國立臺灣大學法律學院法律學系

碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

加密通訊軟體對犯罪偵查之衝擊暨立法對策

The Challenges and Policy Implications in Criminal Investigation in the Encryption of Communication Software.

林彥均

YEN-CHUN LIN

指導教授：林鈺雄博士

Advisor: Yu-Hsiung Lin, Dr. jur.

中華民國　112 年 7 月

July, 2023

doi:10.6342/NTU202301879

中文摘要

隨著網路通訊軟體之普及化以及日新月異之附屬功能，時至今日網路通訊軟體幾乎已完全取代傳統通訊成為主要之通訊工具，而通訊軟體之隱私性及安全性不僅係消費者選擇使用時之重要考量，更係網路通訊商爭取客戶支持之重要條件，隨著端到端加密技術成為時下網路通訊軟體之標準配備，傳統通訊監察已無用武之地，當普羅大眾因加密技術享有更高規格資訊安全保護之同時，犯罪行為也因此受到掩蓋，世界各國的執法機關均面臨前所未有之挑戰。

為制衡加密技術發展對執法產生之衝擊，近來世界多國紛紛掀起對抗加密立法浪潮，賦予執法機關用以對抗加密之執法工具，立法模式大致可分為解密義務及國家木馬 2 種。我國面臨相同執法挑戰之同時，亦嘗試推出立法對策，法務部於 109 年 9 月 8 日公告「科技偵查法」立法草案，係我國首次針對科技偵查干預手段提出立法草案，然卻因遭到諸多質疑未能順利完成立法。

我國憲法第 23 條揭示法治國原則下對於人民基本權利之干預均須有民主正當性的法律為基礎，國家不僅負有追訴犯罪及保護人民之義務，更應確保政府執法手段恪遵法律保留原則、比例原則等憲法基本原理原則，從近期幾件大型跨國合作執法行動可知，後續案件要能成功定罪，仍需有經得起司法檢視之執法依據方能使查緝不法犯罪成果得以維持。準此，本文希冀透過我國現行法制與外國近來立法趨勢相互比對，突顯我國面對加密通訊軟體對執法衝擊實施應有立法對策之重要性及必要性，介紹近年來英、法、德、荷及澳等國對抗加密之立法，作為我國之立法借鏡，並於文末提出本文建議之設備端通訊監察、秘密線上搜索以及解密令狀之草案條文，希冀對我國立法產生拋磚引玉之效果，並對我國整體科技偵查法制規範提出立法建議。

關鍵字：網路通訊軟體、端對端加密、來源端通訊監察、秘密線上搜索、國家木馬、解密義務

doi:10.6342/NTU202301879

Abstract

Communication software has replaced traditional methods of communicating. The privacy and security of communication software are not only an important consideration for consumers but also a selling point for the company to win the market. End-to-End Encryption allows communication software to create secure communication links between devices that prevent intermediate devices from being exposed to sensitive information during transit. While people enjoy higher standards of information security protection due to encryption technology, criminal activities also are covered up. Therefore, law enforcement agencies over the world are facing the same unprecedented challenges.

In order to balance privacy and public safety and prevent criminals from using advances in encryption technology to their advantage, many countries have promoted encryption legislation in recent years. The legislative models can be roughly divided into decryption obligations and lawful hacking. In Taiwan, the government faces the same challenge and announced the Science and Technology Investigation draft, which was the first time Taiwan proposed draft legislation on scientific and technological investigation intervention methods. However, it did not successfully complete the legislative process due to many doubts.

Art. 23 in the Constitution of R.O.C rules that all the fundamental freedoms and rights restrictions should comply with legal reservation and proportionality. Law enforcement in Taiwan needs not only the technology but also the legal basis to combat serious crimes. Hence, the article tries to introduce the encryption legislation in the UK, France, Germany, Netherlands, and Australia as a reference for our country and puts forward legislative suggestions in terms of lawful hacking and decryption obligation.

Keywords: Encryption, End-to-End Encryption, Communication Software, Going Dark, Decryption Obligations, Lawful hacking, Government hacking, Remote Computer Search.

doi:10.6342/NTU202301879

謝辭

終於到了撰寫謝辭這一刻，長達 6 年碩士學位攻讀，因在職身分倍感艱辛，猶記得報考大學母校臺大法學院碩士班甄試時，正值司法官學院教務組調辦事擔任導師期間，因地利之便，想回母校填補自己一直以來對於碩士學位的缺憾，毅然決然參加臺大法學院碩士班刑法組甄試，也順利地獲得攻讀母校碩士學位的機會，有機會把十年檢察官工作的體認與課堂所學相互融合，再把所回學反饋到檢察工作上，我想這就是在職進修可貴之處。

6 年的碩士生涯正巧與我檢察官生涯中最辛苦的一段工作歷程完全重疊，前 3 年歷經臺北地檢署重大犯罪及黑金專組期間，勉強維持利用公餘前往學校修課，碩士生第 4 年開始有幸從臺北地檢署調派士林地檢署擔任主任檢察官，猶記得人在士林地檢署時跟恩師林鈺雄老師報告，碩士班第 4 年終有時間開始起筆研究，希望能有機會跟隨林鈺雄老師撰寫論文，很幸運的獲得林鈺雄老師的首肯後開啟了論文的寫作。回想長達 3 年的碩士論文撰寫，幸好有林鈺雄老師指點明確方向，並時常給予研究方向上的提點，讓我隨時調整修正，讓我能在論文研究這條路上，艱辛且緩慢的前行。碩士論文撰寫的第 1 年初派主任，先生曾揚嶺又因調升臺東地檢署擔任主任檢察官，僅能每日撿拾工作結束、小孩入睡後的深夜或凌晨，每日 1、2 小時的慢慢累積，殊不知論文撰寫的第 2 年竟又因緣際會調任法務部檢察司辦事，檢察司海量的工作數度使我萌生放棄論文撰寫的念頭，卻又在家人的鼓勵下苦撐下來，猶記得論文的初胚版係在 2022 年暑假第一次參加 APEC 資深官員會議後居家隔離期間沒日沒夜的完成，之後又經歷 2 次的大修，撰寫謝辭的此刻，距離當時轉眼又過了 1 年。

2023 年暑假此刻即將完成碩士論文最後一哩路，同時也即將完成檢察司 2 年的調辦事生涯，於次月即將回歸最喜歡的檢察官辦案工作，心中無比充實輕鬆，回想在職進修的日子要感謝的人真的太多，最想感謝父親林詩能、母親徐碧瑛、公公曾武雄及婆婆張桂春一路以來幫忙我照顧女兒曾晨琋及兒子曾晨恩，讓我可以在母親的角色上，毫無後顧之憂地在工作上發展、學業上精進；感謝我的 2 個寶貝，女兒曾晨琋及兒子曾晨恩，「媽媽，你一定要畢業。」這句話，是我每次想要中途放棄時，時刻提醒自己堅持下去的動力，先生曾揚嶺不用多說，是我工作上最好的夥伴，人生中最好的搭檔，時刻「砥礪」我前行，讓我挖掘自己的無限可能。最後，最想感謝恩師林鈺雄老師，以及 2 位論文口試老師王士帆老師及溫祖德老師，對於在職生學術上的不足給予包容及鼓勵，讓我這位實務工作者也能一圓學術夢。文末，身為法務部檢察司一員，深知科技偵查法之重要以及推動立法之困難，願不久後，能盼到我國科技偵查法之問世，使司法正義得以實現。

林彥均 2023 年盛夏 謹誌於 自宅

doi:10.6342/NTU202301879

目錄

doi:10.6342/NTU202301879

doi:10.6342/NTU202301879

doi:10.6342/NTU202301879

第一章　緒論

第一節 前言

「你還在使用電話號碼打電話嗎？」，或者「全臺灣哪個軟體是 2100 萬人每天在使用的？」答案是 LINE。依照 LINE 公司 2019 年公布之臺灣用戶數據，在全臺灣 2300 萬人口數中，有 2100 萬人為 LINE 公司之用戶，滲透率高達百分之 90[1]。而人類對於網路通訊軟體之高度依賴現象，當然已是全球同步進行。隨著科技進步，網路時代之來臨，人手一支智慧型手機早已改變人們的生活方式，擁有複合式功能之網路通訊軟體，同時具備文字傳訊、多媒體傳訊、資料檔案傳輸、線上支付轉帳等功能，幾乎已全面取代傳統通訊方式。而當人類從實體生活，逐步線上化、虛擬化之同時，數據加密對於資訊安全而言，已是必要配備，加密技術對於保障個人資訊隱私、智慧財產、商業機密、網路安全等面向，均有其不可或缺之重要地位。

網路通訊軟體既具備通訊、資訊傳遞甚至線上支付轉帳等功能，軟體之隱私性及安全性，當屬消費者選擇使用網路通訊軟體時之重要考量，網路通訊商於自家軟體上紛紛推出強大之加密功能，於加密技術上相互競逐，端到端加密（End-to-End Encryption，縮寫 E2EE）即為時下大多數網路通訊軟體所使用之加密技術，儼然已成為時下網路通訊軟體之標準配備。

端對端加密技術是一種只有訊息發出方以及接收方得以讀取通訊內容資的通訊加密技術，端對端加密技術用來防止訊息遭竊取，除了參與通訊之使用者以外，包括電信商、網際網路服務商甚至軟體服務商，只要沒有解密金鑰之第三方都難以取得解密訊息，用以保障資訊傳遞之秘密性。

具有強大加密功能之網路通訊軟體，確實帶給人類使用網路通訊時之高

[1] INSIDE，台灣平均每人 200 好友！LINE 首公布台用戶數據，將新增好友分類、一鍵分享，2019 年 10 月 23 日，https://www.inside.com.tw/article/17901-line-friend-new-feature，最後瀏覽日 2023 年 6 月 24 日

doi:10.6342/NTU202301879

度隱私及安全，對於個人隱私、智慧財產、商業機密、網路安全甚至保護言論自由都有著重要貢獻。然而，加密技術使通訊全面保密之同時，亦使不法犯罪者如獲至寶，不同於傳統電信通訊執法機關依法得執行通訊監察且運作順暢，網路通訊軟體因有加密技術之加持，傳統通訊監察技術未能發揮效用，儼然成為犯罪者之最佳犯罪工具，造成世界各國犯罪偵查面臨嚴重挑戰，而此情形勢必日益嚴重。美國聯邦調查局局長 James Comey 在 2015 年曾以「黑暗將至」（Going Dark）一詞，針對加密技術對於執法機關造成之困境乙事下了註解，Comey 說：「FBI 無法杜絕恐怖組織（ISIS）透過社交媒體招募美國人，FBI 的任務是尋找各種蛛絲馬跡，但這些蛛絲馬跡卻因端對端的加密而愈發不可見，意謂著黑暗將至。」Comey 指出，ISIS 組織使用執法機關難以破解之加密技術。此種只允許裝置使用人讀取訊息內容之特性，雖具有保護個人隱私及創新之優點，但另一方面卻影響國家履行保護人民職責之能力。Comey 表示執法機關必須其中取得平衡點，並且強調 FBI 希望的不是後門（back-door），而是在法律授權許可下使用前門，以此方式調查蒐集偵查犯罪及避免恐怖攻擊所需要的證據及資訊[2]。

加密通訊與國家執法兩者間衝突之角力，近來已於世界各國掀起廣泛之討論甚至爭辯，並正掀起一波立法浪潮，嘗試透過立法於支持加密技術發展之同時，規範科技公司之責任及義務，使加密技術不至於成為犯罪者之溫床。

第二節 網路通訊軟體之發展

第一項 即時通訊軟體之興起

即時通信軟體(Instant Messaging, IM)是一種即時的訊息傳遞系統，兩人或多人透過網際網路的鏈結，使用文字、語音、圖片、檔案或視訊進行交

[2] James B. Comey, *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy Statement for the Record*, FBI official website, (July 8, 2015), https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy, last visited 06/24/2023.

doi:10.6342/NTU202301879

流。即時通訊軟體不同與傳統的電子郵件，它的會話交談是即時進行的，進行對話的雙方，就好比是面對面的交談一樣，也因為這樣的即時特性，致使即時通訊軟體對我們的工作、生活以及其他的各種層面，產生了重大的改變。

即時通訊軟體最早出現在個人電腦上，由於其便利性、即時性，受到歡迎的即時通訊軟體非常的多，包含了 Windows Live Messenger（MSN）、AOL、Skype、WhatsApp、 Yahoo！Messenger、QQ、WeChat、LINE、Jabber 等等，所有的即時通訊軟體都來自於芬蘭 1988 年所設計的 IRC（Internet Relay Chat）軟體的啟發，原先 IRC 設計的初衷是希望使用者在閱讀電子佈告欄文章的同時也能即時的建立群組討論與談，軟體應用持續創新演變至今，除了群組討論的功能外，即時通訊軟體更注重人與人之間一對一的即時交談[3]。

第二項　端對端加密技術

端到端加密（End-to-End Encryption，縮寫 E2EE）是透過加密技術達到只有通訊軟體使用人才可經由裝置獲取解密後通訊內容之技術，端對端加密技術用來防止訊息遭竊聽，包括電信服務商、網際網路服務商甚至通信服務商，只要沒有解密金鑰之第三方都難以取得解密訊息，用以保障訊息傳遞時之秘密。

PGP（Pretty Good Privacy）是第一個免費的端對端訊息加密軟體，其中軟體程序由 Phil Zimmermann 編碼，於 1991 年發佈。其原理是利用公開鑰匙密碼學，產生公鑰與私鑰，當加密資訊傳送時雙方先取得對方之公鑰並以此方式進行加密傳輸，當接收後再使用私鑰進行解密。

目前時下各網路通訊商所推出之網路通訊軟體，幾乎都已採用端對端加密技術來保障客戶之資訊安全，而其加密傳輸之原理，大致上均是由發送

[3]秦裕國，行動即時通訊軟體安全設定認知之研究—以 LINE 為例，東吳大學商學院資訊管理學系碩士論文，2016 年 6 月，頁 4、14。

doi:10.6342/NTU202301879

端將所傳輸之資料先行加密，經由伺服器傳給接收端，而資料到達接收端時，須經由解密才能看到發送端傳送之資料內容，而其傳輸過程都是經由封包之形式進行傳送。理論上，資料經過中繼站的伺服器時，會將資料留存在中間經過之伺服器內，而當中間經過的中繼站伺服器不僅一處時，而資料將會留存在這些中繼伺服器上，造成資安之疑慮。而端對端加密（End-to-End Encryption）加密技術之技術原理是發送端及接收端都擁有一把專屬於自己的鑰匙，當發送端將資料傳給接收端時，會下載接收端的鎖頭，將資料加密以及要傳送給何人之身分證明章，待接收端接收到加密之資料後，經由自己的鑰匙解密，即可取得資料之原始內容。反之，過程中任何其他人以攔截等方式取得之資料，因無解密鑰匙，取得之資料也只是一堆亂碼，無法取得可供讀取形式之原始資料[4]。

第三項　網路通訊軟體使用端對端加密技術之現況

全球用戶自 2016 年 2 月已超過 10 億之 WhatsApp，自 2016 年起全面使用端對端加密技術，WhatsApp 公司宣布，全面使用端對端加密技術以此方式對軟體使用者提高資安保護層級，且避免傳輸內容受到監控。WhatsApp 使用的加密技術來自「Signal」加密通訊軟體。WhatsApp 公司 2020 年 10 月公布之加密白皮書上表示：WhatsApp 公司伺服器上沒有儲存任何客戶端身分驗證密鑰，若伺服器的用戶數據庫遭到破壞，也不會洩露任何用戶驗證密鑰。而 WhatsApp 公司均使用白皮書中概述的相同信號協議，WhatsApp 伺服器無法訪問客戶端的密鑰[5]。

LINE 採用者傳輸層加密技術，對於軟體提供之訊息提供公司所開發端對端加密協定(即 Letter Sealing）之服務，Letter Sealing 自 2015 年 8 月起

[4] 黃逸玲，行動通訊 APP 偵查與對策之研究，中央警察大學刑事警察研究所碩士論文，2018 年，頁 25。

[5] WhatsApp Official Website, *WhatsApp Encryption Overview Technical White Paper*, Version 3 (Oct. 22, 2020), https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf, last visited 06/24/2023.

doi:10.6342/NTU202301879

啟用，目前均已成為預設為開啟之功能，由用戶端一開始產生一對 Letter Sealing ECDH 金鑰，存放在用戶端，並上傳公鑰至 LINE 伺服器，再從 LINE 伺服器傳回一個唯一的金鑰代碼[6]。依照 LINE 公司公布之官方資料，LINE 公司目前是使用 2048 位元的 RSA 加密規格，比其低階的 RSA-1024 加密規格使用一般電腦至少必須 2000 年以上才能破解，若是嘗試以具備 640 個節點的超級電腦 ES2，也要超過 10 年才能破解金鑰，以摩爾定律（Moore's law）計算，RSA-1024 加密規格的安全期限落在 2019 年，而 LINE 公司係使用更高規格的 RSA-2048，安全性更高。LINE 公司亦對外公布 LINE 軟體傳輸通道係使用 HTTPS（具備 SSL 層之 HTTP 傳輸通道），以此方式避免傳輸過程內容遭到監聽或截取。最重要的是，訊息只會在伺服器上短暫停留不會儲存[7]。

Signal 的市場競爭策略則是以其極高之加密安全性為主打，以維基解密之前 CIA 探員史諾登（Edward Snowden）為 Signal 之最佳代言人，於官網上標榜 Signal 為最安全之通訊軟體[8]，網路新聞分析 Signal 之安全性最高，因 Signal 由非營利組織營運，標榜伺服器不會儲存、備份使用者之傳輸之內容，軟體預設使用端對端加密功能，Signal 公司更對外直接宣布配合各國司法機關提供者僅限用戶的註冊日以及使用的最後時間[9]。

從上述 LINE、WhatsApp 及 Signal 等各家通訊軟體商對外公告之加密政策不難發現，宣稱連通訊軟體商亦無解密金鑰，或無留存用戶資料及通訊內容等，已是各家通訊軟體商共同之商業模式或競爭策略，就軟體通訊商而

[6] LINE Official Website, *LINE Encryption Overview (Technical Whitepaper) ver. 2.0* (Oct. 2019), https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver2.0.pdf, last visited 06/24/2023.

[7] 認識 LINE 的點對點加密功能：Letter Sealing(訊息保護)，LINE 台灣官方 BLOG，2020,5,15，http://official-blog.line.me/tw/archives/78352086.html，最後瀏覽 2023 年 6 月 24 日。

[8] Signal 官網，https://signal.org/#signal，最後瀏覽 2023 年 6 月 24 日。

[9] TN Choice，降低被監控的風險，常用通訊軟體哪個最安全？，Teck News 科技新報，2023 年 6 月 14 日，https://technews.tw/2021/01/14/common-communication-software/，最後瀏覽日 2023 年 6 月 24 日。

doi:10.6342/NTU202301879

言，不僅可以據此迴避各國政府立法要求之配合義務，更可以此吸引消費者。以 Signal 為例，資料分析平台 SensorTower 數據發現，在美國近來因為種族及警察執法行為所衍生之示威抗議行動升溫期間，Signal 的下載量也跟著暴增，2020 年 5 月 26 日爆發抗議種族歧視及警察暴行之示威遊行以後，Signal 下載使用量有巨量之暴增（從單日低於 8,000 提升到 26,000 次）APP 下載排名也明顯提升（從第 936 名提升到第 126 名）[10]。香港反送中運動中參與示威行動者大量使用 Telegram 通訊工具亦是一事例，香港反送中運動中示威者普遍使用 Telegram 軟體進行聯繫，因使用者相信，Telegram 軟體可以避免訊息遭到官方之監聽掌控，相關報導指出在香港反送中運動期間 Telegram 竟成立了破百個與反送中運動相關群組，示威者利用群組交換抗爭行動所需資訊。Telegram 為保護用戶之身分，更升級使用戶得以隱藏註冊時使用之手機門號，防止用戶身分曝光[11]。上開現象均顯示，通訊軟體加密之安全性、用戶數量之消長以及國家對於各該通訊軟體之監察可能性，均呈現密切相關，國家越是難以實施監察之通訊軟體，以用戶之立場而言，具有更高之吸引力。

第四項　端對端加密技術對犯罪及執法之影響

通訊軟體加密之安全性與用戶數量之正相關現象，在不法犯罪者之使用傾向更是明顯可見，美國聯邦調查局（FBI）及世界多國執法機關進行「特洛伊之盾」（Trojan Shield）跨國執法合作行動，於 2021 年 6 月同步收網，最終達成全球同步緝獲多達 800 餘名不法罪犯之驚人成果。「特洛伊之盾」（Trojan Shield）執法行動源自於加拿大地下通訊商「幻影保全」（Phantom Secure）在 2018 年遭到國際刑警取締後，同意和警方合作以換取減刑機會，

[10] Jason Liu，全美示威潮》前 CIA 探員史諾登都力推！Signal 加密通訊軟體下載量狂速成長，Block Tempo 即時新聞，2020 年 6 月 5 日，https://www.blocktempo.com/signal-face-blurring-tool-ios-android-update/，最後瀏覽 2023 年 6 月 24 日。

[11] 德國之聲，允許用戶隱藏手機號碼　加密通訊軟體 Telegram 升級保護香港示威者，風傳媒，2019 年 09 月 01 日，https://www.storm.mg/article/1656770，最後瀏覽 2023 年 6 月 24 日。

doi:10.6342/NTU202301879

而開發出標榜不受執法機關監察之「ANoM」通訊軟體，在黑幫、跨國販毒等犯罪集團間使用，而 FBI 因在軟體中設置了獲取通訊資料之後門，因此獲取大量犯罪證據，以此方式針對全球不法犯罪進行調查、蒐證，於時機成熟後再全球同步收網[12]。「ANoM」臥底軟體之成功，也許可認是執法機關成功搶下一役，但絕非長遠之計，因「ANoM」臥底軟體之誕生，所花費之代價為 120, 000 美元並給予犯罪者減刑之機會[13]，遑論同樣的「木馬屠城記」難有一演再演之機會。

除此之外，執法手段背後之法律授權依據更是程序合法之前提要件，在歐洲多國掀起之「EncroChat 執法合法性爭議」則為一真實案例。EncroChat 為一家創立於 2016 年之歐洲電信網路公司，以販售內建加密傳訊程式裝置之 Android 加密電話為業，每支售價 1, 000 歐元， 6 個月的使用費用為 1, 500 歐元，EncroChat 手機拿掉了一般常見之功能（如 GPS、鏡頭、麥克風及 USB），但具備以下特殊功能:1. 採用 2 個作業系統，方便犯罪者能在犯罪模式及一般模式中任意切換。2. 輸入特定密碼即可移除裝置。3. 連續輸入錯誤密碼時裝置會自動刪除所儲存資料甚至是通訊方收到之訊息[14]，因而於 2016 年至 2020 年間在歐洲被廣泛用於非法活動，伺服器設於法國境內。法國警方發現 EncroChat 手機廣泛遭犯罪者使用後，於 2017 年啟動調查，與荷蘭警方、歐洲刑警組織 Europol、歐洲司法組織 Eurojust 等進行跨國合作，透過架設伺服器，以伺服器連結至 EncroChat 手機後傳送惡意程式，達成破壞手機裝置之內容刪除功能，亦同時記錄手機密碼與複製應用程式資

[12]盧睿鋐，FBI 秘密開發「罪犯專用通訊軟體」一網打盡全球 800 名罪犯，上報，2021 年 6 月 7 日，https://www.upmedia.mg/news_info.php?SerialNo=115504，最後瀏覽日 2023 年 6 月 24 日。

[13] Tom Allard, *How an informant and a messaging app led to huge global crime sting*, REUTERS (June, 08, 2021), at https://www.reuters.com/world/how-an-informant-messaging-app-led-huge-global-crime-sting-2021-06-08/, last visited 06/23/2023.

[14] 行政院國家資通安全會報技術服務中心，歐洲摧毀 EncroChat 加密通訊網路，行政院國家資通安全會報技術服務中心官網，2020 年 7 月 2 日，https://www.nccst.nat.gov.tw/NewsRSSDetail?seq=16423，最後瀏覽日 2023 年 6 月 24 日。

doi:10.6342/NTU202301879

料，並同時躲避偵測，以此方式蒐集大量犯罪事證[15]，EncroChat 公司不敵執法機關之攻勢，最終於 2020 年 6 月 13 日向用戶發送緊急訊息，通知用戶“我們的域名已被政府實體沒收，建議您立即關閉電源並進行處理所持用之裝置”。依照荷蘭警方所發布之新聞，荷蘭警方透過此次行動查獲 19 個冰毒實驗室、查扣 10 噸古柯鹼和數千公斤之冰毒，逮捕了上百人；英國警方亦因此逮捕 746 名犯罪嫌疑人，追回超過 5400 萬英鎊犯罪所得，查扣包括 AK-47 突擊步槍在內的 77 支槍和 1800 發子彈[16]。法國警方透過此跨國執法行動蒐集到之 EncroChat 傳輸訊息之證據合法性，在後續的刑事訴訟中遭到被告辯護律師之挑戰，辯護人爭執：法國警方逾越令狀授權範圍，且法院核發令狀逾越了法國刑事訴訟法，應屬無效，其中一項受到律師強烈質疑者為法國警方要求 OVH（法國雲端運算公司）修改網絡以執行攔截令狀，律師主張：縱使刑事訴訟法第 706-102-1 條授權透過 IMSI 捕捉器或使用電信營運商設備之方式攔截訊息，但並未容許以改寫伺服器轉移百分之百流量之方式攔截訊息，是以法官「修改網路路由」的命令並不符合上開法條之授權，據此主張證據應予排除[17]。而法國南西上訴法院（Cour d' appel Nancy. ）並未採納被告律師之主張，認定法國警方攔截訊息之行為係在法國法律授權範圍內，律師續向最高法院聲請召開聽證會[18]，法國最高法院於受理後，於 2022 年 2 月 1 日認為本案涉有(1)法院之授權攔截命令將 EncroChat

[15]Europol/Eurojust joint press release, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, Europol Official Website（Aug. 01, 2020）, at https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, last visited 06/24/2023.

[16] France 24, *Police arrest more than 800 in crackdown on EncroChat, encrypted phone system used by organised crime*(July 03, 2020), at https://www.france24.com/en/20200703-france-united-kingdom-netherlands-police-arrests-cyber-crime-hacking-encrochat, last visited 06/24/2023.

[17] Archyde, *appeals are multiplying against French justice*, (03/10/2021), at https://www.archyde.com/appeals-are-multiplying-against-french-justice, last visited 06/24/2023.

[18] Bill Goodwin, *Lawyers take EncroChat hacking operation to French supreme court, Computer Weekly* (July 15, 2021), at https://www.computerweekly.com/news/252504038/Lawyers-take-EncroChat-hacking-operation-to-French-supreme-court, last visited 06/24/2023.

doi:10.6342/NTU202301879

流量重新路由到法國憲兵隊控制之擷取設備，並未記載授權時間、(2)在上開命令之後之延長期間命令是否無效、(3)法院所為網路修改命令是否違法、(4)攔截是否應僅限於法國境內使用之手機及(5)得否以國防機密為由拒絕公開資料[19]，牽涉憲法解釋，於 2022 年 2 月 1 日向法國憲法委員會聲請釋憲[20]。

法國憲法委員會於 2022 年 4 月 8 日就本案所涉之違憲先決（QPC）問題做出決定（Décision n° 2022-987）認定：立法者有責任一方面確保辯護權和對抗性原則之調和，另一方面確保犯罪調查及維護國家根本利益等憲法價值，而國防秘密為其中一部分，法國《刑事訴訟法》第 706-95-11 條等規定，適用於組織犯罪和針對違法行為之特殊調查技術，包括獲取電腦數據，同法第 706-102-1 條規定旨在讓負責調查之當局能夠從有效數據收集和澄清手段中受益，但不會因此削弱情報部門，使其揭露相關技術行動，其目的係為追求調查犯罪之憲法價值，並維護國家根本利益，其次，此特殊偵查手段僅限自由和拘留法官或預審法官授權並有正當理由時用於特別嚴重和複雜之犯罪，依此蒐集之證據須依據刑事訴訟法第 706-95-18 條加以保密。若因此造成某些屬於國防機密之內容免於對抗性，相關法律定有資料保留之規定，且依國防法第 2312-4 至第 2312-8 條規定，法院可以要求對屬於國防機密的訊息解密。綜上所述，系爭規定在上述憲法要求之間取得了平衡，並未違反被告獲得有效司法救濟、尊重私人生及言論自由等憲法保障權利，並未違憲[21]。

除了法國之外，因為 EncroChat 行動攔截到之犯罪證據於歐洲多國刑事

[19] 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 62-63。

[20] LE CONSEIL CONSTITUTIONNEL A ÉTÉ SAISI le 2 février 2022 par la Cour de cassation (chambre criminelle, arrêt n° 173 du 1er février 2022.

