華岡法粹／*Hwa Kang Law Review*
Vol. 66 (2019), pp. 1-52
DOI10.6868/HKLR.201906_(66).01

警察透過資訊科技進入電腦蒐集資料的法律問題

A Study of Legal Issues on Police Infiltrate to Computer System to Collect Informations

黃　清　德*
Ching-Teh Huang

摘　　要

為有效預先防範風險轉變為危害，必須立法授權警察機關得採取許多蒐集資料的措施，這些干預措施會侵害人民的基本權利。在我國警察法危害防止領域內，如何立法因應，避免以追求提升行政效率或保障國家安全為名，發動對人民廣泛性的監控，過度侵害人民的自由權利，深具研究價值。本文以警察法領域為研究範圍，全文計分為五部分，除前言外，分別討論透過資訊科技進入電腦蒐集資料的憲法問題、德國聯邦憲法法院的相關判決與法制、以及我國警察法上的法律依據，最後提出結論與建議。

關鍵詞：科技秘密進入電腦；合理隱私期待；資訊自決權；搜索；通訊監察；概括條款；警察職權行使法

投稿日期：108.04.24　　接受刊登日期：108.06.13　　最後修訂日期：108.06.17

* 東海大學法律學研究所法學博士，臺灣警察專科學校交通管理科副教授兼科主任。
Ph. D. in Law Tunghai University; Associate Professor, Department of Traffic Management, Taiwan Police College.
本文承蒙二位匿名審查老師細心釜正，提供許多寶貴意見，特致上謝忱。

目　次

壹、前言

現代國家面對風險社會潛在的不確定情況，為有效預先防範風險轉變為危害，以避免危害發生，必須採取許多蒐集資訊的措施，往往會試圖透過立法方式，授權行政機關在該「危害尚未發生」時，即得採取限制、禁止的干預性措施，並以預防危害、風險或犯罪等公益理由，作為干預權行使正當化的理論基礎，尤其為預防具有組織、隱密、高科技、智慧、再犯等性質之特別類型的重大危害。這些預防性的規範，例如警察職權行使法規定為預防發生危害在公共場所設置監視器錄存或監視個人的活動蒐集資料[1]、集會遊行活動的蒐集資料[2]、長期跟監監視[3]、遴選第三人蒐集資料[4]、盤查查證身分及交通工具[5]、治安顧慮人口查訪[6]；道路交通管理處罰條例規定有特定範圍的前科紀錄者，不得從事計程車駕駛人[7]；保全業法規定有特定範圍的前科紀錄者不得擔任保全人員[8]等等。這些預防性的規範，大都植基於預測或預設的立場，預測危害與具體危害之間，往往存在著相當落差，稍有不慎，所採取的干預措施將會侵害相對人的基本權利[9]。

現今資訊社會，電腦及網際網路在人們的生活中扮演了極為重要的角色，尤其近年恐怖攻擊事件及其相關活動在國際間日趨頻繁，恐怖分

1　參閱警察職權行使法第 10 條。
2　參閱警察職權行使法第 9 條
3　參閱警察職權行使法第 11 條。
4　參閱警察職權行使法第 12-14 條。
5　參閱警察職權行使法第 6-8 條。
6　參閱警察職權行使法第 15 條。
7　參閱道路交通管理處罰條例第 37 條。
8　參閱保全業法第 10 條之 1。
9　李震山，公權力運用科技定位措施與基本權利保障，人性尊嚴與人權保障，頁 265，元照，2009 年 3 版。

子為避免被發覺，多不再使用傳統的書信或電話通訊方式，轉而使用隱密性極高的電腦與網際網絡系統，以降低違法行為被國家發現的風險並且增強破壞力，更加助長了利用科技犯罪的風潮。因此，傳統的國家安全防禦或偵查措施，例如實體的搜索、扣押等措施，恐怕已經無法有效完成安全偵防或犯罪偵查任務，而必須隨著科技發展考慮更隱密有效的危害防禦或偵查措施。監視與蒐集在網路系統上傳遞或存取的資訊，被視為有效且必要的隱密資料蒐集或偵查措施[10]，透過資訊科技進入電腦蒐集資料（Online-Durchsuchung），這種新型態的危害防禦或偵查措施出現，容許國家機關在一定條件下，可以透過科技隱密方式，入侵特定網路資訊系統，並監視、蒐集儲存在電腦上的資訊，需要特別法律授權[11]。這種對於網路資訊的監視與資料蒐集，並非傳統針對實體物的搜索、扣押或通訊監察措施所能涵蓋。傳統對實體的搜索、扣押，執行時必須有第三人在場，僅能針對現實空間進行搜索，或者將整部實體電腦扣押，並進一步檢視電腦硬碟內的資料；而通訊監察雖然能夠對他人正在進行中的通訊活動進行監聽，但當他人通訊活動已經終止，且資訊留存於電腦空間，即無法透過通訊監察蒐集該資訊。國家蒐集網路上資訊已經成為危害防禦的有效且必要的蒐集資料措施，其對於人民權利的干預強度並不亞於搜索、扣押及通訊監察等相類似的國家行為。

德國北萊茵西伐利亞邦 2006 年 12 月 20 日通過的憲法保護法（Gesetz über den Verfassungsschutz in Nordrhein-Westfalen）第 5 條第 2 項第 11 款，授權憲法保護局為取得資訊，得採取秘密觀察網路並蒐集網際網路資料，特別是可以隱藏性侵入網路通訊或蒐尋網路通訊，以及運用科技方法秘密蒐集儲存在電腦中資訊，聯邦憲法法院在 2008 年宣

10 Manfred Hoffmann, Die Online-Durchsuchung-staatliches “Hacken” oder zulässige Ermittelungsmaßmahne?, NStZ 2005, S. 121.

11 李震山，行政法導論，頁 471，三民，2019 年 2 月修訂 11 版。

告該規定因為欠缺完整配套措施違憲[12]，後來北萊茵西伐利亞邦因此修正憲法保護法規定以為因應。近年德國警察也採取透過資訊科技進入電腦蒐集資料措施[13]，為因應該聯邦憲法法院判決，德國聯邦與各邦警察法也紛紛立法因應，例如，巴伐利亞邦警察任務及職權法（Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei, BayPAG）、萊茵伐茲邦警察及秩序機關法（Rheinland-Pfälzischen Polizei- und ordnungsbehördengesetzes, RhpfPOG），增訂相關配討措施，作為執行依據，2011 年，德國巴伐利亞等邦官員對外表示，曾經運用木馬程式監控竊盜、詐欺、毒品案犯罪嫌疑人的電子郵件及網際網路上的語音通訊，並截取其螢幕截圖[14]。聯邦憲法法院又於 2016 年 4 月 20 日[15]與 6 月 15 日[16]分別對於聯邦刑事局法、巴伐利亞邦警察任務及職權法關於透過資訊科技進入電腦網際網路資料蒐集規定的合憲性，做成判決，足見此問題的重要性。2017 年德國刑事訴訟法第 100b 條，立法授權為了調查重大犯罪的嫌疑人或共犯等理由，得採取此項措施。

近年我國為因應恐怖攻擊事件，也在行政院下設有國土安全辦公室，綜合國內各情治機關蒐集的情資，進行研析和橫向溝通協商，如果發現可能有恐怖攻擊的危機，就會向行政院建議發出不同等級的警報，由相關單位採取因應行動。危害防止是警察主要任務，如果有恐怖攻擊事件發生或為防止重大法益危害，是否也允許警察機關採取透過資訊科技進入電腦蒐集資料措施？警察機關這種透過植入木馬程式或間諜軟

12　BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 165.

13　參見 Michael Ronellenfitsch，「行政罰與刑事罰界線問題之探討」開幕式專題報告「Polizeirecht und Datenschutz」，2013 第一屆國際暨兩岸學術研討會，真理大學，台北，2013 年 5 月 1 日。

14　Nicholas Kulish, *Germans Condemn Police Use of Spyware*, N. Y. Times, Oct. 14, 2011, https://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html, last visited 04.23.2019

15　BVerfG, 1 BvR 966/09 vom 20.4.2016.

16　BVerfG, 1 BvR 2544/08 vom 15.6.2016.

體等，秘密的監視、蒐集人民電腦系統內的數位資料，在法律上應如何評價？均有待進一步加以釐清。在我國警察法危害防止領域內，現行法制上有無可資適用的規定？或是該如何透過立法程序因應，尤其在實體上應具備何種要件，應經過何種程序，以避免以追求提升行政效率或保障國家安全為名，發動對人民廣泛性監控，過度侵害人民的自由權利，將會成為無可迴避的重要課題，值得探討與深思，也深具研究價值[17]！本文主要以警察法領域為研究範圍，合先說明，全文計分為五部分，除前言外，分別討論透過資訊科技進入電腦蒐集資料的憲法問題、德國聯邦憲法法院的相關判決與法制、以及我國警察法上的法律依據，最後提出結論與建議。

貳、透過資訊科技進入電腦蒐集資料的憲法問題

一、透過資訊科技進入電腦蒐集資料的方式

所謂透過資訊科技進入電腦資料蒐集（Online-Durchsuchung），係指警察機關為了蒐集儲存在電腦與網路上的資料，透過資訊科技侵入被蒐集的網際網路的目標系統，有效取得在網路系統上儲存的資訊，或監視他人在網路空間的活動歷程[18]，這種新型態的危害防禦或偵查措施出現，容許警察機關在一定條件下可以入侵特定資訊系統，並監視、讀取與使用存於該電腦的資訊。

警察機關必須先確認以及分析被蒐集的網際網路的目標系統功能，才能進一步入侵該系統。常見的入侵目標系統方式，大約有以下幾種[19]：

---

17 林明鏘，由防止危害到危險預防，警察法學研究，頁 37，新學林，2011 年。

18 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 5.

19 Stefan Hozner, Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, 2009, S. 11 ff. 轉引自馮聖宴，國家駭客！？-德國聯邦憲法法院關於「線上搜索」

（一）刺探利用

所謂「刺探利用」（Exploits），係指警察機關利用資訊系統既存的安全性漏洞入侵將被蒐集的目標系統。這種入侵方式又可進一步分為兩種類型，分別是「零時差刺探利用」（Zero-Day-Exploit）以及「低於零時差刺探利用」（Less-Than-Zero-Day-Exploit）。前者指利用作業系統生產者「已經發現並公告」的系統安全性漏洞的入侵軟體，由於安全性漏洞已公告周知，這種軟體要發生入侵系統的效果，就必須在安全性公告當日，系統使用者尚未使用對抗漏洞措施前入侵目標系統，這種入侵軟體不適合警察機關用來入侵目標系統，因為目標系統使用者隨時可以修補該安全性漏洞並採取對抗入侵措施，導致線上蒐集資料失敗。反之，後者係指利用系統生產者尚未發現的安全性漏洞入侵軟體，由於系統生產者尚未知悉安全漏洞存在，亦無法公告或修補該漏洞，系統使用者便無法採取對抗入侵軟體的措施，使用此種入侵方式顯然極為有效，但仍有系統使用者發現漏洞後採取反入侵措施的風險。

（二）後門程式

所謂「後門程式」（Backdoor），係指未經用戶允許，且利用不正當手法，侵入電腦系統進行監視或操控的程式。「後門程式」可以繞過軟體安全性控制，而以較隱密方式進入資訊系統的方法，部分軟體提供者在設計軟體開發時會設計後門方便修補程式，若目標系統存有後門程式軟體，警察機關即可透過後門程式進入目標系統。

（三）特洛伊木馬程式

「特洛伊木馬」（Trojan Horse）是一個木馬程式，可以盜取用戶的個人資訊，甚至是遠端控制對方的電腦作，通過各種手段傳播或者騙取

判決簡介（上），http://www.justuslaw.com.tw/news_detail.php?class=145, last visited 04.23.2019.

