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's Thesis

自動車牌辨識與預防性資料儲備——以刑事程序為中心

Automatic License Plate Recognition and Data Retention: Focusing on Criminal Procedure

李友銓

Yu-Chuan Lee

指導教授：林鈺雄 博士

Advisor: Yu-Hsiung Lin, Dr. jur.

中華民國 113 年 8 月

August 2024

doi:10.6342/NTU202403953

國立臺灣大學碩士學位論文
口試委員會審定書

自動車牌辨識與預防性資料儲備——

以刑事程序為中心

Automatic License Plate Recognition and Data Retention:
Focusing on Criminal Procedure

本論文係李友銓君（學號：R10A21059）在國立臺灣大學法律學系完成之碩士學位論文，於民國 113 年 5 月 31 日承下列考試委員審查通過及口試及格，特此證明

指導教授：林鈺雄

口試委員：

李寧修

王士帆

林鈺雄

謝辭

這本論文得以產出，首先要感謝我的指導教授——林鈺雄老師。大學時期的我曾經只想著早日通過律師考試、順利執業，卻在大四那年選修老師的課程後，開始對「經濟刑法」與「科技偵查」產生濃厚的興趣。能夠拜入老師門下，無疑是我在研究所期間最幸運的事情，除了在學術研究上獲得充足的養分，從老師的言行舉止中亦深受啟發，面對社會上發生的各種怪象，老師總是不畏權貴、仗義執言，同時，也努力在工作與生活之間取得平衡，不願偏廢，此等風骨與生活態度，每每令我心生嚮往。

我也要感謝口試委員王士帆老師和李寧修老師。閱讀兩位老師的著作，總有醍醐灌頂之感，能在感興趣的領域中尋得指引，已是福氣，能請到兩位老師閱讀本篇不成熟的論文，並指點迷津，更是萬幸。文中部分不完整之處若非經兩位老師提出，單憑自己，縱然在書桌前繼續思索個一年半載也不會發覺。另外，我想特別感謝大學時期的導師——薛智仁老師。薛老師總是樂於與我討論人生規劃，在我躊躇該開始律師工作或是參加研究所入學考試時，薛老師說：「反正你現在基本上是不會餓死了，到退休大概還有 40 年的時間，真的要急著進入職場嗎？還是先在研究所培養解決問題的能力，順便享受出國交換的機會？」回首望去，真的很感謝在人生的抉擇路口能遇見薛老師。

謝謝爸媽讓我可以無後顧之憂地完成學業，並支持我到德國漢堡大學交換，開拓視野。謝謝阿嬤、姐姐和妹妹平時對我的照顧。此外，也想謝謝熊門的大家一直以來的陪伴與加油打氣，欣如、家維、白白、怡凡、林容、奕崴、昀霈、家羽、于甄、謦麟、冠宇，特別是珮群，總是主動提醒我畢業待辦的大小事務，同時用優異的表現促使我積極向上，如果沒有你，我大概沒辦法準時畢業。還要謝謝怡萱、惠姐姐和瑋婷時常找我去買飯，讓我走在路上看起來比較不可憐。

謝謝 2414 的大家舉辦了各種活動，幫研究生排憂解悶，李揚、康熙老師、Johnny、尚珉學姐、Ryan、蕭、張、許彣、柔予、Mason、鵬哲，還有一起參加

doi:10.6342/NTU202403953

的薩琳、允然跟黑哥。謝謝藝瑋和 Jenny 雖然對論文毫無概念，卻總是堅定地鼓勵我一定可以順利完成。謝謝法圖的大家經常互相關心、勉勵，最溫暖的玉珠姐、雅茹、脩閔、任麒、Mia、道心、紀晴、苡萱、睿軒、亭宇、日弘、家銘、羽希、承翰。謝謝我的 bro 暐旭學長，從大學一路陪伴我到現在，終於要一起離開這間學校了。還有時不時恐嚇我要讀四年的盧跟阿舉，很高興最後沒有讓你們稱心如意。最後，我想謝謝千瑜在這段時間裡承接了我所有的情緒，深夜離開總圖，有時因為達成進度而歡欣雀躍，有時因為期限將近而焦躁不安，你總是不厭其煩地接起電話，聽我分享枯燥乏味的論文進度話題，謝謝你給我面對明日的勇氣。

大學四年，加上三年的研究生生活，終於要和「台大學生」這個身分告別。很慶幸過去的自己足夠努力，才能讓身邊環繞著優秀且溫暖的人們，祝福大家未來一切順利，也希望能與大家一直保持聯繫。

李友銓

2024 年 8 月於台大總圖 B1 自習室

doi:10.6342/NTU202403953

摘要

我國路口監視器除了一般影像錄製以外，更逐漸新增自動辨識車牌號碼，並予以即時比對的功能。這些經由軟體量化處理的資料，能夠輕易地相互連結，並且發揮同 GPS 偵查的效果——描繪出特定人完整的行車軌跡。不同的是，GPS 偵查尚且是針對具有犯罪嫌疑，或對刑事追訴有所貢獻者；自動車牌辨識系統卻是全天候、持續不間斷地蒐集、儲備一般人民的行車資訊。於此，為了未來可能的偵查需求，授權警察機關得以預防性儲備這些個人資料，就如同一面揮舞打擊犯罪的大旗，一面迫使人民承受其私人生活遭受探知、揭露的風險。則資料蒐集的地點應有何限制？資料儲備應限於多長期間？資料調取又應符合哪些程序要件？遂成為本文研究重點。

本文以德國《刑事訴訟法》第 163g 條為借鏡，具體考察立法過程，以此理解德國立法者嚴格排除預防性車牌辨識資料儲備的實際緣由，同時藉由歐盟法上因課予會員國強制儲備通信紀錄義務所引發的爭議，反思我國實務上預防性儲備車牌辨識資料措施，對於人民基本權利之自由行使可能產生的影響，據以審查現行法下是否具備相當的授權基礎，並提出立法建議。

關鍵詞：科技偵查、車牌辨識、車輛位置資訊、預防性資料儲備、個資保護

doi:10.6342/NTU202403953

Abstract

In addition to regular video recording, surveillance cameras at intersections in our country are increasingly equipped with automatic license plate recognition (ALPR, also known as ANPR) and real-time comparison functionalities. These software-processed data can be easily interconnected, achieving a similar effect to GPS tracking by mapping out the complete driving trajectory of specific individuals. However, unlike GPS tracking, which targets individuals suspected of criminal activity or contributing to criminal prosecution, the ALPR system continuously collects and stores driving information of the general public around the clock. This raises significant concerns: while the police are authorized to reserve these personal data for potential future investigations in the name of crime prevention, the public must endure the risk of their private lives being pried into or exposed. Therefore, questions arise regarding the limitations on data collection locations, the duration of data retention, and the procedural requirements for data retrieval. These issues form the core focus of this study.

This thesis takes Article 163g of the German Code of Criminal Procedure as a principal reference, conducting a comprehensive examination of the legislative process to elucidate the rationale behind the German legislators' stringent exclusion of preventive retention of number plate recognition data. Additionally, it scrutinizes the controversies triggered by the European Union's mandate for member states to retain communication records. Through this analysis, the study critically evaluates the measures adopted in our country concerning the preventive retention of number plate recognition data and their potential impact on the free exercise of fundamental rights by individuals. Based on this thorough evaluation, the thesis reviews the adequacy of the current legal framework and advances legislative recommendations.

Keywords: technological investigation, automatic license plate recognition, vehicle position data, data retention, personal data protection.

doi:10.6342/NTU202403953

簡目

doi:10.6342/NTU202403953

詳目

doi:10.6342/NTU202403953

doi:10.6342/NTU202403953

doi:10.6342/NTU202403953

doi:10.6342/NTU202403953

第一章 緒論

第一節 研究動機

我國大街小巷布滿監視器的事實，早已不是新聞，以臺北市為例，截至 2023 年 5 月 4 日，總計已裝設 1 萬 8,094 支監視器[1]。筆者曾想過，為何我國人民對於這樣的事實不曾感到惶恐，彷彿不會受到監視，反而普遍肯認監視器的架設有助於治安維護，而歡欣鼓舞[2]。目前猜想可能的答案是：正因為監視器被大量地架設，導致資料庫內檔案繁雜，個人生活影像雖然確實被捕捉、拍攝並被儲存於資料庫內，卻某種程度上隱匿於眾多檔案之中而不受揭露。換句話說，人們可能認為路口監視器縱使拍攝到自己的人際往來、私人活動，也會因為在茫茫人海中擷取並挑選出特定人生活影像的過程十分繁複、費時，而確信監視錄影畫面只有在特定情形下，例如涉及犯罪偵查，才會被調取，良好市民的私人生活不至於受到揭露。

不過，這樣的認知可能會隨著自動車牌辨識系統（Automatic License Plate Recognition System）的出現而逐漸瓦解。與過去模糊而難以一眼看出個人身分的監視錄影畫面不同，自動車牌辨識系統能夠不受天氣、光線及車速的影響，清楚辨識出錄影畫面中行經車輛的車牌號碼，倘若連結交通部車籍資料庫便可以間接得知車輛駕駛人的身分。警方使用系統識別出畫面中的車牌號碼後，一方面會結合警政署所建置的「涉案車輛資料庫」，自動即時比對被拍攝到的車輛是否為失竊車輛，或者為犯罪嫌疑人所有；另一方面，系統也會同時將所有量化處理後的車牌資料以及拍攝的時間、地點一併記錄並儲存於資料庫內，待警方日後對特定人產生犯罪嫌疑時，再進一步調取其過去的行車資訊。伴隨特定車輛的身影接連

[1] 參考：臺北市議會第 14 屆第 1 次定期大會，〈錄影監視系統汰舊換新案（機房租賃概況評估）書面報告〉，https://www.tcc.gov.tw/MeetingMinutesDetail.aspx?n=13537&GrpKind=1&FileGrpKindSN=78CF64EB42B0ED5FBB6ADE8CB0036CF7（最後瀏覽日：05/10/2024）。

[2] 選舉過程中也不乏有候選人以增設或汰換路口監視器為其政見，參考：王朝鈺（09/22/2022），〈蔡適應提汰換類比監視器 研擬警消港都加給〉，《中央通訊社》，https://www.cna.com.tw/news/aipl/202209220276.aspx（最後瀏覽日：05/10/2024）。

doi:10.6342/NTU202403953

被不同地點的自動車牌辨識系統捕捉，輔以 GIS(Geographic Information System) 地理資訊系統的疊圖技術，便可以按照時間順序一點一點連結成完整的行車路線，描繪出特定人的移動軌跡。這個過程中，與傳統調閱監視錄影畫面最大的差別在於：員警只需要在系統中輸入特定車牌號碼，便可以十分輕易地使用搜尋功能，調閱該車輛過去所有曾受儲存的行車資料，甚至透過即時比對功能的實施，達到即時（real-time）監控的效果，不再需要憑藉個人辦案經驗，耗時費力地調閱案發地點附近的監視畫面，猜測嫌犯可能的逃亡路線。例如新北市警察局所建置的自動車牌辨識系統（智慧型雲端影像檢索系統，俗稱「雲龍系統」），即具備「特定目標即時告警功能」，警方只需於系統上先行輸入特定車號，俟車輛行經警用車牌辨識攝影機時，系統就會立即發送簡訊或電子郵件通知特定人員，使警員得以即時追查特定車輛之行蹤。過去曾引發社會關注的「高雄少女失蹤案」，少女搭乘高鐵北上至新竹後坐上陌生人的車即失去聯繫，警方便是透過雲龍系統發現該車輛曾出沒於新北市五股、八里，並即將通過關渡橋，藉此預測犯罪嫌疑人後續的行車路線，方順利攔截[3]。

必須意識到的是，這些行駛於公共道路上被蒐集、儲存行車資料的車輛駕駛人，其實大多同你我一般，完全不具備犯罪嫌疑。亦即，警方在對公共安全的具體危害或是刑事犯罪尚未發生之前，就先行預防性儲備所有車輛的行車資訊。此舉事實上使警方掌握了所有車輛駕駛人的具體行蹤。我國實務上曾發生一件駭人聽聞的事情，新北市一名員警因為懷疑老婆外遇，遂以調查案件為由，自行使用雲龍系統之「特定目標即時告警功能」，輸入老婆、老婆的弟弟以及兩名可疑情夫的車牌號碼，持續接收四人的行車資訊，監控時間長達 8 個月，期間一共使用了系統 156 次，獲取 600 多筆車牌辨識資料[4]。這段期間，員警老婆已向法院聲

[3] 陳俊宏（09/01/2020），〈雲龍系統超強大！key「車牌 7923」電眼抓軌跡　攔截載走少女轎車〉，《ETtoday 新聞雲》，https://www.ettoday.net/news/20200901/1798193.htm（最後瀏覽日：03/31/2024）。

[4] 臺灣新北地方法院 111 年訴字第 1180 號刑事判決；吳政峰（07/06/2022），〈警懷疑老婆偷情濫用破案神器「雲龍系統」查足跡〉，《自由時報》，https://news.ltn.com.tw/news/society/breakingnews/4355561，（最後瀏覽日：05/10/2024）。

doi:10.6342/NTU202403953

請保護令，卻不明白為何該名員警總是能掌握她的行蹤，甚至向朋友借車也沒辦法躲避其騷擾，最後向警方申訴，事情才終於水落石出。由此可見，大量的監視錄影畫面不再協助人民隱匿於人群之中，反而使國家機關甚至是非法存取資料者得以透過這些經由量化處理後的車牌辨識資料，更加輕易且精準地得知特定人曾停留在何處？待了多久？與誰見面？參與了什麼活動？

第二節　問題之提出

聽聞上述案例，不禁令人思考，這種得以鉅細靡遺探知特定人行車軌跡的資料庫，於調取過程中難道不需要受到任何限制？為何該名員警僅是泛泛以調查案件為由，就可以持續使用派出所內的公務電腦予以調取？調取期間長達 8 個月、次數多達 156 次且均留下紀錄，為何警察機關內部沒有人察覺異常？再更進一步地思考，整件事情的源頭在於自動車牌辨識系統的資料庫內，存有員警老婆的大量行車資料。不過，員警老婆適時完全不具備犯罪嫌疑，甚至可能這一輩子都與刑事案件毫無關聯，為何需要忍受國家機關蒐集、儲存其行車資訊，甚至因此遭員警非法監視？

有據於此，為了回答上述問題，首先必須探究自動車牌辨識系統干預人民基本權的性質。車牌號碼依行政法令應保持可辨識性[5]，是否會影響其干預性質的判斷？警察機關是否得據以主張其蒐集、儲存及利用車牌辨識資料的行為，並未對人民基本權構成干預？其次，在對公共安全的具體危害或刑事犯罪尚未發生以前，即預防性地儲備人民的個人資料，待日後產生偵查需求時再予以調取，就等同在尚不具備具體事由的情形下，迫使人民承受其個人資料被蒐集、儲備，以及緊隨其後私人生活遭受探知、揭露的風險。則此種預防性資料儲備措施的正當性為何？使用自動車牌辨識系統追查特定車輛之位置資訊，是否存在其他同等有效

[5] 《道路交通管理處罰條例》第 13 條：「汽車行駛有下列情形之一者，處汽車所有人新臺幣二千四百元以上四千八百元以下罰鍰，並責令申請換領牌照或改正：（第一款）損毀或變造汽車牌照、塗抹污損牌照，或以安裝其他器具之方式，使不能辨認其牌號。」

doi:10.6342/NTU202403953

且侵害較小的手段？

事實上，參考德國《刑事訴訟法》第 163g 條的立法過程即可得知，自動車牌辨識系統追查特定車輛位置的方式，基於資料儲存對象與時點的不同，存在三種可能的實施模式。其一，於系統辨識出車牌號碼後，即自動比對警方事先建置的追緝名單，並且僅儲存車牌比對符合的資料，比對不符合者必須立即且不留痕跡地刪除。亦即，僅在特定車輛的位置資訊涉及具體的公共安全危害或刑事犯罪時，方會受到儲存，而不授權警察機關預防性儲備所有人的行車資訊，使不具犯罪嫌疑的一般人免於承擔私人生活遭受探知的風險。這種實施模式在德國法上也被稱作「追緝模式」（Fahndungsmodus）。其二，於對公共安全的具體危害或刑事犯罪發生後，尚未掌握可疑車輛之際，先行授權警方得在一定期間內，暫時不區分行經車輛是否具有犯罪嫌疑，一律先行蒐集、儲存其行車資料，待未來取得更多線索再加以調取，判斷嫌犯可能的逃亡路線。亦即，雖授權警方得以預防性儲備不具犯罪嫌疑之一般人的行車資訊，但是將干預措施的實施時點限於具體公共安全危害或刑事犯罪發生之後的一定期間內，以實施時點控制措施干預基本權的程度。這在德國《刑事訴訟法》第 163g 條的立法過程中被稱為「儲存模式」（Aufzeichnungsmodus）。其三，立法過程中也曾被提出的「記錄模式」（Aufnahmemodus），則是近似於我國現行實務的施行情形，也就是授權警方無須區分行經車輛是否具有犯罪嫌疑，常態使用自動車牌辨識系統預防性蒐集、儲備所有車輛的行車資料，並且在一定期間內予以留存，供未來符合法定要件時調取。

doi:10.6342/NTU202403953

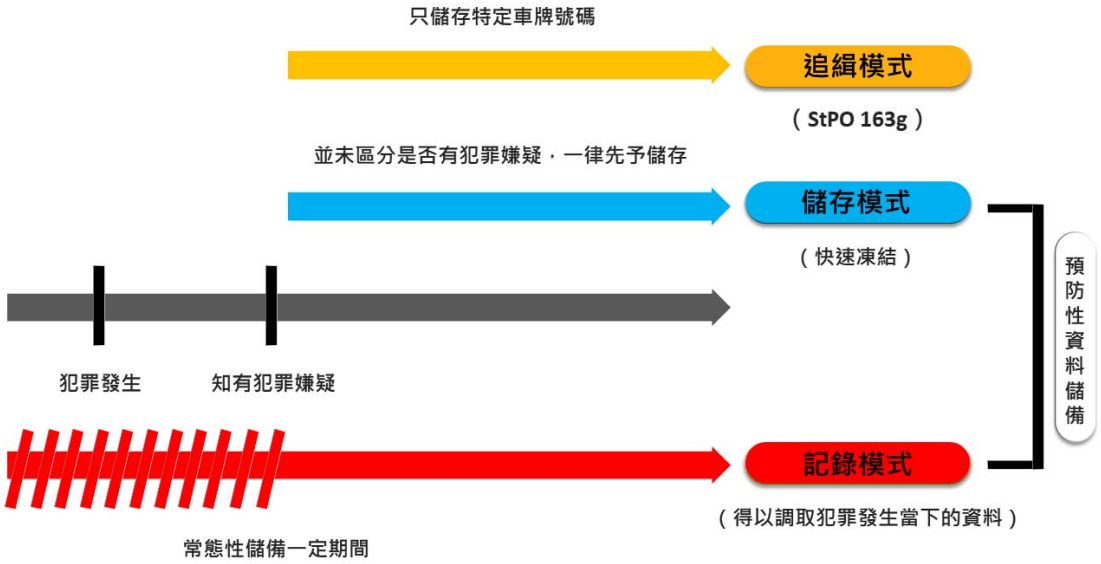

圖 1　自動車牌辨識系統的可能實施模式（筆者自繪）

不難想見，上述三種實施模式會基於各自迫使一般人承受私人生活遭揭露風險的不同，而在基本權干預程度上產生顯著的差異。則我國警方為何選用干預程度最高的「記錄模式」？其他實施模式是否屬於同等有效達成目的且侵害較小的手段？就需要進一步探究。最後，假使以「記錄模式」實施自動車牌辨識系統確實有其必要性，則此種預防性資料儲備措施是否會根據受儲備資料的性質，而在某些情況下為憲法所絕對禁止？若仍有合憲可能，其授權基礎的設計上又應著重於哪些要件，方可通過狹義比例原則的審查？回應上述疑問，遂成為本文的寫作目的。

第三節　研究範圍與研究方法

我國《刑事訴訟法》的發展很高程度地受到德國法影響，因此，本文希望透過考察德國《刑事訴訟法》相關規定，認識基於刑事追訴目的實施自動車牌辨識的可能立法例。同時，由於德國並未同我國一般預防性儲備人民的行車資料，本文期待能以梳理其他預防性資料儲備措施的方式，探討並比較此種措施與其他干預情形的不同之處，藉此對其干預基本權的程度與授權基礎之要件設計產生更通

doi:10.6342/NTU202403953

盤的理解。其中，要以「通信紀錄」之預防性儲備最有討論價值，蓋通訊不會輕易為第三人所知的性質，一方面使其成為憲法保障人民私人生活的重要一環，另一方面卻也是犯罪集團犯案過程中高度仰賴的緣由。基此，是否得以對不具犯罪嫌疑的一般人預防性儲備通信紀錄？若否，應如何處理重大犯罪甚至是國家安全的潛在威脅？若是，應如何避免人民的私人生活淪為國家監視的客體？就多次成為德國聯邦憲法法院（Bundesverfassungsgericht）以及歐盟法院（Court of Justice of the European Union，CJEU）的訴訟標的。有鑑於此，本文亦將爬梳相關裁判，關注其中對於預防性資料儲備的討論，藉以回過頭審視我國預防性儲備車牌辨識資料措施的施行，以及相關授權規定。

第四節　本文架構

本文分為五個章節，第一章緒論希冀透過新北員警「公器私用」，以自動車牌辨識系統監視老婆行蹤的案例，點出自動車牌辨識與預防性資料儲備的可議之處，並提出本文問題意識。第二章首先藉由我國警方所發行的期刊以及相關新聞報導，試圖拼湊出其實際施行自動車牌辨識系統的全貌。隨後，面對車牌號碼依行政法令應具備可辨識性，而產生對其蒐集是否干預人民資訊隱私權的疑問，本文引述德國及美國實務上的有關討論，作為我國法上判斷自動車牌辨識干預性質的參考依據。最後，介紹德國《刑事訴訟法》中以刑事追訴為目的實施自動車牌辨識與即時比對的授權基礎，觀察「不以預防性資料儲備的方式」實施自動車牌辨識之立法可能。第三章的開頭則點出預防性資料儲備對於偵查實務的意義，並梳理德國《刑事訴訟法》立法過程中，曾經一度討論的「預防性車牌辨識資料儲備」，比較在不同時點開始儲備車牌辨識資料的實施模式，其對於人民基本權干預的程度以及偵查成效的差異何在。其後，為探究預防性資料儲備對於個人資料保護與私人生活保障的實質影響，整理歐盟法上曾因課予會員國強制儲備通信紀錄義務，所引發的爭議，嘗試歸納預防性資料儲備措施合憲性審查中的重要因素，

doi:10.6342/NTU202403953

藉此提出預防性車牌辨識資料儲備措施，其授權基礎必須具備的要件。第四章具體審視我國現行法上關於車牌辨識資料儲備、調取，以及即時實施自動比對的授權規定，是否合於上述要求；若無則提出實質立法建議，供立法者參考。第五章總結各章重點，敘明本文結論。

doi:10.6342/NTU202403953

第二章 車牌辨識之基本權干預性質

第一節 自動車牌辨識系統之簡介

第一項 技術原理與實施流程

若想探究自動車牌辨識的干預屬性，必須先清楚認識車牌辨識的技術原理與實施流程。車牌辨識，是指監視錄影設備於前端取得監視影像後，經由網路後送至影像處理機房，並藉由具備深度學習功能的辨識軟體，識別出畫面中所有通過車輛的車牌號碼、車輛型號、顏色、通過時間、地點、行徑方向等資料，將之儲存於雲端後即時與警用資料庫進行比對，或者供未來預防與偵查犯罪所用[6]。簡單來說，車牌辨識的實施流程可以歸納為：取得影像畫面、透過軟體識別行車資料，最後予以儲存或與其他資料比對[7]。

關於監視影像的取得，可以區分為「固定式」與「移動式」。「固定式」是指國家機關透過定點設置之監視器，全天候持續取得監視錄影畫面。我國路口監視錄影器雖然隨處可見，但過去大多為 30 萬畫素的攝影機，一旦車輛與攝影機之間稍有距離，即便是透過肉眼亦難以辨認畫面中的車牌號碼。此外，影像畫面是否清晰，除了與目標物件之間的距離外，亦須考量光線明暗及拍攝角度，換言之，即使拍攝距離尚可，仍有可能因為案發時間適逢夜晚、光線昏暗，或者是受限於固定設置監視器的拍攝角度，而無法拍攝出可識別車牌號碼的畫面供警察機關使用。為此，各縣市近年來紛紛對於監視錄影設備進行升級。以臺北市為例，臺北市政府警察局於 2019 年 7 月開始推動「第一期錄影監視系統汰舊換新統包工程

[6] DIGITIMES 企劃（07/31/2014），〈警政勤務監控再進化 中華電信讓安全再上層樓〉，《DIGITIMES》，https://www.digitimes.com.tw/tech/dt/n/shwnws.asp?CnlID=14&id=0000388450_DU93HKGZ6SFP2ELAEKFU4&packageid=8690&cat=10（最後瀏覽日：03/31/2024）；另外，2007 年 12 月 27 日內政部警政署刑資字第 0960016613 號函之《警察機關車牌辨識系統查緝涉案車輛作業規定》，對於「車牌辨識系統」的定義則為：「係指於交通要道或重要路口設置具有光學影像擷取設備之攝影機，全天候自動擷取行經該路段之車輛車牌，經由車牌辨識系統主機自動與涉案車輛資料比對，辨識相符之車牌影像畫面即為定格顯示螢幕並發出中文警報語音之設備系統。」

[7] 車牌辨識系統又可區分為攝影機本身即具備辨識功能的「前端辨識」，以及於前端取得攝影畫面後，將影像傳輸至後方機房的「中間辨識」及「後端辨識」。參考：周天蔚（2019），〈細說車牌辨識原理與市場〉，《臺灣電信月刊》，193 期，頁 14-15。

doi:10.6342/NTU202403953

案」，將 1 萬 3,699 支路口監視器汰換升級為 200 萬畫素攝影機，並新增部分 500 萬畫素攝影機以及能夠遠端操控鏡頭方向的 PTZ 攝影機，將路口監視器的總數提升至 1 萬 8,094 支，同時也新增了 2,216 支專為車牌辨識與車行軌跡分析所設計的監視器[8]。值得注意的是，雖然依《臺北市錄影監視系統設置管理自治條例》第 10 條規定，臺北市警察局應每半年公告監視器所裝設的位置，然而臺北市警察局並不會明確標示出具備車牌辨識功能之監視器[9]，這也使自動車牌辨識系統隱身於眾多路口監視器之中，產生了秘密實施的性質。

另外，路口監視器雖然得以在固定地點持續取得監視錄影畫面，卻也導致監視影像取得的位置受到侷限，倘若監視器設置的密度不足，例如郊區、河濱道路等區域，或是行為人刻意躲避車牌辨識的裝設位址，警方便無法透過自動車牌辨識系統進行犯罪預防或追訴。有鑑於此，警察機關遂同時使用「移動式車牌辨識系統」[10]。這個系統是在偵防車的前方與左右兩側裝設鏡頭，車上並配有電腦，能夠讓警車即使在時速 40 公里以上的行駛途中，也能辨識行經車輛的車牌號碼，並自動比對其是否為涉案車輛，若比對成功即以語音通知車內員警[11]。同時，新北市警察局考量一般員警使用警車的頻率不高，更研發出所謂的「智慧戰警頭盔」，亦即在警用安全帽上裝設具有車牌辨識功能的攝像鏡頭與小黑盒，讓巡邏員警目

[8] 截至 2023 年 5 月 4 日，總計 1 萬 8,094 支監視器已全數裝設，惟部分仍待引電或待裝設網路。參考：臺北市議會第 14 屆第 1 次定期大會，前揭註 1；顧詔勛、吳松儒、林柏鋒、林啟豐（2021），〈建構臺北市治安電子城牆——新一代影像智慧分析應用〉，《中華技術》，130 期，頁 103-104。另外，桃園市於 2018 年已裝設 9,277 支具備車牌辨識功能之攝影機，佔桃園市全部監視錄影設備的 52%，參考：盧昱嘉（2018），〈天羅地網監錄系統邁入 A.I.應用世代〉，《桃警》，79 期，頁 3。

[9] 筆者曾透過「臺北市單一陳情系統」詢問，得到的回覆是：「該條文係明訂本局及設置機關應將錄影監視器之區位予以公告，藉由公告某區域有『幾支』監視器方式，以方便民眾查閱，並未律定須公告顯示監視器之『類型』。」參考：臺北市政府警察局監視錄影系統網站，https://cctv.police.gov.taipei/News.aspx?n=52DDBB5D1E50AF72&sms=94AC2E5C069CB36A（最後瀏覽日：03/31/2024）。

[10] 相較於固定式車牌辨識可在車輛通過特定地點時觸發拍攝功能並予以記錄，移動式車牌辨識系統所拍攝的影像背景更加複雜，需要仰賴影像校正與深度學習，訓練軟體區別車輛與非車輛的能力，參考：蔡馥璟、高大宇（2018），〈基於警政應用與大數據之辨識移動式車牌研究〉，《警學叢刊》，49 卷 3 期，頁 91-93。

[11] 王善嫣（08/26/2022），〈1 秒辨識車牌！ 嘉義市警車升級「嘉 e 智能巡邏車」上路 2 個月破案 29 件〉，《自由時報》，https://news.ltn.com.tw/news/society/breakingnews/4038428（最後瀏覽日：03/31/2024）。

doi:10.6342/NTU202403953

光所至的車牌，都能即時與涉案車輛資料庫進行比對[12]。

透過路口監視器及移動式裝置取得的監視錄影畫面，會經由網路後送至影像處理機房。車牌辨識軟體必須能在背景複雜的畫面中，自動偵測是否出現車牌以及其所在位置，並精準地分割各個字元，最後再執行字元辨識。實際運作上，辨識軟體會對錄影畫面進行灰階化處理[13]，亦即將原先由紅色（R）、綠色（G）與藍色（B）三種顏色組成的 RGB 彩色影像，轉換成亮度值介於 0～255 間的黑白畫面，其中，數值 0 代表最暗的黑色，255 則表示最亮的白色，轉換後，沿著數值差異極大的部分描繪便可以偵測出圖形中色彩明顯對比之處，通常即為圖形的邊緣。而我國車牌號碼字元的顏色與號牌底色均有明顯差異，灰階化處理後的影像即可清楚偵測出車牌號碼各字元的圖形邊緣，並沿著輪廓描繪出具體字元，輔以形態學的運算排除形狀大小明顯非車牌矩形的部分[14]，再使用像素直方圖法分割字元[15]，就能順利進行字元辨識。目前字元辨識的主要方法有三，分別是「樣板比對」（Template Matching）、「特徵辨識」（Feature Recognition）和「光學字元辨識」（Optical Character Recognition，OCR）[16]。

過去，自動車牌辨識系統僅會識別出畫面中通過車輛的車牌號碼，然而隨著科技進步，文獻上及警察機關的訪談中均已透露，我國現今使用的自動車牌辨識系統所能辨識並儲存的資訊，除了車輛的車牌號碼、通過地點和時間以外，還包

[12] 新北市政府警察局資訊服務網，https://www.police.ntpc.gov.tw/cp-3344-80375-1.html（最後瀏覽日：05/10/2024）；蘇文彬（03/26/2021），〈2021 智慧城市展直擊：新北市警察靠 AI 頭盔過濾可疑車輛，臺北市與業者聯手測試智慧水表〉，《iThome》，https://www.ithome.com.tw/news/143496（最後瀏覽日：03/31/2024）。

[13] 李建興、游凱倫、林應璞（2010），〈即時動態車牌辨識〉，《技術學刊》，25 卷 2 期，頁 153。

[14] 陳先慶（2006），〈神捕——車牌辨識系統〉，《刑事雙月刊》，12 期，頁 57。

[15] 像素直方圖分割法，是指分別統計水平方向和垂直方向上各行各列的黑色像素的個數，根據像素的特點確定分割位置，參考：湯仁愷（2023），〈應用 YOLOv5 和 CNN 深度學習技術於車牌辨識研究〉，《應用 YOLOv5 和 CNN 深度學習技術於車牌辨識研究》，頁 23，國立臺北科技大學車輛工程系碩士班碩士論文；李建興、游凱倫、林應璞，前揭註 13，頁 154-155。

[16] 光學字元辨識又稱「視覺字元辨識」，最普遍使用於 PDF 與 Word 檔案的格式轉換，參考：周天蔚，前揭註 7，頁 16；陳一昌、黃運貴、張芳旭、楊智凱、曹瑞和、田養民、張仲杰（2004），《車牌影像辨識系統與號牌設計改進配合措施之探討》，頁 9-10，交通部運輸研究所；湯仁愷，前揭註 15，頁 24-25。

doi:10.6342/NTU202403953

括車輛的廠牌、型號、顏色[17]，甚至是機車騎士和路上行人的穿著打扮[18]。前板橋派出所所長楊建良就曾於受訪時談到：「某位男子在新北市板橋區搶劫後雖然曾多次變換交通工具，先是搭乘計程車至府中捷運站，後又搭乘捷運至台北轉運站轉乘客運至宜蘭礁溪，再騎摩托車返回家中，途中亦換去行搶時的紅色衣物，卻因為沒有更換鞋子而一路被鎖定[19]。」雖說個人服裝尚非涉及生物特徵之高敏感個人資料，然而其仍屬於得以間接方式識別個人之資料，縱使係於公開場所予以蒐集，亦有構成資訊隱私權干預之虞（詳後續論述）。

值得一提的是，自動車牌辨識系統除了協助警察機關識別、篩選監視畫面中的資訊以外，更會搭配 GIS 地理資訊系統，將相鄰監視錄影設備所取得的車牌號碼、通過時間及行車方向，依照時間順序一一標示於電子地圖之上，並藉此描繪出特定車輛的行車軌跡[20]。試想，倘若具備車牌辨識功能的錄影設備設置密度逐漸提升，蒐集資料的對象、資料保存期間卻又都不受限制，那麼以汽機車作為代步工具的人們，其一整天的行蹤都將被秘密紀錄、悉數網羅。長此以往，隨著時間推移，人民的住所、上班地點、約會對象的住處、假日參加的集會遊行、經常出沒的餐廳、酒吧、健身房、廟宇、教堂，這些與私人生活有著重要關聯性的地點都會被逐一揭露，接著便能如拼圖般一片一片拼湊出個人的家庭關係、人際網絡、宗教信仰、政治立場與性傾向。換句話說，車牌辨識系統除了作為協助警察機關篩選資料的電腦視覺工具，更隱含了將眾多資料相互結合，進而解讀特定人私生活的風險，這也是自動車牌辨識系統與傳統員警在路邊以手動輸入車牌檢查

[17] 盧昱嘉，前揭註 8，頁 3-4。

[18] 文獻指出，智慧分析影像的功能，包括使用軟體識別「行人」、「腳踏車」、「機車」、「汽車」、「卡車」、「公車」，以及其顏色。參考：顧詔勛、吳松儒、林柏鋒、林啟豐，前揭註 8，頁 110-111。

[19] 楊建良表示：「車牌、車色、服裝都可以辨識，不管是開車、騎車或走路，只要鎖定車牌或個人特徵，就可以迅速過濾，從 500 人縮小範圍到 5 至 10 人。」參考：林倖妃（06/14/2021），〈七千警力怎麼照顧六百萬人？新北市靠智慧頭盔升級戰力〉，《天下雜誌》，https://www.cw.com.tw/article/5115224（最後瀏覽日 03/31/2024）。

[20] 吳宗澤（2012），〈地理資訊系統（GIS）與刑案分析之結合運用〉，《刑事雙月刊》，47 期，頁 18-20；盧昱嘉（2012），〈天眼雙雄捍衛桃園——桃園縣政府警察局監視錄影系統簡介〉，《政府機關資訊通報》，297 期，頁 4。

doi:10.6342/NTU202403953

是否為贓車最根本的不同之處。實際應用上，文獻已指出我國警察機關會利用 GIS 系統的疊圖分析功能，將行車紀錄、通聯記錄、網路 IP 位址等不同偵查方式所取得的位置資訊，轉換為相同比例尺的電子地圖，並輔以涉案車輛資料庫套疊分析[21]。

第二項　發展歷史

車牌辨識技術（License Plate Recognition，LPR）最早是由前英國警察科學發展處（the Police Scientific Development Branch，現已改組為內政部科學發展處（Home Office Scientific Development Branch））於 1976 年發明；隨後被設置於 A1 公路和達特福德跨河道路（Dartford Crossing），並於 1981 年首度成功識別贓車，且以此作為逮捕之依據[22]。1993 年，為了防止倫敦市中心繼續遭受愛爾蘭共和軍（Irish Republican Army）的恐怖攻擊，英國倫敦市警察局建立「鋼環安全監控系統」（the Ring of Steel）[23]，於倫敦市區廣泛設置監視錄影系統（CCTV）並配置車牌辨識技術，除了識別車牌號碼以外，更具備偵測人群擁擠場所、非法入侵、街頭犯罪等功能，截至 2012 年止，已識別超過 91,000 件遭通緝或涉案之車輛，並藉此逮捕 550 名嫌犯[24]。另外，為了解決車牌辨識資料多散落於各警察機關，不利整合繪製完整行車軌跡的問題，英國於 1997 年成立「國家自動車牌辨識資料中心」（National ANPR Data Centre，NADC），集中處理各部門所蒐集之車牌辨識資料並予以分析[25]。

我國內政部警政署刑事警察局於 2003 至 2004 年間，先於各縣市警察局建置

---

[21] 吳宗澤，前揭註 20，頁 18-19。

[22] NEXT GENERATION SECURITY CONCEPTS, *The History of License Plate Recognition Technology*, https://ngscinc.com/history-license-plate-recognition (last visited Mar. 31, 2024).

[23] MAS CONTEXT, https://mascontext.com/issues/surveillance/ring-of-steel (last visited Mar. 31, 2024).

[24] 官政哲（2012），〈21 世紀警政新典範——智慧型警政（SMART Policing）〉，《刑事雙月刊》，50 期，頁 48。

[25] 其所蒐集之行車資料，儲存的時間可長達 5 年。*See* NEXT GENERATION SECURITY CONCEPTS, *supra* note 22; REVIVE RESILIENCE, https://revive-resilience.com/case-study/national-anpr-data-centre-nadc/ (last visited Mar. 31, 2024).

doi:10.6342/NTU202403953

1 至 2 套示範性車牌辨識系統，再於全國重要道路及高速公路另行建置 40 套，共計 65 套車牌辨識系統。同時，將所蒐集的行車資料予以彙整，並結合 GIS 地理資訊系統，建構「全國贓車查緝網」，用於查緝贓車、擄人勒贖或肇事逃逸等與汽車相關之犯罪，以此分析車輛動向與嫌犯行蹤[26]。隨後，為了整合各警察機關自行建置車牌辨識系統所蒐集之資訊，強化涉案車輛行徑分析等功能，刑事局於 2006 年另行建置「涉案車輛追緝系統」，作為統合性共通平台[27]。惟因當時具備車牌辨識功能之攝影設備建置數量仍舊不足，所蒐集之行車資訊無法具體掌握涉案車輛動向，難以發揮查緝功能。有鑑於此，刑事局遂於 2008 年至 2010 年間，依據行政院核定之「科技犯罪防制工作中程計畫」，逐年大量增設車牌辨識系統，並建構「涉案車輛監控查緝網」[28]。2008 年，刑事局先於國道高速公路裝設 220 套車牌辨識暨監視錄影系統，隔年則在臺北市等 7 縣市新增 300 套車牌辨識系統，最後於 2010 年完成其餘 15 縣市車牌辨識系統的建置。這些系統能夠自動識別通過車輛之車牌號碼，偵測其是否屬於涉案車輛（含失竊車輛、車牌、涉及刑事案件車輛），並攝錄監控全景影像，結合簡訊即時通報，協助偵查人員追蹤涉案車輛之逃逸路線，俾利後續偵查作為[29]。

同時，考量車牌辨識系統的建置成本十分高昂，且我國路口監視攝影機的設置已達一定數量，全面替換的可能性不高，因此桃園市（彼時為桃園縣）警察局於 2012 年與中華電信共同研究開發「雲龍行車軌跡系統」（以下稱「雲龍系統」）[30]，將桃園縣原有的「天羅地網影像與雲端系統」結合智慧型影像辨識技術[31]，使

---

[26] 依據刑事警察局的文章說明，「全國贓車查緝網」係依《警察職權行使法》第 10 條所建置。然而，查緝贓車、擄人勒贖或肇事逃逸，係為偵查犯罪，而非維護治安，明顯不得以《警察職權行使法》作為相關之授權規定。參考：蘇清偉（2005），〈「全國贓車查緝網」張網打擊犯罪〉，《刑事雙月刊》，4 期，頁 42-43。

[27] 蘇清偉、李耀中（2007），〈加速辦案效率——影像處理分類探討〉，《刑事雙月刊》，20 期，頁 41。

[28] 施宗培、田哲夫（2010），〈科技犯罪偵防工作簡介〉，《刑事雙月刊》，39 期，頁 29。

[29] 田哲夫（2008），〈科技犯罪防制工作中程計畫簡介〉，《刑事雙月刊》，27 期，頁 14-15。

[30] 盧昱嘉，前揭註 8，頁 2。

[31] 智慧型影像辨識技術，是指有效運用雲端運算的能力，快速分析影像內的重要資訊。參考：林明芬、戴偉恒、張正欣（2016），〈雲端智慧影像分析及檢索系統〉，《電腦與通訊》，166 期，頁 83。

doi:10.6342/NTU202403953

原先因畫素過低而辨識度僅有 60%的監視影像，也能藉由攝影機拍攝的廣度和軟體運算技術，達到追蹤車輛行進方向的功能[32]。雲龍系統使用 GIS 技術將行車資料整理於座標一致的電子地圖中，特定車輛被路口監視器捕捉的次數越多，系統所描繪的行車軌跡精準度也會越高，員警辦案時只需在檢索引擎中輸入可疑車色及（部分）車牌號碼，便可篩選出可疑車輛並鎖定其行車軌跡[33]。若將長期取得的監視影像均透過智慧型影像辨識技術處理，除了可以取得特定車輛的歷史軌跡、分析犯罪嫌疑人的逃逸路線，甚至可以用於分析犯罪嫌疑人的生活習性及經常出沒的地點[34]。

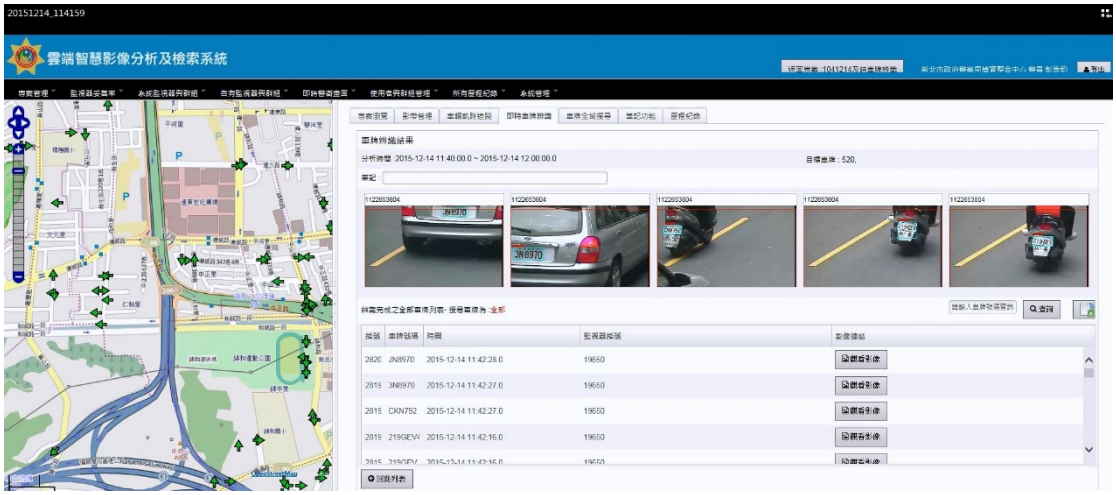

圖 2　雲端智慧影像分析及檢索系統[35]

此外，為了善用雲端運算技術改善治安，內政部警政署於 2012 至 2015 年間著手規畫並實施「警政雲端運算發展計畫」，期待能夠跨縣市整合既有之路口監視器，並且清楚標示出各個監視器的所在位置及拍攝範圍，以供員警快速取得所

32 DIGITIMES 企劃，前揭註 6。
33 葉雲兆、陳武洲、簡大為、留乃俊、鄭惟元（2014），〈警政勤務及港埠物流影像辨識之應用〉，《前瞻科技與管理》，4 卷 1 期，頁 174。
34 盧昱嘉，前揭註 8，頁 4。
35 圖片來源：智慧城市暨物聯網產業網，https://smartcity.org.tw/application_detail.php?id=30（最後瀏覽日 03/31/2024）。

doi:10.6342/NTU202403953

需影像資料，毋庸另行至現場觀察監視器的拍攝角度[36]。其中，整合各縣市車牌辨識系統資料庫，提供辦案員警完整之涉案車輛軌跡，據以分析涉案車輛逃逸路線及地緣關係，並透過解析車牌點位資料庫所蒐集之巨量車牌號碼，搜尋與嫌疑車輛車行時間相近、軌跡雷同之隨行車輛，藉此篩選可能的犯罪同夥，提升員警辦案效率，亦是本計畫的重點之一。不過，根據監察院 2020 年的調查報告指出[37]，由於警政署規劃涉案車輛軌跡查詢系統的過程中，未能衡酌及詳實評估各直轄市、縣（市）政府之財政能力及建置車牌辨識系統之配套條件，亦未積極整合已增設車牌辨識系統之路口監視器，導致車牌辨識系統的建置比率以及各縣市整合作業的完成度，均嚴重低落。例如臺灣本島 19 個直轄市、縣（市）警察局於 2020 年共設置 18 萬 3,097 支路口監視器，扣除 6 萬 7,298 支全景式監視器後，仍有 11 萬 5,799 支路口監視器可增設車牌辨識功能，經查卻僅有 3 萬 5,409 支路口監視器，約占 30.58%有增設，其中亦僅有 2 萬 3,624 支監視器完成資料庫的整合，約占 66.72%。而宜蘭縣、嘉義縣、屏東縣、花蓮縣之縣政府警察局，更因經費不足而完全沒有建置自動車牌辨識系統。對此，警政署回應其後續已完成接收新北市、桃園市、高雄市、新竹縣、苗栗縣、雲林縣等警察局之車牌辨識資料，將總體的整合率提升至 94.44%[38]。

另一方面，由於車牌辨識系統面對車牌嚴重汙損、犯罪嫌疑人頻繁變換車牌，甚至是直接拔除車牌的情形，即無法有效發揮其功能，警政署遂自 2019 年起辦理「涉案車輛行車紀錄雲端創新應用發展計畫」[39]，基於我國 eTag 申裝率高達 93%的背景[40]，於 2019 年至 2022 年間在各縣市重要路口大量裝設 RFID （Radio

[36] 陳宏和（2014），〈警政雲端運算發展計畫執行現況〉，《政府機關資訊通報》，317 期，頁 34。
[37] 監察院（109）年內調字 0030 號調查報告（仉桂美委員、蔡培村委員、林盛豐委員調查），頁 4-7。
[38] 應該辨明的是，汰換現有監視器並增設車牌辨識功能（增設率），以及整合現時具備自動車牌辨識功能的監視器所蒐集之資料（整合率），係屬二事。參考：監察院網站，https://www.cy.gov.tw/CyBsBoxContent.aspx?n=133&s=17082（最後瀏覽日：03/31/2024）。
[39] 警政署向立法院提出的預算案說明，參考：立法院網站，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=33575&pid=188850（最後瀏覽日：03/31/2024）。
[40] 交通部高速公路局網站，https://www.freeway.gov.tw/Publish.aspx?cnid=2925&p=11869（最後瀏覽日：03/31/2024）。

doi:10.6342/NTU202403953

Frequency IDentification，RFID）外碼讀取器，利用無線電訊號接收通過車輛之 eTag 資料[41]，並且將國道及各縣市重要路口所蒐集的 eTag 資料回傳至中心端資料庫，與失竊車輛、涉案車輛之 eTag 編碼進行比對，達到近似於車牌辨識系統的功能。比對如有符合，可介接高速公路局 ETC 系統將 eTag 編碼轉換為車牌號碼，並連結其車籍資料，再與其他偵查方式所取得之行車資料一併整合[42]。倘若涉案車輛適時正行駛於高速公路上，更可依該路段之車流速度，結合其行駛路徑，預測其半小時內將行經之匝道出入口，並顯示於警示系統[43]。

第三項　實際使用情形

自動車牌辨識系統的實際應用十分廣泛，以刑事追訴為例，警方經常憑藉雲龍系統快速鎖定特定車輛的功能，協助民眾尋回失竊車輛，整個過程甚至僅耗費兩小時[44]。而於社會矚目的重大案件中也不乏雲龍系統的身影，例如 2020 年高雄少女失蹤案，便是由新北市警方透過雲龍系統發現犯罪嫌疑人的車輛出現在關渡橋附近，以此預測其後續軌跡並設置攔截點將其逮捕[45]。過往曾發生多起私行拘禁案例，在嫌犯以車輛劫持被害人後，警方之所以能在短短兩三個小時內逮捕嫌犯，也要歸功於車牌辨識系統[46]。此外，實務上偵辦違規焚燒垃圾所造成的空污

---

41 eTag 接收到無線電波後，會反射帶有數位字母編碼的無線電波，再由讀取器處理並獲取資訊。參考：朱耀明、林財世（2005），〈淺談 RFID 無線射頻辨識系統技術〉，《生活科技教育月刊》，38 卷 2 期，頁 74。

42 王振華（2019），〈eTag 掃描設備用於打擊各類犯罪之應用與成效〉，《刑事雙月刊》，93 期，頁 15。

43 王振華，前揭註 42，頁 16。

44 黃佩華、劉俊男（04/17/2021），〈毒蟲騎贓車飆 40km 警「雲龍系統」逮人〉，《華視全球資訊網》，https://news.cts.com.tw/cts/society/202104/202104172038896.html（最後瀏覽日：03/31/2024）；李大仁（04/13/2024），〈新湖警 2 小時偵破機車竊盜案 車主頻頻道謝〉，《台灣好新聞》，https://taiwan-hot.net/news/1064792/%E6%96%B0%E6%B9%96%E8%AD%A62%E5%B0%8F%E6%99%82%E5%81%B5%E7%A0%B4%E6%A9%9F%E8%BB%8A%E7%AB%8A%E7%9B%9C%E6%A1%88+%E8%BB%8A%E4%B8%BB%E9%A0%BB%E9%A0%BB%E9%81%93%E8%AC%9D（最後瀏覽日：05/02/2024）；謝東明（05/01/2024），〈未上鎖熄火愛車不見了 47 歲男停超商前閒晃 2 小時被逮〉，《匯流新聞網》，https://cnews.com.tw/204240501a04/（最後瀏覽日：05/02/2024）。

45 陳俊宏，前揭註 3。

46 王朝鈺（08/28/2022），〈求復合不成持槍擄前女友　警 3 小時內逮人男子收押〉，《中央通訊社》，https://www.cna.com.tw/news/asoc/202208280102.aspx（最後瀏覽日：03/31/2024）；王家珩、江文

doi:10.6342/NTU202403953

案件，由於行為人犯案地點隱密且普遍安排犬隻看守戒護，稽查人員大多難以接近，因此警方除了使用衛星火點偵測系統鎖定棄置垃圾燃燒熱區以外，也會利用自動車牌辨識系統分析可疑車輛的行進軌跡，並比對嫌犯的作案時間，勾勒出犯罪模式[47]。另外，為了積極查辦珍貴林木遭本地盜伐集團及外籍移工竊取的問題，林務局亦持續精進自動車牌辨識系統、無人機、RFID 無線射頻系統等科技器材的應用，將頻繁出入山區且行蹤可疑的車輛予以標示並特別戒備，以此輔助過去以人力為主的林地巡護工作，透過科技器材克服地形障礙與蚊蟲之苦，提升森林護管效率[48]。而在行政院 2017 年提出的「新世代反毒策略行動綱領」中，也計畫於臺灣本島全線濱海道路及港區聯外道路建置固定式車牌辨識系統，據以分析、追蹤目標車輛，即時提供座標、方位等資訊，並連結相關資料庫，俾利即時分析及預測毒品犯罪之動向[49]。

除了刑事追訴以外，自動車牌辨識也基於其他目的被使用，最常見的是用於國道電子收費系統（electronic toll collection，ETC），亦即讓車輛駕駛人不需要特別準備現金或回數票，而是以感應 eTag 電子標籤或是辨識車牌的方式產生紀錄，協助後續完成繳費，毋須停車即可通過收費站。其中，未申裝 eTag 的車輛將會被自動辨識車牌號碼，並連結車主事先於遠通電收網站上填寫的個人資料，或是高速公路局的車籍資料，以寄送帳單[50]。另外，自動車牌辨識也被用於交通違規的科技執法，例如臺北市公館捷運站和新北市板橋火車站周邊均設有違規停車之科技執法設備，只要偵測到違規車輛就會自動辨識其車牌資料，再匯入科技執法

賢（06/11/2022），〈不滿好友欠 2 萬不還　速食店圍毆強擄上車〉，《三立新聞網》，https://www.setn.com/News.aspx?NewsID=1129463（最後瀏覽日：03/31/2024）。

[47] 黃旭昇（03/18/2022），〈衛星火點偵測鎖定　新北山區濫燒垃圾無所遁形〉，《中央通訊社》，https://www.cna.com.tw/news/aloc/202203180201.aspx（最後瀏覽日：03/31/2024）。

[48] 周詩涵、蔡博雅、劉大維（2020），〈國有林盜伐現況及查緝措施〉，《台灣林業雙月刊》，46 卷 3 期，頁 9-10。

[49] 行政院 106 年 7 月 21 日院臺法字第 1060181586 號函；行政院 107 年 11 月 21 日院臺法字第 1070212158 號函；呂美琪（01/02/2022），〈防堵走私犯罪　海巡署擬建車船軌跡分析系統〉，《大紀元》，https://www.epochtimes.com/b5/22/1/2/n13476805.htm（最後瀏覽日：03/31/2024）。

[50] 遠通電收網站，https://www.fetc.net.tw/UX/UX0901SharePoint/UX090101HtmlContent?processId=FT0601003_04（最後瀏覽日：03/31/2024）。

doi:10.6342/NTU202403953

平臺，由員警人工審查後認證舉發[51]。宜蘭監理站也透過自動車牌辨識，於臺 9 線蘇花公路檢查通過車輛是否為車牌號碼已被註銷之「幽靈車」，這些幽靈車大多因為車輛逾期檢驗甚至是失竊多時，方導致車牌被註銷，若放任其繼續行駛於道路上恐生交通危害，宜蘭監理站遂與宜蘭縣警察局合作建立「蘇花改車牌辨識系統黑名單即時通知群組」，在第一時間攔停車牌遭辨識為註銷之車輛，並依《道路交通管理處罰條例》舉發[52]。又，為確保機車定期接受排氣檢驗，降低廢氣排放，各縣市環保局亦紛紛採用自動車牌辨識系統識別行進中的車輛，再與環保署的機車排氣定期檢驗資料庫加以比對，確認其是否已完成當年度的排氣檢驗[53]。新北市政府教育局甚至與警察局合作，透過雲龍系統結合相關資料庫，稽查載送學幼童的專車，其滅火器、安全門等安全設備是否符合法規並定期通過核備。同時，由警察局提供曾查獲違規車輛之車牌號碼，導入雲龍系統後秘密掌握其行車軌跡，分析違規熱點並加強查緝[54]。

另一方面，自動車牌辨識系統也被應用於「區間平均速率科技執法」（以下簡稱為「區間測速」），不同於傳統測速照相僅在偵測到車輛超過速限行駛後，方拍攝其車牌號碼以供後續開罰，區間測速在科技執法路段的起點就會以自動車牌辨識系統識別通過車輛的車牌號碼，並於該車輛通過路段終點時再次辨識，最後將執法路段的距離除上車輛通過的時間，即可算出該車輛的平均速率，以此避免駕駛人僅是在固定式測速照相桿前踩剎車，而未確實遵循速限行駛[55]。換句話說，

---

[51] 蔡亞樺、劉慶侯（05/27/2022），〈北市科技執法增至 13 處　捷運公館站 7/1 起抓違停、併排停車〉，《自由時報》，https://news.ltn.com.tw/news/life/breakingnews/3940980（最後瀏覽日：03/31/2024）；新北市警察局板橋分局網站，https://www.banqiao.police.ntpc.gov.tw/cp-200-61917-11.html（最後瀏覽日：03/31/2024）。

[52] 林俊雄（04/08/2020），〈蘇花改固定式號牌辨識系統科技執法　清明連假取締註銷號牌車輛 60 件！〉，《交通部公路總局臺北區監理所》，https://tpmvo.thb.gov.tw/News_Content_table.aspx?n=931&s=72874（最後瀏覽日：03/31/2024）。

[53] 楊梅華（09/06/2019），〈機車逾期 6 個月未定檢最重可註銷車牌　每年按時定檢避免遭罰〉，《臺北市政府環境保護局》，https://www.dep.gov.taipei/News_Content.aspx?n=CB6D5C560DE4D2DD&s=17A335007E26C408（最後瀏覽日：03/31/2024）；臺東縣環境保護局網站，https://ttepb.taitung.gov.tw/News_Content.aspx?n=13490&s=79082（最後瀏覽日：03/31/2024）。

[54] 黃旭昇（05/07/2020），〈雲龍行車軌跡系統　追蹤幼童車稽查違規〉，《中央通訊社》，https://www.cna.com.tw/news/aloc/202005070304.aspx（最後瀏覽日：03/31/2024）。

[55] 王韻婷（02/26/2022），〈蘇花改用路人注意！　花蓮 2 隧道將開始「區間測速」〉，《TVBS 新聞

doi:10.6342/NTU202403953

區間測速與傳統測速照相的差別在於，傳統測速照相僅在駕駛人違規後，方會取得其行車資料，區間測速則是將所有通過車輛的行車資料一併事先蒐集，並未區分駕駛人是否違規。然而，這些基於取締超速所取得的行車資料，是否在確認車輛並未超速，或者確認超速且完成後續開罰後，亦即達成資料蒐集目的後，即予以刪除？抑或是繼續留存於資料庫內，以待警察機關未來產生調閱需求時將之用於其他目的？同樣的問題也發生在其他使用自動車牌辨識系統的情形中，例如ETC 基於收費目的而蒐集之行車資料，原則上僅得用於國道收費相關事務，然而公務機關若基於執行法定職務，例如警察機關為了預防危害或偵查犯罪而產生調閱需求，只須符合「交通部高速公路局受理公務機關調閱國道 ETC 收費系統資料作業程序」，即可將行車資料用於國道收費以外之其他目的[56]。又如，臺 9 線蘇花公路上原先為了查緝車牌註銷車輛所架設的自動車牌辨識系統，於 COVID-19 疫情期間亦連結居家檢疫者之車籍資料庫，鎖定違反隔離規定出門活動之民眾[57]，此舉明顯是將基於交通執法目的所蒐集的行車資料，用於原先蒐集目的以外之防疫用途。

警察機關使用自動車牌辨識系統所蒐集的行車資料，倘若可以恣意用於原先蒐集目的以外，就等同放任這些行車資料與更多個人資料相互連結，而在相互連結的過程中，即有可能形成與個人人格具有更高度關聯的個人資料，進而產生私人生活被窺探的風險。如同前述，警察機關會將行車紀錄、通聯記錄、網路 IP 位址等不同偵查方式所取得的位置資訊，透過 GIS 地理資訊系統轉換為相同比例尺的電子地圖，並輔以涉案車輛資料庫套疊分析[58]。警察機關亦可將 ETC 收費資

網》，https://news.tvbs.com.tw/cars/1725795（最後瀏覽日：03/31/2024）；連國豐（07/07/2022），〈桃園市警察局交通大隊／台 61 線引進車牌辨識區間測速〉，《iDS 智慧安防雜誌》，https://www.idsmag.com.tw/new_article_result.asp?search_security_id=30829&xmonitor=1&secur_id=HCP011（最後瀏覽日：03/31/2024）；新北市警察局板橋分局網站，前揭註 51。

[56] 參考「交通部高速公路局受理公務機關調閱國道 ETC 收費系統資料作業程序」之具體規範，基本上同於《個人資料保護法》第 5 條、第 15 條及第 16 條。

[57] 黃富溢（02/27/2020），〈蘇花改設「車牌辨識系統」可抓防疫趴趴走〉，《民視新聞網》，https://www.ftvnews.com.tw/news/detail/2020227N03M1（最後瀏覽日：05/10/2024）。

