國立臺灣大學法律學院法律學系

碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

科技偵查與基本權保障—以取得行動裝置位址為例

Technological Investigation and The Protection of Fundemental Rights : Using Obtaining the Location of the Mobile Device as an Example

許欣如

Hsin-Ju Hsu

指導教授：林鈺雄博士

Advisor: Yu-Hsiung Lin, Dr. iur.

中華民國 112 年 8 月

AUG, 2023

doi:10.6342/NTU202302425

doi:10.6342/NTU202302425

謝辭

進入司法官學院受訓之後，研究所全心全意投入研究學習的日子感覺就變得十分遙遠與模糊，終於能在司法官學院學習受訓結束前的時間壓力下，把論文寫完，真的感覺如釋重負。

本論文之所以能順利完成，首先要感謝指導教授林鈺雄老師。老師除了帶給我非常深厚的法學知識，對於研究的嚴謹態度一直是我的榜樣，謝謝老師對我一直以來的督促，希望未來工作也能夠不辜負老師的期望。謝謝王士帆老師與連孟琦老師，在口試過程中給我非常多建議，也提醒我這本論文很多思考上的盲點，給我非常多啟發，真的非常感謝！

謝謝我的家人，無條件支持我完成研究所的學業（經濟上或是心理上），即便很好奇我到底要念多久也貼心的不多問，讓我不致於被壓力壓垮。謝謝我的朋友們（鐵支三重奏高雄人群組、雲端短褲乾媽、子平、怡均還有很多很多），撰寫論文期間謝謝你們給我一切幫忙，謝謝你們承載了我寫論文過程非常多負面情緒，也幫我紓壓不少。謝謝熊門的家維與學弟妹們，感謝你們幫忙了我非常多行政事項的處理。謝謝我的德文老師 Philip（雖然他看不懂），幫助我學習德文，使我不僅能夠處理德文文獻，直到現在也可以持續透過德文接觸更多不同的領域。謝謝好味小姐（雖然她也看不到），謝謝妳分享了很多研究所的心境，讓我知道我不孤單。

謝謝凌宇，謝謝你一直從大學以來都陪伴、支持著我，雖然遲了很多，但我終於跟你一樣畢業啦！未來也請你繼續多多指教！

開始受訓學習之後，才體會到能夠全心全意投入研究學習，真的是一件很幸福的事，謝謝自己一直沒有放棄，你做得很棒！

許欣如

2022.07 在橋頭地方檢察署學習司法官室

doi:10.6342/NTU202302425

論文摘要

現在台灣幾乎人人都有一支以上的手機，且隨身攜帶不會離身。在刑事追訴之領域，檢警機關自然會想利用這個特性，只要定位到手機位址，幾乎就可以找到特定人所在的位址。

過去追訴機關大多使用基地台定位方式，藉由查詢特定手機所使用之基地台，可以推算出被告可能所在之位置，然而此種方式會受限於基地台本身訊號強弱或距離等干擾，會有幾十公尺至幾百公尺之誤差，無法進行精確之定位。而隨著科技科技進步，也出現更多不同的科技偵查手段，其中 IMSI-Catcher 更是改善了基地台定位會有一定誤差的問題，利用 IMSI-Catcher 定位特定手機之誤差僅有幾公尺，大幅提升追訴機關之效率，使得各機關趨之若鶩，紛紛購入以提升偵查效能。

然而，隨著時間過去，關於 IMSI-Catcher 之法律授權基礎爭議也浮出水面，開始有判決認定使用 IMSI-Catcher 並無法律授權基礎，屬於違法之偵查手段，法務部也嘗試提出科技偵查法草案去解決此爭議，然而在立法未通過的情況下，IMSI-Catcher 的授權基礎仍然存有疑問。

本文將嘗試以「定位手機」之目的為出發，探討不同科技手段之原理以及現行法可能有的爭議，並嘗試比較我國目前與德國法制之區別，並作出建議。

關鍵詞：基地台定位、通信紀錄、M 化車、通訊保障及監察法、科技偵查法

doi:10.6342/NTU202302425

Abstract

Almost everyone in Taiwan now has one or more mobile phones, which they carry with them at all times. In the field of criminal prosecution, law enforcement agencies want to leverage this feature. As long as they can pinpoint the location of a mobile phone, they can nearly locate the specific whereabouts of an individual.

In the past, law enforcement agencies mostly relied on base station localization to estimate the possible location of a defendant by querying the base stations used by a specific mobile phone. However, this method is limited by interference from the distance to the base station, resulting in an error range of tens to hundreds of meters, making precise positioning difficult. With advancements in technology, various other technological investigative methods have emerged. Among them, the IMSI-Catcher, has improved the issue of inaccuracies in base station localization. The use of the IMSI-Catcher reduces the positioning error for specific mobile phones to just a few meters, significantly enhancing the efficiency of law enforcement agencies and prompting various organizations to acquire it to enhance investigative effectiveness.

However, as time has passed, controversies have arisen regarding the legal authorization basis for the IMSI-Catcher with court judgments determining that the use of the M vehicle lacks a legal basis and constitutes an illegal investigative method. The Ministry of Justice has attempted to address this controversy by proposing a draft law on technological investigations.

This article aims to explore different technological methods with the purpose of 'mobile phone localization.' It will examine the principles of various technologies and the potential controversies within current laws. Additionally, a comparison will be made between the legal systems in Taiwan and Germany, and recommendations will be provided.

doi:10.6342/NTU202302425

Keywords: base station localization; communication records; IMSI-Catcher; The Communication Security and Surveillance Act; Science and Technology Investigation Act

doi:10.6342/NTU202302425

目錄

doi:10.6342/NTU202302425

doi:10.6342/NTU202302425

doi:10.6342/NTU202302425

doi:10.6342/NTU202302425

doi:10.6342/NTU202302425

第一章　緒論

第一節　緣起

根據 2021 年國家通訊傳播委員會委託財團法人經濟研究院所做之調查，在台灣 16 歲以上民眾使用手機的比例高達 95.4%（包含智慧型手機與傳統手機）[1]，也就是幾乎為人手一機的狀況，故在進行犯罪追訴，追訴機關若想鎖定被告的位址或身分，並近一步發動其他例如逮捕被告、搜索扣押、解救人質等行為，偵測被告所持之行動裝置位址，或是調查被告目前使用的基地台位址是有效率且可達成目的的。

過去實務上若有取得被告犯案時位置的需求，追訴機關通常僅能依據通訊保障及監察法第 3-1、11-1 條調取被告「電信使用人使用電信服務後，電信系統所產生……位置資訊等紀錄」，調取到被告隨身攜帶行動裝置使用之基地台位址，即可推測被告事發時的位址，以供快速判斷被告的涉案可能性，可以作為不在場證明，甚至實務上有利用判定通信紀錄而避免冤案甚至平反[2]。然而調取個人基地台位址仍有不夠精準的問題，因為追訴機關可調取到的僅為被告所持之行動裝置使用基地台之位址，而非行動裝置本身之位址，且精準度會受基地台本身架設密度影響，都市區域雖然基地台架設較為密集，而較郊區的精準度更佳，但也有約 50 公尺之差距，且若被告位於 2 個基地台位置中間，手機接受之訊號可能會「漂浮」造成誤差，又若被告位於高樓層且附近無遮蔽物，也可能捕捉到較遠的基地台而產生更大的偏誤[3]。

---

[1] 財團法人台灣經濟研究院（2021），《109 年通訊市場調查結果報告》，載於：https://www.ncc.gov.tw/chinese/files/21021/5190_45724_210217_2.pdf（最後瀏覽日：2022.08.07）。

[2] 吳忻穎（2018.12.04），〈調取通信紀錄「全民買單」：犯罪偵查也需使用者付費？〉，《鳴人堂》，https://opinion.udn.com/opinion/story/12626/3517129（最後瀏覽日：2022.08.07）。

[3] 鏡傳媒（2020.04.08），〈【台灣模式發光 4】不靠 GPS 也能揪出落跑者　揭居家檢疫追蹤祕技〉，https://www.mirrormedia.mg/story/20200407inv010/?utm_source=feed_related&utm_medium=line&_trms=fc6ad9147eaf2751.1654181097754（最後瀏覽日：2021.10.02）。

doi:10.6342/NTU202302425

但隨著科技持續發展，追訴機關也開始使用更多不同之新興科技偵查方法定位被告所在地，例如直接在被告駕駛之車輛裝設 GPS 或是以 IMSI-Catcher 調查被告所持行動裝置位址。GPS 定位原理是利用 GPS 衛星不斷向地面接收器發動訊號，並利用不同衛星訊號特性以及強弱計算出實際地點，故須另外於被告所有物（例如車輛）安裝接收器，其原理與透過被告本身持有之行動裝置進行定位原理不同[4]，故非於本文討論範圍。IMSI-Catcher 與 GPS 都具有精準定位被告所在位址的功能，但 IMSI-Catcher 定位的標的是被告所持有之行動裝置位址，近年於重大矚目案件扮演極為重要的角色，2012 年李宗瑞性侵案、2015 年陳福祥北市西門町峨眉停車場槍擊案、2020 年羅姓男子拐帶少女藏於住處夾藏等，都是透過警方出動 IMSI-Catcher 鎖定被告位址以縮小搜索範圍，因為 IMSI-Catcher 對於破獲重大案件厥功至偉，各地刑事警察局趨之若鶩，紛紛購買這台「破案神器」[5]。

然而頻繁使用 IMSI-Catcher 這類新興科技偵查手法也引發各種爭議，例如臺北市議員曾於質詢時，質疑臺北市政府警察局局長購買 IMSI-Catcher 的合理性，因為當時 IMSI-Catcher 只需大隊或業管的主管機關簽名同意即可使用，且對其他市民等無關第三人個資管控不足，甚至可以對周圍的人進行監聽[6]。司法機關則首度於桃園地方法院 106 年度易字第 164 號判決處理 IMSI-Catcher 適法性的問題，判決內容宣告使用 IMSI-Catcher 調查手機位址屬於違法強制處分，取得之直接證據無證據能力，雖然二審一度推翻一審之見解，但 2022 年宣判之最高法院 110 年度台上字第 4549 號亦支持一審對於 IMSI-Catcher 證據能力之看法，這對各地追訴機關無疑是一記當頭棒喝。

[4] 衛星定位測量原理，https://gps.moi.gov.tw/sscenter/introduce/IntroducePage.aspx?Page=GPS1（最後瀏覽日 ：2021.10.02）。
[5] 自由時報（2021.02.21），〈淫魔李宗瑞、雙屍煞陳福祥... 都栽在破案神器 M 化車〉，https://news.ltn.com.tw/news/society/paper/1432430（最後瀏覽日：2021.10.02）。
[6] 台北市議會（2016），《台北市議會公報》，105 卷 6 期，頁 2914-2916，台北市議會。

doi:10.6342/NTU202302425

為了亡羊補牢，法務部曾於 2020 年提出之科技偵查法草案，雖看似可以暫時解決目前之法律爭議，卻引起軒然大波，批評者針對本條多認為缺乏法官保留，[7]最終因外界反彈過大而未持續推行[8]。

雖目前仍無相關法規立法，但不代表實務上並沒有再無此類偵查措施的需求。桃園市政府於 2021 年利用年度結餘款，贈送桃園市警察局一台要價 3000 萬元的 IMSI-Catcher，聲稱將提升偵辦重大刑案及特殊案件或緊急救難案件的能力[9]。偵查機關如高檢署於 2022 年科技偵查中心揭牌上路後，也因拘提人犯、執行發監、偵辦共諜案等機敏案件需要，開始對檢事官進行 IMSI-Catcher 操作培訓，並不排除未來編列預算購買 IMSI-Catcher 提升偵查量能[10]。實務上也持續不斷有對於新興科技偵查方法立法的呼籲，呼籲立法機關積極立法，以跟上現今層出不窮利用網路之犯罪[11]。

第二節　問題提出

從上述發展可知，實務上一直有定位被告行動裝置位址以澄清案件之需求，雖目前有通保法第 3-1、11-1 條作為調取通信紀錄的法源依據，但現行調取通信紀錄的規定是否已經沒有違憲之疑慮而能夠滿足相關保障人民的程序需求？而隨著科技日新月異也出現不同的科技方法協助追訴機關，卻隨著科技偵查法的撤案，這些新興科技偵查方法仍維持「妾身未明」的地位，然任何干預人民基本權的強制處分，皆應有事前的明確法律依據供人民遵循與預見，究竟

---

[7] 風傳媒（2020.10.08），〈《科技偵查法》有侵害隱私疑慮？前監委：草案多處不符合法官保留原則〉，https://www.storm.mg/article/3093964?page=2（最後瀏覽日：2021.10.02）；沃草（2020.10.08），〈「科技偵查法」GPS、空拍偵蒐規範寬鬆惹議　法界：偵辦效率不應犧牲隱私〉，https://musou.watchout.tw/read/dKvnOIjZJnJOkpftq8m9（最後瀏覽日：2021.10.02）。

[8] 風傳媒（2020.10.12），〈科技偵查法撤案　民進黨團：法務部無規劃再提出時程表〉，https://www.storm.mg/article/3104587（最後瀏覽日：2021.10.02）。

[9] 自由時報（2021.02.02），〈桃警分局長交接 市府將購 M 化偵防車〉，https://news.ltn.com.tw/news/Taoyuan/paper/1429467（最後瀏覽日：2021.10.02）。

[10] 中時新聞網（2022.02.08），〈辦機敏案件防洩密 高檢署擬建「M 化車」團隊〉，https://www.chinatimes.com/realtimenews/20220208001131-260402?chdtv（最後瀏覽日：2022.03.04）。

[11] 自由時報（2021.10.26），〈拒協助司法調查 WeChat 淪共諜組織避風港〉，https://news.ltn.com.tw/news/politics/paper/1480727（最後瀏覽日：2021.12.02）；天下雜誌（2021.10.25），〈他偵破網紅小玉案　22 年資深警察：網路犯罪，能不能像搶銀行判重刑？〉，https://www.cw.com.tw/article/5118659（最後瀏覽日：2021.12.02）。

doi:10.6342/NTU202302425

以新型科技手段例如 IMSI-Catcher 取得行動裝置位址的相關技術手段中，侵害了何種基本權？我國現行之立法是否為可能的授權基礎？本文將嘗試盤點現行追訴機關定位被告行動裝置位址的不同方式，並對這些疑問做出解答。

第三節　研究範圍與研究方法

隨著新興隱密科技偵查方法的應用（IMSI-Catcher、來源端通訊監察、GPS、無人機等），我國亦出現許多文獻探討其與基本權之關聯與是否具有授權基礎等問題，然本文將以「取得手機定位」之目的為出發點，延伸不同科技方法，從發展已久之通信紀錄調取談起，再探討近年多被追訴機關所使用之 IMSI-Catcher 技術。

因我國立法多繼受德國法，且德國早在 1928 年即有調取通信紀錄之授權規範，更於 2002 年新增 IMSI-Catcher 之授權基礎，隨後實務上又透過判決解釋將靜默簡訊納入授權範圍，學說上也累積許多豐富之討論，故本文將借鑑德國刑事訴訟法之相關內容，輔以聯邦憲法法院與歐洲人權法院等指標判決，先嘗試梳理德國法對於取得行動裝置定位的規範系統，再回到我國，檢視現行使用之科技方法中各個方法侵害之基本權、現行法律依據與程序保障是否充足，以及若無法源依據，未來立法將如何平衡追訴犯罪利益與人民權利保障。

第四節　本文架構

本文將從比較法出發，先分別於第二章與第三章介紹德國刑事訴訟法第 100g 條調取通信紀錄之規定與第 100i 條對行動通訊設備之科技偵查，簡介規範本身立法背景、內容以及其延伸程序保障相關規定，並補充德國相關之實務判決與學說分析。藉由這些背景理解回到我國，先於第四章討論我國已有明文規定之通保法有關調取通信紀錄的部分，先爬梳現行規定再為檢視是否仍有不足之處，再於第五章討論我國使用 IMSI-Catcher 之現況，包括現行實務判決分析以及基本權分析，以及評析 2020 年法務部提出之科技偵查法草案，檢視是否符

doi:10.6342/NTU202302425

合憲法上之要求與做出立法相關結論，最後於第六章為我國目前取得行動裝置之相關規定現況為建議與結論。

doi:10.6342/NTU202302425

第二章　德國刑事訴訟法調取通信紀錄規定

第一節　德國刑事訴訟法第 100g 條規範沿革

第一項　獲取行動裝置位址資訊原理

目前行動裝置通訊是採蜂巢式網路的原理，蜂巢式網路是由多個六角形之細胞（cell）所構成，三個蜂巢六角形之重疊焦點即為基地台（base tower），各基地台又以三個方向之指向性天線組成，每 120 度為一方向角，各自供給三個方向之細胞作為通訊使用。行動裝置開機之後會處於待機模式，為了進行通訊，行動裝置會自動逐一搜尋臨近訊號最強基地台，搜尋到合適之基地台後，行動裝置會傳送裝置本身相關識別碼以及所屬電信給予基地台，這個過程即所謂註冊（registration）[1]。當行動裝置開機、進行通訊時（不論是通話或發送簡訊）、個人位置變動、受到地形以及天氣等因素導致基地台訊號減弱，甚至是定期經一段時間後，行動裝置會再重複註冊之過程，然而重複註冊過程非屬行動裝置持有者可以控制或改變[2]。基地台彼此之間訊號覆蓋範圍會重疊，且行動裝置為了可以於持有者移動中仍保持穩定通訊，會與多個基地台進行註冊[3]，故通常只要行動裝置與三個基地台連線之後，即可利用各基地台為圓心，以基地台訊號強弱所可延伸之範圍為半徑畫圓以及指向性天線方向計算，其重疊焦點即為手機之大概位置，當基地台分佈越密集，所獲得之資訊即更為精確（即所謂三角定位法）[4]。

第二項　涉及之基本權

---

[1] 何明洲（2014），《犯罪偵查原理與實務》，頁 132，中央警察大學出版社（轉引自：黃政龍（2016），《新型態科技偵查作為之法規範研究》， 頁 26-28，中央警察大學警察政策研究所博士論文）。
[2] 廖訓誠、陳芳振、 顏宥安（2016.10），《犯罪偵查技術》，頁 201-202，陳芳振出版。
[3] 詹明華、陳弘斌、宋奕賢（2016.03），〈定位技術在犯罪偵查上之應用〉，《刑事科學》，80 期，頁 5。
[4] 林鈺雄（2021.02），〈科技偵查概論（上）──干預屬性及授權基礎〉，《月旦法學教室》，220 期，頁 53。

doi:10.6342/NTU202302425

秘密通訊自由保護範圍不僅包括通信內容，尚包括通信的詳細情況，意即在哪些人或設備之間是否發生過或試圖進行過通訊、何時發生通訊與通訊頻率等，目的是保護人民即便透過電信系統進行的遠距離之意見交流，交流的形式和內容上亦不會被第三人窺知或竄改，故追訴機關根據德國刑事訴訟法第 100g 條調取通信紀錄之行為干預基本法第 10 條保障之秘密通訊自由[5]。

第三項　立法沿革

德國早在 1928 年就在電信設備法第 12 條 （Fernmeldeanlagengesetz, FAG）規定調取通信紀錄之程序與要件：於調查追訴犯罪時，當通訊已傳送予被告，或是有事實足認通訊係由被告發送或是為被告發送，且調取對犯罪追訴具有重要性，法官或是（急迫情況下）檢察官可要求調取通信紀錄等通訊相關資訊，然而該條文有過於概括而無法符合明確性的問題，無法符合干預資訊自決權之需求，故經過修法討論之後，電信設施法調取通信紀錄規定於 2001 年停止適用，立法者將調取通信紀錄之規定移至德國刑事訴訟法第 100g 條與第 100h 條。隨後，2008 年歐盟頒布 2006/24/EG 指令（下稱 2006 指令），為符合 2006 指令，立法者分別於電信法引入電信業者強制儲存通信紀錄之義務與修訂刑事訴訟法調取規定，規定電信事業需保存一定時間內的通信紀錄，是為確保相關機關能於一定期限內取得特定資料，但後又歷經德國聯邦憲法法院判決其違反基本法與歐盟法院宣判指令無效，故德國又於 2015 年 12 月 18 日重新修定電信法與刑事訴訟法之規定[6]，現行德國刑事訴訟法第 100g 條主要即來自此次重新引入通信紀錄儲存義務規定，本文以下將先從 2008 年之修法引入歐盟 2006 指令為回顧討論。

第一款　歐盟頒布 2006/24/EG 指令後與 BverfG 125, 260

回顧歐盟關於個人資料保護之歷史，於 1995 年歐盟首度頒布個人資料保護指令（95/46/EC，下稱 1995 指令），課與各國需於資料處理過程保障人民基本權利，

[5] Hauck, in: LR-StPO, Bd. 3/1, 27. Aufl., 2019, § 100g Rn. 9-10.
[6] Hauck, (Fn. 5), § 100g Rn. 1.；中文文獻參：Mark A. Zöller（著），王士帆（譯）（2016.04），〈處在德國法與歐洲法緊張氛圍下的通信紀錄調取〉，《月旦法學雜誌》，252 期，頁 224-227。

doi:10.6342/NTU202302425

特別是隱私權，然 1995 指令之目的係為了促進歐盟內部市場整合，指令內已明文指出不適用於刑事法領域；2002 年歐盟再頒布歐盟電子通訊隱私指令（2002/58/EC，下稱 2002 指令），規定電信事業若出於特定目的（例如計算費率時）才得以儲存通訊用戶之通信紀錄，目的達成後必須將通信紀錄匿名化或刪除，於特定情況例如追訴犯罪、維護國家安全時才可限制秘密通信自由而保留個人通信紀錄，但 2002 指令並無規定電信事業有強制儲存通信紀錄之義務。德國據 2002 指令修正了電信法第 95（用戶主資料）、96（出於商業目的儲存通信紀錄）條等規定（現移至電信與電子媒體資料與隱私保護法第 9 條與第 12 條）[7]。

然而，2002 指令使跨國經營之電信事業面臨因各國通信紀錄規定迥然不同而無法妥適處理之困難，且又相繼發生美國 911 恐攻與在馬德里、倫敦的炸彈攻擊，使歐盟各國意識到利用電子通信紀錄作為打擊犯罪之重要手段，歐盟對隱私保障的態度轉變，故於 2006 年 3 月 15 日修正 2002 指令而公布強制儲存通信紀錄指令（2006/24/EC，下稱 2006 指令），細究其內容，包括：指示 2006 指令之目的係為偵查、追訴嚴重犯罪之用（第 1 條）；電信事業有義務儲存第 5 項所涵蓋之通信紀錄並於有必要時提供給國家（第 3 條）；儲存範圍包含得辨識通訊雙方之身分與使用之終端設備資料、通訊時間以及時長、通訊類型、得以特定通訊時位址的資訊等，可以得知該用戶顯示了用戶是否、與誰進行了交流，該交流持續時間以及交流頻率等，透過大量紀錄觀察，可以推測出個人的私人生活，包含日常生活習慣、永久或臨時居住地、每天的活動位置、其社會關係以及身處的社會環境等，然儲存範圍不含通訊內容（第 5 條）；儲存期最低須保存 6 個月，最長可保存 2 年，提供予相關機關調取以作偵查、追訴嚴重犯罪之用（第 6 條）；成員國需制定有關調取通信紀錄之實體與程序要件，調取時須符合歐盟人權公約相關解釋並符合比例原則，成員國亦須確保儲存機關能符合保存資料安全標準（第 4、7 條）。

[7] 唐欣悅（2018），《私人通信紀錄強制供公益目的使用之合憲性研究》，頁 56-58，臺灣大學法律學研究所碩士論文。

doi:10.6342/NTU202302425

德國依據 2006 指令，於 2008 年修正電信法第 113a、113b 條與刑事訴訟法第 100g 條規定，然而電信法強制儲存通信紀錄之規定引發德國國內質疑違反基本法的聲浪，多組團體提起憲法訴訟，有高達 34000 多份聲請，故法院於 2008 年先為暫時處分，命暫停實施電信法第 113b 條第 1 項允許為追訴犯罪而處理通信紀錄之規定，最後於 2010 年 3 月 2 日聯邦憲法法院判決宣告電信法第 113a、113b 條以及刑事訴訟法第 100g 第 1 項第 1 句違反基本法第 10 條第 1 項而無效，然而聯邦憲法法院並未完全否定儲存通信紀錄相關規定，電信事業根據電信法第 96 條以下基於商業目的而收集通信紀錄之規定仍為有效。聯邦憲法法院認為，電信法第 113a、113b 條相較於第 96 條之規定，電信事業不僅非基於商業目的儲存通信紀錄，客戶亦難以影響電信事業之決策，故當國家欲課與電信事業強制儲存通信紀錄之義務（基於追訴犯罪目的），應受到較嚴格之審視[8]。

第一目　裁判背景

BverfG 125, 260[9]之訴訟標的為電信法第 113a、113b 條與刑事訴訟法第 100g 條，於 2007 年 12 月 21 日為轉換歐洲共同體 2006/24/EG 指令之立法（Gesetes zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007）修訂，並於 2008 年 1 月 1 日生效。

電信法第 113a 條規定大眾電信事業（包含一般固網電話、網際網路）有義務儲存通信紀錄，儲存範圍主要包含通訊雙方的號碼與裝置識別碼、通訊時間、通訊時連接的基地台識別碼等，排除對於通訊內容之儲存，儲存期間為 6 個月，超出期限須於 1 個月內刪除，就資料安全需為必要之注意，並僅允許經授權之人員使用資料，相較於電信法第 96 條僅允許電信事業為了計費或排除通訊障礙等列舉目的之必要範圍，才可以儲存通信紀錄，第 113a 條並無此類目的限制。

[8] 蔡宗珍（2018.02），〈電信相關資料之存取與利用的基本權關連性（上）－德國聯邦憲法法院 BVerfGE 125, 260 與 BVerfGE 130, 151 判決評析〉，《月旦法學雜誌》，274 期，頁 107-119。
[9] BVerfG, Urt. v. 02. 03. 2010- 1 BvR 256/08, 1BvR 586/08, 1BvR 263/08= BVerfGE 125, 260.

doi:10.6342/NTU202302425

電信法第 113b 條主要規定依據前條儲存之資料允許使用目的，包含傳輸予其他機關以執行刑事訴追、對於公共安全之危險防範、完成國家情報任務等，而這些調取通信紀錄之要件，應透過個別領域之專法訂定之，電信事業須於符合以上之目的時，傳輸資料於有關機關。

刑事訴訟法第 100g 條則是有關資料使用調取之規定，與上述電信法規定分屬資料處理之不同階段[10]，規定有事實懷疑「以正犯、共犯、未遂犯或預備犯之地位犯個案中犯罪情節重大之犯罪，尤其是第 100a 條第 2 項所列犯罪」或「經由電信通訊實施犯罪」，並且為查清案情或調查被告所在地有必要時，可以於當事人不知情的情況下調取電信法第 96 條或第 113a 條儲存的通信紀錄。管轄之部分，除非有急迫危險，否則僅能由法官命令之。因其為秘密偵查措施，所以允許事後通知，若檢察機關欲為延期通知，需經法院同意。憲法訴願人主張系爭規定侵害秘密通訊自由且不符合比例原則，應宣告其無效[11]。

第二目　裁判內容

第一　干預基本權

基本法第 10 條秘密通訊自由保障人民透過電信等非實體資訊交換過程，保障範圍包括通訊內容以及通訊緊密情狀（哪些人是否、何時、多頻繁進行或嘗試進行通訊之資訊），不僅防止國家任意獲悉上述資訊，也保護取得上述資訊之後的使用處理過程，例如儲存記錄、與既有資料比對或傳輸予其他機關。於通訊紀錄（關係）之保障，應適用較基本法第 2 條第 1 項連結第 1 條第 1 項所導出之資訊自決權（一般人格權）更具體之第 10 條秘密通訊自由（特殊人格權），但過去聯邦憲法法院就資訊自決權所發展出之相關見解，亦適用於秘密通訊自由之保障[12]。

[10] 此即為德國法所稱之「雙門模式」（Doppeltürmodell）。 引自：Dalby, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 113.
[11] BVerfGE 125, 260 (Rn. 1-79).
[12] BVerfGE 125, 260 (Rn. 189-190).

doi:10.6342/NTU202302425

電信法第 113a 條規定提供電信服務者有義務儲存電信之間是否、何時、多頻繁進行或嘗試進行通訊之資訊（即通訊緊密情狀），雖非國家直接儲存，然電信服務業者並無行為空間（Handlungsspielraum），若國家向電信事業調取資料，電信事業須立即提供，故可視電信服務業者為國家履行任務之輔助人（Hilfspersonen），可認電信事業儲存資料之行為，就是國家對祕密通訊自由之直接干預；電信法第 113b 條前段規定電信事業在符合一定目的時，且具備其他專法的調取要件，可將第 113a 條強制儲存通信紀錄傳輸於其他機關，雖非直接規定資訊之使用處理規定，但其係資訊應為何種目的而允許使用之基礎規範，免除電信事業之保密義務，且該傳輸使用資料是基於法律規定所允許，調取時亦需來自國家依據個案所發布之命令授權，可認屬於國家之干預，亦具有干預秘密通訊自由性質；刑事訴訟法第 100g 條則是在符合要件下，允許追訴機關調取電信法第 113a 條之資訊並使用，亦構成祕密通訊自由之干預[13]。

第二　比例原則

德國聯邦憲法法院認為為了達成刑事追訴、防禦危險等目的，而預先且不具理由（anlasslos）儲存通信紀錄，並非自始違反基本法第 10 條之保障，亦非自始就違反基本法，基本法僅禁止出於不確定或尚未確定目的之預先儲存行為。然而，此類儲存行為應限於例外情形，須審查系爭規範的立法理由以及規範本身是否符合特別嚴格的要求，亦即系爭規範需達成正當目的，且符合比例原則[14]。

系爭規定等是為達成追訴犯罪、危險預防或情報蒐集的目的，屬於正當之目的；比例原則部分：此規範雖未必可以完全達到重建通訊的程度，被告亦有可能透過外國電信事業服務、網咖規避儲存義務，然判斷規範是否具有適當性不須以所有個案皆可達成目的為條件，因搜集所有公民之通信紀錄對於該目的之實現已有所助益，故不影響該規範對於達成目的適當性，可以協助釐清日漸增加重要性的電信相關

[13] BVerfGE 125, 260 (Rn. 193-196).
[14] BVerfGE 125, 260 (Rn. 206).

doi:10.6342/NTU202302425

犯罪；侵害較小的措施如快速凍結程序（Quick-Freezing Verfahren），因須有具體之犯罪嫌疑才開啟儲存通信紀錄，不如系爭規定可連續儲存通信紀錄，可以掌握確定具體嫌疑形成以前之資料，故快速冰存程序並無法達成與全面預先儲存相同的效果[15]。

然而就狹義比例原則部分，聯邦憲法法院就此初步認定：電信法第 113a 條非自始即不符合狹義比例原則。儲存六個月的通信紀錄，屬於一種特別嚴重之干預，使國家具有可重建大部分通訊關係之能力，其負面效應來自於大量的紀錄可能具有強大的資訊解讀力（Aussagekraft），雖儲存範圍不包含通訊內容，但在大量資料解讀下足以重構一個人的移動圖像、生活軌跡、個人偏好或是或是組織的決策形成過程，以描繪出個人人格圖像，使個人受到偵查之風險增加，甚至有可能有資料濫用導致更大侵害之可能，而電信業者可能基於各自的企業資源，且可能受限於組織結構問題，難以承擔立法者所要求之資料安全標準，使人民面臨被監視的威脅感，足以影響其他基本權利之行使，然而這些負面效應並非即可推論強制儲存行為違反比例原則，只要符合一定要求即可[16]。

檢視電信法第 113a 條，已部分滿足基本法上要求，範圍包括：通信紀錄非直接由國家儲存，是由委由分散的私人電信事業協助儲存，國家不能直接取得通信紀錄，仍需要先經過事先訂立且要件明確的法律規定才可調取，且調取限於必要範圍內，避免使用於不確定或尚不明確之目的[17]；儲存的通信紀錄不涉及通訊內容，非屬個人之核心領域，並無侵害人性尊嚴以及基本權重要部分之疑，雖儲存期長導致資訊解讀力高，然而立法者亦預先設定一定的儲存期限，仍認為是符合比例原則的，人民可相信儲存期限屆至刪除之後無人可再重建通訊過程，且只有極度例外的情形下才會為其他機關傳輸使用[18]；儲存通信紀錄不是為了完全掌握所有人民的通訊行動，毋寧是對於現今犯罪的反制手段，因為現在犯罪多利用網路通訊進行，造成

[15] BVerfGE 125, 260 (Rn. 207-208).
[16] BVerfGE 125, 260 (Rn. 209-212).
[17] BVerfGE 125, 260 (Rn. 213-214).
[18] BVerfGE 125, 260 (Rn. 215).

doi:10.6342/NTU202302425

追訴犯罪之困難，偵查工具亦需要與時俱進[19]。然而，強制儲存通信紀錄應保持為例外，立法者有義務採取發展更多不同儲存方式[20]。

第三　強制儲存通信紀錄之基本法要求

基於上述強制儲存通信紀錄造成特別嚴重之干預，強制儲存通信紀錄需要特別針對資料安全、資料使用範圍的、透明度、法律保障等規定。

壹　資料安全

因為資料是由私人電信事業進行處理，其可能受限於經濟條件與成本壓力，且大量資料帶來之解讀力可能引發資料濫用之危險，故不僅是資料儲存，資料傳送過程均須符合特別的資訊安全要求，也需持續採納科技新觀點，立法者應建立明確之資料安全標準以供遵循，而資料安全的監督可委由監督機關執行並建立公平處罰方式[21]。

貳　資料使用

因為大量的無理由儲存之通信紀錄會增強資料的資訊解讀力，不能逕認干預程度較監聽通訊內容還小，且不同於依據電信法第 96 條所儲存之通信紀錄，後者是因為與人民之契約關係而儲存（部分儲存可受客戶本身影響），資料使用需要依據各自專業領域建立明確規範，必須為了保護特別高層級的法益才允許為之[22]。

在追訴犯罪的領域，立法者對於允許哪些罪名可調取通信紀錄有判斷空間，然需要事前建立抽象客觀範圍目錄犯罪（不論是參考既有目錄犯罪或是建立新犯罪目錄），不可如刑事訴訟法第 100g 條泛稱「犯罪情節重大之犯罪」等語，且調取記錄與案件重大性成適當比例[23]。

使用通信紀錄須限制於特定目的，當專責機關取得通信紀錄後，必須立刻不拖延的處理、評估該資料，當處理特定目的已不存在時，通信紀錄即應刪除並製成紀

[19] BVerfGE 125, 260 (Rn. 216).
[20] BVerfGE 125, 260 (Rn. 218).
[21] BVerfGE 125, 260 (Rn. 220-225).
[22] BVerfGE 125, 260 (Rn. 226-227).
[23] BVerfGE 125, 260 (Rn. 228-229; Rn. 235).

doi:10.6342/NTU202302425

錄，另外雖允許基於目的變更而傳輸紀錄予其他機關，然變更目的亦需要法律授權，且立法者須另就標記義務訂立規定。調取時尚需注意有特殊信賴關係的個人或團體（例如教會等），此類通訊通常是為了達成心理或社會緊急狀況諮詢，因這些組織與僱員具有保密性義務，應禁止調取傳輸相關通信紀錄[24]。

參　程序要求

首先是公開透明之要求：有鑒於強制儲存個人通信紀錄，使個人有被監視的感覺，無法得知國家掌握多少個人資訊，故通信紀錄調取需要盡可能公開為之，況且若秘密進行，當事人更無法得知以為措施所侵害並為救濟。在刑事程序亦有部分強制處分係於當事人知情的情形執行（例如搜索），除非告知當事人會導致原先的目的無法達成，否則均須告知措施當事人，並至少需要於調取後為事後告知，若有必要不為通知，須經過法官裁定，並應限於例外之情形，然非處分所直接針對而偶然受處分所影響之人，如果告知會造成更嚴重的干預且告知對其顯無利益，可以省略通知並不須經法院同意[25]。

再者是對於有效的法律救濟與制裁體系之要求：因為此偵查手段可能是當事人無法感知、秘密進行的，故原則上需要具有獨立性與受法律拘束的法官決定之，法官須審查聲請是否符合法定要件，並且需於命令中闡述允許的理由，並明確限定調取資料範圍，使電信事業無需自行實質審查而得以執行。因當事人通常無法事前針對調取通信紀錄為爭執，故需要賦予其事後救濟的機會，並且若有資料濫用或侵害之情形，為貫徹國家應保護個人人權，免於受第三人侵害，需要建構合理的制裁體系保護人民的基本權利[26]。

第四　系爭規範違反基本法部分

電信法第 113a 條雖有助於達成打擊嚴重犯罪之目的，非完全違反基本法，然而依據前揭聯邦憲法法院有關合憲性的程序要求，系爭規範缺乏資料安全保護的

[24] BVerfGE 125, 260 (Rn. 238).
[25] BVerfGE 125, 260 (Rn. 239-245).
[26] BVerfGE 125, 260 (Rn. 246-253).

doi:10.6342/NTU202302425

法律設計，資料使用規定亦不符合基本法要求，更無相關監督單位，缺乏有效的制裁體系避免資料濫用，故抵觸基本法第 10 條第 1 項的保障[27]。

電信法第 113b 條第 1 項連結刑事訴訟法第 100g 條調取強制儲存通信紀錄亦抵觸基本法第 10 條第 1 項之保障，因刑事訴訟法第 100g 條之規定並無具體訂立可調取通信紀錄之犯罪類型，而僅抽象稱有情節重大犯罪或利用電信犯罪為前提，後者甚至可以不論犯罪之嚴重程度，大幅擴大可供調取的案件範圍，然而調取強制儲存之通信紀錄應限於例外的狀況，如此立法已超出當初 2006 指令所設定之打擊嚴重犯罪如組織犯罪的目標，雖然無理由儲存所有通信紀錄，對犯罪訴追極有助益，但並非所有有效的偵查手段均應逕認符合基本法，仍須符合一定要求，即調取無故強制儲存通信紀錄應保持例外而有具體的犯罪目錄[28]。

在程序要求部分：第 100g 條條文稱「得於嫌疑人不知情的情況下得調取」，亦不符合憲法上之要求，應僅有在法律有詳細規定、個案具有優越（überwiegenden）利益且經法官同意，才可「秘密」調取根據電信法第 113b 條所儲存之紀錄；再者，第 101 條有關通知受監察人的部分，僅有部分情形下推遲通知須經法官同意，此部分亦不符合基本法要求；最後，追訴機關依據第 100g 條調取通信紀錄須經法官保留，但不是法官直接授權追訴機關取得資料，而是課與電信事業義務傳輸資料，就該命令之形式，現行法並未清楚規定與有關法官裁定的說理義務內容，然而法律應明確規定法院應於個案命令中以符合比例原則之方式明確調取範圍，供電信事業執行。[29]

第二款　歐盟法院宣判 2006/24/EG 指令無效[30]

2014 年 4 月 8 日歐盟法院 C-293/12, C-594/12 判決亦宣告強制儲存通信紀錄之 2006 指令干涉歐盟基本憲章第 7（私人生活權利）、8 條（個人數據保護），雖該指令之目標是為了打擊嚴重犯罪與公共安全，且該指令是適合達到此目的，然而

[27] BVerfGE 125, 260 (Rn. 269-276).
[28] BVerfGE 125, 260 (Rn. 276-279).
[29] BVerfGE 125, 260 (Rn. 280-284).
[30] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014.

doi:10.6342/NTU202302425

指令並不符合比例原則，未賦予資料主體足夠避免濫用的保障，且儲存範圍並無任何區別或例外，違反狹義比例原則，故該指令無效[31]。

第一目　裁判背景

本案由兩案合併而來，分別為愛爾蘭高等法院提出，因國內之公民團體與行政機關就該歐盟指令所制定之內國法有適用上爭議；以及奧地利憲法法院所提出，就指令所轉化之電信法而有多組憲法訴訟，兩案所涉及之爭議皆以 2006 指令之有效性為先決條件，故裁定停止訴訟，向歐洲法院聲請為先決裁判（Vorabentscheidung）。

第二目　裁判內容

第一　干預基本權

歐盟法院認為：2006 指令內容涉及歐盟基本權利憲章第 7 條（保護私人生活）和第 8 條（個人資訊之保護）的權利，甚至有可能影響到憲章第 11 條所保障之言論自由[32]。2006 指令允許強制儲存通信紀錄與調取已偏離了 1995 指令與 2002 指令所揭示之保障，即通信紀錄原則上應保持機密性，即便允許因為計費等目的保留，亦應於達成目的之後刪除或匿名化資料。

判斷 2006 指令是否干涉第 7 條保護私人生活的權利，不需要判斷該私人生活的訊息是否具有敏感性質，也不需判斷個人是否因為干涉而受到不利影響，2006 指令命電信事業有義務「儲存」通信紀錄並保留一段時間本身，即構成對歐盟基本權利憲章第 7 條的干預，而國家依據 2006 指令第 4、8 條立法規定如何「調取」強制儲存之通信紀錄，亦構成對歐盟基本權利憲章第 7 條額外干預。同時 2006 指令亦干預了第 8 條個人資訊保護的權利，這種侵害不但特別嚴重（particularly serious），影響範圍亦廣（wide-ranging），在未通知用戶的情況下保留通信紀錄並隨後利用的事實，很可能使當事人感到其私人生活受到持續監視[33]。

---

[31] Bär, in: BeckOK-StPO, 39. Ed., 2021, § 100g Rn. 2.
[32] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 26-29).
[33] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 33-40).

doi:10.6342/NTU202302425

第二　比例原則

歐盟基本權利憲章第 52 條規定，對歐盟基本權利憲章所承認權利進行任何限制必須由法律規定，並尊重這些權利的本質，亦需遵守比例原則，意指只有當限制是必要的，並目的為維護共同利益或保護他人權利，才能對基本權利做出限制。指令雖然干預了第 7 條與第 8 條的權利，然並無限制其重要內容（Wesensgehalt），前者係因為 2006 指令第 1 條明文禁止電信事業儲存通訊內容，後者係因為 2006 指令第 7 條為有關於資訊保護與資訊安全的規定，即成員國需要採取適當技術與組織措施，以保護數據免遭意外或非法破壞或更改[34]。

就目的正當性而言：雖然該指令係出自於協調成員國之間保留通信紀錄規定統一性的動機，但從其指令第 1 條可以看出，該指令的實質性目標是確保調查、偵查和起訴嚴重犯罪之目的，故可認指令的實質性目標是促進打擊嚴重犯罪，從而最終達到促進公共安全的理念，因根據憲章第 6 條個人享有安全之權利，故歐盟法院亦肯認追訴嚴重犯罪為歐盟為公共利益服務的目標，而隨著現今通訊技術之發展，儲存通信紀錄有助於達成打擊嚴重犯罪（特別是組織犯罪）之目的[35]。

在審查是否符合比例原則時，立法機構的形成空間（Gestaltungsspielraum）可能受涉及憲章所保障的基本權利性質、干預的性質與嚴重性、干預目的等限制。本案因涉及保護個人資料與尊重私人生活重要的基本權利，以及 2006 指令對個人基本權利干預甚深，立法機構的形成空間有限，本案須為嚴格審查之審查基準[36]。

因現今電子通訊使用頻率增加，通信紀錄會是打擊特別是組織犯罪的一大利器，故電信事業保留指令指定的通信紀錄，以便國家追訴機關調取，是適合達成上述目標的方法。然而，打擊犯罪有效性目的本身不能證成保留大量人民的通信紀錄的正當性，根據過去的判決，欲限制憲章第 7 條的權利，在任何情況下都要求保護個人資料安全及將其限制在絕對必要的範圍內，而憲章第 8 條規定之權利

[34] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 38).
[35] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 41-44).
[36] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 45-48).

doi:10.6342/NTU202302425

又對保護尊重私人生活的權利具有特別的重要性[37]，因此，立法必須對干預措施的範圍和應用作出明確的規定，並確定最低保障要求，使其個人資料得到有效保護，防止濫用風險和任何未經授權的調取或使用，特別是 2006 指令的通信紀錄都是自動儲存處理的，存在未經授權的調取的風險，更須採取保障措施[38]。

然而，儲存範圍之部分，2006 指令儲存使用個人通信紀錄並非限於絕對必要之範圍。2006 指令第 3 條、第 5 條規定需儲存「所有用戶」的「固定電話網路、行動電話、網路使用、電子郵件和網路電話的通信紀錄」，即每個人在日常生活中廣泛使用的通訊手段與媒介，因此導致了對幾乎所有歐盟公民的基本權利的侵害，2006 指令的儲存人別範圍涉及所有用戶，對用戶通信紀錄的儲存未區分是否有跡象表明其行為可能與嚴重刑事犯罪有關或至少有間接聯繫，並沒有限制必須與特定時期或特定地理區域或可能以任何方式參與嚴重犯罪的特定群體有關，也無特別對應受職業保密保護之人為區別[39]。

2006 指令嚴重侵害了憲章保障的第 7 條、第 8 條所保障的權利，應限制僅有追訴嚴重犯罪才可以正當化基本權侵害，且應有明確指示嚴重犯罪所指為何，然 2006 指令僅籠統地提及成員國應於其國家法律確定嚴重罪行[40]；儲存期限的部分，2006 指令第 6 條的儲存期限規定至少需保留 6 個月，並無對追求目標、數據主體或指令第 5 條的紀錄種類為區分，並無限制於絕對必要之範圍，僅概括授權會員國自行立法[41]。

在程序的相關保障上，2006 指令第 4 條未明確規範國家調取通信紀錄以及後續使用的相關實體或程序要件，沒有限制於預防和偵查特定的嚴重刑事犯罪或對其進行起訴的目的才可調取，僅稱成員國應根據比例原則的要求決定調取所儲存記錄的程序和要件，亦對強制儲存通信紀錄的調取限制隻字不提，歐盟法院認為

[37] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 49-53).
[38] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 54-55).
[39] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 56-59).
[40] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 60).
[41] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 58-60).

doi:10.6342/NTU202302425

指令應規定成員國需以法院或是獨立行政機構事前審查調取的合法性，並控制調取範圍於絕對必要範圍內[42]。

資料安全的保障方面，歐盟法院指出 2006 指令並無提供憲章第 8 條要求的個人資料安全保障，因 2006 指令第 7 條並無賦予成員國義務制定規則以保護所儲存的大量及敏感的資料，防止未經授權的調取，2006 指令應規定電信事業透過技術與組織措施確保符合嚴格的保護與安全標準，亦應確保紀錄於保存期限屆至被刪除且無法恢復，另外 2006 指令也沒有要求有關數據必須保留在歐盟的領土，無法完全確保前述之數據保護和數據安全要求的遵守情況受有憲章第 8 條所指的獨立機構監督[43]。

綜合以上 2006 指令存在的缺失，可認 2006 指令違反了依據憲章第 7、8、52 條應遵守的限制，故不再須要審查是否侵害公約第 11 條言論自由之問題，應認指令無效[44]。

第三款　重新引入強制儲存通信紀錄規定

雖然歐盟法院於 2014 年 4 月 8 日宣布強制儲存通信紀錄指令無效，根據歐盟法律，德國等會員國不再有義務制定強制儲存通信紀錄之規定，然而 2015 年因於法國發生對查理週刊之恐怖攻擊，因法國當時有強制儲存通信紀錄之規定，雖事實上並未阻止恐怖攻擊之發生，德國卻因此重啟關於強制儲存通信紀錄之討論，立法機構隨後於 2015 年 12 月 10 日通過引進通信紀錄儲存義務和最長儲存期法案（Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015），並於 2015 年 12 月 18 日生效。鑒於上述之實務發展，立法者重新對電信法與刑事訴訟法第 100g 條為重新檢討並對其進行全面修訂[45]。第 1 項大致過去規定相同，調取依據電信法第 96 條基於商業原因儲存之通信紀錄，而若須調取實時以及未來的位置資訊，須另依據同項第 4 句取得，並且刪

[42] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 61-62).
[43] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 66-68).
[44] ECJ, Joined cases C-293/12 and C-594/12 of 8. 4. 2014 (Rn. 69, 71).
[45] Bär, (Fn. 31), § 100g Rn. 3.

doi:10.6342/NTU202302425

除原本第 1 句「甚至在相關人士不知情的情況下」，調整為原則應公開執行之強制處分；第 2 項因聯邦憲法法院與歐盟法院相繼宣布原有強制通信紀錄儲存規定無效，而且兩者對後續立法指引類似，故新法自須以其為依歸，電信法儲存與刑事訴訟法調取之規定皆調整為較為嚴格的要件，限制於追訴目錄犯罪之情形方可調取；並於第 3 項新增了基地台搜索的要件。

後 2021 年又進行修法：原本欲將調取電信媒體法（Telemediengesetz, TMG）第 151 條電信媒體服務（Telemediendiensten）之使用資料（Nutzungsdaten）納入本條範圍，但因受到反對故將調取使用資料移至刑事訴訟法第 100k 條[46]。另外同年因德國為統合電信法、電信媒體法與歐盟一般資料保護規則（General Data Protection Regulation, GDPR）之間的適用問題，故聯邦參議院於 6 月 23 日通過電信現代化法（Telekommunikationsmodernisierungsgesetz v. 23.06.2021），並於同年 12 月生效，其中即包含電信與電子媒體資料與隱私保護法（Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien, TTDSG）[47]，因將部分電信法規定調整移至電信與電子媒體資料與隱私保護法，亦包括儲存通信紀錄之規定，為了商業目的而儲存通信紀錄規定從先前之電信法第 96 條，移至電信與電子媒體資料與隱私保護法第 9 條與第 12 條，無理由而預先強制儲存通信紀錄規定則自電信法第 113b 條，移至電信法第 176 條，故刑事訴訟法第 100g 條之條文亦為相應之調整。

第二節　現行刑事第 100g 條規範分析

第一項　根據電信與電子媒體資料與隱私保護法第 9 條與第 12 條調取通信紀錄（第 1 項）

[46] Köhler, in: Meyer-Goßner/Schmitt-StPO, 65. Aufl.,2022, § 100g Rn. 2.

