網路之刑事追訴
——科技與法律的較勁

王　士　帆*

要　目

DOI：10.3966/102398202016060145006

* 成功大學法律學系助理教授，德國慕尼黑大學法學博士。感謝審查委員寶貴建議及成大法律學系蔡志方老師的討論意見，提升本文可讀性，惟文責當然全在筆者。

投稿日期：一〇四年一月二十三日；接受刊登日期：一〇四年十月八日

責任校對：蘇淑君

摘　要

於今日數位資訊社會，對抗網路犯罪成為刑法與相關刑事訴訟法的重大議題。資訊科技為法律帶來多方面挑戰。當網路成為犯罪工具，國家何嘗不想利用網路追訴犯罪。網路之刑事追訴正是科技與法律的一種較勁。科技固然一日千里，但網路偵查措施不管多精密，終究應回歸基本權干預的審查體系。對於電腦科技犯罪之蒐證，無論是雲端搜索、秘密線上搜索，審查其干預法律依據將是重心所在。因此，探求現行法是否有適當的干預授權基礎，成為網路追訴的首要課題。

關鍵詞：基本權、網路犯罪偵查、網路電話、雲端搜索、秘密線上搜索

壹、前 言

可以進行**網路之刑事追訴**（Strafverfolgung im Internet）嗎？這個問題一語雙關：從科技面來看，涉及**如何**進行，在法律面則應關注**可否**為之。

國際電信聯盟（International Telecommunication Union）統計，二〇一四年全球上網人口達29億人數[1]。網路科技日益發達，拜網路通訊協定（Internet Protocal, IP）之賜，各種聯網設備，從家庭電腦至臺灣城市街頭幾乎人手一機的網路行動裝置[2]，均能上網傳輸。就連愛書成痴的德國也是[3]，「網路已成為重大影響大多數德國民眾生活的媒介。若無網路，他們將清楚感受日常生活之差異。網路斷線所出現的典型後果，可直接比擬為失去駕駛汽車的可能性」[4]。然而，對網路科技倚賴日深的網路世代，拋出不少網路執法問題。各種來自網路或妨害其正常使用的資訊安全犯罪層出不窮[5]。以德國為例，德國二〇一三年以網路為犯罪工具的案件共

1 http://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx，最後瀏覽日：2015年12月10日。

2 資策會創新應用服務研究所在2014年12月30日公布，依其結合Mobile First最新調查數據發現，臺灣12歲以上民眾，有1,432萬人持有智慧型手機或平板電腦（http://www.find.org.tw/market_info.aspx?k=2&n_ID=8304，最後瀏覽日：2015年12月10日）。

3 2014年德國最受歡迎聖誕禮物，書（含電子書）排名第2，電腦第12。務實德國人青睞的第1名是？錢或禮券（http://de.statista.com/statistik/daten/studie/71364/umfrage/beliebteste-kategorien-fuer-weihnachtsgeschenke/，最後瀏覽日：2015年12月10日）。

4 BGH, Urt. v. 24.01.2013 – 3 ZR 98/12, Rn. 17 (BGHZ 196, 101).

5 幾乎所有探討網路安全文獻的共同觀察，如王勁力，電腦網路犯罪偵查之數位證據探究，檢察新論，13期，頁16，2013年1月；石世豪，電信自由化之下通訊安全規範的轉型趨勢——通信秘密、個人資料保護與電信事業的管制變

257,486筆，比二〇一二年成長12.2%（2012：229,408）[6]。所涉層面當然不以單一內國法為限，網路虛擬世界的無國界性，持續挑戰各國刑事法體系與執行面。因為網路偵查跨境畢竟是常態，為確保不侵及他國主權，有賴國際或區域刑事司法之合作[7]。科技帶來的法律問題效應，完全應驗了科技安全應作為「科技法最原始與最核心之規範客體」[8]。

單就一國刑事法領域而言，從實體法的網路犯罪地認定、網路釣魚、妨害網路通訊隱私等[9]，至刑事訴訟線上偵查之合法性，都是伴隨網路而生的議題。我國實定法方面，《刑法》在十多年前已注意電腦網路犯罪。二〇〇三年《刑法》增訂第36章「妨害電腦使

革，全國律師，9卷5期，頁1，2005年5月。

6 德國聯邦內政部警察犯罪統計年報：Polizeiliche Kriminalstatistik 2013, S. 9.（ http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Pressemitteilungen/2014/06/PKS2013.pdf?__blob=publicationFile，最後瀏覽日：2015年12月10日）。

7 詳見*Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl., 2012, Rn. 88ff. und 215; *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl., 2010, Rn. 41ff.。歐盟2013年發布的《攻擊資訊系統指令》（ABlEU 2013 Nr. L 218/8），可參見*Sieber*, in: Europäisches Strafrecht, 2. Aufl., 2014, § 24 Rn. 68ff.

8 蔡志方，科技法律之概念與衍生之問題，載：城仲模教授七秩華誕祝壽論文集第二冊（行政法總論篇），頁1，2008年10月。

9 *Kudlich*, Straftaten und Strafverfolgung im Internet – Zum strafrechtlichen Gutachten für den 69. Deutschen Juristentag 2012, StV 2012, 561-564. 另參閱Helmut Satzger著，王士帆譯，國際刑法與歐洲刑法，頁58-64，2014年4月；王效文，網際網路犯罪與內國刑法之適用，載：民主・人權・正義——蘇俊雄教授七秩華誕祝壽論文集，頁251以下，2005年9月；許恒達，通訊隱私與刑法規制——論「通訊保障及監察法」的刑事責任，東吳法律學報，21卷3期，頁124以下，2010年1月；薛智仁，「網路釣魚」的刑事責任，東吳法律學報，24卷3期，頁149以下，2013年1月。

用罪」，新增第358條至第363條[10]，立法理由提及「保護電腦系統之安全性」（刑法第358條）、「電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害」（刑法第359條）、「鑒於電腦及網路已成為人類生活之重要工具，……有必要以刑法保護電腦及網路設備之正常運作」（刑法第360條）。最近的立法動作，則是在二〇一四年增訂「網路詐欺公眾罪」（刑法第339條之4第1項第3款）。

相較之下，立法者在《刑事訴訟法》則沒有相應的網路追訴配套。唯一動作是二〇〇一年在《刑事訴訟法》第122條將「電磁紀錄」增列為搜索客體（並搭配修改第128條第2項搜索票記載事項），但搜索電磁紀錄之意義為何，立法理由諱莫如深[11]。值得注意且具實務重要性的，反而是一九九九年才制定的《通訊保障及監察法》（下稱「通保法」）。「網路是一種電腦網絡的電子連結」[12]，成為社交網絡的工具，網路追訴一旦干預人民的秘密通訊自由，就應該且只能依《通保法》為之。然而，《通保法》的法律干預授權，可涵蓋所有網路偵查的取證行為嗎？看得出來，這是涉及科技、但屬基本權干預的典型法律問題。科技與法律的較勁，戰場還是回歸基本權干預的審查體系。

水可載舟、亦可覆舟，當網路成為犯罪工具，偵查機關何嘗沒

10 新近說明，如徐育安，資訊風險與刑事立法，臺北大學法學論叢，91期，頁144-151，2014年9月。

11 立法理由如下：一、本條對搜索之對象增列「犯罪嫌疑人」及「電磁紀錄」。二、重新界定「被告」之概念，將偵查中之「被告」正名爲「犯罪嫌疑人」，與經檢察官偵查終結予以追訴之審判中之「被告」資以區別。

12 BVerfGE 120, 274, 276: „Das Internet ist ein elektronischer Verbund von Rechnernetzwerken.“

想過以網路科技追訴網路犯罪。賦予偵查機關越是有效、靈活的網路偵查權限，越應注意過程的秘密性與所取得的資料和基本權干預的緊張關係。面對電腦科技犯罪，在刑事訴訟法上，強制處分的干預授權將是重心所在[13]。在此意義下，若干透過網路或針對電腦的偵查行為，如在**現行法**可找到明確因應現代網路科技的干預授權依據，自非刑事訴訟的違法取證。換言之，就是容許偵查機關利用此網路科技蒐證。問題是，刑事訴訟原始立法所設想的取證情境，本非針對今日網路社會。加上科技之進步一日千里，法律卻難以一夕數變，法律未與時俱進的結果，網路世界極易成為刑事追訴的化外之地。現代化的網路偵查措施，例如放置木馬程式刺探個人電腦資料的**秘密線上搜索**（verdeckte Online-Durchsuchung），多半是帶有秘密性的重大基本權干預行為。**這些新型態偵查手法，已不是技術上能不能執行，而是法律上是否容許與其法律要件如何設計的問題**。因此，在未增訂相關網路追訴規定之前，如何繼續用舊瓶（現行法）裝新酒（新科技偵查），基於基本權干預架構，只能先行**審查現行法是否有提供適當的干預授權基礎，首要即指法律保留原則**[14]。

---

13 *Sieber*, aaO. (Fn. 7), § 24 Rn. 39.

14 從既有法律規定透過解釋探求干預授權，成爲網路刑事追訴文獻的例行、優先任務，如*Gless*, Strafverfolgung im Internet, ZStrR 2012, 6; *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 761f.; *Singelnstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 594; *Kudlich*, Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme, GA 2011, 195; *Roggan*, Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen – Die Problematik der Auslegung von Gesetzen über ihren Wortlaut oder Wortsinn hinaus, NJW 2015, 1995; *Valerius*, Ermittlungsmaßnahmen im Internet – Rückblick, Bestandsaufnahme, Ausblick, JR 2007, 276; *Vogel*, Informationstechnologische Herausforderungen an das Strafprozessrecht, ZIS 2012, 482.

基於上述問題意識，本文以下先就網路偵查的基本權干預特性出發，說明其涉及的傳統基本權與「資訊科技基本權」（IT-Grundrecht，下稱「IT基本權」），以及一般性地探討其干預授權與界限（貳）；其次，具體檢視**國外文獻資料**[15]聚焦探討的幾種常見網路偵查型態，包括通訊監察脈絡下的保全電子郵件、監控網路電話和網路聊天平臺（參）；與置於「網路搜索」脈絡下的雲端搜索、秘密線上搜索（肆）；文末，以結論總結全文（伍）。

最後，筆者想交代本文研究取徑。網路刑事追訴是結合刑事訴訟法與網路技術的科技整合題目，國內相關文獻仍屬少數，因此，不得不借助國外資料。而囿於筆者的法學外文暨國外法律體系的掌握能力，故選擇以德國法及德國、瑞士文獻為本文參考資料。儘管德國與我國法制有若干立法落差，但規範原理是超越不同法秩序的上位共通原則。鑑於德國法豐沛學術能量與規範密度，借鑑該國如何以基本權審查體系面對網路追訴及立法、實務反應，諒有可取之處。其次，在借鑑德國法的比較方法下，以學理為主軸，輔以德國法規和法院見解為具體實例，但為降低規範疏離感，同時避免失焦，筆者僅於相關段落扼要評析我國法現況。惟應說明，本文定位在**針對網路追訴措施提供刑事訴訟法理應有的思考路徑**，即先介紹常見的網路偵查類型，再從可能涉及之人民基本權探求現行法是否有適當的干預授權基礎。惟不諱言，各種偵查類型均可深入發展成獨立專論，且事實上即是如此[16]，筆者期盼能拋磚引玉，讓「科技」

15 Vgl. *Gless*, aaO., 3ff.; *Klesczewski*, Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingreiffen im Internet, ZStW 2011, 737ff.; *Kudlich*, aaO., 193ff.

16 線上搜索如*Kohlmann*, Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz: Bedeutung und Legitimation ihres Einsatzes im Ermittlungsverfahren, 2012; 利用社群平臺偵查如*Ihwas*, Strafverfolgung in Sozialen Netzwerken:

不再是「法律」的化外之地。

貳、網路偵查的基本權干預特性

刑事訴訟法是「憲法之測震儀」[17]、「應用之憲法」[18]。這些非溢美之詞的法治國名言，除了訴求國家實行刑事程序應遵守憲法要求外，尤其在提醒刑事訴訟強制處分若具基本權干預性質者，便不能脫離法律保留與比例原則的限制（參照憲法第23條）[19]。以上憲法誡命，同樣適用在網路科技偵查。換言之，網路偵查時，一樣要先界定是否干預某種基本權，以及探求現行法律有無相關的干預授權基礎。但是，以往刑事訴訟的單一強制處分通常只涉及個人的某一基本權，電腦或網路卻未必如此。在今日社會，電腦不再是單純以電磁紀錄形式存放檔案的限量收納盒。它除工作用途外，龐大的運算能力與儲存空間，提供個人社交管道、珍藏隱私資料。誰侵入他人電腦，電腦使用者在什麼時點處理什麼資料或開啟什麼程式、瀏覽什麼網頁、收發什麼內容的電子郵件（含來源與去向）等等，通通一覽無遺。換言之，針對資訊系統的偵查蒐證，因生活領域受種種基本權保障的大量不同資料同時存放在儲存媒介，都可被立即採知。若將電腦稱為帶有高度人格內涵的**個人資料庫**（persönlicher Datenpool）[20]，一點都不為過。

這種集各式資料於一身的科技設備，使基本權——例如秘密通

Facebook & Co. als moderne Ermittlungswerkzeuge Broschiert, 2014.

