DOI: 10.6482/ECPCR.202010.0014

刑事訴訟上的線上搜索（Online-Durchsuchung）與源頭通訊監察（Quelle-TKÜ）—引進的必要性及實踐上的困境

吳俊毅*

目　次

壹、序言
貳、核心技術原理的介紹
參、遭遇到的困境及其突破
肆、可能涉及到的基本權及干預的正當化基礎
伍、搜索與網路搜索
陸、通訊監察與源頭通訊監察
柒、可能遭遇到的立法與執行上的困境
捌、展望

摘　要

有線以及無線寬頻網路科技的進步，帶動與加速全面數位化與網路化的生活。我們每天都花費許多的時間盯著手機。為了滿足安全性與效率的需求，雲端以及加密技術被大量使用。水能載舟，亦能覆舟，這樣的發展趨勢也有濫用的擔憂。雲端與加密技術，就刑事訴追目的的達成，是一個極為嚴峻的挑戰，甚至可能讓國家陷入束手無策的困境。2017 年德國的刑事訴訟法補充線上搜索與源頭通訊監察的規定，意味者在德國，有了新的調查措施。在我國，為了取得電磁紀錄可以命令搜索扣押，但是，由於線上搜索與源頭通訊監察的技術特性，以及所引起的基本權干預的深度與廣度，搜索扣押與通訊監察的規定無法直接適用。本文想為線上搜索與源頭通訊監察設計專門規定的必要性找到基礎，並勾勒其在強制處分措施體系當中的地位。

關鍵詞：線上搜索、源頭通訊監察、加密技術

* 國立高雄大學法律學系教授、法學院比較刑法研究中心（CrimLaw）主任、德國特里爾大學法學博士

Online Investigation and Source Telecommunication Monitoring of Criminal Procedure Law -Necessary of Import and Dilemma of Realization

Jiuan-Yih Wu*

Abstract

The advancement of wired and wireless broadband network technology has accelerated the realization of all digitization and networking of life. We spend a lot of time using mobile phones every day. In order to meet the requirements of security and efficiency, more and more service providers use cloud and encryption technology. Because of this development trend, people are also worried about the danger of abuse. Cloud and encryption technology is an extremely serious challenge for criminal prosecution, and even makes the country helpless. In 2017, the German Criminal Procedure Law had provisions for online search and source communication monitoring. This means that in Germany, there are new investigation measures. In Taiwan search and seizure can be ordered in order to obtain electromagnetic records. However, due to the technical characteristics of online search and source communication monitoring, as well as the depth and breadth of the fundamental rights interventions caused, the provisions of search seizure and communication monitoring cannot be directly applied. This article intends to find a basis for the necessity of designing special regulations for online search and source communication monitoring, and to explain its status in the system of compulsory sanctions.

Key Words: Online Investigation, Source Telecommunication Monitoring, Encryption, Online-Durchsuchung, Quelle-TKÜ

* Prof. Dr. Jiuan-Yih Wu, Ph. D. of Law University of Trier Germany. Professor Department of Law National University of Kaohsiung（NUK）Director of the Center for Comparative Research in Criminal Law（CrimLaw）College of Law NUK

壹、序言

2017 年德國刑事訴訟法的修法加入了源頭通訊監察（§100 a 德刑訴法）與線上搜索（§100 b 德刑訴法）的規定。加密技術、根據資訊科技系統的通訊架構與雲端技術導入下的事實調查困境與突破的方法，在德國，有了明確的法律基礎。這樣的立法經驗，也給了使用同樣科技的我們，回頭檢視現行的規定面對這些新的科技發展情況是否夠用的想法，如果答案是肯定的，現行的規定到底應該如何適用，相反地，如果答案是否定的，我們是否也需要引進上述德國有規定的調查措施。

德國就新科技發展所產生的對刑事訴追的挑戰開始，逐一檢視問題所對應到的傳統調查措施的每個環節，從涉及到的基本權的角度找出規範不足之處以及應該調整的方向，並據此形成命令與執行新的調查措施的基本原則，以符合明確性、法律保留與比例原則的憲法要求。這提供了非常好的研究方法的啟發。本文想從這股新科技發展趨勢的幾個核心概念的掌握出發，觀察現行的刑事訴追調查方法可能陷入的困境。對照既有的規定，按新科技可能涉及到的基本權及其干預的正當化基礎，先以解釋的方法就程序的階段找出關係上屬於比較接近的法律基礎，當範漏洞出現時，指出為達調查目的規範應該調整的地方。然後，根據前面的研究結果，提出檢討與建議，並且在最後作出展望。

貳、核心技術原理的介紹

一、資訊科技系統的通訊架構

根據電路、類比式的通訊架構，在通訊時必須不間斷地佔用特定的傳輸路徑以及資源，不論是一開始的即時語音服務，還是後來的文件、圖片的遠端複製傳輸技術的傳真服務（Fax）。固定線路（市話）或者無線電話的「線路」與「門號」，都是根據電路連線方式的基礎架構。

後來，網際網路通訊以及封包傳輸技術的普及，長時間以來都是用在電子郵件以及網頁瀏覽的應用層面。隨著寬頻骨幹網路的大量佈建，以及數位化無線寬頻技術發展的重大突破，通訊因此邁入全面數位化的時代，像是目前的第四代無線寬頻網路（4G）以及 2020 年第三季在我國即將開始營運的

第五代無線寬頻網路（5G）[1]，傳統的通訊與網路服務提供者的界線逐漸消融，有更多不具有機線設備的非典型提供者加入電信市場提供服務[2]。在寬頻網路的時代，不再需要不間斷地佔用特定的線路和資源，因為使用電路通訊的機會大幅下滑，造成通訊費用的費率結構的劇烈轉變，像是，按照資料量計算的網路使用費或者無線寬頻網路費，取代了傳統的按通話時間的計費方式。可以隨時隨地連上網際網路享受多元的通訊服務，根據統計，使用手機、平板上網的比率，從2016年10月起，首度超越透過個人電腦上網[3]，行動裝置的硬體與其他多元服務APP的發展是當前的技術重點。在寬頻網路通訊的時代，「門號」或是「線路」不再是通訊架構的必須基礎。只要能夠取得網際網路的入口，不管是有線，還是無線（比方，Wi-Fi），就可以進行通訊。也就是，不再需要用電話或手機撥打電話號碼，而是透過網際網路通訊協定（IT-Protocol）架構底下具有連網能力的個人電腦（PC）或者行動裝置、手機等「資訊科技系統」，就可以突破地理與設備（可在多部設備上）的限制進行通訊。網際網路位址（IP-Address）與登入系統的身份識別碼是建立通訊關係的必要條件[4]。

二、系統鎖定與加密技術的普及

有連結網際網路能力的資訊科技系統或者封閉式的系統，基於安全性的需求，會有系統入口上鎖（管制）的設計，像是，輸入密碼、指紋與臉部辨識…等，以防止無權者使用並且知悉儲存在裝置上的內容，同一部個人電腦可以設定多組登入方式，只有有權者才能登入並使用自己的作業環境和存取資訊，如同一個屋簷下的多個房間，可以讓多人使用相同的裝置而不擔心侵害彼此的隱私與其他的秘密。

資料上鎖技術（Datenverschlüsslungstechinik; Kryptographie）或加密技術，是一種防止無權截取傳遞中資料的網際網路安全措施。這裡的所謂「上

---

[1] 中華電信在2020年6月30日宣布5G開台，成為我國第一家提供5G服務的業者，黃晶琳，5G啟動 中華電6月30日開台搶頭香，https://udn.com/news/story/7240/4667823（最後造訪日：2020年7月9日）

[2] 比方，個人電腦與手機製造商Apple公司，透過其FaceTime APP可以經由網際網路進行語音與視訊即時通訊，並可傳送文字、圖片、影片等訊息。社群網站臉書Face Book也提供Messenger APP讓使用者透過網際網路也可以傳送訊息、圖片、影片與語音等通訊。為因應這樣的技術發展趨勢，2019年5月底通過（尚未開始施行）的「電信管理法」，在未來，所有的電信服務提供者將可被納入。

[3] 紀品志，全球行動上網用量首度超越桌機 https://www.bnext.com.tw/article/41637/mobile-internet-use-passes-desktop（最後造訪日：2020年7月9日）

[4] Arndt Sinn, Neue Heimliche Ermittlungsmasnahmen durch Quellen-telekommunikationsuberwachung und Online-durchsuchung, Taiwan Prosecutor Review（檢察新論），No. 27, 2020, S. 214.