[21] Décision n° 2022-987 QPC du 8 avril 2022., at https://www.conseil-constitutionnel.fr/decision/2022/2022987QPC.htm

doi:10.6342/NTU202301879

訴訟程序中使用，包含法國、荷蘭、英國及德國之多國法院同樣面對EncroChat 證據合法性之法律爭議，德國柏林地方法院 2021 年 7 月 1 日所為之判決，為第一個認定法國及荷蘭警方以此行動取得之訊息證據不具證據能力之判決，德國柏林地方法院認為：縱使系爭行動證據之蒐集符合法國法律，然將於此行動蒐集到之證據用於德國境內仍違反德國內國法之規定，因法國國家憲兵以植入木馬之方式，監視 122 國家境內超過 3 萬名手機使用者，並非全部監視對象均有證據證明其涉有犯罪嫌疑，據此認定系爭干預手段無法通過比例原則之檢視，應屬違法。

惟本案經德國檢察官提起上訴後，德國上訴法院推翻原判決，認定系爭行動所得證據具有證據能力，主要理由為:法國所採取之執法手段，縱使未能符合德國內國法之程序規範，但並不必然造成證據無法在德國刑事訴訟中使用之必然結果，而允許法院對於證據能力進行權衡，本案證據係屬偶然發現，依據德國刑事訴訟法第 100e 條第 6 項之規定是允許例外使用，此外，經權衡本案侵害法益以及所涉犯行，法院認為若證據排除亦已違反德國一般人民之法感情。另外，德國上訴法院更揭示:相互承認法院判決和決定之原則適用於歐洲，依照法國法取得之調查結果也可用於德國，本案德國政府並未參與系爭合法性爭議之執法行為，相關資訊係是在沒有事先諮詢之情況下由法國政府主動提供予德國政府，在證據調查並非基於德國發出之互助請求之前提下，德國法院無權對於其他歐盟成員國家發起符合該國內國法規定之執法行動進行合法性檢視，若如此恐將破壞歐盟成員國彼此間之相互信任[22,23]。

綜上，上述 2 個成功之大規模跨國執法行動更突顯執法機關面對加密

[22] Rechtsprechung KG, 30.08.2021 - 2 Ws 79/21, 2 Ws 93/21.

[23] Gerichte in Berlin, *Kammergericht lässt in einem Rechtsstreit über die Eröffnung eines Hauptverfahrens „EncroChat "-Daten als Beweismittel zu (PM 33/2021)*, (Sep. 2, 2021), at https://www.berlin.de/gerichte/presse/pressemitteilungen-der-ordentlichen-gerichtsbarkeit/2021/pressemitteilung.1122143.php, last visited 06/24/2023.

doi:10.6342/NTU202301879

時代所帶來之執法衝擊，技術與法制必須相輔相成，若未有明確穩固之法律授權基礎為後盾，罪犯落網後直至最終定罪之司法程序，恐將面臨另一場更為艱難之法律戰。

第三節　本文研究動機及目的

隨著網路通訊軟體之普及化以及日益增加之附屬功能，軟體之隱私性及安全性不僅為消費者選擇使用時之重要考量，更係網路通訊商爭取客戶支持之重要條件，隨著端到端加密技術成為時下網路通訊軟體之標準配備，於普羅大眾因加密技術享有更高規格資訊安全保護之同時，犯罪行為也因此受到掩蓋，甚至越是標榜國家難以實施監察之通訊軟體越是受到犯罪者之青睞，此從 Telegram(紙飛機)網路通訊軟體官網標榜自家軟體有閱後即焚(self-destruct)之隱私功能[24]，在我國已成為現今犯罪集團普遍愛用之犯罪聯繫工具[25]即可得到印證。

世界各國執法機關面對加密通訊軟體對執法之衝擊，雖已有法國、荷蘭、歐洲刑警組織 Europol、歐洲司法組織 Eurojust 於 2017 年至 2020 年之 EncroChat 跨國執法行動，以及 2021 年美國 FBI 之「特洛伊之盾」(Trojan Shield) 執法行動等，成功取得犯罪集團使用加密通訊軟體之犯罪事證而破獲不法，然而從後續案件於司法程序衍生之執法合法性抗辯中不難發現，具有經得起後續檢視之執法依據，方能使查緝不法犯罪之成果得以維繫。從而，以科技偵查手段對抗加密技術對執法之衝擊，法制規範面之重要性，不言可喻。

本文希冀能透過我國現行法制與外國近來立法趨勢相互比對，突顯我國面對加密通訊軟體對執法衝擊實施應有立法對策之重要性及必要性，再

[24] Telegram 官網，https://telegram.org/，最後瀏覽日 2023 年 6 月 24 日。
[25] 自由時報，詐團愛用 Telegram 「閱後即焚」功能可滅證，2022 年 11 月 9 日，https://news.ltn.com.tw/news/society/paper/1550560，最後瀏覽日 2023 年 6 月 24 日。

doi:10.6342/NTU202301879

分析並比較近年來法制先進國家為對抗加密所為立法，分析比較法上不同國家之立法模式，提出我國因應加密技術對執法之衝擊可力求突破之立法對策。

第四節 研究範圍及方法

本文研究範圍以法律層面探討為主，涉及技術層面部分因涉及其他專業領域，僅為初淺介紹以利讀者理解，研究主軸圍繞針對加密技術對執法之衝擊外國之立法趨勢、刑事訴訟干預手段與憲法基本權之關係，以及回歸到我國法律體系下可行之立法方式。

本文研究方法採比較研究法與文獻歸納分析法：

（一）比較研究法

世界各國執法機關近年來面臨相同來自加密技術之衝擊，加上歐洲近幾年接連發生多起重大恐怖攻擊事件，於內國法發起對抗加密技術之立法，於歐洲掀起一波對抗加密之立法浪潮，於本文開始研究之初，國內針對德國法上有關科技偵查之法制介紹已有相對上較為豐富之資料，然對於其他國家之介紹較少。是以，本文除德國以外，另挑選英國、法國、荷蘭及澳洲作為研究重點，將研究重點放在上開國家近來法制細節介紹，並擴及新法施行後之觀察及檢討，以上開國家之法制資料、官方報告及學術文獻作為比較法研究對象，於我國科技偵查法制尚未建立之際，參考上開國家之比較法經驗，作為我國未來立法之借鏡。

(二)文獻歸納分析法

本文將嘗試整理歸納並分析國內外針對與「對抗加密立法」以及「科技偵查」相關之國內外法律規範、判決、期刊、著作、研究報告及新聞報導等，形成對於本文研究主題之完整介紹，並透過比對分析並加上本文意見之方式，形成本文結論，對於我國法制做出具體建議。

doi:10.6342/NTU202301879

第五節　本文架構

本文共分為六個章節，第一章序論著重於加密技術發展之介紹，並點出技術發展之現況已對執法產生重大衝擊，建構本文問題意識。第二章從加密通訊監察對世界各國之執法衝擊出發，以國際組織、多國聯盟針對犯罪者因加密技術獲利，致使犯罪更容易受到隱匿所發出之嚴正聲明為例，突顯點出世界各國面臨之執法困境，再帶回我國現況，分析在現行通訊保障及監察法之下，因社會普遍改用具備端對端加密技術之網路通訊軟體，現況面臨通訊監察無用武之地之執法困境，以突顯我國與世界各國執法機關面臨相同之執法挑戰，並進一步分析目前各國普遍採用之立法對策初步可分為「解密義務」、「國家木馬」2 種類型，並為概括之介紹。第三章本文挑選英國、法國、德國、荷蘭及澳洲等 5 個近來針對「對抗加密」經歷修法之法制先進國家，針對修法前後之法制規定以及立法過程進行細部介紹，並推導出進行立法架構規劃時，應針對不同之科技偵查手段所干預之基本權予以區分及討論，方能依其基本權干預種類及強度為程度相當之立法設計。第四章進入我國法制探討，自刑事訴訟干預手段與憲法基本權關係出發，分析傳統刑事訴訟程序與新興科技偵查手段基本權干預之差別，並觀察我國現行刑事訴訟法強制處分體系下有關層級化授權之立法脈絡，探討國家木馬可能涉及之基本權干預，再點出我國法制落後之現狀，帶出立法方向建議。第五章針對我國對抗加密技術之立法對策，具體提出設備端通訊監察、秘密線上搜索以及解密義務之立法芻議以及具體建議草案條文。最後，於第六章綜整本文各章節重點，以作為本文整體結論。

doi:10.6342/NTU202301879

第二章　加密通訊軟體對執法之衝擊

第一節 加密技術對於世界各國執法機關之衝擊

隨著加密技術之技術普及化，不僅是網路通訊軟體，幾乎所有現今數位時代之軟硬體設備均普遍使用加密技術作為資訊安全之基本配備，然而，資安保護以及對於執法之阻礙本是兩面刃，觀察近年來世界各地所發生不法犯罪者利用加密通訊軟體作為犯罪屏蔽之重要事件，即可清楚發現加密技術對於世界各國執法之衝擊，至為嚴重。

第一項　恐怖主義攻擊

加密技術對於世界各國執法機關之衝擊，隨著恐怖攻擊、伊斯蘭武裝組織國崛起等重大恐怖攻擊事件發生，各國政府將未能有效遏止及查緝之主因，歸因加密技術造成執法機關與犯罪者之間的武器不對等，多個國際組織不約而同發出立法倡議，而諸多立法先進國家用以制衡加密技術之立法更如雨後春筍般冒出。同時間，這些新法所創設之干預手段，對於人民基本權利是否造成過度侵害之敏感問題，更持續受到廣泛討論。

以 2016 年法國反恐法之修法過程為例，支持修法方即以 2015 年所發生之巴黎恐怖攻擊事件為例，主張：2015 年法國司法警察資訊及科技軌跡服務中心（le service central de l’ informatique et des traces technologiques de la police judiciaire.）處理之 133 件手機鑑識分析案件中，至少 8 件面臨手機無法解密之困境，其中包含在 2015 年 11 月巴黎恐怖攻擊事件中查扣之 iPhone4S，以及因涉嫌策畫 2015 年對巴黎南郊猶太城(Villejuif)一座教堂發動恐怖攻擊，而於 2015 年 4 月遭逮捕之阿爾及利亞籍嫌犯葛蘭（Sid Ahmed Ghlam）所持用之手機。葛蘭遭捕入獄後，更遭發現其夾帶手機入

doi:10.6342/NTU202301879

獄，對外聯繫超過 6 個月始遭發現，相關對外聯繫紀錄至 2015 年 11 月 13 日便中斷，該日即係巴黎恐怖攻擊發生之日，而法國國家安全局局長邁克爾·羅傑斯將軍（L'amiral Michael Rogers）更曾公開表示「如果沒有加密，就可以避免巴黎襲擊。」[26]

英國 2017 年 3 月 22 日在倫敦西敏寺所發生之恐怖攻擊事件，英國內政大臣（Secretary of State for the Home Department, Home Secretary）也曾公開指出，恐怖攻擊份子是透過 WhatsApp 加密通訊軟體來躲避警方及情報單位之監聽[27]。

第二項　兒童及少年性剝削及網路誘拐

加密技術發展所造成兒童及少年性剝削即網路誘拐犯罪猖獗且難以遏止之問題，亦為世界各國執法機關所關切，依照聯合國兒童基金會估計，3 分之 1 的互聯網用戶是兒童，依照 WePROTECT 全球聯盟（由 98 個國家、39 家全球科技企業和 41 個領先的 NGO 組織組成的聯盟）所出具之 2019 年全球威脅報告[28]中，明確闡述了端對端加密技術對兒童上網帶來高度及嚴重之風險，報告中指出“公開社會大眾使用之社交媒體和通信平台仍然是網路世界中認識及誘拐兒童的最常用方法。2018 年，美國國家失踪和受虐兒童中心（National Center for Missing & Exploited Children，簡稱 NCMEC）處理之全球 1840 萬份兒童性虐待內容報告（child sexual abuse material，簡稱 CSAM）中，Facebook Messenger 負責其中之 1200

[26] *Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 221* (Feb. 25, 2016), at http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp, last visited 06/24/2023.

[27] 陳芊儒，通訊軟體加密技術下個隱私與國家安全保護之平衡，科技法律透析，2019 年 9 月，第 31 卷第 9 期，17 頁。

[28] WePROTECT Global Alliance, *2019 Global Threat Assessment*, at https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf, last visited 06/24/2023.

doi:10.6342/NTU202301879

萬份，NCMEC 在 2019 年 10 月 3 日發表了一份聲明[29]，指出：“現行於網路上用來偵測兒童性虐待內容之工具，在端對端加密技術之環境下是失效的，故於端對端加密技術被設定為預設狀態之情形下，報告面臨了高度遺失風險，如果在沒有解決方案來保護兒童的情況下實施端到端加密，NCMEC 估計一半以上有關全球網路兒童性剝削內容之 CyberTipLine 報告[30]內容將消失。”

第三項 2020 年五眼聯盟聯合聲明

2020 年 10 月，美國、英國、澳洲、加拿大和紐西蘭組成的五眼聯盟，與印度、日本針對加密技術對公共安全造成之重大挑戰，發出聯合聲明表示，聲明中表示:端對端加密技術之發展致使政府監督成為不可能，「對公共安全構成重大挑戰」。五眼聯盟指出：「各國政府和國際機構間認為必須採取行動的共識與日俱增。」「雖然加密相當重要，隱私權和網路安全也必須獲得保護，但不應該犧牲到完全排除執法，和讓科技產業無力對抗最嚴重線上非法內容及活動的地步。」五眼聯盟呼籲科技公司「將公共安全嵌入系統設計內」，「以易讀且可使用的格式」讓執法單位得以進入[31]，可謂迄今最強烈的多國聯合聲明。

---

[29] National Center for Missing & Exploited Children official website, *NCMEC's Statement Regarding End-to-End Encryption,* (Oct. 3, 2019), at https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption, last visited 06/24/2023.

[30] NCMEC 的 CyberTipline 是全國針對全球網路有關兒童性剝削內容之集中報告系統。公共和電子服務商（如 Google、Facebook 等）發現網路上有關誘拐兒童進行性行為、兒童性騷擾、兒童性虐待、兒童色情旅遊、兒童性交易、未經請求發送給兒童的猥褻訊息、誤導性域名和誤導性內容、互聯網上的文字或數字圖像等資訊時，會向 NCMEC 提交報告，NCMEC 後續會將報告轉給所屬國家之執法機關，這類報告通常稱為 CyberTipLine 報告或 CyberTips。註參 National Center for Missing & Exploited Children, CyberTipLine Overview, https://www.missingkids.org/gethelpnow/cybertipline, last visited 06/24/2023.

[31] The United States of Department of Justice Office of Public Affairs, *International Statement: End-To-End Encryption and Public Safety*, (Oct. 11, 2020), at https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety, last visited 06/24/2023.

doi:10.6342/NTU202301879

第二節 加密技術對於我國執法之衝擊

我國執法機關現行實施通訊監察之法律依據係通訊保障及監察法，本法固授權執法機關可在符合法定要件及程序之前提下實施通訊監察，然而，自網路通訊軟體已幾乎可謂全面取代傳統電信通話，且端對端加密技術亦普遍運用於網路通訊軟體，我國通訊監察機關攔截到之訊息實為無法讀取之一連串亂碼，我國執法實務面臨通訊監察日益無用化之挑戰，亦與世界各國執法機關相當。

第一項 我國通訊監察法制現況

我國通訊保障及監察法於 1999 年公布施行，嗣後歷經 2006 年、2007 年、2014 年、2016 年 2018 年多次修正，同時期網路通訊技術雖然已逐漸普及，但歷次修法並未對此進行任何增修。

網路通訊與傳統電信通訊就傳輸方式具有相當之差異，傳統電話透過迴路交換（Circuit Switch），系統在通話時會建立亦專屬線路供通訊之雙方使用，該線路係專屬，不會受到其他通訊之干擾。反之，網路通訊如同網路傳輸，採封包交換（Packet Switch）方式，網路通訊各方透過廣播方式，以封包辨識技術確認封包傳送之對象，並非專屬線路[32]。

依照通訊保障及監察法第 3 條第 1 項第 1 款規定「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。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

[32] 王晴玲，對已具加密功能之通訊軟體之通訊監察之理論與實務，出國報告（出國類別：研究），2015 年 11 月 20 日，頁 39。

doi:10.6342/NTU202301879

待者為限。」，上開條文所述之「電信設備」，參照電信法第 2 條第 1、2 款規定「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。二、電信設備：指電信所用之機械、器具、線路及其他相關設備。」網際網路通訊既屬利用通信設備發送、儲存、傳輸或接受符號、文字、影像及聲音等，核屬通訊保障及監察法規範之「通訊」，依現行法可執行通訊監察，當無疑問。

我國目前通信監察實務上，網際網路通訊監察之監察客體包括以下幾種監察對象：

（一）　以特定 IP 網際網路位置（IP Address）為對象:

IP 位址又稱網際網路上的虛擬地址，功能在於提供網路資訊傳遞及接受過程中辨識傳遞位置，因 IP 位置具有獨立之特性，因次可透過特定 IP 發出郵件或連線主機之 IP 位置進行追蹤[33]。

（二）　以特定電子郵件帳號（E-mail 帳號）為對象:

當偵查機關欲取得特定對象之電子郵件內容時，係以郵件是否屬於秘密通訊自由之保護範圍來區分，針對業已結束之秘密通訊（即收件人已在服務提供者伺服器的網頁郵箱讀取電子郵件或線上讀取完畢而繼續留存在自己的電子郵件信箱裡時，即為已結束之秘密通訊，執法機關應依照搜索、扣押之規定為之；然而，當偵查機關對進行中之電子郵件內容進行監聽[34]，因已涉及通信內容之「攔截」與「開拆」，則應依通訊保

[33] 王晴玲，對已具加密功能之通訊軟體之通訊監察之理論與實務，出國報告（出國類別：研究），2015 年 11 月 20 日，頁 43。

[34] 一般將電子郵件傳輸分為四階段：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

doi:10.6342/NTU202301879

障及監察法取得通訊監察書。

（三）　以特定網路電話帳號（SKYPE 帳號）為對象

監聽「傳輸中」電子郵件之方法有以下 3 種[35]：1、在監聽機房裝設截錄器進行節點封包之截收。2、執法機關要求電信業者或 ISP 業者將伺服器上受監察人的電子郵件，透過轉寄的方式交給監察機關。3、監聽機關進入業者機房同步截收[36]。

觀諸上開我國現行實務上，針對網際網路實施通訊監察之 3 種監察客體，均非現行網路通訊市場上占比最高（甚至最為犯罪者所青睞）之網路通訊軟體，且觀察 110 年地方法院核准通訊監察案件之統計數據，以特定 IP 網際網路位置（IP Address）為對象共 1 線、以特定電子郵件帳號（E-mail）為對象共 5 線、以特定網路電話帳號（Skype）為對象共 3 線。然而，使用網路通訊軟體發送文字、語音及圖像等訊息，既屬通訊保障監察法規範及依法授權執法機關得實施通訊監察之範圍，已如上述，何以實務上並未針對網路通訊軟體執行監聽？主要障礙存在於網路通訊服務商是否與傳統第一、二類電信業者同樣擔負通訊保障及監察法所訂定協力義務？尚

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；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。在 A 和 C 階段，應該且只能依通訊監察規定保全電子郵件，郵箱服務提供者依法負有協助義務，在 D 階段通訊均已結束，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，此時通訊均已結束，不再受秘密通訊自由保護，適用扣押規定保全電子郵件，B 階段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，應適用通訊監察規定，然德國聯邦憲法法院 2009 年表示是用扣押規定，「扣押」伺服器為讀取的電子郵件已成德國實務定見。上開說明參王士帆，〈網路之刑事追訴—科技與法律的較勁〉，《政大法學評論》，第 145 期，2016 年 6 月，頁 358-359。

[35] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院碩士在職專班科技法學組碩士論文，2005 年 6 月, 頁 83。

[36] 王晴玲，對已具加密功能之通訊軟體之通訊監察之理論與實務，出國報告（出國類別：研究），2015 年 11 月 20 日，頁 44。

doi:10.6342/NTU202301879

屬存疑（詳參本文第二節、第一項《業者之協力義務》）。此外，更為實際之困境為網路通訊軟體大多已採用端對端加密技術，現行截收訊息內容之通訊監察方式，截收到的訊息若無解密鑰匙，亦僅係一連串沒有意義之亂碼。

第二項　我國現行法制針對網路通訊軟體實施通訊監察之障礙

第一款　業者之協力義務

我國法有關電信業者協助偵查之相關規定，分散於電信法、通訊保障及監察法以及第二類電信管理規則等法規，而上開法規之規範對象都是電信業，而網路服務業在我國定義上是否屬於電信事業，仍存有極大爭議。

依通訊保障及監察法第 14 條第 2 項規定「電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。」；同條第 4 項規定「電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」前開法定負有協力義務之電信事業，依照通訊保障及監察法施行細

doi:10.6342/NTU202301879

則第 26 條[37]規定，顯然僅針對第一類及第二類電信業者[38]。第一類及第二類電信業者，除依通訊保障及監察法負有國家執行通訊監察之協力義務外，有關電信資料之記錄、保存及提供，均有相關規範。第一類電信業者相關規定有電信事業處理有關機關查詢電信通信紀錄實施辦法第 3 條及第 5 條規定[39]；第二類電信業者相關規定，則有第二類電信事業管理規則第 23 條、

[37] **通訊保障及監察法施行細則第 26 條**
「本法第十四條第二項所稱協助執行通訊監察之義務，指電信事業及郵政事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備及本施行細則所定之其他配合事項。
國家通訊傳播委員會應將本細則施行前經特許或許可設置完成之第一類電信事業之通訊系統及通訊網路等相關資料，提供予法務部調查局或內政部警政署評估其所需之通訊監察功能後，由法務部調查局或內政部警政署依第一類電信事業之業務及設備設置情形，向第一類電信事業提出需求；第一類電信事業應即依該需求，擬定所需軟硬體設備、建置時程及費用之建置計畫，與法務部調查局或內政部警政署協商確定後辦理建置。必要時，由國家通訊傳播委員會協助之。
第一類電信事業於本細則施行前已經同意籌設或許可之新設、新增或擴充通訊系統，於本細則施行時尚未完成籌設或建置者，於其通訊系統開始運作前，應依前項之規定擬定配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫及辦理建置，並於其通訊系統開始運作時同時協助執行通訊監察。本細則施行前交通部已公告受理特許經營之第一類電信業務，其經核可籌設者，亦同。
第一類電信事業新設、新增或擴充通訊系統者，為確認其通訊系統具有配合執行監察之功能，應由法務部調查局或內政部警政署提出監察需求，該電信事業儘速擬定應配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫，經法務部調查局或內政部警政署與該電信事業協調確定後，由國家通訊傳播委員會核發建（架）設許可證（函）後辦理建置，並經國家通訊傳播委員會與法務部調查局或內政部警政署確認符合通訊監察功能後，於其通訊系統開始運作時同時協助執行通訊監察。
前三項建置計畫是否具有配合通訊監察所需之功能發生爭執時，由國家通訊傳播委員會認定並裁決之。第一類電信事業應即依裁決結果辦理。
第二類電信事業須設置通訊監察設備之業務種類，由國家通訊傳播委員會邀集法務部調查局或內政部警政署協調定之，並準用前四項規定辦理。
本法第十四條第三項所稱必要費用，指電信事業及郵政事業因協助執行而實際使用之設施及人力成本。」

[38] 我國電信法將電信事業區分為兩類，依電信法第 11 條「電信事業分為第一類電信事業及第二類電信事業。第一類電信事業指設置電信機線設備，提供電信服務之事業。前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。第二類電信事業指第一類電信事業以外之電信事業。」，本身擁有電信機線設備（如有線傳輸網路、無線電頻率、衛星等）即屬第一類電信，而向第一類電信事業租用電信機線設備，提供公眾通信服務者，即為第二類電信事業。

[39] **電信事業處理有關機關查詢電信通信紀錄實施辦法**
第 3 條
「有關機關查詢通信紀錄應先考量其必要性、合理性及比例相當原則及並應符合相關法律程序後，再備正式公文或附上電信通信紀錄查詢單（格式如附件），載明需查詢之電信號碼、通信紀錄種類、起迄時間、查詢法律依據或案號、資料用途、機關全銜、連絡人姓名、連絡電話、傳真機號碼及列帳電話號碼等，加蓋機關印信及其首長職章，送該電信用戶所屬電信事業指定之受理單位辦理。但案情特殊、情況緊急之查詢，得由法官、軍事審判官、檢察官、軍事檢察官、查詢機關首長或其書面指定人於電信通信紀錄查詢單署名並加蓋職章及連絡人之資料，視同機關正式

doi:10.6342/NTU202301879

第 24 條及第 27 條[40]，上開法規均針對第一、二類電信業者就電信資料、記錄保存以及提供之義務性規範，均有明確規定。

而提供網路通訊軟體予用戶使用之軟體服務商，須透過網路才能運作，應屬網際網路服務提供者之一種，然而，網際網路服務提供者，究竟是否為屬電信業者？尚有爭議。

公文書先傳真之，並經回叫確認為之，查詢後應於三個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本。未於三個工作日內補具公文或查詢單者，電信事業得拒絕受理其再次傳真查詢。」

第 5 條

「前條第一類電信事業通信紀錄之保存期限如下：

一、市內通信紀錄：最近三個月以內。

二、國際、國內長途通信紀錄，最近六個月以內。

三、行動通信通信紀錄：最近六個月以內。

前項期限，自受理查詢日回溯起算。

第二類電信事業通信紀錄之保存期限，依第二類電信事業管理規則之規定。」

[40] **第二類電信事業管理規則**

第 23 條

經營公司內部網路通信服務者，應至少保存其用戶基本資料至契約終止後一年。

前項用戶基本資料，包括公司之內部單位、分公司、分支機構及其關係企業之名稱與地址、公司內部關係證明文件、公司內部撥號計畫及用戶與業者網路連接之專線電路編號等。

如用戶之公司內部關係為其關係企業時，經營公司內部網路通信服務者，應檢具用戶名稱、地址及公司內部關係證明文件報請主管機關備查。

第 24 條

經營公司內部網路通信服務者，應登錄及保存連接網路內部節點之專線電路編號、相關路由表及通信紀錄資料。

前項連接網路內部節點之專線電路編號、相關路由表於經營期間內須持續保存，通話紀錄資料應至少保存六個月。

第 27 條

經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。

前項電信內容之監察事項，依通訊保障及監察法規定辦理之。

經營者對於第一項電信通信紀錄應至少保存期間如下：

一、語音單純轉售服務通信紀錄應保存六個月。

二、網路電話服務通信紀錄應保存六個月。

三、網際網路接取服務：

（一）撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存六個月。

（二）非固接式非對稱性數位用戶迴路（ADSL）用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。

（三）纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。

（四）張貼於留言版、貼圖區或新聞討論群之內容來源 IP 位址與當時系統時間應保存三個月。

（五）免費電子郵件信箱及網頁空間線上申請帳號時之來源 IP 位址及當時系統時間應保存六個月。

（六）電子郵件通信紀錄應保存一個月。

四、虛擬行動網路服務通信紀錄應保存六個月。…」

doi:10.6342/NTU202301879

依照我國固有針對電信業者之分類架構，第一類電信業者本身必須架構電信機線設備以提供服務，而網路服務或其他分封式交換網路服務，則使用到 OSI 通訊協定的第三層以上，由於其架構設置分封式交換設備於數據電路之終端，故符合第二類電信事業之定義，此類服務被稱為加值型服務[41]。我國向來將國內網路服務業者區分為：網路接取服務業者(Internet Access Provider, IAP)、網路內容服務業者(Internet Content Provider, ICP)、網路平台服務業者(Internet Platform Provider, IPP)以及網路應用服務業者(Application Service Provider, ASP)，而在我國現行電信法相關規範，普遍認為僅有第一種網路接取服務業者（IAP）受到電信法之規範，理由在於包含電信法、第二類電信事業管理規則、電信事業處理有關機關(構)查詢電信使用者資料實施辦法等，都只以提供電信設備為基礎之網際網路連線服務提供者(Internet Access Provider)為規範對象，難以涵蓋其他種類之網路服務業者[42]。再者，依照國家通訊傳播委員會 103 年 8 月 20 日通傳法務字第 10300514490 號函釋，通訊軟體服務業並非通訊保障及監察法所稱之「電信事業」。直至目前為止，依照國家通訊傳播委員會之認定，上開 4 類網路服務業者，僅網路接取服務業者（IAP），依照電信法第 2 條第 5 款之規定，屬於電信法規範之電信事業，其餘既非電信事業，不須向國家通訊傳播委員會申請電信經營執照，也非屬國家通訊傳播委員會監管對象，也不受通訊保障及監察法之拘束，而不負法定電信業者應擔負之建置通訊監察所需要系統等法定協力義務[43]。

