有對於草案的恐懼，甚至認為若科技偵查法草案一出，將導致人權嚴重干預，政府可以名正言順的侵害人民隱私權。本文對此立場並不贊同，且認為科技偵查立法之必要性，是急迫且必須的，理由有三。

其一，是科技與生活早已密不可分，科技產品問世速度和網路聯網空間發展，已超乎我們所能想像，從手機、定位裝置、攝錄影設備、通訊軟體、個人資料蒐集分析，大量的個人資訊暴露在我們所使用的各種科技產品中，而且這些資料是來自於我們因為想要使用該項科技，自願同意揭露個人資訊。換言之，這些大量資訊不僅無法完全以文字定義，不斷附加重疊之下，更難以在文義解釋內能完全概括，並已經廣泛共存在日常生活中，因此，應正視問題並儘速充分討論，將現實面所遇到的問題具體化提出，而非迴避消極地以干預人權為由拒之門外。

其二，傳統偵查方式已不足以應對新型態犯罪，近年來不難見到傳統犯

罪，已經搭配「科技」手法，變成新型態犯罪，甚至犯罪集團利用本文所述之定位資訊，用來監控犯罪集團的共犯或被害人，我們無法想像犯罪者還會如何使用這些科技設備，但目前可見的是這已經是「現實」，差別在於犯罪者要花費多少資源去達到目標，尤其對於重大犯罪或組織犯罪集團，相對於偵查資源及司法成本，不若是九牛一毛。在科技發展下，我們在網路空間獲得隱匿性，例如使用 VPN 技術(虛擬專用網絡，通過創建加密隧道並屏蔽 IP 地址，常見使用於將 IP 位址顯示為指定國家，俗稱如翻牆、境外跳板)、洋蔥瀏覽器(Tor/ The Onion Router，利用不斷介接中繼網路，可隱藏使用者真實位址、避免網路監控及流量分析等目的)，可想見在各種科技被犯罪者使用後，若不能給予法律授權依據，將造成執法者武器不對等，更何況科技偵查的立法，不僅在法制面上，還有實務執行需要協力義務的配合，立法不過是給予法律授權基礎，之後才能進一步解決實務困境，故應給予正面評價。

其三、給予法律授權才能有效保障人權的。在資訊科技應用急遽增長的同時，立法機關目前似乎無意對法律條文進一步檢視，偵查機關可能也未必有意揭示偵查技巧。凡此，倘若司法審查層面根本性地欠缺基本權干預意識時，對具體條文能否納入特定新型科技偵查手段，其適用與解釋上或多或少會產生（標準不一致的）爭議，未來仍然可能產生相當的困擾。[185]在實務上，執法人員認為沒有法律禁止，就可以做，這個觀念當然是錯誤的。科技偵查法之立法目的，在於立法後才能有效事前設定、事中管控、事後監督，相對亦是要求執法機關執行科技定位技術偵查，有通知當事人之義務，以及給予救濟途徑。科技時代的干預處分體系，其重點考量在於「資訊」的「質」、「量」、手段造成的「風險」、與受干預者的「抵禦可能性」。並且得以立法或司法，以各種事前、中、後的程序保

[185]黃政龍，新型態科技偵查作為之法規範研究，中央警察大學警察政策所博士論文，頁 171。

障，將所欲取得之「資訊」控制在法定的「框架」之中，不致恣意地「外溢」。[186]綜前所述，科技定位技術偵查在我國刑事訴訟法、警職法、通保法、個資法或相關行政法令，均無適切之法律授權，顯見科技定位偵查手段、程序、救濟，十分缺乏且亟待改善。

目前使用科技偵查技術進行追蹤取得證據，係依照刑事訴訟法第 158 條之 4 衡量是否具有證據能力，在 GPS 判決中法院則是明確回應偵辦刑案並非「無故」之要件，認定違法刑法第 315 條之 1 妨害秘密罪。然而，定位科技偵查技術在判決後就此束之高閣？答案當然是否定。科技定位偵查技術，不僅節省人力、時間，更可以有效保障執法人員安全，在實務上已是不可或缺之科技偵查工具。例如偵辦製毒工廠，多位於渺無人煙或荒山野嶺之僻靜處所，傳統跟監方式根本無從靠近偵查，除極易使犯罪者察覺外，甚至可能造成執法人員人身安全受到危險，在此種情形，使用空拍機、定位科技工具變成唯一的選擇。又如例如擄人勒贖或嚴重危害社會治安重大案件(例如陳進興案)，執法人員如果可以在贖金內或使用物品上吸附定位器材，或使用定位偵查方式竭盡所能找尋位置，亟可能爭取到更多偵查時效，且不需像傳統偵查方式，為了找人封鎖街巷逐層逐樓查訪，造成人民更多的不便。科技偵查手段在現今已廣泛運用，是趨勢也是現實。

還有一個問題是，科技定位技術偵查設備是否需要由統一規格購買及使用，以管制蒐集所得資料。在科技偵查法之設備端通訊監察(例如木馬程式)，該科技因恐有超乎法訂規範的使用內容，故須有一定之技術擔保，例如在德國，2017 年立法通過後，德國花費 600 萬歐元(新臺幣約 2 億多元)，研發出 2 個新的「符合法治國要求的木馬」。在技術方面，總共經過 TÜV IT、 BSI

[186]施育傑，科技時代的偵查干預處分——兼論我國法方向，月旦法學雜誌，306 期，2020 年 11 月，頁 166-168。在該文章作者據此簡稱為「資訊框架」理論。

（聯邦資訊安全局）及 BKA（聯邦警事局）3 個單位及 5 個技術測試程序。[187] 而本文所討論之科技定位技術，因功能有限毋需大費周章建立系統，惟仍建議應要有完整的設備功能公開說明及定期統計數據，以完善監督鍊。

第一項　科技偵查法草案

科技偵查法草案，起源於 GPS 偵查欠缺法源依據之判決，最高法院在 106 年度臺上字第 3788 號刑事判判決理由附帶表示，GPS 追蹤器的使用，是檢、警機關進行偵查的工具之一，以後可能會被廣泛運用，期待立法機關儘速就 GPS 追蹤器的使用要件、事後救濟，研議制訂法律。在 108 年法務部曾嘗試將 GPS 偵查法制化於通訊保障及監察法內[188]，並採取檢察官許可即可使用全球定位系統，只是側重於犯罪偵查之便利，而缺少對於人民秘密通訊自由及隱私權的憲法保障意識，因而引發抨擊，繼 109 年 5 月 M 化車第一審法院判決後，法務部 109 年 9 月 8 日公告科技偵查法草案，共有 7 章、28 條。

該草案概要內容分別是：立法目的（第 1 條）、專有名詞解釋（第 2 條），解釋本法科技設備或技術、隱私空間、非隱私空間、全球定位系統、非侵入性調查、通訊、資訊系統或設備、設備端通訊監察之定義；監視、攝錄與追查位置（第 3 至 13 條），非隱私空間、全球定位系統，以及隱私空間的非侵入性調查；設備端通訊監察（第 14 至 18 條）；數位證據搜集與保全（第 19 至 21 條）；救濟（第 22 至 23 條）；罰則（第 24 至 26 條）；附則（第 27 至 28 條），本文所討論之科技定位技術偵查，訂定於該草案第 3

[187]林鈺雄，科技偵查立法藍圖 ——刑事訴訟目的之試金石（下），2020 年 10 月 23 日舉辦之「法治國之科技偵查與科技防疫」座談會發言紀錄。
[188]劉昌坪，《通保法》擬寬修 偵查便利就好，秘密通訊自由無所謂？ETtoday 新聞雲，2018 年 10 月 19 日、https://www.ettoday.net/news/20181019/1285209.htm(最後瀏覽日：2022 年 3 月 10 日)。

條至第 13 條，及第 22 條至 28 條。

第二項　科技定位技術偵查監視相關規範

第一款 該草案第 3 條（非隱私空間之監視、攝錄與追查位置）

第 3 條：「偵查中檢察官認有必要時，得使用科技設備或技術，對於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」。實施本章調查時，若受調查對象或標的以外之人或物將無可避免地涵蓋於調查內容，亦得為之。在草案說明指出，此種方式係於公共場合為傳統上物理跟監、追蹤之延伸，而在無合理之隱私期待且必要之情況下，治安或預防危害等目的進行之監看、錄影等作為，則係依警察職權行使法及其他法律規定，而非以本法作為實施依據。另調取已存在之監看、與聞、測量、辨識、拍照、錄音、錄影資料作為證據，例如調閱路口監視器畫面，係依據刑事訴訟法等規範授權，亦非本法適用範圍。

本條說明係參考德國刑事訴訟法第 100h 條(住宅外監視科技方法與長期監視)，常見偵查作為有以望遠鏡、攝影機、照相機拍攝特定場所之出入口，以調查被告進出情形，實務常見如架設遠端攝影機，是使用科技器材及長期監視的基礎條款。有批評認長期監視僅需檢察官許可且可擴及第三人範圍，擔憂侵害人權。本文認為在層級化保留原則下，最基礎的偵查發動由檢察官許可，並無不妥，且刑案發動偵查起源，本就始於有犯罪發生，且在偵查階段無法完全區分同行之人、車輛，是否與案件有相關，無可避免會蒐集到第三人資料，因而若無可避免之範圍只要並非故意為之，應無所謂無限擴充範圍之可能。

第二款 該草案第４條（非隱私空間之以科技設備或空中技術之調查）

第 4 條：「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之調查者，應予立案，自立案之日起，實施之累計期間不得逾 30 日。有繼續實施之必要者，至遲應於期間屆滿之 5 日內，檢附調查所得資料，敘述理由報請檢察官許可後續行之，續行累計期間每次不得逾 30 日。」

以科技設備或技術在非隱私空間於空中進行之調查，通常以空拍(無人)機為之，亦得由人員於航空器上進行調查，未來若有其他技術或設備，自不待言，但於空中蒐集資訊之範圍較廣，且長期實施會產生較高之基本權干預，應在基礎規範下進行特別規範。另本條之調查性質上未必以多日不間斷方式為之，亦可能以單次、短時間的方式實施，為保障隱私權，並避免實施期間產生爭議，實施期間係以累積實施之日數為準，不需連日持續不間斷之實施。換言之，空中調查非隱私空間的立案規定，規範的是檢察事務官、司法警察官或司法警察自行立案調查，若由檢察官發動或指揮檢察事務官、司法警察官或司法警察，就不需要立案程序。部分批評認為，依據草案內容，檢察事務官、司法警察官或司法警察立案運用空拍機後，累計超過 30 天才需報請檢察官核准，太過寬鬆。

第三款 該草案第 5 條（利用全球定位系統等追蹤位置功能之調查）

第 5 條：「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。檢察事務官、司法警察官或司法警察因調查犯罪情形即蒐集證據，必要時得報請檢察官許可後，實施前項調查。檢察官、檢察事務官、司法警察官或司法警察實施調查累計期間不得逾 2 個月，有繼續實施之必要者，至遲逾期間屆滿之 5 日前，以書面記載具體理由，由檢察官或司法警察官報請檢察官同意後，聲請該管法院許可。前

項累計期間每次不得逾 30 日，有繼續實施之必要者，至遲逾期間屆滿之 5 日前，以書面記載具體理由，由檢察官或司法警察官報請檢察官同意後，聲請該管法院許可。」

該草案立法理由說明，長期、大量蒐集、追蹤、比對行為人之位置資訊，將使行為人個人活動之積累即和產生內在關聯，私人生活圖像即行為模式得以形成，故經由追蹤位置對他人進行長期且密集之資訊監視與紀錄，可能達到干預隱私權之程度，全球定位系統為目前最普遍之追蹤位置技術，但因科技日新月異，追蹤技術之設備或技術不限於特定一種或數種，係針對實施追蹤位置調查程序進行規範，無論偵查機關以何種設備或技術實施追蹤位置，均應遵守本條程序規定。例如行動軟體定位、定位偵防車(M 化車)、物聯網或任何其他設備技術進行追蹤位置，均應遵守本規範。並進一步說明，追蹤位置調查實施期間長短不同，干預隱私權程度亦不同，短期實施難以有「圖像效果」，干預長度較低，長期實施，干預程度較高，故應以層級化方式設計區分。本條文較具爭議，首先在發動門檻之要件過低，只要為檢察官認為有必要時就可以執行 2 個月的 GPS 偵查，而未參酌重罪原則、最小侵害性、最後手段性等原則，且使用長達 2 個月才需法官令狀，保留密度過低。其二是實施多長的時間會造成「圖像效果」，在我國，因對於實施期間無相關統計資訊，經過法官許可實施 30 日之規定係以何作為基準亦遭質疑。參美國 GPS 追蹤器採法官保留令狀原則，每次實施期間為 45 日；德國在第 100i 條「使用科技設備調查行動通訊設備」(M 化車)，命令最長期限為 6 個月，得每次不超過 6 個月之延長。