鎖」，是透過數學公式將資料作不規則的排列[5]，像是把一幅圖畫切割成許多的不規則小塊拼圖然後打散，藉此讓人不曉得這幅畫的主題。寄件者使用「上鎖程式」把想要傳送的資料「鎖住」儲存並進行傳送，相對地，收件者這邊必須要有「開鎖程式」才能將所收到的前述資料「打開」而知悉完整的內容，以便作後續的處理，比方，閱讀、聆聽、觀察 或是加工。在加密的資料的傳遞過程中，沒有「金鑰」（鑰匙），就無從介入並且得知資料的內容。由於各家都有自己的演算法，想要解鎖可說是瞎子摸象難上加難，沒有國家能「即時地」用自己的「鑰匙」解鎖，即便有國家號稱有能力解鎖，取決於演算法的難度差異，也要大費周章地耗掉一段或長或短的時間，甚至到通訊都已經結束才能解鎖或者根本就解不開。

加密技術是70年代跨國性金融機構為了實行自動化，針對所產生的保障支付安全需求而發展出來。在今天，由於資料保護意識的高漲，加密技術因此也被廣泛地使用在通訊秘密的保護上面。經過加密的資料會造成國家安全單位或刑事訴追機關在監察時的困難，甚至是一場無止境的攻防挑戰[6]。所以，一些國家制訂了限制鎖碼技術使用以及擴散（出口）的規定；在美國，在電子簽章或個人密碼的領域，限制有被鬆綁，因為這兩者對於電子商務的發展是相當重要的條件。不過，在私人通訊的領域，管制仍然被堅持，原因是基於國家安全的理由。由此可知，加密技術的限制，主要的壓力來源應該是來自於國家。但是，這個限制嘗試終究是失敗的，因為，在網際網路，特別是無線寬頻網路的快速發展與普及化，產生了對於個人通訊與資訊安全保護的高度需求。長期以來，加密技術已經悄悄地透過許多檯面下的管道被使用。對於這股趨勢沒有一個國家有能力防堵。有些國家，像是，美國或是中國大陸，透過其龐大市場的威脅，讓業者把備份鑰匙放在國家拿得到的明顯處[7]，為必要時預留一道後門，至於市場規模不大的國家，或許國民還可以享受加密技術的保障利益。

---

5 Christian Becker/ Dirk Meinike, StV 2011, S.50.

6 王士帆，「網路之刑事訴追 - 科技與法律的較勁」，政大法律評論，2016年第145期，頁36以下，註82。

7 比方，Apple的雲端服務iCloud自2018年3月份起，在中國的用戶資料就交由中國的合作夥伴「雲上貴州公司」負責，並且首度把中國大陸Apple ID用戶金鑰移轉到美國本土以外保存，高敬原，蘋果向錢看，中國iCloud業務轉由陸企營運，用戶隱私亮紅燈，https://www.bnext.com.tw/article/47757/apple-will-begin-storing-chinese-customer-icloud-data-at-new-china-data-center-from-next-month; linli, 蘋果將用戶資料加密金鑰移到中國境內，引發隱私擔憂，https://technews.tw/2018/02/26/apple-to-start-putting-sensitive-encryption-keys-in-china/（最後造訪日：2020年7月9日）

三、雲端技術與通訊概念的新解

傳統對於通訊概念的理解，是指人與人之間透過電子媒介形成的管道所進行的意見交換過程。「人對人」這一點是通訊概念的核心要素[8]。邁入到行動通訊的時代，因為行動裝置移動所產生的行動管理資訊，比方，基地台位置資訊，是行動裝置與基地台之間自動進行通訊的歷史紀錄，因為並沒有人打電話，描述的是一個「機器對機器」的通訊。在個人電腦無法上網的「單機時代」，系統當中資料的存取管理，不會經過對外的網路，也就是不透過電子媒介。進入到網際網路時代，個人會從網際網路服務提供者（Internet Service Provider=ISP）的伺服器瀏覽網頁資料，描述的是一個「人對機器」的通訊關係。在雲端技術發展之後，有連線能力的個人電腦、行動裝置可透過有線或無線寬頻網路連接雲端硬碟存取資料（同步化），還有，系統也可以設定自動與外部系統或雲端連線進行資料的存取，以更新系統或者外部系統上面的資料狀態，這同樣是「人對機器」以及「機器對機器」的通訊關係。如果堅持「人對人」這一點來理解通訊的概念，手機的待機資訊、瀏覽網頁的情形、使用雲端服務的情況等，是無法被通訊的概念所涵蓋的。不過，就個人來說，這些過程事實的紀錄，還是有保密的利益，對於這樣的需求，透過電子媒介所形成的管道進行的通訊過程，如果堅持要「人對人」而不採功能的觀察方式考慮到當今的科技發展情況，「人對機器」或者「機器對機器」的通訊情形就無法落在秘密通訊保障基本權的保護範圍內，會有保護不周的擔憂[9]。

參、遭遇到的困境及其突破

一、執行搜索的通知義務會危及調查目的

儲存在個人電腦、行動裝置或者雲端的電子化處理資料，按照刑訴法第128、第128-1條，為了調查事實與證據，法院可依聲請或依職權命令搜

[8] 最高法院106年度台非字第259號判決。在德國，Arndt Sinn, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272, sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334), S. 4.

[9] Arndt Sinn, a.a.O., S. 4; Fredrik Roggan, Die Strafprozessuale Quelle-TKÜ und Online-Durchsuchung: Elektronische Überwachung für Beschuldigte und die Allgemeinheit, StV 2017, S. 822.

索。一方面，由於使用者對於資訊安全的要求，裝置或者雲端等資訊系統都有入口門禁的機制，比方，須透過輸入密碼、掃描比對生物性特徵（指紋、臉部），通過辨識之後才能使用（解鎖）裝置或進入（登錄）雲端，以存取裝置或雲端裡的資料。另一方面，導入雲端技術後，個人可隨時隨地在多部裝置，登入雲端而且在同步化的作業環境存取資訊。在執行搜索命令時，指揮機關或者輔助機關公務員，對目標裝置或者系統的所有人、持有人、保管人負有通知義務，在搜索命令執行前最晚到開始執行時，比方，第一線的執行機關公務員應表明其身份並出示書面的搜索命令（令狀）。當依法實行這個通知義務時，縱使可以扣押個人電腦、平板與手機，接下來會面臨一個問題，在握有裝置或雲端的入口鑰匙者不配合時，國家刑事訴追機關將無法立即進入裝置或者雲端。甚至還可能有時間讓措施相對人自行或者在他人協助下透過其他的裝置登入雲端，刪除或移動應發現的資料，搜索的目的會無法達成。