近年來，我國電信管理法制在 2019 年產生重大變革，立法院於 2019

[41] 黃逸玲，行動通訊 APP 偵查與對策之研究，中央警察大學刑事警察研究所碩士論文，2018 年，頁 19。
[42] 廖有祿、張維平、蘇莞筑、劉怡汎，網路平台業者紀錄保存規範之研究，2013 年犯罪偵查學術與實務研討會，2013 年 5 月 30 日，頁 26。
[43] 王晴玲，對已具加密功能之通訊軟體之通訊監察之理論與實務，出國報告（出國類別：研究），2015 年 11 月 20 日，頁 53-54。

doi:10.6342/NTU202301879

年 5 月 31 日三讀通過電信管理法，自 2020 年 7 月 1 日起正式施行，規範功能取代了舊有電信法。電信管理法一改傳統電信法管制架構，將電信法針對特許／許可制改為自願登記制，自 2020 年 7 月 1 日起，新進市場之第一類及第二類電信事業若無使用無線電頻率或電信號碼等電信資源，則可以自由選擇是否向國家通訊傳播委員會辦理電信事業登記。且依照電信管理法第 83 條規定，於新法施行之日起 3 年內若尚未申請登記之第一類或第二類電信事業，則應由主管機關依原有法令管理。是以，依照電信管理法之規定，只有第一類電信事業必強制要求應於新法施行後三年內，向國家通訊傳播委員會辦理電信事業之登記及許可，第二類電信事業則可自行依照營運需求，決定是否要改依電信管理法辦理新法登記[44]。

電信管理法公布施行後，關於我國網路服務業者（包含通訊軟體商）可否納入電信商範疇之爭議，是否會因此改變？有論者認為依照電信管理法第 3 條第 1 項第 2 款對「電信服務」的定義：「利用公眾電信網路提供公眾通信之服務」，以及同條項第 3 款對「電信設備」的定義：「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。」，以往對於通訊軟體在何種情形下會被認定屬於電信服務之爭議，在新法下有較清楚之定義，只要未使用到公眾電信網路者，就不屬電信服務[45]，故解釋上可得出電信管理法實施後，只要是使用到公眾電信網路的通

[44] 儘管電信管理法已公告施行，然原電信法的規範效力並未立即結束。一方面係因行政院僅公告電信管理法部分條文生效；另一方面，根據電信管理法第 83 條第 1 項「本法施行之日起三年內，依電信法取得許可、特許之電信事業，或獲核准籌設者，應向主管機關 辦理登記。」以及第 3 項「依電信法取得許可、特許之電信事業，或獲核准籌設者未於第一項規定之期限內辦理登記者，其原有籌設、特許或許可執照於本法施行三年後之次日起，失其效力。」之規定，電信法在這三年的過渡期間內仍屬有效之法律。上開說明參黃銘輝，淺談當前課予通訊服務業者協力義務的困境與突破（下），桃律通訊，第 22 期，2021 年 3 月 1 日，第 3 版。

[45] 朱百強、簡維克，電信法規環境之新面貌：論電信管理法通過後之機會與挑戰 ，2019 年 8 月 30 日，理律法律事務所官網，https://www.leeandli.com/TW/Newsletters/6316.ht ，最後瀏覽日 2023 年 6 月 24 日。

doi:10.6342/NTU202301879

訊軟體，即可將其認定為電信服務[46]。亦有認為配合電信管理法未來對於電信業者改採「自願登記制」，未來即有「未為電信事業登記的電信服務」存在的空間。依此脈絡分析，有論者認為未來在電信管理法正式施行之後，既然有無登記不影響其是否屬於「電信事業」之認定，解釋通訊保障及監察法之「電信事業」時，即可擺脫有無電信執照的束縛，循此軌跡將未依電信管理法為電信事業登記的通訊軟體業者，納入通訊保障及監察法「電信」事業的概念之中，令其負擔法定通訊監察協力義務[47]。然而，上開解釋方式是否能為主管機關甚至司法實務普遍接受，仍有待持續觀察。惟可以確定者是，在我國現行法律架構下，有關通訊軟體商是否負有執行通訊監察之協力義務，或是記錄、保存、提供電信資料之義務，顯已不敷當今實務所需，而此種現況，在面對端對端加密技術對執法機關之衝擊時，更顯迫切。

第二款　端對端加密技術

過去執法機關只要依通訊保障及監察法聲請法院核發通訊監察書，即可對通訊監察書上所載「對象」、「時間」及「範圍」內之私人通訊內容進行截收，以此方式獲得犯罪偵查所需資訊。上開情形在端對端加密技術成為網路通訊軟體之「標準配備」後面臨極大挑戰。正如同本文於第一章、第二節、第二項《端對端加密技術》之介紹，當通訊監察對象是使用加密軟體傳送通信內容時，執法機關縱使依法可將通信內容截取，除非有解密金鑰，否則開拆後之結果僅係一長串沒有意義之亂碼，無法取得如同訊息接收方所取得之「可被閱讀形式」之訊息。

[46] 黃銘輝，淺談當前課予通訊服務業者協力義務的困境與突破（下），桃律通訊，第 22 期，2021 年 3 月 1 日，第 2 版。
[47] 同上註。

doi:10.6342/NTU202301879

過去加密技術發展初期，世界各國執法機關尚可仰賴 Brute-Force（暴力攻擊法，亦即透過反覆 try-error 之方式破解密碼，因手段暴力，也被稱為暴力攻擊法[48]）之方式，以嘗試每個可能密碼之方式進行解密，而這種解密方法是否可行?取決於必須花費多少時間猜到密碼，而其時間的花費又會與密碼設定之長度、複雜度。假設某一台電腦可以在一秒鐘內恢復 DES(The Data Encryption Standard，數據加密標準，使用的 56 位元密鑰)，同一台電腦需要 149 兆年才能破解 AES(Advanced Encryption Standard，進階加密標準，區塊長度固定為 128 位元，金鑰長度則可以是 128，192 或 256 位元）。至於 2048 位元的 RSA 加密，理論上大約需要 4000 個量子位元（qubit)，若以目前 Google 和 IBM 20 個量子位元之量子電腦，花費 46 億年都無法破解。

然而，加密技術發展至今技術已日益精進、純熟，以目前使用率較高之幾家網路通訊軟體而言，例如：WhatsApp，是使用 256 位元之密鑰；Line 則是使用 2048 位元的 RSA 密鑰，傳統之暴力攻擊法已無使用實益。執法機關面對加密之通訊資訊，當無法再採用現行法律授權之「截取」之監聽方式，而應另謀應對策略。

第三節 世界上常見立法對策

在介紹世界各國用以對抗加密技術之立法例之前，應先予說明者是，現今加密技術之應用範圍，不僅在本文前面介紹之 LINE、WhatsApp、Signal 等網路通訊軟體，而係廣泛、普遍應用在所有網路資訊軟硬體設備上，如人手一機之手機、雲端硬碟、硬碟全碟加密工具等，無不應用加密技術來

[48] OS Kerr and B Schneier, *Encryption Workarounds*, (Mar. 22, 2017) , 106 Georgetown Law Journal 989, 994 (2018).

doi:10.6342/NTU202301879

提高資料之安全性，亦同樣致使執法機關傳統之搜索、扣押等干預手段受到阻礙（如：搜索、扣押電腦、手機等數位裝置但無法解開密碼）。是以，本節所概述有關「對抗加密」之常見立法對策，並不僅限於網路通訊軟體，尚包含用以抗衡全部數位加密技術之立法對策。

目前世界各國用以對抗加密之立法對策，大致可分為「解密令狀」以及「國家木馬」2 種方式。解密令狀是以司法機關核發令狀之方式，強制持有解密鑰匙之對象交出解密金鑰；而國家木馬則係立法授權國家可以於法定要件下，合法使用駭客技術突破加密技術之屏障。除了以上 2 種常見解密立法對策外，理論上仍存在其他解決途徑，例如：強制後門（自設計之初就隱藏在代碼中的漏洞）或是金鑰託管系統[49]（key escrow system，即將用戶通信的密鑰交由一個金鑰託管代理來管理，當政府取得合法授權時由此系統向政府提供對加密密鑰的查看權限。），或是透過立法禁止或控制加密（例如：北非之突尼西亞）[50]，然均存在過度侵害人權、不利資安發展等疑慮，難以受到多數民主法制國家之青睞。以下僅就多數國家採用之解密令狀以及國家木馬 2 種方式介紹：

第一項 解密令狀（Unlock Orders）

執法機關在破解加密資訊時，大多面臨欠缺相對應之技術、駭客工具等問題，且世界大部分民主法制國家，採取支持加密技術發展之基本態度，故對於加密技術之使用並不予以限制，於此情形下，現階段諸多國家之立法趨勢係採用以司法令狀之方式，強制密鑰持有人交出解密鑰

[49] H Abelson et al, *The risks of key recovery, key escrow, and trusted third-party encryption*, Columbia Academic Commons, (June 28, 2010), at https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W, last visited 06/24/2023.
[50] UNESCO, *Human Rights and Encryption*, (2016), at https://unesdoc.unesco.org/ark:/48223/ pf0000246527, last visited 06/24/2023.

doi:10.6342/NTU202301879

匙或協助解密。

解密鑰匙可能在設備使用人之持有中，亦有可能是軟體、程式或設備開發商。當解密之義務相對人是設備持有人自己之情形下，有認為要求提供解密金鑰之情形有違反不自證己罪原則之疑慮，但歐洲人權法院在桑德斯案（Saunders）中曾宣示，不自證己罪原則係源自於被告之緘默權，使用違反被告意願所取得之證據資料並未違反不自證己罪原則，因此類證據已具有異於被告意願之獨立存在性[51]。然而，有關不自證己罪原則之爭議並未因就此停歇，仍有論者認為縱使密碼具有獨立存在性，然實際上無法獨立於犯罪嫌疑人意願之方式取得[52]，對此歐洲人權法院在 Funke 案中曾宣示，執法機關強迫犯罪嫌疑人交出執法機關相信其存在之文件，而並未設法以其他方式取得該項文件時，係違反歐洲人權公約的第 6 條人民接受公平審判之權利[53]；在 JB 案中，歐洲人權法院則認定，在沒有相當理由確信犯罪嫌疑人持有解密資料時，以任何形式（如罰金、追訴）強迫犯罪嫌疑人交出上開資訊，違反歐洲人權公約的第 6 條人民接受公平審判之權利[54]。

除此之外，解密令狀在實務操作面上最大的困難，可能是面對被告輕易地以「忘記密碼」等語推託，而法院又該如何驗證被告是否「真的忘記」？倘無法檢驗此類抗辯是否屬實，違反令狀之法律制裁手段當無法有效執行。準此，現採用解密令狀之立法例，大多將解密義務人鎖定軟體、程式或設備開發商，解密之客體包含特定之訊息、對話、內容或是程式解密所需之金鑰。現有針對「解密令狀」之質疑包含：解密令狀之有權機關範圍？在

[51] Saunders v the United Kingdom App no 19187/91 (ECtHR, 17 December 1996).
[52] Thiago Moraes, *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures*, 6 EUR. DATA PROT. L. REV. 41 (2020). 47.
[53] Funke v France App no 10828/84 (ECtHR, 25 February 1993).
[54] JB vSwitzerland App no 31827/96 (ECtHR, 03 May 2001).

doi:10.6342/NTU202301879

何種情形下可以強制私人企業協助執法[55]？當解密金鑰的設計技術無法明確係由軟體、程式或設備開發商甚至其他對象持有之情形下，要如何精準確定解密令之開立對象，恐也是執行上之一大困難。

為避免偵查或國安秘密洩漏，解密令狀於立法例上往往伴隨「禁言命令」(gag order)，限制解密令狀之義務人將訊息透漏給其他人知悉，對此亦有論者認為，禁言命令限制了義務人將收到令狀之消息公開，無法使社會大眾知悉，恐使相關者之權利受到恣意侵害，甚至影響渠等司法救濟之機會。另外，科技公司為履行解密令狀所生之負擔乃係另一更為實際之問題，在 FBI 與 APPLE 公司之案件中，其中一項爭議即為 APPLE 公司必須研發一種新軟體來協助 FBI 取得 iOS 8+之加密資料，其所生成本費用究竟應由哪一方來負擔[56]。

第二項　國家木馬（Government Hacking）

執法機關使用國家木馬[57]查緝犯罪，係對抗加密時代網路所暗藏之各種犯罪之一大利器，近來最著名之案例莫過於美國 FBI 自 2011 年開始啟動之魚雷行動（Operation Torpedo），本案源自於荷蘭警方於 2011 年破獲

[55] OS Kerr and B Schneier, *Encryption Workarounds*, (Mar. 22,2017) , 106 Georgetown Law Journal 989, 1000-1005 (2018).

[56] J Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data, Under the All Writs Act* (2016), Electronic Journal 1443.

[57] 各國為避免植入木馬、駭入、侵入等名詞之負面意涵，多美化其名稱，如英國之法案使用「電腦網路之利用」（Computer Network Exploitation）或「設備干預」（Equipment Interference）；美國常見用語則為「網路調查技術」（Network Investigative Techniques, NITs），亦有稱為合法駭入（Lawful Hacking）、合法擷取（Lawful Access）、司法警察駭入（Police Hacking）、惡意軟體（Malware）、司法警察軟體（Policeware）；荷蘭稱為「對電腦之調查」（Investigation in a Computer, Onderzoek in Een Geautomatiseerd Werk）；另常見俗稱包含政府木馬、國家駭客、國家病毒、政府駭入、線上搜索及遠端電腦搜索等。註引自朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 46；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 49-87。

doi:10.6342/NTU202301879

大型兒童色情網站，進而發現伺服器架設於美國內布拉斯加州貝爾維尤市，荷蘭將此情資通報美國 FBI，美國 FBI 發現此網站架設於暗網上，使用者僅能透過使用洋蔥瀏覽器（Tor Browser）連結暗網，而利用洋蔥瀏覽器匿名以及暗網伺服器位址和資料隱匿加密之特性，隱藏網站使用者之 IP 位置來躲避查緝，FBI 在法官支持之下取得使用網路調查技術（Network Investigative Technique）令狀，利用植入國家木馬之方式，使犯罪者下載兒童色情圖檔時同時，附帶將木馬程式植入設備，並於打開圖檔時啟動木馬程式並向執法機關回傳 IP 位置，以此方式成功破獲散播兒童色情圖檔之犯罪集團，總計 25 人遭到起訴，其中 19 人經判決有罪[58]。國家木馬之偵查手段在查緝暗網犯罪具有不可或缺之角色，根據國際警察局長協會 2015 年報告指出「若缺少國家木馬作為執法工具，執法機關將無法有效偵辦及起訴暗網犯罪」[59]。

目前世界各國執法機關執入木馬之方式，大致可分為以下 4 種方式:(一)物理接觸法：透過秘密接觸到電子設備之方式執入木馬程式，例如：執法人員利用海關檢查的機會，接觸設備以植入木馬，或是透過已感染的移動式資訊設備植入，於電腦偵測到插入後自動開啟系統，間接啟動木馬設備[60]；(二) 遠端執入：透過向目標電子設備發送訊息並使用社交工程誘騙打開附件或點選連結之方式，秘密安裝木馬程式；(三) 利用輸入用戶姓名及密碼，以釣魚或社交工程猜測密碼，此種方式之侵入性較小[61]；(四) 利用作業系統安全性漏洞：在系統服務商尚未填補系統漏洞之前，繞過系

[58] Jose Pagliery, *FBI hackers took down a child porn ring*, CNN Business, (Jan. 25 2016), at https://money.cnn.com/2016/01/25/technology/fbi-child-porn/, last visited 06/24/2023.

[59] IACP summi Report, *Privacy and Public Safety: A LAW Enforcement Perspective on the Challenge of Gathering Electronic Evidence* (2015), at https://www.theiacp.org/sites/default/files/2019-05/IACPSummitReportGoingDark_0.pdf, last visited 06/24/2023.

[60] 高儀庭、金孟華，以木馬程式作為我國科技偵查手段之研究，萬國法律，第 240 期，2021 年 12 月，頁 5。

[61] 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 47

doi:10.6342/NTU202301879

統內建安全防護系統竊取資料[62]。

常見用於解密之木馬程式包含：Brute-force（暴力攻擊法，亦即透過反覆 try-error 之方式破解密碼，因手段暴力，也被稱為暴力攻擊法[63]）；Zero-day exploits（零日攻擊，指利用尚未修補之程式的安全漏洞所進行之攻擊）以及 Full Disk Encryption（FDE）-oriented attacks（全盤加密取向攻擊）

（一） 暴力攻擊法（Brute-force）

暴力攻擊法是以嘗試每個可能密碼之方式解密，這種解密方法是否可用，取決於必須花費多少時間猜到密碼，而其時間的花費又會與密碼設定之長度、複雜度呈現正向關係[64]。目前常見之「端對端加密」之通訊軟體，例如：WhatsApp，是使用 256 位元之密鑰；Line 則是使用 2048 位元的 RSA 密鑰[65]。早期，因為一般密碼設定之長度較短、複雜度較低，使用暴力攻擊法來破解密碼看似足夠，以 iPhone 手機 6 位數之密碼為例，嘗試全部一百萬可能的密碼組合需耗時 22 小時。然而，手機大廠後來使用許多機制來防堵暴力攻擊法，例如 Android 的 5+系統則預設在 5 次密碼嘗試錯誤後，須等待 30 分鐘才能再次嘗試。Apple 的 iOS8+系統則預設當密碼嘗試數次都失敗後，須等待一段時間，才能繼續嘗試之機制，iOS 系統甚至可以設定在 10 次連續嘗試錯誤後可以刪除全部資料[66]。在美國著名之 FBI 及蘋果公司發生爭議之 Sam Bernadin 案中，FBI 即曾要求法院發出令狀，

[62] 高儀庭、金孟華，以木馬程式作為我國科技偵查手段之研究，萬國法律，第 240 期，2021 年 12 月，頁 5

[63] OS Kerr and B Schneier, *Encryption Workarounds*, (Mar. 22,2017) , 106 Georgetown Law Journal 989, 994 (2018).

[64] *See id.*, at 993-996 .

[65] 何煒華 秦裕國，行動通訊軟體 LINE 的安全設計探討，2016 年第十屆資訊科技國際研討會/第六屆臺灣網路智能學會學術論壇，2016 年 4 月 23 日, http://163.17.20.49/AIT2016/paper/ft_159.pdf，最後瀏覽日 2023 年 6 月 27 日

[66] Apple, *loS Security: loS 12.1* (2018), at https://www.apple .com/business/site/docs/iOSSecurityGuId.e.pdf, last visited 06/24/2023.

doi:10.6342/NTU202301879

命蘋果公司將「anti-brute-force-attack」功能失效，並表示只要將該功能關閉，即可以輕易駭入手機裝置內[67]。

（二） 零日攻擊(Zero-day exploits)

零日攻擊是指利用尚未修補之程式的安全漏洞所進行之攻擊，所謂的零日漏洞是指軟體、硬體已被公開但仍未完成修補之漏洞。而當開發人員針對漏洞進行修補更新後，漏洞即變成「已知」漏洞 （即 N-day 漏洞）。而零日攻擊則是針對上述廠商尚未釋出修補更新的漏洞開發出之攻擊手法或是惡意程式，即為零日攻擊（或稱零時差攻擊）。因為這些尚未修補之漏洞是固定的，因此可以被利用、訪問、監視，從軟體程序提取資料或損壞軟件程序，零日攻擊甚至有全球交易市場，國家將其使用於軍事、情報和網路執法，而犯罪集團則用以竊取資訊、破壞系統[68]。

（三） 全盤加密取向攻擊

目前已有許多技術可用來規避全盤加密。例如： 冷啟動攻擊(Cold Boot attack)，冷啟動攻擊之原理是基於能量逐漸衰減的物理法則，電腦 DRAM 和 SRAM 記憶體上的數據，都會在電力漸減而消失，即使斷電後數分鐘，記憶體仍有一些資料殘留，而且不管使用任何加密法，所有加密金鑰在能量完全衰減前，都會儲存在記憶體上。不管筆記本電腦或是手機，就算已登出及關機，只要電力未完全衰減，就可以進行冷啟動攻擊，從記

[67] Manhattan District Attorney's Office, *Report Of The Manhattan District Attorney's Office On S martphone Encryption And Public Safety*,(2015) at https://www.manhattanda.org/wp-content/ themes/ dany/files/11.18.15%2oReport%20on%2oSmartphone%20Encryption%20and%2OPublic%2OSafety.pdf, last visited 06/24/2023.

[68] M Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, Social Science Research Network (2015), 410, 449-451.

doi:10.6342/NTU202301879

憶體中把加密鑰匙取得[69]。

（四） 邪惡女傭攻擊（Evil maid attack）

這是一種最原始的電腦設備攻擊方法， 利用在電腦設備無人監控之狀態，只要透過一個物理性的設備接口，利用極短時間即可竊取資料後離開，而不留下痕跡，取名為邪惡女傭是因為女傭往往常有機會獨留於飯店內，而有與電子設備獨處之機會，可輕易趁此機會侵入電腦[70]。侵入管道包括支持數據快速交換或與設備內存直接交互的通訊端口，例如，雷電接口，傳統 USB 也是攻擊管道之一，用於攻擊的小型設備被插入 USB 接口，它會在用戶開機時被啟動並發動 BadUSB 攻擊。

第四節 小結

加密技術對於執法機關之衝擊，並非僅止我國，而全球執法機關所面臨之共同挑戰，此從前述跨國組織及多國聯盟於近年來接連發出之嚴正聲明即清楚可見，於此背景下，諸多國家紛紛透過立法之方式施以對策，而常見之立法對策大致為解密令狀及國家木馬 2 種。解密令狀係透過政府發出強制性令狀之方式強制密鑰持有人交出解密鑰匙或協助解密，國家木馬則係立法授權國家合法使用植入木馬之方式取得執法機關所需之資訊。上開 2 種方式各有利弊優缺，從國家角度而論，解密令狀將解密義務附加於持有解密鑰匙之軟體、程式或設備開發商，節省國家發展高端木馬技術之

[69] 龐博文，暗網潛航——電腦鑒識術——冷徹心扉，香港頭條日報專欄，2020 年 7 月 27 日，https://hd.stheadline.com/news/columns/1118/20200727/871392/%E5%B0%88%E6%AC%84-%E6%9A%97%E7%B6%B2%E6%BD%9B%E8%88%AA-%E9%9B%BB%E8%85%A6%E9%91%92%E8%AD%98%E8%A1%93%E2%94%80%E2%94%80%E5%86%B7%E5%BE%B9%E5%BF%83%E6%89%89，最後瀏覽日 2023 年 6 月 25 日。

[70] INSIDE，「凡走過不留下痕跡」Thunderbolt 恐成最新入侵管道 5 分鐘資料全竊走，聯合新聞網，2020 年 5 月 12 日，https://udn.com/news/story/7086/4558340，最後瀏覽日 2023 年 6 月 25 日。

doi:10.6342/NTU202301879

困難、時間耗費與成本，對國家而言係較為節省時間及成本之方式，然而，解密令狀受制於持有解密鑰匙之私部門是否配合，於網路服務無國界之現今時代，持有解密鑰匙者亦非一定在境內或本國公司，縱有違反令狀之處罰，國家是否有足夠能力確保解密令狀執行無礙，仍屬存疑。相反地，國家木馬在國家不受制於私部門之觀點上佔有優勢，僅要依法定程序取得授權，後續之執行可望比解密令狀順暢。然而，國家木馬係國家發展駭客技術以秘密的方式對人民所使用之電腦設備植入木馬，此種方式就隱私權之侵害疑慮遠高於解密令狀，立法難度較高，另就技術面而論，無論政府自行發展國家木馬，或係對外採購，政府均必須具備能為木馬程式為技術擔保之專業能力，以確保木馬係在法令授權範圍內執行，除規範面以外，未來執行及監督面所面臨之技術問題可能更具挑戰。

反觀我國，因加密通訊軟體之普及，通訊保障及監察法原授權執法機關得透過依法實施通訊監察之方式查緝不法犯罪之立法初衷，已因加密技術之發展無法發揮效用，實際出現法治面與技術面之現實落差，如何透過立法解決國家犯罪偵查之困境，已為國家不應迴避之問題。觀諸世界諸多立法先進國家，自 2016 年起掀起了一波對抗加密之立法浪潮，在支持加密技術發展對於資訊安全所帶來之正面影響以外，另著眼於加密技術對於執法及國家安全之重大衝擊下，立法賦予國家針對加密資訊調查之法定權力，上開立法例實足作為我國立法之參考，本文將於下一章節依序介紹英國、法國、德國、荷蘭及澳洲立法例，作為我國後續立法借鏡。

doi:10.6342/NTU202301879

第三章 外國立法例介紹

第一節 英國

第一項 調查權規範（Regulation of Investigatory Powers Act 2000）

英國 2000 年立法制定之調查權規範（Regulation of Investigatory Powers Act ，以下簡稱 RIPA）即係以「解密」為規範中心，RIPA 自 2007 年 10 月 1 日起施行，內容包含有強制解密之法律授權規範、「通訊截取權（interception of communication）」以及「以解密或接觸之方式獲取被加密、密碼方式保護之電磁紀錄（the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed）」[71]，本法第三部分係「受加密保護電磁紀錄之調查」[72]，以法律授權情報機關、警察、國家刑事局及稅務海關總署依法行使其包含沒收、扣押、檢查、搜索、通訊內容攔截等法定職權時所取得之電磁紀錄受到加密保護時，上述政府機關可經法院、內閣大臣許可發出第 49 條通知（Section 49 Notice），強制特定人針對受加密保護之電磁紀錄，交出解密之鑰匙或將之轉換為可以理解之形式[73]。第 49 條通知即為上述「解密令狀」之典型。

根據 RIPA 第 49 條的規定，第 49 條通知必須取得法官（一般情形）或內閣大臣書面聲請許可後發出，許可必須基於有相當理由確信符合以下

[71] *See* Regulation of Investigatory Powers Act 2000, c. 23, introductory text (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/introduction, last visited 07/03/2023.
[72] Regulation of Investigatory Powers Act 2000, c. 23, § 49–56 (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/part/III, last visited 07/03/2023.
[73] *See id.* at § 49, 56(1).

doi:10.6342/NTU202301879

要件：①受通知義務人擁有解密鑰匙、②基於「保障國家安全」、「預防、偵查犯罪」或「英國的經濟利益」之目的為之、③解密係為確保政府機關有效行使或適當履行任何法定權力或法定職責所必須、④目的與手段間符合比例原則及⑤沒有解密通知下取得受保護之訊息內容為不合理可行的。

聲請書應以書面載明：受保護信息、理由、受通知義務人的職務、職級或職位、聲請人的職位，職級或職位、通知期限、闡明解密之方式及如何提供等事項。向法官或內閣大臣聲請許可之細部程序規範，則會依受加密保護之電磁紀錄之來源，區分為「依法院、內閣大臣核發令狀取得」、「情報單位無令狀取得」、「他機關於無令狀之情形下依法令授權取得」、「非依法令授權取得」等情形而有程度不同之規範。

解密通知必須給予受通知義務人 7 日以上之期間以完成其義務。解密通知發出之對象，原則上在解密鑰匙係由法人持有時，則要求必須對具有履行解密義務能力之諸多人中最高之「senior officer」發出，所謂「senior officer」係指董事、經理人、秘書等主管階層，對僱員發出僅可在沒有其他公司合夥人、職位更高者被認為具有履行解密義務之可行性時[74]。

第 49 條通知之配套措施包含以下幾個面向：國家對於為履行第 49 條解密義務所生之花費，國家應給予適當之金錢補償[75]；資料必須以安全之方式留存，解密鑰匙在使用完畢後必須儘速銷毀[76]；明知卻拒絕履行第 49 條之解密義務者屬刑事犯罪，最重可處 2 年以下有期徒刑，若係在國家安全、兒童猥褻案件，最重可處 5 年以下有期徒刑[77]。除此之外，該法另有關於禁止洩密（tipping off）之規範，其規範對象包含受通知之解密義務人及任何

[74] *See id.* at § 49(5)(6)
[75] *See id.* at §52
[76] *See id.* at §55
[77] *See id.* at §53(5),(6),(10)

doi:10.6342/NTU202301879

人於過程中知道系爭通知或其內容之人，違反禁止洩密之保密義務者屬刑事犯罪，最重可處 5 年以下有期徒刑[78]。RIPA 第 65 條規定成立 IPT (Investigatory Powers Tribunal)特別法院，處理有關本法所生之爭訟。

英國自 2007 年開始施行 RIPA，如同上述介紹之第 49 條通知，可謂針對「解密」已有明確且具強制力之法律規範，然從英國 2012 至 2015 由國家技術協助中心(National Technical Assistance Centre[79]，以下簡稱 NTAC）所公布之歷年年度報告之統計數據可發現，2012 年至 2013 年報告期間，共有 26 案經法官核准發出之解密通知，其中有 19 案受解密通知之義務人未遵守其解密義務[80]；2013 年至 2014 年報告期間，共有 33 案係經法官核准發出之解密通知，其中 17 案受解密通知之義務人未遵守其解密義務[81]；2014 年至 2015 年報告期間共有 38 案經法官核准（其中 37 案列入統計）發出解密通知，其中 22 案受解密通知之義務人未遵守其解密義務[82]。然而，因違反 49 條通知之解密義務遭依同法第 53 條規定判決有罪者，2012 至 2013 僅有 3 件、2013 至 2014 僅有 2 件，2014 至 2015 僅有 3 件[83]，從上可知大部分的案件政府最終亦未追究或起訴其違反 49 條通知之法律責任，此種現象不僅代表 RIPA 所採取之解密令狀方式，實際上未能有效發揮，

[78] *See id.* at §54

[79] NTAC(國家技術協助中心)係一政府機關，隸屬於英國政府通信總部(Government Communications Headquarters，簡稱 GCHQ，屬於英國情報機構和國家安全機關）轄下，法定任務截取通訊、數據紀錄之回復、解密、分析及提供技術建議等。

[80] Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2012–2013 12, 4.11（2013）, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246455/0577.pdf, last visited 07/03/2023.