17 *Roxin/Schünemann*, Strafverfahrensrecht, 28. Aufl., 2014, § 2 Rn. 1.

18 BVerfGE 32, 373, 383.

19 李佳玟，程序正義的鋼索，頁187-188，2014年6月；林鈺雄，刑事訴訟法（上）——總論篇，頁21-22，2013年9月，7版。

20 例如*Valerius*, aaO. (Fn. 14), 279.

訊自由[21]、資訊隱私權[22]——的傳統範圍界定在網路偵查上趨於模糊，個別基本權的射程距離變得較難確定[23]。舉例來說，秘密通訊自由保障的，是在空間隔離下的整體通訊過程之秘密性，因為傳輸中容易受到第三人侵害，故保護時點開始於消息之傳送、結束於送達[24]。在自己電腦中的郵件管理軟體（如Outlook或Windows Live Mail）寫信，則該電子郵件的秘密通訊自由保護範圍，依上述說法，乃始於「傳送」郵件，傳送之前的書寫或暫存，當然不受秘密通訊自由保護。但換個場景：如果是網路連線到電子郵箱提供者的Webmail上寫信，答案仍一樣嗎？文獻就認為，Webmail本身已受秘密通訊自由保護，登入Webmail即進入通訊自由保護範圍，而與使用者要在上面書寫的Email無關[25]。

---

21 參見司法院釋字第631號解釋文：「憲法第12條規定：『人民有秘密通訊之自由。』旨在確保人民就**通訊之有無、對象、時間、方式及內容**等事項，有**不受國家及他人任意侵擾**之權利。」

22 參見司法院釋字第603號解釋文：「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**。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。」

23 *Kudlich*, aaO. (Fn. 14), 195.

24 Maunz/Dürig/*Dumer*, GG, 72. Ergänzungslieferung, 2014, Rn. 62; *Pieroth/Schlink/Kingreen/Poscher*, Grundrechte, 29. Aufl., 2013, Rn. 826 und 838.

25 *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 1. Aufl., 2009, Rn. 816; *Kudlich*, aaO. (Fn. 14), 202.

一、網路偵查干預之基本權：傳統基本權與IT基本權

㈠傳統基本權

某一網路偵查措施是否為法律許可，如前所述，並不脫離刑事訴訟基本權干預的審查體系[26]。因此，在此審查體系下，首先應探究：系爭偵查措施干預人民的什麼基本權？刑事訴訟偵查行為所干預的基本權，原則上不同於審判程序上的訴訟行為，後者以干預**程序基本權**（Verfahrensgrundrecht）為主，典型之例如（限制）對質詰問權、上訴權，或證據聲請權，而前者則是以涉及**實體基本權**（materielles Grundrecht）居多。在網路偵查方面，可能涉及的基本權[27]，以傳統所熟悉的秘密通訊自由、人格權、居住自由及——德國聯邦憲法法院為資訊系統新創的——「資訊科技基本權」[28]最為密切相關。

網路功能上是一種對外聯繫工具，因此，網路偵查與秘密通訊自由之緊張關係首當其衝。個人利用網路與他人的視訊交談、收發電子郵件，或使用網路電話，只要雙方通訊尚未終結，則通訊活動均在秘密通訊自由的保障範圍[29]。除此之外，網路通訊的**周邊資料**

---

26 強制處分與基本權干預合法化的審查體系，參見林鈺雄，同註19，頁311以下。

27 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 760; *Kudlich*, aaO. (Fn. 14), 195-198.

28 BVerfGE 120, 274. 關此，簡介如*Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 78-81; 相關中文文獻，如何賴傑，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，208期，頁236-238，2012年9月。詳細分析線上搜索與可能涉及之基本權，可參見謝碩駿，警察機關的駭客任務——論線上搜索在警察法領域內實施的法律問題，臺北大學法學論叢，93期，頁15-26，2015年3月。

29 從人權公約角度，結論亦相同：*Grabenwarter/Pabel*, EMRK, 5. Aufl., 2012, § 22 Rn. 25; *Peters/Altwicker*, EMRK, 2. Aufl., 2012, § 14 Rn. 3.

（Randdaten），亦即，不屬於通訊內容的網路通信紀錄或通信使用者資料等，也受秘密通訊自由保障[30]。現代人儲存在個人電腦或雲端硬碟的數位資料巨幅成長，要從中探知個人生活型態輕而易舉。諸如觀察日常處理的電腦檔案、瀏覽之網頁與頻率、透過網路的人際互動，甚至是電子日記、私密錄影種種直接觸及私人核心領域的電磁紀錄，從這些私人資料普遍可勾勒出個人的人格圖像，故也涉及人格權或資訊隱私權。最後，由於數位資料原則上存放在電腦系統，國家侵入電腦則另涉及下述的「IT基本權」之侵害。

㈡IT基本權

IT基本權，完整稱作資訊科技基本權，在德國，是其聯邦憲法法院二○○八年BVerfGE 120, 274創造的基本權干預新審查標準[31]。該法院於審理危險預防性的秘密線上搜索一案，提出**保障資訊科技系統私密性與完整性的基本權**（Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme），文獻有稱之為「資訊科技基本權」[32]或「電腦基本權」（Computergrundrecht）[33]。德國聯邦憲法法院所持理由是：「使用資訊科技與人格發展及人格之危害緊密連結，因此形成基本權保護的需求。鑑於不受阻礙之人格發展，人民對國家尊重資訊系統之

30 參見司法院釋字第631號解釋。

31 BVerfG, Urt. v. 27.02.2008 –1 BvR 370/07 und 1 BvR 595/07.

32 如*Buermeyer*, Zum Begriff der „laufenden Kommunikation“ bei der Qullen-Telekommunikationsüberwachung („Qullen-TKÜ“) – Ein Beitrag zu den gebotenen legislativen Konsequenzen aus der Online-Durchsuchungs-Entscheidung des BVerfG, StV 2013, 470; *Luch*, Das neue „IT-Grundrecht” – Grundbedingung einer „Online-Handlungsfreiheit”, MMR 2011, 75.

33 如*Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, 2012, S. 99; *Kudlich*, aaO. (Fn. 14), 198.

私密性與完整性具有正當期待與信賴」[34]。「一般人格權包含保障資訊科技系統私密性與完整性的基本權，其保護範圍主要在讓使用者享有資訊科技系統製作、處理、儲存資料的私密性；一旦資訊系統受到攻擊，以致他人可使用該資訊系統的效能、運算與儲存內容，即構成此基本權的侵害」[35]。

應注意，德國聯邦憲法法院是將「保障資訊科技系統私密性與完整性的基本權」當作人格權範疇內的一種**補遺性基本權**（Auffanggrundrecht），**只在其他特別基本權保護範圍所不及時，才加以檢驗**[36]。憲法法院清楚表示：「秘密通訊自由的保障範圍並未包含資訊系統的私密性與完整性」[37]，「秘密侵害資訊科技系統以取得資料，如果不在秘密通訊自由保障範圍所及者，將出現保護漏洞。對此保護漏洞，應以『保障資訊科技系統私密性與完整性的一般人格權』加以填補」[38]。具體來說，國家若在私人電腦安裝間諜程式，目的是為了監控網路電話，且技術上也只能監控網路電話時，則以秘密通訊自由作為唯一干預授權的審查標準。反之，侵入電腦如既未干預通訊，也非截取儲存之個人隱私資料，個人則仍可主張享有資訊科技免於遭受國家干擾的電腦基本權[39]。

其實，於德國刑法領域，早在一九八〇年代即有侵害IT基本權的處罰規範（§ 202a StGB）[40]。**電腦犯罪**的核心犯罪（狹義之電腦

---

34 BVerfGE 120, 274, 306.

35 BVerfGE 120, 274, 302.

36 *Vogel*, aaO. (Fn. 14), 482。關於補遺性基本權，參見*Pieroth/Schlink/Kingreen/Poscher*, aaO. (Fn. 24), Rn. 387。有認爲電腦基本權本來就落在資訊自主決定權保護範圍，質疑電腦基本權的存在必要性，參見謝碩駿，同註28，頁25-26。

37 BVerfGE 120, 274, 306f.

38 BVerfGE 120, 274, 308.

39 *Kudlich*, aaO. (Fn. 14), 198.

40 詳見徐育安，同註10，頁131。

犯罪），是以電腦為攻擊客體的不法行為，其保護法益即電腦資訊系統的**私密性、完整性與可使用性**（Confidentiality, Integrity and Availability; Vertraulichkeit, Integrität und Verfügbarkeit）[41]。如果一般人入侵他人電腦，早應以刑法相繩，偵查機關何獨能例外呢？現在，德國聯邦憲法法院將IT基本權的保護陣線拉到對抗國家機關的干預行為，相當具有未來性的指標意義。簡言之，IT基本權往後不只是適用在秘密線上搜索的議題而已。資訊科技未來會怎樣進展而深入個人生活領域，永遠無法預測，國家將怎樣「善用」科技新武器亦不可得知。但是最起碼，當偵查機關未符合法定干預要件或在立法者尚未提供法定干預基礎，卻不當侵入個人資訊系統時，受干預者如無其他特別基本權可資具體主張者，至少還有IT基本權可作為防禦權利的最後防線。

二、探求干預授權與界限

從以上說明，不難理解偵查機關對電腦有強烈的蒐證慾望，希冀透過電腦一網打盡，但**科技上**做得到對資訊系統「翻箱倒櫃」（例如間諜程式的搜尋），不表示**法律上**就（已）容許。這時，網路之刑事追訴又回到基本權干預脈絡的基本立場。網路偵查除非是不涉及基本權干預的行為，例如例行性的網路巡邏

41 也因爲如此，狹義之電腦犯罪又被稱爲「CIA犯罪」。Vgl. *Sieber*, aaO. (Fn. 7), § 24 Rn. 2 und 17. 歐洲理事會推動的《網路犯罪公約》，可參見徐育安，同註10，頁127-129；馮震宇，網路犯罪與網路犯罪公約（上／下），月旦法學教室，4/5期，頁124-136/115-124，2003年2/3月。該公約與我國刑法妨害電腦使用罪章的立法關聯，可參見廖宗聖、鄭心翰，從網路犯罪公約談我國妨害電腦使用罪章的修訂，科技法學評論，7卷2期，頁57以下，2010年12月；蔡蕙芳，妨害電腦使用罪章：第一講：保護法益與規範功能，月旦法學教室，126期，頁62以下，2013年4月。

（Streifenfahrt）[42]，否則，與其他強制處分沒有不同，一樣需有合憲性之法律干預授權基礎。結果簡言之，**「網路追訴之基本權干預」應有法律保留原則的適用，而且應遵守比例原則**[43]。

以網路通訊為例，說明法律干預授權基礎在網路偵查的重要性。電子郵件是透過電子無體物之媒介（Medium）即時傳輸信息的通訊活動，乃今日普遍使用的通訊工具。對即時進行之電子郵件的證據保全——有別於通訊已結束的電子郵件[44]——，若要監控其內容，應依干預電子郵件之通訊活動的取證規定[45]。我國在一九六七年修正的《刑事訴訟法》第135條扣押實體郵件規定，對於保全「通訊中之電子郵件」顯然不適格[46]。立法者一九九九年制定的《通保法》，具體規範偵查機關干預通訊監察的法定基礎，以「保障人民秘密通訊自由及隱私權」（通保法第1條）。其中，所保障的通訊，乃指「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信」（通保法第3條第1

---

42 *Roxin/Schünemann*, aaO. (Fn. 17), § 32 Rn. 2。關於網路聊天室的偵查行爲，參見本文參、三。

43 *Kudlich*, aaO. (Fn. 14), 195; *Singelnstein*, aaO. (Fn. 14), 594; *Vogel*, aaO. (Fn. 14), 482; 林鈺雄，同註19，頁444：「新舊強制處分都有一個共通之處：同樣干預人民的基本權利，因此，無論就其立法或司法層次，同樣應受法律保留與比例原則的控制」。