所以，在這裡，會產生一個「秘密執行」搜索的需求。因為駭客行為的啟發，對目標裝置或雲端植入「國家木馬」（Staattroja）獲得認真的考慮。技術上，係國家也利用目標資訊科技系統的資安漏洞，以間諜軟體滲透資訊系統的方式，然後從遠端透過網際網路取得在當中應發現的資料[10]。

二、加密的通訊過程無法監察

對於加密的通訊，國家刑事訴追機關想監察加密的通訊，沒有「金鑰」不可能介入通訊的過程並知悉通訊的內容。儘管實務上有機關不甘示弱宣稱可以獨力解鎖，但還是需要耗費時間，可能在成功解鎖時通訊的狀態早就已經結束，或者根本解不開[11]。

通訊監察係對「進行中」的通訊，對於已結束的通訊不得命令通訊監察。想要看加密的通訊內容，方法上，要從發訊端或者收訊端在加密前想傳遞的或解鎖後所接收的通訊內容，所介入的並不是通訊的過程，而是介入到資訊科技的系統，比方，LINE 的聊天室、Face Book Messenger 或 WeChat 的對話框裡面的文字訊息、圖片檔案、聲音檔案或影片檔案，不過，如果是即時的語音或者視訊，就只能發現使用服務的紀錄。德國刑訴法第 100 條 a 以「源頭通訊監察」（Quelle-TKÜ），與同法第 100 條 b 的線上搜索（Online-Durchsuchung）切開規定來描述這樣的措施。在作法上，也是只能對儲存「通訊內容」的裝置或資訊科技系統進行搜索，措施相對人不配合時以及會

[10] Fredrik Roggan, StV 2017, S. 824.
[11] Fredrik Roggan, StV 2017, S. 823.

危及搜索的目的時，命令執行線上搜索，故源頭通訊監察又被稱為「小線上搜索」（kleine Online-Durchsuchung）[12]。

肆、可能涉及到的基本權及干預的正當化基礎

一、祕密通訊自由

憲法第12條：「人民有秘密通訊的自由。」在使用電信進行通訊的情形，通訊的內容資料以及使用通訊所產生的狀態資料（比方，通訊參與者、起迄時間、通訊長度…等通聯紀錄）係落在祕密通訊自由基本權的保護範圍裡[13]。取得加密的通訊並知悉其內容資料與相關的狀態資訊，描述的是對於憲法第12條所保障的祕密通訊自由的干預。

命令實行源頭通訊監察的情形，因為有一道加密的通訊過程，對此會涉及到憲法第12條的祕密通訊自由的干預。不過，有問題的是，因為缺乏金鑰，只能在通訊「加密前」或是「解鎖後」知悉通訊的內容資訊與狀態資訊，此時，資料是否屬於通訊而涉及對於憲法第12條基本權的干預。對此，在德國，根據聯邦憲法法院的判決，受到保障的通訊必須是進行中的通訊（die laufende Telekommunikation）。知悉加密前或者解鎖後的通訊的動作，如果作法上是透過植入間諜軟體而由遠端取得儲存在目標裝置上面的通訊，性質上，與透過木馬程式取得儲存在有連線能力裝置上的資料的「線上搜索」（Online-Durchsuchung）的情況並無不同[14]。與秘密通訊自由的交集係透過資料的來歷，以「是否經過通訊傳送方式」來進行切割。因為取得的資料有歷經「加密的通訊傳送過程」，所以，針對加密前或解鎖後的通訊資料，而在通訊源頭調查的動作，仍可被祕密通訊自由的基本權保護範圍所涵蓋[15]。沒有經過加密傳送的通訊，還是適用一般的通訊監察措施，而且使用通訊監察

---

[12] Arndt Sinn, a.a.O., S. 7; Fredrik Roggan, StV 2017, S. 825.

[13] 司法院大法官會議解釋釋字第631號解釋。

[14] Stephan Beukelmann, NJW 2017, S. 440; Cristian Becker/ Dirk Meinick, StV 2011, S. 51; Andreas Popp, Die "Staatstrojaner"-Affäre: (Auch) ein Thema für den Datenschutz. Kurzer Überblick aus strafprozessualer und datenschutzrechtlicher Sicht, ZD 2012, S. 53. 中文的介紹，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，第93期，2015年，頁13以下。

[15] 反對的看法，比方，在電子郵件通訊的情形，認為儲存在目標資訊科技系統上的電子郵件，因為通訊已經結束，而不會落在祕密通訊自由的保護範圍內，謝碩駿，前揭文，第20頁以下。德國修法前看法的介紹，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，頁239以下。

的時機就侷限在通訊過程當中[16]。

按照憲法第23條，在符合必要性、比例原則下，對於秘密通訊的干預應該根據立法院制定的法律（法律保留）才能取得正當化的基礎。有鑒於通訊監察措施實施時對於這個基本權影響的深度與廣度，按照司法院大法官會議釋字第631號解釋，應該由法官來決定（法官保留原則）。另外，在方法上，德國文獻的看法認為，禁止同步使用間諜軟體從遠端遙控目標裝置上的攝影機，如果可因此觀察到住宅內部的情況的話[17]，但可控制裝置上的麥克風同時監聽語音通訊的內容並且錄音[18]。至於國家使用木馬程式方式的情形，德國文獻上有討論認為，這裡會產生一個矛盾，也就是，一方面國家要致力於維護資訊安全，另一方面卻是要利用資訊安全的漏洞，甚至在碰到資安系統沒有漏洞並且成功阻擋監察措施時，要求業者幫國家開「後門」[19]。

二、資訊科技系統的保密性與完整性

經過通訊傳送過程而儲存的通訊資料，與其他儲存在資訊科技系統的資料，是否公開以及讓他人加工使用，資料的擁有者對此享有自由決定的利益，因為不違反憲法的價值秩序，也受憲法第22條所保障[20]。在德國，聯邦憲法法院根據基本法第2條與第1條將此視為個人資訊自決權並且加以保障。按照德國聯邦憲法法院在2008年2月27日的判決，更進一步說明，在此情形，會涉及到植基在德國基本法第2條第1項與第1條第1項的個人資訊自決權的「資訊科技系統的保密性與完整性」（Vertraulichkeit und Integrität informationstechnischer Systeme）基本權的干預[21]。這個基本權在德國基本法

[16] 德國刑事訴訟法第100條a第1項第1句和第3句區分一般通訊監察與源頭通訊監察，在後者，可以使用監察措施的時機被立法者擴大，亦即，第3句描述的情況，「當相對人的通訊內容和狀態在公用網路進行中的通訊傳送過程是以加密的方式存在時，就可監察和儲存，則可監察並且儲存其儲存在資訊科技系統的通訊內容與狀態。」反對的看法，認為應該限於通過傳送過程才可監察和儲存，以避免濫用的風險，修法前的討論，比　方，Thomas Stadler, Zulässigkeit der heimlichen Installation von Überwachungssoftware, MMR 2012, S. 19, 20; Detlef Burhoff, ZAP Fach 22, S. 904; Marie-Theres Tinnefeld, Die "Staatstrojaner" aus verfassungsrechtlicher Sicht - Gedanken zum Prüfbericht des Bayerischen Landesbeauftragten für den Datenschutz, ZD 2012, S. 453。修法後的討論，Tobias Singelnstein, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017, S. 2648.

[17] Arndt Sinn, a.a.O., S. 10.

[18] Lisa Blechschmitt, Strafverfolgung im digitalen Zeitalter, MMR 2018, S. 365.

[19] Lisa Blechschmitt, MMR 2018, S. 365; Maximilian Heim, Staatstrojaner im Einsatz, NJW-Spezial, 2/2018, S. 120.