[81] Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013–2014 14, 4.13–4.15（2014）, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laId.-4-September-2014.pdf, last visited 07/03/2023.

[82] Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2014–2015 15–16, 4.17–4.22 (2015), p15-16, at https://www.statewatch.org/media/documents/news/2015/jul/uk-surveillance-comm-annual-report.pdf, last visited 07/03/2023.

[83] Daniel Severson, *The Encryption Debate in Europe, Jean Perkins Foundation Working Group on National Security*, Technology, and Law (Hoover Institution), Aegis Series Paper No. 1702 (March 21, 2017).

doi:10.6342/NTU202301879

英國國會也因此於之後進行了大規模之修法。

第二項　調查權力法（Investigatory Power Act 2016）

英國國會在 2016 年制定調查權力法（Investigatory Power Act 2016[84]，簡稱 IPA），該法在 2016 年 11 月 29 日獲得女王簽署而生效。長達 291 頁之法案全面更新及鞏固英國情報單位及執法機關有關通訊數據調查之權力，故又被稱為監聽者憲章（Snoppers' Charter）。本法授權之監察方法，包含針對通訊內容、數據（包含元數據【metadata】）之截取、保留、設備端干預及解密。針對原本 RIPA 第 49 條通知之相關程序為更細部之規範。此外，更引進對上述授權令狀之司法監督，IPA 不僅是修正英國原已存在 RIPA 所建構之解密法制，更創設新的干預方式。

第一款　互聯網連接紀錄之保留

IPA 所規範之監察權利包含截取、保留、設備端干預及解密，其中大部分都是過去已存在者，其中僅有 1 項為完全新創設之干預，即要求電信事業（telecommunications operator[85]）保留互聯網連接紀錄（Internet connection records，簡稱 ICRs）[86]。ICRs 之定義，依立法過程中英國政府提出之 ICRs 說明資料，互聯網連接紀錄（ICRs）是一種有關客戶使用互

[84] InvestigatoryPowersAct2016, c.25 (U.K.), at https://www.legislation.gov.uk/ukpga/2016/25/contents, last visited 07/03/2023.

[85] 英國法上「電信事業」之範圍與我國不同，依照 IPA 第 261(10)(11)有關電信事業之定義，包含於英國境內、境外提供電信服務、部分或全部控制或提供電信系統之事業，又所謂電信服務包含任何接入或使用電信系統（無論該系統是否由提供該服務的人提供）之服務。是以，英國的電信事業包含於網路上提供服務之事業，例如網路零售業或是網路郵件服務業等。註參 IPCO, *Annual Report of the Investigatory Powers Commissioner 2020*, Jan 6 2022, p90. Investigatory Powers Act 2016, c. 25, § 261(10) (11) (U.K.).

[86] Daniel Severson, *Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill,* Lawfare (Mar. 14, 2016, 12:17 PM), at https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers-bill, last visited 07/03/2023.

doi:10.6342/NTU202301879

聯網服務之通信數據紀錄，在客戶使用網頁或即時通訊服務時由提供互聯網服務之通信服務業者紀錄下來，而藉由執法機關、情報機關向通信服務業者取得。過去英國並無法律明定要求通信事業保留上開互聯網連接紀錄，IPA 立法授權國務大臣得以發出保留通知（Retention Notice）[87]，經司法委員核准後生效[88]（Judicial Commissioner，簡稱 JC，司法委員之介紹詳參下述第五款《司法審查程序-DOUBLE LOCK 制度之介紹》），通知可針對一個或以描述性定義之方式針對多個業者發出，資料範圍可包含所有或是以描述性定義之方式定義資料範圍[89]，強制業者保留上開紀錄最多至 1 年，使執法機關、情報機關得以調取上開紀錄[90]。

依據本法所創設之調查權力專員辦公室（Investigatory Power Commission Office，簡稱 IPCO）所公布之 2019 年年報，2019 年 7 月，司法委員首次核准了第一個有關互聯網連接紀錄之保留通知，要求某特定電信事業保留互聯網連接紀錄，這項通知是出於試驗之目的，由內政部與執法機關共同執行，復於同年 10 月再次基於測試目的核准第二個有關另一家電信事業之互聯網連接紀錄保留通知[91]。

第二款　解密通知

IPA 保留原本 RIPA 之第 49 條解密通知之規範及架構，並將 IPA 所創設之各項程序保障適用於原本之第 49 條解密通知，例如：將 RIPA 之第 49 條通知納入本法所創設之新調查權力專員（Investigatory Powers

[87] Investigatory Powers Act 2016, c. 25, § 87(U.K.).
[88] *See id.* at §89.
[89] *See id.* at §87（2）(U.K.).
[90] Fact Sheet, Investigatory Powers Bill: Internet_Connection_Records (ICRs), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530556/Internet_Connection_Records_factsheet.pdf, last visited 07/03/2023.
[91] IPCO, *Annual Report of the Investigatory Powers Commissioner 2019*, (Dec. 15, 2020), p16.

doi:10.6342/NTU202301879

Commissioner 【簡稱 IPC】，詳參本節後第五款《司法審查程序-DOUBLE LOCK 制度之介紹》)之綜合監督下的。IPC 為 IPA 所創設，負責審核、監督之專責人員，負責檢視政府機關有關數據調查權力之使用情形並向總理提出年度報告。IPC 針對受加密保護之電磁資訊需嚴格審查[92]，執法機關也須在發出第 49 條通知時通知 IPC[93]。此外，IPA 更擴大第 49 條通知之範圍，依照原 RIPA 之規定，第 49 條通知解密之客體僅限於通訊內容（communication），IPA 將其擴大至通訊內容之二手資料，即元數據(包含收、發、時間、長度、方式、路徑)。

IPA 創設基於國家安全目的之「國家安全通知」，用以取代 1984 年電信法中之“power of direction”，用以強制經營者採取符合國務大臣認為必要的特定步驟以維護國家安全，例如：為所從事的工作提供便利情報機構處理緊急情況，或為了協助情報部門更安全或更有效地執行其功能而提供的服務或設施[94]。國家安全通知之一個重要限制為政府不能使用國家安全通知在“其「主要目的（main purpose）」是為了進行依本法應取得令狀或授權的事情”[95]。亦即，政府不能以國家安全通知，作為規避本法其他授權法定程序之用。對此，英國學者有認為「主要目的（main purpose）」之法條用語留有解釋空間，政府可能會在特殊情況下（例如在察覺到重大恐怖襲擊中）依國家安全通知要求解密[96]。

第三款　技術能力通知

[92] Investigatory Powers Act 2016, c. 25, § 229(3) (e) (U.K.).
[93] *See id.* at §233 (4) (a).
[94] *See id.* at §252(2)-(3).
[95] *See id.* at §252(5) (U.K.).
[96] Daniel Severson, *The* En*cryption Debate in Europe, Jean Perkins Foundation Working Group on National Security*, Technology, and Law (Hoover Institution), Aegis Series Paper No. 1702 (March 21, 2017) p11.

doi:10.6342/NTU202301879

IPA 新創設針對解密之干預手段，為第 253 條之「技術能力通知(Technical capacity notice)」。國務大臣經司法委員核准後，可以根據本條規定向電信商發出技術能力通知，要求電信商或郵政運營商(telecommunications or postal operators)提供任何有關授權事項之任何協助，以技術能力通知對電信商或郵政運營商施加為完成授權事項之任何適用義務、任何步驟[97]。政府可透過技術能力通知，要求電信商或郵政運營商提供不確定範圍的設備、設施、服務，甚至包含要求取消施加在電磁紀錄上之電子保護，遵守、處理及揭露任何資訊[98]。國務大臣發出技術能力通知前，需事先諮詢技術諮詢委員會(the Technical Advisory Board)、可能承擔上開義務之人員、代表以及法定職權與之相關人員[99]。技術能力通知之發出對象，不限於英國境內，對英國境外者亦可[100]。又因技術能力通知涵蓋之義務型態包羅萬象，法律亦規定技術能力通知發出時，需考量成本、技術上可行性以及對用戶所生之影響[101]。期限部分並未硬性規定，僅要係國務大臣認定合理之期限即可[102]。

第四款 設備端干預(Government Hacking)

英國調查權力法有關國家木馬使用之名稱為設備端干預(Equipment Interference)，設備端干預之規定包含 IPA 第 5 部分之設備端干預「A Targeted Equipment Interference Warrant」(授權獲取對象之通訊內容、數據及其他資訊時)，以及第 6 部分第 3 章之「Bulk Equipment Interference Warrant」。第 5 部分「目標型（Targeted）」設備端干預與第 6 部分第 3 章

[97] Investigatory Powers Act 2016, c. 25, § 253 (1) (2).
[98] *See id.* at §253 (5)..
[99] *See id.* at §253 (6).
[100] *See id.* at §253 (8).
[101] *See id.* at §253 (6).
[102] *See id.* at §253 (7).

doi:10.6342/NTU202301879

「大量型（Bulk）」設備端干預」之差別，在於第 6 部分「Bulk Power」係僅限於情報單位使用，經由國務大臣發出經司法委員核准後生效[103]，主要目的為獲取對象之“海外”通訊內容、數據及其他資訊[104]，用以調查已知威脅以及識別新的威脅，第 6 部分「Bulk Power」總共包含攔截、通信數據的採集、設備端干預等種類之干預手段，授權情報機關得以大量蒐集已知對象或其他可疑對象之資訊。相較之下，「目標型（Targeted）」干預係針對能通過必要性、目的性及比例原則檢視之特定對象，但「目標型（Targeted）」干預仍可取得大量資料，但必須符合授權目的(例如預防嚴重犯罪、國家安全)之必要性及比例原則之檢視[105]。

設備端干預之細部規範訂於 2018 年英國內政部公布之設備端干預操作規範（Equipment Interference Code of Practice）[106]。依照上開操作規範 3.2、3.3，「設備端干預」之定義為「設備端干擾權限是使用一系列技術，以遠端或物理設備交換之方式，從設備端獲取通信內容(communications)、設備數據（equipment data）或其他訊息（any other information」；「設備干擾包含不同複雜程度之操作方式，低度為在無人看管的情況下秘密地從對象的設備中下載數據，或者使用對象之登錄憑證訪問其電子設備之保存數據。更複雜的設備干擾操作可能涉及利用軟體現有漏洞，以獲得對設備或網絡的控制權，以遠程搜索資料或監視設備的用戶。」；「設備端干預之令狀係授權取得儲存在設備或透過設備儲存之通訊內容、資料，當要截取進行中通訊，要依照 IPA 第 2 部分或第 6 部分第 1 章取得攔截令始得為

[103] *See id.* at §79.
[104] *See id.* at §136(2).
[105] IPCO, *Investigatory Powers*, IPCO's official website, at https://www.ipco.org.uk/investigatory-powers/the-powers/, last visited 07/03/2023.
[106] UK Government Home Office, *'Equipment Interference Code Of Practice'* (2018), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, last visited 07/03/2023.

doi:10.6342/NTU202301879

之」[107,108]。本法授權木馬植入之方式包含物理接觸方式植入和遠端植入（例如，通過有線和/或將軟體安裝到設備上）[109]。設備端干預令狀期間一般為6個月，符合令狀更新之法定要件時得以延長[110]。

依照IPA第102條至第104條之規定，原則上僅有情報機關及執法機關首長才擁有設備端干預令狀之核發權[111]，又依其目的區分為：基於情報防禦目的核發，必須由國務大臣親自發出；基於預防、查緝重大犯罪之目

[107] *See id.* at 14.

[108] 自2018年英國內政部公布之設備端干預操作規範上開定義可知，IPA之「設備端干預」就技術層面而言均係以科技技術之方式，自遠端或物理接觸方式秘密取得電子設備上之資料。又依其獲取之資料內容區分為：取得「已儲存之資料」（核其性質屬於秘密線上搜索，一般稱為「大木馬」）以及截取通訊內容（性質屬於來源端通訊監察，一般稱為「小木馬」），後者情形則仍須取得攔截令後始得為之。

[109] UK Government Home Office, *'Equipment Interference Code Of Practice'* (2018), p.12, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, last visited 07/03/2023.

[110] Investigatory Powers Act 2016, § 107

[111] UK Government Home Office, *'Equipment Interference Code Of Practice'* (2018), p.22-23, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, last visited 07/03/2023.
Sections 102 to 104 and 106 provide that these are:
The Director General of the Security Service,
The Chief of the Secret Intelligence Service,
The Director of the Government Communications Headquarters (GCHQ),
The Chief of Defence Intelligence,
The Chief Constable of a police force maintained under section 2 of the Police Act 1996,
The Commissioner, or an Assistant Commissioner, of the metropolitan police force,
The Commissioner of Police for the City of London,
The chief constable of the Police Service of Scotland,
The Director General of the National Crime Agency,
The Chief Constable of the British Transport Police Force,
The Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland,
The Chief Constable of the Ministry of Defence Police,
The Provost Marshal of the Royal Navy Police,
The Provost Marshal of the Royal Military Police,
The Provost Marshal of the Royal Air Force Police,
An immigration officer who is a senior official and who is designated for the purposes by the Secretary of State,
An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioner for Her Majesty's Revenue and Customs,
A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State,
The Chair of the Competition and Markets Authority,
The chairman, or a deputy chairman, of the Independent Police Complaints Commission, and
The Police and Investigations and Review Commissioner

doi:10.6342/NTU202301879

的核發時則需由執法機關首長（或緊急情況下指定適當代表）為之[112]，令狀發出後需經司法委員授權後始生效（即下段所介紹之 Double Lock 制度）。執法機關原則應基於偵查、預防重大犯罪之目的為之，「重大犯罪」係指犯罪者合理預期將遭受 3 年以上有期徒刑之判決、犯罪行為涉嫌使用暴力、獲取鉅額財產利益或由多人共同犯罪[113]，例外情形亦可用於預防、減輕人民生命、身體、心理上之傷害，如用來協助找尋弱勢者（vulnerable persons）。「Bulk equipment interference warrant」僅限於情報機關基於國家安全或國家安全兼具預防、偵查重大犯罪、經濟福祉之目的時為之[114]。

核發設備端干預令時應進行手段與目的之間具關聯性、比例原則、最小侵害手段性等比例原則之審核，評估時應考量基本權侵害之嚴重性、受干預主體（或任何其他可能受影響的人）的財產、隱私權、授權行為帶來預期的效果之間進行權衡，不應超過或恣意[115]。在選擇令狀程序之發出、更新、修正及終止時，應考量敏感性較高之訊息應採取程序保障密度較高之程序、公眾對於電信、郵政系統整體安全性之利益以及任何其他隱私權保護之公共利益[116]。其他程序保障規定包含：「資料必須以安全之方式留存，且在使用完畢後必須儘速銷毀」、「禁止蒐集非授權範圍之加密資料」以及 Double Lock 之核准程序。

有關管轄部分，除了國家刑事局(National Crime Agency)以及情報機關以外，其他執法機關使用設備端干預原則上須符合英國領土關聯性（British Islands Connection）之要件[117]，即至少必須有部分行為、設

[112] *See id.* at 27.
[113] *See id.* at 24.
[114] *See id.* at 29.
[115] *See id.*
[116] *See id.* at 30.
[117] Investigatory Powers Act 2016, § 107.

doi:10.6342/NTU202301879

備端干預或相關資訊出現或是可能出現在英國[118]，然考量設備端干預之使用目的，常用於調查暗網犯罪，而暗網又係透過具備隱藏 IP 位置特性之「The Onion Router」(洋蔥路由器）進行連接，故基本上木馬執行前，執法機關根本無從知悉干預之「對象設備」所在位置。因此，英國法上「British Islands Connection」之定義其實非常寬鬆，僅要有任何令狀授權之行為在英國境內實施(無論「設備」所在位置為何)，例如執行機關於英國境內實施遠端植入木馬之行為，縱使「設備」位於境外，此種情形因為植入木馬（hacking）的行為係在英國境內執行，亦會符合 British Islands Connection[119]。

另外，為了確保設備端干預之執行係針對英國境內之調查或運作執行，無論是否具備英國領土關聯性(British Islands Connection)，對外於境外之設備進行干預，除非符合調查對象是英國國民、可能成為英國刑事或民事訴訟對象、可能影響英國國民或產生可能在英國法院作為證據使用之素材等要件，否則均為法律所禁止[120]。惟本法亦肯認執法機關可透過與國家刑事局(National Crime Agency)以及情報機關等有權在不具英國領土關聯性（British Islands Connection）情形下執行設備端干預之機關進行合作，例如英國內政部所公布之設備端干預操作規範中舉例：執法機關發現國外暗網涉嫌誘拐英國境內兒童，然而無法基於暗網匿名之特性無法辨別犯罪嫌疑人及被害人，此時執法機關需要透過情報單位協助分析「大量型(Bulk)」設備端干預」所取得之資料以取得被害人以及英國境內犯罪嫌疑人之身分[121]，英國文獻亦指出在暗網及加密技術用於犯罪之情形下，

[118] Gemma Davies, *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers*, Journal of Criminal Law 84 (407), (Oct. 2020), p.15.
[119] *See id.* at 17.
[120] Equipment Interference Code Of Practice' (2018) , p.17.
[121] *See id.* at 111.

doi:10.6342/NTU202301879

情報機關協助執法機關偵辦嚴重犯罪之情形日益常見[122]，英國政府所公布之「大量型（Bulk）」設備端干預」執行案件中亦強調「大量型（Bulk）」設備端干預」取得資訊在 30 個月內已協助緝獲 50 名涉嫌兒童及少年性剝削之犯嫌，據此肯認「大量型（Bulk）」設備端干預」之數據對於幫助執法機關偵辦犯罪具有不可或缺之重要地位[123]。

有鑑於此，英國有論者認為基於設備端干預常用於暗網犯罪調查，而暗網犯罪又具有位置隱匿之特性，雖然設備端干預操作規範已規定在設備位置以科技方式刻意隱匿而未知之情形，倘有證據顯示案件具英國領土關聯性而後續調查具正當性時，亦可針對「所在地未知」之設備進行設備端干預，然建議未來可進一步參考荷蘭立法方式（詳參本文第四節第二項部分），明確規範設備端干預執行後發現設備位於境外後之處理程序，使實務執行更有明確依據[124]

第五款　司法審查程序－Double Lock 制度

Double Lock 是 IPA 所創設之司法審查程序，為本法創設之程序保障規範之一，明定國務大臣核發後須經司法委員(Judicial Commissioner，由現任或前任高級法官經總理任命後任之)核准後生效，本法明定司法委員進行審查時，要獨立、嚴格行使職權，不得違背公共利益或偏重國家安全、犯罪偵查及經濟利益[125]。在英國法上司法審查制度（judicial review）與上訴制度不同，因司法審查制度不同於上訴制度，因為法院通常不應以其認

[122] *See id.* at 17.
[123] UK Government, O*perational Case for Bulk Powers*, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf, p.12, last visited 07/04/2023.
[124] Gemma Davies, *Shining a Light on Policing of the Dark Web : An Analysis of UK Investigatory Powers*, Journal of Criminal Law 84 (407), (Oct. 2020), p.20
[125] Investigatory Powers Act 2016, §229 (6)

doi:10.6342/NTU202301879

為是「正確」的決定替代之，法院只會做出合法與否之判斷，而司法審查制度是對決定提出挑戰，而非僅對於決定本身為對錯之判斷[126]。值得注意的是並非所有 IPA 授權之干預手段均適用 Double Lock 程序，例如接觸資料則無庸經過司法委員之審核，而只需要監察機關之高級官員簽核[127]，其簽核前需諮詢經相關專業訓練之人，以確認是否符合本法規範。

須經司法委員核准後生效之干預方式如下:

干預方式	是否需經司法委員核准	備註
大量通信數據 Bulk Communications Data	是	
目標型通信數據 Targeted Communications Data	否	執法機關由通信數據授權辦公室核准 司法委員核准僅限基於確認新聞來源目的之案件[128]
大量設備端干預 Bulk Equipment Interference	是	
目標型設備端干預	是	原則需要司法委員核准，急迫情

[126] Daniel Severson, *Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill*, Lawfare Blog，2016 年 3 月 14 日，at https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers-bill, last visited 07/04/2023.

[127] Investigatory Powers Act 2016, §63(1)

[128] 舊法《調查權規範》（Regulation of Investigatory Powers Act，簡稱 RIPA)期間曾發生警方非法使用本法查閱記者確認新聞來源。註參 Patrick Wintour，British police's use of Ripa powers to snoop on journalists to be reined in，2014 年 10 月 12 日，at https://www.theguardian.com/world/2014/oct/12/police-ripa-powers-journalists-surveillance, last visited 07/04/2023.

doi:10.6342/NTU202301879

干預方式	是否需經司法委員核准	備註
Targeted Equipment Interference		形除外。
大量型攔截 Bulk Interception	是	
目標型攔截 Targeted Interception	是	原則需要司法委員核准，急迫情形除外。

(表格引自 Investigatory Powers Commissioner's Office 【IPCO】官網)

除個案司法監督外，本法亦規定一般性之司法整體監督制度，由IPC（Investigatory Powers Commissioner）負責，IPC 具有司法委員之身分，負責向總理提出年度報告、揭露嚴重錯誤（serious error）及肩負事後通知之任務[129]，依本法規定，錯誤揭露限於「 嚴重」之錯誤，所謂嚴重係指對受監察對象造成嚴重偏見、侵害，事後通知之程序要求亦係歐洲法院一再強調之法律正當程序[130]，藉由 IPC 事後通知使受監察對象獲知其受監察之訊息，也才使其得透過向 IPT（Investigatory Powers Tribunal）起訴來行使權利，並於本法創設第二審級之救濟制度[131]，然而得以上訴第二審之理由受有很大限制，僅限於具法原則、實務重要性或有其他具說服力理由之情形，始得提起上訴[132]。

[129] Investigatory Powers Act 2016, § 231

[130] Association for European Integration and Human Rights and Ekimhzhiev App no 62540/00 (ECtHR, 28 June 2007), paras 90-91; cf Kennedy v UK (2010) 52 EHRR 4.

[131] Investigatory Powers Act 2016, § 242

[132] *See id.* at § 242 (7)

doi:10.6342/NTU202301879

第三項　立法過程

IPA 制定過程諸多科技公司都表達反對之意見，Apple, Facebook, Google, Microsoft, Mozilla, Twitter, 以及 Yahoo 都在 IPA 草案階段提出書面意見，包含擔心政府在未來會阻止他們發展端對端加密。不僅科技公司提出「加密技術發展未來是否遭受限制」之質疑，調查權力法草案聯合委員會出具之報告，亦提出：

「我們同意政府有關試圖接觸加密通訊及電磁紀錄需要令狀之政策，是在不破壞加密鑰匙及在系統安裝後門之前提下，草案應予修正以茲釐清（第 16 點建議）。

政府仍需在草案中明確表明，提供端對端加密通信或其他不可解密的通信服務對通信服務業者而言若屬不可行，則不能要求其提供此等內容之解密副本。我們建議《工作守則》草案與法案一起發布，以供議會審議。（第 17 點建議）[133]」

英國政府針對聯合委員會上開意見，則回應如下：

「修訂後的法案已明確規定，從通信中刪除加密的義務，僅限於對承擔義務的公司為自己的商業目的已執行之電磁加密。法案已明確表明，通信服務業者之義務包括解密及技術協助，因履行義務恐衍生之

[133] *Joint Committee Report on the Draft Investigatory Powers Bill, HL Paper 93*, HC 651 79 (2016), at https:// www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf, last visited 07/04/2023.

doi:10.6342/NTU202301879

成本花費需納入考量[134,135]。」

英國議會審理 IPA 法案之過程中，諸多討論環繞在“何謂技術可行或技術上不可行”，以釐清科技公司之「解密」或「提供技術協助」之義務範圍。技術可行性是否包括考慮所提供的協助是否會損害基礎設施的整體安全性？其他用戶之安全、隱私是否納入考量[136]？法律是否會要求電信運營商投入資源以開發其解密能力？ 技術可行是指單一通信服務業者（CSPs）之能力？亦或產業龍頭者之能力？值得注意的是，最後通過之法律，有明文要求任何政府單位提出技術能力通知時，應權衡整體公眾利益及通訊安全，但並沒有要求國務大臣發出技術能力通知時，將成本及技術可行性納入考量，也沒有提供在何種情形下為「成本太高」或「不具技術可行性」之相關指引[137]。關於通信服務業者（如 WhatsApp、iMessage）所擔憂及在國會立法過程中受到激烈討論之端對端加密服務未來是否會遭禁止之問題，最終通過之法律並未明文規定，以至於有觀察者擔憂未來政府恐會以技術服務通知，來禁止通信服務業者提供端對端加密服務[138]。

對 IPA 法案持肯定態度者有如《安德森報告》的作者戴維·安德森（David Anderson QC），他在電訊報上針對英國調查權力法寫道：

---

[134] Home Department, *Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny*, Cm 9219 40–41 (2016), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file /504174/54575_Cm_9219_WEB.PDF, last visited 07/04/2023.

[135] 而英國政府之後公布之實務守則草案也明訂移除加密之義務僅限於自己公司（已經）使用之加密上。註參 Home Office, *Interception of Communications: Draft Code of Practice* 59 ¶ 8.4 (2016), at https://www.gov .uk/government/uploads/system/uploads/attachment_data/file/561091/16-10-18_Interception_code_of _practice_draft.pdf, last visited 07/02/2023.

[136] Daniel J. Weitzner, *The Encryption Debate Enters Phase Two,* Lawfare (Mar. 16, 2016, 12:13 PM), at https://www.lawfareblog.com/encryption-debate-enters-phase-two, last visited 07/02/2023.

[137] *See id*. at 10.

[138] Natasha Lomas, *UK Surveillance Bill Includes Powers to Limit End-to-end Encryption,* TechCrunch (July 15, 2016), at https://techcrunch.com/2016/07/15/uk-surveillance-bill-includes-powers-to-limit-end-to -end-encryption/, last visited 07/02/2023.

doi:10.6342/NTU202301879

「IPA 法案進行了合併，並明確提到了情報和執法部門可以使用的權力，該法案“使最重要的事情做好了。通過宣揚執法機關和情報機構行使或渴望行使的每一項非凡權力，它恢復了法治並為坦率行為樹立了國際基準[139]。」

英國學界亦有認為 IPA 對於英國監察法制算是一大進度，因 1984 年電信法、1997 年警察法、1994 年情報工作法，英國早已存在廣泛之監察現狀，IPA 使監察之爭議更為透明。IPA 有幾項重要的聲明，包含要求政府行使本法授權時要考慮：隱私保護之重要性、最小侵害手段性、通訊之整體公眾利益等，且將歐洲人權法院、歐盟法院過去對於通訊數據調查類型案件之相關宣示放入其中。為避免使司法委員之審核淪為國務大臣之橡皮圖章，本法要求司法委員獨立且嚴格地行使職權，更明定司法委員進行審核時，不得違背公共利益或偏重國家安全、犯罪偵查及經濟利益，但未來還要視司法委員之個人人格、其所獲得之資訊為何等等因素，才能決定性影響司法委員獨立行使職權之使命[140]，但可預見的是，司法委員進行必要性跟比例原則審核時，將會有異於法官或一般政府獨立機關之發展[141]。

第二節　法國

第一項　早年立法–內部安全法及刑事訴訟法

法國早於 2000 年代初期即有解密相關之干預處分授權依據。立法模

[139] David. Anderson QC, David. Anderson: *The Investigatory Powers Bill is still a work in progress*, The Telegraph (March. 2, 2016, 09:21AM), at https://www.telegraph.co.uk/news/uknews/law-and-order/12180439/David-Anderson-The-Investigatory-Powers-Bill-is-still-a-work-in-progress.html, last visited 07/02/2023.