[58] 吳宗澤，前揭註 20，頁 18-19。

doi:10.6342/NTU202403953

料庫、科技執法資料庫與原先已跨縣市彙整之行車資料庫一併整合，描繪出更加詳盡的行車軌跡。舉例而言，特定人可能於上午 10 時抵達交往對象的住所，停留約 2 小時（遭路口固定式車牌辨識系統拍攝），下午 1 時將車輛停放在臺北市行天宮附近之公有停車場（於停車場入口受到車牌辨識）[59]，下午 3 時出沒於凱達格蘭大道附近參加由在野黨號召之集會遊行（警用車輛移動式車牌辨識），傍晚 6 時行經辛亥隧道（區間測速）至貓空用餐（路口監視器），晚上 11 時違停在臺北市著名同志酒吧入口處（科技執法），凌晨 2 時出現在某友人住家，直至早上 9 時方離開（智慧戰警頭盔）。如此，警察機關透過車牌辨識資料之整合，即可勾勒出特定人一整天的生活軌跡，並據以獲知其人際往來、宗教信仰、政治傾向，甚至是性傾向、外遇對象等與私人生活高度關聯之資訊。而這還僅僅只是一天的資訊量，倘若持續掌握特定人一個月，甚至是一年的行車軌跡，便可以依照其出入特定處所的次數與頻率，對其私人生活做出更精確的推論。換句話說，單純被科技執法設備辨識為違規停車，或者是某日經由自動車牌辨識設備進出停車場的行車資訊，雖然看似零碎且無意義，而無礙於個人生活，縱使被他人得知亦無關痛癢，卻可能在這些資料相互連結的過程中，憑藉車輛停留的時間、地點推知駕駛人的實際行蹤，以此拼湊甚至形塑出完整的私人生活圖像，進而影響個人自由發展其生活與人格的權利。

第二節　車牌辨識系統之干預屬性

介紹完自動車牌辨識系統的技術原理與實際使用情形後，如果對於其廣泛的應用以及探知私人生活的風險感到不安，而欲予以限制，首先必須回答的問題是：

[59] 新竹市路邊收費停車格及公有停車場之車牌辨識系統，原係為繳費目的所設置，近期卻會自動查驗是否為車牌號碼已被註銷之車輛。參考：彭慧婉（08/10/2023），〈加強註銷車牌取締　竹市監理站與市府善用智慧停車柱〉，《台灣好報》，https://newstaiwan.net/2023/08/10/%E5%8A%A0%E5%BC%B7%E8%A8%BB%E9%8A%B7%E8%BB%8A%E7%89%8C%E5%8F%96%E7%B7%A0%E3%80%80%E7%AB%B9%E5%B8%82%E7%9B%A3%E7%90%86%E7%AB%99%E8%88%87%E5%B8%82%E5%BA%9C%E5%96%84%E7%94%A8%E6%99%BA%E6%85%A7%E5%81%9C/（最後瀏覽日：03/31/2024）。

doi:10.6342/NTU202403953

自動車牌辨識系統具體干預人民何種基本權利？是否會因為其所蒐集的車牌辨識資料，包括車牌號碼、通過時間、地點、行車方向甚至是車輛外觀，均屬於公共場所下的資料，且車牌號碼依《道路交通管理處罰條例》第 13 條第 3 款必須具有公示性，而不屬於基本權的保護範圍？關於這個問題，可能會因為對於我國資訊隱私權的內涵理解不同，而產生完全相左的答案。以下，將依序介紹德國法及美國法上關於車牌辨識系統干預屬性的討論，再回過頭來觀察我國歷年來司法院大法官所作成的相關解釋，界定我國資訊隱私權的保護範圍。

第一項　德國法

第一款　自動車牌辨識構成對個人資訊自決權之干預

德國聯邦憲法法院於 2008 年曾作成一則與自動車牌辨識系統相關的重要裁判（下稱「2008 年第一次車牌辨識裁判」）[60]，該裁判涉及黑森邦（Hessen）的《公安法》[61]與什勒斯維希-霍爾斯坦邦（Schleswig- Holstein）的《一般行政法》[62]，當地警方依據這兩部法規施行自動車牌辨識，具體實施流程是先透過錄影設備取得行車影像，再使用軟體識別畫面中的車牌字母與號碼，取得資料後自動與警方的追緝資料庫（Fahndungsdateien）相互比對。如果比對結果符合，系統會發出比對符合通知（Treffermeldung），同時將車牌號碼及識別時間、地點等資訊予

[60] BVerfG, Urteil des Ersten Senats vom 11. März 2008 - 1 BvR 2074/05 -, Rn. 1-185, BVerfGE 120, 378 – 433. 中文說明可參考：林容（2021），《隱密科技偵查與基本權保障》，頁 90-92，國立臺灣大學法律學研究所碩士論文；林容（2020），〈人臉辨識技術做為科技偵查手段之法律問題（一）〉，《法務通訊》，3028 期，頁 5；柯羿良（2023），《自動車牌辨識系統之偵查適法性──以德國法為借鏡》，頁 69-73，國立臺北大學法律學研究所碩士論文。

[61] 系爭條文：Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung §14 Abs. 5:
§14 於公共場所及易生危害之公共設施的資料蒐集、處理與利用。
（5）為與追緝名單（Fahndungsbestand）進行比對，警察機關可以自動蒐集公共街道和廣場上的機動車牌資料。比對不符的資料應立即刪除。

[62] 系爭條文：Allgemeinen Verwaltungsgesetzes für das Land Schleswig-Holstein §184 Abs. 5:
§184 於公開活動與集會和公共場所的資料蒐集。
（5）警察機關依據本法或其他法規於公共交通場所實行檢查（bei Kontrollen），為自動比對追緝名單（Fahndungsbestand），得公開使用科技方法識別機動車輛車牌。秘密蒐集資料僅在公開蒐集會危害措施行使目的時，方可為之。資料比對不符者應立即刪除。比對符合者適用第 4 項第 3-5 句規定。禁止地毯式地（flächendeckend）固定實施第 1 句和第 2 句的科技方法。

doi:10.6342/NTU202403953

以儲存，警方也可能會憑藉此通知採取攔停等後續措施；倘若比對結果不符合，先前所拍攝到的行車影像以及經由電腦軟體識別出的車牌號碼，則會被立即且不留痕跡地刪除[63]。換句話說，德國警方是以「追緝模式」實施自動車牌辨識，而僅在車牌號碼與追緝資料庫比對符合時，才會將車牌辨識資料予以儲存，與前述我國並未區分車輛駕駛人是否具有犯罪嫌疑，一律預防性儲備其行車資訊的模式，有著根本上的差異，「追緝模式」不會迫使不具犯罪嫌疑的一般人承受行車軌跡受到揭露的風險。另外，德國警方也同時利用固定式及移動式的車牌辨識系統，固定式系統可同時識別前方及後方來車，移動式系統則多被裝設於警用交通工具[64]。

針對上述自動車牌辨識措施干預屬性的判斷，德國聯邦憲法法院首先說明，之所以會由德國《基本法》第 2 條第 1 項人格權結合第 1 條第 1 項人性尊嚴，發展出「個人資訊自決權」（informationelle Selbstbestimmung），提前於人格權有危險的階段便提供保護[65]，係考量現代電子資訊技術發展的背景，其促使個人資料的永久保存成為可能，甚至得以不受時空限制，無論身在何處均可於短時間內輕鬆調取。這些受到儲存的個人資料，日後可能與其他個人資料相互結合並揭露更多資訊，進一步形成推論特定人行為的基礎，這個過程中不只損害了人民受《基本法》保障「保持資訊秘密性」的權利（Geheimhaltungsinteressen），甚至可能產生行動自由的干預[66]。同時，也因為現代化電子資訊技術所能處理的資料量遠遠超過傳統方式，其間所產生的風險也使個人資訊自決權的保護需求應運而生。

至於透過電腦系統大範圍自動化蒐集資料，而難免基於技術原因順帶蒐集部分瑣碎資料的情形，應如何判斷是否個別資料蒐集行為均獨立構成個人資訊自決權的干預？德國聯邦憲法法院表示，縱使大範圍的資料蒐集最終僅是作為縮小比對範圍的一種方式，資料蒐集本身也可能構成干預，因為它使國家機關取得個人

63 Vgl. BVerfG, NJW 2008, 1505, 1505.
64 Vgl. BVerfG, NJW 2008, 1505, 1505.
65 Vgl. BVerfG, NJW 2008, 1505, 1506 (Rn. 63).
66 Vgl. BVerfG, NJW 2008, 1505, 1506 (Rn. 64).

doi:10.6342/NTU202403953

資訊並且形成可供日後實施比對的基礎;關鍵在於:考量整體的監控及使用目的,國家機關對於相關個人資訊是否已經產生強烈的興趣,而可以肯定此時已經具備構成干預個人資訊自決權的品質[67]。應注意的是,個人資訊自決權的保護範圍並不僅限於本質上十分敏感的資訊,即使是表面上看起來資訊量輕微而不甚重要的個人資料,依據不同目的進行資料處理後,也會基於與其他資料相互連結的可能性,對於個人隱私及行為自由產生影響。換句話說,在現代電子資訊處理技術的背景下,不論資訊內容為何,都不再有不重要的個人資料了[68]。除此之外,更不會因為個人資料可被公開取得就不受資訊自決權保障。即使個人進入公共場域,資訊自決權仍會保障其個人資料不會在自動資訊蒐集的過程中被任意地儲存與利用[69]。

基於上述說理,德國聯邦憲法法院認為,車牌號碼雖然依法令必須裝設,屬於可被公開取得之個人資料,仍無礙其受個人資訊自決權之保障。某交通工具於特定時間通過特定地點的資訊,經由查詢聯邦汽車運輸管理局(Kraftfahrt-Bundesamt)的註冊登記,即可將該行車資訊連結至車輛所有人[70]。警察機關於比對符合的情形,將系統所取得的車牌辨識資料予以儲存,提供給國家機關並產生未來進一步使用的可能,已經構成對於個人資訊自決權的干預[71]。然而,另一方面,針對比對不符合隨即刪除車牌辨識資料的情形,德國聯邦憲法法院表示:如果資料一經記錄後立即不留痕跡地刪除,且在整個過程中保持匿名性而無法與個人產生關聯,則應認此時並未干預個人資訊自決權。有基於此,本案所使用的車牌辨識系統,如果在識別車牌號碼後立刻與警方的追緝資料庫進行比對,而且於

---

[67] 由於本段文字的內容十分重要,提供原文作為參考:„Maßgeblich ist, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet hat, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist.“ Vgl. BVerfG, NJW 2008, 1505, 1506 (Rn. 65).

[68] Vgl. BVerfG, NJW 2008, 1505, 1506 (Rn. 66).

[69] Vgl. BVerfG, NJW 2008, 1505, 1506 (Rn. 67).

[70] 這段話實際上代表,車牌辨識系統所蒐集的資訊屬於可識別個人之資料,而受德國基本法第 2 條第 1 項結合第 1 條第 1 項之個人資訊自決權所保障。Vgl. BVerfG, NJW 2008, 1505, 1507 (Rn. 70 f.).

[71] Vgl. BVerfG, NJW 2008, 1505, 1507 (Rn. 73).

doi:10.6342/NTU202403953

比對不符合的情形，能夠在法律上及技術上確保資料保持匿名性，並且立即以不留痕跡且不可能建立個人關聯性的方式刪除，就不構成對於個人資訊自決權之干預[72]。

第二款　比對不符合立即刪除仍構成干預

德國聯邦憲法法院的上開見解，主要是以國家機關是否儲存個人資料並使其成為日後實施比對之基礎作為判斷標準，也因此推論出在比對不符合立即刪除資料的情形，因為沒有儲存相關資料，並未產生其未來與各式各樣個人資料相互連結，而得以創造更多個人資料的可能性，甚至是進一步探知私人生活的風險，遂認為此時不構成個人資訊自決權的干預。然而，有疑義的是，雖然國家機關並未將車牌辨識資料儲存以供日後使用，但是確實在識別出車牌號碼的那個時刻，就已經「取得」了個人資料，只是後續選擇將其刪除。德國聯邦憲法法院於前述建構個人資訊自決權干預的判斷標準時，雖有提及必須「考量整體的監控及使用目的，國家機關對於相關個人資訊是否已經產生強烈的興趣，而可以肯定此時已經具備構成個人資訊自決權干預的品質」，後續論述上卻並未針對這個部分作出說明，因此也引來德國部分學說見解的批評。有見解即指出，國家機關無法藉由後續的刪除行為來否定先前識別車牌號碼並與追緝資料庫相互比對的行為已經構成個人資訊自決權的干預，且基於基本權保護及法安定性（Rechtssicherheit）的考量，若是仰賴後續不確定的處理方式來判斷先前的措施是否具備基本權干預性質，亦可謂毫無說服力[73]。另有見解認為，德國聯邦憲法法院上開見解不當地對於個人資訊自決權之干預設置過高的門檻，較合理的作法應該是於干預正當性的層次方判斷其是否能通過比例原則的審查，而不是在一開始就否定其具備基本權干預的性質，蓋縱使是自動化且在短時間內的資料蒐集，也可能對於人民基本權利的自由行使產生嚴重影響。於比對不符合而立即將資料刪除的情形，透過自動

[72] Vgl. BVerfG, NJW 2008, 1505, 1506 f. (Rn. 68).
[73] Breyer, Kfz-Massenabgleich nach dem Urteil des Bundesverfassungsgerichts, NVwZ 2008, 824, 825.

doi:10.6342/NTU202403953

車牌辨識系統識別車牌號碼並即時與警方追緝資料庫相互比對的行為，就已經構成個人資訊自決權的干預，蓋人民在這個過程中無法預期警方後續的作為，更可能因此產生被監視的心理壓力[74]。

2018 年德國聯邦憲法法院再次針對邦警察法授權警察機關實施車牌辨識作成裁判（下稱「2018 年第二次車牌辨識裁判」）[75]，並且明確推翻了 2008 年第一次車牌辨識裁判的見解，認為於比對不符合並立即刪除車牌辨識資料的情形，仍然構成個人資訊自決權的干預。其案例事實略為：巴伐利亞邦（Bavaria）的警察得本於其警察法授權，基於防止危害（Gefahrenabwehr）的目的秘密實施車牌辨識，這個車牌辨識系統會將行經車輛的車牌號碼、通過時間、地點和行駛方向記錄下來，並且與警方依據個案設計的追緝資料庫相互比對。與前述規定相同，如果比對結果不符合（Nichttreffer），所取得的車牌辨識資料同樣會被電腦自動立即且不留痕跡地刪除；如果系統回報比對符合，警察會親自觀看車牌辨識系統所拍攝到的車牌畫面，人工確認是否確實與追緝資料庫的車牌號碼吻合，倘若系統判斷有誤，而屬於「偽比對結果符合」（unechter Treffer）的情形，則整個過程會被警察手動刪除；相對的，如果確實符合追緝資料庫內的車牌號碼（echter Treffer），自動車牌辨識所取得的資料將會被儲存，並可能引發後續措施。本案聲請人的主要住所位於巴伐利亞邦，同時在奧地利有另一居所，因此往返於兩地的過程中時常必須行駛於巴伐利亞邦的高速公路，他擔心可能會受到警方依上開授權實施車牌檢查的影響，因此請求行政法院判決巴伐利亞邦停止蒐集他的行車資訊甚至是與警方追緝資料庫相互比對，並間接地質疑該授權規定的正當性[76]。

關於自動車牌辨識系統於比對不符合立即將資料自動刪除的情形是否構成個人資訊自決權的干預，2018 年第二次車牌辨識裁判所依循的判斷標準基本上

---

[74] Lachenmann, Das Ende des Rechtsstaates aufgrund der digitalen Überwachung durch die Geheimdienste, DÖV 2016, 501, 507 f.

[75] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 1-176, BVerfGE 150, 244-309. 中文說明可參考：林容，前揭註 60，頁 92-94；林容，前揭註 60，頁 5-6；柯羿良，前揭註 60，頁 73-82；林容（2020），〈人臉辨識技術做為科技偵查手段之法律問題（二）〉，《法務通訊》，3029 期，頁 5。

[76] Vgl. BVerfG, NJW 2019, 827, 827.

doi:10.6342/NTU202403953

與 2008 年第一次車牌辨識裁判完全相同，亦即對於自動資料蒐集而言，只有在資料蒐集之初並無特定目標，僅只是基於技術原因順帶蒐集某些資料，但在蒐集後又因為國家機關對其欠缺興趣，而以技術上保持匿名的方式，立即毫無痕跡地刪除，才會認為整個過程缺乏個人資訊自決權的干預性質。因此，判斷的關鍵仍舊在於：國家機關對於相關個人資訊是否有著強烈的興趣，而應肯定此時的自動資料蒐集事實上已經具備個人資訊自決權干預的品質[77]。雖然判斷標準相同，2018 年第二次車牌辨識裁判卻據此作出了不同的推論。德國聯邦憲法法院認為：本案所使用的自動車牌辨識系統，事實上包含車牌號碼識別階段以及車牌號碼比對階段，透過這兩個階段的資料處理，警察機關得以分析出職務上所需的重要資訊。對於警察機關而言，唯有自動車牌辨識系統詳實記錄所有行經車輛的車牌號碼並予以比對，才能夠完整發揮其檢查目標車輛是否通過特定路段的功能。也就是說，事後因比對不符合而被刪除的資料，最初仍然是基於特定目的被警察機關蒐集[78]，一開始對於這些後續比對不符合的車牌辨識資料亦予以蒐集，並非只是單純出於技術原因且毫無目的，反而是使自動車牌辨識系統具備控制性質、作為搜索手段的必要資訊，警察機關其實是有意識地將此種以車牌號碼識別與比對方式實施的控制措施，加諸於所有人身上。有基於此，如果人們在公共場所被警察機關以資料比對的方式檢查其是否具備警察執行勤務上所需要的特定資訊，即使該資料在檢查後被立即刪除，也應該認為警察機關對於這些必須接受檢查的資訊事實上具有強烈的興趣[79]。此外，資料處理是由電腦軟體自動化進行，並不會影響其干預性質的判斷；相對的，反而應該意識到自動化資料處理事實上擴大了警方的控制能力[80]。

資料一經比對不符合立即刪除，表面上看來不會對資料主體造成實際影響或引發任何後續措施，然而仍不改變警察機關在檢查車牌的過程中，對其個人資料

[77] Vgl. BVerfG, NJW 2019, 827, 829 (Rn. 43).
[78] Vgl. BVerfG, NJW 2019, 827, 830 (Rn. 50).
[79] Vgl. BVerfG, NJW 2019, 827, 829 (Rn. 49).
[80] Vgl. BVerfG, NJW 2019, 827, 830 (Rn. 50).

doi:10.6342/NTU202403953

具有強烈興趣的事實。被檢查的車輛駕駛人必須不具備任何警察機關適時所需的特定資訊，才能繼續不受阻礙地行駛於道路上，而這個檢查行為本身就應該被認為干預了人民的自由，因為公民基本上可以在不被國家任意記錄、不需要說明自己的行為是否正當、不暴露在持續受監視的感覺下四處活動，這是共同體自由（die Freiheitlichkeit des Gemeinwesens）的特質之一[81]。如果這類措施可以在任何時間、地點，基於任何目的檢查行經車輛是否被列於追緝名單上，根本無法通過比例原則的審查。相反的，其必須出於特定原因，且具備干預個人資訊自決權的正當性方可施行。另外，德國聯邦憲法法院也指出，本案自動車牌辨識系統與一般交通違規檢查的不同之處在於：一般交通違規檢查，例如測速照相、闖紅燈，是在沒有記錄車牌號碼或蒐集其他個人資料的情況下實施檢查，個人資料只有在資料主體具有相關違規情事的前提下才會被加以儲存，此際因為資料主體發生違反交通法規的情事在先，而使得後續個人資訊自決權之干預具備特定原因，這與本案車牌辨識系統在受干預人毫無犯罪嫌疑或違法情事的前提下即蒐集其個人資料的情形完全不同[82]。

本文認為，2018 年第二次車牌辨識裁判的擔憂並非空穴來風，即使是資料比對後結果不符而立即刪除的情形，亦應肯定於車牌號碼識別與相互比對的階段即已構成個人資訊自決權的干預。原因在於，此種於人民尚不具備犯罪嫌疑，即自動化比對、檢查其是否符合特定要件的措施，一方面迫使人民揭露特定資訊，另一方面則可能因為比對目的不明確以及秘密實施的性質，導致車輛駕駛人難以預期自己是否會遭受攔停詢問，進而產生心理壓力，影響行為自由。

試想，倘若警察機關基於內部應用大數據運算的結果，發現滿足「25 歲至 40 歲、生理性別男、無正常收入超過 2 年、具有犯罪前科、原住民或台中人」這些條件的人，高機率違法持有槍械或毒品，因此秘密地將大致符合這些條件的車

[81] Vgl. BVerfG, NJW 2019, 827, 830 (Rn. 51). 文獻上對於共同體自由（die Freiheitlichkeit des Gemeinwesens）並無特別的說明，本文認為德國聯邦憲法法院這裡所指的並非是特定的基本權，而是指人民毋須在時常感覺受監視的社會中生活，這是人民在社會中自由行使基本權的基礎。

[82] Vgl. BVerfG, NJW 2019, 827, 830 (Rn. 52).

doi:10.6342/NTU202403953

輛所有人加入比對名單之中，並且在比對符合時予以攔停並盤查。則人民單純行駛於道路上，完全不具備犯罪嫌疑，卻必須揭露自己「是否具有」犯罪前科，「是或不是」原住民，並且通過警方的檢查後才能相安無事地繼續行駛於道路上。面對警方秘密實施自動化比對措施，更有可能因為檢查目的與要件設定不明，無法確信自己不會受到影響，遂改變行車路線，避免遭受誤解。於此，若主張比對不符合即不構成個人資訊自決權的干預，明顯是忽略了「不具有犯罪前科」、「不是原住民」本身，根本無法從特定車牌號碼的英文數字中推得而知，因此也是一種個人資料的蒐集，只是因為國家機關適時不需要而予以刪除[83]。此時，透過自動車牌辨識系統實施比對與檢查之目的是否明確且正當？上述篩選條件是否隱含歧視性的風險[84]？若認為比對不符合即不構成干預，則「碰巧」比對不符合的民眾，均無置喙餘地。

另一方面，在「偽比對結果符合」（unechter Treffer）的情形，實際上也隱含個人行車資訊遭受探知的風險[85]。相關報導即指出，2016 至 2017 年間薩克森邦（Saxony）警察機關使用的自動車牌辨識系統雖然在第一階段顯示了 31,831 個比對符合的結果，但是經由警察人工比對後確實符合者只有 873 個，偽比對符合的比例高達 97.25%[86]。換句話說，即使並非比對名單上所列的車輛，仍有可能在警方親自檢查並手動刪除的過程中，被員警知悉其位置資訊。2008 年第一次車牌辨識裁判忽略比對不符合情形亦可能對人民基本權利的行使產生影響，逕行否

[83] 學說另有見解認為，自動車牌辨識措施檢查用路人身分的效果，相當於將所有人民視為潛在的違法者，進而擴大警方監視的權力，有牴觸自由憲政國家原則之虞。Vgl. Roßnagel, Verdachtslose automatisierte Erfassung von Kfz-Kennzeichen, DAR 2008, 61, 62.

[84] 歐盟執法指令（Law Enforcement Directive, LED）第 11 條第 3 項即指出，特種資料的剖析（profiling）若對自然人造成歧視性的結果，應被禁止。*See* Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. 中文說明可參考：李寧修（2023），〈警察運用資料職權之合憲性觀察——以德國聯邦憲法法院【自動化資料分析】判決為中心〉，《月旦法學雜誌》，341 期，頁 90-91。

[85] Hofmann, Autonomes Fahren – kein Problem des Datenschutzes, ZD 2023, 18, 20.

[86] Marcus Engert (15. Okt., 2018), Wie die Polizei Millionen Autofahrer mit einem System überwacht, das nicht funktioniert, BuzzFeed News, online verfügbar unter https://www.buzzfeed.com/de/marcusengert/kennzeichenerfassung-der-polizei-funktioniert-nicht.

doi:10.6342/NTU202403953

定此時的基本權干預性質，直接抹去了比對結果不符合者提起救濟的可能，無疑是為個人資訊自決權設置過高的干預門檻，無利於人民基本權的保障[87]。較合理的做法應該是肯定其基本權干預的性質，並在後續干預授權基礎的設計上，考量此種情形干預程度相對輕微、權利救濟需求較低，而於「通知受干預人」等相關程序擔保上予以放寬或免除。

第二項　美國法

美國聯邦憲法增修條文第 4 條規定：「人民享有其個人人身、住宅、文書或物件不受不合理搜索及扣押之權利，令狀核發，非基於相當理由，不得為之，相當理由應有宣誓誓詞或證詞之支持佐證。令狀應記載明確特定應搜索地點及應搜索扣押之人或物件[88]。」（“The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”）基此，國家機關所實施的偵查行為若是構成美國聯邦憲法增修條文第 4 條意義的搜索，就必須具備法官簽發的令狀，始為合法。至於此處的「搜索」應如何理解，美國聯邦最高法院早期是以警察機關是否侵犯人民的「財產權」作為判斷標準[89]，因此判斷重點就會落在警察機關是否有「物理侵入」（physical intrution）憲法所保護的區域[90]，也曾本於這種著重是否有實際物理侵入的標準，否定警察機關於住宅外監聽的「搜索」性質[91]。這樣的論點在 1967 年的 *Katz* 案後發生轉變[92]，美

[87] 相同見解：Lachenmann, (Fn. 74), S. 507 f. 學說上另有見解從人臉辨識的角度來贊同 2018 年第二次車牌辨識裁判的見解，認為持續的監視會帶給人們嚴重的心理壓力，這不符合自由法治國的原則（Grundsätzen eines liberalen Rechtsstaats）。Vgl. Kulick, „Höchstpersönliches Merkmal“ – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, NVwZ 2020, 1622, 1624.

[88] 翻譯參考：溫祖德（2016），〈臨檢盤查與警犬執法〉，《檢察新論》，19 期，頁 191-192。

[89] Boyd v. United States, 116 U.S. 616 (1886).

[90] 王兆鵬（2007），《美國刑事訴訟法》，二版，頁 107，元照。

[91] Silverman v. United States, 365 U.S. 505 (1961).

[92] Katz v. United States, 389 U.S. 347 (1967). 本案案例事實略為：聯邦調查局探員在未取得令狀的情況下，於公共電話亭的外圍裝設監聽設備，以此竊聽被告撥打公共電話參與賭博犯罪的過程。

doi:10.6342/NTU202403953

國聯邦最高法院於本案透過「隱私期待」（expectation of privacy）的說理，重新理解憲法增修條文第 4 條的搜索行為，並認為憲法增修條文第 4 條所要保護的是「人」，而非「場所」，因此判斷標準應該是「隱私期待」，而非「財產權」。即使人民身處公共場所，只要其欲保有隱私，仍有可能受憲法保護[93]。Harlan 大法官也更進一步在本案的協同意見書中指出，憲法增修條文第 4 條實際上要保護的是人民的「合理隱私期待」（reasonable expectation of privacy），亦即：個人必須顯現其對於所主張之隱私有真正之主觀期待；且該期待必須是社會認為屬客觀合理之期待[94]。此判斷標準一經提出後即受重視，美國實務上後續涉及適用憲法增修條文第 4 條與否的案件多會著重說明被告是否具備合理隱私期待，於車牌辨識的案例中亦然。本文以下透過兩則美國聯邦巡迴上訴法院的裁判，說明美國實務上目前對於車牌辨識是否構成憲法增修條文第 4 條搜索的看法。

第一款　警察機關手動輸入車牌號碼查對，不構成搜索

美國實務上曾發生一起涉及警方使用執法資料網（Law Enforcement Information Network）調查車牌號碼是否構成搜索的案件[95]，*United States v. Ellison* 的案例事實略為：警員 A 於日常巡邏途中發現某車輛疑似違反交通法規怠速停滯於商店外，然其並未上前要求駕駛離去，反而將警車停靠在一旁後開始默默觀察，同時將該車輛的車牌號碼手動輸入於巡邏車內的執法資料網進行調查。調查結果顯示該車輛的車主 B 事實上仍有尚未執行到案的逮捕令（outstanding felony

關於本案的中文介紹可參考：吳維雅（2019），〈FBI 也駭人？執法部門植入惡意軟體遠端監視法制之初探——以美國聯邦法為中心〉，《檢察新論》，26 期，頁 202-203；王兆鵬，前揭註 90，頁 108。

93 Katz v. United States, 389 U.S. 347, 351 (1967) "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

94 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) "[f]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."" 翻譯參考：司法院釋字第 689 號解釋林子儀大法官及徐璧湖大法官提出之部分協同部分不同意見書，頁 11。

95 United States v. Ellison, 462 F.3d 557 (6th Cir. 2006).

doi:10.6342/NTU202403953

warrant）[96]，便據此向前盤查，逮捕後執行附帶搜索的過程中同時也發現車主 B 違法攜帶兩把槍械。

針對這個案件，地方法院經過事實調查後發現被告當時並未違規停車，因此警員 A 使用執法資料網調查被告車牌號碼的行為，實際上並不具備「相當理由」而屬違法，其後續發現的槍械也應依毒樹果實原則予以排除[97]。然而，聯邦第六巡迴上訴法院的見解卻完全不同。聯邦第六巡迴上訴法院認為地方法院的上開見解，是建立在車主 B 對於其車牌號碼具有合理隱私期待而須適用憲法增修條文第 4 條的前提之上，才需要討論警方使用執法資料網調查被告車牌號碼的行為是否具有憲法所要求的「相當理由」。但是，由於車牌號碼本身的用途就是使執法機關辨別身分，依照相關行政法規也必須保持車牌可被輕易識別，因此駕駛人並無法對其車牌號碼的資訊主張具有合理隱私期待，警員 A 於本案使用執法資料網調查車牌號碼的行為自無須具備相當理由[98]。此外，關於使用執法資料網的行為是否構成憲法增修條文第 4 條的搜索，聯邦第六巡迴上訴法院認為執法資料網之所以被創設，本就是為了警方後續勤務的執行，例如尚未執行到案的逮捕令，其相關資訊即是為了使警方得以順利完成逮捕，因此難以想像調查車牌號碼此種非隱私資訊會破壞駕駛人的合理隱私期待，畢竟使用執法資料網的過程並未使警方獲得先前從未取得的資訊，毋寧只是讓警方更快找到相關資訊[99]。

聯邦第六巡迴上訴法院見解的問題在於：如果將手動輸入車牌號碼查對的行為理解為一種查驗身分的手段，警察機關是否得以對不具備犯罪嫌疑的一般人逕行實施，即不無疑義。蓋依照美國刑事訴訟法的思維，攔阻（stop）[100]實際上屬

---

[96] 尚未執行到案的逮捕令（outstanding felony warrant）是指已針對特定對象簽發逮捕令，惟尚未順利緝捕到案的情形。參考：吳維雅（2020），〈公共場所運用人臉辨識科技執法適足性之研析——以美國憲法第四修正案為框架〉，《檢察新論》，28 期，頁 164。

[97] United States v. Ellison, 462 F.3d 557, 559 (6th Cir. 2006).

[98] *Id*., at 560-561.

[99] *Id*., at 562.

[100] 我國法上的用語為「盤詰」及「盤查」。參考：《警察勤務條例》第 11 條：「警察勤務方式如下：…二、巡邏：劃分巡邏區（線），由服勤人員循指定區（線）巡視，以查察奸究，防止危害為主；並執行檢查、取締、盤詰及其他一般警察勤務。三、臨檢：於公共場所或指定處所、路段，由服勤人員擔任臨場檢查或路檢，執行取締、盤查及有關法令賦予之勤務。」

doi:10.6342/NTU202403953

於美國憲法上對人的扣押，亦為憲法增修條文第 4 條的規範客體，雖然因為情況急迫而免除形式上令狀的要求，卻不能免除實質上相當理由的要件，只是因為攔阻侵犯人民權利的程度較逮捕（arrest）低，而在發動要件上從相當理由降至具備「合理的懷疑」（reasonable suspision）即可[101]，非謂可對不具犯罪嫌疑的一般人恣意實施。Moore 法官於其不同意見書即指出，雖然本案使用執法資料網查驗身分的方式，並沒有實質地攔停人民使其接受檢查，看似較一般攔阻情形的侵害程度輕微，然而濫用裁量權限（abuse of discretion）的疑慮卻未因此消除[102]。聯邦第六巡迴上訴法院多數意見雖然宣稱，使用執法資料網的過程並未使警方獲得先前從未取得的資訊，但事實上執法資料網內究竟涵蓋多大範圍的資料？執行何種公務時方能獲得使用權限？這些問題都並未被釐清。縱使車牌號碼本身沒有隱私利益，警員是否可以在人民不具備犯罪嫌疑、裁量權限也不受拘束的情況下，取得這些原先需要在人民具備一定程度犯罪嫌疑的情況下方可取得的資料，實有疑義[103]。紐澤西州最高法院（New Jersey Supreme Court）便曾於 1998 年作成裁判，認為警方執行勤務時雖得使用巡邏車內的移動數據終端用機（mobile data terminals），隨機輸入車牌號碼查詢，然而卻只能確認汽車牌照和註冊所有人的駕照狀態以及該車是否被通報為贓車，不允許在不具備合理懷疑的情況下，進一步連結至監理機關資料庫內車輛登記所有人的其他個人資料，例如姓名、社會安全號碼、地址和前科紀錄[104]。

本文認為，由於美國聯邦憲法增修條文第 4 條的適用效果嚴格，亦即非屬急迫情況下只要構成憲法意義上的「搜索」，實質上必須具備相當理由，形式上亦須取得法官簽發的令狀，始為合法。於此，配合上美國司法實務所提出的合理隱

101 王兆鵬（2003），《路檢、盤查與人權》，頁 107，元照。
102 *Ellison*, 462 F.3d at 568-569 (Moore, J., dissenting).
103 *Id.*, at 566-567, 571-572.
104 State v. Donis, 157 N.J. 44, 55-56, 723 A.2d 35 (1998). 於此呼應了本文前述所舉的例子，亦即警方是否得基於有犯罪前科者違法攜帶槍械、酒駕的機率較高，就逕自將具有前科者的車牌號碼輸入於比對名單之中，過濾並攔停盤查這些人？一方面關乎前科紀錄可能產生的歧視效果；另一方面則涉及在無合理懷疑的情形下，逕行探知人民是否具有犯罪前科等個人資料。

doi:10.6342/NTU202403953

私期待標準，就會使得非急迫性干預人民隱私權的措施，其程序保障的設計只能選擇將之認定為不受相當理由和令狀原則拘束的「非搜索」行為，或是必須符合上述誡命的「搜索」行為，而未如德國法般，於肯定該措施干預個人資訊自決權的性質後，雖然在正當性的審查上必須符合法律保留原則與比例原則，然而並未一律「綁定」相對法官保留原則的程序擔保，而是由立法者設定不同層次的要件，如法官保留、檢察官保留、紀錄義務、刪除義務、目的拘束原則等，層級化地針對不同程度的干預措施提供程序保障。也因此，第六巡迴上訴法院面對本案手動輸入一筆車牌資料查對身分此種影響較為輕微的情形，就傾向於透過合理隱私期待的標準，否定其構成憲法增修條文第 4 條的搜索。不過，若是觀察德國聯邦憲法法院於兩次車牌辨識裁判的討論即可得知，Moore 法官提出的不同意見書並非是庸人自擾。正如德國聯邦憲法法院強調以「追緝模式」實施自動車牌辨識，據以排除預防性資料儲備，對於干預程度影響的重要性，並指出：「與基於特定原因實施的資料蒐集相比，對於不具備法律上原因的一般人蒐集資訊通常會被認為是較高程度的個人資訊自決權干預。如果大量不具犯罪嫌疑的一般人被納入系爭干預措施的實施範圍之下，就可能會產生一種『恫嚇效果』（Einschüchterungseffekt），進而損害人民基本權利的行使，若因而導致系爭干預措施被濫用的風險，並形塑人民時時受到監視的心理壓力，該措施的公正性（Unbefangenheit）就會備受質疑[105]。」本案警員 A 得以在車主 B 不具犯罪嫌疑的情況下，進行原先依照攔阻法理，必須具備合理懷疑方可實施的身分查驗，破壞原先裁量權限標準的同時也擴張了可以「事實上」攔停的對象，亦即，可以取得資料的對象。這種不以受干預人具備犯罪嫌疑為限，而實際上可能波及所有人的措施，應該被視為一種較高程度干預個人資訊自決權的措施。當然，手動輸入與自動檢查是否對於資料取得對象的數量與範圍有著根本性的影響？此際升高的干預程度，是否就因此使其構成美國聯邦憲法增修條文第 4 條意義上的搜索而

[105] Vgl. BVerfG, NJW 2008, 1505, 1507 f. (Rn. 78).

doi:10.6342/NTU202403953

必須適用令狀原則？仍然必須要轉換至美國刑事訴訟實務的思維，依據合理隱私期待的判斷標準重新認定。

第二款　自動車牌辨識是否構成搜索，仍有疑義

上述針對不具犯罪嫌疑的一般人手動輸入車牌號碼檢查身分的問題，在自動車牌辨識的情況下更為顯著。原因在於，相比於手動輸入單筆車牌號碼連結資料庫查詢身分，自動車牌辨識系統更進一步強化了警察機關資料蒐集與比對的能力。一方面，即使車輛於夜間高速行駛，警方仍然能夠憑藉自動車牌辨識系統蒐集所有通過特定路段車輛的車牌資料；另一方面，警方得以將自動車牌辨識系統取得的資料與其他資料相互連結，例如藉由各個時間點取得的車輛位置資訊描繪出駕駛人的行車軌跡，長此以往，隨著資料庫內累積的訊息與時俱增，警方甚至有可能透過車牌辨識資料庫的資料推論特定人的日常行為舉止[106]。於此，警方使用自動車牌辨識系統追查被告行蹤的行為是否構成美國憲法增修條文第 4 條意義上的搜索，就顯得至關重要。

美國聯邦最高法院（Supreme Court of the United States）就曾於 2018 年 *Carpenter v. United States*，針對警察機關調取被告長達 127 天的歷史性行動電話基地台位置紀錄是否構成憲法意義上的搜索作出裁判[107]。該裁判一開始整理了美國聯邦最高法院過往曾討論人民對於其「位置資訊和移動軌跡（physical location and movements）」是否享有合理隱私期待的相關判例。首先，美國聯邦最高法院於 *United States v. Knotts* 中認為，由於在公共場域中駕駛交通工具的移動軌跡屬於人民自願對外公開的資訊，人民因而無法對此享有合理的隱私期待[108]。然而法院

[106] *See* Linda M. Merola, Cynthia Lum, Breanne Cave & Julie Hibdon, *Community support for license plate recognition*, 37 Policing: Int'l J. Police Strat. & Mgmt. 30, 34 (2014).

[107] Carpenter v. United States, 138 S. Ct. 2206 (2018). 中文介紹可參考：溫祖德（2021），〈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。

[108] United States v. Knotts, 460 U. S. 276, 281-282 (1983). 本案案例事實略為：警方在被告購買的毒品原料桶上安裝無線電追蹤器（Beeper），並以此從明尼亞波里斯（Minneapolis）的原料購買處持續追蹤至被告在威斯康辛州（Wisconsin）的湖邊小屋（連續車程超過 5 小時）。

doi:10.6342/NTU202403953

於 *Knotts* 案中也說明，如果對公民 24 小時型態的全面監視（twenty-four hour surveillance of any citizen of this country）成為可能，就必須考慮適用不同的憲法原則[109]。30 年後，*United States v. Jones* 基於聯邦調查局探員安裝 GPS 取得被告 28 天行車軌跡是否構成憲法意義上的搜索，再次討論了是項爭議[110]。雖然 *Jones* 案多數見解最後重申了財產權基準的重要性，表示 *Katz* 案僅是新增了隱私權基準，以此提供人民更完善的保障，並沒有取代「物理侵入」的判斷標準[111]。但是法院同時也強調，*Jones* 案的多數見解並不欲將財產權基準認定為憲法意義上搜索的唯一判斷標準，在不涉及物理性侵入的電子訊號資訊傳輸情形，仍會適用 *Katz* 案提出的合理隱私期待標準[112]。Sotomayor 大法官提出的協同意見書也指出，GPS 監控能夠產生人民在公共場域精準且完整的移動軌跡，這會使得人民大量有關家庭、政治、職業、宗教和性的資訊受到揭露[113]。有基於此，*Carpenter* 案的多數見解肯認人民對於其完整的移動軌跡享有合理的隱私期待，並認為本案所涉及的歷史性行動電話基地台位置紀錄事實上是比 GPS 更嚴重的隱私權侵害[114]。原因在於，過去警方若欲調查特定人先前的行蹤，往往受限於記錄的匱乏和記憶的不足，如今警方得以憑藉歷史性行動電話基地台位置紀錄回溯並重建特定人過去的行止，時間更可長達 5 年，這是無法以其他偵查方式所取得的資訊。更甚者，行動電話基地台持續記錄所有人的位置資訊，而不只是那些具有犯罪嫌疑而接受調查之人，與 GPS 偵查的情形不同，警方不需要提前判斷他們是否以及何時欲調查特定人，等同於任何人一旦被判斷具有犯罪嫌疑，其過去 5 年的位置資訊和移動軌跡，包含其背後隱含的家庭、政治、職業、宗教和性相關資訊就會受到揭

109 *Id.*, at 283-284.
110 United States v. Jones, 565 U. S. 400 (2012). 中文介紹可參考：溫祖德（2018），〈從 Jones 案論使用 GPS 定位追蹤器之合憲性——兼評馬賽克理論〉，《東吳法律學報》，30 卷 1 期，頁 131-138。
111 *Id.*, at 409. “[t]he Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”; 李榮耕（2015），〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《國立臺灣大學法學論叢》，44 卷 3 期，頁 915。
112 *Id.*, at 411. “[S]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.”
113 *Id.*, at 415 (Sotomayor, J., concurring).
114 Carpenter v. United States, 138 S. Ct. 2206, 2217-2218 (2018).

doi:10.6342/NTU202403953

露。另外，雖然行動電話基地台位置資訊的精準度尚不比 GPS，目前約可將目標位置範圍縮小至方圓 50 公尺內，但是正如 Brandeis 大法官所言，當政府得以使用影響更為深遠的方式侵犯隱私權時，法院有義務確保科學的進展不會損及憲法增修條文第 4 條對人民的保障[115]。綜上所述，*Carpenter* 案結論上認為警察機關調取 7 天以上的歷史性行動電話基地台位置紀錄，考量此紀錄揭露個人訊息的深度及廣度，以及不可避免被蒐集資訊的性質，構成憲法增修條文第 4 條的搜索，應由法院審查是否具備相當理由且簽發令狀後，始可為之[116]。

美國實務上也曾有案件涉及警方調取自動車牌辨識資料庫是否構成憲法意義上搜索的爭議[117]。*United States v. Yang* 的案例事實略為：被告 C 被監視器拍攝到，其駕駛自租車公司短期租用的汽車竊取郵筒內的信件，警方前往租車公司詢問後卻發現，C 已經逾期六天未歸還汽車，甚至將租用汽車內的 GPS 裝置關閉使得租車公司無法得知其位置資訊或是遠端熄火。有鑑於此，警方轉而向由私人公司 D 所營運，美國境內最大的車牌辨識資料庫調取資料，試圖取得租用汽車及被告 C 的位置資訊。D 公司透過裝設於拖車及警用交通工具上的移動式車牌辨識系統，拍攝行經車輛的車牌後識別其車牌號碼，並與拍攝時間地點一併儲存於資料庫內，執法機關只要固定付費便可使用該資料庫。於 2016 年 12 月，該資料庫已經儲存了近 50 億筆車牌辨識資料，並估計於 2019 年 3 月取得超過 65 億筆資料。警方查詢該資料庫後僅得出一筆於 C 已逾期未歸還汽車的期間所辨識到的車牌資料，隨即憑藉這筆資料前往指定地點，目視發現該租用車輛停放在 C

---

115 *Id.*, at 2223; Olmstead v. United States, 277 U. S. 438, 473-474 (1928).

116 之所以將構成搜索的紀錄調取時長設定為「7 天以上」，只是單純因為本案警方前後一共聲請了兩個調取令，第一個要求調取被告 127 天的位置紀錄，第二個要求調取被告在另一個州 7 天的位置紀錄。法院因此認為其無須決定是否在一定期間內的基地台位置紀錄調取即不構成憲法意義上的搜索。*See* Carpenter v. United States, 138 S. Ct. 2206, 2217-2218 (2018) "[w]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." 然而，這也引來批評，事實上警方聲請的第二個調取令只取得了被告 2 天的位置紀錄，多數意見最後為何選擇以 7 天作為標準，而不是 2 天，並未說明。遑論多數意見雖然提及了 7 天以下的紀錄調取或許有可能不構成搜索，卻對於其判斷標準隻字未提。*See Id.*, at 2234, 2266-2267 (Kennedy, J., joined by Thomas, J., and Alito, J., dissenting; Gorsuch, J., dissenting).

117 United States v. Yang, 958 F.3d 851 (9th Cir. 2020).

doi:10.6342/NTU202403953

的住所外後，便據此向法院聲請核發搜索票，隨後在 C 的住所內找到 C 本人、失竊的信件以及違法持有的槍械。

可惜的是，聯邦第九巡迴上訴法院於本案並未正面處理自動車牌辨識系統是否構成憲法增修條文第 4 條搜索的爭議，反而是以一種相對取巧的方式迴避這個問題。其認為，該筆資料所顯示的時間為晚間 11 點 24 分，且正好是被告 C 租約到期的那一天，由於適時已超過租車公司的營業時間，觀察雙方簽訂的租賃契約並沒有繼續付費以延長期限的相關條款，租車公司也曾試圖使用車內的 GPS 裝置定位車輛，故應認被告 C 針對自動車牌辨識系統於其違約未歸還車輛期間揭露位置資訊的行為，不能主張合理的隱私期待[118]。也因為本案使用自動車牌辨識資料庫僅涉及一筆已違反租約期限仍未歸還車輛的資料，因此無須決定警察機關取得被告於租約期間使用車輛的位置資訊是否構成搜索的問題[119]。

相較之下，Bea 法官提出的協同意見書就正面地表示，警察機關使用車牌辨識資料庫的行為，因為資料庫內的資料無法完整地顯現出被告 C 的移動軌跡，並未破壞被告 C 的合理隱私期待，因此不適用憲法增修條文第 4 條的令狀原則[120]。*Carpenter* 案多數見解雖然肯認人民對於其完整的移動軌跡享有合理的隱私期待[121]，但是根據本案 D 公司負責人在證據排除聽審程序的證詞，系爭資料庫雖然含有近 50 億筆車牌辨識資料，但是平均每年只會取得單一車輛 4 筆的辨識資料，以本案被告 C 為例，警方調取其行車資料的期間，被告 C 雖然駕駛了 10 萬 5 千英里，卻只有一筆的辨識資料[122]。Bea 法官據此推論，法院作出判斷時雖然必須考量系爭措施於未來可能的發展，但是以本案被告 C 僅被取得一筆資料為例，警察機關完全無法透過車牌辨識資料庫取得人民完整的移動軌跡，其背後與家庭、政治、職業、宗教和性相關的資訊也未受揭露，因此不會構成憲法意義上的搜索。儘管如此，Bea 法官最後也說明，如果伴隨科技持續發展，車牌辨識未來得以取

118 *Id.*, at 861.
119 *Id.*, at 861-862.
120 *Id.*, at 864 (Bea, J., concurring).
121 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
122 *Yang*, 958 F.3d at 862.

doi:10.6342/NTU202403953

得的位置資訊性質與範圍若可比擬（comparable）*Carpenter* 案中的行動電話基地台，則有適用憲法增修條文第 4 條的可能[123]。

申言之，聯邦第六巡迴上訴法院雖然在 *Ellison* 案基於車牌依法必須保持公示性的說理，表示駕駛對於其車牌號碼所涵蓋的資訊不具有合理的隱私期待。然而，伴隨自動車牌辨識系統擴大警方蒐集與比對資訊的能力，以及資料統整後描繪出特定人完整行車軌跡的可能，若是僅憑車牌具有公示性的說法即欲主張自動車牌辨識系統不構成憲法意義上的搜索，顯然是過於草率。*Jones* 案結論上雖然是以財產權基準認定 GPS 的搜索性質，惟其論證過程中也承認在不涉及物理性侵入的電子訊號資訊傳輸情形，仍會適用 *Katz* 案提出的合理隱私期待標準。配合 Sotomayor 大法官具體指出，位置資訊背後所隱含與私人生活高度相關的家庭、政治、職業、宗教與性的資訊，*Carpenter* 案肯認了人民對於其完整移動軌跡享有合理的隱私期待，並且將長時間歷史性行動電話基地台紀錄的調取認定為憲法意義上的搜索。雖然，*Yang* 案的多數意見迴避了自動車牌辨識系統是否構成搜索的爭議，Bea 法官甚至直言自動車牌辨識在當時完全不可能使警察機關掌握人民完整的移動軌跡，人民對於自動車牌辨識資料不能享有合理的隱私期待。然而，隨著未來科技發展和資金的挹注，系統設置的覆蓋完整率將日漸提升，自動車牌辨識勢必會成為警方偵防的利器。伴隨車牌辨識資料與時俱增地累積，使用自動車牌辨識資料庫描繪個人移動軌跡的能力將更為完備且精準，屆時，美國實務將無可避免地再次面對自動車牌辨識系統是否構成憲法增修條文第 4 條搜索的爭議[124]。

---

[123] *Id*., at 862 (Bea, J., concurring).

[124] 學說上也有見解依據馬賽克理論（mosaic theory）認為自動車牌辨識系統構成美國憲法意義上的搜索。*See* Jessica Gutierrez Alm, *The Privacies of Life: Automatic License Plate Recognition in Unconstitutional under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 Hamline L. Rev. 127, 127-160 (2015).

doi:10.6342/NTU202403953

第三項　我國法

第一款　釋字第 603 號解釋「資訊隱私權」之內涵

我國警察機關於全國各縣市重要路口及高速公路路段裝設自動車牌辨識系統，同時在警用車輛安裝移動式車牌辨識系統，將所有通過車輛的車牌號碼一律預防性儲備至資料庫內以供日後追訴刑事犯罪所用，是否構成基本權干預？必須先探討保障匿名及隱私的一般人格權（亦屬我國憲法第 22 條所稱之「其他自由及權利」）以及由此導出的「資訊隱私權」之基本權保障領域（Schutzbereich）具體為何[125]。「資訊隱私權」的用語首見於我國司法院釋字第 603 號解釋，其於解釋文表示：「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障（本院釋字第 585 號解釋參照）。其中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。」憲法法庭於 111 年憲判字第 1 號判決【肇事駕駛人受強制抽血檢測酒精濃度案】除了重申上述意旨，也指出：「國家基於公益之必要，雖非不得立法強制取得所必要之個人資訊，惟其取得與利用個人資訊之目的、範圍與程序等重要事項，均應以法律明確規定，如授權以命令定之，亦應符合授權明確性原則；且應依個人資訊之屬性、取得方式、利用目的與範圍等，設定相當之正當法律程序以及確保該等資訊不受濫用與不當洩露之適當防護機制，始無違憲法第 23 條之法律保留原則，而符合憲法保障人民資訊隱私權之意旨。」其後，111 年憲判字第 13 號判決【健保資料庫案】再度引述司法院釋字第 603 號解釋關於資訊隱私權

[125] 參考：林鈺雄（2021），〈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 48-49。

doi:10.6342/NTU202403953

的論述之餘，也進一步強調：「資訊隱私權保障當事人原則上就其個資，於受利用之前，有同意利用與否之事前控制權，以及受利用中、後之事後控制權。除當事人就獲其同意或符合特定要件而允許未獲當事人同意而經蒐集、處理及利用之個資，仍具事後控制權外，事後控制權之內涵並應包括請求刪除、停止利用或限制利用個資之權利。」

觀察司法院釋字第 603 號解釋對於資訊隱私權內涵的描述，可以發現其雖使用「隱私」的用語，然而實際上卻著重於個人資料的自主控制，近似德國聯邦憲法法院於 1983 年人口普查案提出個人資訊自決權之內涵[126]。對此，學說上即有認為資訊隱私權與資訊自主（決）權似乎僅是名稱上有所差異，其內涵與保障範圍應無太大分別，而可互相通用，我國大法官之所以稱其為資訊隱私權，僅是因為過往的司法院解釋向來使用「隱私權」的用語，並且認為資訊隱私為隱私權的保障範圍之一，因此若是另外採用資訊自主權的概念或用語，可能會導致身體隱私及空間隱私的保障需要另尋權利基礎，反生困擾[127]。另有見解認為，司法院釋字第 603 號解釋應以「資訊自主權」作為論證的基調，方較為周延[128]。理由在於：資訊自主（決）權事實上屬於資訊隱私權的前哨，涉及資訊自主權的個人資料蒐集、處理或利用，未必會關乎個人的隱私，若是使用「資訊隱私權」的概念，可能會導致未來有關個人資料保護的問題，都必須先釐清系爭個人資料與隱私之間的關聯程度，倘若個人資料屬於已公開之資訊而與隱私無涉，是否仍屬於司法院釋字第 603 號解釋「資訊隱私權」的保障範圍，就必須依照每個人對於合理隱私期待的認知不同而定。然而，若是以「資訊自主權」的概念出發，就不會在是否

---

126 BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71. 判決中指出：「在現代化資料處理狀況下，基本法第 2 條第 1 項和第 1 條第 1 項的一般人格權包括了個人保護其本人資料不受無限制地提取、儲存、使用和繼續傳送。就此方面基本權利保障個人，基本上自我決定透露或使用其個人資料之權利。」判決中譯，參考：蕭文生（1999），〈關於一九八三年人口普查法之判決〉，劉孔中（等譯），《西德聯邦憲法法院裁判選輯（一）》，頁 270-326，司法院。

127 學者也因此贊同「資訊隱私權」的用語。參考：黃昭元（2005），〈無指紋則無身分證？換發國民身分證與強制全民捺指紋的憲法爭議分析〉，國際刑法學會台灣分會（等編），《民主、人權、正義——蘇俊雄教授七秩華誕祝壽論文集》，頁 470，元照。

128 李震山（2020），〈論資訊自決權〉，《人性尊嚴與人權保障》，五版，頁 254，元照。

doi:10.6342/NTU202403953

構成基本權干預的層次上發生爭議，因為個人資料的蒐集、處理和利用必然關乎資訊自主權，只需於後續再考量所涉個人資料的敏感性程度，以此設計授權基礎的要件寬嚴[129]。對此，林子儀大法官也曾於釋字第 603 號解釋之協同意見書中指出：「其將資訊隱私權所欲保護之對象限於個人私密之資訊，毋寧過分限縮，而不能因應現今資訊科技發展所可能對個人造成之侵害。蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護[130]。」

第二款　釋字第 689 號解釋之「合理隱私期待」標準

經由上開說明可知，我國司法院釋字第 603 號解釋所提出的資訊隱私權，雖然使用「隱私」的用語，惟其內涵實際上與德國基本法第 2 條第 1 項結合第 1 條第 1 項的資訊自決權相同，皆是基於電腦資訊科技發展的背景，考量無重要意義的中性個人資料經過大量積累並相互連結的過程後，仍會產生形塑私人生活圖像的風險，甚至影響人民自由發展其人格的權利，因而在個人資料的蒐集、處理與利用階段即為人格權提供前置化的保護，縱使是零碎、片段、無意義的個人資料仍屬其保障射程範圍，更不限於個人秘密之資訊。若是依此標準（下稱「資訊自決標準」），個人縱使身處於公共場域仍受資訊隱私權保障，享有個人資料的自主決定權，自為不辯自明之理。不過，針對個人在公共場域中得享有不受他人侵擾之私人活動領域與個人資料自主，司法院釋字第 689 號解釋卻提及了另一個判斷

[129] 李震山，前揭註 128，頁 254-255。
[130] 司法院釋字第 603 號解釋林子儀大法官提出之協同意見書。

doi:10.6342/NTU202403953

標準，其指出：「蓋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念認為合理者。」在此，司法院釋字第 689 號解釋明顯採用了前述 *Katz* 案中 Harlan 大法官所提出的「合理隱私期待」，將之作為個人在公共場域中得主張不受他人持續注視、監看、監聽、接近等侵擾之自由的判斷標準，並再度引發了資訊隱私權之具體內涵及判斷標準為何的爭議。

對此，學說上有見解認為，「資訊隱私」和「資訊自決」各自有著完全不同的內涵和保護射程範圍，二者互為交叉關係，「資訊自決」著重在個人對於資料的自主控制可能性，事實上是一種行為自由[131]；「『資訊隱私』則是對蒐集使用個人資訊進行分析以產出與人有關之各種圖像的『知識／權力』生產活動，進行必要的制衡，以盡可能地避免『知識／權力』之生產透過人之圖像的提供，在人格形成的內在領域中造就過於僵化的自我認識基準[132]。」學者並據此認為司法院釋字第 603 號解釋並未正確認識二者的分別，而誤用「資訊隱私權」的用語指稱「資訊自決」的概念[133]。另有見解認為，「資訊自決」並未限制資訊的範圍，屬於一個較為寬廣的概念，因此「資訊自決」與「資訊隱私」應為包含關係而非交叉關係，「資訊自決權」與「隱私權」之間才具有交叉關係[134]。至於我國釋憲實務上

131 邱文聰（2009），〈從資訊自決與資訊隱私的概念區分——評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，168 期，頁 174。
132 邱文聰，前揭註 131，頁 177。
133 邱文聰，前揭註 131，頁 180。
134 張志偉（2017），〈從資訊自決與資訊隱私的概念區分，檢視被遺忘權的證立問題〉，《萬國法律》，211 期，頁 4。

doi:10.6342/NTU202403953

則幾乎未曾正面探究過兩套判斷標準之間的關係，僅楊惠欽大法官於 111 年憲判字第 13 號判決提出的部分不同意見書曾說明：「資訊隱私權應係針對隱私權中關於個人資料部分之描述，其著重者係個人生活私密領域之資訊不受他人侵擾自由之保障；至資訊自決權則重在個人對其自身資料享有在何種範圍內、於何時、以何種方式、向何人揭露之自主控制權；惟個人生活私密領域之資訊不受他人侵擾自由之保障，勢須使個人對其自身資訊享有在何種範圍內、於何時、以何種方式、向何人揭露之自主控制權，是二者固各有著重之權利內涵，然於憲法裁判進行個案法規範對人民基本護之限制，是否違反比例原則之審查時，係應就該法規範之規範意旨，整體判斷所涉之基本權面向；於與個資相關之法規範審查，該法規範或僅涉資訊隱私權或資訊自決權，或係兼及二者。實則，就現今之大數據時代，所面對個資未經當事人同意之大規模蒐集，並建立資料庫儲存之情形，相關法規範是否違反比例原則之審查，除應本於資訊隱私權及資訊自決權之內涵，整體考量審查標的之法規範是否在其等射程範圍，資以判斷個案法規範所涉之基本權外，融入前述司法院釋字第 603 號解釋所稱組織上與程序上必要防護措施等，亦係必要之思考方向。」楊惠欽大法官更於系爭規定涉及何種基本權的討論上表示：「本席認本號判決亦肯認系爭規定一涉及之基本權，係包含資訊隱私權及資訊自決權，僅是仍沿司法院釋字第 603 號解釋為資訊隱私權之用語。是本席以下就系爭規定一是否違反比例原則之意見，雖本於綜合資訊隱私權及資訊自決權之保障意旨予以整體判斷之方向為之，惟仍依本號判決使用資訊隱私權之用語。」言下之意，楊惠欽大法官也肯認「資訊隱私權」與「資訊自決權」事實上屬於兩種不同的概念，並且在法規範的審查上必須分別視其是僅涉及其一或是兼及二者，惟囿於司法院釋字第 603 號解釋的用語，將資訊隱私權與資訊自決權二者的保障一併涵蓋於司法院釋字第 603 號解釋提出的「資訊隱私權」之下。

本文認為上述學說討論仍然無法確實解決是項爭議，原因在於學者們雖然孜孜不倦地定義「資訊隱私」與「資訊自決」，並試圖區分不同概念之間的關係，但是隨著學者之間不同的求學背景而對於憲法上隱私權保障範圍的想像不一，司

doi:10.6342/NTU202403953

法院釋字第 603 號解釋所稱資訊隱私權之內涵應如何界定，似乎將永無休止之日。楊惠欽大法官將資訊隱私權界定為「個人生活私密領域之資訊不受他人侵擾自由之保障」，並認定資訊自決權側重於個人資料之自主控制權，二者保護射程範圍雖然不同，但同時涵蓋於司法院釋字第 603 號解釋提出的「資訊隱私權」之下，雖有用語重複而可能發生概念混淆之疑慮，卻至少正面肯認了二者皆屬憲法所保障的基本權利，且於規範審查同時涉及二者的保障範圍時，亦應綜合整體判斷，結論上值得贊同。然而，是否會因為資訊自決標準並未限制資料保護的範圍，而導致實際應用上架空了合理隱私期待的判斷標準，又或者貫徹資訊自決的判斷標準實際上就是我國大法官之真意，這些問題仍有賴釋憲實務的發展，方能獲得解答。