[20] 司法院大法官會議解釋釋字第603號解釋。

[21] BVerfGE 27.02.2008 – 1 BvR 370/07.

並沒有特別的規定，在適用上，相對於秘密通訊自由（Art. 10 I 德基本法）、住宅的不可侵犯性（Art. 13 德基本法）等基本權，資訊科技系統的保密性與完整性這個基本權具有「補充性」，可填補對基本權保護上面的漏洞。

在實行源頭通訊監察的情形，方法上，若採取植入木馬程式的方式，則是與線上搜索的影響情形相同，都是取得並知悉儲存在有連線能力的資訊科技系統上面的資料。有看法認為，還沒有被傳送出去的資料或是草稿，不能被認為是通訊，對此內容的知悉係涉及到「資訊科技系統的保密性與完整性」，而不涉及秘密通訊自由的基本權[22]。所以，德國文獻上的區別點是在於，所儲存的資料應該要先走完通訊傳送的過程，儲存在發送端或者收件端的資訊科技系統上的資料，可確定、係來自於進行中的通訊過程（Daten aus laufenden Telekommunikations-Vorgängen）時[23]，才能被通訊的概念所涵蓋，換句話說，這個經過加密的通訊過程必須在進行中就已經被監察以及儲存[24]。至於還沒有經過加密傳送過程的資料，因為還不打算被傳送無法被視為通訊而不會落在秘密通訊自由的保護範圍內。所以，在命令實行源頭通訊監察時，只會涉及到秘密通訊自由基本權的干預。

不過，還是有疑問的是，儲存在目標裝置上經過加密傳送過程的「通訊資料」，與通訊傳送過程之間的時間間隔是否有限制，也就是，到了經過多久才不算是通訊而要當作儲存的資料，還是可無限制地被繼續視為是通訊，像是，收到上鎖防護的信件或者包裹，一般在開封後應該不會還一直被當作是信件或者包裹。不過，對於儲存在手機裝置上的通聯紀錄，譬如，警方查看手機最後聯絡的十組電話號碼，按照德國通說的看法卻是完全不同而認為已經不在祕密通訊自由的保護範圍以內，而是只有涉及到個人資訊自決權的保障，因為訊息已經傳達到收件人且傳送過程已經結束[25]。

伍、搜索與網路搜索

一、搜索的命令

要取得電子化處理的資料。根據刑訴法第 122 條命令搜索的實質要件，也就是，在決定是否要同時使用搜索扣押時所要考慮的條件。在這裡，比較

[22] Tobis Singeln/ Benjamin Derin, NJW 2017, S. 2648.
[23] 對此，比方，德國刑訴法第 1 條第 2 款規定，經加密的通訊須正在進行中而能被監察與儲存。Fredrik Roggan, NJW 2015, S. 1998.
[24] Beulke/ Swoboda, Strafprozessrecht, 14. Aufl., 2018, Rn. 254.
[25] 比方，Beulke/ Swoboda, Strafprozessrecht, 14. Aufl., 2018, Rn. 254b.

相關的，首先是搜索扣押的必要性，搜索扣押係為了調查事實、發現具有證據潛力的材料或者應沒收或追徵的標的的有效方法。再來，是嫌疑保留的要求與搜索的目標，從調查階段開始，可搜索被告或犯罪嫌人的住宅、處所、身體、物件，因為這些搜索的目標具有「容量」而能容納前述的應發現的事實、或證據材料、應沒收追徵的標的應「扣押」的標的（§ 133 刑訴法）。刑訴法第 122 條規定，可對「電磁紀錄」進行搜索。電磁紀錄，刑法第 10 條第 4 款有立法定義：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄」是無體的、儲存在資訊科技系統上（比方，硬碟等電子媒介或者雲端）的資料，解釋上，應該是應「扣押」的標的，搜索的目標應該是資訊科技系統（比方，電腦）。此外，搜索的目標的所有人、使用者或者保管者如果是非被告之人，主要是因為具有證據潛力的材料或者應沒收或追徵的標的在他的實力控制關係底下這樣的「關聯性」，按照刑訴法第 122 條第 2 項可根據這個關聯性，比方，對他的資訊科技系統進行搜索，並且扣押儲存在上面的電磁紀錄。性質上，這也可以理解嫌疑保留的要求。至於搜索的措施，是任何可以造成目標內部情況公開的方法。以上的要件一但符合，會逐步獲得向「命令搜索」結論的推進效果。相反的，也要注意比例原則的要求，如果命令搜索會引起相對人的利益極為嚴重的不利影響。則必須立即停止審查並且放棄命令搜索，這是命令搜索實質要件的消極要素。

刑訴法第 128、128-1 條規定同時命令搜索扣押的形式要件，亦即，形成支持或者反對命令搜索扣押所要考慮的條件。首先，對命令有要式性的要求，應制作書面的同時搜索扣押的命令（搜索票）（§ 128 I 刑訴法）。搜索的決定機關採法官保留（§ 128 III 刑訴法）。偵查中的搜索扣押命令係根據檢察官的聲請（§ 128-1 I 刑訴法），調查中是按照經檢察官同意的司法警察的聲請（§ 128-1 II 刑訴法）。

二、搜索的執行

刑訴法第 128-2 條、第 145 條、第 148 條以及第 126 條、第 127 條規定同時搜索扣押命令的執行程序。在執行搜索命令時，通知義務是程序的核心，因為搜索是公開的強制處分措施，應該要在「事前」通知措施相對人，也就是，第一線的指揮執行機關（審判中：法官、偵查中：檢察官、調查中：司法警察）或輔助機關（審判中、偵查中：司法警察），應在執行前或最晚要在執行的當下，表明身分（出示服務證件）、搜索票（書面的搜索命令），雖然刑訴法對此沒有規定，在操作上應該被通知義務的內容所涵蓋。

不論是有體的目標或無體的資訊科技系統，在「事前」應該要讓措施的相對人曉得，「搜索即將或者正要對他的有體目標或資訊科技系統執行。」

三、線上搜索的體系定位

如前所述[26]，有連結網際網路能力的資訊科技系統，基於安全性的需求，會有入口上鎖的設計，像是，輸入密碼、指紋與臉部辨識…等以防止無權者使用並且知悉儲存在裝置上的內容，像是，同一部個人電腦可以設定多組登入方式，只有有權者才能使用自己的作業環境並存取資訊，讓多人可以使用相同的裝置而不擔心侵害彼此的隱私與其他的秘密。在導入雲端技術後，透過入口上鎖的機制，使用者可隨時隨地且不限裝置，透過網路解鎖登入雲端來同步化自己的作業環境且存取資料[27]。在對資訊科技系統或雲端執行搜索的情形，要「事先」對資訊科技系統或雲端的有權使用者實行通知義務。不過，當相對人不配合時或可預期不配合時，因為無法立即解鎖，國家刑事訴追機關在自力解鎖以登入資訊科技系統或者雲端時，這中間的時間耗損可以為措施相對人爭取到時間，特別是，先一步自行從其他裝置遠端進入目標資訊科技裝置或者登入雲端，將應取得的資料刪除或者搬移。如此危及到搜索的目的。對此，「破門效果」的尋找於是成為戰略的指導原則，利用系統的資安漏洞「後門」或者取得「備份鑰匙」，線上搜索（Online-Durchsuchung）就是基於這樣的想法。在相對人不知情下對他的資訊科技系統植入間諜軟體，滲透資訊科技系統並取得當中的資訊，以避免他搶先一步刪除或搬移應取得的電子化處理資料（電磁紀錄）。因此，為了達成搜索的目的，允許秘密地以間諜軟體滲透入目標資訊科技系統，而不實行法定的事先的通知義務[28]。

當今人們對於行動裝置等資訊科技系統和雲端的依賴性非常高，儲存相當可觀的個人資料，包含私密的資料。對相對人基本權的干預強度，在德國，認為是跟對住宅監聽的「大監聽」相當的[29]。相對於傳統的搜索，線上搜索是具有補充性而是最後的手段[30]，並且，只能對被告命令執行。另外，

---

[26] 貳、二。

[27] Arndt Sinn, a.a.O., S. 10.