44 見下文參、一、㈠。

45 *Gless*, aaO. (Fn. 14), 8 (Art. 269ff. chStPO); *Kudlich*, aaO. (Fn. 14), 199; *Valerius*, aaO. (Fn. 14), 275。不同見解，認爲依搜索扣押爲之：王銘勇，網路犯罪之搜索與扣押，法學叢刊，191期，頁58-59，2003年7月。

46 不同意見，王銘勇，同前註，頁58-59：「鑑於電子郵件亦屬通信，且他人就該通信內容不得與聞之秘密性，應認前開刑事訴訟法之規定（按：指刑訴第135條），就電子郵件之情況亦有適用。即網路電信事業服務業者之伺服器中暫時存放受信人電子郵件，亦有該規定之適用。」

項第1款），才將電子郵件正式納為可受通訊監察的客體[47]。再者，秘密通訊自由除通訊內容外，也涵蓋**「通訊之有無、對象、時間、方式」**[48]，偵查機關欲調取網路的通信紀錄或通信使用者資料等周邊資料（Randdaten），即限於立法者事先制定干預之法律授權依據，始可依法為之[49]。為此，《通保法》於2014年增訂第3條之1和第11條之1作為調取通信紀錄的干預授權基礎[50]。

最後，強制處分干預授權既然出於法律保留原則的要求，自應遵守法律保留原則內涵。亦即，在正常法治國家，創設干預授權基礎的權限只在立法者，唯有立法者才能決定是否容許國家發動侵害

47 林鈺雄，同註19，頁445；黃朝義，刑事訴訟法，頁317，2014年9月，4版。不過，《通訊保障及監察法施行細則》第2條第2項稱母法第3條第1項第2款「郵件及書信」，指「信函、明信片、特製郵簡、新聞紙、雜誌、印刷物、盲人文件、小包、包裹或**以電子處理或其他具有通信性質之文件或物品**」，將電子郵件當成實體郵件，這涉及子法逾越母法定義的問題。文獻爲化解上述爭議，主張施行細則第2條第2項「電子處理」之文件，並非電子郵件，而是指「以紙本信封寄送附光碟、磁碟片或其他硬體儲存設備（例如隨身碟）」（許恒達，同註9，頁129）。

48 司法院釋字第631號解釋。另參見李震山，挪動通訊保障與通訊監察天平上的法碼——釋字第631號解釋評析，台灣本土法學雜誌，98期，頁284，2007年9月。

49 *Gless*, aaO. (Fn. 14), 13f.

50 舊法時代的爭議與新法討論，如李榮耕，簡評2014年新修正的通訊保障及監察法——一次不知所爲何來的修法，月旦法學雜誌，227期，頁165-167，2014年4月；林鈺雄，通訊監察之修法芻議——通訊保障及監察法之部分修正條文，萬國法律，192期，頁27-29，2013年12月；張麗卿，通訊保障及監察法之修正與評析，月旦法學雜誌，229期，頁37-39，2014年6月；陳重言，刑事追訴目的之通信（通聯）紀錄調取與使用——兼評2014年初通保修法，檢察新論，16期，頁40以下，2014年7月；陳運財，偵查與人權，頁360-363，2014年4月。

基本權的干預行為以及其合法性要件[51]。這意味著：首先，追訴犯罪的公共利益並不會凌駕法律保留所欲保護的法益，因此，不可以公共利益為由，對刑事訴訟既有的干預權限盡可能朝偵查友善（ermittlungsfreundlich）之方向作法律解釋[52]；其次，網路偵查之基本權干預不得類推適用現行其他干預規定[53]；第三，禁止司法機關混合各種干預授權要件作為新型態網路偵查的核准要件，縱使從比例原則來觀察，這些既有的個別法定要件均屬高度門檻（例如重罪原則、補充性原則，與絕對法官保留要求），亦無不同。因為混合現行個別干預規定，實質上已是創設新的法律授權基礎了。至於比例原則，在個案上雖可限制法定干預權限，但終究不能取代一個刑事訴訟法上並不存在的干預授權基礎[54]。

參、通訊監察脈絡下的網路偵查

以上說明網路偵查的基本權干預特性。而既然涉及基本權干預，網路偵查自應接受干預有無正當性的審查。由於網路是重要通訊工具，網路偵查以自然干預秘密通訊自由為主，相關的通訊監察手段者，以保全電子郵件、監控網路電話，和網路聊天室為大宗[55]。

51 *Valerius*, aaO. (Fn. 14), 277.

52 *Beulke/Meininghaus*, Anm. zu BGH Ermittlungsrichter, Beschl. v. 21.02.2006 – 3 BGs 31/06, StV 2007, 65.

53 *Valerius*, aaO. (Fn. 14), 276.

54 BGHSt 51, 211, 219 Rn. 22.

55 *Klesczewski*, aaO. (Fn. 15), 739.

一、保全電子郵件

保全電子郵件，應以郵件是否屬於**秘密通訊自由之保護範圍**來區分保全措施。監控即時通訊中的電子郵件與保全收件人儲存的電子郵件（或寄件人尚未傳送的電子郵件），前、後所涉基本權不同，干預手段自應不同，授權基礎亦有別。簡單來說，收件人已在服務提供者伺服器的網頁郵箱（Webmail）讀取電子郵件或從該伺服器接收到自己電腦管理程式時，即結束秘密通訊之活動。因為，當通訊抵達收受人而處於其支配領域時，應由收件人自己採取保護措施對抗其不願發生的資料截取，此時再無因空間隔離以致通訊有被侵害的特殊危險[56]。因此，秘密通訊過程已結束的電子郵件，由於不再受到秘密通訊自由保護[57]，所考量的保全手段應不是通訊監察，而是搜索扣押[58]。以下分述之。

㈠搜索扣押電子郵件的儲存載體

在電子郵件之**秘密通訊過程已結束**方面，一般來說，個人電子郵件會儲存在電腦硬碟、行動裝置，或郵箱伺服器。電子郵件是一種電磁紀錄，從物理性質而言，電子郵件並非實體物，不能成為扣押之「物」，但由於存在於實體物件上，國家機關欲取得實體物件的占有支配，應循一般搜索、扣押規定，扣押電子郵件所在的儲存載體，例如直接扣押個人電腦硬碟或郵箱伺服器[59]。

---

56 BVerfGE 115, 166, 184.

57 BVerfGE 115, 166; s. auch *Kudlich*, aaO. (Fn. 14), 196; Maunz/Dürig/*Dumer*, aaO. (Fn. 24), Rn. 62.

58 相同見解，黃朝義，同註47，頁317：「應將網際網路信件之通訊，限於受監察人之現在或未來之通訊，而對於以電磁紀錄形式儲存於電腦中之網際網路信件，可依刑事訴訟法上搜索及扣押之程序加以處理」。

59 *Gless*, aaO. (Fn. 14), 7f.; *Kudlich*, aaO. (Fn. 14), 201; *Roxin/Schünemann*, aaO.

不過，執行扣押資料載體仍應注意**比例原則**[60]。例如所扣押之硬碟有大量資料（想像一下您的電腦有幾筆文件檔）或加密的檔案需要解密，有長時間扣押必要時，應注意硬碟檔案對持有人的重要性，畢竟扣押儲存載體對持有人而言，未必是較輕微的干預手段，例如儲存與客戶往來資料的硬碟被帶走，將損及企業公司正常運作。因此，基於比例原則，偵查機關一方面應儘量避免檢視與追訴犯罪不相關的私密檔案。另一方面，除非扣押之硬碟是「（應或得）沒收之物」（參見刑法第38條第1項），否則，若僅是可為證據之物（參見刑事訴訟法第133條第1項），應採用較輕微的電子保全措施，通常選項是直接複製到偵查機關的儲存媒體或列印所欲保全的資料[61]；至於這些原物替代品的後續審判證據調查，只要確保同一性無虞，即對替代品之真實性不生懷疑時，則依物證性質循書

(Fn. 17), § 34 Rn. 4, § 36 Rn. 8; *Kindhäuser*, Strafprozessrecht, 3. Aufl., 2013, § 8 Rn. 148; *Schlegel*, „Online-Durchsuchung light" – Die Änderung des §110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, HRRS 2008, 24; *Valerius*, aaO. (Fn. 14), 278。黃朝義，同註47，頁240；王銘勇，同註45，頁58。

60 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 774f.; *Kudlich*, aaO. (Fn. 14), 201; *Meyer-Goßner/Schmitt*, StPO, 57. Aufl., 2014, § 94 Rn. 4; *Roxin/Schünemann*, aaO. (Fn. 17), § 34 Rn. 4; *Schlegel*, aaO., 24; *Valerius*, aaO. (Fn. 14), 278。有從電磁紀錄附著設備之扣押必要性來理解：王銘勇，同註45，頁52-53。

61 製作硬碟電磁紀錄之「映像檔」是另一種可能有效保全、但未必干預最輕微的替代作法，即偵查機關對原儲存載體透過位元流，一個個位元（bit for bit）逐一複製，最後製作出完整複製原載體的映像檔，連原載體中已刪除，但可回復的檔案也可在映像檔讀取。偵查機關之後便在該映像檔搜尋程序相關資料或作業，而不必扣押原檔案載體。製作映像檔的好處是，可避免偵查機關毀損或變更載體資料，造成日後的審判證據調查爭議。詳見李榮耕，電磁紀錄的搜索及扣押，國立臺灣大學法學論叢，41卷3期，頁1060-1063，2012年9月。

證或（合併）勘驗方式調查，必要時，尚須進行鑑定[62]。

同理，已讀取的電子郵件存放在雲端硬碟時，雖非存在個人電腦設備，而是放在虛擬空間。但雲端空間本身仍是處於一個有特定真實地理位置的伺服器上，這裡並不涉及網路取證，回歸一般搜索扣押規定即可[63]。亦即，理論上，偵查機關可直接對該雲端伺服器（「物件」）依法聲請搜索、扣押，以保全伺服器內通訊已結束的電子郵件，此時當然也要注意前述保全執行的比例原則。只不過，雲端伺服器一旦在外國，**實際上**可否透過司法互助進行扣押保全，又是另一個問題了。另外，假如搜索被告電腦，發現電腦連結雲端硬碟，雲端硬碟是否亦在原搜索效力所及，則涉及雲端搜索議題[64]。

㈡監控電子郵件通訊

保全電子郵件的另一種情形，是監控即時進行中的電子郵件傳輸。一般將電子郵件傳輸分為四階段[65]：

A傳送階段

寄件人透過電子郵箱服務提供者之伺服器，將電子郵件以封包（Packet）方式寄到收件人的電子郵箱服務提供者之伺服器；

B暫存階段

封包重組後的電子郵件，一定時間內存放在收件人的電子郵箱服務提供者之伺服器；

---

62 *Marberth-Kubicki*, aaO. (Fn. 7), Rn. 618-620; SSW-StPO/*Kudlich/Schuhr*, StPO, 2014, § 88 Rn. 11f., § 249 Rn. 14.

63 *Gless*, aaO. (Fn. 14), 7f.

64 參見本文肆、一。

65 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 779; *Klesczewski*, aaO. (Fn. 15), 744f.

C接收階段

收件人接收可分為兩種情形：一是收件人在自己的電腦裝置接收電子郵件，同時間，郵箱伺服器上的電子郵件可能自動即時刪除、定期刪除或繼續保留；二是收件人直接在郵箱伺服器的Webmail讀取電子郵件。

D管理階段

收件人將接收在自己電腦的電子郵件儲存在電腦硬碟，或線上讀取完畢而繼續留在郵箱服務提供者的伺服器。

上述傳輸流程如何保全電子郵件？先談沒有爭議的情形。在A和C階段，應該且只能依通訊監察規定保全電子郵件，郵箱服務提供者甚至依法負有協助執行義務[66]。這點沒有爭議，德國法理解也是如此（§§ 100a, 100b StPO; § 110 VI TKG）[67]。另一個沒有爭議的保全方式是D階段：由於收件人已接收並儲存電子郵件，或直接在線上讀取而繼續保留在伺服器，無論如何，通訊均已終結，不再受秘密通訊自由保護[68]（但不排除其他基本權利之保障，例如資訊自決權）；如前所述，此時適用扣押規定保全電子郵件[69]。

有爭議的是B階段，爭點在於：應依通訊監察或搜索扣押進行保全呢？德國方面，搜索扣押與通訊監察各有主張，甚至有認為德

---

66 《通保法》第14條第2項：「**電信事業及郵政事業有協助執行通訊監察之義務**；其協助內容爲執行機關得使用該事業之通訊監察相關設施與其人員之協助。」

67 *Beulke*, Strafprozessrecht, 12. Aufl., 2012, Rn. 253b; *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 780; *Klesczewski*, aaO. (Fn. 15), 745f.; *Kudlich*, S aaO. (Fn. 14), 203; *Meyer-Goßner/Schmitt*, aaO. (Fn. 60), § 100a Rn. 6b; *Volk/Engländer*, Grundkurs StPO, 8. Aufl., 2013, Rn. 40.