[47] Bär, (Fn.31), §100g Rn.1. 中文資料參：羅文妗（ 2021.08），《 德國聯邦參議院通過保護數位世界隱私之《電信與電子媒體資料與隱私保護法》 》 ， 載於：https://stli.iii.org.tw/article-detail.aspx?no=66&tp=1&d=8701（最後瀏覽日：2022.08.07）。

doi:10.6342/NTU202302425

第一款　發動要件

依據第 100g 條第 1 項第 1 句，需有一定事實構成懷疑才可發動本條相關強制處分，於此僅需要簡單懷疑（einfacher Tatverdacht）即可，並需有足夠確定的事實依據而非猜測或犯罪學經驗，若事實依據不足，則應可依據更加保護基本權利的調查步驟（andere grundrechtsschonendere Ermittlungsschritte）來補充理由。法官個案決定時除了須考量是否存在這種具體、客觀的犯罪事實證據，也應審查個案是否有阻卻違法事由或是阻卻罪責事由存在[48]。

整個刑事訴訟過程都可以發動此措施，甚至根據刑事訴訟法第 457 條，亦可於刑之執行程序中實施，但若是因執行是第 1 項或第 2 項意義上的犯罪而採取此措施，須考慮到仍要執行的刑期與該措施造成之可能侵害會不會不成比例[49]。

第一目　個案中情節重大之犯罪

首先第 1 項第 1 句第 1 款規定第一種可以調取之情形：「犯了在在個案中情節重大之犯罪，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」，此要件雖屬於不確定法律概念，然而依據聯邦憲法法院的判決，仍符合規範明確性的標準，法條文字使用特別是（insbesondere）第 100a 條第 2 項作為進一步認定適用之標準，須依個案判斷是否重大性，文獻指出需為中度犯罪行為（eine Straftat der mittleren Kriminalitat），嚴重擾亂法律規定的和平，並嚴重損害民眾的法律安全感（Rechtssicherheit）。審查通常以對法益的具體危害程度、損害的程度以及犯罪方式為依據，以實務上之案例可看出排除屬於告訴乃論（Antragsdelikt）之探查數據（刑法第 202a、205 條）、偷竊皮包與手機、無特殊情形之電腦詐欺（Computerbetrug）等行為。另外，無論為正犯或共犯、既遂或是可罰之未遂行為與未遂犯之參與（Teilnahme am Versuch）皆等同視之而可聲請調取通信紀錄[50]。

---

[48] Bär, (Fn. 31), § 100g Rn. 6.
[49] Hauck, (Fn. 5), § 100g Rn. 11.
[50] Bär, (Fn. 31), § 100g Rn. 7.

doi:10.6342/NTU202302425

然而仍有文獻批評所謂「情節重大之犯罪」用語極其模糊，因為立法者希望可以保持適用上之彈性，故沒有所謂情節重大之犯罪的「底線」（Untergrenze），亦不可能從第 100a 條之目錄犯罪推測出具體之刑度範圍，因該目錄犯罪本身包含不同類型之犯罪，缺乏明確統一之結構[51]。

亦有文獻認為，第 100a 條目錄犯罪是自於實務上可能資訊不足案件之歸納和刑事政策的考量，故缺乏明確統一之結構，判斷上行為至少必須「在受保護的法益、構成要件該當行為和目錄行為的刑度方面」具有可比性[52]。

第二目　經由電信通訊實施犯罪

第 1 項第 1 句第 2 款經由電信通訊實施犯罪，是指電信通訊（或是網路）不僅為攻擊對象，更為實施犯罪必要或有用手段的情形，例如刑法第 202a 條窺探電磁紀錄、第 303a 變更電磁紀錄等，因調取通聯紀錄作為澄清是否實施犯罪行為具有重要地位，不需要屬於個案中犯罪情節重大即可調取。本款雖然降低干預門檻，但仍符合憲法要求，因被告濫用電信通訊作為實施犯罪行為的手段，自然也就排除於電信通訊機密性的保護[53]。然而如果經由電信通訊實施犯罪事實上已超過第 1 款的門檻，則應直接適用第 1 款相關要件[54]。

第二款　補充性原則、比例原則

第 1 項第 1 句、第 2 句分別宣示了補充性原則與比例原則之適用，以下分述之：

第一目　補充性原則

第 1 項之調取有「只要為查清案情有必要」的補充性原則適用。若個案係依據「經由電信通訊實施犯罪」聲請調取通信紀錄，立法者於第 1 項第 2 句指示另外的補充性原則，需要另外判斷個案是否符合對於調查事實有顯著困難之情形，然而

[51] Eschelbach, in: Satzger/Schluckebier/Widmaier (Hrsg.), StPO, 4 Aufl., 2020, § 100g Rn. 15.
[52] Hauck, (Fn. 5), § 100g Rn. 21.
[53] Bär, (Fn. 31), § 100g Rn. 9.
[54] Köhler, (Fn. 46), § 100g Rn. 20.

doi:10.6342/NTU202302425

實務上此補充性原則沒有特別意義，特別是在網路犯罪的情況下，因為調取流通信紀錄幾乎總是唯一可用的調查手段[55]。

第二目　比例原則

第 100g 條第 1 句特別提及「調取記錄與案件重大性成適當比例時」（angemessenes Verhältnis zur Bedeutung der Sache），故除了法律明文規定的干預要件，還必須個案審查發動措施是否符合比例原則，需考慮是否存在較小的干預手段，並考量此措施是否會造成過多無關第三人受影響。過去判決對此的解釋認為，由於犯罪本身的嚴重性已為第 100g 條的發動要件，故此要件應以「懷疑的程度」與「該措施可能成功執行的機率」為判斷標準。然而有文獻反對此解釋方式，認為犯罪嫌疑程度本身即已為獨立的發動要件之一，而應依據歐洲人權法院的判決解釋，即因尊重私人生活的基本權利，故對個人資料保護之例外和限制必須限制在嚴格必要的範圍內，並且各國需要採取明確且適當措施與規定，規定最低限度之保障資料安全規定，使個人資料獲得有效的保護，防止濫用的風險和任何未經授權的調取或使用，比例原則應理解為這種保障，故應於具體的個案評估，考慮整體刑事犯罪的嫌疑、調取通信紀錄的執法利益是否超過了保護資料主體的利益，以及有無其他目標明確、干預程度較低的調查措施[56]。

第三款　調取客體

第一目　電信與電子媒體資料與隱私保護法第 9 條與第 12 條儲存之通信紀錄（第 1 項）

雖然電信法第 3 條第 70 款有規定所謂通信紀錄為「提供電信服務過程中收集、處理或使用的紀錄」，而電信與電子媒體資料與隱私保護法第 9 條與第 12 條則具體化可儲存之通信紀錄，電信事業僅能基於建設電信或維持電信運作、計費、建立

[55] Eschelbach, (Fn. 51), § 100g Rn. 20.
[56] Hauck, (Fn. 5), § 100g Rn. 16-18.

doi:10.6342/NTU202302425

連接或是排除檢測電信運作故障之目的儲存（第 9 條第 1 句、第 12 條第 1 項），儲存範圍包括通訊雙方使用之號碼、識別碼、通訊之日期和時間以及使用通訊傳輸的數據量、通訊用戶使用之電信服務、固網連線之端點資訊、為建立和維護電信所需之其他通信紀錄，與過去電信法 96 條規定相同[57]。目前這些通信紀錄至多可儲存 6 個月，原則上電信事業應在期限屆至後立即刪除不需要之資料（第 10 條第 2 項第 2 句），然而因為通常電信帳單採月結制度且保障客戶得要求刪除之權利，故依據本項儲存之資訊通常僅會保存 1 個月左右[58]，即便客戶未行使此要求刪除權利，亦會因為電信公司之儲存成本問題，追訴機關至多可調取 3 個月左右之資訊[59]。

另外有些類似之資訊，雖類似於通信紀錄可以推知個人生活之細節，例如使用電子收費系統（elektronisches Mauterfassungssystem）所獲得之有關駕駛人身分以及位址資訊，這些是否可使用於刑事訴訟程序中，因其為機器之間進行交換所產生，性質上是否為「通信紀錄」雖有爭議，然而聯邦公路收費法（Bundesfernstraßenmautgesetz - BFStrMG）第 7 條第 2 項已有明文規定搜集之資料僅能用於該法所規定之目的，而排除於刑事訴訟程序中使用。而近年為防止 COVID-19 傳播，人類傳染病預防及對抗法（Infektionsschutzgesetz - IfSG）第 28a 條第 1 項第 17 款規定可儲存個人聯絡資訊或是逗留場所相關位址資訊以追蹤疾病傳播路徑與阻斷感染鏈，依據同條第 4 項第這些資訊亦不可使用於其他目的，自然包括禁止使用於刑事訴訟[60]。

第二目　實時或未來之位址資訊

第 1 項第 4 句所規範之調取客體為實時或未來之位址資訊。依據電信與電子媒體資料與隱私保護法第 9 條，行動通訊設備之位置資訊也是通信紀錄之一種，所謂個人位址規定於電信法第 3 條第 56 款，意指「在電信網路或電信服務上收集

[57] Köhler, (Fn. 46), § 100g Rn. 8. 中文文獻參：蔡宗珍，前揭註 8， 頁 112。
[58] Zöller, Vorratsdatenspeicherung zwischen nationaler und internationaler Strafverfolgung, GA 2007, 393, 396.
[59] 王士帆，前揭註 6，頁 227。
[60] Köhler, (Fn. 46), § 100g Rn.10.

doi:10.6342/NTU202302425

或使用的數據，以表明用戶的終端設備在公共可用的電信服務中的位置」。為了實行相關監視措施，允許透過調取實時開機的手機位址資訊。2007 年第 100g 條修法時允許調取舊電信法第 96 條之通信紀錄，刪除了原本法條內通信紀錄需限於「在連接的情形」（Im Falle einer Verbindung）等語，擴張調取通信紀錄之範圍，故即便手機處於待機模式下而不進行通訊、撥打電話而未接通、或是於對方接通前即掛斷之情形，因手機為進行順暢之通訊，本來就會不斷與附近訊號較強之基地台連線，而各個基地台本身即有識別碼，即會產生位址紀錄，不再需要符合較嚴格之第 100a 條要件才能進行調取（不同於第三章之聯邦最高法院調查法官見解）[61]。

然而，立法者認為位址資訊屬於較為敏感資訊，因為其具有建立個人實時移動圖像之可能性，故調取有關位址資訊需要較第 1 項調取其他通信紀錄更為嚴格之授權基礎[62]，所以第 100g 條第 1 項第 1 句刪除「為調查被告行蹤」而允許調取通信紀錄等語，將調取位址資訊移至同項第 4 句，而僅能在調查事實或調查被告位址所必需之範圍內，調取實時或向未來的位址資訊，且尚須符合犯個案中犯罪情節重大之犯罪的要件（第 100g 條第 1 項第 1 句第 1 款），僅符合「經由電信通訊實施犯罪」（第 100g 條第 1 項第 1 句第 2 款）不得調取[63]。

第三目　過去儲存之過去位址資訊

第 1 項第 3 句所規範之調取客體為過去儲存之過去位址資訊。本句的立法原因係因在 BverfG 125, 260 裁判出爐之後，立法者再另重新修正舊電信法第 113b 條（即現在之同法第 176 條）強制儲存過去通信紀錄的規定（含位址資訊），而追訴機關可依據現行較嚴格之第 100g 條第 2 項調取，此部分規定於 2015 年 12 月 18 日生效，然電信法規定之強制儲存通信義務遲至 2017 年 7 月 1 日才生效執行，此時第 100g 條第 1 項第 1 句於同次修法已刪除為調查被告行蹤調取通信紀錄，故執法機關僅能依據當時的第 3 句（現第 4 句），調取電信法第 96 條實時或未來之位

[61] BT-Drs. 16/5846, S. 51. 然有批評認為仍會影響人民之通訊意願，見 Nöding, Die Novellierung der strafprozessualen Regelungen zur Telefonüberwachung, StraFo 2007,456, 459f.
[62] BT-Drs. 16/5846, S. 28.
[63] Köhler, (Fn. 46), § 100g Rn. 9.

doi:10.6342/NTU202302425

址資訊，導致出現漏洞，因執法單位無法調取「過去儲存」之位址紀錄。立法者為解決此爭議，於刑事訴訟法施行法（EGStPO）第 12 條規定，於 2017 年 7 月 29 日前可以依據舊版第 100g 條第 1 項，為調查被告行蹤調取依據舊電信法第 96 條儲存之過去位址資訊。然而在施行法第 12 條到期之後，因為依據第 100g 條第 2 項調取電信法第 176 條通信紀錄門檻極高，且電信事業未必有執行電信法第 176 條的強制儲存義務而可能根本無資料可供調取，導致追訴機關追訴犯罪困難，又當時實務上意見多認為，於施行法第 12 條到期之後，不論資料來源，只要是調取「過去儲存」的位址資訊仍需要依照第 100g 條第 2 項的要件聲請。

最後，於 2019 年 11 月 20 日關於在刑事訴訟中執行（歐盟）2016/680 號指令和根據（歐盟）2016/679 號條例調整數據保護規定法案（Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20.11.2019）解決此爭議，立法者新增第 100g 條第 3 句，將原調取實時位址資訊移至第 4 句，只有符合第 2 項較嚴格的要件下才可以調取依據電信與電子媒體資料與隱私保護法第 9 條與第 12 條過去儲存之位址資訊[64]。

第二項　根據電信法第 176 條調取通信紀錄（第 2 項）

第一款　發動要件

第一目　特別嚴重之犯罪

首先第 2 項第 2 句規範：「某人作為正犯或共犯犯了第 2 句所稱特別嚴重之犯罪，或在未遂可罰之情況下著手實施」此重罪要件，因德國聯邦憲法法院於判決中指出不得僅以一般抽象條款劃定得調取通信紀錄的犯罪行為範圍，須以客觀之指示為之，歐盟法院亦認為須明確限制於為追訴嚴重犯罪目的以證明干預之合理性。

[64] Bär, (Fn. 31), § 100g Rn. 15-17.

doi:10.6342/NTU202302425

雖然德國聯邦憲法法院曾於 2010 年之裁判（2 BvR 236/08）認為刑事訴訟法第 100a 條第 2 項之犯罪目錄符合基本法的相關要求而駁回相關之憲法訴訟，然而 2015 年第 100g 條修法時立法者並未直接適用該條既存之犯罪目錄，而係另立犯罪目錄，雖與第 100a 條之犯罪目錄有所重疊，然考慮到調取強制儲存的資料侵害的基本權程度而大幅縮減犯罪目錄，主要是為打擊恐怖主義或保護高度個人的利益，特別是生命、身體、自由性自主以及組織犯罪等，亦包括以犯罪學經驗而言，過去儲存通信紀錄對於澄清犯罪有重要地位的犯罪類型（例如刑法第 184b 條散布兒童色情作品）[65]，有文獻分析第 100g 條之授權門檻甚至近似於第 100c 條住宅聲音監察，甚至高於第 100a 條電信監察[66]。

然而學界對目錄犯罪之範圍多有批評，例如未包含白領犯罪與電腦犯罪，例如刑法第 263a 條（電腦詐欺罪）、第 202a 條（窺探電磁紀錄）、第 202b 條（截取電磁紀錄）、第 202c 條（對於窺探與截取電磁紀錄之預備）、第 202d 條（資料贓物罪）、第 303a 條（變更電磁紀錄罪）與第 303b 條（干擾電腦使用罪）等，因為這些行為通常僅能依賴電信通訊實施，故調取通信紀錄對於澄清這些與犯罪行為十分有用[67]，並且第 100g 條第 2 項與第 100a 第 2 項、第 100b 條第 2 項條目錄內容皆不盡相同導致實務適用上的複雜[68]。

第二目　個案中亦屬特別嚴重

第 2 項第 1 句規定調取依據第 176 條儲存之通信紀錄必須存在第 100g 條第 2 項的目錄犯罪，且該行為在個案中亦屬特別嚴重，而所謂「特別嚴重」（besonders schwer）的程度是高於第 100a 條第 1 項第 1 句 第 2 款所稱的「嚴重」（schwer），亦高於第 100i 條第 1 項、第 100g 條第 1 項第 2 款的「個案中犯罪情節重大」（Straftat von erheblicher Bedeutung），然而這些措詞都屬於不確定法律概念，在個案中如何區分這些概念仍未有定論，法院對此具有裁量權，判斷之重要依據為侵害

[65] BR-Drucks 249/15, S.31-32.
[66] Dalby, (Fn.10), S. 117-118.
[67] Degenkolb, Vorratsdatenspeicherung, Kriminalistik 15, 598, 601.
[68] Eschelbach, (Fn. 51), § 100g Rn. 29-31.

doi:10.6342/NTU202302425

的法益、侵害行為嚴重性、行為結果、犯罪類型等。然而可能因為通常於偵查階段尚無法完整判斷案件之嚴重性，故此要件通常僅適用於少數案件[69]。

第三目　補充性原則、比例原則

第 2 項與第 1 項相同，皆需符合補充性原則以及比例原則的要求，即只有在對案件事實的調查或對被告下落的確定會十分困難或徒勞無功，以及調取記錄與案件重大性成適當比例時，才能收集這些資料。然而在網路犯罪追訴上，通常除了收集通信紀錄之外無其他調查方法（例如被告之 IP 位址），因此實務上調取通信紀錄仍然是不可或缺的調查方法[70]。

第二款　調取客體：電信法第 176 條之通信紀錄

於 BverfG 125, 260 裁判宣告舊電信法第 113a、113b 條無效之後，立法者於同次修法重新修訂電信法第 113a 條、第 113b 條（現移至同法 176 條以下），並規定最遲於 2017 年 1 月 1 日電信法第 3 條第 44 款所指之定期提供不特定人電信通訊服務的電信事業（包括固網電信、行動通訊、網際網路等）有義務儲存通信紀錄，僅使用戶短期內使用其電信服務之提供者，如飯店、咖啡廳的經營者則並無此儲存義務。電信提供者須確保應儲存之通信紀錄為妥善確實儲存，若電信提供者不紀錄或處理這些通信紀錄，必要時應通知聯邦網路局為其儲存（第 175 條第 1 項第 1 款、第 176 條第 1 項第 2 款）。

第 176 條第 2 項第 1 句第 1 款至第 5 款詳細列出了提供不同通訊服務供應商之通信紀錄儲存範圍，主要須儲存的通信紀錄包含：通訊通話雙方的使用之號碼與識別碼、通訊之日期和時間等，另外儲存範圍甚至涵蓋簡訊服務（SMS）、多媒體訊息（MMS）或類似訊息（如增強型簡訊服務，即 EMS）的傳輸，嘗試進行通訊（例如未接聽、未成功撥出）之紀錄亦同（第 2 項第 2 句）[71]。與本文較為相關之位址資訊，依據第 176 條第 4 項，雖不須儲存精確經三角測量等方式所獲得之交

[69] Eschelbach, (Fn. 51), § 100g Rn. 26.
[70] Bär, (Fn.31), § 100g Rn. 45.
[71] Köhler, (Fn. 46), § 100g Rn. 25-26.

doi:10.6342/NTU202302425

集結果，僅需儲存使用行動電話或網路服務時，通訊雙方各自使用連接之行動通信基地臺，並需紀錄行動通信基地臺的地理位址與主要輻射方向（Hauptstrahlrichtungen）[72]。

為了保障能夠檢查儲存通信紀錄是否符合第 177 條以下有關資料安全之規定，僅限於德國國內儲存。位址資料以外之通信紀錄須保留 10 週，只有位址資料保留 4 週（第 176 條第 1 項），這是因為使用位址資料可建立精確的移動圖像，對個人基本權利之侵害較嚴重[73]。

然而亦有部分資料禁止儲存，第 176 條第 5 項規定，通信內容、用戶所訪問網頁上的資訊和來自電子郵件服務的資料不得儲存。第 6 項則規定不可儲存電信與電子媒體資料與隱私保護法第 11 條第 5 項之通信紀錄，保護個人與社福或教會組織之聯繫，即個人因有緊急需要以遠距通訊為諮詢，來電方之身分應保持匿名，而該社會或教會組織與僱員亦具有特別之保密義務。

電信法第 177 條規定對使用第 176 儲存資料的目的限制，於刑事訴訟領域，電信事業僅能於追訴機關符合刑事訴訟法第 100g 條第 2 項要件時傳送資料（第 177 條第 1 項第 1 款），於危害防止（Gefahrenabwehr）之領域，為了避免對人之生命、身體或自由或是對聯邦或邦的存續造成危險，各邦可以援引相關法定授權基礎要求調取通信紀錄（第 177 條第 1 項第 2 款），第 177 條第 2 項更明確指出強制儲存資料不得用於第 1 項明文列舉以外之目的[74]。分離電信法收集、儲存與傳輸資料與刑事訴訟法調取資料之規定，此類立法模式被稱為「雙門模式」，前者為第一道門，後者為第二道門，兩者互相配合方能使國家取得資料，此為基本法上之要求[75]。

第三項　基地台查詢

[72] Roßnagel, Die neue Vorratsdatenspeicherung, NJW 2016, 533, 536.
[73] Hauck, (Fn. 5), § 100g Rn. 43-45.
[74] Köhler, (Fn. 46), § 100g Rn. 22-30.
[75] Dalby, (Fn. 10), S. 113.

doi:10.6342/NTU202302425

過去允許依據第 100g 條第 2 項第 2 句進行基地台查詢，然而法條文字並未確實指出這就是所謂「基地台查詢」（Funkzellenabfrage），後經修法後獨立至第 100g 條第 3 項，並區分調取來源為因商業目的而儲存通信紀錄或是強制儲存通信紀錄，並明確規定其要件。與第 100g 條前 2 項不同，基地台查詢是調取一定時間內特定基地台所有的通信紀錄，以確定該時段有哪些行動設備登錄於此特定的基地台[76]。

第一款　基地台查詢原理

電信事業於全國各處廣設覆蓋不同範圍與發射功率的基地台以提供通訊服務，基地台各由基地台識別碼（Cell-ID）和位置區標識（LAC）標示。為了進行通訊，行動裝置都必須與最近的基地台（Funkzelle）註冊，行動裝置自動註冊到最近的基地台後，基地台會將其基地台識別碼與位置區標識發送給個別行動裝置方便連接，基地台本身也會暫時儲存此過程產生之通信紀錄。實務上可以透過基地台查詢，確定被告的行動裝置是否在某基地台範圍內，以及停留了多長時間[77]。

第二款　發動要件

基地台查詢的特性在於：對於被告與非被告，干預基本權利的「程度」是相同的，因為都是取得相同之資訊（即特定時間位於某基地台附近），然而干預的「範圍」甚廣，因為電信事業基於經濟考量，不可能提供「特定」人「特定」之基地台，且現在幾乎人手一機，所以在特定時間內會有大量人使用「同一」基地台，當追訴機關發動基地台查詢時，所有使用該基地台之人皆可能被認為是被告，只因其恰巧與被告於同一時間使用同一基地台，影響範圍從上百人到上千人都有可能，而且對於無關第三人而言，不但與可能存在之犯行沒有聯繫關係，且無其他方式避免此干預（因手機是自動註冊到最近基地台），故有學者指出，基地台查詢之特性事實上比較類似刑事訴訟法第 98a 條自動化比對，因皆具有大量比對不特定對象資訊之

[76] Bär, (Fn. 31), § 100g Rn. 47.
[77] Bär, (Fn. 31), § 100g Rn. 48.

doi:10.6342/NTU202302425

特性，與第 100g 條第 1、2 項針對「特定人」調取通信紀錄不同，故與舊法相比，立法者為基地台查詢設立更嚴格的要件，以減少對無關第三者的影響[78]。

第 1 句規定進行基地台查詢需要符合以下要件：符合第 1 項第 1 句第 1 款（犯了在在個案中情節重大之犯罪，尤其是第 100a 條第 2 項所稱之犯罪）、調取記錄與案件重大性成適當比例時、調查事實或找尋被告下落有顯著困難才可進行基地台查詢，其嚴格之要件是為因應使用基地台查詢無可避免會影響到無關第三人之特性，法院於發布個案命令時，應考量該措施是否符合比例原則，例如透過具體之命令內容劃定調取一定時間和地點限制，防止過度調取與本案無關三方之通信紀錄，亦防止建立個人之移動圖像，但若這種限制事實上無法達成，或是無關第三方受影響的程度似乎是不合比例原則的，則不應允許措施實施[79]。另外有文獻認為，不需於有事實跡象表明目標人物在該基地台進行了通訊時才能進行基地台查詢[80]。至於第 2 句明確指出，只有在符合第 100g 條第 2 項較為嚴格要件下，才能進行基地台查詢有關依據電信法第 176 條儲存的資訊。然而由於電信事業不會保存太久此類數據，因此這一規定在實務上無太大意義[81]。

第四項　程序規定（第 101a、101b 條）

第一款　第 101a 條立法緣由

雖德國於 2007 年 12 月 21 日在為轉換歐洲共同體 2006/24/EG 指令之立法新增了第 101 條，統合各秘密偵查處分的程序規定，包含標示義務、通知義務、刪除義務等，以加強基本法第 103 條獲得公平審判權利與第 19 條獲得有效法律保護權利，然聯邦憲法法院於 BVerfG 125, 260 判決宣示依據第 100g 條調取通信紀錄原則上應公開執行措施，除非有礙於追訴目的實行才可以事後告知，故無法再適用第 101 條之程序規定，立法者因此於 2015 年 12 月 10 日的引進通信紀錄儲存義務和

[78] Roericht, Die Neureglung der Funkzellabfrage, Kriminalistik 17, 175, 175-176.
[79] BT-Drs. 14/5846, S. 55.
[80] Bär, Die Neuregelung zur Erhebung von Verkehrsdaten (§ 100g StPO) – Inhalt und Auswirkungen, NZWiSt 2017, 81, 85.
[81] Bär, (Fn. 31), § 100g Rn. 52.

doi:10.6342/NTU202302425

最長儲存期法案（Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015）新增第 101a、101b 條為第 100g 條之程序性規定，主要係以第 100a 條電信監察與其程序規定第 100e 條為參考，然法條文字僅籠統提及第 100e 條，究竟第 101a 條應適用連結第 100e 條哪項規定，僅能以整體脈絡體系解釋。

然而有學者認為 BVerfG 125, 260 的多數意見僅強調「強制處分若為公開措施如搜索等處分，須事先告知當事人；若為秘密偵查措施，則為了保障當事人權利至少須事後為告知。」此概念，事實上多數意見並未宣示第 100g 條為應公開執行的強制處分，甚至更傾向其為秘密偵查措施，然立法者卻誤解多數意見的意義，將第 100g 條自第 101 條刪除，而另立 101a 條作為其程序規定，卻並未認知第 100g 條調取通聯紀錄於現實上通常是偵查階段早期執行的處分，過早告知被告會造成無法達成追訴犯罪之目的，故第 101a 條是將例外變成原則的錯誤立法[82]。從警察實務角度而言亦認為非公開調取通信紀錄才是常規而非例外，因調取通信紀錄通常是於前期偵查程序，用以進一步確定參與之共犯與發動其他如通信監察等偵查措施，為避免損及追訴目的，因此大部分情形下調取通信紀錄皆無法公開進行[83]。

第二款　第 101a 條程序規定內容

首先是第 1 句連結第 100a 條第 3 項規定調取通信紀錄之發動對象：此措施僅能對被告或為被告發送、傳達或收受通訊之人（即訊息傳遞者 Nachrichtenmittler）或是被告使用其通訊系統之人（即器材提供者 Anschlussinhaber）發動，排除證人或是受害人[84]。

管轄的部分，依據第 1 項第 1 句連結第 100e 條第 1 項，若是依據第 100g 條第 1、3 項調取依電信與電子媒體資料與隱私保護法第 9 條與第 12 條儲存之通信紀錄的情形，需由檢察官書面聲請，並經由法官裁定為事前保障。若有急迫危險情

[82] Hauck, (Fn. 5), § 101a Rn.2-3.
[83] Degenkolb, (Fn. 67), S. 602
[84] Bär, (Fn. 31), § 101a Rn. 23.

doi:10.6342/NTU202302425

況下，檢察官可以先逕而為之，並且需在 3 個工作日內得到偵查法官的確認，否則該命令無效，若 3 日未獲得法官確認或是被拒絕，該命令立即失效，然而不具有追溯效力。

然而依據第 1 項第 2 句，若為第 100g 條第 2、3 項調取依電信法第 176 條儲存之通信紀錄的情形，因侵害基本權甚鉅，且此類資料會強制儲存一段期間，不同於因商業目的所儲存之資料有電信事業即時刪除的危險，故適用絕對法官保留，檢察官並無緊急權限[85]。

命令形式、內容、期限部分：依據第 101a 條第 1 項第 1 句連結第 100e 條第 3 項第 1、2 句，法官應以書面裁定的形式發布命令，命令內容包含：盡可能提供該措施所發動對象之姓名、地址以及行動裝置標示符、措施的類型、調取範圍、調取資訊類型，特別是須區分資料來源為第 100g 條第 1 項或第 2 項，前者須說明個案之嚴重性，後者須說明其根據的目錄犯罪、該資訊對於追訴程序的用意、即便此措施可延長執行，仍應說明措施結束日期，且如果是實時或向未來調取通信紀錄，法官亦可要求須於一定時間定期報告調查結果，以便於期限屆至前審查是否應繼續允許調取通信紀錄[86]。

根據第 101a 條第 1 項第 1 句第 1 款、第 2 項特別要求法官的命令須說明調取的資料與時間段（包含實時調取與已儲存之通信紀錄），亦可對個案作出不同限制（例如說明僅須要調取早上在辦公室、晚上在家裡、只有來自國外的電話），並需說明調取通信紀錄措施本身以及調取範圍的適當性與必要性而是否符合比例原則，應減少調取被認為敏感資料的位址資料，避免建立不必要的移動圖像，除非是在個案下為了澄清連續犯罪而需建立連續之移動圖像，同時詳細說明決定理由也可供以事後審查，保護通常無法事先表達意見之被告，若為延長措施亦須說明理由，決定是否延長需考慮先前已獲得之資訊，亦可提及最初命令之原因。第 2 款規定須

[85] Bär, (Fn. 31), § 101a Rn. 14, 20.
[86] Hauck, (Fn. 5), § 101a Rn. 12.

doi:10.6342/NTU202302425

告知傳輸通信紀錄之電信事業有義務報告哪部分資訊係來自於電信法第 176 條之強制儲存，以便確定第 3 項標記義務與第 101b 條報告義務能確實履行[87]。

基地台查詢部分，因基地台查詢是由基地台儲存的「所有」通信紀錄判斷某「特定」手機是否於特定時間內位於該基地台附近，故法官無法於命令中特定目標對象之終端設備標示符（第 100e 條第 3 項第 2 句第 5 款），且電信事業為了提供穩定的通訊服務，不會僅提供特定人特定之基地台使用，基地台覆蓋範圍之間可能重疊，難以確定特定時間的特定區域究竟是由哪個基地台提供服務，也無法得知特定時間內，特定基地台覆蓋範圍多廣[88]，故依據第 101a 條第 1 項第 3 句，僅需具體指定一定空間與時間上的電信範圍即可（例如：「從 A 點到 B 的點鐵路沿線所有基地台，包括與鐵路相鄰的 1 公里寬的地區」），然需盡可能為具體之限制，一方面是可以能夠獲得刑事訴訟所需的資料，另一方面也可以避免對人民的無限制監視，從而影響到眾多無關第三人。在個別情況下，空間和時間限制之範圍取決於犯罪的嚴重性和可能受到影響的無關第三人數量[89]。

期限的部分規定在第 1 項第 1 句連結第 100e 條第 1 項第 4、5 句，期限規定僅適用於實時或向未來調取通信紀錄，至多不可超過 6 個月，但只要在發動要件仍存在的情況下，即可聲請延長，一次可延長 3 個月，並且並無規定命令最長期限。

根據同法第 36 條第 2 款，由檢察官負責此強制處分之執行。特別需注意的是，即便存在急迫危險之情況，而由檢察官先為緊急命令，仍應以書面為之，不可以口頭命令取代，因為口頭命令可能違背立法者將此措施盡可能設計為公開之立法設計。第 101a 條第 1 項第 1 句與第 100a 條第 4 款規定了電信事業的協力義務，又依據 2017 年 6 月 21 日生效之電信監控條例（Telekommunikations-Überwachungsverordnung, TKÜV）第 30 至 35 條，規定電信事業有關調取通信紀錄

[87] Bruns, in: KK-StPO, 8. Aufl., 2019, § 101a Rn. 7.
[88] Roericht, (Fn. 78), S. 175.
[89] Hauck, (Fn. 5), § 101a Rn. 11-15.

doi:10.6342/NTU202302425

之程序規定，電信事業根據第 100g 條提出的調取請求必須以數位之資料格式回覆，並必須確保在任何時候都能以電子方式接收來自追訴機關之請求，並按照聯邦網路局的規範，將通信紀錄實時提供給追訴機關，或是一定時間內匯集資訊後再提供，不得拖延[90]。

若發動措施前提已不存在，檢察官必須立即終止措施實施，並通知管轄法院（第 1 項第 1 句連結第 100e 條第 5 項第 1、2 句），亦須告知電信事業不需繼續傳輸通信紀錄[91]。

另尚有標記義務、立即分析義務、刪除義務：第 3 項第 1 項第 1 句到第 3 句規定：需標記根據第 100g 條收集的所有個人資料，且需標記是否為依據電信法第 176 條所儲存之資料，傳輸通信紀錄給其他機關時亦需保留標記，確保可追溯調取通信紀錄的去向並保障符合資料使用限制。同項尚規定調取的通信紀錄須立即進行分析，避免繼續長期儲存資料造成更嚴重的基本權干預。第 3 項第 4 句連結第 101 條第 8 項規定了刪除義務，若調取之通信紀錄不需要再用於刑事偵查起訴或可能的司法審查，則應立即刪除，但若屬於第 160a 條第 1 項第 1 句中提及有拒絕證言權的應守職業秘密之人的通信紀錄，因有第 160a 條第 1 項第 3 句之立即刪除義務的特別規定，故應優先適用直接將通信紀錄刪除。另本項並未明確提及是否適用第 101 條第 8 項封鎖通信紀錄之義務[92]。

如果要再利用（Weiterverwendung）通信紀錄，區分為以下情況：若是依據第 100g 條第 1 項調取電信與電子媒體資料與隱私保護法第 9 條與第 12 條之通信紀錄，再利用需根據刑事訴訟法第 479 條；若是根據第 100g 條第 2 項、第 1 項第 3 句或第 3 項第 2 句調取電信法第 176 條過去儲存之通信紀錄，再利用則需根據刑事訴訟法第 101a 條第 4 項（同法第 479 條之特別規定），因資料使用於原儲存目的範圍以外之目的會構成對基本權額外的干預，故電信法第 177 條第 1 項 第 2 款

[90] Bär, (Fn. 31), § 101a Rn. 16.
[91] Köhler, (Fn. 46), § 101a Rn. 15.
[92] Bruns, (Fn. 87), § 101a Rn. 8-9.

doi:10.6342/NTU202302425

規範需另有明確的授權規定，才允許資料的再利用。再利用之通信紀錄須在原程序亦可使用（verwertbar），且需符合一定使用目的。

於刑事訴訟領域，在非第 264 條程序意義上同一案件情形下，需是出於為調查第 100g 條第 2 款之目錄犯罪或出於調查被告位址之目的，且不能僅單純出於為調查目錄犯罪之目的，仍需符合第 100g 條第 2 項其他要件（補充性原則等）方可允許調取通信紀錄再利用，即假設替代干預（hypothetischer Ersatzeingriff）；在危險預防領域，需出於為保護對個人生命、身體、自由或為國家聯邦的存續目的，因為這些都是較高價值之法益，符合以上之要件才可於未經當事人同意下再利用（第 1 句）。再利用後需製成紀錄保存，一旦不再需要這些通信紀錄則必須立即刪除，然而若為了未來可能的司法審查而保存，亦必須製成紀錄（第 2 句到第 5 句）[93]。

第 5 項則規定與第 4 項相反的情形，即先以為預防目的（präventiv）調取依據電信法第 176 條儲存之通信紀錄，而再利用於刑事訴訟之情形，此類情形於實務上更為常見，此項也是為了符合電信法第 177 條第 1 款使用目的限制。要件包含：需於個案中符合第 100g 條第 2 項之要件（或第 100g 條第 3 項第 2 句），才可以於未經當事人同意之下在刑事訴訟程序使用為預防目的所調取之通信紀錄。以預防目的調取依據電信與電子媒體資料與隱私保護法第 9 條與第 12 條之通信紀錄用於刑事訴訟則係根據刑事訴訟法第 161 條第 3 項之規定[94]。

最後是通知義務：依據第 6 項第 1 句，若依據第 100g 條調取通信紀錄，需通知參與受干預電信通訊之人。通知之時點部分，因聯邦憲法法院將第 100g 條定位為應「公開」執行的措施，所以依據第 33 條需保障當事人的聽審權，應於命令決定「前」通知當事人表達意見，除非出現第 33 條第 4 項第 1 句「預先聽詢可能危及命令目的」的情形，才可以不需事前通知當事人表達意見，並且法官必須說明個案中不事先通知的理由。然而實務上經常都是不事先聽詢的例外情形，因調取通信

[93] Bär, (Fn. 31), § 101a Rn. 31-33.
[94] Bär, (Fn. 31), § 101a Rn. 34.

doi:10.6342/NTU202302425

紀錄往往是作為偵查的起點，後續尚可能發動其他例如電信監控等偵查措施，故不宜事先聽詢。

根據第 6 項第 1 句需由檢察官負責通知當事人，告知內容包含命令內容與執行情況、執行期間與範圍、後續救濟管道與聲請救濟期限（第 6 項第 2 句連結第 101 條第 4 項第 2 句、第 7 項），詳細內容見第三章關於第 101 條之部分。

若存在值得保護的優勢利益，則可準用第 101 條第 4 項第 3 句不予通知當事人；若存在第 101 條第 5 項情形，即可能危及調查目的、危及他人之生命、身體、人身自由，或是重要之財產則可以推遲通知，這種情形檢察官可以一併聲請調取通信紀錄命令與遲延通知，然與第 101 條不同的是，為符合聯邦憲法法院於 BverfG 125, 260 判決所設立之原則，準用第 101 條第 4 項第 3 句不予通知時，不能僅由檢察官自行決定，而須經法院同意（第 6 項第 2 句第 1 款）；準用第 101 條第 5 項遲延通知，不僅是推遲 12 個月以上之通知，每次推遲皆須經法院同意，第一次延期通知至多為 12 個月（第 6 項第 2 句第 2 款）[95]。

在準用第 101 條第 4 項第 4 句之情形，對非為處分所針對之目標人物，若該處分僅對該人造成輕微干預，且認為對該人通知無利益者，得不予通知該非目標人物。本句所指對象為目標人物（即第 100a 條第 3 項）「以外」之人，因調取通信紀錄措施影響範圍甚廣，然非目標人物可能只是意外才被一併調取通信紀錄（例如與被告為日常業務交易之人），對基本法第 10 條所保障之秘密通訊自由干預不大，即可經利益衡量之後免予通知，並且此利益衡量判斷不須經由法院為之[96]。