第四款 該草案第 9 條（以科技設備或技術之隱私空間調查）

第 9 條：「檢察官、檢察事務官、司法警察官或司法警察調查最重本刑三年以上有期徒刑之犯罪，有相當理由認為「隱私空間」內之人或與本案

有關，得使用科技設備或技術，自該隱私空間以外之處所，對該隱私空間內之人或物秘密實施非侵入性之監看、測量、辨識、拍照、錄影之調查。前項調查之累計期間，每次不得逾 30 日。有相當理由任需繼續調查者，至遲應於期間屆滿之 5 日前，以書面聲請該管法院許可。」

草案說明指出，隱私空間屬於具有隱私或秘密之合理期待之場所，故隱私空間之言論及談話，屬於通保法所規範，應依通保法程序為之。為維護隱私權，本法對偵查機關以科技設備或技術蒐集隱私空間之犯罪資訊，設下多重規範與限制，限定僅得對於最重本刑三年以上有期徒刑，提高發動之必要門檻、限定蒐證方式、法官保留，再者執行機關應以非侵入性方式進行調查，例如以高倍數照相機，透過未經窗簾遮掩之窗戶，拍攝屋內毒品製造情形，或透過熱顯像設備，探知內部溫度等情形。所謂的「非侵入性調查」，依照第 2 條第 5 款，是指對目標空間無物理性之侵入，調查設備或人員均在目標空間以外之處，以科技設備或技術，在該處搜集目標空間內之調查方式。另最重本刑 3 年以上有期徒刑，才可以啟動，這個門檻相當於通訊保障及監察法第 11-1 條的調取通訊紀錄及通訊使用者資料。

第三項　爭點及評析

第一款　隱私空間不只存在於地上物

在草案第 2 條，科技設備監視空間之區分，分成隱私空間、非隱私空間、空中及非空中。隱私空間，系指住宅、建築物、交通工具或其他具有隱蔽設施之地上物之內部空間，且具有隱私或秘密之合理期待。隱私空間以外的空間，即為非隱私空間。有學者認為，從第二條的定義上來看，隱私空間必須是地上物空間，此種立法方式，雖把規範的對象限制在一定範圍中，使執法者在執法時操作便利，但反言之，卻會大大限縮隱私的保護，因為隱私

不只存在地上物內，例如執法人員使用 X 光機顯像器來照射包包內攜帶物品的危險物品、架設體溫感測器針對每個來往的民眾監測體溫、在公共場所偵測包包內的手機訊號，都可能有隱私期待。以地上物區分隱私空間之規範過於狹隘。[189]。

本文認為隱私權本有高度及低度期待之區分，在公共場所身體、物件通常暴露於外，一般情形仍為多數人可共聞共見，若要主張與私密領域相同的隱私是有困難的，且可能造成實務執行判斷的困難，故贊同草案原條文，較為妥適可行。

第二款　發動門檻過低

在科技偵查法草案中，科技定位技術偵查之調查，隱私空間採取絕對法官保留，非隱私空間，則區分為空中監視(空拍機)之檢察官許可，及全球定位系統(GPS、M 化車)之使用 2 個月以上始需法官保留。在評論聲浪，有認為空中監視之調查，宜採相對法官保留，另全球定位系統，應縮短在至少在使用超過 2 天以上時，即應取得法官令狀。[190]亦有學者，提出應參酌奧地利、瑞士法制，認為在瑞士裝設 GPS 僅需檢察官許可；在奧地利，檢察官許可期限也有 3 個月[191]，並非要採取法官保留才是符合人權。本文認為，在現有的偵查程序，尚有其他干預屬性不低於科技定位技術偵查手段，亦非採用絕對法官保留原則，例如通保法通訊紀錄調取、刑訴法第 205-2 條毛髮、唾液、尿液、聲調之採取等。法官保留原則的基本目的在於建立一具備獨立與中立特性的機關，使相對人的基本權利能在

[189]李榮耕，立法院第 10 屆第 2 會期，「科技偵查手段引發人權爭議」公聽會報告，立法院司法及法制委員會，109 年 10 月。

[190] 新時代法律學社，科技偵查法草案的四點聲明，https://m.facebook.com/neweraassn/posts/940240333175061，2020 年 10 月 07 日。(最後瀏覽日 2022 年 2 月 5 日)

[191]潘怡宏，科技偵查立法藍圖 ——刑事訴訟目的之試金石（下），2020 年 10 月 23 日舉辦之「法治國之科技偵查與科技防疫」座談會發言紀錄。

面對國家公權力措施發生衝突時，得獲得充分的考慮與保障。[192]然而過度嚴格的「法官保留」要求恐怕亦會使偵查機關綁手綁腳，使偵查錯失良機或因無偵查之工具而無以蒐證，導致發現真實減損。另觀美國法制，科技定位技術偵查雖採法官保留原則，惟核發令狀的是治安法官。治安法官在美國是負責審理初審、微罪及核發令狀，與我國的「法官」定義上並不相同。科技定位技術偵查蒐集的僅是位置資訊，且無物理性侵害，故認為採一定期間之相對法官保留原則，層級化授權已足。

惟本文認為，在科技偵查法草案中，規範空中監視之調查僅需檢察官許可，全球定位系統（M 化車、GPS）需使用 2 個月以上才需法官保留之審查密度，發動門檻確實過低，故難免遭致非議。

第三款　限於重罪或排除微罪

該草案第 9 條，調查最重本刑三年以上有期徒刑之犯罪且有相當理由，可得使用科技設備或技術，自該隱私空間以外之處所，對該隱私空間內之人或物秘密實施非侵入性之監看、測量、辨識、拍照、錄影之調查。常見應用例如使用紅外線熱顯像儀用偵測住宅內生物跡象、使用空拍機拍攝住宅內的活動情形等，被抨擊認為公權力如可使用類似「狗仔隊」的偵查作為，審查密度應該要再提高改為「最輕本刑」而非「最重本刑」。重罪原則可區分為列舉重罪(例如通保法的監聽)或是排除微罪(通保法的通信紀錄調取)，立法採嚴格的重罪原則，是為了在侵害基本權與強制處分間取得平衡。嚴格的重罪原則，確實可能減少執法機關聲請的件數，但此種限制與保障人權是否能劃上等號，本文深感質疑。對照刑事訴訟法搜索之規範，不論對人或物的搜索，都需要有相當理由，但是對於罪名並沒有限制。

[192] 林鈺雄，刑事訴訟法(上冊)，2007 年 9 月 5 版，頁 289。

科技定位技術偵查，目的僅是「找人」，即獲得位置資訊，雖有隱私權及資訊自決權之侵害但畢竟輕微。在實務應用，取得位置資訊僅是調查犯罪及保全證據前置偵查手段，為的是實施後續的偵查作為及強制處分，本文認為採取排除微罪之立法方式，應已足夠。

第四款 無類似通保法之證據排除規範

依通保法第 18 條之 1 第 3 項：「違反第 5 條、第 6 條或第 7 條規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據或其他用途」，採絕對證據排除法則。而科技偵查法草案第 27 條規定「本法施行前，以第 5 條、第 9 條的方式所實施的調查，其調查所得有無證據能力，應審酌人權保障及公共利益的均衡維護。」僅處理立法前之「第 5 條、第 9 條實施之調查方式」，卻未處理立法後「證據排除」問題而被認為立法粗糙。亦有認為按在未正式立法完成實施，在之前運用科技設備或技術侵入隱私空間，已屬不法，因而調查所得本屬違法，原不具有證據能力；豈能透過立法容許回溯使之被賦予再審酌公共利益的均衡，而使之具有證據能力。[193]本文亦認同應增訂證據排除規範，將未依法取得或陳報之證據絕對排除，避免恣意偵查。

第五款 上網公告的期程與方式

有關制定法律草案，在公告後尚需立法院審議，然在本次科技偵查法草案僅公布 5 天時間過於倉促，被認為是暗度陳倉而受到強烈抨擊。在 105 年行政院為強化與國際規範接軌，落實開放透明政府，對外洽簽國際投資及經貿協定，發布 105 年 9 月 5 日院臺規字第 1050175399 號函，規定各機關

[193]李永然，ETtoday 法律新聞，《科技偵查法》恐上演《全民公敵》，2020 年 9 月 21 日，https://www.ettoday.net/news/20200921/1813977.htm#ixzz7UnC9qca0(最後瀏覽日 2022 年 3 月 10 日)

研擬之法律或法規命令草案,自 105 年 10 月 1 日起,應公告周知至少 60 日,使各界能事先瞭解,並有充分時間表達意見。在公告周知 60 日規定,有兩個例外,(一)情況急迫顯然無法事先公告周知,或法律草案經主管機關檢視確認與貿易、投資或智慧財產權無關者,得免為公告周知。(二)情況特殊,有定較短期間之必要者,各機關得另定較短之期間,並應於草案內容公告時,一併公告其理由。

法務部為回應質疑聲浪對此說明,公告未達 60 天之理由說明則是行政院函釋之後,其係指有關「貿易、投資與智慧財產權」之法案才需要公告 60 天,其他則無此限制。另外,法務部有將法案之預告置於「眾開講」網站上直至 110 年 11 月 25 日,經計算大約有 70 天,因此實際公告有 70 天之久,並無外界所說蒙混之嫌。法務部在經歷多次專家學者會議,始提出草案公告,可謂付出相當大的努力,但以情況特殊來縮短公告期程,反而造成輿論誤會,實在可惜。

第六款 主張以專法制定或刑事訴訟法修法

在蒐集文獻資料時發現,事實上有很多國家因為歷史背景或政治考量,並未制定類似科技偵查法之法案[194],因此,亦有部分意見認為應該考量是否有立法的必要性。在我國最高法院 106 年度臺上字第 3788 號刑事判決後,107 年法務部曾嘗試將 GPS 偵查法制化於通訊保障及監察法內,惟因採取檢察官許可,被認為過於側重偵查便利性遭到抨擊。108 年立法院委員[195]爰擬具「刑事訴訟法」增訂部分條文草案,在搜索扣押章節下增訂第十一章之一「全球定位追蹤監察程序」,列為強制處分一種,採法官保留原則,然而法

[194]例如韓國、泰國、越南。

[195]立法院議案關係文書,提案日期:中華民國 108 年 4 月 26 日、院總第 246 號委員提案第 23197 號、資料來源:立法院第 9 屆第 7 會期第 11 次會議議案關係文書、提案人:尤美女、連署人:劉建國等 17 人。

案立法意見未形成共識而石沉大海，直至本次經歷 M 化車判決，科技偵查法制化才再度受到重視。在本次科技偵查法草案，有主張以專法制定或刑事訴訟法修法，公聽會及研討會各方討論意見整理如次：

一、專法

科技偵查法跟通保法、刑事訴訟法有很多競合。科技偵查法如以特別法的方式處理，可因應科技領域變化。如以刑事訴訟法修法，以基本法而言會牽一髮而動全身，相較之下，特別法的修正較為彈性。[196]

科技偵查法規範有不少刑事實體法之處罰，與刑事訴訟法全部為程序法之性質不同；而通訊保障及監察法的部分，因其僅涉及通訊，許多科技偵查手段如空拍機、GPS 等都與通訊無關，因此尚難將科技偵查規範於刑事訴訟法或通訊保障及監察法。[197]

無論定在哪一個法，重要的是要兼顧科技偵查需求及人權保障，立法上立法院這邊要怎麼選擇，本院都尊重。科技偵查有別於傳統的強制處分，專法其實有助於針對科技偵查的特殊性，建立完整健全的司法審查機制、發動門檻、程序監督及事後救助。[198]

《科技偵查法》草案應比照《通訊保障及監察法》模式，更名《科技偵查及保障法》，且草案應加強程序保障規定，尤其是大幅提高法官保留密度。包含 GPS 追蹤器、無人機在內的監視目的之科技偵查，宜採「相對法官保留」之立法原則；至少在使用超過 2 日以上時，即應取得法官之令狀。目

196 蔡碧玉，司法新聲第 135 期、109 年 11 月、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。

197林錦村司長，中華警政研究學會，警政與警察法相關圓桌論壇（三十三）【科技偵查法制】，2020 年 12 月 30 日

198 葉麗霞，科技偵查立法藍圖 ——刑事訴訟目的之試金石（下），2020 年 10 月 23 日舉辦之「法治國之科技偵查與科技防疫」座談會發言紀錄。

前法務部公告草案，於使用 GPS 追蹤 2 個月後始需經過法官核准，法官保留密度顯然太低，呼籲法務部從善如流，重新檢討草案第 3 條至第 7 條之立法原則。[199]

二、修法

德國刑事訴訟法，是在搜索扣押章節裡面增加了使用科技方法，如果用我國現行法來思考科技偵查條文的位置，我覺得有三種可能性的。第一種是放在刑事訴訟法的搜索扣押後，增訂第 153 條之 1 以下條文，例如科偵法草案總共 28 條，就變成第 153 條之 1 到第 153 條之 28。第二個選項，是刑事訴訟法增訂第 455 條之 48 以下，我覺得較不可行，因為現在是到第 455 條 47，再往後加條文，立法技術和記憶會變得困難。現在有第 455 條之 2 的協商，第 455 條之 12 的第三人沒收程序，第 455 條之 38 的被害人訴訟參與，如果再加上科偵法草案的 28 條，刑訴條文會變成第 455 條之 48 到第 455 條之 76，過於膨脹並不妥適。第三個選項，是放在刑事訴訟法第 512 條後面，就是增訂第 513 條科技偵查編，我想這個應該是可行的，如果願意放在刑事訴訟法，我當然是樂觀其成。[200]