68 BVerfGE 115, 166, 183f.

69 參見本文參、一、㈠。

國法根本欠缺干預依據[70]。正確而言，電子郵件傳送經過郵箱服務提供者之伺服器，直到收件人讀取前仍屬秘密通訊過程，如欲進行保全，自應適用通訊監察規定[71]。可是，德國實務卻支持扣押說，頂多是各級法院原先爭辯到底適用一般扣押規定或核准門檻較高的郵件扣押。在德國聯邦憲法法院二〇〇九年表示適用扣押規定（尤其是郵件扣押）並特別強調應遵守比例原則即可為之後[72]，「扣押」伺服器未讀取的電子郵件已成實務定見。德國實務採取扣押說，顯然有意規避通訊監察的核准高門檻（重罪原則、補充性原則等）[73]。

撇開德國實務偏好巧門的心態不談[74]，扣押說完全忽視暫存在業者郵箱伺服器的電子郵件，在收件人未讀取之前，其通訊（仍）處於傳輸進行中，依然受到秘密通訊自由的保障，故不應單純以電子郵件傳輸技術上的幾種階段就區分不同法律保障。此外，德國實務奉為上意的德國聯邦憲法法院電子郵件扣押說，案情乃是針對「公開」扣押而發。該裁判事實是被告知悉扣押裁定內容（以伺服器郵件為扣押物），亦即，偵查機關並非秘密保全伺服器郵件，而是在被告知悉下的「公開」複製伺服器郵箱的電子郵件到偵查機關

70 Vgl. *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 781ff.

71 *Beulke*, aaO. (Fn. 67), Rn. 253b; *Gless*, aaO. (Fn. 14), 11; *Heghmanns*, Strafverfahren, 1. Aufl., 2014, Rn. 521; *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 783; *Kindhäuser*, aaO. (Fn. 59), § 8 Rn. 82; *Kudlich*, aaO. (Fn. 14), 203; *Roxin/Schünemann*, aaO. (Fn. 17), § 36 Rn. 6; *Valerius*, aaO. (Fn. 14), 279。德國文獻之各式爭論，另見何賴傑，同註28，頁243-244。

72 BVerfGE 124, 43。該裁判之介紹，參見何賴傑，同註28，頁241-242。

73 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 782.

74 在A和C階段的傳輸階段擷取電子郵件，技術上畢竟較爲不便，爲求效率，偵查機關通常會在B或D階段「扣押」電子郵件。vgl. *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 779.

儲存裝置。如此一來，若要秘密保全暫存郵箱伺服器的電子郵件，德國聯邦憲法法院的扣押說是否仍能逕自套用，顯有疑問，不值採納[75]。

二、監控網路電話——以Skype為例

㈠技術面：來源端電信監察（Qullen-TKÜ）

秘密通訊自由保障重心之一的電話，從固網電話、無線電話發展到網路電話，讓相關的通訊監察技術與法規面臨挑戰[76]。傳統的固網電話（例如市內電話、公用電話），透過銅線或光纖線等實體媒介傳輸訊息，由於有線連結的用戶端點特定，監聽受監察人的固網通話技術上較為簡單。一九九〇年代起，無線行動電話逐漸普及，偵查機關對無線電話的通訊監察技術曾歷經一波挑戰。此後，網路電話崛起，以Skype為例，它打著網內免費、網外低廉的優質通訊口號廣受歡迎，尤其是智慧型手機等行動裝置激增，個個又可安裝Skype的今日，除電信法規的討論外[77]，偵查機關可否監聽Skype電話的爭辯成為刑事法與科技的另一場較勁。Skype網路電話的交談內容，符合秘密通訊自由的保障範圍（參見通保法第3條第1項第1款通訊定義），殆無疑義[78]。若要監控網路電話，通訊監察規定是可列入考慮的干預授權依據。既然如此，現行法似乎已有干預授權基礎，網路電話之監察何須討論「可否」依法為之？問題癥結在科技層面。

---

75 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 785.

76 *Gless*, aaO. (Fn. 14), 11f.

77 關此，參見李志仁，電信資訊匯流下之法律爭議——以Skype爲例，科技法律透析，18卷12期，頁43以下，2006年12月；vgl. *Gless*, aaO. (Fn. 14), 12.

78 *Gless*, aaO. (Fn. 14), 11; *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 810.

網路電話的技術原理[79]，是一種去中央化的網際協議通話技術（VoIP: Voice-over-IP），將語音切割成資料封包，不經中央伺服器，而是透過網路自行搜尋最近的路徑，傳送至受話方，達成語音通話。這種以使用客戶為收受基點的點對點（P2P: Peer to Peer）傳輸，與即時通訊軟體（Instant Message）的網路通話不同，後者因透過業者的中央伺服器傳輸封包訊息，偵查機關仍可依通訊監察規定在業者線路聽取交談[80]。對刑事追訴而言，網路電話的點對點傳輸特性，正好是秘密通訊取證合法性的法律爭議所在。理由何在？簡言之，Skype網路電話對傳輸的資料封包，使用加密技術：網路電話將語音訊號（語音的資料封包）從源頭端開始編碼加密處理，透過網路傳輸到目的端的受話方，再解密還原成聲音。亦即，網路電話傳輸的資料封包要送到使用者的終端設備才會被解碼，也才會組合成有意義的通訊內容。

資料封包加密是Skype的資安政策[81]，卻也是偵查機關監察網路電話的技術難題。偵查機關雖然可依《通保法》規定，在符合通訊監察要件下，要求網路服務業者協助進行資料傳輸線路的「一般」通訊監察。但所紀錄的，只是被加密的亂碼資料，並無多大意義。真要將加密的VoIP資料流解密並還原成可聽辨（hörbar）的語音，若不是顯著費勁，就是完全不可能，視加密技術而定[82]。而

79 李志仁，同註77，頁45。

80 *Klesczewski*, aaO. (Fn. 15), 741.

81 Skype安全政策：「Skype使用國際承認和接受的標準加密演算法，這些演算法經得起多年分析和攻擊的時間考驗。這保護您的通訊內容不會落入駭客和犯罪分子的手中。如此一來，我們就能夠幫助確保使用者的隱私權，以及使用者間互相發送資料的完整性。」（http://www.skype.com/zh_TW/security/，最後瀏覽日：2015年12月10日）

82 *Buermeyer*, aaO. (Fn. 32), 470f.; *Klesczewski*, aaO. (Fn. 15), 742。據臺灣iThome電腦報周刊2014年6月30日報導，若要對RSA-1024的加密規格進行解密，「目

且，即便現在破解了，業者日後若採用新加密技術，偵查機關又要找尋新破解法。所以，偵查機關如要監聽Skype的網路電話，雖不以通訊服務提供者之協助為必要，但應在語音信號尚未編碼加密前的網路裝置發話端或已解密後的受話端，安裝側錄軟體記錄未加密或已解密的資訊內容，再秘密線上傳輸給偵查機關。這種監控的木馬程式，俗稱「政府間諜軟體」（GovWare）。由於是在網路電話通話雙方各自的端點進行監控，德國因此稱為**來源端電信監察**（Quellen-Telekommunikationsüberwachung, Qullen-TKÜ）[83]。

㈡法律面：欠缺干預授權基礎

監控網路電話雖近似於傳統的電話監聽（錄），同樣是侵害秘密通訊自由，但可否單單以**電話監聽**的刑訴干預授權——例如德國《刑事訴訟法》第100a條——為執行依據，極有爭議[84]。爭點在於，監聽網路電話，如前所述，必須在網路通話雙方之一作為安裝間諜軟體的來源端，即以侵入個人資訊系統為前階準備措施。但目前的通訊監察條款有無包含這種「讓電腦中毒」的附隨干預權限，不無疑問。

前一般家用電腦最少需要花費2000年才能解開，而動用日本超級電腦ES2的640個節點資源，找出RSA-1024密碼使用的解密金鑰，也要花上10年的時間」，「而LINE使用同級更高規格的RSA-2048，安全性自然也更高。」（http://www.ithome.com.tw/news/89032，最後瀏覽日：2015年12月10日）

83 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 810; *Klesczewski*, aaO. (Fn. 15), 742; *Kudlich*, aaO. (Fn. 14), 205f.; Vermerk des Genealbundesanwalts beim BGH v. 29.10.2010, Rechtliche Zulässigkeit der sog. „Quellen-TKÜ", StV 2013, 476。補充說明：加密技術的運用不以網路電話爲限，也可能包括加密的網路聊天室或以Https（Hypertext Transfer Protocol Secure: https://）連線的網站，參見 *Buermeyer*, aaO. (Fn. 32), 471.

84 *Kudlich*, aaO. (Fn. 9), 564f.（列出正反意見代表）

以我國法來說，並以Skype為例，其屬我國第2類電信業務[85]，依法雖有協助偵查機關通訊監察的義務（參見通保法第14條），然此協助國家干預人民秘密通訊自由的義務範圍，仍取決於法律有無干預授權基礎。那麼，現行法有提供偵查機關要求Skype在其軟體置入間諜程式的法律依據嗎？傳輸間諜程式是《通保法》所稱執行通訊監察的「其他類似之必要方法」？[86]就算是，間諜程式傳輸、裝置到私人住宅內的網路使用設備，又如何與我國法通訊監察裝置不入家門的禁令相容（參見通保法第13條第1項但書）？[87]以上種種疑問即便都寬鬆審查，間諜軟體的取證目的，也應受限於以「進行中的網路通話」為紀錄對象，執行期間不得獲取或知悉其他資料，避免一網打盡。惟緊接的問題卻是，今日科技上有這種會辨識哪些是網路電話語音封包、哪些是非語音封包的間諜程式嗎？過去做不到[88]，假如今日技術上尚未能達成篩選要求，一旦安裝間諜軟體，會讓偵查機關全面監控電腦資料流通[89]。德國聯邦憲法法院對此說到「對資訊系統的危害，已不只是單純監控進行中的秘密通訊。尤其是也可以獲知與通訊無關的信息，例如個人電腦的用途、

85 參見《連科通訊股份有限公司經營第二類電信事業營業規章》（http://skype.pchome.com.tw/purchase/rule.html，最後瀏覽日：2015年12月10日）。

86 《通保法》第13條第1項：「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。」

87 德國法之討論，參見如*Kudlich*, aaO. (Fn. 14), 196f.; *Valerius*, aaO. (Fn. 14), 279f.

88 幾年前已指出網路電話監察技術的侷限性者，如李志仁，同註77，頁54。

89 就此而言，會類似或等同後述的「秘密線上搜索」（*Heghmanns*, aaO. (Fn. 71), Rn. 521; *Klesczewski*, aaO. (Fn. 15), 744），以致於德國有——少數——文獻不區分秘密線上搜索與來源端通信監察，如*Beulke*, aaO. (Fn. 67), Rn. 253c.

瀏覽特定網頁的頻率等等，傳輸檔案的內容；更甚者，如果被感染的資訊系統有控制住家設備的功能的話，那也可探知個人在住家內的舉動」[90]。為了監控網路電話而安裝一個科技尚未能控制的間諜程式，會成為侵犯IT基本權的一種獨立干預行為，這就不是目前的通訊監察規定所能正當化的權利干預了。

準此，目前只能推論為來源端電信監察欠缺法律授權基礎，故屬違法偵查措施[91]。唯有這樣解釋，才能確保**法律支配科技**，否則，就會出現政府間諜程式不受監督的干預危險[92]。

㈢未來立法可能性

最後應稍補充的是，監控網路電話的非難重點是間諜程式之安裝，基於法律保留要求，這個執行動作在**現行法**因欠缺干預依據，以致不得為之。不過，未來如果增訂妥適的法律干預基礎，結論自然翻轉。

舉例來說，瑞士二〇一一年甫施行的全新刑事訴訟法（Schweizerische Strafprozessordnung），相較於其他「資深」的刑事訴訟法典，算是較為契合科技時代的立法例，但它同樣欠缺來源端電信監察的干預授權[93]。惟瑞士於二〇一三年已提出刑訴修正草案，欲授權偵查機關秘密傳輸間諜軟體到資料處理系統，以刺探通

90 BVerfGE 120, 274, 308f.

91 *Beulke*, aaO. (Fn. 67), Rn. 253c; *Heghmanns*, aaO. (Fn. 71), Rn. 521; *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 811; *Kudlich*, aaO. (Fn. 14), 206f.; *Roxin/Schünemann*, aaO. (Fn. 17), Rn. 3.