至於準用第 101 條第 4 項第 5 句為確定資料主體身分調查之規定，與第 101 條第 4 項第 4 句相同，第 101 條第 4 項第 5 句是針對目標人物以外之人之規範。需衡量處分對該人的侵害強度、確定其身份所耗費之成本以及對該人產生的不利影響、調查身分是否可能又再進一步加深侵害等因素，判斷後認為有必要時，才得

[95] Köhler, (Fn. 46), § 101 Rn. 31-38.
[96] Köhler, (Fn. 46), § 101 Rn. 17.

doi:10.6342/NTU202302425

進行調查，因檢察官負有通知當事人之義務，故立法者將本句權限委予檢察官為之[97]。

第三款　第 101b 條程序規定內容

第 101b 條第 1、5 項要求製作強制處分措施的年度統計。根據第 1 項第 1、2 句，各邦和聯邦總檢察長必須向聯邦司法局報告在其職責範圍內下令的措施，並由聯邦司法局編寫報告於網路上公布。第 100g 條的部分，需分別統計根據第 100g 條第 1、2、3 項所聲請命令數量、執行命令數量與延期命令數量（第 5 項第 1 款）；統計依據調取通信紀錄的週數分別計算第 100g 條第 1 至 3 項命令數量、因通信紀錄不可使用的命令數量與因無通信紀錄而無法執行的命令數（第 5 項第 2 款）[98]。

第五項 調取限制：對應守職業秘密者的保護

德國聯邦憲法法院和歐洲法院都在裁判中明確指出，為符合比例原則，在規範強制儲存通信紀錄時，需要另以特別規定保護負有職業保密義務之人，雖電信法第 176 條第 6 項連結電信與電子媒體資料與隱私保護法第 11 條第 5 項已有規定對社會或教會領域的個人和組織強制儲存通信紀錄儲存的例外，即電信事業不具有儲存這些個人和組織通信紀錄的義務，然為達成此目標，國家需事先向 1000 多家電信事業提供排除儲存通信紀錄的名單，且不斷更新範圍，以現實情況而言，完全將這部分人排除在儲存通信紀錄的義務之外是不必要也是不可行的，況且這份名單的編纂、傳送與更新本身就會造成極大的資料濫用風險，故更好之方式應為排除「使用」與職業守密關係有關的儲存數據，故立法者透過修訂刑事訴訟法第 100g 條第 4 款解決此爭議。然本項規定屬於刑事訴訟法第 160a 條之特別規定，僅適用依據第 100g 條第 2 項調取電信法第 176 條通信紀錄之情況，若依據第 100g 條第 1 項調取電信與電子媒體資料與隱私保護法第 9 條與第 12 條通信紀錄，則回歸適用第 160a 條的保護[99]。

---

[97] Hauck, (Fn. 5), § 101a Rn. 36.
[98] Bruns, (Fn. 87), § 101b Rn. 2, 6.
[99] Hauck, (Fn. 5), § 101a Rn. 56.

doi:10.6342/NTU202302425

第 100g 條第 4 項規定包含了兩重保護的概念，即證據取得禁止和證據使用禁止。第 4 項第 1 句規定：不可對第 53 條第 1 項第 1 款至第 5 款意義上的應守職業秘密者調取通信紀錄，相較於第 160a 條所列之神職人員、辯護律師、律師與國會議員，第 53 條第 1 項第 1 至 5 款涵蓋範圍更廣，例如懷孕衝突法（Schwangerschaftskonfliktgesetz）所規定諮詢中心之代表或成員、為提供毒品成癮諮詢之單位或個人等。如果仍取得應守職業秘密之人的通信紀錄，根據第 2 句禁止作為證據使用，此句規範與第 160a 條第 1 條第 2 句內容一致。

第 4 項第 3 句和第 4 句中關於刪除和製成紀錄的程序性規定也對應第 160a 條第 1 項第 3 句和第 4 句。第 4 項第 5 句則是有關應守職業秘密者與第三方通訊所產生通信紀錄調取規定，本句內容與第 160a 條第 1 款第 5 句一致，意指如果調取通信紀錄之目標對象原先不是對應守職業秘密者本人，而是針對他人，但調取過程中自該他人獲得了根據第 53 條應受保護的通信紀錄，則亦適用上述證據使用取得與禁止規定，例如調取被告的通信紀錄的過程中，卻發現被告係與跟自己的醫生或律師通訊，則此部分之通信紀錄就不可使用必須刪除，但被告其他通信紀錄仍可繼續在刑事訴訟中不受限制地使用。第 6 句同第 160a 條第 3 項，擴大對職業秘密持有者的保護，即也適用於根據第 53a 條應守職業秘密之人的輔助人。然而，如果應守職業秘密之人涉犯庇護罪（Begünstigung）、阻礙刑罰罪（Strafvereitelung）或贓物罪（Hehlerei）等，則不再適用上述規定的保護[100]。

第六項　證據使用禁止

不論是自原因程序（Ausgangsverfahren）或是程序意義上同一犯罪，只要是合法取得之通信紀錄皆可作為證據使用，然而若違反第 100g 條的實體要件或是第 101a 條程序規定，例如該通信紀錄已超出電信法第 176 條儲存期間之通信紀錄或是違反法官保留等情形，此時應適用證據使用禁止原則並採取嚴格標準。通信紀錄在審判期日時可以文書形式（Urkundsbeweis）呈現，也可以透過訊問證人及鑑定

[100] Bär, (Fn. 31), § 101a Rn. 56-58.

doi:10.6342/NTU202302425

人，確認通信紀錄有經過正確記錄與複製，或是判斷由通信紀錄所做出的推論（例如由基地台位址推測被告大致所在位置）是否合理[101]。

第七項　事後審查

即使在該措施終止後，參與通訊之人仍可有透過第 101a 條第 6 項第 2 句連結第 101 條第 7 項第 2 句獲得後續法律保護，聲請法院審查命令內容與執行方式。

第八項　通訊結束後的通信紀錄調取

因為基本法第 10 條祕密通訊自由的保障於通訊內容到達接收人時即中止，因此時通訊落入接收人支配範圍，接收人可以自行採取刪除等不同措施防止他人獲悉，與第 100g 條欲保障之秘密通訊自由無關，而僅受資訊自決權保障，故第 100g 條第 5 項僅用以澄清，於通訊過程結束後，調取通信紀錄僅受一般規定即第 94 條（為證據目的保全及扣押物件）以下的規定拘束，追訴機關可以扣押之方式取得例如 SIM 卡等儲存通信紀錄的載體，不需要符合第 100g 條第 1、2 項「個案中犯罪情節重大之犯罪」或「犯罪在個案中亦屬特別嚴重」等要件，亦可以對證人等第三人發動搜索扣押，惟搜索扣押時仍須考量通信紀錄的特別應保障性以及發動措施是否符合比例原則[102]。以下介紹 BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (LG Karlsruhe)裁判，此判決即是處理通訊結束後，儲存於當事人可自行支配範圍之通信紀錄究竟應適用搜索扣押，亦或是較為嚴格之調取通信紀錄規定。

第一款　裁判背景

一名德國地方法院法官於 2002 年 9 月時因涉嫌洩漏偵查秘密予擔任記者之友人，造成偵查工作無法繼續進行，涉犯侵害職務秘密罪嫌（der Verletzung von Dienstgeheimnissen ，刑法第 353b 條），故檢察官將該名法官列為被告進行調查，先調查其辦公室電話的通信紀錄，然而並沒有發現與記者聯絡之跡象，故檢察官於

[101] Köhler, (Fn. 20), § 101a Rn. 19-22.
[102] Köhler, (Fn. 20), § 101 Rn. 44.

doi:10.6342/NTU202302425

2002 年 12 月聲請搜索該名法官之住所，然因記者線人群體較大，無法證明對該名法官之具體懷疑，法院僅允許調取該名法官使用通訊設備的通信紀錄，而未允許搜索其住處，檢察官對此提出抗告，法院於 2003 年 1 月 28 日始允許搜索、扣押，檢察官於 2 月 5 日實施搜索，目的係取得法官的手機與電腦的通信紀錄，並扣押其電腦、偵查相關文件副本及其手機分項帳單，以便取得可能與記者有接觸的證據。然而，經搜索扣押並分析取得之證據後，該名法官於可能的犯罪時間並無與記者通訊之證據。在搜索結束之後，法官提出救濟，主張該搜索違法而認為搜索令所載之犯罪嫌疑不存在，然地區法院認為基於該案之急迫性，發出搜索令當時或救濟時法院皆不需要進行更廣泛嚴謹的調查，抗告後聯邦憲法法院因為本案違反基本法第 103 條聽審請求權而發回地方法院，然地區法院最終仍認定該名法官確實有搜索令上所載之犯罪嫌疑，搜索令仍合法[103]。

法官再向聯邦憲法法院提出救濟，主張：搜索其住處以取得通信紀錄的行為，除了侵害基本法第 103 條聽審請求權與第 13 條住宅權的保障，另也侵害第 10 條所保障之祕密通訊自由，祕密通訊自由保障不應叫僅以訊息抵達用戶的設備為保護終點，因為現今科技發展導致許多電信服務其實並非屬用戶的可控制範圍（Machtbereich），儲存在設備內資訊應無失去保護價值，許多情況下用戶根本無從得知或控制通信紀錄的儲存與否以及儲存位置，導致是否受秘密通信自由保護僅取決於純粹技術上的條件，例如儲存在伺服器內的電子郵件受到祕密通訊自由的保障，儲存於設備內的通信紀錄卻無法受到同等保護，這是非常矛盾的。另從用戶設置手機解鎖密碼之行為可看出，用戶也希望保障通信紀錄的保密性，此與已列印出的電子郵件性質不同，故在搜索儲存於設備內的通信紀錄時，應適用刑事訴訟法第 100g 條關於調取通信紀錄的規定。[104]

第二款　裁判內容

[103] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 1-36).
[104] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 41-43).

doi:10.6342/NTU202302425

第一目　秘密通訊自由

法院於判決重申祕密通訊自由的保障目的是保障通訊雙方的私人訊息交流，保障人格發展與人性尊嚴，因為遠距通訊通常需要仰賴他人的通訊系統而容易被第三人入侵，所以要盡可能使其置於與現場交流相同的地位，防止不必要的資訊搜集。保障範圍不限於法律制定時已知的通信技術，無論何種傳輸技術（透過電纜或是無線電）或表達形式（文字、語音、圖案）均受保護。祕密通訊自由保障範圍含通訊內容與通信紀錄。通信紀錄包含：何人或何設備之間是否、何時和多長時間發生過或試圖進行過通訊，在個別情況下，通信紀錄可以分析出有關交流關係與交流強度，並可能可以推論出通訊內容。由於數位化（Digitalisierung），每使用電信系統進行通訊都會留下通信紀錄，而可以被儲存以及分析，取得這些資訊自屬於基本法第 10 條之範疇[105]。

然而在通訊過程「結束」後存儲在通訊用戶控制範圍的通信紀錄不受基本法第 10 條的保護（即本案情形），而僅是受資訊自決權（基本法第 1 條第 1 項連結第 2 條第 1 項）的保護，並且在個案中可能另外受基本法第 13 條住宅權保護。這是基於祕密通訊自由原始的保護目的，因為通訊雙方想要進行遠距離通訊，就需要把通訊內容委託給第三人協助傳輸，通訊雙方會喪失通訊的保密性而容易被第三方所侵害，祕密通訊自由即旨在對抗這種危險並彌補隱私損失。然而祕密通訊自由於通訊內容到達收件人之後，通訊過程即告中止，通訊雙方可以自己採取保護措施以防免不必要的入侵，此時通信紀錄與通訊內容與用戶自身繕打的文件並無二致，僅受資訊自決權的保護。

雖然用戶並無法於一開始決定是否要儲存通信紀錄，且專家於言詞辯論時指出，通信紀錄通常無法透過手機本身的刪除功能而完全消除紀錄，可能需要透過特別的軟體，然而劃定祕密通訊自由與資訊自決權的界線，「用戶是否能在任何情況下安全將儲存於設備中的通信紀錄刪除」並不是決定性的標準，具有決定性意義的

[105] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 63-72).

doi:10.6342/NTU202302425

標準是儲存在設備內通信紀錄是否與儲存在他私人領域的其他資料（例如用戶儲存於手機內的通訊錄）有可比性，如果類似，那所謂傳輸過程會產生之風險就不復存在，通信紀錄已經實際於用戶自己的支配範圍內，用戶已經可以透過手機本身加密或是銷燬硬體本身達到保護資料之目的，意即用戶造成影響的可能性已經改變，通常追訴機關無法於用戶不知情的情況下獲取，這就證明並無特別的保護需求[106]。

另外必須指出，不能一概認為秘密通訊自由保障係以訊息到達終端設備保護之終點，受基本法第 10 條保護祕密通訊自由也會因第三人入侵其終端設備而受到威脅，對於這種干預，祕密通訊自由是否提供人民保障是取決於保障的目的，同時考慮到具體的危險情況，而非以純粹性技術條件認定。如果正在進行的通訊過程被監聽，即便通訊內容被記錄在終端設備上，也會對通訊的保密性造成侵犯，然而一旦通訊結束，儲存在用戶支配範圍的通訊內容和通訊情況就不再存在與使用通訊設備作為通信媒介所具有的相同的具體風險。

第二目　資訊自決權

法院先說明：雖然基本法第 13 條住宅權相對資訊自決權是更為具體的自由權，然而若作為一般人格權的具體保障的資訊自決權，若僅與特殊自由權保護範圍部分重疊，或是已經獨立形成自身的保護範圍，則資訊自決權不會被特殊自由權取代。本案即為此種情形，雖然進入法官的住所進行搜索也侵害基本法第 13 條的住宅權，然而因為搜索的客體是法官的通信紀錄，基於完整保障遠距離的通訊的機密性，資訊自決權會作為秘密通訊自由的補充，所以不會被住宅權所取代[107]。

在現代資料自動化處理的背景下，需要藉由保護個人不被無限制地收集、儲存、使用和公開個人資料保障人格自由發展。資訊自決權保護個人原則上可以自己決定公開和使用其個人資料的權利，以在個人決定的基礎上進行規劃和決定，如果個人無法預期誰在什麼時候、什麼情形會知道其個人情況或資料，就會產生寒蟬效應

[106] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 73-79).
[107] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 83-85).

doi:10.6342/NTU202302425

並導致其他基本權利的行使受到損害，個人在自我決定的基礎上進行規劃和決定的自由會因此受到很大的抑制。這不僅只是保障個人利益，更是公民社會的基礎，因為自決是自由民主社會的基本條件。以本案通信紀錄而言，秘密通訊自由與資訊自決權是互補的關係，在傳輸過程結束後，資訊自決權能保障保持遠距的通訊的機密性[108]。

隨著使用通訊設備的普及以及數位化，電信事業或是個人終端設備本身儲存了各種通信紀錄，包括通訊連接時間、頻率，甚至是通訊地點，電子通訊不僅用於個人交流，更延伸至日常交易等行為，累積之資訊具有強大的資訊解讀能力，除了可以推測出通訊內容與關係，甚至可以建構個人的人格全貌（Persönlichkeitsprofils），而資訊自決權保護個人免受任何形式的個人資料收集，本案之搜索命令，具體和明確地旨在扣押儲存電信通信紀錄的數據載體，即侵害資個人之資訊自決權[109]。

搜索個人通訊設備上的通信紀錄是否需要適用與第 100g 條相同嚴格的要件，法院認為：第 94 條以下之搜索扣押規定是為了達成追訴犯罪的目的，屬於國家權力之重要任務，屬於正當目的，搜索通信紀錄亦應為達成目標所適當且必要的手段。在衡量「搜索通信紀錄所帶來的基本權侵害」與「於科技進步時代追訴犯罪的有效性」二者時，如果需要如同第 100g 條為「為澄清個案中情節重大之犯罪」才可以搜索扣押個人通訊設備上的通信紀錄，會因為干預門檻過高導致無法順利進行追訴，且相較於第 100g 條向電信事業調取通信紀錄，搜索扣押的干預行為其實較不嚴重，因為搜索扣押屬於公開行為，可以透過第 106 條以下在場權相關規定，消除國家秘密進行的風險，必要時透過律師在場監督搜索之執行，並無建立個人移動圖像之可能，且執行搜索不需透過第三方（電信事業）為之，不需考慮電信事業是否有採取資料安全措施，或面臨與客戶之間的利益衝突，因搜索時通信紀錄已掌握於當事人支配範圍內，而搜索被告的前提本就較搜索第三方（例如電信事業）要求更

[108] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 86-90).
[109] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 91-93).

doi:10.6342/NTU202302425

低，故法院認為，不需要於搜索扣押當事人儲存之通信紀錄時另外適用第 100g 條的要件[110]。

第三目　搜索扣押儲存之通信紀錄保障

基於前述通信紀錄原則上受秘密通訊自由保障，例外儲存於當事人掌控範圍時以資訊自決權為補充保護，具有特別應保障性（Schutzwürdigkeit），進行搜索扣押時仍須考量個案的嫌疑程度以及調取通信紀錄對於個案的必要性，若調查的刑事犯罪屬於微罪、欲進行扣押的通信紀錄的證據意義不大，或是嫌疑不明確，都不應允許該措施。即便必須調取通信紀錄，也應限制於絕對必要範圍內，避免取得過多與訴訟無關之資料，例如若僅須取得短期內的通信紀錄，不需要扣押整個終端設備，僅以現場查看終端設備已足。[111]

第三節　現行強制儲存通信紀錄規定爭議

雖然立法者於 2015 年重新制定強制儲存通信紀錄規定時，已嘗試滿足聯邦憲法法院與歐盟法院對於強制儲存通信紀錄之立法要求，避免違反基本法與歐盟人權憲章所保障之基本權，然而隨著歐盟法院後續於 2016 年 12 月 21 日的判決中進一步說明關於強制儲存通信紀錄之立法方針，修法後電信法與刑事訴訟法是否能符合這些要求仍有待觀察。

第一項　歐盟法院 C-203/15, C-698/15 裁判

第一款　裁判背景

雖然歐盟法院 C-293/12, C-594/12 判決已有對有關強制儲存通信紀錄明確討論，然而成員國一方面仍對於「判決是否適用於強制儲存通信紀錄之國內法」與「是否完全禁止強制儲存通信紀錄」有疑義，另一方面，亦有成員國認為該判決僅與 2006 指令有關，法院並未對各國強制儲存通信紀錄規定為任何立法標準，然而 2002 指

[110] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 93-113).
[111] BVerfG 2 BvR 2099/04 (Zweiter Senat) - Urteil vom 2. März 2006 (Rn. 119-122).

doi:10.6342/NTU202302425

令第 15 條仍與此類強制儲存通信紀錄法規有相關，故歐盟法院 2016 年 12 月 21 日宣判本案以杜爭議[112]。

本案係由兩案合併，其一因瑞典電信事業 Tele2 Sverige AB 基於 C-293/12, C-594/12 判決宣告 2006 指令無效，於 2014 年 4 月 14 日起拒絕繼續強制儲存所有人民之通信紀錄，瑞典郵政電信管理局認為 Tele2 Sverige AB 違反國內法強制儲存通信紀錄之義務，責令其應繼續儲存，故 Tele2 Sverige AB 提出訴訟，瑞典斯德哥爾摩行政法院則為了釐清相關問題向歐盟法院提出確認。另一案件為英國公民向英國高等法院提出對 2014 年資料保留存取與調查權力法案（Data Retention and Investigatory Powers Act 2014, DRIPA）之訴訟，認為其有關強制儲存所有公民之通信紀錄規定違反歐盟憲章第 7、8 條，故英國高等法院同樣向歐盟法院提起訴訟以確認[113]。

第二款　裁判內容

第一目　2002 指令範圍第 15 條與憲章第 7、8 條之解釋

首先 2002 指令規範範圍針對國家立法強制電信事業儲存通信紀錄之規定，歐盟法院認為歐盟成員國有關之立法均應符合 2002 號指令第 15 條之要求，這些要求不僅拘束成員國電信事業「儲存與處理」通信紀錄之立法，亦拘束成員國「調取」這些通信紀錄之立法規定。

依據第 2002 指令第 1 條第 2 款與第 2 條，2002 指令為第 1995 指令的「詳細說明和補充」，目的是確保憲章第 7 和 8 條規定的權利受到充分尊重，即無論各國基礎技術發展，都能確保所有電子通訊服務能夠繼續保證對個人資訊和隱私的高度保護，以保護用戶免受新技術和日益增長的自動儲存和處理資訊的能力所帶來的隱私風險，指令第 5 條第 1 項即規定成員國原則上應保障使用向公眾提供電

[112] Roßnagel, Vorratsdatenspeicherung rechtlich vor dem Aus?, NJW 2017, 696, 696-697.
[113] 陳韻竹（2017.05），〈論歐盟法院 No. C-203/15 判決之國家資料保留規範議題〉，《科技法律透析》，29:5 期，頁 50-51。

doi:10.6342/NTU202302425

信之通訊內容與通信紀錄之保密性，第 2 項禁止成員國原則上不可於未經用戶同意之情形儲存通信紀錄[114]。

第 15 條第 1 項則規定第 5 條即禁止儲存通信紀錄之例外[115]，允許成員國限制通信紀錄保密性義務之範圍，然該規定應為狹義解釋，意指成員國原則仍應禁止儲存通信紀錄，儲存之行為應保持為例外規定，本項允許國家僅能為了「國家安全、國防、公共安全、預防犯罪、偵查追訴犯罪、防止未經授權使用電子通訊系統」等明文列出之目的，於必要且適當相稱之範圍儲存通信紀錄，並依據第 2 項、第 3 項，限制需以法律為之，且遵守歐盟憲章之基本原則，故 2002 指令第 15 條亦應以憲章所保障之基本權利解釋為依歸[116]。

國家規定電信事業強制儲存通信紀錄，以便於特定條件下調取，可能干預了憲章第 7 條（尊重私人生活）、第 8 條（保護個人資料）與第 11 條（言論自由）規定，國家要限制憲章保障基本權之行使，需以法律規定，並係為追求歐盟承認之共同利益或保護他人之權利自由所必要。關於強制儲存通信紀錄需以嚴格標準審查是否符合比例原則，即僅能於有限時間內（während einer begrenzten Zeit）基於明文列出之目的進行，且限制於絕對必要範圍內[117]。

本案所涉及之法案，皆為國家強制電信事業無理由儲存人民之通信紀錄（包含位址資訊），儲存範圍與已宣告無效之 2006 指令基本上相同，包含通訊雙方身份，以及通訊的日期、時間、持續時間和性質，用戶的終端設備的位置，經由資訊整體分析，可以推測出個人生活如居住地、生活習慣、社會關係等，這些與通訊內容一樣屬於敏感訊息，這對憲章所保障之第 7、8 條權利是非常嚴重之侵害，使個人感覺私人生活持續受監視之壓力。雖然因不儲存通訊內容而不干預基

114 ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 82-84).
115 另一例外為指令第 6 條所規定允許電信事業於提供服務與計算費用、行銷等目的於必要範圍內儲存與處理，於目的不存在之後必須將資料刪除或匿名化。ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn.86).
116 ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 88-91).
117 ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 92-96).

doi:10.6342/NTU202302425

本權利之重要內容（Wesensgehalt），仍有可能因儲存通信紀錄而影響人民之通訊行為，進而干預憲章第 11 條之言論自由[118]。

有鑒於強制儲存通信紀錄所可能侵害基本權的嚴重程度，歐盟法院認為只有在打擊嚴重犯罪（Bekämpfung der schweren Kriminalität）才可以正當化，然而即便是為了打擊組織犯罪或恐怖主義之重要目標，也不可以直接正當化強制儲存所有人民之通信紀錄之規定，儲存通信紀錄之規定應保持為例外，如此一來方符合 2002 指令之體系[119]。

本案涉及之內國法案，儲存涵蓋所有電子通訊手段的所有通信紀錄，除了未特別排除應守職業秘密者，內國法也並沒有限制儲存之通信紀錄與公共安全的威脅之間存在聯繫，亦即未限制保留特定時段、特定地理區域或特定可能與嚴重犯罪相關之人之通信紀錄，這超出前所述及應將儲存通信紀錄限於絕對必要之限度內的標準，不符合憲章之要求[120]。

第二目　立法要求

強制儲存通信紀錄部分，雖 2002 指令第 15 條允許各國限制人民秘密通訊自由而得以儲存通信紀錄，然而需符合一定準則。首先國家應制定明確規定，確立資料儲存與使用之範圍，並且必需規定如何保障個人資料安全，避免個人資料遭到濫用。再者於追訴犯罪之領域，除了需要限制儲存通信紀錄於絕對必要之範圍，並且儲存通信紀錄與欲達成之目標須存在客觀之關聯，意旨國家需限制儲存範圍至少需與嚴重犯罪具有間接聯繫，這種聯繫可以透過地理區域劃分，例如追訴機關以客觀證據認定某地或某個地理區域，正在準備或實施犯罪之風險已有升高[121]。

調取強制儲存通信紀錄之部分，國家追訴機關若需要調取這些強制儲存之通信紀錄，需以明確而有拘束力之法律為規定調取之實體與程序要件，限於為了

[118] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 97-101).
[119] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 102-104).
[120] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 105-107).
[121] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 108-111).

doi:10.6342/NTU202302425

「國家安全、國防、公共安全、預防犯罪、偵查追訴犯罪、防止未經授權使用電子通訊系統」之目的。又在追訴犯罪領域，需係為追訴特別嚴重之犯罪，調取範圍以絕對必要範圍為限，與欲達成之目標需至少具有間接聯繫，即原則上僅允許調取涉嫌計畫、實施或已經實施犯罪或參與這類嚴重犯罪之人的通信紀錄[122]。

程序上除非有正當之緊急事由，於追訴刑事犯罪領域原則上需要在國家相關機關提出聲請後，由法院或是獨立之行政機關為事前控制，一旦確定告知當事人不影響調查之目的，國家機關應遵照相關程序規定通知資料主體，使資料主體得知侵害之事實，並可以行使 2002 指令第 15 條第 2 項與 1995 指令第 22 條明文保障之救濟權利[123]。

有關資料安全之部分，即便 2002 指令第 15 條允許成員國規定電信事業儲存通信紀錄，仍須符合 2002 指令第 4 條第 1 項之要求，即考慮到所保留的資料量、資料本身的敏感性和未經授權使用的風險，電信事業需採取適當的技術和組織措施，確保儲存的資料得到有效保護，防止濫用風險和任何未經授權的使用，通信紀錄必需存儲在歐盟境內，並在其儲存期結束時進行銷燬。根據憲章第 8 條第 3 項成員國必須於國內設立獨立機構，負責確保歐盟個資保護相關法律之遵守情形[124]。最後，法院作出結論：2002 指令第 15 條雖允許政府立法規定電信事業儲存通信紀錄，然須符合相關立法限制，強制電信事業無理由儲存通信紀錄並不符合指令之意旨[125]。

第二項　歐盟法院 C-511/18, C-512/18, C-520/18 裁判

第一款　裁判背景

2020 年 10 月 6 日歐盟法院再度針對 2002 指令第 15 條有關國家立法強制電信事業儲存通信紀錄回應。於 C-511/18, C-512/18, C-520/18 判決中，係分別處理法

[122] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 115-119).
[123] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 120-121).
[124] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 122-123).
[125] ECJ, Joined cases C-203/15 and C-698/15 of 12. 21. 2016 (Rn. 125).

doi:10.6342/NTU202302425

國與比利時之國內法，因其均有強制儲存通信紀錄之規定，而提交於歐盟法院為裁決。

第二款　裁判內容

首先裁判回應 2002 年指令第 15 條第 1 項是否應排除國家立法強制電信事業儲存通信紀錄與位址資訊。再重申歐盟法院 C-203/15, C-698/15 裁判之立場，2002 指令旨在保護電子通訊服務的用戶個人資料和隱私免受新技術所帶來的風險，故原則上通信紀錄僅能於特定條件下進行處理或儲存，位置資訊更僅能於匿名或經同意下方能處理，第 15 條第 1 項則是對上述保護個人資料安全義務設立例外，僅能於國家安全、預防犯罪、偵查追訴犯罪等明文列出之目的，於必要且適當相稱之範圍儲存通信紀錄，並需遵守歐盟法律之原則，僅能於上述列出的目的範圍立法，各國課與對電信事業儲存通信紀錄的義務，以便在適當情況下調取這些資料，因這些資訊可以獲得對個人生活之相關細節，隨著資訊的數量與種類增加，其干預更強，不僅干預憲章第 7 條保護私人生活的權利和第 8 條個人資訊保護的權利，更可能涉及憲章第 11 條所保障的言論自由，對應守職業秘密者影響更為劇烈，然而該有關私人生活訊息是否具有敏感性質，以及有關人員是否因這種干預而遭受不利，甚至是後續是否有使用這些資料均在非所問，因儲存本身即構成干預，且具有濫用與非法侵入之風險[126]。

依據憲章第 52 條第 1 款，各國可以法律限制這些權利之行使，然該法律須為必要且相稱，解釋 2002 指令第 15 條第 1 項，除了上述之基本權，尚須考量憲章所保障第 3 條、第 4 條、第 6 條和第 7 條所規定的權利的意義，以及國家具有保護安全和打擊嚴重犯罪的任務，以促進保護他人的權利和自由，然而必須建立相關程序與實體規定以調和不同基本權利之間的衝突[127]。

[126] ECJ, Joined cases C-511/18, C-512/18 and C-520/18 of 10.6.2020 (Rn. 105-119).
[127] ECJ, Joined cases C-511/18, C-512/18 and C-520/18 of 10.6.2020 (Rn. 121-128).

doi:10.6342/NTU202302425

雖然 2002 指令第 15 條規定各國可以法律限制秘密通訊自由之行使，然而須經嚴格之比例原則檢驗，衡量措施所造成權利干預之嚴重性與欲達成之公益目標是否平衡，限制憲章第 7 條、第 8 條之權利須於絕對必要範圍內。為了滿足比例原則，各國須制定明確且有拘束力之規定以指示措施可以行使之要件與範圍，並建立對資料安全最低限度的保障，避免被第三人濫用。儲存通信紀錄時儲存的紀錄需與欲追求之目的有客觀之聯繫[128]。

其中關於為打擊犯罪和保護公共安全而規定預防性儲存通信紀錄和位置資訊立法之部分，法院再度重申過去立場：僅有於追訴嚴重犯罪方能與儲存通信紀錄帶來之對憲章第 7 條、第 8 條干預衡平，儲存通信紀錄應保持為例外狀態，然而強制無理由一律儲存所有通信紀錄已超出 2002 指令第 15 條所要求之絕對必要的限度，與現代民主社會所不合，即便是為了追訴嚴重犯罪亦同。這種普遍且不加區別儲存通信紀錄規定涵蓋了幾乎所有人以及所有電子通訊手段，卻沒有對基於所追求目標而為區別、限制或例外，並無限制可能與犯罪相關之特定地理區域或是特定時間，甚至可能與嚴重犯罪並無直接或至少間接關聯，故即便各國依據憲章第 3 條、第 4 條、第 7 條有打擊嚴重刑事犯罪之積極義務，亦無法正當化此類強制儲存通信紀錄之干預[129]。

然而若為限定範圍、有目的儲存通信紀錄，則可認為國家追訴嚴重刑事犯罪之積極義務與造成基本權利之侵害達成衡平，而所謂限定範圍，意指需有客觀的規則標準判斷特定人士與嚴重犯罪至少存在間接關聯，亦可以地理區域為劃分，例有非歧視性證據指出嚴重犯罪風險特別高之地點，或是經常有大量人員出入的地方或基礎設施，或機場、火車站或收費站等，儲存期屆至則需刪除或予以匿名化。結論上，歐盟法院針認為 2002 指令第 15 條並不排除為了打擊嚴重犯罪，而規定根據

[128] ECJ, Joined cases C-511/18, C-512/18 and C-520/18 of 10.6.2020 (Rn. 129-133).
[129] ECJ, Joined cases C-511/18, C-512/18 and C-520/18 of 10.6.2020 (Rn. 140-145).

doi:10.6342/NTU202302425

客觀和非歧視性的標準，按資料主體的類別或透過地理區域做區分標準，有針對性地儲存通信紀錄和位置資料，儲存期限需限於必要之範圍但可延長的時間[130]。

第三項　德國國內之發展

第一款　對歐盟法院判決之回應

有文獻批評雖然立法者嘗試在 2015 年修法中滿足 BverfG 125, 260 與歐盟法院在 C-293/12, C-594/12 裁判中的要求，電信法之部分，區分了不同通信紀錄之儲存期間（位址資訊 4 週，其餘通信紀錄 10 週）、為保護個人與社會或教會組織之聯繫而禁止儲存其通信紀錄與嚴格限制調取儲存通信紀錄之目的。刑事訴訟法第 100g 條之部分，限制調取門檻於特別嚴重之犯罪、程序上認為此措施為公開措施，原則上需事先聽取當事人意見，且採絕對法官保留，需於調取命令詳細說明理由以及限定調取範圍等[131]，但有部分忽略了裁判內所揭示的原則：

第一目　強制儲存通信紀錄之效益

實務上存在許多規避強制儲存通信紀錄的可能性，可能導致該規範預計獲得之效益有限也相當不確定，例如使用合法之匿名軟體、WhatsApp 等通訊軟體服務等，使恐怖份子可以輕易規避國家的監控，然而可以肯定的是，目前強制儲存通信紀錄規定是對於幾乎所有人民自由之侵害，且侵害程度聯邦憲法法院也認為不亞於對於通訊內容之電信監控，應不容忽視此基本權利侵害[132]。

第二目　未限制儲存範圍於絕對必要之範圍

為保護 2002 指令第 15 條之權利，歐盟法院認為國家立法強制儲存「所有公民」、「於所有時間以及地理空間內」、「沒有具體一定理由」、「與刑事犯罪沒有聯繫」之通信紀錄，並沒有符合將儲存範圍限制在「絕對必要之範圍」此原則，應僅有在有一定事實構成與嚴重刑事犯罪有聯繫之情況下才可以儲存通信紀

130 ECJ, Joined cases C-511/18, C-512/18 and C-520/18 of 10.6.2020 (Rn. 146-150, 160).
131 Roßnagel, (Fn. 72), S. 538.
132 Nachbaur, Vorratsdatenspeicherung „light“ – Rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, 215, 217.

doi:10.6342/NTU202302425

錄，即需考量措施所涉及之通信紀錄、使用通訊手段、通訊雙方身分與儲存期這些要件，然而德國聯邦憲法法院 BverfG 125, 260 裁判並沒有為此儲存範圍之限制[133]，故 2015 年新修訂之電信法第 176 條以下並沒有落實這個原則，仍儲存所有註冊用戶之通信紀錄[134]。然而有文獻反駁，即便儲存大量通信紀錄的干預強度極高，但考量到雙門模式的作用機制和目的，包含電信法第 113c 條限制使用通信紀錄之目的與刑事訴訟法第 100g 條第 2 項非常嚴格的干預門檻，這種極高的侵害以被緩衝，就這一點而言是值得讚同立法者的[135]。

另外值得注意的是，歐盟法院 C-203/15, C-698/15 裁判內未具體說明通信紀錄可以儲存多長時間[136]，雖然第 176 條修法之後為追訴機關帶來了確定性，然而實務上認為目前一般通信紀錄 10 週、位置紀錄 4 週之期限過短，遠低於德國聯邦刑事調查局所研究之追訴機關需求，相較之下依電信與電子媒體資料與隱私保護法第 9 條與第 12 條為收費等目的而儲存之資料卻可以保留最長達 6 個月，導致對嚴重犯罪追訴困難，而呼籲修法延長儲存期限[137]。

第三目　未落實對於應守職業秘密者的保護

有認為電信法第 113b 條亦無落實對應守職業秘密者的保護，僅有規定不儲存個人與社會或教會組織之聯繫之通信紀錄，而不同於刑事訴訟法第 53 條所提及之應守職業秘密者，後者涵蓋較多不同職業[138]。

另有文獻認為，歐盟法院有關落實對於應守職業秘密者的保護的要件，是置於「儲存」之脈絡討論，故對應守職業秘密者的保護不應僅止於證據使用禁止，而是一開始即不應儲存其通信紀錄。現行法設計為電信法第 113b 條僅排除對個人與社會或教會組織之聯繫之通信紀錄儲存，而刑事訴訟法第 100g 條第 4 項連結第 53 條保護僅限禁止調取與證據使用禁止，雖然可以理解基於禁止儲存之成

133 Oehmichen/Mickler, Die Vorratsdatenspeicherung – Eine never ending story?, NZWiSt 2017, 298, 307.
134 Roßnagel, (Fn. 112), S. 698; Oehmichen/Mickler, (Fn. 133), S. 307.
135 Dalby, (Fn. 10), S. 116.
136 Priebe, Vorratsdatenspeicherung und kein Ende, EuZW 2017, 136, 139.
137 Hauck, (Fn. 5), § 100g Rn. 46.
138 Roßnagel, (Fn. 112), S. 698.

doi:10.6342/NTU202302425

本很高，甚至是技術上不可能，所以才如此規定，換句話說，即便判決未明文承認，歐盟法院認為不能僅透過證據使用禁止以彌補侵害，是認為任何形式的強制儲存通信紀錄法律與歐盟憲章皆無法兼容，可以認為該歐盟法院的判決已經敲響這種強制儲存通信紀錄規範的喪鐘。立法機構不應該將對應守職業秘密者的保護委由其他州立法機關自行立法，立法機關應於電信法規定儲存與使用目的之間存在「實質性聯繫」，以及電信法第 113c 條（資料使用）應須包括與刑事訴訟法第 100g 條第 4 項類似之設計[139]。

第二款　暫停電信法第 176 條之儲存義務

2015 年修法增訂強制儲存通信紀錄之規定後，立即有人向聯邦憲法法院提起假處分主張暫停實施強制儲存規定。然而，於 2016 年 6 月 8 日聯邦憲法法院拒絕該聲請，認為雖儲存所有人民之通信紀錄，會產生相當大的威懾力，使人感到不斷被監控，但是這種干預只有在資料確實被調取時才會被鞏固和具體化為可能無法彌補的損害，況且文獻上也認為，需要調取無具體理由而儲存的通信紀錄須符合第二道門，即第 100g 條第 2 項，於滿足嚴格之程序實體要件下（例如法官保留）才可調取，衡量刑事追訴之利益與造成之侵害之下，認為不需要透過假處分暫停儲存通信紀錄[140]。

然而 2017 年 6 月 22 日明斯特高等行政法院裁判保留通信用戶所有通信紀錄和位址資料不符合歐盟法律，認為德國電信法第 176 條規定需強制儲存所有公共電信服務的用戶在幾乎所有電子通信手段方面的所有通信紀錄和位置數據，而沒有將通信紀錄儲存範圍限於絕對必要之限度內，未限制僅能儲存與嚴重刑事犯罪至少具有間接聯繫之人的通信紀錄，故暫停聲請人即網際網路供應商 Spacenet 強制儲存通信紀錄義務，認為上開電信法規定違反歐洲法院 2016 年 12 月 21 日裁判內之要求。

---

139 Nachbaur, (Fn. 132), S. 216.
140 Petri, Die Vorratsdatenspeicherung, ZD 2021, 493, 495.

doi:10.6342/NTU202302425

雖然明斯特高等行政法院此裁判本身效力僅及於訴訟當事人，然而德國聯邦網路局於 2017 年 6 月 28 日藉此宣布暫停了電信事業之儲存義務，電信事業即便拒絕於 7 月 1 日開始執行儲存義務，聯邦網路局亦不會依據電信法第 149 條對其處以罰鍰，亦無任何強制措施強迫電信事業依據電信法第 176 條提供通信紀錄，這導致自 7 月 1 日起幾乎沒有電信事業儲存通信紀錄，而使追訴機關於大多數情況下都無法依據刑事訴訟法第 100g 條第 2 項調取相應之通信紀錄[141]。

前述明斯特高等行政法院裁判經上訴後，2019 年時德國聯邦最高行政法院已終止訴訟，向歐盟法院提交聲請初步裁決，要求澄清 2002 指令第 15 條是否支持無理由一律儲存通信紀錄之規定，聯邦最高行政法院認同電信法強制儲存通信紀錄相關規定應受 2002 指令相關解釋拘束，然而過去歐盟法院之裁判（C-203/15, C-698/15 裁判）已認為 2002 指令第 15 條已排除強制無理由儲存所有通信紀錄之規定，僅能於限定時間、地點範圍內儲存，亦需限制儲存通信紀錄類別與通訊類別，必需至少與嚴重犯罪具有間接關聯，且需有防止資料遭濫用之措施，單純因為被告有使用通訊系統之事實並不能構成儲存所有通信紀錄之充分理由。

然而聯邦最高行政法院認為，現行電信法第 176 條以下包含許多基本權利防護措施（Schutzvorkehrungen），例如不儲存通信內容本身或是有職業保密義務之通信紀錄、降低儲存期至 10 個或是 4 個星期、刑事訴訟法第 100g 條第 2 項之嚴格調取門檻、第 101a 條之程序配套等，已大大降低建立完整人格圖像之風險，亦提出歐盟基本權利憲章第 6 條要求成員國有保護公共安全的義務，相較於儲存特定犯罪風險升高之通信紀錄，此係基於已知的資訊，而往未來開始儲存通信紀錄，強制儲存所有通信紀錄方能重建真正發生於過去之事件，而有助於實現此目標。聯邦最高行政法院進一步認為，因成員國有義務必須平衡保護人民之公共安全任務與為達成任務所造成之基本權干預，故不同於歐盟法院之意見，應無法直接斷定強制儲存所有通信紀錄之行為違反歐盟基本權利憲章之要求，換句話說，聯邦最高行

[141] Bär, (Fn. 31), § 100g Rn. 66.

doi:10.6342/NTU202302425

政法院認為無法於過去歐盟法院之判決得知，是否可於整體權衡之情形下引入強制儲存通信紀錄之規定，並輔以程序保障，以對抗新興電信手段所造成之追訴嚴重犯罪如恐怖主義、組織犯罪與兒童性剝削等重大犯罪[142]。

[142] BVerwG, 25.09.2019 - 6 C 12.18 - und - 6 C 13.18.

doi:10.6342/NTU202302425

第三章　德國刑事訴訟法對行動通訊設備之科技偵查規定

第一節　現行刑事訴訟法第 100i 條規範分析

第一項　立法背景

早在 1996 年，羅德史瓦茲公司（Rohde & Schwarz）開發並改良名為 GA 900 的設備，即所謂的 IMSI-Catcher，其功能包含確認周邊待機的行動裝置的數字標識（包含 IMSI 與 IMEI）與定位周邊行動裝置的確切位置，於 1998 年聯邦刑事警察局已開始使用 IMSI-Catcher 查緝跨國毒品運輸或挾持人質等重大犯罪。

隨後 IMSI-Catcher 亦應用於刑事追訴犯罪領域，但追訴機關使用 IMSI-Catcher 之授權基礎仍眾說紛紜，聯邦政府認為基於壓制性目的（repressive Zwecke）使用 IMSI-Catcher 授權基礎應為刑事訴訟法第 100a 條結合第 161 條[1]；亦有文獻支持直接以第 100a 條為授權基礎，因 IMSI 等行動裝置標示符或是位置資訊亦可解釋為電信監察之範圍[2]；追訴機關與維安機關於 1998 年至 2001 年已逕自使用 IMSI-Catcher 逾 30 次，其主張的授權依據為刑法第 34 條緊急避難[3]，然而當時就已經被批評：以刑法第 34 條為授權基礎有規避基本法要求可能，暫且不論國家本身是否可主張刑法第 34 條，該條文對於侵犯基本權利的法定授權內容、目的和程度上都不夠具體，且第 34 條應僅限用於避免危險目的，而非作為壓制性追訴犯罪用之措施（repressive Maßnahmen），故本條不符合基本法保障之法律保留原則，不可據以為授權基礎。總體而言，2002 年聯邦議會立法前之文獻大多認為追訴機關使用 IMSI-Catcher 因缺乏授權基礎而有違反基本法之可能[4]。

2002 年 8 月 6 日德國聯邦議會於刑事訴訟法新增第 100i 條以解決授權基礎爭議，並於同年月 14 日起施行，2006 年聯邦憲法法院以 2 BvR 1345/03 不受理裁定

[1] BT-Drs. 14/6885, S. 1.
[2] Bär, Der IMSI-Catcher - neue Eingriffsermächtigung in § 100i StPO, MMR 2003, VI, VII f.
[3] Bär, (Fn. 3), VIII f.
[4] Harnisch/Pohlmann, Strafprozessuale Maßnahmen bei Mobilfunkendgeräten, HRRS 2009, 202, 206.