就算是偵查犯罪行為，發動界線仍應還是小心謹慎，例如通保法，就有規範一定罪名及法官保留原則，且應以最小侵害、最低限度為原則為之。若法務部認為需要處理科技偵查，應修改「通保法」不是立新法律。[201]

在修法與專法的討論，本文贊同以專法處理較為妥適，理由是在探討科技偵查的實質內容，與通保法並不相符，應放在刑事訴訟法。但若放在刑事

[199] 楊雲驊，科技偵查與人權保障研討會、109 年 10 月 7 日、主辦單位：新時代法律學社。
[200] 王士帆，科技偵查立法藍圖 ——刑事訴訟目的之試金石（上），2020 年 10 月 23 日舉辦之「法治國之科技偵查與科技防疫」座談會發言紀錄。
[201] 自由時報，科技偵查法爭議 法界：修通保法即可不需立新法，2020 年 9 月 16 日，(最後瀏覽日 2022 年 2 月 10 日)，https://news.ltn.com.tw/news/politics/breakingnews/3293422。

訴訟法內增加新的篇章，在修訂上較無彈性，且基於科技偵查的特殊性與變動性，制定專法可能會是較為可行的方式。以下將科技偵查法草案、刑事訴訟法、通保法之層級化授權化比較如次：

科技偵查法草案、通保法、刑事訴訟法之層級化授權比較				
	補充性原則	**命令權限：法官保留/急迫權限**	**罪名限制**	**期間**
住宅監聽	絕　對　禁　止			
通訊監察/非住宅談話監聽(通保法第 5、6 條)	不能或難以其他方法蒐集或調查證據	法院命令/檢察官及司法警察	限列舉重罪＋個案情節重大	每次不得逾 30 日，得延長，若逾一年，應重行聲請
通聯記錄(通保法第 11-1 條)		法院命令/檢察官；列舉重罪:檢察官及司法警察	最重本刑三年以上/最輕本刑十年以上及列舉重罪	
使用科技設備監視(科偵法草案)		隱私空間：法官保留 非隱私空間：空中監視(檢察官許可)、全球定位系統(一定期間以上法官保留)	隱私空間最重本刑三年以上/非隱私空間無限制	空中監視每次 30 日/全球定位系統逾 2 個月向法院聲請,每次不得逾 30 日
搜索、扣押(刑訴法)	相當理由	法院命令/檢察官及其偵查人員	不限罪名	
偵查機關一般授權條款(刑訴法)	檢察官及司法警察有權進行偵查及調查(第 228 條第 1 項,、第 229 條第 1 項、第 230 條第 1、2 項、第 231 條第 1、2 項)			
1、本圖表來源：2020 年 10 月 7 日、科技偵查與人權保障研討會、新時代法律學社主辦、引言人連孟琦老師。 2、本圖表另參草案規範內容整理比較。 3、目前偵查手段授權之層級化，最上層（住宅監聽）為干預基本權重大，審核最為嚴格，依次排序到最下層為最為寬鬆之一般偵查授權條款。				

第六章　結論與建議

第一節　結論

找人是犯罪偵查的基本功，從傳統的跟監、裝設攝影機、全球定位系統，涵括了有肖像權、隱私權、人格權、資訊權，如一一檢視刑事訴訟法等相關法令之干預授權基礎，竟會發現我國既有法令難以尋得適切的法律依據。科技產品如雨後春筍問世，傳統偵查方式配合科技設備，便可能產生較嚴重的基本權干預，在科技發展下，衍生問題陸續浮現，雖透過判決帶動新觀念和發展，但立法之路仍舊漫漫。本文所述比較法中可見，現今多數法治國早已逐漸重視並且建立明確法制規範，在科技與人權的較勁下，本文贊同在秉持我國裁判強制處分法定原則[202]之思維脈絡，給予法律授權基礎，才是有效的解決之道。

本文將實務應用於科技定位技術偵查工具逐一臚列說明，可發現在其他領域及法令上，研發科技定位技術應用早已行之有年，然而在偵查領域，卻仍遲遲未給予法律授權基礎。觀察國外法制，美國早期在財產權判斷基準到合理期待隱私權的界線，在思維流變，陸續在 2012 年 Jones 案 GPS 判決，2014 年 Tate 案 StingRay 判決後，認為使用該項技術符合令狀原則。另在德國， 2002 年即在刑事訴訟法創設 IMSI-Catcher 法律基礎，2019 年修法第 100h 條涵蓋 GPS 及空拍機之科技設備監視之規範，均可做為立法借鏡。

科技定位技術偵查我國並非首創（雖然不同國家科技設備名稱不同），在抨擊制定科技偵查法是所謂「嚴重侵害人權」、「全民公敵監視」同時，我們也許應考量，更有前瞻性地與時俱進制定法令，將科技框架並納管，要求透明的數位監督，才是務實的解決之道。有關科技定位技術偵查在我國科

[202] 最高法院 106 年度臺上字第 3788 號刑事判決。

技偵查法草案，本文試圖綜整提出立法建議，期盼在偵查干預授權及基本人權保障下，科技定位技術偵查能早日落實法制化之路。

第二節　立法建議

一、《科技偵查法》應更名為《科技偵查及保障法》。第一條可參照通保法及個資法之立法目的(參通保法第一條立法目的，為保障人民秘密通訊自由及隱私權及不受非法侵害；個資法第一條立法目的，為規範個人資料之蒐集、處理及利用，以避免人格權受侵害)，將科技偵查可能干預之基本權納入立法目的，使立法理由及宗旨更為明確。

第一條：「為規範科技偵查，『保障隱私權及人格權』，並有效追訴犯罪，確保國家安全，維護社會秩序，特制定本法」。

二、第四條【非隱私空間之以科技設備或技術空中監視、攝錄與追查位置】與第五條【利用全球定位系統等追蹤位置功能之科技設備或技術實施調查】應加以合併：

第◯條「1.檢察官、檢察事務官、司法警察官或司法警察，於犯罪偵查時，為查明案情或調查被告或犯罪嫌疑人所在地之必要，得於住宅外，使用全球衛星定位系統或其他為監視目的之科技設備。2.對於被告或犯罪嫌疑人以外之人，已有相當理由可信其與被告有聯繫或可能聯繫，且非使用前項規定之科技設備難以查明案情或調查被告或犯罪嫌疑人所在地者為限，亦得於住宅外對其為之。3.前二項之處分，使用逾二日或持續不斷使用超過 24 小時者，應經法官核准。但於偵查中確有相當理由認為情形急迫，非迅速實施該處分，難以查明案情或調查被告或犯罪嫌疑人所在地者，亦得由檢察官、檢察事務官、司法警察官為之。4.前項但書情形，由檢察官為之者，應於實施後三日內陳報該管法院；由檢察事務官、司法警察官或司法警察為之者，應於執行後三日內報告該管檢察署檢察官及法院。法院認為不應准許者，應

於五日內撤銷之。5.違反前項規定，執行後未陳報該管法院，或陳報後經法院撤銷者，審判時法院得宣告所取得之證據，不得作為證據」。[203]將空中監視及全球定位系統相類設備，發動門檻修正為使用逾 2 日或不間斷使用超過 24 小時，即需要法官保留，以衡平人權保障。

三、第十條【以科技設備或技術監看、測量、辨識、拍照、錄影隱私空間之「急迫情形」逕行實施，不許可立即停止】：

第◯條「1.檢察官、檢察事務官、司法警察官或司法警察有相當理由認須實施前條之調查而情況急迫者，得逕行實施。2.前項情形，由檢察官為之者，應於實施後三日內聲請該管法院許可；由檢察事務官、司法警察官或司法警察為之者，應於實施後三日內報請檢察官同意聲請該管法院許可。『法院認為不應准許者，應於五日內撤銷之。3. 違反前項規定，執行後未陳報該管法院，或陳報後經法院撤銷者，審判時法院得宣告所取得之證據，不得作為證據』」，並刪除原條文「檢察官或法院於報請日或聲請日逾三日未為同意或許可之表示或裁定者，視為不同意或不許可」部分條文。比照通保法條文，急迫情形亦需陳報法院審核證據能力，經法院撤銷者，審判時法院得宣告所取得之證據，不得作為證據，以避免恣意偵查。

四、第二十七條「本法實施前，以第五條、第九條之方式所實施之調查，其調查有無證據能力，應審酌人權保障及公共利益之均衡維護」刪除：

本條文僅處理立法前之第五條、第九條實施之調查方式，卻未處理其他調查方式之立法方式，甚為粗糙。按在未正式立法完成實施，運用科技設備或技術侵入隱私空間，尚屬不法，因而調查所得本屬違法，原不具有證據能力；不宜透過立法容許回溯，而使之具有證據能力。

[203]新時代法律學社，科技偵查法草案的四點聲明，https://m.facebook.com/neweraassn/posts/940240333175061，2020 年 10 月 07 日。(最後瀏覽日 2022 年 3 月 5 日)

參考文獻

一、中文文獻

(一)專書

李榮耕，數位時代的搜索扣押，初版，元照出版，2020 年 4 月。

林山田，刑法通論(上)，2008 年 1 月。

林鈺雄，刑事訴訟法上冊十版，新學林出版，2020 年 9 月。

許文義，個人資料保護法論，2001 年。

連孟琦，德國刑事訴訟法—附德國法院組織法選譯，元照出版，2019 年 9 月。

陳樸生，刑事訴訟法實務，1999 年。

黃清德，科技定位追蹤監視與基本人權保障，元照出版，2011 年 11 月。

曾德文，資通科技犯罪偵查通訊篇，2013 年 8 月。

黃朝義，刑事訴訟法程序基礎理論，新學林出版，2020 年 1 月。

鄭厚塋，警察百科全書，2000 年 1 月。

(二)期刊論文

王皇玉，刑法對隱私權的保障-以刑法第 315 條之 1 為中心，台灣法學雜誌第 122 期，頁 37-39。

王士帆，德國聯邦最高法院刑事裁判 BGHSt 63, 82 —發送「無聲簡訊」的法律基礎—，司法周刊，109 年 12 月 31 日，頁 2-3。

王士帆，科技偵查立法藍圖（上）——刑事訴訟目的之試金石，月旦裁判時報，103 期，102-122 頁。

王士帆，刑事法與憲法對話：科技犯罪與偵查會議實錄——科技偵查與令狀原則與談稿，月旦法學月刊第 4 期，2021 年 4 月，頁 1-6。

王士帆，M 化車法制出路-德國 IMSI-Catcher 科技偵查借鏡，2022 年 3 月，臺北大學法學論叢，第 121 期，頁 55-117。

王士帆，德國科技偵查規定釋義，法學叢刊，第 66 卷第 2 期，頁 85-132。
王兆鵬，重新定義高科技時代下的搜索，月旦法學雜誌，2003 年 2 月、93 期，頁 166-182。
安守中，GPS 與都卜勒勒偏移量的基礎介紹，全華科技圖書股份有限公司，2005 年 10 月，頁 2-85。
何信慶，從立法審議過程談新修正通訊保障及監察法，司法新聲第 111 期，頁 27-50。
吳世琳、張自強、葉禹良、許冠傑，無線網路定位技術應用於即時救援，臺灣職能治療研究與實務雜誌，4 卷 2 期，2008 年 12 月，頁 139 – 150。
吳巡龍，檢察官傳訊方式及任意偵查，2009 年 2 月出版，刑事法雜誌，頁 1-21。
吳坤龍、刑事局通訊監察中心，刑事雙月刊第 31 期，從神秘的獵狐到 M 化的宿命，頁 44-46。
吳俊毅，德國刑事訴訟上使用衛星定位技術進行監察之研究，中正大學法學期刊， 107 年 4 月 29 日，頁 29-75。
吳俊毅，刑事訴訟上的線上搜索（Online-Durchsuchung）與源頭通訊監察（Quelle-TKÜ） —引進的必要性及實踐上的困境，刑事政策與犯罪研究論文集，頁 461-484。
李榮耕，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，國立臺灣大學法學論叢，2015 年 9 月，44 期，頁 875-886。
李榮耕，簡評二〇一四新修正的通訊保障及監察法—一次不知所謂何來的修法，月旦法學雜誌第 227 期，2014 年 4 月，頁 148-175。
李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，2010 年 6 月，115 期，頁 127-129。