目標使用者執行該程式，以達到盜取密碼等各種資料的目的。一個完整的特洛伊木馬套裝程式包含兩部分：服務端（伺服器部分）和用戶端（控制器部分）。植入對方電腦的是服務端，而駭客正是利用用戶端進入執行服務端的電腦。執行了木馬程式的服務端以後，會產生一個有著容易迷惑用戶的名稱的進程，暗中打開埠（Port），向指定地點發送資料（如網路遊戲的密碼，即時通訊軟體密碼和用戶上網密碼等），甚至可以利用這些打開的埠進入電腦系統[20]。木馬程式的特色在於其通常隱藏並附著於系統使用者利用的特定檔案中，在使用者下載或開啟該檔案同時，也連帶啟動木馬程式運作。

（四）按鍵紀錄程式

「按鍵記錄程式」（keylogger）會記錄鍵盤活動，會攔截並儲存所有鍵盤活動，而讓某人或其他應用程式有機可乘，將按鍵記錄加以分類，以挑選出如登入憑證與信用卡號碼等有價值的資訊。若國家機關使用此程式，則可獲取入侵目標系統所需的帳號或密碼，順利入侵目標系統。

（五）系統使用者本身或其他國家協力機關裝置入侵軟體

最後一種入侵目標系統的方式，便是系統使用者在使用其他軟體裝置時，無意識地將某種入侵系統的軟體也裝載於系統或硬體中，或者未執行線上蒐集資料的國家機關，本於其協力義務入侵目標系統電腦所在實體領域，並裝置入侵程式於該電腦中，使得執行線上蒐集資料的國家機關得以入侵目標系統。

---

20 有關特洛伊木馬程式的敘述，http://zh.wikipedia.org/wiki/%E7%89%B9%E6%B4%9B%E4%BC%8A%E6%9C%A8%E9%A9%AC_(%E7%94%B5%E8%84%91), last visited 05.04.2018.

二、透過資訊科技進入電腦蒐集資料涉及的基本人權

透過資訊科技進入電腦蒐集資料的方式在技術上可以做到，尤其在「危害尚未發生」時即得以蒐集資料，問題是在法律上是否允許，尤其這措施強烈干預人民居住自由、營業自由、資訊隱私權、一般行為自由、人性尊嚴等基本人權，會涉及到我國現行法制上是否有相關的授權依據，說明如下：

（一）秘密通訊自由

警察透過資訊科技進入電腦蒐集資料是否會干預人民秘密通訊自由？憲法第 12 條規定：「人民有秘密通訊之自由」，秘密通訊亦屬言論自由表達方式之一，憲法特別將此種方式視為基本權加以保障，同時寓有私生活領域不受侵擾、隱私維護、資訊自決權以及人格形成自由之保障的意義，國家非有法令的依據，不得對人民秘密通訊的自由加以侵擾。所謂秘密，屬個人化的事項，個人得決定是否使他人知悉的情事[21]。傳統意義的秘密通訊自由是一種古典的人權，具有濃厚的防衛權色彩，從我國制憲史的解釋角度，秘密通訊自由的內涵，似可初步界定其保障範圍為書信秘密、郵件秘密及電報秘密，秘密通訊權即是用來防止國家濫用郵政權來揭露、知悉人民通訊信件的內容。然而，在現今通訊科技高度發展的資訊社會型態中，通訊的媒介多元，以電話、傳真、電子郵件（E-mail）、網際網路、衛星通訊的方式[22]，已逐漸取代傳統的通訊方式，不受空間距離的限制，可謂通訊已無國界，通訊速度提升、費用更為低廉等，傳統的秘密通訊自由概念必須予以擴張，無論人民使用何種

21　李惠宗，憲法要義，頁 219，元照，2015 年 7 版。

22　李惠宗，同前註，頁 219。

通訊媒體，都受到憲法保障[23]。

秘密通訊自由可以防禦來自國家以及其他私人的侵害[24]，秘密通訊自由係人民對於通訊內容，甚至對通訊雙方－即真實的發訊人及收訊人－擁有保密，無須告知國家機關的權利。秘密通訊自由保障人民在通訊過程中，有隱密的權利，均可列入秘密通訊自由的範疇[25]，凡人民使用通訊媒體，不論係以書信、郵件、電報、電話、傳真、衛星通訊或網際網路的通訊方式，均屬秘密通訊自由的保障範圍，自不應拘泥於制憲者當時的認知，應衡酌日常生活的觀念、傳統意涵及前瞻的思考，合理解釋秘密通訊自由的內涵，新型態的通訊方式應受到憲法第 12 條的保障[26]。然而對於通訊已經終結，儲存在電腦系統的資料，因為已經不再是通訊，所以不再是秘密通訊所要保障的客體[27]，透過資訊科技進入電腦進行資料蒐集，恐怕無法援引我國憲法秘密通訊自由加以對抗[28]。

（二）居住自由

憲法第 10 條規定人民有居住自由，旨在保障人民有選擇其居住處所，營私人生活不受干預的自由。居住自由的保護領域，係指任何人在其居住空間內享有一安寧居住空間，國家公權力不得非法侵入，人民在安寧居住空間內發展其人格，同時衍生出人民隱私權[29]，居住自由的保

23 吳　庚，憲法的解釋與適用，頁 205，三民，2003 年；陳新民，中華民國憲法釋論，頁 256-257，三民，2001 年 4 版。

24 Ingo von Münch/Philip Kunig/Brun-Otto Bryde, Grundgesetz-Kommentar, 5. Aufl., 2000, Art. 10 Rn. 14; 李惠宗，憲法要義，頁 206，元照，2009 年 5 版。

25 陳新民，同註 23，頁 256-257。

26 黃清德，科技定位追蹤監視與基本人權保障，頁 138，元照，2011 年。

27 李育典，憲法，頁 258，元照，2013 年 6 版。

28 陳英鈐，「通訊監察保障之建置及運用－論德國聯邦憲法法院線上搜索與資訊隱私權保護判決對我國基本權體系應有的回應」，21 世紀資訊法制之新趨勢學術研討會，台灣行政法學會，台北，2010 年 1 月 30 日。

29 陳新民，憲法學釋論，頁 257 以下，三民，2015 年修訂 8 版。

護雖以住宅為中心，但不限於住宅，並包括住宅及其附屬空間、工作房、營業處所及其周圍的土地[30]。

國家若侵入住宅並搜索、扣押物品，除侵犯居住自由外也構成隱私權的嚴重侵害。然國家為增進公共利益的必要，於不違反憲法第 23 條所規定的要件以及法律程序下，非不得以法律對於人民居住自由予以限制（釋字第 596 號、第 454 號解釋參照），國家機關仍得進入人民的住宅或營業場所搜索或扣押。為刑事訴追目的所進行的住宅搜索必須由司法機關所核發的搜索票；對於基於行政檢查目的所進行的進入室內資料蒐集，並不認為需有法官保留原則的適用，司法院大法官第 535 號解釋也認為「除法律另有規定外，警察人員執行場所之臨檢勤務，應限於已發生危害或依客觀、合理判斷易生危害之處所、交通工具或公共場所為之，其中處所為私人居住之空間者，並應受住宅相同之保障。」警察職權行使法第 6 條第 4 項規定：「警察進入公眾得出入之場所，應於營業時間為之，並不得任意妨礙其營業。」並未明白要求行政調查必須要有法官保留的適用。如果透過資訊科技進入住宅中的電腦蒐集資料，是由侵入住宅或穿透住宅的方式為之，也構成居住自由的干預；透過網際網路上蒐集資料樣態繁多，未必都是由入侵住宅的方式為之，例如對於在住宅以外場所使用手機、手提電腦的情形，因此必須要有其他基本權的保護，才能避免浮濫透過資訊科技進入電腦蒐集資料[31]。

（三）營業自由

我國憲法沒有明文提及職業自由、工作自由或營業自由，但依照司法院大法官解釋，憲法第 15 條規定人民之工作權應予保障，包括人民得自由選擇工作及職業的自由[32]，亦包括營業自由[33]、營業秘密[34]。雖有

30　李震山，警察行政法論，頁 278-279，元照，2016 年修訂 3 版。

31　陳英鈐，同註 28，頁 84-85。

32　參閱司法院釋字第 404、411、510、514、584、606、612 號解釋。

認為營業自由一詞的憲法保障依據，應由憲法第 22 條的概括保障條款中導出營業自由的主張者[35]，但自釋字第 514 號以來，大法官皆以憲法第 15 條的工作權與財產權的保障規定為依據[36]，營業自由受到憲法所保障應無疑問[37]。警察機關透過資訊科技進入電腦蒐集資料時，容易看到不相關人的信件內容與資料，尤其進入蒐集的如果是公司的電腦時，會蒐集察看到該公司客戶儲存於其電腦系統中的資料[38]，或營業上的機密資料，凡此種種皆涉及營業自由。

---

33 參閱司法院釋字第 538 號解釋。

34 參閱司法院釋字第 585 號解釋理由書。

35 黃越欽大法官於司法院釋字第 514 號解釋的不同意見書中，以德國基本法中的職業選擇自由並不同於我國憲法第 15 條的工作權，不應將兩者「穿鑿附會」、「混為一談」為由，認為營業自由不在工作權與財產權的保障範圍之內，應由憲法第 22 條導出。黃大法官的論點可說是建立在憲法第 15 條所保障之「工作權」非屬自由權性質之職業自由或工作自由，而是受益權或社會權性質的前提之上。基此而主張營業自由固為職業選擇自由的一環，但不具社會權的性質，因而與憲法第 15 條之保障無關。

36 若不論大法官協同意見書或不同意見書中的意見，則主要是在司法院釋字第 514、538、606 號解釋文與解釋理由書中論及營業自由的憲法保障依據。釋字第 514 號解釋：「人民營業之自由為憲法上工作權及財產權所保障。有關營業許可之條件，營業應遵守之義務及違反義務應受之制裁，依憲法第二十三條規定，均應以法律定之，其內容更須符合該條規定之要件。」解釋理由書中更明確指出：「人民營業之自由為憲法第十五條工作權及財產權應予保障之一項內涵。基於憲法上工作權之保障，人民得自由選擇從事一定之營業為其職業，而有開業、停業與否及從事營業之時間、地點、對象及方式之自由；基於憲法上財產權之保障，人民並有營業活動之自由」對營業自由定下了範圍，認為人民的工作權包括營業活動自由、開業及停業自由、營業時間自由、選擇營業地點自由、營業對象自由及營業方式自由等。釋字第 606 號解釋理由：「人民營業之自由為憲法上工作權及財產權所保障，本院釋字第五一四號解釋足資參照」。

37 蔡宗珍，營業自由之保障及其限制，台灣大學法學論叢，第 35 卷，第 3 期，頁 287，2006 年 5 月。

38 李震山，同註 9，頁 259。

（四）資訊隱私權

在美國法中，資訊隱私權乃「隱私權」所涵蓋的重要類型之一，我國憲法並未明文保障隱私權，直到釋字第 585 號解釋，大法官明白地表示隱私權為憲法第 22 條所保障的權利，並揭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的核心價值，基於人性尊嚴與個人主體性的維護及人格發展的完整，為保障個人生活私密領域免於他人侵擾及個人資料的自主控制；大法官在釋字第 603 號解釋詳細地闡述資訊隱私權，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、向何人揭露的決定權，並保障人民對其個人資料的使用有知悉與控制權及資料記載錯誤的更正權，確定隱私權屬憲法第 22 條所保障的權利。個人資料有其私密性，因此隱私權中有關個人資料的部分，即稱之為資訊隱私權[39]。

「資訊自決權」則是較屬於德國法的概念與用語[40]。資訊自決權的用語，乃由德國聯邦憲法法院於 1983 年人口普查案判決[41]，自一般人格權進一步闡釋發展出資訊自決權理論[42]，亦即所有的個人資料均受到保護[43]，人有權自己決定，是否或在如何範圍內公開個人資訊，而且資訊

39　李震山，資訊權－兼論監視器設置之法律問題，多元寬容與人權保障－以憲法未列舉權之保障為中心，頁 196，元照，2007 年 2 版。

40　黃昭元，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，載民主人權正義－蘇俊雄教授七秩華誕祝壽論文集，頁 469，元照，2005 年。