doi:10.6342/NTU202302425

中確立本條之合憲性，2007 年於電信監察和其他秘密偵查措施法修正案與 2007 年 12 月 21 日為轉換歐洲共同體 2006/24/EG 指令之立法（Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007）經部分修正，刪除嚴格之使用目的限制，不再限制僅能於「為進行電信監聽準備」、「為進行暫時逮捕準備」、「為基於羈押令或緊急安置令逮捕準備」之目的才能使用 IMSI-Catcher[5]。

因 2002 年德國立法當時大多逕以使用 IMSI-Catcher 為討論，故本文以下亦直接以「使用 IMSI-Catcher」之用語介紹第 100i 條之內容，但事實上 2002 年立法當時其實並非以具體技術手段為法條內容，也就是法條文字中並沒有出現「IMSI-Catcher」之用詞，而是以此強制處分欲達成之目的作為法條內容，這是為了保留法條文字的「科技開放性」，以便因應未來可能出現其他新興科技偵查手段，例如 2018 年聯邦憲法法院即認定本條可為追訴機關發送靜默簡訊之授權基礎[6]。

第二項　IMSI-Catcher 技術原理

IMSI-Catcher 在台灣又稱為 M 化車，原名為「M 化偵查網路行動電話定位系統」，之所以稱為 M 化係指其具有行動化（Mobil）、可攜帶（portable）甚至可以於行進中（Mobil）使用的特性，實務上通常會配置於一般人無法查覺之休旅車內。IMSI-Catcher 之功能包含 ：收集行動裝置 IMSI（International Mobile Subscriber Identity，國際移動使用者辨識碼）或 IMEI（International Mobile Equipment Identity，國際行動裝置辨識碼）以及定位行動裝置位址，甚至可以開啟目標手機之麥克風以進行側聽[7]，關閉加密訊息軟體之加密功能以監聽通話內容等[8]，具有極高的技術濫用風險。所謂 IMSI 是儲存於 SIM 卡內之資訊，可用以識別移動使用者的 15 碼數

[5] Hauck, in: LR-StPO, Bd. 3/1, 27. Aufl., 2019, § 100i Rn. 1.
[6] Bruns, in: KK-StPO, 8. Aufl., 2019, § 100i Rn. 2.
[7] 曾德文（2013.08），《資通科技犯罪偵查. 通訊篇》，頁 343，自刊；廖訓誠、陳芳振、顏宥安（2016.10），《犯罪偵查技術》，頁 215，陳芳振自刊。
[8] Ronellenfitsch, Datennotwehr, DuD 2008, 110, 114.

doi:10.6342/NTU202302425

字，包含移動國家代碼（MCC，Mobile Country Code）、行動網路代碼（MNC，Mobile Network Code）與移動訂戶辨識代碼（MSIN，Mobile subscription identification number）依序連接；IMEI 則是對應手機的資訊，每一台手機均有獨一無二的 IMEI，由 15-17 碼數字組成，即類似手機硬體本身之身分證[9]。本文以下介紹第 100i 條相關之兩個功能：收集行動裝置 IMEI 與 IMSI 與定位行動裝置位址。

首先是收集行動裝置 IMEI 與 IMSI 資訊，IMSI-Catcher 所利用之原理為一般行動裝置開機進入待機模式時，行動裝置會自動向臨近之基地台註冊，行動裝置會同時傳送這些數字標示符給基地台，以便進行即時通訊，而 IMSI-Catcher 對於這些行動裝置而言，就與一般平常之基地台無異（故 IMSI-Catcher 亦稱為虛擬基地台），但因為 IMSI-Catcher 所會發出較強之訊號，會「欺騙」周遭之行動裝置，使周遭之行動裝置「誤認」有訊號更強之基地台，截斷與原先基地台之連接，轉而向 IMSI-Catcher 此虛擬基地台註冊，行動裝置即會再次傳送數字標示符以進行註冊，IMSI-Catcher 即會獲得這些資訊。因為 IMSI-Catcher 是訊號較強之虛擬基地台，作用範圍也遠比一般基地台範圍更小，故收集目標人物之行動裝置符之前須知道該目標人物大致位址，並逐台「捕捉」手機並進行資料蒐集比對，在可能的不同地點重複這個過程之後，確定資料可能的交集並取得有可能的 IMSI 或 IMEI 號碼，即可利用這些資訊調取第 100j 條用戶主資料（Bestandsdaten）進行比對。

至於 IMSI-Catcher 搜集行動裝置位址之原理與前述搜集 IMEI 與 IMSI 之原理相同，在追訴機關事先取得目標人物使用的手機號碼或 IMSI 等足以辨識個人的資訊後，將這些資訊輸入 IMSI-Catcher，偽裝成一般的基地台的 IMSI-Catcher，因訊號較強而欺騙周遭之行動裝置接收訊號，若周遭之手機處於待機模式即會向 IMSI-Catcher 註冊，藉由比對門號或 IMEI 或 IMSI 等，確認目標人物之行動裝置有位於 IMSI-Catcher 作用範圍內，經過重複多次測量以獲得可能之結果，再藉由主動發送訊號給予目標手機等手段（例如發話給予手機確認被告聲音），確認是

[9] ITRead01.com（2019.02.08），序列號, IMEI,IMSI,ICCID 的含義，https://www.itread01.com/content/1549571975.html（最後瀏覽日：2021.08.10）。

doi:10.6342/NTU202302425

否為目標人物之行動裝置。不同於以基地台定位，IMSI-Catcher 不會受限於固定基地台有固定設置位置，在捕捉到行動裝置之後可以獲得更精確的位址資訊[10]。

然而 IMSI-Catcher 有其技術限制，若行動裝置正在進行通訊（無論是通話、發送簡訊等），則 IMSI-Catcher 無法取得有關該行動裝置之資訊[11]，且行動裝置在被 IMSI-Catcher「捕捉」再到「釋放」的過程中，會有大約幾秒的時間完全無法進行通訊，亦無法撥打與警察等緊急電話進行聯繫，甚至可能與一般基地台互相干擾造成訊號中斷[12]。

IMSI-Catcher 於實務上的重要性在於，被告可能使用多張 SIM 卡混淆追訴機關，其中尚可能包含未登記、以他人名義購買或竊取所得之 SIM 卡，追訴機關利用 IMSI-Catcher 取得行動裝置標識號碼可以再調取用戶主資料，確認行動裝置用戶身份，並進一步進行電信監聽或調取通信紀錄等偵查措施[13]；取得目標人物行動裝置位址可以保障追訴機關的安全，亦可確保逮捕之執行[14]。

第三項　發動要件

追訴機關可於整個刑事訴訟期間發動本條所規定之強制處分，如果於執行階段執行個案中情節重大之犯罪，特別是第 100a 條第 2 項之目錄罪行，且該個案即將執行的刑期與此強制處分所生之侵害合於比例原則時亦可適用[15]。

第 100i 條將調查內容分為兩項：蒐集行動裝置之 IMSI 或 IMEI 資訊以及定位行動裝置的位址，舊法時針對這兩種功能（目的），分別設立不同發動要件與門檻，因過去立法者認為需要達到主要措施（Hauptmaßnahme）的較高門檻，才可以正當化準備性措施（Vorbereitungsmaßnahmen）之實施，提高的發動門檻亦可保障可能受影響的第三人，故若是為進行電信監聽準備而須取得手機 IMEI 和 IMSI 資訊（第

[10] Fox, Der IMSI-Catcher, DuD 2003, 212, 213f.；曾德文（2013.08），前揭註 8，頁 344-345。
[11] BVerfG, Bschl. v. 22.8.2006 - 2 BvR 1345/03.
[12] 不同單位估計受影響時間不同，亦有電信事業估計在使用 M 化車時，整個受影響區域可能有長達 5 至 10 分鐘都不能進行通訊。Fox, (Fn. 11), 213 f.
[13] Bruns, (Fn. 6), § 100a Rn. 7.
[14] Bruns, (Fn. 6), § 100i Rn. 3-4.
[15] Hauck, (Fn. 5), § 100i Rn. 22.

doi:10.6342/NTU202302425

1 項第 1 款），須符合第 100a 條電信監聽之發動門檻規定；若是為進行暫時逮捕準備或是為基於羈押令、緊急安置令而逮捕準備，而須知道被告所在位址，則須為犯個案中犯罪情節重大之犯罪，亦須符合輔助性條款之要件[16]。

然此區別已於 2007 年修法時刪除，現行法規定只需要是「為了確認被告下落以便執行之後的逮捕」或是「為了調查事實所必要」之目的即可發動，以擴大適用範圍。另外雖然法條並無明文規定，但因為實務上仍有此需求，故亦可為執行逮捕被告的執法人員安全而發動，或是為進行第 100g 條調取通信紀錄準備[17]。

另須注意，雖然 IMSI-Catcher 於技術尚可達成監聽行動裝置等不同功能，但若追訴機關欲進行電信監察或是通信紀錄調取，仍須分別依據第 100a 條與第 100g 條為授權基礎，不可一概以第 100i 條為授權規定。

第一款 調查行動裝置之 IMSI 與 IMEI

第 1 項第 1 款之發動要件為「有事實懷疑以正犯、共犯、未遂犯或預備犯之地位犯個案中犯罪情節重大之犯罪，尤其是第 100a 條第 2 項所列犯罪」，無論是正犯或共犯、既遂或未遂，追訴機關皆可發動本款[18]。

對此刑事犯罪須達初始嫌疑之程度，且在個案中情節重大，雖不限於第 100a 條的目錄犯罪，但目錄犯罪可以作為重要性門檻的一個指標，故法條文字以「尤其是（insbesondere）」表達，可知本款較第 100a 條的發動門檻更低，有見解主張本款解釋上不得為輕罪，至少需為中度犯罪行為（eine Straftat der mittleren Kriminalitat），嚴重擾亂法律規定的和平，並嚴重損害民眾的法律安全感（Rechtssicherheit）[19]，法官審查時應具體考量損害的程度、犯罪的性質和危險性以及對公眾的威脅判斷，雖對這個要件有裁量空間，但仍須以一定事實為基礎並

[16] Hilger, Gesetzgebungsbericht: Über den neuen § 100i StPO, GA 2002, 557, 559.
[17] Hegmann, in: BeckOK-StPO, 39. Ed., 2021, § 100i Rn. 8-9; BT-Drs. 16/5846 S. 56.
[18] Köhler, in: Meyer-Goßner/Schmitt-StPO, 65. Aufl., 2022, § 100i Rn. 8.
[19] Köhler, (Fn. 18), § 100i Rn. 6.

doi:10.6342/NTU202302425

具體化，不可僅基於傳言[20]。然亦有批評此對於情節重大之犯罪的解釋只是一再闡述用語的不確定性而有過於模糊的問題[21]。

在利用本款調查行動裝置之 IMSI 和 IMEI 後，追訴機關即可以再以這些資訊向電信事業收集用戶主資料 （第 100j 條）、進行電信通訊監察（第 100a 條）、調取通聯紀錄（第 100g 條）或長期監視（第 163f 條）等[22]。

第二款　調查行動通訊設備之位置

第 1 項第 2 款要件與第 1 項第 1 款相同。追訴機關可先依據刑事訴訟法第 100j 條向電信事業調取相關 IMEI 與 IMSI 號碼，協助定位行動裝置位址，在定位確定行動裝置的精確位置後，可以逮捕被告或是確認手機持有者是否於特定時間點出現在犯罪地點作為證據。

發動本款定位確定被告手機位址期間，因被告本身可能會移動，故追訴機關可以為了達到定位精確地點之目的而建立移動圖像[23]，但有學說見解即認為不可為進行事實調查之目的（Sachermittlungen）建立被告之移動圖像，而僅能依據較嚴格的第 100a 條為之[24]。

第四項　發動對象

首先是目標人物：第 3 項準用第 100a 條第 3 項規定，規定此措施僅能針對目標人物（Zielperson），也就是被告或為被告發送、傳達或收受通訊之人（即訊息傳遞者 Nachrichtenmittler）或是被告使用其通訊系統之人（即器材提供者 Anschlussinhaber），其中對器材提供者發動本條之措施時，不以器材提供者認知到被告有使用他的通訊技術系統為必要。不可對證人或是第 160a 條所規定之有拒絕證言權的職業秘密守密人發動本條措施[25]。

---

[20] Bruns, (Fn. 6), § 100a Rn. 30; Harnisch/Pohlmann, (Fn. 4), S. 215.
[21] Eschelbach, in: Satzger/Schluckebier/Widmaier (Hrsg.), StPO, 4. Aufl., 2020, § 100i Rn. 9.
[22] Hauck, (Fn. 5), § 100i Rn. 24.
[23] Hilger, (Fn. 17), S. 558.
[24] Hauck, (Fn. 5), § 100i Rn. 28.
[25] Hauck, (Fn. 5), § 100a Rn. 176; Bruns, (Fn. 6), § 100i Rn. 8.

doi:10.6342/NTU202302425

第三人的部分，本節第三項討論 IMSI-Catcher 之技術原理已有提及 IMSI-Catcher 會「欺騙」周遭手機進行註冊，故任何行動裝置只要落入 IMSI-Catcher 之作用範圍即會留下資料，包括周遭之無關第三人，故立法者在第 2 項規定只能在技術上不可避免的範圍內取得第三人之資訊，並且只能用於資料比較的目的，使用完畢確認非目標人物之資訊即需要立刻刪除，禁止事後改變使用目的作為證據使用，本項為刑事訴訟法第 477 條資料利用的特別規定故應優先適用[26]，即便是偶然發現，亦不可作為證據或是作為偵查開端使用（Spurenansatz）[27]。立法者之所以如此立法是因為考量到聯邦憲法法院可能的要求，應僅在絕對必要的情況下干預第三人的基本權利[28]。然亦有見解批評認為本項規定不切實際，因舊法第 100b 條尚有資訊利用的相關規定，然而現在若啟動 IMSI-Catcher 之後發現另案涉犯殺人罪被告位於 IMSI-Catcher 作用範圍內，追訴機關卻因為第 2 項的限制而完全不可使用偶然發現之資訊，這對追訴機關而言是證據的重大損失，故應重新制定特殊資料使用規定[29]。

第五項　程序規定

第一款 管轄

聯邦憲法法院認為因本條影響基本權甚鉅，且性質上不可能事先聽取被告之意見，故依據第 3 項第 1 句準用第 100e 條第 1 項第 1 句至第 3 句，需由檢察官以書面聲請，並經由第 162 條偵查法官（Ermittlungsrichter）的裁定為事前保障。若有急迫危險，檢察官具有權限可以先逕行發布命令，檢察機關之偵查人員則無此緊急權限，然而檢察官需在自發布緊急命令起算 3 日內得到偵查法官的確認，否則該命令無效，若 3 日未獲得法官確認或是被拒絕，該命令立即失效，然而不具有

[26] Köhler, (Fn. 17), § 100i Rn. 14.
[27] Rogall, Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, JZ 2008, 818, 827.
[28] Hegmann, (Fn. 17), § 100i Rn. 22.
[29] Hauck, (Fn. 5), § 100i Rn. 30.

doi:10.6342/NTU202302425

溯及效力，故先前取得之資訊仍可使用，除非有法律錯誤才有可能導致證據使用禁止[30]。

此偵查措施是由檢察官執行，因為通常只有追訴機關具備相關技術設備，所以通常不須藉由電信事業的協助，然追訴機關可向電信事業調取 IMSI 或 IMEI 等用戶主資料協助定位被告行動通訊設備[31]。當發動之前提不復存在，或是發動不符合比例原則，原則上應由檢察官下令立即中止措施，除非調查之目的係於審理中確認被告下落，才由法官決定終止之決定。另外若再度滿足第 100i 條之要件，亦可重複實施（第 100e 條第 5 項第 1 句）[32]。

第二款　裁定形式、內容與期限

第 3 項第 1 句準用第 100e 條第 3 項第 1 句規定了裁定之形式與內容，包括：裁定應以書面為之，裁定內容除了須包含裁定的目的（即為依據第 1 項第 1 款調查行動通訊設備之數字標示符，或依據第 1 項第 2 款調查行動通訊設備之位置）、被告姓名與地址等基本資訊，考慮到此措施有可能會收集大量無關之第三人之資訊，為符合比例原則之要求，即便此措施最長可以實施 6 個月，仍應說明實施期限，且法官應要求執行機關定期報告調查結果。另因被告可針對裁定為事後救濟，故法官須依據第 34 條敘明裁定之理由並闡述其滿足第 100i 條的要件，並告知被告法律救濟途徑。而若為檢察官所發布的緊急命令，即便是劫持人質之等危急情況，亦應以書面為之，並除了需滿足上述的內容要求，更須敘明急迫危險的情況提供法院審查，不可事後補記命令之理由[33]。

期限的部分，依據第 3 項第 2 句規定至多僅能使用 IMSI-Catcher 偵查 6 個月，但根據同項第 3 句，只要在發動要件仍存在的情況下，即可向法院聲請延長，但延長不得逾 6 個月，此時僅得由法院同意為延長，法院應以先前獲得之資訊為判斷是否延長措施，不可由檢察官自行命令延長，因此時應不可能有遲延危

[30] Hauck, (Fn. 5), § 100i Rn. 32-35.
[31] Köhler, (Fn. 18), § 100i Rn. 16.
[32] Köhler, (Fn. 18), § 100i Rn. 20.
[33] Hauck, (Fn. 5), § 100i Rn. 36-41, 43-49.

doi:10.6342/NTU202302425

險之存在，亦不可追溯性延長措施期限。法院在決定措施之期限時，須衡量個案行為之具體嚴重性、犯罪嫌疑程度等，亦可裁定較 6 個月更短的期限[34]。

第三款　第 101 條之程序規定

2007 年立法者於電信監察和其他秘密偵查措施法修正案與 2007 年 12 月 21 日為轉換歐洲共同體 2006/24/EG 指令之立法（Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007）修正第 101 條，整合為適用於秘密偵查措施之程序規定。後經歷次修法後，第 101 條程序規定適用之強制處分包含自動化比對（第 98a 條）、郵件扣押（第 99 條）、電信通訊監察（第 100a 條）、線上搜索（第 100b 條）、住宅聲音監察（第 100c 條）、住宅外聲音監察（第 100f 條）、住宅外之其他科技設備（第 100h 條）、用科技設備調查行動通訊設備（第 100i 條）、臥底偵查員（第 110a 條）、邊境警察檢查時所得資料之儲存及比對（第 163d 條）、由警方臨檢時進行監視之通報（第 163e 條）和長期監視（第 163f 條）。

本條所規定之程序保障包含標記、通知與刪除等，並為了符合基本法第 103 條第 1 款獲得公平審判的基本權利和第 19 條第 4 款規定的有效法律保護的要求，本條另有規定對秘密偵查措施追溯性的法律保護[35]。

第 100i 條適用本條之程序規定為標記義務、通知義務、救濟、刪除與封鎖義務[36]。

---

[34] Hauck, (Fn. 5), § 100i Rn. 39.
[35] Bruns, (Fn. 6), § 101 Rn. 1-2.
[36] 第 101 條【秘密措施之程序規定】節錄
（1）依第 98a 條、第 99 條、第 100a 條至第 100f 條、第 100h 條、第 100i 條、第 110a 條、第 163d 條至第 163f 條所為之措施，除有特別規定外，適用以下規定。
（2）（略）
（3）第 1 項所稱措施取得之個人資料，應製作相關標示。傳遞與其他單位後，應由其維持標示。
（4）第 1 項所稱措施之應受通知人如下：
（略）
8.於第 100i 條，被鎖定之人。
通知時，應告知第 7 項事後權利保護之可能性與救濟期間。當通知與受干預人之優勢值得保護利益相牴觸，不予通知。此外，第 1 句第 2 款及第了款所稱之人，而非該措施所針對者，如所受干預

doi:10.6342/NTU202302425

首先是標記義務的部分，為了滿足聯邦憲法法院於 BVerfGE 100, 313 和 BVerfGE 109, 279 裁判所闡述之要求，故於本條第 3 項規定標記義務，只要是「關於特定或可識別個人事實情況的個人資訊」（德國聯邦個人資料保護法第 46 條第 1 款）均須標記，確保使用這些資訊符合第 479 條第 2 項的傳遞資訊及使用限制。本項並未明確規定應如何進行標記，基本上僅需標記至可識別出該資訊來源為第 100i 條偵查手段，例如透過蓋章之方式標記，並應於適當情形說明係基於何種犯罪而獲得資料。如果在同一調查案卷中，例如在評估說明、中期和最終報告、起訴書或判決書中，又再複製或提及同一秘密偵查措施的結果，則不需再為標記[37]。

根據同項第 2 句，標記義務亦延伸至資料之接收者，接收者有義務保持現有之標記，當追訴機關後續再發動本條第 1 項意義上的秘密措施時，必須為標記[38]。

再來是通知義務第 4 項規定對於第 1 項所列之調查措施，應通知受處分之相對人命令本身和為執行該命令而採取的措施。通知相對人之目的是因為本條所規定之偵查措施通常具有秘密性，相對人通常不可能事前得知以對該措施進行辯

非屬重大，且可認為其對通知無利益時，得不予通知。對第 1 句所稱之人進行確認身分之調查，只在考慮措施對其干預強度、確認身分之耗費與由此對該人或他人產生之損害而有必要時，始得為之。（5）通知可能不危及調查目的、個人生命、身體之不可侵犯性與人身自由，以及重要之財產價值時，在第 110a 條情形還包括不危及瓶續使用臥底偵查人員之可能性時，應為通知。依第 1 句規定暫緩通知時，應在卷宗記錄理由。

（6）依第 5 項暫緩之通知，未於措施結束後 12 個月內補行通知者，必須法院同意始可繼續暫緩通知。法院決定繼續暫緩通知之期間。通知之要件有幾近確定之可能性在未來也不會成立時，法院得為終局免除通知之同意。數項措施在緊密時間關連性內執行時，第 1 句之期間以最後措施結束之時起算。在第 100b 條和第 100c 條之情形，第 1 句之期間為 6 個月。

（7）第 6 項之法院裁判，由核准措施之管轄法院為之，除此之外由該管檢察官所在地之法院為之。第 4 項第 1 句所稱之人，亦得自措施結束後至收到通知後之 2 週內，向第 1 句之管轄法院聲請審查措施及其執行種類和方式之合法性。對於法院之裁判，得提起立即抗告。已提起公訴且被告已獲通知時，本案審理法院於終局裁判對該聲請作出決定。

（8）由措施取得之個人資料，如不再為刑事追訴和可能發生之法院審查措施所需要時，應立即刪除。刪除應在卷宗予以記錄。當僅為可能發生之法院措施審查而暫緩刪除時，資料在未經受干預人同意時僅得為該目的而使用：個人資料之處理應予以相應限制。

中文翻譯：連孟琦（2016.09），《德國刑事訴訟法——附德國法院組織法選譯》，1 版，元照，頁 35-36。

[37] Köhler, (Fn. 18), § 101 Rn. 3.

[38] Eschelbach, (Fn. 21), § 101 Rn. 3.

doi:10.6342/NTU202302425

護，故追訴機關於執行命令結束後予以通知，讓當事人有機會請求法院法院審查該命令和措施執行，保障其基本法第 103 條受公平審判之權利，不論調查結果為何，因仍存在國家干預基本權利之事實，故即便追訴機關發動偵查措施後沒有獲得任何有用之訊息，亦須通知相對人。

聯邦憲法法院的判決指出：唯有透過通知數據主體，才能保證有效的法律保護，如果連事後的通知都付之闕如，相對人自不可能主張資料取得或使用的非法性，遑論請求刪除的權利，然而立法者可以規定，考慮到其他第三方受憲法保護的合法利益，通知義務容有例外，但須限制在絕對必要的範圍內[39]。

依據第 4 項第 1 句第 12 款，追訴機關執行第 100i 條之命令後，僅需通知目標人物即可，立法者已做出不需通知無關第三人之立法決定。於 2 BvR 1345/03 聯邦憲法法院不受理裁定中已闡述不需通知無關第三人之合比例性，原因在於，因為技術上不可避免 IMSI-Catcher 蒐集無關第三人資訊，但蒐集無關第三人資訊係僅用於匿名比較是否為目標人物行動裝置的目的，經比對後若不符合則會立即刪除，實務執行上聯邦刑事警局稱第三人的資訊會保持匿名不會比對真實身份，且僅會於執行任務期間暫時儲存第三人資訊，執行完畢後會立即刪除而無法復原，故干預基本權利程度較低。若追訴機關欲通知無關第三人干預之事實，則自須先該確認通知的人別，反而需要先識別比對個人資訊，即可能加深對基本權利的侵害，且調查第三人的身份需耗費大量成本，例如因為手機的使用者不一定與手機或 SIM 卡登記在其名下的人相同[40]。

由檢察官負責以書面通知目標人物，電信事業不得主動通知當事人，根據第 7 項第 2 句，漏未通知亦可以請求救濟，但並不會導致證據使用禁止。檢察官可指示司法警察準備通知書，另警察可以協助檢察官在執行干預措施過程中留意是否有得或必須省略通知的情形[41]。

---

[39] Hauck, (Fn. 5), § 101 Rn. 15-16.
[40] BVerfG, Bschl. v. 22.8.2006 - 2 BvR 1345/03.
[41] Köhler, (Fn. 18), § 101 Rn. 4; Eschelbach, (Fn. 21), §101 Rn. 30.

doi:10.6342/NTU202302425

通知的內容必須足以確保隨後的救濟可能性，雖不須鉅細靡遺告知命令的內容與細節以及結果，然而至少應說明命令之法律依據、實施時間、命令之類型以及期限，依據第 4 項第 2 句，應告知可以主張後續法律救濟以及救濟期限，若未進行通知即暫停救濟期間計算[42]。

依據第 4 項第 3 句，若通知與受干預人之優勢值得保護利益相牴觸，為避免通知導致加深基本權干預而應不予通知，例如經調查後發現犯罪嫌疑不存在、未達開啟審判程序之充分嫌疑、通知可能有造成不利於目標人物之聲譽或業務的可能，或者需保護稅捐保密（Steuergeheimnis）等，必須為個案之利益權衡。然而若是對應守職業秘密者執行命令或有侵犯私人生活核心領域的情況，因為應手職業秘密者應僅於例外情況會受強制處分之干預，故此時應為通知。不予通知之決定不須由法院為之，僅由檢察官自行決定即可，而有關不予通知之決定應按照第 5 項第 2 句製成案卷紀錄[43]。

根據第 101 條第 5 項第 1 句，只要可能危及調查目的、危及他人之生命、身體之不可侵犯性及人身自由，以及重要之財產價值，與危及繼續使用第 110a 條臥底偵查員之可能性之情形，即可延後通知目標人物，並必須依照第 2 句，將延期通知的情形製成案卷紀錄。

所謂「危及調查目的」，係取決於是否可以預期在目標人物尚未知曉的措施的情況下仍然可以獲得相關的證據，如果目標人物已知該措施或是措施已結束，通常此期待即不存在；而「危及他人之生命、身體之不可侵犯性及人身自由，以及重要之財產價值」，以及「危及繼續使用第 110a 條臥底偵查員之可能性」則主要係為保護臥底偵查員以及其親屬，非公開之警察與線人（nicht offen ermittelnde Polizeibeamte und V-Personen），因缺乏法律授權基礎，故不得適用本項，另外單純為防止公共危險亦不得適用本句而延後通知[44]。

[42] Hauck, (Fn. 5), § 101 Rn. 28; Bruns, (Fn. 6), § 101 Rn. 22.
[43] Köhler, (Fn. 18), § 101 Rn. 16.
[44] Hauck, (Fn. 5), § 101 Rn. 39-41; Eschelbach, (Fn. 21), § 101 Rn. 26.

doi:10.6342/NTU202302425

第 6 項第 1、2 句規定如果根據第 5 項延後通知沒有在措施終止後的 12 個月內執行通知，需要由法院決定推遲的期限，但如果得通知之要件將來極有可能不會出現，法院得依據同項第 3 句同意免予通知，即不需要再反覆審查延期通知之期限，聯邦憲法法院亦肯認此做法符合基本法，因為「將來極有可能也不會出現」這個要件門檻極高，可以避免法院認定過度草率。

同項第 4 句規定本項延期通知起算方式為：若有數個措施在時間上有密切的聯繫，則從最後一個措施的完成開始計算。法院之決定必須以可理解的方式並根據事實說明理由，決定是否推遲通知須考慮：被指控的罪行的重要性和程度、相關人員之利益、偵查程序範圍與複雜性以及程序進行之方式，若允許推遲通知，須進一步說明推遲之期限，通常不會超過 1 年，而若期限屆滿後，上述延期通知之理由仍然存在，則可再聲請由法院重新准許延期通知[45]。

根據第 7 款第 1 句，此決定由管轄命令之法院為之，檢察官可以對法院的拒絕同意延期通知救濟，否則檢察官必須執行通知[46]。

刪除與封鎖義務係依據第 8 項第 1 句，若如果獲得的資訊（在此指依第 3 項經標記之資訊）不須要用於刑事偵查起訴，也不需要用於後續可能的司法審查，則必須刪除這些資訊，刪除的方式根據聯邦資料保護法的規定，須使個人資料完全無法被識別，包含將硬碟格式化或將儲存於電子儲存設備的資訊刪除。然而若該秘密偵查措施的結果已被用於其他調查，則不受刪除義務的約束，判決終結後亦為了後續可能之再審需求而不予以刪除。是否刪除通常由檢察機關決定，若為案件審理期間則由法院決定，必須將刪除製成案卷紀錄，該記錄必須指出被刪除的資料的類型和範圍，但只包括其一般的、抽象概括的內容（第 8 項第 2 句）。依據第 3 句，如果只是在司法審查的情況下延後刪除，使用於任何其他用途都需要得到當事人的同意，並且資料必須被相應地封鎖。然若是有關第 160a 條第 1

[45] Hauck, (Fn. 5), § 101 Rn. 38.
[46] Eschelbach, (Fn. 21), § 101 Rn. 28-29.

doi:10.6342/NTU202302425

項第 1 句中提及有拒絕證言權的職業秘密守密人之資訊，特別是辯護律師之資訊等，第 160a 條第 1 項第 3 句 之立即刪除義務優先於本款之規定。

然而立法者未考慮之爭議問題係，如果刪除了部分個人資料，但該刪除之資訊之證據價值因其他新的證據的出現而發生變化，則被告可能反而失去了使用該刪除資料為自己辯護之可能性，亦無法於再審中使用這些資訊[47]。

最後是是事後審查的部分：依據第 7 項第 2 句，目標人物可以聲請法院審查處分之合法性及其執行之種類與方式，並且可依據第 3 句提出抗告。目標人物須於收到通知後 2 週內提出救濟，即便未受通知，目標人物亦可以「漏未通知」的事由（通知亦為執行措施之一部）提起救濟，此時因為檢察官並未通知，所以 2 週的救濟期限不起算，然通常並不會導致證據禁止使用，除非其受辯護之權利受到損害且影響判決本身。如果未被通知的數據主體故意遲遲不向法院提起救濟，並且在有理由認為其可以採取行動以保護權利的情況下，卻仍然不提起救濟，那麼可認為其違反誠信而對調查措施並無法律保護的需求[48]。

救濟之管轄權需要取決於訴訟進行階段，偵查階段提起公訴前，依據第 1 句應由管轄命令處分之法院為之，提起公訴之後，管轄權會移轉至受訴法院為之（同項第 4 句），法院通常會將該救濟與本案訴訟一起決定，避免矛盾之情形。若於刑事訴訟最終結束後，管轄命令處分之法院再度負責給予後續法律保護[49]。

為了使當事人可有效提出法律救濟，應允許當事人獲知資訊之權利。以第 100i 條而言，若被調查之對象為被告，則可基於此程序地位查閱案卷以進行救濟；若被調查之對象為第三人（即訊息傳遞者與器材提供者）則係根據第 475 條，其律師可查閱案卷。查閱範圍包括該秘密調查措施的命令以及聲請，原則上亦包含該聲請該命令所依據事實之案卷部分，如果救濟係針對執行之合法性，原則上亦必須允許查閱有關執行的類型和方式的案卷部分，提供其調查結果摘要。

[47] Bruns, (Fn. 6), § 101 Rn. 39; Hauck, (Fn. 5), § 101 Rn. 61-62.
[48] Hegmann, (Fn. 17), § 101 Rn. 51.
[49] Eschelbach, (Fn. 21), § 101 Rn. 36.

doi:10.6342/NTU202302425

然而若經利益衡量而為了保全後續不損害調查之刑事司法利益，就應命延期查閱案卷[50]。

法院可就處分之合法性及其執行種類與方式為審查，法院須依據命令發佈當時的調查狀況與已獲資訊，審查發出命令時是否有超出其判斷餘地。然管轄命令之法院僅判斷該命令是否合法，不判斷其證據能力與否，對於命令的合法性的認定，對受訴法院並無任何拘束力（Bindungswirkung），證據使用禁止的問題應由本案受訴法院獨立處理，故證據使用禁止的認定不因未提起本條的救濟而有影響[51]。

第六項　證據使用禁止

審理時，如果違法本條第 2 款或非屬涉嫌情節重大犯罪的情況下，甚至是違反法官保留都應應該要適用證據使用禁止原則。然而，即便適用證據使用禁止原則（依附性證據使用禁止），通常也沒有實際意義，因為依據本條獲得的資訊通常僅作爲偵查之起點（Ermittlungsansatz），只有在承認放射效力的情況才能禁止使用[52]。

第二節　合憲性爭議

雖然立法者於 2002 年透過第 100i 條的立法，看似解決使用 IMSI-Catcher 授權基礎爭議，然仍遭受部分文獻批評，批評之原因為：基本法第 10 條祕密通訊自由保障範圍除了包含通訊內容，更涵蓋通訊情況，以保障通訊參與者具有與不使用技術媒介進行通訊時相同的安全性，然而第 100i 條授權允許使用 IMSI-Catcher 所進行調查即侵害這種安全性，進而影響個人之通訊意願，侵害秘密通訊自由，然而 2002 年立法時並無提及基本權侵害範圍，違反基本法 19 條第 1 項第 2 句的指明所限制的基本權利條款（Zitiergebot）的義務，此義務要求立法機關須清楚表明是否限制基本權以及干預之程度，指名義務具有警告功能（Warnfunktion），可以發揮

[50] Eschelbach, (Fn. 21), § 101 Rn. 34; Bruns, (Fn. 6), § 101 Rn. 38.
[51] Köhler, (Fn. 18), § 101 Rn. 25b-26.
[52] Hauck, (Fn. 5), § 100i Rn. 57.

doi:10.6342/NTU202302425

不止是形式上說明限制權利內容之功能，更可使人民得知國家行使權利底線。當立法時新的法案已與過去法律限制之基本權利截然不同，而產生新的侵犯基本權利之可能時，即適用此指明義務，違反指明義務之要求通常會導致法律無效，而第100i 條是為了新的科技調查方法所增訂之全新條文，非對現有之規範進行更改，故未指名本條有干預祕密通訊自由之可能，應不符合指明義務之要求[53]。

第 2006 年聯邦憲法法院於 2 BvR 1345/03 不受理裁定中提及德國刑事訴訟法法第 100i 條所干預之基本權，裁定最終認定依據第 100i 條使用 IMSI-Catcher 蒐集手機之 IMSI 或 IMEI 資訊以及手機位址，僅干預一般行為自由與資訊自決權，與秘密通訊自由無關。

第一項　裁判背景

於 2003 年分別有五組訴願提出憲法訴願，分別為德國著名人權團體、律師、牧師、記者以及稅務顧問等，主要主張：基本法第 10 條除了保護通訊內容，也保護包含行動設備位址之通訊過程時的緊密情狀，故保護範圍延伸至通訊時之位址與使用之卡號，而刑事訴訟法第 100i 條授權追訴機關調查處理此類資訊，即侵害基本法第 10 條，且該立法違反基本法 19 條的指明所限制的基本權利條款的義務；對基本權的侵害是不符合比例原則的，因被告可以輕易以購買登記於他人名下之 SIM 卡或是竊取他人手機以規避 IMSI-Catcher 調查其身分，IMSI-Catcher 亦須干涉大量無關第三人才有可能找到目標人物，除了存在根本無法達成目的之可能，亦有過度干預之危險；IMSI-Catcher 立法時未考慮部分訴願人之職業性質（例如律師）與當事人具有特殊信賴關係，追訴機關可能應用 IMSI-Catcher 可以定位之功能透過他們而找到被告或嫌疑人，使他們成為此措施的目標，架空對有拒絕證言權的職業秘密守密人之保護；即便是無關第三人，因為 IMSI-Catcher 的技術性質，行動裝置只要落入 IMSI-Catcher 之訊號範圍，亦會被「捕捉」以進行進一步之掃描與比對，也構成對基本法第 10 條之威脅，無關第

[53] Gercke, Rechtliche Probleme durch den Einsatz des IMSI-Catchers, MMR 2003, 453, 455.

doi:10.6342/NTU202302425

三人僅要意識到行動裝置處於待機模式即有可能被追訴機關所定位，即可能導致訴願人降低通訊意願，關閉行動裝置而受到不利影響，且法條未規定對無關第三人之告知義務，故訴願人不可能採取救濟行為；最後，第 100i 條文字稱「相當重要之刑事犯罪」亦不精確，有侵害明確性原則之疑義[54]。

第二項　裁判內容

針對訴願人主要的主張，首先聯邦憲法法院認為，訴願人雖主張第 100i 條違反應保障其職業的特殊信賴的主張，但因 IMSI-Catcher 的原理是會捕捉附近「所有」待機中的行動裝置，而可能會干預附近「所有」攜帶待機中行動裝置人民的基本權，只要攜帶行動裝置極有可能受有影響，故訴願人是否為需特別保障信賴關係的職業，對於判斷第 100i 條是否違反基本法並不重要[55]。接下來法院進一步探討第 100i 條所涉及之基本權：

第一款　秘密通訊自由

第一目　保障目的與範圍

保障通訊、郵政和電信的秘密性是為了使人民可以私下交流訊息、思想和意見，而不為外人所知悉，進而自由發展其人格。遠距通訊的特點在於，通訊各方之間的存在物理上的距離，而需要使用並信賴於非通訊雙方所能支配的通訊管道，使第三方（包含國家）有可能從中干涉而不被通訊雙方所知，秘密通訊自由即是在防止這種不必要的資訊收集，以保證遠距離的隱私，盡可能使個人能有如同現場交流訊息之保護狀態。祕密通訊自由保護範圍包括通訊內容，也包括通訊過程中的緊密情狀（alle näheren Umstände），這是由於數位化之發展，電信事業在個人進行通訊之後都會儲存有關個人通訊過程的蛛絲馬跡（personenbezogene Spuren），電信事業儲存和使用這些通信紀錄，可用以判斷在哪些人或哪些終端設備之間是否發生過或試圖發生通訊，何時發生通訊，以及發生過多少次，這些

[54] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 19-27).
[55] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 43-45).

doi:10.6342/NTU202302425

溝通聯繫頻率、持續時間和時間之資訊提供了關係類型和強度的線索，並使人們能夠得出有關內容的結論，故亦應予以保護。然而對通訊過程中的緊密情狀保護，只限於與通訊內容具有根本相關的情況，因為這些資訊才可以反面推論出通訊內容[56]。

第二目　本條不干預祕密通訊自由

裁定認為：追訴機關依據第 100i 條使用 IMSI-Catcher 取得行動裝置位址，並不會干預個人之間實際上或試圖進行的通訊過程，因為在使用 IMSI-Catcher 時，只有技術設備之間（手機與 IMSI-Catcher）才有相互 「交流」，而對於基本法第 10 條電信之解釋應不同於電信法第 3 條第 22 款之純粹技術性電信概念，基本法第 10 條保障的是人民之間的個人相聯繫過程，因為這種過程會透過第三方所支配管道進行，才會具有傳輸過程的脆弱性和易受監控性之特殊危險，故使用 IMSI-Catcher 不干預秘密通訊自由所欲保護的「人為」發起的訊息交流；再者因為追訴機關以 IMSI-Catcher 收集資訊時，需要行動電話處於待機狀態下，若為通訊進行中則無法偵測相關資訊，而待機狀態僅是進行通訊的技術前提，僅是「保持交流的可能」仍不同於人為進行資訊交換的交流，這種「設備之間的溝通」不具有任何個人通訊的特點，亦與秘密通訊自由所保障之通訊緊密情狀不同，因為單純取得行動裝置位置不可能得知通訊關係和內容，追訴機關只是透過該通訊設備的位置來了解一個人的位置，只有當行動裝置實際用於傳輸交流訊息和意見之過程，才能享受基本法第 10 條第 1 款的保護，並僅能在符合刑事訴訟法第 100a 條、第 100g 條等較嚴格要件下才能進行電信監察（針對通訊內容）與調取通信紀錄（針對通訊過程中的緊密情狀）[57]。

即便可能因使用行動通訊設備而被追訴機關收集相關資訊，進而影響個人通訊意願，且使個人並不具備同現場交流之相同安全性，仍不干預秘密通訊自由，因

[56] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 50-54).
[57] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 55-57).

doi:10.6342/NTU202302425

通訊秘密本身並沒有因為對通訊意願的干預而受到危害，祕密通訊自由僅保護實際之通訊過程，「保持可能之交流」並仍非屬於真正發生之通訊[58]。最後，追訴機關使用 IMSI-Catcher 時，取得的相關資訊不是先由支配通訊過程之電信事業先儲存再由追訴機關調取，而是由執法部門自行創建了一個外部的、虛擬的訊號單元，而直接取得資訊，此種取得資訊之方式非屬祕密通訊自由保障範圍[59]。

綜上，第 100i 條並無干預人民之祕密通訊自由，而在第 100i 條並未祕密通訊自由之前提下，立法者自然即無違反基本法第 19 條指明所限制的基本權利條款的義務[60]。

第二款　資訊自決權

第一目　保障目的與範圍

基本法第 2 條第 1 項連結第 1 條第 1 項保障了所謂「資訊自決權」，保障目的是因為現今資訊數據分析領域持續發展，如果個人無法得知其個人資訊被何人、何時且如何被獲悉與利用，可能會引發寒蟬效應，導致個人無法行使其他基本權利，建立個人在自我決定的基礎上的行為自由可能也會受到影響，故資訊自決權不僅是對個人利益的保障，因自我決定更是公民行動和參與的自由民主社會的基本條件，故資訊自決權也可以說是為了共同利益。其保障範圍包括個人不會被無限制的蒐集、儲存、利用、移轉其個人資訊，即個人可以自行決定其個人資料如何使用之意[61]。

就與通訊相關之資料而言，秘密通訊自由是資訊自決權的特別規定，應優先適用，這是基於前文所述通訊過程中存在之特別危險，但即便未侵害秘密通訊自由，蒐集利用通訊資料之行為仍有可能侵害資訊自決權[62]。

第二目 本條干預資訊自決權

[58] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 60-61).
[59] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 62).
[60] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 63).
[61] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 65).
[62] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 66-67).

doi:10.6342/NTU202302425

依據第 100i 條使用 IMSI-Catcher 取得行動裝置之 IMSI 或 IMEI 以及位址，雖然未侵害秘密通訊自由，但因這些都是屬於個人資訊，故應認干預資訊自決權。若國家欲限制資訊自主權行使，須以明確法律規範，使人民可以清楚認知到規範內容要件與範圍，而第 100i 條係為達成國家追訴犯罪之任務，即透過對刑事犯罪偵查、認定被告是否有罪、對有罪之人施以處罰以及釋放無辜之人，此皆屬於刑事司法之基本任務，可確保國家之法律和平，屬於限制資訊自決權之正當目的，符合目的正當性。再審查適當性與必要性，以 IMSI-Catcher 取得行動裝置 IMEI、IMSI 或是位址是對於實現追訴犯罪之目標是合適且必要的，因可透過調查上述資訊可進一步進行電信監察，實務上例如聯邦刑事警察局也證實有使用 IMSI-Catcher 之必要，即便可能因為被告使用多張 SIM 卡或是外國的 SIM 卡造成調查困難，仍不能否定第 100i 條之實現預期目的之手段適當性與必要性[63]。

對於訴願人而言，資訊自決權並未受有過度之干預。雖然透過 IMSI-Catcher，追訴機關可以得出「何人攜帶著何行動裝置而位於何虛擬基地台範圍內」之訊息，然而考量到現代社會使用電子通訊之頻率日益增加，範圍幾乎滲透到生活中每個角落，亦提升犯罪實行之有效性，對於追訴機關而言，亦須跟上技術發展之腳步，不應僅將 IMSI-Catcher 認為屬於完善補充傳統刑事調查方法，而應將其置於現今電子通訊技術發展的背景下理解。對於無關第三人，追訴機關須保障其不會受到超出絕對必要範圍之影響，而根據實務上之操作，無關第三人的資訊會於匿名比較後立即被刪除，故對無關第三人之基本權干預較小，若欲通知其基本權受干預之事實，反而須先識別分辨大量無關第三人之個人身分，可能造成更大侵害，故免除對無關第三人之通知是可接受的[64]。

第三款　一般行為自由

[63] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 68-75).
[64] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 76-77).

doi:10.6342/NTU202302425

技術上使用 IMSI-Catcher「捕捉」到一部行動電話，會使該行動電話有幾秒無法進行任何通訊，這類對電信的干擾，不屬於秘密通訊自由範圍，而是屬於侵害一般行為自由的範圍，因為一般行為自由可以保護任何種類之活動，然追訴機關使用 IMSI-Catcher 時會盡量先以靠近被告預期之位址為主，且其技術是一次僅「捕捉」一台手機，且無法影響正在通訊中的行動裝置，非所有覆蓋區域的手機皆受影響，此干預程度並未超過使用手機每天可能發生的接收和傳輸干擾，考慮到刑事司法的需要，這種輕微干預在任何情況下都是可以接受的[65]。

第三項　對裁判之質疑

對於裁判有關刑事訴訟法第 100i 條不干預秘密通訊自由之結論，學者對此有不同意見，反對者不僅對於該裁定程序部分頗有微詞，認為不受理裁定僅具有程序效力，因不受理裁定之理由應僅為向訴願人闡述不受理本身之原因，不具有德國聯邦憲法法院法第 31 條的拘束力，故未實質解決第 100i 條之合憲性爭議[66]。另亦有見解對於其實體討論內容亦頗有微詞，認為依據第 100i 條使用 IMSI-Catcher 仍屬於秘密通訊自由之範疇，以下整理相關見解與討論：

第一款　祕密通訊自由亦保障非真正連接數據

第一目　真正與非真正通信紀錄無區別實益

秘密通訊自由的保護範圍包括通訊內容與通訊情況，即是否、何時、多長時間以及在哪些人之間發生或試圖進行通訊，至於通訊時行動裝置之位址是否以及保護之範圍仍有爭議，如果個人實際有與他人進行通訊或試圖與他人進行通訊，通訊發生的地點（及行動裝置之位址）自屬基本法第 10 條所保護範圍，因為位置資訊是通訊的整體情況的其中一個面向，此即所謂真正（echt）通信紀錄的位置資訊。

---

[65] BVerfG, 22.08.2006 - 2 BvR 1345/03 (Rn. 80-84).