李震山，個人資料保護與警政資訊管理，「資訊管理學術暨警政資訊實務研討會」論文集，中央警察大學，1966 年 3 月，第 4-20 頁。
林安邦，德國「資訊自主權」之概念在我國法律上之應用，公民訓育學報 12 期 ，2002 年 7 月，頁 109-122。
林老生、郭清智，整合 Wi-Fi 與 GPS 技術於室外定位之研究，臺灣土地研究，18 卷 1 期，2015 年 5 月，頁 1-19。
林鈺雄，干預保留與門檻理論－司法警察（官）一般調查權限之理論檢討，政大法學評論第 96 期，2007 年 4 月，頁 189-232。
林鈺雄，科技偵查立法藍圖（上）——刑事訴訟目的之試金石，月旦裁判時報，103 期，102-122 頁。
林利芝，從美國最高法院 United States v. Jones 案分析美國政府運用 GPS 定位追蹤器探知個人位置資訊之適法性，2018 年 1 月、月旦法學雜誌、頁 177-188。
范里，跟監應屬刑事訴訟上之基本權干預——評最高法院 102 年度台上字第 3522 號判決，刑事法雜誌，58 卷 2 期，2014 年 4 月，頁 75-83。
邱文聰，科技防疫與個人資料保護，中央研究院法律學研究所研究員，「法治國之科技偵查與科技防」研討會，臺灣法學會主辦，2020 年 10 月 23 日。
陳士杰、韓邦郡、王安妮、石宛璇、杜念庭，以行動裝置與穿戴式設備為基礎之孩童隨身照護機制之研究，臺東大學綠色科學學刊， 5 卷 2 期， 2015 年 11 月，頁 151-160。
陳詩經，衛星定位系統，船舶科技，9 期，1992 年 4 月。
陳重言，刑事追訴目的之通信(通聯)紀錄調取與使用一兼評 2014 年初通保修法,檢察新論第 16 期,2014 年 7 月,頁 50-55。
陳宗奇，合理隱私期待之末路？-近期歐洲人權法院隱私權相關判決概述，律師法學期刊，202012 月，第五期，頁 93-95。

陳運財，偵查之基本原則與任意偵查之界限，東海大學法學研究 1995 年 9 月，9 期，頁 31。
陳運財，GPS 監控位置資訊的法定程序，台灣法學雜誌，293 期，2016 年 4 月 14 日，頁 59-74。
許福生，科技設備監控在性侵害犯之運用，月旦法學雜誌，166 期，2009 年 3 月，頁 92-110。
許恒達，GPS 抓姦與行動隱私的保護界限——評臺灣高等法院一〇〇年度上易字第二四〇七號刑事判決，月旦裁判時報，24 期，2013 年 12 月，頁 59-78。
許恒達，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，2010 年 1，頁 119-120 月。
許義寶，警察蒐集與利用個人資料職權之研究——以警察職權行使法第十七條為中心，高雄大學法學院，2019 年 9 月第 15 卷 1 期，頁 71-114。
施育傑，科技時代的偵查干預處分——兼論我國法方向，月旦法學雜誌，306 期，2020 年 11 月，頁 166-168。
崔文、殷志揚、陳昭男，行動網路定位技術概觀，電腦與通訊 115 期，2006 年 3 月，頁 54-60。
黃俊麟，中共衛星航太科技與反衛星系統發展，國防雜誌，22 卷 4 期，2007 年 8 月，頁 40-52；林明武、林輝龍，導航衛星於電子戰作為之研究，國防雜誌，25 卷 5 期，2010 年 10 月，頁 75-87。
黃政龍，美國行動電話定位追蹤法規範研究、警大法學論集，第 18 期 99 年 4 月，頁 171-172。
程正孚，藍芽的演進，台灣電信月刊，108 年 3-4 月號，頁 13-14。
楊雲驊，司法改革雜誌 62 期，2006 年 6 月 25 日，頁 32-35，保障「私人生活不可侵犯之核心領域」—德國聯邦憲法法院對於「住宅內監聽」（大監聽）違憲審查判決簡評。

楊雲驊，「通訊保障及監察法」實施前電話監聽合法性及證據評價的探討——評最高法院九〇年台上字第八四八號、九一年台上字第二九〇五號及 八七年台上字第四〇二五號判決，台灣本土法學雜誌，57 期，2004 年 4 月，頁 37-54。

楊雲驊，科技偵查與人權保障研討會、109 年 10 月 7 日、主辦單位：新時代法律學社。

詹明華、邱紹洲、易序忠，通聯紀錄在犯罪偵查上之應用－行動電話持機人之動態與靜態分析，警學叢刊第 33 卷第 2 期，中央警察大學，2002 年，頁 111-131。

詹明華、李文章，全球衛星定位系統在犯罪偵防上之應用，刑事科學，第 59 期，2005 年 9 月，頁 11-15。

詹明華、陳弘斌、宋奕賢，定位技術在犯罪偵查上之應用，刑事科學，第 80 期，2016 年 3 月，頁 1-13。

葛祥林，數位化、大數據和人工智慧對刑事訴訟的衝擊，高大法學論叢，2020 年 3 月，第 15 卷第 2 期，頁 54。

溫祖德，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，2020 年，297 期，頁 133-135。

劉靜怡，通訊監察與民主監督：歐美爭議發展趨勢之反思，中央研究院歐美研究所《歐美研究》第四十七卷第一期，106 年 3 月，頁 43-106。

劉靜怡，大法官保護了誰？——釋字第 689 號的初步觀察，月旦法學雜誌，197 期，2011 年 10 月，頁 47-61。

劉靜怡，科技偵查立法藍圖 ——刑事訴訟目的之試金石（下），2020 年 10 月 23 日舉辦之「法治國之科技偵查與科技防疫」座談會；主辦單位：台灣法學會憲法行政法委員會、台灣法學會刑事法委員會；協辦單位：元照出版公司。

賴進貴，導航系統發展與地圖問題之探討，中華民國地圖學會會刊， 7 期， 1996 年 12 月，頁 27-35。

薛智仁，衛星定位追蹤之刑責－評臺灣高等法院 100 年度上易字第 2407 號判決，科技法學評論，11 卷 1 期，2014 年 6 月，頁 119-154。薛智仁，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，刑事程序法定原則，月旦刑事法評論，2018 年 11 期，頁 28-29。謝碩駿，警察機關的駭客任務——論線上搜索在警察法領域內實施的法律問題，2015 年 3 月，臺北大學法學論叢，頁 21-24。
蔡蕙芳，從美國隱私權法論刑法第 315 條之 1 與相關各構成要件(下)，興大法學 7 期，2010 年 6 月，頁 36-37。
簡宏偉、吳麗芬、洪振耀、劉倢旻、吳卓葳、林瑜，大數據運用與隱私保護－手機定位資訊於防疫應用之法律問題研析，國土及治理季刊，第八卷第三期，109 年 9 月，頁 64-75。
羅春秋，中共「北斗」導航衛星發展及其軍事戰略意涵，國防雜誌，29 卷 6 期，2014 年 11 月，頁 63-79。
(三)碩博士論文
朱翊雯，結合 TOA 及 AOA 混合式定位技術於地面無線定位之應用，成功大學電機工程學系碩士論文。
林誠澤，GPS 科技定位偵查與刑事訴訟法的搜索概念，國立政治大學法律學系碩士班碩士學位論文。
林永瀚，論前偵查程序，國立政治大學法律學研究所碩士論文。吳梓榕，一般偵查措施的合憲控制——從偵查程序之自由形成原則出發，政治大學法律學研究所碩士論文。
黃政龍，新型態科技偵查作為之法規範研究，中央警察大學警察政策所博士論文。
(四)大法官釋字：
1、司法院釋字第 443 號。
2、司法院釋字第 585 號。

2、司法院釋字第 603 號。

3、司法院釋字第 631 號。

4、司法院釋字第 689 號。

(五)判例（決）：

1、最高法院 101 年度台上字第 5635 號判決。

2、最高法院 102 年度台上字第 3522 號判決。

3、最高法院 106 年度台上字 3788 號判決。

4、最高法院 106 年度台非字第 259 號判決。

5、高等法院 101 年度上易 2814 判決。

6、臺灣高等法院 109 年度上易字第 1683 號刑事判決。

7、臺灣高等法院 98 年度上字第 108 號民事判決。

8、高等法院台南分院 102 年度上訴字第 75 號判決。

9、臺灣高等法院臺南分院 105 年度上易字第 393 號刑事判決。

10、臺灣桃園地方法院 106 年度易字第 164 號刑事判決。

(六)翻譯文獻

王士帆，德國聯邦最高法院刑事裁判 BGHSt 44, 13 ——住宅外長期監視錄影，司法周刊 2054 期，2021 年 5 月 14 日，頁 2-3。

陳怡凱節譯，司法院德國聯邦憲法法院裁判選輯（十三）100 年 5 月，「Nordrhein-Westfalen 邦警察法上之電子搜尋追緝是否侵犯資訊自決之基本權」裁定(BVerfGE 115, 320) 德國聯邦憲法法院 2006 年 4 月 4 日第一庭裁定。

蔡宗珍節譯，司法院歐洲人權法院裁判選譯（一），Von Hannover v. Germany, no.59320/00, § 51, ECHR, 2004-VI.。

蔡宗珍 張君魁節譯，司法院歐洲人權法院裁判選譯（四）2018 年 11 月，Uzun v. Germany 歐洲人權法院第五庭於 2010 年 9 月 2 日之裁判(案號：35623/05)。

蕭文生節譯，司法院西德聯邦憲法法院裁判選輯（一），關於「一九八三年人口普查法之判決」，109 年 10 月，第 288-348 頁。

劉靜怡節譯，司法院歐洲人權法院裁判選譯（四），Mosley v. The United Kingdom, no.48009/08, §§ 16-25, ECUR, 10 May 2011。

謝碩駿譯，司法院德國聯邦憲法法院裁判選輯（十四）102 年 04 月，「預防性電信監察」判決(BVerfGE 113, 348, 1 BvR 668/04)德國聯邦憲法法院第一庭 2005 年 7 月 27 日。

二、外文文獻

(一)英文文獻

美國司法部政策說明，Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators，2015 年 9 月 3 日

Tamir Israel、Christopher Parsons，加拿大多倫多大學蒙克國際研究中心公民實驗室研究報告，2016 年 8 月 1 日。

Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967)

Oliver v. US , 466 US 170, 104 S.Ct. 1735 (1984)

Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564 (1928)

United States v. Miller, 425 U.S. 435, 443 (1976)

Couch v. United States, 409 U.S. 322, 335 (1973)

Smith v. Maryland, 442 U.S. 735, 743－44 (1979)

Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018)

Riley v. California, 134 S. Ct. 2473, 189 L. Ed. 2d 430, 24 Fla. L. Weekly Supp. 921, 60 Commc'ns Reg. (BNA) 1175 (2014)

State v. Andrews, 227 Md. App. 350, (Md. Ct. Spec. App. 2016)

United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016)

Kyllo v. United States , 533 US 27 (2001)
United States v. Thomas , 757 F.2d 1359, 1366－67 (2d Cir.1985)
State v. Tate, 849 N.W.2d 798, 2014 WI 89 (Wis. 2014)
United States v. Garcia, 906 F.3d 1255 (11th Cir. 2018)
United States v. Marquez, Case No.: 3:19-cr-4626-BTM-1 (S.D. Cal. Nov. 25, 2020)
United States v. Knotts, CASE NUMBER 6:20-CR-00086-JDK (E.D. Tex. Mar. 23, 2021)
United States v. Jones, 132 S. Ct. 945 (2012)
ECHR Köpke v. Germany, no.420/07, 2010。
ECHR Mehmedovic v. Switzerland, no. 17331/11, 2019。
ECHR Antović and Mirković v. Montenegro, no. 70838/13, 2017, §43。
Big Brother Watch and Others v. the United · Kingdom (application nos. 58170/13, 62322/14 and 24969/15)。
Roman Zakharov v. Russia, no. 47143/06, 4 December 2015，歐洲人權法院網站。

德國刑事訴訟法——附德國法院組織法選譯

(連孟琦，元照出版公司、2016 年 9 月出版)

第 100f 條 【住宅外聲音監察】

(1) 符合下列情形時，即使受干預人不知情，亦得使用科技設備，對住宅外之非公開言談進行監聽及記錄，即當一定事實構成懷疑，某人作為正犯或共犯犯了第 100a 條第 2 項所稱之犯罪，且該犯罪在個案 中亦屬嚴重，或在未遂可罰之情況下著手實施，並且查清案情或調 查被告所在地採用其他方式可能無望或非常困難時。

(2) 處分僅得針對被告。針對其他人之處分僅得在下列情形命令之，即當根據一定事實可以認為其他人與被告有聯繫或將建立此種聯繫，且預計處分可查清案情或調查被告所在地，並且為查清案情或調查被告所在地採用其他方式可能無望或非常困難時。

(3) 即使將無可避免地干預其他人，亦得執行處分。

(4) 第 100b 條第 1 項、第 4 項第 1 句及第 100d 條第 2 項規定準用之。

第 100h 條 【住宅外之其他科技設備】

(1) 即使受干預人不知情，若查清案情或調查被告所在地採取其他方式可能收效不大或困難時，亦得在住宅之外 1. 拍照，2. 使用其他特別為監視目的所設之科技設備。第 1 句第 2 款之處分，僅在調查對象為十分重大之犯罪時才得為之。

(2) 處分僅得針對被告。針對其他人：1. 第 1 項第 1 款之處分，僅在查清案情或調查被告所在地採取其他方式可能收效甚微或非常困難時，才得為之。2. 第 1 項第 2 款之處分，僅在根據一定事實可以認為其他人與被告有聯繫或將建立聯繫，且預計處分可查清案情或調查被告所在地，並且採用其他方式可能無望或非常困難時，才得為之。

(3) 即使將無可避免地連帶干預第三人，亦得執行處分。

第 100i 條 【用科技設備調查行動通訊設備】

(1) 若一定事實有理由懷疑某人作為正犯或共犯犯了在個案中亦屬十 分嚴重，尤其是第 100a 條第 2 項所稱之犯罪，或在未遂可罰之情況 下著手實施，或以一犯罪進行預備時，只要為查清案情或調查被 告所在地有必要，得採用科技設備調查 1. 行動通訊設備之機器號碼或機器中所使用卡片之卡號，及 2. 行動通訊設備所在位置。

(2) 第三人之個人資料，僅在為達成第 1 項之目的，出於技術原因無可 避免時，才得在執行處分時附帶取得。2 除為調查所尋找之機器號碼及卡號而對比資料外，不得使用該個人資料，且在處分結束後 應儘速刪除。

(3) 第 100a 條第 3 項及第 100b 條第 1 項第 1 句至第 3 句、第 2 項第 1 句及第 4 項第 1 句之規定準用之。命令最長期限為 6 個月。當第 1 項所稱之要件仍然持續成立時，得為每次不超過 6 個月之延長。

附錄二

美國司法部 Cell-site Stimulator 說明原文

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology

Cell-site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell-site simulators fulfill critical operational needs.