92 *Gless*, aaO. (Fn. 14), 18.

93 *Gless*, aaO. (Fn. 14), 12f.; *Pieth*, Schweizerisches Strafprozessrecht, 2. Aufl., 2012, S. 147。關於瑞士新刑訴，參見王士帆，全新刑事訴訟法典——瑞士刑訴改革與整合，政大法學評論，118期，頁105以下，2010年12月。

訊內容及其通訊紀錄等周邊資料（Art. 269ter chStPO）[94]。德國方面，亦不排除立法可能性，至少以德國聯邦憲法法院二〇〇八年的立場來看，其不但為此預留伏筆，也指定立法規格：「假如來源端電信監察只用來監察進行中的通訊內容，秘密通訊自由就成為唯一干預授權判斷標準。這必須有科技防護配套與法律授權規定」[95]、「干預資訊系統的法律授權規定，不但應保護私人生活核心領域不受侵犯，其核准與否，原則上應採法官保留」[96]。

三、網路聊天平臺

㈠網路巡邏與加入聊天

第三種與秘密通訊自由有關的網路偵查是**網路聊天平臺**。網路世界提供各種聊天平臺，可能是特定主題論壇或社交網站，交流模式從純粹在網頁公開留言到與任何人即時交換資訊等等。而發言的資格，有的是開放網民路過留言，也有嚴格到驗證註冊身分才取得登入「會員」資格。但無論如何，除非個人自願或肉搜被迫曝光，否則網民多半使用偽名或代號行走於網路聊天平臺[97]。有心利用網路犯罪的人，例如常見的兜售毒品、散布色情，當然也清楚網路匿名性帶給他躲避追緝的優點。既然如此，偵查機關可否秘密監控聊

94 BBl 2013, 2807.

95 BVerfGE 120, 274, 309.

96 BVerfGE 120, 274, 331, 336.

97 實例如最高法院101年度台上字第1227號判決：「原判決已敘明吳○文化名『玟玟』，透過網路聊天室，以一天可賺取新台幣5千元至1萬元之報酬，邀約已滿18歲女子從事性交易工作，待相約見面後，上訴人及吳○文即提出性交易所得五五分帳，並供住宿等條件引誘之，並以吳○文承租之住處爲從事性交易女子之居住處所。吳○文再透過網路聊天室，招攬不特定男客，媒介與該女子從事性交易」。

天室談話？或者，可否如同在真實世界喬裝虛偽朋友般，在虛擬世界也裝扮成「虛偽網友」，透網路平臺蒐集資訊？換言之，在本文主題下，這又是一個檢驗需不需要法律干預授權的問題[98]。

網路聊天（室）的偵查行為有數種模式。一般認為[99]，警察在公開聊天平臺的**網路巡邏**（Streifenfahrt），例如在無登入帳號控管的網頁、部落格，或聊天室[100]，與真實世界的街頭巷坊巡邏並無二致。所以，在任何人皆得自由進出的公開論壇或網頁，網路巡邏無須特別干預授權，以**一般偵查條款**（例如我國刑事訴訟法第230條、第231條）為網路聊天的取證依據即足。相反的，如果是破解安全措施，入侵密閉的聊天室秘密監控，這時會與秘密通訊自由有關，則應符合通訊監察規定。不過，由於秘密通訊自由只在保障通訊雙方的秘密談話不受國家無權侵入，當國家成為通訊之一方而探知通訊內容時，該通訊則不受秘密通訊自由保護[101]。準此，假如密閉聊天室的聊天者（之一即可，通常是聊天室主人）邀請虛偽網

98 *Kudlich*, aaO. (Fn. 9), 566; *Rosengarte/Römer*, Der „virtuelle verdeckte Ermittler“ in sozialen Netzwerken und Internetboards, NJW 2012, 1764ff.; *Soiné*, Verdeckte Ermittler als Instrument zur Bekämpfung von Kinderpornographie im Internet, NStZ 2003, 225ff.

99 *Gless*, aaO. (Fn. 14), 15; *Klesczewski*, aaO. (Fn. 15), 739 u. 752; *Kudlich*, aaO. (Fn. 14), 199f.

100 實例如最高法院103年度台上字第869號判決：「呂○雪竟基於販賣第二級毒品甲基安非他命之營利意圖，於民國101年8月17日，在新北市○○區○○街○巷○號『百麗旅館』，上網至『UT網際空間北部人聊天室』，以『板橋府中誰要呼』之暱稱上線聊天，網路巡邏員警賴○融察覺有異，詢問：『安喔』、『找男生呼嗎』、『你即時通多少』等語，呂○雪回覆稱：『恩』、『你拿回去玩啦』，及雅虎奇摩即時通之帳號『aabbcc0000000』等語，員警以該即時通帳號聯絡，呂○雪稱：『你要？』、『要過來嗎？』、『3.5K』等語，並提供0000000000號行動電話供購買毒品聯絡之用。」

101 BGHSt 39, 335, 344.

友（警察）一對一或多人聊天，便與秘密通訊自由無涉[102]。

㈡網路臥底偵查

偵查機關匿名加入網路聊天，雖不涉及秘密通訊自由，但不排斥其他基本權的審查，除了警察喬裝引誘自白的傳統爭議外[103]，尤其是人格權中的**資訊隱私權或自我言語權**（Recht am eigenen Wort）[104]。自我言語權是一種對自己言語之人格權，乃屬一般人格權中的自我表達權（Recht der Selbstdarstellung），在刑事訴訟法脈絡下，自我言語權是私人秘密電話錄音或得通訊一方同意之監聽的常見法律爭點[105]。德國聯邦最高法院早在一九六〇年的BGHSt 14, 358（私人錄音案）即表示：「**個人言語權在今日也屬於一般人格權之內涵**。說話者的人格透過其思想上的對外陳述而傳達出來，雖然有時須視其陳述內容而定（或多或少），但絕對是以聲音作為個人標誌。準此，對於誰可以聽取他說話，以及說話內容是否可被保存或由聽取者隨記憶流逝，乃是由說話者自己決定，且是獨自決定。因而，說話者的言語與聲音可否記錄在錄音帶或其他聲音載

102 BVerfGE 120, 274, 341; vgl. *Klesczewski*, aaO. (Fn. 15), 753.

103 所涉爭議，主要是有無違反緘默權告知義務與禁止詐欺訊問。實例如最高法院103年度台上字第2147號判決：「證人即警員林○男之證述，上訴人與林○男間之通訊監察譯文、上訴人與王○明間網路通訊軟體對話內容等證據，詳爲說明上訴人有原判決事實欄所載之先在網路聊天室用『高雄→煙可幫』暱稱吸引有意購買毒品者，警員林○男乃喬裝欲購買甲基安非他命，上訴人即報價並約林○男試用毒品，嗣上訴人再以通訊軟體與王○明聯絡，由王○明帶一包甲基安非他命前來」。新近討論，如王士帆，警察喬裝誘話與一般偵查條款——德國聯邦最高法院刑事裁判BGHSt 55, 138譯介（上／下），司法周刊，1714/1745期，版2-3/3，2014年9月19/26日。

104 *Pieroth/Schlink/Kingreen/Poscher*, aaO. (Fn. 24), Rn. 376 und 846.

105 自我言語權在刑事訴訟法基本權干預之審查方面，可參見林鈺雄，同註19，頁324。

體，以及其言語與聲音可否用這些紀錄載具再次播放和對誰播放，也全都保留給說話者單獨決定」[106]。

網路聊天者因信賴虛偽網友而洩漏個人資料，然網路世界虛虛實實，德國聯邦憲法法院認為對「網友」身分之信賴，一般而言並不值得保護，也就是不構成資訊自決權之干預[107]。可是，如果驗證註冊會員的身分控管越嚴格、臥底時間越長，以及越是主動參與聊天以求達到偵查取證目的之網路聊天，對被告或第三人的隱私權或資訊自主權的干預可能就越深。以德國法及瑞士法為例，此時不但應該且只能發動「臥底偵查」這種強制處分（德國：§§ 110a ff. StPO；瑞士：Art. 285a ff. StPO）[108]。

以驗證申請會員真實身分為例，例如跨國犯罪組織經營的情色、賭博網站要求登入者必須輸入身分證字號與手機回訊查證[109]，這就需要核准虛擬身分（Legende）的臥底偵查。理由其實不難理解，所謂提供網路聊天室驗證為真的「虛擬身分」，不是隨意捏造暱稱這麼單純，而是涉及偽造、變造可得進行法律行為的身分資料，連審理交易糾紛的民事法院都可被臥底偵查的虛擬身分蒙

106 BGHSt 14, 358, 359f.。值得一提者，「**不計代價之發現真實，向來並非刑事訴訟法之基本原則**」正是出於BGHSt 14, 358，其介紹可參見王士帆，禁止不計代價發現真實與私人不法取證——德國聯邦最高法院刑事裁判BGHSt 14, 358譯介，司法周刊，1599期，版2-3，2012年6月21日。

107 BVerfGE 120, 274, 345.

108 *Gless*, aaO. (Fn. 14), 15f.; *Kudlich*, aaO. (Fn. 9), 566; *Marberth-Kubicki*, aaO. (Fn. 7), Rn. 529ff.; *Rosengarte/Römer*, aaO. (Fn. 98), 1767。有認爲德國《刑事訴訟法》1992年新增的臥底條款並未涵蓋數位時代的網路臥底，故應制定新的授權基礎：*Roggan*, aaO. (Fn. 14), 1996.

109 目前申辦手機門號（含超商購買易付卡），也需臨櫃提供有效雙證件查驗，如身分證、健保卡或駕照等。因而，知悉登記在網頁會員的手機門號，即可調查門號使用者的真實身分，但這當然要符合《通保法》第11條之1的調取規定。

蔽[110]。光想想，要持有雙證件才能購買手機門號、有手機門號才能讓聊天網站查驗、查驗成功始能進入會員管制的聊天室，一環扣一環，自以為聊天室已嚴格過濾身分的會員，如何料到層層把關後的匿名網友竟是偽造雙證件的警察呢？因此，長期臥底計畫、使用偽造之虛擬身分，需另有特別的干預授權基礎，在我國現行法並無臥底條款的特別立法下，結論就是違法取證。

上述網路聊天區分不同干預授權依據的標準，免不了出現模糊地帶，甚至有認為主動與被鎖定者接觸的網路聊天就應遵守臥底偵查條款[111]。干預授權內容模糊是一般偵查條款本身的固有問題[112]，面對新興科技與其所涉及的基本權界定尤其如此。但模糊絕不是無庸區分、甚至放棄特別干預授權的正當理由，至少在所侵犯者乃是立法者或釋憲機關承認的基本權清單時，一般偵查條款即顯不足[113]。如何對網路聊天室之秘密偵查作出更細緻化的評價，既是國內外實務[114]、也是學界仍待深入的課題。

110 *Meyer-Goßner/Schmitt*, aaO. (Fn. 60), § 110a Rn. 7; SSW-StPO/*Eschelbach*, 2014, § 110a Rn. 7.

111 *Gless*, aaO. (Fn. 14), 15.

112 關此，可參見林鈺雄，干預保留與門檻理論——司法警察（官）一般調查權限之理論檢討，政大法學評論，96期，頁189以下，2007年4月。另比較薛智仁，司法警察之偵查概括條款？——評最高法院102年度台上字第3522號判決，月旦法學雜誌，235期，頁235以下，2014年12月。

113 具體判斷類型及舉例，參見林鈺雄，同前註，頁217-221。

114 德國實例，如BGHSt 41, 42; 41, 64。瑞士實例，可參考瑞士聯邦法院：BGer, Strafrechtliche Abteilung, Urt. v. 08.03.2010 – 6B_743/2009. Dazu Anm. *Gless*, forumpoenale 2010, S. 2ff.