[28] 採秘密實行係為了保障調查目的的達成，相同的看法，李榮耕，「初探遠端電腦搜索」，東吳法律學報，第 29 卷第 3 期，2018 年 1 月，頁 70 註 85。

[29] Arndt Sinn, a.a.O., S. 11; Soiné, Michael, Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497.

[30] 德刑訴法第 100 條 b 第 1 項第 3 款：「（1）在相對人不知情下，得以科技方式干預相對人使用的資訊科技系統並從中取得資料（線上搜索），當（…）3. 調查事實或被告的所在地，以其他方式根本上是有困難的或無望的。（…）」

只有在特別重大的可罰行為案件才能使用[31]。

因此，秘密執行搜索命令的線上搜索，對照對於基本權的干預強度，現行刑訴法並沒有法律基礎。

陸、通訊監察與源頭通訊監察

是否可以根據通保法命令執行源頭通訊監察。以下的兩個點可以呈現我國目前的討論情況。

一、通訊與通訊監察的概念

通保法第3條和第5條描述的是命令通訊監察的實質要件，在判斷「是否」可以使用通訊監察措施時所根據的條件。

通保法第3條：「(1)本法所稱通訊如下：

一、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。

二、郵件及書信。

三、言論及談話。

(2)前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」

通保法所指的通訊，涵蓋使用電子媒介、紙本媒介以及當面口頭方式進行的意見交換過程。如前所述，使用加密技術與封包傳送技術的通訊，係讓人透過電子媒介所形成的管道來進行意見交換[32]，是否可以被通保法第3條第1項第1款與第2項的「電信」所包含。對於電信與電信設備，通保法並沒有立法定義，研究方法上，可以參考立法者在其他的法領域或者相同法領域的規定，對於電信與電信設備的描述來加以掌握，像是，電信法以及還未生效的、用以取代電信法的電信管理法，因為只有涉及到對於電信概念的理解，在介紹上，想以現行的電信法為主，新法的規定會在相關段落透過註解來作對照式的介紹。

---

[31] 德刑訴法第100條b第1項第1、2款：「(1)在相對人不知情下，得以科技方式干預相對人使用的資訊科技系統並從中取得資料(線上搜索)，當(…)1.根據特定事實而認為有以正犯或參與犯實行第二項所指的特別重大的可罰行為，或是，在有處罰未遂犯的情形，以未遂犯的方式實行、2.在個案中，行為是特別重大的(…)」至於德刑訴法第100條b第1項第1款特別重大的可罰行爲是規定在同條的第2項。

[32] 本文，貳、二。

電信法第2條第1款：「本法用詞定義如下：一、電信：指利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息[33]。二、電信設備：指電信所用之機械、器具、線路及其他相關設備[34]。…八、通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則[35]。電信號碼係指電話號碼或用戶識別碼[36]。」以及電信法第20-1條：「（1）電信網路使用之編碼、用戶號碼、識別碼等電信號碼，由電信總局統籌規劃及管理；統籌規劃之電信網路編碼計畫，由電信總局公告之。（2）前項電信號碼，非經電信總局或受電信總局委託機關（構）[37]之核准，不得使用或變更。…（6）第1項至第3項電信號碼之核配、調整與收回、受委託者之資格、條件與委託管理事項及其他應遵行事項之管理辦法，由電信總局訂定之。（7）從事電信網際網路位址及網域名稱註冊管理業務之監督及輔導事項，由電信總局辦理之；其監督及輔導辦法，由電信總局訂定之。…」按照前述電信法第2條，「其他科技產品」應該可以包含非根據電路通訊技術基礎而是透過網際網路的資訊科技系統的通訊軟體[3839]，像是，網路通訊APP，LINE。另外，在通信紀錄裡，電信號碼是指電話號碼或用戶識別碼，又按照後來補充規定的電信法第20-1條，在電信網路的架構下，電信號碼又可以包含電信網路使用之編碼、用戶號碼、識別碼。似乎通訊的架構可以建立在門號以及網際網路的基礎上面。不過，觀察通保法第11條第1項第3款通訊監察書應載事項的規

[33] 電信管理法對於「電信」並沒有立法定義。

[34] 電信管理法第2條第3款對「電信設備」有新的定義，「本法用詞，定義如下：（…）三、電信設備：指用以操作或控制光、電傳送、接收通訊傳播訊息，並具備傳輸、交換、接取功能之設備。」

[35] 電信管理法第9條第2項對「通信紀錄」有新的定義，納入基於網路通訊架構進行通訊所產生的紀錄，「前項所稱通信紀錄，指用戶或電信使用人使用電信服務後，公眾電信網路所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄，並以公眾電信網路性能可予提供者為限。」

[36] 電信管理法第68條第1項對「電信號碼」有新的立法定義，不再使用電路通訊架構的電話號碼，「電信號碼包含公眾電信網路之編碼、識別碼及用戶號碼。」

[37] 按照電信管理法第2條，未來廣播電視與電信事業的主管機關為國家通訊傳播委員會。

[38] 可以直接被電信管理法第2條第3款的「電信設備」所涵蓋。

[39] 比方，刑訴法第189條第1項：「證人係依第177條第2項以科技設備訊問者，經具結之結文得以電信傳真或其他科技設備傳送予法院或檢察署，再行補送原本。」這個規定講的是遠距訊問證人具結結文副本的通知方式，目前的技術可以使用傳真。掃描資料，然後將資料透過電子郵件或是通訊軟體傳送，像是，LINE、Facebook Messenger，因為皆能提供「遠端複製」的功能，可以視為這裡的「其他科技設備」。同樣的道理，電信法的「其他科技產品」，著眼在「所提供的通訊功能」這一點，也可以理解為使用加密技術的通訊軟體或是具連線能力的資訊科技系統進行通訊的情形。

定，通訊監察措施所針對的通訊關係係透過「監察通訊種類及號碼等足資識別之特徵」來確定。解釋上，通訊種類是根據通訊關係的建立標準來分類，比方，通訊係透過全程固定網路或是移動的入口網路來實行。至於號碼則是指門號，所以，根據通保法對於通訊技術的理解，還是將得監察的通訊限縮在門號架構底下所進行者。不過，通保法第 3 條卻沒有對通訊的概念作這樣的立法定義限縮，因為資訊的傳送、接收、儲存都被視為是通訊的過程。所以，從第一代行動通訊技術將門號與資訊科技系統結合的裝置開始，一直到現在的第四代（4G；LTE）與即將開始的第五代（5G）行動通訊技術，在不透過門號建立通訊關係的架構底下，也可以只走（無線寬頻）網際網路進行通訊。所以，未透過門號而是透過網際網路與加密技術的架構所設計的通訊軟體所進行的通訊，儘管符合通保法第 2 條第 1 項第 1 款與電信法第 2 條第 1 款意義底下的「電信」定義，不過，卻因為通保法第 11 條通訊監察書應該記載事項對於命令通訊監察形式要件的理解，這樣對於通訊的局限性解讀，而可能讓透過網路架構進行的電信無法成為通訊監察的標的。由此可以發現，通保法的立法者並沒有意會到透過網際網路使用資訊科技系統進行的通訊與透過門號的電路通訊架構所進行的通訊的差別。