第三款　具公示性質之車牌號碼仍受資訊隱私權保障

關於公共場域中干預資訊隱私權的判斷標準，究竟應適用釋憲實務上普遍引述的資訊自決標準，還是釋字第 689 號解釋所提及的合理隱私期待標準，對於自動車牌辨識干預性質的判斷至關重要。例如於前述 *Yang* 案的案例事實，在國家機關使用自動車牌辨識系統僅儲存到受干預人一筆車牌辨識資料的情形，受干預人是否仍然可以主張其受到基本權的干預，就與判斷標準為何息息相關。蓋若依據司法院釋字第 603 號解釋所提出的資訊自決標準，因為警察機關透過查核監理機關的註冊資料，即可將車牌號碼連結至車輛所有人，因此特定車輛之車牌號碼及其出沒時間、地點屬於足資識別的個人資料，國家機關蒐集此種個人資料自然構成資訊隱私權之干預。然而，若是依據合理隱私期待標準，則有可能因為車牌號碼本來的用途即是使執法機關得以辨識身分，且依行政法規也必須保持公示性，而難以對於僅一筆的車牌辨識資料儲存主張享有合理的隱私期待。

於此，學說有見解認為既然我國釋憲實務同時肯認了資訊自決權（資訊隱私權）及不受侵擾之隱私權，那麼針對自動車牌辨識的合法性審查，就必須同時通

doi:10.6342/NTU202403953

過合理隱私期待標準及資訊自決標準的檢驗，方可認其為合法[135]。此見解結論上與楊惠欽大法官之意見書相同，於我國釋憲實務尚未明確區分兩種判斷標準的適用情形之前，本文基於基本權保障的觀點從之。蓋正如楊惠欽大法官所言，我國資訊隱私權包括了側重個人生活私密領域不受侵擾的「資訊隱私」面向，以及著重個人資料自主控制的「資訊自決」面向。二者保障人民基本權的內涵有所不同，雖然因襲司法院釋字第 603 號解釋之用語，而在我國釋憲實務上皆涵蓋於「資訊隱私權」的保障範圍，然而在法規範或基本權干預審查同時涉及二者之保障範圍時，應綜合整體判斷。倘若僅因自動車牌辨識系統涉及公共場域的資訊蒐集，即欲以合理隱私期待為準繩，排除資訊自決標準的適用，則明顯是忽略了釋字第 603 號解釋乃是基於電腦資訊科技發展的背景，考量無重要意義的中性個人資料經過大量積累並相互連結的過程後，仍會產生形塑私人生活圖像的風險，甚至影響人民自由發展其人格的權利，故發展出近似德國法上個人資訊自決權內涵的「資訊隱私權」，而車牌辨識資料正是其所謂儲存後會與其他個人資料相互連結，以對特定人私人生活產生精確推論的情形，當然必須納入其保護範圍並謹慎審視。

同時，相比於釋字第 689 號解釋曇花一現地提及合理隱私期待標準，釋字第 603 號解釋所提出的資訊自決標準，已成為我國釋憲實務上穩定發展的資訊隱私權內涵，這從 111 憲判字 1 號判決、111 憲判字 13 號判決仍持續引用，並在此基礎上繼續細緻化其內涵，建構「確保資訊不受濫用與不當洩露適當防護機制」、「請求刪除、停止利用或限制利用個資之事後控制權」等資訊隱私權干預之憲法誡命，即可得知。單憑車牌號碼具有公示性，即欲透過合理隱私期待標準否定少量車牌辨識資料儲存的干預性質之反對意見者，必須提出足夠充分的說理，方得免除資訊自決標準的適用，畢竟一旦否定了此際的干預性質，不僅免去了立法者為遵守法律保留原則而賦予人民的程序保障，也同時剝奪了受影響人提起救濟的權利。

[135] 連孟琦（2023），〈刑事偵查與個人資訊自決權（資訊隱私權）之保護——以德國 2021 年 6 月新增刑事訴訟法自動化車牌辨識規定（§163g StPO）為例〉，《檢察新論》，32 期，頁 88-89。

doi:10.6342/NTU202403953

依據上開說理，由車牌號碼、出沒時間、地點所組成的車牌辨識資料，由於車牌號碼可依循交通部之車籍資料庫連結至特定人，縱使駕駛人並非車輛所有人，也可透過詢問車輛所有人或調閱監視錄影畫面等方式推得而知，因此屬於《個人資料保護法》第 2 條第 1 款所規定「得以間接方式識別該個人之資料」，而涵蓋於資訊隱私權之保障範圍。據此，警察機關縱使僅蒐集到少量的車牌辨識資料，仍然對特定人構成資訊隱私權之干預，而應符合法律保留原則、明確性原則以及比例原則。

另一方面，倘若在個案中涉及國家機關蒐集、儲存或調取大量車牌辨識資料，以此描繪出特定人完整的行車軌跡，甚至是持續使用自動車牌辨識系統達到即時（real-time）監控的效果，則不論是依據資訊自決標準或是合理隱私期待標準，均會構成資訊隱私權的干預。我國最高法院便曾於偵查機關違法使用 GPS 的判決中表示：「有無隱私權合理保護之期待，不應以個人所處之空間有無公共性，作為決定其是否應受憲法隱私權保障之絕對標準。即使個人身處公共場域中，仍享有私領域不被使用科技設備非法掌握行蹤或活動之合理隱私期待…然由小貨車須由駕駛人操作，該車始得移動，且經由車輛移動之信息，即得掌握車輛使用人之所在及其活動狀況，足見車輛移動及其位置之信息，應評價為等同車輛使用人之行動信息，故如就『車內之人物及其言行舉止』而言，因車輛使用人經由車體之隔絕，得以確保不欲人知之隱私，即難謂不屬於『非公開之活動』…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[136]。」假使自動車牌辨識系統裝設的密度達一定程度，輔以軟體運算特定車輛在各個被捕捉的地點之間最有可能的行經路徑，就可以發揮同 GPS 般繪製特定人完整行車軌跡的效果。此時，縱使是依據個人生活私密領域不受侵擾之合理隱私期待標準，亦會對個人構成（資訊）隱私權的重大干預。

[136] 最高法院 106 年度台上字第 3788 號刑事判決。

doi:10.6342/NTU202403953

第三節　德國法上自動車牌辨識授權基礎之建構

肯定自動車牌辨識系統對於資訊隱私權（資訊自決權）的干預性質後，必須進一步探討應如何設計自動車牌辨識的授權基礎，方可使其於形式上符合法律保留與明確性原則的要求，更於實質上符合比例原則的誡命。對此，前述兩則德國聯邦憲法法院關於自動車牌辨識的裁判中多有闡述，以下節錄重要部分供我國法參考，並於其後介紹德國《刑事訴訟法》於 2021 年所新增的自動車牌辨識授權規定。

第一項　德國聯邦憲法法院提出之要求

首先，對於干預授權基礎的憲法要求，亦即其要件之寬嚴，取決於基本權干預的種類與程度[137]，因此，必須先判斷自動車牌辨識系統實際上多大程度地干預個人資訊自決權。德國聯邦憲法法院說明，影響個人資訊自決權受干預程度的因素，包括資訊的性質、蒐集資訊的地點與情狀、受該措施干預的對象，以及資訊未來可能被利用的方式[138]。資訊的性質除了資訊本身與個人人格的關聯性高低，也應該考量其日後是否可能與其他資料相互連結而產生與個人人格更高程度的關聯[139]。有鑑於此，對於自動車牌辨識系統干預個人資訊自決權程度的判斷，必須視其使用情境（Verwendungskontext）而定[140]。例如，如果國家機關只是為了尋找失竊車輛而實施自動車牌辨識，此時儲存車牌號碼比對符合者的行車資訊，並不是要據此推論駕駛人的其他行為，或者供未來與其他資料相互連結，則所蒐集資料與個人人格之間的關聯性即相對較低[141]。同時，車牌號碼與車輛行駛方向

137 Vgl. BVerfG, NJW 2008, 1505, 1507 (Rn. 75).
138 Vgl. BVerfG, NJW 2008, 1505, 1507 (Rn. 76).
139 Vgl. BVerfG, NJW 2008, 1505, 1507 (Rn. 77).
140 國內有學者將之翻譯為「利用文脈」。參考：劉芳伶（2021），〈論運用「車牌辨識技術」所為「N 系統偵查」之適法性判斷構造與要件〉，《軍法專刊》，67 卷 4 期，頁 109。
141 Vgl. BVerfG, NJW 2008, 1505, 1508 (Rn. 82).

doi:10.6342/NTU202403953

存在於公開場所的事實，雖然不會否定警方蒐集個人資料的基本權干預性質，卻也會降低自動車牌辨識對於個人資訊自決權的干預程度[142]。更重要的是，如果是基於特定目的而實施自動車牌辨識，例如上述為了尋找失竊或是識別積欠事故保險費車輛的情形，則只會儲存部分具有法律上原因之特定人的資料。干預措施蒐集資料的對象，是否具備如違反法律等可歸責於己的法律上原因，或者不以此為限而事實上可能及於所有人，於個人資訊自決權干預程度的判斷上舉足輕重。與基於特定原因實施的資料蒐集相比，對於不具備法律上原因的一般人蒐集資訊通常會被認為是較高程度的個人資訊自決權干預[143]。原因在於，倘若大量不具犯罪嫌疑的一般人被納入系爭干預措施的實施範圍之下，就可能會產生一種「恫嚇效果」，進而損害人民基本權利的行使，若因而導致系爭干預措施被濫用的風險，並形塑人民時時受到監視的心理壓力，該措施的公正性就會備受質疑[144]。

另一方面，假使國家機關實施自動車牌辨識的目的是為了探知駕駛人的日常活動，個人資訊自決權的干預程度就會發生轉變。根據自動車牌辨識系統設置地點的不同，警方除了取得駕駛人的行車資訊本身以外，也有可能間接地獲知駕駛人的其他行為，或是在與其他個人資料相互連結的過程中產生更多資訊。例如設置於特定停車場或是重要出入路段的自動車牌辨識系統，除了使警方知悉駕駛的停車位置，更可以透過這個停車地點，據以推論駕駛可能正在參與附近會場的某個活動，像是一場足球賽或是一個重要的會議，在這種情況下，該措施的實施就可能會造成其他基本權的干預，例如使用自動車牌辨識系統將公民集會遊行會場附近可能屬於參與群眾的車輛一一記錄，即有可能產生言論自由的干預[145]。尤有甚者，如果警方被授權得以車輛位置資訊對駕駛人的日常活動做出推論，且將系統多次取得的車牌辨識資料秘密儲存並整合成完整的行車軌跡，自動車牌辨識將可以作為一種新型態的科技監視工具。此時自動車牌辨識系統就不僅止於協助警

142 Vgl. BVerfG, NJW 2008, 1505, 1508 (Rn. 83).
143 Vgl. BVerfG, NJW 2008, 1505, 1507 f. (Rn. 78).
144 Vgl. BVerfG, NJW 2008, 1505, 1507 f. (Rn. 78). 由此可見我國於人民尚不具備法律上原因即將其行車資訊予以儲存的實施模式，屬於較嚴重的個人資訊自決權干預，詳後述。
145 Vgl. BVerfG, NJW 2008, 1505, 1508 f. (Rn. 88).

doi:10.6342/NTU202403953

方找到特定車輛，開啟後續逮捕等措施的工具，而是在與其他資料相互連結的過程中，直接產生警方所需要的特定資訊，成為一種可能與個人人格具備高度關聯性的新興干預措施。若是警察機關藉此詳盡地蒐集特定人的資料，並與其他資料相互連結來更進一步地推論受干預人的言行舉止，例如受干預人基於什麼原因在特定地點長時間停留？與誰見面？做了什麼？此種干預措施甚至會產生形塑人格圖像的風險[146]。此外也須注意，自動車牌辨識系統秘密實施的性質也會加劇其干預個人資訊自決權的程度。因為在隱密實行基本權干預措施的情形，受干預人將因此失去事前參與程序的機會，亦無法在事中要求停止這個措施持續干預其基本權，事後救濟也可能會比公開實施的干預措施來得困難[147]。雖然在一般情況下，除非警方刻意隱匿裝置或是選擇從車輛後方拍攝，否則人民通常可以發現自動車牌辨識系統的攝影設備，但是即使人民看見了攝影設備，也會因為無法得知其是否被列於比對名單之上？比對結果為何？資料是否被儲存？而無法主動尋求法律救濟[148]。

藉由自動車牌辨識系統的使用情境，確立其具體干預個人資訊自決權的程度後，德國聯邦憲法法院強調，法律明確性原則（Bestimmtheitsgebot）是為了讓具有民主正當性的立法者，對於國家機關實施措施可干預的基本權種類及範圍做出決定，同時使行政機關在執行法律時得以遵循立法者所劃定的界線，並讓司法機關可以有效監督。不僅如此，法律明確性原則也使人民得以事前預見其可能會在什麼樣的條件下受到基本權的干預[149]。由於法律明確性原則之寬嚴，也取決於基本權干預的類型與嚴重程度。因此，干預授權基礎必須明確表現出是否事實上涵蓋干預程度更高的情形。如果單憑條文無法明確排除更高程度侵害基本權的可能，就必須視立法者是否在要件上做出同樣嚴格的設計[150]。而授權基礎若是涉及資訊自決權的干預，法律明確性的誡命同時會產生一個重要的功能，亦即確保干預措

146 Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 90-92).
147 Vgl. BVerfG, NJW 2008, 1505, 1508 (Rn. 79).
148 Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 89).
149 Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 94).
150 Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 95).

doi:10.6342/NTU202403953

施的發動原因及相關資料的使用目的受到一定程度的限制，以此強化憲法上「所蒐集資訊之目的拘束性」要求（Gebot der Zweckbindung der erhobenen Information）[151]。畢竟，假使不針對資料蒐集與使用的目的做出限制，就可能導致資料被國家儲存後，被用於與原先蒐集目的完全不同的各種原因，而無法預見資料未來將如何被使用[152]。有基於此，德國聯邦憲法法院指出，自動車牌辨識的實施必須基於足夠具體、客觀特定的原因（Anlass），使警方的行為可預見且可審查，對此，立法者可以選擇將特定個別的風險明定於條文中的發動要件，或是以類型化的方式描述符合的風險情境[153]。而關於自動車牌辨識如何進行狹義比例原則的審查，德國聯邦憲法法院表示，考量到自動車牌辨識系統干預的對象包括不具備法律上原因的任何人，若大範圍地在公共場所秘密實施可能會使人們產生受監視的心理壓力，因此實施自動車牌辨識必須是為了保護重大或與之相當的重要公共利益，如生命、身體及自由法益，或是為維護聯邦與邦的存續與安全[154]。若是將自動車牌辨識用於追訴刑事犯罪，依照上開標準也必須至少是為了追訴重大犯罪行為（Straftaten von zumindest erheblicher Bedeutung）[155]。同時，為維護受干預個人法益與需保護公共利益之間的權衡，自動車牌辨識不允許被地毯式（flächendeckend）實施[156]。

關於如何將上述標準實際應用於審查上，可以參考 2008 年第一次車牌辨識裁判的說理。其指出系爭黑森邦《公安法》與什勒斯維希-霍爾斯坦邦《一般行政法》，因為沒有針對條文內的「追緝名單」做出明確的定義，透過其他法律規定、實務裁判或是學說見解也無法具體推知其意涵，以致於警方可以憑藉條文的模糊性，去蒐集所有他們想調查的車牌號碼與行車軌跡，資料比對的範圍也未受到限

[151] Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 96). 翻譯參考：蔡宗珍（2018），〈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 78。
[152] Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 97).
[153] Vgl. BVerfG, NJW 2019, 827, 834 (Rn. 91-94).
[154] Vgl. BVerfG, NJW 2019, 827, 834 f. (Rn. 99).
[155] Vgl. BVerfG, NJW 2019, 827, 841 (Rn. 165).
[156] Vgl. BVerfG, NJW 2019, 827, 835 (Rn. 100).

doi:10.6342/NTU202403953

制，而違反了法律明確性原則[157]。此外，系爭規定僅規範警方得蒐集車牌資料，但是在使用車牌辨識系統取得拍攝畫面並加以識別的過程中，勢必會取得其它資訊，例如駕駛人的樣貌與車內的乘客，此時，系爭條文並未針對其他資訊是否可以儲存，或者應一律刪除，亦有違反法律明確性原則的疑慮。蓋授權實施車牌辨識若只是為了立即找出特定車輛，那麼原則上就應該將可蒐集的資料範圍限定於車牌號碼、時間地點與行駛方向；然而自動車牌辨識系統的實施目的若是包含監視特定人行蹤的情形，就可能得以一併蒐集其他相關資訊。惟查系爭條文並未明確規定其資料蒐集目的，以致於可被蒐集的資料範圍也無法從條文本身推得而出[158]。德國聯邦憲法法院最後也表示，由於系爭規定對於資料蒐集與利用的目的欠缺明確性，以致於涵蓋了許多更高程度嚴重侵害基本權的情狀，包括對特定人的監視，或者是廣泛且普遍地常設性使用自動車牌辨識系統，同時，由於條文並沒有將個人資料的儲存與特定目的進行連結，而只是透過「追緝名單」的要件加以蒐集，這就有可能導致資料蒐集的原始目的雖然已經消除（例如贓車已被尋獲），警察機關仍然可以依循一些廣泛且不明確的原因，持續保留並利用該個人資料。因此，最終認定系爭規定無法通過狹義比例原則的審查[159]。

另外也必須特別注意，自動車牌辨識的授權基礎是否能夠通過狹義比例原則的審查，也和授權基礎中是否對個人資料保護提供充足的程序擔保息息相關。2018 年第二次車牌辨識裁判格外強調，關於個人資訊自決權干預的比例原則審查，整體上還需符合透明性（Transparenz）、個人權利保護（individuellen Rechtsschutz）和監督控制（aufsichtliche Kontrolle）的要求[160]。以自動車牌辨識隱密實施的性質為例，德國聯邦憲法法院說明，依照自動車牌辨識追蹤特定車輛的實施目的，允許其以隱密的方式實施是符合適當性與必要性的，且與其他高程度干預個人資訊自決權的隱密措施相比，隱密實施自動車牌辨識並不需要通知資訊自決權

157 Vgl. BVerfG, NJW 2008, 1505, 1510 (Rn. 100-102).
158 Vgl. BVerfG, NJW 2008, 1505, 1514 f. (Rn. 157-161).
159 Vgl. BVerfG, NJW 2008, 1505, 1515 f. (Rn. 170-178).
160 Vgl. BVerfG, NJW 2019, 827, 835 (Rn. 101).

doi:10.6342/NTU202403953

受干預之人，即使是經系統比對符合並將資料儲存的受干預人亦然[161]。蓋其若是能在後續程序中得知其車牌資料曾遭比對及儲存，並可向法院尋求救濟，秘密實施車牌辨識即可被認為具有衡平性[162]。至於監督控制部分，巴伐利亞邦的個資保護官可以達成這方面的要求。然而，由於 2018 年第二次車牌辨識裁判的系爭規定並未課予警察機關紀錄實施車牌辨識的義務，而應認其無法通過狹義比例原則的審查。原因在於，秘密實施基本權干預措施的過程中，受干預人無法適時監督執法人員，更無法及時尋求救濟，此時，國家機關實施自動車牌辨識是否確實留存紀錄，就變得至關重要。課予國家機關留存發動自動車牌辨識紀錄的義務有三個好處：其一，如果當局有義務說明其發動車牌辨識的原因，就會使當局自行檢視其發動是否合法；其二，相關紀錄使得數據保護官員得以介入監督，這在個人資料保護救濟方法有限的情況下更顯重要；其三，實施記錄的留存也使得法院事後可以客觀的審查其發動與執行的合法性[163]。

簡單整理德國聯邦憲法法院的上述見解：首先，由於自動車牌辨識系統依循使用情境的不同，可能只是定位特定車輛開啟後續偵查措施的工具，也可能是隱含形塑人格圖像風險的新型態監視手段，因此立法者必須先確定實施自動車牌辨識的具體目的為何，並透過此一實施目的規範資料可蒐集的對象，同時限制資料可比對的範圍，方可界定出系爭自動車牌辨識干預個人資訊自決權的程度，以此設計相對應寬嚴的發動要件。再者，考量對於不具法律上原因的一般人大規模實施自動車牌辨識，可能使其產生受監視的心理壓力，因此必須對自動車牌辨識實施的時間與空間範圍做出限制。最後，基於秘密實施使受干預人不易救濟的負面影響，透過記錄義務及監督控制機制彌補受干預人的救濟權利，並確保執行過程中符合立法者建構的法定要件。

161 Vgl. BVerfG, NJW 2019, 827, 840 (Rn. 154).
162 Vgl. BVerfG, NJW 2019, 827, 840 (Rn. 154).
163 Vgl. BVerfG, NJW 2019, 827, 840 (Rn. 156 f.).

doi:10.6342/NTU202403953

第二項　德國《刑事訴訟法》第 163g 條規定

為了符合上述德國聯邦憲法法院對於國家機關實施自動車牌辨識所提出的憲法要求，德國立法者於 2021 年 6 月 25 日以包裹立法的方式通過「刑事訴訟法繼續發展與其他規定改革法案」（das Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften），並於同年 7 月 1 日起正式生效，其中即新增了《刑事訴訟法》第 163g 條以刑事追訴為目的實施自動車牌辨識措施的授權基礎。立法者首先於草案中指出[164]：在此之前，依據《聯邦警察法》及各邦警察法的規定，國家機關得為防止危害實施自動車牌辨識[165]，或是基於其他法規的授權，將自動車牌辨識用於高速公路收費或廢氣排放管制（禁止柴油車於特定區域通行），卻尚未具備以刑事追訴為目的實施自動車牌辨識的明確授權基礎。雖然有見解認為，司法警察能夠依據德國《刑事訴訟法》第 100h 條住宅外監視錄影[166]，結合第 98c 條資料比對的規定，據以實行自動車牌辨識。然而，立法者認為這些規定並無法滿足德國聯邦憲法法院上述對於法律明確性的

---

164 Vgl. BT-Drs. 19/27654, S. 84.

165 例如：《聯邦警察法》（BPolG）第 27b 條和第 34 條、《巴伐利亞邦警察任務及職權法》（BayPAG）第 39 條、《布蘭登堡邦警察法》（BbgPolG）第 36a 條、《漢堡邦警察資料處理法》（HmbPolDVG）第 19 條、《黑森邦公共安全與秩序法》（HSOG）第 14a 條、《梅克倫堡-佛波門邦公共安全與秩序法》（SOG M-V）第 43a 條、《萊茵-法爾茲邦警察與秩序機關法》（RPflPOG）第 27b 條、《什勒斯維希-霍爾斯坦邦一般行政法》（LVwGSH）第 184 條第 5 項、《下薩克森邦警察與秩序機關法》（NPOG）第 32a 條、《柏林邦一般安全與秩序法》（ASOG Bln）第 24c 條、《圖林根自由邦警察職權法》（ThPAG）第 33 條第 7 項、《薩克森邦警察法》（SächsPDVG）第 58 條以及《巴登-符騰堡邦警察法》（PolG BW）第 22a 條。Vgl. BT-Drs. 19/27654, S. 84.

166 德國《刑事訴訟法》第 100h 條：

（1）即使受干預人不知情，若以其他方法調查犯罪事實或探查被告所在地成效不大或有困難者，得於住宅外

1. 記錄圖像，

2. 使用其他特別為監視目的所設計之科技方法。

第 1 句第 2 款之措施，僅限針對重大犯罪為之。

（2） 措施僅可對被告為之。針對其他人，

1. 第 1 項第 1 款之措施，以其他方法調查犯罪事實或探查被告所在地成效不大或顯有困難者，始得為之。

2. 第 1 項第 2 款之措施，僅在有事實認為其與被告有聯繫或將聯繫，且預期可調查犯罪事實或探查被告所在地，而以其他方法將無結果或有顯著困難時，始得命令。

（3） 措施無可避免連帶干預第三人時，亦得執行之。

（4） 第 100d 第 1 項和第 2 項之規定準用之。

翻譯參考：王士帆（2021），〈德國科技偵查規定釋義〉，《法學叢刊》，66 卷 2 期，頁 117。

doi:10.6342/NTU202403953

要求。理由在於[167]，第 100h 條僅授權偵查機關得於住宅外基於監視目的紀錄圖像，並未授權偵查機關得將所蒐集的圖像持續與廣泛的資料進行比對，然而，持續與大量資料相互比對卻正是自動車牌辨識實施的主要目的，也是其干預資訊自決權的特性所在。另外，也不能僅憑第 98c 條的規定即欲正當化自動車牌辨識的實施，蓋第 98c 條僅簡單規定：「為查明犯罪或調查因刑事程序目的被追緝之人所在地，得將出於某刑事程序之個人資料與其他為刑事追訴或刑罰執行或危險防禦所儲存之資料，進行機械化比對[168]。」並未具體規定資料得基於什麼目的在什麼樣的條件下接受比對，也沒有針對資料處理作出明確的限制，無法正當化自動車牌辨識干預資訊自決權的嚴重程度。

此外，依照德國《刑事訴訟法》第 101 條第 4 項第 7 款的規定，偵查機關依據第 100h 條實施住宅外監視錄影，必須通知「被鎖定之人與重大連帶受干預之人」[169]。因此，若是將第 100h 條適用於自動車牌辨識的情形，可能會導致所有通過自動車牌辨識系統遭比對的車輛駕駛人都必須受到通知，然而這不僅曠日廢時，在執行上也會因為資料一經比對不符即刪除而難以達成，且 2018 年第二次車牌辨識裁判也認為，若資料經比對符合而儲存的受干預人能夠在後續程序中得知其曾受自動車牌辨識，即無礙其救濟權利的行使[170]。反面推論，對於資料比對不符立即刪除的受干預人而言，通知義務就並非必要。

據此，有鑑於現行規範均無法適當地授權自動車牌辨識的行使，為了符合法律保留及明確性原則的要求，立法者決定在德國《刑事訴訟法》創設一個自動車牌辨識的獨立授權規定，並將其使用情境設定在尋找與定位已被偵查機關知悉身分的犯罪嫌疑人，或是在一定程度內，例如經由目擊證人描述或者監視錄影畫面所拍攝到的可疑嫌犯，將其用於確認此等犯罪嫌疑人的身分，而非同第 163e 條或第 163f 條一般著重於犯罪事實之偵查[171]。因此，德國《刑事訴訟法》中的自

[167] Vgl. BT-Drs. 19/27654, S. 84-85.
[168] 林鈺雄、王士帆、連孟琦（2023），《德國刑事訴訟法註釋書》，頁 153，新學林。
[169] 林鈺雄、王士帆、連孟琦，前揭註 168，頁 205。
[170] Vgl. BVerfG, NJW 2019, 827, 840 (Rn. 154).
[171] Kölbel/Neßeler, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur StPO, Bd. 2,

doi:10.6342/NTU202403953

動車牌辨識將會是一個較為限縮的授權基礎，在開始實施的階段就必須限制和確認資料得以比對與儲存的範圍，避免自動車牌辨識被偵查機關用作一種新型態的科技監視工具，同時提供個人資料保護的相關程序擔保，方能達成聯邦憲法法院上述的要求，據以通過狹義比例原則的審查。

德國《刑事訴訟法》第 163g 條全文規定如下[172]：

(1)1 若存在足夠之事實依據表明發生重大犯罪行為，且可合理認定，處分有助於辨識嫌疑人身分或其所在地，得在受干預人不知情下，於限定地點之公共交通場所，藉由科技方法自動蒐集車牌資料以及地點、時間及行駛方向。2 自動化資料蒐集僅得暫時性且不得地毯式實施。

(2) 1 依第 1 項蒐集之車牌資料得與下列車牌資料進行自動化比對：

1. 核發給被告或由被告使用，或

2. 核發給被告以外之人或由該人使用，當根據一定事實可認為該人與被告有聯繫或將建立此種聯繫，而且調查被告所在地採用其他方式成功希望渺茫或非常困難時。

2 自動化比對應在第 1 項自動蒐集資料後儘速為之。3 當有比對結果符合時，應儘速以手動方式檢查依第 1 項蒐集之車牌資料以及在第 1 句所稱之其他特徵是否相符。4 當比對結果不符或經手動檢查確認比對結果不符時，第 1 項所蒐集之資料應立即且不留痕跡地刪除。

(3)1 第 1 項及第 2 項之處分命令由檢察官以書面為之。2 命令應說明處分之要件存在並詳細記載應當與第 2 項第 1 句自動化蒐集之車牌資料進行比對之特徵。3 命令應記載實施之公共交通場所（第 1 項第 1 句）之限定地點，且命令應定期間。4 遲延即有危險時，命令亦得以口頭且由檢察機關之偵查人員(《法院組織法》第 152 條）為之；於此情形應於三日內向命令者取得第 2 句及第 3 句所要求之書面記載。

2024, § 163g Rn. 6.

172 參考：連孟琦，前揭註 135，頁 99。

doi:10.6342/NTU202403953

(4) 當處分要件已不存在或已達成處分目的時，應儘速終結處分。

第一款　資料蒐集的範圍與要件

首先，由於 2018 年第二次車牌辨識裁判指出，若要將自動車牌辨識用於刑事追訴，則必須是偵查重大犯罪的情形方可通過比例原則的審查[173]。有基於此，立法者在此處便規定自動車牌辨識的行使必須「存在足夠之事實依據表明發生重大犯罪行為」，於此毫無疑問地引用了德國《刑事訴訟法》第 152 條第 2 項「開始嫌疑」（Anfangsverdacht）之門檻，亦即須依據事實證據顯示可能發生了可追訴之重大犯罪，而非單純臆測[174]。不過，考量依第 163g 條實施的自動車牌辨識系統僅可儲存比對符合之資料，比對不符合的資料必須立即刪除，立法者認為此處的干預程度並不需要透過明確列舉的重罪目錄來正當化自動車牌辨識的行使，而是可以經由司法實務上針對德國《刑事訴訟法》第 81g 條第 1 項第 1 句、第 98a 條第 1 項和第 100h 條第 1 項第 2 句等規定所發展出的標準，將重大犯罪理解為「中度犯罪以上之罪，亦即使人感覺法和平性被擾亂，或者顯著影響國民對於法安定性的感受」[175]。於此，德國《刑法》第 12 條所定義之「重罪」（Verbrechen）與「輕罪」（Vergehen），是否即為此處「重大犯罪」之區別標準，即有疑義。對此，所稱「重罪」，亦即「最輕本刑一年或一年以上有期徒刑之罪」，自然屬此處所稱之重大犯罪[176]。至於最輕本刑為未滿一年之有期徒刑或罰金之「輕罪」[177]，則並非必定不屬於此處之重大犯罪。學說有見解認為仍應以其最重本刑是否為二年以上有期徒刑作為判斷標準[178]；另有見解主張應以系爭案件之宣判刑是否可預

173 Vgl. BVerfG, NJW 2019, 827, 841 (Rn. 165).
174 參考：林鈺雄（2023），《刑事訴訟法（下冊）》，12 版，頁 84，自版。Vgl. Roggan, Der Einsatz von Automatischen Kennzeichenlesesystemen (AKLS) zu Fahndungszwecken, NStZ 2022, 19, 19.
175 Vgl. BT-Drs. 19/27654, S. 86; Köhler, in: Meyer-Goßner/Schmitt (Hrsg.), Strafprozessordnung, 65. Aufl., 2022, § 163g Rn. 2. 中文翻譯，參考：連孟琦，前揭註 135，頁 99-100；王士帆，前揭註 166，頁 119。
176 林鈺雄、王士帆、連孟琦，前揭註 168，頁 199。
177 翻譯參考：何賴傑、林鈺雄（審譯）（2019），《德國刑法典》，2 版，頁 25，元照。
178 Köhler, a.a.O. (Fn. 175), § 98a Rn. 5.

doi:10.6342/NTU202403953

期為不可緩刑之刑度，也就是「一年以上有期徒刑」而定[179]，惟其同時也強調此種事前預測有其難處，尤其是偵查初期，故有關要件存否之認定，應依事前觀點而定，縱使裁判後宣告刑遠低於一年有期徒刑之標準，亦不可據此逕認該次自動車牌辨識之實施違法[180]。

而為了滿足法律明確性的誡命，立法者也清楚規定自動車牌辨識的實施僅可基於辨識嫌疑人身分或所在地的目的，達到以明確的資料蒐集目的劃定資料蒐集與比對範圍的功能。據此，第 163g 條將資料蒐集的範圍限定在「車牌資料、地點、時間以及行駛方向」，「車牌資料」除了一般車輛的車牌之外，於解釋上也包括外國車牌、已作廢車牌（entwertete Kennzeichen）以及僅用於保險目的之車牌號碼（Versicherungskennzeichen）[181]。除了這些資料以外，若是將自動車牌辨識系統用於識別車內的乘客人數、甚至是使用人臉辨識技術識別車內特定人的身分，都無法涵蓋在本條的授權範圍內。可以想見，這將會導致自動車牌辨識系統無法將特定車輛的行車軌跡直接地連結至特定人，畢竟車輛使用人並不會總是車輛的所有人，甚至還需考慮租用車輛的情形[182]。不過，關於車輛使用人的資訊，多數情況下均可於後續調查程序中得知，排除透過自動車牌辨識系統直接蒐集車內乘客資訊的可能性，可以降低個人資料之間相互連結的便捷性，據以有效限制系爭措施的干預程度，本文予以肯定。

此外，資料蒐集的地點必須是公共交通場所，不包括不特定多數人得以自由出入的私人空間，適用範圍較第 111 條公眾得出入地點設置檢查哨的規定來得窄[183]，可以預見實際運用上大多會設置於高速公路或主要幹道（Fernstraße）之上[184]，且不限於傳統的固定式車牌辨識系統。蓋立法者原先的條文用語為：「於公共交通處所的特定位置」（bestimmten Stellen im öffentlichen Verkehrsraum），隨後考量「移

[179] 德國《刑法》第 56 條。
[180] Vgl. Roggan, (Fn. 174), S. 19-20.
[181] Vgl. Roggan, (Fn. 174), S. 20.
[182] Vgl. Roggan, (Fn. 174), S. 20.
[183] Vgl. BT-Drs. 19/27654, S. 87; Vgl. Köhler, a.a.O. (Fn. 175), § 163g Rn. 3.
[184] Vgl. BT-Drs. 19/27654, S. 87.

doi:10.6342/NTU202403953

動式車牌辨識」的必要性，而將「特定位置」的要件移除，因此第 163g 條涵蓋了「固定式」及「移動式」的車牌辨識系統的授權[185]。同時，條文也明確規定允許偵查機關在當事人不知情的狀況下，秘密地實施自動車牌辨識。

另一方面，第 163g 條第 1 項第 2 句對於自動車牌辨識的實施設下了「暫時性」以及「非地毯式（nicht flächendeckend）」的限制。關於此處禁止地毯式實施的規定，同樣是來自於 2018 年第二次車牌辨識裁判的論述及系爭警察法規定[186]，立法者於此原封不動地引用為法條文字。對此，學說見解認為，第 163g 條雖然授權偵查機關得使用「移動式」車牌辨識系統，在施行上卻必須特別注意德國聯邦憲法法院所劃下的界限，亦即應禁止「地毯式」或者「全面覆蓋式」地施行，而僅在局部範圍內（punktuell）個別可預期得以成功達成目的之地點（einzelne erfolgversprechende Stelle）實施[187]。有鑑於此，這個要件事實上排除了偵查機關在所有警用車輛上裝設移動式車牌辨識系統以偵查特定案件的可能性，同時，若將固定式車牌辨識系統全面架設於公共交通場所的所有路段，也不合於憲法要求[188]。不過，「非地毯式」的要件雖然看似能夠限制自動車牌辨識系統的干預程度，卻也引來了不少批評。原因在於，雖然立法者期待在個案中能夠依照所涉犯罪的嚴重程度，分別設定時間與地區範圍的限制，據以符合比例原則的要求，卻會因為「地毯式實施」在文義上只能解釋為「完全涵蓋特定區域」，而無法說明何謂「特定區域」。因此，若是將特定區域理解得非常廣闊，例如一整座城市，那麼偵查機關實際的干預措施無論如何都不會「完全涵蓋」特定區域，進而致使這個要件難以發揮限縮系爭措施的干預程度，藉以使系爭規定通過比例原則審查的功能[189]。即使立法草案中表示，透過「可合理認定有助於辨識嫌疑人身分或其所在地」的

[185] Vgl. Höltkemeier, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafprozessordnung mit GVG und EMRK, 5. Aufl., 2022, § 163g Rn. 11 f.
[186] Vgl. BVerfG, NJW 2019, 827, 835 (Rn. 100). 德國聯邦憲法法院於審查巴伐利亞邦警察法的規定時，認為「非地毯式」的要件有助於限縮自動車牌辨識的實施地點，且可透過「有助於達成目的之要件」加以理解，因此符合法律明確性的要求。
[187] Vgl. BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 115.
[188] Vgl. Roggan, (Fn. 174) S. 20.
[189] Vgl. Roggan, (Fn. 174) S. 20.

doi:10.6342/NTU202403953

要件（zweckgebundenen Erfolgsaussicht），即可有效地將自動車牌辨識系統的設置地點限縮在以事前觀點可預期犯罪嫌疑人或與其聯繫之第三人會出沒的地方，排除恣意（ins Blaue hinein）地毯式實施自動車牌辨識的可能[190]。然而學說指出，這種有助於達成目的的要件事實上仍無法達成限制空間上實施密度的效果。以追查特定犯罪嫌疑人行蹤之目的為例，基本上城市中的各個角落在此種觀點下都有助於達成目的，而得以「正當」實施車牌辨識，因此，「非地毯式」的要件實際上有違反法律明確性之虞[191]。

而關於時間上的限制，法條僅規定自動車牌辨識的實施必須是「暫時性的」（vorübergehend），卻同樣並未做出其他說明，這會導致干預措施的實施期間可能長達幾個月，甚至是數年。對此，立法者認為自動車牌辨識的實施本就會因為目的達成而產生終止義務，授權基礎的設計上無須賦予其明確的最長期限[192]。學說上則有認為自動車牌辨識的時間與空間限制，必須視其發動的目的而定，一般情況下自動車牌辨識的實施期間只能限於幾天之內，但是在特別嚴重犯罪的偵查情形，例如 1977 年的劫機事件，或是 2016 年柏林聖誕市集卡車衝撞事件，若遲遲無法發現被告行蹤，縱使在全國的主要幹道連續一個月實施自動車牌辨識，仍然合乎比例原則[193]。

第二款　資料比對範圍與程序

依據第 163g 條第 1 項蒐集到的車牌辨識資料，其得以比對的車牌資料範圍僅限於登記為被告所有或由被告所使用的車輛，或者是與被告有聯繫或正在建立聯繫的第三人，其所登記或使用的車輛，且必須有足夠事實依據證明該車輛是由被告所使用，或第三人確實與被告有某種聯繫，方可予以比對，據以正當化資料

[190] Vgl. BT-Drs. 19/27654, S. 87.
[191] Vgl. Roggan, (Fn. 174) S. 20; Zaremba, Die neue Befugnis zum Einsatz automatischer Kennzeichenlesesysteme – Teil 2, SVR 2022, 209, 212.
[192] Vgl. BT-Drs. 19/27654, S. 88.
[193] Moldenhauer, in: Barthe/Gericke (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl., 2023, § 163g Rn. 8.

doi:10.6342/NTU202403953

比對及儲存所造成的資訊自決權干預[194]。與登記為被告所有或由被告所使用的車輛之車牌號碼相互比對時，不同於與第三人車輛比對，並不限於「採用其他方式可能成功希望渺茫或非常困難」的情形，有學者認為這是因為立法者已經透過重大犯罪的開始嫌疑以及時間地點限制等要件來達成比例原則的要求[195]。而在比對程序上，與目標車牌號碼的比對必須在車牌辨識資料蒐集後立即進行，若是經由車牌辨識系統比對後顯示比對結果符合（Treffer），則必須立即人工手動確認是否屬於確實符合的情形，以此排除基於技術原因所不可避免的偽比對符合情形（unechter Trefferfall）。同時，為了盡可能地降低自動車牌辨識干預資訊自決權的程度，在比對結果不符合以及偽比對符合的情形，就必須立刻且不留痕跡地刪除原先所蒐集的車牌辨識資料。

第三款　發動程序

由於德國聯邦憲法法院在兩次車牌辨識裁判中均未指出相關授權基礎必須具備法官保留的要件方可通過比例原則的審查，立法者據此認為在此種比對不符合立即刪除資料的自動車牌辨識授權中，法官保留程序並非必要[196]，並將第 163g 條規定設計為「檢察官保留」。亦即，自動車牌辨識處分的命令原則上由檢察官以書面為之，命令中必須記載：「重大犯罪的開始嫌疑」、「是否有事實足認該措施能夠達成確認被告身分或行蹤的目的」、「將會予以比對的車牌號碼（包含被告和與被告聯繫的第三人）與其符合第 2 項要件的事證」以及「實施車牌辨識時間和地點的限制」，透過詳實的書面記載達成 2018 年第二次車牌辨識裁判中對於記錄義務的要求，而不可僅是泛泛指稱相關路段的普遍重要性，給予千篇一律且同公式般的說明[197]。儘管如此，學說上仍有認為若是依照德國聯邦憲法法院過去的

194 Vgl. Höltkemeier, a.a.O. (Fn. 185), § 163g Rn. 15 f.
195 Vgl. Höltkemeier, a.a.O. (Fn. 185), § 163g Rn. 6; Moldenhauer, a.a.O. (Fn. 193), § 163g Rn. 6.
196 Vgl. BT-Drs. 19/27654, S. 85.
197 Vgl. Roggan, (Fn. 174) S. 22.

doi:10.6342/NTU202403953

裁判，此等秘密實施且嚴重干預基本權的措施，應採取法官保留原則[198]。另外，第 163g 條同時也規定，在情況急迫、遲延即有危險時，實施自動車牌辨識的命令亦得由《法院組織法》第 152 條意義下檢察機關之偵查人員發布。這通常是適用在犯罪發生後不久，僅知悉與犯罪相關車輛的車牌號碼而仍無法得知犯罪嫌疑人身分的情形[199]，此時是否能夠順利追訴犯罪往往取決於相關偵查措施何時能開始協助調查，因此立法者賦予一線偵查人員此種口頭發布命令的權限，並規定其必須在 3 日內完成書面命令且詳細記載上述事項，以確保此次自動車牌辨識的施行亦符合法定要件。然而，學說則有見解認為，在各邦檢察機關 24 小時都有檢察官待命的背景下，即使情況急迫，偵查人員仍然必須先嘗試聯繫檢察官，並由檢察官發布口頭命令[200]。

第四款　終結處分與資料刪除

第 163g 條第 4 項明確規定當處分要件已不存在或已達成處分目的時，應儘速終結處分。處分要件已不存在的情形，可能是在後續偵查的過程中，重大犯罪的開始懷疑已不復存在，或者是基於其他線索，例如得知被告本人已經逃亡到國外，而認自動車牌辨識已經無法達成確認被告身分或行蹤的目的。至於處分目的已達成則是已確認被告之身分或行蹤，自不待言。此際依照本條項規定，就必須立即終止車牌辨識的實施。值得注意的是，對於因車牌比對結果符合而儲存的「車牌資料、地點、時間及行駛方向」，若不再需要用於刑事追訴或是可能發生的司法審查時，就必須依照德國《刑事訴訟法》第 101 條第 8 項立即刪除。其具體規定為：「若經由處分所獲得之個人資料，不再為刑事追訴以及可能發生之法院審

198 Gilga, Automatisierte Kennzeichenerfassung in der Strafverfolgung – aktueller Regierungsentwurf, ZD-Aktuell 2021, 05041. 德國聯邦律師協會也表示應有適用法官保留之必要。Vgl. Bundesrechtsanwaltskammer (2021), Stellungnahme Nr. 68/2020 November 2020 - Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften, in https://www.bundestag.de/resource/blob/833398/fd6533787284e438ecf88284d547f94b/stellungnahme-knauer_brak.pdf（最後瀏覽日：04/25/2024）

199 Vgl. Höltkemeier, a.a.O. (Fn. 185), § 163g Rn. 17; BT-Drs. 19/27654, S. 88.

200 Claus, Fahndung mittels automatischer Kennzeichenlesesysteme, jurisPR-StrafR 3/2022 Anm. 1.

doi:10.6342/NTU202403953

查處分所需要，應儘速刪除。刪除應記入案卷。當僅為可能發生之法院審查處分而暫緩刪除時，在未經受干預人同意時，資料僅得為此目的而使用；資料之處理應做相應限制[201]。」另一方面，如果要將實施自動車牌辨識所蒐集到的資料，用於其他刑事案件的偵查，則根據第 161 條第 3 項、第 479 條第 2 項第 1 句，必須符合「假設替代流程」（hypothetischer Ersatzeingriff），亦即另案的偵查情境也足以正當化自動車牌辨識實施，始可為之。又，若欲將已取得的資料用於防止危害的目的，則必須符合第 479 條第 2 項第 2 句的要件[202]。

第五款　通知義務與救濟

如前所述，避免適用第 100h 條第 1 項所產生依據第 101 條第 4 項第 7 款必須通知重大連帶受干預之人的義務，也是本次修法新增第 163g 條的緣由之一。因此，第 101 條第 4 項第 13 款針對第 163g 條所課予的通知義務，其「目標人物」（Zielperson）在解釋上就僅及於在檢察官的書面命令或偵查人員的口頭命令中，持續受比對的車牌號碼擁有者，而不包括經車牌辨識系統蒐集與比對後，因比對結果不符合或者是偽比對符合而立即將其資料刪除的受干預人[203]。通知內容包括第 101 條第 7 項的事後權利保護之可能性與救濟期間，亦即，受干預人得自收到通知時起 2 週內，向管轄法院聲請審查干預措施及其執行種類和方式的合法性。若本案已經檢察官提起公訴且被告亦獲通知，則應由本案審理法院於終結程序的裁判中對於違法實施干預措施的聲請作出決定[204]。不過，2018 年第二次車牌辨識裁判中明確肯認遭自動車牌辨識系統蒐集資料之行經車輛，縱使資料經自動化比對結果不符而立即刪除，仍構成個人資訊自決權之干預，立法者於此卻免去了通知此等受干預人之義務，是否亦同時排除其向法院提起救濟的權利？即有疑義。對此，學說見解指出，接受通知並非司法救濟的必要條件，資料比對結果

[201] 連孟琦，前揭註 135，頁 101。
[202] Vgl. Höltkemeier, a.a.O. (Fn. 185), § 163g Rn. 21.
[203] Vgl. Roggan, (Fn. 174) S. 22.
[204] 林鈺雄、王士帆、連孟琦，前揭註 168，頁 206。

doi:10.6342/NTU202403953

不符而未獲通知之受干預人，倘若基於其他原因得知自動車牌辨識實施之情事，而認此次實施存在時間或地點之限制上不符合比例原則等違法之虞，仍然得向法院提起救濟[205]。

另一方面，考量隱密干預措施的實施目的以及案件所涉人員的安危，德國《刑事訴訟法》亦設有延遲通知的規定。例如依照第 101 條第 4 項第 3 句，若是通知與受干預人優勢值得保護的利益相互牴觸，則無須通知受干預人。又依第 101 條第 5 項規定，在通知不會危及本案的調查目的、所涉人員的生命、身體之不可侵犯性、人身自由以及重要的財產價值時，即應通知[206]。反面言之，在涉及上述重要利益時，通知義務即可被暫緩。受暫緩的通知若是延遲時間達 12 個月，則需法院同意方可繼續延緩，若在緊密的時間內有數次干預措施的執行，則以最後措施結束的時間點起算（第 101 條第 6 項）。

[205] Vgl. Roggan, (Fn. 174) S. 22; Köhler, a.a.O. (Fn. 175), § 101 Rn. 25.
[206] 林鈺雄、王士帆、連孟琦，前揭註 168，頁 206。

doi:10.6342/NTU202403953

第三章 預防性儲備車牌辨識資料之正當性

經由上一章的介紹可以得知，德國刑事訴訟法及警察法僅授權警察機關以「追緝模式」實施自動車牌辨識，亦即自動車牌辨識系統在識別車牌號碼後必須立即與名單內的資料相互比對，並且在比對不符合及偽比對符合的情形立刻不留痕跡地刪除一開始所取得的車牌辨識資料，以此將後續因長時間儲存資料所可能產生資料遭濫用與竊取的風險，控制在具有違反法律規定甚至是犯罪嫌疑的特定人身上，據以排除對於不具犯罪嫌疑之一般人構成相對嚴重之資訊自決權干預的情形。然而，此種「追緝模式」某程度上也大幅限制了偵查成效。原因在於，倘若犯罪發生後短時間內無法透過證人的陳述或是監視錄影畫面取得可疑車輛的車牌號碼，例如行為人趁四下無人侵入住居竊盜、被害人死亡後陳屍多日方被人察覺，又或者是擄人勒贖案發生後無法得知嫌疑車輛的車牌號碼，這些情形下偵查機關既無從透過自動車牌辨識系統即時比對並掌握犯罪嫌疑人之行蹤，也無法調閱幾天前的車牌辨識紀錄追查線索，更遑論逕自將現有的車牌辨識資料先行儲存後供日後查緝所用。不同於此，參考我國自動車牌辨識系統的實施流程即可發現，我國警察機關是透過自動車牌辨識系統將所有行經車輛的車牌號碼、通過時間、地點、行徑方向，甚至是駕駛人和行人的衣著打扮，全都一網打盡，亦即在不區分對象是否違反法律規定或是具備犯罪嫌疑的前提下，一律預防性地儲備自動車牌辨識系統所取得的影像檔以及經過量化的資料，待日後產生偵查需求時再予以調取[207]。

針對不具犯罪嫌疑之一般人所實施的干預措施，通常會被認為是一種對於個人基本權較高程度的干預，例如我國《刑事訴訟法》中搜索以及身體檢查處分之授權規定，依受干預人為被告或不具犯罪嫌疑之一般人（第三人）即設有寬嚴不同的發動要件。對此，學說有見解認為，雖然在偵查程序中尚未完全肯定被告確

[207] 有學者指出，伴隨大量資訊蒐集權限立法，現代警察法制逐漸從具體的危害防止，轉向潛在性、推測性的危險預防。參考：林明鏘（2010），〈由防止危害到危險預防：由德國警察任務與權限之嬗變檢討我國之警察法制〉，《國立臺灣大學法學論叢》，39 卷 4 期，頁 175-179。

doi:10.6342/NTU202403953

實為犯罪行為人，但是依循其犯罪嫌疑的高低仍然在一定程度上存在其為國家刑罰權行使對象之可能，此際基於發現真實的公共利益，透過比例原則權衡干預措施所損害及維護的利益後，即可使被告在必要情形負有忍受刑事程序進行的義務（Duldungspflicht）[208]；反之，不具犯罪嫌疑的一般人（第三人）因為尚不存在成為犯罪行為人的可能，並非國家刑罰權行使的對象，在比例原則的觀點下，對其所實施的基本權干預措施就必須適用較高的發動門檻[209]。

相對於此，德國聯邦憲法法院於兩次車牌辨識裁判中則從另一個面向觀察並提出論述。首先，於 2008 年第一次車牌辨識裁判中，由於尚不認為「資料比對不符合且立即刪除的情形」構成個人資訊自決權的干預，為了強調「追緝模式」下自動車牌辨識系統僅會儲存比對結果符合者之行車資料，其闡述自動車牌辨識系統的干預程度時曾特別指出：「倘若大量不具犯罪嫌疑的一般人被納入系爭干預措施的實施範圍之下，就可能會產生一種『恫嚇效果』，進而損害人民基本權利的行使，若因而導致系爭干預措施被濫用的風險，並形塑人民時時受到監視的心理壓力，該措施的公正性就會備受質疑[210]。」其後，2018 年第二次車牌辨識裁判轉而承認「追緝模式」下對於資料比對不符合者亦構成干預的同時，也肯認了自動車牌辨識措施事實上將所有車輛駕駛人均納入實施範圍之下，並進一步表示：

---

208 Stein, Die Ungleichbelastung von Beschuldigten und Nichtbeschuldigten durch strafprozessuale Eingriffsermächtigungen, in: Samson/Dencker/Frisch/Frister/Reiß (Hrsg.), Festschrift für Gerald Grünewald zum siebzigsten Geburtstag, 1999, S. 690 ff.