肆、網路「搜索」脈絡下的網路偵查

接下來要討論網路搜索脈絡下的網路偵查：雲端搜索和秘密線上搜索。應先說明兩點：第一，所謂網路搜索，不是指偵查機關利用搜尋引擎網站進行「網路搜尋」，後者屬於上述網路巡邏的一種偵查型態[115]。第二，技術上來看，不論雲端搜索與秘密線上搜索，兩者都必須網路連線始能為之，且都以搜尋可為證據的電磁紀錄為目的；惟前者是法律定義的公開搜索，後者則是間諜程式自動、秘密刺探電腦資料。因此，正確來說，秘密線上搜索是偷植木馬、後門程式（Trojaner- und Backdoor-Programm），這完全不符合刑事訴訟法理解的「搜索」[116]，但鑑於德國相沿成習，本文從之[117]。

一、雲端「搜索」

㈠保全雲端儲存資料

「你今天雲端了嗎？」雲端運算（Cloud Computing），不只是我們今日或視或聽的科技詞彙，實際生活也享受雲端運算之便利，如果每天脫離不了網路的話。舉例來說，Google Chrome瀏覽器使用者一定能體會雲端運算的方便性：在自己電腦的Chrome瀏覽器編輯常用網頁「書籤」，即便借用他人網路裝置上網，一樣可藉由輸入自己的Gmail帳號、密碼，登入帶有自己書籤的Chrome瀏覽器。Google網頁描述說「可在不同的裝置間切換，作業不中

115 參見本文參、三、㈠。

116 *Fezer*, Anm. zu BGHSt 51, 211, NStZ 2007, 535; *Malek/Popp*, Strafsachen im Internet, 2. Aufl., 2015, Rn. 485.

117 德國文獻另有其他少數幾種稱法，參見何賴傑，同註28，頁233-234。

斷」，十分貼切。這種把慣用軟體帶著走的行動性，某程度實現「整個網路就是我的電腦」的想像[118]。

雲端運算具有集中運算資源、隨選服務、動態配置運算資源等特色，利用其提供的硬體設備，為雲端使用者提供儲存、程式運用、網路平台部署等。以**雲端儲存**（Cloud-Storage）來說，使用者所需資訊儲存於與網路連結的雲端伺服器，不論身在何處，均可以網路存取雲端儲存資料。雲端運算近年來成為各國積極推動的科技產業，相關法律探討如雨後春筍，涵蓋資訊安全、個資保護、著作權等等面向[119]。在刑事法領域亦（應）不例外，**雲端偵查**（Ermittlung in der Cloud）正為刑事追訴帶來新挑戰[120]。

於此，與刑事訴訟偵查措施較有密切關聯性的是雲端儲存。雲端儲存這種電腦服務的「外包」（Outsourcing）型態，將可為證據的檔案散存在分散系統，不但可能儲存在不同的雲端提供者，也可能在不同國家。面對雲端儲存，偵查機關關心的是：當搜索被告電腦，發現應扣押之物存放在網路連結的雲端硬碟時，可否依搜索扣押規定加以保全？還是說，這又是一個因科技造成的欠缺干預授權之例？

---

118 「網路就是電腦」（The Network Is The Computer）是美國Sun Microsystems公司於1980年代提出的宣傳口號，該公司於2010年正式被甲骨文公司併購（http://www.oracle.com/us/sun/index.html，最後瀏覽日：2015年12月10日）。

119 討論文獻如李治安，當法律漫步在雲端，法學新論，25期，頁49以下，2010年8月；張乃文，雲端運算環境之法規遵循議題剖析，科技法律透析，25卷7期，頁21以下，2013年7月；劉定基，雲端運算與個人資料保護——以台灣個人資料保護法與歐盟個人資料保護指令的比較爲中心，東海大學法學研究，43期，頁53以下，2014年8月。

120 問題概覽，可參閱*Obenhaus*, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, 651ff.

㈡德國立法模式：德國《刑事訴訟法》第110條第3項

被告將檔案儲存在雲端，自然要承擔資訊安全破功的洩漏風險，這包含偵查機關逕自找上雲端儲存地的業者，直接發動搜索、扣押，業者也多半沒有迅速銷毀被告雲端檔案或隱匿的動機[121]。然而，如果搜索被告電腦發現雲端硬碟，偵查機關可以「點」或「滑」進去嗎？這個小動作之所以成為法律問題，原因在於雲端硬碟並不是安裝在受搜索客體的電腦主機裡，而是在與該受搜索物件空間隔離的一處伺服器上。簡單說，由於搜索票上記載的應受搜索物為電腦主機，雲端硬碟既非受搜索物，而且，如將受搜索物侷限於實體物的話，雲端硬碟這種虛擬空間，亦不得搜索。為幫偵查機關解套，二〇〇八年德國立法者在其《刑事訴訟法》第110條執行搜索之**文件檢閱**（Durchsicht von Papieren）規定增訂第3項。

何謂執行搜索之文件檢閱？依德國法而言[122]，文件檢閱是決定扣押前的搜索執行動作之一，目的在檢查所發現文件的證據適格（Beweisgeeignetheit）。亦即，檢查、翻閱系爭文件是否為應扣押物，如果肯定，即行扣押，否則應發還持有人。當然，假如偵查機關自始知悉或從外觀判斷出是不得扣押的文件（例如公務秘密、職業秘密之文書），既然本來就不可扣押，自也不得檢閱。執行搜索發現的「文件」，只有檢察官或其授權的偵查人員才有權檢閱（§ 110 I StPO），其他執行人員除非事先獲得持有人同意其檢閱，否則，應在持有人面前以官章封緘該文件並交予檢察官（§ 110 II StPO）。

德國法認為，允許檢閱的「文件」指所有具有思想內涵的客

121 *Kudlich*, aaO. (Fn. 9), 565.

122 *Herrmann/Soiné*, Durchsuchung personlicher Datenspeicher und Grundrechtsschutz, NJW 2011, 2925; SSW-StPO/*Hadamitzky*, 2014, § 110 Rn. 1ff.

體，也包含數位資料載體或儲存裝置上具有可讀性的電磁紀錄，例如筆電或智慧型手機內的影音、文字檔[123]。雲端運算時代對電磁紀錄的檢閱也有影響，問題就是前述的例子：如果搜索被告電腦才發現欲保全的電磁紀錄，乃存放在與該電腦連結的內網伺服器或外網的雲端硬碟，那還可否檢閱？[124]德國為此——同時為配合《網路犯罪公約》（Cyber-crime Convention）第19條第2項要求[125]——而修法（§ 110 III StPO），將偵查機關之檢閱範圍延伸至電子儲存媒介物，亦即，當透過系爭媒介物可進入另一與之「空間分離的儲存媒介」（räumlich getrennte Speichermedien），且所搜索之資料有遺失之虞時，該「空間分離的儲存媒介」也在檢閱範圍（§ 110 III S. 1 StPO）。遇有輸入帳號、密碼始能登入的情形，偵查機關亦得「破解」，這類似於為執行搜索而行使直接強制力[126]。檢閱遠端儲存之電磁紀錄後，發現具有調查重要性者，則應予保全（§ 110 III S. 2 StPO）。如此一來，「搜索客體只限於實體物」的傳統說法，已被德國法揚棄[127]。延伸檢閱後，倘發現為應保全之物，例如在服務提供者郵箱伺服器內已被收信人讀取的電子郵件（含夾帶的附件），通常由偵查機關複製、儲存帶走[128]，而非像扣押主

123 *Roxin/Schünemann*, aaO. (Fn. 17), § 35 Rn. 14; *Schlegel*, aaO. (Fn. 59), 24; SSW-StPO/*Hadamitzky*, 2014, § 110 Rn. 10.

124 如所發現遠端資料是正在進行中的通訊，例如Email，則應回歸通訊監察規定，參見本文參、一、㈡。

125 *Bär*, Transnationaler Zugriff auf Computerdaten, ZIS 2011, 54.

126 *Meyer-Goßner/Schmitt*, aaO. (Fn. 60), § 105 Rn. 13; *Obenhaus*, aaO. (Fn. 120), 653。我國法可參考《刑事訴訟法》第144條第1項「因搜索及扣押得開啓鎖扃、封緘或爲**其他必要之處分**」，亦有認爲此規定可作爲破解所扣押硬碟的防密措施，如王銘勇，同註45，頁53-54。

127 *Schlegel*, aaO. (Fn. 59), 25.

128 *Kindhäuser*, aaO. (Fn. 59), Rn. 148; *Meyer-Goßner/Schmitt*, aaO. (Fn. 60), § 110

機硬碟一樣扣押「雲端」，實際上也不可能從被告個人電腦去扣押連結的雲端硬碟。總而言之，依德國法，遠端儲存設備也在搜索票的搜索效力所及，某程度可說是真正的「線上搜索」[129]。於此，由於回歸搜索相關規定，偵查機關自應遵守包含搜索扣押必須具體特定、明確之要求，以避免釣魚搜索[130]。

這種遠端獲取的立法干預授權，在今日無線儲存裝置普及的情形，例如無線硬碟、WiFi記憶卡，都可派上用場。而更典型之例，當然是前述的網路儲存空間。但應注意，由於一國立法者只能授權於本國內的高權干預行為，偵查機關檢閱的延伸範圍僅限於存放在本國領域內的伺服器，諸如本國公務機關、企業，或學校內網的郵箱伺服器；一旦伺服器設置在外國，則只能循司法互助途徑解決，否則會引發干預他國主權的國際法紛爭[131]。從這一點，也可預期雲端運算必定帶給刑事偵查的網路無國界難題：當資料使用者將資料分散在各種雲端儲存提供者的不同空間時，光是前階段的「查明」資料實際儲存地就已棘手，甚至連雲端使用者對雲端實際伺服器位置通常都毫無所悉。以Line為例，其資訊處理和儲存的伺服

---

129 Rn. 6; *Obenhaus*, aaO. (Fn. 120), 652; SSW-StPO/*Hadamitzky*, 2014, § 110 Rn. 22. *Herrmann/Soiné*, aaO. (Fn. 122), 2925.

130 關於搜索明確性，參見如朱石炎，刑事訴訟法論，頁130，2015年8月，5版。我國實務見解如最高法院100年度台上字第5065號判決：「刑事訴訟法第128條第2項明文列舉搜索票法定必要之應記載事項，此據以規範搜索票之應記載事項者，即學理上所謂『概括搜索票禁止原則』。其第2款『應扣押之物』，必須事先加以合理的具體特定與明示，方符明確界定搜索之對象與範圍之要求，以避免搜索扣押被濫用，而違反一般性（或稱釣魚式）搜索之禁止原則」。

131 *Bär*, aaO. (Fn. 125), 54f.; *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn 791; *Kudlich*, aaO. (Fn. 9), 566; *Meyer-Goßner/Schmitt*, aaO. (Fn. 60), § 110 Rn. 22; SSW-StPO/*Hadamitzky*, 2014, § 110 Rn. 22.

器，「可能位於世界上其他國家」，「透過繼續使用我們的服務，即視為您同意您的資訊可能被跨國傳輸，同意Line在您的資訊提交國之外的某個國家處理及儲存您的資訊」[132]。即便查得一清二楚，後端還有各國刑法適用法競合衍生的管轄權衝突等著本國司法單位協調。

㈢我國法之搜索「電磁紀錄」

德國法的遠端搜索規定，授權偵查機關的搜索延伸到與應搜索物網路連結的雲端硬碟。這對我國法因應雲端搜索的實務需求頗有啟發。我國立法者當然可以仿照德國立法，以求干預規範明確。但在此之前，不妨先思考我國《刑事訴訟法》第122條允許的搜索「電磁紀錄」，可否作為搜索電腦連結雲端的干預授權。

電磁紀錄，「謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄」（參見刑法第10條第6項）。二〇〇一年我國《刑事訴訟法》第122條將「電磁紀錄」增列為搜索對象。實體的資料儲存媒介物，例如硬碟、隨身碟，本來就可成為搜索的「物件」，以求發現被告儲存其中的「電磁紀錄」。單就此點而言，增列電磁紀錄似乎疊床架屋[133]。惟從另一角度來看，德國法因應網路社會創設的搜索「空間分離的儲存媒介物」規定，在我國法卻（也許意外）無此立法迫切性。理由是，我國搜索「電磁紀錄」的立法干預授權，已能讓搜索涵蓋到與個人電腦、行動裝置等

132 出自Line隱私政策（http://terms.line.me/line_rules/?lang=zh-hant，最後瀏覽日：2015年12月10日）。又，單單在2010年Google雲端運算中心在全球至少有12個，其中約有1百萬台伺服器同時運行，參見李治安，同註119，頁55。

133 林鈺雄，同註19，頁413：「若是電磁紀錄存在於某個實體之『物』（例如電腦硬碟或隨身碟）者，本來就可被『物件』的概念所包含」。

空間相隔、卻又因網路相連的其他儲存媒介上之電磁紀錄[134]。不過，如前所述，鑑於不干涉外國主權原則，偵查機關此時的搜索延伸範圍，只限於位在本國領域內的儲存媒介上之電磁紀錄。此外，既然是依搜索規定為之，自應遵守搜索相關規定，例如基於搜索票記載明確性，應記明雲端儲存空間為應受搜索之電磁紀錄（參照刑事訴訟法第128條第2項第3款）。

二、秘密線上搜索（verdeckte Online-Durchsuchung）

㈠定　義

電腦硬碟內的電磁紀錄，可以依傳統的扣押方式保全，亦即扣押儲存載體，惟應注意比例原則[135]。另一種非傳統的保全方式，是德國法所稱的「**秘密線上搜索**」。

秘密線上搜索，是指偵查機關變成國家駭客，傳輸、安裝木馬程式或後門程式到被告的個人資訊系統（電腦、行動裝置等），例如寄發夾帶木馬的電子郵件給被告，或者利用送廠維修、海關檢查時偷偷安裝。惡意程式會對資訊系統的儲存資料進行「搜索／搜尋」，只要被告用該中毒電腦上網，惡意程式所搜尋的資料會秘密複製、傳送到偵查機關手上[136]。如果依然不能想像秘密線上搜索的破壞力，那來看一則「德國之聲」（Deutsche Welle）二〇一四年十一月二十四日的報導[137]：

---

134 另參見黃朝義，同註47，頁238：「將搜索之客體擴及於『電磁紀錄』，直接將以往之概念加以擴及至『無體物』搜索」。

135 參見本文參、一、㈠。

136 德國文獻定義大同小異，僅見*Beulke*, aaO. (Fn. 67), Rn. 253c; *Kudlich*, aaO. (Fn. 9), 564; *Valerius*, aaO. (Fn. 14), 276.