As with any law enforcement capability, the Department must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the Department must continue to assess its tools to ensure that practice and applicable policies reflect the Department's law enforcement and national security missions, as well as the Department's commitments to accord appropriate respect for individuals' privacy and civil liberties. This policy provides additional guidance and establishes common principles for the use of cell-site simulators across the Department.[1] The Department's individual law enforcement components may issue additional specific guidance consistent with this policy.

BACKGROUND

Cell-site simulators, on occasion, have been the subject of misperception and confusion. To avoid any confusion here, this section provides information about the use of the equipment and defines the capabilities that are the subject of this policy.

Basic Uses

Law enforcement agents can use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity. This technology is one tool among many traditional law enforcement techniques, and is deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

[1] This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. When acting pursuant to the Foreign Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy.

How They Function

Cell-site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

What They Do and Do Not Obtain

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

MANAGEMENT CONTROLS AND ACCOUNTABILITY[2]

Cell-site simulators require training and practice to operate correctly. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their agency to use the technology and whose training has been administered by a qualified agency component or expert.

[2] This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.

2. Within 30 days, agencies shall designate an executive-level point of contact at each division or district office responsible for the implementation of this policy, and for promoting compliance with its provisions, within his or her jurisdiction.

3. Prior to deployment of the technology, use of a cell-site simulator by the agency must be approved by an appropriate individual who has attained the grade of a first-level supervisor. Any emergency use of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by the executive-level point of contact for the jurisdiction, as described in paragraph 2 of this section, or by a branch or unit chief at the agency's headquarters.

Each agency shall identify training protocols. These protocols must include training on privacy and civil liberties developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

LEGAL PROCESS AND COURT ORDERS

The use of cell-site simulators is permitted only as authorized by law and policy. While the Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or the applicable state equivalent), except as provided below.

As a practical matter, because prosecutors will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in the immediately following section of this policy ("Applications for Use of Cell-Site Simulators").

There are two circumstances in which this policy does not require a warrant prior to the use of a cell-site simulator.

1. *Exigent Circumstances under the Fourth Amendment*

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval in order to be lawfully deployed. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. In addition, the operator must obtain the requisite internal approval to use a pen register before using a cell-site simulator. In order to comply with the terms of this policy and with 18 U.S.C. § 3125,[3] the operator must contact the duty AUSA in the local U.S. Attorney's Office, who will then call the DOJ Command Center to reach a supervisory attorney in the Electronic Surveillance Unit (ESU) of the Office of Enforcement Operations.[4] Assuming the parameters of the statute are met, the ESU attorney will contact a DAAG in the Criminal Division[5] and provide a short briefing. If the DAAG approves, the ESU attorney will relay the verbal authorization to the AUSA, who must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125. Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours has passed, whichever comes first.

2. *Exceptional Circumstances Where the Law Does Not Require a Warrant*

There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. In such cases, which we expect to be very limited, agents must first obtain approval from executive-level personnel at the agency's headquarters and the relevant U.S. Attorney, and then from a Criminal Division DAAG. The Criminal Division shall keep track of the number of times the use of a cell-site simulator is approved under this subsection, as well as the circumstances underlying each such use.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition,

---

[3] Knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).

[4] In non-federal cases, the operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

[5] In requests for emergency pen authority, and for relief under the exceptional circumstances provision, the Criminal Division DAAG will consult as appropriate with a National Security Division DAAG on matters within the National Security Division's purview.

if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in section 1 directly above).

APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

When making any application to a court, the Department's lawyers and law enforcement officers must, as always, disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement agents must consult with prosecutors[6] in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.[7]

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.

2. An application or supporting affidavit should inform the court that the target cellular device (*e.g.*, cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.

3. An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

---

[6] While this provision typically will implicate notification to Assistant United States Attorneys, it also extends to state and local prosecutors, where such personnel are engaged in operations involving cell-site simulators.

[7] Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (*e.g.*, tradecraft, capabilities, limitations or specifications). Sample applications containing such technical information are available from the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division. To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS, which will coordinate with appropriate Department components.

DATA COLLECTION AND DISPOSAL

The Department is committed to ensuring that law enforcement practices concerning the collection or retention[8] of data are lawful, and appropriately respect the important privacy interests of individuals. As part of this commitment, the Department's law enforcement agencies operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence,[9] the Department's use of cell-site simulators shall include the following practices:

1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.

2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.

3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

Agencies shall implement an auditing program to ensure that the data is deleted in the manner described above.

STATE AND LOCAL PARTNERS

The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies.

TRAINING AND COORDINATION, AND ONGOING MANAGEMENT

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Each law enforcement agency shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the

---

[8] In the context of this policy, the terms "collection" and "retention" are used to address only the unique technical process of identifying dialing, routing, addressing, or signaling information, as described by 18 U.S.C. § 3127(3), emitted by cellular devices. "Collection" means the process by which unique identifier signals are obtained; "retention" refers to the period during which the dialing, routing, addressing, or signaling information is utilized to locate or identify a target device, continuing until the point at which such information is deleted.

[9] It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent investigators know or have reason to believe that information is exculpatory or impeaching they have a duty to memorialize that information.

responsibility of each agency with respect to the way the equipment is being used (*e.g.*, significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). We expect that agents will familiarize themselves with this policy and comply with all agency orders concerning the use of this technology.

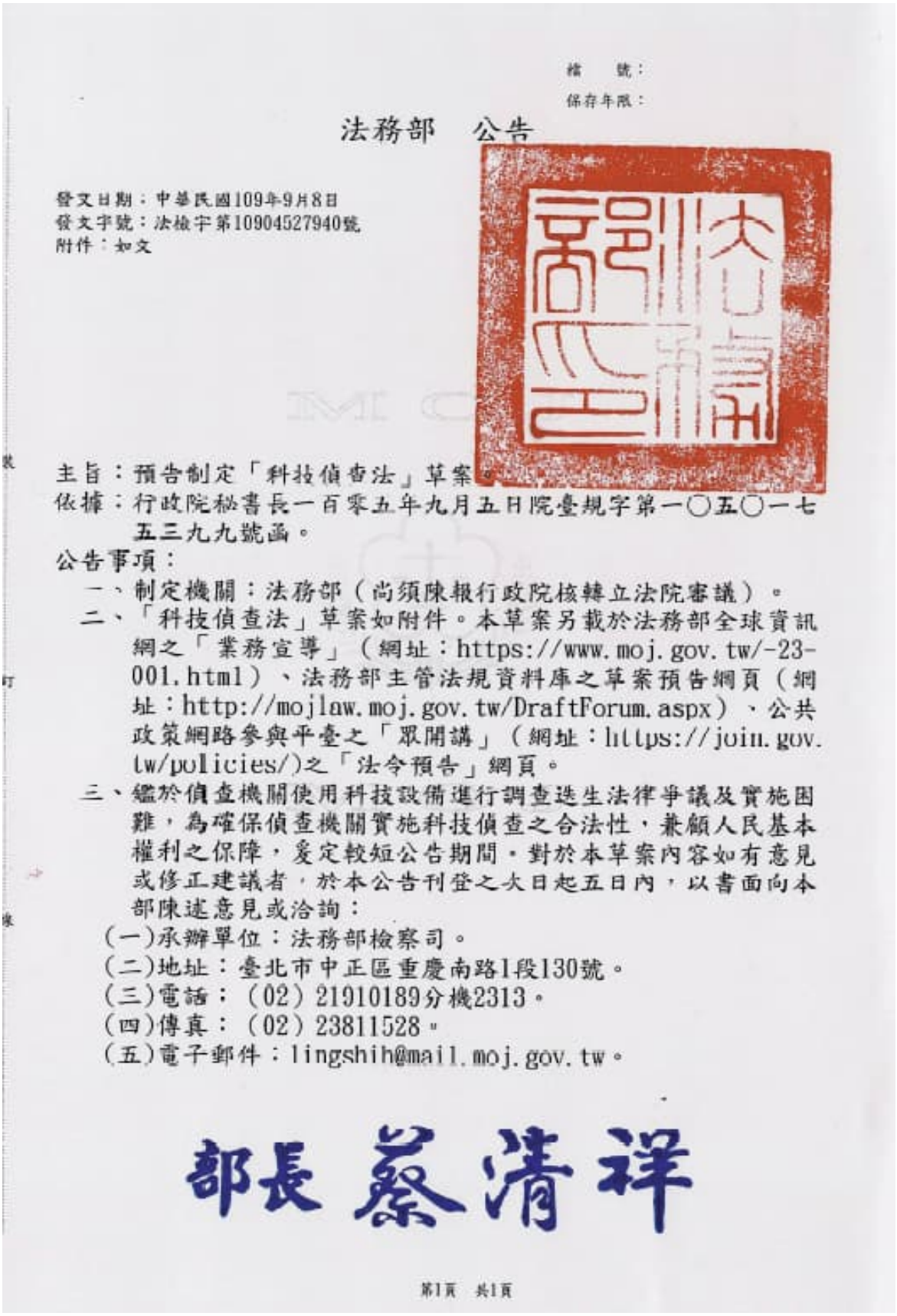
Each division or district office shall report to its agency headquarters annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction; the number of deployments at the request of other agencies, including State or Local law enforcement; and the number of times the technology is deployed in emergency circumstances.

Similarly, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent. Model materials will be provided to all United States Attorneys' Offices and litigating components, each of which shall conduct training for their attorneys.

* * *

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. This policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

我國科技偵查法草案



檔　　號：
保存年限：

法務部　公告

發文日期：中華民國109年9月8日
發文字號：法檢字第10904527940號
附件：如文

主旨：預告制定「科技偵查法」草案。

依據：行政院秘書長一百零五年九月五日院臺規字第一〇五〇一七五三九九號函。

公告事項：

一、制定機關：法務部（尚須陳報行政院核轉立法院審議）。

二、「科技偵查法」草案如附件。本草案另載於法務部全球資訊網之「業務宣導」（網址：https://www.moj.gov.tw/-23-001.html）、法務部主管法規資料庫之草案預告網頁（網址：http://mojlaw.moj.gov.tw/DraftForum.aspx）、公共政策網路參與平臺之「眾開講」（網址：https://join.gov.tw/policies/)之「法令預告」網頁。

三、鑑於偵查機關使用科技設備進行調查迭生法律爭議及實施困難，為確保偵查機關實施科技偵查之合法性，兼顧人民基本權利之保障，爰定較短公告期間，對於本草案內容如有意見或修正建議者，於本公告刊登之次日起五日內，以書面向本部陳述意見或洽詢：

(一)承辦單位：法務部檢察司。
(二)地址：臺北市中正區重慶南路1段130號。
(三)電話：（02）21910189分機2313。
(四)傳真：（02）23811528。
(五)電子郵件：lingshih@mail.moj.gov.tw。

部長 蔡清祥

第1頁　共1頁

條文	說明
第一章 總則	本章揭示立法目的及各章相關專有名詞之定義。
第一條 為規範科技偵查，以保障人權，並有效追訴犯罪，確保國家安全，維護社會秩序，特制定本法。	一、現今科技日新月異，偵查機關大量運用科技設備或技術，進行必要之科技偵查作為。因科技偵查作為往往涉及人民基本權之干預，有明文加以規範之必要。藉由本法所規範之要件與程序，設定執法標準與界限，以確保偵查機關實施調查之合法性，並切實保障人民基本權。 二、因犯罪手法隨著科技發展而日趨縝密化與國際化，為避免犯罪調查之手段落後於科技發展之腳步，有效追訴犯罪，確保國家安全及維護社會秩序，力求人權保障與犯罪偵查之平衡，爰參酌外國立法例、我國現行相關法制及實務發展，制定科技偵查法。
第二條 本法名詞定義如下： 一、科技設備或技術：用以補充人類感官功能不足之科學設備與技術。 二、隱私空間：住宅、建築物、交通工具或其他具有隱蔽設施之地上物之內部空間，且具有隱私或秘密之合理期待者。 三、非隱私空間：前款以外之空間。 四、全球定位系統：以衛星接收儀接收衛星系統之訊息，並計算接收儀座標位置之測量技術。 五、非侵入性調查：對目標空間無物理性之侵入，調查設備或人員均在目標空間以外之處，以科技設備或技術，在該處蒐集目標空間內資訊之	就本法重要名詞之意義進行定義，以資簡潔並避免爭議，茲說明如下： 一、科技設備或技術：因人類感官功能有限，需藉由科技始能增強偵查作為之效果，但亦因此造成較高之基本權干預。故對科技設備或技術進行定義，於此範圍內，始有以本法加以規範之必要，純以人類感官功能進行之調查，非本法規範範疇。 二、隱私空間與非隱私空間：調查之場所是否涉及隱私權，為本法第二章之核心，需符合住宅、建築物、交通工具或其他具有隱蔽設施之地上物之內部空間，及具有隱私或秘密之合理期待二項要件，始構成本