[140] Lorna Woods, *the Investigatory Powers Act 2016*, 3 EUR. DATA PROT. L. REV. 103-104(2017).

[141] Thiago Moraes, *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures*, 6 EUR. DATA PROT. L. REV. 41 (2020). 50.

doi:10.6342/NTU202301879

式係依「國安目的」及「執法目的」分別規定於內部安全法（CODE DE LA SECURITE INTERIEURE）以及刑事訴訟法（CODE DE PROCÉDURE PÉNALE）。

內部安全法授權國家情報和安全部門，在符合「保護國家安全」、「保護“法國經濟和科學潛力基本要素之安全”」、「防止恐怖主義行為」、「壓制組織犯罪」及「防止非法團體重組（例如：被禁止之仇恨團體或私人準軍事團體）」等法律列舉特定目的時，依法可以截取及閱讀私人通訊[142]。程序上須由國防部長、內政部長或負責國土安全之機關首長書面申請，經總理或其授權之人書面授權[143]。依上開程序取得之「加密資料」，得向加密服務提供商要求解密[144]，其方式不限於解密金鑰，亦包含任何足使加密資訊變成得以閱讀形式之任何軟體及資訊[145]。加密服務提供商除可證明自己無能力解密，否則應在 72 小時之內解密或向授權其使用加密服務之業者提出解密請求[146]。

法國刑事訴訟法早於 2004 年即規定，執法機關基於刑事犯罪偵查之目的，經預審法官、人身自由與羈押法官核發令狀後進行私人電信通訊之截取、錄音及抄錄[147]，依照同法第 230-1 及 230-2 之規定，當截取所取得之資訊或業已扣押之電磁紀錄經加密時，執法機關得經預審法官、檢察官或系爭偵查案件之管轄法院核准後，要求適當之個人或法人執行技術操作使其轉為得以理解之形式[148]，並授權執法機關得向技術支持中心（Technical support center）提出技術協助之要求，技術支持中心係 2002 年法國內政部

[142] CODE DE LA SECURITE INTERIEURE [INTERIOR SECURITY CODE] art. L811-3, L852-1.
[143] *See id.* art. L821-4.
[144] *See id.* art . L871-1.
[145] *See id.* art R871-3.
[146] *See id.* art L871-1.
[147] CODE DE PROCÉDURE PÉNALE [CODE OF CRIMINAL PROCEDURE] art. 100,706-95
[148] *See id.* art. 230-1.

doi:10.6342/NTU202301879

所創建[149]，數據解密為其執掌之其中一項任務[150]。

第二項　2015 年後之一連串立（修）法

2015 年法國巴黎發生嚴重恐怖攻擊之後，法國長時間處於緊急狀態，法國國會在 2015 至 2016 年間進行一連串之立法，擴大了政府監視以及合法駭客之法律授權，針對原本已立法授權執法機關在刑事案件調查時開出之解密令狀，擴大、加重對於未能遵守之刑事處罰，針對情報調查，創建新的強制性公開訊息和解密程序[151]。

第一款　刑事訴訟法（French Code of Criminal Procedure)

2016 年 6 月 3 日修正之刑事訴訟法 706-73 條以下之「特殊偵查技術」規定，適用於同法第 706-73 條及第 706-73-1 條列舉重罪，強化了執法機關對抗組織犯罪、恐怖主義以及資助恐怖主義犯罪之偵查權。

同法第 706-95-1 條係有關遠端訪問「通訊內容」之規定，針對執法機關針對原有 706-95 條截取、記錄和轉錄以電子通信方式發送的通信訊息之偵查手段，授權執法機關可以使用遠端訪問之方式執行訊息截收。程序上由檢察官聲請，經人身自由與羈押法官授權、或由預審法官為之，期限 1 個月，可延長 1 次。

同法第 706-102-1 條則是有關秘密線上搜索之規定，授權執法機關基

[149] Décret n°2002-1073 du 7 août 2002 d’ application de l’ article 30 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d’ assistance [Decree No. 2002-1073 of August 7, 2002, Applying Article 30 of Law No. 2001-1062 of November 2001 Regarding Everyday Security and Creating the Technical Support Center] (as amended on May 9, 2014)

[150] Circulaire relative au fonctionnement du centre technique d’ assistance *(*C.T.A.*)* [Circular Regarding the Functioning of the Technical Support Center *(*C.T.A.*)*], MINISTÈRE DE L’ INTÉRIEUR, DE LA SÉCURITÉ INTÉRIEURE ET DES LIBERTÉS LOCALES [MINISTRY OF THE INTERIOR, OF INTERIOR SECURITY, AND OF LOCAL FREEDOMS] (Mar. 27, 2003)

[151] Bhairav Acharya, Kevin Bankston, Ross Schulman, and Andi Wilson Thompson, *'Deciphering the Encryption Debate In Europe: France'* (Open Technology Institute 2017b), July.2017, at https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf, last visited 07/03/2023.

doi:10.6342/NTU202301879

於刑事偵查之目的設置技術設備，以秘密之方式、自任何地方，透過植入駭客程式之方式訪問電腦設備，截取、保存或傳輸設備端之電磁紀錄[152]。程序要件採法官保留，當未經設備所有（使用）人知悉或同意之情況下，進入私人處所、車內以物理植入程式時，程序上由檢察官聲請經人身自由與羈押法官授權、或由預審法官為之，當進入住宅且非在同法第 59 條規定之上午 6 點至晚上 9 點間為之時，亦須由檢察官聲請經人身自由與拘留法官授權、或由預審法官為之，此項授權可基於對設備植入程式之單一目的，移除程式時相關程序規範亦同。同法第 2 項授權檢察官聲請經人身自由與羈押法官授權、或預審法官為之，得以遠端植入程式之方式取得同法第 706-102-1 條電磁紀錄。同法第 706-102-5 條是有關特定專業領域人員之特別規定，對於設備及所持電磁資訊係涉及原刑事訴訟法就搜索有特別限制規定之處所（如律師事務所、新聞媒體、司法機關、國會議員之住家及車輛），則不得以植入程式之方式為之[153]。

國家情報和安全部門使用國家木馬之授權立法起於 2015 年情報法（Intelligence Act of 2015）修正法國內部安全法 853-2 條規定[154]，授權內閣部長得以書面請求法國總理許可授權法國情報單位使用國家木馬，法國總理發出國家木馬許可前，必須向職司國家情報蒐集技術之國家監督委員會（Commission nationale de contrôle des techniques de renseignement, 簡稱 CNCTR[155]）諮詢[156]，法國總理之決定雖不受到 CNCTR 諮詢結果之拘束，但若係與監督委員會之建議相違，此項授權可能會受到法國最高行政

[152] CODE DE PROCÉDURE PÉNALE [CODE OF CRIMINAL PROCEDURE] art. 706-102-1

[153] *See id.* art.706-102-5

[154] CODE DE LA SECURITE INTERIEURE [INTERIOR SECURITY CODE] art. L853-2.

[155] 依據 2015 年情報法之規定，CNCTR 為獨立委員會，由 9 名委員組成，成員包含議長指定的 4 名議員、4 名法官以及 1 名電信國家監管局指定之技術專家。註引自 CNCTR 官網，https://data.guardint.org/en/entity/kl3bl230jmn.，最後瀏覽日 2023 年 6 月 30 日。

[156] Felix Treguer, *"Internet Surveillance in France's Intelligence Act"*, HAL, 2016 年 11 月 19 日, at https://halshs.archives-ouvertes.fr/halshs-01399548/document, last visited 07/04/2023.

doi:10.6342/NTU202301879

法院之挑戰[157]。

第二款　數位共和法（Digital Republic Law）

法國 2015 年後之修法過程中，「強制後門」之立法引發激烈的爭辯，法國國民議會右派代表娜塔莉·柯希亞斯柯-莫里塞（Nathalie Kosciusko-Morizet）所提出之數位共和法案（Digital Republic Bill）即主張「技術製造商必須考慮因案件偵查且獲得司法授權後，授權警察使用硬體的必要性。」[158]，更引用希伯來聖經中，大衛與歌利亞（David and Goliath）以小勝大之故事，主張法國應站出來對抗這些將企業利益放在法國國家安全之前矽谷大企業[159]，提出法國應該要做立法先驅之觀點，主張加密不應妨害執法部門之調查，提出「國務院有權要求硬體設備製造商在所生產之產品設立後門」之法案版本。反對論者認為，「強制後門」之立法將反向驅使企業不在法國進行加密技術之設計或提供[160]，時任法國數位部長之 Axelle Lemaire 於強制後門的修法爭論中採反對立場，認為“強制後門的提議等同設計漏洞”，主張“有了後門，個人數據根本不受保護”、“即使意圖是值得被讚許的，但它同時也為那些沒有那麼值得稱讚意圖之人敞開了大門，更不用說當這些公司計畫為設計漏洞時，將對這些公司的信譽造成經濟損失之可能性了”[161]。

2016 年 10 月，法國數位共和法（Digital Republic Law）立法通過，

---

[157] Internal Security Code, Art. L821-8.

[158] Digital Republic Bill (No. 3318), Amendment No. CL92 (Jan. 4, 2016) (Fr.), at http://www.assemblee-nationale .fr/14/amendements/3318/CION_LOIS/CL92.asp, last visited 07/02/2023.

[159] Bhairav Acharya, Kevin Bankston, Ross Schulman, and Andi Wilson Thompson, *'Deciphering the Encryption Debate In Europe: France'* (Open Technology Institute 2017b), (July, 2017), at https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf, last visited 07/04/2023.

[160] Joshua Eaton, *With or Without Evidence, Terrorism Fuels Combustible Encryption Debate*, Christian Sci. Monitor (Mar. 28, 2016), at http://www.csmonitor.com/World/Passcode/2016/0328/With-or-without-evId.ence-terrorism-fuels-combustible-encryption-debate, last visited 07/04/2023.

[161] Liam Tung, *Encryption Backdoors by Law? France Says "Non,"* ZDNet，Jan 18, 2016, at http:// www.zdnet.com/article/encryption-backdoors-by-law-france-says-non/ last visited 07/05/2023.

doi:10.6342/NTU202301879

其中更新諸多涉及網路中立性、接觸政府資訊以及資訊隱私之相關規定[162]，立法過程中受到激烈爭辯之「強制後門」立法，最後在國會以 1 票之差未能通過[163]。法國在數位共和法制定後，確立了加密技術對於保護人民隱私權之重要性，並賦予法國數據保護監管機關「Commission Nationale de l'Informatique et des Libertés」，簡稱「CNIL」）為獨立行使資料隱私保護之權責機關，CNIL 的任務之一即為「與科技資訊之變化並駕齊驅，向社會大眾公告其對於隱私權之影響」[164]、「促進包含加密技術在內之科技使用，以促進隱私權保護」[165]，數位共和法賦予 CNIL 更大的權利以制裁違反隱私保護相關法規之事件，從數位共和法最後確立之宗旨，均可發現法國之立法方向係往支持強化加密技術以保護資訊隱私之方向邁進。

第三款　國際電子通信法（International Electronic Communications Law）

為因應加密技術對於國安及犯罪偵查之影響，法國國會通過國際電子通信法（International Electronic Communications Law），修正了法國內部安全法（Code de la sécurité intérieure）第四章有關國際電子通信的監視措施（Des mesures de surveillance des communications électroniques internationales）之部分規定[166]，新法授權政府可基於國家安全或包含對抗

[162] Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Oct. 8, 2016, p. 235, at https://www.legifrance.gouv.fr/affichTexte.do;jsessionId.=689260AE5CAF2A74BA1806E0C4ADD D67.tpdila17v_1?cidTexte=JORFTEXT000033202746&categorieLien=Id.., last visited 07/05/2023.

[163] Daniel Severson, *"Encryption Legislation Advances in France,"* Lawfare, April 14, 2016, at https://www.lawfareblog.com/encryption-legislation-advances-france, last visited 07/05/2023.

[164] Loi78-17 du 6 janvier 1978 modifée art.11 (4) (Fr.), https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978 -modifiee#Article1.

[165] Loi 2016-1321 du 7 octobre 2016 pour une République numérique art. 59(2)(f) (Fr.), at https://www .legifrance.gouv.fr/affichTexte.do;jsessionid=689260AE5CAF2A74BA1806E0C4ADDD67.tpdila17v_1?cidTexte =JORFTEXT000033202746&categorieLien=id.

[166] Loi 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationals [Law 2015-1556 of November 30, 2015 on International Electronic C

doi:10.6342/NTU202301879

恐怖主義、促進科技、經濟及工業利益等在內之其他國家基本利益之目的蒐集外國情報[167]，並有權保留數據，法國政府依法可儲存國外通訊之內容最長 1 年、元數據(metadata)最長 6 年[168]，當資訊加密時，情報單位於蒐集加密資料後最長可儲存 8 年，在尚未解密之前通訊內容儲存之 1 年期限不予起算，在絕對必要之範圍內，得以永久保留加密資料，超過保留期限則必須銷毀[169]。

第四款　反恐法

2016 年 6 月法國修正反恐法，加重在刑事、恐怖主義調查案件中，拒絕針對加密通訊內容提供技術協助之罰責，修正了 2001 年 11 月施行之法國刑法(Code pénal)妨害司法罪章(Des entraves à l' exercice de la justice)中第 434-15-2 條有關拒絕提供解密金鑰之刑事處罰規定，修正後之刑法第 434-15-2 條規定“任何人明知將作為預備、促進、實施刑事犯罪之加密訊息之解密金鑰，而拒絕提供、使用或與有關單位合作時，可處 3 年以下有期徒刑併科 270, 000 歐元之罰金，如果合作原可避免某項犯罪之實施或限制其影響，則可處以 5 年以下有期徒刑和 450, 000 歐元罰金”[170]，此次修

---

ommunications], Journal Officiel de la République Française [J.O.] [Official Gazette of France], （Dec. 1, 2015）, p. 22, 185.

[167] Code de la Sécurité Intérieure art. 811-3 (Fr.), at https://www.legifrance.gouv.fr/affichCode.do;jsessionid=EB7E1CB999CD31779A3967D448C9619B.tpdila17v_1idSectionTA=LEGISCTA000030935034&cId.Texte =LEGITEXT000025503132&dateTexte=20170129.

[168] Code de la Sécurité Intérieure art. 854-5 (Fr.), at https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=279B93BCE1C89CA30D48D9BE0715558E.tpdila17v_1?Id.Article=LEGIARTI000031550341&cidTexte=LEGITEXT000025503132&dateTexte=20170129&categorieLien =id&oldAction=&nbResultRech=.

[169] Code de la Sécurité Intérieure art. 822-2 (Fr.), at https://www .legifrance.gouv.fr/affichCodeArticle.do;jsessionid=279B93BCE1C89CA30D48D9BE0715558E.tpdila17v_1 ? idArticle=LEGIARTI000030935068&cidTexte=LEGITEXT000025503132&dateTexte=20170129&categorieLien =Id.&oldAction=; Code de la Sécurité Intérieure art. 854-8 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&Id.Article=LEGIARTI000031550357&dateTexte =&categorieLien =cid.

[170] Code Pénal art.434-15-2(Fr.), at https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=CD80FBE41F7648FD56B1C5D53B5AC1F3.tpdila23v_1? idArticle=LEGIARTI000032654251&cidTexte=LEGITEXT000006 070719&categorieLien=id&dateTexte=.

doi:10.6342/NTU202301879

正將罰金提高了 6 倍之多。

反恐法之修法過程在國會經過諸多角力，原本參議院之版本僅將拒絕解密之罰金訂為 150, 000 歐元[171]，共和黨議員埃里克·喬蒂（Éric Ciotti）提出之版本則要求所有電信設備製造商、電信服務商及網路服務商須交出關於恐怖攻擊調查所需之全部通訊相關資料，違反者最高可處 200 萬歐元罰金，並限制在法國境內市場銷售商品、服務，最高 1 年[172]，埃里克·喬蒂之法案版本提到：2015 年法國司法警察資訊及科技軌跡服務中心（le service central de l’ informatique et des traces technologiques de la police judiciaire.）處理之 133 件手機鑑識分析案件中，至少 8 件面臨手機無法解密之困境，其中包含在 2015 年 11 月巴黎恐怖攻擊事件中查扣之 iPhone4S，以及因涉嫌策畫 2015 年對巴黎南郊猶太城(Villejuif)一座教堂發動恐怖攻擊，而遭逮捕之阿爾及利亞籍嫌犯葛蘭（Sid Ahmed Ghlam）所持用之手機[173]，葛蘭遭捕入獄後，更遭發現其夾帶手機入獄，對外聯繫超過 6 個月始遭發現，巧合的是，相關對外聯繫紀錄至 2015 年 11 月 13 日便中斷，該日即係巴黎恐怖攻擊發生之日，而國家安全局局長邁克爾·羅傑斯將軍（L’ amiral Michael Rogers）於此法案表示「如果沒有加密，就可以避免巴黎襲擊。」[174]。

修法過程中，除了提高罰金以外，亦有針對提供加密商品、服務業者拒絕協助解密之刑事責任提高等提案，然最終均未在國會通過。例如修法過程中曾有關 Apple 與美國 FBI 有關解密之爭論乙事即被提出，國民議會

[171] Bill to Combat Organized Crime, Terrorism, and Their Financing art. 4 quinquies (Senate version of Mar. 23, 2016), at http://www.senat.fr/leg/pjl15-492.html.

[172] Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 221 (Feb. 25, 2016), at http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp.

[173] Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Amendment No. 221 (Feb. 25, 2016), at http://www.assemblee-nationale.fr/14/amendements/3515/AN/221.asp

[174] *See id.*

doi:10.6342/NTU202301879

最初提出之反恐法修正草案中，在拒絕就該公司所研發、提供之加密技術之解密技術時，將刑罰提高至 35 萬歐元以及 5 年以下有期徒刑，上開提案至上議院法律委員會所提出之報告中，雖同意針對製造加密服務之私人課以高強度之刑事責任之基調，但卻認為在反恐法中修正是多餘且適得其反的，理由是認為此項項修正將混亂刑法體系，因現有刑法中已有相關處罰規定[175]。

除此之外，其他較為激進之立法提案也遭到國會否決，例如：法國刑事訴訟法第 60 之 1 條規定在恐怖主義調查中，未能及時向司法警察提供「有關」或「用於查明真相」的訊息，最高可處以 3, 750 歐元的罰金[176]，而國民議會修正版本將本條規定之罰金提高至 15, 000 歐元，並增加 2 年以下有期徒刑之刑事處罰，上議院刪除了有關有期徒刑之規定，理由認為刑期之規定並不妥當且有為刑罰必要性，尤其在個人是「未能」完成國家之要求，而非「拒絕」之情形[177]。然而，實際上，在法國國會嘗試立法修正刑事訴訟法第 60 之 1 條規定的同時，現行規定之刑事處罰實際上尚未使用過[178]，上開修正案最終並未於議會通過。

法國這一系列修法過程中有著激烈的立法爭論，如共和黨埃里克·喬蒂（Éric Ciotti）等議員主張政府面對有效執法與加密之爭議，政府所要面對者都是國際大企業，以刑罰課以重罰有其必要性，更認為要搭配一段期間之禁止市場銷售，他表示“向這些公司發出信號的唯一途徑是，他們的

[175] Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Commission of Laws Report (No. 491) (Mar. 23, 2016), at http://www.senat.fr/rap/l15-491-1/l15-491-17.html.

[176] Code de Procédure Pénal art.60-1 (Fr.), at https://www.legifrance.gouv.fr/affichCodeArticle.do?cid Texte =LEGITEXT000006071154&idArticle=LEGIARTI000006575048&dateTexte=&categorieLien=cid.

[177] Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), Commission of Laws Report (No. 491) (Mar. 23, 2016), at http://www.senat.fr/rap/l15-491-1/l15-491-17.html.

[178] Guillaume Champeau, *5 ans de prison en cas de refus de communiquer des données chiffrés*, Numerama (Mar. 3, 2016), at http://www.numerama.com/politique/149981-5-ans-de-prison-en-cas-de-refus-de -communiquer-des-donnees-chiffrees.html.

doi:10.6342/NTU202301879

財務獎勵措施永遠不能超越民主國家的法律[179]”；社會主義黨雅恩·加呂（Yann Galut）則表示“多國已正在進行相同的立法，因為令人沮喪的偵查是不被允許的”；上議院法律委員會之報告中，帕斯卡爾·波佩林（Pascal Popelin）譴責科技龍頭企業拒絕合作之行為，表示這些科技龍頭“偽以自由之名義”為自己不合理之行為進行辯護，儘管政府已經可以根據法國部分法令提出解密之要求，然這些法令並未對不遵守之行為訂定處罰[180]。

另一方面，在國民議會的第一次會議中亦有反對論者發出警告，認為“應考慮解密金鑰落入中國、朝鮮或敘利亞這樣專制政權政府手中會發生什麼後果”。法國司法部長讓-雅克·於爾沃阿（Jean-Jacques Urvoas）則認為，國內立法無法有效產生影響，惟有國際合作才能解決這個問題，並表示法國已針對此問題與歐盟、美國進行討論[181]。

綜觀法國這波修法爭論之最終角力結果，法國以法律強制技術協助，並再次提高拒絕提供協助之罰金刑度。針對加密制度，最終係採用 CNIL 之立場，同意強化加密技術對於個人生活隱私之重要性，並拒絕採用強制後門之設立，法國網絡安全局（French Network and Information Security Agency，簡稱 ANSSI）在 2016 年公布之備忘錄中也支持強化加密技術，拒絕強制後門之相同立場[182]。

第三節 德國

德國過去存在能否單以監聽之法律授權（修正前之德國刑事訴訟法第 100a 條）作為國家以植入木馬程式方式監聽加密網路通訊之爭論，此爭論在德國 2017 年 8 月 24 日生效之「刑事程序更有效率與更契合實務調整法

[179] Bill to Combat Organized Crime, Terrorism, and Their Financing (No. 3515), National Assembly’s First Meeting (Mar. 3, 2016), at http://www.assemblee-nationale.fr/14/cri/2015-2016/20160140.asp.
[180] *See id.*
[181] *See id.*
[182] Martin Untersinger, *La CNIL Très Favorable au Chiffrement des Données*, Le Monde (Apr. 9, 2016, 10:23AM), at http://www.lemonde.fr/pixels/article/2016/04/09/la-cnil-tres-favorable-au-chiffrement-des-donnees _4899172_4408996.html#hWGj18UR5tA1CCWt.99, last visited 07/04/2023.

doi:10.6342/NTU202301879

案」(Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens) 公布後消除，上開法案新增一種針對加密過通訊資料，賦予德國刑事追訴機關於德國刑事訴訟法之新興干預手段：來源端電信監察(Quellen-Telekommunikationsüberwachung)。

第一項　德國刑事訴訟法秘密偵查之概述

德國刑事訴訟法之規範體系，秘密偵查干預手段規定在第 99 條至第第 101b 條以及第 110a 條至第 110c 條，共有 18 條規定，各條規範內容為:第 99 條、第 100 條(郵政扣押)；第 100a 條（通訊監察與來源端通訊監察)、第 100b 條（線上搜索)、第 100c 條（家宅內監聽)、第 100d 條（核心私人領域與拒絕證言保護)、第 100e 條（第 100a 條至第 100c 條之程序規範)、第 100f 條（家宅外監聽)、第 100g 條（通信紀錄調取)、第 100h 條（家宅外科技手段監察)、第 100i 條（行動通訊設備監察)、第 100j 條（未來電信紀錄之調取)、第 101 條秘密偵查程序規範、第 101a 條（相關程序特別規定)、第 101b 條（統計調查及報告義務)、第 110a 條（臥底偵查)、第 110b 條（臥底偵查程序）及 110c 條（臥底權限)。

從上開法規體系足以發現，「來源端通訊監察」係規定在原德國刑事訴訟法第 100a 條通訊監察之後，建立在原通訊監察制度下之規範下，透過擴張執行方式，實際上同時擴充傳統通訊監察之概念，藉由雙重干預（Doppelnatur）[183]之立法技術，納入對於 IT 基本權之

[183] 所謂雙重干預（或稱雙門模式【Doppeltürmodell】、雙重管制模式）係德國聯邦憲法法院在公民通信資料儲存案發展出之偵查概念，指立法者對於資料之取得，規範上並不僅限於對於傳輸資料之干預，而得藉由對於儲存資料之干預為之，但是應存在於個別法規之授權，而不能混和比較資料取得之規範為之，此一概念主要在危險預防法規中有廣泛運用，隨著第 100a 條第 1 項第 3 句「假設替代干預」法規確立，成為刑事偵查法制之一部。註轉引自鄭惟容，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研究所碩士論文，2019 年，頁 87。

doi:10.6342/NTU202301879

干預手段，因應現今時代通訊方式之轉變[184]。

第二項　來源端通訊監察

第一款　來源端通訊監察概述

「來源端通訊監察」一詞源自於德文「Quellen-Telekommunikationsüberwachung」（簡稱Quellen-TKÜ」），係因應網路通訊加密技術發展後，傳統通訊監察干預手段不敷使用，而發展出「於通訊各自來源端植入木馬，以此方式取得尚未加密或已經解密之資訊內容」之新興干預手段，又因此種干預方式，是在通話雙方之端點設備植入木馬程式，德國因此將其命名為來源端（或稱設備端）通訊監察[185]。

德國增訂來源端通訊監察之立法方式，是在刑事訴訟法原本第100a條第1項通訊監察之條文，增加第2句及第3句之兩種來源端通訊監察得以適用之情形。其條文內容分別為：「當為了尤其得以依未加密方式進行監察與記錄而有必要時，亦得以科技方法侵入受干預人所使用之資訊科技系統，進行電信通訊之監察與記錄」（第100a條第1項第2句）；「儲存於受干預人資訊科技系統之通訊內與狀態亦得監察與記錄，當其在公共電信線路以加密方式所進行之傳輸過程原本即可監察與記錄者」（同條項第3句）[186]。易言之，德國將來源端通訊監察依其所欲取得通訊資訊之狀態，區分為第100a條第1項第2句「傳輸過程中之通訊監察」[187]以及第3句「儲存資料之監察」[188]。

上開立法值得關注之一點在於上開立法某程度擴張德國傳統上針對

[184]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研究所碩士論文，2019年，頁81。
[185] 朱富美，國安偵查與基本權保障-「科技偵查法」草案「設備端通訊監察」章評析與建議，法學叢刊，第260期，2020年10月，頁85。
[186] 王士帆，德國科技偵查規定釋義，法學叢刊，第262期，2021年4月，頁88。
[187] § 100a Abs. 1 S. 2 StPO.
[188] § 100a Abs. 1 S. 3 StPO.

doi:10.6342/NTU202301879

通訊監察範圍之界定。傳統上，德國針對「通訊秘密權」之權利保障範圍，係以「始於終端，終於終端」[189]作為區分界線[190]，符合「通訊進行中」之一切內容性或非內容性之資料，都能夠成立通訊秘密權之保護[191]。德國聯邦憲法法院在電子郵件扣押案認定，性質屬於「尚未寄出」或「已經接收」之訊息，因「通信尚未開始或已經結束」，其性質應屬保全扣押之範疇，並不在秘密通訊自由權保障範圍以內[192]。易言之，依照通訊傳輸架構以及受侵害之基本權，若屬「進行中之通訊」，應屬秘密通訊自由權保障範疇，以通訊監察為其干預授權；至於並非傳輸過程，而係業已結束或尚未開始而儲存於設備內之通訊內容，應屬個人資訊自主決定權之保護範疇，應援引以搜索扣押為干預依據。

然而，此種以「傳輸過程」與「存儲狀態」區分不同干預授權領域之方式，在面對「加密技術」發展所帶來之衝擊，以及偵辦重大犯罪時對於秘密偵查之需求，已有重新思考並調整之必要。從德國刑事訴訟法第 100a 條第 1 項第 3 句之立法理由說明可知，來源端通訊監察是緊扣「公共電信線路以加密方式所進行之傳輸過程『原本』即可監察與記錄」為核准要件，所以和傳統之電信監察具有功能等價，也就是說，未加密通訊內容本來自核准電信監察令狀開始即可實施監察，因而已儲存之電信通訊內容及狀態亦得以比照辦理[193]。是以，第 100a 條第 1 項第 3 句之來源端通訊監察，雖是針對「已儲存」之通訊資訊，但要件上必須限於儲存時間點讚在「核准之通訊監察期間內」，故性質毋寧是相較於 100b 條線上搜索（詳後述）