41　BVerfGE, 65, 1ff. 判決中譯，參閱蕭文生，關於「一九八三年人口普查法」之判決，西德聯邦憲法法院裁判選輯（一），頁 288 以下，司法週刊雜誌社，2000 年。

42　Vgl. Ingo von Münch/Philip Kunig/Brun-Otto Bryde, a.a.O. (Fn.24), Art. 1 Rn. 36.

43　德國聯邦憲法法院關於人口普查案中指出：「欲決定資訊自決權對於國家要求國民提供涉及人身資料之侵害的作用範圍，不能只針對資料的性質而定，決定性的因素乃在於資料實用性和使用可能性。就此，一方面取決於該資料蒐集所欲追求的目的，另一方面則視資訊技術上，資料處理與資料結合的可能性而定；一項原本看來不重要的資料，可能在資料處理後得到新的意義，就此而言，在自動化資料處理的情形下，已不再有所謂『不重要』的資料存在。」參閱李震山，同註 9，

的使用過程也必須是依據當初蒐集的目的[44]。亦即「資訊自決權」，係指每個人基本上有權自行決定，是否將其個人資料交付與利用[45]。我國大法官釋字第 603 號解釋揭示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。易言之，個人資料非經本人許諾，不得任意蒐集、儲存、運用及傳遞，若基於公益的理由，必須限制該權利，當然必須具備憲法上要求的原則。資訊自決權由憲法上人性尊嚴的要求所導出，因人性尊嚴要求人本身即是目的，不得被物化以及人必須得以自治，不得處於被操控的他治他決的地位，以維護人的主體性，原則上，立法者只有在重大公共利益的考量下，才得以限制資訊自決權[46]，並僅得以法律限制之[47]。資訊自決權肯認每一個人對於涉及自己資料提供、利用的決定過程，皆有積極參與及形成自我決定的可能，並且尚得以之作為抗拒他人恣意干涉的消極自由權，唯有如此，作為主體性的個人，其人性尊嚴，才不致受貶損[48]。從大法官第 603 號解釋的見解來看，資訊自決與資訊隱私權實為一體的兩面，所指涉的範圍似乎沒有什麼差距。

資訊自決要求應在本人同意之下，方能蒐集、儲存、傳遞及利用有關個人的資料，亦即個人應有決定何時以及在何種限度下將個人的生活事實公開呈現的權利[49]，因此，警察透過資訊科技進入電腦，人民在不知情的狀況下，儲存在電腦中的資料，例如電子郵件、電腦書寫的文字、

頁 229。

44 Walter Schmitt Glaeser, Schutz der Privatspäher, in: Heidelberg, Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 6.1989, S. 66 Rn. 43.

45 李震山，同註 9，頁 221。

46 Dipl.-Kfm. Gerhard F. Müller, Michael Wächter, Eine systematische Darstellung des Bundesdatenschutzgesetzes, 1991, S. 2.

47 Stefen Zeitler, Allgemeines und Besonderes Polizeirecht für Baden-Württemberg, 1998, Rn. 365.

48 李震山，同註 9，頁 214-215。

49 黃清德，同註 26，頁 160。

照片、購物紀錄、通訊錄、甚至整個家庭生活上點點滴滴的紀錄等等各項輸入的資料，都被秘密的蒐集，人民無法充分安全的綜觀哪些涉及他自己的資料，已經被蒐集或利用等，而無法決定其公開個人資料的範圍；即使知道資料已經被蒐集，但也無法知悉或參與後續資料的利用、保存問題，亦會使資訊自決權受到影響，這種趨勢無疑地已強烈威脅到個人資料的隱密性以及自主決定的權利，當個人資料輕易地暴露於有心人的侵襲與操控之後，個人隱私及其權益尊嚴飽受威脅，嚴重受到侵害。

（五）一般行爲自由

一般行為自由（Allgemeine Handlungsfreiheit）係指一般人格權（Allgemeine Persönlichkeit）中的行為自由，即在遂行人格自由發展中，個人行為除非傷及他人權利，或違反憲政秩序或道德法（Sittengesetz），應有其完全作為或不作為的自由。德國基本法第 2 條第 1 項除保障人格自我發展與型塑權外（Recht auf freie Entfaltung der Persönlichkeit），尚保障一般行為自由[50]。一般行為自由所強調者，在於人格的自由發展，沒有其他個別基本權受到干預時，審查是否一般行為自由受侵害[51]，作為其他個別基本權的補充[52]，乃具有補充性質的自由權概括條款（subsidiäre Generalklausel der Freiheitsrechte）[53]，亦即，必須是未涉及其他個別基本權利所涵蓋的保護領域時，才援引一般行為自由作為保護基礎[54]，以免掏空個別基本權利的保障內容，著重權利主體的行為保障

50　Vgl. Ingo von Münch/Philip Kunig/Brun-Otto Bryde, a.a.O. (Fn.24), Art. 2 Rn. 1, 2.

51　Vgl. Gerrit Manssen, Staatsrecht II, 2. Aufl., 2002, Rn. 199.

52　Vgl. Gerrit Manssen, a.a.O., Rn. 868.

53　司法院釋字第 666 號解釋大法官林錫堯、陳敏、陳春生協同意見書：「…『一般行為自由』（allgemeine Handlungsfreiheit）……此種基本權之性質屬補遺性基本權（Auffanggrundrecht），若個別基本權利保障範圍所及之事項與內涵，即非其保障範圍所涵蓋。換言之，係居於其他基本權利之後，僅在特別基本權之保護領域所不及之處，始生作用。」

54　Das Bonner Grundgesetz: Kommentar, Art. 2 Abs. 1 Rn. 81; Walter Schmitt Glaeser,

[55]。而人格自由發展應以個人自我形塑權為核心，即自我決定「我是什麼」的權利[56]。美國聯邦憲法第 9 增修條文規定：「本憲法對於一定權利之列舉，不得解釋為否定或輕視人民所保有的其他權利。」與我國憲法第 22 條規定：「凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。」分別以正面與反面的規範方式，規定憲法所保障的自由權利，不限於憲法所明文列舉。憲法第 22 條從文義而言，係概括性權利規定，從理論言，應為導出「新興人權」保障的重要規定。

我國憲法第 22 條規定賦予人民有一般的自由權利，其功能與德國基本法第 2 條的「一般行為自由」或「人格發展自由」同義[57]；陳春生等三席大法官在司法院大法官釋字第 666 號解釋協同意見書指出，德國基本法第 2 條第 1 項保障的一般行為自由與我國憲法第 22 條規定的功能相同[58]，因此一般行為自由應屬於我國憲法第 22 條保障的範圍。

國家對人民資料的蒐集、建檔所形成的心理制約，即是產生此種人性異化病徵的一種可能形式[59]。當個人知道自己可能正在被政府監視之

---

a.a.O. (Fn. 44), S. 47 Rn. 9.

55 司法院釋字第 666 號解釋大法官林錫堯、陳敏、陳春生協同意見書：「…『人格自由發展』（Freie Entfaltung der Persönlichkeit）之規定，依學理上之闡述，係保障兩項基本權，一為『一般行為自由』（allgemeine Handlungsfreiheit）；另一為『一般人格權』（allgemeines Persönlichkeits-recht）。……前者乃具有補充性質之自由權概括條款（subsidiäre Generalklausel der Freiheitsrechte），著重權利主體之行為保障…。」

56 Vgl. Niklaus Lumann, Grundrecht als Institution, 1965, S. 55 f., 75; 李震山，同註 39，頁 234-235。

57 李惠宗，同註 21，頁 396。

58 司法院釋字第 666 號解釋大法官林錫堯、陳敏、陳春生協同意見書：「如同我國憲法第二十二條規定之功能德國基本法第二條第一項規定：『每個人於不侵害他人權利、不牴觸合憲秩序及公序良俗之情形下，皆有自由發展其人格之權利』，此係關於『人格自由發展』（Freie Entfaltung der Persönlichkeit）之規定，依學理上之闡述，係保障兩項基本權，一為『一般行為自由』（allgemeine Handlungsfreiheit）；另一為『一般人格權』（allgemeines Persönlichkeitsrecht）。」

59 李建良，「戶籍法第八條捺指紋規定」釋憲案鑑定意見書，台灣本土法學雜誌，

下時，他的行為就會不自然，不敢表現自己，已經對個人內在產生一種「心理制約」，不僅短時間內會影響到個人的行為自由，經過長時間的「內化」過程後，將達到行為模式規格化的作用，如同侵害個人行為自由於無形。警察利用資訊科技進入電腦蒐集資料干預基本權的同時，往往也干預了一般行為自由，對個人自主決定本身的干預，將造成個人不願意或不放心將資料儲存在電腦中的心理制約[60]，進而導致在思想、言語、行動各層面上的「精神上寒蟬效應」，並可能同時影響民主社會重要的價值秩序：思辯民主的形成[61]。

（六）人性尊嚴

德國基本法第 1 條第 1 項規定：「人性尊嚴不可侵犯，對其之尊重與保護係所有國家權力之義務。」為德國基本法明文規範「基本權」保障的重要條文[62]。依照德國聯邦憲法法院的論述[63]，憲法中人性尊嚴的核心內容有二：其一為，人本身即是目的，不得被要求或視為一種工具或手段；其二，人得以自治（律）自決，不應處於被操控的他制（律）他決的地位。因此，高度屬人化且已成為人格一部分的「個人資料」，不能令其商品化或物化，以貶抑人性尊嚴[64]。

我國憲法憲法增修條文第 10 條第 6 項規定：「國家應該維護婦女之

第 73 期，頁 43，2006 年 8 月。

60 李震山，個人資料保護與監視錄影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，第 4 期，頁 47，2005 年 12 月。

61 Andrew E. Taslitz, *The Fourth Amendment In The Twenty-First Century: Technology, Privacy, And Human Emotions*, 65:2 LAW AND CONTEMPORARY PROBLEM. 125, 127 (2002).

62 蕭淑芬，論基本權核心概念之規範－一個比較法學的觀察，東海大學法學研究，第 19 期，頁 11-12，2003 年 12 月。

63 BVerfGE 9, 89 (95); E 50, 166 (175); E 57, 250 (275); E 72, 105 (118)., Vgl. Ingo von Münch/Philip Kunig/Brun-Otto Bryde, a.a.O. (Fn.24), Art. 1 Rn. 19, 20.

64 李震山，同註 9，頁 11-15。

人格尊嚴，保障婦女之人身安全，消除性別歧視，促進兩性地位之實質平等。」得否作為人性尊嚴保障的直接依據？李震山大法官認為從規範內容的目的言，依該條文的解釋，不應得到國家只維護婦女人格尊嚴的結論，因為在同條文中有：「……消除性別歧視，促進兩性地位平等」。在整個條文的邏輯、結構與體系上看，既是強調兩性平等，在解釋上自不得引用「列舉其一，排除其他」的法理，排斥男性的人格尊嚴保障，應是所有「人的尊嚴」皆需保障[65]。該條文中捨人性尊嚴而採人格尊嚴，兩用語或有其差異，人性尊嚴即是人的尊嚴，其核心在強調每個人有「人格自我形塑」的自治自決權，從而每個人有其獨立性，以及個人間有其差異性。人性尊嚴除自主性外，尚包括不得以自主權為前提，將自身物化、商品化、工具化。譬如：若尊重個人成為他人工具與奴隸的意願，似乎合於人格自我形塑自由，但卻違反人性尊嚴中不得將人物化、商品化的要求[66]。人性尊嚴是基本權的基礎，具有「人的主體性」與「人的自由意志應受尊重」的兩個基本內涵；人性尊嚴也是先國家性的基本權的一種[67]，乃生為一個人即擁有的權利，無待國家加以規定，國家不得加以剝奪[68]。

警察機關如果為發現真實，不計代價採取任何非法手段，不當運用

65 同前註，頁 20-22。

66 德國聯邦最高法院經常引德國基本法第 2 條第 1 項一般人格權，作為隱私權保護之依據，但也都同時或附帶援引基本法第 1 條第 1 項人性尊嚴條款。依學者 Wolfgang Kahl 之研究，此並不表示上兩項權利是屬「雙胞胎基本權利」（Zwillingsgrundrecht），毋寧說是，為明確化一般人格權之內容及包護範圍，借助憲法價值判斷中具客觀放射效果（objective Ausstrahlungswirkung）之人性尊嚴，作為上位憲法原則。德國基本法雖將兩者分別規定，仍無法區隔兩者之密切關係，參見 Wolfgang Kahl, Die Schutzerganzungsfunction von Art. 2 Abs.1, Grundgesetz, 2000, S. 6-7.