[66] Nachbaur, Standortfeststellung und Art. 10 GG - Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", NJW 2007, 335, 335.

doi:10.6342/NTU202302425

然而有學者認為：基本法第 10 條對祕密通訊自由保護範圍應延伸至行動裝置處於待機模式下所生成的位置資訊，意即所謂 「非真正的」（unecht）通信紀錄，理由在於：為了進行通訊，行動裝置需要連續不間斷註冊距離最近的電信事業的基地台，這個註冊的過程無法與行動裝置的硬體本身分離，故前述裁定理由所稱「在待機模式下，不是人而只是『機器』在相互交流」，這種說法並沒有觸及問題的核心，因為任何人攜帶待機模式下的行動裝置，都表明了個人準備進行交流之意，為使行動裝置註冊周邊基地台而打開設備的行為，就可以被定性為通訊過程的啟動，換句話說，不是行動裝置，而是「使用者」本身已經準備進行通訊，故打開行動裝置進入待機模式，即可視為聯邦憲法法院所稱之「人為」交流，已超越純粹之技術登錄過程（rein technischer Einbuchensvorgang），故真正與非真正通信紀錄並無區別實益，均應受祕密通訊自由之保障[67]。

第二目　實務相同見解

聯邦最高法院偵查法官於 BGH, Ermittlungsrichter, Beschluß vom 21. Februar 2001 – 2 BGs 42/2001 此裁判中提出類似觀點，認為即便行動裝置並未進行通訊（nicht telefoniert wird），行動裝置所處之位址資訊仍屬於祕密通訊自由保障之範疇，因處於待機狀態屬於通訊過程之一部分，故追訴機關可依照第 100a、100b 條進行電信監聽時一併向電信事業調取手機位於何基地台之資訊。

第一　裁判事實

2001 年 1 月 25 日聯邦最高法院應檢察長的聲請，准許依當時之刑事訴訟法第 100a 條、第 100b 條授權監聽手機通訊，授權取得資訊內容包含命電信事業需定期傳送行動裝置位置資訊，電信事業對此授權命令提出不服，認為行動裝置若非處於通訊的情況，就不屬於第 100a 條的範圍。

第二　裁判要旨

[67] Nachbaur, (Fn. 66), S. 337.

doi:10.6342/NTU202302425

聯邦最高法院偵查法官認為：根據刑事訴訟法第 100a、100b 條發出的命令，電信事業有義務向追訴機關報告用以確定行動裝置位址所需之基地台資訊，無論該行動裝置是否處於待機模式或進行通訊，其理由在於：第 100a、100b 條為干預受基本法第 10 條保護的祕密通訊自由的法定授權，旨在規範記錄需透過技術設備以克服實體距離的所有通訊形式，對於第 100a、100b 條之解釋必須以祕密通訊自由為依歸，而保障範圍涵括到立法當時尚未出現的傳輸技術，故秘密通訊自由的解釋是開放且動態的，必須對應當時數位化儲存和處理資訊等技術發展。

而究竟如何解釋祕密通訊自由保障之通訊情況範圍，電信法與其相關規定至少可以作為基本的指引，例如 2000 年 12 月制定之電信資料保護規則（Telekommunications-Datenschutzverordnung, TDSV）第 2 條第 4 款中明確將通信紀錄（Verbindungsdaten）定義為在提供和供應電信服務的過程中收集的資訊（bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben），可見通信紀錄可包括進行實際通訊前所收集的紀錄；又根據電信法第 3 條第 16 款將電信通訊為（Telekommunikation）定義為「透過電信系統以符號、語言、影像或聲音形式傳送、傳輸和接收任何類型的訊息的技術過程」，而可認為因為手機須不斷向基地台註冊通報位置，確保了處於待機模式的手機的通訊準備，而保持隨時可以接聽的狀態是通訊必不可少的一部分，故即使未進行通訊，行動裝置位址亦與通訊過程相關。綜合以上理由，聯邦最高法院偵查法官認為調取未進行通訊的手機位址資訊亦屬於基本法第 10 條秘密通訊自由保障範圍。

與獲知通訊之內容相較，取得行動裝置位址資訊明顯對人民造成之干預較小，第 100a 條本身文字亦有明文規定可以用以確定被告行蹤，故聯邦最高法院認為可以直接適用第 100a、100b 條調取行動裝置無論是通訊中或是待機狀態下之位址資訊。另外，雖透過紀錄機器之間通訊資訊（Kommunikation von Maschinen）來確定行動裝置位址亦有侵害基本法第 1 條第 1 項連結第 2 條第 1 項保障之一般人格權

doi:10.6342/NTU202302425

（資訊自決權）的問題，然有鑒於現今科技技術之發展，基本法第 10 條的祕密通訊自由是更具體的基本權利，須優先適用。

第二款　調取行動通訊設備位置侵害保障目的

根據聯邦憲法法院的見解，保障秘密通訊是為了防止個人因預期會被第三人監控，造成隱藏或改變透過通訊系統交流想法的形式和內容，也保護人對不受監視的信任，故如果國家利用行動通訊的技術條件的特殊性，以確定設備和設備所有者的位置數據，導致通訊參與者必須考慮到他們使用手機可能被收集位置數據，國家就有可能妨礙個人對於行動裝置的使用意願，造成基本權之侵害[68]。

第四項　對裁定之肯定

然亦有學者贊同聯邦憲法法院之裁定結論，認為依據第 100i 條使用 IMSI-Catcher 應不屬於秘密通訊自由之範疇。

第一款　僅處於待機模式不等同於進入特定通訊狀態

基本法第 10 條第 1 項條所稱之電訊（Fernmeldeverkehr）即所謂的電信（Telekommunikation）應為獨立解釋，即應獨立於刑事訴訟法、電信法或電信資料保護規則討論，應先確定基本法第 10 條第 1 項保護秘密通訊自由的範圍，刑事訴訟法就可以採用此憲法解釋為相應調整。以歷史解釋方法解釋，一開始保障祕密通訊自由主要是針對書信秘密，是防止國家任意開拆閱覽私人書信之行為，之後隨著郵政與電信科技之發展，祕密通訊自由同樣扮演補償隱私損失之角色（Ausgleichsfunktion），因個人須藉由非自己可控制的電信事業進行資訊交換，不同於現場交流可以透過音量控制或位置選擇避免被第三人竊聽，遠距通信更可能容易受外部侵害而產生隱私損失。祕密通訊自由保障範圍應包括雙方的通訊內容，亦延伸到會顯露通訊雙方關係的通訊情況，保護通訊情況是因為個人有決定如何進行交流方式的自由，而與他人的交流關係本身就是私人生活之一部，第三人可能

[68] Nachbaur, (Fn. 66), S. 337.

doi:10.6342/NTU202302425

藉通信情況而推論出個人生活型態。然而，相較於刑事訴訟法第 100g 條規範調取通信紀錄是為保護通訊緊密情況，單純取得行動裝置位址，已經與上述保護祕密通訊自由原始的出發點相距甚遠。

雖然反對聯邦憲法法院裁定的見解認為：從目的論的角度來看，個人打開行動裝置進入待機模式而有溝通意願，與開始撥打特定號碼所發出的溝通意願難以區別。然而，可以進行特定通訊是因為個人有主動發起按下按鍵的行為，這個主動發起通訊的行為直接與為進行遠距通訊的目的相關，這種需由個人主動發起的通訊準備特性，不會出現在處於待機模式的行動裝置上，故追訴機關以 IMSI-Catcher 取得個人行動裝置標示符或位址，係利用行動裝置於待機模式下會自動註冊周邊訊號最強基地台的原理，此過程個人無法主動控制，可認與主動按下按鍵進行通訊的行為相距甚遠，故反對裁定之見解並無道理[69]。

另從手機通訊技術而言，只要做出按下按鍵等具體行為，表示欲進行特定的通訊，即屬於通訊過程的一部（通訊過程的開始），此時當然就受到基本法第 10 條的全面保護，相對的若僅有單純的交流意願（待機模式），不是交流過程本身的一部分，應僅為一般的、概括的「交流的開始」，不能被認為進入通訊的緊密情狀，即不具有保護的必要性。

雖然反對裁定的論點亦指出：欲進行通訊，行動裝置需連續註冊距離最近的電信事業的基地台中，這個過程無法與行動裝置的硬體本身分離，意即通訊與行動設備之間的依賴性，然而若贊成此論點，將個人的一般概括的通訊意願納入基本法第 10 條的保護範圍，甚至可能推論出只要單純持有文具和墨水，因可認為具有以書信進行遠距通訊之一般概括通訊意願，即受到基本法第 10 條的保護，而有過度擴張保護範圍之嫌[70]。

第二款　秘密通訊自由保障之時間範圍

[69] Harnisch/Pohlmann, (Fn. 4), S. 211-216.
[70] Hauck, (Fn. 5), § 100i Rn. 7-13.

doi:10.6342/NTU202302425

反對裁定的主張雖指出，秘密通訊自由應保護個人遠距通訊不受第三人干預，以避免影響人民使用行動通訊設備之意願，故應將祕密通訊自由保護範圍擴張至技術啟用階段（technische Anbahnungsphase）。但這個主張忽略第 10 條祕密通訊自由之時間保障範圍僅限於「通訊過程」，亦即當訊息交流（Informationsaustausch）本身遭到國家入侵干預時，才可認為屬國家發動措施之對象而值得保護，並且當該訊息交流過程不再處於易受第三方干預的狀態（意即通訊終止），保護即告終止[71]。

第三款　秘密通訊自由之補償功能

若主張基本法第 10 條的補償功能保護範圍可以延伸至行動裝置處於待機模式的情形，則必須將秘密通訊自由的通訊概念作廣義解釋，除了具體發生之通訊關係，亦須包含單純準備通訊之狀態（bloße Kommunikationsbereitschaft）；或是將秘密通訊自由解釋成獨立於通訊而為超越通訊之人格保護（kommunikationsübersteigenden Persönlichkeitsschutzgehalt），涵蓋了現今擁有通訊手段的人的人格所有組成部分，使保護範圍不僅包括可支配的通訊技術，更再延伸到使用各類社交網站等，但這種廣義解釋方式不僅超出了第 10 條原本之範圍，更像是對於一般人格權之保護，對於通訊概念應解釋為具有社會意義的訊息交換（sozialerhebliche Mitteilung von Informationen），不該延伸至獨立於訊息交換之技術界線（technische Einhegung），因這種技術性資訊會至少受到一般人格權之保護[72]。

第四款　秘密通訊自由係為保護通訊機密性

有主張追訴機關使用 IMSI-Catcher 可能導致有幾秒的時間被捕捉手機無法進行任何通訊，故侵害祕密通訊自由，但此主張忽略基本法第 10 條第 1 項的保護目的是設定在保護通訊機密性（Vertraulichkeit）的基礎上，不能以「使用電信的自由」（Fernmeldefreiheit）的意義解釋，後者僅涉及基本法第 2 條第 1 項保護的

[71] Hauck, (Fn. 5), § 100i Rn. 15-16.
[72] Hauck, (Fn. 5), § 100i Rn. 18.

doi:10.6342/NTU202302425

一般行為自由，而聯邦憲法法院亦已闡釋使用 IMSI-Catcher 使手機有幾秒無法進行通訊屬於合理之干預，不侵害一般行為自由[73]。

第三節　靜默簡訊

第一項　靜默簡訊技術原理

靜默簡訊（Stille SMS，stealth ping）的原理是利用行動裝置為了進行通訊，必須不斷向周邊可使用的行動通信基地臺註冊，而追訴機關即利用這個原理而發送靜默簡訊，用戶之行動裝置需處於待機狀態下並處於準備通訊之狀態[74]，追訴機關在特定的軟體幫助下，向特定手機號碼發送靜默簡訊，此種靜默簡訊有兩個特色，其一是對接收人而言，因為接收簡訊之手機不把這則簡訊作為普通簡訊，因此這封簡訊不會顯示於接收手機的螢幕，亦即當事人無法透過手機的收件匣查看，因此不會注意到接收簡訊的事實，在用戶沒有注意到的情況下，行動裝置收到這條簡訊後會向行動通信基地臺發出確認訊息，從而電信業者會自此產生通信記錄，除了手機號碼亦包括位置資訊，即可確認時手機用戶當時在哪個基地台的資訊，準確度取決於個別基地台的範圍，在城市地區有可能誤差僅有幾百公尺之內，但在其他地區可能誤差會到幾公里的距離，用戶不能透過自己的自主決定影響是否生成位址資訊[75]。另一個靜默簡訊的特色是，如果發送靜默簡訊時目標手機並未開機處於待機模式，之後目標手機即便開機，該發送之靜默亦不會像一般簡訊到達目標手機[76]。

在德國實務上以 IMSI-Catcher 來確定行動裝置位址的重要性已經降低，德國聯邦刑事警察局使用靜默簡訊數量自 2014 年起即超越 IMSI-Catcher，至 2017 年甚至發出高達 234,835 次無聲簡訊[77]，其原因在於：使用 IMSI-Catcher 必須先知道被告的 IMSI 或 IMEI 等特定手機標示符，且受限於 IMSI-Catcher 作用範圍，必須先

---

[73] Hauck, (Fn. 5), § 100i Rn. 20.
[74] Eisenberg/Singelnstein, Zur Unzulässigkeit der heimlichen Ortung per 'stiller SMS', NStZ 2005, 62, 63.
[75] Bär, (Fn. 17), § 100g Rn. 27.
[76] Landtag NRW, Drs. 15/3300, S. 4. (zitiert nach Krüger, Die sogenannte „stille SMS“ im strafprozessualen Ermittlungsverfahren, ZJS 2012, 606, 606.)
[77] 王士帆（2020.12），〈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〉，《司法週刊》，2036 期，頁 2-3。

doi:10.6342/NTU202302425

確認用戶的大概位置，但靜默簡訊於實務的意義在於追訴機關不需要於目標人物附近即可追蹤其大致位址，不受執行地點之限制，且降低被發生的風險，個人攜帶手機就如同追訴機關於其身上安置追蹤器一般，定位速度也更快亦不會影響無關第三人，所以 IMSI-Catcher 已經逐漸被靜默簡訊所取代[78]。

第二項　判決背景

隨著追訴機關使用靜默簡訊之案件數量逐年上升，其法律授權基礎也開始廣為討論。聯邦政府提出可以第 100a 條、第 100b 條、第 100g 條、第 100i 條與第 161 條等為組合成為靜默簡訊之授權基礎，然而主流文獻對此多有批評，認為現行刑事訴訟法第 100a 條與第 100g 條等不可為靜默簡訊之授權基礎，因為第 100a、100b 條規定皆無法管理「主動生成數據」之行為，僅能被動收集，第 100i 條應僅限可直接確定行動裝置位置之科技方法，而第 161 條則應靜默簡訊非對基本權利之輕微干預故不可為授權基礎，亦質疑拆分靜默簡訊為「發送簡訊」與「調取通信紀錄」二行為而分別判定授權基礎，因只有在有明確授權規範的情形下，才能確定侵害被告資訊自決權是否合理，而且人民才可以對追訴機關可以採取何種措施以追訴犯罪有預見可能。相反的，若將調查措施切分，而以不同授權基礎合法化，將導致追訴機關可以透過多種組合規避立法者立法時的預想以及預設的法律保障，人民也不再對權利侵害有預見可能，且鼓勵追訴機關使用任何技術上可能的措施，忽略對基本權的保障，故超出個別規範所規定的干預措施，必須有一個單獨的、足夠具體的法律依據，應僅在例外情況下允許不同授權基礎組合，例如調查方法明顯可分或該調查方法僅為整體調查行為附帶之一部，且該部分對基本權利侵害輕微。然而，發送靜默簡訊非整體調查方法附帶之一部，而因一定須先發送簡訊才能產生後續的通信紀錄，為整體措施的重要部分而不可分離，故以靜默簡訊調查被告位址，不可以分割為「發送簡訊」與「調取通信紀錄」，而分別給予授權基礎，故文獻認為如此不符合法律授權原則，應制定全新

[78] Harnisch/Pohlmann, (Fn. 4), S. 209-216.

doi:10.6342/NTU202302425

授權規範，避免這種隨著科技發展即開放並擴展偵查工具之傾向，給予追訴機關確實之法律依據[79]。聯邦憲法法院至今亦未對靜默簡訊之法律定位為回應，僅有聯邦最高法院此判決為分析[80]。

本案被告參與庫德工人黨（PKK，認定為外國恐怖組織），警察為了掌握其行蹤去向，向線民取得其使用之手機門號後，使用公務電腦安裝軟體設定每 2 小時發送一次「無聲簡訊」長達 10 日，因手機接收簡訊後，電信事業會取得該簡訊相關之通訊紀錄（包含手機位址），故警察再向檢察官聲請向電信事業調取相關資訊進行調查，之後被告被判處 2 年 4 個月之有期徒刑。被告不服，主張發送無聲簡訊並無相關法律依據而提起上訴主張救濟[81]。

第三項　判決要旨

第一款　第 100a 條連結偵查概括條款非授權基礎

檢察總長主張使用靜默簡訊之授權基礎來自於第 100a 條連結第 161 條第 1 項第 1 句、第 163 條第 1 項的偵查概括條款，然而聯邦最高法院否決此一見解，而再重申先前判決所劃定的標準，即雖秘密通訊自由的保障範圍不僅包括通訊內容，也包含通訊之緊密情狀，通訊係指透過非實體之媒介將訊息傳遞予「個人」，然而靜默簡訊即缺乏此種個人之間資訊交換的性質，僅為機器之間的交流，無法推測出存在的通訊關係或內容。再者，第 100a 條的法條文字使用「監聽與紀錄」而取得已經存在之通訊內容，然而靜默簡訊是偵查機關主動發送簡訊生成新資訊，已逾越文意範圍，應有另外授權基礎，且因透過靜默簡訊，可能生成個人大致的行動軌跡，已影響個人資訊自決權甚鉅（基本法第 2 條第 1 項連結第 1 條第 1 項），不可以偵查概括條款為之[82]。

---

[79] Eisenberg/Singelnstein, (Fn. 74), S. 67; Smith, Kurzer Zwischenstand zu Recht und Praxis der „stillen SMS“, VR 2012, 334, 335f.

[80] BGH, Beschl. v. 8.2.2018 − 3 StR 400/17= BGHSt 63, 82。

[81] 王士帆，前揭註 77， 頁 2-3。

[82] BGHSt 63, 82 (Rn. 5-6).

doi:10.6342/NTU202302425

第二款　第 100h 條第 1 項第 1 句第 2 款非授權基礎

第 100h 條第 1 項第 1 句第 2 款允許於住宅外使用其他特別為監視目的所設計之科技方法，然聯邦最高法院亦否決本款做為授權基礎，原因在於：與同項第 1 款相較，本款的「其他科技方法」應理解為非製作影音紀錄，亦非紀錄住宅內外之非公開談話，而係以監視為目的，而欲判別是否為本款所稱之以監視目的之其他科技方法，須視其實際使用情境而定，本案的靜默簡訊是符合此其他科技設備的前提。

然而，第 100h 條第 1 項第 1 句第 2 款的前提限制於「住宅外」使用，區分取得住宅外之標準為應取得資料之狀況，而靜默簡訊取得之資訊狀態範圍（住宅內外），繫諸於個人自己攜帶手機到何地，非屬偵查機關所可控制，且使用靜默簡訊目的也不是為了觀察個人私人空間發生之活動，應不涉及基本法第 13 條住宅權之保障範圍，因基本法第 13 條是一種對個人空間的保護，並不是一種概括、不問獲取型態之保障[83]。

第三款　第 100i 條第 1 項第 2 款為發送靜默簡訊之授權基礎

由上述分析，第 100h 條第 1 項第 1 句第 2 款或許可以作為授權基礎，然而第 100i 條第 1 項第 2 款應構成此條之特別規定而優先適用。第 100i 條第 1 項第 2 款係用於找尋被告之行動裝置位址，2002 年立法制定時雖然是以 IMSI-Catcher 此特定技術為參考，然而文字上保留未來可能出現不同科技手段之「科技開放性」，並未侵害授權明確性之要求，因已明確其範圍限定於「調查行動通訊設備位置作為使用科技方法」[84]。

2002 年立法時，雖僅能於因執行押票或監護安置票而需要暫時拘捕行為人，才能適用第 100i 條第 1 項第 2 款調查被告被告手機位址，然而於 2007 年修法時此前提已為刪除，立法者指出只要需要事實調查所必要即可，當然可用於準備調

[83] BGHSt 63, 82 (Rn. 7-9).
[84] BGHSt 63, 82 (Rn. 11-13).

doi:10.6342/NTU202302425

取第 100g 條之通信紀錄而使用。故靜默簡訊之發送授權基礎為第 100i 條第 1 項第 2 款，後續再依照第 100g 條第 1 項第 1 句第、第 3 句連結電信法第 96 條第 1 項第 1 句第 1 款和第 5 款，或依第 100g 條第 2 項連結電信法第 113b 條第 4 項調取通信紀錄[85]。

第四項　判決相關討論

聯邦最高法院判決確立授權基礎之後，學界討論的聲音並未止息，出現多篇判決評析與討論，綜觀其內容，首先對於發送靜默簡訊涉及之基本權部分，肯定聯邦最高法院之見解，即以發送靜默簡訊確定手機位址非屬基本法第 10 條的保護範圍，因追訴機關發送靜默簡訊並不意味著進入（干預）了一個已經存在的、享有保密保護的通訊過程，而是實際上是一種強加的做法，由警方主動生成這種「通訊」，基本法第 10 條並不保護這種「強加」通信過程，即無法保障國家不與私人發生通訊關係，而只對有意識發生的通訊內容和詳細情況提供保密保護[86]。

在授權基礎之部分，大多肯定聯邦最高法院拒絕以第 100a 條、第 100g 條與第 161 條為授權基礎之論點，前者係因靜默簡訊並非於具體發生之通訊關係中產生，且第 100a、100g 條之授權方式不涵蓋主動製造資訊；後者係因使用靜默簡訊作為偵查手段對基本權侵害甚鉅，整個過程皆為秘密進行而為當事人所不知，雖然行動裝置本身即會因技術原因自動向基地台註冊而生成位置資訊，而電信事業可以透過電信法第 96 條儲存並為國家所調取，然而國家透過主動不斷發送靜默簡訊可以更精確確定被告位置，也可以進一步建立移動圖像，侵害性質更類似於電信法第 176 條命電信事業強制儲存通信紀錄[87]，由長時間發送靜默簡訊可能產生被告之移動圖像，可能推測出被告之生活慣習，嚴重侵害資訊自決權，與普

[85] BGHSt 63, 82 (Rn. 14).
[86] Hauck, (Fn. 5), §100i Rn.20; Farthofer, Der Einsatz neuer Ermittlungsmaßnahmen Das Beispiel stille SMS, ZIS 2020, 190, 191; Rückert, „Stille SMS“, NStZ 2018, 611, 613.
[87] Rückert, (Fn. 86), S. 613.

doi:10.6342/NTU202302425

遍認為偵查概括條款所可以授權之干預程度相距甚遠，故不得以偵查概括條款為之[88]。

然而，聯邦最高法院仍有部分論點並無解決學界質疑之聲浪，文獻上提出的論點主要為：

第一款　以第 100i 第 1 項第 2 款作為發送靜默簡訊之疑義

聯邦最高法院認為第 100i 條第 1 項第 2 款應為第 100h 條第 1 項第 1 句第 2 款的特別規定而應優先適用，此論點容有疑問，因發送靜默簡訊確實可以達到將被告手機轉為為監視目的所設之科技設備，符合第 100h 條的條文內容，然而，聯邦最高法院以刑事訴訟法第 100i 條的技術開放性和立法歷史等理由證明其為發送靜默簡訊之基礎，反而不甚合理，因即便解釋第 100i 條的措辭並不要求使用某些特定技術手段，2007 年第 100i 條的修法時立法者於立法理由明確指出，「（第 100i 條修法）允許使用 『IMSI-Catcher』來進行監視措施與根據第 100g 條收集通信紀錄做準備」，也就是說，立法機關並不想在這次修法中對靜默簡訊進行規範，甚至於同一次修法文件中將其形容為「有法律爭議」（rechtlich umstrittene）的措施，並透過該次對第 100g 條修法，因刪除調取位址資訊須有建立連接之前提，故可直接調取待機中手機之位址資訊，將靜默簡訊認定為可有可無的（entbehrlich）措施，故第 100i 條顯然是為 IMSI-Catcher 量身定做，也就是手機位址須要由技術手段「直接」確定，發送靜默簡訊只有確保手機將其位置傳達給電信事業，尚須透過查詢相應的數據才能確定位置。簡言之，第 100i 條應解釋為能夠直接確定位置而無需對電信事業採取任何進一步調查措施的科技手段[89]。

針對上述的質疑，亦有文獻反駁：發送靜默簡訊可以達到將被告手機轉為為監視目的所設之科技設備的功能，雖符合第 100h 條的條文內容，然而第 100i 第 1 項第 2 款是特別為確定手機位址所制定之立法，屬於更具體的規範而應適用，

[88] Bär, BGH: Verwertung von mittels „stiller SMS“ erlangten Standortdaten, MMR 2018, 824, 827; Puschke, BGH: Verwertung von durch „stille SMS“ erlangten Standortdaten, NJW 2018, 2809, 2811-2812; Rückert, (Fn. 86), S. 614.
[89] Rückert, (Fn. 86), S. 613.

doi:10.6342/NTU202302425

此行為並未超出立法者特別使用的以保留科技開放性的條文內容「科技方法」範圍，且立法者係於立法理由允許以第 100i 條之措施已準備依據第 100g 條調取通信紀錄；再者，第 100i 條未限縮為須直接確認被告行動裝置位置，應允許間接透過電信事業確定，此時數據主體亦有獲得額外對通信紀錄的保障，因需要符合調取通信紀錄額外的第 100g 條法律依據才可以查詢資料，且至少保證發送與調取前後二行為之授權強度相同[90]；最後，從被告的角度而言亦是值得贊同的，因為第 100i 條係採相對法官保留而比第 100h 條可由檢察官自行決定更為嚴格[91]。

第二款　以第 100g 條第 2 項連結電信法第 113b 條第 4 項調取通信紀錄之必要性

有文獻指出，雖以第 100g 條為調取通信紀錄而非發送靜默簡訊之基礎，係正確認識第 100g 條無法涵蓋主動生成資訊，然而聯邦最高法院所引用的規範鏈是有疑問的，從實務之角度，發送通信紀錄通常是為調查被告「實時」之位址，亦即「發送簡訊」與「調取通信紀錄」是同時進行，很難想像以第 100g 條第 2 項連結電信法第 113b 條第 4 項之實際應用，況且第 100g 條第 2 項干預門檻較第 100g 條第 1 項實時查詢更為嚴格[92]。

第三款　以不同授權基礎為組合之疑義

為了達成透過靜默簡訊得知被告位置之目的，發送簡訊與調取通信紀錄兩步驟是彼此依附而無法分離的，拆分為兩階段並分別給予授權基礎，似乎會有悖於刑事訴訟體系中基本權干預規範的明確性原則，聯邦最高法院本身亦早在 2007 年有關線上搜索的判決就曾指出，不可將干預行為的個別要素結合起來以創造法律授權基礎，這會違背基本法第 20 條第 3 款之基本權干預的法律保留原則，然而聯邦最高法院關於使用靜默簡訊的判決並沒有處解釋這個爭議，而已遠超過科

[90] Puschke, (Fn. 88), S. 2811.
[91] Ruppert, Rechtsgrundlage für das Versenden sogenannter »stiller SMS«, JR 2019, 297, 300; Bär, (Fn. 88), S. 824.
[92] Ruppert, (Fn. 91), S. 301.

doi:10.6342/NTU202302425

技開放性之解釋範圍，而可能於後續引發無限多種授權基礎組合，使人民無法預期授權基礎之種類[93]。

[93] Farthofer, (Fn. 86), S. 195.

doi:10.6342/NTU202302425

第四章　我國調取通信紀錄規定

第一節　調取通信紀錄之立法發展

我國實務上亦會利用調取通信紀錄進行偵查，其中以取得手機通訊之位置資訊為例，追訴機關可以藉此分析嫌疑人在場與否，例如某案案發地點於台北市，但是手機基地台顯示於新竹市，除非手機為他人使用，或是雖未位於案發現場之基地台範圍內但相距不遠且相距時間短，則可能是剛離開犯案現場；手機位址亦可用於分析受監察人之生活作息、亦可分析住居所範圍，例如以夜間或清晨使用之基地台則可能可以推論其住居所地點，透過這些推論與經驗法則，可為我國重要之偵查工具之一[1]。

我國於 1999 年 7 月 14 日公布並施行通訊保障及監察法，當時僅有規定對通訊「內容」之監察，而忽略對於通訊之緊密情狀（通信紀錄）之規範，即便於 2007 年通保法為有關通訊監察之大幅修正或是釋字第 631 號解釋公布均未改變此狀況，甚至釋字第 631 號已明確說明：「通訊之有無、對象、時間、方式」亦屬憲法第 12 條秘密通訊自由的保障範圍，國家欲進行限制，需有法律依據且符合比例原則方可為之[2]。

除了立法怠惰以外，實務上為學者所詬病的是，判決多缺乏對調取通信紀錄授權基礎、證據能力之討論，即便有判決對此為分析，亦認為：彼時之通保法之相關規定，均係針對通訊內容監察，沒有對通信紀錄調取之規定，而需探求其他法律授權基礎，而電信法第 7 條第 2 項授權電信總局所頒布之當時之電信事業處理有關機關查詢電信通信紀錄實施辦法第 3 條規定：「有關機關查詢通信紀錄應先考量其必要性、合理性及比例相當原則，並應符合相關法律程序後，再備正式公文或附上電信通信紀錄查詢單（格式如附件），載明需查詢之電信號碼、通信紀錄種類、

[1] 何明洲（2006.09），〈通聯分析在科技偵查上應用之研究〉，《警學叢刊》，37 卷 2 期，頁 16-17。

[2] 林鈺雄（2013.12），〈通訊監察之修法芻議——通訊保障及監察法之部分修正條文一〉，《萬國法律》，192 期，頁 28。

doi:10.6342/NTU202302425

起迄時間、查詢依據或案號、資料用途、連絡人、連絡電話或傳真機號碼、及指定之列帳相關資料等，送該電話用戶所屬電信事業指定之受理單位辦理。」，被認為已符合法律保留原則與比例原則之要求，故不需另為立法規範。

然而，學者認為雖電信法屬於法律層級之規定，後者查詢辦法卻僅屬於命令之位階，若國家限制基本權之行為應以立法院通過而經總統公布施行之「法律」為之，另以實質內容而言，亦不符合規範明確性之要求，亦欠缺相關程序保障規定，例如聲請權人、法官保留規定、調取要件等保障，充其量僅規定電信事業之配合義務。這造成了實務上是由職司追訴犯罪之檢察官或警察為自行控制調取通信紀錄與否或範圍，而不是以客觀且中立之法院為事前或事後審查[3]，難以期待追訴機關會自認其行為不符合比例原則。雖亦有文獻指出或許可以個資法第 15 條第 1 款或是個資法第 16 條為授權基礎，然亦面臨規範密度不足的問題，欠缺有關聲請單位、調取要件與救濟相關規定，難為正當之授權基礎[4]。

2013 年特偵組召開記者會指控立法院院長、法務部部長、高檢署檢察長等涉嫌關說之行為，然而特偵組偵辦利用通訊監察與調取通信紀錄之過程，引起社會大眾極大之批評，以此為修法導火線，最終於 2014 年修訂通保法之規定以杜爭議，除了修訂對於監聽（通訊監察）本身之限制，與本文相關之通信紀錄部分，新增第 3-1 條有關通信紀錄與通訊使用者資料之規定[5]。其中第 1 項通信紀錄定義為：「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。」，其範圍較電信法第 2 條第 8 款更為詳盡[6]，立法理由稱是為保障憲法第十二條人民秘密通訊自由並落實司法院大法官會議第 631 號解釋意旨，而將通信紀錄納入通訊監察法制範圍，總算對釋字與學說呼籲保障秘密通訊自由之聲音做出回應以落實法律保留原則。

---

[3] 林鈺雄（2014.01），〈通聯紀錄之調取－－從幾則基地台相關判決談起〉，《台灣法學雜誌》，239 期，頁 52-60。

[4] 陳重言（2014.07），〈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》，16 期，頁 44。

[5] 陳重言，前揭註 4， 頁 41。

[6] 陳重言，前揭註 4， 頁 41。

doi:10.6342/NTU202302425

調取這些資料係採「非微罪原則」，限制於三年以上有期徒刑之罪才可調取，偵查中係由檢察官或是司法警察官報請檢察官許可，向該管法院聲請調取票，然符合特定重罪或是緊急急迫情況，則可由檢警自行發動，然而後者須向法院補聲請調取票（通保法第 11-1 條），然而因修法過程倉促，故直至今日仍引起不少學說相關批評。本章將以調取手機位址（基地台位址）此目的出發，檢視現行通保法之規定是否符合憲法上之要求，並輔以學說實務為分析。

第二節　調取通信紀錄涉及之基本權

我國釋字第 631 號說明：憲法 12 條秘密通訊自由保障範圍不僅止於保護遠距通訊內容，更及於可以分析出通訊關係甚至是內容的通訊緊密情狀，包含是否、與誰、多常、在哪裡進行通訊等資訊，亦說明針對通訊內容之監察須遵守一定憲法上之原則，例如：法律保留原則、法官保留原則與比例原則等限制。國家要求私人之電信事業有協力義務提供其所生成之通信紀錄以得知通訊緊密情狀，雖按照釋字第 631 號之意旨屬於干預行為，但未必須完全受到與通訊內容監察之相同保障[7]。另最高法院 106 年台非 259 號判決為因應遠距通訊容易受第三者（包含國家）之特性而補充秘密通訊自由是針對「實時進行」之通訊為保護。然有文獻主張，對於「通信紀錄」之保護應予以延伸，意指即便通訊結束亦受秘密通訊自由之保護，係為避免國家於通訊後任意調取其通信紀錄而用以分析人民之通訊關係與生活慣習[8]。

另外，雖然因通信紀錄可得識別出個人之身分故屬於個人資料，故國家調取之行為亦屬於干預資訊自決權之行為，然而秘密通訊自由與資訊自決權為特別法與普通法之關係，故僅依特別人格權之秘密通訊自由判斷即已足[9]。

第三節　調取通信紀錄相關規定分析

[7] 溫祖德（2021.12），〈偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查－從美國聯邦最高法院判決檢視我國法制〉，《政大法學評論》，167 期，頁 242。
[8] 詹鎮榮（2003.09），〈秘密通訊自由〉，《法學講座》，21 期，頁 5-6。
[9] 許宗力（2003.09），〈基本權利：第六講—基本權的保障與限制（上）〉，《月旦法學教室》，11 期，頁 68。

doi:10.6342/NTU202302425

第一項　發動要件

第一款　發動目的

2014 年通保法修法之後，因通保法限制為追訴 3 年以上有期徒刑之案件才可以調取通信紀錄，故自文意與整體脈絡解釋，通保法僅能為「追訴犯罪」之目的而發動，故有部分文獻就此批評為了找尋失蹤或是自殺人口、救災行為等皆無法據此調取通信紀錄，故應於通保法再為修正，新增為維護治安等目的而允許調取通信紀錄[10]，法務部之新聞稿亦認為，通保法規定嚴格限制追訴機關調取通信紀錄，卻又對行政機關調取通信紀錄廣開大門，這個狀況十分矛盾，而有修正通保法之必要[11]。然本文認為防止現實（或未來）之危險畢竟與追訴過去發生之犯罪性質迥異，前者較後者可能更重視時效性，是否適合規定於相同法典而適用相同授權基礎仍有疑問，故仍應將通保法調取通信紀錄之規定保留於追訴犯罪之目的，亦有文獻支持此看法，認為通保法並非調取通信紀錄行為之「專屬規定」，即便存在通保法亦不妨礙其他法領域新增調取通信紀錄之規定，或許可以個資法第 15 條第 1 款結合如警察職權行使法第 28 條第 1 項、精神衛生法第 33 條第 2 項、行政執行法第 36 條、消防法第 16 條、社會救助法第 26 條等規定作為授權基礎，但此類規範亦可能有授權密度不足之問題[12]，然其亦非通保法需新增「為防止現實（或未來）之危險」目的之理由，應各自交由相關法規主管機關等討論修法方向。警政署於 2019 年電信管理法之立法過程中曾呼籲於該法第 9 條新增「依法執行與公眾生命、身體、健康或財產安全有關之機構」且為「急難救助」的目的即可調取通信紀錄之規定，然而因反彈過大而並未成功[13]。

---

[10] 林豐裕、李欣倫、李鎮宇（2014.07），〈簡評 2014 年通訊保障及監察法增修條文－－兼論新法對於實務運作之衝擊〉，《檢察新論》，16 期，頁 66、 69。相同見解見：黃朝義（2014.04），〈通聯記錄調取與另案監聽修法評析〉，《中央警察大學法學論集》，26 期，頁 8。

[11] 法務部（2014.07.25），《救災救難不能陷入觸法爭議》，載於：https://www.moj.gov.tw/2204/2795/2796/56926/（最後瀏覽日：2021.10.02）。

[12] 陳重言，前揭註 4， 頁 44-45。

[13] 自由時報（2019.03.19），〈電信管理法修法 NCC：加入網路通訊符合科技發展〉，https://news.ltn.com.tw/news/life/breakingnews/2731925（最後瀏覽日：2021.10.02）。

doi:10.6342/NTU202302425

第二款　非輕罪原則、必要與關聯性原則

通保法第 11-1 條直接規定須為追訴最重本刑 3 年以上有期徒刑之罪，且於本案之偵查有必要性及關連性時方可調取通信紀錄（非輕罪原則、必要與關聯性原則），2014 年立法時條文為經協商通過，所以無法得知特別限定「最重本刑 3 年以上有期徒刑之罪」之理由，僅能自部分提案立委之理由可大約推估係特別為排除「通姦、妨礙名譽」之輕罪所設。

實務與學說皆批評此立法之不妥，認為設立年以上之門檻並沒有通盤考慮到刑事訴訟強制處分整體體系，例如於刑事訴訟法之搜索扣押之要件即無類似之罪刑門檻，僅因立法者認為調取通信紀錄較通訊監察干預程度較低而作出此設計[14]。並且此門檻本身過於嚴格，反而延滯犯罪追訴之效率，硬性規定一定罪刑門檻，反而忽略可能個案情節輕重之問題，而不符合比例原則之要求，並且忽略調取通信紀錄對於追訴特定犯罪具有實益，但因該非輕罪之門檻，只要低於 3 年有期徒刑之門檻反而一律不能調取，具體例如：刑法第 235 條散布猥褻物品罪、刑法第 251 條第 3 項散布不實影響民生必需物品價格資訊罪、刑法第 310 條第 2 項加重誹謗罪、刑法第 318-1 條洩漏電腦秘密罪等，此類犯罪皆因罪刑門檻未達第 11-1 條之要求，然調取通信紀錄可知例如被告於案發當時是否真的有使用網路（IP 位址等），對於澄清是否犯此類犯罪十分具有助益[15]。

另外第 11-1 條第 3 項有規定「最輕本刑十年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪防制條例等罪」之情形，適用不同之程序規定，立法當時係為緩和新法可能造成之偵查效率延滯的問題，故執法機關主張新增例外條款，提出以最輕本刑 10 年以上之罪以及先前核准通訊監察案件之案件類型，取其較多之類型為參考，然而貪污治罪條例與公職人員選舉罷免法因較為敏感而

[14] 鄭逸哲、黃沛文（2014.09），〈動機雖屬正當，立法未免粗糙──簡評通保法關於「調取行為」之修正〉，《月旦法學雜誌》，232 期，頁 23。
[15] 陳重言，前揭註 4， 頁 52-53。

doi:10.6342/NTU202302425

為立法者所剔除，而成為現行之條文，以犯罪類型作為區分程序規定之標準為我國「獨樹一格」之立法[16]。此項學者認為亦應同時解釋為輕罪原則之例外（實體要件），因上述之法案中有部分的罪名未達到非輕罪原則之門檻 3 年以上有期徒刑，故亦應一併解釋為實體與程序要件之例外，避免造成體系之矛盾[17]。

第二項　調取客體

2014 年修法時，立法者規定依據第 11-1 條，檢察官或是司法警察官於符合一定要件之情況下，可調取通信紀錄或是通訊使用者資料，將通信紀錄與通訊使用者資料為並列規定，甚至於第 3 項規定符合一定重罪可不經法官同意即調取「通信紀錄」，而未規定「通訊使用者資料」，因同為協商通過之條文，而無法得知立法者之真意，即便案件符合第 3 項之重罪，文意上亦無法調取通訊使用者資料，看似會造成調取通訊使用者資料之門檻較調取通信紀錄門檻更高。

然學者有批評此立法設計本身即大有問題，認為前者干涉憲法第 12 條所保障之秘密通訊自由，後者僅干預第 22 條保障之資訊自決權，應為不同之授權基礎[18]，甚至有主張後者因屬於個人身分之基本資料，為個人與電信事業簽定服務契約當時即自願交出之靜態資訊如姓名地址等[19]，其內容並不會因為單次之通訊行為而改變，也無法顯示單次通訊內容，遑論推測出個人之生活相關圖像，故非屬秘密通訊自由之保障範圍[20]，相較於部分較為敏感之通信紀錄（例如可推測出個人生活型態之位址資訊、可知道個人互動交往對象之通信對象資訊）不需為法官保留[21]或甚至有主張其屬於任意偵查之範圍[22]，亦有文獻直接認為依照舉輕以明重之法理，因個人對通訊使用者資料具有較低之隱私期待，故檢察官或司法警察官等於符合第 11-

[16] 何信慶（2014.07），〈從立法審議過程談新修正通訊保障及監察法〉，《司法新聲》，111 期，頁 42。
[17] 陳重言，前揭註 4， 頁 54。相反見解見：何信慶，前揭註 20， 頁 44。
[18] 陳重言，前揭註 4， 頁 50。
[19] 黃朝義，前揭註 10， 頁 15。
[20] 鄭逸哲、黃沛文，前揭註 14，頁 22。
[21] 李榮耕（2010.06），〈論偵查機關對通信紀錄的調取〉，《政大法學評論》，115 期，頁 140-141。
[22] 黃朝義，前揭註 10，頁 15-16。

doi:10.6342/NTU202302425

1 條第 3 項之重罪時，可自行調取「通訊使用者資料」[23]。自德國刑事訴訟法觀察亦可得出應分開規定之結論，調取通信紀錄係規定於第 100g 條，調取用戶主資料（Bestandsdatenauskunft）則規定於第 100j 條，兩者之授權門檻亦不同，後者偵查輔助人員（Ermittlungspersonen）甚至可於急迫情況下發動，本文認為，有鑒於通信紀錄與通訊使用者資料係干預不同基本權，兩者應為層級化規定並區別對待，故本文後續提及第 11-1 條皆僅論述通信紀錄之部分。