至於通訊監察的方法則是規定在通保法第 13 條第 1 項。

> 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。」

通保法第 3 條第 1 項的通訊，涵蓋電信、書信以及當面口頭談話。同法第 13 條描述了對於這些通訊內容的監察與儲存方法。同時，通訊的過程，在電信的情況，根據通保法第 3 條第 1 項第 1 款通訊的過程，是由發送、傳輸、接收、儲存等階段所組成，要特別注意的是，「發送、接收、儲存」都被立法者視為是通訊的過程。對於通訊監察的標的是否限於「進行中」的通訊，對此，通保法的立法者似乎並沒有特別就「暫時儲存狀態」與「永久儲存狀態」加以區分。在未加密的情況，可以根據通保法第 3 條第 1 項與第 13 條第 1 項對進行中或者結束後的通訊進行監察。

不過，最高法院對於通訊的概念卻是與立法者分歧的。最高法院持限縮的看法認為，通訊的過程，會隨著訊息送達接收方後，訊息的傳遞過程隨即終止，整個通訊過程同時也告結束[40]。內容資訊在傳送之前或者傳送結束後，因為已經不再處於通訊過程當中，而不是通訊的內容。至於已經送達服

[40] 最高法院 106 年度台非字第 259 號判決。

務提供者的伺服器而還沒有被接收方下載或者讀取的內容資訊，是否通訊的過程還在繼續中，而仍然可以視為是通訊的內容，按照最高法院的看法，在這個時候，通訊的過程並沒有結束[41]。換句話說，儲存在雲端或者伺服器中已經被下載或者讀取過的內容資訊，從功能的角度，就只是備份，通訊過程應該算是已經結束。

二、是否可根據通保法命令執行源頭通訊監察立法與實務不同調

誠如在上一段所提到的，對已經儲存的通訊內容也可進行監察，特別是未加密的通訊。在源頭通訊監察的情形「實行時機」所需要的加密前、解鎖後等階段，因為根據通保法允許對「已儲存的」、「未加密」的通訊內容進行監察，可以被通保法第 3 條第 1 項所描述的通訊三階段所涵蓋，通保法第 3 條因此也可以作為源頭通訊監察的法律基礎。至於監察的方法，如果是使用植入間諜程式的情況，像是，木馬程式，透過遠端遙控來滲透目標資訊科技系統，並知悉加密前或是解鎖後的、來自通訊過程而儲存在資訊科技系統上的資料，如果不會有造成大監聽影響的危險（§ 3 I 但書 通保法），通保法第 13 條第 1 項似乎並不禁止使用，比方，操控目標裝置上的鏡頭、或者麥克風以錄音、攝影，甚至是錄影的方式來取得加密前或者解鎖後的通訊內容與狀態，但不能啟動鏡頭或者麥克風監看或者監聽裝置所在處所空間裡的對話或者內部情況[42]。在這樣的情況，可能會涉及到個人生活的核心領域，在德國，德刑訴法第 100 條 d 第 3 項是不得執行監察措施的規定[43]，解釋上，不得使用技術上「可能」取得與個人私生活核心領域有關資料的方法，像是，啟動目標系統上的麥克風或者攝影鏡頭[44]。在數位化的應用程面擴大到生產製造領域，有所謂的「工業 4.0」的概念被提出，在個人的生活領域也有智慧家電或者數位助理的產品上市，比方，Amazon Echo 的 Alexa、Apple Homepod 以及 Google Home。在原理上，這些語音助理系統係透過裝置上的多組麥克風隨時等待特定的開啟系統關鍵詞，透過網際網路連線到外部的人工智慧資料庫。就這一點，如果滲透進入系統操縱智慧助理的麥克風對裝置所在空間進行監聽，因為不是取得儲存在系統上的資料，不允許根據線上搜索或源頭通訊監察的方式來執行[45]。

---

[41] 最高法院 106 年度台非字第 259 號判決。

[42] Arndt Sinn, a.a.O., S. 8; Soiné, Michael, NStZ 2018, S. 504.

[43] 德刑訴法第 100 條 d 第 3 項：「在第 100 條 b 的措施，如果能在技術上確定，資料涉及到個人生活活動的核心領域，則不得取得。」

[44] Bruns, Karlsruher Kommentar StPO § 100d, Rn. 9.

[45] 在德國，類似的看法，Daniel Rüscher, Alexa, Siri und Google als digitale Spione im Auftrag

不過，有鑒於前面提到的[46]，立法者與最高法院對於通訊監察的標的是否限於禁行中的通訊的不同調。最高法院採取限縮解釋認為不得對已經結束的通訊根據通保法進行監察。可能是沒注意到通訊因為加密而在進行中無法監察的困境，要等到通訊的內容解鎖後或者趁著加密前動手，順著這個邏輯，對於結束的通訊內容得似乎可能會落到搜索或者線上搜索的區塊。

柒、可能遭遇到的立法與執行上的困境

一、線上搜索與監察網際網路架構通訊時資訊科技系統的特定

刑訴法第 122 條不能作為線上搜索的法律基礎。不過，其規定可以對資訊科技系統上的電磁紀錄進行搜索扣押。刑訴法第 128 條描述了命令的形式要件，按照同條第 1 項，搜索扣押的命令應該以書面的方式作成（搜索票），而且，刑訴法第 128 條第 2 項第 3 款，對於搜索扣押的標的指示僅以「應搜索的電磁紀錄」帶過。線上搜索的目標是與網際網路具有連線能力的資訊科技系統。在導入雲端技術之後，一個作業環境不限於綁定一部終端裝置。有別於單機時代，可以透過對硬體的特定來確定目標的資訊科技系統。在線上搜索的情況，資訊科技系統並非僅對應到單一的終端裝置，這裡會產生需要對目標的資訊科技系統特定的需要。在未來，對於線上搜索的目標的特定，在命令的形式要件上面，可以參考德刑訴法第 100 條 e 第 3 項第 6 款，「在書面命令中，盡可能地精確標示取得資訊的資訊科技系統。」

源頭通訊監察儘管可根據通保法命令。不過，按照通保法第 11 條，這個規定的第 3 款把通訊監察書中的監察措施標的稱為「監察通訊種類及號碼等足資識別之特徵。」監察通訊的種類，應該是像是，有線電話或者無線電話、網際網路。號碼應該是電話號碼、移動通訊的號碼（電話號碼、IMEI 碼、IMSI 碼），在網際網路的情況，應該是指由數字所組成的固定 IP 位址[47]。現行通保法對於通訊技術的理解，似乎還是侷限在電路通訊的門號架構底下的通訊傳送過程，即使擴大理解可以包含走封包傳送的網際網路通訊，也只能涵蓋一部分的情況，亦即只限於使用固定 IP 的通訊傳送過程。

但是，在源頭通訊監察的情形，因為通訊傳送過程受到加密，而把實行措施的時機向前或往後延伸到加密前與解鎖後的階段。在這兩個階段，

---

der Ermittlungsbehörden? NStZ 2018, S. 693.