67 人性尊嚴是否為一項獨立基本權？相關論述詳請參閱李建良，自由、平等、尊嚴（下）－人的尊嚴作為憲法價值的思想根源與基本課題，月旦法學雜誌，第 154 期，頁 199-200，2008 年 3 月；李震山，同註 9，頁 21-23。

68 李惠宗，同註 21，頁 92。

資訊科技進入電腦蒐集資料，尤其過程中許多非犯罪嫌疑人與非滋擾者成為資料被蒐集的對象，嚴重限制個人自我決定權，連帶干預到第三人的權利，已因侵害個人的主體性以及自由應受尊重「內在領域」的自由，而傷及人性尊嚴。

三、小結

警察機關為了蒐集儲存在電腦與網路上的資料，透過資訊科技侵入被蒐集的網際網路的目標系統，有效取得在電腦網路系統上儲存的資訊，或監視他人在網路空間的活動歷程，尤其在「危害尚未發生」時即得以蒐集資料，在技術上可以做到，但問題是在法律上是否允許？尤其這措施強烈干預人民居住自由、營業自由、資訊隱私權、一般行為自由、人性尊嚴等基本人權，應該要有明確的法律授權依據，以符合法治國的要求，而我國現行法制上是否有相關的法律授權依據，應加以深思與探討，面對新興資訊科技問題，法律應如何審查新興科技所產生的基本權利侵害，將是一個新的挑戰。

參、德國聯邦憲法法院關於透過資訊科技進入電腦資料蒐集判決與法制

一、德國透過資訊科技進入電腦蒐集資料的法制概況

德國聯邦最高法院判決指出，刑事訴追機關執行透過資訊科技進入電腦網際網路蒐集資料，並無法在刑事訴訟法上找到法律依據[69]，德國

69 Vgl. Manfred Hoffmann, a.a.O. (Fn. 10), S. 121; BGHSt 51, 211; BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 7. 轉引自陳英黔著，台灣行政法學會主編，通訊監察保障之建制及運用－論德國聯邦憲法法院線上搜索判決對我國資訊隱私權的啟發，資訊法制、土地規劃與損失補償之新趨勢，頁 293-312，元照，2010 年 9 月。

聯邦與各邦紛紛提出法律修正案，以回應判決的要求。德國北萊茵西伐利亞邦在其邦法位階之憲法保護法（Verfassungsschutzgesetz）中明文規範線上搜索，授權邦憲法保護局（Bundesamt für Verfassungsschutz）得基於危險防禦目的，在一定條件下侵入他人資訊系統進行線上蒐集資料。憲法保護法第 5 條第 2 項第 11 款，明文規範授權憲法保護局得為預防性的秘密線上蒐集資料與監控[70]（heimlicher Zugriff auf informationstechnischer System）：為取得資訊作為情報手段，憲法保護局得採取秘密觀察網路並進行其他搜尋，特別是秘密侵入網路通訊或搜尋網路通訊，以及運用科技方法秘密搜集資訊科技體系，憲法保護局可以藉此監視網路通訊及透過技術性方式獲取其內容。此項規定包含秘密參與以及秘密蒐集兩個特別的干預構成要件，但是兩者皆被聯邦憲法法院認為該規定欠缺完整配套措施宣告違憲[71]。後來北萊茵西伐利亞邦憲法保護法、德國聯邦刑事局法、巴伐利亞等邦警察法紛紛修法加以因應。2017 年 7 月 18 日德國刑事訴訟法第 100b 條，立法授權為了偵查該條第 2 項所指特別重大犯罪的嫌疑人或共犯，或是利用其他方式調查事實或確定被告的所在地將更加困難或無望時，得採取此項措施，該立法採重罪原則、最後手段原則及比例原則。

二、德國聯邦憲法法院關於透過資訊科技進入電腦蒐集資料判決

本案[72]的原告有 1a、1b、2a、2b、2c 等五人，1a 是新聞記者，主要從事線上出版的工作，因工作性質，常常瀏覽反憲法之人及組織的網站，他也與他人共同經營網站聊天室，致力於資料保護問題，右翼極端

70 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 5.
71 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 165.
72 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333).

分子亦會參加其聊天室。1a 為了私人及工作的目的，於硬碟中儲存這些資訊。1b 為北萊茵西伐利亞邦左派政黨（DIE LINKE）中的積極成員，遭受到該邦憲法保護局的監視，他也自己使用自己的電腦接連網路從事其政治活動，也使用網路為私人通訊以及金融帳戶進行消費的交易。2a 與 2b 為法律事務所的合夥人，2a 專門為尋求政治庇護者代言，而其客戶中有一個為庫德族勞工黨（PKK）的領導人，也受到憲法保護局的監視，2a 使用其家中及辦公室連接電腦的網路，辦公室的網路同時也被 2b 及 2C 使用，2C 為受雇於法律事務所的自由業者[73]。這五名提起憲法訴願的訴願人本身並非憲法敵對人士或敵對組織的成員，但卻因為透過網路與被憲法保護局監視的人士有某種聯繫，因此成為憲法保護局線上蒐集資料的對象。原告以北萊茵西伐利亞邦（Nordrhein-Westfalen）憲法保護法中相關的秘密線上蒐集資料與監控條文違反基本法第 2 條第 1 項連結第 1 條第 1 項人格權保護、基本法第 10 條第 1 項通訊自由權以及基本法第 13 條第 1 項家宅不受侵犯權為由，向聯邦憲法法院提起憲法訴願。

此種為因應極端主義及恐怖主義者，利用資訊科技經由網際網路侵入電腦蒐集資料，此種資料若國家用以往的資料蒐集方法，例如查封電腦及儲存硬碟難以獲得，而且不同於搜索房屋，人民無法事前受到警告，甚至可以得到使用者當下正在使用的資訊，如果長期監視更可遏止

73 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 116-118. 另請參閱林佳儀，國家進行非侵入性線上資訊蒐集分析之基本權利類型探究－以「電腦基本權」創設問題為中心，該文參考德國聯邦憲法法院，認為我國亦有發展出電腦基本權新興權利之空間，使基本權利保障盡可能無漏洞之功能，http://www.law.ntu.edu.tw/center/%E5%85%AC%E6%B3%95%E4%B8%AD%E5%BF%83/graduate_file/%E5%9C%8B%E5%AE%B6%E9%80%B2%E8%A1%8C%E9%9D%9E%E4%BE%B5%E5%85%A5%E6%80%A7%E7%B7%9A%E4%B8%8A%E8%B3%87%E8%A8%8A%E8%92%90%E9%9B%86%E5%88%86%E6%9E%90%E4%B9%8B%E5%9F%BA%E6%9C%AC%E6%AC%8A%E5%88%A9%E9%A1%9E%E5%9E%8B%E6%8E%A2%E7%A9%B6.pdf，最後瀏覽日期：2019 年 4 月 18 日。

有關加密及其他預防措施，並且可以蒐集密碼以及個人的使用習慣，這些皆是傳統的調查方法難以獲得的。這種資料蒐集措施，引起了德國法學界許多的討論，認為其究竟是一種國家「駭客」或者是合法調查措施[74]；法院實務上態度前後也有很大的改變，2006 年 2 月 21 日德國聯邦最高法院肯定其合法性，認為屬於德國刑事訴訟法中的搜索，但在同年的 11 月 25 日，聯邦最高法院一反前述立場，認為這種措施違法，2007 年德國聯邦最高法院仍維持此一立場，認為這種資料蒐集措施不屬於刑事訴訟法中的搜索，且刑事訴訟法中也沒有任何依據[75]。

德國聯邦憲法法院於 2008 年 2 月 27 日宣布，北萊茵西伐利亞邦 2006 年 12 月 20 日立法通過，為了國家安全的目的，賦予國家得於電腦及網路上蒐集人民資訊的權力，所制定的北萊茵西伐利亞邦憲法保護法第 5 條第 2 項第 11 款規定違憲，並認為現有的基本權出現漏洞，故創設電腦基本權，作為一般人格權保障的特殊面向，其從德國基本法第 1 條第 1 項人性尊嚴的保障及基本法第 2 條第 1 項一般人格權中導出，認為科技資訊系統親密性與整合性保障權，旨在確保使用者所創造、擁有及儲存在資訊科技系統中的資訊的利益受到保障而可維持其秘密性，此為保障個人主體性及人性尊嚴所不可或缺[76]。此基本權所保障的客體涵蓋的範圍包括儲存於網路服務提供中的資料，如其所提供的儲存空間以及短期記憶體中的暫時性或永久性資訊，故可保障人民使用網路的過程當中，各種紀錄不受國家任意的蒐集、分析，亦可解決居住自由限定於空間面向的保障不足的情形，其所欲保障者為利用網路的秘密性及人格的整合性，故人民利用網路、網站的過程中，所需附隨公開或透露給資訊交換者之片段、零碎的資訊，國家亦不得任意蒐集拼湊建立人

74 Vgl. Manfred Hoffmann, a.a.O. (Fn.10), S. 121.

75 何賴傑，論德國刑事程序「線上搜索」與涉及電子郵件之強制處分，月旦法學雜誌，第 208 期，頁 234-236，2012 年 9 月。

76 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 201.

格圖像[77]。

於合憲性控制方面，德國聯邦憲法法院認為北萊茵西伐利亞邦憲法保護法並未盡其立法義務，憲法保護機關所採取的調查措施是否侵害了某些基本權的問題，須進行複雜的評價與衡量，此主要且應優先由立法者處理。立法者對其任務，亦即以適當立法措施具體化所有基本權的任務，不能僅以在構成要件上連結到一種可能相關基本權的方式，而將該等基本權應如何履行的決定權轉交給執行法規的行政機關。北萊茵西伐利亞邦憲法保護法，將網際網路蒐集資料的發動要件及程序，皆援引規範秘密通訊之基本法第 10 條施行法，立法者並未於此法本身規定此種新型態的國家干預行為的合憲程序及控制要件，並且第 5 條第 2 項第 11 款後段更用「與干預秘密通訊自由有本質及強度相等性」作為適用基本法第 10 條施行法的要件，而委由行政機關判斷有無達到此種干預程度。對於北萊茵西伐利亞邦憲法保護法第 5 條第 2 項第 11 款後段這種規定新型態的調查措施的法規範來說，不符明確性要求。為了在程序上確保受監控者的利益，必須要有程序上的措施考量基本權的侵害強度，原則上此種干預必須事先取得法院的許可（法院保留）[78]，唯有經由獨立並且中立的機構，對於預計採行的秘密偵查措施進行預防性的控制，才能滿足有效基本權利保障的要求。聯邦憲法法院並非毫無例外否定此項措施的合憲性，憲法法院認為只要有事實依據顯示，對重要優越利益存有具體危害，例如生命、身體、自由以及為避免危害國家存立或人類生存之公共利益，且有相當高的可能性，該具體危害於可見的未來即將發生，在符合法官保留原則以及對私人核心生活領域有防護措施時，該法律就不致違憲，對於為了預防危害透過資訊科技進入電腦蒐集資料措施，提出了可以合法獲得法律授權的標準[79]。

77　BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 201-203.

78　BVerfG, 1 BvR 370/07 vom 27.2.2008, Leitsätze 3.

79　何賴傑，同註 75，頁 237、244。

三、德國警察法修法因應動向

為因應資訊時代的迅速蓬勃，規範警察蒐集資料的法制必須隨之進展，以達兼顧維護治安與人權保障的功效，德國是一個警察法學發達國家，制定有許多比較完整的警察蒐集資料法制[80]，值得我國參考。德國為因應上述聯邦憲法法院 2008 年 2 月 27 日判決，聯邦與各邦警察法紛紛修法增訂相關配套措施因應，授權警察透過資訊科技進入電腦網際網路資料蒐集，遂成為警察機關有效危害防止的新措施，針對修法後的聯邦刑事局法、巴伐利亞邦警察任務及職權法關於透過資訊科技進入電腦網際網路資料蒐集的規定，聯邦憲法法院又再次分別於 2016 年 4 月 20 日與 6 月 15 日作成判決。以下簡要加以說明：