137 http://www.dw.de/hochkomplexer-spionage-trojaner-entdeckt/a-18082441 ， 最 後瀏覽日：2015年12月10日。

「資訊科技安全公司發現一個名為Regin的精密間諜木馬程式，它已監控全球各地企業與政府部門多年。專家表示，這個新發現的木馬程式可能出自情報機關之手，因為設計極為複雜——Regin會秘密侵入被鎖定者的電腦中長期潛伏，可隨監控者指令，自行截取電腦螢幕畫面、盜取密碼、監視資料流通（含獲取通訊紀錄），甚至重製已被電腦使用者刪除的檔案。」

㈡探求刑事訴訟之干預授權

德國聯邦檢察總長曾為一起恐怖組織罪名，以搜索、扣押結合電信監聽、住宅監聽等干預要件，聲請法院核准發動線上秘密搜索。二〇〇七年德國聯邦最高法院最終裁定駁回檢察總長的聲請，此裁判即BGHSt 51, 211[138]。目前為止，德國學說與實務普遍接受BGHSt 51, 211觀點，均認秘密線上搜索因現行法尚乏干預授權依據，故不得為之[139]。BGHSt 51, 211受到學者正面肯定[140]，實無庸本文錦上添花，以下僅列出其中三個關鍵的基本權干預審查項目及理由：

1. 秘密線上搜索並非刑事訴訟之搜索

「刑事訴訟法合法搜索的圖像，乃是偵查人員親身出現在搜索地點以及公開偵查」[141]。偵查機關於執行搜索時應讓特定人在場

138 BGH, Beschl. v. 31.01.2007 – StB 18/06。本則裁判之介紹，參見王士帆，偵查機關木馬程式：秘密線上搜索——德國聯邦最高法院刑事裁判BGHSt 51, 211譯介，司法周刊，1779期，版2-3，2015年12月25日；何賴傑，同註28，頁236。

139 *Hilgendorf/Valerius*, aaO. (Fn. 7), Rn. 796f.; *Kudlich*, aaO. (Fn. 9), 564; *Roxin/Schünemann*, aaO. (Fn. 17), § 35 Rn. 2; *Volk/Engländer*, aaO. (Fn. 67), Rn. 56a.

140 如*Beulke*, aaO. (Fn. 67), Rn. 253c; *Kudlich*, aaO. (Fn. 14), 193.

141 BGHSt 51, 211, 212 Rn. 5.

（§§ 105 II, 106 I StPO）。搜索在場規定乃在課予偵查機關義務。此外，受搜索人於搜索執行完畢後，得請求發給搜索證明；受搜索人欲做此請求的前提，是即時通知其有進行搜索。此條文用意，在保障受搜索人得直接於搜索完畢後知悉搜索理由，藉此獲得審查搜索合法性的機會，必要時可請求事後之權利救濟[142]。再者，相較於刑事訴訟法的公開搜索，任何秘密搜索基於本身所升高之干預強度，乃成為一種具有獨立新性質的強制處分。公開執行搜索時，視個案之情形，受干預者可能主動交付搜索標的，以避免被搜索，甚至當欠缺搜索要件時，受搜索人可阻止搜索。然而，秘密搜索卻使被告失去這些防禦可能性[143]。

2. 線上秘密搜索不是通訊監察[144]

藉電腦病毒將應受搜索之電腦資料傳送給偵查機關時，雖然電腦使用者必須在「線上」，以致這些被傳送的資料本來就是原有網路資料串流的一部分。不過，此情形不會使秘密線上搜索變成電信通訊，因為此時並非監察被告與他人之間的通訊，而是：為了找尋證據或其他可能之偵查線索，偵查機關刻意鎖定特定電腦，在電腦開始通訊之前，即啟動所儲存的電腦資料傳輸至偵查單位。因此，電腦「上線」狀態中的資料流（Datenfluss）僅是基於科技理由而被利用來傳送放置於儲存媒介的資料。

3. 否定混合各別干預授權基礎的合併觀察（Zusammenschau）[145]

即便於符合一般搜索要件之外，另外還具備通訊監察與住宅監聽（§§ 100a, 100c StPO）規定的高度干預要件，例如存在重罪嫌

142 BGHSt 51, 211, 213 Rn. 6.
143 BGHSt 51, 211, 215 Rn. 10.
144 BGHSt 51, 211, 217f. Rn. 18.
145 BGHSt 51, 211, 218f. Rn. 22.

疑、補充性原則，而且「特別」謹慎地遵守比例原則，偵查機關仍不得實施秘密線上搜索。為了創設一個科技上可能進行之新偵查措施的法律干預基礎，而合併某些干預授權規定的個別要素，乃於法不合。如此作法，將牴觸干預基本權之法律保留原則。比例原則在個案上雖可限制法定干預權限，但終究不能取代一個並不存在的干預授權基礎。

㈢未來立法可能性

總言之，依德國刑事訴訟法，秘密線上搜索欠缺干預授權規定。不過，就跟來源端電信監察（Qullen-TKÜ）一樣[146]，不表示未來不得制定干預授權基礎。當然，社會氛圍是否允許這種對個人電腦資料——如同個人資料庫——一網打盡地刺探，有待新干預條款的基本權保障密度而定。

對此，重要的立法風向球與指標是二〇〇八年德國聯邦憲法法院創設IT基本權的裁判[147]。其強調：只要有事實依據顯示，對重要優越利益（生命、身體、自由，及為避免危害國家存續等公共利益）存在具體危害，且未來有即將發生此等危害的高度可能性時，在符合法官保留及私人生活核心領域有防護措施之下，立法者得准許秘密線上搜索[148]。德國聯邦立法者接獲聯邦憲法法院的「提醒」，同年底即依憲法法院意旨，在《聯邦刑事警察局與聯邦與各邦刑事事件合作法》（Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, BKAG）制定針對恐怖主義的危險預防性之秘密

146 參見本文參、二、㈢。
147 參見本文貳、一、㈡。
148 BVerfGE 120, 274。關此介紹，參見何賴傑，同註28，頁236-238。

線上監控條款（§ 20k BKAG），即允許聯邦刑事局（Bundeskriminalamt）為防止國際恐怖主義之危害，得實施線上搜索，利用科技工具秘密侵入人民資訊設備內從中蒐集資訊。該法於二〇〇九年生效後，各邦加緊立法的進度也不遑多讓[149]。德國未來如要制定刑事追訴層次的秘密線上搜索，至少應符合聯邦憲法法院前述要求[150]。

伍、結　論

網路之刑事追訴，正是科技與法律的一種較勁。科技固然一日千里，但刑事訴訟網路偵查措施，不管是多精密的技術，終究應回歸基本權干預的審查體系。就此而言，瞬息萬變的科技是領先了緩動的法律條文，不過，保護人民基本權的法律理念始終支配科技。偵查機關進行網路偵查，應注意其對人民基本權的干預可能性。網路偵查——視型態而定——所涉及的，不只傳統基本權，如秘密通訊自由與人格權，還可能包括德國聯邦憲法法院因應網路時代創設的IT基本權（即「秘密通訊自由的保障範圍並未包含資訊系統的私密性與完整性」）。無論如何，網路偵查一旦干預人民基本權，根據法律保留原則，該措施必須在現行刑事訴訟法事先取得干預授權基礎，始得為之，否則就是違法取證。**探求現行法是否有適當的干預授權基礎**，成為網路之刑事追訴的首要課題（本文貳）。

網路是一種對外聯繫工具，網路偵查與秘密通訊自由之緊張關係首當其衝。相關的網路偵查手段，以保全電子郵件、監控網路電話和網路聊天室為大宗。**保全電子郵件**，應以郵件是否屬於**秘密通**

149 *Kudlich*, aaO. (Fn. 9), 564 Fn. 44。關於德國邦層次的警察預防性線上搜索規定，可參見謝碩駿，同註28，頁5-7。

150 *Kudlich*, aaO. (Fn. 14), 204; *derselb.*, aaO. (Fn. 9), 564.

訊自由之保護範圍區分保全措施，所涉基本權不同，干預手段自不同，授權基礎亦有別。在不受秘密通訊自由保護的電子郵件，例如尚未傳送或通訊已結束的電子郵件，以搜索扣押儲存載體為主，但應注意執行之比例原則。至於監控即時通訊中的電子郵件，由於正是秘密通訊自由保障的通訊活動，故應以通訊監察規定為之。**監控網路電話**方面，以Skype為例，礙於去中央化的封包加密技術，目前技術上只能在用戶端安裝側錄軟體記錄未加密或已解密的資訊內容，再秘密線上傳輸給偵查機關。這種**來源端電信監察**（Qullen-TKÜ）的偵查手段，由於有科技濫用疑慮，至少現行法查無充分的干預授權依據。至於**網路聊天平臺**的偵查，型態可能是網路巡邏、秘密刺探密閉談話內容，或網路臥底偵查，各自適用不同干預授權基礎（本文參）。

「網路搜索」脈絡下的網路偵查，指雲端搜索和秘密線上搜索。**雲端搜索**是針對雲端運算而來，尤其是與個人網路設備連結的雲端硬碟。於此，為滿足干預規範明確性，可考慮增訂類似德國法的遠端搜索（§ 110 III StPO），亦即，當搜索電腦等資料儲存媒介物，發現可透過其進入一與之「空間分離的儲存媒介」（räumlich getrennte Speichermedien），且所應搜索資料有遺失之虞時，該「空間分離的儲存媒介」也在搜索範圍內。然在立法之前，不妨先思考我國《刑事訴訟法》第122條允許的搜索「電磁紀錄」，可否作為搜索電腦連結雲端的干預授權。至於德國所稱的**秘密線上搜索**（verdeckte Online-Durchsuchung），是一種顛覆性的新網路偵查手法，簡言之，即偵查機關成為國家駭客，在個人電腦設備輸入木馬程式等惡意軟體，監控或掌控電腦活動。德國聯邦最高法院BGHSt 51, 211認為秘密線上搜索於現行法並無干預授權依據，既非刑事訴訟理解的搜索，亦非通訊監察。不過，就與來源端電信監察一樣，德國未來是否允許這種對個人電腦資料一網打盡之刺探，有待新干

預條款的基本權保障密度而定。對此，重要的立法方向指引是二〇〇八年德國聯邦憲法法院創設IT基本權的裁判（本文肆）。

資訊科技確實帶給刑事法多方面挑戰。再以德國法為例，其網路科技偵查的焦點是**E-隱私領域**（e-Sphäre）的偵查干預正當性，而審判法庭的重頭戲是**E-刑事司法**（e-criminal-justice）[151]。如何享受科技之便，同時又能維護法律原則或理念，實有賴各法律領域集思廣益[152]。至於作為本文主題的網路之刑事追訴，刑法學（Strafrechtswissenschaft）的任務應該是怎樣的圖像呢？謹以瑞士Gless教授的一段話代答[153]：**「刑法學的任務是研究機關實務、新立法草案與現行法對刑事程序的影響，當刑事程序根深蒂固的基本原則被一點一滴侵蝕時，還要挺身異議。任何強制處分都需要法律授權基礎，即是其中一個基本原則。」**

---

151 德國聯邦司法暨消費者保護部（Bundesministerium der Justiz und für Verbraucherschutz）以刑事司法現代化、數位化爲目標，2012年公布《刑事電子文書草案》（Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen），有意將刑事程序的文書、訴訟及證據調查電子化（2014年10月版草案：http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RefE_ElektronAkteStrafsachen.pdf?__blob=publicationFile，最後瀏覽日：2015年12月10日）。

152 蔡志方，同註8，頁15：「當今之科技法規，在屬性上亦呈現其多元、不統一之特色，乃顯而易見者。準此，科技法之研究洵有賴於公法、民法、刑法與基礎法學者共同黽勉從事」。

153 *Gless*, aaO. (Fn. 14), 22.