第一款　通信紀錄之儲存規定

第一目　2019 年電信管理法立法前

我國對通信紀錄最早之定義見於 91 年交通部電信總局修訂之電信事業處理有關機關查詢電信通信紀錄實施辦法，規定「指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可予提供者為原則」，接著 94 年電信法第 2 條第 8 款亦規定通信紀錄之規定，通信紀錄指「電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則。電信號碼係指電話號碼或用戶識別碼」，而後 103 年通保法修法於第 3-1 條第 1 項再定義何謂通信紀錄，即追訴機關所可以調取之資訊範圍，包括「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」，文意上大致相同[24]，其中即包括本文所討論之電信使用人使用電信服務後，電信事業所產生之位置資訊（基地台資訊）。

然為調取通信紀錄以追訴犯罪，必先有相關「儲存」通信紀錄之規定，然以上之規定均非通信紀錄之「儲存」規定。因我國目前調取之通信紀錄係來自電信事業，這些私人經營之電信業者儲存這些通信紀錄是為了計算費率之商業需求，故會搭

[23] 何信慶，前揭註 16，頁 43-44。
[24] 林容（2021.03），《隱密科技偵查與基本權保障》，頁 139，臺灣大學法律學研究所碩士論文。

doi:10.6342/NTU202302425

配用戶之基本資料以進行識別，這些片段的資訊可以透露連結出有關個人橫跨時間與空間之一切資訊，若國家命令儲存這些極度個人化可以透露私生活之資訊留待後續使用，會對個人私人生活經營或發展自主人格造成極大的威脅，只要儲存期間尚未屆滿而未經刪除，這些海量的解讀力極高之資訊即掌握於第三人手上，而如同「不定時炸彈」[25]。

然而，通保法本身第 14 條第 2 項要求「電信事業及郵政事業有協助執行『通訊監察』之義務」，但此條文於 2007 年修正後再無更動，而 2014 才新增調取通信紀錄之授權基礎，除了從立法沿革難解釋為儲存通信紀錄之授權規範[26]，通保法法條內使用「通訊監察」之文字也大多指向針對通訊內容之監察[27]，而通保法施行細則亦不見相關規定[28]。

此時通信紀錄之儲存規定係於電信法第 14 條第 6 項（第一類電信）與第 16 條第 9 項（第二類電信）所授權之子法內，包括[29]：行動通信業務管理規則第 72-1 條、行動寬頻業務管理規則第 76 條、固定通信業務管理規則第 49-1 條、第三代行動通信業務管理規則第 76 條、無線寬頻接取業務管理規則第 74 條、一九００兆赫數位式低功率無線電話業務管理規則第 58-1 條、電信事業網路互連管理辦法第 25 條等，然而回到電信法第 14 條與第 16 條本身之授權範圍似乎不包含通信紀錄之「儲存」，是否符合授權明確性仍有爭議，顯見我國法律並未認知到通信紀錄之「儲存」與「調取」分屬不同階段，而僅集中資料調取之階段，然因儲存之資料本身具有極大之資訊解讀力，且有被濫用之風險，故儲存行為本身即應符合一定資料安全要求，然目前僅能仰賴各電信事業與人民簽訂之服務契約為約定，而有違反憲法第 23 條

[25] 唐欣悅（2018），《私人通信紀錄強制供公益目的使用之合憲性研究》，頁 29-30，臺灣大學法律學研究所碩士論文。
[26] 唐欣悅，前揭註 25， 頁 105-106。
[27] 例如區別通保法第 11 條「通訊監察書」與第 11-1 條之「調取票」之用語。
[28] 唐欣悅，前揭註 25， 頁 105。
[29] 相關法條整理：蔡宗珍（2018.02）， 〈電信相關資料之存取與利用的基本權關連性（下）－德國聯邦憲法法院 BVerfGE 125, 260 與 BVerfGE 130, 151 判決評析〉，《月旦法學雜誌》，275 期，頁 80-81。

doi:10.6342/NTU202302425

之疑義[30]，並且即便電信事業與個人簽訂可以儲存通信紀錄之條款，通常目的亦係為計算費率之用，客戶並無同意追訴機關向電信事業調取為追訴犯罪之用[31]。綜上之分析，我國此時缺乏如同德國電信與電子媒體資料與隱私保護法第 9 條與第 12 條（甚至是電信法第 176 條）有關通信紀錄之明確包含儲存目的、儲存範圍與保存期限之「法律」規範[32]。

第二目　2019 年電信管理法立法後

我國目前適用之電信法是自 1958 年起施行，然為跟上不斷變化之數位媒體與多元通訊服務之發展，同時為了符合國際發展趨勢，故於 2019 年 5 月 31 日經立法院三讀通過並於 2020 年 7 月 1 日起正式施行電信管理法，目前電信法所規定之一類電信中，台灣人最常使用之中華電信、台灣大哥大與遠傳電信等，均已於 2020 年底前完成身分之轉換，轉至電信管理法管理[33]。

其中與通信紀錄儲存相關之規定於第 9 條，包括第 1 項儲存應通信紀錄予用戶查詢、第 2 項儲存通信紀錄之範圍、第 3 項授權主管機關另訂相關事項之部分與第 4 項電信事業具有配合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。然細究第 9 條之內容，本條僅規定提供「用戶」調取通信紀錄而允許「儲存」之規定，這可自立法理由得到印證：「一、為確保用戶查詢通信紀錄及帳務紀錄之權利，爰第一項明定電信事業對用戶使用電信服務所生通信紀錄及帳務紀錄，應確保紀錄正確，並保存一定期間及保障其秘密之義務；該電信事業提供予用戶之電信服務，因該電信服務所得產生之通信紀錄及帳務紀錄，應提供用戶查詢……三、就通信紀錄與帳務紀錄之保存期間、查詢作業程序、收費方式及其他相關事項，授權主管機關另訂定辦法，爰訂定第三項。四、依通訊保障及監察法等規定，電信事業有協助執行通訊監察、調取通信紀錄及通

[30] 蔡宗珍，前揭註 29， 頁 81。
[31] 唐欣悅，前揭註 25， 頁 106。
[32] 林容，前揭註 24， 頁 140。
[33] 財團法人台灣經濟研究院（2021），《109 年通訊市場調查結果報告》，頁 37-38，載於：ttps://www.ncc.gov.tw/chinese/files/21021/5190_45724_210217_2.pdf。

doi:10.6342/NTU202302425

訊使用者資料之義務。故協助執行通訊監察、調取通信紀錄及通訊使用者資料亦為電信事業之經營義務之一，爰訂定第四項」[34]，仍不同德國刑事訴訟法第 100g 條第 1 項與第 2 項直接明確說明調取之資料儲存依據分別為何。

第二款　通保法第 3-1 條之解釋

通保法第 3-1 條第 1 項規定涵蓋可以調取之通信紀錄範圍，包括本文所討論之位址資訊，我國目前調取所有通信紀錄種類，無論是通訊是否進行通訊、雙方之號碼、通訊時間或位址等，皆適用相同之授權基礎門檻，並無如同德國刑事訴訟法明確區別第 100g 條第 1 項第 1 句（調取位址資訊以外之通信紀錄）、第 100g 條第 1 項第 4 款（調取實時或未來之位址資訊）以及第 100g 條第 2 項（調取儲存之過去位址資訊），並異其授權門檻。首先是比較「位址資訊以外之通信紀錄」與「位址資訊」，德國立法當時是因認為後者具有建立個人移動圖像之潛力，具有了解甚至是預測個人生活行為可能，故其授權門檻較前者更高。手機位址本身又可再分為「實時或向未來位址資訊」或是「過去位址資訊」，德國因認為儲存資料庫更難以預測其侵害資料範圍後者干預基本權程度較為嚴重而給予較嚴格之授權基礎標準（需為一定目錄犯罪且採絕對法官保留）。相較於德國之刑事訴訟法規定，我國通保法立法密度較為不足[35]。

除了立法層級化與密度不足之問題，目前通保法通信紀錄內所指之「位址」究竟應解釋為取得「實時或向未來」或是「過去儲存」？因欠缺如同德國刑事訴訟法實時（Echtzeit）或是過去儲存（gespeicherter）等語，故解釋上迭生爭議。

查詢我國目前之法院判決，有部分判決認為通保法第 11-1 條可以調取儲存之過去位址資訊[36]，例如新竹地方法院 111 年度金訴字第 98 號判決，法院調閱兩名被告使用之通信紀錄資訊判斷，兩名被告常在同時間使用位址相同或類似之基地

[34] 唐欣悅，前揭註 25， 頁 122-123。
[35] 林鈺雄（2021.02），〈科技偵查概論（上）──干預屬性及授權基礎〉，《月旦法學教室》，220 期，頁 53。
[36] 陳重言，前揭註 4， 頁 45。

doi:10.6342/NTU202302425

台，彼此之間非素昧平生而有交誼，而有共同為詐欺行為之可能，排除其互不認識之主張；士林地方法院 106 年度訴字第 183 號判決則是法院藉由調閱之行動電話之雙向通聯紀錄以判斷被告當時位於案發現場而有涉案之可能；高等法院高雄分院 97 年度上更(二)字第 44 號判決，辯護人亦主動請求調取 94 年之通信紀錄與基地台位址以證明被告案發當時非位於案發現場，雖法院後拒絕辯護人之請求，但拒絕之理由在於電信事業僅保留 6 個月內通信紀錄。然而也有判決認為可依本條取得實時或未來之位址資訊，例如進行通保法第 5 條等即時之通訊內容之監察時（現譯台之情形），可以取得受監察人正常通話、未接通話與無通話所使用之行動電話基地台地址與方向角[37]，判決所附之監聽譯文亦會有使用之通訊基地台資訊，實務上之運用以高等法院 104 年度上訴字第 1912 號判決為例，該案為現譯台掌握被告等人之手機基地台位址，確認被告等人已到某地接應毒品，通知司法警察利用此資訊到現場為逕行拘提並扣押相關證據，但以上提及之判決皆無特別指出「調取儲存之過去位址資訊」或是「調取實時或未來之位址資訊」這個區分。桃園地方法院 106 年度易字第 164 號判決首度對此問題作出回應，認為通保法第 11-1 條的規定是取得目標對象所在之「歷史基地台紀錄」，而與 IMSI-Catcher 可以取得「實時」之手機位址的性質不同，而不能為其法律授權基礎，然此判決並未解釋如此解釋之理由。

第一目　主張通保法第 11-1 條為調取儲存之過去位址資訊

學說亦有支持通保法第 3-1 條僅限於已經發生而儲存之通信紀錄，不包含對於通信紀錄的即時調取，其理由大致可以整理為：以文義而言，通保法第 3-1 條即明確說明：「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」，故解釋上自為使用通訊服務之後，電信事業自動產生之數據，故為調取過去儲存之通信紀錄[38]；且兩者之初始的紀錄目的不同，調取儲存之通信紀錄，

[37] 曾德文（2013.08），《資通科技犯罪偵查. 通訊篇》，頁 196，自刊。
[38] 李榮耕（2020.04），〈居家電子監控於防疫期間之運用及其法源疑義〉，《月旦醫事法報告》，42 期，頁 96。

doi:10.6342/NTU202302425

這些通信紀錄的儲存目的與來源是電信事業為了提供服務計算費用所必要，因此時追訴機關尚未提出調取之請求，然而調取即時通信紀錄，除了是電信事業為商業目的所儲存，尚帶有為追訴機關犯罪偵查的目的；調取即時通訊紀錄有針對特定人，對其進行個人追蹤的性質，有類似 GPS 之即時追蹤效果，調取儲存之通訊紀錄，於儲存當時並無針對特定人之意圖；調取即時之通信資料對個人基本權利侵害較大，個人應對即時調取手機位址有較高之隱私期待，有被追訴機關掌握並尾隨之可能，調取過去通信紀錄僅會取得個人過去之行蹤以及最後出現之位址，而在調取相同時間長的資料而言，例如調取 30 日之實時基地台紀錄以及調取 30 日之儲存過去基地台紀錄，即時調取可能會造成長時間並持續干預用戶基本權之情形，不同於調取過去通信紀錄可能僅有短時間調取一次，如此一來可能會引發寒蟬效應；最後，通保法第 11-1 條未如同通訊監察第 12 條第 1 項、第 2 項規定之監察期限屆至須聲請繼續延長監察等規定可言，故追訴機關可能會無止盡的調取個人即時通信紀錄。就以上之理由，取得即時之位址資訊較取得過去儲存之位址資訊侵害更為嚴重，故其發動門檻或心證門檻皆須更高，應將通保法之規定解釋限縮於調取「過去之通信紀錄」[39]。

第二目　主張文義並未限制

有文獻主張，雖通信紀錄之定義為使用電信服務「後」所產生之之資訊，然依此推論，事實上只要是將手機開機進入待機模式，時時刻刻都在產生各種手機位址資料，故調取實時之手機位址其實亦可被通信紀錄之文意所包含，採限制於調取過去儲存之通信紀錄似乎有過度拘泥於文意之可能，而應直接修法，仿照德國法第 100g 條第 1 項第 4 款與第 2 項為區分而杜絕此爭議[40]。

---

[39] 陳敬于（2018.04），《犯罪偵查中位址資訊之取得及使用》， 頁 162-167，國立臺北大學法律學研究所碩士論文。同見解李榮耕（2015.09），〈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》，44 卷 3 期，頁 934-935；溫祖德，前揭註 11，頁 243。

[40] 林容，前揭註 24， 頁 140。

doi:10.6342/NTU202302425

亦有主張，通保法第 11-1 條規定文意並無限制僅能調取儲存之位址資訊，故兩者皆可直接適用通保法相關規定調取。因調取實時或未來之位址資訊可能是為緊急需求，較可能適用通保法第 11-1 條第 1 項但書之緊急例外，可由檢察官逕行為之，而依據同條第 4 項須事後向法院補行聲請調取票，然而相較於調取儲存之過去位址資訊是針對已發生之事件以釐清特定人是否犯罪，縮小偵查範圍以節省司法資源，追訴機關實時取得手機位址之行為使手機成為一種類似個人貼身之電子追蹤器，故實時取得個人資訊即如同發動對人之搜索，而應比照我國搜索被告之心證門檻，即應要求採取相當理由基準[41]。

第三目　本文見解

首先本文贊同目前通保法調取通信紀錄之規定並無指明為「調取儲存之過去位址資訊」或是「調取實時或未來之位址資訊」之看法，就文義而言事實上無法得出確切之答案，因目前我國調取之通信紀錄，無論是過去或實時之資訊均係來自電信事業為商業目的而自動生成並儲存之資料，邏輯上是必先經由生成資料經由儲存紀錄才可為調取，追訴機關調取實時或向未來通信紀錄僅是經由電信事業生成與追訴機關調取時間相距極短而已，文意上仍屬於使用通信服務「後」所產生之資料。

再者本文亦認同「調取儲存之過去位址資訊」或是「調取實時或未來之位址資訊」干預基本權程度不同這個看法，然而認為調取儲存之過去位址資訊反而有可能造成更為嚴重之基本權侵害。首先自德國刑事訴訟法觀察，其亦區別第 100g 條第 1 項第 4 句與同條第 2 項，認為後者會造成更大的侵害故調高其授權門檻。雖有論點主張與調取儲存之過去通信紀錄相較，調取即時或向未來之通信紀錄包括了電信事業儲存計費之目的，更包括了追訴機關個人追訴犯罪之目的，故有針對個人之特性，而可能造成更大基本權侵害，然而我國目前調取之通信紀錄之紀錄來源是一

[41] 黃政龍（2016），《新型態科技偵查作為之法規範研究》， 頁 290-291，中央警察大學警察政策研究所博士論文。

doi:10.6342/NTU202302425

律由私人所經營之電信事業所儲存處理，追訴機關僅進行聲請調取之行為，亦即電信事業「儲存」通信紀錄之行為是針對「所有」使用通訊服務之人，追訴機關欲「調取」特定通信紀錄之行為，不論是調取過去或是實時之通信紀錄，均有針對「特定人」之特性，故此理由並非區分基本權侵害程度之因素；另一理由即時手機位址具有較高之隱私期待，因有被隨時跟蹤尾隨之可能，相較於取得儲存之位址，僅會得知最後出現之地點，此理由亦應不具說服力，因追訴機關依據通保法為調取通信紀錄時，係已存在具體之犯罪嫌疑，故不論調取資料種類均為調查「過去」之犯罪行為，現實上均可能於後續發動跟蹤尾隨（搜索）之行為，故亦非判斷兩者基本權侵害高低之判準；最後認為調取實時通信紀錄與儲存之過去通信紀錄干預之「次數」不同，故前者之干預較嚴重亦無道理，即便追訴機關僅調取儲存之過去通信紀錄「一次」，亦可能因調取範圍時間跨度極大而使追訴機關能解讀出之生活細節更為詳盡，此處判斷基本權侵害程度之重點是調取之「資訊量多寡」而非調取行為究竟是幾次[42]。

第三項　程序規定

調取通信紀錄相關之程序規定亦位於第 11-1 條。首先第 1、3 項規定管轄的部分：原則上須以書面聲請法院核發調取票，但若有急迫情形不及事先聲請或者前述之部分重罪例外情形，則可例外經檢察官同意後為調取，但前者之情形須向法院補聲請調取票。對於此程序規定，有部分文獻認為失之過苛，司法警察甚至須先報請檢察官許可，方可向法院聲請調取票，冗長之來往的過程可能長達數天即可能錯失良機[43]，甚至有建議應直接增列司法警察亦有緊急權限[44]。

再者是聲請形式之部分：原則上，檢察官聲請時調取通信紀錄時須填具聲請書，聲請書之內容係準用第 11 條第 1 項通訊監察書之內容，而法官允許之調取票應記載事項則列在第 11-1 條第 5 項，故此部分有批評檢察官之聲請書內容應對應法院

[42] 同見解：林鈺雄，前揭註 35，頁 55。
[43] 黃朝義，前揭註 10，頁 7。
[44] 林豐裕、李欣倫、李鎮宇，前揭註 10，頁 69。

doi:10.6342/NTU202302425

所核發之令狀內容，例如檢察官向法院聲請搜索票即需依據搜索票核發之形式內容為之（刑事訴訟法第 128-1 條第 1 項），然而此立法設計是讓檢察官利用監察通訊「內容」之通訊監察書聲請調取得知通訊「情況」之通信紀錄，似乎有所矛盾[45]，事實上有部分立法者提案時意識到兩者之區別，故其提出之草案僅準用第 11 條第 1 項第 1、2、3、5、7、9 款，且於理由說明應僅準用性質相符之部分[46]，然而最後經協商仍修改為直接準用第 11 條第 1 項。目前實務上於檢察機關實施通訊監察應行注意要點第 4 條所附之聲請書格式即有對應調取票之內容，包含「案由」、「應調取之通信紀錄」以及「有效時間（起迄時間）」。另外依據檢察機關實施通訊監察應行注意要點第 5 條，檢察官因急迫情形須指揮司法警察官等調取通信紀錄時，得以口頭指揮或發指揮書之方式為之，惟以口頭指揮後需補發指揮書。依據第 11-1 條第 7 項，立法者將核發調取票定為不公開之程序，此立法與德國刑事訴訟法第 101a 條將調取通信紀錄定為原則應公開為之的程序有所不同。

最後，為落實資訊公開使全民得以監督，2014 年新增第 16-1 條，通訊監察執行機關、監督機關應於每年製作通訊監察相關之統計資料年報上網公開並送立法院備查，第 3 項第 1 款即包含調取通信紀錄。目前公佈之 2021 年之統計資訊，法務部與司法院公佈之統計資訊類別包含聲請人（警察、憲兵機關、檢察官）、罪名、調取類別（第 11-1 條第 1 項或是第 3 項等），並列出准駁（包含部分准駁）之情形，因我國欠缺通信紀錄之執行期限，故不同於德國第 101b 條之報告義務須額外公布聲請延長命令之數量。

2014 年同次修法時，為配合通保法之修正，於刑事訴訟法第 404 條第 1 項第 2 款、第 416 條第 1 項第 1 款得抗告、準抗告之裁定與處分新增「通訊監察」，立法理由稱係為貫徹「有權利即有救濟之原則」，並且明文強調「法院不得以已執行終結而無實益為由駁回」，作為完善保障人民權利之一環。然而有文獻認為，雖然

[45] 李榮耕（2014.04），〈簡評二○一四年新修正的通訊保障及監察法－一次不知所為何來的修法〉，《月旦法學雜誌》，227 期，頁 166。

[46] 立法院公報處（2014），《立法院公報》，103 卷 8 期 4117 號，四冊，頁 444，立法院。

doi:10.6342/NTU202302425

通保法之法案本身即涵蓋調取通信紀錄之意涵，然而以通保法本身之整體之脈絡觀察，「通訊監察」應僅適用於對於通訊「內容」之監察，例如第 11 條使用「通訊監察書」而第 11-1 條使用「調取票」等用語，或是第 16-1 條第 3 項將「通訊監察」與「調取案件」並列，顯示兩者之差異，故調取通信紀錄並無法主張刑事訴訟法第 404 條與第 416 條以為救濟[47]。

第四節　現行規定之缺漏檢討

雖然立法者已於第 3-1、11-1 條規定調取通信紀錄之相關規定，然而因立法過程倉促，其仍有所缺漏而被多數文獻批評，本文將以這些文獻與第二章之德國刑事訴訟法為對照，嘗試找出目前通保法仍有待改善之處：

第一項　明確「儲存」與「調取」客體

過去我國立法者並未意識到「儲存」與「利用」通信紀錄屬於不同之階段而應分為規定，立法者僅集中於資料利用調取之階段立法（通保法），而忽略資料必先經儲存之過程方可使用，對儲存之規定付之闕如而係以授權之行政規則為之，除了有規定本身未必符合授權明確性之疑慮，這些行政規則本身規範密度亦不足夠，雖我國目前無類似於德國電信法第 176 條由國家直接命令電信事業有強制儲存通信紀錄之規定，比對較為類似因商業目的而儲存之電信與電子媒體資料與隱私保護法第 9 條與第 12 條，德國之法律規定即包含儲存目的、可儲存之資料範圍，以及目的達成後必須刪除資料之義務，然而我國這些行政規則僅籠統提及應儲存通信紀錄以及儲存時間，並無刪除之相關義務。而後 2019 年之電信管理法則於第 9 條明定電信事業得儲存通信紀錄之規定，並於授權之電信事業用戶查詢通信紀錄及帳務紀錄作業辦法補充儲存範圍（第 2 條第 2 款）、儲存時間（第 4 條第 2 項）等規定，而補足過去「儲存」通信紀錄規定不足之問題，雖有部分改善，然而仍欠缺儲存目的與刪除相關規定，而目前通保法第 3-1 條或是第 11-1 條本身仍無規定調

[47] 陳重言，前揭註 4， 頁 58。

doi:10.6342/NTU202302425

取資料來源，不同於德國刑事訴訟法第 100g 條指出調取資料來源為何，並無連結整體資料先經「儲存」再由追訴機關聲請「調取利用」之兩個過程，而未來應為修法加以明確。

第二項 通保法調取通信紀錄規定層級化

前已說明我國之通保法第 11-1 條第 1 項將調取通信使用者資料與通信紀錄規定並列規定，且原則上適用相同之授權門檻，然而兩種資料來源與涉及之基本權殊異，干預基本權之程度即有差異，故參考德國刑事訴訟法第 100g 條、第 100j 條之規定應分為授權基礎，並且考慮調取通信紀錄干預秘密通訊自由權而可推測或獲得特定通訊之內容，甚至影響個人之通訊意願，通信使用者資料僅為個人與電信事業簽訂契約時提供之個人如姓名或地址資訊，而無法自個別通訊過程得知當事人社會溝通交往之關係，故亦可考慮此差異而設計不同之授權門檻，取得通信紀錄應較取得通信使用者資料更為嚴格。

再者，我國係將所有通信紀錄一併規定於同一調取規定，包含發送方、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，即是否、與誰、於何時、於何地、以何種方式進行通訊之資訊，然而部分國內文獻已指出並非所有通信紀錄均應適用相同之保護，特別是位址資訊（使用行動通訊設備之基地台位址），因位址資訊相較於其他通信紀錄具有建立個人移動圖像、追蹤預測其行為之能力[48]，以德國第 100g 條第 1 項與第 4 項之要件比較亦可得出相同結論，取得實時位址資訊相較於取得其他通信紀錄更為嚴格，前者不可以僅因經由電信通訊實施犯罪即調取，須為在個案中情節重大之犯罪才可以調取，故通保法亦應同時考慮此差異而為層級化之規範，設計取得位址資訊嚴格於取得其他通信紀錄之規範。

最後調取位址資訊本身，亦可能造成程度不同之干預。技術上追訴機關可調取「過去儲存」或是「實時、向未來」之位址資訊，雖然目前我國實務上以及部分文

[48] 林鈺雄，前揭註 42， 頁 53。

doi:10.6342/NTU202302425

獻傾向將第 11-1 條解釋為調取過去儲存之通信紀錄，因為條文以「電信使用人使用電信服務『後』」之文字，然而因邏輯上必先製造儲存資訊才有調取之可能，故實時之通信紀錄事實上亦為取得使用電信服務「後」之資訊，故無法僅因文字即斷定為取得過去儲存之位址資訊，未來通保法第 11-1 條應明確其文字以杜爭議。應更動第 11-1 條之文字之目的除了是為明確調取範圍以外，更是因為兩者干預基本權程度亦不相同。調取過去儲存之通信紀錄，是追訴機關「海撈」過去之儲存之資訊，因更無法預測其資料庫之範圍，故其侵害較短時間調取之實時通信紀錄侵害更高。

綜上所論，我國通保法第 11-1 條之門檻應調整為層級化之立法，不應一體適用相同規定，依基本權干預之種類分類，干預程度自輕微至嚴重應依序為「通信使用者資料」、「位址資訊以外之通信紀錄」、「實時或向未來之位址資訊」，干預最嚴重為「過去儲存之位址資訊」，並依此順序為不同之保護與授權門檻。

第三項　非輕罪原則

從前述我國通保法目前對於調取通信紀錄與通信使用者資料適用相同門檻，而建議應予以調整，應調整之要件即包含第 11-1 條限定發動要件須為追訴最重本刑三年以上有期徒刑之罪，以及部分重罪可以直接不經法院同意即調取之規定，此「最重本刑 3 年以上有期徒刑之罪」要件本身即應刪除，因以罪名限定發動門檻之立法模式於我國少見，似乎僅見於通訊監察之犯罪目錄（通保法第 5、6 條）與於刑事訴訟法之預防性羈押（刑事訴訟法第 101-1 條），而忽略個案之情節輕重，並完全封鎖未達最重本刑 3 年以上有期徒刑之罪取得通信紀錄之可能，然而取得通信紀錄對於追訴現代大量使用網路通訊之時代具有重要之意義，實務亦肯定其於偵查初期對於澄清被告是否犯罪有所助益，故應予以刪除。

再者，於調整「位址資訊以外之通信紀錄」、「實時或向未來之位址資訊」與「過去儲存之位址資訊」之門檻時，比較德國第 100g 條第 1 項第 1 句（調取位址資訊以外之通信紀錄）、第 100g 條第 1 項第 4 句（調取實時或向未來之位址資訊）

doi:10.6342/NTU202302425

與第 100g 條第 2 項（調取過去儲存之位址資訊），僅有第 100g 條第 2 項因為無理由預先儲存所有人民之通信紀錄，而為避免濫用故聯邦憲法法院於判決令立法者須以明確之犯罪目錄為之，前二者並無此犯罪目錄之限制，而是使用「犯了在在個案中情節重大之犯罪，尤其是第 100a 條第 2 項所稱之犯罪」與「經由電信通訊實施犯罪」為之。

第四項　程序規定缺漏

德國刑事訴訟法將第 100g 條調取通信紀錄之程序規定另立於第 101a 條，我國係一併將其置於通保法第 11-1 條，比較二者規定之內容，我國通保法之內容似乎較為簡陋，以下將針對程序規定分析我國較不足之處：

第一款　發動對象

首先是發動對象之部分：雖我國通保法第 4 條有定義何謂「受監察人」，除了被告亦包含為其發送、傳達、收受通訊或提供通訊器材、處所之人，立法理由稱係參考德國第 100a 條電信監察之規定，而擴大得受監察之範圍，避免被告利用這些人以躲避監察[49]，然以通保法其他規定例如第 15 條之文字，受監察人似乎所指為被監察通訊「內容」之目標人物，而非被調取通信紀錄之人，而第 11-1 條條文本身，似乎對於調查具有必要性及關連性時即可調取，並不限於被告本人，甚至包含任何第三人，然此解釋方式忽略對第三人之保護，有過度侵害第三人之秘密通訊自由而違反比例原則之危險，故有主張或許可以限縮解釋之方式，解釋第 11-1 條第 1 項之條文限定僅能針對被告或是犯罪嫌疑人為之[50]，然而此解釋方式亦有可能有被告利用第三人之行動裝置以躲避調查之可能，故或許直接明確規定可對通保法第 4 條之人調取通信紀錄為宜，德國刑事訴訟法即規定調取通信紀錄之發動對象適用與電信監察相同之發動對象規定（第 100g 條第 1 句連結第 100a 條第 3 項），即被告、訊息傳遞者或是器材提供者。

---

[49] 立法院公報處（1995），《立法院公報》，84 卷 5 期 2762 號，上冊，頁 110，立法院。
[50] 陳重言，前揭註 4， 頁 50-51。

doi:10.6342/NTU202302425

第二款　執行期限

通保法於第 12 條規定通訊監察之實施期限，然而其適用範圍不包含調取通信紀錄，目前與執行期間相關之規定為通保法第 11-1 條第 5 項，規定調取票上需記載有效期間，又檢察機關實施通訊監察應行注意要點第 4 條之調取通信紀錄聲請書亦已有規定須載明起迄時間為限定範圍之方式，而電信法與電信管理法之行政規則本身即有儲存期間，以此為間接之控制，故文獻有認為應明確於通保法規定通信紀錄調取期間作為調取範圍之直接限制[51]。

以本文主張通保法第 11-1 條之文意並無限制僅能取得過去儲存之通信紀錄並應為層級化立法之立場，未來修法應區分為位址資訊以外之通信紀錄、實時位址資訊與過去儲存之位址資訊，以取得實時位址資訊而言，自然同德國刑事訴訟法第 101a 條應設立明確之處分期限，避免無止境之取得被告之位址資訊建立過度詳盡之移動圖像，即便是取得過去儲存之通信紀錄，雖可能有一定儲存期限，然而亦應於聲請與發佈命令時載明可調取之時間範圍，以符合比例原則。

第三款　調取通信紀錄監督機制

因強制處分具有干預基本權利之性質，故法律制度須設計合理之監督制度，使人民得以救濟保障自身權利，亦促使追訴機關合法執行強制處分。監督強制處分又可分為兩種管道，其一為證據使用禁止之規定，另一為強制處分事前與事後之審查機制[52]。

以事先之審查機制即管轄的部分，目前調取所有通信紀錄皆為相對法官保留原則，於急迫情形不及事先聲請或是有部分重罪例外可由檢察官核發調取票，雖釋字第 631 號有指示須採法官保留原則，然此部分係針對對通訊「內容」之監察，調取通信紀錄是否應適用相同標準仍有疑問[53]，甚至有部分文獻認為過度阻礙追訴之

[51] 陳敬于，前揭註 39， 頁 199-200。
[52] 林鈺雄（2020.09），《刑事訴訟法 上冊》，10 版，頁 336-337，新學林。
[53] 張麗卿（2014.06），〈通訊保障及監察法之修正與評析〉，《月旦法學雜誌》，229 期，頁 39。

doi:10.6342/NTU202302425

效率，而應放寬使司法警察亦可於急迫情形不及事先聲請時調取通信紀錄[54]。本文認為，以本文所討論之取得行動裝置位址（無論是實時或是過去儲存）而言，不宜放寬使司法警察亦可調取，因不論是取得行動裝置實時或是過去儲存之位址，皆有建立移動圖像之潛力，已非對於基本權之輕微干預，尤有甚者，長時期、大量儲存人民之位址資訊經之分析使用，具有極強之資訊解讀力而可分析出個人社會與交往關係，具有極大之濫用風險，對照德國刑事訴訟法第 101a 條區分調取過去儲存之通信紀錄採絕對法官保留，調取實時之位址資訊係採相對法官保留原則，雖緊急急迫情況下檢察官亦可發動緊急命令，而亦未放寬偵查輔助人員調取。綜合上述就非輕罪原則之檢討，本文認為就調取通信紀錄而言仍應採取相對法官保留原則，然應刪除立法標準不明之第 11-1 條第 3 項重罪例外之規定，僅規定於急迫情形不及事先聲請時，檢察官可例外先為調取再聲請補發調取票。

事後審查機制不僅可審查事前所發布之原處分是否合法，更可發揮一併審查「執行期間」是否合法之功能，甚至主張刪除相關資訊等，並且因我國目前審查調取票之程序為不公開進行（通保法第 11-1 條第 7 項），故更需要事後審查程序使當事人得以針對處分救濟，目前我國強制處分之事後救濟程序為刑事訴訟法第 404 條與第 416 條之抗告與準抗告規定，雖依前述有文獻認為因此 2 條允許救濟之範圍為「通訊監察」，故調取通信紀錄不可主張抗告或準抗告救濟，而應採合憲性解釋將調取通信紀錄包含進「通訊監察」之範圍[55]。本文認為雖刑事訴訟法第 404 條、第 416 條未必有直接排除調取通信紀錄之意涵，畢竟調取通信紀錄係規定於「通訊保障及監察法」，法規名稱亦無提及調取通信紀錄本身，或許亦可解釋為可進行抗告或準抗告，然而因我國目前抗告與準抗告之規定係為原則上不可救濟，而明文列出可救濟之範圍之立法模式（第 404 條第 1 項、第 416 條第 1 項），而應立法明確說明調取通信紀錄屬於可提起救濟之範圍。

[54] 林豐裕、李欣倫、李鎮宇，前揭註 10，頁 69。
[55] 陳重言，前揭註 4， 頁 58。

doi:10.6342/NTU202302425

第四款　通知之規定

依據第 11-1 條第 7 項，核發調取票之程序採不公開進行，故當事人無法於事前得知追訴機關調取其通信紀錄之審核與實際執行之情形，自然無法對處分核發表示任何意見。通保法雖於第 15 條之有關於通知之規定，然而僅限於對第 5 條、第 6 條等針對通訊內容之監察，雖然於 2014 年同次修法時有針對此條進行修正，然而仍直接排除第 11-1 條調取通信紀錄，因該條文係經協商通過，無法探求立法者排除調取通信紀錄之原因，對當事人而言，若連於執行完畢後亦無法得知調取之事實，更不可能進一步主張相關救濟之權利。與之相較，德國刑事調取通信紀錄雖採原則上應事先聽取當事人意見之立法，然而因實務上通常將調取通信紀錄作為偵查前期之強制處分，為避免打草驚蛇而通常會以避免公開而危及偵查之原因而轉為事前不公開之程序，事後之通知即扮演保護人民受公平審判之角色，故第 101a 條第 6 項亦詳盡規定有關通知之規定，包含通知對象、通知內容、通知期限、延期通知與例外不予通知之規定，我國之通保法第 15 條即與之類似，同樣包含了通知對象、期限、以及延期與例外不予通知之規定，雖仍有部分例如通知內容之未詳盡規定之處，至少目前通保法第 15 條應一體適用於調取通信紀錄。

第五節　基地台查詢？

第一項　我國目前實務發展

我國文獻又有稱為「基地台資料轉儲」[56]或是「基地台通聯紀錄[57]」，即同德國刑事訴訟法第 100g 條第 3 項之基地台查詢規定，於不知道特定被告之身分時，鎖定特定地理區域之基地台以查詢所有特定時間內使用該基地台之相關通信紀錄，以縮小可能之嫌疑人範圍，我國實務稱之為「洗蜂巢」[58]。

---

[56] 黃政龍，前揭註 41，頁 35 。

[57] 邱紹洲（2001），《通聯紀錄在犯罪偵查上之應用》， 頁 12，中央警察大學刑事警察研究所碩士論文。

[58] 黃政龍，前揭註 41，頁 35 。

doi:10.6342/NTU202302425

於我國目前最著名亦明確指出基地台查詢之使用案例即為發生於 2004 年 3 月 19 日之「三一九槍擊案」，不明人士朝時任總統陳水扁與時任副總統呂秀蓮槍擊。為調查不明人士之身份，追訴機關調取了該年 2 月至 4 月台南縣市與高雄縣市之所有通信紀錄（後擴張調取範圍於嘉義、屏東甚至是全國），總共調取了 19789133372 筆通信紀錄[59]。另外以「基地台通聯紀錄」之關鍵字查詢司法院法學資料檢索系統，亦有案件係以案發地點特定電信事業基地台作為調取目標，而非同一般調取通信紀錄是鎖定特定人為之[60]。

然而其適法性曾受質疑，電信事業除非有特殊案情需要也多半不願意協助調取基地台查詢資料，理由有二：其一是因電信事業處理有關機關查詢電信通信紀錄實施辦法第 4 條有關機關必須備正式公文或附上電信通信紀錄查詢單，然而其內容須註明有關「需查詢之電信號碼」，然而基地台查詢無法特定欲查詢之電信號碼，導致電信事業為避免後續糾紛而拒絕提供；再者因我國目前使用行動通訊設備者數量漸長，如果調取尖峰時期基地台所儲存之通信紀錄，其資訊量可能極大而會影響到系統之正常運作[61]。

第二項　使用基地台查詢之法律授權基礎

有見解認為，追訴機關可直接主張通保法第 11-1 條之規定為基地台查詢。因基地台本身具有儲存所有使用該基地台終端設備之通信紀錄，故調取基地台內之資料仍亦符合通保法第 3-1 條第 1 項通信紀錄之定義，追訴機關於填具調取票聲請書時，雖無特定之手機號碼以供電信事業特定，惟可於表格中之「其他欄位」

---

[59] 刑事警察局（2005），《0319 總統、副總統槍擊案專案報告》，頁 125-127，載於 https://web.archive.org/web/20120314123845/http://www.cib.gov.tw/news/0319end_report.aspx。

[60] 參照臺灣高雄地方法院 94 年度重訴字第 118 號刑事判決：「被告丙○○、己○○部分訊據被告丙○○、己○○對於上揭共同擄人勒贖之犯罪事實，均坦承不諱，核與被害人即證人戊○○及證人張蓓蓓證述之情節相符，且有其等待贖款處之遠傳基地台通聯紀錄、安信徵信事業有限公司及一一新安徵信社之華南銀行大昌分行活期存款帳戶存摺封面及內頁影本、內政部警政署刑事警察局 94 年 7 月 8 日刑醫字第 0940100148 號鑑驗書、戊○○93 年 7 月 21 日案發當天行動電話 0000000000 之通聯紀錄、被害人戊○○手繪相關街道圖各 1 紙、93 年 7 月 20 日案發地地下停車場監視錄影帶翻拍照片 3 紙附卷可稽，被告丙○○、己○○之自白與事實相符，堪採為認定事實之證據，本件被告丙○○、己○○共同擄人勒贖之犯罪事實事證明確，被告丙○○、己○○之犯行洵堪認定。」

[61] 邱紹洲，前揭註 57，頁 12。

doi:10.6342/NTU202302425

填寫欲查詢之基地台編號以供判斷。但基地台查詢可能影響大量不特定第三人之權利，侵害程度更為嚴重，故應立法補足相關程序規定（調取期限、資料使用與銷燬等）。

然本文認為，不宜直接以通保法第 11-1 條作為基地台查詢之法律授權基礎。首先，德國刑事訴訟法第 100g 條第 3 項亦是為了因應其與調取通信紀錄特性之不同，且原先於法條並未明確指出「基地台查詢」等語而迭生爭議，故為明確其授權要件方將其獨立出來規定，基於具有會影響大量無關之第三人之特性，要件相較於調取位址資訊以外之通信紀錄更為嚴格，在程序上亦針對其特性於第 101a 條第 1 條第 3 句為不同之命令形式規定，法官僅須於命令中說明一定空間或時間範圍為限定即可。

雖通保法第 11-1 條之文意似乎沒有限制調取之通信紀錄係因「特定手機之方式」或是「特定基地台之方式」取得，然基地台查詢畢竟不同於目前之調取通信紀錄運作實務，無法於調取通信紀錄聲請書上載明特定手機之身分並且特定調取時間，僅能特定區域以縮小範圍，其影響之無關第三人數可能難以估計，且無法條明確規定其命令形式等細節，若位於人口密集之區域影響範圍與程度可能更為嚴重，故應另外制定授權基礎。

doi:10.6342/NTU202302425

第五章　IMSI-Catcher 於我國刑事訴訟法之定位

第一節 緣起：臺灣桃園地方法院 106 年度易字第 164 號判決

在台灣，雖然可以從媒體報導以及實務屆對科技偵查法的呼籲可知，實務上事實上使用 IMSI-Catcher 作為定位被告之偵查工具已久，然以「M 化車」、「M 化偵查網路系統」為關鍵字於司法院法學資料檢索系統搜尋，目前僅少數判決有提及此關鍵字，其中桃園地方法院刑事判決 106 年度易字第 164 號判決及其上訴判決有確實處理 IMSI-Catcher 於刑事訴訟法之地位以及證據能力相關議題，故本文以此判決為討論對象：

第一項　案例事實

被告等人共組詐騙集團，先向他人購買多張登記於他人名下之 SIM 卡，再以桃園某地（被告其中一人之住所）為詐騙機房，使用購買之門號撥打電話予多名被害人，誆騙被害人之子女涉入毒品交易糾紛而被綁架，需支付一定金額為贖金，使部分被害人陷於錯誤而交付金錢，被告之行為涉犯恐嚇取財罪。

警察接獲告訴人報案之後，即分別調取告訴人與人頭號碼之通聯紀錄以及門號申登人資訊，發現人頭號碼撥打詐騙電話時所在的基地台位址，集中於桃園某地鄰近的某 A、B、C 基地台，於是於 2015 年 6 月 3 日先將所有申登人之門號與相關手機序號輸入 IMSI-Catcher，於基地台周邊進行測定，其中一組門號於當日仍在使用，警方便向電信業者要求對該門號（以 IMEI 為基礎向電信業者請求門號）進行即時定位，並輔以 IMSI-Catcher 特定出被告等人所在之精確位置，目前 IMSI-Catcher 之使用依據為內政部警政署刑事警察局訂定之「執行 M 化定位勤務作業流程」。接著警方在附近埋伏進行蒐證，發現該處入口設有監視器，並且有人手提便當進入該處，顯示有多人在內的跡象，且進入該處之人亦有參與組織犯罪之前科，故確認該地址為被告等人之詐騙機房，綜合以上獲得的資訊，向桃園

doi:10.6342/NTU202302425

地檢報請指揮，並向法院聲請搜索票於同年 6 月 9 日搜索該地，經搜索之後獲得詐騙使用之手機、SIM 卡、金融卡、金錢以及毒品等物。

第二項　臺灣桃園地方法院 106 年度易字第 164 號判決

第一款　侵害之基本權

一審判決認為，釋字第 689 號係揭示一般行為自由、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，然而警察使用 IMSI-Catcher 取得該桃園詐騙集團機房的地址，侵害釋字第 689 號所保障之隱私權，因不論被告處於公開場所與否，仍享有一定之不受他人持續監控之自由，追訴機關使用 IMSI-Catcher 即可不受時間地點限制，定位追蹤以及蒐集、處理與利用該等個人資料，已對被告造成並非輕微之干預。

第二款　使用 IMSI-Catcher 並無法律授權基礎

雖使用 IMSI-Catcher 限制個人之隱私權，然隱私權非屬無限保障之權利，依據憲法第 23 條仍得由法律限制之，然而在立法者制定有關基本權干預之授權規定以前，不得類推現行刑事訴訟法的強制處分規定而為對當事人不利之造法。