（一）德國 2008 年 12 月修正的聯邦刑事局法（Bundeskriminalamtgesetz, BKAG）第 20k 條規定，授權聯邦刑事局（Bundeskriminalamt, BKA）為防止國際恐怖主義的危害，防止人民生命、身體或自由的緊急危害，或是國家受到脅迫狀態或人類存在的公共利益的緊急威脅，得不用通知當事人，得實施網際網路蒐集資料，利用科技工具秘密侵入人民的資訊科技系統設備蒐集資訊，資料銷毀等在同條文也都有相關規定，此措施有法官保留原則適用[81]。例如，為了對抗國際恐怖主義對於國家的危害，聯邦刑事局可以祕密侵入關係人的資訊系統並擷取資料，以防止國家受到脅迫[82]。針對修正後聯邦刑事局法關於實施網際網路蒐集資料的規定，德國聯邦憲法法院於 2016 年 4 月 20 日判決指出，資料於符合其蒐集目的的情形下，立法者得允許其除於原先的偵查程序外，只要該蒐

80 陳正根，德國警察資料蒐集法制發展之新趨勢，警察與秩序法研究（三），五南，頁 111，2018 年 8 月。

81 Vgl. BKAG § 20 k.

82 何賴傑，同註 75，頁 238。

集機關將其使用於自身任務的履行，所要保障的法益同一，且係為追訴或預防同類型犯罪，即不會違反目的拘束原則；立法者亦得就目的外利用的情形加以規範，依據比例原則的要求，目的之改變應假定為資料的重新蒐集，其後續利用資料的行為仍須有保障特定法益或追訴犯罪的正當目的；而依據聯邦刑事局法實施網際網路蒐集所得的資料，必須有現存緊急的具體危險情況存在，方得為目的外利用[83]。

（二）巴伐利亞邦 2008 年 8 月修正警察任務及職權法（BayPAG）第 34d 條規定，授權邦警察機關，為防止人民生命、身體或自由的緊急危害，或是國家受到脅迫狀態或人類存在的公共利益的緊急威脅，得不用通知當事人，在別無其他方法可以使用時，得利用科技工具侵入人民的資訊科技設備蒐集資訊；在無可避免的情況下，也可以蒐集第三人資料；資料銷毀等在同條文也都有相關規定；該項措施的發動的對象、範圍、期間等，必須得到法官書面同意[84]。例如有具體訊息指稱恐怖分子將劫持或攻擊民航客機，為防止機上乘客生命、身體緊急危害，在別無他法可使用時，警察機關得利用科技工具侵入人民的資訊科技設備蒐集資訊。對於修正後的巴伐利亞邦警察任務及職權法第 34d 條，關於實施網際網路蒐集資料的規定，所提出的憲法訴願，德國聯邦憲法法院認為，本件憲法訴願所涉及的相關法律已經修改或納入其他相關法律規定，而且提起憲法訴願的四位巴伐利亞邦議會議員並非現在的利害關係人等等原因，本件憲法訴願不具備德國聯邦憲法法院

83　BVerfG, 1 BvR 966/09 vom 20.4.2016, Leitsätze 2, 該判決詳細說明，請參閱李寧修，「自由與安全之衡平：國家預防性干預行政之理論與法制研究」，科技部補助專題研究計畫成果報告期末報告（MOST 104-2410-H-034-007），頁 6-11，2016 年 10 月 30 日。

84　Vgl. BayPAG § 34 d.

法第 93a 條應予以受理要件，本件憲法訴願不合法，於 2016 年 6 月 15 日做出拒絕受理判決[85]。

（三）萊茵伐茲邦警察及秩序機關法（RhpfPOG）第 31c 條規定，授權邦警察機關在危害防止的領域內，為了防止人民生命、身體或自由的緊急危害，或是國家受到脅迫狀態或人類存在的公共利益的緊急威脅，得不用通知當事人，實施網際網路資料蒐集措施，在無可避免的情況下，也可以蒐集第三人資料；資料銷毀等在同條文也都有相關規定[86]。

四、小結

觀察上述 2008 年德國聯邦憲法法院裁判，聯邦憲法法院非常重視法規範明確性原則、程序正當性、以及憲法比例原則的要求，為了補充現有之基本權漏洞，創設電腦基本權，作為一般人格權保障的特殊面向，聯邦憲法法院為了人權保障努力不遺餘力。透過資訊科技進入電腦網路蒐集資料成為警察機關有效履行危害防止任務的新措施，當愈來越多的危害透過科技設備藏身在電腦網路建構的虛擬世界，警察機關為達危害防止無漏洞，必須試圖使用科技設備將這些危害找出，以防止他們對實體世界的法益造成威脅與實害[87]。而德國聯邦與各邦警察法也本著有事實依據顯示，對重要優越利益存有具體危害，例如生命、身體、自由以及為避免危害國家存立或人類生存之公共利益，且有相當高的可能性，該具體危害於可見的未來即將發生，在符合法官保留原則以及對私人核心生活領域有防護措施的精神，迅即修法因應，以符合聯邦憲法法院要求，例如在要件上需有對個人生命、身體、自由或公共利益重大急

85 BVerfG, 1 BvR 2544/08 vom 15.6.2016, Absatz-Nr. 1, 11-12.

86 Vgl. RhpfPOG § 31 c.

87 謝碩駿，警察機關的駭客任務－論線上搜索在警察法領域內實施的法律問題，台北大學法學論叢，第 92 期，頁 6-7，2015 年 3 月。

迫危害，或是國家受到脅迫狀態或人類存在的公共利益的緊急威脅，至於何謂「急迫危害」、「緊急威脅」，都必須從嚴解釋，以防免警察機關恣意。在程序上須出於別無他法，在無可避免的情況下，可以蒐集第三人資料或須經過法官書面同意等相關配套措施；又對於所蒐集資料的目的外利用，德國聯邦憲法法院於 2016 年 4 月 20 日判決，針對修正後聯邦刑事局法關於實施網際網路蒐集資料的規定，指出必須有現存緊急的具體危險情況存在，方得為目的外利用；2017 年德國刑事訴訟法第 100b 條，也立法授權為了偵查該條第 2 項所指刑法或其他法律所規定的特別重大犯罪的嫌疑人或共犯，或是利用其他方式調查事實或確定被告的所在地將更加困難或無望時，得採取此項措施[88]。這些規定都值得我國深思與將來相關立法時借鏡！

肆、我國警察法上透過資訊科技進入電腦網路蒐集資料的法律依據

透過資訊科技進入電腦網際網路蒐集資料強烈干預人民基本權，德國聯邦憲法法院裁判特別提出必須符合法規範明確性原則、程序正當性、以及比例原則的要求。警察機關為達成危害防止無漏洞，當面對新興危害時，在我國現行法制下，可否採取透過資訊科技進入電腦網路蒐集資料措施？以下嘗試分別從國家情報工作法、通訊保障及監察法、警察職權行使法等相關法律規定，加以分析、探討及說明如下：

一、依據國家情報工作法

國家情報工作法第 3 條第 2 項規定：「行政院海岸巡防署、國防部總政治作戰局、國防部憲兵司令部、內政部警政署及法務部調查局等機關，於其主管之有關國家情報事項範圍內，視同情報機關。」因此，內

88　Vgl. StPO § 100 b.

政部警政署於其主管的有關國家情報事項範圍內視同情報機關，負責情報蒐集，第 7 條第 2 項規定：「情報機關蒐集資訊，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式，並應遵守相關法令之規定。」情報機關得採取秘密方式蒐集情報，制度上保障秘密行使職權，不容易監督，該規定所涉及蒐集社會或重大治安事務等資訊，與一般警察保防工作互有重疊，警察機關在此範圍內有權蒐集資料，傳遞給情報機關作為情報上使用，職權行使方法應具有合法性與具體明確的授權。為保障人民權益並兼顧情報工作之特殊性，情報機關運用通（資）訊截收和錄影（音）方式蒐集資訊時，其蒐集之對象、範圍、程序、監督及應遵行的事項，應由主管機關依情報工作的特性訂定專門之法律；第 7 條第 2 項並無授權情報機關透過資訊科技進入電腦秘密蒐集資料，因此無法作為警察透過網際網路進入電腦蒐集資料的依據；而第 7 條第 3 項規定：「情報機關執行通訊監察蒐集資訊時，蒐集之對象於境內設有戶籍者，其範圍、程序、監督及應遵行事項，應以專法定之；專法未公布施行前，應遵守通訊保障及監察法等相關法令之規定。」則是關於情報機關執行通訊監察蒐集資訊對象、範圍、程序、監督及應遵行事的規定，也無授權警察透過資訊科技進入電腦秘密蒐集資料。

二、依據通訊保障及監察法

通訊保障及監察法第 13 條第 1 項規定通訊監察的方式，係指：「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」申言之，倘司法警察於執行蒐證工作時，對於人民具有隱私秘密合理期待的通訊，實施截收、監聽、錄音、攝影等相類行為，必須

符合第 5 條、第 6 條[89]所規定的要件，取得法官所核發的通訊監察書後始得執行，否則應負損害賠償等責任[90]，違反第 5 條、第 6 條規定進行監聽行為情節重大者，所取得的內容或所衍生的證據，於司法偵查、審判或其他程序中，均不得採為證據[91]。通訊保障及監察法所規範的通訊，屬憲法第 12 條秘密通訊自由保障的範圍[92]。通訊保障及監察法第 13 條規定的通訊保障監察方法除監聽等手段外，還有「其他類似之必要方法」的概括條款規定，如果以通訊保障及監察法作為透過資訊科技進入電腦網際網路蒐集資料的依據，則通訊監察的基本原則[93]，例如重罪原則、最後手段性原則、令狀原則、一定期限原則、事後通知原則、相關性原則等，都應該遵守。然而，除前述學者認為通訊結束儲存在電腦中的資料已經不再是通訊的見解[94]外，實務上最高法院歷年來審理涉及通訊保障及監察法的案件，也都是以偵查機關取得「正在進行中」的通訊內容為主[95]，認為通訊保障及監察法所規範的通訊監察，重在過程，應限於「現時或未來發生」的通訊內容，不包含「過去已結束」的通訊內容[96]。

89　通訊保障及監察法第 5 條係得發通訊監察書的規定，例如重罪原則、最後手段原則、令狀原則、證據排除原則等；第 6 條則為緊急通訊監察的規定。

90　通訊保障及監察法第 19 條第 1 項規定：「違反本法或其他法律之規定監察他人通訊或洩漏、提供，使用監察訊所得之資料者，負損害賠償責任。」第 2 項規定：「被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。」

91　為落實人權保障，2007 年 7 月 11 日修正通訊保障及監察法第 5 條第 5 項規定，明定違反本條之相關規定執行監聽所取得之證據應予排除。至於違法之情節是否重大，則應由法官據個案予以審核。

92　參閱司法院釋字第 631 號解釋。

93　參閱吳秋宏，司法院釋字第 631 號解釋與監聽法制評析（上），司法週刊第 1385 期，頁 2-3，2008 年 4 月 17 日；吳秋宏，司法院釋字第 631 號解釋與監聽法制評析（下），司法週刊，第 1386 期，頁 2-3，2008 年 4 月 24 日。