209 林鈺雄（2004），〈從基本權體系論身體檢查處分〉，《國立臺灣大學法學論叢》，33 卷 3 期，頁 183-184；林鈺雄（2023），《刑事訴訟法（上冊）》，12 版，頁 435，自版。學說上另有見解認為，之所以能以犯罪嫌疑的有無，區別被告與第三人干預措施之發動要件，其原因在於：刑事訴訟法上之基本權干預措施達成保全證據或程序目的之預期效益，會因為犯罪嫌疑的有無而產生差異。例如，基於經驗法則而認為在被告處所發現被告本人或證據的可能性較高，反之存在於第三人處所的可能性則較低，因二者達成搜索目的之預期效益不同而導致後者必須適用較為嚴格的發動要件。參考：薛智仁（2017），〈羈押事由之憲法界限〉，《國立臺灣大學法學論叢》，46 卷 4 期，頁 1924；薛智仁（2021），〈第三人搜索之另案扣押——最高法院 110 年度台上字第 1979 號刑事判決〉，《台灣法律人》，2 期，頁 193-194。本文認為此見解欲擺脫「忍受義務」可能有違無罪推定原則的隱憂，確屬獨到，然而實務上亦曾出現被告仰賴律師事務所不易遭搜索的性質，而將相關證據置放於律師事務所的案例，是否可以僅憑日常經驗，逕認證據存放於第三人處所的可能性較低而應適用較嚴格的要件，似乎仍有討論餘地。此外，本文所要處理的預防性車牌辨識資料儲備，並未區分受干預人是否具備犯罪嫌疑，一律儲存其車牌辨識資料，而與第三人搜索於發動措施之際即基於有無犯罪嫌疑而對應寬嚴之要件，情形有所不同。因此本文在此不欲繼續探討「忍受義務」的論理是否正當。

210 Vgl. BVerfG, NJW 2008, 1505, 1507 f. (Rn. 78).

doi:10.6342/NTU202403953

「加深自動車牌辨識措施干預程度的原因在於，系爭措施的干預對象並非僅限於客觀上陷於危險情境（in einer Gefahrenlage）之人，反而涵蓋了一開始根本不具備法律上原因的不特定多數人。事實上，任何人都有可能成為系爭措施的干預對象，這種資料蒐集措施原則上會被認為是較嚴重的干預。另外，系爭措施隱密實施的性質，同樣也加深了其干預程度。這可能會使人民產生一種受到監視的感覺，特別是干預措施實施範圍寬廣的情形，正如本案中基於追緝目的而在公共場所連續檢查大量人民。縱使於資料比對結果不符合的情形，受干預人並不會意識到其曾遭受自動車牌辨識，仍然不能以此否認其干預程度。因為這僅僅排除了資料比對符合時可能對受干預人帶來的後續不便，卻並未消除系爭措施的控制性質（Kontrollcharakter）以及其對於個人自由的固有損害，同時更整體地影響了『社會自由』（Freiheitlichkeit der Gesellschaft）[211]。」

早在 1983 年人口普查案的裁判中，德國聯邦憲法法院就已觀察到個人資料自主控制對於人民自由發展其人格的重要性，甚至會影響人民一般行為自由、集會結社自由等基本權的行使，方提出個人資訊自決權的保障。例如其曾闡述：「人民如果無法確定自己可能的脫序行為（abweichende Verhaltensweise）是否會在任何時候被記錄，並且以資料的形式被長期地儲存、利用或者進一步傳輸，便會試著避免從事這些行為引發關注。例如，如果人民擔心自己參與集會遊行或異議活動，可能會遭受政府記錄並使自身暴露於風險之中，就可能會放棄行使憲法上所保障的基本權利（《基本法》第 8 條、第 9 條之集會結社自由）。這不只會損害人民自由發展的機會，同時也損及了公共利益。因為自主決定自由（Selbstbestimmung）是一個立基於人民行為能力與參與能力所建構之自由民主共同體的核心運作條件[212]。」而於上述裁判中，德國聯邦憲法法院則指出自動車牌辨識系統之干預對象不以具備法律上原因者為限，事實上可能將所有車輛駕駛

[211] Vgl. BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 98.
[212] Vgl. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 146. 翻譯參考：程明修（2023），〈基本權釋義學之挑戰——疊加之基本權干預〉，《公法研究》，7 期，頁 39。

doi:10.6342/NTU202403953

人納入干預措施的實施範圍，致使其對於一般人民基本權利之自由行使產生了「恫嚇效果」，輔以其隱密實施的性質，加深了人民受到監視的感受，而不只對個人自由造成損害，同時更整體地影響了「社會自由」。

這種於基本權干預程度的判斷上，納入「整體社會自由」的觀點，學說有見解稱之為「水平疊加之基本權干預」（die horizontale Eingriffsaddition），認為「如果同一基本權利之複數基本權主體同時受到具有干預性質之同一措施影響時，那麼該基本權利所保護之（整體，gesamt）社會價值實現就會受到威脅[213]。」同時，學說見解也主張涉及水平疊加之基本權干預措施在比例原則的審查過程中，在系爭措施的「必要性」上應特別注意是否存在得以限制系爭措施之實施範圍，減少干預其他基本權主體而在總體上降低負擔（insgesamt weniger belastungsintensiv），卻同等有效的手段；而於「衡平性」的審查上，除了系爭措施對個人所造成的負擔外，也須一併考量該基本權保護之社會價值所受到的威脅[214]。

2018 年第二次車牌辨識裁判雖然並未使用「水平疊加之基本權干預」的用語，卻明顯考量到自動車牌辨識系統所干預的對象包括不具備法律上原因的任何人，若大範圍地在公共場所秘密實施可能會使人們產生受監視的心理壓力，因此將自動車牌辨識的實施限於為保護重大或與之相當的重要公共利益，如生命、身體及自由法益，或是為維護聯邦與邦的存續與安全[215]，因此用於追訴刑事犯罪之目的就必須是為追訴「重大犯罪行為」[216]，同時，為了維護受干預個人法益與需保護公共利益之間的權衡，更明確禁止地毯式實施自動車牌辨識[217]。德國《刑事訴訟法》第 163g 條之「追緝模式」尚且立即刪除比對不符合者之資料，不同於此，我國警方並未區分受干預人是否具有犯罪嫌疑，一律預防性儲備車牌辨識資料的作法，伴隨個人的行車軌跡被秘密地以資料的形式長期儲備於警用資料庫內，

[213] Vgl. Brade, Die horizontale Eingriffsaddition, DÖV 2019, S. 852, 852f. 中文文獻可參考：程明修，前揭註 212，頁 19-20、44-45。
[214] Vgl. Brade, (Fn. 213), S. 858. 程明修，前揭註 212，頁 43-44。
[215] Vgl. BVerfG, NJW 2019, 827, 834 f. (Rn. 99).
[216] Vgl. BVerfG, NJW 2019, 827, 841 (Rn. 165).
[217] Vgl. BVerfG, NJW 2019, 827, 835 (Rn. 100).

doi:10.6342/NTU202403953

隨時供國家機關調取、利用，甚至必須承受資料遭非法竊取的風險，自動車牌辨識系統對於人民之恫嚇效果在此有了顯著的提升，而隱含嚴重影響人民自由行使其基本權利之風險。

有鑑於此，針對我國預防性儲備車牌辨識資料的實施方式，本文以下欲探討其是否具「必要性」，又或者事實上存在其他侵害程度較小且同等有效的手段。其中，德國《刑事訴訟法》第 163g 條立法過程中曾多次討論的「追緝模式」、「儲存模式」以及「記錄模式」，就成為很好的考察對象。不過，假使常態地預防性儲備車牌辨識資料真有其必要性，或者因為立法者具有廣泛評估與預測的形成自由而通過必要性審查[218]，下一個問題則是：此種不以干預對象具有法律上原因為限，事實上可能將所有人納入干預範圍的措施，其對於人民所造成的恫嚇效果，以及對整體社會自由的威脅，應如何於衡平性審查中評價？其干預授權基礎又應如何設計，方得具備干預資訊隱私權（資訊自決權）之正當性？

對此，可惜的是，提出「水平疊加之基本權干預」觀點的學者尚無法完整地說明。然而，本文考量歐盟法上有關「預防性通信紀錄儲備」的爭議，亦存在此種因預防性資料儲備而對人民基本權利之自由行使產生恫嚇效果的影響，決定透過爬梳德國聯邦憲法法院與歐盟法院的相關裁判，整理出預防性資料儲備措施於比例原則的審查過程中應特別關注的事項，以及其干預授權基礎的設計上必須具備的實質要件。期待能藉以探究我國預防性儲備車牌辨識資料，待嗣後產生偵查需要再予以調取的實施模式，是否以及如何設計其干預授權基礎方能具備憲法上之正當性。

第一節　德國法關於預防性儲備車牌辨識資料的討論

第一項　警方並未確實刪除車牌辨識資料所引發的爭議

在 2018 年第二次車牌辨識裁判公布後不久發生了一起值得討論的案例。15

[218] Vgl. Brade, (Fn. 213), S. 858. 程明修，前揭註 212，頁 43。

doi:10.6342/NTU202403953

歲的少女 Rebecca 在 2019 年 2 月 18 日離奇失蹤後引發社會關注，偵查過程中，檢察官及 Rebecca 的家人向媒體透露曾於 2 月 18 日和 19 日在柏林與奧得河畔法蘭克福之間的高速公路上，憑藉自動車牌辨識系統取得可疑目標車輛兩次的辨識紀錄，此舉間接承認了實務上實施自動車牌辨識系統的方式，除了警察法上所謂一經比對不符合立即刪除相關資料的「追緝模式」（Fahndungsmodus）之外，另外還包括在取得法院裁定許可後，開始在一定的空間範圍內，將所有行經自動車牌辨識系統車輛的車牌號碼、通過時間、地點、行駛方向以及自車輛後方所拍攝的影像一律預防性儲存的「儲存模式」（Aufzeichnungsmodus）[219]，以利警方在後續偵查的過程中調閱所需資訊。

布蘭登堡邦資料保護與文件檢查權利官（Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht，LDA Brandenburg）進一步調查發現，布蘭登堡邦的警察機關為了偵查某起重大組織犯罪，於 2017 年 9 月取得法院裁定許可後，連同檢察官所發布的命令，開始持續延長「儲存模式」的施行，不斷透過自動車牌辨識系統蒐集車輛駕駛人的行車資訊，截至少女失蹤案發生的時點，期間已長達 19 個月，由於「儲存模式」的資料儲存對象不以處於追緝名單上且比對符合者為限，而是一律預防性儲備所有行經車輛的資料，又正好儲存到本案所需要的車牌辨識資料，遂應柏林警方的請求予以傳輸[220]。

[219] Zaremba, Die neue Befugnis zum Einsatz automatischer Kennzeichenlesesysteme – Teil 1, SVR 2022, 168, 168; Arzt/Müller/Schwabenbauer, Informationsverarbeitung im Polizei- und Strafverfahrensrecht, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl., 2021, Rn. 1166-1169; FOCUS online (2019), Fall Rebecca enthüllt breiten Einsatz von KESY – doch System ist hoch umstritten, in: https://www.focus.de/panorama/welt/kennzeichenerfassung-fall-rebecca-enthuellt-breiten-einsatz-von-kesy-doch-system-ist-hoch-umstritten_id_10425614.html. （最後瀏覽日：04/10/2024）; Stern (2019), Kennzeichenfahndung Kesy im Fall Rebecca – darum ist die Polizei jetzt "stinksauer", in: https://www.stern.de/auto/news/rebecca-reusch--aerger-um-kennzeichenfahndung-kesy-8613232.html. （最後瀏覽日：04/10/2024）

[220] Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht (2020), Tätigkeitsbericht Datenschutz 2019, S.101-102, in: https://www.lda.brandenburg.de/lda/de/service/informationsmaterial/details/~24-03-2020-taetigkeitsbericht-datenschutz-2019. （最後瀏覽日：06/24/2024）

doi:10.6342/NTU202403953

第一款　案例事實

公民 A 在報紙上讀到相關消息後，驚覺警察機關在自己平時行駛的 11 號公路上也曾以所謂的「儲存模式」實施自動車牌辨識系統，將自己的行車資訊一併儲存，公民 A 因此向法院提起救濟，主張依據德國聯邦憲法法院 2018 年第二次車牌辨識裁判，縱使是在資料比對後因不符合而立即刪除，仍然構成個人資訊自決權的干預，而此種儲存模式下並未區分受干預人是否具備犯罪嫌疑，將所有用路人的資訊一律儲存，顯然是一種對於個人資訊自決權更為嚴重的干預，偵查機關若欲以德國《刑事訴訟法》第 100h 條作為干預授權基礎，明顯已違反法律保留與明確性原則。另外，縱使第 100h 條可作為自動車牌辨識系統「儲存模式」的授權依據，考量此際更為嚴重之干預性質，行車資訊遭儲存之受干預人已該當第 101 條第 4 項第 1 句第 7 款之「重大連帶受干預之人（erheblich mitbetroffenen Personen）」，而依同條第 7 項第 2 句規定，公民 A 應可在接受偵查機關通知後兩週內向管轄法院聲請審查此次自動車牌辨識措施之合法性，然而偵查機關卻遲遲並未通知，故公民 A 認適時其自身救濟權利之行使已受侵害[221]。

第二款　裁判要旨

第一目　「儲存模式」構成個人資訊自決權的干預

公民 A 提起的救濟先後被奧得河畔法蘭克福區法院（das Amtsgericht Frankfurt（Oder））及地方法院（Landgericht）裁定駁回，理由是法院認為公民 A 的行車資訊只是偶然地（zufällig）被蒐集，其並非第 101 條第 4 項第 1 句第 7 款所稱「被鎖定之人或重大連帶受干預之人」，偵查機關在此無須踐行通知義務[222]。隨後，公民 A 於 2019 年 8 月 6 日就本案向布蘭登堡邦憲法法院（Verfassungsgericht des Landes Brandenburg）提起憲法訴願（Verfassungsbeschwerde），主張本案雖然

[221] Vgl. VerfGBbg, Beschluss vom 19. März 2021 - VfGBbg 62/19 -, Rn. 6.
[222] Vgl. VerfGBbg, Beschluss vom 19. März 2021 - VfGBbg 62/19 -, Rn. 7-8.

doi:10.6342/NTU202403953

涉及聯邦層級的刑事訴訟法規範，但是《布蘭登堡邦憲法》（Verfassung des Landes Brandenburg）同德國《基本法》均保障人民之個人資訊自決權，地方法院忽視德國聯邦憲法法院 2018 年第二次車牌辨識裁判中，明確指出自動車牌辨識系統干預實施路段上所有用路人資訊自決權之論理，並駁回其提出的聲請，已違反《布蘭登堡邦憲法》第 6 條第 1 項及德國《基本法》第 19 條第 4 項的救濟權，且偵查機關於「儲存模式」中並未區分受干預人是否具備犯罪嫌疑，一律儲存其行車資訊，明顯構成更為嚴重的個人資訊自決權干預，縱使此次措施已經終了，為了防止偵查機關違法實施自動車牌辨識的行為重複發生，區法院與地方法院也應該以合於《布蘭登堡邦憲法》及德國《基本法》保障人民個人資訊自決權的意旨，解釋並適用相關刑事訴訟法規範[223]。對此，布蘭登堡邦憲法法院認為，當聯邦層級的法規範適用於布蘭登堡邦的法院或政府機關而涉及《布蘭登堡邦憲法》所保障之基本權時，司法審查上就必須同時檢視德國《基本法》以及《布蘭登堡邦憲法》，因而受理本案[224]，並採納公民 A 的主張，認為 2018 年第二次車牌辨識裁判已經肯認了自動車牌辨識對於所有行經車輛的干預性質，系爭「儲存模式」屬於更嚴重的干預情形，地方法院的上述裁判違反《布蘭登堡邦憲法》第 6 條第 1 項對於人民受個人資訊自決權干預時的救濟權利，故將其撤銷發回[225]。

第二目　第 100h 條結合第 163f 條無法作為授權基礎

3 年後，奧得河畔法蘭克福地方法院於 2022 年 7 月 22 日就本案再次作成裁判，適時德國《刑事訴訟法》第 163g 條已修法通過並正式生效，布蘭登堡邦的警察機關也終止了「儲存模式」的實施，改僅以「追緝模式」使用自動車牌辨識系統[226]。但是，地方法院仍然於裁判中指出，布蘭登堡邦警察機關過去曾以「儲存模式」實施自動車牌辨識的行徑，已違反了《基本法》第 20 條第 1 至 3 項的

[223] Vgl. VerfGBbg, Beschluss vom 19. März 2021 - VfGBbg 62/19 -, Rn. 12.
[224] Vgl. VerfGBbg, Beschluss vom 19. März 2021 - VfGBbg 62/19 -, Rn. 23.
[225] Vgl. VerfGBbg, Beschluss vom 19. März 2021 - VfGBbg 62/19 -, Rn. 39-52.
[226] Vgl. LG Frankfurt/O., ZD 2023, 104, 105.

doi:10.6342/NTU202403953

法律保留原則[227]。首先，地方法院說明，自動辨識車牌號碼（資料蒐集）、與目標車輛相互比對（資料使用）、隨後將取得的資料儲存至資料庫內（資料儲存）以及未來具體應用於刑事程序中（進一步的利用），都分別構成對於個人資訊自決權的干預。而正如 2018 年第二次車牌辨識裁判所言，自動車牌辨識系統干預基本權的對象涵蓋了所有行經實施路段的車輛，輔以其隱密實施的性質，加深了對於個人資訊自決權的干預程度，此外，自動車牌辨識系統能夠在一定程度上創造出特定人的移動軌跡，這會使人民產生其私人生活時時受到監視的心理壓力，進而損害其基本權利的自由行使[228]，這也是為什麼德國聯邦憲法法院最後會認為偵查機關只有在追訴重大犯罪並賦予人民充足的程序擔保下，始可以「追緝模式」實施自動車牌辨識。

上述有關自動車牌辨識系統的特質，在偵查機關以「儲存模式」實施自動車牌辨識的情形中變得更為顯著。蓋「儲存模式」下，偵查機關除了得以持續且地毯式蒐集大部分人口的行車資料，並且在數年間不斷地將資料儲存至龐大的資料庫內之外，倘若偵查機關在各個時點都能針對不同的案件產生刑事訴訟法第 100h 條第 1 項第 2 句所稱「重大犯罪」的開始嫌疑，那麼偵查機關在期限上就可能完全不受限制地保有這些車牌辨識資料的存取權限，例如實務上就曾經發生過偵查機關保有至少 3 年期間內所有的車牌辨識資料。基於其大規模地針對不具犯罪嫌疑之一般人儲備資訊，以確保未來產生追訴需求時得以存取的性質，這種「儲存模式」實際上已經構成歐盟法上討論強制儲存通信紀錄義務時所稱的「預防性資料儲備（Vorratsdatenspeicherung）」[229]。根據歐盟法院在相關裁判中的論述（請見後續介紹），預防性資料儲備雖然並非必然違憲，卻相當嚴重地加劇了對於個人資訊自決權的干預程度。而在預防性儲備車牌辨識資料的情形，就很有可能會對人民造成與「追緝模式」相比更深層的恫嚇效果或是心理壓力，也可能如

[227] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 51.
[228] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 57.
[229] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 59.

doi:10.6342/NTU202403953

布蘭登堡邦警察機關的實務運作一般，因為資料的檢閱和利用不受法律明確規範而產生被濫用的風險[230]。

有基於此，地方法院認為：德國《刑事訴訟法》第 100h 條第 1 項第 1 句第 2 款雖然授權偵查機關為查清案情或被告所在地，得在住宅外使用其他特別為監視目的所設之科技設備，而於文義上似乎可作為偵查機關以「儲存模式」實施自動車牌辨識之授權依據，但是必須基於合憲性限縮解釋予以排除。原因在於，基於其可能對人民造成的恫嚇效果和心理壓力，以及預防性資料儲備的爭議，以「儲存模式」實施自動車牌辨識系統事實上屬於高程度干預人民個人資訊自決權的措施，然而欲作為其授權基礎的第 100h 條卻並未提供相對應的程序擔保，反而缺乏了資料儲存、刪除和安全性的相關規定、資料調取的要件與有效的法官保留，甚至未能確保個人權利的有效保護以及足夠的透明性[231]。例如，德國聯邦憲法法院曾於 2018 年第二次車牌辨識裁判中指出，立法者必須針對自動車牌辨識的實施作出時間與空間上的限制，方可合乎憲法的要求[232]，2021 年新增的第 163g 條也據此賦予自動車牌辨識系統「暫時性」以及「非地毯式」的限制。這對於更高程度干預個人資訊自決權的「儲存模式」而言更為重要，亦即其若欲滿足憲法上的要求，則僅能設置在依事前觀點可合理認定犯罪嫌疑人在不久的將來會通過的地點。然而實務上布蘭登堡邦的警察機關卻將所有自動車牌辨識系統同時開啟並全天候不間斷地實施，第 100h 條或是通常一併適用的第 163f 條對此情形卻根本無法發揮限制效果[233]。

另一方面，地方法院進一步說明：考量長時間巨量儲備大部分人口的行車資料並提供調取的過程中，所產生形塑完整移動軌跡的可能以及資料遭濫用的風險，「儲存模式」的授權基礎對於資料蒐集、處理和利用的規範密度勢必要比「追緝模式」更加細緻。但是，在第 100h 條中卻完全未見相關規範。於此，2018 年第

[230] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 59.
[231] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 70.
[232] Vgl. BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 115.
[233] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 71.

doi:10.6342/NTU202403953

二次車牌辨識裁判中甚至曾論及：「...系爭條款確保資料比對不符合後被立即刪除，這符合了憲法上的要求...」[234]，似乎是表明立即刪除比對不符資料的必要性，而否定了預防性儲備車牌辨識資料的可能[235]。即使不作這樣的推論，而認為預防性儲備車牌辨識資料的措施並未被憲法所禁止，此種更高程度的個人資訊自決權干預，自然必須建立對於資料儲存、刪除與處理的限制與透明性之規範，方可滿足憲法的要求。然而，觀察第 100h 條第 1 項規定，卻無法得知資料蒐集的範圍是否只及於車牌號碼、時間、地點和行徑方向？也不清楚何種資料將會與之比對，資料之間是以何種方式相互連結和儲存？何人得以在什麼條件下調取這些資料[236]？而對於法官保留的程序擔保，第 100h 條的適用上雖然必須同時考量第 163f 條，亦即在持續不間斷地超過 24 小時或是超過 2 日時必須取得法官許可，但是地方法院的裁判指出：實務上法官時常因為不熟悉自動車牌辨識系統的「儲存模式」，而並未意識到在其許可對特定人實施長期監視的同時，也授權了偵查機關以「儲存模式」使用自動車牌辨識系統。授權偵查機關對特定人實施長期監視可能造成的影響與範圍，在這種情況下變得無法確定，使得此際適用的法官保留失去了程序擔保的實質意義[237]。此外，個案中長期監視處分與儲存模式的射程範圍究竟多大，時常繫於偶然而無法確定的情形，也導致了其因欠缺透明性而無法合乎憲法上的要求。偵查機關可能因為現存基於其他案件以儲存模式實施自動車牌辨識系統所預防性保有的行車資料庫，而對於本案只須聲請相對小範圍內的預防性車牌辨識資料儲備，即可輕鬆通過法官的審查，也可能在個別長期監視處分彼此相互連結的效果下，基於另案偵查的需求而將資料持續保留，使得偵查機關在數年內都可以迴避將資料刪除的義務。但是第 100h 條和第 163f 條中也未見針對此種情形相應的程序控制或保護機制[238]。

[234] Vgl. BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 160.
[235] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 72.
[236] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 72.
[237] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 73.
[238] Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 74.

doi:10.6342/NTU202403953

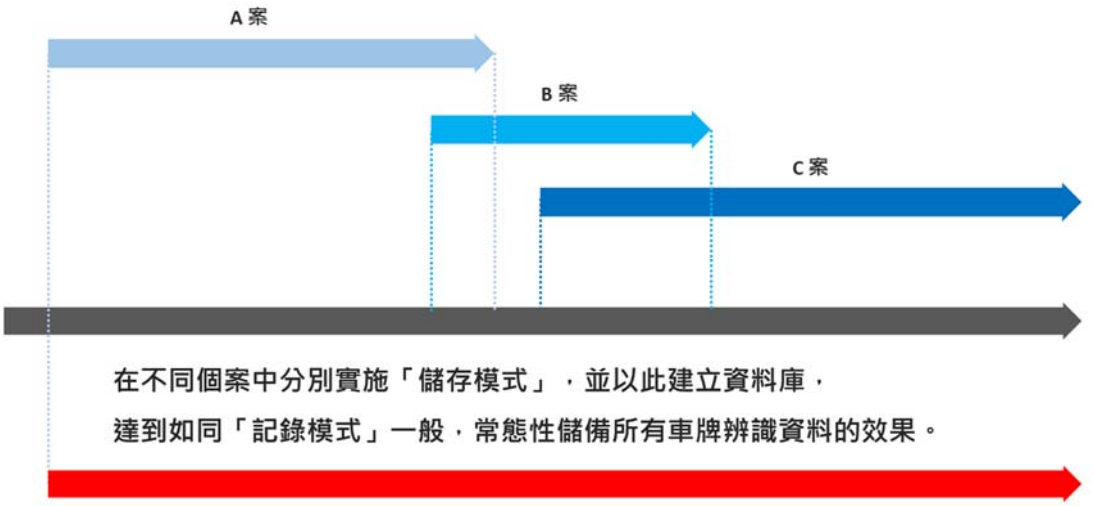

圖 3　布蘭登堡邦警方曾以「儲存模式」違法建立資料庫（筆者自繪）

第二項　第 163g 條經討論後並未納入預防性資料儲備

上述案件發生在 2021 年德國立法者新增《刑事訴訟法》第 163g 條規定的前後，其中有關第 100h 條是否得以作為偵查機關基於刑事追訴目的實施自動車牌辨識之干預授權基礎，以及緊隨其後第 101 條第 4 項第 1 句通知義務的相關討論，都間接促成了第 163g 條的立法，也可據此推論立法者為何會在草案中對於這部分特別說明[239]。值得注意的是，立法過程中曾經一度考慮是否應將偵查機關在實務上所施行的「儲存模式」納入新法的授權範圍中，然而最終考量預防性車牌辨識資料儲備將對人民構成個人資訊自決權的嚴重干預，而決定先行暫緩，待日後觀察偵查機關實施新法第 163g 條的經驗，再行決定是否有必要進一步立法授權。以下整理立法過程中的相關討論：

第一款　聯邦參議院提出之「儲存模式」

最初，由德國聯邦政府於 2021 年 1 月向德國聯邦參議院提出的「刑事訴訟法繼續發展與其他規定改革法案」中，自動車牌辨識系統的授權規定設計上基本

[239] Vgl. BT-Drs. 19/27654, S. 84-85.

doi:10.6342/NTU202403953

同於現行法第 163g 條[240]，亦即偵查機關在實施自動車牌辨識的過程中，車牌號碼一經識別必須立即與發布命令上的車牌號碼進行比對，比對不符合以及偽比對符合的資料必須立即不留痕跡地刪除，沒有預防性儲備資料的可能（追緝模式）。但是，德國聯邦參議院法制委員會（Rechtsausschuss）和內政委員會（Ausschuss für Innere Angelegenheiten）隨後於 2 月依據《基本法》第 76 條第 2 項提出了不同的意見，認為應該於德國《刑事訴訟法》中新增第 100k 條並刪除草案中原先提出的第 163g 條。

法制委員會及內政委員會提出的意見中（下稱「委員會意見」）新增德國《刑事訴訟法》第 100k 條全文如下[241]：

(1)1 符合第 2 項第 1 句或第 3 項第 1 句和第 2 句的情形，得在受干預人不知情下，於限定地點之公共交通場所，在一定時間內藉由科技方法自動蒐集車牌資料以及地點、時間及行駛方向。

(2) 1 若有事實足認發生重大犯罪行為，依第 1 項蒐集之車牌資料得與下列車牌資料進行自動化比對：

1. 核發給被告或由被告使用，或

2. 核發給被告以外之人或由該人使用，當根據一定事實可認為該人與被告有聯繫或將建立此種聯繫，

僅在可合理認定，處分有助於辨識嫌疑人身分或其所在地，且於第 2 款情形調查被告所在地採用其他方式成功機會渺茫或非常困難時，方可認措施的行使具有正當性（追緝模式）。2 自動化比對應在第 1 項自動蒐集資料後儘速為之。3 當有比對結果符合時，應儘速以手動方式檢查依第 1 項蒐集之車牌資料以及在第 1 句所稱之其他特徵是否相符。4 當比對結果不符或經手動檢查確認比對結果不符時，第 1 項所蒐集之資料應立即且不留痕跡地刪除。

(3) 1 若有事實足認發生第 100a 條第 2 項所稱之重大犯罪，於可合理認定處分有

[240] Vgl. BR-Drs. 57/21, S. 11.
[241] Vgl. BR-Drs. 57/1/21, S. 6-8.

doi:10.6342/NTU202403953

助於調查犯罪事實或辨識嫌疑人身分或其所在地，且採用其他方式成功機會渺茫或非常困難時，得實施第 1 項之自動資料蒐集。2 資料的蒐集必須依個案重大性合於適當比例。3 根據本項結合第 1 項實施的資料蒐集必須與其他基於本項蒐集之資料分別依個案各自儲存；第 2 項第 2 至 4 句於此不適用（儲存模式）。

(4) 自動車牌辨識應於事前取得處分命令：

1. 1 第 2 項結合第 1 項之處分命令由檢察官以書面為之。2 命令應說明處分之要件存在並詳細記載應當與第 2 項第 1 句自動化蒐集之車牌資料進行比對之特徵。3 命令應記載實施之公共交通場所（第 1 項第 1 句）之限定地點，且命令應定期間。4 遲延即有危險時，命令亦得以口頭且由檢察機關之偵查人員(《法院組織法》第 152 條）為之；於此情形應於三日內向命令者取得第 2 句及第 3 句所要求之書面記載。

2. 1 第 3 項結合第 1 項之處分命令應由法院核准；遲延即有危險時，命令亦得以口頭且由檢察官或檢察機關之偵查人員（《法院組織法》第 152 條）為之。2 由檢察官或檢察機關偵查人員發布之口頭命令未於 3 日內獲法院准許者，失其效力。3 第 100e 條第 1 項第 4 句、第 5 句以及第 3 項第 1 句於此準用，惟延長命令應針對個案記載該措施必要性與衡平性的重要考量，特別是有關資料蒐集範圍與保留期間。

(5) 1 當處分要件已不存在或已達成處分目的時，應儘速終結處分。

委員會意見中表示，聯邦政府提出的草案僅授權偵查機關以「追緝模式」使用自動車牌辨識系統，並未適當地處理德國《刑事訴訟法》欠缺自動車牌辨識干預授權基礎的立法漏洞，將阻礙偵查機關繼續實施過去實務上主要採行的「儲存模式」。而面對組織犯罪或是由幫派或企業主導的跨境財產犯罪，正是仰賴「儲存模式」賦予偵查機關在必要且合理的期間內分析資料的可能性，才得以調查複雜的犯罪事實。例如，將所蒐集的車牌號碼與犯罪發生的時間地點相互連結，或

doi:10.6342/NTU202403953

是在接連發生的竊盜案中，透過比對並識別所謂的「前導車（Pilotfahrzeuge）」[242]，以此進一步偵查犯罪集團的結構。有鑑於此，為了避免第 163g 條立法後，偵查機關無法繼續依第 100h 條以「儲存模式」實施自動車牌辨識，委員會意見遂對其提出的條文作出修改，並移至第 100k 條。其中，條文第 3 項是針對「儲存模式」的授權，其主要是參考第 100g 條第 3 項「調取基地台全區紀錄」的規定，但是在發動要件上設定明確的重罪目錄而更為嚴苛，亦即限於具備第 100a 條第 2 項重大犯罪之開始嫌疑的情形，同時必須採用其他方式成功達成目的之機會渺茫或非常困難，並滿足比例原則的要求，始得為之[243]。

程序擔保方面，委員會意見認為長時間（längeren Zeitraum）累積自動車牌辨識系統預防性蒐集的資料不僅違反比例原則，從資料保護的觀點更是無法接受[244]。因此，為了避免相互重疊的「儲存模式」命令可能導致偵查機關在實務上免於第 101 條第 8 項所課予的資料刪除義務，委員會意見遂於第 100k 條第 3 項第 3 句特別強調「儲存模式」處分命令下所蒐集的車牌辨識資料，必須分別「依個案各自儲存」，如此方有可能貫徹第 101 條第 8 項於個人資料不再為刑事追訴和可能發生的司法審查所需要時，必須立即將其刪除之規範意旨[245]，同時避免因偵查機關得以長期保有並持續調取其預防性儲存之資料，大幅提升「儲存模式」干預個人資訊自決權的程度，使得相關授權基礎必須適用更為嚴格的要件而無法通過比例原則的審查。又，考量「儲存模式」在一定期間內同時對不具犯罪嫌疑的一般人大量儲備資料的性質，故將其設計為相對法官保留[246]。此外，雖然準用第 100e 條第 1 項第 4 句、第 5 句以及第 3 項第 1 句允許延長「儲存模式」的實施，但是必須詳細說明個案中資料蒐集範圍與保留期間係基於何種考量而符合必要性與衡平性，以利後續的司法審查，進而達到有效的權利保障[247]。

---

[242] 又稱「領航車」或「護衛車」。謹慎的犯罪集團於犯案時通常會安排一輛前導車先行或隨同主要車輛抵達現場，觀察現場情況後如有異常就立刻通知後方的主要車輛。
[243] Vgl. BR-Drs. 57/1/21, S. 10.
[244] Vgl. BR-Drs. 57/1/21, S. 10.
[245] Vgl. BR-Drs. 57/1/21, S. 10.
[246] Vgl. BR-Drs. 57/1/21, S. 11.
[247] Vgl. BR-Drs. 57/1/21, S. 11.

doi:10.6342/NTU202403953

第二款　另一種預防性儲備資料的可能：「記錄模式」

上述法制委員會及內政委員會提出的意見經德國聯邦參議院表決多數同意並採取相應的立場[248]，因此德國聯邦政府必須對此作出回應。德國聯邦政府於其同年 3 月向德國聯邦眾議院正式提出的立法草案中，就自動車牌辨識干預授權基礎的設計上仍維持原先僅授權「追緝模式」的方案。針對聯邦參議院聲明中提到至少應授權偵查機關，於面對如恐怖攻擊或暴力屠殺（Amoklauf）此等重大犯罪，得於特定路段，例如嫌犯可能的逃亡路線，在一定期間內以「儲存模式」實施自動車牌辨識系統，藉此產生更多調查線索[249]。立法草案中僅回覆：將會繼續審查「儲存模式」針對不具犯罪嫌疑之一般人大量蒐集與儲存個人資料，所造成的高程度資訊自決權干預[250]。

法案進入審查程序後，德國聯邦眾議院法律與消費者保護委員會（Ausschusses für Recht und Verbraucherschutz）為聽取專家學者、利益團體代表和其他訊息提供者之意見而召開公聽會。其中，慕尼黑高等檢察署（Generalstaatsanwaltschaft München）提出的意見書再次重申了「儲存模式」對於偵查實務的重要性，強調「追緝模式」下若於犯罪發生當時，例如恐怖攻擊發生後，無法即時取得可疑車輛的車牌號碼，就無從立刻以自動車牌辨識系統的比對功能展開偵查，而實務上通常需要另外詢問目擊者或是調閱監視錄影器才能特定可疑車輛，但這普遍需要耗費數小時甚至數天，屆時縱使實施「追緝模式」也難收其效[251]。除了「儲存模式」以外，慕尼黑高等檢察署更進一步主張，立法者

---

248 Vgl. BR-Plenarprotokoll, 1001. Sitzung, 05.03.2021 S. 76 f.

249 Vgl. BT-Drs. 19/27654, S. 141. 相同見解：Gerwin Moldenhauer (2021), Schriftliche Stellungnahme zu der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 14. April 2021, in: https://www.bundestag.de/resource/blob/833212/18eb818300c57fcd3078f98c2b25bcd6/stellungnahme-moldenhauer.pdf.（最後瀏覽日：04/10/2024）

250 Vgl. BT-Drs. 19/27654, S. 150.

251 Vgl. Alexander Ecker (2021), Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften BT-Drucksache 19/27654, S. 6, in: https://www.bundestag.de/resource/blob/833394/c88ea0f555076a893f8fdcee0f4d5808/stellungnahme-ecker.pdf.（最後瀏覽日：04/10/2024）；肯認應增定「儲存模式」授權基礎之相同見解：Bernard Südbeck (2021), Stellungnahme zur Vorbereitung der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des

doi:10.6342/NTU202403953

應擴張第 163g 條的適用範圍，授權刑事追訴機關得基於偵查目的（Ermittlungszwecke）在有限制的長時間內（begrenzten längeren Zeitraum）儲備車牌辨識資料[252]，並將後續資料經人工比對的結果用於刑事程序（本文將此種實施模式稱為「記錄模式」（Aufnahmemodus））[253]。慕尼黑高等檢察署表示，此種「記錄模式」的授權將可有效地改善偵查實務，特別是在對抗組織犯罪或跨境財產犯罪的情形，偵查機關得以據此比對不同犯罪現場附近重複出現的車牌號碼，藉以鎖定特定車輛，並進一步調查與分析犯罪集團之結構[254]。

而有關調取透過「記錄模式」蒐集之資料以實行人工比對的干預授權基礎，慕尼黑高等檢察署建議立法者可以參考電信通訊監察的相關立法，尤其是德國《刑事訴訟法》第 100a 條對於重罪清單犯罪的開始懷疑、採用其他方式成功達成目的之機會渺茫或非常困難，且應合於比例原則。實施程序上必須適用法官保留，並準用第 100e 條第 1 項第 4 句和第 5 句規定，亦即初次核准施行的期間不得逾 3 個月，而於施行時間期滿後若認核准施行的要件仍繼續存在，得延長施行，但每次延長不得逾 3 個月。據此，即可在符合偵查實務需求的前提下，排除大眾對於持續延長實施自動車牌辨識系統的疑慮[255]。慕尼黑高等檢察署甚至表示：不能理解為何相較於通信紀錄，對於用路人而言屬於公開資訊的車牌號碼在法律上需要以更敏感的方式處理[256]。

針對上述有關「儲存模式」和「記錄模式」，此等在一定期間內預防性儲備特定範圍內所有用路人車牌辨識資料的立法建議，德國聯邦眾議院法律與消費者

Deutschen Bundestages am 14.04.2021, in: https://www.bundestag.de/resource/blob/833556/f0cf1155f11821264bce5932dec41d0f/stellungnahme-suedbeck.pdf（最後瀏覽日：06/25/2024）；Axel Isak (2021), Stellungnahme zur Vorbereitung der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 14.04.2021, in: https://www.bundestag.de/resource/blob/832970/b3853259a3e235142af251e8a766a73c/stellungnahme-isak.pdf.（最後瀏覽日：06/25/2024）；Moldenhauer, (Fn. 248).

[252] 此處在用語上明顯與前述委員會意見中表示「長時間（längeren Zeitraum）累積自動車牌辨識系統預防性蒐集的資料不僅違反比例原則，從資料保護的觀點更是無法接受」的觀點，有所呼應。Vgl. BR-Drs. 57/1/21, S. 10.

[253] Ecker, (Fn. 251), S. 7-8.

[254] Ecker, (Fn. 251), S. 7.

[255] Ecker, (Fn. 251), S. 8.

[256] Ecker, (Fn. 251), S. 7.

doi:10.6342/NTU202403953

保護委員會於 6 月提出的審查報告及決議建議表示：基於預防性儲備車牌辨識資料將對所有用路人造成強烈的個人資訊自決權干預，至少就目前提出的草案來看，委員會不建議聯邦眾議院擴大自動車牌辨識系統的適用範圍[257]。創設出合於憲法要求而使刑事追訴機關得以預防性儲備車牌辨識資料的授權基礎，雖然並非不可想像，但是必須更謹慎地檢視在何種情況下始有擴大實施自動車牌辨識系統的必要性，方可合於比例原則[258]。有鑑於此，委員會建議現階段應暫緩預防性儲備車牌辨識資料的相關立法，先觀察並評估未來偵查機關實施第 163g 條「追緝模式」的施行經驗與實務需求。最終，誠如所見，「刑事訴訟法繼續發展與其他規定改革法案」並未納入「儲存模式」或「記錄模式」的相關授權。

第三項　「儲存模式」與「記錄模式」之立法評析

首先，綜合觀察奧得河畔法蘭克福地方法院和德國聯邦參議院對於「儲存模式」授權基礎的設計與要求，可以整理出以下幾點：其一，自動車牌辨識的設置地點與施行期間應受限制，必須是依事前觀點可合理認定犯罪嫌疑人在不久的將來會通過的地點，偵查機關方可在一定的期間內於此實施；其二，必須從條文文義中可清楚得知資料可得蒐集的範圍（如車牌號碼、時間、地點和行駛方向）以及得與之相互連結、比對的資料範圍，同時，也務必明確規定資料儲存的方式與期間，偵查機關又須具備何種要件方可獲得資料的調取權限；其三，個案適用上應有事實足認重大犯罪發生，聯邦參議院甚至要求干預授權基礎設計上必須規範明確的重罪目錄；其四，僅在採用其他方式成功達成目的之機會渺茫或非常困難的情形始可實施（必要性），更應滿足狹義比例原則的要求；其五，考量其預防性儲備不具犯罪嫌疑的一般人個人資料之特性，程序擔保上設計為相對法官保留原則，法院在核准「儲存模式」的施行時亦應清楚認識其干預所有用路人個人資訊自決權的性質，且發動命令及延長命令必須詳實記載施行緣由，以利後續司法

[257] Vgl. BT-Drs. 19/30517, S. 16-17.
[258] Vgl. BT-Drs. 19/30517, S. 17.

doi:10.6342/NTU202403953

審查；其六，為了避免偵查機關迴避資料刪除義務而持續保有大部分人口的行車資料長達數年，個案蒐集的車牌辨識資料應分別儲存，並且在實施目的達成且無後續司法審查之需求時立即刪除，不得用於原先蒐集目的以外之其他案件。另一方面，關於慕尼黑高等檢察署所提出的「記錄模式」，則是比照調取通信紀錄的立法，於授權基礎設計上參考德國《刑事訴訟法》第 100a 條第 2 項的重罪清單，並適用法官保留。

必須特別說明的是，布蘭登堡邦警察機關過去實務上曾經使用，以及德國聯邦參議院於後續立法過程中提出的「儲存模式」，與此處慕尼黑高等檢察署所提出的「記錄模式」，雖然同為未區分受干預人是否具有犯罪嫌疑之預防性車牌辨識資料儲備，但是彼此間於措施實施的時點上卻有所不同。申言之，上述的「儲存模式」限於有事實足認重大犯罪發生的情形，始可向法院聲請「自此時點開始」不區分用路人是否具備犯罪嫌疑，在處分期間內一律預防性地儲備其車牌辨識資料；與之相對的，「記錄模式」則是常態性地實施自動車牌辨識系統，持續不間斷地蒐集資料並一律預防性儲存至資料庫內，並且在「有限制的長時間內」予以留存，待日後對特定車牌號碼產生偵查需求時再行調閱。換言之，「記錄模式」並未限制刑事追訴機關開始儲存車牌辨識資料的時點，使其得以基於犯罪偵查目的調取過去一定期間內所有相關的車牌辨識資料。

參照我國警察機關使用自動車牌辨識的流程可以得知，我國的施行模式基本上同於所謂的「記錄模式」，同樣是常態性地實施自動車牌辨識系統，預防性儲備所有用路人的行車資料，供日後偵查所用[259]。如果從偵查成效的觀點來看，相比於「記錄模式」，聯邦參議院所提出的「儲存模式」事實上仍有可能無法在偵查實務上發揮預期的效果，特別是犯罪結果經過一定時間後才被發現的情形，例如登山客發現棄屍，經法醫鑑定死者已經死亡超過 7 日；或是被害人出國旅行兩

[259] 例如新北市政府警察局將自動車牌辨識系統取得的錄影檔保存 1 個月，照片檔保存 6 個月。參考：新北市政府警察局刑事警察大隊網站，https://www.cic.police.ntpc.gov.tw/cp-774-54872-28.html（最後瀏覽日：04/09/2024）。當然，於程序擔保上則不如慕尼黑高等檢察署提出之意見嚴謹，詳後續討論。

doi:10.6342/NTU202403953

個月後，返家時才發現屋內一陣凌亂，貴重物品均已遭竊；甚至是被害人遭擄人勒贖，但是被綁架的當下並無其他目擊證人，而於被害人隔日仍未返家，方由家人報警處理。這些情況下，由於犯罪情事並未被立即知悉，偵查機關無從在第一時間啟用「儲存模式」預防性儲備犯罪地點附近的車輛資訊，因此縱使在事後實施自動車牌辨識，也難以有效地蒐集線索。或許可以據此推論，這也是為什麼布蘭登堡邦的警察機關會試圖迴避刪除義務，並且透過長期監視處分命令相互堆疊的方式，藉此達到同「記錄模式」般常態性在一定期間內儲備所有車牌辨識資料的效果，再透過另案偵查之假設替代流程加以調取，以收偵查成效。

然而，若是從基本權干預的視角觀察，則不難發現賦予偵查機關預防性地在一定期間內留存所有用路人行車資訊的權限，將大幅地增強自動車牌辨識系統干預個人資訊自決權的程度。蓋社會上絕大多數人一輩子均為不具犯罪嫌疑，不負忍受義務的一般人，強制在一定期間內儲備其行車資料，基於車輛位置資訊背後所隱含與家庭、政治、職業、宗教和性相關之資訊，以及持續累積後形塑人格圖像的可能，無異於使一般人在此期間內暴露在行車資料被無權使用，甚至私人生活遭探知、侵擾的風險之中。這也是為什麼德國聯邦眾議院最後會採納法律與消費者保護委員會的建議，暫緩預防性儲備車牌辨識資料的相關立法，將第 163g 條的授權範圍限制在「追緝模式」，待評估未來偵查機關的施行經驗後再決定何種情況下具有預防性儲存車牌辨識資料的必要性，且符合比例原則。而相比於「儲存模式」限制在有事實足認重大犯罪發生的時點，方開始預防性地儲備用路人的行車資料；「記錄模式」於資料儲存階段則未做出相關限制，常態性地蒐集並留存所有用路人的行車資訊，在資料使用階段方以「重大犯罪之開始懷疑」作為調取要件，等同於在沒有確切重大犯罪發生，尚未產生追訴需求的時點，就要求所有用路人承受行車資料被無權使用，甚至是私人生活遭探知的風險。這種不以發生具體刑事案件為限，而得以全天候持續不間斷蒐集人民行車資訊的干預措施，其對於人民基本權利之自由行使所產生的恫嚇效果，自然是有過之而無不及，而屬於更深一層的個人資訊自決權干預。這也是德國聯邦參議院法制委員會及內政

doi:10.6342/NTU202403953

委員會雖然一方面提出「儲存模式」的立法建議，另一方面卻特別規範個案蒐集資料應各自分別儲存，避免使警察機關實際上持續掌握所有車輛長期的行車資訊，並強調第 101 條第 8 項資料刪除義務之緣由所在。其更表示：長時間（lange Zeiträume）累積自動車牌辨識系統預防性蒐集的資料不僅違反比例原則，從資料保護的觀點更是無法接受[260]。

值得注意的是，德國律師協會（Deutsche Anwaltverein，DAV）針對「刑事訴訟法繼續發展與其他規定改革法案」的意見書中指出：第 163g 條事實上只是將自動車牌辨識技術引入《刑事訴訟法》相關偵查手段中的第一步，可以預見的是，倘若刑事追訴機關在未來社會矚目重大案件的偵查過程中，抱怨立法者不適當地將自動車牌辨識系統限縮於「追緝模式」，排除警察在案情未明即於犯罪現場附近蒐集並儲存車牌辨識資料的可能，進而導致相關線索嚴重匱乏而無法發揮偵查成效，就會促使立法者進一步修法擴張偵查機關使用自動車牌辨識系統的權限[261]。未來立法選擇上，是否考量「儲存模式」或「記錄模式」此等預防性儲備車牌辨識資料的手段，將嚴重致使不具犯罪嫌疑之一般人暴露於私人生活遭探知的風險，而應繼續從根本上禁止；又或者基於追訴重大犯罪的公共利益，將資料儲備期間控制在「有限制的長時間內」，而認其仍有合於比例原則的可能，就成為了德國立法者需要持續觀察與評估的課題，同時也是當前繼續探究我國以「記錄模式」實施自動車牌辨識系統之正當性，必須處理的前提。

第四項　「記錄模式」與「預防性儲備通信紀錄」之相似性

由於德國《刑事訴訟法》第 163g 條最終並未納入「儲存模式」或「記錄模式」，隨著立法過程結束，預防性儲備車牌辨識資料對於人民可能造成更嚴重恫

[260] Vgl. BR-Drs. 57/1/21, S. 10.

[261] 德國律師協會也基於這個理由，反對第 163g 條的立法。Vgl. Stefan Conen (2021), Stellungnahme für den DAV zum Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften, Deutscher Bundestag, in: https://www.bundestag.de/resource/blob/833986/60d3907bfc6ebded666c4671a4fb061c/stellungnahme-conen_dav-data.pdf. （最後瀏覽日：04/10/2024）

doi:10.6342/NTU202403953

嚇效果的討論也戛然而止，如此一來，應如何評價我國以「記錄模式」實施自動車牌辨識的正當性，遂成難事。不過，不論是「儲存模式」或「記錄模式」的倡議者，都曾在立法過程中主張其與德國《刑事訴訟法》第 100g 條第 3 項「調取基地台全區通信紀錄」的相似性，更建議應準用第 100a 條第 2 項之重罪目錄[262]，於此便提供了本文另一個觀察預防性車牌辨識資料儲備的視角。

詳言之，基於車輛位置資訊背後所隱含與家庭、政治、職業、宗教和性相關之資訊，若是將其系統性地持續大量蒐集、儲備，即會產生形塑個人人格圖像之風險，使國家機關得以對個人之私人生活做出精確的推論。而「記錄模式」不以干預對象具有法律上原因為限，事實上將所有人納入實施範圍，就等同於使所有人民承擔此等風險，致使其因擔憂私人生活遭揭露而無法自由行使其基本權利，產生所謂的「恫嚇效果」。這也是為什麼德國立法者選擇將「記錄模式」拒之門外。同樣地，通信紀錄表示出人民就通訊之有無、對象、時間、方式等資訊，系統性地持續蒐集通信紀錄，亦可據此準確地推論特定人之私人生活。目前實務上也不以受干預人具有法律上原因為限，無差別地預防性儲備所有人的通信紀錄，將所有人民暴露於私人生活遭探知的風險之中，而隱含了嚴重的恫嚇效果。以我國法為例，國家通訊傳播委員會依《電信管理法》第 9 條第 3 項制定《電信事業用戶查詢通紀錄及帳務作辦法總說明》，其中第 4 條第 2 項即課予電信業者保存通信紀錄至少一年的義務；《通訊保障及監察法》第 11 條之 1 則規定通信紀錄之調取以偵查最重本刑三年以上之罪為限。相對於此，德國法則考量預防性儲備通信紀錄對於人民的嚴重恫嚇效果，而在近 20 年間，先是將通信紀錄的儲備期間由 6 個月縮短為 10 週，涉及位置資訊之通信紀錄進一步限制為 4 週，而後德國聯邦憲法法院又依循歐盟法院的見解，主張：縱使是為了重大犯罪之偵查此等重要公共利益，無差別預防性儲備通信紀錄仍然無法合於比例原則，並宣告《電信法》相關規定違憲。同時，關於此等受預防性儲備之通信紀錄的調取規定，德國

[262] Vgl. BR-Drs. 57/1/21, S. 6-8; Ecker, (Fn. 251), S. 8.

doi:10.6342/NTU202403953

立法者認為其干預嚴重程度不亞於通訊內容的監察，而依通信紀錄的儲備原因分別準用了德國《刑事訴訟法》第 100a 條第 2 項或第 100g 條第 2 項之重罪清單（詳後續論述）。

有鑑於「記錄模式」與預防性通信紀錄儲備的相似性，本文認為有必要考察德國聯邦憲法法院以及歐盟法院於預防性通信紀錄儲備裁判中的相關論述，以此理解此等措施對於人民所產生的恫嚇效果應如何減緩，又應如何設計其施行要件始可具備干預之正當性，始可正確理解「記錄模式」對於人民基本權的干預程度[263]。不過，正式開始梳理相關裁判以前，必須先認識到預防性儲備車牌辨識資料與通信紀錄的不同之處，以便於後續考察過程中加以留意。首先，車牌辨識資料與通信紀錄雖然均屬於經系統性大量蒐集後，得以拼湊出特定人人格圖像之個人資料，且預防性儲備的實施模式又使得系爭措施的干預對象事實上及於所有人而產生恫嚇效果，然而，不同於車牌辨識資料是於公共交通場所被蒐集，通訊原則上不輕易為通訊雙方以外之第三人知悉的性質，致使通信紀錄本身的資料敏感性明顯高於車牌辨識資料，特別是僅存取少量資料的情形，二者干預人民基本權的程度顯然有異，而可能影響其資料儲備或調取之干預授權基礎的要件設計。

另一方面，通信紀錄與車牌辨識資料根本性的不同在於，電信或網路服務業者原本就會基於收費目的，而在與消費者訂立契約時取得預防性儲備通信紀錄的同意。換句話說，縱使不存在國家機關追訴刑事案件的需求，消費者為了享有電子通訊服務，本來就必須承擔通信紀錄被預防性儲備，所隱含私人生活遭受揭露的風險，只是可能伴隨著國家機關的立法，而導致人民必須承擔資料儲備期間因此延長所衍生的風險。例如電信服務業者本僅需要儲備 1 個月的通信紀錄即可滿足收費目的，國家機關卻立法強制電信服務業者儲備 6 個月的資料。不同於此，車牌辨識資料庫卻是自始至終由國家機關一手創設，若不是為了滿足刑事追訴的

[263] 奧德河畔法蘭克福地方法院於審理布蘭登堡邦警察機關濫用「儲存模式」而保有長時間的車牌辨識資料時，也曾指出其實際上已經構成歐盟法院討論強制儲存通信紀錄義務時所稱的「預防性資料儲備」（Vorratsdatenspeicherung）。Vgl. LG Frankfurt/O., Beschluss vom 22.7.2022 – 22 Qs 40/19, Rn. 59.

doi:10.6342/NTU202403953

需求，人民根本無須承擔其所帶來的風險。則刑事追訴之目的是否正當？車牌辨識資料之預防性儲備是否能有效達到此目的？是否存在其他侵害較小但同等有效的手段？資料儲備期間應限於多長？資料調取又應具備何等要件？就會受到更嚴格的檢視，而有賴國家機關給出合乎憲法要求的答案。此外，通信紀錄是由電信或網路服務業者預防性儲備於其伺服器內，待符合法律規定時方由國家機關取得，因此在資料儲備階段仍散落於各個業者的手上，較不容易遭國家機關濫用。相對於此，「記錄模式」下卻是由警察機關自行蒐集、儲備車牌辨識資料，無形中升高了這些資料被國家機關濫用的風險，勢必也會對資料調取授權規定的設計造成影響。

以下，本文將梳理歐盟法上因強制會員國預防性儲備通信紀錄所產生的爭議，觀察德國聯邦憲法法院和歐盟法院面對此等措施對人民產生的恫嚇效果，以及對於社會自由的整體影響，於其干預授權基礎上課予了何等憲法要求。期待能藉此回過頭評價我國實務上警察機關大規模地以「記錄模式」實施自動車牌辨識系統，是否具備合於憲法的授權規定。

第二節　歐盟預防性儲備通信紀錄之爭議

對於個人資料保護，歐盟法相關規範首次出現於 1995 年的「個人資料處理與自由流通之保護指令」（95/46/EC 指令，下稱「1995 年指令」）[264]，該指令第 1 條開宗明義表示，其目的在於課予會員國保護人民基本權利與自由之義務，特別是個人資料處理層面上的隱私權；且為達此目的，不允許會員國限制個人資料在各會員國之間的自由流通[265]。指令中對於「個人資料」、「資料處理」等概念作出明確的定義，並概括性地規範資料處理原則、資料主體權利、司法救濟、資料傳

[264] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 蔡宗珍（2018），〈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 108。

[265] 歐盟 95/46/EC 指令第 1 條。

doi:10.6342/NTU202403953

輸於第三國等事項。然而，其並未特別指涉電信領域之個人資料，並且將涉及維護國家安全、公共安全與刑事犯罪領域的個人資料排除於本指令的適用範圍之外，留待各會員國自行決定[266]。其後，2002 年歐盟「電信領域個人資料處理與隱私保護指令」（2002/58/EC 指令）開始制定電信領域個人資料的相關規範，其中除了通訊紀錄之外，也包括了通訊過程中雙方的位置資訊。但是，是否以及如何儲備此種通訊過程中所產生的資料，於適時仍是留待各會員國自行決定。2006 年，歐盟為了應對國際上恐怖攻擊頻傳，情勢愈演愈烈，遂透過「預防性儲備通信紀錄指令」（2006/24/EC 指令），要求會員國於內國法課予電信或網路服務業者儲備通信紀錄的義務，以利後續使用，卻也進一步產生了：此種預防性儲備通信資料的指令是否違反《歐洲聯盟基本權利憲章》（Charter of Fundamental Rights of the European Union），以及轉換後的內國法是否符合本國憲法的爭議。本文以下將依照時間順序逐步介紹德國聯邦憲法法院以及歐盟法院對於預防性儲備通信紀錄的論理，並著重於此等措施是否具備容許性，以及在何種要件下方具正當性的討論，期待能夠藉此回過頭來反思我國預防性儲備車牌辨識資料之容許性，並進一步檢視相關授權基礎。

第一項　2002 年「電信領域個人資料處理與隱私保護指令」

為了將 1995 年指令的內涵具體實現於電信領域的個人資料，並做出各細緻的規範，歐盟於 2002 年另行制定「電信領域個人資料處理與隱私保護指令」（2002/58/EC 指令，下稱「2002 年指令」）[267]。其中，關於通訊服務訂閱者或使用者的通信紀錄，原則上若不再為通訊傳輸所需，就必須刪除或不可回復地去識別化（made anonymous）。例外規定公共電子通信服務提供者或公共通訊網路經營者（以下簡稱「電信或網路服務業者」）得基於收費目的留存並處理通信紀錄，

[266] 歐盟 95/46/EC 指令第 3 條第 2 項。

[267] *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

doi:10.6342/NTU202403953

當帳單可合法爭執或可請求付款期限已過則必須予以刪除或去識別化；或是在取得服務訂閱者或使用者的同意後，得為行銷或提供加值服務處理通信紀錄，但應允許服務訂閱者或使用者得在任何時候將同意撤回[268]。另外，通訊過程所產生的位置資訊只有在去識別化的情形，或是取得服務訂閱者或使用者的同意後，於提供加值服務的必要範圍內，方可進行資料處理[269]。同時，會員國應立法確保通訊內容及相關紀錄之秘密性，特別應立法禁止未得通訊使用者同意之監聽、竊聽、儲存或是其他攔截或監控通訊內容與通信紀錄之行為[270]；但是，會員國得為維護國家安全、國防、社會安全，或為預防、偵查、確認與追訴犯罪，或防範電信系統的無權使用，於民主社會所必要、適當且合於比例原則的範圍內，立法授權在一定期間內儲備通信紀錄和電信使用者的位置資訊[271]。由此可見，2002 年指令基本上認為除了基於收費目的，或是取得使用者同意的情形以外，通信紀錄原則上若不再為通訊傳輸所需，即應立即刪除或去識別化；例外容許會員國得基於維護國家安全、國防、社會安全，或為預防、偵查、確認與追訴犯罪，或為達防範電信系統的無權使用之目的，另行立法授權在符合比例原則的要件下進行儲備[272]。

第二項　2006 年「預防性儲備通信紀錄指令」

雖然 2002 年指令授權歐盟會員國得基於上述目的，在一定期間內，於犯罪或公共安全威脅尚未發生時即預防性地儲備通信紀錄與位置資訊，然而各會員國對此卻反應不一。部分國家考量預防性儲備通信紀錄將嚴重干預人民的秘密通訊自由，故拒絕立法；其他國家雖有制定相關法規，彼此之間對於得預防性儲備的資料類型、儲備要件以及留存期間卻有著顯著的差異。這一方面使得歐盟境內跨國提供電信或網路服務的業者，面對不同法規要求產生了營運上的障礙[273]；另一

[268] 歐盟 2002/58/EC 指令第 6 條。
[269] 歐盟 2002/58/EC 指令第 9 條。
[270] 歐盟 2002/58/EC 指令第 5 條第 1 項。
[271] 歐盟 2002/58/EC 指令第 15 條第 1 項。
[272] 參考：蔡宗珍，前揭註 264，頁 108-109。
[273] 歐盟 2006/24/EC 指令立法說明第 6 點。

doi:10.6342/NTU202403953

方面則導致預防與偵查犯罪的需求無法被滿足。輔以當時歐盟境內恐怖攻擊頻傳的背景[274]，為了協調各會員國內國法課予電信或網路服務業者預防性儲備通信資料的義務，以確保受儲備之通信資料得於事後用於重大犯罪之偵查、確認與追訴，歐盟於 2006 年進一步制定了「預防性儲備通信紀錄指令」（2006/24/EC 指令，下稱「2006 年指令」）[275]，放棄原先例外容許另行立法的立場，改為強制要求各會員國立法授權通信紀錄與位置資訊之預防性儲備。

2006 年指令課予會員國儲備通信紀錄義務的資料類型可以區分為以下六大類：其一，追蹤與識別通訊來源端所必要的資料，例如固網電話與行動電話的電話號碼、訂閱者或註冊者的姓名和地址，或是網路通訊時，關於網路連接、電子郵件與網路電話的使用者識別碼（user ID）、電話號碼、姓名、地址和 IP 位址；其二，追蹤與識別通訊終端所必要的資料；其三，識別通訊日期、時間、持續期間所必要的資料，於固網電話與行動電話的情形，是指通訊開始與結束的日期和時間，於網路連接、電子郵件與網路電話的情形，則是指登入與登出網路服務的日期和時間、經網路服務業者分配的動態與固態 IP 位址以及使用者識別碼；其四，識別通訊種類所必要的資料；其五，識別使用者通訊設備或聲稱屬於其設備所必要的資料；其六，識別行動通訊設備位置資訊所必要的資料，包括通訊開始時行動通訊設備所使用的基地台位置（Cell ID），以及通訊過程中透過基地台位置識別行動電話地理位置的資料[276]。簡單來說，2006 年指令強制會員國預防性

[274] 例如 2006/24/EC 指令立法說明第 10 點就提到，2005 年發生的倫敦自殺炸彈恐怖攻擊事件讓歐盟理事會意識到應盡快採納預防性儲備通信紀錄的措施。*See* Lucy Rodgers, Salim Qurashi, and Steven Connor, *7 July London bombings: What happened that day?*, BBC (July 3, 2015), https://www.bbc.com/news/uk-33253598; Arianna Vedaschi & Valerio Lubello, *Data Retention and its Implications for the Fundamental Right to Privacy*, 20 TILBURG L. REV. 14, 18-19 (2015).

[275] *See* Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[276] 翻譯參考：蔡宗珍，前揭註 264，頁 109-110；指令制定的討論過程中，「第 29 條個資保護工作小組（Article 29 Data Protection Working Party, WP29）」曾提議僅預防性儲備通訊開始時行動設備的位置資訊，以避免描繪出特定人的移動軌跡。*See* ARTICLE 29 Data Protection Working Party, *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM (2005)438 final of 21.09.2005)* (Oct. 21, 2005), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf.

doi:10.6342/NTU202403953

儲備的資料涵蓋了在各個通訊過程中，得以特定通訊發話端、接收端的真實身分、地理位置，以及通訊發生的時間日期、持續長短的各類資訊[277]。但是，並不包括通訊的實際內容，本指令也明確地將「通訊內容」排除於預防性資料儲備的效力範圍[278]。

依據 2006 年指令，會員國應確保由電信或網路服務業者所產生或處理的上述資料，皆會受到預防性儲備，其中也包括通訊來源端曾嘗試開始通訊，但未獲對方接通的情形（unsuccessful call attempts）所產生的資料，但不包括通訊自始即未連接的情況（unconnected calls）[279]。上述資料於通訊完成後至少應保存 6 個月，至多不超過 2 年[280]。會員國並應於本指令自 2006 年 3 月 15 日生效之時起一年半內，即 2007 年 9 月 15 日前，完成將本指令內容轉換為內國法的立法工作[281]，惟涉及網路連接、電子郵件與網路通話之通訊紀錄與位置資訊，其立法程序得經聲明後遲延至三年內完成[282]。

第三項　德國聯邦憲法法院 BVerfGE 125, 260 裁判

第一款　裁判背景

為完成 2006 年指令賦予歐盟會員國的立法義務，德國立法者於《電信法》（Telekommunikationsgesetz）新增了第 113a 條及第 113b 條，其中，第 113a 條課予電信與網路服務業者將其用戶使用通訊服務過程中所產生的通信紀錄與位置資訊，一律儲存 6 個月的義務。資料儲存範圍基本上同於 2006 年指令的規定，亦即通訊過程中，得以特定出通訊發話端、接收端的真實身分、地理位置，以及通訊發生的時間日期、持續長短的各類資料。第 113b 條則規定，依第 113a 條儲

277 蔡宗珍（2014），〈政府監控概觀——兼淺析歐盟 2006 年強制儲存通信紀錄指令〉，《台灣法學雜誌》，244 期，頁 27-28。
278 歐盟 2006/24/EC 指令第 5 條第 2 項。
279 歐盟 2006/24/EC 指令第 3 條。
280 歐盟 2006/24/EC 指令第 6 條。
281 歐盟 2006/24/EC 指令第 15 條第 1 項。
282 歐盟 2006/24/EC 指令第 15 條第 3 項。

doi:10.6342/NTU202403953

存之資訊僅得用於：追訴刑事犯罪（第一款）；防止對於公共安全的重大危害（第二款）；履行聯邦和邦憲法保護機關、聯邦情報局和軍事保安局之法定職責（第三款）。而《刑事訴訟法》第 100g 條則作為以刑事追訴為目的，調取通信記錄之授權基礎。

由於此種無差別預防性儲備通信記錄及位置資訊的措施，涉及了所有的通訊服務使用者，而不論其是否具有犯罪嫌疑，且系爭規定中資料儲備期間長達 6 個月，因此，在立法過程中即產生了許多爭議，立法通過後更隨即被多組人馬提起憲法訴願。德國聯邦憲法法院最後受理三組憲法訴願並併案審查，於此探究依循 2006 年指令轉換之《電信法》第 113a 條及第 113b 條是否有違德國《基本法》對於人民秘密通訊自由之保障[283]。且鑑於本案牽涉範圍過廣，聯邦憲法法院於受理後作成定暫時處分（einstweilige Anordnung）裁定，將電信或網路服務業者已依《電信法》第 113a 條預防性儲備的通信紀錄及位置資訊，限於用作《刑事訴訟法》第 100a 條所列重大犯罪之追訴[284]。

第二款　裁判見解

德國聯邦憲法法院必須面對的問題可以歸納為以下幾點：（一）本案是否涉及 2006 年指令的效力問題，而應裁定停止訴訟程序，送請歐盟法院為先決裁判？（二）無差別預防性儲備通信記錄所干預之基本權為何？（三）是否完全沒有合於比例原則的可能？（四）若無差別預防性儲備通信記錄並非憲法上所絕對禁止，則於授權基礎上應如何設計方可合於憲法要求？

283 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 1-345.
284 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 88; 李寧修（2015），〈預防性通信資料存取之憲法界限——以歐盟儲備性資料存取指令（2006/24/EG）之發展為借鏡〉，《興大法學》，17 期，頁 106。

doi:10.6342/NTU202403953

第一目 無須送請歐盟法院為先決裁判

本案首當其衝的是關於 2006 年指令的效力問題，如果在指令框架下將「無差別預防性儲備通信記錄」之義務轉換為內國法，完全沒有合於德國《基本法》的空間，就有必要回過頭審視 2006 年指令是否有違歐盟對於人民基本權利之保障，而根本無效。對此，聯邦憲法法院認為，倘若立法者對於本案系爭法規做出修正，則 2006 年指令並不會影響德國《基本法》對於人民基本權利的保障，故認本案並無送請歐盟法院為先決裁判的必要[285]。換句話說，聯邦憲法法院於此基本上肯定了無差別預防性儲備通信記錄 6 個月的措施，在符合一定要件下，仍有合於德國《基本法》的可能，因此並未質疑也不欲挑戰 2006 年指令於歐盟法保障人民基本權利觀點下之合法性。

第二目 預防性儲備通信紀錄構成秘密通訊自由之干預

關於系爭措施所干預之基本權，聯邦憲法法院指出：《基本法》第 10 條第 1 項秘密通訊自由的保障範圍並不僅限於實際的通訊內容，還包括了通訊情狀的秘密性，尤其是是否、何時以及多麼頻繁地發生通訊，或是什麼人或什麼裝置之間是否曾經嘗試進行通訊[286]。有基於此，對於通信過程中所產生之通信紀錄的資料蒐集與儲存、與其他資料相互比對、分析、選作未來用途或是傳輸給第三方，都分別會獨立構成對於秘密通訊自由的干預，《電信法》第 113a 條無差別預防性儲備通信記錄、第 113b 條規範此等資料的傳輸可能以及《刑事訴訟法》第 100g 條授權對於此等資料的具體利用，也都因此分別構成對於《基本法》第 10 條第 1 項秘密通訊自由之干預[287]。

[285] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 183.
[286] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 189.
[287] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 190.

doi:10.6342/NTU202403953

第三目 無差別預防性儲備 6 個月通信紀錄之容許性

至於無差別預防性儲備 6 個月通信記錄是否必然違憲？聯邦憲法法院本於其前述立場，進一步表示：基於刑事追訴、防止危害與國安情報領域中的適當目的，在尚不具備具體事由的情況下儲備 6 個月的通信紀錄，並不必然違反《基本法》第 10 條第 1 項秘密通訊自由的保障，立法者仍得為追求合憲目的，在符合適當性、必要性與狹義比例原則的要求下設計相關干預授權基礎。換言之，如果法規設計上能夠充分考量系爭措施嚴重干預基本權的性質，授權基礎也並非必定不能通過狹義比例原則的審查[288]。針對系爭《電信法》第 113a 條，首先於合憲性目的審查上，聯邦憲法法院認為有效偵查犯罪、防止危險與完成國安情報任務，均屬得以正當化秘密通訊自由干預之合憲目的，尚未產生具體事由的情形下即預防性地儲備通信紀錄，其本身並不會構成違法干預基本法第 10 條第 1 項之目的。聯邦憲法法院強調，《基本法》第 10 條第 1 項並未完全禁止資料之預防性蒐集與儲備，而是禁止對於此等資料不符合比例原則地蒐集，特別是不受目的限制地蒐集。因此，應該被嚴格禁止的是基於不特定且尚未能特定之目的所實施的個人資料儲備。不過，欠缺具體事由即預防性地儲備資料，也只有在特殊情況下方可被例外允許，其授權基礎的要件設計上必須特別嚴格，尤其是受儲備資料之後續使用目的[289]。

聯邦憲法法院也表示，預防性地儲備通信記錄以利後續傳輸予負責刑事追訴、防止危險或國安情報的有權機關，確實能達成上述合憲目的，滿足適當性的要求。蓋此種預防性通信紀錄儲備措施能避免通信紀錄於通訊目的達成後即被刪除，創造了原先不存在的偵查可能。同時，通訊服務的蓬勃發展，近年來也反映於犯罪的準備與實施。另外，立法者所創設的通信記錄儲備義務是否能夠完整地重建所有通訊過程，並非系爭規定是否具備適當性的判斷重點，即使此種預防性資料儲備義務無法將所有的通信紀錄連結至特定人，例如犯罪嫌疑人刻意使用他人的網

[288] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 205.
[289] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 206.

doi:10.6342/NTU202403953

路熱點、網咖、外國網路電信服務或是以假名註冊預付卡門號，藉此躲避刑事追訴機關透過通信紀錄追查身分，也不能據此認定系爭規定不具適當性。原因在於，適當性並不要求系爭規定必須在每一個個案中均達成目的，而是僅要求其具備促進目的實現的效果[290]。

另一方面，無差別預防性儲備 6 個月通信紀錄的措施，以達上述有效偵查犯罪、防止危害與完成國安情報任務之目的，也可被認為具有其必要性，而不存在其他干預程度較小但同等有效的手段。聯邦憲法法院於此特別強調，尤其是所謂的「快速凍結（Quick-Freezing）」程序，其不同於普遍且無差別的預防性通信紀錄儲備措施，而僅在個案中出現具體緣由後，例如基於特定的犯罪嫌疑，方開始儲備相關通信紀錄。然而，快速凍結程序只有在相關通信紀錄尚未經電信或網路服務業者刪除而仍然存在時，才有機會取得其「開始實施時點」之前的通信紀錄，而不如持續性通信紀錄儲備措施，能有效確保過去六個月內完整的通信紀錄受到留存[291]。

即使《電信法》第 113a 條預防性儲備 6 個月通信記錄的措施無差別地影響了絕大多數的人民，並且構成格外嚴重的秘密通訊自由干預，聯邦憲法法院仍然基於以下理由認為其不必然違反狹義比例原則：其一，通信紀錄並非直接由國家儲備，而是經由私人電信或網路服務業者執行此種預防性儲備的措施，如此一來，資料在儲存階段仍散落於各個公司的資料庫內，並未直接提供給國家，立法者仍然能夠透過通信紀錄調取以及進一步使用的授權規定，確保通信紀錄不會被用於不確定或尚不確定的目的當中，並考量此種措施嚴重的干預性質，將資料得被調取與利用的部分限制在絕對必要的範圍內。同時，憑藉資料儲存與調取在結構上

[290] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 207.