[189]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研究所碩士論文，2019 年，頁 88。
[190] 我國最高法院 106 年度台非字第 259 號刑事判決同此見解。
[191]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研究所碩士論文，2019 年，頁 72。
[192] 針對「已讀取但繼續保留在伺服器之電子郵件，德國聯邦憲法法院 2009 年之裁判認為仍受到秘密通訊自由權之保障，但得以扣押手段取得」註引自王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 93。
[193]王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 96-97。

doi:10.6342/NTU202301879

之一種「小型線上搜索」[194]。

第二款　聲請要件

德國來源端通訊監察既作為傳統通訊監察之補充手段，聲請要件比照原有通訊監察之「重罪原則」、「必要性」、「關聯性」及「最後手段性」等規定，原則由檢察官聲請法官核准，急迫情形例外由檢察官為之，並於 3 日內聲請法官確認[195]，命令期間為 3 個月，必要時得延長之，每次延長不得逾 3 個月。禁止監察私人生活核心領域，若取得者不得使用且應立刻刪除，過程應予以紀錄[196]。而針對新增之來源端通訊監察，新增之程序配套規範則包含同條第 5 項「技術性擔保」[197]及第 100a 條第 6 項書面記錄義務等規定。

第三款　「技術性擔保」

德國刑事訴訟法第 100a 條第 5 項規定實施來源端通訊監察時，必須以技術方法確保只可監察與記錄「進行中之電信通訊（第 1 項第 2 句）」或「依第 100e 條第 1 項核准對於在公共電信線路以加密方式進行傳輸時亦得監察與紀錄之通訊內容與紀錄，自核准時點開始之通訊內容與狀態（第 1 項第 3 句）」;「系統只可進行為取得資料所必須之改變」;「措施結束時，技術上應儘可能使所進行之變更自動回復」;「所採用之方法應依科技狀態防止他人無權使用。所複製之資料應依科技狀態保護免於變更，無權刪除或無權知悉。」[198]。本條規定可認德國立法者以法律明文規定僅有在使用之軟體可確保只會取得法律明確設限範圍以內之資訊，而以技術保證不會取得法律授權範圍以外資料時，其依法所為之來源端通

[194]同上註，頁 97。
[195] § 100e I StPO
[196] § 100d I II StPO.
[197] § 100a Abs. 5 StPO.
[198] 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 90-91。

doi:10.6342/NTU202301879

訊監察才是合法的。亦即，即使係依 100a 條第 1 項第 3 句監察與記錄儲存於電腦系統的通信內容和狀態，也唯有在執法機關使用之軟體足以擔保取得之內容限於「自核准時點之後的通信內容與狀態」，始為合法，因此種情形才會與一般電信監察成為功能等價，一個無法擔保上開取證限制之軟體，自始不得使用[199]。是以，倘若木馬無法自動判決資訊儲存之時點，亦即，對於所存取的通訊方已儲存之通訊內容和狀態，無法判決受干預人儲存時點是在核准來源端通訊監察之前或之後者，會成為違法之來源端通訊監察，必須停止監察[200]。

觀諸上開針對來源端通訊監察之特殊程序規範，應可理解為德國立法者有鑑於來源端通訊監察有別於傳統通訊監察或以扣押方式取得通訊內容之基本權侵害類型，來源端通訊監察具有侵害「使用者對於其所使用之資訊科技系統之『完整性』」與『秘密性』期待」之性質，程序保障上應更優於傳統通訊監察，且應針對資訊科技系統之「完整性」及「秘密性」為「最小侵害手段」之設計，從而有關於「在關連且必要的系統干預，應盡可能輕微和自動回復原狀，並盡可能阻止第三人在使用國家軟體下進行干預（第 100a 條第 5 項第 1 句第 2、3 款）」、「應擔保從設備端複製資料之可靠性及完整性，防止他人無權知悉（第 100a 條第 5 項第 2、3 句）」等有別於其他干預手段之程序規範，應可認為係針對其作為侵害 IT 基本權之干預手段之特性而生之程序保障規範。

第四款　書面記錄義務

第 100a 條第 6 項為特別書面記錄義務之規定，立法目的是為了讓法院事後得有效針對來源端通訊監察之核准與執行進行合法性監督，尤其

[199] Prof. Dr. Mark A. Zöller，譯者王士帆，來源端電信監察與線上搜索-德國刑事追訴機關之新手段，司法新聲，130 期，頁 109，2019 年 4 月。

[200]王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 98。

doi:10.6342/NTU202301879

針對執行面是否遵守上述技術擔保規定，透過留存書面記錄之方式確保受干預人救濟權。法定書面紀錄內容應包含「科技方法名稱」「使用時點」、「資訊技術系統識別資料」以及「所採取非暫時性之變更」、「說明得調查取得之資料」以及「執行機關」[201]。

第五款　通信服務商之協力義務

同法第 100a 條第 4 項「通信服務商之協力義務」規定明定「根據電信監察與記錄命令，任何提供或參與電信通訊業務之人應協助法院、檢察官及其執行警察職務之偵查人員(法院組織法第 152 條)實施本條文之措施，並應立即提供必要回復，至於是否與在如何範圍之內採取防護措施，則由《電信通訊法》（Telekommunikationsgesetz）及《電信通訊監察規則》（Telekommunikations-Überwachungsverordnung）訂定之。[202]」。立法理由中並未包含義務之具體內容，而是一般性參閱電信法及電信監察規則，但排除提供「解密金鑰」以及「後門」之義務[203]。

本條關於通訊服務商之協力義務，射程範圍包含一切涉及提供或協助通訊之網路應用服務供應商或網路服務供應商，均屬應遵守本條協力義務之主體，負有與相關偵查人員協力進行後續偵查行為之義務[204]。若通訊服務商設於境外，內國之網路服務供應商之合作夥伴則負有協力義務[205]。

第三項　線上搜索（Online-Durchsuchung）

第一款　線上搜索與來源端通訊監察之概念區分

德國刑事訴訟法第 100b 條線上搜索(Online-Durchsuchung，俗稱大木

[201] 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 99。
[202] 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 90。
[203] Prof. Dr. Arndt Sinn，譯者黃則儒，新的秘密偵查措施-來源端通訊監察及線上搜索，檢察新論，第 27 期，2020 年 2 月，頁 230。
[204]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研究所碩士論文，2019 年，頁 70。
[205]同上註，頁 70。

doi:10.6342/NTU202301879

馬），與同法第 100a 條規定之植入木馬（俗稱小木馬）誠屬不同，在德國法制上有明確之區分。以秘密且科技方法入侵，以此方式取得加密的「進行中之通訊資料」，此種偵查手段規定在刑事訴訟法第 100a 條第 1 項第 2 句之「來源端通信監察」(Quellen-TKÜ)；若國家係以上開科技手段取得已儲存、之前加密傳輸之通信內容及狀態，則規定在刑事訴訟法第 100a 條第 1 項第 3 句之「小型線上搜索」(時間和內容均受到限制之線上搜索)；而第 100b 條之線上搜索，則係授權德國執法機關得以在受干預人不知情之狀況下，合法使用科技方法入侵受干預人使用之資訊科技系統(即植入木馬程式之方式)取得資料。

從德國刑事訴訟法關於 100a 條第 2 句及第 3 句之「來源端通信監察及」以及「線上搜索」之明確區分，大木馬與小木馬共通之處包括「以植入木馬方式干預」、「秘密偵查手段」以及「必須是一般電信監察沒有預期效果（以其他偵查方法調查案件事實或偵查被告住居所，實屬困難或根本毫無希望）時，才能採用」[206]。而兩者最大之差異在於取得之資料性質及內容，依照刑事訴訟法第 100a 條立法理由所示，第 100a 條所創設之兩種干預手段，所提取的資訊並未超出那些傳統通訊監察途徑所可能調查的，故是將來源端通信監察定性為「一般」電信監察的補充規範，而第 100b 條之線上搜索，其取得之資料範圍則無設限，作為侵害性較高之偵查方式，於原則上允許偵查機關對於資訊科技系統之內部儲存資料進行全面性地取證作業[207]。根據德國文獻上的討論，線上搜索是秘密執行且持續性的取得個人資料，可能包含過去多年的資料，也可能涉及個人私密領域，取得後甚至可透過資料分析掌握個人使用行為，其干預強度遠超過傳統通訊監

[206] Prof. Dr. Mark A. Zöller，譯者王士帆，來源端電信監察與線上搜索-德國刑事追訴機關之新手段，司法新聲，第 130 期，頁 107-108，2019 年 4 月。
[207] 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研究所碩士論文，2019 年，頁 158

doi:10.6342/NTU202301879

察或搜索扣押[208]。

第二款 2017 修法前之法律爭議

德國在 2017 修法前，針對秘密線上搜索得否援引修法前之干預手段為之，實務裁判曾有一番變化。在 2006 年間聯邦最高法院裁定[209]認為，執法機關得援引刑事訴訟法第 102 條之搜索規定為秘密線上搜索之法律依據，裁定指出搜索之定義，係指偵查機關針對特定對象或一定處所，為尋找被藏匿物而具目標性之找尋行為，因此做為證據方法之資料，其是否以傳統有體物形式存在均非所問，且偵查法官指出，秘密線上搜索並無違反刑事訴訟法第 102 條之規定，搜索本得依其性質、目的、基本權干預程度，不必然毫無例外的公開進行，裁定最後做出「搜索得於受搜索人不知情之狀況下秘密進行，且執法人員也未必要在搜索處所親自實施」之結論[210]。然而，上開裁定出爐後，德國聯邦最高法院旋於同年 11 月又出現另一截然不同見解[211]，認為「搜索行為必須公開進行，且依刑事訴訟法第 106 條第 1 項第 1 句之規定，可知搜索處所居住人即客體持有人擁有在場權，不應將搜索視為不需在場之強制處分」，因而做成「因德國刑事訴訟法當時並未明文授權偵查機關進行秘密線上搜索，不得類推適用搜索之規定，否則無異架空強制處分需遵守法律保留原則之憲法誡命要求」[212]。

之後，德國聯邦檢察總長又嘗試以包裹聲請之方式，一次援引不同之干預手段為依據，請求法院核准此種複合式之干預處分[213]，德國聯邦最高

---

[208] 吳俊毅，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的困境，刑事政策與犯罪研究論文集（23），法務部司法官學院，2020 年，頁 479。

[209] BGH, Beschluss vom 21.02.2006.

[210] 何賴傑，論德國刑事訴訟程序「線上搜索」與涉及電子郵件之刑事處分，月旦法學雜誌，第 208 期，2012 年 9 月，頁 235。

[211] BGH, Beschluss vom 25. 11. 2006.

[212] 何賴傑，論德國刑事訴訟程序「線上搜索」與涉及電子郵件之刑事處分，月旦法學雜誌，第 208 期，2012 年 9 月，頁 236。

[213] 案例事實：聯邦檢察總長以偵辦被告涉嫌成立恐怖組織及其他罪名進行偵查程序，援引刑事訴訟法第 102 條、105 條第 1 項、第 94 條、第 98 條、第 169 條第 1 項第 2 具，請求法院准許對被告使用之個人電腦/筆電儲存之資料進行搜索扣押，且聲請許可偵查機關得以秘密執行此措施，得

doi:10.6342/NTU202301879

法院 BGHSt 51, 211 對此做成裁判，自此確定秘密線上搜索不得援引德國刑事訴訟法第 102 條搜索之規定作為依據，也不得使用結合多種干預授權要件之方式，秘密線上搜索缺乏法律授權依據不得為之[214]，法院提示「基於創設一個新新偵查手段之法律授權依據，而合併多個不同干預授權依據之要件是不合法的，此種方式將牴觸干預基本權之法律保留原則[215]」。聯邦最高法院 BGHSt 51, 211 之見解嗣後在德國學界獲得支持[216]，也進而催生嗣後 2017 年刑事訴訟法第 100b 條線上搜索之立法。

早於刑事訴訟法，德國聯邦刑事警察局與聯邦及各邦刑事事件合作法自 2008 年底即針對預防恐怖主義危險定有線上搜索之規定，之後的德國聯邦憲法法院[217]裁判，針對聯邦刑事警察局法之秘密干預手段進行審查，裁判明確揭示「為了預防國際恐怖主義之危險，授權聯邦刑事警察局使用秘密監控措施（住宅監聽、線上搜索、電信監察、電信資料調取以及使用特殊資料取得手段之住宅外監控），原則上與基本法之基本權規定相符」之意旨，此裁判也促使德國聯邦刑事警察局法有關線上搜索相關規定之重新修正，新法以秘密干預資訊科技系統作為危險預防性線上搜索之法律依據，並於 2018 年 5 月 25 日施行[218]。

第三款 刑事訴訟法第 100b 條線上搜索

第一目 聲請要件

2017 年德國刑事訴訟法新增之線上搜索規定，其一般性實體要件規定

對被告傳輸、安裝為此設計之電腦程式，以複製其放置在電腦儲存媒體之檔案，並將之傳送給偵查機關檢視。案例事實參王士帆，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，司法週刊，第 1779 期，2015 年 12 月，頁 2-3。

[214] BGHSt 51, 211, 218 F. Rn. 22.

[215] 陳俞伶，網路搜索之法規範研究-以雲端硬碟搜索及線上搜索為核心，國立清華大學科技法律研究所碩士論文，2018 年 7 月，頁 124。

[216]何賴傑，論德國刑事訴訟程序「線上搜索」與涉及電子郵件之刑事處分，月旦法學雜誌，第 208 期，2012 年 9 月，頁 238。

[217] BVerfGE 141, 220.

[218] 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 102。

doi:10.6342/NTU202301879

在第 100b 條，程序規範部分則分為第 100d 條之「私人生活核心領域及拒絕證言權人禁止干預」規定以及第 100e 條之一般執行程序規範。依照第 100b 條第 1 項規定「有下列情形時，即使受干預人不知情，仍得以科技方法侵入資訊科技系統，並得由該系統取得資料：(1) 有事實懷疑成立第 2 項所稱嚴重犯罪之正犯、共犯或未遂犯；(2) 個案中犯罪情節重大，並且 (3) 以其他方法調查犯罪事實或探查被告所在地顯有困難或預期無結果[219]」。

線上搜索規定如同德國法上其他重大干預基本權之強制處分，要件上採取「列舉重罪原則」及「補充性原則」。另有鑑於現今時代人們對於行動裝置之高度依賴性，立法者評價線上搜索對相對人之基本權干預強度，與德國刑事訴訟法上基本權干預程度最高之住宅監聽（即大監聽）相當[220]，從而，相對於傳統搜索而言，線上搜索僅係補充性地位，且必須是符合最後手段之要件時才能使用[221]。是以，列舉重罪部分，本條列舉之重罪採取與住宅監聽相當之「特別重大犯罪」，門檻相較於 100a 條更高，「特別重大犯罪」依聯邦憲法法院之標準，特別重大犯罪是指最重本刑 5 年以上之罪[222]，而立法者考慮到線上搜索之干預強度與住宅監察可以比擬，第 100c 條第 2 項住宅內監聽之列舉重罪也成為線上搜索之列舉重罪[223]。所謂補充性條款係指僅有在「以其他方法調查犯罪事實或探查被告所在地顯有困難或預期無結果」時，始能發動線上搜索，此點亦為比例原則之具體展現[224]。

---

[219] 同上註，頁 99。

[220] 林鈺雄，科技偵查概論：干預屬性及授權基礎(下)，《月旦法學教室》，第 221 期，2021 年 3 月，頁 51；施育傑，數位、科技與刑事程序干預處分-資訊框架理論之建構，2020 年政治大學法律學系博士論文，181 至 184 頁；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 12 月，頁 198 至 215。

[221] 吳俊毅，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的困境，刑事政策與犯罪研究論文集（23），法務部司法官學院，2020 年,頁 472。

[222] BVerfG, Urt. V. 03.03.2004-1 BvR 2378/97, 1084/99, Rn. 235, 238, 241.

[223] Prof. Dr. Arndt Sinn，譯者黃則儒，新的秘密偵查措施-來源端通訊監察及線上搜索，檢察新論，第 27 期，2020 年 2 月，頁 232。

[224] 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 103。

doi:10.6342/NTU202301879

第二目　受干預人

依同條第 3 項之規定，線上搜索之受干預人，原則上僅限被告，對於第三人之資訊系統進行干預，僅限被告使用他人之資訊科技系統、或是存在發現真實或調查被告所在地必要性、或無可避免地必然會干預到他人之資訊科技系統時[225]，亦即「如果僅以入侵被告資訊系統，無法發現真實或調查共同被告所在地時，偵查機關得例外性地對於他人所有之資訊科技系統進行線上搜索之干預」，而第三人線上搜索補充性原則之必要性審查，必須限縮於針對被告為線上搜索不足以就刑事追訴所必要之真實發現或所在地查明，而必須針對第三人進行線上搜索之干預之要件為釐清[226]。

分析本條線上搜索之要件，係以第 100b 條第 2 項之法定重罪作為干預門檻，明定線上搜索之受干預人，必須根據一定事實為基礎足以釋明受干預人事實上有參與犯罪，且嫌疑重大，並符合最後手段性。而當偵查機關認定被告使用第三人所有之資訊科技系統設備時，則可依照第 100b 條第 3 項第 2 句之規定提出線上搜索令狀之聲請[227]。至於「無可避免地必然會干預到他人之資訊科技系統時」，解釋上德國法容許搜索牽連到未提供資訊科技系統給被告使用之無關第三人，此種情形包含：第三人使用被告資訊科技系統、與被告在網路上有互動，偵查機關於此情形依本條規定得存取無犯罪嫌疑之第三人之資訊[228]。

第三目　干預方式

執行線上搜索之科技方式，德國刑事訴訟法係使用「資訊科技系統」

[225] 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研究所碩士論文，2019 年，頁 164；張麗卿，監察網路通訊作為抗制犯罪手段之原則及界線，輔仁法學，第 57 期，2019 年 6 月，頁 177-178。

[226]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研究所碩士論文，2019 年，頁 205。

[227] 同上註，頁 202-203。

[228] 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 104。

doi:10.6342/NTU202301879

之一般性描述文字，以此方式刻意涵蓋現在以及未來可能發展出的設備[229]，而就其之存取範圍，本條並未針對資料性質、時間設限，亦包含舊的、在干預處分命令前所儲存之資料[230]。從條文文義為「由該系統取得資料」，本條僅授權偵查機關可以透過植入木馬之方式秘密取得受入侵資訊科技系統之資料，並不允許主動製造資料，亦即並未授權例如：秘密啟動麥克風、攝影機等功能蒐集資料，亦即只允許偵查機關被動探知訊息，不得主動開啟受干預系統之功能[231]。德國有學者主張「外部行為之偵查」，不管性質屬於音訊或影訊之偵查，均應予全面禁止，因認此種監察模式已非從資訊設備蒐集資料，而是利用資訊系統從事取證行為[232]。而本條並未授權偵查機關為了植入木馬而秘密進入他人住居，亦意味者偵查機關僅能透過遠端植入木馬或是過犯罪偵查詐術之方式植入木馬[233]。

第四目　程序規定

線上搜索僅可依檢察官聲請，由其所屬轄區邦地方法院為線上搜索及住宅監聽特別成立之三位合議庭法官核准為之，不得由單一偵查法官決定，線上搜索之核准法庭亦不可職司刑事審判程序[234]，避免法院在審判程序使用被告因被依法暫緩通知或免予通知而不知悉之監察資訊[235]。若有遲延即生危險之情形，得例外由線上搜索法庭之審判長單獨核准，然須於 3 日內經合議庭補正認可，否則即失其效力[236]。

---

[229] 同上註，頁 103。
[230] Prof. Dr. Arndt Sinn，譯者黃則儒，新的秘密偵查措施-來源端通訊監察及線上搜索，檢察新論，第 27 期，2020 年 2 月，頁 232。
[231]自王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 103。
[232]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研究所碩士論文，2019 年，頁 238。
[233] 張麗卿，監察網路通訊作為抗制犯罪手段之原則及界線，輔仁法學，第 57 期，2019 年 6 月，頁 176。
[234] §74a IV GVG.
[235] 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 12 月，頁 206。
[236] § 100e II S. 1-3 StPO.

doi:10.6342/NTU202301879

執行期間不得逾 1 個月[237]，自線上搜索核准之日起算，而非執行監察之日起算[238]，線上搜索核准之要件依偵查結果認有繼續存在時，得延長之，每次得延長 1 個月，無執行總期限，另考量到線上搜索係屬基本權之重大干預，新法規定若執行期間已達 6 個月之聲請延長，應由高等法院內不職司審理刑事審判程序之法庭裁定之[239]。

特別程序規定部分，依第 100b 條第 4 項之規定，來源端通訊監察之技術擔保與書面記錄義務，於線上搜索準用之。而線上搜索之技術性擔保，應確保：對於個人資訊科技系統，只可進行為取得資料所必須之變更；執行搜索結束時，技術上應盡可能使所進行之變更自動回復；所採用之方法應依科技狀態防止他人無權使用；所複製之資料應依科技狀態保護免於變更、無權刪除或無權知悉。若技術上無法做到上開擔保，則不得使用否則將構成違法線上搜索[240]。

第五目　取證限制

德國法刑事干預處分向來定有針對「私人生活核心領域」以及「拒絕證言權人」取證之特別限制，依第 100d 條第 1 項之規定，「有事實根據認為線上搜索只會取得出自私人生活核心領域之資訊時，不得進行線上搜索」，而由線上搜索取得之「私人生活核心領域資訊」，不得作為證據使用，法定絕對證據使用禁止之規定[241]。依第 100d 條第 2 項、第 3 項之規定，執行過程取得此核心領域資訊應立即刪除，並以書面紀錄，或交由檢察官送交核准法院決定資料之證據使用能力與刪除，法官關於證據能力之裁判對

[237] § 100e II S. 4-6 StPO.
[238]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 12 月，頁 206。
[239]同上註，頁 207。
[240]王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 104。
[241] 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 12 月，頁 208。

doi:10.6342/NTU202301879

後續程序具拘束力[242]。對於刑事訴訟法第 53 條規定享有拒絕證言權利之人（如神職人員、律師、公證人、國會議員和醫師等等），依法不得對其職業秘密所保護之談話或內容進行線上搜索，在線上搜索執行期間或執行後發覺有上開情形者，所取得之資訊，不得為證據，且應立即刪除並以書面記錄[243]。對於因親屬關係或職業輔助人而有拒絕證言權之人，在不涉及私人生活核心領域前提下，考量信賴關係之重要性與調查案情或探查被告所在地之追訴利益未失均衡，始得為證據使用，屬於法定相對證據使用禁止之規範[244]。然而，當有一定事實懷疑上開具有拒絕證言權身分之人有參與犯罪或資訊贓物罪、包庇犯罪利益、妨礙司法或贓物罪時，則失去線上搜索取證禁止與證據使用禁止之保護[245]

第四項　立法過程

2016 年末由北萊茵威斯特法倫邦社會民主黨（SPD）議員 Thomas Kutschaty 以及巴伐利亞邦基督教社會聯盟（CSU）議員 Winfried Bausback 所領導做出之「德國刑事程序增進效率並契合實務擴張法案草案」，請求德國國會針對刑事程序進行改革之立法行動，原提出之 22 點修正建議[246]，實際上並未包含線上搜索[247]。然而法案審議過程驟然發生變化，由聯盟黨（CDU/CSU）議員 Patrick Senburg 建議納入過去聯邦司法與消費者保護部部長 Heiko Mass 於 2014 年至 2015 年間曾提出之來源端通訊監察草案建議，至第二讀會暨第三讀會之前，德國國會司法與消費者保護委員會突然決議希望加入「線上搜索及來源端通訊監察」制度於「德國刑事程序增

[242] 同上註，頁 209。
[243] § 100d V S. 1 StPO.
[244] 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 12 月，頁 209。
[245]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 12 月，頁 209。
[246]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研究所碩士論文，2019 年，頁 98
[247]同上註，頁 98

doi:10.6342/NTU202301879

進效率並契合實務擴張法案草案」中[248]，隨即把來源端通訊監察及線上搜索納入本法案草案，之後在第二讀會及第三讀會通過，於 2017 年 8 月 24 日正式施行[249]。

德國有學者認為上開立法過程具有嚴重爭議，連立法程序也有些奇怪。理由包含上開兩種干預措施並未出現在原始的立法草案，是直到德國聯邦國會的法律暨消費者保護委員會才「偷渡」到立法程序，且認為此次立法雖有複雜的技術基礎和重大的法治國疑慮，卻沒有進行專家公聽會，反而在德國聯邦國會改選前一刻才進入立法程序[250]，上開倉促且具爭議之立法過程，導致後來依據德國聯邦憲法法院之公告，直至 2019 年 8 月為止，已有 5 件針對本法案所提出之違憲聲請案[251]，且縱使立法已經通過，於德國國會仍存在著許多質疑的聲音[252]。

第四節　荷蘭

第一項　早年立法-2002 年情報安全法

荷蘭很早即有國家木馬以及技術協助通知之相關法律。2002 年情報安全法（Intelligence and Security Services Act 2002 ）第 24 條、第 25 條授權荷蘭情報單位以侵入自動化設備之方式進行通訊內容之監察，例如：引入技術設備解密儲存或持有於自動化設備中之加密訊息[253]。同法亦有關於技術協助之規範，授權情報單位得以書面之方式，要求任何對於上開儲存於自動化設備之加密訊息，具有解密知識之人，提供解密所需之所有合作

[248]同上註，頁 99
[249]同上註，頁 98-100
[250] Prof. Dr. Mark A. Zöller，譯者王士帆，來源端電信監察與線上搜索-德國刑事追訴機關之新手段，司法新聲，第 130 期，頁 107，2019 年 4 月。
[251] 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，國立成功大學碩士論文，2019 年，頁 100。
[252]同上註。
[253] Intelligence and Security Services Act 2002, arts. 24–25 (Neth.), at https://fas.org/irp/world/netherlands /intel-act-2002.doc (unofficial English translation), last visited 06/30/2023.

doi:10.6342/NTU202301879

[254]。荷蘭的刑事訴訟法也有類似的規定，對於涉及恐怖主義等嚴重犯罪的案件，檢察官得合理假設某人知道通信加密方式，並要求其提供知識或協助解密[255]。

第二項 2018 年第三部電腦犯罪法(Computer Crime Act 2018 III)

2015 年 11 月巴黎恐怖攻擊事件以後，荷蘭眾議院要求內閣政府進行解密相關立法之修正，荷蘭司法安全部長及經濟部長共同於 2016 年 1 月 4 日提出 1 份關於解密之評估報告[256]，此份評估聲明中指出加密技術保護了國人為政府蒐集之個人資訊、政治及軍事通訊安全，更保障個人隱私權，就經濟發展部分加密技術之使用足以增強荷蘭之國際競爭地位，為新創企業、數據中心和雲計算等有吸引力的商業及創新氛圍做出貢獻，對於荷蘭安全通信和數據儲存之信心，以及荷蘭數字經濟未來增長潛力至關重要[257]。聲明中針對加密技術對於執法之阻礙表示：加密技術確實造成即時取得有助於保護國家安全及犯罪偵查之訊息，變得複雜、延遲甚至不可能，因而現在已無其他選擇授權執法機關對於技術之使用權，在不使加密技術同時易遭罪犯、恐怖分子和外國情報機構攻擊的情況下。進行執法，結論上採取荷蘭不針對加密技術之發展性、可用性或使用上立法限制之基本立場[258]。

---

[254] *See id*. arts. 24(3), 25(7).

[255] Wetboek van Strafvordering (Code of Criminal Procedure), § 126m (6) (Neth. 2012), at http:// www.ejtn.eu /PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf (un official English translation), last visited 06/30/2023.

[256] Letter from G.A. Van der Steur, Minister of Security and Justice, and H.G.J. Kamp, *Minister of Economic Affairs, to the President of the House of Representatives of the States General rega rding the Cabinet's View on Encryptio*n, No. 708641 (Jan. 4, 2016) (English translation), https:// www.enisa.europa.eu/about-enisa /structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on –encryption, last visited 06/30/2023.