調查方式。 六、通訊：利用電信設備或其他技術發送、儲存、傳輸或接收，具有隱私或秘密之合理期待之符號、文字、影像、聲音或其他信息。 七、資訊系統或設備：利用通訊軟 體、網路或其他相類之資訊科技發送、儲存、傳輸或接收通訊之系統或設備。 八、設備端通訊監察：侵入受監察人所使用之資訊系統或設備，在通訊尚未加密前之發出端或已解密後之收取端，記錄未加密或已解密之通訊內容之方式，而實施之通訊監察。	法之「隱私空間」定義，非同時符合該二項要件者，即為「非隱私空間」。例如，一般住宅及旅館房間，應屬「隱私空間」無疑；有圍牆之庭院、未遮蔽之陽台，因相鄰之較高位置之人，以目視之方式即可合法觀看之，無圍牆之庭院及房屋附連圍燒之土地，平視即可合法觀看之，均不具有隱私或秘密之合理期待；公共空間或公眾得出入之場所，例如百貨公司、公共汽車等，均無隱私或秘密之合理期待，均屬「非隱私空間」。 三、全球定位系統：因全球定位系統為目前最普遍之追蹤位置技術，且列明於本法第五條，爰加以定義之。 四、非侵入性調查：因本法第九條規範對於隱私空間實施非侵入性調查之程序，故對此調查方式進行定義。 五、通訊、資訊系統或設備及設備端通訊監察：因本法第三章係設備端通訊監察之程序規範，故需將通訊、資訊系統或設備及設備端通訊監察加以定義，以利界定該偵查作為之範圍。
第二章 監視、攝錄與追查位置	本章規範偵查機關使用監視、攝錄與追查位置之科技設備或技術進行蒐證及調查之聲請、核准、期間、事後通知等程序，以保障人民基本權。並考量不同調查方式對基本權干預程度之高低，以不同之程序密度進行層級化規範。
第三條 偵查中檢察官認有必要時得使用科技設備或技術，對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、	一、本條為本章之基礎性規範，第一項為以科技設備或技術對非隱私空間實施調查之條件及方式之基礎性通則規範與授權。

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。 除另有規定外，實施本章調查時， 若受調查對象或標的以外之人或物將無可避免地涵蓋於調查內容，亦得為之。	二、本法第二條已就非隱私空間進行定義，除非隱蔽空間之要件外，尚須符合無合理隱私期持之要件，在此前提下，不需過度限制執法機關以科技設備或技術進行調查。但為保障人權，避免偵查機關任意實施不必要之調查，仍規定須限於必要時始可進行調查，且調查之方式限於監看、與聞、測量、辨識、拍照、錄音、錄影。前述方式以外之偵查作為，自非本條之授權範圍。至於為治安或預防危害等目的進行之監看、錄影等作為，則係依警察職權行使法及其他法律規定，而非以本法作為實施依據；調取已存在之監看、與聞、測量、辨 識、拍照、錄音、錄影資料作為證據，例如調取路口監視器畫面，係依據刑事訴訟法等規範及授權為之，亦非本法之適用範圍，併此敘明。 三、以科技設備或技術實施監視、攝錄與追查位置之調查時，與案件無關之人可能無可避免地一併遭涵蓋於內，例如以錄影機拍攝特定場所之出入口，以調查被告進出之情況時，所有曾進出該處之人，將無可避免地一併遭到入鏡。但因調查處所為非隱私空間，且此情並非偵查機關所能預先查知或避免，自不應妨礙偵查之實施，爰參考德國刑事訴訟法第一百h條第三項之規定，於第二項規定，除另有規定外，偵查機關於此情況亦得實施本章之調查。
第四條 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之調查者，應予立案，自立案	一、不同之科技設備或技術對於基本權干預之高低有異，第三條係非隱私空間實施調查之基礎規範及授權

之日起，實施之累計期間不得逾三十日。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。 前項續行實施之累計期間，每次不得逾三十日。	規定，特定偵查作為若有較高之基本權干預，自應進一步規範之。 二、以科技設備或技術在非隱私空間於空中進行第三條之調查，通常係以「空拍機」、「無人機」為 之，亦得由人員於航空器上進行調查，未來若有其他技術或設備，自不待言。此種調查亦屬非隱私空間調查之一種，原依第三條規定為之即可。但較之一般非隱私空間之調查，以科技設備或技術於空中蒐集資訊之範圍較廣，且長期實施會產生較高之基本權干預效果，應在第三條之基礎規範下進行特別規範。故以實施期間作為規範空中調查方式之核心，在開始實施時，因基本權干預程度輕微，檢察事務官、司法警察官或司法警察有調查犯罪之必要者，得依第三條之規定逕行實施之，實施一段期間後，應設置額外之規範程序。故規定若實施期間超過三十日，需報請檢察官許可，始可為之，以資慎重。至於檢察官親自或指揮檢察事務官、司法警察官或司法警察在非隱私空間實施此種調查，則與本條無涉，仍依第三條規定為之。 三、為確保檢察事務官、司法警察官或司法警察遵守調查期間之規範，應先予立案始能進行調查，以利事後查考，或供檢察官對於續行調查與否進行期間之審查。另，因本條之調查性質上未必以多日不間斷之方式為之，亦可能以單次、短時間之方式實施。為保障隱私權，並避免實施期間產生爭議，第一項之實施之期間，係以累計實施之日數為

	準，不需連日持續不間斷之實施。例如，連續三日，每日均實施一小時之調查，第四日未實施，第五日再實施一小時之調查，構成累計四日之調查。 四、本條既係基於第三條之基礎規範上之特別規定，自以第三條規範之非隱私空間調查為限。若於空中對隱私空間進行調查，應屬第九條至第十二條之規定範疇，應依該等規定辦理，併此敘明。
第五條 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。 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。 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。 前項許可實施之累計期間，每次不得逾三十日，有繼續實施之必要者，至遲應於期間屆滿之五日前，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，聲請該管法院許可之。 前二項之聲請經法院駁回者，不得聲明不服。	一、長期、大量蒐集、追蹤、比對行為人之位置資訊，將使行為人個別活動之積累集合產生內在關連，私人生活圖像及行為模式得以形成。故經由追蹤位置對他人進行長期且密集之資訊監視與紀錄，可能達到干預隱私權之程度，自應設置較嚴謹之程序加以處理。 二、全球定位系統為目前最普遍之追蹤位置技術，但因科技日新月異，追蹤位置之設備或技術不限於特定一種或數種，本條係針對實施追蹤位置調查之程序，而非針對特定設備或技術進行規範。無論偵查機關以何種設備或技術實施追蹤位置，均應遵守本條之程序規定為之。故除全球定位系統外，偵查機關以其他具有追蹤位置功能之設備或技術，例如行動電話軟體定位、定位偵防車(M化車)、物聯網或任何其他設備或技術進行追蹤位置，均受本法效力所及，應遵守本法之規範。 三、追蹤位置調查對隱私權之干預程度，會因實施期間長短而有不 同，短期實施時因難以形成「圖像效

	果」，隱私權干預之程度較輕，長期實施時，干預程度較 高。從而，對於追蹤位置調查之法律架構，應以層級化之方式設計，區分短期實施與長期實施， 而為相異之處理。爰於第一項及第二項規定初次實施追蹤位置調查，得由檢察官依職權或由檢察事務官、司法警察官或司法警察聲請檢察官許可後為之。 四、檢察官或檢察事務官、司法警察官或司法警察實施追蹤位置調查二個月後，受調查人之科人生活圖像及行為模式將逐漸形成，若繼續實施，干預隱私權之程度將隨之提高，若需繼續實施，自應有更嚴謹之程序規範，以保障隱私權。爰參考刑事訴訟法第九十三條之三限制出境之規定，於第三項及第四項規定應向法院聲請許可，始可繼續實施，並規定許可後實施之期間限制，以利隱私權之保障。至於累計期間之認定方式，與第四條相同，併此敘明。 五、參考刑事訴訟法第一百二十八條之一第三項規定，於第五項明定延長實施之聲請經法院駁回者，不得聲明不服。
第六條 前條第三項及第四項之許可，應用許可書。 前項許可書應記載下列事項： 一、案由及涉犯之法條。 二、受調查人或物。但受調查人不明者得不予記載。 三、使用之科技設備或技術。 四、裝設前款科技設備或技術之方法。 五、執行機關。 六、實施期間，逾期不得實施之意旨。	一、前條追蹤位置調查之實施期間逾二個月者，已對隱私權等基本權產生較高程度之干預，爰於本條規定法院之許可需以書面為之，並列明必要記載事項，以資慎重。 二、許可書應記載受調查人，以資特定受調查之對象，但若受調查人不明時，例如檢警偵辦毒品危害防制條例案件，知悉某貨櫃藏有毒品一批，惟不知該批毒品為何人所有，

七、其他適當之指示。 核發許可書之程序，不公開之。	得例外不予記載受調查人。另，因追蹤位置之設備或技術眾多，許可書應將實施之特定設備或技術載明之，以限定執行機關之實施方式，避免濫用。又，為實施調查，可能有必要在特定場域裝置設備，例如汽車內，此時應由執行機關敘明需以此方式裝置設備或技術，經法官許可後，始可為之，避免執行機關任意選擇裝設方式。法官並得於許可書上另對執行人員為適當之指示，以因應個案需求。 三、參考刑事訴訟法第一百二十八條第四項之規定，於第三項明定核發許可書之程序，不公開之。
第七條 檢察事務官、司法警察官或司法警察有實施第五條調查之必要而情況急迫者，得逕行實施。 前項情形，應於實施後三日內報請檢察官許可。檢察官許可者，實施期間自前項實施之日起算；檢察官不許可者，應即停止實施；檢察官於報請日起逾三日未為許可與否之決定 者，視為不許可。	一、因應偵查犯罪之時效性及緊急狀況等急迫情形，例如偵辦毒品危害防制條例案件有立即向上溯源之必要，或擄人勒贖案件被害人有生命危險而有緊急營救之必要等情形，爰參考刑事訴訟法第一百三十一條規定，檢察事務官、司法警察官或司法警察可例外逕行實施追蹤位置調查，但應於三日內陳報該管檢察官審查。 二、檢察官認為應許可該調查者，實施之期間應自第一項實施之日起算，復續之程序即回歸第五條、第六條及第八條之規定辦理。若檢察官認為不應許可，或逾三日未為決定，檢察事務官、司法警察官或司法警察自應立即停止實施，爰為第一項、第二項規定。
第八條 執行機關實施第五條及第七條之調查結束時，應即敘明受調查人之姓名與年籍、實際調查期間、有無獲得調查目的之資料，陳報許可調查之檢察官。	一、為保障受調查人之隱私權，於本條規定追蹤位置調查完畢後之陳報與通知程序，但係依實施情況以及對於隱私權干預程度之不同，為層

第五條調查之累計期間逾二個月者，執行機關應於調查結束後，將前項事項報由檢察官陳報法院通知受調查人，但通知有妨害調查目的之虞或不能通知者，不在此限。 前項不通知之原因消滅後，執行機關應報由檢察官陳報法院補行通 知。原因未消滅者，應每三個月向法院補行陳報未消滅之情形。逾期未陳報者，法院應於十四日內主動通知受調查人。 第二項情形，調查結束後，執行機關逾一個月仍未為陳報者，法院應於十四日內主動通知受調查人。但不能通知者，不在此限。	級化之規範。 二、二個月內之短期追蹤位置調查， 對於隱私權之干預輕微，實施完畢後，應陳報許可調查之檢察官，由檢察官對於調查之合法性及適當性進行監督，但毋庸通知受調查人，爰為第一項之規定。若係檢察官依職權為追蹤位置調查者，自無庸為陳報程序，自不待言。 三、追蹤位置調查之期間逾二個月者，對於隱私權之干預提高，此時有使受調查人事後能知悉其曾遭追蹤位置調查之必要，故應通知受調查人。因調查期間逾二個月需經法院許可始得為之，爰於第二項規定執行機關應將該事項報由檢察官陳報法院通知受調查人，但若通知受調查人有妨害調查目的之虞或不能通知者，則准許延後通知。 四、若有延後通知之情事，執行機關應於原因未消滅時，每三個月向法院補行陳報未消滅之情形，逾期未陳報者，法院應於十四日內主動通知受調查人，以保障受調查人之權利，爰規定第三項及第四項。
第九條 檢察官、檢察事務官、司法警察官或司法警察調查最重本刑三年以上有期徒刑之犯罪，有相當理由認為隱私空間內之人或物與本案有關， 得使用科技設備或技術，自該隱私空間以外之處所，對該隱私空間內之人或物秘密實施非侵入性之監看、測 量、辨識、拍照、錄影之調查。 前項情形，應由檢察官或由檢察事務官、司法警察官報請檢察官同意後，向該管法院聲請許可。 第一項調查之累計期間，每次不得逾三十日，有相當理由認需繼續調查者，至遲應	一、隱私空間屬於具有隱私或秘密之合理期待之場所，故隱私空間之言論及談話，屬於通訊保障及監察法第三條第二項、第一項第三款之通訊。從而，對於隱私空間之言論及談話之調查，應依通訊保障及監察法所定之程序為之。因此，監看、測量、辨識、拍照、錄影，僅限於監看、測量、辨識、拍照、錄影，不涉及言論及談話之調查，合先敘明。 二、偵查機關若有對隱私空間內之活動