[46] 捌、一。

[47] 類似的看法，李榮耕，「通訊保障及監察法」，新學林出版股份有限公司 2018 年版，第 242 頁。

通訊的內容與狀態是儲存在目標的資訊科技系統上面。想要從這裡取得資料，要如何特定目標的資訊科技系統，現行通保法第 11 條第 3 款對此並沒有規定。德國刑訴法第 100 條 e 第 3 項規定，源頭通訊監察應該以書面方式為之，應該記載「應該透過措施取得的資訊種類以及對於程序的重要性」（§ 100e III 第 4 款德刑訴法）、「在第 100 條 a 措施（一般通訊監察、源頭通訊監察）的情形，門號的號碼（Rufnummer），或其他應監察線路或終端裝置的其他識別，且基於特定事實認為，該識別並非同時分配給其他的終端裝置；在第 100 條 a 第 1 項第 2 句和第 3 句的情形，應盡可能精確地標示應干預的資訊科技系統。」（§ 100e III 第 5 款德刑訴法）。

線上搜索與源頭通訊監察都是針對資訊科技系統，措施的目標應該要如何特定，需要使用足以識別的方式來做詳細的描述。相較於上述德國的規定，對於線上搜索和源頭通訊監察，現行的刑訴法和通保法並未提到資訊科技系統的識別方法，可以確定立法者並沒有注意到網際網路的通訊架構、導入雲端技術、加密技術使用到通訊傳送過程等的科技發展情形。

二、取得資訊區分不易所形成的濫用風險

線上搜索係針對有連結網際網路能力的資訊科技系統加以滲透。以取得儲存在上面的資料。源頭通訊監察係因為通訊的過程使用加密技術，只能在源頭端知悉通訊的內容，比方，為了取得在發訊方加密前的通訊內容，或是為了取得在收訊方解鎖後的通訊內容，在方法上，國家刑事訴追機關跟在線上搜索的情形類似，在不得進入住宅的情形下，也會以植入木馬病毒等間諜程式的方式滲透到源頭端的資訊科技系統[48]。儘管理論上可以把儲存在目標資訊科技系統上面的資料區分為通訊內容與非通訊內容，前者是源頭通訊監察的調查目的，後者是線上搜索的調查目的，也因此，在德國，把源頭通訊監察稱為「小的線上搜索」（kleine Online-Durchsuchung）。但是，在實際操作上，一旦滲透到目標資訊科技系統，原先是根據源頭通訊監察的命令，在執行時，尋找應取得的通訊內容的過程中，不可避免地會接觸且知悉目標資訊系統上其他的資料內容，在過濾後分離出想要取得知悉的通訊內容。就這一段過程，跟線上搜索在目標資訊科技系統上尋找並過濾出想扣押的資料的情況其實並沒有什麼不一樣。目前，線上搜索，在技術上，並沒有辦法做到不觸及其他資料而精準地確定通訊內容，而在執行上，變成線上搜索與源頭訊監察通通混在一起[49]。除此之外，在源頭通訊監察的情形，無可避免地會

[48] 謝碩駿，前揭文，第 13 頁以下

[49] 有看法認為德刑訴法第 100 條 a 第 1 項第 3 句的源頭通訊監察是違憲的，比方，Fredrik

接觸到儲存在目標資訊科技系統上面的（過程未加密的）一般通訊內容與過程加密的、解鎖需耗費較大的通訊內容，對此，在技術上是難以過濾並且區分出這兩種不同型態的通訊內容[50]。

在線上搜索與源頭通訊監察的情況，根據德國文獻上的討論，因為秘密執行且持續的時間不會只是單次或幾個小時的「點狀」，而是持續一段比較長的時間（幾天或者月）的「帶狀」型態，還有，可以取得的資訊可能涉及到橫跨許多年的老舊資料，還有可能涵蓋個人的私密或最私密領域的資料，像是，文字、聲音、圖畫或影像等，甚至分析所取得的資料掌握個人的完整使用行為。相較於傳統的通訊監察或者搜索扣押，線上搜索的干預強度是遠遠超過的[51]。這樣「一網打盡」（totalitäres Potential），在德刑訴法第 100 條 b 的設計上，對照同法第 100 條 c「大監聽」的命令前提並沒有更多的要求，但影響卻是遠遠超越的，有看法因此認為現行德國線上搜索的規定是不符合比例原則的[52]。

除此之外，在線上搜索的情況，滲透到目標的資訊系統時，可能也可以操縱並啟動綁定系統裝置的硬體設備，比方，麥克風、攝影鏡頭等，對系統所在的三度空間進行即時的聲音、影像監察，這樣的行為與取得的資料，本質上描述的是「大監聽」的情況，可能會涉及到憲法保障的個人的住宅不可侵犯性的基本權。但是，在技術上，實行此線上搜索時，因為無法避免越權的情形，在沒有自我克制的情況下，容易發生毫無節制濫用的風險，也因此有違反比例原則的疑慮[53]。

三、刑事訴追利益與網路安全政策的目的衝突

德國文獻上，不論是依法的線上搜索與源頭通訊監察，還是違法的網路攻擊行為，在方法上，都是走目標系統的安全漏洞以滲透進入到系統裡[54]。一般來說，為了吸引更多的使用者，需要提供自家的系統是沒有漏洞的安全保證，系統製造商都會竭盡所能去防範或是關閉系統上面的安全漏洞，防

Roggan, StV 2017, S. 825.

[50] 在德國，根據德刑訴法第 100 條 a 第 1 項第 2 句，對於未加密的通訊內容，也可以使用介入儲存此內容的資訊科技系統來取得。在此情形，因為並沒有進行中的通訊，與同條項第 3 句的源頭通訊監察變成沒有區別，最終會造成通訊監察係針對「進行中的通訊」被整個架空，Fredrik Roggan, StV 2017, S. 824.

[51] 相同的看法，李榮耕，前揭文，頁 70 以下。

[52] Fredrik Roggan, StV 2017, S. 828 f.

[53] Fredrik Roggan, StV 2017, S. 826.

[54] Arndt Sinn, a.a.O., S. 8; Lisa Blechschmitt, MMR 2018, S. 366; Maximilian Heim, NJW 2018, S. 120 f.; Benjamin Derin/ Sebastian J. Golla, Der Staat als Manipulant und Saboteur der IT-Sicherheit? NJW 2019, 1114.

範任何對系統的攻擊行為，當然，也包含國家的合法系統滲透行為。另一方面，資訊架構的安全也是國家的資訊安全政策內容，國家對此也負有保護義務[55]，會定期或不定期以行政指導方式通知資訊安全的漏洞提醒人民注意防範。在這裡，會產生一個不可視而不見的目的衝突[56]。

在執行線上搜索與源頭通訊監察時，為了秘密滲透進入目標資訊科技系統，需要走系統上面的資訊安全漏洞或是安全弱點[57]。在這裡，描述了一個有效國家刑事訴追的利益：不安全的資訊安全漏洞。留著不去關閉這個已知的系統安全上的弱點，同時給了其他無權者一張通關門票，讓所有使用相同系統的使用也曝露在攻擊行為的危險裡[58]。

如果讓系統製造商負有義務，讓系統留有安全漏洞，或者刻意地置入專屬安全漏洞所形成的「專屬通道」以方便國家的系統滲透行為。如果不這樣做，系統的安全技術會擋下所有的系統攻擊行為，也包括國家的線上搜索和源頭通訊監察等對資訊科技系統的監察措施。所以，保留資安漏洞以便於實行線上搜索與源頭通訊監察，可能與國家的保護義務是相抵觸的[59]。

捌、展望

1. 因為網際網路與封包傳輸的通訊架構，以及通訊過程導入加密技術，為了有效訴追犯罪，使用線上搜索與源頭通訊監察首見於德國刑訴法。根據線上搜索的命令，可以在相對人不知情之下對他執行搜索並取得應扣押的電子化處理資料。源頭通訊監察則是擴大通訊過程的範圍，是對於過程加密的通訊，取得其加密前或解密後的內容，事實上，執行時，根本沒有進行中的通訊[60]。
2. 在執行上，線上搜索和源頭通訊監察都是滲透進入目標的資訊科技系統。由於資訊種類不易區分，秘密長期實行，可能會取得巨量且極為私密的個人資料。加上技術上無法阻絕操控系統啟動其他硬體裝置（麥克風、攝影鏡頭）可能對住宅不可侵犯性的影響。缺乏自我克制下，濫用危險的陰影