[291] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 208; Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 249 (2007). 第 163g 條立法過程中曾討論的「儲存模式」，基本上就屬於所謂的「快速凍結」程序。由於「快速凍結」程序將干預措施限縮在個案中具備特定犯罪嫌疑的情形始可實施，因此可以減緩預防性資料儲備措施對於人民所造成的心理壓力，以及其自由行使基本權利的影響。然而也正如聯邦憲法法院指出，「快速凍結」於偵查犯罪、防止危險或提供國安情報的效果上，仍比不上常態性持續儲備資料之措施。

doi:10.6342/NTU202403953

的區別，促成資料使用的透明性與監督機制[292]。其二，將通信紀錄預防性地儲備6個月，並未破壞《基本法》第10條第1項秘密通訊自由的保障，也沒有違反《基本法》第1條第1項之人性尊嚴，或是第19條第2項的重要內涵（Wesensgehalt），故並未為《基本法》所禁止。儘管系爭措施的影響層面非常廣泛，卻仍受到一定的限制，例如通訊實際內容即被明確地排除於儲存範圍。又，考量系爭措施儲備通信紀錄的程度與資訊解讀能力（Aussagekraft）[293]，保存期間6個月雖然相當長久且已達到得以合於比例原則之上限，但是公民可以相信，除非具有特別嚴重的原因，否則其資料在期間經過後即會被刪除且不可能被任何人重建[294]。其三，新型態的通訊方式不同於以往，不受時間與空間的限制，且不被外界察覺，這同時也使罪犯們得以秘密地溝通與行動，讓四散的犯罪團體得以聚集並有效地合作，同時，幾乎不受阻礙地通訊也使知識、行動意願和犯罪能量的彼此交織成為可能，因此，通訊關係的重建對於防止危險與刑事追訴就產生了重要的意義。此外，考量通訊過程通常不為公眾知悉，無法同其他領域的線索般透過社會上的偶然記憶，例如證人的指述，來重建過去的事件，通信過程只會陷於因通訊紀錄經刪除而完全無法得知，或是因資料受儲備而仍有探知可能，這兩種情形。有鑑於通訊紀錄的特殊性，應使立法者於此得在各種利益之間權衡，並顧及國家任務履行的重要性，決定多大程度地刪除或保留這些通信紀錄[295]。

然而，聯邦憲法法院也強調欠缺具體事由下無差別預防性地蒐集資料，仍然只有在特殊情況下方可被例外允許，此次無差別預防性儲備通信紀錄的立法，並不能被視為未來預防性儲備其他有利於防止危險或刑事追訴之資訊的開端；反而應迫使立法者在考慮創設新的資料儲備義務或授權時，必須整體考量現行法下已存在的各種資料儲備而有所克制[296]。

---

[292] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 214.
[293] 翻譯參考：蔡宗珍，前揭註264，頁122。
[294] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 215.
[295] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 216 f.
[296] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 218.

doi:10.6342/NTU202403953

第四目 干預授權基礎之憲法要求

有鑑於無差別預防性通信紀錄儲備措施之資料儲備規模與潛在資訊解讀能力，「資訊安全」遂成為其授權基礎是否合於比例原則的重要考量之一，特別是此種由私人電信或網路服務業者儲存資料的情形，畢竟私人業者一般僅看重經濟效益與成本支出，維護資訊安全的意願極其有限；於此同時，通信紀錄資料庫內多樣化的資訊價值卻可能會吸引無數的有心人士，進而產生遭非法存取的風險。有基於此，此種無差別預防性儲備 6 個月通信紀錄的干預措施就必須適用一個特別高的資訊安全標準，其嚴格程度甚至超越對於一般儲備通信紀錄措施的憲法要求，且於資料儲存與傳輸方面皆應有所適用，更需要有效地確保儲備期間屆滿後，資料即被刪除[297]。聯邦憲法法院進一步說明，《基本法》雖然並未明確特定出具體應採用何種資訊安全措施，但是考量系爭措施嚴重干預秘密通訊自由的性質，立法者所採取的措施必須合於當前科技發展水準（wie den Stand der Technik），以維護受預防性儲備通信記錄的資訊安全，因此，聯邦憲法法院參考本案鑑定意見書中現行技術下可得應用的資訊安全機制，明確指出立法者必須使電信或網路服務業者將其依《電信法》第 113a 條所蒐集的資料，獨立儲存於使用非對稱式加密技術且未與網路連接的設備當中，並另外將加密資料的解密金鑰儲存至不同的設備，同時，對於解密金鑰的調取程序應適用「四眼原則（Vier-Augen-Prinzip）」[298]，再詳細記錄資料取存與刪除時所產生的數據軌跡，且實施自動糾錯程序[299]，如此，方可滿足《基本法》對於此等措施所要求的特別高資訊安全標準。此外，立法者也應該制定一套納入資料保護官而公開透明的監督機制，同時涵蓋對於違反資訊安全規定的適當制裁[300]。

另一方面，《電信法》第 113b 條調取受儲備通信紀錄之規定，於設計上不只

[297] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 222.
[298] 四眼原則是指相關程序必須獲得兩個人的核准，甚至是兩個人均在場的情形方可實行，屬於內部控制的重要概念。
[299] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 224.
[300] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 225.

doi:10.6342/NTU202403953

關乎其自身的合憲性，同時也影響了無差別預防性儲備資料的授權基礎是否能合於比例原則。由於第 113a 條並未區分資料儲備對象，而事實上儲備了幾乎所有通訊服務使用者的通信紀錄，且這些受預防性儲備的通信紀錄一旦經過分析，不僅得以深入探知特定人的私人生活，在某些情況下甚至可以對其個人性格與行動軌跡做出詳盡的推論，因此，考量是項措施嚴重的干預性質，此種系統性儲備 6 個月之通信記錄所應適用的調取規定，自然與《電信法》第 96 條針對電信或網路服務業者基於收費或加值服務目的儲備用戶資料的使用授權有所不同，在此甚至不能輕率地推論此等資料的調取利用，其干預秘密通訊自由的嚴重程度不如通訊內容的監察[301]。有基於此，此種資料的使用必須是基於特別重大的公共利益，方可被視為合憲。以刑事追訴為例，系爭資料的調取必須於個案中具備重大犯罪的嫌疑始可為之，立法者在此具有一定的裁量權限，得以選擇準用現有的重罪目錄，或是另行創設全新的清單，然而最終必須具體決定哪些刑事犯罪的追訴情形得以調取系爭資料，不能透過概括授權條款或是泛泛地於授權基礎中指稱「重大犯罪（Straftaten von erheblicher Bedeutung）」，同時，立法者也必須確保重罪目錄中所列犯罪確實屬於相當嚴重的犯罪，且資料利用符合比例原則[302]。

關於程序保障方面，聯邦憲法法院表示：立法者應使干預授權基礎符合「透明性」的要求，因此，受儲備通信紀錄的使用必須盡可能公開，亦即應考量在資料使用前即通知資料主體的可能性，以此消除無差別預防性資料儲備帶給人民因害怕受到監視而產生的心理壓力。若是為了避免危害資料使用目的，而未在第一時間通知資料主體，至少也應於資料使用目的達成後踐行通知。倘若基於特定事由而縱使在目的達成後仍無法通知資料主體，就必須獲得法院許可並定期接受審查[303]。此外，考量系爭措施嚴重干預秘密通訊自由的性質，以及其隱密實施的方式，聯邦憲法法院認為原則上應適用法官保留，並且須於令狀中清楚記載資料調

[301] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 227.
[302] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 228 f.
[303] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 240-244.

doi:10.6342/NTU202403953

取的種類、範圍以及原因[304]。同時，也應於授權基礎中針對資料的後續使用，制定相關監督機制與權利救濟程序，如果資料主體在措施實施前沒有機會避免其通信記錄遭到利用，就必須使其得於日後尋求司法救濟[305]。

第三款　裁判簡評

聯邦憲法法院於論述無差別預防性通信紀錄儲備的基本權干預程度時，認為無論立法者如何設計受儲備資料的後續利用，都會無可避免地升高人民無辜地被迫接受進一步調查的風險。原因在於，人民之所以受到調查，並非總是可歸責於己，有時僅是恰好在倒楣的（ungünstig）時間點上處在某個通訊區域內，或者與特定人有所聯繫，就被迫接受廣泛的調查並承受必須解釋自身行為的壓力[306]。此外，人民一方面普遍對於其通信紀錄具有隱私期待，另一方面卻無法立即察覺其資料受到預防性儲備以及未來可能被如何使用，也導致此種措施成為更高程度的干預。因此，不以具備法律上原因為要，而將所有人納入潛在干預對象的無差別預防性通信紀錄儲備，可能會讓人民產生一種受到監視的威脅感，進而影響人民基本權利的自由行使[307]。

在此，聯邦憲法法院於干預程度的判斷上，將系爭措施的干預對象不以具備法律上原因為要，可能使人民產生受到監視的心理壓力，並影響基本權利的自由行使納入考量，明顯與聯邦憲法法院於兩次車牌辨識裁判中，基於自動車牌辨識系統所造成的恫嚇效果，而主張其屬於對個人資訊自決權的重大干預，論理相同。值得一提的是，*Carpenter* 案中，美國聯邦最高法院也曾表示，歷史性行動電話基地台位置紀錄之調取相比於 GPS 偵查的情形屬於更嚴重的隱私權侵害，蓋警方不需要提前判斷他們是否以及何時欲調查特定人，即可事先掌握所有人的資料，

304 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 247-250.
305 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 251.
306 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 212. 程明修，前揭註 212，頁 29。
307 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 212.

doi:10.6342/NTU202403953

等同於任何人一旦被判斷具有犯罪嫌疑，其過去 5 年的位置資訊和移動軌跡，包含其背後隱含的家庭、政治、職業、宗教和性相關資訊就會受到揭露[308]，其結論上也與德國聯邦憲法法院的判斷不謀而合。由此可見，前述學說上所提出的「水平疊加之基本權干預」，並非空穴來風。

面對預防性儲備 6 個月通信紀錄對於人民所造成的重大秘密通訊自由干預，聯邦憲法法院基於「通信紀錄於儲存階段不受國家機關掌握」、「儲備期間受到合理限制」以及「通信紀錄對於犯罪偵查的重要性」，而主張其仍有通過狹義比例原則審查的可能。其中，有關「通信紀錄於儲存階段不受國家機關掌握」，聯邦憲法法院表示：「通信紀錄於儲存階段仍散落於各個公司的資料庫內，立法者仍然能夠透過通信紀錄調取以及進一步使用的授權規定，確保通信紀錄不會被用於不確定或尚不確定的目的當中，並考量此種措施嚴重的干預性質，將資料得被調取與利用的部分限制在絕對必要的範圍內。同時，憑藉資料儲存與調取在結構上的區別，促成資料使用的透明性與監督機制[309]。」不過，若以此觀察以「記錄模式」實施自動車牌辨識的情形，則會發現由於資料蒐集、儲備以及調取均是由警察機關自行為之，在結構上欲促成資料使用的透明性以及相關的監督機制愈發困難，進而致使「記錄模式」的干預程度亦隨之提升。

另一方面，德國聯邦憲法法院於本裁判中不只聲明資訊安全對於預防性資料儲備措施的重要性，更具體地指出立法者於授權基礎的設計上應採行哪些措施。此舉雖有影響立法自由之虞，但是卻能有效避免資訊安全淪為口號式的宣導，本文在此予以肯定。其次，本裁判於比例原則審查上的說理十分細緻，先是強調「適當性並不要求系爭規定必須在每一個個案中均達成目的，而是僅要求其具備促進目的實現的效果」，後又將系爭措施與所謂的資料快速凍結程序相互比較，完整回應預防性通信紀錄儲備措施的適當性與必要性審查過程中，可能遭遇的質疑。美中不足的是，6 個月的儲備期間為何是能夠合於比例原則的最上限期間，從聯

[308] Carpenter v. United States, 138 S. Ct. 2206, 2217-2218 (2018).
[309] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 214.

doi:10.6342/NTU202403953

邦憲法法院的說理中並無法清楚得知，不過這可能也是這類涉及期間設定的規範都會產生的問題。

最後，聯邦憲法法院強調，資料儲備與資料調取二者授權基礎之合憲性，應合併觀察，並且透過對於資料調取規定加諸重罪原則、法官保留及相關程序擔保的方式，證述資料儲備授權基礎的合憲性。更直觀地來看，聯邦憲法法院在預防性通信紀錄儲備措施對於人民秘密通訊自由的干預，以及國家安全與重大犯罪之預防、追訴的公共利益之間，做出了明確的決斷，認為後者相較於前者而言更加值得保護。換句話說，在此見解下，基於維護國家安全與重大犯罪之預防、追訴所保護的公共利益，人民必須常態性地承受其通信紀錄受儲備，所帶來私人生活恐遭探知的風險。畢竟，再好的資訊安全措施，都不可能同資料未受儲備一般，完全排除是類風險。此種價值取捨是否合適，端視人民對於政府角色的期待為何。不過，針對這個問題，歐盟法院顯然有不同的看法。

值得關注的是，聯邦憲法法院特別指出：「此次無差別預防性儲備通信紀錄的立法，並不能被視為未來預防性儲備其他有利於防止危險或刑事追訴之資訊的開端；反而應迫使立法者在考慮創設新的資料儲備義務或授權時，必須整體考量現行法下已存在的各種資料儲備而有所克制…公民對於自由的感受（Freiheitswahrnehmung）不允許被全面地捕捉與紀錄，這是德意志聯邦共和國的憲法特質（verfassungsrechtlichen Identität）之一[310]。」對此，學說見解有認為，所謂「有所克制」，是指立法者必須避免經預防性儲備的資訊在現代資訊科技的各種串連下，廣泛且完整地掌握公民的各項活動，進而導致原先基於犯罪追訴或危險預防目的所儲備的資料，反過頭來危害了其應保護的公民自由[311]。因此，未來關於預防性資料儲備的干預措施都必須通過「雙重的比例原則審查」，除了干預措施本身對於人民基本權所造成的干預是否合於比例之外，更應考量現存所有

[310] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 218.
[311] Roßnagel, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238, 1240f. 黃昭元老師於司法院釋字第 603 號解釋強制按捺指紋案中也曾提出相似觀點。參考：黃昭元，前揭註 127，頁 486。

doi:10.6342/NTU202403953

受國家機關預防性儲備的資料，對於公民自由所造成的負擔是否合乎比例原則。有據於此，未來立法者或許只能更換其欲預防性儲備的資料，而不能任意地新增或組合各種預防性資料儲備措施。例如，立法者如果決定仰賴通信紀錄的預防性儲備以打擊犯罪，就不能同時又預防性儲備行車資訊等其他資料，以此避免廣泛且完整地掌握公民的各項活動。也就是說，立法者必須選擇最有效達成犯罪追訴與危險預防的手段，同時也應避免造成各方面的社會監控[312]。

本文認為，所謂「雙重的比例原則審查」，其實是提醒法律人不能僅著眼於個案中該項干預措施所欲儲備的資料，而忽略了各種經預防性儲備的資料相互串聯後，可能共同地產生形塑特定人人格圖像的效果，殊值傾聽。試想，監視錄影畫面本身難以特定個人身分，縱使人民遭受監視器拍攝其日常活動的身影，多半也會因為身分未受暴露而認其私人生活並未受到嚴重揭露；自動車牌辨識系統雖然能透過車籍資料連結至特定人，惟單純以觀，也只是位置資訊，無法顯示出特定人的具體活動內容與對象，縱使受預防性儲備似乎也無傷大雅。不過，將監視錄影畫面與自動車牌辨識系統兩相結合後，不但可以即時且明確得知特定人的位置資訊，更可以清楚檢視其過去一定期間內的日常舉止、社會交往，假使儲備期間並未受到限制，就等同於迫使不具犯罪嫌疑的一般人必須持續承受私人生活遭受探知的風險，一來一往之間，似乎就達到了我國人民極力抗拒的「人臉辨識」之效果？倘若進一步結合通信紀錄，更可以鉅細靡遺地拼湊出特定人的人格圖像。或許，這同時也可以回應慕尼黑高等檢察署所提出的疑問，亦即為何車牌辨識資料相比於通信紀錄，資料敏感性明顯較低，德國立法者卻不願採行「儲存模式」或「記錄模式」等預防性車牌辨識資料儲備措施？原因即在於，在現行法允許預防性儲備通信紀錄的情況下，德國立法者不願意再進一步透過預防性資料儲備措施的立法，廣泛且完整地掌握公民的各項活動，致使原先欲保護的公民自由反而受到這些措施的危害。在我國儲備人民至少一年以上的通信紀錄，以及遍地裝設

312 Roßnagel, (Fn. 311), S. 1240.

doi:10.6342/NTU202403953

監視錄影器的背景下，車牌辨識資料是否得以預防性儲備？又應如何儲備？值得在雙重比例原則審查下的觀點深思。

第四項　歐盟法院 C-293/12 及 C-594/12 裁判

第一款　裁判背景

2006 年指令課予會員國無差別預防性儲備至少 6 個月通信紀錄的義務，不只在德國引發爭議，於其他會員國也產生了經轉換後的內國法是否違反本國憲法，以及 2006 年指令是否合於《歐盟基本權利憲章》對於歐盟人民基本權利保障的質疑。根據歐洲聯盟運作條約（Treaty on the Functioning of the European Union，TFEU）第 267 條規定，歐盟法院對於條約和有關歐盟機構與歐洲中央銀行之法令的有效性與解釋，具有先行裁決權，會員國內國法官於審理案件時發生條約或聯盟機構所制定之法規的效力或解釋問題時，得請求歐盟法院為先決裁判（Preliminary Ruling）[313]。有據於此，2012 年愛爾蘭高等法院（Irisch High Court）及奧地利憲法法院（Österreichischer Verfassungsgerichtshof）面對涉及 2006 年指令的爭議案件，便決定暫時停止訴訟程序，送請歐盟法院為先決裁判，請求其審查 2006 年指令是否合於《歐盟基本權利憲章》第 7 條、第 8 條和第 11 條之意旨。歐盟法院考量兩個案件所涉問題相同，遂合併審理並作成裁判。

第二款　裁判見解

歐盟法院於本裁判的論理可以分為兩個層面：其一，2006 年指令課予會員國無差別預防性儲備 6 個月通信紀錄之立法義務，是否對人民構成《歐盟基本權利憲章》第 7 條、第 8 條和第 11 條之干預；其二，其所構成的干預是否具有合憲性目的？是否合於比例原則？

[313] 翻譯參考：台灣歐洲聯盟研究協會網站，https://www.eusa-taiwan.org.tw/europe_detail/107.htm（最後瀏覽日：04/15/2024）。

doi:10.6342/NTU202403953

第一目 2006 年指令之干預性質

關於 2006 年指令具體干預歐盟人民何種基本權利，歐盟法院首先論述到：系爭指令強制儲存與通訊過程相關的各種類型資訊，使得通訊發送方與接收方的身分、通訊所使用的方法、通訊時間、地點甚至是通訊發生的頻率，都可以透過這些資料得知。這可能進而導致特定人的私人生活，例如每日生活習慣、長期或短暫的住所、日常移動軌跡、活動參與、人際關係以及社交環境，均可被據此推論。有基於此，即使 2006 年指令明確排除通訊實際內容的儲存，也不難想像（not inconceivable）通訊紀錄之預防性儲備會對人民依據《歐盟基本權利憲章》第 11 條行使言論自由產生影響[314]。

另外，2006 年指令預防性儲備通信紀錄的義務，已經損及了由 1995 年指令和 2002 年指令所建立的對於隱私權之保護體系。蓋原先依照 2002 年指令，電信和網路服務業者必須確保通訊的秘密性，並且除為收費目的或取得使用者同意的情形之外，在通信紀錄已非實施通訊所必要時即應立即刪除[315]。在此對於隱私權干預的判斷並無涉於相關資訊是否敏感，或者受干預人是否產生實際的不便利[316]。系爭指令課予電信和網路服務業者在一定期間內無差別預防性儲備通信紀錄的義務，基於通信紀錄與私人生活之間的關聯性，實已干預了人民依《歐盟基本權利憲章》第 7 條所享有私人生活受尊重之權利[317]。同時，2006 年指令第 4 條及第 8 條要求會員國應立法授權經預防性儲備之通信紀錄，得以不受不當遲延的方式儲存並傳輸給有權機關，此種授權國家機關調取資料的規定，也會進一步對《歐盟基本權利憲章》第 7 條構成獨立的干預[318]。此外，由於 2006 年指令涉及個人資料處理，自然也構成《歐盟基本權利憲章》第 8 條個人資料保護之干預[319]。特

[314] Joined Cases C-293/12 & C-594/12, Digit. Rts. Ir. Ltd. v. Minister of Commc'ns, Marine and Nat. Resources, ECLI:EU:C:2014:238, ¶¶ 26-28 (Apr. 8, 2014).
[315] *Id.*, ¶ 32.
[316] *Id.*, ¶ 33.
[317] *Id.*, ¶ 34.
[318] *Id.*, ¶ 35.
[319] *Id.*, ¶ 36.

doi:10.6342/NTU202403953

別值得注意的是，2006 年指令所規範的無差別預防性儲備通信紀錄措施，基於其廣泛（wide-ranging）的影響層面，必須被視為特別嚴重的干預。尤有甚者，在通訊服務使用者未受通知的情況下使用這些預防性儲備的通信紀錄，更有可能讓人民產生其私人生活淪為持續監視之客體的感受[320]。

第二目 2006 年指令未將措施限於「絕對必要」情形

肯定 2006 年指令的干預性質後，歐盟法院接著論述其是否具備干預正當性的問題，並且聚焦於《歐盟基本權利憲章》第 7 條及第 8 條之干預正當性。首先，關於合憲性目的審查，歐盟法院肯認對抗重大犯罪以維護公共秩序，屬於符合憲法要求的公共利益，並舉《歐盟基本權利憲章》第 6 條同時賦予人民享有安全之權利為例，表示 2006 年指令所預防性儲備之電信紀錄，於通訊蓬勃發展的背景下對於犯罪預防與追訴格外重要，故認系爭指令具備合憲性之目的[321]。隨後，歐盟法院開始進行比例原則的審查，並指出：有鑑於系爭指令對於私人生活與個人資料保護的嚴重干預程度，歐盟立法者的裁量權限必須受到限縮，故在此針對 2006 年指令採取嚴格的審查標準[322]。

關於適當性的審查，歐盟法院考量現今電子通訊服務蓬勃發展，其重要性也隨之提升，根據 2006 年指令無差別預防性儲備的通信紀錄能夠提供刑事追訴機關更多機會釐清重大犯罪，故應認此種資料的儲備得以適當達成該指令所追求的目的[323]。而於必要性的審查上，歐盟法院指出：對抗重大犯罪，特別是組織犯罪和恐怖攻擊，雖然對於維護公共安全而言至關重要，卻不能僅憑此等重要公共利益逕自認定系爭無差別儲備通信紀錄之措施具有其必要性。同時，根據歐盟法院穩定的裁判見解，涉及私人生活應受尊重之權利而損害或限制個人資料保護，必

320 *Id.*, ¶ 37.
321 *Id.*, ¶¶ 41-44.
322 *Id.*, ¶ 48.
323 *Id.*, ¶ 49.

doi:10.6342/NTU202403953

須限於「絕對必要（strictly necessary）」的情形始可為之[324]。此種情形下，歐盟相關立法也必須明確界定措施的範圍與應用，並提供一定程度的資訊安全保障，以確保資料遭儲備的受干預人能有效保護其個人資料不受任何非法存取[325]。

由於 2006 年指令預防性儲備通信紀錄的範圍，包括所有類型的電子通訊，並涵蓋所有電信和網路服務的使用者與訂閱者，而事實上及於整體歐盟人民，考量通訊服務對於個人日常生活與日俱增的重要性，歐盟法院據此認為 2006 年指令所欲實施的措施必須同於法院過去穩定的裁判見解，將此種涉及私人生活應受尊重之權利而損害或限制個人資料保護的干預措施，限制在「絕對必要」的情形始可實施[326]，並且基於以下五個主要理由認定 2006 年指令並未滿足此等要求：第一，系爭指令雖致力於對抗重大犯罪，卻並無要求受儲備的資料與公共安全的威脅之間必須具有一定的關聯性，特別是未曾將應預防性儲備的資料範圍限縮在可能涉及重大犯罪的特定期間、特定區域或特定群眾之內，或者是基於特定原因，而可認對於預防、偵查或起訴重大犯罪有所貢獻之人[327]。反而是涵蓋了沒有事實證據指出其行為與重大犯罪之間具有直接或間接甚至是遙遠關聯的一般人，同時也包括在內國法下負有職業保密義務（obligation of professional secrecy）之人[328]。第二，考量是項措施嚴重的干預性質，只有足夠重大的犯罪預防或追訴方能正當化此等資料之利用，但是系爭指令卻交由各會員國自行決定何種犯罪屬於 2006 年指令第 1 條所稱之重大犯罪[329]，也未將資料的調取與後續使用嚴格限制在符合上述目的之情形，只是泛泛地規定應符合必要性與比例原則，更未透過法院或獨立機關的事前審查機制，確保有權機關僅在絕對必要的情形調取資料[330]。第三，指令僅規定通信紀錄之儲備期間應介於 6 個月至 2 年，卻未考量不同類型的通信紀錄對於達成授權目的之有效性（usefulness）有所差異，而應分別對其儲備期間

[324] *Id.*, ¶ 52.
[325] *Id.*, ¶ 54.
[326] *Id.*, ¶ 56.
[327] *Id.*, ¶ 59.
[328] *Id.*, ¶ 58.
[329] *Id.*, ¶ 60.
[330] *Id.*, ¶¶ 61-62.

doi:10.6342/NTU202403953

設定不同長度的限制，甚至也沒有將期間設定建立在具體事實依據之上，難以確保其限於絕對必要的情形[331]。第四，指令第 7 條並未具體規範系爭措施所儲備之巨量資料，其可能具備之資料敏感性或遭受非法存取之風險[332]，且合併觀察 2006 年指令第 7 條、2002 年指令第 4 條第 1 項以及 1995 年指令第 17 條第 1 項，也難以得出系爭措施必須適用特別高資訊安全標準的結論，反而允許電信或網路服務業者在決定資訊安全應適用的標準時，得將經濟成本納入考量[333]，更遑論其不能確保儲備期間經過後，資料是以不可回復的方式被刪除[334]，無法擔保受儲備之資料能有效對抗資料遭無權濫用或非法存取的風險，而違反《歐盟基本權利憲章》第 8 條之保障。第五，根據《歐盟基本權利憲章》第 8 條第 3 項規定，干預個人資料保護之措施應受獨立主管機關監督，然而 2006 年指令卻未見相關規範，無法滿足《歐盟基本權利憲章》對於系爭措施之憲法要求[335]。

最終，歐盟法院基於上述理由，認為 2006 年指定未將預防性儲備通信紀錄的措施限縮在絕對必要的情形，該措施對於《歐盟基本權利憲章》第 7 條及第 8 條所構成的干預，不符合《歐盟基本權利憲章》第 52 條第 1 項之比例原則，而宣告 2006 年指令無效。至於第 11 條言論自由干預的部分則未繼續論述。

第三款　裁判簡評

歐盟法院鑑於涉及私人生活權利之個人資料保護具有獨特的地位，而賦予其僅在「絕對必要」的情形始可干預的限制。然而，若依據歐盟法院於本裁判中認定 2006 年指令不符合「絕對必要」情形的第一點論述，亦即受預防性儲備的資料與公共安全的威脅之間必須具有一定的關聯性[336]，則似乎是徹底排除了無差別預防性儲備通信紀錄之可能。回顧德國聯邦憲法法院於 BVerfGE 125, 260 之見

331 *Id.*, ¶¶ 63-64.
332 *Id.*, ¶ 66.
333 *Id.*, ¶ 67.
334 *Id.*, ¶ 67.
335 *Id.*, ¶ 68.
336 *Id.*, ¶ 59.

doi:10.6342/NTU202403953

解，其於必要性的審查上特別指出，必須考量適時是否具備干預程度較小但同等有效達成目的之手段，並強調「快速凍結」此種有待具體犯罪嫌疑出現後，方開始實施的預防性資料儲備，無法同常態實施的措施一般有效[337]。相較之下，歐盟法院於此則未說明，此種限於具備一定關聯性的「有差別」預防性資料儲備，是否能夠同無差別預防性資料儲備措施一樣有效，而得以據此認定 2006 年指令所設計的措施不具必要性，實屬一論理上之缺漏。本文認為，所謂「絕對必要」的標準，其實是把系爭措施干預基本權的程度限制在一定範圍之內，藉以使其後續得以通過狹義比例原則的審查，不過，歐盟法院於本裁判中，也並未說明倘若未加此一限制，無差別預防性儲備通信紀錄措施於狹義比例原則的審查上，可能會產生什麼問題，實屬可惜。

第五項　歐盟法院 C-203/15 及 C-698/15 裁判

第一款　裁判背景

歐盟法院 C-293/12 及 C-594/12 裁判（下稱：「數位權利裁判」）[338]於 2014 年宣告 2006 年指令溯及失效後便產生了一個爭議，亦即原先會員國將 2006 年指令內容轉換為內國法，並據此課予電信和網路服務業者無差別預防性儲備通信紀錄的義務，此種內國法是否在 2006 年指令被宣告無效之後，即於歐盟法的層次上失所附麗？相關業者是否可以拒絕繼續儲備通信紀錄[339]？2014 年 4 月 9 日，也就是數位權利裁判作成的隔天，瑞典的 Tele2 電信公司（Tele2 Sverige）便向瑞典郵政及電信總局（Swedish Post and Telecom Authority）表示：基於 2006 年指令已被宣告無效，其將停止繼續儲備用戶的通信紀錄，並且將過去已儲備之通信紀

337 Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 208.

338 由於歐盟法院 C-293/12 裁判的原告為愛爾蘭數位權利團體（Digital Rights Ireland），歐盟法院於 C-203/15 及 C-698/15 裁判對其引述時將之稱為“the *Digital Rights* judgment”，本文因此翻譯為「數位權利裁判」。

339 參考：唐欣悅（2019），《私人通信紀錄強制供公益目的使用之合憲性研究》，頁 82-83，國立臺灣大學法律學研究所碩士論文。

doi:10.6342/NTU202403953

錄予以刪除[340]。對此，瑞典司法部的研究報告則認為：數位權利裁判並不能被理解為普遍且無差別的（general and indiscriminate）資料儲備原則上應被禁止（to be condemned），而應具體評估瑞典內國法對於資料儲備的程度，例如資料調取規定、資料儲備期間以及資訊安全保護，方可確認瑞典內國法規定是否合於歐盟法秩序[341]，有據於此，瑞典郵政及電信總局遂向 Tele2 電信公司課予重新開始儲備通信紀錄的義務。Tele2 電信公司則認為此種資料儲備的義務已經違反了《歐盟基本權利憲章》對於人民基本權的保障，並向行政法院提起撤銷訴訟。案經上訴至斯德哥爾摩上訴行政法院（Administrative Court of Appeal of Stockholm, Sweden），法院認為本案涉及歐盟 2002 年指令第 15 條第 1 項的解釋適用，亦即：普遍且無差別地預防性儲備通信紀錄是否合於歐盟 2002 年指令第 15 條第 1 項的規定？若否，則是否會因為具體規範受預防性儲備資料之調取要件、資訊安全措施、儲備期間和刪除義務，而被允許[342]？便裁定停止訴訟程序，送請歐盟法院為先決裁判。

另一方面，英國政府於 2006 年指令被宣告無效後，於 2014 年 7 月另行制定「資料儲備與調查權力法（Data Retention and Investigatory Powers Act，DRIPA）」，授權英國內政大臣（the Secretary of State for the Home Department）得在事前未經司法或獨立行政機關審查的情況下，基於法規授權目的要求任何電信或網路服務業者儲備最多 12 個月的通信紀錄，並且可以在滿足「2000 年調查權力條例法（Regulation of Investigatory Powers Act 2000,RIPA 2000）」的要件，或者是取得法院或獨立行政機關的核准時調取這些通信紀錄。這同樣也引起英國公民的不滿，並向法院提起救濟，案件輾轉經內政大臣上訴至英格蘭及威爾斯上訴法院（Court of Appeal (England and Wales)），法院認為本案亦涉及：（一）數位權利裁判是否僅針對 2006 年指令宣告無效，或者應以裁判中對於《歐盟基本權利憲章》第 7

[340] Joined Cases C-203/15 & C-698/15, Tele2 Sverige and Watson, ECLI:EU:C:2016:970, ¶ 44 (Dec. 21, 2016).
[341] *Id.*, ¶ 46.
[342] *Id.*, ¶ 51.

doi:10.6342/NTU202403953

條及第 8 條保障內涵的闡述，檢視會員國內國法調取受儲備資料之相關授權基礎是否合於《歐盟基本權利憲章》的要求？（二）數位權利裁判是否擴張了《歐盟基本權利憲章》第 7 條及第 8 條的保障範圍，而使其超越歐洲人權法院（European Court of Human Rights）於裁判中對於歐洲人權公約（European Convention of Human Rights）第 8 條所建構的內涵[343]？故亦送請歐盟法院為先決裁判[344]。歐盟法院考量兩案所涉問題相似，遂併案審理。

第二款　裁判見解

第一目　以 2002 年指令規範預防性通信紀錄儲備

本案所涉及的第一個問題是：根據《歐盟基本權利憲章》第 7 條、第 8 條及第 52 條第 1 項保障基本權之意旨，是否應將 2002 年指令第 15 條第 1 項理解為其排除了會員國內國法基於對抗犯罪目的，而普遍且無差別地儲備所有通訊使用者之通信紀錄及位置資訊的立法可能？對此，即有必要檢視「普遍且無差別地儲備通信紀錄」是否落入歐盟法的規範範圍。首先，依據 2002 年指令第 1 條第 3 項規定，本指令不應適用於有關公共安全、國防、國家安全以及刑事法領域的活動；另一方面，第 15 條第 1 項卻規定：「會員國得為維護國家安全、國防、社會安全，或為預防、偵查、確認與追訴犯罪，或防範電信系統的無權使用，於民主社會所必要、適當且合於比例原則的範圍內，立法授權在一定期間內預防性儲備通信紀錄和電信使用者的位置資訊。」兩者合併觀察，似乎有所矛盾，然而歐盟法院指出，於此不能逕自依據 2002 年指令第 1 條第 3 項的規定，認為預防性儲備通信紀錄的措施並非 2002 年指令所規範的範圍，否則，第 15 條第 1 項並不需要特別指出，國家基於何等目的得以採行此種措施；相對的，從 2002 年指令的

[343] 歐盟法院認為先決裁判的正當性只在於能夠有效解決歐盟法解釋適用的問題，而不是在處理一般性或假設性的問題，並表示英格蘭及威爾斯上訴法院所提出的第二個問題無益於 2002 年指令的解釋適用，故不受理。*See Id.*, ¶¶ 126-133.

[344] *Id.*, ¶ 59.

doi:10.6342/NTU202403953

體系觀察，應該將第 15 條第 1 項理解為：會員國基於維護國家安全、國防、社會安全，或為預防、偵查、確認與追訴犯罪，或防範電信系統遭無權使用，而儲備通信紀錄的措施，屬於 2002 年指令第 15 條第 1 項的規範範圍，而且也明確授權會員國僅有在符合指令所規範的要件時，始得為之。

歐盟法院透過上述說理，在 2006 年指令經宣告無效後，將會員國內國法相關的預防性儲備通信紀錄措施，特別是本案所涉及的無差別預防性儲備情形，解釋為 2002 年指令的規範對象，如此即可使相關措施的實施必須合於 2002 年指令的規定內容。隨後，歐盟法院說明：2002 年指令旨在避免任何與通訊相關的資訊遭無權存取，以此保障秘密通訊自由[345]；更欲力求確保《歐盟基本權利憲章》第 7 條、第 8 條的保障[346]，而欲賦予所有通訊方式對於個人資料與隱私的高標準保護[347]，以應對新興科技與自動資料儲存和處理技術的發展[348]，基此，指令第 5 條第 1 項原則上禁止任何人在未獲得使用者同意的情形下儲存其通信紀錄，第 6 條也規定電信或網路服務業者僅可為收費或加值服務目的處理使用者的通信紀錄，並且在目的達成時即須刪除或以不可回復的方式去識別化，第 9 條甚至規定位置資訊只有在特定情形下獲得使用者同意或經去識別化後，方可處理，且上述關於通信紀錄的處理必須在設計上將所需要的資料量嚴格限制在最低限度[349]。由此可見，2002 年指令是以保護通信紀錄不受蒐集、處理為原則，指令第 15 條第 1 項雖然提供了會員國基於上述目的儲備通信紀錄的可能，卻必須被嚴格地解釋適用，絕不能將此種屬於禁止儲備通信紀錄原則的例外情形，反過來視為原則，否則將使指令第 5 條的保障形同具文[350]。

有據於此，歐盟法院考量 2002 年指令第 15 條第 1 項已詳盡地規範會員國得

345 歐盟 2002/58/EC 指令立法說明第 21 點。
346 歐盟 2002/58/EC 指令立法說明第 2 點。
347 *See* Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector /* COM/2000/0385 final - COD 2000/0189 */; Joined Cases C-203/15 & C-698/15, *supra* note 340, ¶ 82.
348 歐盟 2002/58/EC 指令立法說明第 6 點及第 7 點。
349 歐盟 2002/58/EC 指令立法說明第 30 點。
350 Joined Cases C-203/15 & C-698/15, *supra* note 340, ¶ 89.

doi:10.6342/NTU202403953

儲備通信紀錄之目的，基於本條項必須嚴格解釋適用的觀點，就應該認為會員國也只可基於指令所規範之目的儲備通信紀錄[351]，且必須如條文所定符合歐盟法的一般原則，特別是應以合於《歐盟基本權利憲章》對於基本權保障意旨的方式解釋本指令[352]。因此，本案所涉透過內國法強制電信和網路服務業者無差別預防性儲備通信紀錄，以在未來有必要時供有權機關調取的措施，依照數位權利裁判的見解，就會涉及其是否合於《歐盟基本權利憲章》第 7 條、第 8 條以及第 11 條的保障[353]。同時，依據歐盟法院過往的裁判見解，此種涉及私人生活應受尊重之權利而損害或限制個人資料保護的干預措施，也僅有在「絕對必要」的情形始可為之。至此，歐盟法院已經成功地將數位權利裁判中的說理，建構為 2002 指令第 15 條第 1 項的內涵，如此一來便可以使用數位權利裁判中花費許多篇幅闡述的「絕對必要」標準，審視會員國內國法相關的預防性儲備通信紀錄措施。

第二目 無差別預防性儲備通信紀錄逾越「絕對必要」

隨後，歐盟法院將上述標準涵攝於瑞典內國法對於通信紀錄普遍且無差別預防性儲備的規定，再度指出系爭規定並未要求受儲備的資料與公共安全危險之間應具備一定的關聯性，特別是未將預防性儲備的資料範圍限縮在可能涉及重大犯罪的特定期間、特定區域或特定群眾之內，或者是基於特定原因，而可認對於預防、偵查與起訴重大犯罪有所貢獻之人，因此逾越了絕對必要的情形，在民主社會下無法依據 2002 年指令第 15 條第 1 項被視為正當。歐盟法院也強調，2002 年指令第 15 條第 1 項並未阻止會員國透過立法程序，基於對抗重大犯罪的目的，在將資料類型、通訊方式、對象和儲備期間限縮在絕對必要的情形下，實施針對性（target）通信紀錄與位置資訊儲備[354]。受儲備的資料與所欲達成之目的間必須

[351] *Id.*, ¶ 90.
[352] *Id.*, ¶ 91.
[353] *Id.*, ¶ 92.
[354] *Id.*, ¶ 108.

doi:10.6342/NTU202403953

持續地具備一定程度的關聯[355]。關於實際上應如何設定此種針對性通信紀錄儲備措施的標準，會員國立法者必須基於客觀證據認定受資料儲備的對象與重大犯罪之間至少具備間接的關聯性，而可認對於追訴重大犯罪或預防公共安全之重大威脅有所幫助；或者，會員國也可以使用地理位置上的標準界定通信紀錄儲備措施的實施範圍，例如基於客觀事實證據判斷特定區域具備較高程度的風險發生重大犯罪[356]。

第三目　資料調取亦應限於「絕對必要」

另一方面，本案所涉及的第二個問題是：根據《歐盟基本權利憲章》第 7 條、第 8 條以及第 52 條第 1 項，2002 年指令第 15 條第 1 項是否應被解釋為：會員國內國法於設計受儲備通信紀錄之調取規定時，必須基於對抗重大犯罪之目的，並須於事前通過法院或行政獨立機關的審查，且確保資料被保存於歐盟境內？對此，歐盟法院本於上述相同的說理，認為 2002 年指令第 15 條第 1 項必須被嚴格地解釋適用，會員國僅得基於此條項所規定之目的調取受預防性儲備的通信紀錄。同時，雖然 2002 年指令第 15 條第 1 項的用語為「犯罪」，但為了使此等嚴重干預合於比例原則，亦僅有「重大犯罪（serious crime）」的預防、調查、偵查與起訴能夠正當化此種預防性儲備通信紀錄之調取[357]。此外，歐盟法院再次強調此種措施必須限於絕對必要的情形，亦即會員國內國法必須依據客觀標準，制定有權機關能夠在何種情況下調取涉嫌計畫、實施犯罪之人或可能受牽連之人（being implicated）的通信紀錄。而在有權機關為保護國家安全或防止恐怖攻擊而調取通信紀錄的情形，則可以另外對於依客觀證據可認有助於打擊此類活動之人的調取通信紀錄[358]。

為了確保內國法所規定的調取要件被確實遵守，除情況急迫外，受儲備通信

[355] *Id.*, ¶ 110.
[356] *Id.*, ¶ 111.
[357] *Id.*, ¶ 115.
[358] *Id.*, ¶ 119.

doi:10.6342/NTU202403953

紀錄之調取必須於事前通過法院或獨立行政機關的審查[359]。同時，若通知資料主體其通信紀錄遭調取的事實，並不會危害有權機關正在進行的調查，就必須立即踐行相關通知[360]。這對於 2002 年指令第 15 條第 2 項保障受干預人救濟權利的意旨也有其必要性[361]。另外，指令第 15 條第 1 項也並未排除指令第 4 條對於資訊安全的保障，考量受儲備通信紀錄的資料敏感性與遭非法存取的風險，電信和網路服務業者必須以適當的科技方法提供一個特別高標準的資訊安全程序，以此確保資料的完整性與秘密性[362]。特別是，內國法必須制定資料儲備期間屆滿即不可回復地刪除的規定[363]，也應設置獨立機關，監督資料調取規定的設計與執行是否符合歐盟法規範，否則即剝奪了人民依《歐盟基本權利憲章》第 8 條第 1 項和第 3 項所享有的權利[364]。

第六項　歐盟法院 C-793/19 及 C-794/19 裁判

第一款　2015 年德國《電信法》修法內容

自從德國聯邦憲法法院 BVerfGE 125, 260 裁判宣告《電信法》第 113a 條、第 113b 條以及《刑事訴訟法》第 100g 條的相關內容，因違反《基本法》第 10 條第 1 項對於人民秘密通訊自由的保障而無效後，德國關於預防性儲備通信紀錄的立法便停滯多年，甚至一度遭歐盟執行委員會（European Commission）指責德國違反 2006 年指令之立法義務，並向歐盟法院提起訴訟求償罰鍰，此爭議最終伴隨著數位權利裁判宣告 2006 年指令無效而落幕[365]。2015 年，德國立法者參考聯邦憲法法院裁判，以及歐盟法院於數位權利裁判的說理，另行制定「引入通信紀錄儲備義務及最高儲備期間法案(Gesetz zur Einführung einer Speicherpflicht und

[359] *Id.*, ¶ 120.
[360] *Id.*, ¶ 121.
[361] *Id.*, ¶ 121.
[362] *Id.*, ¶ 122.
[363] *Id.*, ¶ 122.
[364] *Id.*, ¶ 123.
[365] 李寧修，前揭註 284，頁 108。

doi:10.6342/NTU202403953

einer Höchstspeicherfrist für Verkehrsdaten）」[366]，並於同年 12 月正式生效。值得注意的是，其中仍舊並未依據客觀的事實基礎針對特定的對象儲備通信紀錄，而維持著「普遍且無差別」的預防性通信紀錄儲備。不過，除了這部分以外，本法案確實致力於將數位權利裁判依據《歐盟基本權利憲章》第 7 條、第 8 條及第 52 條第 1 項所提出的私人生活與個人資料應受保護之內涵，貫徹於條文內容。例如：《電信法》第 113b 條第 4 項將行動通訊位置資訊的儲備範圍，限制在通訊開始時的通訊發送方與接收方之位置資訊，而不及於整個通訊過程中雙方全程的位置資訊，藉以降低描繪特定人完整移動軌跡的風險。第 1 項並依據通信紀錄的資料類型制定不同的儲備期間，將位置資訊的儲備期間規定為 4 週；位置資訊以外的通信紀錄則為 10 週。同條第 8 項亦規定儲備期間屆滿後，電信或網路服務業者必須儘快以不可回復的方式刪除相關資料，至遲不得超過期間屆滿後 1 週。同條第 5 項也明確地將通訊內容、網頁瀏覽紀錄（Daten über aufgerufene Internetseite）以及電子郵件服務使用紀錄，排除於本條儲備通訊紀錄義務之範圍。

此外，針對德國聯邦憲法法院與歐盟法院均相當重視的資訊安全保障，第 113d 條規定，具有儲備通信紀錄義務的電信和網路服務業者必須對於受儲備之資料提供符合當前科技發展水準的資訊安全措施，以確保資料免受無權存取，而此處所稱的資訊安全措施應包括：對受儲備資料使用特別安全的加密程序，並將資料儲存在與常規業務分開的特定儲存設備之中，且應將此儲存設備斷網以避免他人透過網路存取，藉此將得以存取資料之人限制在獲得資料控管者授權的對象，最後，獲得資料控管者授權之人，於調取資料時應至少有兩名人員在場（四眼原則）。又，為確保程序上的規定能被確實遵守，第 113e 條基於監督目的規範相關的紀錄義務，亦即對於受預防性儲備通信紀錄之閱覽、複製、修改、刪除和封鎖，都必須紀錄資料存取的時間、人員、目的和類型。而有關通信紀錄之調取，第 113c 條規定，受儲備之通信紀錄得於刑事追訴機關基於法律規定請求時予以傳輸，用

366 Vgl. BT-Drs. 18/5088.

doi:10.6342/NTU202403953

於特別重大犯罪（besonders schwerer Straftaten）之追訴；或者為防止對個人生命、身體、自由或是對國家或邦存續之具體危險，得基於法律規定傳輸於各邦危險防止機關。於此也再次顯示了，資料的蒐集、儲存、處理和利用都分別構成獨立的個人資訊自決權干預，必須要基於明確的法律規定授權，方得為之[367]。據此，《刑事訴訟法》第 100g 條也相應地做出修正，而規定了三種類型通信紀錄的調取授權：第一，關於電信或網路服務業者為提供通訊服務或達收費目的，而依《電信法》第 96 條儲存的通信紀錄，刑事追訴機關得於偵查重大犯罪，例如《刑事訴訟法》第 100a 條第 2 項之重罪，或利用電信通訊犯罪之情形，依循相對法官保留予以調取。第二，關於電信或網路服務業者依《電信法》第 113a 條和第 113b 條預防性儲備之電信紀錄，僅可用於追訴第 100g 條第 2 項所列舉之重罪，並適用絕對法官保留。第三，若是偵查機關以基地台為單位調取特定基地台一定期間內全部的通信紀錄，同樣必須視其屬於依《電信法》第 96 條或第 113a 條和第 113b 條儲備之通信紀錄，而適用不同的重罪門檻與法官保留程序。另外，《刑事訴訟法》第 101a 條與第 101b 條也分別課予偵查機關通知資料主體以及作成統計報告之義務。

第二款　裁判背景

雖然《電信法》的新法內容對於儲備期間、儲備資料範圍、資訊安全與調取要件，都做出了一定的限制，但是，由於其仍未對於儲備通信紀錄之對象設定具體的標準，而維持普遍且無差別的通信紀錄儲備，在修法過程中即產生了許多爭議。德國 SpaceNet 網路服務業者認為《電信法》的規定違反了《歐盟基本權利憲章》及《基本法》對於人民基本權利的保障，遂向科隆行政法院（Verwaltungsgericht Köln）提起訴訟，請求法院核發暫時命令（einstweilige

[367] 我國有學者將此種不同階段的資料蒐集、處理和利用均構成干預的情形，稱為「共構式複合性干預」。參考：蔡宗珍，前揭註 151，頁 73。

doi:10.6342/NTU202403953

Anordnung），以免除其儲備通信紀錄之義務[368]。案經一審法院駁回聲請後[369]，上訴至北萊茵威斯特法倫邦高等行政法院（OVG NRW, Higher Administrative Court of North-Rhine Westphalia），高等行政法院認為此次修法強制電信和網路服務業者儲備通信紀錄的對象，不但並未要求受儲備的資料與對抗重大犯罪或防止嚴重危險此等所欲追求之目的間具備關聯性，反而在未對儲備通信紀錄的群體、時間和地點做出限制的情形下，無差別地（unterschiedslos）幾乎涵蓋了所有的通訊服務使用者，從《歐盟基本權利憲章》第 7 條、第 8 條及第 52 條第 1 項的觀點來看，無法合於歐盟 2002 年指令第 15 條第 1 項的規定[370]，且認為《電信法》儲備通信紀錄的相關規定屬於對電信和網路服務業者依《歐盟基本權利憲章》第 16 條享有營業自由的干預，此等干預僅有在符合第 52 條第 1 項比例原則時始為正當[371]，故最終核准 SpaceNet 暫時命令之聲請，排除其在訴訟程序結束之前遵循《電信法》儲備通信紀錄的義務。

案經上訴至德國聯邦最高行政法院（Bundesverwaltungsgericht），聯邦最高行政法院認為本案涉及《歐盟基本權利憲章》第 7 條、第 8 條及第 52 條第 1 項一方面保障人民私生活不受侵擾與個人資料受保護的權利，另一方面於第 6 條規定人民亦享有安全的權利，且《歐洲聯盟基本條約》第 4 條將涉及國家安全的事務劃分為各會員國自身的權限範圍，則在綜合觀察上述條文後，是否應將 2002 年指令第 15 條解釋為：會員國內國法於規範電信或網路服務業者儲備通信紀錄之義務時，倘若並未要求受儲備之資料必須「具備時間或地點上的特定原因」，則縱使於儲備範圍明確排除了通訊實際內容、網頁瀏覽紀錄、電子服務使用資料或可能透露與社會或教會（social or ecclesiastical sphere）特殊關連的資料，且將位置資訊的儲備期間限制為 4 週，位置資訊以外的通信紀錄儲備期間為 10 週，同時賦予有效確保資料免遭無權使用的保護措施，並且除 IP 位址以外，僅將受預

368 唐欣悅，前揭註 339，頁 96。
369 Vgl. VG Köln, 25.01.2017 - 9 L 1009/16.
370 OVG Nordrhein-Westfalen, Beschluss vom 22.06.2017 - 13 B 238/17, Rn. 39.
371 OVG Nordrhein-Westfalen, Beschluss vom 22.06.2017 - 13 B 238/17, Rn. 131.

doi:10.6342/NTU202403953

防性儲備之通信紀錄用於特別重大犯罪之追訴，或是對個人生命、身體、自由或是對國家或邦存續具體危險之防止；此等預防性儲備通信紀錄之立法，是否仍為2002年指令第15條所禁止？有基於此，聯邦最高行政法院遂裁定停止訴訟程序，送請歐盟法院為先決裁判[372]。歐盟法院考量本案與德國電信（Telekom Deutschland）所涉及的另一案件爭點相似，故合併審理。

第三款　裁判見解

第一目 通信紀錄以不受儲備為原則

指令內容的解釋適用，不能只囿於文義，更應考量指令的背景和目標，特別是指令之所以被制定的緣由[373]。基此，歐盟法院本於與2016年C-203/15及C-698/15裁判（下稱：*Tele2*案）相似的論理方式，透過引述2002年指令的相關條文及立法說明（recital），表示2002年指令旨在確保人民不論使用何種技術的電子通訊服務，其個人資料與隱私均能受到高標準的保護，藉以實現《歐盟基本權利憲章》第7條、第8條之保障[374]。因此，2002年指令是以通信紀錄維持匿名且不受儲備為原則，指令第15條第1項作為指令第5條、第6條和第9條所提供之保障的例外規定，就必須受限於嚴格的解釋，絕不能反過來將此種禁止儲備通信紀錄原則下的例外規定解釋成原則，否則將使指令第 5 條形同具文[375]。此外，有鑑於通信紀錄的資料敏感性，其可能會揭露受干預人有關私人生活不同方面的資訊，其中甚至包括了歐盟法所特別保護的資訊，如個人的性傾向、政治意見、宗教、哲學、社會或其他信仰以及健康狀況。若是整體觀察這些持續累積的通信紀錄，可能進而導致特定人的私人生活，例如每日生活習慣、長期或暫時住所、日常移動軌跡、活動參與、社交關係以及社交環境，均可被據此推論，甚至

372 Vgl. BVerwG, 25.09.2019 - 6 C 13.18.
373 Joined Cases C-793/19 & C-794/19, SpaceNet AG, Telekom Deutschland GmbH v. Bundesrepublik Deutschland, ECLI:EU:C: 2022:702, ¶ 49 (Sept. 20, 2022).
374 歐盟2002/58/EC指令立法說明第2點、第6點和第7點。
375 Joined Cases C-793/19 & C-794/19, *supra* note 373, ¶ 57.

doi:10.6342/NTU202403953

能勾勒出特定人的人格圖像（profile），因此從隱私權的觀點來看，通信紀錄的資料敏感性並不下於實際的通訊內容[376]。有基於此，儲備通信紀錄的措施構成了《歐盟基本權利憲章》第 7 條、第 8 條之干預，同時也妨礙了通訊服務使用者行使其受《歐盟基本權利憲章》第 11 條保障之言論自由[377]。

當然，《歐盟基本權利憲章》第 7 條、第 8 條及第 11 條所保障之基本權利並非絕不能受到干預，依照 2002 年指令第 15 條第 1 項，會員國內國法仍得基於保護國家安全和追訴重大犯罪之目的，在民主社會下符合適當性、必要性與衡平性的情形儲備通信紀錄。然而應注意的是，指令立法說明第 11 點特別指出：考量此等措施的性質，其必須與所欲達成的目的之間嚴格地符合比例原則[378]。又，基於歐盟法院過去的裁判見解，涉及私人生活應受尊重之權利而損害或限制個人資料保護的干預措施，僅在「絕對必要」的情形始可為之，更必須權衡此等干預所追求的公共利益與其影響的基本權利[379]。具體而言，於此必須衡量儲備通信紀錄對於 2002 年指令第 5 條、第 6 條和第 9 條造成限制的嚴重程度，並且視其與所欲追求的公共利益之間相互權衡下是否符合比例原則[380]。為了滿足比例原則審查的要求，立法者必須對於措施的範圍與應用制定清楚且精確的規範，更必須具體指出在何種情形下，此等儲備通信紀錄的措施會被施行，以將其限制在絕對必要的情形[381]。有據於此，會員國內國法儲備個人資料的措施，受儲備的資料與所欲追求的目的之間都必須基於客觀標準存在一定的關聯性[382]。

第二目 無差別儲備通信紀錄之容許性

由歐盟法院上述立場可以得知，其認為 2002 年指令是以保護通信紀錄不受

376 *Id.*, ¶ 61.
377 *Id.*, ¶ 62.
378 *Id.*, Recital 11, "[S]uch measures must be appropriate, 'strictly proportionate' to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."
379 *Id.*, ¶ 67.
380 *Id.*, ¶ 68.
381 *Id.*, ¶ 69.
382 *Id.*, ¶ 70.

doi:10.6342/NTU202403953

儲備為原則，若是對其儲備則違反了 2002 年指令第 5 條、第 6 條及第 9 條的保障，並構成對於《歐盟基本權利憲章》第 7 條、第 8 條及第 11 條之干預。而在邏輯上對於儲備通信紀錄所構成的干預情形，可以區別為：並未區分資料受儲備對象的「無差別通信紀錄儲備」；以及依具體標準針對特定對象儲備資料的「針對性通信紀錄儲備」。由於前者並未區分通信紀錄受儲備的對象，不考量受干預人是否具有犯罪嫌疑，因此屬於一種普遍性、預防性的措施；後者則視其所設定的標準，而可能是預防性，或是針對具有犯罪開始嫌疑之人而帶有刑事追訴的性質。