法院接著審查可能之授權基礎：內政部所制定之「執行 M 化定位勤務作業流程」非法律保留所稱之「法律」，因為其性質非屬立法機關作出「立法」決定，故不可為授權基礎。又不可以通保法第 3-1 條、第 11-1 條調取通聯紀錄為授權基礎，理由在於上開通保法條文，係為保護秘密通訊自由，授權調取「過去」之通聯紀錄（又稱歷史基地台紀錄），而向電信事業（第三人）取得資訊的規定，然而 IMSI-Catcher 是藉由通訊設備與 IMSI-Catcher 本身之訊號強弱判斷位址，是利用個人通訊設備本身，並無干預通訊雙方之通訊過程，是追訴機關不透過第三人而直接連接手機取得定位之偵查行為，警察亦於本案證稱無論是本案或是過去使用 IMSI-Catcher，實務上皆無聲請調取票之作為，故目前使用 IMSI-Catcher 並無法律授權依據。

doi:10.6342/NTU202302425

法院反駁檢察官之主張被告不具有合理隱私期待的主張，認為 IMSI-Catcher 雖然與 GPS 的運作原理不同，然皆可以取得取得一般人能力所不能及之精確定位，且無論是否有犯罪嫌疑，皆對目標人物造成干預，就此被告不因被害人已報案而喪失其「合理隱私期待」，仍適用相關法律保留原則。

自處分干預基本權的程度以及風險考量，若干預一般人格權且程度輕微如跟監之行為，僅需適用刑事訴訟法第 230、231 條概括授權條款即可，然而若為干預基本權利較嚴重之「強制處分」，則應有明確法律授權規定為之，本案 IMSI-Catcher 干預程度非屬輕微，不可逕以概括授權條款為之，否則無異於開放偵查機關，不需先留待立法機關立法，即可先行使用新興偵查工具，而進一步侵蝕對人民基本權利之保障。

第三款　證據能力

既然以 IMSI-Catcher 取得手機位址並無授權基礎，使用 IMSI-Catcher 自屬違法，基於保護法治國、法律保留原則之誡命，故以 IMSI-Catcher 定位直接取得之證物（即該機房地址資訊、警察操作 IMSI-Catcher 過程之證述）皆無證據能力。然而後續發動之搜索取得證物，雖然律師主張適用毒樹果實原則排除其證據能力，然法院經權衡後認定具有證據能力，因為所聲請之搜索票並非以全以 IMSI-Catcher 定位作為依據，而是輔以跟監、基地台、前科紀錄等資訊，並且根據過去慣例，警察已按照內部流程申請使用 IMSI-Catcher，非刻意違法，且警察亦是善意信賴法院所發出之搜索票進行搜索，搜索所得之證物與 IMSI-Catcher 連結已屬微弱，故認定搜索取得之證物有證據能力。因排除透過 IMSI-Catcher 所得知之本案地址的證據能力，所以法院在衡諸事實時僅能以合法取得之基地台位址為判斷案發地點之依據，在綜合其他證據之後，判決被告等無罪。

第三項　臺灣高等法院 109 年度上易字第 1683 號判決

第一款　IMSI-Catcher 侵害之基本權

doi:10.6342/NTU202302425

然而二審法院推翻一審法院之見解，判決被告等恐嚇取財罪有罪。二審法院認為，一審法院所引用之釋字第 689 號揭示內容不足以排除 IMSI-Catcher 之證據能力，因釋字第 689 號係闡述個人於公共場所之隱私權與維護公益的新聞自由衝突，在權衡之下，若認特定報導具有公益性，屬於大眾關注且具有新聞價值而必須揭露進行跟追採訪，則當事人之隱私權必須退讓，該跟追行為具有正當性，故不需受社維法之處罰。二審法院就此解釋脈絡整理出，隱私權非絕對不可侵犯之權利，而是可與其他權利所欲追求的價值與公益以進行合理權衡，如跟追行為考量其目的與人、事、時、地、物之背景，認有正當理由而不違法。在本案中，警察因應科技之進步，輸入被告等之持有門號之 IMSI 或 IMEI 進入 IMSI-Catcher 進行定位，是為了達成國家追訴犯罪之公益，具有正當性，雖使用現代科技設備有侵害當事人隱私權之虞，然非重大、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。權衡之下，應屬當事人應容忍之合理範圍，故符合憲法第 23 條之比例原則。

第二款　證據能力

二審法院經權衡後認為：現今犯罪之少數人，使用新興犯罪手法與設備，造成追訴之困難，而一般循規蹈矩之社會大眾，應期待追訴機關有能力與設備打擊犯罪，以保障其人身以及財產安全，而本案警方使用 IMSI-Catcher 前，是經過被害人報案、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、基地台等方式再出動 IMSI-Catcher，非以 IMSI-Catcher 作為唯一蒐集資訊來源，且 IMSI-Catcher 所蒐集而得的地點，非通訊內容也無個人行動影像，僅使用訊號進行定位並不精確並無法取得「具體」的地址，好比災難生存跡象搜索的訊號顯示，故無實質妨礙秘密可言。IMSI-Catcher 於本案僅是縮小警方之搜索範圍，且警方後續亦有利用不同偵查知識判斷該位址為詐騙集團機房才聲請搜索票，在權衡追訴已發生之犯罪偵查的利益後，依刑事訴訟法第 158 條之 4

doi:10.6342/NTU202302425

認定使用 IMSI-Catcher 所取得之證據（桃園某地地址資訊以及操作 IMSI-Catcher 之警察證述）有證據能力，自然後續搜索所得亦有證據能力可於訴訟上使用。

第四項　最高法院 110 年度台上字第 4549 號判決

第一款　IMSI-Catcher 侵害之基本權

最高法院再度重申，為了保障人性尊嚴與維護個人主體之發展，隱私權與資訊自主權為釋字第 603 號與釋字第 689 號肯認屬於憲法第 23 條之權利，透過隱私權與資訊自主權，人民享有個人生活私密領域免於他人侵擾及個人資料之自主控制，自己決定是否、何範圍內、向何人、以何種方式揭露自己的個人資訊。國家雖然可以公權力限制隱私權與資訊自主權，但是需以法律為之。

以 IMSI-Catcher 的功能，可以追蹤個人貼身物品手機之位址或是識別碼，也就是可以不間斷追蹤手機使用者之位址，但因上開資訊本身，並非通訊過程中附帶產生之資訊，並無人與人之間交流之性質，也無法藉由該資訊得知存在的通訊關係，故並無侵害祕密通訊自由之虞，但因可以藉由上開資訊獲知手機使用者身份等資料，屬於可以連結獲得有關該手機使用者之個人資料之「中介資訊」，故仍有侵害隱私權及資訊自主權之可能。

最後，個人是否對手機位址資訊具有合理隱私期待？最高法院認為，現代生活中，幾乎人手都有手機，仰賴電信事業提供服務進行通訊，以一般社會通念，實難想像僅是因為需要獲得電信事業服務而打開手機，就有可能被 IMSI-Catcher 之虛擬基地台原理所利用，進而持續、緊密追蹤而提供個人資訊，個人應對「免於受他人使用科技設備非法掌握」有合理隱私期待。

第二款　證據能力

國家為犯罪偵查時，可為「任意偵查」或是「強制偵查」之行為，若為「強制偵查」之行為，因為已干預憲法所保障人民之基本權，故需以法律為之，才能符合憲法第 23 條的要求。以 IMSI-Catcher 能夠不間斷、密集取得人民手機位址

doi:10.6342/NTU202302425

資訊，已侵害人民資訊自主權與隱私權甚鉅，甚至對非目標人物造成資訊自主權附帶之干預，屬於「強制偵查」行為，即需有法律明確之授權。

以目前現行法而言，刑事訴訟法第 228 條第 1 項、第 230 條第 2 項、第 231 條第 2 項僅為對檢察官、司法警察官及司法警察發動偵查或調查為抽象之誡命規定，欠缺明確之；警察職權行使法第 11 條第 1 項則是基於防止犯罪之目的，對無合理隱私期待之對象進行觀察，與追訴已發生犯罪之刑事訴訟程序迥然不同；通保法相關規定則因 IMSI-Catcher 原理非屬干預遠距通訊之性質，僅為機器之間之溝通，與通保法所保障之遠距通信性質不同；末個人資料保護法第 15 條第 1 款僅係對公務機關蒐集及處理個人資料為應符合特定目的及執行法定職務必要範圍之抽象性規定，沒有明確規範如何蒐集與處理資料；最後刑事訴訟法搜索規定部分，因目前我國搜索僅限物理性侵入有形空間或侵害受搜索人財產權而對其身體、物件、電磁紀錄及住宅或其他處所進行蒐證，IMSI-Catcher 蒐證即難以與公開進行之搜索類比，故上揭規定皆無法成為 IMSI-Catcher 之授權基礎，以 IMSI-Catcher 蒐證之行為即為違法偵查，立法應另立授權基礎，規定有關使用方式、期間、蒐集資訊之保存暨使用、事後救濟與通知義務等事項。

最高法院認為，二審法院判決未說明 IMSI-Catcher 干預人民基本權屬性及法律授權基礎，即論斷使用 IMSI-Catcher 符合公益，而可以釋字第 689 號與憲法第 23 條肯定其適法性，難謂無理由欠備之違誤。又二審判決後說明 IMSI-Catcher 無法顯示精確地址，實質無妨礙秘密可言，應係指使用 IMSI-Catcher 並無違法之虞，然而二審判決卻又在最後依據刑事訴訟法第 158 條之 4 去判斷使用 IMSI-Catcher 之證據能力，然而第 158 條之 4 係處理「違法」取得證據是否可以於訴訟上使用，如此論理有判決理由矛盾之違誤。末若以 IMSI-Catcher 係為違法取證行為，則後續再以搜索票進行搜索取得之證據，是否與 IMSI-Catcher 違法取證據有直接性關係、是否可以使用於刑事訴訟程序上，二審判決亦未說明，有理由欠備之違法。基於上述之原因，最高法院撤銷二審判決，發回二審。

doi:10.6342/NTU202302425

第五項　臺灣高等法院 111 年度重上更一字第 42 號判決

更一審認為 IMSI-Catcher 可以不限時間、地點，蒐集目標對象之位址資訊，進而處理利用這些資訊，干預了人民之隱私權與資訊自主權，然在欠缺授權基礎之情形下（更一審判決未說明有何「可能」之授權基礎），屬於違法之偵查行為，依據刑事訴訟法第 158 條之 4 規定，應認違反法定程序，該地址等直接證據無證據能力。

至於後續發動搜索所扣得之物，更一審認為，警察係以 IMSI-Catcher 作為查找被告位置之手段，然有輔以跟蹤、埋伏、調閱監視器、查訪相關證人等方式確認，再依據被害人筆錄、所調閱之通聯、分析資料、現場埋伏查抄之車輛及訪查報告等資訊向法院聲請搜索票獲准才發動搜索，IMSI-Catcher 僅作為縮短偵查流程之工具，且搜索票聲請之流程因適用自由證明程序，聲請搜索票的證據本身不需要有證據能力。警方依據內部規定申請使用「IMSI-Catcher」，善意信賴法院核發之搜索票發動搜索扣押，是相關搜索、扣押取得之證據，與「IMSI-Catcher」之連結已相對薄弱，故搜索取得之證據不適用「毒樹果實理論」，而認有證據能力。

第二節　使用 IMSI-Catcher 定位手機位址涉及之基本權：刑事訴訟法基本權干預審查體系

第一項　強制處分定位之轉變

強制處分係追訴機關為了追訴犯罪之任務，於程序中保全被告或是保全證據所為之行為，當然一行為亦有可能兼有兩種目的，例如刑事訴訟法第 101 條所規定之羈押，追訴機關可基於「逃亡或有事實足認為有逃亡之虞者」而羈押以保全被告，亦可基於「有事實足認為有湮滅、偽造、變造證據或勾串共犯或證人之虞者」而羈押以保全證據。

doi:10.6342/NTU202302425

早期訴訟行為論認為，強制處分性質上屬於完成訴訟過程的行為，僅為訴訟行為，而所謂訴訟行為意指為開啟、進行或終結訴訟之一切行為，訴訟行為除非有法律特別規定，否則不可以單獨對其進行救濟，僅能依附本案一同審查，因為為了終結單個刑事訴訟案件可能會經過數以百計之訴訟行為，若皆可允許救濟，有可能造成訴訟遲延、甚至是因為救濟採分別審查制度（甚至允許其再抗告救濟），造成與實體裁判矛盾之問題。

然而，於 1950 年德國學者 Niese 提出「雙重性質（功能）的訴訟行為」，主張部分訴訟行為可能兼具程序與實體之性質，例如通訊監察除了可以於程序上達成保全證據，亦具有侵害人民實體權利之秘密通訊自由的特性。基於這個想法，德國學者 Amelung 進一步提出，刑事訴訟法應捨「強制處分」之用語，以「刑事訴訟上之基本權干預」取而代之，理由在於，強制處分之用語已經無法涵蓋當代不斷出現的新興干預行為，例如通訊監察並無如傳統強制處分可對被告施以強制力壓制其意志執行的特性，而是於當事人不知情下實施，但不可否認通訊監察仍有干預秘密通訊自由之性質，我國亦有學者贊成以此取代強制處分之用語。

除了用語的轉變，此學說對後續最大的貢獻是對於救濟之影響。因其為具有干預基本權利性質的公法行為，故應同受憲法基本原則如法律保留原則、比例原則與有權利即有救濟等拘束，並揚棄過去訴訟行為論認為強制處分不可單獨救濟之想法，因除了有關強制處分之證據能力認定，審判程序僅會針對本案之罪與罰進行，根本不會審查強制處分之合法性，因此強制處分事實上沒有管道可以進行救濟與審查，故現在立法設計大部分強制處分皆有獨立之事前審查與事後救濟機制[1]。

第二項　基本權利問題體系

憲法作為保障人民各種自由權利與人民與國家之間關係之基本規範，憲法文字相較於其他法律較為簡單與抽象，亦使用許多不確定法律概念，使憲法具有規

[1] 林鈺雄（2020.09），《刑事訴訟法 上冊》，10 版，頁 311-313，新學林。

doi:10.6342/NTU202302425

範上之開放性（normative Offenheit），這些不確定法律概念之解釋會因不同社會文化成長背景，造成每個人對基本權內涵的解釋莫衷一是，故需要建立一套統一架構以應用思考，以充實基本權之內涵，故可應用於實際案例中思考，有助於實現基本權利之規範效力。對於基本權利之討論，通常都是研究「國家是否侵害人民權利」之議題，只有在人民之基本權受有國家侵害時，才有必要討論是否具有憲法上之正當化事由，然而判斷基本權是否受到國家侵害，又以理解基本權之保障範圍為前提要件，故在判斷基本權力問題時，需先對基本權利之構成要件進行解釋，再判斷基本權利是否受到國家限制、最後是是否存在阻卻違憲事由審查。

於刑事訴訟領域，通常是由國家追訴機關（檢察官、司法警察）執行並直接干預人民，其行為可歸責於國家，符合基本權問題之前提，接著若判定一訴訟行為屬於刑事訴訟法上的基本權干預，即應受憲法之相關原則拘束（比例原則、有權利有救濟），以保障人民之權利，故本文將以此架構審查，分別為判定基本權範圍、分析強制處分是否造成基本權干預，以及基本權干預行為是否正當（包含是否有授權基礎與是否符合比例原則），若皆通過方認為此訴訟行為為合法且合憲之行為[2]。

第三項　基本權之範圍與國家是否干預基本權

首先需先界定基本權利之保障範圍（Schutzbereich des Grundrechts），此屬於憲法解釋的問題，透過具體化劃定保障範圍，掌握國家是否侵害此「客體」，需自現實觀察，以理解基本權利之打擊範圍與於實際生活領域之各種切面（Wirklichkeitsausschnitt），方能實現基本權之保護功能（Schutzwirkung），防止國家之侵害並於必要時可排除侵害。解釋基本權利之構成要件要素可分為：事物的保障範圍（sachlicher Schutzbereich）與人的保障範圍（personaler Schutzbereich），前者是與基本權相關之行為方式、法益、特性與狀態，基本權保障的可以是積極之行為亦可是消極之不作為，甚至可以是一種狀態或單純存續；後者是保障主體的問

[2] 林鈺雄（2021.09），《刑事訴訟法實例解析》，4 版，頁 119-120，新學林。

doi:10.6342/NTU202302425

題，關注的是基本權之歸屬，亦「誰」可以主張受到基本權之保護。對基本權構成要件之解釋，若解釋過於寬泛，將多數國家行為納入基本權之保護範圍，使國家皆需對其行為提出合憲之正當化理由；相對的，若解釋範圍過於狹窄，使人民自始排除於憲法之保護範圍而無法主張保護，故解釋時須以法學方法論為本，衡諸憲法之文意與其背景發展、體系等，考量社會通念為之[3]。

然基本權並非可以完全自由行使，若無界限之行使將使權利主體之間出現衝突，失去基本權之功能，故國家對權利主體基本權之行使劃定一定界線，此非因為國家具有高於人民優越地位，而正是因承認基本權利之存在，故國家須協調權利主體之能夠彼此和諧行使，進而避免影響到憲法所保障如第 23 條之其他公益，然而此「劃定」權利行使範圍之行為（又稱基本權利之限制），對權利主體而言，即為對基本權利之干預（Eingriffe），影響基本權利之防禦功能，故國家不得恣意為之，否則是對基本權利之違法侵害（Verletzungen）[4]。

所謂對於基本權利之干預，通常是公權力主體所為之行為，對基本權主體行使基本權造成不利益，兩者之間具有一定之關聯性，包括命人民為一定行為或禁止人民某作為。傳統對於侵害的概念通常認為：該行為具有目的性、直接性、法效性、下命性之特性，換句話說即為國家出於一定干預基本權的意欲之目的，對基本權造成直接干預，而得以以強制力壓制人民意志之法律行為。然而隨著時代演進與社會文化變遷，這個概念已經無法涵蓋所有國家基本權干預行為，可能造成基本權保障不足，故現在認為對於對基本權之干預，應理解為「因國家行為致使權利主體無法完善行使基本權」，即不論其目的性、直接性與法效性[5]。

自前述 IMSI-Catcher 一系列判決即可看出，法院爭執之核心問題即是「於刑事訴訟使用 IMSI-Catcher 進行手機定位而縮小警方搜索範圍」此訴訟行為，是否有侵害當事人隱私權之虞，若肯定該訴訟行為造成基本權利侵害，又是否有正當

[3] 李建良（1997.03），〈基本權利理論體系之構成及其思考層次〉，《人文及社會科學集刊》，9:1 期，81-83 頁。
[4] 陳新民（1992.07），〈論憲法人民基本權利的限制（上）〉，《律師通訊》，154 期，頁 23。
[5] 李建良，前揭註 3， 頁 30-36。

doi:10.6342/NTU202302425

理由（法律授權基礎）予以正當化，本文以下將以基本權利問題體系討論，以分析各審判決。

第一款　秘密通訊自由

上揭判決在一二審皆未提及有關 IMSI-Catcher 祕密通訊自由之分析，直到最高法院才有相關解釋，又依據第三章德國聯邦憲法法院之判決，係先就 IMSI-Catcher 是否干預秘密通訊自由討論，且一審判決本身亦有引用通保法調取歷史基地台通信紀錄之條文為授權基礎討論，通保法第 1 條開宗明義指出：「為保障人民『秘密通訊自由』及隱私權不受非法侵害」，故分析以 IMSI-Catcher 定位手機位址是否有干涉秘密通訊自由仍有必要性，故本文先就此為判斷。

第一目　秘密通訊自由之基本權範圍

憲法第 12 條僅有規定：「人民有秘密通訊之自由」，經我國釋字第 631 號稱：「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」，除了解釋秘密通訊自由是為了保障個人能夠自主發展其人格，更揭示秘密通訊自由為隱私權之特別規定。因現今人民溝通需大幅仰賴各種無法自己掌控過程之通訊工具，不斷藉由這些通訊工具建立社會關係與發展人格，若受到國家之不法侵害，相較於過去較少使用通訊工具的時代，會造成更大的痛苦[6]。

判斷祕密通訊自由的事物保障範圍，需先解釋何謂秘密通訊自由之「通訊」此上位概念。然而，釋字第 631 號本身並未對何謂「通訊」進行定義，僅能由相關文獻進行探討。「通訊」有認為應為利用資訊傳遞系統傳輸訊息之一切過程（資訊交通行為[7]）的總稱，不論傳送形式，只要是可以乘載、儲存與傳遞訊息之系統均屬之，故不論是有體之書信或無體之網路電子郵件、甚至是現今廣泛使用之即時通訊

[6] 詹鎮榮（2003.09），〈秘密通訊自由〉，《法學講座》，21 期，頁 1。
[7] 許育典（2019.09），《憲法》，9 版，頁 265，元照。

doi:10.6342/NTU202302425

軟體訊息均屬之。這些通訊方式與人面對面、以空氣為介質溝通不同，因通訊各方存在距離，而需仰仗其他通訊媒介例如書信、電話等進行意見交流，在通訊的過程中會喪失對於通訊之掌握[8]。許志雄大法官在釋字第 756 號協同意見書提及，所謂的通訊是利用通訊系統，將個人想法與意思表達給他人的一種行為，亦即發信者與收信者內部封閉的資訊傳遞，黃昭元大法官亦在同號釋字之部分協同意見書認為，秘密通訊自由與一般表意自由之差距在於，秘密通訊自由具有對應之權利主體，寄信方寄出訊息，就會有相對的收件人接收訊息。綜合以上論點，可以說秘密通訊自由的「通訊」需要有人與人之間交流、溝通與意見交換之性質。

秘密通訊自由保障的重點並非通訊行為本身，通訊行為是指通訊主體基於自己的意志決定「是否」要與他人進行通訊，此為憲法第 22 條一般行為自由之保障範圍（人民依其意志作為或不作為），秘密通訊自由之保護重點在於「個人通訊之隱密性[9]」，一方面禁止國家以積極行為介入通訊行為，另一方面也禁止利用之電信事業洩漏因職務而得知之通訊內容與通信紀錄[10]。當事人需「主觀」將特定通訊內容定位為「私人通訊」，即具有不希望其通訊曝光於通訊雙方以外之意圖，如果當事人無此意圖，例如公開發送之公開信，則屬於「公開通訊」而不受秘密通訊自由保障，判斷標準僅取決於當事人之主觀想法而非通訊之外觀（例如是否彌封、透過明信片為之），只要有事實足認當事人對通訊內容具有隱私或秘密合理期待即可，不彌封訊息不可推論為允許國家任意干預，若無法由事實判斷當事人是否具有隱私或秘密合理期待，基於保障人權之觀點，仍應將其解釋為私人通訊[11]。然有學者認為，以對通訊「內容」是否有隱私或秘密合理期待為區分不甚合理，因爲若通訊內容若為私下閒聊或周知事實，甚至是毒品交易訊息、犯罪要約等，國家反而可以對其進行通訊監察，無啻是以通訊內容反推保護範圍而不甚合理，蓋因秘密通訊自由本身應為價值中立的，故應將有隱私或秘密合理期待範圍擴張，亦即只要對通訊

[8] 詹鎮榮，前揭註 6， 頁 2-3。
[9] 李惠宗（2020），《憲法要義》，8 版，頁 237，元照。
[10] 李仁淼（2014.01），〈秘密通訊自由與監聽〉，《月旦法學教室》，135 期，頁 6。
[11] 詹鎮榮，前揭註 6， 頁 5。

doi:10.6342/NTU202302425

「內容」或通訊「過程」有隱私期待，均受秘密通訊自由保護。[12]然而目前通保法第 3 條第 2 項是採取前者之看法，僅規定「通訊，以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」。

釋字第 631 號闡釋保密客體包含「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」，故除了通訊內容，其餘的是保護所謂「通訊情況」，前者即為通訊之實質內容保障，後者則是針對通訊之有無、對象、時間、方式這些與通訊相關資訊的保護，從通訊內容延伸至通訊情況之保護，是因通訊情況這類延伸的電子紀錄通常不容易與通訊內容區分，而一併納入保護範圍，在此範圍內通訊中的手機位址資訊自然屬於此類通訊情況，而應受到保護[13]，通保法第 3-1 條第 1 項之條文內容亦揭示此點。

雖然祕密通訊自由是隱私權的特別規定，非所有通訊皆受祕密通訊自由所保障，以保障時點而言，秘密通訊自由之保障時點自發信者將通訊送出之後，至收信者獲得通訊而置於自己可支配範圍即告終止，在此之前或之後均不受秘密通訊自由保障，而需尋求其他基本權以供保護，因此段區間才有通訊本身溢脫通訊雙方可支配之可能[14]。

最高法院 106 年度台非字第 259 號判決中討論追訴機關取得賭客利用 Hibox 網路傳真服務傳真簽單影像（下稱 Hibox 傳真），應適用通保法或刑事訴訟法的搜索扣押為區辨，其論述對於秘密通訊自由所保障之「時的範圍」頗值參考。最高法院認為，祕密通訊自由保障的目的是因通訊過程中，通訊雙方無法自行直接掌控，而易受國家或第三人從中干預、侵擾甚至是截取訊息，為避免此危險而有特別保護之必要，故規定秘密通訊自由的權利保障，保障對象是雙方之秘密通訊過程，故與隱私權不同，隱私權通常僅涉及「個人」之保障，所以通訊秘密自由

[12] 吳秋宏（2008.04），〈司法院釋字第 631 號解釋與監聽法制評析（上）〉，《司法周刊》，1385 期，頁 2-3；李惠宗，前揭註 9， 頁 238。
[13] 李震山（2007.09），〈挪動通訊保障與通訊監察天平上的法碼－釋字第六三一號解釋評析〉，《台灣法學雜誌》，98 期，頁 284。
[14] 詹鎮榮，前揭註 6， 頁 5。

doi:10.6342/NTU202302425

的時的保障範圍應始於「訊息發出，而隨訊息送達接收方傳遞過程結束而告終止」，因為當通訊已落入當事人之掌控範圍，可以決定自行留存或是刪除而為處理，上述所陳之被截收之危險即不存在，僅受隱私權保障；另外，此判決亦以釋字第 631 號有關通保法之解釋延伸出，認為釋字第 631 號說明通保法用語使用「監控與過濾……紀錄」，故須先為「監控」才「紀錄」存在的可能，非指紀錄於監控過濾時即已存在，並且提及通訊監察具有「受監察人無法即時知悉權利侵害之事實，而無法及時主張救濟」與「需於一定時間內實施」之特性，故相較於搜索扣押，通訊監察對人民權利侵害較深，故認我國大法官解釋也採相同之解釋；最後判決自通保法之體系解釋，包括第 5 條第 2 項、第 5 條第 4 項、第 11 條第 1 項第 6 款監察期間規定、第 12 條第 1 項前段、第 13 條第 2 項、第 16 條第 1 項前段，可知通訊監察具有一定時間性，期間必須保持通訊暢通，並需定期製作報告以確認是否有續行監聽之必要，若是調閱過去已結束之通訊，自無保持通訊暢通與定期檢討是否有續行監聽之必要。綜上這些解釋方法，實務見解已承認秘密通訊自由是針對「現時」之通訊為保護。

至於人之保護範圍，以自然人而言，因現今通訊科技之進步而可以輕易使用各種通訊工具聯繫不同國家之對象，且秘密通訊自由旨在保障防止國家對通訊過程之不當侵害，故不論是本國人或是外國人，只要通訊過程時全部或一部位於我國領域內，均得為基本權主體而享有保障，因通訊具有涉及「雙方」之資訊交換行為的特性，故除了訊息傳送人，訊息接收人亦為通訊參與人，共同受秘密通訊自由之保障[15]。

第二目　使用 IMSI-Catcher 不干預秘密通訊自由

劃定秘密通訊自由之範圍之後，接續判斷使用 IMSI-Catcher 定位手機位址是否構成干預。以 IMSI-Catcher 之技術而言，IMSI-Catcher 是作為一虛擬基地台，捕捉「待機」手機向其連接，經此註冊過程而取得手機位址。然而自上述之分

[15] 詹鎮榮，前揭註 6， 頁 6。

doi:10.6342/NTU202302425

析，秘密通訊自由所保障的是人與人之間有意識之資訊交換，且通訊者須主觀上認定其屬於私人通訊，而因使用 IMSI-Catcher 時是利用手機為保持通訊，與訊號較強之 IMSI-Catcher 自動連接而開啟一連串訊號交換之原理，使用手機之人並不會發現，自然不可能有將其定義為私人通訊之意圖，故自始並不存在所謂人與人資訊交流的「通訊」可言，而既不存在應保護的通訊內容，可能推論出的通訊內容而需一併保護之通訊情況（被告手機位址）亦不需保護[16]；另外自干預目的觀察，追訴機關也無意求得受干預人與誰、什麼時間、什麼地點通訊之情形，而只是需要「受干預人現在位於何地」之資訊，故與秘密通訊自由無涉[17]；況且以目前技術而言，正在進行通訊中的手機亦無法為 IMSI-Catcher 捕捉，故正在通訊中的手機（此時受秘密通訊自由保障）之位址（亦受秘密通訊自由保障）也不會為 IMSI-Catcher 所知。綜上，以 IMSI-Catcher 取得手機位址之行為並不干涉被告或第三人之秘密通訊自由。

第二款　資訊自決權與隱私權

第一目　事物保障範圍

隱私權非憲法明文保障之權利，首見於釋字第 293 號：「銀行法第四十八條第二項規定：……旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」然此時未說明其屬於憲法第 22 條之範圍，後在釋字第 603 號明文肯認隱私權為憲法第 22 條之保障對象。

釋字第 603 號揭示資訊隱私權之保護目的為「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

[16] 王士帆（2022.03），〈M 化車法制出路－德國 IMSI-Catcher 科技偵查借鏡〉，《臺北大學法律論叢》，121 期，頁 87。
[17] 林鈺雄（2021.02），〈科技偵查概論（上）──干預屬性及授權基礎〉，《月旦法學教室》，220 期，頁 56-57。

doi:10.6342/NTU202302425

法第二十二條所保障 （本院釋字第五八五號解釋參照）」[18]為保障人性尊嚴與個人人格發展，故個人得以主張隱私權而拒絕他人（包含國家）探知、儲存或處理有關自己的個人資訊[19]。得受保障之資訊僅限所謂「個人資訊」，即與個人身分相關之資料，以我國個人資料保護法第 2 條之定義，範圍包含個人出身、健康資料、財務資料、宗教信仰、政黨傾向，亦包括個人的聯絡方式與地址等得以直接或間接方式識別該個人之資料[20]。

與隱私權密切相關的資訊自決權，則是強調較為積極的面向，即個人可以自行控制資訊之流向，釋字第 603 號認為「就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權[21]」。

釋字第 689 號同樣提到對隱私權的保障，並另外處理在公開場所是否仍受隱私權保障。雖然本號釋字主要是處理私人之間之基本權衝突（經國家介入），而刑事訴訟法是國家對私人之關係，但實務上刑事判決仍不乏將其當成基本權侵害判斷標準，其內容闡述：「個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通

[18] 雖使用「資訊隱私權」之用語，然林子儀大法官之協同意見書認為其行為即類似德國人口普查案之所衍生之資訊「自決」權。
[19] 李惠宗，前揭註 9， 頁 451。
[20] 李震山（2020），論資訊自決權，氏著，《人性尊嚴與人權保障學術論文集》，頁 243，元照。
[21] 許育典，前揭註 7， 頁 361-362。

doi:10.6342/NTU202302425

念認為合理者」，強調於因科技持續發展，而出現更多不同追蹤監視科技，故個人即便位於公共場所亦受隱私權之保護，但容有一定限制。即便是私人之間都要遵守相關原則避免侵害隱私權，國家具有能夠發動強制處分以及使用最新科技以追蹤私人之情況，更應受到此基本權之拘束。[22]

第二目　使用 IMSI-Catcher 干預資訊自決權

個人位址應屬於個人資料的一種，使用 IMSI-Catcher「捕捉」手機向其註冊，並以訊號強弱判斷其所在位置，因應現在人手一機的時代且輕巧易攜帶之特性，檢警使用 IMSI-Catcher 找尋被告手機位址，因為誤差極小，故藉由手機定位，也幾乎可以相等於知道被告個人所在的位址，即可進一步發動其他偵查行為（例如逮捕、搜索等），且個人無法控制手機所連上之基地台，導致個人無法控制與決定其有關位址的資訊是否揭露以及如何被揭露。另外更大的侵害在於，若累積一定時間內的個人手機位址紀錄，甚至可以推測分析出個人之行動足跡[23]，例如先前疫情期間，疾病管制署或各地市政府每日皆會公布確診足跡，雖然利用與科技原理與 IMSI-Catcher 不同，但新聞媒體或大眾即可由這些公布的一兩日甚至更長之足跡位置，以個案單日長時間所位於的位置而大致推論出其之工作、是否有兼差、平常習慣購物地點等，甚至可以描繪出一個人的人格圖像[24]。

即便個人位於公開場所，雖然所有人包含一般私人或國家機關以肉眼即可觀察其位置，但私人通常不會長期、有系統地對個人進行追蹤，但國家利用 IMSI-Catcher 捕捉個人位址之效率較人力跟監更高，且更容易鎖定到被告個人，尚有被國家大量搜集資料作為分析人格圖像之危險，以我國釋字第 689 號強調個人「享

[22] 施育傑（2020.05），《數位、科技與刑事程序干預處分 ──資訊框架理論之建構》， 頁 411-412，國立政治大學法律學研究所博士論文。
[23] 王士帆，前揭註 16， 頁 89。
[24] 疫情當時之新聞例如：TVBS 新聞網（2022.04.08），〈警出遊後確診！ 足跡意外揭女「在酒店工作」〉，https://news.tvbs.com.tw/local/1761269（最後瀏覽日：2022.08.04）。

doi:10.6342/NTU202302425

有依社會通念得不受他人『持續』注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主」標準而言，應已逾越個人之合理期待[25]。

再者，以我國著名之最高法院 106 年度台上字第 3788 號判決為參考，判決稱「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」，雖該案屬於不同之科技方法，為追訴機關於被告車輛主動裝設 GPS 以定位行蹤，然依據舉輕以明重之道理，因平常人民應會將手機隨身攜帶，其與個人之連結會較車輛更為緊密，而類似個人專屬貼身之追蹤器[26]，且手機本身即為個人所有，人民對其信賴程度高，而不會懷疑其已遭到追訴機關所利用[27]，故對基本權干預應較使用 GPS 定位被告程度更為嚴重，故應得出相同結論，即追訴機關利用科技設備 IMSI-Catcher，從茫茫人海中「撈」出特定被告，並取得精確的位置，亦應已限制目標人物之隱私權（資訊自決權）。

第三款　一般行為自由

第一目　事物保障範圍

一般行為自由亦非我國憲法明文承認之權利，首度出現於釋字第 689 號：「為維護個人主體性及人格自由發展，除憲法已保障之各項自由外，於不妨害社會秩序公共利益之前提下，人民依其意志作為或不作為之一般行為自由，亦受憲法第二十二條所保障」，然而，釋字第 689 號並未清晰闡明其內涵而著重於一般行為自由之下位概念（行動自由），許志雄大法官於釋字第 749 號之協同意見書中闡述其內涵

[25] 薛智仁（2014.12），〈司法警察之偵查概括條款？－評最高法院一○二年度台上字第三五二二號判決〉，《月旦法學雜誌》，235 期，頁 240。
[26] 王士帆，前揭註 16， 頁 89-90，同見解見： 林鈺雄，前揭註 17， 頁 56-57。
[27] 林容（2021.03），《隱密科技偵查與基本權保障》，頁 124，臺灣大學法律學研究所碩士論文。

doi:10.6342/NTU202302425

以及審查基準：「一般行為自由，因範圍廣泛，及於一切生活領域有關之行為，而不以有關人格利益或自律者為限，且未直接牽涉個人尊嚴之維護，是尚不宜列入人權範疇。惟其可排除國家之『違憲強制』或『違憲侵害』，有助於個人主體性之實現，故應為受憲法保障之其他權利，只是一般行為自由之審查密度通常較低，有關規制立法之違憲可能性亦相對減少」。

從以上之實務發展，可見一般行為自由以為我國釋憲實務上普遍承認之權利，其保護人之一切之作為與不作為，其範圍包山包海，故一般行為自由之性質應屬於補充性權利，意即個案中無其他更具體之基本權存在時，才可以作為審查依據，然而無論是我國釋字第 689 號或是隨後的釋字第 749 號，均無將一般行為自由作為唯一審查基礎，與原先之補充性特性不同，而是帶有「錦上添花」的意味，擴展人民基本權利保障範圍[28]。

第二目　使用 IMSI-Catcher 干預一般行為自由

第二章介紹 IMSI-Catcher 之技術背景有提及，使用 IMSI-Catcher 時，因為手機被「欺騙」而與 IMSI-Catcher 這個虛擬基地台連接，進而傳送 IMSI 或 IMEI 等足以辨識出個人之資訊，追訴機關再以這些資訊進行比對，這個過程會使個別手機有幾秒的時間無法進行任何通訊（甚至有估計影響時間可能長達 10 分鐘），影響人民「進行通訊」之行為。這種個人可以自行決定是否與他人進行通訊之自由，即屬於第 22 條一般行為自由之保障範圍，不受秘密通訊自由之保護[29]。

對被告而言，追訴機關使用 IMSI-Catcher 蒐集齊位址資訊，使其手機技術上出現干擾而無法進行撥打電話或傳送簡訊等行為，自屬對一般行為自由之干預。特別的是，因為 IMSI-Catcher 須要先與不特定手機進行連接，待連接手機傳送資訊進行匿名比對之後，才能確認是否為被告本人再進一步蒐集資訊，故 IMSI-Catcher

[28] 李仁淼（2020.01），〈一般行為自由與一般人格權〉，《月旦法學教室》，207 期，頁 6-7，相同見解：張永明（2018.02），〈一般行為自由與一般人格權作為憲法保障之基本權〉，《月旦法學雜誌》，273 期，頁 39。

[29] 詹鎮榮，前揭註 6， 頁 3-4。

doi:10.6342/NTU202302425

亦有可能連接到非目標人物，雖進行比對之後與被告資訊不符即會「釋放」該手機連接回原本之基地台，但這個過程亦造成該非目標人物無法使用手機進行通訊，亦干預其一般行為自由。

第四款　小結

經上述之分析，依我國釋字對於基本權保障的闡釋，我國追訴機關使用 IMSI-Catcher 探知被告之手機位址，對被告而言，不干預憲法第 12 條之秘密通訊自由，但即便不受秘密通訊自由保護，此行為仍干預憲法第 22 條所承認之隱私權（資訊自主權），不論被告位於公開場所與否，並且因會有幾秒甚至幾分鐘無法正常進行通訊，亦干預憲法第 22 條所衍生之一般行為自由[30]。

故前述之 IMSI-Catcher 一審法院認為：「依據前述『M 化車』之作用，可知其原理係利用「虛擬基地台」的方式，透過已知的 IMEI 或 IMSI，藉『M 化車』與目標設備之間的訊號連結，進而定位目標設備，藉此定位所欲偵查之對象。該定位科技方法，係藉訊號之強弱連結以探知資訊，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。……，前述『M 化車』使用之結果，已對目標對象之前揭**（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，粗體為筆者自行補充）**基本權，造成並非輕微的干預」此部分之見解應可值贊同。

然而二審法院之論理出現矛盾，雖先稱：「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（粗體為筆者自行加註）**，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。」似

[30] 林鈺雄（2023.02），〈以 M 化車探知手機位置資訊之合法性〉，《月旦法學教室》，244 期，頁 26-27。

doi:10.6342/NTU202302425

乎所指使用 IMSI-Catcher 進行定位手機是屬於侵犯隱私權之行為（但仍於容忍範圍），但後在「２、使用『M 化車』取證有證據能力：」此段又稱：「M 化車僅僅是以訊號定位，無法顯示地址，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。（粗體為筆者自行加註）**」，在此後段的論述又似乎否定 IMSI-Catcher 取得手機即時位址有侵犯隱私權的可能，然而就目前 IMSI-Catcher 之技術發展，其誤差極小不受室內室外所影響，難謂其無侵害隱私權之性質，且有無顯示地址亦不應該成為判斷是否侵害隱私權之判准，即便是依據通保法調取通信紀錄，而利用三角定位方法取得手機位址，甚至是於車輛裝設 GPS 觀察被告之行動軌跡，皆無法獲得一個具體之「XX 市 XX 區 XX 路 X 號」之地址，然而實務或學說皆未否認其侵害秘密通訊自由或資訊自決權之性質[31]，這部分也是最高法院判決認為二審法院未明確說明而撤銷發回之部分。

又一二審判決因是處理被告（目標人物）是否有罪之問題，故僅討論 IMSI-Catcher 侵害被告基本權利之部分，最高法院另從 IMSI-Catcher 取得被告位址之整體行為觀察，認為在找到真正的被告手機位址之前，這個過程尚會使其周邊不特定多數人亦受影響，其手機亦為 IMSI-Catcher 所捕捉並且比對，雖並不會辨識出其身分並且資料會於執行結束後刪除，但已附帶干預非目標人物之資訊自主權。另外本文認為 IMSI-Catcher 作用時會造成在比對期間內，周邊目標與非目標人物會無法自行決定是否進行任何通訊，亦干預一般行為自由。

第四項　形式與實質阻卻違憲事由

確定國家有侵害人民基本權利之事實後，國家需主動證明侵害之正當性，即提出所謂「阻卻違憲事由」，否則即為違法之侵害。阻卻違憲事由又可分為 2 種：「形式阻卻違憲事由」，意指國家為基本權侵害之行為，須有法律明文之限制，又

[31] 林容，前揭註 27， 頁 150-151。

doi:10.6342/NTU202302425

稱法律保留原則（憲法第 23 條）；「實質阻卻違憲事由」，則是審查國家之侵害行為的內容是否符合比例原則。

我國憲法第 23 條規定：「以上各條列舉之自由權利，除為防止妨礙他人自由避、免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」此即為「法律保留原則」。而所謂法律，係指經立法者三讀通過並經總統公布之法律（憲法第 170 條）[32]。於刑事訴訟領域尤為重要，刑事訴訟法第 1 條第 1 項即規定：「犯罪，非依本法或其他法律所定之訴訟程序，不得追訴、處罰。」，宣示所謂刑事程序法定原則，意即所有訴訟程序進行中所為的行為或處分，均須有法律規定，並且需要由具民主正當性的立法者事先立法以供人民預見並落實權力分立之意涵[33]。

第一款　可能授權基礎

依據上述分析可知使用 IMSI-Catcher 侵害資訊自主權與一般行為自由（然程度較為輕微），故接著需先審查現行法制是否有法律授權基礎（形式阻卻違憲事由），本文將由前文判決與學說文獻提及之法律規範為討論。

第一目　執行 M 化定位勤務作業流程

追訴機關於本案主張，使用 IMSI-Catcher 皆依內政部警政署刑事警察局訂定之「執行 M 化定位勤務作業流程」辦理。需為重大刑案包括：擄人勒贖、故意殺人、 槍彈、組織犯罪、強盜、重大詐欺、重大恐嚇取財、毒品或急難救助等方可使用，並需按照通保法第 5 條向法院聲請通訊監察書或聲請第 11-1 條之通信紀錄調取票以進行定位，並且據該通訊監察書或通信紀錄調取票，申請單位須另外填報申請表予執行單位進行審核[34]。然而就「執行 M 化定位勤務作業流程本身」並非法律層次之規定，僅為行政規則，僅拘束其內部使用 IMSI-Catcher 之流程，條文內容

[32] 李建良，前揭註 3， 頁 90-91。
[33] 薛智仁（2018.12），〈刑事程序法定原則〉，《月旦刑事法評論》，11 期，頁 21-26。
[34] 由於內政部警政署刑事警察局訂定之「執行 M 化定位勤務作業流程」並無全文公布，僅由台北市議會質詢內容為參考，資料來自：台北市議會（2016），《台北市議會公報》，105 卷 6 期，頁 2914-2916，台北市議會。

doi:10.6342/NTU202302425

全無公開而人民自然無法知其內容而有所預見其基本權利干預與否與範圍，故不可為「法律保留原則」之法律。於本案一審判決亦指出其並非法律層次之規定，故不可為法律授權基礎，此看法亦為最高法院所支持。

第二目　通保法第 3-1、11-1 條

通保法第 1 條即揭示其保障目的：「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。」雖隱私權亦包涵於保障範圍，然觀察 103 年於第 1 條法條內容新增「隱私權」之修法理由稱：「『言論及談話』應歸屬憲法第二十二條隱私權之保障，為保障人民秘密通訊自由及隱私權不受非法侵害，爰修正原條文，俾符實際。」以及新增第 3-1 條調取通信紀錄之修法理由：「為保障憲法第十二條人民秘密通訊自由並落實司法院大法官會議第 631 號解釋意旨，將通信紀錄納入通訊監察法制範圍內，爰增訂通信紀錄之定義。」可見以通保法第 3-1、11-1 條授權調取通信紀錄之「電信使用人使用電信服務後……位址」，是為了保障憲法第 12 條之秘密通訊自由而非隱私權，故於通保法之脈絡，第 1 條所稱保護隱私權僅針對保護對言論與談話之干預。然而就上述有關基本權干預之分析，使用 IMSI-Catcher 獲知目標人之手機位址，不干預秘密通訊自由而為憲法第 22 條所保障之隱私權，故不得適用本法為授權基礎。