於期間屆滿之五日前，以書面記載具體理由，由檢察官或由檢察事務官、司法警察官報請檢察官同意後，聲請該管法院許可。 前二項之聲請經法院駁回者，不得聲明不服。	以科技設備或技術進行調查之必要，因行為人對於隱私空間具有高度合理隱私期待，自需設立更嚴謹之程序，以保障人權。 三、為維護隱私權，本法對偵查機關以科技設備或技術蒐集隱私空間之犯罪資訊，設下多重規範與限制：限定罪名、提高發動之必要門檻、限定蒐證方式、法官保留、限制實施期間。首先，僅得對於最重本刑三年以上有期徒刑之犯罪實施對隱私空間之調查。其次，限於有相當理由需使用科技設備或技術進行調查者，始可為之，提高發動門檻。再者，執行機關不得以物理性侵入隱私空間之方式進行調查，僅得從目標之隱私空間以外之處所，以非侵入性之方式進行調查，以減少隱私權干預之程度。所謂非侵入性調查，業已定義於本法第二條第五款，指對目標空間無物理性之侵入，調查設備或人員均在目標空間以外之處，以科技設備或技術，在該處蒐集目標空間內資訊之調查方式，例如以高倍數照相機，透過未經窗簾遮掩之窗戶，拍攝屋內毒品製造情況，或透過熱顯像設備，探知內部溫度等情況，以此在外部、非侵入之方式，間接探知、蒐集證據。所謂物理性侵入，係指有實質的調查設備或人員進入隱私空間之謂，例如開門入屋拍照、在屋內裝置攝影機等方式，均非本法所許。再者，採法官保留原則，由法院對於調查之開啟進行適法性審查，經法院許可後始可實施。最後，規範實施期間之限制，期滿若

	有相當理由認需繼續調查者，需再經許可始能為之。以前述多重限制條件進行嚴謹之規範與審查，保障隱私權，並昭慎重，爰規定第一項至第三項。至於累計期間之認定方式，與第四條相同，併此敘明。 四、參考刑事訴訟法第一百二十八條之一第三項規定，於第四項明定聲請經法院駁回者，不得聲明不服。 五、第三條第二項已規定，進行本章之調查時，第三人有時可能無可避免地一併遭涵蓋於內，偵查機關於此情況亦得實施調查，該規定於本條之調查自亦有適用，併此指明。
第十條 檢察官、檢察事務官、司法警察官或司法警察有相當理由認需實施前條之調查而情況急迫者，得逕行實施。 前項情形，由檢察官為之者，應於實施後三日內聲請該管法院許可；由檢察事務官、司法警察官或司法警察為之者，應於實施後三日內報請檢察官同意後聲請該管法院許可。法院許可者，實施期間自前項實施之日起算；檢察官不同意或法院不許可者， 應即停止實施。檢察官或法院於報請日或聲請日起逾三日未為同意或許可之表示或裁定者，視為不同意或不許可。	一、前條之調查亦有因應偵查犯罪之時效性及緊急狀況等急迫情形，有立即實施必要之情況，故參考刑事訴訟法第一百三十一條之規定，檢察官檢察官、檢察事務官、司法警察官或司法警察有相當理由認需實施前條之調查而情況急迫者，可例外先進行調查，但應於三日內陳報該管法院進行准駁之審查。 二、若法院認為應許可實施，期間應自實施之日起算，後續之程序即回歸第九條、第十一條及第十二條之規定辦理。若檢察官不同意或法院認為不應許可，或檢察官或法院於報請日或聲請日起逾三日未為同意或許可之表示或裁定者，執行機關應停止實施，爰規定第一項及第二項。
第十一條 前二條之許可，應用許可書。第六條第二項及第三項之規定， 於前項程序準用之。	一、以科技設備或技術對隱私空間進行調查，對隱私權等基本權有相當之干預，故於本條規定應以許可書為之，以資慎重。 二、許可書應記載之事項與審核程序不

	公開，均與第六條之情形相同，爰準用之，以資簡潔。
第十二條 執行機關實施第九條及第十條之調查結束時，應即敘明受調查人之姓名與年籍、實際調查期間、有無獲得調查目的之資料，報由檢察官陳報法院通知受調查人。但通知有妨害調查目的之虞或不能通知者，不在此限。 第八條第三項及第四項之規定， 於前項程序準用之。 第九條及第十條之調查所得資 料，除已供案件證據之用留存於該案卷或為後續偵查或調查目的有必要長期留存者外，由執行機關於調查結束後，保存五年，逾期予以銷燬。調查所得資料全部與調查目的無關者，執行機關應即報請檢察官許可後銷燬 之。	一、為保障受調查人之權利，俾利其事後能知悉其遭第九條及第十條之調查，爰於本條規定執行機關於調查結束時，應將執行結果等事項報由檢察官陳報法院通知受調查人。 二、若在個案上通知受調查人而有妨害調查目的之虞者，則准許延後通知，並準用第八條第三項及第四項，執行機關於原因未消滅時，應每三個月向法院補行陳報未消滅之情形，逾期未陳報者，法院應於十四日內主動通知受調查人，以保障受調查人之權利。 三、因第九條及第十條之調查係針對隱私空間所為，對於隱私權干預程度較高，就調查所得資料之後續保管與處理應有額外規範。爰參考個人資料保護法第十一條第三項、通訊保障及監察法第十七條第一項及第二項之規定，於第三項規定，調查所得資料除作為證據所用而留存於案卷，或因案件暫時未有具體發展，但為保留後續偵查或調查之可能，而必要長期留存等情形外，其他情況，於保存該資料五年後即應銷燬。若所得資料全部與調查目的無關者，執行機關應即報請檢察官許可後銷燬之。
第十三條 除另有規定外，檢察官為執行刑事裁判而有對應執行之人或物實施調查之必要者，得實施本章之調查。	本法係針對刑事偵查進行規範與授權，但刑事執行亦有運用科技設備或技術防止人犯逃匿、搜尋應執行之人或物等需求，且此時係基於執行刑事裁判而為之必要處置，更具有實施之基礎及正當性。爰於本條規定檢察官為執行刑事裁判，而有對應執行之人或物實施調查之

	必要者,得實施本章之調查,以符實需,相關程序應遵照第三條至第十二條之規定為之。但若其他法律另對檢察官以科技設備或技術執行刑事裁判有所規範者,應依其規範為之,例如刑事訴訟法第一百一十六條之二第一項第四款,對於停止羈押之被告實施科技設備監控,應依該法相關規定為之。
第三章 設備端通訊監察	一、目前社會已步入數位時代,利用網路以通訊軟體諸如 Line、Skype 等,進行通話、視訊、傳送檔案及文字等通訊模式盛行,已逐漸取代傳統固網電話之通訊方式。但對於通訊軟體進行通訊監察,在技術上通常無法以通訊保障及監察法所規範之方式,在傳輸過程擷取資料進行通訊監察,而必須在通訊之設備端進行訊息擷取,產生通訊保障及監察法未規範之另一基本權干預,故有另行立法之必要。 二、詳言之,設備端通訊監察所干預之基本權,除秘密通訊自由外,另構成對資訊科技基本權之獨立且重大之干預。此係因設備端通訊監察之取證技術係入侵通訊方使用之資訊科技設備而非電信線路,受干預人對於電信線路完整性之信賴並未受到干預,而係其資訊終端設備的秘密性及完整性之信賴遭到干預。學理上認為此種干預屬於「資訊科技基本權」之干預,並非通訊保障及監察法效力之範疇,故無論在規範面或技術面,通訊保障及監察法均無法因應此類新興通訊方式,故不宜由修正通訊保障及監察法之方式為之,有另立法明定之必要。

	三、從而，為因應科技進步造成之通訊模式改變，避免犯罪調查手段落後，爰在通訊保障及監察法對於通訊監察所設定之基本原則下，於本法第三章訂定對於設備端通訊監察之相關規範，以資因應科技發展、社會變遷，並保障人民秘密通訊自由及隱私權不受非法侵害。
第十四條 有事實足認被告或犯罪嫌疑人涉有通訊保障及監察法第五條第一項各款所列罪嫌，並危害國家安 全、經濟秩序或社會秩序情節重大， 而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得實施設備端通訊監察。 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。 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。 前三項之程序，準用通訊保障及監察法第五條及第六條之規定。	一、利用網路以通訊軟體或類似技術進行之通訊，多數係採取去中心化之網際協議通話技術，並將訊息切割為資料封包，不經中央伺服器，透過網路自行搜尋最近的路徑，傳送至受話方，屬於通訊參與者之間「端點對端點」之傳輸。由於傳輸過程使用加密技術，訊號自源頭端即開始編碼，透過網路傳輸到目的端受話方，再解密還原成訊息。目前在科技上往往無法比照傳統電信監察之方式，在電信服務業者線路上擷取訊息，因為只能取得傳輸過程中的加密亂碼，無法擷取到有內容意義的訊息，該亂碼通常無法即時或事後解碼，或可解碼但所費成本過高、時間過長。因此，此類通訊監察之實施，必須在通訊尚未加密前之發出端或已解密後之收取端，即記錄未加密或已解密的通訊內容，始有可能進行有效之通訊監察，為確保實施之有效性、因應科技日新月異之發展，同時兼顧實施方式之適當性，並保障秘密通訊自由、隱私權及資訊科技基本權，另參酌德國、奧地利及端士等國均立法規範此種調查，爰參考德國刑事訴訟法第一百a條，於本條規範設備端通訊監察之程序。

	二、因設備端通訊監察屬於秘密通訊自由及隱私權之干預，其發動之程序及要件，應比照通訊保障及監察法之標準，爰就其基本要件如罪名限定、情節重大、法官保留、最後手段性、緊急實施等重要事項比照該法規範之，程序細節則準用該法第五條及第六條之規定，以資簡潔。
第十五條 為避免國家安全遭受危害，而有對於通訊保障及監察法第七條第一項各款之通訊實施設備端通訊監察，以蒐集外國勢力或境外敵對勢力情報之必要者，綜理國家情報工作機關首長得核發設備端通訊監察書，實施設備端通訊監察。 前項情形，受監察人在境內設有戶籍者，設備端通訊監察書之核發，應經該機關所在地之高等法院專責法官同意。 前二項之程序，準用通訊保障及監察法第七條至第九條之規定	情報工作機關發動設備端通訊監察之程序與要件，亦應比照通訊保障及監察法之標準，爰就其基本要件比照該法規範之，程序細節則準用該法第七條至第九條之規定，以資簡潔。
第十六條 實施設備端通訊監察，得以實體接觸、網路傳輸或其他必要方法，侵入受監察人所使用之資訊系統或設備。 核准設備端通訊監察之後，實際閉始實施設備端通訊監察之前已結束之通訊，亦得取得之， 監察內容顯然與監察目的無關，且法律明定不得作為他用者，不得作成書面紀錄，並應即時銷燬相關資料。	一、設備端通訊監察之實施，係以侵入受監察人所使用之資訊系統或設備之方式為之，已於第十四條及第十五條規定之。至於侵入之方式，因科技或資訊技術發展永不停歇，不宜也無法事前列舉設限，故規定以實體接觸、網路傳輸或其他科技技術上一切適當之方式為之皆可，惟必須於聲請時載明，並經過法官之核准，爰為第一項規定。但若執行機關在取得設備端通訊監察書後，技術上能以截收後解密等方式進行監察，不需侵入系統，或以其他侵害程度較低之方法進行監察，自無不許之理。 二、設備端通訊監察允許取證之時點係以核准監察之時點為準，而非執行機關實際侵入資訊系統或設備之