其中，對於本案系爭規定是否合於《歐盟基本權利憲章》至關重要者，正是「無差別預防性通信紀錄儲備」是否以及在何種要件下，得以正當化實施？對此，歐盟法院根據措施所欲追求的公共利益，得出不同的結論。其認為：2002 年指令第 15 條第 1 項所列舉的目的之間，在比例原則的觀點下，基於其各自的重要性而有著階級（hierarchy）上的差異。因此，考量維護國家安全的重要性明顯超越 2002 年指令第 15 條第 1 項所列舉的其他目的，歐盟法院認為根據《歐盟基本權利憲章》第 7 條、第 8 條、第 11 條和第 52 條第 1 項，其並未排除會員國內國法，基於維護國家安全之目的，於國家安全遭逢真實存在或可預見（genuine present or foreseeable）的重大威脅時，普遍且無差別地預防性儲備通信紀錄與位置資訊，並且透過有效的法院或獨立行政機關審查，確認此等威脅真實存在、相關的要件與保障措施已被滿足，且儲備期間被限制在絕對必要的情形，僅在威脅持續存在時才得以延長[383]。

至於會員國內國法若是基於預防、偵查、確認與追訴犯罪之目的而儲備通信紀錄，首先基於比例原則的考量，應僅有為對抗重大犯罪，方可正當化儲備通信紀錄措施對於《歐盟基本權利憲章》第 7 條和第 8 條的嚴重干預[384]。其次，歐盟法院認為：若基於此等目的而欲普遍且無差別地預防性儲備通信紀錄，則已超出

[383] *Id.*, ¶ 72.
[384] *Id.*, ¶ 73.

doi:10.6342/NTU202403953

了「絕對必要」的情形，而無法依照 2002 年指令第 15 條第 1 項，在民主社會中被認為是合理的措施[385]。原因在於：如前所述，通信紀錄的秘密性從隱私權的觀點而言至關重要，儲備通信紀錄對於人民行使《歐盟基本權利憲章》第 7 條私生活受保護的權利與第 11 條言論自由，會產生嚇阻的效果（dissuasive effect），考量儲備通信紀錄嚴重的基本權干預性質，歐盟法院認為有必要依據 2002 年指令所建構的體系，將此等措施的實施視為民主社會下的例外情形，而並非原則。因此，縱使是為了對抗重大犯罪或預防對公共安全的嚴重威脅，此等重要的公共利益，通信紀錄也不應該被系統性且持續性地儲備。

建立上開論證依據後，歐盟法院開始審查德國《電信法》系爭條文的正當性，並指出：系爭條文事實上仍然維持普遍且無差別的預防性通信紀錄儲備。原因在於：儘管系爭規定於通訊資料的儲備範圍排除了通訊實際內容、網頁瀏覽紀錄，並且僅在行動通訊開始時留存所使用基地台的位置資訊，依然不影響其所儲備之通信紀錄，能夠準確推論特定人私人生活的性質。例如，系爭規定雖然排除網頁瀏覽紀錄的儲備，卻課予網路服務業者儲備使用者 IP 位址的義務，而 IP 位址事實上可用於追蹤使用者完整的「點擊流（clickstream）」[386]，並得知使用者全部的線上活動，掌握此等資訊也足以建立使用者詳盡的人格圖像，而構成對於《歐盟基本權利憲章》第 7 條和第 8 條的嚴重干預[387]。且從 SpaceNet 的書面報告也可得知，系爭規定雖然排除電子郵件紀錄的儲備，卻也只佔了整體通信紀錄非常小的一部分[388]。此外，觀察德國聯邦政府提供的資料，僅有 1,300 個公民、政府機關或是社會或宗教團體，依《電信法》第 113b 條第 6 項被排除於通信紀錄儲備的對象，相比於德國整體的通訊服務使用者僅佔一小部分，更未排除律師、醫師或新聞工作者等具有職業保密義務之人。有基於此，系爭規定之通信紀錄儲備措

385 *Id.*, ¶ 74.
386「點擊流」可以清楚記錄網路服務使用者在同一頁面，以及不同頁面之間的活動（點擊）紀錄，參考：江義平、許蕙婷（2014），〈網路使用者日常線上資訊行為之探勘研究〉，《電子商務研究》，12 卷 1 期，頁 7。
387 Joined Cases C-793/19 & C-794/19, *supra* note 373, ¶ 79.
388 *Id.*, ¶ 80.

doi:10.6342/NTU202403953

施，實際上涉及了全體人民，不顧其甚至不具備與刑事追訴目的之間接關聯性，而等同於課予了電信和網路服務業者，不具理由、並未依照群眾、時間或地點因素作出區別之無差別預防性儲備通信紀錄的義務，因此不能被視為是針對性資訊儲備措施。

另一方面，關於系爭規定對於儲備期間的限制以及資訊安全措施的保障，是否得以正當化此種普遍且無差別地儲備通信紀錄的措施，歐盟法院表示：將儲備通信紀錄限制在一定的期間內，確實是其得以依 2002 年指令第 15 條第 1 項正當化實施的關鍵因素，系爭規定將通信紀錄的儲備期間依據其是否屬位置資訊而區別為 4 週和 10 週，相較於 *Tele2* 案中瑞典《電信法》之儲備期間的確明顯縮短[389]。然而，儲備通信紀錄措施的嚴重干預性質，主要是源自於其儲備資料的數量與類別，進而導致整體觀察此等資料時得以精準地推論特定人的私人生活[390]。據此，對於通信紀錄的儲備，不論時間長短皆屬於嚴重的干預。雖然通信紀錄之儲備事實上是否對個人私生活的權利造成影響，必須實際調閱受儲備的資料始可得知，而似乎在比例原則的權衡上產生障礙，但是這仍不影響儲備通信紀錄產生資料遭濫用之風險所構成的基本權干預性質。歐盟法院於此也參考了鑑定意見，認為儲備 10 週之通信紀錄以及 4 週之位置資訊仍舊分別產生了準確推論特定人私人生活的可能[391]。此外，歐盟法院也強調，縱使系爭規定依循歐盟法院過去的裁判見解，提供了充分的資訊安全保障，在本質上（by its very nature）仍然無法消除甚至是彌補普遍且無差別的通信紀錄儲備措施對於 2002 年指令第 5 條、第 6 條以及《歐盟基本權利憲章》第 7 條、第 8 條和第 11 條的嚴重干預性質[392]。最後，雖有論者主張對於特別重大犯罪的處理方式應該同於面對國家安全威脅，然而歐盟法院表示：保護國家安全的重要性在於，透過預防和處罰如恐怖攻擊般，足以破壞基本憲政秩序或是國家的政治、經濟或社會結構之行為，甚至是直接對

389 *Id.*, ¶¶ 85-86.
390 *Id.*, ¶¶ 87-88.
391 *Id.*, ¶¶ 89-90.
392 *Id.*, ¶ 91.

doi:10.6342/NTU202403953

社會、人民或國家本身造成威脅之活動，而據以保護國家的重要功能和社會的主要利益。因此不同於犯罪，甚至是特別嚴重的犯罪，對於國家安全的威脅必須是真實存在，或者至少是可預見的，始可基於足夠具體的事實情境，正當地在一定期間內普遍且無差別地儲備通信紀錄與位置資訊。同時，也基於國家安全威脅嚴重且具體的本質，而與影響公共安全甚至是發生重大犯罪的一般性、常態性（general and permanent）風險有所區別[393]。基此，特別嚴重的犯罪不得與國家安全威脅為相同處理，否則等同於在國家安全與公共安全之間創設一個新的類別，並且將對於國家安全的相關要求套用於其中[394]。

第三目 無差別儲備通訊使用者資料及 IP 位址之容許性

論述至此，歐盟法院徹底排除了基於危害防止或刑事追訴目的，普遍且無差別地預防性儲備所有類型之通信紀錄的可能性。隨後，歐盟法院表示，刑事追訴的有效性並不會只仰賴一種偵查方式，而是所有可能的偵查方式，並指出根據《歐盟基本權利憲章》第 7 條、第 8 條、第 11 條和第 52 條第 1 項，2002 年指令第 15 條第 1 項並未排除會員國為了對抗重大犯罪或預防對公共安全的嚴重威脅，而於以下四種情形預防性儲備通訊相關資訊[395]：第一，普遍且無差別地儲備通訊服務的使用者資料；第二，在絕對必要的期間內，普遍且無差別地儲備分配予網路連線來源端的 IP 位址；第三，基於客觀且非歧視性的因素，根據群眾類型，或者使用地理位置上的標準，在絕對必要的期間內實施針對性的通信紀錄與位置資訊儲備（the targeted retention of traffic and location data）；第四，依據有權機關的決定，要求電信或網路服務業者在特定期間內快速凍結（expedited retention / quick freeze）其所保有的通信紀錄和位置資訊，並且於事後接受有效的司法審查。

首先，由於 2002 年指令並未賦予「通訊服務使用者資料」特別的保障，因

393 *Id.*, ¶¶ 92-93.
394 *Id.*, ¶ 94.
395 *Id.*, ¶ 75.

doi:10.6342/NTU202403953

此指令自然並未禁止會員國內國法為了對抗重大犯罪或預防對公共安全的嚴重威脅，甚至是一般程度的犯罪或威脅，而普遍且無差別地儲備所有通訊服務的使用者資料。不過，有疑義的是，歐盟法院於先前論述方強調 IP 位址事實上可以用於追蹤使用者完整的「點擊流（clickstream）」，並藉以得知使用者全部的線上活動，而認為對 IP 位址普遍且無差別地預防性儲備，構成對《歐盟基本權利憲章》第 7 條和第 8 條的嚴重干預，甚至阻礙人民行使受第 11 條保障之言論自由，為何此處卻產生與其他通信紀錄無差別儲備情形不同的結論呢？對此歐盟法院表示，考量網路犯罪，特別是於網路上取得、散播、傳輸或提供兒童色情製品的情形[396]，IP 位址可能是唯一能夠調查行為人身分的手段，為了在系爭基本權利之間取得必要的平衡，最終認為 2002 年指令第 15 條第 1 項並未排除會員國內國法基於對抗重大犯罪、預防對公共安全的嚴重威脅，或是保護國家安全之目的，於嚴格限制資料調取授權規定的前提下，在絕對必要的期間內，僅針對 IP 位址普遍且無差別地預防性儲備，不以受干預人與所欲達成的目的之間具備間接關聯性為必要[397]。

第四目 針對性通信紀錄儲備

另外，歐盟法院指出部分會員國於爭執無差別儲備通信紀錄之必要時，對於所謂「針對性通信紀錄儲備」的理解過於限縮。蓋依據《歐盟基本權利憲章》第 7 條、第 8 條、第 11 條和第 52 條第 1 項解釋 2002 年指令第 15 條，並不會將針對性通信紀錄儲備的範圍，限制在重大犯罪已發生後，警方判斷其可能的發生地點，或是已產生犯罪嫌疑之特定人[398]。相反的，會員國內國法得基於客觀證據，於特定群眾的通信紀錄和位置資訊與重大犯罪之間至少具備間接的關聯性，而得

[396] 特別是歐盟 2011/93 指令第 2 條定義下的「兒童色情製品（child pornography）」。*See* Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.
[397] Joined Cases C-793/19 & C-794/19, *supra* note 373, ¶¶ 100-103.
[398] *Id.*, ¶ 104.

doi:10.6342/NTU202403953

以對於追訴重大犯罪或防止對公共安全的重大威脅有所貢獻時，予以針對性地儲備[399]。而鑒於實施針對性通信紀錄儲備的不同目的，例如重大犯罪之預防、偵查、確認或起訴，可能受到針對性資料儲備的對象就會是在這些程序當中，基於客觀且非歧視性的因素而被特定之人，例如當下正受到警方偵查或其他監視措施的被告，或是雖然適時不具備重大犯罪之開始嫌疑，但具有重大犯罪前科紀錄且再犯可能較高者[400]。

此外，會員國立法者也可以選擇使用地理位置上的標準，於合於比例原則的情形實施針對性通信紀錄儲備。例如基於客觀且非歧視性的事實依據，而可認某地區具有準備或實施重大犯罪的高程度風險，包括過去曾發生多起重大犯罪的區域，或是像經常接待大量遊客的地點或設施，此種特別容易遭受重大犯罪的場所，又或者是重要戰略位置（strategic location），如機場、車站、港口或公路收費站[401]。由此可知，所謂針對性通信紀錄儲備之立法模式，亦不限於有權機關已掌握具體跡象指出特定地區正在準備或已經發生重大犯罪，而包含了依據某地區的平均犯罪率，此種客觀且非歧視性的因素，而在一定期間內針對特定地區的群眾，預防性地在其尚不具備犯罪嫌疑時儲備其通信紀錄與位置資訊[402]。此種地理位置上的限制應隨著情況不同而有所調整，以有效對抗重大犯罪，也必須將儲備期間限制在絕對必要的情形[403]。儘管針對性通信紀錄儲備，因為需要對於可受儲備的群眾與區域提供詳盡的標準，而可能在施行上有所困難，會員國仍應遵循 2002 年指令的誡命，切勿將儲備通信紀錄之例外規定轉變為原則，而反過來實施普遍且無差別的通信紀錄與位置資訊儲備[404]。

399 *Id.*, ¶ 105.
400 *Id.*, ¶¶ 106-107.
401 *Id.*, ¶ 108.
402 *Id.*, ¶ 109.
403 *Id.*, ¶ 111.
404 *Id.*, ¶ 113.

doi:10.6342/NTU202403953

第五目 通信紀錄之快速凍結

基於 2002 年指令第 6 條，一旦通信紀錄不再為通訊服務所需，電信或網路服務業者原則上就必須將其刪除或是去識別化，例外基於收費目的，或是經使用者同意而提供加值服務或用於行銷的情形，電信或網路服務業者得繼續留存其通信紀錄至目的達成的時點。換句話說，事實上電信或網路服務業者可能基於上述原因，而留存通訊服務使用者一定期間內的通信紀錄。倘若在此期間結束時產生了繼續儲備這些通信紀錄的必要情形，歐盟法院表示：2002 年指令第 15 條第 1 項並未排除會員國立法授權有權機關依據事後將受有效司法審查的決定，要求電信或網路服務業者在一定期間內快速留存或凍結其適時仍保有的通信紀錄[405]。而依據《歐盟基本權利憲章》第 8 條第 2 項規定，個人資料的處理應基於具體明確之目的，會員國立法者於此也必須為快速凍結通信紀錄的授權規定，制定明確之實施目的，並且在目的達成後將受儲備之通信紀錄刪除[406]。且考量快速凍結通信紀錄對於《歐盟基本權利憲章》第 7 條和第 8 條構成嚴重的干預，也應認僅有為對抗重大犯罪和維護國家安全此等重要公益，並且將資料調取限制在絕對必要的情形下，始可正當化此種措施的實施[407]。

歐盟法院也強調：快速凍結通信紀錄的對象，並不限於已經被認定為對於公共安全或國家安全造成威脅之人，或者是已具備重大犯罪或破壞國家安全之開始嫌疑者；而是可以於絕對必要的情形，及於有助於釐清犯罪事實之人，例如被害人、被害人的朋友或是同事，具體來說可能是在對於公共安全的威脅或是重大犯罪發生之前，與被害人有過通訊聯繫之人[408]。此外，快速凍結通信紀錄的範圍也可能是以地理位置為標準，例如預備實施或已發生重大犯罪，或是準備危害國家安全的可疑地點，又或者是重大犯罪被害人失蹤的位置[409]。警察機關也可以在偵

405 *Id.*, ¶¶ 114-115.
406 *Id.*, ¶ 116.
407 *Id.*, ¶ 116.
408 *Id.*, ¶¶ 117-118.
409 *Id.*, ¶ 119.

doi:10.6342/NTU202403953

查犯罪的初期即使用此等措施，加強偵查的效率[410]。

第四款　後續發展

根據《電信現代化法案》（Telekommunikationsmodernisierungsgesetz），德國自 2021 年 12 月 1 日起，將先前的《電信法》第 113a 條移至第 175 條、第 113b 條改為第 176 條[411]。然而，在此過程中並未針對條文進行實質性修訂，仍維持普遍且無差別的預防性通信紀錄儲備[412]。伴隨歐盟法院作成先決裁判，德國聯邦最高行政法院也依循其見解，認為德國《電信法》第 175 條第 1 項第 1 句，以及第 176 條課予電信或網路服務業者儲備通信紀錄之義務，由於並未透過客觀標準，使受儲備的通信紀錄與所欲追求之目的間存在一定的關聯性[413]，且其所授權普遍且無差別儲備之 IP 位址，並非僅用於重大犯罪之追訴或對公共安全嚴重威脅之防止[414]，而違反了歐盟法院對於 2002 年指令第 15 條第 1 項的解釋。據此，基於歐盟法優先原則（Grundsatzes des Vorrangs des Unionsrechts），聯邦最高行政法院認為上述規定不予適用（kommen nicht in Betracht）[415]，免去了電信和網路服務業者預防性儲備通信紀錄之義務。

有基於此，雖然德國《刑事訴訟法》第 100g 條第 2 項仍保有通信紀錄之調取規定，授權偵查機關得在符合法定要件下調取依《電信法》第 176 條預防性儲備之通信紀錄，然而，由於電信和網路服務業者已無儲備之義務，此種通信紀錄是否得以順利調取，遂成偶然[416]。

---

410 *Id.*, ¶ 120.
411 Vgl. Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz - TKMoG).
412 Bär, in: Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 50. Aufl. 2024, TKG § 176.
413 Vgl. BVerwG, Urteil vom 14.08.2023 - 6 C 7.22 -, Rn. 39.
414 Vgl. BVerwG, Urteil vom 14.08.2023 - 6 C 7.22 -, Rn. 42.
415 Vgl. BVerwG, Urteil vom 14.08.2023 - 6 C 7.22 -, Rn. 46.
416 Bär, (Fn. 412), StPO § 100g.

doi:10.6342/NTU202403953

第五款　裁判簡評

歐盟法院於本案透過 2002 年指令的整體架構，認為指令第 15 條關於會員國得立法授權有權機關基於維護國家安全、國防、社會安全，或為預防、偵查、確認與追訴犯罪，或防範電信系統的無權使用，而儲備通信紀錄與位置資訊，屬於一例外規定，而必須受限於例外從嚴解釋。隨後，又指出上述目的之間具有階級上的差異，維護國家安全之目的明顯較其他目的重要，因此會員國內國法於面臨真實存在或可預見的國家安全威脅時，為維護國家安全得在絕對必要的期間內普遍且無差別地儲備通信紀錄；反之，基於其他目的時，由於其不如國家安全威脅般具體，而是一般性、常態性的風險，鑒於 2002 年指令對於原則與例外的設定，而表示會員國內國法縱使是基於追訴重大犯罪或防止對公共安全之嚴重威脅，也不應無差別預防性儲備通信紀錄，否則是把儲備通信紀錄的例外授權轉換為原則性規定，並且破壞國家安全與公共安全之間的階級關係。有疑義的是，梳理通篇判決內容後，似乎只有看到歐盟法院根據系爭措施所保護的公共利益以及所儲備的通訊紀錄種類，作出不同的權衡結論，卻並未看到詳盡的權衡過程，而有違說理義務之嫌。

首先，歐盟法院從儲備通信紀錄措施的干預性質出發，認為此種措施的干預性質是源自於其所儲備的資料數量與類型，導致在整體觀察下會產生得對特定人私人生活作出精確推論的風險，且同時隱含了此等資料遭濫用的危害，而認其屬於對《歐盟基本權利憲章》第 7 條、第 8 條和第 11 條的嚴重干預。然而另一方面卻又指出，縱使對於儲備此等資料的設備提供完善的資訊安全措施，在本質上也無法減緩甚至彌補此種措施的干預性質。本文同意歐盟法院此處的論述，蓋原先應遭刪除的資料，若非國家機關的相關措施根本不會受到儲備，進而產生遭受揭露及濫用的風險，且縱使具備完善的資訊安全措施，實際上也無法完全抹去受儲備之資料被政府官員無權濫用，或者是遭外部駭客非法存取的風險，因此即使具備符合當代技術水準的資訊安全設備，對於資料儲備措施干預程度上的減緩仍

doi:10.6342/NTU202403953

有其極限，蓋人民對於政府的不信賴，以及面對科技發展下持續出現的新興資料竊取技術所產生的恐懼，確實會使通信紀錄受預防性儲備、且資料調取不透明的情形影響其基本權利之自由行使。

然而，若是在面對真實存在或可預見的國家安全威脅時，於歐盟法院的見解下仍可普遍且無差別地儲備通信紀錄，就代表此種因資料恐遭濫用的風險所構成的基本權干預，並非絕對不能在與重要公共利益相互權衡後，被正當地干預[417]。歐盟法院僅憑國家安全與公共安全之間的階層關係，就得出了會員國內國法縱使是基於追訴重大犯罪或防止對公共安全之嚴重威脅，也無法無差別預防性儲備通信紀錄的權衡結論，本文認為稍嫌速斷，而有先射箭再畫靶之嫌。具體而言，歐盟法院於此至少要回答兩個問題：其一，於必要性審查的層次，歐盟法院必須說明其所提供的立法可能，包括 IP 位址的無差別儲備以及通信紀錄之快速凍結，在綜合利用下是否屬於與無差別儲備所有通信紀錄的措施，同等有效達成目的之手段？其二，於狹義比例原則審查的層次，歐盟法院必須具體權衡會員國內國法為追訴重大犯罪或防止對公共安全的嚴重威脅，是否在任何長度的期間內儲備通信紀錄，均無法通過狹義比例原則之審查？

關於第一個問題，德國聯邦憲法法院於 BVerfGE 125, 260 的見解明顯與歐盟法院有所不同，聯邦憲法法院認為「快速凍結」程序只有在相關通信紀錄尚未經刪除時，才有機會取得其核准實施時點以前的通信紀錄，而不如持續性儲備措施般能確保過去一定期間內完整的通信紀錄受到留存[418]，且考量通訊過程在一般情況下並不會為他人知悉，一經刪除則難以透過證人指述或其他方式重建過去所發生的事實，而認為無差別預防性儲備通信紀錄的措施有其必要性。相對於此，歐盟法院在通信紀錄儲備的不同立法可能之間，彼此在達成目的上是否同等有效，就未見其說明。例如歐盟法院於判決中不斷強調針對性儲備通信紀錄的標準，必

[417] Sandhu, Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union, EuR 2017, 453, 463.
[418] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 208.

doi:10.6342/NTU202403953

須基於客觀且非歧視性的因素，就不禁令人懷疑針對性儲備通信紀錄措施的法律明確性和有效性之間是否會互相衝突[419]。此外，或有見解認為，由於實務上電信或網路服務業者基於收費或提供加值服務的目的，均會在一定期間內留存使用者的通信紀錄，因而透過通信紀錄之快速凍結程序，甚至是搭配 IP 位址之無差別儲備措施，就可以發揮與無差別儲備通信紀錄同等有效的偵查效果[420]。然而，這又會衍生第二個問題，亦即電信或網路服務業者基於收費目的而固定在通訊服務結束後一定期間內留存通信紀錄，這事實上也是一種在尚未懷疑使用者的支付能力或支付意願，即予以實施的無差別預防性通信紀錄儲備[421]。假使電信或網路服務業者基於收費目的，或是為了避免消費者爭執，固定留存一個月，甚至是三個月的通信紀錄，而合於 2002 年指令第 6 條的規定。則會員國基於重大犯罪之偵查或是對公共安全嚴重威脅之防止，此等重要公共利益，而欲無差別預防性地儲備通信紀錄，對比之下勢必在一定期間內亦能合於狹義比例原則。歐盟法院僅憑例外從嚴解釋的說理，就抹去了這種立法可能，亦未見其對於狹義比例原則審查的具體權衡過程，本文認為歐盟法院事實上已經決定了欲在民主社會下排除此種無差別儲備通信紀錄措施的常態施行（射箭），再將 2002 年指令規定上的原則與例外關係作為相關理由（畫靶）。

正如歐盟法院基於 IP 位址對於偵查兒童色情犯罪的必要性，而在權衡過後允許會員國內國法授權有權機關在絕對必要的期間內，普遍且無差別地預防性儲備 IP 位址。其他種類的通信紀錄之預防性儲備，對於特定重大犯罪而言，必然也是偵查過程中關鍵，甚至是唯一的利器。國家安全雖然在位階上優於公共安全，而得以正當化無差別儲備通信紀錄之實施，卻不能以此反面證述，偵查其他重大

[419] 學說上有見解贊同歐盟法院在此情形下，仍限縮於針對性通信紀錄儲備。Vgl. Puschke, Die Vorratsdatenspeicherung – eine (un)endliche Geschichte?, GSZ 2024, 23, 26.

[420] Gutmann/Wollenschläger, Die Vorratsdatenspeicherung von IP-Adressen im Spannungsfeld von Freiheit und Sicherheit: verfassungsrechtlicher Rahmen und konkrete Ausgestaltung, GSZ 2023, 249, 251.

[421] Bull (2023), Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit – Rasterfahndung, Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung und Antiterrordatei in der Rechtsprechung des Bundesverfassungsgerichts, S. 17, in: https://link.springer.com/referenceworkentry/10.1007/978-3-658-37532-4_52-1. （最後瀏覽日：04/22/2024）

doi:10.6342/NTU202403953

犯罪，或是防止對公共安全之嚴重威脅的公共利益，無法正當化此等措施之實施。歐盟法院於會員國已大幅縮短資料儲備期間，並提供充分資訊安全措施的情形下，仍完全抹煞會員國內國法自行決定是否採行無差別預防性儲備通信紀錄之立法可能，此舉是否恰當？實有可議之處。

第三節　我國預防性儲備車牌辨識資料之容許性

梳理完歐盟法院對於預防性通信紀錄儲備的觀點後，結合前述德國聯邦憲法法院對於自動車牌辨識系統干預正當性的討論，本文以下嘗試將法院論述過程中所提出的審查標準，合併於比例原則的架構中，具體檢視我國自動車牌辨識系統並未區分行經車輛是否具犯罪嫌疑，一律預防性地儲備其車牌辨識資料的措施，在憲法層次上是否具備容許性；若是，在狹義比例原則的層面上又應該具備那些要件，方可通過審查？

第一項　合憲性目的

警察機關使用自動車牌辨識系統「識別行經車輛之車牌號碼」、「將資料儲存至資料庫內」以及「即時與涉案車輛名單相互比對」，分別屬於對個人資料的蒐集、處理與利用行為，於我國法下均獨立構成對個人資訊隱私權（資訊自決權）之干預，已如前述。關於此等預防性資料儲備措施之合憲性目的審查，參照德國聯邦憲法法院所言，尚未產生具體事由下即預防性地儲備個人資料，並非為憲法所絕對禁止；相對的，應該被嚴格禁止的是基於不特定且尚未能特定之目的所實施的個人資料儲備[422]。有基於此，判斷重點就會在於系爭授權基礎的設計上，對於此種尚未出現具體事由即預防性施行的資料儲備，是否在後續資料利用的授權上，能夠限於特定的目的。因此，倘若我國自動車牌辨識系統之相關授權基礎，能將資料儲備以及嗣後資料利用之目的明確限於犯罪偵查、危害防止和國家安全

[422] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 206.

doi:10.6342/NTU202403953

維護，則均屬得正當化資訊隱私權干預之合憲目的，不會因為其於具體事由尚未出現時即預防性地儲備資料而有所不同。

第二項　適當性

我國自動車牌辨識系統固定設置於各縣市重要路口以及高速公路之出入口，並搭配裝置於警用車輛和智慧戰警頭盔之「移動式車牌辨識系統」，廣泛蒐集資料並長期累積後，得以搭配電腦軟體運算出特定人的完整行車軌跡，並用於追查對犯罪偵查、危險防止和國家安全維護有所貢獻之人的特定行蹤，於實務上甚至可以達到在 2 個小時內尋回失竊車輛的效果[423]，故應認基於上述目的實施自動車牌辨識系統之相關授權基礎具備適當性。此處須特別說明的是，正如德國聯邦憲法法院所言，適當性並不要求系爭授權基礎必須在每一個個案中均達成目的，而是僅要求其具備促進目的實現的效果[424]，因此於預防性儲備通信紀錄的案例中，德國聯邦憲法法院即指出，縱使因為部分犯罪嫌疑人刻意使用網路熱點、外國網路電信服務，或是以假名註冊預付卡門號，而使通信紀錄之預防性儲備措施無法重建特定通訊過程，進而導致刑事追訴機關難以藉此確認通訊使用者身分，也不能據此認定系爭規定不具適當性。同理可證，即使在部分案例中，犯罪嫌疑人透過汙損或變更車牌的方式，致使自動車牌辨識系統無法重建特定車輛的行車軌跡，而難以追查特定犯罪嫌疑人之下落，也不能據此而認自動車牌辨識系統的相關授權規定不具備適當性。

第三項　必要性

關於必要性的審查，於此必須探討除了我國此種並未區分行經車輛是否具備犯罪嫌疑，一律予以蒐集並預防性儲備的實施模式以外，是否具備其他對個人資

[423] 黃佩華、劉俊男，前揭註 44。
[424] Vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 207.

doi:10.6342/NTU202403953

訊自決權干預程度較小但是同等有效的手段。由於自動車牌辨識系統所蒐集的資料不如通信紀錄的類型多元，在邏輯上較難想像僅預防性儲備部分車牌辨識資料的手段，例如僅預防性儲備通訊使用者資料或是 IP 位址的這種立法可能。因此，討論重點就會在於：德國現行法所實施的「追緝模式」以及立法過程中曾討論的「儲存模式」(車牌辨識資料之快速凍結)，這兩種對於自動車牌辨識系統的實施時間與資料儲存對象做出限制的手段，是否與我國實務上一律預防性儲備的施行模式同等有效？

顯而易見地，「追緝模式」和「儲存模式」均無法取得措施開始實施時點以前的車牌辨識資料，而非同等有效之手段。如前所述，犯罪結果並不一定在當下即為他人知悉，試想登山客於爬山過程中發現棄屍，經法醫鑑定死者已經死亡超過 7 日；或是被害人出國旅行兩個月後，返家時才發現屋內一陣凌亂，貴重物品均已遭竊。此等情形若是以「追緝模式」或「儲存模式」實施自動車牌辨識系統，由於犯罪結果發生後經過一段時間方為人所知，行為人適時已不知去向，刑事追訴機關若無法從其他線索特定行為人的身分或車牌號碼，於「追緝模式」下根本無從比對車牌號碼，而於「儲存模式」也會因為行為人早已無影無蹤，難以憑藉犯罪現場的車牌辨識資料儲備，具體掌握犯罪嫌疑人的行蹤甚至是確認其身分；反之，倘若刑事追訴機關常態地預防性儲備車牌辨識資料，則可以依據資料調取的授權規定，在合於比例原則的要件下調取偵查所需資料，例如於「棄屍案」中，調取 7 天前事發當時案發地點附近的車牌辨識資料，連結車籍資料庫後確認其中是否有車主曾與被害人有所往來，進一步產生更多偵查線索；或是於「貴重物品遭竊案」中，先行透過監視錄影畫面查找可疑車輛，特定車牌號碼後調取其車牌辨識資料以描繪完整的脫逃軌跡，藉此於犯罪嫌疑人跨縣市犯案或是逃跑過程中頻繁變更交通方式製造斷點的情形，鞏固偵查成效。應特別指出的是，於歐盟法院的裁判見解中花費不少筆墨介紹的「通信紀錄快速凍結程序」，其之所以能發揮一定程度的偵查效果，主要是因為電信或網路服務業者普遍會基於收費目的留存一定期間內的通信紀錄，因此刑事追訴機關縱使於犯罪發生後方開始儲備相關

doi:10.6342/NTU202403953

資料，仍可取得部分「開始實施時點之前」的資料而有助於犯罪偵查。不同於電信或網路服務業者普遍性地對所有通訊服務使用者儲備資料，車牌辨識資料僅有在高速公路收費站才有可能被私人業者預防性地儲備，而在追查特定人身分或行蹤的效益上大幅地減損，因此難認車牌辨識資料之快速凍結程序（儲存模式）是所謂同等有效之預防或偵查犯罪手段。

另一方面，依據歐盟法院穩定的裁判見解，涉及私人生活應受尊重之權利而損害或限制個人資料保護的干預措施，必須限於「絕對必要」的情形始可為之[425]；而歐盟法院也透過這個要件，排除普遍且無差別地預防性儲備通信紀錄之立法可能。此等見解是否會影響我國預防性車牌辨識資料儲備措施之容許性，似有其討論必要。首先，車牌辨識資料具體上是特定車輛通過某地點的時間及其行駛方向，此等資料大量累積之後，搭配電腦軟體的運算，可以將一個個被自動車牌辨識系統捕捉的時間地點連接，描繪出特定人完整的行車軌跡，因此，整體觀察這些受儲備的車牌辨識資料，不僅可以探知特定人的私人生活，在某些情況下甚至能夠對其個人性格與行動軌跡做出詳盡的推論，而在歐盟法院的見解下亦須限於「絕對必要」的情形始可實施。不過，在此若是直接將歐盟法院對於預防性通信紀錄儲備的見解，援引於預防性車牌辨識資料儲備的情形，藉以排除無差別預防性資料儲備的可能，本文認為是有張飛打岳飛、拿橘子與蘋果相比的問題。原因在於：歐盟法院排除無差別預防性儲備通信紀錄的見解，很大一部分是建立於 2002 年指令規範體系所建構出的原則與例外關係，這也是為什麼歐盟法院考量通訊使用者資料並非 2002 年指令的規範範圍後，於必要性與狹義比例原則的審查上未就相關問題再多作論述。而車牌辨識資料亦非歐盟法秩序下原則不受儲備之個人資料，難以透過例外從嚴解釋的法學方法據以排除無差別預防性儲備的立法可能。此外，仰賴現代電子通訊的蓬勃發展，通訊雙方曾經發生通訊的事實基本上可以期待不為外人所知，而屬於敏感性較高的個人資料；相較之下，車輛行駛於公共

[425] Joined Cases C-793/19 & C-794/19, *supra* note 373, ¶ 52.

doi:10.6342/NTU202403953

交通場域，基於車牌號碼的公示性質，難以期待不被他人得知，在資料敏感性的判斷上自然無法與通信紀錄等同視之，也因此無法直接比附援引歐盟法對於通信紀錄的保障，以及緊隨其後的對於預防性儲備通信紀錄措施所作成之限制。

然而，這並不代表預防性車牌辨識資料儲備措施就不需要在資料儲備範圍上受到限制，事實上，關於基本權干預措施的授權基礎，立法者本來就會在發動要件上設計一定的限制，藉此降低系爭措施干預基本權的程度，以利後續通過狹義比例原則的審查。如同德國聯邦憲法法院於 2018 年第二次車牌辨識裁判，判斷系爭《巴伐利亞邦警察任務及職權法》規定是否合憲時所述：立法者在設計以追緝模式實施自動車牌辨識的授權基礎時，必須一方面衡量其干預基本權的性質與程度，另一方面具體界定實施措施應具備的事實要件或是所得保護的重要公益，以符合比例原則的要求。因此，地毯式實施自動車牌辨識的模式不應被允許，反而應考量系爭干預授權基礎所欲防止之具體危險的嚴重與急迫程度，再加強或放寬實施自動車牌辨識的空間限制[426]。聯邦憲法法院也進一步指出：系爭條文中定有不允許有權機關地毯式實施自動車牌辨識的要件，即是將實施自動車牌辨識的空間範圍限制在可能有助於追查特定人下落或身分的特定地點，而不是授權有權機關盡可能地擴大實施空間，直至覆蓋其全部的管轄範圍，進而導致用路人的一舉一動都必須受到檢查[427]。最終，聯邦憲法法院於判斷系爭規定是否符合狹義比例原則時，也很大程度地仰賴於這個限制空間範圍的要件上[428]，德國立法者後續也對《刑事訴訟法》第 163g 條加上了「非地毯式」的要件。

而考量預防性儲備車牌辨識資料措施相較於「追緝模式」構成更嚴重的個人資訊自決權干預，且資料儲備與資料調取二者授權基礎之合憲性應合併觀察[429]，

---

426 BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 100.
427 BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 115.
428 BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 122, 151 f.
429 我國有學者稱之為「唇齒條款」，亦即資料之後續利用若無提供法律上足夠之保障（唇亡），則原先資料蒐集的授權基礎亦屬違憲（齒寒）。參考：李震山（2006），〈警察機關設置監視錄影器的法制問題－人權保障與治安維護的動態平衡〉，《台灣本土法學雜誌》，86 期，頁 120；李震山（2006），〈德國抗制恐怖主義法制與基本權利保障〉，《月旦法學雜誌》，131 期，頁 20。德國聯邦憲法法院於 2010 年審查《電信法》第 113b 條的合憲性時也提出相同看法，認為其不只關乎自身的合憲性，同時也影響了無差別預防性儲備資料的授權基礎是否能合於比例原則。Vgl.

doi:10.6342/NTU202403953

則若是立法者於車牌辨識資料蒐集與儲備的授權基礎設計上，並未相當嚴格地在空間範圍上作出限制，就有可能導致後續資料調取的規定必須限於預防或偵查特別重大的犯罪，例如最輕本刑為五年甚至十年以上有期徒刑之罪，始可正當化地毯式實施預防性車牌辨識資料儲備，對於不具犯罪嫌疑之一般人所帶來的嚴重恫嚇效果，而符合衡平性的要求。然而，此舉不但不利於民主社會下人民自由發展其人格的權利，更會因為恪遵比例原則的誡命而只能在極其有限的偵查情境中發揮成效。有基於此，本文認為預防性車牌辨識資料的儲備措施，必須限於依據客觀的事實證據，於事前可認對於預防或追訴重大犯罪有所幫助的地點，據以實施所謂的針對性車牌辨識資料儲備。於此可參考前述歐盟法院裁判中對於客觀地理位置標準的說明，將我國自動車牌辨識系統設置的地點限於：過去曾發生多起重大犯罪，平均犯罪率較高的區域，或是因為遊客眾多而容易遭受重大犯罪的場所，又或者是重要的戰略位置和交通樞紐，例如機場、車站、港埠、高速公路交流道和各縣市重要路口。

第四項　狹義比例原則

我國自動車牌辨識系統在對公共安全之具體危害或犯罪嫌疑尚未發生之前，即預防性地儲備所有通過系統車輛的行車資料，並使用資料量化技術，大幅促進各個地點所儲備的行車資料，其間持續積累並相互結合後連接成完整行車軌跡的便捷性。而基於其描繪完整行車軌跡之可能，若是整體觀察這些車牌辨識資料，即會產生探知或揭露特定人私人生活不同面向資訊的風險，例如個人的性傾向、政治意見、宗教、哲學、社會或其他信仰以及健康狀況，甚而導致其每日生活習慣、長期或暫時住所、日常移動軌跡、活動參與、社交關係以及社交環境，均可被據此推論，進而勾勒出特定人之人格圖像。尤有甚者，為了達成追查犯罪嫌疑人身分或下落的目的，我國自動車牌辨識系統於預防性資料儲備階段，未曾實際

BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 226.

doi:10.6342/NTU202403953

公布固定式車牌辨識系統的設置地點，同時輔以移動式車牌辨識，使其具備隱密實施干預措施的性質。此種隱密實施的性質不只導致受干預人因為不清楚其基本權遭受干預的事實，而無法於事前或事中尋求救濟，更可能致使人民駕駛交通工具的過程中，因為無法得知其行車資料是否正在被持續蒐集、儲備？受儲備之資料是否會遭到濫用、竊取？而產生私人生活持續受監視的心理壓力，長久下來，甚至可能在行車路線、留滯地點的選擇上發生改變，最終基於此種「恫嚇效果」影響人民基本權利的自由行使。

另外，即使根據前述見解，將我國自動車牌辨識系統得儲備資料的地點，限制在依客觀事實證據，可認對於預防或追訴重大犯罪有所幫助的地點，然而此種空間限制要件的明確程度，必然與偵查手段的實際成效以及其背後隱含對於人民基本權可能的干預程度相互牽連。申言之，倘若在授權基礎的要件設計上十分明確且嚴格，例如僅限於機場、車站、港埠和高速公路交流道，而排除以「容易發生犯罪之地點」或「容易遭受犯罪之地點」此種不確定法律概念建立空間標準，則降低預防性儲備車牌辨識資料干預程度的同時，卻也大幅降低了此種偵查手段可發揮的效益。因此，本文仍支持立法者於干預授權基礎的設計上，以不確定法律概念建立預防性車牌辨識資料儲備規定所應具備的空間限制。然而，這也表示即使對於預防性車牌辨識資料儲備增添空間上的限制，仍囿於不確定法律概念的解釋空間而難以明確限縮可實施資料儲備的範圍，再加上我國自動車牌辨識系統是以常態性、不受時間限制的方式儲備資料，故縱使基於空間限制的要件，實施針對性資料儲備，仍難以有效降低其干預程度。

綜上所述，我國預防性儲備車牌辨識資料的措施，實際上屬於一種相當嚴重的個人資訊自決權干預，但是參考歐盟法院對於預防性儲備通信紀錄措施的權衡結果，針對性儲備車牌辨識資料若是為了保護相對重要的公共利益，在符合一定要件下，仍有可能通過狹義比例原則的審查。有鑑於此，即有必要針對車牌辨識資料的性質，嚴謹地制定的資料儲備以及資料調取的授權規定。關於資料儲備規定，首當其衝的即是資料儲備期間的限制，資料具體而言可以在多長的時間內被

doi:10.6342/NTU202403953

儲備，一方面賦予了刑事追訴機關相對的偵查可能，一方面也使人民被迫在此期間內承受資料遭濫用而導致私人生活被探知的風險，因此有必要由立法者權衡偵查需求及對人民資訊隱私權的干預程度後，劃定符合衡平性的儲備期間。對此，本文參酌新北市政府警察局將自動車牌辨識系統所取得之照片檔保存 6 個月的實務標準[430]，推論警察機關儲備 6 個月車牌辨識資料即可有效達到追訴重大犯罪的效果，而依資料最小化原則認為應將預防性儲備車牌辨識資料的期間限制在 6 個月，並以此作為後續制定資料調取授權規定之參考依據。

另外，對於預防性資料儲備可能對人民造成時刻受到監視的心理壓力，而產生影響其自由行使基本權利的恫嚇效果，事實上應該從三個面向分別處理：第一，應該要賦予系爭措施符合科技發展水準的資訊安全措施，使人民確保其受儲備的個人資料，不會遭內部人員無權濫用，或是被外部駭客非法竊取，蓋資訊安全措施雖然無法根除預防性資料儲備措施所帶來的心理壓力，卻能夠在一定程度內限制資料遭竊取或濫用的風險，而防止系爭措施干預資訊自決權的程度持續升高。第二，必須使人民信賴其受儲備的個人資料，僅有為保護同等重要的公共利益時，方有被調取、知悉的可能，而不是只要國家機關產生任意需求時，均會受到利用。有鑑於此，於刑事追訴方面，立法者在設計預防性儲備資料的調取授權時，應以例示或列舉方法規範「重罪清單」，始可正當化預防性儲備資料之利用；同時，考量資料調取基於偵查目的，往往無法於事前通知資料主體，使其喪失於事前或事中救濟或制止的機會，且為了判斷資料調取是否確實符合重大犯罪的偵查情形、調取數量與範圍是否符合比例原則，就應該透過法官保留的程序，由客觀中立的法官決定核准與否。第三，對於資料被調取、利用的受干預人，必須於踐行通知不會危害偵查目的時，通知其資料被調取的範圍與緣由，使人民確信其個人資料若確實被調取，其必定能獲得通知且保有事後救濟的機會，而不會持續地被蒙在鼓裡，日復一日擔憂私人生活是否已被揭露。

[430] 新北市政府警察局刑事警察大隊網站，前揭註 259。

doi:10.6342/NTU202403953

關於資訊安全措施，立法者本來即有必要於授權此等預防性資料儲備措施時，提供符合當代科技發展水準的技術保障，而不能一方面欲收偵查成效，另一方面卻以成本考量罔顧人民私人生活遭受探知的風險。不過，對於重罪原則及法官保留的適用，考量車牌辨識資料是於公共交通場域被蒐集，資料敏感性較低，短期內的車牌辨識資料累積，尚不會對於特定人產生人格圖像遭形塑的風險，例如車主下班後發現車輛遭竊，報案後使用即時比對功能卻又遲遲找不到車輛，於是調取過去 8 個小時車牌辨識資料的情形，此種情形既然尚不會對特定人產生形塑人格圖像之風險，即有依據資料取得期間的長短，做出更細緻規範的必要。因此，本文認為具體上可參考德國《刑事訴訟法》第 163f 條對於長期監視情形所作成的權衡結果，將連續 24 小時或 6 個月內累積達 2 日的車牌辨識資料調取，限於偵查我國《通訊保障及監察法》第 5 條第 1 項重罪的情形，並在調取程序上適用相對法官保留原則；而在調取受預防性儲備之車牌辨識資料，未達連續 24 小時且 6 個月內累積未達 2 日的情形，則僅需是偵查最重本刑三年以上的「非輕罪」，且得由檢察官或司法警察官自行為之。當然，此際為了避免偵查機關「化整為零」[431]，規避長期資料調取所應適用的重罪要件與法官保留程序，即有賴於詳細記錄資料存取與刪除時所產生之數據軌跡，並以書面說明調取事由的義務，且透過在體制上建立「內部」與「外部獨立」之監督機關，於事中和事後檢視偵查機關的資料利用行為是否符合授權規範、資料儲備期間屆滿後是否確實以不可回復的方式被刪除。同時，為了避免人民產生其私人生活淪為國家機關持續監視之客體的感受，並確保其提起救濟的權利，更應於資料調取前後，無礙於重大犯罪偵查目的之時點，通知受干預人其資料被調取的範圍與緣由。

[431] 學說上有見解於討論 GPS 的授權基礎時，基於警方恐將長期監視切割為數個法定期間以內的活動，分別逐次實施藉以規避法官保留，反對科技定位監控的短期例外程序設計。參考：李榮耕，前揭註 111，頁 958。

doi:10.6342/NTU202403953

第四章 我國車牌辨識授權規定之審視與立法建議

本文參考德國立法過程中曾提出的「儲存模式」及「記錄模式」，並梳理歐盟法院對於預防性通信紀錄儲備的考量與誡命後，於上一章的結尾提出了常態性在一定期間內預防性儲備車牌辨識資料時（「記錄模式」），理想上授權基礎應具備之相關要件。以下，本文欲討論我國現行法下是否具備實施自動車牌辨識系統的授權規定，並檢視其是否符合上述要求，而得以通過比例原則的審查。具體上，可以依據自動車牌辨識系統的實施流程與方式，區分為三種情形討論，分別是：「車牌辨識資料庫的建立」、「受儲備車牌辨識資料的調取」以及「即時比對功能的使用」。

第一節　車牌辨識資料庫的建立

關於蒐集、儲存車牌辨識資料，並且進而建立資料庫的授權基礎，必須重視系爭規定是否明確規範資料可蒐集的範圍？自動車牌辨識系統的設置地點是否受到限制？資料儲備期間是否符合資料最小化原則？儲備期間屆滿是否應立即刪除？由於我國實施自動車牌辨識系統的方式，是在對公共安全的具體危害以及犯罪嫌疑尚未發生以前，就預防性地對於所有行經車輛儲備資料，因此，應該考慮的是預防危險的相關授權基礎，而不會是用於追訴具體犯罪嫌疑的《刑事訴訟法》規定。

第一項　《警察職權行使法》第 10 條

《警察職權行使法》（下稱：「警職法」）旨在維持公共秩序、保護社會安全，其中亦有資料蒐集的相關授權。《警職法》第 10 條規定：「（第一項）警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，為維護治安之必要時，得協調相關機關（構）裝設監視器，或以現有之攝影或其他科技工具蒐集資料。（第二項）依前項規定蒐集之資料，除因調查犯罪嫌疑或其他違

doi:10.6342/NTU202403953

法行為，有保存之必要者外，至遲應於資料製作完成時起一年內銷毀之。」單從文義來看，《警職法》第 10 條第 1 項「以現有之攝影或其他科技工具」似可包括具有車牌辨識功能的監視器；且其將設置地點限於「經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所」，符合上文所述，必須將自動車牌辨識系統的設置地點限於依循客觀事實證據，可認對於偵查犯罪有所貢獻的地點；同條第 2 項亦具備資料儲備期間以及資料刪除義務的規定。然而，基於以下三點理由，本文認為《警職法》第 10 條不得作為建立車牌辨識資料庫的授權基礎：

第一款 未授權影像資料之識別與量化

過去查緝贓車，警方必須在受害人報案後，逐一調閱車輛遺失地點附近的監視錄影畫面，通常需要耗時 3 至 10 天才能夠鎖定失竊車輛的位置。而在自動車牌辨識系統架設以後，員警只需要在系統中輸入特定車牌號碼，最快 2 個小時就能找到失竊車輛[432]。箇中奧妙就在於，自動車牌辨識系統將監視錄影畫面中所出現的車牌號碼量化（數據化）以後，大幅提升了相同車牌資料之間相互連結的便捷性，促使各個地點所拍攝到的同一車輛資料，輕易地被統整、連結成完整的行車軌跡，也使警方得以使用「搜尋」功能快速掌握所需要的特定車輛資料。而在驚嘆偵查效率的同時，反而應該意識到的是，資料經量化後更容易描繪完整行車軌跡的性質，實際上也導致資料受儲備的人民，更容易暴露在私人生活遭揭露的風險之中。例如於前述員警濫用自動車牌辨識系統監控老婆行蹤的案例之中，若其僅是調閱監視錄影畫面，根本難以具體甚至即時地掌握老婆的活動；相對的，使用自動車牌辨識系統經量化過後的資料，就能夠非常準確且即時地捕捉到車輛每一次通過自動車牌辨識系統的時間與地點。有基於此，使用識別與量化技術實施的影像資料蒐集，明顯與一般影像蒐集所造成的資訊隱私權干預程度有所不同，

[432] 季大仁，前揭註 44；謝東明，前揭註 44。

doi:10.6342/NTU202403953

經過識別與量化的影像資料能夠更輕易地篩選出特定資料並且使其相互連結，產生更高程度探知特定人私人生活的可能性以及風險，因此，倘若系爭授權基礎僅授權一般影像蒐集，自然不得用於識別與量化資料，此種干預程度更高的情形。

《警職法》第 10 條授權警察機關得為維護治安之必要，協調相關機關裝設監視器，或以現有之攝影或其他科技工具於公共場所蒐集資料。關於「現有之攝影或其他科技工具」，假如不以同條項所例示的「監視器」加以理解，而認為其泛泛授權警方於公共場所使用科技工具蒐集資料，則伴隨科技與時俱進的發展，「現有」的攝影工具對於影像資料的解讀能力只會越來越強大，倘若允許其涵蓋本文所探討的自動車牌辨識情形，那麼行人衣物的款式與顏色是否也在自動識別的範圍之內[433]？涉及高敏感性生物資料蒐集的「人臉辨識」，在這種條文理解下又有何不可呢？由此可見，若未將系爭條文所規定的「現有之攝影或其他科技工具」，限縮解釋為與監視器相同而僅具備一般影像蒐集功能的工具，伴隨而來的即是《警職法》第 10 條之要件授權明確性[434]，以及狹義比例原則審查的問題。有據於此，本文認為自動車牌辨識系統既然於資料蒐集的當下，就使用軟體識別車牌號碼，再儲存於資料庫內，事實上就導致這些受預防性儲備的車牌辨識資料，其相互連結的便捷性與可能性大幅提升，受干預人基於此等資料在一定期間內儲備於資料庫中，所承受之私人生活遭探知與揭露的風險，也會跟著水漲船高，因此，不得使用《警職法》第 10 條此種一般影像蒐集的授權規定，建構自動車牌辨識系統之資料庫[435]，而應於授權基礎上清楚規範警察機關得以量化與儲存的資料具體為何，例如僅及於「車牌號碼」及「行駛方向」，而不及於駕駛人和乘客的衣著打扮甚至是臉部資訊，如此始可實際衡酌系爭措施干預人民資訊隱私權的程度，設計符合比例原則的資料使用目的以及調取程序要件，同時，更不會導致

433 林倖妃，前揭註 19。

434 李震山（2023），〈警察職權行使法的回顧與展望：以科技工具蒐集或利用資料規定為例〉，警察法學與政策，5 期，頁 12。

435 學說上亦有相同見解，認為以現有攝影或其他科技工具為之，應受立法目的之拘束，而僅限於「單純的影像觀看或監視過程的錄影」。參考：蔡庭榕、簡建章、李錫棟、許義寶（2005），《警察職權行使法逐條釋論》，頁 260，五南。

doi:10.6342/NTU202403953

《警職法》第 10 條產生違反法律明確性的疑慮。

第二款　未授權以隱密方式蒐集資料

《警職法》第 10 條雖然並未明確規定裝設監視器蒐集資料必須以「公開方式」為之，然而學說上基於《警職法》第 4 條第 1 項：「警察行使職權時，應著制服或出示證件表明身分，並應告知事由。」以及《行政程序法》第 5 條：「行政行為之內容應明確。」而認國家機關若不欲事先公告並以合適方法使人民知悉監視系統的所在位置，則必須具有明確的立法授權，否則將使《警職法》第 10 條與同法第 11 條、第 12 條及第 13 條的界限模糊，產生權力濫用之虞[436]。本文亦肯認此一見解，蓋監視器同為並未區分受干預人是否具備犯罪嫌疑之預防性資料儲備措施，伴隨資料持續積累，容易對人民產生時刻受到監視的心理壓力，進而影響其基本權利的自由行使。若是以隱密方式為之，致使人民於日常生活中無法知悉其當下是否正受資料蒐集，喪失了選擇是否前往資料蒐集區域的行為自由，更有可能因此提心吊膽地面對每一天的活動參與，顯然是更為嚴重的資訊隱私權干預情形。因此，參考《警職法》第 4 條第 1 項的規定，此種措施自然是以公開施行為原則，將其對於人民的恫嚇效果控制在一定程度之內，國家機關若欲以隱密方式預防性蒐集、儲備資料，自然應於授權基礎中明確制定相關要件，《警職法》第 10 條也據此應被理解為：警察機關裝設監視器並蒐集資料，應以公開方式為之[437]。

不同於監視器強調維護治安的需求，而具備公開實施的性質；自動車牌辨識

---

436 李震山（2004），〈從公共場所或公眾得出入之場所普設監視錄影器論個人資料之保護〉，《東吳法律學報》，16 卷 2 期，頁 76；李震山（2005），〈個人資料保護與監視錄影器設置之法律問題研究－以警察職權行使法第十條為中心〉，《警察法學》，4 期，頁 62。

437 相同見解：蕭文生（2004），〈自基本權保障觀點論街頭監視錄影設備裝設之問題〉，法治斌教授紀念論文集編輯委員會（編），《法治與現代行政法學：法治斌教授紀念論文集》，頁 258-259；林明鏘（2023），〈具有雙重性質之警職法——近 20 年的重要司法裁判回顧與分析〉，警察法學與政策，5 期，頁 112-113；李寧修（2021），〈警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例〉，《警察法學》，20 期，頁 425；林錦鴻（2005），《警察運用監視器之法律問題分析－以警察職權行使法為中心》，頁 142-143，國立臺灣大學法律學研究所碩士論文。

doi:10.6342/NTU202403953

系統，基於追查特定人行蹤與身分的目的，於施行上多是隱密為之。觀察我國現行實務，警察機關雖然依法必須公告所有監視錄影器的設置地點，卻不會標示具備自動車牌辨識功能者，致使自動車牌辨識系統得以藏身於茫茫錄影設備之中。此外，移動式車牌辨識系統雖然具有警車及警察制服的外觀，民眾卻難以知悉員警所使用的行車紀錄器是否具備自動車牌辨識的功能，更遑論員警從後方拍攝車牌的情形，人民根本無從得知其資訊隱私權已受干預。倘若隱密實施的干預處分之所以被認為屬較高程度的基本權干預，是肇因於其導致受干預人不易於事前及事中提起救濟，則不論是並未清楚標示車牌辨識功能的固定式車牌辨識系統，或者是人民難以知悉其曾受資訊隱私權干預的移動式車牌辨識系統，縱使有執行公務的外觀，均應被認為係屬於非公開而有礙於人民於事前或事中主張救濟權利的干預措施。

於此，是否有可能為了降低其對於人民資訊隱私權的干預程度，於授權規定要求警察機關必須公告自動車牌辨識系統的設置地點？本文持反對意見，認為此舉將導致其干預人民資訊隱私權的程度不減反增。原因在於，自動車牌辨識系統之所以能夠掌握特定人的行蹤，很大程度上是仰賴其隱密實施的性質，倘若警察機關網站上詳細公告自動車牌辨識系統的設置地點，憑藉現有的科技技術，不難想像民眾可以同測速照相的手機應用程式一般，將自動車牌辨識系統的架設地點標示於電子地圖之上，並且於行駛途中，即將通過車牌辨識系統時予以警示，供駕駛人自行選擇是否要變換路線，以避免其行車資料遭國家機關儲備、比對。甚至，有心人士更可以經由軟體運算，在犯案結束後迅速規劃出一條不會經過自動車牌辨識系統的逃亡路線，逃避警方的追捕。可以想見，面對犯罪嫌疑人躲避自動車牌辨識系統追查的情形，警方的應對方式基本上就是繼續架設更多的自動車牌辨識系統，拉高裝置密度以及覆蓋率，抹去「不會經過自動車牌辨識系統之逃亡路線」的可能性。然而，這同時也表示，人民日常駕車行駛於道路上也將全面籠罩於預防性車牌辨識資料儲備措施之下，前述曾多次強調的對於架設地點之空間限制，終將付諸東流。有鑑於此，相比於公開實施地點後，為了達到查緝特定

doi:10.6342/NTU202403953

人下落的目的而逐漸全面覆蓋式的架設，本文認為隱密實施並且嚴格控制自動車牌辨識系統的架設地點，雖然可能會使人民處於私人生活時時受到監視的憂慮之中，卻仍然勝過全面覆蓋式（地毯式）架設自動車牌辨識系統後，導致資料庫內切切實實地存有人民鉅細靡遺之行車資料的情形，因此，自動車牌辨識系統的實施仍應以隱密的方式為之。

不過，這同時也代表《警職法》第 10 條無法作為此種於公共場所使用科技工具隱密蒐集資料的授權基礎，警察機關若欲以自動車牌辨識系統，於公共場所秘密地蒐集並儲備通過車輛之行車資料，必須另外立法授權。

第三款　儲備期間一年有違資料最小化原則

資料最小化原則（data minimization），是指國家機關基於特定目的蒐集資料，必須限縮在達成目的所需要的最小資料範圍[438]，也就是說，從比例原則的必要性觀點出發，倘若適時為了達成目的而有蒐集或儲存更小範圍資料，此種同等有效且侵害程度較小的手段，就必須予以適用。《警職法》第 10 條第 2 項規定警察機關於公共場所使用科技方法蒐集資料後，至遲應於 1 年內將資料銷毀。不過，根據資料表示，目前新北市政府警察局僅會將自動車牌辨識系統所取得的錄影檔保存 1 個月，照片檔保存 6 個月[439]。因此，應可據此推論，6 個月的車牌辨識資料儲備，其實就足以因應實務上的偵查需求。如此一來，在資料最小化原則的觀點下，就必須於授權基礎明確限制警察機關至多僅可將車牌辨識資料儲備 6 個月。蓋參考前述德國聯邦憲法法院以及歐盟法院對於預防性通信紀錄儲備的討論，儲備期間的長短對於預防性資料儲備措施的干預程度判斷而言，至關重要，其一方面決定了國家機關可以取得多大範圍的資料，並且基於資料數量與性質的不同，

[438] 劉青峰（2023），〈COVID-19 疫情下資訊自決權之研究——以歐洲人權公約第 8 條作為比較法對象〉，《中原財經法學》，50 期，頁 248-249；范姜真媺（2022），〈防疫措施與個人資料保護間之取捨、衡平〉，《月旦法學雜誌》，323 期，頁 51；許芳瑜（2016），〈歐盟對於行動健康服務之個人資料隱私保護之發展〉，《科技法律透析》，28 卷 7 期，頁 63-64。

[439] 參考：新北市政府警察局刑事警察大隊網站，前揭註 259。

doi:10.6342/NTU202403953

而在資料累積、相互連結的過程中對於特定人私人生活作成更精確的推論；另一方面，則是決定了受干預人必須在多長的期間內，承受其個人資料恐被濫用、竊取，以及伴隨而來私人生活遭受揭露的風險。這也是為什麼德國《電信法》修法會大幅地縮短儲備期間，試圖以此通過後續的狹義比例原則審查。有鑑於此，既然 6 個月的車牌辨識資料儲備，即可滿足實務上的偵查需求，立法者在制定相關授權基礎時，自然必須清楚限制車牌辨識資料的儲備期間，避免使人民為了想像上虛無飄渺之未來可能偵查需求，而不必要地承受一整年的資料儲備、累積所帶來的風險。相對的，倘若警察機關抗辯車牌辨識資料應儲備更長的期間，以因應實務需求，則必須提出客觀的事實證據，供立法者權衡，不可泛泛指稱。