94　李育典，同註 27，頁 258。

95　例如最高法院 97 年度台上字第 2979 號、第 2743 號刑事判決。

96　最高法院 106 年度台非字第 259 號刑事判決。

尤其對於通訊終結，儲存在電腦系統的資料進行網際網路資料蒐集，與通訊保障及監察法是對於正在進行中的通訊監察的本質應有差異[97]，因此通訊保障及監察法第 13 條「其他類似之必要方法」的概括規定，也不能作為透過資訊科技進入電腦蒐集資料的方法，通訊保障及監察法無法作為警察透過資訊科技進入電腦蒐集資料的依據[98]。至於調取「通信紀錄」與「通訊使用者資料」，依第 11 條之 1 第 1 項及第 2 項規定：「檢察官偵查最重本刑三年以上有期徒刑之罪，有事實足認通信紀錄及通信使用者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。聲請書之應記載事項，準用前條第一項之規定。」「司法警察官因調查犯罪嫌疑人犯罪情形及蒐集證據，認有調取通信紀錄之必要時，得依前項規定，報請檢察官許可後，向該管法院聲請核發調取票。」要調取通信紀錄及通信使用資料，程序上必須向該管法院聲請核發調取票，該規定也無法作為警察機關透過資訊科技進入電腦網際網路蒐集資料的依據。

三、依據警察職權行使法第 11 條

從警察職權行使法第 6 條以下列舉的警察類型化措施的規定來看，比較可能和網際網路資料蒐集措施相關的，應該是該法第 11 條第 1 項[99]「以目視或科技工具蒐集資料」長期監視的規定。依據第 11 條第 1 項的規定，警察為了防止犯罪發生，在必要時得對該項所列舉的兩款

97 相同見解，何賴傑，同註 75，頁 233。

98 相同見解，謝碩駿，同註 87，頁 28-29。

99 警察職權行使法第 11 條第 1 項規定：「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動：一、有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。二、有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。」

對象，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動。由於第 11 條第 1 項的觀察及動態掌握等資料蒐集活動，目的在於「事前防止犯罪發生」，而非「事後蒐集犯罪證據」，因此確實屬於警察危害防止的範疇。第 11 條長期監視發動要件包括：（一）有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。（二）有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。（三）一定期間之觀察。（四）警察局長書面同意。監視範圍則有下列限制：1. 無隱私或秘密合理期待之行為或生活情形。2. 監視方式包含「目視」與利用電子設備的錄音、錄影等「科技方式」進行觀察及動態掌握等資料蒐集活動[100]。

然而，「以科技工具進行資料蒐集活動」，科技工具是否包括透過資訊科技進入電腦網際網路秘密蒐集資料，恐怕也有爭議[101]。縱然認為可以包含「透過資訊科技進入電腦網際網路資料蒐集」措施，但是，其侷限於蒐集「對其無隱私或秘密合理期待之行為或生活情形」範圍，在這個前提下，「透過資訊科技進入電腦網際網路」隱密蒐集資料的措施，已經侵害隱私，顯然應該被排除在警察第 11 條第 1 項的授權範圍外。尤其透過網際網路要蒐集的是儲存在人民電腦硬碟內的資訊，應該只限於「有權使用該儲存設備者」才得以瀏覽[102]，如果要將這樣的資料劃歸

100 蔡震榮，警察職權行使法概論，頁 164-167，五南，2016 年 3 版。

101 警察可不可以依據警察職權行使法第 11 條的規定，做為利用衛星定位系統跟監，追蹤、掌握特定人的行蹤？有採肯定見解者，認為科技的發展，在法律運用上，本即協助執法者解決問題。汽車追蹤器只要無法監聽車內人員談話內容，僅可查詢車子方位和所在位置，並對有特定犯罪之虞者方得採取本項措施，侵害人民權益輕微，應屬允許，請參閱李翔甫，警察法規，頁 211，新學林，2009 年。也有採否定的看法，認為警察職權行使法第 11 條之立法係以警察犯罪預防為目的，並非為刑事偵查而設。若允許警察得於犯罪發生之先前領域，使用衛星定位系統，公益與私益間，難免有失均衡，請參閱蔡庭榕等，警察職權行使法逐條釋論，頁 284-285，五南，2005 年。

102 相同見解，謝碩駿，同註 87，頁 30。另我國在 2003 年 6 月 25 日新增刑法第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併

到「無隱私或秘密合理期待」的領域內，恐怕無法自圓其說。透過資訊科技進入電腦網際網路蒐集資料會干預人民資訊隱私，既然第 11 條第 1 項要蒐集的是「無隱私或秘密合理期待」的資訊，那麼就不能作為警察法領域內實施網際網路秘密蒐集資料的法律授權依據。再從比較法上，警察職權行使法第 11 條立法主要參考的德國聯邦與各邦統一警察法標準草案第 8 條有關長期監視、藉由科技工具秘密執勤攝影錄音的規定，以及德國聯邦國境保護法第 28 條有關長期監視、藉由科技工具秘密執勤攝影、錄音蒐集資料的規定[103]，並沒有授權警察機關透過資訊科技進入電腦網際網路蒐集資料，因此，也可以推知警察職權行使法第 11 條不得做為警察機關透過資訊科技進入電腦蒐集資料的依據。

四、依據警察職權行使法第 28 條

上述國家情報工作法、通訊保障及監察法與警察職權行使法列舉的警察類型化措施的規定，都無法作為警察透過資訊科技進入電腦網際網路蒐集資料的依據，最後可以思考是否可以援引警察職權行使法第 28 條第 1 項概括條款作為依據？概括條款授權警察蒐集資料，藉以執行警察任務防止具體或抽象危害[104]，具有補結構規範遺漏功能[105]，可以發揮規範完整功能的優點；但是也會產生對於法安定性、權力分力的挑戰、以及對於個別基本權利理論體系及保障範圍輕忽的缺點[106]。

科十萬元以下罰金。」其立法理由指出：「鑒於對無故入侵他人電腦之行為採刑事處罰已是世界立法之趨勢，且電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性，此種行為之危害性應已達科以刑事責任之程度，為保護電腦系統之安全性，爰增訂本條。」

103 蔡震榮，同註 100，頁 162-164。

104 Vgl. Bodo Pieroth/Bernhard Schlink/Michael Kniesel, Polizei - und Ordnungsrecht mit Versammiungsrecht, 9. Aufl. 2016, § 13, Rn. 14 ff.

105 Vgl. Bodo Pieroth/Bernhard Schlink/Michael Kniesel, a.a.O., § 7, Rn. 11 ff.

106 李震山，同註 30，頁 212-213。

要以有限的條文規範無窮的社會現象，並冀求能與時俱進的實踐其規範功能，似乎不太可能。立法者除了在立法當時盡可能就規範內容依列舉原則詳為規定外，必須再輔以概括性規定，才能承接立法者所意識到某些暫時無法明確規定的漏洞，並避免修法頻繁危及法的安定性。然法律概括條款仍應受法治國「法律明確性」憲法原則的制約，李震山大法官在司法院釋字第 702 號解釋部分不同意見書即指出[107]：「概括條款，本就是以公權力具有專業追求公益權責的預設所為之立法制度設計，自始就偏向賦予公權力運作的彈性空間，因此，就其所潛藏的行政與司法權運作恣意的可能性，人民就不易節制。概括條款形成與運作的相關過程包括：(一)、概括條款中抽象概念的選定，例如公共安全、社會秩序、公序良俗、公益、危害等，皆屬立法者優先享有的『話語權』。理論上，其是經主權者所同意而運用的措詞，亦相當程度展現主流價值觀；實際上，由於複雜不確定的社會現象，執法機關往往透過法律提案權取得先入為主的優勢，此時概括條款中抽象用語的選取，對法律執行已具有定調功能。(二)、對該等抽象概念之詮釋及涵攝，執法機關則擁有先位的判斷權限。若其判斷涉及高度屬人性、透過社會公正人士或專家所為專業判斷，或由獨立行政職權之委員會所為之決定，基於『判斷餘地』(Beurteilungsspielraum）理論尚會受到司法審查的尊重，從而降低審查密度。(三)、當個案涉及基本權利保護必要，而人民就公權力有關不確定法律概念之辭義鑽研或章句析解等『文字釋義操作』，產生恣意或濫權之質疑時，往往會尋求法院救濟，期以節制執法的恣意或不公。但受前述立法制度設計之框限，以及向來尊重行政專業的理由下，法院施展空間並不大，人民以其先天不利的講述能力對抗公權力，經常是徒勞無功，最後只餘求助於釋憲者一途。由上可知，司法院大法官以『法律明確性原則』作為概括條款合憲性的主要量尺，就權力分立相互

107 司法院釋字第 702 號解釋李震山大法官部分不同意見書。

制衡與人權保障就有非比尋常的意義，亦是展現違憲審查功力之所在」。

警察職權行使法第 28 條第 1 項即是警察職權的概括規定[108]，第 28 條第 1 項明文規定：「警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。」從「為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況」這個要件來看，該項規定適用在警察法危害防止領域內。而其立法理由也在因應社會政經文化等的快速變遷，以免如果出現新興危害，因為法律一時難以因應而不予處理，無從維護公共安全與秩序，以及保障個人生命、身體、自由、名譽與財產，賦予警察出面處理的相應職權，因此參考德國聯邦與各邦統一警察法標準草案第 8 條第 1 項規定予以明文規定。該規定的適用要件包含[109]：（1）制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產。「現行危害」指現行存在的危害；「公共安全」是指個人生命、身體、自由、名譽或財產、法秩序以及國家設施等不得受到任意侵害；「公共秩序」是指個人於整體公開行為，應遵守所有不成文的規範，以做為共同生活必要的條件。「公共安全」保護實定法所承認的法益，確保法秩序不受侵害[110]；「公共秩序」則創設法規範以外的保護法益，兩者互為構成要件[111]。（2）行為或事實狀況所引發。危害的發生，可能是人的行為所肇致，亦有可能是物的狀況所引起。（3）採取必要的措施。所謂「必要」是一種比例原則的考量，若警察的目的以其他方式不能或相當困難達到時，警察採取的措施即屬必要，若危害尚屬輕微，警察的介入即無必要。該條規定賦與警察「得採取其他必要之措施」彰顯「警察法上概括條款」的補遺漏

108 李震山，同註 30，頁 213；蔡震榮，同註 100，頁 241。

109 蔡震榮，同前註，頁 244-245。

110 Christoph Gusy, Polizei - und Ordnungsrecht, 10. Aufl., 2017, § 3, Rn. 79 ff.

111 Christoph Gusy, Polizeirecht, 5. Aufl., 2003, § 3, Rn. 95.

承接功能，授權警察機關可以採取其他必要措施，而「透過資訊科技進入電腦蒐集資料」是否在「其他必要措施」的範圍內，可以作為警察機關實施進入電腦蒐集資料的法律授權依據，值得進一步加以探究。

由於透過資訊科技進入電腦網際網路蒐集資料措施對人民基本權干預程度非常強烈，而警察職權行使法第 28 條第 1 項規定使用許多不確定法律概念，因此，有認為以警察法上的概括條款作為警察機關實施網際網路蒐集資料的授權依據，恐怕會招來質疑。例如 Wolf-Ruediger Schenke 教授即認為，比類型化措施干預程度更強烈的措施，不能以警察法上的概括條款當作法律依據即，理由如下：

（一）警察危害防止措施如果會對基本權造成強烈干預，該措施的構成要件應該由立法者詳加規定，警察機關不得將警察法上的概括條款當做此種措施的授權基礎[112]。

（二）立法者透過類型化措施的規定，明文授權警察機關可以採取某一項危害防止措施，就等於把「與該項措施相近的、或是較該措施干預程度更為強烈的措施」默示地排除在授權範圍之外，所以，比類型化措施干預程度更強烈的措施，不能以警察法上的概括條款當作法律依據[113]。

國內學者謝碩駿則基於以下理由，認為警察法上概括條款可以作為警察透過資訊科技進入電腦網際網路蒐集資料的法律依據[114]：

（一）上述 Wolf-Ruediger Schenke 教授的說法並不否認警察法上概括條款的適用範圍可以涵蓋「對基本權干預程度強烈的危害防止措施」，立法者是不是真的像 Wolf-Ruediger Schenke 教授所說，透過類型化措施規定，已經預設了「警察危害防止措施對基本權干