[55] Benjamin Derin/ Sebastian J. Golla, NJW 2019, 1114.
[56] Fredrik Roggan, StV 2017, S. 829.
[57] Arndt Sinn, a.a.O., S. 8; Lisa Blechschmitt, MMR 2018, S. 366.
[58] Fredrik Roggan, StV 2017, S. 829.
[59] Benjamin Derin/ Sebastian J. Golla, NJW 2019, 1115.
[60] 相反地，認為在源頭通訊監察的情形仍有即時進行的通訊，黃則儒、廖先志，從德國2017年通訊監察法制修正論我國對通訊軟體監察之立法方向，檢察新論，第24期，2018年8月，頁143。

一直揮之不去，在德國實務上至今還沒有相關的案例[61]。

3. 當然不能容許存有一個犯罪實行的刑事訴追真空領域。在未來，如果考慮導入刑事訴訟上的線上搜索與源頭通訊監察的「專門規定」，應該要注意濫用的風險與技術上控管的難度，在設計上，樹立比較高的發動門檻作為命令的實質要件，像是，封閉且不易擴張的表列行為[62]、重大嫌疑保留、以及補充性原則[63]…等。同時，也因為對於基本權影響的深度與影響範圍的廣度，在命令的形式要件上採取法官保留的設計，且在偵查中給予檢察官與司法警察緊急權。藉此表態，線上搜索與源頭通訊監察應該符合法律保留的要求，且按照比例原則是不能被輕易命令的。
4. 在德國，還有一個更重要的困境有待克服，亦即，如何執行線上搜索與源頭通訊監察，比方，如何植入間諜軟體以及根據電信服務法有配合義務的業者的範圍。還有，通訊監察與防堵資安風險之間的平衡點要如何取得，在執行上，似乎找不到一個具有說服力的理由，且可能會動搖人民對於國家資訊行為的信賴[64]。

---

[61] Stephan Beukelmann, Online-Durchsuchung und Quelle-TKÜ, NJW 2017, S. 441. 認為缺乏科技配套而難以控制，恐不符比例原則而有高度的違憲疑慮，鄭惟容，當國家成為駭客-論德國新時代的網路偵查與線上搜索，國立成功大學法律學系碩士學位論文，頁 281。

[62] 類似的看法，認為應該涉及到國家存續、以及對生命、身體完整性等法益的重大侵害的可罰行為，謝碩駿，前揭文，第 59 頁。此外，著眼在線上搜索的秘密實行特性，以及對於基本權影響比較高的深度或者比較大的廣度，認為除了命令搜索扣押的要件外，還應該根據命令通訊監察的實質要件，李榮耕，前揭文，頁 82。

[63] 王士帆，當科技偵查駭入語音助理 -- 刑事訴訟準備好了嗎？ 臺北大學法學論叢，第 112 期，2019 年，頁 235。

[64] Benjamin Derin/ Sebastian J. Golla, NJW 2019, 1116 f; Arndt Sinn, Taiwan Prosecutor Review（檢察新論）, No. 27, S. 245.

參考文獻

期刊論文

王士帆（2016），網路之刑事訴追 - 科技與法律的較勁，政大法律評論，第 145 期，頁 339-390

王士帆（2019），當科技偵查駭入語音助理 -- 刑事訴訟準備好了嗎？ 臺北大學法學論叢，第 112 期，頁 191-242

李榮耕（2018），初探遠端電腦搜索，東吳法律學報，第 29 卷第 3 期，頁 70.

何賴傑（2012），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 49-87

黃則儒、廖先志（2018），從德國 2017 年通訊監察法制修正論我國對通訊軟體監察之立法方向，檢察新論，第 24 期，頁 131-144

謝碩駿（2015），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，第 93 期，頁 1-78

外文專書

Beulke, Werner/ Swoboda (2018), Sabine, Strafprozessrecht, 14. Aufl., 2018, Verlag C. F. Müller.

Rolf, Hannich (Hrsg) (2018), Karlsruher Kommentar StPO, 6. Aufl. 2008, Verlag C. H. Beck (按照責任作者與條號引用)

外文期刊論文

Becker, Christian / Meinike, Dirk (2017), Die sog. Quellen-TKÜ und die StPO – Von einer „herrschenden Meinung und ihrer fragwürdigen Entscheidung“, StV 2011, S.50 ff.

Beukelmann, Stephan, Online-Durchsuchung und Quellen-TKÜ Aufsatz, NJW 2017, S. 440.

Popp, Andreas (2012), Die "Staatstrojaner"-Affäre: (Auch)ein Thema für den Datenschutz. Kurzer Überblick aus strafprozessualer und datenschutzrechtlicher Sicht, ZD 2012, S. 51 ff.

Blechschmitt, Lisa (2002), Strafverfolgung im digitalen Zeitalter, MMR 2018, S. 361 ff.

Burhoff, Detlef, Auskunft über Telekommunikationsverbindungsdaten, ZAP Fach 22, 02/2002, S. 359 ff.

Derin, Benjamin / Golla, Sebastian J. (2019), Der Staat als Manipulant und Saboteur der IT-Sicherheit? NJW 2019, S. 1114.

Heim, Maximilian (2018), Staatstrojaner im Einsatz, NJW-Spezial, 2/2018, S. 120.

Roggan, Fredrik (2017), Die Strafprozessuale Quelle-TKÜ und Online-Durchsuchung: Elektronische Überwachung für Beschuldigte und die Allgemeinheit, StV 2017, S. 821 ff.

Rüscher, Daniel, Alexa (2018), Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden? NStZ 2018, S. 678 ff.

Stadler, Thomas (2012), Zulässigkeit der heimlichen Installation von Überwachungssoftware,

MMR 2012, S. 18 ff.

Singelnstein, Tobias (2017), Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens (2017), NJW 2017, S. 2646 ff.

Sinn, Arndt (2017), Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272, sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18 (6)334)

Tinnefeld, Marie-Theres (2012), Die „Staatstrojaner" aus verfassungsrechtlicher Sicht - Gedanken zum Prüfbericht des Bayerischen Landesbeauftragten für den Datenschutz, ZD 2012, S. 451 ff.

Sinn, Arndt (2020), Neue Heimliche Ermittlungsmasnahmen durch Quellen-telekommunikationsuberwachung und Online-durchsuchung, Taiwan Prosecutor Review（檢察新論）, No. 27，S. 212 ff.

Soiné, Michael (2018), Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497ff.

學位論文

鄭惟容（2019），當國家成為駭客 - 論德國新時代的網路偵查與線上搜索，國立成功大學法律學系碩士學位論文，未出版，國立成功大學。

網路資料

linli（2018），蘋果將用戶資料加密金鑰移到中國境內，引發隱私擔憂，2020年7月9日取自「科技新報」網址：https://technews.tw/2018/02/26/apple-to-start-putting-sensitive-encryption-keys-in-china/

高敬原（2018），蘋果向錢看，中國iCloud業務轉由陸企營運，用戶隱私亮紅燈，2020年7月9日取自「數位時代」網址：https://www.bnext.com.tw/article/47757/apple-will-begin-storing-chinese-customer-icloud-data-at-new-china-data-center-from-next-month

紀品志（2016），全球行動上網用量首度超越桌機，2020年7月9日取自「數位時代」網址：https://www.bnext.com.tw/article/41637/mobile-internet-use-passes-desktop

黃晶琳（2020），5G啟動 中華電6月30日開台搶頭香，2020年7月9日取自「聯合新聞網」網址：https://udn.com/news/story/7240/4667823