	時點。從而，法院核准設備端通訊監察之後，受監察人之通訊即屬於可受監察之狀態，並非於侵入資訊系統或設備後之通訊始可監察。職是，在核准監察後執行機關尚未入侵資訊系統或設備之時段，可監察之通訊雖已結束，但仍可依其現有之狀態（例如已儲存之對話文字）進行監察。爰參考德國刑事訴訟法第一百a條第一項，於第二項明定，只要是在核准監察之期間內，受監察人所有通訊內容和狀態，即便進行時點是在資訊系統或設備被入侵之前，執行機關皆得進行監察。至於在法院核准設備端通訊監察時點之前，受干預人之資訊系統或設備所儲存的通訊，則不得進行監察，自不待言。 三、另參考通訊保障及監察法第十三條之規定，於第三項明定監察內容顯然與監察目的無關者，不得作成書面紀錄，並應即時銷燬相關資料。
第十七條 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。 一、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刪除。 二、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、因本法授權執行機關以入侵資訊系統或設備之方式進行設備端通訊監察，此實施方式必須對於資訊系統或設備進行必要之變更，且監察或取得之資訊範圍可能超過通訊之範圍，及於資訊系統或設備內之其他資料。從而，本條規範執行機關實施設備端通訊監察時，僅能存取通訊內容與狀態，不得存取其他儲存於個人資訊系統或設備之資料，以防止監察範圍超出通訊之範圍。並於監察結束後確保原先為實施監察而對於資訊系統或設備進行之改變均復原，以保障執法之純潔性及受監察人之權利。此外，也

	應該避免執行機關侵入受監察人之資訊系統或設備後，致其處於更脆弱之狀態，而淪為第三方的攻擊對象。惟，因設備端通訊監察所涉及之技術處於隨時更新、變動之狀態，執行機關所應確保者，係在現行相關科技水準下，於技術可達成之範圍內為之。入侵資訊系統或設備後，在現行相關科技水準下所必然產生之不可復 原、防止等事項，尚不在本條之技術擔保範圍內。 二、準此，爰參考德國刑事訴訟法第一百a條第五項之規定，於本條規定，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，確保僅就通訊進行監察、對受監察人之資訊系統或設備僅進行為取得資料所必要之變更、設備端通訊監察結束時，曾經進行之變更應即時回復，曾經植入之軟體即時刪除、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等技術擔保事項。
第十八條 通訊保障及監察法第十條至第十一條、第十二條、第十四條、第十五條第一項至第四項、第十六條至第二十三條、第三十二條之一之規定，於設備端通訊監察準用之。	一、有關設備端通訊監察之實施期 間、續行與停止設備端通訊監察之程序、設備端通訊監察結束復之通知、報告與監督、相關統計資料年報、監察所得資料之保 管、使用及銷燬、監察所得內容或所衍生之證據相關規範、違反相關規定所課與之民事與行政責任及立法院之監督等事項，因其性質均與通訊保障及監察法相關規範事項相同，爰準用該法相關規定，以資簡潔。 二、至於通訊保障及監察法第十五條第五項及第六項之規定，係屬該法對於電信事業之規範或通知用戶之

	規定，該法第十一條之一為調取通信紀錄及通信使用者資料之規定，性質上均與本法無涉，該法第十三條之規範事項已規定於本法第十五條。故上述規定均不在準用範圍，併此敘明。
第四章 數位證據蒐集與保全	一、由於數位與網路科技之發展，數位證據之蒐集與保全為重要之偵查方式，為明確規範數位證據蒐集與保全，保障人民權利，並避免數位證據滅失而妨害犯罪之調查、追訴與審判，於本章訂定數位證據之蒐證與保全方式及範圍。 二、刑事訴訟法已明定電磁紀錄為搜索及扣押之標的之一，本章之規定，係對於數位證據或電磁紀錄之搜索、扣押之範圍、方式及手段，或已完成數位證據之扣押後，證據之分析與提取等事項，進行補充性、澄清性規定。從而，本章相關處置係屬搜索、扣押及證物處理之一部分，本身並非獨立之強制處分。
第十九條 電磁紀錄之搜索及扣押範圍，及於可讀取該電磁紀錄且與其在空間上分離之其他儲存設備。	一、由於數位與網路科技之發展，電磁紀錄儲存方式已不限於傳統之硬碟、光碟等型態，透過網路之雲端儲存設備進行資料存取，係現今社會相當普遍之方式。但各類犯罪也因此得以與此新興科技結合，使犯罪施行得以突破地域限制。執法機關若無法及時保全存放於雲端儲存設備之相關證據，將造成難以調查或訴追犯罪之結果。 二、因雲端儲存設備僅是儲存型態之改變，對其內之電磁紀錄進行搜索、扣押所產生之基本權干預，其本質與對於傳統儲存設備及電磁紀錄之搜索、扣押並無二致。為避免雲

	端儲存設備成為犯罪偵查之漏洞，並兼顧人權之保障，爰參酌網路犯罪公約第十九條第二項及德國刑事訴訟法第一百十條第三項之規定，於本條明定有關電磁紀錄之搜索及扣押，其範圍包含雲端儲存設備或其他相類似之具延伸性質且於空間上分離之儲存設備，以杜爭議，並與時俱進地發展新型態科技偵查手段。
第二十條 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。	一、執行電磁紀錄之搜索或扣押時， 犯罪嫌疑人或第三人可能利用遠端存取功能將儲存設備內之證據迅速湮滅、變更或移轉。為避免該情況發生，爰於第一項前段明定得對於行動裝置、儲存設備、電腦或其他相類之設備及其內之電磁紀錄，進行必要之保全處分，以維持其與開始搜索或扣押時之完整性及同一性。至於實際執行方式，因個案及所涉設備不同，且科技持續發展之緣故，若由法律加以明定，恐有掛一漏萬之虞，應由執行人員視實際案件需要，在搜索或扣押之目的範圍內為之即可。 二、因執行搜索或扣押之現場、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，亦可能利用自身之科技設備進行湮滅、變更或移轉電磁紀錄，故保全之處分亦及於「人」，例如管制行動、交付行動電話或資訊設備等，爰為第一項後段之規定。 三、為確保第一項之處分得以落實， 爰於第二項明定被告、犯罪嫌疑人、第一項之設備或電磁紀錄之所有

	人、持有人、保管人或其他相關之人無正當理由拒絕或抗拒前項之保全者，得用強制力保全之，以免執行搜索或扣押前或過程中，相關電磁紀錄即遭湮滅或竄改，但不得逾必要之程度。
第二十一條 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，得以科技設備或技術為下列處置，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，於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。	一、因電磁紀錄具有許多與實體證據不同之特性，對之進行蒐集、保全、搜索或扣押時，常需利用資訊科技設備為之。例如：儲存設備可能設置帳號、密碼或其他保護措施，執行人員必須加以破解、變更或需利用系統之漏洞而入侵之，以取得必要之證據；已刪除之聯繫紀錄有必要加以復原，以明瞭共犯之間之犯意聯絡情形；為避免電磁紀錄遭到遠端修改或刪除，需將之複製加以保全。為避免偵查機關於調查時過度干預電磁紀錄，保障人民權 利，爰於本條對於調查方式加以明定並授權，以杜爭議，並避免犯罪偵查漏洞之發生。至於已合法扣押（例如合法搜索後之扣 押、依據法院核發之扣押裁定而扣押）或經犯罪嫌疑人或第三人自願性交付之行動裝置、儲存設備、電腦或其他相類之資訊設備或其內之電磁紀錄，本係合法取得之犯罪證據，自應允許偵查機關進行必要之處置，亦加以明定之。另，本條之規定，係對於實施數位證據搜索、扣押時之範圍、方式及手段，或已完成數位證據之扣押後，證據之分析與提取等事項，進行補充性、澄清性規定，該等處置係屬搜索、扣押及證物處理之一部分，本身並非獨立之強制處分，已說明如前，應予

	辨明。 二、本條之處置可能對於行動裝置、儲存設備、電腦或其他相類之資訊設備及其內之電磁紀錄進行變更、破解、復原等必要措施，導致其狀態或內容發生變動，為避免日後發生證據同一性之爭議，爰於第二項明定實施本條之處置時，應依相關科技，於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。
第五章 救濟	依本法所為之偵查作為可能構成基本權利之干預，應視程度給予受干預人（即受調查人）救濟之機會，以保障人民基本權。爰於本章規定受干預人得對法院相關之裁定提起抗告，亦得對檢察官相關之處分聲明不服。
第二十二條 受調查人就法院關於第五條第三項及第四項、第九條第二項及第三項、第十條第二項、第十四條第二項及第三項、第十五條第二項之裁定，得提起抗告。依第十八條準用通訊保障及監察法第十二條第一項之裁定，亦同。 受調查人就檢察官關於第五條第一項及第二項、第七條第二項之處分，得聲請該管法院撤銷或變更之。	依本法所為之偵查作為可能構成基本權利之干預，應視程度給予受干預人（即受調查人）救濟之機會，以保障人民基本權。爰於本條規定受干預人得對法院就追蹤位置、隱私空間調查及設備端通訊監察之裁定提起抗告，亦得對檢察官就追蹤位置之相關處分向法院聲請撤銷或變更。
第二十三條 前條第一項之程序，準用刑事訴訟法第四百零三條至第四百十九條之規定。 前條第二項之程序，準用刑事訴訟法第四百十六條之規定。	因抗告及聲明不服均有其刑事訴訟法之相關程序，爰分別加以準用之，以有所依循。
第六章 罰則	設備端通訊監察對於秘密通訊自由、隱私權、資訊科技基本權均構成重大之干預，若其實施未遵守本法之程 序，對於人民權益。至於與本法相關，但本章未規範處罰之行為態樣，仍得由刑法或刑事特別法加以處罰。

第二十四條 除第十四條第三項情形外，公務員未經法院可實施設備端通訊監察仍實施者，處五年以下有期徒刑。	一、本法係刑事程序之規範，對於設備端通訊監察訂定相關實施程序，係以國家機關及公務員為規範對象，而非一般人民。故本條之處罰主體為公務員，一般人入侵他人資訊系統或設備而取得通訊內容，應依其他法律規定，例如刑法第三百十五條之一加以處罰。 二、設備端通訊監察之實施應嚴守本法所定之程序，若未經法院許可實施設備端通訊監察，例如未向法院許可實施設備端通訊監察，或聲請後遭駁回等情況，卻仍侵入他人所使用之資訊系統或設備實施設備端通訊監察，對於秘密通訊自由、隱私權、資訊科技基本權均造成侵害，爰訂定本條處罰此類行為。至於依本法第十四條第三項之規定，因情形急迫，而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，嗣後再聲請法院核發設備端通訊監察書之情形，暨該聲請遭駁回但尚未知悉駁回結果時實施之設備端通訊監察等情況，因均係依本法所規定之程序辦理，自非本條所處罰之範疇。
第二十五條 公務員或曾任公務員之人因職務知悉或持有依本法之規定實施設備端通訊監察通訊所得應秘密之資料，而無故洩漏或交付之者，處三年以下有期徒刑。	公務員或曾任公務員之人因職務知悉或持有依本法之規定實施設備端通訊監察所得應秘密之資料，有嚴守秘密之義務，若無故洩漏或交付他人，對於秘密通訊自由、隱私權、資訊科技基本權均造成侵害，爰訂定本條處罰此類行為。
第二十六條 前二條之罪，須告訴乃論。	前二條之罪所侵害之秘密通訊自由、隱私權、資訊科技基本權均屬個人法益，爰規定該二條之罪均須告訴乃論。

第七章 附則	本章規定本法之施行日，以及本法施行前所為之空中調查、追蹤位置及隱私空間調查，於本法施行後之證據能力認定事宜。
第二十七條 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。	一、本法施行前，法律未明確授權或規範第五條、第九條所定，於實施追蹤位置之調查、實施對隱私空間非侵入性調查之程序。本法施行前所為之此類調查（例如司法警察逕行實施追蹤位置調查），相關證據是否應排除，應調和並兼顧人權之保障及真實之發現，以衡平之方式為之，避免一律排除，致使與事實相符之證據，無可例外地遭摒棄；亦避免一律允許，導致基本權過度遭到干預。 二、因此，法院應斟酌個案實施之程序是否與本法規定相符（例如司法警察實施追蹤位置調查使否先經檢察官許可）、情節、期間、目的、干預權益之種類及輕重、犯罪所生之危險或實害、如依法定程序有無發現該證據之必然性、該證據對被告訴訟上防禦不利益之程度等各種情形，以為認定證據能力有無之標準，俾能兼顧理論與實際。爰參考刑事訴訟法第一百五十八條之四之規定，其調查所得有無證據能力，由法院於個案審酌人權保障及公共利益之均衡維護後，依個案認定之。至於第三條、第四條係屬在非隱私空間實施蒐證，在本法施行前以該條之方式所為之調查，與現行法制相符，自具有證據能力，無須另為個案權衡。 三、本法第三章設備端通訊監察之規定，因屬對於秘密通訊自由、隱私

	權及資訊科技基本權之重大干預，且不在現行通訊保障及監察法授權範圍內，在本法施行前，應不得實施該偵查作為，自無須於個案審酌其證據能力。
	四、至於本法第四章之規定，係對於實施數位證據搜索、扣押時之範圍、方式及手段，或已完成數位證據扣押後，證據之分析與提取等事項，進行補充性、具體性、澄清性規定，該等處置係屬搜索、扣押及證物處理之一部分，本身並非獨立之強制處分作為，本法施行前本得實施之，並無本法施行前是否欠缺授權依據之問題，自無須適用本條規定。
第二十八條 本法自公布後六個月施行。	規定本法之施行日。