112 Wolf-Ruediger Schenke, Polizei - und Ordnungsrecht, 8. Aufl., 2013, Rn. 50

113 Wolf-Ruediger Schenke, a.a.O., Rn. 50.

114 謝碩駿，同註 87，頁 32-34。

預程度」的上限的看法，仍有商榷餘地[115]。

（二）立法者明文詳細列舉類型化措施，乃是因為這些職權是警察機關在面對傳統危害時經常行使的「類型化措施」，將這些措施的行使要件予以類型化，這和「該措施對於基本權干預程度的輕重」根本無關[116]。「類型化措施規定」與「警察法上概括條款」這兩種授權規定的殊異之處在於，「類型化措施規定」涉及的是「典型的警察危害防止措施」，而「警察法上概括條款」則適用於「非典型的警察危害防止措施」。

（三）立法者基於「讓警察機關得採取非類型化措施，以因應新興危害類型」的考量，並未要求「只有基本權干預程度輕微的措施，始能適用警察法上的概括條款」。如果硬要將警察職權行使法第 28 條第 1 項得適用範圍限縮在「對於基本權干預輕微的措施」，恐怕警察機關在面對新興危害時，於絕大多數情況下很難適用此一規定採取「有效的基本權保護措施」，從國家保護義務的角度來看，反而導致警察職權行使法第 28 條第 1 項的規定，因違反「禁止保護不足原則」而有違憲之虞。

（四）警察機關基於違害防止的目的，要侵入人民的電腦系統內實施資料蒐集，在找不到其他法律授權條款的情形下，確實可以將警察法上的概括條款當作法律授權依據。

（五）「非類型化的警察違害防止措施」如果已經被警察機關頻繁的實施，而在事實上成為「類型化措施」，則立法者有義務將這樣的措施明文規定在「類型化措施」條款中。一旦透過資訊科技進入電腦網際網路蒐集資料在事實上已經成了「類型化的危害防止措施」，那麼警察機關只能在立法者對尚未完成立法之前的「過渡

115 同前註，頁 32-34。

116 Vgl. Christoph Gusy, a.a.O. (Fn. 110), § 4, Rn. 184.

期間」，以警察法上概括條款作為透過資訊科技進入電腦蒐集資料的法律依據。

警察職權措施性質屬干預性者，首先應適用特別授權的類型化措施，無類型化措施的規定可適用時，才適用概括性職權條款，以避免概括條款被濫用，並保障人民權益。概括條款主要目的在保護公共安全或公共秩序，亦即保護國家及其機關的安全與存續、個人生命身體自由名譽及財產安全、所有法規的維護以及所有不成文的個人公共行為規範。欲以警察法的概括規定做為實施干預措施的依據，應特別注意以下幾點[117]：

（一）以特別授權方式為依據的列舉式立法應力求完備，藉以將概括條款的適用，限制於某特定範圍。

（二）執法人員對於概括條款的補充性及承接性功能，要有充分認識，並有行政中立與自我約束的能力，避免以行政效率或便宜為理由，濫用概括條款。

（三）人民救濟管道要暢通，使司法得以充分審查行政機關適用不確定法律概念的情形，除收審查監督的效果外，也可以將不確定法律概念具體化。

（四）若警察的目的以其他方式不能或相當困難達到時，則此時警察採取的措施即屬必要，若危害尚屬輕微，警察的介入即無必要，必要即屬比例原則的考量[118]。

本文基於以下幾點理由認為，警察職權行使法第 28 條第 1 項概括規定，尚不得作為透過資訊科技進入電腦秘密蒐集資料的授權依據：

（一）警察職權行使法第 28 條第 1 項的立法理由，係為因應社會政經文化等的快速變遷，以免如果出現新興危害，因為法律一時難以

117 李震山，同註 30，頁 225-226。

118 Rudolf Samper/Heinz Honnacker, Polizeiaufgabengesetz, 15. Aufl., 1992, § 11, Rn. 4; 蔡震榮，同註 100，頁 277。

因應而不予處理，無從維護公共安全與秩序，或個人生命、身體、自由、名譽或財產之行為或事實狀況；而且警察職權行使法第 2 條的警察職權規定以及第 6 條以下也盡力完備以特別授權方式為依據的列舉式立法。但是警察透過資訊科技進入電腦網路祕密資料蒐集的措施，比警察職權行使法已經明文類型化的設置監視器蒐集資料、長期跟監監視、遴選第三人蒐集資料、任意盤查查證身分及交通工具、治安顧慮人口查訪等措施，對於基本權的干預程度更為強烈，在要件及程序上應該要有個別明確的法律授權。

（二）人民並無從知悉警察透過網際網路祕密資料蒐集，以致人民救濟管道無法暢通，無法收到審查監督的效果。

（三）德國聯邦與各邦為因應上述 2008 年德國聯邦憲法法院判決，聯邦與各邦警察法均紛紛修法，明定警察透過資訊科技進入電腦網路祕密蒐集資料的相關要件及程序與相關配套措施；而且我國在 2003 年制定警察職權行使法時，主要參考的德國聯邦與各邦警察法也沒有相關的授權規定，足見我國如果欲以警察職權行使法第 28 條第 1 項的規定，作為警察透過資訊科技進入電腦網路蒐集資料措施的依據，在比較法上，也值得商榷。

（四）尤其前述德國聯邦憲法法院 2008 年 2 月 27 日判決，特別提到北萊茵西伐利亞邦憲法保護法因欠缺配套措施，不符法規範明確性原則、程序正當性、以及比例原則的要求。因此，要以警察職權行使法第 28 條第 1 項概括條款的規定，作為警察法上警察透過資訊科技進入電腦秘密蒐集資料的法律授權依據，難認與法規範明確性原則、程序正當性原則、比例原則等法治國原則相符合。

（五）法院見解：警察具有危害防止與犯行追緝的任務與職權[119]，警察

119 李震山，同註 30，頁 325。

依據警察職權行使法等警察法來防止危害發生，甚至在「危害尚未發生」時，得立法採取限制、禁止的干預性措施，一旦有犯罪嫌疑或犯罪發生，就應該依據刑事訴訟法等相關刑事法調查追訴犯罪，刑事訴訟法採法定原則，發動的門檻比警察法嚴格[120]；警察為達成危害防止任務，甚至在「危害尚未發生」時，即得立法授權警察採取限制、禁止的干預性措施，然而參照德國聯邦憲法法院 2008 年 2 月 27 日判決，為防止具體危害，立法授權運用資訊科技進入電腦蒐集資料，在實體要件以及程序上，仍然必須符合法規範明確性原則、程序正當性、以及比例原則的要求，才能彰顯警察在保障人權的前提下，有效達成危害防止職責。雖然我國法院實務上還沒有關於警察為防止危害，可否透過資訊科技祕密進入電腦蒐集資料的案例；但是法院曾經對於司法警察在沒有法律明確授權下，不得以概括條款作為運用衛星定位器 GPS 蒐集位置資訊依據的判決。該判決有深入的論證、分析與說明，頗值得在思考警察為了防止危害，得否以警察法上概括條款作為運用資訊科技進入電腦蒐集資料法律依據的問題時參考。判決內容簡要摘錄如下：

高雄地方法院 105 年度易字第 110 號判決認為[121]：「…新興隱密及科技之偵查方法，……如本案之裝設 GPS 衛星定位器蒐證等手段，並未單獨個別立法規範，以偵查手段及快速變遷且科技日新月異，侵害人民基本權程度不亞於傳統強制處分，容許以……概括條款，而無視於受干預基本權之種類、程度，授權偵查（輔助）機關以上開刑事訴訟法第 228 條第 1 項、第 230 條第 2 項、第 231 條第 2 項規定全面性幾近空白授權之方式允許在偵

120 陳英淙，論警察危害防止與刑事追訴的分與合，政大法學評論，第 151 期，頁 119，2017 年 12 月。

121 請參閱臺灣高雄地方法院 105 年度易字第 110 號刑事判決。

查（輔助）機關認有犯罪嫌疑之際即可干得預人民受憲法保障之基本權，難認符合憲法上法律明確原則以及增加偵查（輔助）機關濫權偵查之危險且欠缺合法性控制、監督之機制……亦會架空法律保留原則。」

高雄高分院肯定高雄地院上述見解，認為[122]：「……以裝設 GPS 衛星定位器於犯罪嫌疑人使用車輛之行為，係以秘密方式針對特定嫌疑人進行調查、蒐集犯罪事證或相關資訊之國家公權力行為，蒐集車輛使用資訊過程中搭配使用輔助科技設備，干預人民基本權之程度將更為嚴重，基於法治國原則，此等行為首應有法律明文，並應遵守其他相關法律原則，蓋蒐集犯罪證據固然重要，惟更重要者實為發動此等行為之程序及要件，或不合目的性、或以不正手段非法取得，人民基本權之保障將蕩然無存。」

最高法院同樣地也認為[123]：「……依強制處分法定原則，強制偵查必須現行法律有明文規定者，始得為之，倘若法無明文……偵查機關非法安裝 GPS 追蹤器於他人車上，已違反他人意思，而屬於藉由公權力侵害私領域之偵查，且因必然持續而全面地掌握車輛使用人之行蹤，明顯已侵害憲法所保障之隱私權，自該當於『強制偵查』，故而倘無法律依據，自屬違法而不被允許。又刑事訴訟法第 228 條第 1 項前段、第 230 條第 2 項、第 231 條第 2 項及海岸巡防法第 10 條第 1 項、第 2 項、第 3 項之規定，……自不得作為裝設 GPS 追蹤器偵查手段之法源依據。」

五、小結

從以上論述得知，我國國家情報工作法、通訊保障及監察法、警察

122 請參閱臺灣高等法院高雄分院 105 年度上易字第 604 號刑事判決。

123 請參閱最高法院 106 年度台上字第 3788 號刑事判決。

職權行使法等法律都無明確授權，無法作為警察為防止危害透過資訊科技進入電腦路蒐集資料的依據；在法院實務上，不論是高雄地方法院、高雄高分院、最高法院對於偵查機關在沒有法律授權下安裝 GPS 追蹤器於他人車上判決指出，新興隱密及科技的偵查方法，侵害人民基本權程度不亞於傳統強制處分，容許以概括條款，而無視於受干預基本權的種類、程度，授權偵查（輔助）機關以全面性幾近空白授權的方式，允許在偵查（輔助）機關認有犯罪嫌疑之際即可干得預人民受憲法保障的基本權，難認符合憲法上法律明確原則以及增加偵查（輔助）機關濫權偵查的危險且欠缺合法性控制、監督之機制，會架空法律保留原則；基於法治國原則，此等行為應有法律明文，並應遵守其他相關法律原則，發動此等行為的程序及要件，或不合目的性、或以不正手段非法取得，人民基本權之保障將蕩然無存；刑事訴訟法第 228 條第 1 項前段、第 230 條第 2 項、第 231 條第 2 項規定的概括授權，不得作為裝設 GPS 追蹤器偵查手段的法源依據。在思考警察為了防止危害，得否以警察法上概括條款作為運用資訊科技進入電腦蒐集資料的法律依據時，頗具參考價值；縱然在警察危害防止領域，採取限制、禁止的干預措施的門檻較犯罪偵查領域寬鬆，但採取科技隱密方式的特殊調查方法，仍需有特別法律授權[124]，也有學者指出，如果認為警察職權行使法第 28 條所稱的「其他必要措施」包含任何法律所未規定的職權在內，則不僅警察職權行使法不用再細行規範其他個別警察職權行使的要件、程序及救濟條款，因為僅有此一概括條款，就可以完全取代警察職權行使法第 6 條至第 27 條的內容，則「依法行政原則」或「法律保留原則」即形同崩潰[125]。為解決此問題，應該參考上述德國相關法律規定，盡速在我國警察職權行使法中訂定相關規定，作為警察為防止危害透過資訊科技進入電腦路

124 李震山，同註 11，頁 470。

125 林明鏘，警察職權行使法基本問題之研究，台灣本土法學雜誌，第 56 期，頁 126-127，2004 年 3 月。

蒐集資料的依據，才能達成法治國依法行政原則並讓危害防止無漏洞。

伍、結論與建議

警察依據法律明定的類型化措施，遂行保護公共秩序、公共安全以及人民生命、身體、自由、財產、財產以及防止危害任務。但面對社會變遷產生新興危害，法律往往無法跟上腳步，明定職權措施，因此不得不允許概括條款的存在。警察透過進入電腦網路網際措施秘密蒐集資料，確實有助於警察遂行危害防止任務，但該措施對人民基本權干預程度非常強烈，然而檢視上述我國警察法制，都無法作為授權依據。面臨社會變遷或科技發展時，法律通常有三種因應之可能性：一為不作為，因此可能產生法律的漏洞；二為積極立法，可能會形成法律肥大與規範不穩定的危險；三為以現行規範適用於新的事件，但是可能會破壞明確性要求，特別是涉及基本權干預時，法律保留原則具有重大意義[126]。資訊社會資訊科技日新月異，面對著科學新穎進步特性，法律如何跟上與如何規範科學恐是重點，以警察透過資訊科技進入電腦網際網路蒐集資料而言，現行法律規範不論在要件或程序上都不足以因應科技進步的要求，此種透過資訊科技秘密進入電腦網際網路秘密蒐集資料措施，對人民基本權利的侵害與法治國家人權保障之間如何取得平衡，應該將相關要件與程序，在規範我國警察職權行使的法制中明文加以規定，以符合法律保留等相關法治國原則的要求，將是無法迴避也是必須盡速面對的問題！

科技工具就如同公權力的延伸，科技工具越來越細緻化，越來越進步，使公權力效率更提升，但同時對人權干預的風險也隨著更加提升，此時人民權利的保障也越來越重要，公權力透過科技追求到多方面的滿

126 Vgl. Hans Kudlich, Mitteilung der Bewegungsdaten eines Mobiltelefons als Überwachung der Telekommunikation-BGH NJW 2001, 1587, JuS 2001, S. 1165.