[257] *Id*., 原文「Being able to use encryption strengthens the international competitive position of th e Netherlands and contributes to an attractive business and innovation climate for, for example, s tart-ups, data centres and cloud computing. ConfId.ence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy, which is mainly in the digit al economy.」

[258] *Id.*, 原文「The cabinet is therefore of the opinion that at this point in time it is not desirable

doi:10.6342/NTU202301879

在肯認加密技術發展重要性之同時，荷蘭針對制衡加密技術對執法之衝擊，在 2018 年 9 月 21 日公布第三部電腦犯罪法（Computer Crime Act 2018III ），該法於 2019 年 3 月 1 日生效，本法旨在提高解決網路犯罪偵查之效率，除修訂了荷蘭刑法（Dutch Criminal Code ，簡稱 DCrC）內有關網路犯罪之規定，亦針對解密對執法造成之阻礙，於刑事訴訟法（Code of criminal Procedure，簡稱 DCCrP）增訂「解密令狀」、「國家木馬（Hacking Power）」及「下架（刪除移轉）權（The Power to Make Content Inaccessible）」。

1. 解密令狀（刑事訴訟法第 125k 條）

第三部電腦犯罪法修訂了刑事訴訟法第 125k 條，授權執法機關可以解密令狀，要求相對人提出解密金鑰或解密後的資料[259]。解密令狀只可針對擁有加密技術之法人為之，犯罪嫌疑人本身基於不自證己罪原則，不得為解密令狀之相對人，新法並無針對解密令狀創設新的程序保障規範，而僅適用原有刑事訴訟法一般程序保障規定[260]。

2. 國家木馬（刑事訴訟法第 126nba、126uba 及 126zba 條）

第三部電腦犯罪法修訂了刑事訴訟法第 126nba、126uba 及 126zba 條[261]有關國家木馬之授權規定。該法授權執法機關基於調查嚴重犯罪之目的，可以合法透過遠端植入木馬之方式截取加密資訊，透過設備或相互連接之系統，以程式對犯罪嫌疑使用中之電腦數據（如電腦、手機、伺服器等）進行自動化處理。立法者認為合法木馬技術授權，係解決科技發展以及電腦設備、系統廣泛用於通訊及數據儲存所帶來之挑戰必要之條件，程序要件包含：（1）限於最輕本刑 8 年以上有期徒刑或法律列舉重罪，列舉重罪

to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands.」

259 Wetboek van Strafvordering (Code of Criminal Procedure), Section 125k.

260 Thiago Moraes, *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures*, 6 EUR. DATA PROT. L. REV. 41 (2020). 52.

261 Wetboek van Strafvordering (Code of Criminal Procedure), Sections 126nba, 126uba 126zba

doi:10.6342/NTU202301879

包含：兒童及少年性剝削(Section 240b DCrC)、誘拐（Section 248e DCrC)、招募參與恐怖組織(Sections 131 and 205 DCrC)、組織犯罪（Section 140 DCrC)、詐欺及洗錢(Section 420bis DCrC)等、(2）國家木馬對於犯罪之偵查有必要性及急迫性[262]、(3）僅能針對單一、特定干預對象為之、(4）期限以 4 週為限，得延長 1 次[263]、(5）法官事前令狀授權，急迫情況可取得司法官口頭同意並於 3 天內補正書面令狀[264]。

依照第三部電腦犯罪法解釋性備忘錄所載，核准國家木馬時必須通過比例原則及輔助性原則之測試[265]。以木馬手段干預之標的限於現有特殊偵查之相同客體，例如舊法規定針對特定使用者身分、系統監視等監察手段，新法施行後則可以打開麥克風、鏡頭等方式為之；舊法針對監聽通訊內容、搜索電腦系統內電磁紀錄之權利，新法施行後可以此方式取得可理解形式（非加密）之內容。刑事訴訟法第 126nba(1)條明定執法人員以國家木馬執行之目的包括(1)確認電腦或使用者之特徵(尤其為使用者身分)、(2)記錄秘密通訊過程（攔截電子通訊和口頭通訊)、(3)進行系統性遠距觀察、(4)在令狀授權期限內確保資料（包含已儲存在電腦內和遠距入侵後增加之電腦資料)、(5)下架資料（刪除非法資料，通常為複製資料作為證據之後）[266]。

荷蘭是少數針對「設備位置所在地不明」情形涉有管轄特別規定之國家，荷蘭允許針對刻意隱匿而使所在位置不明之設備植入木馬，且規定於執行後若發現設備所在地屬其他國家司法管轄，後續執行應透過司法互助方式為之，然而若向該國提出司法互助請求，然他國並未回復，荷蘭警方

[262] *See id.* art. 126nba (1).
[263] *See id.* art., 126nba (3).
[264] *See id.* art, 126nba (4), (5).
[265] *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices Study*, European Parliament, May 2017, p.94.
[266] 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 57。

doi:10.6342/NTU202301879

則仍可繼續執行[267]。

程序保障部分，立法者針對國家木馬之授權，特別增訂調查期間所有登入紀錄必須留存[268]，紀錄調查過程，但此登入紀錄不會併入案件資料內，被告若欲檢視須另外提出請求。另外其他程序保障規範包含（1）提出年度報告，針對國家木馬提出使用統計數據，相關資料必須在資料取得 2 年後納入統計、（2）偵查結束後木馬程式原則上須完全移除，但若具困難性或危險性不在此限，然應通知該電腦之行政管理者[269]、（3）除非危急調查，原則上事後應通知受干預對象之義務[270]。國家木馬之執行受到荷蘭公共秩序和安全檢查局（Public Order and Safety Inspectorate ）之監督[271]，其木馬程式應符合一定技術要求，且技術與調查人員分離，由專門技術人員負責執行，另由調查案件之人員進行蒐集資料之分析[272]。若是使用零日攻擊之木馬程式，取得特別授權後可延遲向廠商揭露此項系統漏洞[273]。

3. 下架（刪除移除）權（刑法第 54a 條、刑事訴訟法 125p 條）

另外，第三部電腦犯罪法修正刑法第 54a 條有關電信服務公司之相關規範，增訂政府命電信服務商使數據不可訪問「inaccessible」之權利。針對其性質屬於非法、犯罪之訊息內容，修法前都是仰賴通信服務商以自願通知並刪除的方式處理，第三部電腦犯罪法修正刑事訴訟法第 125p 節，授權檢察官可命令通信服務商使數據「不可訪問」。上開命令僅可針對嫌犯為警拘留之案件，檢察官須書面記載犯罪行為、聲請不可訪問之數據以及前開數據對於結束刑事犯罪或防止新犯罪係屬必要向法官事前

[267] Gemma Davies, *Shining a Light on Policing of the Dark Web : An Analysis of UK Investigatory Powers*, Journal of Criminal Law 84 (407), Oct. 2020, p.19
[268] Wetboek van Strafvordering (Code of Criminal Procedure*),* Section 126ee.
[269] *See id.* art. 126nba (6).
[270] *See id.* art 126bb.
[271] *See id.* art. 126nba (7).
[272] 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 59。
[273] *See id.* art. 126ffa (3).

doi:10.6342/NTU202301879

聲請[274]，令狀相對人有聽證權，並於聽證期間獲得法律協助之權利[275]。

第五節　澳洲

第一項　早年立法

澳洲很早就立法授權國家木馬之國家，有異於其他國家以專法之方式規範國家木馬，澳洲之國家木馬的法令授權散落於諸多不同法令中。其立法規範大致可區分為：基於執法目的之國家木馬，規定在 1979 年的電信（協助和訪問）法（the Telecommunications【Assistance and Access】Act of 1979，簡稱 TIA Act），基於國安目的之國家木馬規定在 1979 年澳洲安全情報組織法（the Australian Security Intelligence Organization Act of 1979 ，簡稱 ASIO Act）。

澳洲安全情報組織法 Sec. 25A[276]係澳洲最早關於國家木馬之法律授權，當時此權力專屬於澳洲特勤局，授權其基於國安之目的，取得令狀後為之，當時的法律用語雖無「駭客（Hacking）」一詞，但因該法授權監察之客體為「對於電腦…電腦系統…電腦網路或任何上述軟硬體之綜合」等，使澳洲政府開發一系列針對性系統[277]。1999 年澳洲安全情報組織立法修正案，明確立法授權政府基於國安情報之目的使用國家木馬[278]，同法於 2014 年進行修正，擴大國家木馬之使用範圍[279]，2016 年澳州總理曾表示「澳洲

[274] *See id.* Section 125p.
[275] *See id.* Section 125p (4).
[276] Australian Security Intelligence Organisation Act 1979 (Cth) s 25A (Austl.).
[277] Carlos Liguori, *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*, 26 MICH., TELECOMM. & TECH. L. REV. 317 (2020), 340.
[278] Australian Security Intelligence Organisation Legislation Amendment Act 1999 (No. 161), Parliament of Australia, available at http://www.austlii.edu.au/au/legis/cth/num_act/asiolaa1999664/sch1.html (last visited August 2, 2016), amending the Australian Security Intelligence Organisation Act 1979 § 25A, Parliament of Australia, available at http://www. austlii.edu.au/au/legis/cth/consol_act/asioa1979472/s25a.html, last visited 06/30/2023.
[279] National Security Legislation Amendment Bill (No. 1) 2014, Parliament of Australia, at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query%3DId.%3A%22legislation%2Fbillhome%2Fs969%22;rec=0 last visited 06/30/2023.

doi:10.6342/NTU202301879

政府的駭客攻擊能力，非常強大」[280]。至於基於執法目的之國家木馬，係規定在電信（協助和訪問）法，因法條用語概括，早已足以概括竊聽（wiretapping）以外之截取方式。

第二項　2018 年電信和其他法律修正（協助和訪問）法

澳洲在 2018 年大規模修正電信和其他法律修正（協助和訪問）法（Telecommunications and Other Legislation Amendment 【Assistance and Access)】Act 2018，簡稱 TOLA Act）[281]，本法於 2018 年 12 月 8 日經澳洲國會修正通過，旨在大規模擴張澳洲政府基於執法、國安目的用以對抗加密技術之手段，授權政府接觸包含通訊內容、電腦資料在內加密電磁紀錄，故又稱為反加密法案。修正重點包括該法授權澳洲執法機關、情報機關可以要求、強制通訊服務商提供技術協助或以令狀之方式獲取資料，相較於 1979 年電信（協助和訪問）法以及 1997 年電信法僅適用於澳洲境內擁有或經營通訊基礎設施的傳統業者及服務提供者，TOLA ACT 將其規範主體擴張至「指定通信服務商」（Designated communications providers，DCPs），亦即不僅傳統之電信公司，包含設備、應用程式之服務商等，將通訊產業鏈上的所有業者都包含在內[282]。

TOLA ACT 大規模修正包含「1997 年電信法」、「1979 年電信（攔截和訪問）法」、「2004 年《監視設備法》」、「1914 年犯罪法」、「1987 年刑事事項互助法」、「1979 年澳大利亞安全情報組織法案」、「1901 年海關法」等多部內國法，作為澳洲面對加密技術所帶來之挑戰之應對措施[283]，其內

[280] *Australia Admits Government Hack Attacks*, Boosts Cyber Security, PhysOrg, Apr. 21, 2016, at http://phys.org/news/2016-04- australia-hack-boosts-cyber.html.

[281] Telecommunications and Other Legislation Amendment *(*Assistance and Access*)* Act *2018* (Cth) (Austl.).

[282] 陳芊儒，通訊軟體加密下個人隱私與國家安全保護之平衡，科技法律透析，2019 年 9 月，第 31 卷第 9 期，21 頁。

[283] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (TO LA Bill), Explanatory Memorandum, p. 2.

doi:10.6342/NTU202301879

容包含 5 個 Schedule。Schedule 1 創設一系列要求通信服務商提供協助之請求，賦予國家合法請求或強制向安全機構提供技術協助之權力。Schedule 2 賦予聯邦、州及國土法之執法機關得以透過取得電腦訪問令狀（The Computer Access Warrant 【CAW】）秘密執行線上搜索[284]。Schedule 3 和 4 修正《犯罪法》和《海關法》下的搜索令之框架，擴大執法機構從電子設備蒐集證據的能力[285]。Schedule 5 賦予自願向澳洲情報安全組織（Australian Security Intelligence Organisation，簡稱 ASIO） 提供協助者之民事豁免權。並賦予澳洲情報安全組織一項新的權力，授權澳洲情報安全組織可以強制特定對象提供電腦設備上保存之數據[286]。

第一款 Schedule 1 通信服務商協助義務

TOLA ACT 的 Schedule 1 通信服務商協助請求之架構，係修正澳洲「1997 年電信法」中有關電信業提供政府合理必要協助之規範架構。Schedule 1 通信服務商協助義務人之範圍，包含「電信業者」(carrier)、「服務提供者」(carriage service provider)以及任何所製造、生產或提供之服務為終端使用者使用之企業[287]，並統稱為指定通信服務商(Designated Communications Providers Etc., DCPs)，其範圍幾乎涵蓋了電訊供應鏈之所有業者及人員。凡提供澳洲境內人員服務或產品之通信服務商，縱使未在澳洲設立營業處所，均有適用[288]。

TOLA ACT 在立法方式上，兼採鼓勵與強制通信服務商配合雙管齊下之方式，創設以下三種干預手段[289]：

1. 技術協助請求（Technical Assistance Request，簡稱 TAR）

[284] *See id*. at 4.
[285] *See id* at 5.
[286] *See id* at 6.
[287] Sec. 317C of the Telecommunications Act 1997.
[288] 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 66。
[289] Sec. 317A of the Telecommunications Act 1997.

doi:10.6342/NTU202301879

澳洲安全情報組織、澳洲情報局及澳洲信號及攔截機構，基於國家安全、外交利益、國家經濟福祉、刑事重罪(最輕本刑 3 年以上之罪)或涉外犯罪之偵查及執行，依法可要求科技公司提供自願性的協助，(例如：協助解密、提供技術及存取權限等)。因技術協助請求本質上為對通信服務商提出自願協助請求，故程序上無須外部授權[290]，僅須於發出 7 日內應通知情報和安全總檢查長(Inspector-General of Intelligence and Security)[291]或州、領地負責檢查系爭事務之檢查機構。另外，澳洲內政部針對技術協助請求之使用情形應製作年度報告詳盡報告技術協助請求使用情形統計數據並予以公開[292]。然而，澳洲安全情報局、澳洲秘密情報局及澳洲國防情報局相關技術協助請求之年報為獨立製作，且不對外公開[293]。

2. 技術協助通知（A Technical Assistance Notice，簡稱 TAN）

技術協助通知是具有強制力的協助要求，用於相對人已有特定科技技術，足使執法人員得以取得解密訊息，強制通信服務商在其能力可做到的範圍提供合理、合乎比例原則及可執行之技術協助。TAN 發出之主體為澳洲安全情報組織、澳洲情報局及澳洲信號及攔截機構機關之機關首長（Chief Officers）或其指定之人[294]，基於國家安全或執行刑事重罪或涉外犯罪之目的，違反即有法律制裁。州警發出技術協助通知前必須取得聯邦警察 Australian Federal Police（AFP)專員之同意。一旦發出技術協助

[290] Parliamentary Joint Committee on Intelligence and Security, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, (2021 DEC.), at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf, p.90, last visited 07/04/2023.

[291] Telecommunications and Other Legislation Amendments (Assistance and Access) Act 2018 (TOLA Act), s. 317HAB.

[292] TOLA Act, s. 317Zs. See also Department of Home Affairs, Telecommunications (Interception and Access) Act 1979 Annual Report 2018-2019.

[293] Australian Security Intelligence Organisation Act 1979 (ASIO Act), s. 94 (2BA).

[294] The definition of 'chief officer' is set out in s. 317ZM of the TOLA Act as the Commissioner of the AFP, the Chief Executive Officer of the Australian Crime Commission, and the Commissioner of Police (however designated) of the relevant State or Territory.

doi:10.6342/NTU202301879

通知，澳洲安全情報組織（ASIO）總監或機關首長應於 7 日內通知相關監督機關[295]，澳洲國防情報局（Australian Signals Directorate）以及澳洲秘密情報局（Australian Secret Intelligence Service，簡稱 ASIS，為澳洲外國情報蒐集機構）並無發出技術協助通知及技術能力通知之權力。

3. 技術能力通知（Technical Capability Notice，簡稱 TCN）

技術能力通知用於要求科技公司在產品或服務中加入新功能，使政府取得通訊內容「Introduce weakness to one target those are confect to particular person」，此權力專屬於司法部長（Attorney-General），澳洲安全情報組織總監（Director-General of Security）或攔截機構之機關首長基於國家安全及執行刑事重罪或涉外犯罪等目的得請求司法部長簽發技術能力通知[296]，然技術能力通知僅有在通信主管機關首長同意下始發生效力[297]，澳洲內政部稱此為三道鎖之機制（triple-lock mechanism[298]）。技術協助通知及技術能力通知均無司法審查權之設計[299]。

技術能力通知不可要求系統商建造或提供系統性弱點（systemic weakness）或系統性漏洞（systemic vulnerability）[300]，而所謂系統性弱點或系統性漏洞並不包括引入特定人相關系統或設備之「目標技術（target technologies）」，而此「人」之身分可否特定亦在所不論[301]。依據澳洲內政部向澳洲議會情報與安全聯合委員會提出之意見書，針對「目標技術（target technologies）」之定義為細部之說明，目標技術所針對之弱點（weakness）

---

[295] TOLA Act, s. 317MAB

[296] *See id*. s. 317T(1)、(2)、(3)

[297] *See id*. s. 317TAAA.

[298] Parliamentary Joint Committee on Intelligence and Security，Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018，(2021 DEC.), at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf, p.91.

[299] *See id*.

[300] TOLA Act, s. 317ZG.

[301] *See id*. s. 317B.

doi:10.6342/NTU202301879

跟漏洞（vulnerability）僅能針對特定人使用之設備或是與特定對象牽涉之相關技術為限[302]，例如：由犯罪者操作或涉嫌犯罪的單一設備，被歸類為目標技術定義的(e) 段，反之，若是特定型號的手機、電子設備，或與特定人員無關的任何設備，將太寬泛而不能落入「目標技術」之定義範圍，此種方式將確保了干預對象以外者所享有之加密服務且不受影響，也反應國家依法取得個人資訊時合法令狀或授權之必要性[303]。

技術能力通知之核發應符合必要性、合理性及比例原則之外，尚須符合切實可行（practicable）及技術可達(technically feasible)之要求，依照澳洲內政部之說明，切實可行（practicable）及技術可達(technically feasible)在發出技術協助請求及技術協助通知之場合，是指業者現有能力之運用範圍內，但在技術能力通知之場合，係指新能力之開發係屬業者能力所及。相反的，如果若是對於要採取何種技術程序才能達到執法機關需求目的無法清楚說明，或者根本不存在可達到執法機關需求目的之技術，則不符合切實可行（practicable）及技術可達(technically feasible)。技術可行性之檢視同樣受到法律規範之限制，例如：若技術上可取得對象目標點對點通訊之加密資訊，但技術上卻造成非對象目標之訊息亦遭政府取得之重大風險，在法律概念之下即非屬技術可行，因為將違反法律所禁止之系統性風險[304]。

本法規定政府發出技術協助通知及技術能力通知前，必須先行諮詢通信服務商。此外，通信服務商可針對技術能力通知以書面方式向司法部長提出評估結果，司法部長收到通信服務商之評估結果後，應任命 2 位評估員（assessor），其中一名必須具備技術知識來確定系爭能力通知是否有建立系統性弱點之潛在風險，以及有無適當層級之安全許可，另一位評估員

[302] Department of Home Affairs, Supplementary Submission 16.2, p. 9.
[303] Department of Home Affairs, Submission 16, p. 18.
[304] Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997(Cth): Administrative guidance for agency engagement with designated communications providers*, Document <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrativeguidance.pdf>, p. 6, last visited 07/04/2023.

doi:10.6342/NTU202301879

必須曾任職高等法院、聯邦法院、最高法院州或領地的法院或領地地區法院法官至少 5 年且現已退休。評估員必須評估下列事項：(1) 技術能力通知與 Section 317ZG 法律規定是否相符。(2) 是否具合理性且符合比例原則。(3) 遵循技術能力通知是否切實可行。(4) 遵循技術能力通知是否技術可達。(5) 技術能力通知是否符合最後手段性以及可有效實現系爭合法目標[305]。

TOLA ACT 規定，通信服務商協助政府時可得到適當的經濟補償且免於特定民事責任，另針對爭議最大之後門問題，TOLA ACT 於第 317ZG 條第 1 項明文揭示技術協助通知及技術能力通知不包含賦予政府要求業者於加密裝置中導入後門之權利[306]。本法施行後，國安人員及司法人員依令狀攔截或擷取之電腦資料，執行時遇到加密或其他困難，即得選擇上開三種協助請求或通知，不需再向法院聲請令狀或其他司法許可[307]。

第二款 Schedule 2 電腦訪問令（Computer Access Warrant）

TOLA ACT 的 Schedule 2 為有關電腦訪問令（Computer Access Warrant）之規定，授權澳洲安全情報組織(Australian Security and Intelligence Organisation，又簡稱 ASIO)與執法機關（僅限調查最輕本刑 3 年以上重罪）可以取得電腦訪問令（Computer Access Warrant)，透過物理接觸或從遠端進入電腦取得所有設備內儲存之資訊[308]。執法機關須向法官或行政上訴法院（Administrative Appeals Tribunal）聲請[309]，澳洲安全情報組織則是向司法部長提出聲請[310]。

---

[305] *See id*.at 20.

[306] 陳芊儒，通訊軟體加密技術下個隱私與國家安全保護之平衡，科技法律透析，2019 年 9 月，第 31 卷第 9 期，頁 22。

[307] 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月，頁 52。

[308] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Explanatory Memorandum, p. 4.

[309] Surveillance Devices Act 2004, Part 2, Division 4.

[310] ASIO Act, s. 25A

doi:10.6342/NTU202301879

本法施行前，依照「2004 年《監視設備法》」，情報機關與執法機關雖擁有監視設備之權利，卻僅限於監視輸出及輸入之資訊，不包括儲存在裝置內之歷史資料，澳洲安全情報組織進入電腦端攔截訊息，必須分別取得攔截令(Interception Warrant)以及電腦訪問令（Computer Access Warrant）[311]。另外，修法前執法機關雖可透過取得延遲通知搜索令之方式進行秘密搜索，但執行方式僅限於實際接觸搜索場所，致使執法人員執行時增加額外風險，然而實際執行上要實際接觸搜索場所進行秘密搜索實屬困難，存有執法人員安全以及暴露偵查行動之諸多風險，舊法規定未能符合加密時代執法機關所需。

TOLA ACT 修正原有「1979 年澳大利亞安全情報組織法案」以及「2004 年監視設備法」之規定，擴大電腦訪問令（Computer Access Warrant）授權內容包含:執行令狀所需之對人、對物強制力[312]，例如：強制力安裝或移除電腦，或排除阻撓執行令狀之人[313]；於令狀授權之任何時間進入令狀授權場所[314]；以及在令狀期間至末日起算 28 日內進行隱藏訪問（Concealment of access），隱藏訪問之方式包含：秘密進入特定場所、使用其他電腦或遠端傳遞訊息、攔截傳輸中之訊息、或添加、複製、刪除或更改電腦內其他數據或傳輸中的通信[315]。針對遠端搜索必定會面臨的跨境問題，此次修法於 2004 年監視設備法中新增第 43A 條規定若電腦訪問令狀涉及遠端搜索外國或者是根據外國法律註冊並在澳洲領海領空外之船舶或飛機上之電

[311] Independent National Security Legislation Monitor (INSLM), *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters (TOLA Act Report)*, p. 80.

[312] Surveillance Devices Act 2004, s. 27 E(6)(a)

[313] Department of Home Affairs, Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers, Document, at https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrativeguidance.pdf, p. 57, last visited 07/01/2023.

[314] Surveillance Devices Act 2004, s. 27 E(6)(b)

[315] *See id.* s. 27 E(7)

doi:10.6342/NTU202301879

腦數據時，應取得外國有權同意電腦搜索官員之同意（appropriate consenting official[316]）否則不得核發或執行該令狀[317]。違反第 43A 條規定所取得之證據，無證據能力[318]。

TOLA ACT 之電腦訪問令（Computer Access Warrant）係屬澳洲因應加密通訊軟體之措施，授權範圍包含進入電腦攔截經過通訊系統之對話內容[319]，無庸再另外取得攔截令(Interception Warrant)，依其立法目的之說明，係有鑑於加密通訊軟體時代，通訊內容於傳輸過程中為加密狀態，但停留在裝置時一般非呈現加密狀態，電腦訪問令授權執法機關可以秘密進入設備取得未加密狀態之通訊內容。

Schedule 2 另外創設另一搭配電腦訪問令之協助通知，授權執法機關或情報單位可以要求特定人針對進入電腦、複製設備或將資料轉換為可理解形式之目的，對特定人提出提供訊息或協助之要求，程序上必須經由法官或或行政上訴法院成員同意下發出[320]。

執法機關取得電腦訪問令，無論該令狀是否執行，應於令狀停止後由機關首長儘速向上級陳報，針對有執行之電腦訪問令，陳報內容應包含細節資訊[321]，執法機關陳報細節內容應包括因而逮捕、起訴或使兒童獲得保護之相關數據[322]。澳洲聯邦監察使辦公室(Commonwealth Ombudsman)擁有監督電腦訪問令之執行之權利[323]，並與州監察機關所執行之調查相互合

[316] *See id.* s.41
[317] *See id.* s. 43(A)
[318] *See id*.s.43(B)
[319] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Sch. 2.
[320] Department of Home Affairs, Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers,Document, at https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrativeguidance.pdf, p. 56, last visited 07/01/2023.
[321] Surveillance Devices Act 2004, s. 49 (2B)
[322] *See id*. s. 50.
[323] *See id*. s. 55

doi:10.6342/NTU202301879

作[324]，執法機關執行隱匿訪問（concealment of access)監察活動，應向執行結束後 7 日內向澳洲聯邦監察使辦公室提出報告[325]。澳洲安全情報組織執行電腦訪問令之部分，則應向司法部長提出報告，報告內容應包括執行隱匿訪問、截取對話內容及移除設備之細節及效益以及任何有關嚴重干擾、中斷或妨礙他人合法技術使用之資訊[326]。

依照內政部每年提出之監控設備年報資料顯示，本法施行後，2018 年至 2019 年澳洲聯邦警察取得 16 張電腦訪問令、澳洲刑事情報委員會取得 1 張；2019 年至 2020 年澳洲聯邦警察取得 16 張電腦訪問令、澳洲刑事情報委員會取得 4 張[327]。

第三款　Schedule 3 及 4 搜索令架構之修正

TOLA ACT 第 3 及第 4 Schedule 則是為因應科技之發展，修正了澳洲「1914 年犯罪法」以及「1901 年海關法」有關執法機關以及澳洲邊防署(Australian Border Force)有關搜索令（search warrant）之架構以及協助命令（assistance orders）之規定。

Schedule 3 是有關執法機關部分，主要修正 5 個部分：１、引進「帳戶資料」(account-based data）概念，２、擴張執法單位可接觸電磁紀錄之範圍，３、允許以遠端方式執行搜索，４、增加可以將電子設備自搜索處所移出、扣留進行檢查之法律授權，５、修正有關協助令之要件以及違背之處罰。

所謂「帳戶資料」(account-based data）係指：某人持有某電子服務之終端使用者帳戶或可能為該帳戶的用戶，並且可以接觸該電子服務提供的

[324] *See id*. s. 58.
[325] *See id*. s. 49B.
[326] ASIO Act, s. 34
[327] Department of Home Affairs, *Surveillance Devices Annual Report 2018-19*, p. 19 and Surveillance Devices Annual Report 2019-20, p. 20.

doi:10.6342/NTU202301879

數據，則將其視為與此人有關之帳戶資料（account-based data）[328]。簡言之，只要可以透過特定人取得或使用之帳戶資料，即屬此特定人相關之帳戶資料，在特定人死亡之情形，只要該帳戶過去為此特定人持有或使用亦可，執法機關僅需證明特定人可能為該帳戶使用者，甚至為使用者之一即為已足[329]，概念上更為廣泛。本法施行後，執法機關對於電磁資料搜索之範圍，擴及該人相關之「帳戶資料（account-based data）」[330]易言之，只要該「帳戶所有人」所有、承租、使用甚至曾經使用之電腦，都可為搜索的客體。

執行方式上授權執法機關得使用「其他電子設備」執行搜索以取得目標帳戶資料，亦即包括遠端搜索[331]，只要在令狀期間內，執法機關可以在任何處所、時間執行遠端搜索，不論在搜索對象面前為之，或是秘密執行均可[332]，並允許在合理情況下添加、複製、刪除或更改資料。

Schedule 4 則是有關澳洲邊防署搜索權及協助令狀之規定，內容大致與 Schedule 3 有關執法機關之規定相同。TOLA ACT 施行前，澳洲邊防署雖擁有依令狀為處所搜索之權利，卻不包含搜索電腦及所儲存之資料之權利[333]，而僅得透過協助令狀之方式取得電磁資料，TOLA ACT 施行後，澳洲邊防署依法得以在執行特定地點搜索時，得以對電腦設備執行搜索。然而，不同於 Schedule 3 有關執法機關之規定，澳洲邊防署之電磁紀錄搜索權並不包括「帳戶資料（account-based data）」，屬於傳統上對於人的搜

[328] Crimes Act 1914 - SECT 3CAA

[329] *The Independent National Security Legislation Monitor (Dr James Renwick CSC SC), Report on Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 and related matters.*, (June 30,2020), p. 89, at https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf, last visited 07/01/2023.

[330] Crimes Act 1914, s. 3F (2A) and s. 3F(2B).