參考文獻

一、中　文

1. Helmut Satzger著，王士帆譯，國際刑法與歐洲刑法，2014年4月。
2. 王士帆，全新刑事訴訟法典——瑞士刑訴改革與整合，政大法學評論，118期，頁105-163，2010年12月。
3. 王士帆，禁止不計代價發現真實與私人不法取證——德國聯邦最高法院刑事裁判BGHSt 14, 358譯介，司法周刊，1599期，版2-3，2012年6月。
4. 王士帆，警察喬裝誘話與一般偵查條款——德國聯邦最高法院刑事裁判BGHSt 55, 138譯介（上／下），司法周刊，1714/1745期，版2-3/3，2014年9月。
5. 王士帆，偵查機關木馬程式：秘密線上搜索——德國聯邦最高法院刑事裁判BGHSt 51, 211譯介，司法周刊，1779期，版2-3，2015年12月。
6. 王勁力，電腦網路犯罪偵查之數位證據探究，檢察新論，13期，頁13-28，2013年1月。
7. 王效文，網際網路犯罪與內國刑法之適用，載：民主・人權・正義——蘇俊雄教授七秩華誕祝壽論文集，頁251-273，2005年9月。
8. 王銘勇，網路犯罪之搜索與扣押，法學叢刊，191期，頁45-62，2003年7月。
9. 石世豪，電信自由化之下通訊安全規範的轉型趨勢——通信秘密、個人資料保護與電信事業的管制變革，全國律師，9卷5期，頁1-20，2005年5月。
10. 朱石炎，刑事訴訟法論，5版，2015年8月。
11. 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，208期，頁230-244，2012年9月。
12. 李志仁，電信資訊匯流下之法律爭議——以Skype為例，科技法律透析，18卷12期，頁43-62，2006年12月。
13. 李佳玟，程序正義的鋼索，2014年6月。
14. 李治安，當法律漫步在雲端，法學新論，25期，頁49-65，2010年8月。
15. 李榮耕，電磁紀錄的搜索及扣押，國立臺灣大學法學論叢，41卷3期，頁

1055-1115，2012年9月。
16.李榮耕，簡評2014年新修正的通訊保障及監察法——一次不知所為何來的修法，月旦法學雜誌，227期，頁148-175，2014年4月。
17.李震山，挪動通訊保障與通訊監察天平上的法碼——釋字第631號解釋評析，台灣本土法學雜誌，98期，頁283-291，2007年9月。
18.林鈺雄，干預保留與門檻理論——司法警察（官）一般調查權限之理論檢討，政大法學評論，96期，頁189-231，2007年4月。
19.林鈺雄，刑事訴訟法（上）——總論篇，7版，2013年9月。
20.林鈺雄，通訊監察之修法芻議——通訊保障及監察法之部分修正條文，萬國法律，192期，頁25-39，2013年12月。
21.徐育安，資訊風險與刑事立法，臺北大學法學論叢，91期，頁113-167，2014年9月。
22.張乃文，雲端運算環境之法規遵循議題剖析，科技法律透析，25卷7期，頁21-40，2013年7月。
23.張麗卿，通訊保障及監察法之修正與評析，月旦法學雜誌，229期，頁25-45，2014年6月。
24.許恒達，通訊隱私與刑法規制——論「通訊保障及監察法」的刑事責任，東吳法律學報，21卷3期，頁109-158，2010年1月。
25.陳重言，刑事追訴目的之通信（通聯）紀錄調取與使用——兼評2014年初通保修法，檢察新論，16期，頁40-59，2014年7月。
26.陳運財，偵查與人權，2014年4月。
27.馮震宇，網路犯罪與網路犯罪公約（上／下），月旦法學教室，4/5期，頁124-136/115-124，2003年2/3月。
28.黃朝義，刑事訴訟法，4版，2014年9月。
29.廖宗聖、鄭心翰，從網路犯罪公約談我國妨害電腦使用罪章的修訂，科技法學評論，7卷2期，頁57-89，2010年12月。
30.劉定基，雲端運算與個人資料保護——以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究，43期，頁53-106，2014年8月。
31.蔡志方，科技法律之概念與衍生之問題，載：城仲模教授七秩華誕祝壽論文

集第二冊（行政法總論篇），頁1-68，2008年10月。

32.蔡蕙芳，妨害電腦使用罪章：第一講：保護法益與規範功能，月旦法學教室，126期，頁62-72，2013年4月。

33.薛智仁，「網路釣魚」的刑事責任，東吳法律學報，24卷3期，頁149-184，2013年1月。

34.薛智仁，司法警察之偵查概括條款？——評最高法院102年度台上字第3522號判決，月旦法學雜誌，235期，頁235-256，2014年12月。

35.謝碩駿，警察機關的駭客任務——論線上搜索在警察法領域內實施的法律問題，臺北大學法學論叢，93期，頁1-78，2015年3月。

二、外　文

1. *Bär*, *Wolfgang*, Transnationaler Zugriff auf Computerdaten, ZIS 2011, S. 53ff.

2. *Beulke*, *Wener/Meininghaus*, *Florian*, Anm. zu BGH Ermittlungsrichter, Beschl. v. 21.02.2006 – 3 BGs 31/06, StV 2007, S. 63ff.

3. *Beulke*, *Werner*, Strafprozessrecht, 12. Aufl., 2012.

4. *Bode*, *Thomas*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, 2012.

5. *Buermeyer*, *Ulf*, Zum Begriff der „laufenden Kommunikation“ bei der Qullen-Telekommunikationsüberwachung („Qullen-TKÜ“) – Ein Beitrag zu den gebotenen legislativen Konsequenzen aus der Online-Durchsuchungs-Entscheidung des BVerfG, StV 2013, S. 470ff.

6. *Fezer*, *Gerhard*, Anm. zu BGHSt 51, 211, NStZ 2007, S. 535ff.

7. *Gercke*, *Marco/Brunst*, *Phillip*, Praxishandbuch Internetstrafrecht, 1. Aufl., 2009.

8. *Gless*, *Sabine*, Anm. zu BG, Strafrechtliche Abteilung, Urt. v. 08.03.2010 – 6B_743/2009, forumpoenale 2010, S. 2ff.

9. *Gless*, *Sabine*, Strafverfolgung im Internet, ZStrR 2012, S. 3ff.

10. *Grabenwarter*, *Christoph/Pabel*, *Katharina*, EMRK, 5. Aufl., 2012.

11. *Heghmanns*, *Michael*, Strafverfahren, 1. Aufl., 2014.

12. *Herrmann*, *Klaus/Soiné*, *Michael*, Durchsuchung personlicher Datenspeicher und Grundrechtsschutz, NJW 2011, S. 2922ff.

13.*Hilgendorf*, *Eric/Valerius*, *Brian*, Computer- und Internetstrafrecht, 2. Aufl., 2012.
14.*Ihwas*, *Saleh Ramadan*, Strafverfolgung in Sozialen Netzwerken: Facebook & Co. als moderne Ermittlungswerkzeuge Broschiert, 2014.
15.*Kindhäuser*, *Urs*, Strafprozessrecht, 3. Aufl., 2013.
16.*Klesczewski*, *Diethelm*, Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingreiffen im Internet, ZStW 2011, S. 737ff.
17.*Kohlmann*, *Diana*, Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz: Bedeutung und Legitimation ihres Einsatzes im Ermittlungsverfahren, 2012.
18.*Kudlich*, *Hans*, Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme, GA 2011, S. 193ff.
19. *Kudlich*, *Hans*, Straftaten und Strafverfolgung im Internet – Zum strafrechtlichen Gutachten für den 69. Deutschen Juristentag 2012, StV 2012, S. 560ff.
20.*Luch*, *Anika D.*, Das neue „IT-Grundrecht“ – Grundbedingung einer „Online-Handlungsfreiheit“, MMR 2011, S. 75ff.
21.*Malek*, *Klaus/Popp*, *Andreas*, Strafsachen im Internet, 2. Aufl., 2015.
22.*Marberth-Kubicki*, *Annette*, Computer- und Internetstrafrecht, 2. Aufl., 2010.
23.*Maunz*, *Theodor/Dürig*, *Günter*, GG, 72. Ergänzungslieferung, 2014.
24.*Meyer-Goßner*, *Lutz/Schmitt*, *Bertram*, StPO, 57. Aufl., 2014.
25.*Obenhaus*, *Nils*, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, S. 651ff.
26.*Peters*, *Anna/Altwicker*, *Tilmann*, EMRK, 2. Aufl., 2012.
27.*Pieroth*, *Bodo/Schlink*, *Bernhard/Kingreen*, *Thorsten/Poscher*, *Ralf*, Grundrechte, 29. Aufl., 2013.
28.*Pieth*, *Mark*, Schweizerisches Strafprozessrecht, 2. Aufl., 2012.
29.*Roggan*, *Fredrik*, Die „Technikoffenheit“ von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen – Die Problematik der Auslegung von Gesetzen über ihren Wortlaut oder Wortsinn hinaus, NJW 2015, S. 1995ff.
30.*Rosengarte*, *Carsten/Römer*, *Sebastian*, Der „virtuelle verdeckte Ermittler“ in

sozialen Netzwerken und Internetboards, NJW 2012, S. 1764ff.

31. *Roxin*, *Claus/Schünemann*, *Bernd*, Strafverfahrensrecht, 28. Aufl., 2014.

32. *Satzger*, *Helmut/Schluckebier*, *Wilhelm/Widmaier*, *Gunter* (Hrsg.), StPO, 1. Aufl., 2014.

33. *Schlegel*, *Stephan*, „Online-Durchsuchung light" – Die Änderung des §110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, HRRS 2008, S. 23ff.

34. *Sieber*, *Ulrich/Satzger*, *Helmut/von Heintschel-Heinegg*, *Bernd* (Hrsg.), Europäisches Strafrecht, 2. Aufl., 2014.

35. *Singelnstein*, *Tobias*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593ff.

36. *Soiné*, *Michael*, Verdeckte Ermittler als Instrument zur Bekämpfung von Kinderpornographie im Internet, NStZ 2003, S. 225ff.

37. *Valerius*, *Brian*, Ermittlungsmaßnahmen im Internet – Rückblick, Bestandsaufnahme, Ausblick, JR 2007, S. 275ff.

38. *Vogel*, *Joachim*, Informationstechnologische Herausforderungen an das Strafprozessrecht, ZIS 2012, S. 480ff.

39. *Volk*, *Klaus/Engländer*, *Armin*, Grundkurs StPO, 8. Aufl., 2013.

The Investigation in Internet: A Confrontation between Technology and Law

Shih-Fan Wang*

Abstract

Information Technology has brought many challenges to the law. The fight against cybercrime in the substantive criminal law and the corresponding rules of criminal procedure are significant issues in today's digital information society. The Internet has become a tool for criminals. Then why are countries worldwide still hesitant in using the Internet to track and prosecute crimes? The investigation in internet serves as a type of confrontation between technology and law. Although technology advances at dizzying speeds, online detection measures—no matter how carefully designed—should be based on a scrutiny system underpinned by basic rights. The collection of evidence for cybercrimes—regardless of cloud searches or hidden online searches—must be based around a review of laws violated. As a result, whether existing laws have a proper and legal basis for intervention has become the most important issue in prosecuting online criminals.

* Assistant Professor, Faculty of Law, National Cheng Kung University; Dr. jur. Munich University, Germany.

Received: January 23, 2015; accepted: October 8, 2015

Keywords: Basic Right, Investigation in Internet, Internet Phone, Cloud Search, Hidden Online Search (verdeckte Online-Durchsuchung)