足，但是若忽略其風險及法令規章的整備，最後可能會悔不當初[127]，因此，如何規範警察透過網際網路蒐集以及利用資料的措施，已經成為不可阻擋的趨勢[128]，本文建議應該可以參照上述德國聯邦刑事局法與巴伐利亞邦警察任務及職權法、萊茵伐茲邦警察及秩序機關法規定，以及德國聯邦憲法法院相關判決意旨，只要有事實依據顯示，對重要優越利益存有具體危害生命、身體、自由以及為避免危害國家存立或人類生存之公共利益，且有相當高的可能性，該具體危害於可見的未來即將發生，將相關要件與程序，在我國警察職權行使法中明文加以規定，授權警察機關，為防止人民生命、身體或自由的緊急危害，或是國家受到脅迫狀態或人類存在的公共利益的緊急威脅，得不用通知當事人，在別無其他方法可以使用時，得利用科技工具侵入人民的資訊科技設備蒐集資訊；在無可避免的情況下，也可以蒐集第三人資料；該項措施的發動的對象、範圍、期間等，必須得到法官書面同意，作為規範警察為了防止危害透過網際網路蒐集資料措施的依據；資料於符合其蒐集目的的情形下，只要該蒐集機關將其使用於自身任務的履行，所要保障的法益同一，即不會違反目的拘束原則；亦得就目的外利用的情形加以規範，依據比例原則的要求，目的之改變應假定為資料的重新蒐集，其後續利用資料的行為仍須有保障特定法益或追訴犯罪的正當目的。又 2017 年德國刑事訴訟法第 100b 條，立法授權為了偵查該條第 2 項所指刑法或其他法律所規定的特別重大犯罪的嫌疑人或共犯，或是利用其他方式調查事實或確定被告的所在地將更加困難或無望時，得採取此項措施。德國刑事訴訟法第 100b 條在重罪原則、最後手段原則以及比例原則精神下，得以採取此措施，也值得我國在偵查犯罪的相關立法時參考。

國家為維護公共利益與保障個人自由之間，常會發生在法律授權

127 李震山，同註 39，頁 260。

128 Christopher Slobogin, *Public Privacy: Camera Surveillance Of Public Places And The Right To Anonymity*, 72 MISS. L. J. 213, 233 (2002).

上，自由與安全之間應如何的適度決定選擇的問題。經由冷靜的檢驗、思考、辯證新科技的特質以及其對於基本人權的影響，唯有經由如此的對話，方能建立一個可以確保合理平衡科技與人權保障的法律架構[129]，面對永無止境的新型態資訊科技問題，法律也將面對一些新挑戰，例如法律應如何面對新興科技所產生的基本權利侵害？究竟應該繼續以傳統方式或提出另一種思考方式加以審查？這是法律的宿命無可迴避，上述德國聯邦憲法法院提出的法規範明確性原則、程序正當性原則、比例原則等法治國原則的要求，以及所蒐集資料的目的外利用應遵守的原則，都值得我國在面對新興科技蒐集資料立法時參考。

129 William A. Herbert, *No Direction Home: Will The Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?,* 2:2 I/S: A JOURNAL OF LAW POLICY 409, 473 (2006).

參考文獻

中文

一、專書

吳　庚，憲法的解釋與適用，三民，2003 年 4 月。

李育典，憲法，元照，2013 年 2 月 6 版。

李惠宗，憲法要義，元照，2009 年 9 月 5 版。

李惠宗，憲法要義，元照，2015 年 9 月 7 版。

李翔甫，警察法規，新學林，2009 年 9 月。

李震山，資訊權－兼論監視器設置之法律問題，多元寬容與人權保障－以憲法未列舉權之保障為中心，元照，2007 年 9 月 2 版。

李震山，公權力運用科技定位措施與基本權利保障，人性尊嚴與人權保障，元照，2009 年 2 月 3 版。

李震山，論資訊自決權，載人性尊嚴與人權保障，元照，2011 年 10 月 4 版。

李震山，人性尊嚴之憲法意義，人性尊嚴與人權保障，元照，2011 年 10 月 4 版。

李震山，警察行政法論，元照，2016 年 10 月修訂 3 版。

李震山，行政法導論，三民，2019 年 2 月修訂 11 版。

林明鏘，由防止危害到危險預防，警察法學研究，新學林，2011 年 7 月。

陳正根，德國警察資料蒐集法制發展之新趨勢，警察與秩序法研究（三），五南，2018 年 8 月。

陳英鈐，通訊監察保障之建置及運用－論德國聯邦憲法法院線上搜索與資訊隱私權保護判決對我國基本權體系應有的回應，21 世紀資訊法治之新趨勢學術研討會論文集，台灣行政法學會，2010 年 1 月 30 日。

陳英鈐，通訊監察保障之建制及運用－論德國聯邦憲法法院線上搜索判決對我國資訊隱私權的啟發，資訊法制、土地規劃與損失補償之新趨勢，元照，2010 年 9 月。

陳新民，中華民國憲法釋論，三民，2001 年 1 月 4 版。

陳新民，憲法學釋論，三民，2015 年 5 月修訂 8 版。

黃昭元，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，民主人權正義－蘇俊雄教授七秩華誕祝壽論文集，元照，2005 年 9 月。

黃清德，科技定位追蹤監視與基本人權保障，元照，2011 年 11 月。

蔡庭榕等，警察職權行使法逐條釋論，五南，2005 年 2 月。

蔡震榮，警察職權行使法概論，五南，2016 年 5 月 3 版。

蕭文生，關於「一九八三年人口普查法」之判決，西德聯邦憲法法院裁判選輯（一），司法週刊雜誌社，2000 年。

二、期刊論文

何賴傑，論德國刑事程序「線上搜索」與涉及電子郵件之強制處分，月旦法學雜誌，第 208 期，2012 年 9 月。

吳秋宏，司法院釋字第 631 號解釋與監聽法制評析（上），司法週刊，第 1385 期，2008 年 4 月 17 日。

吳秋宏，司法院釋字第 631 號解釋與監聽法制評析（下），司法週刊，第 1386 期，2008 年 4 月 24 日。

李建良，「戶籍法第八條捺指紋規定」釋憲案鑑定意見書，台灣本土法學雜誌，第 73 期，2006 年 8 月。

李建良，自由、平等、尊嚴（下）－人的尊嚴作為憲法價值的思想根源與基本課題，月旦法學雜誌，第 154 期，2008 年 3 月。

李震山，個人資料保護與監視錄影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，第 4 期，2005 年 12 月。

林明鏘，警察職權行使法基本問題之研究，台灣本土法學雜誌，第 56 期，2004 年 3 月。

陳英淙，論警察危害防止與刑事追訴的分與合，政大法學評論，第 151 期，2017 年 12 月。

蔡宗珍，營業自由之保障及其限制，台灣大學法學論叢，第 35 卷，第 3 期，2006 年 5 月。

蕭淑芬，論基本權核心概念之規範－一個比較法學的觀察，東海大學法學研究，第 19 期，2003 年 12 月。

謝碩駿，警察機關的駭客任務－論線上搜索在警察法領域內實施的法律問題，台北大學法學論叢，第 92 期，2015 年 3 月。

英文

Herbert, William A., *No Direction Home: Will The Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2:2 I/S: A JOURNAL OF LAW POLICY (2006).

Kulish, Nicholas, *Germans Condemn Police Use of Spyware*, N.Y. Times, Oct. 14. 2011.

Slobogin, Christopher, *Public Privacy: Camera Surveillance Of Public Places And The Right To Anonymity*, 72 MISS. L. J. (2002).

Taslitz, Andrew E., *The Fourth Amendment In The Twenty-First Century: Technology, Privacy, And Human Emotions*, 65:2 LAW AND CONTEMPORARY PROBLEM. (2002).

德文

Glaeser, Walter Schmitt, Schutz der Privatsphäer, in:Josef Isensee und Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepulik Deutschland, Bd. 6.2001.

Gusy, Christoph, Polizeirecht, 5. Aufl., 2003.

Gusy, Christoph, Polizei-und Ordnungsrecht, 10. Aufl., 2017.

Hoffmann, Manfred, Die Online-Durchsuchung-staatliches “Hacken” oder zulässige Ermittelungsmaßmahne?, NStZ 2005.

Hozner, Stefan, Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, 2009.

Kahl, Wolfgang, Die Schutzerganzungsfunction von Art.2 Abs.1, Grundgesetz, 2000.

Klein, Friedrich/Hermann von Mangoldt, Das Bonner Grundgesetz: Kommentar, Bd. 1, 4. Aufl., 1999.

Kudlich, Hans, Mitteilung der Bewegungsdaten eines Mobiltelefons als Überwachung der Telekommunikation-BGH NJW 2001, 1587, JuS 2001.

Kunig, Philip/von Münch, Ingo/Bryde, Brun-Otto, Grundgesetz-Kommentar, 5. Aufl., 2000.

Lumann, Niklaus, Grundrecht als Institution, 1965.

Manssen, Gerrit, Staatsrecht II, 2.Aufl., 2002.

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael, Polizei-und Ordnungsrecht mit Versammiungsrecht, 9. Aufl.

Samper, Rudolf /Honnacker, Heinz, Polizeiaufgabengesetz, 15. Aufl., 1992.

Schenke, Wolf-Ruediger, Polizei- und Ordnungsrecht, 8. Aufl., 2013.

Wächter, Michael/Müller, Dipl.-Kfm. Gerhard F., Eine systematische Darstellung des Bundesdatenschutzgesetzes, 1991.

Zeitler, Stefen, Allgemeines und Besonderes Polizeirecht für Baden-Württemberg, 1998.

Abstract

In order to effectively prevent risks from turning into hazards, it is necessary for the legislation to authorize the police to take measures to collect information. However, these measures may violate the human rights. In police law, how to legislate so that the monitoring is not excessive and human rights are not infringed, in the name of improving efficiency or safeguarding national security, has profound research value.

Within the scope of police law, this article is divided into five parts. In addition to the preface, it discusses the constitutional issues of secret infiltration of computers to collect informations, the relevant judgment of the German Federal Constitutional Court and legal systems, the legal basics of police law in my country, and at last, states conclusions and recommendations.

Keywords: Secret Infiltration of an Computer System, Reasonable Expectation of Privacy, Right to Informational Self-Determination, Search, Communication Surveillance, General Clause, Police Power Exercise Act