另外原因在於：使用 IMSI-Catcher 僅需追訴機關（警察）自行執行使用即可，不需要透過第三方之電信事業協助，故與通保法第 14 條第 2 項所規定之：「電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。」以及電信管理法第 9 條第 4 項：「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。」不同，以 IMSI-Catcher 為找尋被告行動通訊裝備位址並不會影響秘密通訊自由保護，因非屬於利用通訊雙方利用非自己可控制之通訊系統進行通訊而造成第三人從中干涉之危險[35]。

[35] 王士帆，前揭註 16， 頁 93-94。

doi:10.6342/NTU202302425

就此一審法院亦認為，通保法授權的是調取調取過去已儲存之通信紀錄（即歷史基地台紀錄），且 IMSI-Catcher 是直接連結目標對象之手機進行即時定位，技術原理非為國家介入通訊過程，與通保法不符，故不適用通保法為授權基礎，此無法適用通保法之結論應予贊成。最高法院則是認為 IMSI-Catcher 非介入人與人溝通之過程，故不適用通保法，與本文之觀點較為類似。

第三目　刑事訴訟法

如果自「從被告處取得資訊」之目的觀點出發，可能可以討論適用第 122 條、第 133 條以下搜索扣押之規定。然而，於我國不論是以「物理性侵入特定空間以獲得有體物」或是「是否侵害合理隱私期待」為搜索之標準，仍均需符合一定程序要求，立法者特別於法條中確立對「在場權」之保障[36]，藉由在場權之保障，可以監督追訴機關執行搜索是否合法，亦可為日後於訴訟上爭執之證明管道，此屬於被告於刑事訴訟法上之基本權保障[37]。在場權內容包括第 145、150 條應使當事人在場，依第 125 條應付與證明書於受搜索人，可見我國對於搜索之想像為一個原則上應公開執行之措施而不具有秘密性，然而以 IMSI-Catcher 取得被告之確切手機位址，其性質自然不可能使被告即時在場見證如何操作 IMSI-Catcher 而取得其位址，故被告無法行使在場權之保障而糾正程序違法之處，與搜索扣押之性質不符，結論上即不可以搜索扣押相關規定為授權基礎。最高法院則是直接認為我國搜索與美國法不相同，不以是否侵害合理隱私期待作為判斷搜索之標準，我國之搜索應係指物理性侵入有形空間或侵害受搜索人財產權而對其身體、物件、電磁紀錄及住宅或其他處所進行蒐證，又其中搜索電磁紀錄需以已存在之電磁紀錄為限，並不能以秘密方式進行搜索，與 IMSI-Catcher 之概念、方法及本質均不相同，故不可適用或類推適用搜索之規定，與本文之結論相同。

---

[36] 薛智仁（2018.04），〈GPS 跟監、隱私權與刑事法－評最高法院 106 年度台上字第 3788 號刑事判決〉，《月旦裁判時報》，70 期，頁 49。

[37] 林鈺雄，前揭註 1， 頁 442。實務上相同見解見最高法院 94 年度台上字第 4929 號刑事判決。

doi:10.6342/NTU202302425

一審判決有另提及不可以第 228 條第 1 項、第 230 條第 2 項與第 231 條第 2 項為授權基礎，因 IMSI-Catcher 已相當程度干預基本權，認為其屬於類似羈押、搜索扣押等干預基本權程度較嚴重之「強制偵查」，故應有待立法者立法授權之而不可以「科技進展」一概取代「法律保留」之保障，即須有法律明文之規定方可為之，最高法院則是認為上開條文性質僅為抽象誡命。

對於偵查概括條款之定位，有文獻指出因該條款缺乏明確性，立法者無法於文字中使人民得以預見干預之基本權範圍與程度，亦缺乏法院判決將認定標準明確化，於刑事政策上亦會造成程序警察化之趨勢，故應將其解釋成純粹任務分配之規定[38]，若按照此說之想法，因本條非強制處分之授權條款，自不可為 IMSI-Catcher 或是任何偵查行為之授權基礎。

相對的，有論者認為因為隨著科技進步發展更多不同監控科技，以及對於基本權、干預等概念之擴張，越來越多訴訟行為被視為「刑事訴訟上之基本權干預」，造成法律授權基礎不足之問題，但若要求所有刑事訴訟上之基本權干預均須有獨立且明確之法律規定可能緩不濟急，延宕追訴之效率，故可參考公法上「層級化法律保留原則」（abgestufte Vorbehalte）之概念，即如釋字第 443 號所說明之：「何種事項應以法律直接規範或得委由命令予以規定，與所謂規範密度有關，應視規範對象、內容或法益本身及其所受限制之輕重而容許合理之差異」，故所謂「門檻理論」主張：如果干預基本權達一定程度，即須明確且獨立之授權基礎，反之，若干預程度較為輕微如短期跟監，則以一般授權基礎即可為之（刑事訴訟法第 230 條第 2 項、第 231 條），而我國實務 102 台上 3522 判決亦已認為短期跟監得以一般授權基礎為授權基礎即可[39]。然而仍需檢驗干預基本權之程度，至於如何審查干預基本權之程度，則有提出幾個具體標準，包含「是否為已有立法明確具體授權之行為、是否為干預古典基本權利清單之行為、是否為符合刑法構成要件該當性之行

[38] 薛智仁，前揭註 25， 頁 245-253。
[39] 林鈺雄，前揭註 1， 頁 321-325。

doi:10.6342/NTU202302425

為」，若為肯定，則應認為需有另立授權基礎[40]。暫不論偵查概括條文之效力，以我國目前之實務見解，於車輛裝設 GPS 記錄車輛於公開場所移動位置，以掌握個人之生活作息圖像，尚缺乏合適之刑事訴訟法授權基礎，而有待立法者立法補足，故為基本權違法侵害之行為，而 IMSI-Catcher 可以取得個人「隨身攜帶」之手機位址，不論其位於公開或非公開場所，不同於車輛尚需停放於一定地點（路邊停車位、地下停車場均有可能），與個人真正所在位置尚有差距，IMSI-Catcher 對基本權之侵害程度應較裝設 GPS 更為嚴重，且若連續取得手機位址，累積之資訊所帶來的解讀力可能可以進一步得知個人之人格圖像，故亦無法以概括授權條款為之。

第四目　警察職權行使法

雖然警職法有規定得以科技方法取得一定資訊之規定，例如第 9 條以科技方法取得集會遊行或其他公共活動參與者之行為活動、第 10 條以科技方法於可能發生犯罪案件之公共場所或公眾得出入之場所蒐集資料與第 11 條以科技工具對無隱私或秘密合理期待之行為或生活情形蒐集資料，雖然以 IMSI-Catcher 取得個人手機位址之行為看似可以對應「以科技方法」搜集資料條文之文意，然而這些條文目的為「為維護治安之必要時」、「為防止犯罪」，可見警職法之功能是規範警察預防犯罪行政勤務之作用法[41]，並非刑事訴訟法之目的為追訴「已發生」之犯罪，故不可適用警職法相關規定為授權基礎[42]。

第五目　個人資料保護法

依據個資法第 15 條第 1 款規定，公務機關應出於特定目的，而得於執行法定職務必要範圍內，蒐集處理個人資料，而使用 IMSI-Catcher 取得個人手機位置，進而推知出個人位址，某種程度而言亦為國家追訴機關取得個資法第 2 條個人資料之行為。然而，從規範性質上而言，個資法第 15 條僅為告知「公務機關」於「何

[40] 林鈺雄（2007.04），〈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》，96 期，頁 214-221。
[41] 另可參照最高法院 109 年度台上字第 4338 號刑事判決。
[42] 王士帆，前揭註 16， 頁 95-96。

doi:10.6342/NTU202302425

種情況下」蒐集處理資料方為合法，本身並無明確規定個案上究竟取得資料之要件為何，非屬「作用法」，個資法第 15 條第 1 款應僅作為連結各行政組織法之用，以劃分「各行政機關之間」權限範圍與任務分配，然而欲向人民蒐集處理資料，屬於「人民與機關之間」之法律關係，即不可以此組織權限劃分規定作為授權規定，否則可能違反釋字第 535 號之意旨[43]。於刑事訴訟領域，因該規範缺乏要件與範圍之明確性，更不可能為授權基礎，否則只會成為包山包海的另一概括授權條款[44]。

第二款　小結

綜合以上之分析，目前於刑事訴訟上使用 IMSI-Catcher 調查手機位址定位，仍缺乏具體之法律授權基礎，故為違法之基本權侵害行為[45]。因缺乏法律授權基礎，即毋庸審查此行為是否符合比例原則（實質阻卻違憲事由）。一審判決亦有相同結論，認為因欠缺授權基礎，故認違反法治國以及法律保留原則之憲法誡命。然而於二審判決中，前述已提及其內容未明確表明使用 IMSI-Catcher 是否干預當事人之隱私權，即便退一步言，肯定二審的意思為使用 IMSI-Catcher 具有干預當事人隱私權之性質，二審卻直接以憲法第 23 條為審查，認為追訴犯罪屬於正當之目的，衡量「國家刑事追訴之利益」」與「對個人隱私權之影響」後，認定未逾越依社會通念所認不能容忍的界限故此「行為」符合憲法第 23 條之比例原則，省略了應先審查是否符合憲法第 23 條的形式法律保障之要求，並未進一步探究現行法律是否有法律授權基礎，而直接審查實質阻卻違憲事由。

第五項　證據使用禁止

即便追訴機關可利用強制處分達到取得證據之目的，然而需符合一定實體以及程序規定，以保障人民之權利，若違反相關取證規定，即違反證據「取得」禁止之規範。而後續法院於訴訟上禁止特定證據作為判決認定基礎，則為證據「使用」

---

[43] 謝碩駿（2019.04），〈行政機關蒐集個資之法律依據〉，《月旦法學教室》，198 期，頁 14-16。另可參考釋字第 535 號：「查行政機關行使職權，固不應僅以組織法有無相關職掌規定為準，更應以行為法（作用法）之授權為依據，始符合依法行政之原則」。

[44] 薛智仁，前揭註 35， 頁 50。

[45] 林鈺雄，前揭註 30，頁 28-30。

doi:10.6342/NTU202302425

禁止之範疇。其中若為違法取得之證據，而後續為法院認定禁止使用，因依附於前階違法之取證行為，故為所謂「依附性證據使用禁止」或是「非自主證據使用禁止」[46]。經前述分析，以 IMSI-Catcher 取得證據缺乏合適法律授權基礎，故為違法之偵查行為，故以下討論藉由 IMSI-Catcher 取得直接以及間接證據相關問題。

第一款　IMSI-Catcher 取得之直接證據

追訴機關使用 IMSI-Catcher 取得個人手機精確位址以推測出被告實際所在地點，此「位址資訊」因違反法律保留原則，為侵害個人資訊自決權之行為，立法者之所以立法限制可使用之強制處分，是為了使人民預知國家追訴行為之界限，藉由法律決定國家與被告之資訊地位，故對於無法律規定之強制處分，國家有不干預（不作為）之義務，若違反不干預之義務則可能會延伸出法院禁止證據使用該證據之義務[47]。

於我國應依刑事訴訟法第 158 條之 4 判斷其證據能力，而本條依附性證據使用禁止究竟應依何種標準判斷，學說以及實務曾題出許多見解，包含權利領域理論、規範保護目的理論、權衡理論以及三階段審查基礎說等[48]。

若以我國目前實務主要採取之權衡理論為刑事訴訟法第 158 條之 4 之判斷標準[49]，可以認為該違法取得證據違背法定程序，因根本就無「法定程序」存在，遑

[46] 林鈺雄（2020.09），《刑事訴訟法 下冊》，10 版，頁 15-16，新學林。
[47] 林鈺雄，前揭註 46， 頁 31。
[48] 林鈺雄，前揭註 46， 頁 22-31。
[49] 參照最高法院 93 年度台上字第 664 號刑事判決：「刑事訴訟，係以確定國家具體之刑罰權為目的，為保全證據並確保刑罰之執行，於訴訟程序之進行，固有許實施強制處分之必要，惟強制處分之搜索、扣押，足以侵害個人之隱私權及財產權，若為達訴追之目的而漫無限制，許其不擇手段為之，於人權之保障，自有未周。故基於維持正當法律程序、司法純潔性及抑止違法偵查之原則，實施刑事訴訟程序之公務員不得任意違背法定程序實施搜索、扣押；至於違法搜索、扣押所取得之證據，若不分情節，一概以程序違法為由，否定其證據能力，從究明事實真相之角度而言，難謂適當，且若僅因程序上之瑕疵，致使許多與事實相符之證據，無例外地被排除而不用，例如案情重大，然違背法定程序之情節輕微，若遽捨棄該證據不用，被告可能逍遙法外，此與國民感情相悖，難為社會所接受，自有害於審判之公平正義。因此，對於違法搜索、扣押所取得之證據，除法律另有規定外，為兼顧程序正義及發現實體真實，應由法院於個案審理中，就個人基本人權之保障及公共利益之均衡維護，依比例原則及法益權衡原則，予以客觀之判斷，亦即宜就(一)違背法定程序之程度。(二)違背法定程序時之主觀意圖（即實施搜索、扣押之公務員是否明知違法並故意為之）。(三)違背法定程序時之狀況（即程序之違反是否有緊急或不得已之情形）。(四)侵害犯罪嫌疑人或被告權益之種類及輕重。(五)犯罪所生之危險或實害。(六)禁止使用證據對於預防將來違法取得證據之效

doi:10.6342/NTU202302425

論相關程序作為被告與第三人之程序保障配套可言，且通常被告根本無從得知此秘密偵查措施實施，造成被告訴訟上防禦不利益，且禁止此證據應有助於預防未來同類之違法取證，應予禁止使用[50]。

一審亦認為，因追訴機關自始未試圖或實際取得任何檢方核准或法院令狀，因違反法治國、法律保留相關原則而認為該資訊無證據能力。另外一審判決亦基於相同理由排除承辦小隊長之證詞，因其證詞內容包含使用 IMSI-Catcher 後而直接獲知之過程及資訊，為避免相同證據內容，經轉換形式而「復活」（從書面變成言詞），故亦排除此部分證據能力。

第二款　IMSI-Catcher 取得之間接證據

然而於實務上追訴機關以 IMSI-Catcher 發動偵查，並不會僅止於取得被告位址而已，追訴機關會以這個位址做偵查起點，例如先前之新聞媒體報導，警察得知位址之後發動「逮捕」行蹤成謎之被告以搶救人質，或是像本案，警察藉由此資訊報請檢察官指揮而按照相關程序「合法」向法院聲請搜索票，以進行「搜索」被告之詐騙機房扣押恐嚇取財相關證據，扣押手機、使用之 SIM 卡以及毒品等，這些證據才是「主要」認定是否構成恐嚇取財之證據，此即涉及證據使用禁止之射程範圍，即「放射效力」的問題。

我國放射效力之理論發展放射效力主要是承襲自於美國法之「毒樹果實理論」，指的是經由非法之證據取得（毒樹），再經由合法之程序衍生出其他證據，因其為毒樹所衍生之毒果，故亦應不得使用，以保護依附性證據使用禁止之目的。然而雖有主張違法之合法衍生證據皆須一律排除或一律准以使用之見解，然而各自有癱瘓追訴犯罪之可能或是鼓勵追訴機關違法取得證據之缺失，故現在無論是美國或

果。(七)偵審人員如依法定程序，有無發現該證據之必然性。(八)證據取得之違法對被告訴訟上防禦不利益之程度等情狀予以審酌，以決定應否賦予證據能力」。

[50] 王士帆（2023.05），〈最高法院 M 化車判決——破案神器跌落神壇〉，《檢察新論》，32 期，2023 年 5 月，頁 83-85。

doi:10.6342/NTU202302425

是德國均採取較為折衷之立場，而發展出毒樹果實之例外，包含獨立來源、必然發現與稀釋例外等以作為放射效力範圍之劃分標準[51]。

我國雖有部分實務見解明文指出我國並無引進英美之毒樹果實理論，然而大多仍有引進相關概念，如 97 台上 4797 號判決認為：「實施刑事訴訟程序之公務員違法取得證據後，進一步衍生取得之證據，縱與先前之違法取證具有如毒樹、毒果之因果關聯性，然該進一步採證之程序，苟屬合法，且與先前違法取證係個別獨立之偵查行為，刑事訴訟法並無排除其作為證據之明文。必先前違法之取證，與嗣後合法取得證據之行為，**二者前後密切結合**致均可視為衍生證據取得程序之一部，該衍生證據之取得因而存在違法事由，始得依其違法之具體情況，分別適用刑事訴訟法證據排除之相關規定，判斷其有無證據能力」，可認為我國實務並未採取一律使用或排除衍生證據之立場，主要是以前階違法取證與後續合法之取證行為是否有「直接之因果關係」或「是否有介入其他偵查行為」為判準，可見我國已於案件中實質運用毒樹果實理論[52]。

以本案為例，一審法院即認為因警察非直接且唯一以 IMSI-Catcher 取得之位址為聲請搜索票基礎，IMSI-Catcher 僅作為縮小範圍之用，尚調取相關通信紀錄確定手機使用基地台位址、進行實地跟監以及查詢之車牌確定人別以及前科等行為，才報請指揮向法院聲請搜索票進入被告詐騙機房進行搜索，中間介入許多不同偵查行為，故法院認為以 IMSI-Catcher 取得被告位址與後續發動搜索所得，彼此之間的連結關係已屬薄弱，無直接因果關係，故不排除這些搜索所得之證據能力。然而本案經搜索而扣押「年籍資料名冊」、「手機」、「向他人收購之 SIM 卡」等物，足以認定有使用這些手機撥打電話為恐嚇取財之行為，雖一審認定其證明力不足而無法證明被告等人有罪，但設想若於該位址搜索扣押到更為充足之證據，可能即可證明被告等人確實有實行恐嚇取財之行為。換句話說，本案判定被告有罪與否

[51] 林鈺雄，前揭註 46， 頁 37-40；王兆鵬/ 張明偉/ 李榮耕（2020），《刑事訴訟法（上）》，5 版，頁 157-162，新學林。

[52] 同見解：99 年度台上字第 6279 號；王兆鵬/ 張明偉/ 李榮耕，前揭註 51， 頁 157-158。

doi:10.6342/NTU202302425

之關鍵並非 IMSI-Catcher 所取得之位址資訊，有無排除 IMSI-Catcher 取得之「直接」證據能力與否，對於本案有罪與否之認定可能並無關連。

另外，前述已指出二審不應逕以憲法第 23 條判斷取得 IMSI-Catcher 是否合法，二審於判斷證據能力亦出現矛盾之處：在認為使用 IMSI-Catcher 符合憲法第 23 條的要求而為「合法」之取證行為後，又論述取得的直接或間接證據皆需經過刑事訴訟法第 158 條之 4 進行權衡，而權衡追訴犯罪之後認有證據能力。然而刑事訴訟法第 158 條之 4 屬於證據使用禁止的概括條款，其前提是針對「國家違法」取得的證據（依附性證據使用禁止）進行權衡，故二審對於以 IMSI-Catcher 取得證據的行為究竟為違法或合法並未明確解釋[53]，此亦係被最高法院指摘有瑕疵之部分。

第三款　小結

以 IMSI-Catcher 取得個人手機位址而推測出個人之位址資訊（直接證據），雖然可以利用刑事訴訟法第 158 條之 4 權衡後排除其證據能力，然而因為後續尚會發動其他合法之偵查行為，例如向法院聲請搜索票進行搜索扣押、現場實地跟監，即會稀釋前階違法之程度，故依我國實務一貫之立場通常會得出不排除衍生證據之結論，然而後面這些衍生證據可能才是判斷有罪與否之關鍵，既切斷與前階段違法使用 IMSI-Catcher 之關聯，使得前階段為保障人權而排除 IMSI-Catcher 證據能力之努力前功盡棄。

第三節　科技偵查法草案評析

2020 年 9 月 8 日法務部公告「科技偵查法」草案，目的為「進行必要之科技偵查作為，為規範偵查機關實施此類調查之合法性，切實保障人民基本權，並避免犯罪調查之手段落後於科技發展之腳步，影響國家安全及社會秩序」，故公告此草案並給予人民 5 日表達意見之機會。然而引發許多討論與反彈[54]，後法務部稱會再

[53] 林容，前揭註 27， 頁 152。
[54] 例如：全國律師聯合會（2020.09.17），〈本會對法務部科技偵查法草案之新聞稿〉，http://www.twba.org.tw/News_detail.asp?N_id=1252（最後瀏覽日：2021.10.02）。

doi:10.6342/NTU202302425

蒐集各方意見，彙整進行修正，之後才會向行政院呈報進行立法程序[55]，但至目前為止，皆無進一步之行動，本文將結合上述德國法之借鑒與我國目前之實務發展已提出建議。

與本文較相關的為第 5 條之規定：

科技偵查法第 5 條

（第一項）偵查中檢察官認有必要時，得使用全球定位系統或其他具有追蹤置功能之科技設備或技術實施調查。（第二項）檢察事務官，司法警察官或司法警察因調查犯罪情形及蒐集證據，必要時得報請檢察官許可後，實施前項調查檢察官，檢察事務官，司法警察或司法警察實施前二項調查之累計間，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。（第三項）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。（第四項）前二項之聲請經法院駁回者，不得聲明不服。

第 5 條立法說明中揭示「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遁蹤位置，均受本法效力所及，應遵守本法之規範。」可見其預計將 GPS、IMSI-Catcher 等所有可能之追蹤人或使用之物（車、手機）之方式「包裹」成單一條規定。

然草案如此規定似有不當。首先在於以第 5 條整體採包裹立法，單以其中提及之 GPS 比較 IMSI-Catcher：於德國使用 IMSI-Catcher 適用第 100i 條之授權規定，GPS 則是適用第 100h 條，為不同之規定，比較兩者干預基本權之程度，手機為個人隨身攜帶之物品，同前文之描述就像個人隨身之追蹤器，與個人關係相較於裝設

[55] 中央廣播電台（2020.10.14），〈科技偵查法 蔡清祥：待彙整研議各界意見後修正提出〉，https://www.rti.org.tw/news/view/id/2082213（最後瀏覽日：2021.10.02）。

doi:10.6342/NTU202302425

GPS 於車輛等物體上更為緊密，獲得之位址資料也更為精確，干預資訊自決權之程度較嚴重[56]，並且裝設 GPS 可能僅會影響同樣使用相同被裝設 GPS 物體（例如車輛）之人，而 IMSI-Catcher 會影響訊號範圍內無法辨識之不特定第三人，使其無法進行通訊，其影響之「範圍」應更為廣泛；最後，第三章提及 IMSI-Catcher「技術上」甚至可以達到監聽、打開目標手機麥克風進行竊聽之功能，為追訴機關所濫用之科技風險更高，與單純使用 GPS 進行定位所面臨之風險不同，故本文認為不應任意將這些所有科技手段合併立法[57]。

於受調查人之部分，雖於第 6 條第 2 款、第 8 條、第 22 條第 1、2 項反覆提及「受調查人」此概念，文意上可認為是發動 IMSI-Catcher 所針對之對象，然而事實整部科技偵查法並未定義何謂「受調查人」之範圍，不同於德國直接於第 100i 條引用電信監察規定將範圍限制於「被告或為被告發送、傳達或收受通訊之人或是被告使用其通訊系統之人」，等同於第 100a 條電信監察之範圍，於我國或許可考慮直接引入通保法第 4 條「受監察人」之概念[58]，明確其範圍。

管轄之部分，第 5 條規定原則由檢察官下令為之即可，第 7 條規定緊急時司法警察亦可發動此權限，於整體調查時間超過 2 個月即需經該管法院許可。本文認為，暫且不論 IMSI-Catcher 其他功能濫用之風險，而僅論其調取手機位址資訊之功能而言，雖然單一個位址資訊可能無足輕重，但透過長時間調取片段之位址資訊，即可能分析拼湊出一個人的移動圖像，甚至分析出住居所、工作地點甚至是喜好與傾向，而長達 2 個月之資料儲存，經比較與分析，應已經可以達到這種效果[59]，況且比較類似之強制處分如通保法第 3-1、11-1 條調取手機通信紀錄之位址資

---

[56] 林容，前揭註 27， 頁 143。

[57] 林彥均（2023.04），〈自基本權干預建構我國科技偵查之層級化授權體系－「科技偵查法」草案 GPS 及 M 化車部分之評析〉，《法學叢刊》，68 卷 2 期，頁 32-33。

[58] 通保法第 4 條：「本法所稱受監察人，除第五條及第七條所規定者外，並包括為其發送、傳達、收受通訊或提供通訊器材、處所之人。」然而本條除了用語與科技偵查法之「受調查人」不同。

[59] 另可見：臺北律師公會（2020.09.14），〈台北律師公會就法務部公告預告 「科技偵查法」草案之聲明〉，
https://www.tba.org.tw/%E6%9C%83%E5%93%A1%E6%9C%8D%E5%8B%99/%E6%96%B0%E8%81%9E%E7%A8%BF/%E6%96%B0%E8%81%9E%E7%A8%BF%E5%85%A7%E9%A0%81/?ID=5887（最後瀏覽日：2021.10.02）。

doi:10.6342/NTU202302425

訊（三角定位），其獲得之資訊較 IMSI-Catcher 更不精準，尚為原則法官保留，除非有第 11-1 條第 1 項但書之急迫之狀況或是符合第 11-1 條第 3 項重罪原則，才可由檢察官逕行為之且若為第 11-1 條第 1 項但書之情形，需於兩日內聲請補發調取票，反而使用 IMSI-Catcher 進行精準定位僅由職司追訴犯罪之檢察官為之，不甚妥當。

第 8 條第 2 項有關通知義務亦有相同問題，草案認為僅在調查期間超過 2 個月才需進行通知，立法理由稱因 2 個月內之短期位置偵查對隱私權干預仍屬「輕微」，故為層級化之規定而不需通知受調查人，然通知受調查人之目的是因為無論為檢察官下令或法院命令允許使用 IMSI-Catcher 之情形，均為不公開之程序，當事人無法透過公開程序表達其意見，亦無法於處分執行當下知悉為干預之事實，通知受調查人是為了確保其可對該處分進行救濟，德國刑事訴訟法第 101 條第 4 條亦是基於這個想法，故無論受干預之時間長短均應通知受調查人，況且於檢察官命令之情形，第 22 條第 1 條允許受調查人向法院聲請撤銷或變更檢察官之命令，如果未經通知，受調查人即無法得知受干預之事實，遑論對其提起救濟而聲請撤銷。

最後，科技偵查法亦欠缺對第三人之保障，為因應 IMSI-Catcher 一啟動即不可避免影響到無關第三人之技術特性，第三人之手機位址資訊亦有可能被 IMSI-Catcher 儲存蒐集，雖係為匿名比對而未確認身分，通常實務使用完畢亦會刪除，但為避免資料濫用之風險，亦應如德國刑事訴訟法第 100i 條第 2 項課與一律刪除第三人資訊之義務或是另外制定偶然發現資料之使用規定。

doi:10.6342/NTU202302425

第六章　結論

目前實務上追訴機關若想達到「取得手機定位」之目的，可能會使用通信紀錄（基地台三角定位）或是 IMSI-Catcher 等科技方法為之。

以我國法之繼受來源德國法而言，德國早就在 1928 年就有有調取通信紀錄之授權規範，後為因應歐盟之不同指令，陸續進行多次修法，目前刑事訴訟法規範調取通信紀錄資料來源有二：一是電信事業為商業目的所儲存之通信紀錄，二是立法規範電信事業需「強制」儲存所有人之通信紀錄。另外，為因應調取通信紀錄可能帶來之基本權侵害，立法者另訂有相關程序規範，將調取通信紀錄定義為原則上應公開為之的強制處分。

至於 IMSI-Catcher 技術，雖然德國一開始使用時也欠缺合法之授權基礎，然而於 2002 年就立法新增授權基礎，隨後實務上又透過判決解釋將靜默簡訊納入授權範圍，亦有配套相關程序規定（管轄、期間、命令內容、救濟等）。

回到我國目前之法治狀態，雖然同 IMSI-Catcher 經過一段「法無明文」之時期，然我國於 2014 年已將調取通信紀錄正式納入通保法之授權範圍，以實現釋字第 631 號保障秘密通訊自由之見解，因立法過程倉促，故細看條文內容與德國刑事訴訟法第 100g 條之規定相較，我國不管是在規範本身或是配套之程序仍有許多不足之處。

欲調取通信紀錄則必須先有所謂「通信紀錄」存在，我國目前尚未有同德國極具爭議性之強制儲存通信紀錄規定，而係仰賴電信事業基於商業目的所儲存之通信紀錄，然而目前通保法第 3-1 條與第 11-1 條並無法顯示出先由電信是業處理儲存後再由追訴機關為調取之兩道程序分為把關之關係。

而調取規定本身亦存在不少問題：首先是將通訊使用者資料、通信紀錄、過去與實時位址資訊等一併包裹處理，忽略這些資訊之間干預基本權種類與程度皆不相同，而一併規定於第 11-1 條內，相較於德國以「過去儲存之位址資訊、實時或向未來之位址資訊、其他通信紀錄、通信使用者資料」為基本權干

doi:10.6342/NTU202302425

預程度最嚴重至輕微順序設計不同要件，我國則有授權密度明顯不足之問題，而有待未來修法以為區分。於實體門檻部分，應刪除立法原因不明確之非輕罪原則門檻，以較為彈性之設計符合偵查之需求。最後有關程序配套之部分，因通保法當初立法時係僅有針對通訊內容之「通訊監察」，部分如發動對象、執行期限與事後抗告準抗告等監督機制之法條用語多以「通信監察」為之，是否可直接適用於通訊監察仍有疑問，而有待修法明確之。

自 2020 年之 IMSI-Catcher 一審判決認定使用 IMSI-Catcher 所得之直接證據無證據能力以及科技偵查法草案公佈之後，學界亦有不少建議修法之呼籲，實務上也一再於各種新聞中顯示確有此偵查工具之需求，然而截至目前 2022 年為止仍無實質進展，這些建議就如同狗吠火車，然而轉向我國法律所多參考之德國，其亦是先經過追訴機關先行使用此類偵查工具而喚起國內之討論與重視，隨後立法建立完善之實體發動要件與程序保障。

參考德國刑事訴訟法第 100i 條之條文與實務討論，就制定這些新興科技偵查使法之授權基礎而言，應釐清其干預之基本權以及干預態樣究竟為何，是否可納入目前既有之強制處分體系，而就分析之後，可以發現追訴機關使用 IMSI-Catcher 之目的並非關心手機是否進行通訊或是窺視通訊內容，充其量僅為得知手機之真確位置，進而得知行動裝置使用者之位址，故 IMSI-Catcher 係干預資訊自決權而非秘密通自由，且係秘密為之而甚至有影響無辜第三人之可能，而無法納入現有之強制處分體系，故應另立授權基礎為之。

考慮其實體授權門檻時，可將其造成之侵害程度等納入考量，因追訴機關使用 IMSI-Catcher 之不干預祕密通訊自由，僅干預資訊自決權，而無法得知其可能與思想較為相關之通訊內容，故干預門檻不需較通訊監察之相對法官保留更高。最後，國家以強制處分干預人民權利時，亦應賦予人民一定程序保障以為救濟，以 2020 年之科技偵查法而言，雖然內有部分程序規定，然對照德國作為第 100i 條之程序配套 101 條，仍略顯不足，例如對受調查人範圍界定、通知受干預事實與刪除等規定不足，特別是考慮到 IMSI-Catcher 具有影響周邊不特

doi:10.6342/NTU202302425

定第三人進行通訊之特性，亦有可能為追訴機關短期收集資料，應規定對第三人資訊之刪除或再利用規定。

doi:10.6342/NTU202302425

參考文獻

一、中文部分

（一）專書

1. 王兆鵬/ 張明偉/ 李榮耕（2020），《刑事訴訟法（上）》，5 版，新學林。
2. 李惠宗（2020），《憲法要義》，8 版，元照。
3. 李震山 （2020），《人性尊嚴與人權保障學術論文集》，5 版，元照。
4. 林鈺雄（2020.09），《刑事訴訟法 上冊》，10 版，新學林。
5. 林鈺雄（2020.09），《刑事訴訟法 下冊》，10 版，新學林。
6. 林鈺雄（2021.09），《刑事訴訟法實例解析》，4 版，新學林。
7. 許育典（2019.09），《憲法》，9 版，元照。
8. 連孟琦（2016.09），《德國刑事訴訟法——附德國法院組織法選譯》，1 版，元照。
9. 曾德文（2013.08），《資通科技犯罪偵查. 通訊篇》，自刊。
10. 廖訓誠、陳芳振、顏宥安（2016.10），《犯罪偵查技術》，陳芳振自刊。

（二）學位論文

1. 黃政龍（2016.07），《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研究所博士論文。
2. 唐欣悅（2019.07），《私人通信紀錄強制供公益目的使用之合憲性研究》，國立臺灣大學法律學研究所碩士論文。
3. 施育傑（2020.05），《數位、科技與刑事程序干預處分 ──資訊框架理論之建構》，國立政治大學法律學研究所博士論文。
4. 林容（2021.03），《隱密科技偵查與基本權保障》，國立臺灣大學法律學研究所碩士論文。
5. 陳敬于（2018.04），《犯罪偵查中位址資訊之取得及使用》，國立臺北大學法律學研究所碩士論文。

doi:10.6342/NTU202302425

6. 邱紹洲（2001），《通聯紀錄在犯罪偵查上之應用》，中央警察大學刑事警察研究所碩士論文。

（三）期刊文獻

1. Mark A. Zöller（著），王士帆（譯）（2016.04），〈處在德國法與歐洲法緊張氛圍下的通信紀錄調取〉，《月旦法學雜誌》，252 期，頁 223-235。
2. 王士帆（2020.12），〈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〉，《司法週刊》，2036 期，頁 2-3。
3. 王士帆（2021.04），〈德國科技偵查規定釋義〉，《法學叢刊》，66 卷 2 期，頁 85-132。
4. 王士帆（2022.03），〈M 化車法制出路－德國 IMSI-Catcher 科技偵查借鏡〉，《臺北大學法律論叢》，121 期，頁 55-117。
5. 王士帆（2023.05），〈最高法院 M 化車判決——破案神器跌落神壇〉，《檢察新論》，32 期，2023 年 5 月，頁 78-86。
6. 何明洲（2006.09），〈通聯分析在科技偵查上應用之研究〉，《警學叢刊》，37 卷 2 期，頁 1-20。
7. 何信慶（2014.07），〈從立法審議過程談新修正通訊保障及監察法〉，《司法新聲》，111 期，頁 27-50。
8. 吳秋宏（2008.04），〈司法院釋字第 631 號解釋與監聽法制評析（上）〉，《司法周刊》，1385 期，頁 2-3。
9. 李仁淼（2014.01），〈秘密通訊自由與監聽〉，《月旦法學教室》，135 期，頁 6-8。
10. 李仁淼（2020.01），〈一般行為自由與一般人格權〉，《月旦法學教室》，207 期，頁 6-9。
11. 李建良（1997.03），〈基本權利理論體系之構成及其思考層次〉，《人文及社會科學集刊》，9:1 期，39-83 頁。
12. 李榮耕（2010.06），〈論偵查機關對通信紀錄的調取〉，《政大法學評論》，

doi:10.6342/NTU202302425

115 期，頁 115-147。

13. 李榮耕（2014.04），〈簡評二○一四年新修正的通訊保障及監察法－一次不知所為何來的修法〉，《月旦法學雜誌》，227 期，頁 148-175。
14. 李榮耕（2015.09），〈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》，44 卷 3 期，頁 871-969。
15. 李榮耕（2020.04），〈居家電子監控於防疫期間之運用及其法源疑義〉，《月旦醫事法報告》，42 期，頁 93-102。
16. 李震山（2007.09），〈挪動通訊保障與通訊監察天平上的法碼－釋字第六三一號解釋評析〉，《台灣法學雜誌》，98 期，頁 283-291。
17. 林彥均（2023.04），〈自基本權干預建構我國科技偵查之層級化授權體系－「科技偵查法」草案 GPS 及 M 化車部分之評析〉，《法學叢刊》，68 卷 2 期，頁 19-41。
18. 林鈺雄（2007.04），〈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》，96 期，頁 189-232。
19. 林鈺雄（2013.12），〈通訊監察之修法芻議——通訊保障及監察法之部分修正條文一〉，《萬國法律》，192 期，頁 25-39。
20. 林鈺雄（2014.01），〈通聯紀錄之調取－－從幾則基地台相關判決談起〉，《台灣法學雜誌》，239 期，頁 49-62。
21. 林鈺雄（2021.02），〈科技偵查概論（上）──干預屬性及授權基礎〉，《月旦法學教室》，220 期，頁 46-57。
22. 林鈺雄（2023.02），〈以 M 化車探知手機位置資訊之合法性〉，《月旦法學教室》，244 期，頁 26-29。
23. 林豐裕、李欣倫、李鎮宇（2014.07），〈簡評 2014 年通訊保障及監察法增修條文－－兼論新法對於實務運作之衝擊〉，《檢察新論》，16 期，頁 60-71。
24. 張永明（2018.02），〈一般行為自由與一般人格權作為憲法保障之基本

doi:10.6342/NTU202302425

權〉，《月旦法學雜誌》，273 期，頁 28-46。

25. 張麗卿（2014.06），〈通訊保障及監察法之修正與評析〉，《月旦法學雜誌》，229 期，頁 25-45。
26. 許宗力（2003.09），〈基本權利：第六講—基本權的保障與限制（上）〉，《月旦法學教室》，11 期，頁 64-75。
27. 陳重言（2014.07），〈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》，16 期，頁 40-59。
28. 陳新民（1992.07），〈論憲法人民基本權利的限制（上）〉，《律師通訊》，154 期，頁 21-38。
29. 陳韻竹（2017.05），〈論歐盟法院 No. C-203/15 判決之國家資料保留規範議題〉，《科技法律透析》，29:5 期，頁 49-56。
30. 黃朝義（2014.04），〈通聯記錄調取與另案監聽修法評析〉，《中央警察大學法學論集》，26 期，頁 2-23。
31. 溫祖德（2021.12），〈偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查－從美國聯邦最高法院判決檢視我國法制〉，《政大法學評論》，167 期，頁 171-256。
32. 詹明華、陳弘斌、宋奕賢（2016.03），〈定位技術在犯罪偵查上之應用〉，《刑事科學》，80 期，頁 1-13。
33. 詹鎮榮（2003.09），〈秘密通訊自由〉，《法學講座》，21 期，頁 1-15。
34. 蔡宗珍（2018.02），〈電信相關資料之存取與利用的基本權關連性（上）－德國聯邦憲法法院 BVerfGE 125, 260 與 BVerfGE 130, 151 判決評析〉，《月旦法學雜誌》，274 期，頁 105-132。
35. 蔡宗珍（2018.02），〈電信相關資料之存取與利用的基本權關連性（下）－德國聯邦憲法法院 BVerfGE 125, 260 與 BVerfGE 130, 151 判決評析〉，《月旦法學雜誌》，275 期，頁 67-86。
36. 鄭逸哲、黃沛文（2014.09），〈動機雖屬正當，立法未免粗糙──簡評通保

doi:10.6342/NTU202302425

法關於「調取行為」之修正〉，《月旦法學雜誌》，232 期，頁 18-27。

37. 薛智仁（2014.12），〈司法警察之偵查概括條款？－評最高法院一○二年度台上字第三五二二號判決〉，《月旦法學雜誌》，235 期，頁 235-256。

38. 薛智仁（2018.04），〈GPS 跟監、隱私權與刑事法－評最高法院 106 年度台上字第 3788 號刑事判決〉，《月旦裁判時報》，70 期，頁 42-60。

39. 薛智仁（2018.12），〈刑事程序法定原則〉，《月旦刑事法評論》，11 期，頁 20-44。

40. 謝碩駿（2019.04），〈行政機關蒐集個資之法律依據〉，《月旦法學教室》，198 期，頁 14-16。

二、德文部分

（一）註釋書

1. Becker, Jörg-Peter/ Erb, Volker/ Esser, Robert/ Graalmann-Scheerer, Kristen/ Hilger, Hans/ Ignor Alexander (Hrsg.), Löwe- Rosenberg Großkommentar, Die Strafprozessordnung und das Gerichtsverfassungsgesetz Band 3/1 §§94-111a, 27. Aufl.,2019. (zitierte: LR-StPO)

2. Meyer-Goßner, Lutz/ Schmitt, Bertram/ Köhler, Marcus, Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 65. Aufl., 2022. (zitierte: Meyer-Goßner/Schmitt-StPO)

3. Hannich, Rolf (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl., 2019.(zitierte: KK-StPO).

4. Graf, Jürgen Peter (Hrsg.), Beck'scher Online-Kommentar StPO mit RiStBV UND MiStra, 39. Ed. 1.10.2021. (zitierte: BeckOK-StPO)

5. Widmaier, Gunter/ Satzger, Helmut/ Schluckebier, Wilhelm (Hrsg.), Strafprozessordnung, 4. Aufl., 2020.

（二）期刊文獻

doi:10.6342/NTU202302425

1. Bär, BGH: Verwertung von mittels „stiller SMS“ erlangten Standortdaten, MMR 2018, 824 ff.
2. Bär, Der IMSI-Catcher - neue Eingriffsermächtigung in § 100i StPO, MMR 2003, VI ff.
3. Bär, Die Neuregelung zur Erhebung von Verkehrsdaten (§ 100g StPO) – Inhalt und Auswirkungen, NZWiSt 2017, 81 ff.
4. Dalby, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113 ff.
5. Degenkolb, Vorratsdatenspeicherung, Kriminalistik 15, 598 ff.
6. Eisenberg/Singelnstein, Zur Unzulässigkeit der heimlichen Ortung per 'stiller SMS', NStZ 2005, 62 ff.
7. Farthofer, Der Einsatz neuer Ermittlungsmaßnahmen Das Beispiel stille SMS, ZIS 2020, 190 ff.
8. Fox, Der IMSI-Catcher, DuD 2003, 212 ff.
9. Gercke, Rechtliche Probleme durch den Einsatz des IMSI-Catchers, MMR 2003, 453 ff.
10. Harnisch/Pohlmann, Strafprozessuale Maßnahmen bei Mobilfunkendgeräten, HRRS 2009, 202 ff.
11. Hilger, Gesetzgebungsbericht: Über den neuen § 100i StPO, GA 2002, 557, 559 ff.
12. Krüger, Die sogenannte „stille SMS“ im strafprozessualen Ermittlungsverfahren, ZJS 2012, 606 ff.
13. Nachbaur, Standortfeststellung und Art. 10 GG - Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers”, NJW 2007, 335 ff.
14. Nachbaur, Vorratsdatenspeicherung „light“ – Rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, 215 ff.
15. Nöding, Die Novellierung der strafprozessualen Regelungen zur

doi:10.6342/NTU202302425

Telefonüberwachung, StraFo 2007,456 ff.

16. Oehmichen/Mickler, Die Vorratsdatenspeicherung – Eine never ending story?, NZWiSt 2017, 298 ff.
17. Petri, Die Vorratsdatenspeicherung, ZD 2021, 493 ff.
18. Priebe, Vorratsdatenspeicherung und kein Ende, EuZW 2017, 136 ff.
19. Puschke, BGH: * Verwertung von durch „stille SMS“ erlangten Standortdaten, NJW 2018, 2809 ff.
20. Rogall, Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, JZ 2008, 818 ff.
21. Roericht, Die Neureglung der Funkzellabfrage, Kriminalistik 17, 175, 175 ff.
22. Roßnagel, Die neue Vorratsdatenspeicherung, NJW 2016, 533 ff.
23. Roßnagel, Vorratsdatenspeicherung rechtlich vor dem Aus?, NJW 2017, 696 ff.
24. Rückert, „Stille SMS“, NStZ 2018, 611 ff.
25. Ruppert, Rechtsgrundlage für das Versenden sogenannter »stiller SMS«, JR 2019, 300 ff.
26. Smith, Kurzer Zwischenstand zu Recht und Praxis der „stillen SMS“, VR 2012, 334 ff.
27. Zöller, Vorratsdatenspeicherung zwischen nationaler und internationaler Strafverfolgung, GA 2007, 396 ff.

doi:10.6342/NTU202302425