值得一提的是，根據國家通訊傳播委員會依《電信管理法》第 9 條第 3 項所制定的《電信事業用戶查詢通信紀錄及帳務紀錄作業辦法》，其中第 4 條第 2 項規定，電信事業應將通信紀錄及帳務紀錄自紀錄發生時起至少保存 1 年。則在本文見解下，是否會導致資料敏感性較低的車牌辨識資料，反而必須適用較為嚴格的 6 個月儲備期間規定，而有違我國立法者對於資料儲備期間權衡結果的一致性？首先必須說明的是，正如前所述，儲備期間的限制對於預防性資料儲備措施而言至關重要，我國這種立法授權行政機關自行決定儲備期限的模式，在歐盟法或是德國法的觀點下是否能夠通過法律明確性的審查，已顯有疑義，更遑論其竟然是規定「至少」保存 1 年，此種制定資料儲備期間「下限」而非「上限」的立法方式，明顯是以警察機關的偵查成效為主要考量，罔顧人民個人資料的保護。蓋於比例原則的觀點下，必須先確認系爭措施可能干預基本權的程度以後，才有辦法嚴謹地審查授權基礎的要件是否具備適當性、必要性與衡平性。此種制定資料儲備期間「下限」，容任儲備期間不受限制地持續延長，也等同於放任系爭措施干預人民資訊隱私權的程度持續增長，而在文義上涵蓋了儲備人民過去五年、十年甚至是五十年的通信紀錄，這種立法方式，根本不可能通過比例原則的審查。有據於此，自然不得以我國現行法下關於通信紀錄儲備期間的規定，指稱本文將車牌辨識資料儲備期間限為 6 個月的見解過於嚴苛。此外，縱使我國現行法是將

doi:10.6342/NTU202403953

通信紀錄的儲備期間定為至多 1 年，仍無礙於此處結論。蓋本文是以資料最小化原則，亦即從必要性的觀點提出 6 個月儲備期間的建議，立法者若對於敏感性更高的資料訂立超出 6 個月的資料儲備期間，只能說明儲備高於 6 個月的車牌辨識資料，仍有通過衡平性審查的可能，卻不能據此回過頭來影響比例原則審查下，第二階段必要性審查的功能與結論。

第二項　地方自治法規：以《臺北市錄影監視系統設置管理自治條例》為例

我國《憲法》第 118 條規定：「直轄市之自治，以法律定之。」又，依《地方制度法》第 18 條第 11 款，直轄市警政、警衛之實施屬於直轄市之自治事項。因此，我國各直轄市為健全錄影監視系統的設置管理，均分別制定相關自治條例，則此等自治條例是否得以作為建立自動車牌辨識資料庫的授權基礎，亦有必要說明。然而，經由上述對於《警職法》第 10 條的檢視，不難看出此種錄影監視系統的自治條例，亦無法作為建立自動車牌辨識資料庫的授權基礎。

以《臺北市錄影監視系統設置管理自治條例》（下稱「臺北市錄影自治條例」）為例，第 3 條第 1 項規定：「本自治條例所稱錄影監視系統，指市政府所屬各機關於本市公共場所設置之攝錄影音設備。」第 12 條第 1 項：「公務機關因執行職務之需要，得向設置機關申請調閱錄影監視系統影音資料，必要時並得複製、利用。」則從《臺北市錄影自治條例》的相關條文中亦無法看出，其是否授權警察機關透過軟體加以識別與量化錄影監視系統所取得的影像資料，自然不得以一般影像資料蒐集的授權規定，逕行實施對於人民資訊隱私權干預程度更高的影像識別與資料量化，因此，無法作為自動車牌辨識資料蒐集與儲備的授權依據。其次，依《臺北市錄影自治條例》第 10 條規定：「依本自治條例設置之錄影監視系統，警察局及設置機關應每半年公告其設置區位。」目前實務上，臺北市政府警察局雖然會完整公告監視錄影設備的設置地點，但是並不會標示出具有車牌辨識功能

doi:10.6342/NTU202403953

的監視器，再搭配移動式車牌辨識系統的實施，事實上使自動車牌辨識系統具備隱密施行的性質，而基於前述的說明，自動車牌辨識系統的隱密施行也有其必要性，據此，自然不得以《臺北市錄影自治條例》此種授權警察機關公開架設監視錄影器的授權，實施自動車牌辨識資料的隱密蒐集。最後，《臺北市錄影自治條例》第 13 條同《警職法》第 10 條，將資料保存期間定為一年，而鑑於前述資料指出，6 個月的車牌辨識資料儲備既然已足以應對實務上偵查需求，基於資料最小化原則就應該在資料儲備的授權基礎上，明確地將資料儲備最高期間定為 6 個月，否則無法通過必要性的審查。

第三項　《道路交通管理處罰條例》第 7 條之 2

《道路交通管理處罰條例》（下稱：「道交條例」）第 7 條之 2 第 1 項第 7 款授權警察機關得以科學儀器取得證據資料，以此證明汽車駕駛人之行為違規；同條第 2 項並規定，科學儀器之設置地點應定期於網站公布。因此，其同屬授權警察機關使用科學儀器蒐集資料之規定。不過，《道交條例》第 1 條開宗明義表示，本法旨在「加強道路交通管理，維護交通秩序，確保交通安全」，同法第 7 條之 2 於 2014 年的修法理由也表示：「本法之立法目的係在於維護交通安全，非以處罰為目的」，則基於資料蒐集目的明確性的要求，違規取締之目的達成後，警察機關即應將車輛辨識資料刪除，不得以維護交通安全的法規，巧令名目地蒐集汽車駕駛人的行車資料之後持續留存，供警察機關於偵查犯罪時予以調取[440]。且《道交條例》第 7 條之 2 第 1 項亦已列舉本條授權警察機關蒐集資料所欲規範的情形，明顯非為犯罪追訴所設[441]。此外，學說上亦有見解指出，警方依據本法使用科學儀器蒐集違規行為的證據資料，必須具有「目的性」與「針對性」，例如測

[440] 關於偵查機關為追訴犯罪調取基於其他目的蒐集之車牌辨識資料，詳參後續《個人資料保護法》第 15 條及第 16 條的討論。

[441] 同為維護交通安全的「違規停車取締」，由於並未列於《道交條例》第 7 條之 2 第 1 項，而不得以本法授權警察機關使用監視器蒐集證據資料取締，更遑論是以此授權警方預防性儲備車牌辨識資料，供後續犯罪追訴所用。參考：劉靜怡（2016），〈監視科技設備與交通違規執法〉，《月旦法學雜誌》，248 期，頁 77。

doi:10.6342/NTU202403953

速照相儀器僅會拍攝「特定」超速車輛；倘若全天候持續拍攝，而涵蓋未違規之車輛，則屬資料蒐集與行為監控的情形，必須另外依據特別規定且具正當理由，始得為之[442]。最後，再參考同條第 2 項公布設置地點的規定，即可清楚得知《道交條例》第 7 條之 2 不得作為警方以隱密方式預防性儲備車牌辨識資料，供後續偵查犯罪時調取之授權依據。

第四項　立法建議

既然現行法下並無預防性儲備車牌辨識資料之授權基礎，我國警方使用自動車牌辨識系統，對於不具犯罪嫌疑的一般人大量蒐集、儲備其行車資料之措施，即已違反了法律保留原則，於立法者尚未制定授權基礎之前，不得繼續實施。因此，本文以下嘗試擬定條文，提供立法者作為參考。

增訂《警職法》第 10 條之 1 全文如下：

1. 警察對於有事實足認經常發生或容易遭受犯罪案件之公共交通場所，為防止危害或犯罪之必要，得以科技工具秘密蒐集行經車輛之車牌號碼、時間、地點及行駛方向。
2. 依前項規定蒐集之資料，除因調查犯罪嫌疑或其他違法行為，依法律規定有保存之必要者外，至遲應於資料製作完成時起六個月內銷毀。
3. 依第一項規定蒐集之資料，應以符合當前科技發展水準之技術加密。
4. 依法律規定調閱、複製或利用第一項規定所蒐集之資料，應至少有兩名人員在場，並作成以下紀錄：

   一、 資料存取時間。

   二、 資料存取人員。

   三、 資料存取範圍與事由。

[442] 李建良（2015），〈公法類實務導讀【交通裁決事件系列（十一）】【道路監視錄影資料與交通違舉證方法】〉，《台灣法學雜誌》，272 期，頁 129-130。

doi:10.6342/NTU202403953

首先，針對自動車牌辨識系統資料蒐集與儲備的授權基礎，必須對其施行地點作出限制，避免警察機關全面覆蓋式地建置自動車牌辨識系統。因此，本文將其要件設計為「有事實足認經常發生或容易遭受犯罪案件之公共交通場所」。不過，仍有必要透過立法理由或施行細則，將歐盟法院前述對於客觀地理位置標準的說理納入其中，亦即，應基於客觀且非歧視性的事實依據，而認某地區具有準備或實施重大犯罪的高程度風險，包括過去曾發生多起嚴重犯罪的區域，或是像經常接待大量遊客的地點或設施，此種特別容易遭受嚴重犯罪的場所，又或者是重要戰略位置，如機場、車站、港口或高速公路收費站。同時，亦可參考我國學說見解對於《警職法》第 10 條所提出的建議，將「經常」理解為「同一場所在相距不久的相當期間內，有具體事實，足認為有二次以上之犯罪發生」，並且將特定地區同一期間內的犯罪發生率，與全國、同一縣市、同一鄉鎮市或同一警察轄區的犯罪發生率互相比較，作為是否「經常發生」的參考依據，甚至應考慮以同一犯罪類型為判斷標準[443]。

其次，參考《警職法》第 4 條與《行政程序法》第 5 條之規定，國家機關若欲以科技工具隱密蒐集資料，必須具有明確的立法授權。基此，本文於規定中明確授權警察機關得以秘密方式蒐集資料，並且將資料可蒐集範圍限於「車牌號碼、時間、地點及行駛方向」，排除警察機關依據本條規定，以科技工具識別車內駕駛人、乘客與路上行人之衣物顏色，甚至是臉部資訊的可能性。此外，權衡實務偵查需求以及人民資訊隱私權之保障，將車牌辨識資料的儲備期間限制為 6 個月，期間屆滿時除為調查具體犯罪嫌疑，而依法律規定得以繼續保留之外，應立即以不可回復的方式予以刪除、銷毀。最後，為了避免國家機關所建置的車牌辨識資料庫，遭外部駭客竊取而致使人民完整的行車軌跡輕易為他人所知，蒐集與儲備車牌辨識資料之警察機關應以符合當前科技發展水準的加密技術，確保受儲備資料之安全性。同時，為了排除內部人員濫用的可能性，依據資料利用規定有

443 蔡庭榕、簡建章、李錫棟、許義寶，前揭註 435，頁 257。

doi:10.6342/NTU202403953

權存取車牌辨識資料者，於調取利用時應遵循「四眼原則」，至少命兩名人員在場，並確實記錄資料調取的時間、人員、範圍以及事由。雖然，《個人資料保護法》第 18 條已規定：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」並且於《個人資料保護法施行細則》第 12 條對於「安全維護事項」定有不同面向的事宜[444]，然而，考量預防性車牌辨識資料儲備措施對於人民自由行使基本權利的影響，而較一般干預資訊隱私權的情形更為嚴重，自然有在具體干預授權基礎制定更細緻的資訊安全規範之必要性。另外，必須強調的是，鑑於量化處理後資料相互連結的便捷性，本條第 4 項所稱「依法律規定調閱、複製或利用」，必須是於要件中明確規範「車牌辨識資料」之授權規定，於資料目的外使用的情形更應排除以《個資法》的空泛規定作為授權依據，始可避免資料一經政府儲備隨即在各個機關流用的情形發生。

第二節　受儲備車牌辨識資料的調取

車牌辨識資料經預防性儲備後，若欲基於追訴犯罪之目的調取並加以利用，事實上是使偵查機關得以確實得知特定人的行車資訊，而對資料被調取之特定人構成更進一步的資訊隱私權干預，因此，必須具備獨立的授權基礎，始可符合法

444 《個人資料保護法施行細則》第 12 條：
1. 本法第 6 條第 1 項但書第 2 款及第 5 款所稱適當安全維護措施、第 18 條所稱安全維護事項、第 19 條第 1 項第 2 款及第 27 條第 1 項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。
2. 前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：
一、配置管理之人員及相當資源。
二、界定個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。
六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。
十一、個人資料安全維護之整體持續改善。

doi:10.6342/NTU202403953

律保留原則。又依據前開說明可知，預防性儲備資料的調取授權，必須是為了維護同等重要的公共利益，並且在資料安全、法官保留、事後通知、刪除義務均有對應規定，始可確保預防性資料儲備以及嗣後調取資料的授權規定，二者均得通過比例原則的審查。有鑑於此，縱使立法者遵循上述立法建議，制定《警職法》第 10 條之 1，仍必須視現行法下是否具備此等資料之調取授權規定；若否，則亦須提出立法建議。

第一項　《警察職權行使法》第 17 條

《警職法》第 17 條規定：「警察對於依本法規定所蒐集資料之利用，應於法令職掌之必要範圍內為之，並須與蒐集之特定目的相符。但法律有特別規定者，不在此限。」則警察機關是否得將其依循新法《警職法》第 10 條之 1 所儲備的車牌辨識資料，用於刑事案件之追訴，即有疑義。然而，本文建議增訂之《警職法》第 10 條之 1，是授權警察機關在對公共安全的具體危害或犯罪嫌疑尚未發生以前，即基於防止危害或犯罪之目的，預防性地儲備特定地點的車牌辨識資料，因此，其目的在於危害或犯罪之防止，而與刑事犯罪發生以後，基於對特定人之開始嫌疑而實施追訴行為的情形有所不同。據此，若欲將警察機關依據《警職法》第 10 條之 1 所儲備的車牌辨識資料用於刑事追訴，事實上屬於原始蒐集目的以外之「目的外使用」，考量《警職法》第 17 條「法令執掌」亦應理解為「警察防止危害與預防犯罪之範圍」[445]，自然不得以《警職法》第 17 條作為偵查機關基於刑事追訴目的調取特定人車牌辨識資料的授權依據。

第二項　《刑事訴訟法》第 230 條、第 231 條

針對以刑事追訴為目的調取原先非基於偵查原因所蒐集之資料，我國《刑事訴訟法》上並無具體的授權規定，只得討論是否得依司法警察的一般偵查權限為

[445] 蔡震榮（2016），《警察職權行使法概論》，3 版，頁 201，五南。

doi:10.6342/NTU202403953

之。關於《刑事訴訟法》第 230 條、第 231 條是否得作為司法警察偵查權限的一般性規定，學說上見解分歧，有見解認為系爭條文除了界定司法警察實施措施的時點及目的之外，對於措施可干預的基本權類型與程度卻完全不置可否，不符合法律明確性的要求而不得作為司法警察干預人民基本權利的授權基礎[446]。另有見解考量現代干預概念與法律保留領域的雙重擴張，主張有必要在一定範圍內承認司法警察的一般調查權限，惟應排除立法者已特別授權之干預措施、涉及干預憲法列舉基本權的情形，以及該當刑法構成要件之干預[447]。本文認為，考量現代基本權保護範圍與干預概念持續擴張，法律保留原則的適用範圍也隨之提升，在邏輯上確實有承認一般調查權限的必要性，方不會致使警方輕微干預人民基本權的措施亦構成違法取證行為。不過，有鑑於《刑事訴訟法》第 230 條、第 231 條連可能涉及基本權的類型均未規範，其法律明確性實有相當程度的疑慮，因此在適用上只能限於絕對輕微的基本權干預情形，例如司法警察的短期目視跟監，始為現行法下合於憲法的解釋。

我國實務曾有見解認為，路口監視器是基於一般犯罪預防等行政目的，對於在公共場所或公眾得出入場所之不特定多數人公開活動的影像紀錄，而非針對特定犯罪所為偵查目的之蒐證攝影；考量用路人對其公開活動之隱私或秘密合理期待甚低，警方若僅是「事後」調取特定單點的監視錄影畫面，既然其質量及其密度尚不足以建構、窺知特定人日常生活隱私之全貌，對其個人基本權利（隱私權）之干預甚微，則屬《刑事訴訟法》第 230 條、第 231 條一般偵查干預授權之範疇[448]。本文認為，法院強調警方「事後」的調取行為，是想表示警方於使用路口監視器蒐集資料的階段尚未對特定人產生「目的性」或「針對性」，嗣後僅調取特定單點的監視錄影畫面，也確實符合干預質量輕微的情形。不過，這個見解的隱

446 薛智仁（2014），〈司法警察之偵查概括條款？——評最高法院一〇二年度台上字第三五二二號判決〉，《月旦法學雜誌》，235 期，頁 244-250。

447 林鈺雄（2007），〈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；林鈺雄，前揭註 209，頁 324。

448 最高法院 111 年度台上字第 3086 號刑事判決。

doi:10.6342/NTU202403953

憂在於，倘若警方連續調取同個地點三天、五天甚至是一個星期、一個月的監視錄影畫面，又或者在某個監視錄影片段觀察到特定人的身影後，繼續調取周遭附近的監視錄影畫面，試圖掌握更多偵查線索，此時應如何判斷在何種程度以上的監視錄影畫面調取，即非屬干預質量「輕微」的情形？倘若實務上頻繁發生員警對於干預程度輕微的判斷與受干預人或是法院不同，是否會導致人民的資訊隱私權暴露在違法取證的風險之中？申言之，基於電子資訊技術發展的背景，個人資料的永久保存及相互結合成為可能，這是保障人民資訊隱私權的核心意旨，也是其干預程度容易伴隨個人資料的利用範圍而瞬息萬變的主要原因。關於如何判斷調取監視錄影畫面的干預程度是否輕微，首要任務是課予偵查機關詳實記錄資料調取範圍及原因的義務，倘若沒有確實地記錄，則偵查機關只需於證據調查完畢以後，在法庭上提出最具有證明效果的「特定單點」監視錄影畫面，就永遠都會屬於干預質量輕微的情形，更可以撇頭不顧其偵查過程中大量調閱涵蓋特定人身影的監視錄影畫面，所構成之資訊隱私權干預，受干預人此際若欲提起相關救濟，也無從透過實施紀錄證明警方違法取證。其次，必須由立法者設定一個想像上一旦超出這個時間範疇，即有可能構成非輕微資訊隱私權干預的監視錄影畫面調取門檻，並且對應地設計檢察官保留或法官保留等程序擔保，確保資料調取的範圍在個案中符合比例原則，同時課予偵查機關通知受干預人其資料曾遭調取之義務，以利受干預人提起救濟[449]。

觀察《刑事訴訟法》第 230 條、第 231 條，若欲將其作為偵查機關調取監視錄影畫面的授權基礎，卻無法得出其必須於調取資料時確實紀錄調取範圍與原因的結論，遑論資料調取是否在一定程度上應適用法官保留的判斷標準。雖然法院或許可以在綜合一切事證後，認定個案中的監視錄影畫面調取行為屬於輕微的干預情形，而為合法的取證行為。但是，偵查機關是否得以在調取監視錄影畫面的

[449] 至於監視錄影畫面中人數眾多、出入繁雜的情形，具體上應對何人踐行通知，或可參考德國《刑事訴訟法》第 101 條第 4 項第 7 款針對第 100h 條住宅外監視錄影所設計的通知規定，將通知對象限於「被鎖定之人與重大連帶受干預之人」。

doi:10.6342/NTU202403953

當下，即依循系爭條文判斷其行為合法性，藉以發揮法律保留及明確性原則中，透過明確立法授權「使行政機關在執行法律時得以遵循立法者所劃定界線」的功能[450]，實有疑義。有鑑於此，本文認為，基於法律保留及明確性原則之誡命，《刑事訴訟法》第 230 條、第 231 條無法作為偵查機關調取監視錄影畫面的授權依據。

上述問題於警方調閱車牌辨識資料的情形更為嚴重，蓋車牌辨識資料係經軟體識別並量化過後的資料，其資料之間相互連結的可能性與便捷性均非監視錄影畫面此種類比資訊所可比擬。也就是說，受干預人更有可能單純因為少量資料的調取，就產生私人生活受到探知的風險，更何況依本文見解，警察機關得不區分受干預人是否具有犯罪嫌疑，秘密地預防性儲備六個月的車牌辨識資料，則多大程度上的資料調取必須受到諸如重罪清單及法官保留程序，此等更嚴格的要件限制，就必須由立法者定奪。有據於此，本文認為車牌辨識資料的調取利用行為，並非輕微之資訊隱私權干預，司法警察不得依《刑事訴訟法》第 230 條、第 231 條一般調查權限逕行為之。

第三項　《個人資料保護法》第 15 條、第 16 條

既然《刑事訴訟法》並無以刑事追訴為目的，調取基於犯罪預防所蒐集之車牌辨識資料的授權規定，則若涉及同一警察機關原先基於危害防止所蒐集之資料，是否得用於犯罪追訴，似乎只能討論《個人資料保護法》（下稱「個資法」）第 16 條但書，此一關於公務機關目的外使用個人資料之規定。對此，學說有見解肯認警察依治安目的所蒐集之資料，得依《個資法》第 16 條但書規定用於刑法追訴，但並未具體說明是依據但書第幾款規定[451]。另一方面，倘若原先基於危害防止目的取得個人資料之機關（A 機關），出於協助刑事追訴之原因而將個人資料傳送

[450] Vgl. BVerfG, NJW 2008, 1505, 1509 (Rn. 89).
[451] 參考：許義寶（2020），〈論警察蒐集與利用個人資料之職權〉，陳淳文（等著），《如沐法之春風——陳春生教授榮退論文集》，頁 537。

doi:10.6342/NTU202403953

予另一機關（B 機關），實務上會將 A 機關的行為理解為個人資料的利用，將 B 機關的行為理解為個人資料的蒐集，再分別討論其是否各自符合《個資法》第 16 條以及第 15 條，對於公務機關利用或蒐集、處理個人資料的規定。例如，我國海岸巡防機關（以下稱：「海巡機關」）為了查緝走私及其他犯罪調查，依《海岸巡防法》第 12 條第 2 項制定《海岸巡防機關與警察移民及消防機關協調聯繫辦法》，其中第 7 條規定：「海巡機關依法執行職務時，得使用警察及移民機關建立之資訊系統查詢相關作業資料。必要時亦得請求警察機關支援刑事鑑識工作。」並因此曾發函詢問「個人資料保護委員會籌備處」：海巡機關基於查緝走私及犯罪調查目的，以逐案查詢方式介接警政署車牌辨識系統，是否符合《個資法》第 15 條規定，而屬於合法的個人資料蒐集？對此，個人資料保護委員會籌備處回覆：若海巡機關以逐案查詢方式在符合比例原則下，於必要範圍內蒐集、處理車牌辨識資料，則可認符合《個資法》第 15 條第 1 款所定「執行法定職務之必要範圍」；同時，關於警政署傳送車牌辨識資料的行為，參考《個資法》第 16 條但書第 1 款所稱「法律明文規定」，包括法律或法律具體明確授權之法規命令[452]，因此，基於《海岸巡防機關與警察移民及消防機關協調聯繫辦法》第 8 條規定：「海巡機關與警察、移民機關應相互合作，密切協調，彼此提供有關之犯罪情報及資料，共同打擊犯罪。」以及第 9 條：「海巡機關與警察、移民機關間，得建立相關資訊、通信網路與資料庫連結交換系統。雙方各級勤務指揮中心，應密切保持聯繫。遇有緊急或重大狀況時，應即時相互通報。」警政署於必要範圍內傳送車牌辨識資料，符合《個資法》第 16 條但書第 1 款所定「法律明文規定」得為目的外使用的情形。

若依上述見解，似乎《警職法》第 10 條之 1 一經增定，警察機關甚或是海巡機關即可依循《個資法》及《海岸巡防法》相關規定，調取偵查犯罪所需的車牌辨識資料。然而，暫且先不討論《個資法》第 15 條及第 16 條可否作為國家機

[452] 參考《個人資料保護法施行細則》第 9 條。

doi:10.6342/NTU202403953

關蒐集、處理或利用個人資料的授權基礎，基於前述說明可知，預防性資料儲備措施容易使人民產生時刻受到監視的心理壓力，而影響其基本權利之自由行使，也導致此等措施干預人民資訊隱私權的程度直線上升。為了處理其所造成的心理壓力，原則上必須將受預防性儲備資料之利用限於同等重要的公共利益，而於刑事追訴上恪守重罪原則，並且由客觀中立的法官審查此際是否符合重大犯罪的追訴情形、資料調取範圍是否符合比例原則，使人民得以確信其受預防性儲備之資料，僅在同等重要的情形下才會被使用，其私人生活不至淪為國家機關恣意監視的客體。本文另外考量短期內的車牌辨識資料調取，尚不會對特定人產生人格圖像遭形塑的風險，遂主張未達連續 24 小時或 6 個月內累積未達 2 日的車牌辨識資料調取，因其對於資料被調取之特定人的資訊隱私權干預程度尚非特別重大，故認此時僅需排除刑事追訴機關將預防性儲備之車牌辨識資料用於偵查輕罪的情形，而將資料利用門檻設定為「偵查最重本刑三年以上之罪」，並得由檢察官、檢察事務官、司法警察官自行為之。不過，調取連續 24 小時的車牌辨識資料，或是 6 個月內數次分別調取，時間累積超過 2 日的情形，考量此際車牌辨識資料的積累，已經產生了揭露特定人私人生活，甚至是形塑其人格圖像的嚴重風險，即有必要將資料利用門檻設定為重大犯罪之偵查情形，具體而言，得準用《通訊保障及監察法》第 5 條第 1 項之重罪清單，並且於資料調取程序上適用相對法官保留原則，於人民資訊隱私權之保障與刑事追訴機關的急迫偵查需求之間取得平衡。

觀察《個資法》第 15 條和第 16 條，根本無法得出車牌辨識資料的調取利用，基於其預防性資料儲備的性質，原則上必須限於偵查重大犯罪的情形，並適用法官保留原則，僅在例外短期調取的程序上改為適用「非輕罪原則」的結論。反而容易致使刑事追訴機關調取車牌辨識資料的範圍，一方面不合乎所應對應的重罪門檻，另一方面在程序上沒有客觀中立的法官確保個案中的資料調取範圍符合比例原則。試想，單憑《個資法》第 16 條的文義，偵查機關是否可以為了增進公共利益，基於偵查一般犯罪的目的利用特定人過去 6 個月所有的車牌辨識資

doi:10.6342/NTU202403953

料，並同時持續存取其未來繼續產生的車牌辨識資料？假以時日，不停地累積特定人三年五年的行車軌跡，這種措施難道不需要客觀中立的法官監督嗎？海巡機關是否也可以依據《個資法》第 15 條的規定，為了執行查緝走私的法定職務，逕自做出相同的事情？僅憑條文中的「必要」，即可確保刑事追訴機關的偵查行為均符合比例原則？有鑑於此，本文認為車牌辨識資料長期累積後既然得以探知特定人的私人生活，於法律明確性及比例原則的觀點下，自然不得以《個資法》第 15 條和第 16 條此種一般性的規定，作為車牌辨識資料的調取授權基礎，而有另行立法的必要。

第四項　立法建議

基於上述討論可知，縱使我國立法者增定預防性儲備車牌辨識資料之授權規定，我國現行法上亦無基於刑事追訴目的，調取特定人車牌辨識資料的授權依據。因此，本文以下嘗試提出立法建議，供立法者參考。

增訂《刑事訴訟法》第 153 條之 11 全文如下：

1. 檢察官偵查通訊保障及監察法第 5 條第 1 項所列之罪，有事實足認下列車牌辨識資料於本案之偵查有必要性及關連性時，除有急迫情形不及事先聲請者外，應以書面聲請該管法院核發調取票。

   一、車牌號碼核發給被告或由被告使用。

   二、車牌號碼核發給被告以外之人或由該人使用，且根據相當理由可認為該人與被告有聯繫或將建立聯繫，若以其他方法調查，合理顯示為不能達成目的或有重大危險情形。

2. 法院核發第一項調取票應記載下列事項：

   一、案由及涉嫌觸犯之法條。

   二、資料調取對象。

   三、資料調取理由。

doi:10.6342/NTU202403953

四、資料調取期間。

五、資料調取人員。

六、資料蒐集機關。

3. 核發調取票之程序，不公開之。

4. 情形急迫而不及事先聲請者，檢察官應於調取後三日內陳報該管法院補發調取票。法院認為不應准許者，檢察官應立即將已取得之車牌辨識資料銷毀。

5. 檢察官、檢察事務官、司法警察官偵查最重本刑三年以上有期徒刑之罪，有事實足認第一項所列車牌辨識資料於本案之偵查有必要性及關連性時，得以書面命令記載第二項各款事項，調取未達連續二十四小時且六個月內累積未達二日的車牌辨識資料。

6. 依本條實施車牌辨識資料之調取，應於通知無害於偵查目的時，書面通知受調取人。若於調取後三個月內仍未通知，應向法院陳報未通知之原因。逾期未陳報者，法院應於十四日內主動通知受調取人。

7. 車牌辨識資料調取目的達成後，應立即銷毀。

本文參考德國《刑事訴訟法》第 163f 長期監視條款，以「連續 24 小時或累積達 2 日」為分界點，區分長期及短期的車牌辨識資料調取，於長期資料調取情形，既然隱含形塑特定人人格圖像的嚴重風險，則必須適用重罪原則及法官保留，由客觀中立的法官決定檢察官所聲請的調取資料範圍是否合於比例原則。而於短期資料調取情形，由於尚不會產生上述風險，為了使實務上得以更有效率地處理車輛失竊等問題，故將其調取程序設計為「非輕罪原則」，並且得由檢察官、檢察事務官及司法警察官自行為之，不過，仍然課予其記錄義務，供後續監督及救濟所用。立法者亦可考量特定犯罪的偵查實務需求，設計類似《跟蹤騷擾防制法》第 18 條第 4 項之例外規定，使其不受此處「重罪原則」及「非輕罪原則」之限制，併與敘明[453]。此外，基於被告以外之第三人並非國家刑罰權之對象，若欲調

[453] 《跟蹤騷擾防制法》第 18 條第 4 項：「檢察官偵查第 1 項之罪及司法警察官因調查犯罪情形、蒐集證據，認有調取通信紀錄及通訊使用者資料之必要時，不受通訊保障及監察法第 11 條之 1

doi:10.6342/NTU202403953

取其車牌辨識資料以偵查犯罪，必須根據相當理由可認為該人與被告有聯繫或將建立聯繫，且若以其他方法調查，合理顯示為不能達成目的或有重大危險情形，始得為之。另一方面，考量車牌辨識資料之蒐集、儲備與調取均為秘密實施，自有必要課予偵查機關通知義務，以利受干預人得知其資料曾受調取之事實，並明確告知資料調取之案由及範圍，使受干預人得對此提起救濟。又，為避免偵查機關泛泛以偵查需求為由，遲遲不肯踐行通知義務，應命其在一定期間經過後，陳報法院尚未通知之緣由，並且於其逾期未陳報時，由法院通知受干預人，鞏固其救濟權利。

第三節　即時比對功能的使用

除了預防性地儲備所有通過車牌辨識系統用路人之行車資料，待日後產生偵查需求時再予以調取的預防性資料儲備模式之外，自動車牌辨識系統同時還具備了即時比對的重要功能。例如新北市政府警察局所建置的自動車牌辨識系統（智慧型雲端影像檢索系統，俗稱「雲龍系統」），就具有「特定目標即時告警功能」，警員只需於系統上先行輸入特定車號，俟車輛行經警用車牌辨識攝影機時，系統即會立即發送簡訊或電子郵件通知特定人員，使警員得以即時追查特定車號之車輛行蹤[454]。此種即時比對功能通常是基於特定車牌號碼之所有人或使用人的犯罪嫌疑，基於犯罪追訴之目的而試圖釐清其行蹤或身分。因此，必須探究我國現行法下是否存在以刑事追訴為目的實施此種即時比對功能的授權依據。

同時，必須注意的是，根據德國聯邦憲法法院 2018 年第二次車牌辨識裁判的見解，此種即時比對功能的實施，除了對於資料經比對符合而行蹤被揭露的特定人構成個人資訊自決權（資訊隱私權）的干預之外，其他用路人雖然得以相安無事地繼續行駛於道路上，看似沒有受到任何不利處分，但是，實際上此種措施

第 1 項所定最重本刑 3 年以上有期徒刑之罪之限制。」

[454] 參考：臺灣新北地方法院 111 年訴字第 1180 號刑事判決。

doi:10.6342/NTU202403953

會對於所有用路人產生時時受到檢查的心理壓力，亦即其之所以能夠繼續不受阻礙地行駛於道路上的前提，是其已經通過警方的檢查且適時不具備警方所需要的資訊[455]。有鑑於此，如何避免警方濫用此種自動比對並篩選特定人的措施，以降低其對於人民自由行使基本權利的影響，就變得至關重要。對此，本文認為於適用上至少必須排除輕微犯罪的偵查情形，才不會導致人民因為涉及「誹謗罪」或「公然侮辱罪」此等輕微犯罪，其行蹤就必須被員警以科技方法揭露。基此，本文認為必須限於偵查最重本刑三年以上之罪，且一旦達成確認特定人身分或行蹤的目的，即須終止措施的實施，不得繼續探知特定人的行車軌跡。同時，更應課予偵查機關記錄措施實施以及通知受比對人的義務，以利後續監督及救濟。另一方面，倘若偵查機關使用即時比對的功能，不僅止於查明特定人的行蹤或身分，而是欲持續探知其行車軌跡，以利偵查線索的蒐集，則此時自動車牌辨識系統作為一種新型態的監視手段，考量完整行車軌跡背後所隱含探知特定人家庭、政治、宗教、性相關資訊的風險，即有必要透過法官保留程序，確保受監視的對象與期間長短，和其所涉犯罪嫌疑相互權衡之下，符合比例原則之誡命。

第一項　《刑事訴訟法》第 122 條

關於是否得以我國《刑事訴訟法》搜索之相關規定，作為以自動車牌辨識系統實施即時比對功能的授權依據，必須先予說明的是，我國搜索規定與美國憲法意義上的搜索有所不同。美國憲法意義上搜索的判斷方式，可區分為基於是否「物理侵入」憲法所保護區域的「財產權標準」，以及是否侵害人民合理隱私期待的「隱私權標準」。而在 *Jones* 案之後，國家機關並未「物理侵入」憲法所保護區域，但涉及破壞人民隱私期待的情形，基本上都會落入美國憲法增修條文第 4 條搜索的討論範圍，判斷其是否須具備相當理由並遵循令狀原則。與之相對的，我國憲法對於基本權有著更細緻的分類，並且於《刑事訴訟法》對應特定措施所干

[455] Vgl. BVerfG, NJW 2019, 827, 830 (Rn. 50 f.).

doi:10.6342/NTU202403953

預基本權的類型與程度不同，分別設計「搜索」、「身體檢查處分」和「通訊監察」等授權規定。據此，若欲以我國《刑事訴訟法》搜索之相關規定，作為實施自動車牌辨識即時比對功能的授權基礎，則必須詳細探究其所規範的基本權干預情境是否確實相符。

對此，觀察《刑事訴訟法》搜索之相關規定，即可知我國搜索是以公開實施為原則[456]。例如，《刑事訴訟法》第 145 條規定，執行人員除依法得不用搜索票之情形外，應向在場人員提示搜索票；又，依第 148 條至第 150 條規定，執行人員須命令或通知特定人在場。對比之下，自動車牌辨識系統的即時比對功能既然是以隱密的方式實施，自然應認為其並不在我國《刑事訴訟法》搜索規定的授權範圍之內。蓋干預措施的施行係公開或隱密，事實上涉及受干預人得否在事前及事中及時提起救濟，並有效地在措施實施當下中斷偵查機關的違法取證行為。以隱密方式實施的干預措施，事實上剝奪了上述可能，迫使受干預人僅得在措施施行結束後，才得以通知等方式得知其基本權曾受干預之事實，且在此時點才可以開始主張權利救濟，顯然是更為嚴重的基本權干預情形。立法者如欲授權偵查機關得以隱密方式干預人民基本權利，應於授權基礎中明確規範，而非謂現行法下並無隱密偵查的相關規範，偵查機關即得使用原則上應以公開實施的偵查手段逕行為之。據此，既然我國搜索是以公開實施為原則，偵查機關不得以此實施自動車牌辨識系統的即時比對功能。

第二項　《刑事訴訟法》第 230 條、第 231 條

前已述及，《刑事訴訟法》第 230 條、第 231 條雖然得作為司法警察一般調查權限的授權依據，但考量其法律明確性有相當程度的疑慮，解釋適用上只能限於絕對輕微的基本權干預情形。本文此處所討論的即時比對功能，係以科技方法

[456] 薛智仁（2018），〈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 48。

doi:10.6342/NTU202403953

秘密描繪特定人行車軌跡，進而查緝其身分及行蹤，此等資料的蒐集隱含探知特定人私人生活的風險，又是以秘密方式實施而不利受干預人及時救濟，自然不得認為係屬輕微之干預情形，警察機關不得以《刑事訴訟法》第 230 條、第 231 條作為以自動車牌辨識系統實施即時比對功能的授權依據。

第三項　《個人資料保護法》第 15 條、第 16 條

我國實務上曾經發生一件令人匪夷所思的事情。交通部高速公路局（以下稱「高公局」）基於收費目的，與遠通電收公司合作在全臺高速公路上架設 ETC 收費門架、車輛偵測器及攝影機等相關設備（以下稱「ETC 設備」），由於當時警政署尚未自行建置完整的自動車牌辨識系統，便希望高公局能夠將 ETC 設備所蒐集的車牌號碼，結合警政署建立的「高速公路涉案車輛即時通報系統」，於車輛通過 ETC 設備收費時自動比對其是否為失竊車輛或涉案車輛，並且在比對結果符合時，由高公局將車牌辨識資料傳輸予警政署供後續偵查犯罪所用。為確保其行為合於《個資法》規定，警政署曾發函詢問法務部，並且得到肯定的答覆。法務部認為[457]：高公局為協助警政署偵察刑事犯罪而開放 ETC 設備所蒐集之資料供通報系統進行比對，就高公局而言，屬於目的外利用個人資料的行為，而預防或追訴犯罪既然是「為維護國家安全或增進公共利益」之情形，即符合《個資法》第 16 條但書第 2 款的規定；此外，警政署以通報系統取得比對符合車輛的車牌辨識資料，屬於個人資料的蒐集行為，基於「犯罪預防及刑事偵查」為警政署法定職務之一環，且其並非事前、全面地蒐集車牌辨識資料，而僅蒐集與利用比對結果符合者之資料，因此肯認其資料蒐集行為符合《個資法》第 15 條第 1 款所定「執行法定職務必要範圍內」，其資料利用行為則合於《個資法》第 16 條本文規定，屬於法定職務範圍內之利用[458]。

[457] 106 年 8 月 7 日法務部法律字第 10603510070 號函。
[458] 高公局後續制定的「交通部高速公路局受理公務機關調閱國道 ETC 收費系統資料作業程序」，其內容基本上同於《個資法》之規定。

doi:10.6342/NTU202403953

法務部依循《個資法》第 16 條「為維護國家安全或增進公共利益」以及第 15 條「執行法定職務必要範圍內」此等寬泛的要件，肯認警政署得以常態式地透過涉案車輛即時通報系統介接高公局基於收費目的所架設的 ETC 設備，即時比對並蒐集、利用特定人的行車資料。若依此見解，國家機關只要是為了執行法定職務，似乎即可不受阻礙地蒐集、處理和利用個人資料，試問：國家機關的何等作為並非是為了增進公共利益呢？「必要」的要件真的能夠將國家機關蒐集、處理或利用個人資料的行為限於符合比例原則的情形嗎？還是會導致個人資料一經國家機關蒐集，即會在各個機關之間流通？對此，我國學說見解即有認為，《個資法》第 15 條第 1 款所稱「法定職務」僅是在宣誓公務機關於何種情況下蒐集個人資料始為合法，本身並無授權國家機關得在何等要件下採取何種個人資料蒐集措施，而只是一個組織法的規定，國家機關若欲蒐集個人資料，必須另外具有作用法性質的法律依據，不能僅憑組織法的抽象規定對人民採取干預基本權的措施[459]。有基於此，於我國警方尚未具備以刑事追訴為目的蒐集、利用車牌辨識資料之授權基礎的前提下，自然不得允許警政署依據《個資法》第 15 條規定，取得高公局為達收費目的而以 ETC 設備蒐集的車牌辨識資料[460]。

尤有甚者，如前所述，自動車牌辨識系統的即時比對功能雖然僅會使警方取得符合比對名單的特定車牌資訊，然而，事實上是強迫所有用路人不停地接受檢查。倘若此等檢查措施無須受到限制，即會導致用路人陷於時刻受到檢查的心理壓力之中。因此，本文主張應參考德國《刑事訴訟法》第 163g 條規定，排除輕微犯罪偵查情形的適用，並且在措施達成確認特定人身分或下落的目的時即予終

459 謝碩駿（2019），〈行政機關蒐集個資之法律依據〉，《月旦法學教室》，198 期，頁 16；李建良（2017），〈資料流向與管控環節－個資保護 ABC〉，《月旦法學雜誌》，272 期，頁 28；李建良之發言紀錄，參考：邱文聰、林子儀、張陳弘、顏厥安、范姜真媺、陳銘雄、李建良、吳全峰、陳昭如（2018），〈最高行政法院一〇六年度判字第五四號判決（健保資料庫案）會議記錄〉，《月旦法學雜誌》，272 期，頁 79；蔡宗珍，前揭註 151，頁 83-84；范姜真媺（2018），〈檢視行政機關蒐集利用個資之問題及展望〉，《法學叢刊》，63 卷 2 期，頁 37；范姜真媺（2019），〈自實務判決檢視行政機關蒐集、處理或利用個人資料之問題〉，《警察法學》，18 期，頁 95-96。

460 相同見解：田炎欣(2014)，〈警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討(下)〉，《台灣法學雜誌》，257 期，頁 89-90；蔡震榮，前揭註 445，頁 199-200。

doi:10.6342/NTU202403953

止，避免持續取得行車資料，描繪完整行車軌跡後產生探知特定人私人生活的風險。同時，倘若偵查機關欲以類似 GPS 的方式，將自動車牌辨識系統作為新型態的監視工具，長期監視特定人的行蹤，則必須適用法官保留程序。據此，倘若如法務部函釋所言，警政署得依《個資法》第 15 條逕行取得高公局基於收費目的所蒐集的車牌辨識資料，則如何能確保警方對所有用路人實施檢查的措施，是為了偵查相對嚴重的刑事犯罪，而維護了同等重要的公共利益，且其對特定人行車資訊的取得甚至是長期監視特定人行蹤的情形，整體均符合比例原則？因此，考量《個資法》第 15 條組織法的性質，其要件過於空洞，並未授權國家機關得據此干預人民基本權利，更無法藉此有效控制國家機關的個人資料蒐集行為符合比例原則，本文認為警方不得依《個資法》第 15 條取得高公局或其他國家機關所蒐集的車牌辨識資料，用於即時與涉案車輛名單相互比對。

第四項　《刑事訴訟法》第 153 條之 1

有鑑於偵查實務上高度借重科技設備的新興調查方法與日俱增，立法院於 2024 年 7 月 16 日三讀通過《刑事訴訟法》第 11 章之 1「特殊強制處分」。其中，新增《刑事訴訟法》第 153 條之 1 授權偵查機關對被告或有相當理由認為與被告有所關聯之第三人，使用全球衛星定位系統（GPS）或「其他非以辨識個人生物特徵之科技方法」追蹤位置，是否得作為偵查機關使用自動車牌辨識系統追蹤位置之授權依據？遂有疑義[461]。

---

[461] 《刑事訴訟法》第 153 條之 1：

I. 為調查犯罪情形或蒐集證據認有必要時，得使用全球衛星定位系統或其他非以辨識個人生物特徵之科技方法對被告或犯罪嫌疑人追蹤位置。

II. 對第三人實施前項調查，以有相當理由可信與被告、犯罪嫌疑人、證人或應扣押之物或電磁紀錄有所關連時為限。

III. 前二項實施期間，不得逾連續二十四小時或累計逾二日，實施當日不足二十四小時，以一日計。有再次或繼續實施之必要者，至遲應於再次實施前或期間屆滿前，由檢察官依職權或由司法警察官報請檢察官許可後，以書面記載第一百五十三條之五第一項各款之事項與實施調查之必要性及其理由向該管法院聲請核發許可書。

IV. 實施第一項、第二項調查前，可預期實施期間將逾連續二十四小時或累計逾二日者，得於實施前，依前項規定向該管法院聲請核發許可書。

V. 前二項法院許可之期間，每次不得逾三十日。有繼續實施之必要者，至遲應於期間屆滿之

doi:10.6342/NTU202403953

首先必須辨明的是，本條所授權的干預對象僅限於被告、犯罪嫌疑人或「有相當理由可信與被告、犯罪嫌疑人、證人或應扣押之物或電磁紀錄有所關連」之第三人，亦即，不及於不具備法律上原因之一般人。因此，此種旨在刑事追訴之干預措施，自然不得作為於具體犯罪或危險尚未發生，即預防性儲備車牌辨識資料的授權依據。換句話說，我國警察機關於實務上利用自動車牌辨識系統，不區分受干預人是否具備法律上原因，一律長期、大量地預防性儲備車牌辨識資料，再於嗣後調取的作為（記錄模式），不得依此規定主張其行為適法。

其次，有疑義者在於：《刑事訴訟法》第 153 條之 1 是否得作為偵查機關使用自動車牌辨識系統之即時比對功能，追蹤特定人位置的授權依據？也就是說，在不涉及預防性資料儲備的前提下，依循近似於德國《刑事訴訟法》第 163g 條「追緝模式」的實施方法，將比對不符合者的資料立即刪除而僅保存比對符合者的資料，是否即可將《刑事訴訟法》第 153 條之 1 作為偵查機關以「追緝模式」實施自動車牌辨識系統的授權依據？

對此，基於自動車牌辨識措施對於一般人民可能產生的恫嚇效果，本文認為縱使不涉及預防性資料儲備，新增《刑事訴訟法》第 153 條之 1 仍然無法作為實施「追緝模式」之授權依據。申言之，相比於僅針對單一特定人的 GPS 偵查措施，「追緝模式」係在茫茫人海中以一種流刺網式持續檢查的手段追蹤特定人之位置，由於不以干預對象具備法律上原因為要，而事實上涵蓋了所有人，2018 年第二次車牌辨識裁判即已指出此種隱密實施的檢查措施可能會使人民產生一種受到監視的感覺，進而影響其基本權利的自由行使，甚至整體地影響社會自由[462]。被檢查的車輛駕駛人必須不具備任何警察機關適時所需的特定資訊，才能繼續不受阻礙地行駛於道路上，此種檢查行為本身就應該被認為干預了人民的自由，因為公民基本上可以在不被國家任意記錄、不需要說明自己的行為是否正當、不暴

二日前，由檢察官依職權或由司法警察官報請檢察官許可後，以書面記載具體理由向該管法院聲請核發許可書。

462 BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 98.

doi:10.6342/NTU202403953

露在持續受監視的感覺下四處活動，這是共同體自由的特質之一。如果這類措施可以在任何時間、地點，基於任何目的檢查行經車輛是否被列於追緝名單上，根本無法通過比例原則的審查[463]。有鑑於此，即使德國《刑事訴訟法》第 100h 條結合第 163f 條已授權偵查機關使用 GPS 追蹤特定人的位置，德國立法者仍舊考量「比對措施」對於人民帶來的嚴重基本權干預，而於 2021 年另行制定《刑事訴訟法》第 163g 條[464]。

面對此種事實上涵蓋所有人，而可能對人民產生恫嚇效果，並影響社會自由的干預措施，於授權規定的設計上應注意到以下三點：其一，必須在授權基礎中清楚規範國家機關得以蒐集與比對的資料範圍、干預措施的實施範圍，以及基於何種目的始得為之，如此方符合法律明確性原則、目的拘束原則及資料最小化原則。其二，應排除將此種干預措施用於輕微犯罪的偵查情形，避免人民因秘密承受檢查措施的心理壓力持續擴大，影響社會自由甚鉅而無法通過衡平性的審查。其三，應課予實施機關明確的記錄義務，以利受干預人後續提起救濟，並使司法得以審查其措施之施行是否符合法定要件。

有基於此，《刑事訴訟法》第 153 條之 1 第 1 項所稱「其他非以辨識個人生物特徵之科技方法」，雖然在文義上似乎包含自動車牌辨識系統，然而有鑑於經量化後的個人資料具有更高強度相互連結的便捷性與可能性，於授權規定上應清楚規範出得以蒐集與比對之資料種類與範圍，方可符合法律明確性的要求，例如可蒐集與比對的資料僅及於車牌號碼以及通過特定地點之時間，而不及於車內乘客或路上行人的衣著打扮。基於 GPS 偵查手段所設計的《刑事訴訟法》第 153 條之 1，對於此等要件均付之闕如，於條文中根本無從知悉偵查機關得以蒐集與比對人民的何等資料，更遑論條文中並未規定「比對不符合者之資料必須立即刪除」此一重要程序，倘若貿然以此使用自動車牌辨識系統，無法完全排除預防性資料儲備的疑慮，難以有效地限制系爭措施的干預程度，於法律明確性原則的觀點下，

[463] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, Rn. 51.
[464] Vgl. BT-Drs. 19/27654, S. 84-85.

doi:10.6342/NTU202403953

無法作為以「追緝模式」實施自動車牌辨識的授權依據。

此外，為了避免人民必須時時刻刻接受自動車牌辨識系統檢查其身分資訊，加深其心理壓力，影響人民基本權利之自由行使，本文認為自動車牌辨識系統的即時比對功能，雖無須適用重罪原則，惟仍須排除將其用於輕微犯罪的偵查情形，方為衡平。具體而言，應限於偵查最重本刑三年以上之罪，始為妥適。《刑事訴訟法》第 153 條之 1 係以 GPS 此種單一對象的偵查手段為考量基準，在要件設計上並未慮及自動車牌辨識系統此種秘密檢查措施對於一般人民可能產生的心理壓力，因此並未排除輕微犯罪的偵查情形，不宜作為以「追緝模式」實施自動車牌辨識的授權依據。

最後，《刑事訴訟法》第 153 條之 1 於實施期間未超過連續 24 或累積未達 2 日的短期實施情形，並未課予偵查機關記錄曾實施系爭措施的義務。對此，筆者僅能猜測或許是因為實務上短期 GPS 偵查的情形較為罕見[465]，致使此處的記錄義務未受重視。不過，不同於 GPS 偵查需要實地裝設而多用於長期追蹤特定人位置的情形，自動車牌辨識系統僅需於公務電腦中輸入特定車牌號碼，即可迅速且即時地取得特定人的車輛位置資訊，過去曾發生的「新北員警監視老婆案」，員警便是透過公務電腦多次短期地登入系統監視老婆行蹤。有鑑於此，縱使是使用自動車牌辨識系統短期追蹤特定車輛位置的情形，為了防免警察機關「化整為零」，規避發動系爭措施所應遵循的法定要件，記錄義務實屬至關重要。《刑事訴訟法》第 153 條之 1 漏未規範短期追蹤情形的記錄義務，再度顯示無法作為「追緝模式」之授權規定。

第五項　立法建議

鑑於我國現行法下並無以刑事追訴為目的，實施自動車牌辨識與即時比對的授權基礎，本文以下嘗試提出立法建議。

[465] 李榮耕，前揭註 111，頁 958。

doi:10.6342/NTU202403953

新增《刑事訴訟法》第 153 條之 12 全文如下：

1. 檢察官、檢察事務官、司法警察官、司法警察偵查最重本刑三年以上有期徒刑之罪，有事實足認措施有助於辨識被告或犯罪嫌疑人之身分或其所在地，得於公共交通場域秘密以科技方法自動蒐集車牌號碼、時間、地點及行駛方向。
2. 依第一項蒐集之車牌號碼得與下列車牌資料進行自動化比對：

   一、車牌號碼核發給被告或由被告使用。

   二、車牌號碼核發給被告以外之人或由該人使用，且根據相當理由可認為該人與被告有聯繫或將建立聯繫，若以其他方法調查，合理顯示為不能達成目的或有重大危險情形。
3. 自動化比對應在第一項自動蒐集資料後儘速為之。當有比對結果符合時，應儘速以人工方式檢查是否確實相符。當比對結果不符或經人工檢查確認比對結果不符時，第一項所蒐集之資料應立即刪除或依警察職權行使法第十條之一規定處理，不得利用。
4. 第一項之命令應以書面為之，並詳細記載以下事項：

   一、案由及涉嫌觸犯之法條。

   二、自動化比對對象及理由。

   三、措施實施地點及時間。

   四、措施實施機關及人員。
5. 當措施發動要件已不存在，或已確認被告或犯罪嫌疑人之身分或其所在地，應儘速終結措施。
6. 已確認被告或犯罪嫌疑人之身分或其所在地，仍有實施之必要者，應由檢察官或司法警察官報請檢察官許可後，以書面記載第四項各款事項，聲請該管法院核發許可書。使用前項科技方法前，預計確認被告或犯罪嫌疑人之身分或其所在地後仍將繼續實施者，亦同。
7. 措施終結後，應以書面通知受自動化比對對象第四項所記載之事項。

doi:10.6342/NTU202403953

為了避免刑事追訴機關於輕微犯罪的偵查情形，就使用即時比對功能掌握特定人的行蹤，加深即時比對功能此種檢查措施可能對人民造成的心理壓力，因此，本文將其發動要件設定為「偵查最重本刑三年以上有期徒刑之罪」，並且參考德國《刑事訴訟法》第 163g 條的規定，透過「有事實足認措施有助於辨識被告或犯罪嫌疑人之身分或其所在地」的要件，限縮偵查機關得以實施即時比對功能的公共交通場域，避免其配合移動式車牌辨識系統，恣意且全面覆蓋式地實施比對。同時，明確地將資料可蒐集範圍限定在「車牌號碼」、「時間」、「地點」及「行駛方向」，控制比對措施對於人民資訊隱私權的干預程度。此外，考量被告以外之第三人並非國家刑罰權的對象，自有必要設定更高的發動門檻，因此限於「根據相當理由可認為該人與被告有聯繫或將建立聯繫，若以其他方法調查，合理顯示為不能達成目的或有重大危險情形」。

另一方面，為了避免偵查機關藉故實施即時比對，卻遲遲未進行比對而在手邊保留大量的車牌辨識資料，新增《刑事訴訟法》第 153 條之 2 第 3 項規定自動化比對應於資料蒐集後儘速為之，偵查機關僅可保留並利用比對符合的車牌辨識資料，比對不符合或是經人工確認後不符合者，系統應立即將該資料自動刪除，或是依照新增定的《警察職權行使法》第 10 條之 1 規定，以符合當前科技發展水準的技術加密後儲備於資料庫內，並僅於未來符合車牌辨識資料調取授權時方得予以調取，偵查機關不得逕行利用之。同時，為了避免偵查機關掩蓋實施自動化比對的事實，並協助受干預人及法院事後審視偵查機關比對行為的合法性，於第 4 項規定課予其紀錄措施實施的義務。此外，第 153 條之 2 第 1 項作為偵查機關確認特定人身分或下落的手段，原則上一旦捕捉到特定人的行蹤後，即可迅速實施逮捕等後續措施，尚不至於對特定人產生完整行車軌跡遭描繪後，私人生活被探知的風險。因此，一方面由第 5 項規定當措施發動要件已不存在，或者已達成確認被告身分或其所在地之實施目的，即應終止措施的施行，控制其對於受比對人干預資訊隱私權的程度；另一方面基於門檻理論的觀點，既然已排除基於輕微犯罪偵查而恣意實施的可能性，又課予偵查機關終止時點的限制以及紀錄義務，

doi:10.6342/NTU202403953

而將此種措施對於人民資訊隱私權的干預控制在一定程度，考量實務上大多將其用於查緝贓車的情形，為與偵查效率求取平衡，因此授權檢察官、檢察事務官、司法警察官及司法警察得自行為之。不過，倘若偵查機關欲將自動車牌辨識系統的即時比對功能，用作類似 GPS 的監視工具，於確認被告身分或其所在地後繼續探知其行車資訊，則有必要適用法官保留程序，確保措施的施行在個案中符合比例原則，因而另外定有第 6 項規定。最後，本條第 1 項及第 6 項所授權的自動車牌辨識即時比對，均是以隱密方式實施，為了使受干預人得以主張權利救濟，應於措施終結後，以書面通知受自動化比對對象第 4 項所記載之事項。

第四節　監督機制

行文至此，雖然本文已經對於預防性車牌辨識資料儲備措施的實施地點作出限制，並將資料儲備期間限於 6 個月；且針對車牌辨識資料的調取授權也依照資料時間長短所反映出的資料量，作出不同程度的重罪門檻與程序擔保；更原則性地排除偵查機關將即時比對功能用作監視工具的可能性，例外賦予法官保留程序的保障。然而，本文所提出的立法建議，仍然使自動車牌辨識系統的實施隱含許多風險：

第一項　立法建議的不足之處

第一，為了避免自動車牌辨識系統實施地點之公布，將有害其追查特定人身分或行蹤之目的，甚至促使警察機關更全面覆蓋式地架設自動車牌辨識系統，將人民完整的行車軌跡悉數網羅於資料庫內，產生嚴重的心理壓力以及資料外洩風險，本文主張應使自動車牌辨識系統繼續以隱密的方式實施。然而，這同時也表示，人民無法同路口監視器的設置情形一般，在政府機關的網站上取得設備架設的實際地點，並逐一檢視其是否符合法定要件，而非恣意架設。則縱使在干預授權基礎上規範實施地點的限制，是否會因為難以監督而淪為空談，進而導致自動

doi:10.6342/NTU202403953

車牌辨識系統最終同我國路口監視器的現狀一般，舉目皆是？

第二，目前我國自動車牌辨識系統是由各縣市警察局分別架設，各自蒐集資料後儲備於其資料庫內，並由警政署執行資料庫的整合，換句話說，除了各縣市本身的資料庫內存有車牌辨識資料以外，更可透過警政署的整合系統調取其他縣市所蒐集的車牌辨識資料，則如何確保各個縣市所儲備的車牌辨識資料於 6 個月的儲備期間經過後，均是以不可回復的方式銷毀，並且於資料調取、利用目的達成後確實刪除，以避免資料持續累積而得以掌握特定人過去一年甚至三年、五年的完整行車軌跡，亦成問題。

第三，本文基於門檻理論的思維，將部分干預程度相對輕微的自動車牌辨識系統使用情形，例如未達連續 24 小時且 6 個月內累積未達 2 日的車牌辨識資料調取，以及一旦確認被告身分或其所在地即予終止的即時比對功能實施，授權檢察官、檢察事務官、司法警察官甚至是司法警察得自行為之，並且期待能透過「記錄義務」以及「通知義務」的設計，確保其施行符合法定要件。然而，前述新北員警使用雲龍系統「特定目標即時告警功能」監視老婆及其友人行蹤的案例中，員警監視老婆的期間長達 8 個月，總共取得了 600 多筆資料，事情曝光後警方查閱系統紀錄，發現該名員警在此期間內一共違法查詢了特定人行車資料 156 次，調取時間及對象均有清楚的數據紀錄，這 8 個月以來卻完全沒有其他警員發現異常。由此可知，記錄義務所能發揮的監督功能亦有其極限，為了顧及偵查效率及職務分配，而在特定情形授權偵查機關甚至是司法警察得自行為之，是否會適得其反，也值得進一步思考。

第二項　建置監督機制的必要性

上述問題，本文反覆思量許久，最終認為應從自動車牌辨識系統的設計以及監督機制的建構著手，確保其施行情形符合法定要件所設，以達立法者所預想之權衡結果。具體而言，應可區分為各縣市警察局及警政署之內部監督功能，以及

doi:10.6342/NTU202403953

警政署以外，獨立監督機關之建置。以下分別論述：

第一款　內部監督單位

首先，為了避免司法警察化整為零，刻意使用相對輕微的干預授權基礎規避長期監視或調取資料所應適用的嚴格要件，並使記錄義務發揮其所應具備的監督功能，本文認為在自動車牌辨識系統的設計上，應將各派出所之公務電腦針對同一車牌號碼所得查詢的資料量，限制在未達連續 24 小時且 6 個月內累積未達 2 日的時間範圍。倘若超出此一範圍，系統將拒絕存取指令的要求，員警必須向各縣市警察局的單一窗口申請調取。如此一來，其申請調取的過程中勢必需要向申請窗口提出法院所核准的調取票，或者是以書面表示適時所偵查的重大犯罪以及情況急迫的原因，始可調取。亦即透過各縣市警察局單一調取窗口的建立，避免「新北員警監視老婆案」中，員警自行使用派出所公務電腦持續調閱資料的情形再度發生。另一方面，自動車牌辨識系統也可以在特定車牌號碼多次被加入比對名單，或者實施比對取得資料時間過長時，自動跳出警示通知，使各縣市警察局或是警政署的內部監督單位得知相關訊息，並要求實施比對功能的員警說明事由。例如，一般情形下查緝贓車只需要 2 個小時即可確認被告的行蹤，特定車牌號碼基於查緝贓車的原因被加入比對名單，已取得位置資訊後措施卻繼續施行，長達 7 日仍未終止，甚至在近期頻繁地被加入比對名單之中。此際，內部監督機關應可在系統中祕密設置跳出警示通知的各種要件，以利其篩選並追查可能的違法使用情形。

至於上述措施具體的法律依據，本文認為或可依據《個資法》第 18 條規定，將警察機關保有車牌辨識資料所應辦理的「安全維護事項」，納入《個資法施行細則》第 12 條第 2 項所規範得包括之「配置管理之人員及相當資源」（第 1 款）、「個人資料之風險評估及管理機制」（第 3 款）、「事故之預防、通報及應變機制」（第 4 款）、「個人資料蒐集、處理及利用之內部管理程序」（第 5 款）以及「使

doi:10.6342/NTU202403953

用紀錄、軌跡資料及證據保存」(第 10 款),並以此建構上述之單一調取窗口、內部監督單位以及系統自動提示警示通知的功能。或者,亦可考慮直接增定於前述《刑事訴訟法》第 153 條之 11 及第 153 條之 12 的規定之中[466]。

第二款　外部獨立監督機關

然而,即使內部監督單位和警示通知功能的設計,能夠解決司法警察化整為零的疑慮,資料儲備期間屆滿後是否確實刪除?或者因為記憶體尚有空間就繼續留存?自動車牌辨識系統的設置地點是否違反法定要件?甚至配合移動式車牌辨識而全面覆蓋式地施行?這些問題,都不會因為內部監督單位的建立就迎刃而解。因此,本文認為有必要於各縣市警察局及警政署之外,從外部建構獨立監督機關來處理此事。

對此,我國釋憲實務有關個人資料保護之獨立監督機關的討論,首見於司法院釋字第 603 號解釋:「主管機關尤應配合當代科技發展,運用足以確保資訊正確及安全之方式為之,並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施,以符憲法保障人民資訊隱私權之本旨。」雖然本號解釋主要是以指紋資料庫應具備的防護措施為討論核心,不過,許宗力大法官與曾有田大法官共同提出的協同意見書中提到:「資訊科技之發達,固使國家得以更快速、方便的自動化方式蒐集、儲存、利用與傳遞個人資訊,但同時也使儲存於國家資料庫中之個人資訊處於外洩或遭第三人竊取、盜用之更大風險中。是基於基本權的保護義務功能,國家有義務採取適當之組織與程序上保護措施,使個人資訊隱私權免於遭受第三人之侵害。同時基於當代資訊科技發展之開放性,國家並有義務不斷配合資訊科技發展的腳步,採取隨科技進步而升級之動態性的權利保護措施,以有效保護人民之資訊隱私權。為確保此項目標之達成,國家所採取組織保護措施並應包括設

[466] 學說上有見解認為《個資法施行細則》第 12 條僅臚列若干項目,並未具體規範其要件與內涵,更未課予操作的義務,而充其量只是指引式的規範內容。參考:張志偉(2023),〈個資保護與資料安全〉,《當代法律》,22 期,頁 15-16。

doi:10.6342/NTU202403953

置獨立、專業之資訊保護官，以幫助在資訊科技洪流中不具有自保能力之一般人民保護其個人資訊安全。」林子儀大法官的協同意見書也指出：「人民面對國家資訊蒐集的無奈之一是，一旦個人資訊脫手，個人其實已經很難再有控制之可能。且除非具體問題發生，否則人民對於機關內部的資訊保管及運用情形，實則一無所悉，也無從確認國家是否良好地保護其資訊安全並予以正當使用。本案突顯行政上對個人資料使用範圍及目的低度管制的實務，尤其是一項重大警訊。如果行政機關能夠事先對資料庫建立法制、技術、組織及程序上的種種安全閥，以確保所蒐集資料之安全與正當使用，例如由建立行政之獨立管制機關，代替缺乏專業能力的一般民眾監督政府資料庫之運用情形，而非率爾大規模啟動強制性的指紋資料蒐集，而對嗣後資訊保管與運用之管制草草帶過，則國家蒐集資訊之正當性亦將隨之提高。」近 17 年後，憲法法庭 111 年憲判字第 13 號判決再次引述司法院釋字第 603 號解釋的用語時，去除了「指紋」相關的說詞，而表示：「就資訊隱私權之保障而言，除應以法律明確訂定蒐用個資之目的及要件外，應配合當代科技發展，運用足以確保資訊正確及安全之方式，並對所蒐集之個資採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨（司法院釋字第 603 號解釋參照）。」就此明顯是認為，此種組織上與程序上必要之防護措施，為保障人民資訊隱私權重要之一環，而非僅限於指紋等高敏感性個人資料的蒐集、處理或利用情形，始有適用。

可惜的是，面對我國個人資料保護相關法制欠缺獨立監督機關的現狀，111 年憲判字第 13 號判決僅作成警告性宣示，不願作出違憲宣告。蔡宗珍大法官提出的部分協同、部分不同意見書中認為，獨立監督機關的建立與否與本件聲請案之訴訟標的無涉，大法官既然並未在審理過程中周全地實質審查相關法制，則僅得作成警告性宣示。然而，其也表示：「於公務機關取用個資之情形，個資當事人欲主張權利尤為困難，蓋個資當事人認識並獲取公務機關違法事證之難度更高；且於進入司法救濟程序前，取用個資之公務機關有「選手兼裁判」之便，進入事後救濟性質之司法救濟程序後，取用個資之公務機關更往往有「木已成舟」之現

doi:10.6342/NTU202403953

實處境及公益目的護持。因此，個資保護架構如未引進第三方監理機制，由不參與個資取用之獨立監督機關掌理人民個資保護任務，並建立個資法領域完整之行政管制體系，則個資當事人面對有極大個資恣意取用空間之公務機關，長期以往，人民憲法上之資訊隱私權恐有實質淪喪之虞[467]。」相對於此，黃昭元大法官於其部分不同意見書則認為，我國《個資法》及其他法律欠缺有關個人資料保護之獨立監督機制，已達違憲程度而應為清楚的違憲宣告，並表示：「或許由於上述解釋宣告（按：司法院釋字第 603 號解釋）強制蒐集全民指紋之戶籍法規定違憲，因而阻止了全民指紋資料庫之建置，以致主管機關也不再構思應如何建立上述解釋所要求之組織上及程序上防護措施，即使其手中一度掌有 6、7 百萬人（主要是受刑人及役男等）之指紋資料。時至今日，個資法或其他相關法律，對於我國政府建置管理之各種資料庫（包括本案涉及之健保資料庫、財政部之財稅資料庫及其他政府機關建置之各類資料庫），均仍無任何有關獨立監督機制（尤其是獨立機關）的明文要求。就此而言，確實是我國有關個人資料保護法制的一大缺陷[468]。」

比較法上，關於德國的個人資料保護監督機制，學說有見解將之稱為「二根支柱之監管模式（Zwei-Säulen-Modell）」[469]，亦即一方面依據《聯邦個人資料保護法》（Bundesdatenschutzgesetz）第 5 條課予公務機關設置「資料保護監察人（Datenschutzbeauftragter）」之義務，其作為機關內部的監督單位，提供個人資料保護法規解釋適用之諮詢，確保機關內部蒐集、處理或利用個人資料的行為遵循法律規定，並且與外部的監督機關保持聯繫；另一方面，依據《聯邦個人資料保

[467] 憲法法庭 111 年憲判字第 13 號判決蔡宗珍大法官提出，林俊益大法官、張瓊文大法官加入之部分協同、部分不同意見書。

[468] 憲法法庭 111 年憲判字第 13 號判決黃昭元大法官提出，許宗力大法官、許志雄大法官、謝銘洋大法官、楊惠欽大法官加入之部分不同意見書。此外，許宗力大法官也認為，透過「建置含獨立第三方監督機制之組織與程序保護規定」，將系爭高敏感特種個資遭濫用或不當外洩的可能性減至最低，方得確保其符合最小侵害之要求。參考：憲法法庭 111 年憲判字第 13 號判決許宗力大法官提出之部分不同意見書。

[469] 李寧修（2022），〈展望健保個資開放利用之新篇章：簡評 111 年憲判字第 13 號判決〉，《當代法律》，11 期，頁 19。

doi:10.6342/NTU202403953

護法》第 8 條以下規定，於聯邦層級設置「聯邦個人資料保護及資訊自由監察官（Bundesbeauftragte für Datenschutz und Informationsfreiheit，BfDI）」[470]，其依同法第 10 條規定完全獨立地行使職權，並得主動或應聲請監督、調查或建議公務機關蒐集、處理或利用個人資料之事務。

至於我國，目前仍係採分散式管理，由中央目的事業主管機關或直轄市政府、縣（市）政府依權責辦理。而為了回應憲法法庭於 111 年憲判字第 13 號判決作成的警示性宣告，2023 年 5 月 31 日《個資法》修正公布第 1 條之 1，規定自「個人資料保護委員會」成立之日起，改由個人資料保護委員會擔任主管機關。同年 12 月 5 日，「個人資料保護委員會籌備處」正式成立，時任行政院長陳建仁表示欲以此建立個人資料保護之獨立監督機制，其職責包括研擬組織法規、修訂個資保護法規、規劃公務與非公務機關個人資料保護事務監督、查核、通報、陳情等相關機制以及規劃推動並執行個人資料保護相關教育訓練、宣導與人才培育等工作[471]。籌備處主任李世德也透露，希望於 2025 年 8 月完成個人資料保護委員會之設置[472]。

本文認為，個人資料保護的獨立監督機制，不僅對於健保資料庫此等高敏感性個人資料的蒐集、處理或利用而言至關重要，從我國自動車牌辨識的實務運作即可得知，即使是處於公共交通場域且依行政法令具有公示性質的車牌資料，經由公務機關系統性自動化蒐集、處理後，也能夠匯聚成特定人完整的行車軌跡，進而對其私人生活產生遭受探知與揭露的嚴重風險。此時，針對此種國家機關秘密實施的資料蒐集措施，倘若不存在具備專業知識與充分資源而得以獨立監督之客觀第三方，不但使人民於事前、事中無法得知其資訊隱私權遭受干預之事實，

---

470 李寧修，前揭註 437，頁 414-415、429-430；李震山（2008），〈公權力運用定位科技措施與基本權利保障〉，城仲模教授古稀祝壽論文集編輯委員會（編），《二十一世紀公法學的新課題——城仲模教授古稀祝壽論文集——I. 憲法篇》，頁 363-364，新學林。

471 行政院網站，https://www.ey.gov.tw/Page/9277F759E41CCD91/fec13417-8b26-466f-a59d-cc1aaee75a25（最後瀏覽日：05/09/2024）。

472 曹悅華（12/05/2023），〈李世德曝個資會籌備處目標　將觸及科技應用〉，《工商時報》，https://www.ctee.com.tw/news/20231205700896-430104（最後瀏覽日：05/09/2024）。

doi:10.6342/NTU202403953

縱於事後順利進入救濟程序，也往往會陷於蔡宗珍大法官所指「木已成舟」的窘境。具體而言，縱使立法者於自動車牌辨識資料蒐集的授權基礎中，充分考量預防性儲備車牌辨識資料對於人民自由行使基本權利所帶來的心理壓力，而在規定中加入實施地點的限制，試圖遏止警察機關全面覆蓋式地實施，實際上也可能會因為欠缺外部獨立的監督機關，而在保持措施秘密實施性質的前提下，無法使警察機關逐年公告自動車牌辨識系統建置地點[473]；此外，資料儲備期間屆滿後是否確實刪除？資料使用目的達成後是否立即銷毀？亦均為措施實際執行上是否貼合立法者預設權衡結果的重要因素。有鑑於此，實有必要透過具備專業知識的外部獨立監督機關，逐年要求警察機關對於自動車牌辨識系統的實施地點提出報告，於監督機關中設置專家學者，共同檢視系統設置的地點與密度是否符合比例原則；同時，不定期抽查警察機關是否符合儲備車牌辨識資料的期間限制、期間經過後資料是否係以不能回復的方式銷毀；並與內部監督單位保持聯繫，審視系統自動警示通知要件的設立是否完善，並介接各縣市警察局的車牌辨識調取系統，檢視調取紀錄上是否出現可疑情形。

如同許宗力大法官於「健保資料庫案」的部分不同意見書所言，我國政府罔顧欠缺第三方獨立監督機制的事實，強制蒐集人民健保資料後逕自為目的外使用，「先上車後補票」（也不知道什麼時候才會補票）、「先做了再說」[474]。我國警察機關也同樣為了偵查犯罪的需求，一股腦兒地在欠缺獨立監督機關，甚至欠缺法律授權的情形下，逕自建置自動車牌辨識系統，大規模儲備人民完整的行車資料。

---

[473] 事實上，即使同路口監視器公布設置地點，倘若缺乏具備專業知識與監督權責的獨立機關，是否能夠發揮監督效果，仍有疑義。例如，依資料顯示，臺北市的路口監視器自 2013 年起即依循學說所述，以同一犯罪類型為判斷標準，並且將特定地區同一期間內的犯罪發生率，與全國、同一縣市、同一鄉鎮市或同一警察轄區的犯罪發生率互相比較。亦即，其注重各個轄區「竊盜」與「暴力」之十萬人口比以及人口密度，有所憑地選擇路口監視器的設置地點。然而，其結果仍如吾人所視，臺北市最終被打造為舉目皆是監視器的城市。這是否符合比例原則？或者事實上肇因於監視器維護治安的迷思而過度干預了人民的資訊隱私權？實有賴專家學者於建置路口監視器的決策階段具體討論。參考：黃郁文、林啟豐、吳松儒等（2013），〈建構臺北市治安電子城牆——新一代錄影監視系統工程實務〉，《中華技術》，100 期，頁 206-207；蔡庭榕、簡建章、李錫棟、許義寶，前揭註 435，頁 257。

[474] 憲法法庭 111 年憲判字第 13 號判決許宗力大法官提出之部分不同意見書。

doi:10.6342/NTU202403953

則我國資訊隱私權的保障是否已「實質淪喪」，答案似乎呼之欲出。雖然，個人資料保護委員會適時仍在籌備階段，甚至曾經以函釋表示海巡機關介接警政署車牌辨識資料庫符合我國《個資法》規定，本文仍然對於我國政府願意踏出建置個人資料保護獨立監督機關的第一步給予肯定並寄予厚望，期許其未來能夠發揮端正視聽的功能。同時，本文也必須鄭重表示，倘若個人資料保護委員會未來流於形式，甚至隨意擴張解釋《個資法》相關規定，無法發揮獨立監督的功能，則縱使立法者對於警察機關使用自動車牌辨識系統的情形，量身打造相關授權基礎，也會因為監督機制的實質匱乏，未能使實際施行情形符合法規設計，而無法通過比例原則的審查。

doi:10.6342/NTU202403953

第五章 結論

伴隨科技發展，我國警方近年來增設的路口監視器，除了一般影像蒐集之外，還具備了自動辨識通過車輛的車牌號碼、顏色，並且即時比對涉案車輛名單的功能。雖然，車牌號碼本即屬監視錄影畫面中所涵蓋的資訊，且依行政法令具有公示性質，警方使用軟體加以識別的行為，看似只是節省人工比對的時間。不過，相比於傳統監視錄影畫面，自動車牌辨識系統將特定車輛於某時間點出現在特定位置的資料予以量化後，能夠輕易地透過 GIS 系統的疊圖功能，按照時間順序描繪出特定車輛的完整行車軌跡。也就是說，經過量化處理的個人資料，其個別資料之間相互連結的便捷性與可能性會大幅提升，這一方面使警方得以省去許多時間心神一一比對，另一方面卻使人民私人生活受到窺探的風險隨之提升。此外，我國警方使用系統識別出車牌號碼後，並不會區分車輛所有人是否具有犯罪嫌疑，而一律預防性儲備於資料庫內，進而導致不具犯罪嫌疑的一般人，其完整的行車軌跡也會受到留存。實務上就曾經發生基層員警懷疑老婆外遇，暗中使用自動車牌辨識系統監視老婆行蹤的案例。有鑑於此，本文遂於第一章提出問題意識：自動車牌辨識系統之干預性質為何？此種措施於犯罪嫌疑尚未發生，即預防性儲備人民完整的行車軌跡，迫使其承受私人生活遭受揭露的風險，是否為憲法上所絕對禁止？若否，則其干預授權基礎所應具備的要件為何？基此，本文以下整理研究成果，予以回應。

為探究自動車牌辨識系統之干預性質，本文以德國法及美國法作為參考對象。對此，德國聯邦憲法法院於 2008 年第一次車牌辨識裁判中認為，車牌號碼比對符合後儲存於資料庫內，使其產生未來與更多個人資料相互連結的可能性，因此構成個人資訊自決權之干預；反之，倘若車牌號碼比對不符合後立即刪除，既然在整個過程中保持匿名性而無法與個人產生關聯，則不構成干預。不過，2018 年第二次車牌辨識裁判推翻此一見解，重申自動資料蒐集是否構成個人資訊自決權干預，其判斷標準在於：國家機關對於相關個人資料是否有著強烈的興趣；並表

doi:10.6342/NTU202403953

示，唯有自動車牌辨識系統蒐集並比對所有行經車輛的車牌號碼，才能完整發揮檢查目標車輛是否通過特定路段的功能，因此，警察機關是有意將此種措施加諸於所有駕駛人身上，而對所有車牌資料具有強烈的興趣。人民之所以能夠繼續安穩地行駛於道路上，是因為其已經通過警方的檢查，然而，公民基本上可以在不被國家任意記錄、不需要說明自身行為是否正當、不暴露在持續受監視的感覺下四處活動，這是共同體自由的特質之一。因此，縱使車牌號碼經蒐集後自動化比對，且比對不符合立即刪除，仍構成個人資訊自決權之干預。

另一方面，關於車牌辨識是否構成美國憲法增修條文第 4 條之搜索，實務曾有判決針對員警手動輸入車牌號碼檢查的情形，表示車牌號碼的功用本在使執法機關辨別身分，且依行政法規也須保持可識別性，因此駕駛人無法對其車牌資訊享有合理隱私期待，員警手動輸入車牌號碼的檢查行為也毋需具備相當理由。若依此見解，則車牌辨識措施似乎不該當美國憲法意義上之搜索。不過，於 *Carpenter* 案中，美國聯邦最高法院已肯認人民對於其完整的移動軌跡享有合理隱私期待，則自動車牌辨識資料庫內的資訊若可描繪特定人完整的行車軌跡，警察機關之資料調取行為亦應構成搜索。可惜的是，2020 年 *Yang* 案的多數意見並未正面處理這個問題；Bea 法官則於協同意見書中表示，單就本案資料顯示，美國自動車牌辨識資料庫尚不具備形塑人民完整移動軌跡的能力，因此警方調取車牌辨識資料並不構成搜索。

我國司法院釋字第 603 號解釋所提出的「資訊隱私權」，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。雖是使用「隱私」的用語，卻著重於個人資料的自主控制，而近似德國法上個人資訊自決權之內涵。不過，釋字第 689 號解釋一方面肯認人民縱使於公共場域，其個人資料自主仍受法律保護；另一方面卻引述了合理隱私期待的判斷標準。如此一來，是否表示公共場域中資訊隱私權的保障範圍，僅限於人民享有合理隱私期待者？警察機關若僅蒐集、儲存少量的車牌辨識資料，是否即不構成資訊隱私權之干預？對此，本文認為，釋字第 603 號解釋是基於電腦資訊科技發展的背景，

doi:10.6342/NTU202403953

考量無重要意義的中性個人資料經過大量積累並相互連結的過程後，仍會產生形塑私人生活圖像的風險，甚至影響人民自由發展人格的權利，故發展出資訊隱私權的保障。而自動車牌辨識系統，正是透過大量積累單點位置資訊，描繪出完整行車軌跡，而得以對特定人之私人生活做出精確的推論。因此，切不可單純以車牌辨識資料係於公共場域蒐集，即抹去少量資料蒐集之干預性質。於我國釋憲實務尚未正面處理此一爭議之前，針對自動車牌辨識的干預性質判斷，應同時檢驗合理隱私期待標準以及資訊自決標準。有據於此，縱使是少量車牌辨識資料的儲備，亦屬個人資料之蒐集而構成干預；此外，倘若受儲備的資料量足以描繪特定人完整的行車軌跡，則不論是依何種判斷標準，均會干預特定人之資訊隱私權。

肯認車牌辨識的干預性質後，為探討其授權基礎應具備的要件，本文參考德國《刑事訴訟法》第 163g 條規定，卻發現德國法上以刑事追訴為目的實施自動車牌辨識的措施，必須於資料蒐集後即時與追緝名單相互比對，並且將比對結果不符合的資料立即刪除，不得預防性儲備車牌辨識資料（追緝模式）。此外，由於第 163g 條僅授權偵查機關儲存資料比對符合者，且於措施達成辨識嫌疑人身分或其所在地之目的後，應立即終結。因此，自動車牌辨識系統並不會被用作同 GPS 般的新型態監視工具，而僅是尋找特定人位置資訊的暫時性手段，得由檢察官自行以書面命令發動。然而，實施措施必須限於一定期間內，且僅可在事前可合理認定有助於達成目的的地點，不可地毯式施行，據以符合比例原則。

「追緝模式」雖然有效地限制自動車牌辨識系統的干預程度，然而，於重大犯罪發現後，尚無具體車牌號碼可供比對的情形，卻難收偵查成效。第 163g 條的立法過程中，也曾討論是否應授權警方得於重大犯罪發生後，尚未對特定人產生開始嫌疑的時點，先行預防性儲備犯罪地點附近的車牌辨識資料，供後續用於偵查犯罪嫌疑人可能的逃亡路線（儲存模式）；另外，慕尼黑高等檢察署更主張，應授權警方得常態性儲備一定期間內的車牌辨識資料，並於後續資料調取規定加諸重罪門檻與法官保留等程序擔保，藉以取得偵查成效與人權保障之平衡（記錄模式）。然而，德國聯邦眾議院最終考量車牌辨識資料之預防性儲備，將對所有

doi:10.6342/NTU202403953

車輛駕駛人構成嚴重的個人資訊自決權干預，故決定暫緩相關立法，先觀察「追緝模式」的施行經驗，再評估實務需求。

由於德國法上並未授權警察機關預防性儲備車牌辨識資料，難以單憑現行法規推斷此種實施模式是否為憲法上所絕對禁止，或者於授權基礎的設計上應著重何種考量。因此，本文基於預防性通信紀錄儲備與「記錄模式」的相似性，決定藉由考察預防性通信紀錄儲備的爭議，理解此種於對公共安全的具體危害或犯罪嫌疑尚未發生，即預防性儲備人民資料的措施，其基本權干預程度與正當化之需求應如何評價。

為因應國際恐怖攻擊頻傳的局勢，歐盟於 2006 年發布指令，要求會員國立法課予電信和網路服務業者無差別預防性儲備 6 個月至 2 年通信紀錄的義務。對此，德國聯邦憲法法院表示：基於刑事追訴、防止危害與國安情報領域中的適當目的，無差別預防性儲備 6 個月的通信紀錄，構成《基本法》第 10 條秘密通訊自由之干預，然而並非憲法上所絕對禁止。尚未產生具體事由即預防性儲備通信紀錄，若對於後續資料使用目的作成嚴格的限制，則系爭規定仍可通過合憲性目的審查。此種措施得促進犯罪預防與追訴，具適當性；所謂資料快速凍結程序亦非同等有效之手段，通過必要性審查。不過，受預防性儲備的通信紀錄一旦經過分析，不僅得以深入探知特定人的私人生活，甚至可以對個人性格與行動軌跡做出詳盡的推論，因而屬於嚴重的秘密通訊自由干預。立法者於干預授權基礎的設計上，必須賦予其合於當前科技發展水準的資訊安全措施，包括資料應獨立儲備於斷網且加密的設備當中，並且將資料調取限於兩名有權人士在場的情形。此外，資料儲備與資料調取規定的合憲性，二者應合併觀察，資料調取僅得基於特別重大的公共利益，於刑事追訴即限於列舉重罪的偵查情形，並應規範通知義務，適用法官保留程序。

相對於此，歐盟法院則以裁判宣告 2006 年指令無效。其認為：涉及私人生活應受尊重之權利而損害或限制個人資料保護，必須限於「絕對必要」的情形始可為之，系爭措施並未將預防性儲備通信紀錄的範圍，限縮在可能涉及重大犯罪

doi:10.6342/NTU202403953

之特定期間、區域或群眾之內，反而涵蓋了與重大犯罪之間毫無關聯的一般人，甚至包括了在會員國內國法下負有職業保密義務之人，已違反「絕對必要」的限制。後續裁判中，歐盟法院更基於 2002 年指令的條文架構主張：通信紀錄之預防性儲備，迫使人民承受私人生活遭受揭露的風險，而屬民主社會下的例外情形。基此，即使是為了預防或追訴重大犯罪此等重要公共利益，仍舊不得無差別預防性儲備通信紀錄，否則即是使此種例外情形轉為原則。另外，歐盟法院也表示：基於預防或追訴重大犯罪之目的，可實施針對性通信紀錄儲備，亦即，基於客觀且非歧視性的事實依據，可認特定地區具有準備或實施重大犯罪的高度風險，包括過去曾發生多起重大犯罪的區域，或如經常接待大量遊客的地點或設施，此等特別容易遭受重大犯罪的場所，又或者是重要戰略位置，如機場、車站、港口或公路收費站，則可予以針對性儲備。此外，會員國內國法亦可授權偵查機關於重大犯罪發生後，快速凍結現有的通信紀錄。

本文認為，歐盟法院駁斥無差別預防性通信儲備的理由，主要是建構在 2002 年指令的原則與例外關係之上，因此無法直接適用於預防性車牌辨識資料儲備的情形。不過，這並不表示預防性車牌辨識資料儲備的實施範圍即可不受限制，基於資料儲備與資料調取之授權規定，二者應合併觀察的法理，車牌辨識資料之預防性儲備仍應受到實施地點的限制，不可全面覆蓋式地施行；否則，將使系爭措施所取得的資料僅得用於特別重大犯罪的追訴情形，方可通過狹義比例原則的審查。然而此舉不但使其無法於偵查實務中發揮成效，更會導致資料庫內存有人民鉅細靡遺的行車資訊。有鑑於此，自動車牌辨識系統的實施地點，必須限於依據客觀事實證據，於事前可認對於預防或追訴重大犯罪有所幫助的地點，不可全面覆蓋式地施行。此外，資料調取必須限於維護同等重要的公共利益，因此原則上應須限於重大犯罪的偵查情形，並適用相對法官保留；例外於連續未達 24 小時且 6 個月內累積未達 2 日，此種短期資料調取情形，考量其尚不至產生形塑特定人人格圖像之風險，因此僅排除用於輕微犯罪的偵查情形，並授權檢察官、檢察事務官及司法警察官得自行為之。另外，為了控制資料遭濫用、外流的風險，立

doi:10.6342/NTU202403953

法者必須賦予系爭措施合於當前科技發展水準的資訊安全保障，並課予偵查機關記錄資料調取、刪除的義務，且應於通知無礙於偵查目的時，通知資料受調取之人，使其得以主張權利救濟。

透過預防性通信紀錄儲備的爭議，理解預防性儲備車牌辨識資料所干預資訊隱私權的程度，以及授權基礎上應具備的要件後，即應以此審視我國現行法規定，若有不符則提出立法建議。於此，本文依據自動車牌辨識系統的實施流程與方式，區分三種情形討論，分別是：「車牌辨識資料庫的建立」、「受儲備車牌辨識資料的調取」以及「即時比對功能的實施」。

關於預防性儲備車牌辨識資料，據以建立資料庫之授權基礎，現行法下或可討論《警職法》第 10 條。不過，《警職法》第 10 條的授權範圍並未涵蓋識別與量化影像資料，此種干預程度更高的情形；更未授權警察機關得以隱密方式蒐集資料；且同條第 2 項規定資料儲備期限為 1 年，亦有違反資料最小化原則之虞。基此，《警職法》第 10 條不得作為警方建構車牌辨識資料庫的授權依據。同樣地，各直轄市為健全錄影監視系統的設置管理，雖得自行制定相關自治條例，然而以《臺北市錄影監視系統設置管理自治條例》為例，其仍與《警職法》第 10 條有著相同問題。另外，《道交條例》第 7 條之 2 雖授權警察機關為取締交通違規得以科學儀器蒐集證據資料，然而，本法目的僅在維護交通安全，違規取締目的達成後即應將資料刪除，不可擅自留存供後續刑事追訴調取。

鑑於現行法下並無預防性儲備車牌辨識資料，以建構資料庫之授權基礎，我國警方大量架設自動車牌辨識系統，預防性儲備車牌辨識資料的措施，實已違反《憲法》第 23 條法律保留原則。以下提出立法建議，供立法者參考。

新增《警職法》第 10 條之 1 全文如下：

第十條之一　警察對於有事實足認經常發生或容易遭受犯罪案件之公共交通場所，為防止危害或犯罪之必要，得以科技工具秘密蒐集行經車輛之車牌號碼、時間、地點及行駛方向。	一、使用自動車牌辨識系統預防性蒐集人民大量車輛位置資訊並持續儲備，將可據以準確推論個人之私人生活，有礙人民自由行使基本權利之虞，自應設置較嚴謹之

doi:10.6342/NTU202403953

依前項規定蒐集之資料，除因調查犯罪嫌疑或其他違法行為，依法律規定有保存之必要者外，至遲應於資料製作完成時起六個月內銷毀。 依第一項規定蒐集之資料，應以符合當前科技發展水準之技術加密。 依法律規定調閱、複製或利用第一項規定所蒐集之資料，應至少有兩名人員在場，並作成以下紀錄： 一、資料存取時間。 二、資料存取人員。 三、資料存取範圍與事由。	程序。 二、為避免警方全面覆蓋式實施自動車牌辨識，悉數網羅人民之車輛位置資訊，實施地點應限於「有事實足認經常發生或容易遭受犯罪案件之公共交通場所」。亦即基於客觀且非歧視性之事實依據，而認某地區具有準備或實施重大犯罪之高度風險，包括過去曾發生多起嚴重犯罪之區域，或經常接待大量遊客之地點或設施，此種特別容易遭受嚴重犯罪之場所，又或是重要戰略位置和交通樞紐，如機場、車站、港口或高速公路收費站。 三、本條授權警察機關得以秘密方式蒐集資料，並將資料蒐集範圍限於「車牌號碼、時間、地點及行駛方向」，排除警察機關依據本條規定，以科技工具識別車內駕駛人、乘客與路上行人之衣物顏色，甚至是臉部資訊之可能。 四、權衡實務偵查需求以及人民資訊隱私權之保障，將車牌辨識資料之儲備期間限制為 6 個月，期間屆滿除為調查具體犯罪嫌疑，而依法律規定得以繼續留存外，應立即以不可回復之方式予以刪除、銷毀。 五、為避免車牌辨識資料遭竊取，致使人民完整行車軌跡輕易為他人所知，警察機關應以符合當前科技發展水準之加密技術，確保受儲備資料之安全性。同時，為排除內部人員濫用之可能，資料調取利用應遵循「四眼原則」，至少命兩名人員在場，並記錄資料調取時間、人員、範圍以及事由。

doi:10.6342/NTU202403953

	六、第四項所稱「依法律規定調閱、複製或利用」，必須是於要件中明確規範「車牌辨識資料」之授權規定，於資料目的外使用的情形更應排除以《個人資料保護法》作為授權依據。

增定上述條文後，仍須討論現行法下是否具備車牌辨識資料的調取授權。首先，由於《警職法》第 17 條僅授權警察機關得將其依本法所蒐集的資料，用於防止危害與預防犯罪，故不得作為基於刑事追訴目的調取車牌辨識資料的授權規定。另外，《刑事訴訟法》第 230 條及第 231 條雖可作為司法警察偵查權限的一般性規定，然而在適用上只限於絕對輕微的基本權干預情形。車牌辨識資料屬於經過量化的個人資料，其資料間相互連結的便捷性與可能性大幅增加，更可透過 GIS 疊圖功能描繪出特定人完整的行車軌跡，自然不屬於輕微的基本權干預情形。至於《個資法》第 15 條及第 16 條，對於受預防性儲備資料之調取規定，原則上應適用的重罪門檻與法官保留程序，均付之闕如，絕不可作為受儲備車牌辨識資料之調取授權。

據此，本文提出立法建議，新增《刑事訴訟法》第 153 條之 11 全文如下：

第一百五十三條之一　檢察官偵查通訊保障及監察法第 5 條第 1 項所列之罪，有事實足認下列車牌辨識資料於本案之偵查有必要性及關連性時，除有急迫情形不及事先聲請者外，應以書面聲請該管法院核發調取票。 一、車牌號碼核發給被告或由被告使用。 二、車牌號碼核發給被告以外之人或由該人使用，且根據相當理由可認為該人與被告有聯繫或將建立聯繫，若以其他方法調查，合理顯示為不能達成目的或有重大危險情形。 法院核發第一項調取票應記載下列事項：	一、鑑於大量車牌辨識資料之調取足以描繪特定人過去一定期間內之完整行車軌跡，據以探知、揭露特定人之私人生活，隱含形塑其人格圖像之風險。檢察官基於刑事追訴目的而欲予以調取，原則上應限於重大犯罪之偵查情形，並適用相對法官保留程序。 二、被告以外之第三人並非國家刑罰權對象，必須根據相當理由可認該人與被告有聯繫或將建立聯繫，且若以其他方法調查，合理顯示為不能達成目的或有重大危險情形，始得調取其車牌辨識資料。 三、未達連續 24 小時且 6 個月內累積未達 2 日的車牌辨識資料調取情

doi:10.6342/NTU202403953

一、案由及涉嫌觸犯之法條。 二、資料調取對象。 三、資料調取理由。 四、資料調取期間。 五、資料調取人員。 六、資料蒐集機關。 核發調取票之程序，不公開之。 情形急迫而不及事先聲請者，檢察官應於調取後三日內陳報該管法院補發調取票。法院認為不應准許者，檢察官應立即將已取得之車牌辨識資料銷毀。 檢察官、檢察事務官、司法警察官偵查最重本刑三年以上有期徒刑之罪，有事實足認第一項所列車牌辨識資料於本案之偵查有必要性及關連性時，得以書面命令記載第二項各款事項，調取未達連續二十四小時且六個月內累積未達二日的車牌辨識資料。 依本條實施車牌辨識資料之調取，應於通知無害於偵查目的時，書面通知受調取人。若於調取後三個月內仍未通知，應向法院陳報未通知之原因。逾期未陳報者，法院應於十四日內主動通知受調取人。 車牌辨識資料調取目的達成後，應立即銷毀。	形，尚不至產生形塑人格圖像之風險，故授權檢察官、檢察事務官、司法警察官得自行為之，並僅排除用於輕微犯罪之偵查情形。 四、為使受干預人事後得審視資料受調取事由，據以主張權利救濟，法院及檢察官、檢察事務官、司法警察官授權調取特定人車牌辨識資料，應詳細記載第二項所列事項。 五、車牌辨識資料之蒐集、儲備與調取均係秘密實施，故應課予偵查機關通知義務，以利受干預人提起救濟。又，為避免偵查機關遲延踐行通知，應命其於資料調取後三個月，陳報法院尚未通知之緣由，倘逾期未陳報，則由法院通知受干預人，鞏固其救濟權利。 六、基於目的拘束原則，資料調取目的達成後應立即銷毀，避免資料持續受留存而產生與更多個人資料相互連結，進一步探知特定人私人生活的可能性。

除了預防性儲備車牌辨識資料，待日後產生偵查需求再予以調取，自動車牌辨識系統也同時具備即時比對的重要功能。因此，亦須審視現行法下是否具備相關授權基礎。首先，我國《刑事訴訟法》第 122 條以下之搜索規定，既然是以公開實施為原則，自然並未授權偵查機關秘密實施自動車牌辨識與比對。同時，此種秘密比對措施，致使受干預人無法於事中及時主張權利救濟，並非干預程度輕微的情形，因此亦不得以《刑事訴訟法》第 230 條及第 231 條作為干預授權基礎。此外，針對我國警政署憑藉《個資法》第 15 條，即介接高公局基於收費目

doi:10.6342/NTU202403953

的所蒐集的車牌資料，必須認識到的是，《個資法》第 15 條僅為組織法規定，不得作為國家機關干預人民基本權之依據，且更進一步觀察，《個資法》第 15 條的文義涵蓋了偵查機關以此實施即時監視的嚴重干預情形，對於相關程序擔保卻未有建樹，則縱使將其視為作用法，亦有違法律明確性原則。因此，警政署不得依《個資法》第 15 條蒐集國家機關基於其他目的取得之車牌辨識資料。最後，《刑事訴訟法》第 153 條之 1 係為 GPS 此種針對單一對象的偵查手段所創設，未能考量到秘密實施的比對措施可能對於人民基本權利的自由行使產生嚴重影響，而在要件設計上並未清楚規範國家機關可蒐集與比對的資料範圍，亦無法在實施流程上明確排除預防性資料儲備的疑慮，若將其用作「追緝模式」的授權基礎，將有違法律明確性原則。

綜上所述，現行法亦不具備以刑事追訴為目的，實施自動車牌辨識與即時比對的授權基礎，警察機關之作為已違反法律保留原則。據此，以下提供立法建議，新增《刑事訴訟法》第 153 條之 12 全文如下：

第一百五十三條之二　檢察官、檢察事務官、司法警察官、司法警察偵查最重本刑三年以上有期徒刑之罪，有事實足認措施有助於辨識被告或犯罪嫌疑人之身分或其所在地，得於公共交通場域秘密以科技方法自動蒐集車牌號碼、時間、地點及行駛方向。 依第一項蒐集之車牌號碼得與下列車牌資料進行自動化比對： 一、車牌號碼核發給被告或由被告使用。 二、車牌號碼核發給被告以外之人或由該人使用，且根據相當理由可認為該人與被告有聯繫或將建立聯繫，若以其他方法調查，合理顯示為不能達成目的或有重大危險情形。 自動化比對應在第一項自動蒐集資料後儘速為之。當有比對結果符合	一、偵查機關實施自動車牌辨識即時比對車輛駕駛人是否涉及刑事案件，乃全天候持續檢查用路人身分，應限於最重本刑三年以上有期徒刑之罪之偵查情形，始得為之。 二、實施即時比對，應限於有事實足認措施有助於辨識被告身分或其所在地之公共交通場域，不可全面覆蓋式實施。 三、被告以外之第三人並非國家刑罰權對象，必須根據相當理由可認該人與被告有聯繫或將建立聯繫，且若以其他方法調查，合理顯示為不能達成目的或有重大危險情形，始得比對其車牌資料。 四、為避免偵查機關留存大量車牌辨識資料，比對應於資料蒐集後立即自動化進行，資料比對不符合

doi:10.6342/NTU202403953

時，應儘速以人工方式檢查是否確實相符。當比對結果不符或經人工檢查確認比對結果不符時，第一項所蒐集之資料應立即刪除或依警察職權行使法第十條之一規定處理，不得利用。 第一項之命令應以書面為之，並詳細記載以下事項： 一、案由及涉嫌觸犯之法條。 二、自動化比對對象及理由。 三、措施實施地點及時間。 四、措施實施機關及人員。 當措施發動要件已不存在，或已確認被告或犯罪嫌疑人之身分或其所在地，應儘速終結措施。 已確認被告或犯罪嫌疑人之身分或其所在地，仍有實施之必要者，應由檢察官或司法警察官報請檢察官許可後，以書面記載第四項各款事項，聲請該管法院核發許可書。使用前項科技方法前，預計確認被告或犯罪嫌疑人之身分或其所在地後仍將繼續實施者，亦同。 措施終結後，應以書面通知受自動化比對對象第四項所記載之事項。	應即銷毀，或依警察職權行使法第十條之一以符合當前科技發展水準之技術加密後儲備，待未來依本法第一百五十三條之二另行調取，偵查機關不得逕行利用之。 五、偵查機關若欲將自動車牌辨識系統之即時比對功能，用作類似 GPS 之監視工具，而於確認被告身分或其所在地後持續探知其行車資訊，則有必要適用法官保留程序，確保措施之施行於個案中符合比例原則。 六、本條第一項及第六項所授權之自動車牌辨識即時比對，均是以隱密方式實施，為使受干預人得主張權利救濟，應於措施終結後，以書面通知受自動化比對對象第四項所記載之事項。

為避免司法警察規避長期資料調取與即時比對所應適用的重罪門檻和法官保留，本文認為應將各派出所公務電腦得對同一車牌號碼查詢的資料量，限制在未達連續 24 小時且 6 個月內累積未達 2 日的時間範圍。超出此一範圍則須向各縣市警察局之單一窗口申請調取，並同時提出法官核准之調取票，或者以書面說明情況急迫的緣由。警政署更應於資料調取系統設置警示通知功能，於員警連續多次調取特定車牌資料時，自動警示內部監督單位介入處理。最後，考量自動車牌辨識系統的實施地點是否依循客觀事實證據，並合乎比例原則，實有賴專家學者於建置階段共同參與討論，且於建置後不定期抽查實際施行情形；此外，資料儲備期間屆滿後是否係以不可回復的方式刪除、銷毀，而非容任其繼續留存，對

doi:10.6342/NTU202403953

於人民資訊隱私權的保障亦至關重要。據此，立法者若欲從本文見解，授權警察機關得以隱密方式，預防性儲備人民 6 個月的車牌辨識資料，則應同時建構外部獨立之監督機關，確保警察機關的實際作為符合法規要件設計，否則仍會肇因於監督機制的匱乏，違反比例原則之誡命。

doi:10.6342/NTU202403953

參考文獻

壹、中文部分

一、專書

王兆鵬（2003），《路檢、盤查與人權》，元照。

王兆鵬（2007），《美國刑事訴訟法》，二版，元照。

何賴傑、林鈺雄（審譯）（2019），《德國刑法典》，2版，元照。

林鈺雄（2023），《刑事訴訟法（上冊）》，12版，自版。

林鈺雄（2023），《刑事訴訟法（下冊）》，12版，自版。

林鈺雄、王士帆、連孟琦（2023），《德國刑事訴訟法註釋書》，新學林。

陳一昌、黃運貴、張芳旭、楊智凱、曹瑞和、田養民、張仲杰（2004），《車牌影像辨識系統與號牌設計改進配合措施之探討》，交通部運輸研究所。

蔡庭榕、簡建章、李錫棟、許義寶（2005），《警察職權行使法逐條釋論》，五南。

蔡震榮（2016），《警察職權行使法概論》，3版，五南。

二、書之篇章

李震山（2008），〈公權力運用定位科技措施與基本權利保障〉，收於：城仲模教授古稀祝壽論文集編輯委員會（編），《二十一世紀公法學的新課題—城仲模教授古稀祝壽論文集— I. 憲法篇》，頁335-365，新學林。

李震山（2020），〈論資訊自決權〉，收於：氏著，《人性尊嚴與人權保障》，五版，頁239-314，元照。

許義寶（2020），〈論警察蒐集與利用個人資料之職權〉，收於：陳淳文（等著），《如沐法之春風—陳春生教授榮退論文集》，頁525-561，元照。

黃昭元（2005），〈無指紋則無身分證？換發國民身分證與強制全民撚指紋的憲法

doi:10.6342/NTU202403953

爭議分析〉，收於：國際刑法學會台灣分會（等編），《民主、人權、正義—蘇俊雄教授七秩華誕祝壽論文集》，頁461-508，元照。

蕭文生（1999），〈關於一九八三年人口普查法之判決〉，收於：劉孔中（等譯），《西德聯邦憲法法院裁判選輯（一）》，頁270-326，司法院。

蕭文生（2004），〈自基本權保障觀點論街頭監視錄影設備裝設之問題〉，收於：法治斌教授紀念論文集編輯委員會（編），《法治與現代行政法學：法治斌教授紀念論文集》，頁233-262，元照。

三、學位論文

林容（2021），《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，臺北。

林錦鴻（2005），《警察運用監視器之法律問題分析—以警察職權行使法為中心》，國立臺灣大學法律學研究所碩士論文，臺北。

柯羿良（2023），《自動車牌辨識系統之偵查適法性—以德國法為借鏡》，國立臺北大學法律學研究所碩士論文，臺北。

唐欣悅（2019），《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，臺北。

湯仁愷（2023），〈應用YOLOv5和CNN深度學習技術於車牌辨識研究〉，《應用YOLOv5和CNN深度學習技術於車牌辨識研究》，國立臺北科技大學車輛工程系碩士班碩士論文，臺北。

四、期刊文獻

王士帆（2021），〈德國科技偵查規定釋義〉，《法學叢刊》，66卷2期，頁85-132。

王振華（2019），〈eTag掃描設備用於打擊各類犯罪之應用與成效〉，《刑事雙月刊》，93期，頁14-17。

田炎欣（2014），〈警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討（下）〉，

doi:10.6342/NTU202403953

《台灣法學雜誌》，257期，頁85-95。

田哲夫（2008），〈科技犯罪防制工作中程計畫簡介〉，《刑事雙月刊》，27期，頁12-15。

朱耀明、林財世（2005），〈淺談RFID無線射頻辨識系統技術〉，《生活科技教育月刊》，38卷2期，頁73-87。

江義平、許蕙婷（2014），〈網路使用者日常線上資訊行為之探勘研究〉，《電子商務研究》，12卷1期，頁5-26。

吳宗澤（2012），〈地理資訊系統（GIS）與刑案分析之結合運用〉，《刑事雙月刊》，47期，頁16-21。

吳維雅（2019），〈FBI也駭人？執法部門植入惡意軟體遠端監視法制之初探—以美國聯邦法為中心〉，《檢察新論》，26期，頁198-219。

吳維雅（2020），〈公共場所運用人臉辨識科技執法適足性之研析—以美國憲法第四修正案為框架〉，《檢察新論》，28期，頁142-168。

李建良（2015），〈公法類實務導讀【交通裁決事件系列（十一）】【道路監視錄影資料與交通違舉證方法】〉，《台灣法學雜誌》，272期，頁125-138。

李建良（2017），〈資料流向與管控環節—個資保護ABC〉，《月旦法學雜誌》，272期，頁25-31。

李建興、游凱倫、林應璞（2010），〈即時動態車牌辨識〉，《技術學刊》，25卷2期，頁151-165。

李寧修（2015），〈預防性通信資料存取之憲法界限—以歐盟儲備性資料存取指令（2006/24/EG）之發展為借鏡〉，《興大法學》，17期，頁87-140。

李寧修（2021），〈警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例〉，《警察法學》，20期，頁391-437。

李寧修（2022），〈展望健保個資開放利用之新篇章：簡評111年憲判字第13號判決〉，《當代法律》，11期，頁12-20。

李寧修（2023），〈警察運用資料職權之合憲性觀察—以德國聯邦憲法法院【自動

doi:10.6342/NTU202403953

化資料分析】判決為中心〉,《月旦法學雜誌》,341期,頁80-98。

李榮耕(2015),〈科技定位監控與犯罪偵查:兼論美國近年GPS追蹤法制及實務之發展〉,《國立臺灣大學法學論叢》,44卷3期,頁871-969。

李震山(2004),〈從公共場所或公眾得出入之場所普設監視錄影器論個人資料之保護〉,《東吳法律學報》,16卷2期,頁45-92。

李震山(2005),〈個人資料保護與監視錄影器設置之法律問題研究—以警察職權行使法第十條為中心〉,《警察法學》,4期,頁21-75。

李震山(2006),〈德國抗制恐怖主義法制與基本權利保障〉,《月旦法學雜誌》,131期,頁5-20。

李震山(2006),〈警察機關設置監視錄影器的法制問題—人權保障與治安維護的動態平衡〉,《台灣本土法學雜誌》,86期,頁114-122。

李震山(2023),〈警察職權行使法的回顧與展望:以科技工具蒐集或利用資料規定為例〉,警察法學與政策,5期,頁1-20。

周天蔚(2019),〈細說車牌辨識原理與市場〉,《臺灣電信月刊》,193期,頁13-27。

周詩涵、蔡博雅、劉大維(2020),〈國有林盜伐現況及查緝措施〉,《台灣林業雙月刊》,46卷3期,頁5-14。

官政哲(2012),〈21世紀警政新典範—智慧型警政(SMART Policing)〉,《刑事雙月刊》,50期,頁44-50。

林明芬、戴偉恒、張正欣(2016),〈雲端智慧影像分析及檢索系統〉,《電腦與通訊》,166期,頁82-90。

林明鏘(2010),〈由防止危害到危險預防:由德國警察任務與權限之嬗變檢討我國之警察法制〉,《國立臺灣大學法學論叢》,39卷4期,頁167-212。

林明鏘(2023),〈具有雙重性質之警職法—近20年的重要司法裁判回顧與分析〉,警察法學與政策,5期,頁87-122。

林容(2020),〈人臉辨識技術做為科技偵查手段之法律問題(一)〉,《法務通訊》,3028期,頁3-6。

doi:10.6342/NTU202403953

林容（2020），〈人臉辨識技術做為科技偵查手段之法律問題（二）〉，《法務通訊》，3029期，頁4-6。

林鈺雄（2004），〈從基本權體系論身體檢查處分〉，《國立臺灣大學法學論叢》，33卷3期，頁149-200。

林鈺雄（2007），〈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。

林鈺雄（2021），〈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。

邱文聰（2009），〈從資訊自決與資訊隱私的概念區分—評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，168期，頁172-189。

邱文聰、林子儀、張陳弘、顏厥安、范姜真媺、陳銘雄、李建良、吳全峰、陳昭如（2018），〈最高行政法院一○六年度判字第五四號判決（健保資料庫案）會議記錄〉，《月旦法學雜誌》，272期，頁63-84。

施宗培、田哲夫（2010），〈科技犯罪偵防工作簡介〉，《刑事雙月刊》，39期，頁27-32。

范姜真媺（2018），〈檢視行政機關蒐集利用個資之問題及展望〉，《法學叢刊》，63卷2期，頁29-60。

范姜真媺（2019），〈自實務判決檢視行政機關蒐集、處理或利用個人資料之問題〉，《警察法學》，18期，頁91-128。

范姜真媺（2022），〈防疫措施與個人資料保護間之取捨、衡平〉，《月旦法學雜誌》，323期，頁45-58。

張志偉（2017），〈從資訊自決與資訊隱私的概念區分，檢視被遺忘權的證立問題〉，《萬國法律》，211期，頁2-15。

張志偉（2023），〈個資保護與資料安全〉，《當代法律》，22期，頁13-20。

許芳瑜（2016），〈歐盟對於行動健康服務之個人資料隱私保護之發展〉，《科技法律透析》，28卷7期，頁54-71。

doi:10.6342/NTU202403953

連孟琦(2023),〈刑事偵查與個人資訊自決權(資訊隱私權)之保護—以德國 2021 年 6 月新增刑事訴訟法自動化車牌辨識規定（§163g StPO）為例〉,《檢察新論》,32期，頁87-103。

陳先慶（2006),〈神捕—車牌辨識系統〉,《刑事雙月刊》,12期，頁56-58。

陳宏和（2014),〈警政雲端運算發展計畫執行現況〉,《政府機關資訊通報》,317期，頁32-38。

程明修(2023),〈基本權釋義學之挑戰—疊加之基本權干預〉,《公法研究》,7期,頁15-47。

黃郁文、林啟豐、吳松儒等（2013),〈建構臺北市治安電子城牆—新一代錄影監視系統工程實務〉,《中華技術》,100期，頁204-219。

溫祖德（2016),〈臨檢盤查與警犬執法〉,《檢察新論》,19期，頁191-205。

溫祖德(2018),〈從Jones案論使用GPS定位追蹤器之合憲性—兼評馬賽克理論〉,《東吳法律學報》,30卷1期，頁121-167。

溫祖德(2021),〈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。

葉雲兆、陳武洲、簡大為、留乃俊、鄭惟元（2014),〈警政勤務及港埠物流影像辨識之應用〉,《前瞻科技與管理》,4卷1期，頁163-187。

劉芳伶（2021),〈論運用「車牌辨識技術」所為「N系統偵查」之適法性判斷構造與要件〉,《軍法專刊》,67卷4期，頁91-122。

劉青峰(2023),〈COVID-19 疫情下資訊自決權之研究—以歐洲人權公約第 8 條作為比較法對象〉,《中原財經法學》,50期，頁227-315。

劉靜怡（2016),〈監視科技設備與交通違規執法〉,《月旦法學雜誌》,248期，頁73-84。

蔡宗珍（2014),〈政府監控概觀—兼淺析歐盟2006年強制儲存通信紀錄指令〉,《台灣法學雜誌》,244 期，頁 25-29。

doi:10.6342/NTU202403953

蔡宗珍（2018），〈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105-131。

蔡宗珍（2018），〈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。

蔡馥瑔、高大宇（2018），〈基於警政應用與大數據之辨識移動式車牌研究〉，《警學叢刊》，49卷3期，頁81-96。

盧昱嘉（2012），〈天眼雙雄捍衛桃園—桃園縣政府警察局監視錄影系統簡介〉，《政府機關資訊通報》，297期，頁2-6。

盧昱嘉（2018），〈天羅地網監錄系統邁入A.I.應用世代〉，《桃警》，79期，頁2-5。

薛智仁（2014），〈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。

薛智仁（2017），〈羈押事由之憲法界限〉，《國立臺灣大學法學論叢》，46卷4期，頁1879-1951。

薛智仁（2018），〈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。

薛智仁（2021），〈第三人搜索之另案扣押—最高法院 110 年度台上字第 1979 號刑事判決〉，《台灣法律人》，2期，頁190-198。

謝碩駿（2019），〈行政機關蒐集個資之法律依據〉，《月旦法學教室》，198期，頁14-16。

蘇清偉（2005），〈「全國贓車查緝網」張網打擊犯罪〉，《刑事雙月刊》，4期，頁42-43。

蘇清偉、李耀中（2007），〈加速辦案效率—影像處理分類探討〉，《刑事雙月刊》，20期，頁39-43。

顧詔勛、吳松儒、林柏鋒、林啟豐（2021），〈建構臺北市治安電子城牆—新一代

doi:10.6342/NTU202403953

影像智慧分析應用〉,《中華技術》,130期,頁100-115。

貳、德文部分

一、書之篇章

Arzt, C./Müller, M./Schwabenbauer T. (2021). Informationsverarbeitung im Polizei- und Strafverfahrensrecht. In Bäcker/Denninger/Graulich (Hrsg.), *Lisken/Denninger, Handbuch des Polizeirechts* (7. Aufl., Rn. 1164-1169). C.H.BECK.

Stein, U. (1999). Die Ungleichbelastung von Beschuldigten und Nichtbeschuldigten durch strafprozessuale Eingriffsermächtigungen. In Samson/Dencker/Frisch/Frister/Reiß (Hrsg.), *Festschrift für Gerald Grünewald zum siebzigsten Geburtstag* (S. 685-712). Nomos Verlagsgesellschaft Baden-Baden.

二、註釋書

Barthe, C./Gericke, J. (Hrsg.) (2023). *Karlsruher Kommentar zur Strafprozessordnung (9. Aufl.), § 163g.* C.H.BECK.

Graf, J. (Hrsg.) (2024). *BeckOK StPO mit RiStBV und MiStra (50. Aufl.), TKG § 176*. C.H.BECK.

Knauer, C./Kudlich, H./Schneider, H. (Hrsg.) (2024). *Münchener Kommentar zur StPO (Bd. 2), § 163g.* C.H.BECK.

Meyer-Goßner, L./Schmitt, B./Köhler, M. (2022). *Strafprozessordnung (65. Aufl.), § 163g.* C.H.BECK.

Satzger, H./Schluckebier, W./Widmaier, G. (Hrsg.) (2022). *Strafprozessordnung mit GVG und EMRK (5. Aufl.), § 163g.* Carl Heymanns.

doi:10.6342/NTU202403953

三、期刊文獻

Brade, A. (2019). Die horizontale Eingriffsaddition. *Die Öffentliche Verwaltung*, 852-859.

Breyer, P. (2008). Kfz-Massenabgleich nach dem Urteil des Bundesverfassungsgerichts. *Neue Zeitschrift für Verwaltungsrecht*, 824-828.

Claus, S. (2022). Fahndung mittels automatischer Kennzeichenlasesysteme. *juris PraxisReport Strafrecht*, Anm. 1.

Gilga, C. (2021). Automatisierte Kennzeichenerfassung in der Strafverfolgung – aktueller Regierungsentwurf. *Newsdienst ZD-Aktuell, 05041*.

Gutmann, T./Wollenschläger, F. (2023). Die Vorratsdatenspeicherung von IP-Adressen im Spannungsfeld von Frei-heit und Sicherheit: verfassungsrechtlicher Rahmen und konkrete Ausgestaltung. *Zeitschrift für das Gesamte Sicherheitsrecht*, 249-257.

Hofmann, K. (2023). Autonomes Fahren – kein Problem des Datenschutzes. *Zeitschrift für Datenschutz*, 18-22.

Kulick, A. (2020). „Höchstpersönliches Merkmal“ – Verfassungsrechtliche Maßstäbe der Gesichtserkennung. *Neue Zeitschrift für Verwaltungsrecht*, 1622-1627.

Lachenmann, M. (2016). Das Ende des Rechtsstaates aufgrund der digitalen Überwachung durch die Geheimdienste. *Die Öffentliche Verwaltung*, 501-511.

Puschke, J. (2024). Die Vorratsdatenspeicherung – eine (un)endliche Geschichte? *Zeitschrift für das Gesamte Sicherheitsrecht*, 23-28.

Roggan, F. (2022). Der Einsatz von Automatischen Kennzeichenlesesystemen (AKLS) zu Fahndungszwecken. *Neue Zeitschrift für Strafrecht*, 19-23.

Roßnagel, A. (2008). Verdachtslose automatisierte Erfassung von Kfz-Kennzeichen, *Deutsches Autorecht*, 61-65.

Roßnagel, A. (2010). Die „Überwachungs-Gesamtrechnung” – Das BVerfG und die

doi:10.6342/NTU202403953

Vorratsdatenspeicherung, *Neue Juristische Wochenschrift*, 1238-1242.

Sandhu, A. (2017). Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union. *Europarecht*, 453-469.

Zaremba, U. Die neue Befugnis zum Einsatz automatischer Kennzeichenlesesysteme – Teil 1. *Straßenverkehrsrecht*, 168-173.

Zaremba, U. Die neue Befugnis zum Einsatz automatischer Kennzeichenlesesysteme – Teil 2. *Straßenverkehrsrecht*, 209-214.

四、網路文獻

Bull, H.P. (2023). Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit – Raster-fahndung, Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung und Antiter-rordatei in der Rechtsprechung des Bundesverfassungsgerichts. In https://link.springer.com/referenceworkentry/10.1007/978-3-658-37532-4_52-1.

Bundesrechtsanwaltskammer. (2021). Stellungnahme Nr. 68/2020 November 2020 - Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften. In: https://www.bundestag.de/resource/blob/833398/fd6533787284e438ecf88284d547f94b/stellungnahme-knauer_brak.pdf.

Conen, S. (2021). Stellungnahme für den DAV zum Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften. In https://www.bundestag.de/resource/blob/833986/60d3907bfc6ebded666c4671a4fb061c/stellungnahme-conen_dav-data.pdf.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht. (2020). Tätigkeitsbericht Datenschutz 2019. In https://www.lda.brandenburg.de/lda/de/service/informationsmaterial/details/~24-03-2020-taetigkeitsbericht-datenschutz-2019.

doi:10.6342/NTU202403953

Ecker, A. (2021). Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Fortent-wicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften BT-Drucksache 19/27654. In https://www.bundestag.de/resource/blob/833394/c88ea0f555076a893f8fdcee0f4d5808/stellungnahme-ecker.pdf.

Isak, A. (2021). Stellungnahme zur Vorbereitung der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 14.04.2021. In https://www.bundestag.de/resource/blob/832970/b3853259a3e235142af251e8a766a73c/stellungnahme-isak.pdf.

Moldenhauer, G. (2021). Schriftliche Stellungnahme zu der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 14. April 2021. In https://www.bundestag.de/resource/blob/833212/18eb818300c57fcd3078f98c2b25bcd6/stellungnahme-moldenhauer.pdf.

Südbeck, B. (2021). Stellungnahme zur Vorbereitung der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 14.04.2021. In https://www.bundestag.de/resource/blob/833556/f0cf1155f11821264bce5932dec41d0f/stellungnahme-suedbeck.pdf.

參、英文部分

一、期刊文獻

Alm, Jessica Gutierrez. 2015. The Privacies of Life: Automatic License Plate Recognition in Unconstitutional under the Mosaic Theory of Fourth Amendment Privacy Law. *Hamline Law Review* 38:127-160.

Bignami, F. 2007. Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law* 8:233-255.

doi:10.6342/NTU202403953

Merola, Linda, Cynthia Lum, Breanne Cave, and Julie Hibdon. 2014. Community Support for License Plate Recognition. *Policing: An International Journal* 37:30-51.

Vedaschi, Arianna, and Lubello, Valerio. 2015. Data Retention and its Implications for the Fundamental Right to Privacy. *Tilburg Law Review* 20:14-34.

doi:10.6342/NTU202403953