[331] Crimes Act 3F (2B)(c)；Customs Act paragraph 199B (2)(c).

[332] Crimes Act, s 3F (2E).

[333] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Revised Explanatory Memorandum, p. 23.

doi:10.6342/NTU202301879

索，針對搜索對象所持有之電子設備或所儲存之電磁資料為搜索標的[334]。此外，澳洲邊防署依舊有海關法之規定，可向法官聲請令狀，強制與標的電腦（Computer）相關之特定人，提供澳洲邊防署取得、複製電磁紀錄或將其轉換形式所必要之資訊或協助，而 TOLA ACT Schedule 4 擴充協助令狀之範圍，不僅限於電腦（Computer），更擴及電磁資料儲存設備(data storage device)，此外，也加重違反協助令狀之處罰，從原本的 6 個月以下有期徒刑，提高至最重可處 5 年以下有期徒刑及 300 罰金單位[335]（一般案件）、10 年以下有期徒刑及 600 罰金單位[336]（重罪案件）[337]。

第三項　修法過程及修法後審查

TOLA 法案之立法過程十分倉促，法案最早於 2018 年 9 月提出，期間縱有諸多爭議，然仍在強大的催促立法聲浪中迅速在同年底通過[338]，附帶要求獨立國家安全立法監督機關（The Independent National Security Legislation Monitor ，簡稱 INSLM）須在立法生效後的 18 個月內進行單獨的法定審查。

INSLM 2020 年公布針對 TOLA ACT 的審查報告(下稱 INSLM 審查報告)[339]指出，目前技術協助通知及技術能力通知，缺乏獨立之監督機制，審查報告建議修訂 TOLA ACT，以取消機關首長和司法部長簽發技術協助通知及技術能力的權力，報告建議該權力賦予之對象，應為在行政上訴

---

[334] Customs Act, s 199A(1).

[335] 相當於 63,000 澳幣

[336] 相當於 124,000 澳幣

[337] *The Independent National Security Legislation Monitor (Dr James Renwick CSC SC), Report on Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* and related matters., (June 30,2020), p. 94, at https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf, last visited 07/01/2023.

[338] C Barker, M Biddington and H Portillo-Castro,*Telecommunications and Other Legislation (Assistance and Access) Bill 2018*, Bills digest, 49, 2018 – 19, Parliamentary Library, Canberra, 3 December 2018.

[339] *The Independent National Security Legislation Monitor (Dr James Renwick CSC SC), Report on Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 and related matters*., (June 30,2020) , at https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf, last visited 07/01/2023.

doi:10.6342/NTU202301879

法院中依法設立之辦公室。 此修正建議將保護機密信息，並允許對諸如“系統弱點”之類的技術問題做出獨立裁判，並確保通知之發出機關，會納入人權，隱私和技術等因素考量[340]。

INSLM 審查報告還建議給予州及地方反貪腐委員會同意或申請上開通知之權力，且不應將通信服務商視為自然人個人，除非該自然人並非受僱人而係個體經營者之情形[341]。INSLM 審查報告之結論認為 TOLA ACT 是為回應“走向黑暗（going dark）”必要之立法，也肯認 Schedule 2 電腦訪問令之相關規定及程序保障，以及 Schedule 3 及 4 擴大搜索令及協助令之規定均屬必要且符合比例原則[342]，並認為對於違反協助義務之處罰，引進罰金刑作為徒刑以外之另一種刑罰方式，係屬正確之方向[343]。然而，INSLM 審查報告認為縱使 Schedule 3 及 4 提高協助令違反之刑罰效果仍無法解決實際上因違反本條而遭起訴及定罪之比例低之問題，以 TOLA ACT 施行前 17 年為計算標準：澳洲聯邦警察以違反本協助義務追訴者有 63 件，最終僅有 23 件定罪，其中 9 件判決有期徒刑、4 件判決擔保釋放、9 件判處罰金以及 1 件少年案件；澳洲邊防署同期間本協助義務追訴者僅 8 件，僅有 2 件最終為有罪判決，均判處罰金刑，均顯示違反協助令之刑事處罰，仍因難以舉證、刑罰相當性之問題，於個案中難以發揮效用[344]。

結論上，INSLM 審查報告認為缺少獨立之決策機關暨技術建議，就無法充分考慮所涉及到之隱私及其他問題，這是審查報告認為最大的疑慮，虛擬世界中，人民對於程序保障之需求已高於真實世界，為達成比例原則，澳洲政府必須在虛擬世紀中，對於「必要性」以及「日益增加之程序保障

[340] *See id*. at 24-25.
[341] *See id*. at 44.
[342] *See id*. at 39.
[343] *See id*. at 40.
[344] *See id*. at 247.

doi:10.6342/NTU202301879

需求」間取得平衡[345]。

澳洲議會情報與安全聯合委員會（Parliamentary Joint Committee on Intelligence and Security）也在 2021 年 12 月針對 TOLA ACT 提出審查報告(下稱澳洲議會委員會審查報告)[346]，內容包含針對 TOLA ACT 擴大執法機關對於雲端資料之搜索權與美國 2018 年雲端法(Clarifying Lawful Overseas Use of Data Act 【CLOUD Act】[347])之相容性進行審查。向澳洲議會情報與安全聯合委員會提出 TOLA ACT 與美國雲端法相容性質疑意見者包含：

1. 澳洲法律委員會（Law Council of Australia[348]）認為有關 TOLA ACT 擴大執法機關雲端搜索權，恐導致澳洲未能符合美國 2018 年雲端法所規定得與美國簽署雲端資料取得雙邊協議之資格，如此恐導致澳洲未來必須循固有耗時之司法互助（MLAT）程序取得相關雲端資料之質疑[349]，且 TOLA ACT 規範業者協助解密之義務，與美國 1994 年通

[345] *See id*. at 142.

[346] Parliamentary Joint Committee on Intelligence and Security, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, 2021 DEC., at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf, last visited 07/01/2023.

[347] 美國《雲端法》（CLOUD Act），全名為《釐清境外合法利用資料法》（Clarifying Lawful Overseas Use of Data Act），於 2018 年 3 月 23 日頒布生效，該法更新《1986 年儲存通訊紀錄法》（Stored Communications Act of 1986），並釐清海外資料合法取得：無論資料儲存地在美國境內或境外，美國執法機構均可合法請求通訊紀錄的保存或揭露。《雲端法》授權美國與其他值得信賴的國家進行雙邊協議，以取得重大犯罪之電子證據。其他國家必須擁有相應的完善法規、隱私、公民權利之保護，方具備與美國簽署雙邊協議的資格，透過雙邊協議，締約雙方可憑對方國家的搜索票等法律文件，直接對通訊服務提供者強制執行。《雲端法》闡明美國與相當多國家長久以來的原則，即假設一間公司在特定國家的司法管轄權範圍內，則其所產生的資料應接受該國的管制，資料儲存地為何，在所不問。註引自朱翊瑄，美國《雲端法》（CLOUD Act），2019 年 8 月，資策會科技法律研究所網頁，https://stli.iii.org.tw/article-detail.aspx?no=67&tp=5&d=8291，最後瀏覽日 2023 年 7 月 3 日。

[348] 澳洲法律委員會成立於 1933 年，由澳州各法律協會和律師協會組成，為澳洲法律專業機構。

[349] Law Council of Australia, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)*, p. 8, at https://www.lawcouncil.asn.au/publicassets/1545dc90-50d8-e911-9400-005056be13b5/3646%20-20Review%20of%20the%20amendments%20made%20by%20the%20Assistance%20and%20Access%20Act.pdf, last visited 07/05/2023.

doi:10.6342/NTU202301879

訊協助法(Communications Assistance for Law Enforcement Act 1994)規定允許業者提供其無法解密之加密服務之規定不符，依照美國 Stanford 互聯網與社會中心的網絡安全監控副主任 Riana Pfefferkorn 曾引用§2523(b)(3) US Code 所述‘與澳洲簽立任何協議都應明確禁止“有關業者提供解密數據之義務”，TOLA ACT 有關業者解密義務恐影響澳洲與美國依照雲端法簽立雙邊協議[350]。

2. 商業軟體聯盟（Business Software Alliance，簡稱 BSA）認為技術協助通知及技術能力通知之發出之標準恣意且不透明，普遍缺乏審查或監督，如此恐無法滿足美國雲端法簽訂執行協議國家之先決條件[351]。

針對上開質疑意見，澳洲議會委員會審查報告最終採納美國司法部 2020 年 4 月向澳洲議會情報與安全聯合委員會提出之書面說明，美方表示：TOLA ACT 有關業者協力義務之規範並不影響美澳雙方進行之雲端協議，美國雲端法規定依本法簽訂之協議對於加密是採中立之態度，雲端法協議不會創設新的有關業者解密或提供解密後資訊之義務（18 U. S. C. 2523（b）(3)），也不會禁止或限制業者履行原有依照內國法之解密協助義務，雲端法不會阻止夥伴國家在其內國法訂定有關解密相關要求，也不會因此使其簽立雲端協議之資格[352]。澳洲議會委員會審查報告最終採納依照美國司法部所做之說明，認定 TOLA ACT，將不致於對澳洲與美國依雲端法簽定協議乙事產生預先排除之影響[353]。

---

[350] *See id*. at 9.

[351] BSA | The Software Alliance, Submission 6, p. 3. See also International Civil Liberties and Technology Coalition, Submission 19, p. 8-9.

[352] US Department of Justice, Submission 30, p. 1.

[353] Parliamentary Joint Committee on Intelligence and Securitym, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, 2021 DEC., at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf, p.27, last visited 07/05/2023.

doi:10.6342/NTU202301879

針對 Schedule 1 通信服務商協助請求之實務運作情形，澳洲議會委員會審查報告指出自 2018 年立法通過後，執法機關實際使用過者為技術協助請求（TAR），一般而言，技術協助請求是機關與通信服務商彼此間協商結果，使用現行技術或開發新的技術以達成協助目的，透過類似契約協議之方式完成，通信服務商也因為技術協助請求（TAR）獲得民事責任以及 1995 年刑法典中相關刑責之豁免[354]。而技術協助通知(TAN)及技術能力通知(TCN)至今均尚未使用[355]。

TOLA ACT 針對通信服務商施以諸多技術協助義務規範，澳洲科技公司普遍提出諸多質疑或給予負面評價，澳洲議會委員會審查報告引述通信商職業公會（Communication Alliance）於 2019 年 12 月進行了一項調查，調查結果百分之 95 受訪業者認為 TOLA ACT 對於澳洲科技公司在全球市場之發展產生負面影響，百分之 61 業者收到國內外客戶反應，會擔憂 TOLA ACT 對公司所生產產品或提供服務所造成之影響[356]。

美國 Stanford 大學法學院網路與安全中心(The Center for Internet and Society at Stanford Law School）副主任 Riana Pfefferkorn 也指出，TOLA ACT 減損澳洲科技公司相對於其他外國公司之競爭力，使外國公司顯得更據吸引力，澳洲政府不能一方面希望澳洲新創產業在

[354] Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*, at Document https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrativeguidance.pdf, last visited 07/05/2023.

[355] Parliamentary Joint Committee on Intelligence and Security, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, 2021 DEC., at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf, p.109, last visited 07/05/2023.

[356] *See id.* at 35.

doi:10.6342/NTU202301879

網路安全領域具有國際領導地位，另一方面卻反其道而行[357]，有鑑於上面產業對於 TOLA ACT 影響之疑慮，澳洲議會委員會審查報告之結論具體建議澳洲政府於審查報告提出後，進行為期 3 年調查，針對資訊與通信科技產業受到 TOLA ACT 之經濟影響評估提出報告並對大眾公開（Recommendation 4. 75）[358]。

TOLA ACT 現行有關技術協助通知以及技術能力通知之核發，無須通過司法審查之部分亦受到批評，澳洲私隱專員公署（Office of the Australian Information Commissioner，OAIC）即建議 TOLA ACT 應予修法使技術協助通知以及技術能力通知之核發也須經過司法權之審查[359]。

相對於澳洲科技公司於澳洲議會委員會審查期間，針對 Schedule1 通信服務商協力義務提出諸多質疑或反對意見，澳洲科技公司及社會大眾針對 Schedule2 至 4 有關政府進入電腦令以及擴大搜索令之部分所提意見明顯少了許多[360]。有關 Schedule2 電腦訪問令之部分，澳洲議會委員會審查報告與 INSLM 審查報告同樣關注在電腦訪問令有關隱匿訪問（concealment of access）之部分，審查報告認為法律並無明確限制隱匿訪問之期間限制，澳洲議會委員會審查報告因而建議，政府針對電腦訪問令之隱匿訪問，應在干預對象隱私保護及執法必要中取得平衡，建議修正「2004 年《監視設備法》」、「1979 年澳大利亞安全

[357] Riana Pfefferkorn, *Submission 4 to Parliamentary Joint Committee on Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, p.6

[358] Parliamentary Joint Committee on Intelligence and Security, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, 2021 DEC., at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf, p.49, last visited 07/05/2023.

[359] *See id.* at 91-92.

[360] *See id.* at 59.

doi:10.6342/NTU202301879

情報組織法案」，規定情報機關與執法機關執行應設計有異於司法部長、核發令狀者以外之外部監督，設定執行期限(如：6 個月)並賦予外部審核機制[361]。

第六節　木馬技術及相關規範

自上述介紹之英國、法國、德國、荷蘭及澳洲立法例，均可發現國家木馬已係世界諸多法治先進國家肯認得以基於國家安全、執法等目的使用之技術設備。然而，上開內國法規定雖可得知木馬技術之「使用」規範，然對於木馬技術之來源是否有所限制？有無技術擔保相關規範？自屬立法後執行面之重要問題，值得進一步探究。

第一項　歐盟國家現況

各國木馬技術涉及國家安全機密事項，相關公開資訊不多，然從歐洲議會 2017 年公布之「執法機關使用木馬技術之法律框架：識別、評估和實踐比較」委託研究報告[362]中可約略窺知一二。世界各國執法機關所使用之木馬大致可分為「國家研發」(in-house development）以及「購買現成[363]」(off-the-shelf)2 種模式。絕大部分的國家採取「購買現成」市售符合出口規範(詳後述）木馬之方式，而德國、法國及義大利則是兼採「國家研發」途徑[364]。

---

[361] *See id.* at 68-69.

[362] European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices Study*, (March 2017), at https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2017)583137, last visited 07/05/2023.

[363] 公開資料中可見市售具監視功能之木馬軟體包含：Pegasus by NSO group, Cobwebs Technologies, Cognyte, Black Cube, Blue Hawk CI, BellTroX, Cytrox107, Predator, Candiru, Reign / QuaDream, Paragon108; Dark Basin, Circles system, SS7 attack, Cobalt Strike, FinSpy, NetWire, P6 intercept, Galileo, PC 360, Karma, Epeius, StealthAgent, Crimson, Invisible Man, Unlimited Interception System, Skylock, Windshield, Phoreal, Soundbite, OceanLotus tester, Ocean Lotus encryptor, Ocean Lotus Cloudrunner, Ocean Lotus MAC, Komprogo.109。相關廠商包含 Cellebrite, FinFisher, Blue Coat, Hacking Team, CyberPoint, L3 Technologies, Verint and NSO Group. 註轉引自 IPOL | Policy Department for Citizens' Rights and Constitutional Affairs, Pegasus and surveillance spyware, May 2022, p.22.〈ANNEX2：List of Spyware〉

[364] European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices Study*, (March 2017), at https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2017)583137, p 60-61, last visited 07/05/2023.

doi:10.6342/NTU202301879

上開報告列舉現在或過去曾採用「國家研發」途徑之國家包含:法國、德國及義大利 3 個國家。法國執法機關過去曾使用鍵盤測錄器（keylogger）之方法蒐證，之後由法國司法部及內政部共同開始開發遠端植入之木馬程式，然嗣後在法國研發之國家木馬獲得授權不久後，又因爭議事件而使國家木馬被初始化（reinitialised），而並未為法國執法機關實際使用[365]。德國聯邦刑事警察局（BKA）在 2011 年曾使用外購之木馬程式，然事後遭發現程式具有啟動筆記型電腦麥克風及鏡頭之法律授權以外之功能後，聯邦刑事警察局（BKA）則不再使用外購木馬程式之方式，而改為國家自行研發之途徑，為此德國內政部成立 Zentrale Stelle für Informationstechnik im Sicherheitsbereich」（ZITis）新網路安全部門提供執法機關有關木馬技術之支援協助[366]。義大利則是在 2017 年的相關法律草案規定義大利必須使用自行研發之木馬而非向私人機構採購，且不能減損受干預設備之資訊安全等級，且必須於結束後移除。另外，直接規定國家木馬可以使用之科技技術者，僅有荷蘭第三部電腦法，其正面規定執法機關可以使用零日攻擊之木馬程式，且必須將漏洞利用報告給相關機關，但取得特別授權後可延遲揭露，另依照荷蘭非政府組織之報告，實務上荷蘭執法機關受允許可以購買市售利用已知或未知系統漏洞之木馬程式[367]。

在歐洲，隨著 Gamma Group 公司、義大利 Hacking Team 等公司販售木馬程式相關細節陸續公布，木馬程式販售後被用於大規模監視、干擾及截收而造成人權侵害之問題日益受重視，例如 FinFisher 木馬程式為總部在慕尼黑的 Gamma Group 公司所開發，販售予各國政府作為情報及執法目的使用，然而縱使當初係作為前開合法目的販售之用，然嗣後卻被發現巴林政府在 2010 至 2012 年之間使用 FinFisher 木馬程式針對律師事務所、記者以及反

[365] *See id.* at 60.
[366] *See id.*
[367] *See id.* at 61.

doi:10.6342/NTU202301879

政府領袖等進行監控，民間因而呼籲應修改軍商兩用貨品出口管制規範而使木馬程式受到監管[368]。

第二項　瓦聖納協定及歐盟軍商兩用貨品及技術出口管制清單

現行有關跨國軍商兩用貨品出口管制規範主要係依《關於常規武器與兩用產品和技術出口控制的瓦聖納協定》（The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Good and Technologies，下稱瓦聖納協定）之非強制性多邊協定，共有 42 個國家參與簽署，瓦聖納協定於 2012 年至 2013 年進行修正，將「滲透軟體」、「行動電話攔截或干擾設備」及「IP 監視系統」等木馬程式納入規範[369]，要求各國應禁止對可能會被用來侵害人權之商品發放出口許可證[370]，以防止販售木馬程式之科技公司出售木馬程式給侵害人權之國家政府。在歐盟層級，則另有具法律強制效力之《歐盟軍商兩用貨品及技術出口管制清單暨一般軍用貨品清單》（【EC】No 428/2009，下稱歐盟軍商兩用貨品及技術出口管制清單，後於 2021 年 5 月 20 日由 No 2021/821 歐盟新兩用物項出口管制規則取代，詳後述)予以規範，歐盟軍商兩用貨品及技術出口管制清單於 2014 年修正，將「滲透軟體」、「行動電話攔截或干擾設備」及「IP 監視系統」等木馬程式納入規範，並於歐盟兩用協調小組（Dual-use Coordination Group，簡稱 DUCG)下成立監控技術專家小組（the Surveillance Technology Expert Group，簡稱 STEG），負責審查與網絡監控技術出口管制相關事項[371]。

---

[368] Marczak, B. et al., *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Munk School of Global Affairs*., (Oct. 15 2015), at https://tspace.library.utoronto.ca/handle/1807/97784., last visited 07/05/2023.

[369] Bauer, S. and Bromley, *the Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.*, (March 2016).

[370] The Wassenaar Arrangement – On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, About Us. http://www.wassenaar.org/., last visited 07/05/2023.

[371] Coalition against Unlawful Surveillance (CAUSE), *'A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation*', (June 2 2015).

doi:10.6342/NTU202301879

然而，縱有上開國際規範，尚有論者認實際效用仍有限，因瓦聖納協定不具法拘束力，且各國對於規範內容之解釋、應用差異甚大，尚難發生效用，而歐盟軍商兩用貨品及技術出口管制清單雖有法拘束力，然因無論係瓦聖納協定或是歐盟軍商兩用貨品及技術出口管制清單當時均係以 FinFisher 木馬程式為模型來形塑規範內容，並不能有效涵蓋現今多樣之木馬程式，因而仍有論者呼籲應直接禁止對人權低度保障之國家出售木馬程式[372]。

歐盟執委會也於 2016 年 9 月 28 日向歐洲議會提出一項現代化建議案，有別於傳統軍商兩用貨品及技術出口管制清單的管制側重於軍事風險，尤其是大規模殺傷性之武器擴散，2016 年 9 月 28 日公布之建議案引進人類安全(Human security)新興概念，相對於傳統國家安全之概念，特別著眼於人權保護觀點檢視規範正當性[373]，尤其針對網路監視商品可能對歐盟造成之人權侵害以及危害歐盟數據基礎設施[374]，希望擴大網路監視商品之定義，另外加入中心監控以及數據保留系統或設備等國際規範中未列舉之商品，並加上概括條款以囊括所有可能對人權造成嚴重侵害之商品，課予歐盟成員國於發放出口證時將商品最終目的地國家履行人權及國際人道主義等情形列入考量。此項建議案自 2019 年 10 月開始歐盟執委會、歐盟議會以及歐洲理事會之三方協商，終於 2021 年 5 月 20 日通過 No 2021/821 歐盟新兩用物品出口管制規則，自 2021 年 9 月 8 日施行[375]。歐盟新兩用物品出口管制規則，旨在強化新興軍民兩用物品之出口管制，管制的範圍包含物品之出口、仲介、技術援助、過境和技術移轉，依照 No 2021/821 歐盟新兩用物品出口管制規則，任何可能涉及侵犯人權之產品、服務、軟體或技術之出口，出口商都必

[372] European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices Study,* (March 2017), at https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2017)583137, p 31, last visited 07/05/2023.

[373] Machiko Kanetake, ' *The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches*', Business and Human Rights Journal, Vol. 4(1), (2019), p. 155-162.

[374] Beatrix Immenkamp, *Review of dual-use export controls,* EPRS | European Parliamentary Research Service, July 2021, p3.

[375] *See id*. at 3-5.

doi:10.6342/NTU202301879

須取得許可證，而出口商及各會員國主管機關在聲請及審核許可證時應針對最終收貨人及最終用途進行盡職調查[376]，預防可能之人權侵害，各會員國應特別考慮網路監控商品被用於內部鎮壓、嚴重侵犯人權或違反國際人道主義法之風險。為確保規則之落實，各會員國應採取適當措施制定有效、符合比例原則且具嚇阻力之罰則確保執行[377]。

第三項　歐盟對會員國使用木馬程式之態度

歐洲議會公民權利和憲法事務政策部於 2022 年 5 月針對以色列木馬開發公司 NSO Group 所研發之 Pegasus（飛馬）木馬及其他監視軟體公布分析報告。此項分析報告源自於 NSO Group 所研發之 Pegasus（飛馬）木馬陸續遭揭露用於監視歐洲多國政要，如：法國總理馬克宏及至少 5 位內閣大臣[378]、西班牙總理桑傑士及國防部長羅布雷斯[379]等。依照此分析報告，歐美多國政府雖未正面承認購買 Pegasus（飛馬）木馬，但依照相關新聞報導，上開分析報告認歐美多國政府有購買此類木馬軟體之跡象。針對此現象，歐盟執委會於 2022 年 4 月 19 日明確表示不會調查歐盟國家使用 Pegasus 事件，因為歐盟執委會無權處理國家安全問題，是否受到違法監視僅能在國家司法層級尋求救濟[380]。歐盟資料保護監督機關(European Data Protection Supervisor, 簡稱 EDPS)則關注此現象於歐洲可能造成之人權侵害問題，強調此類木馬軟體之違法使用將造成前所未有之基本權侵擾，嚴重威脅隱私權，雖然依照歐洲聯盟條約（Treaty on European Union，簡稱 TEU）國家安全是各會員國保有之核心領域，然而各會員國仍必須尊重歐洲人權公約和

[376] Regulation (EU)2021/821, Art. 2 (21), Art.5.2.
[377] Regulation (EU)2021/821, Art. 25.
[378] Spyware 'found on phones of five French cabinet members, The Guardian, Jon Henley and Stephanie Kirchgaessner, (Sep. 23 2021), at https://www.theguardian.com/news/2021/sep/23/spyware-found-on-phones-of-five-french-cabinet-members, last visited 07/03/2023.
[379] IPOL, Policy Department for Citizens' Rights and Constitutional Affairs, Pegasus and surveillance spyware, (May 2022), p.10
[380] *See id*. at 15.

doi:10.6342/NTU202301879

歐洲人權法院判例所揭示基於國家安全所為之監視行為仍有其限制。此外，倘係基於執法目的使用木馬監視軟體應遵循歐盟相關法律及歐洲聯盟基本權利憲章（Charter of Fundamental Rights of the European Union）、隱私及電子通訊指令（ePrivacy Directive）以及執法指令（law enforcement directive）[381]等規定。歐盟資料保護監督機關 EDPS 最終結論認為"經常性使用"Pegasus（飛馬）或與其功能相當之木馬與歐盟法治無法相符，僅有針對打擊不法之特殊情形，且必須採行相當程度之監督措施（如：加強木馬監督，落實歐盟隱私和數據保護法、司法審查、刑事訴訟權利保護、禁止基於非法情報目的輸入、不濫用國家安全、解決法治問題、公民社會支持），此外，針對此類木馬亦應加強落實歐盟軍商兩用貨品及技術出口管制清單，甚至將其涵蓋到進口面向，以保護歐盟人民的基本權[382]。

綜上，自瓦聖納協定、歐盟軍商兩用貨品及技術出口管制清單甚至歐洲議會公民權利和憲法事務政策部 2022 年 5 月公布之分析報告，大致可得出以下結論，現行國際規範並無禁止木馬軟體之採購，然有鑑於其侵害基本人權之高度可能性，現階段透過瓦聖納協定、歐盟軍商兩用貨品及技術出口管制清單，自出口許可證核發面向予以管制，並成立監控技術專家小組為出口許可項目之審查。然而，使用面向上，木馬是否為合法使用則是內國法層級之問題，需透過各國制訂法律、訂定相關使用規範，並落實監督機制等方向，以確保木馬之合法使用。

第四項　德國聯邦刑事警察局（BKA）訂定之標準化服務描述

至於內國法規範國家木馬之採購使用，有德國聯邦刑事警察局（BKA）針對來源端通訊監察所使用之科技技術定有標準化服務描述（Standardisierende Leistungsbeschreibung 簡稱 SLB），此乃德國政府針對來

[381] *See id*. at 17.
[382] *See id.*

doi:10.6342/NTU202301879

源端通訊監察時所訂定之最基本標準，要求德國政府使用監察軟體，必須經過一連串的測試，確保符合法律規定以及上述標準化服務描述要求後才能使用，內容類似於我國資訊委外開發案建議書的徵求說明書[383]。

SLB 內容大致涵蓋以下面向：軟體製造商、供應商專業能力和可信度、製造商和供應商應提供充足之原始碼以及與測試軟體功能相關之資訊，使測試機構能夠從原始碼中確認程序的創建過程、原始碼檢查應由技術上合適的專家（例如：受德國聯邦資訊安全局《BSI》認可的測試實驗室）進行檢查、建構符合 BSI 標準之資訊安全規範、以數據傳輸備份技術防止未經授權之使用，並確保資訊之機密性、完整性、真實性以及可用性、綜合日誌紀錄、確保監控軟體符合法律規定之要求(不包括法律授權範圍以外之功能、只限於取得進行中之通訊、只為必要之變更、確保無未經授權之人非法取得、防止遭被監察人發現)、必須通過最新防火牆、防毒軟體之偵測等等[384]。為確認來源端通訊監察軟體符合上開標準化服務描述木馬軟體須經過 5 道測試程序：TÜV IT 公司之軟體測試（確認符合 SLB）、德國聯邦資訊安全局的滲透測試、德國聯邦刑事警察局的功能測試、系統測試以及採購驗收測試[385]。

第七節 小結

綜觀本章所介紹之英國、法國、德國、荷蘭及澳洲等國近年來針對加密技術所為之立法，均可發現上開國家在立法過程中面對國家安全、犯罪偵查與加密技術對於資通安全以及個人隱私權保護等利益權衡之下，最終均維持支持加密技術發展之基本立場，然賦予國家為保護國家安全、執行犯罪偵查之制衡武器以資平衡，多國於立法過程中曾出現之「後門爭議」，於上開

[383] 林國翔、沈士豪、李鎮宇，取得加密通訊內容因應對策—從通訊監察技術觀點出發，臺灣警察專科學校警專學報，第 7 卷第 6 期，2021 年 2 月，頁 38。
[384] Bundeskriminalamt official Website, at https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html, last visited 07/04/2023.
[385] 林國翔、沈士豪、李鎮宇，取得加密通訊內容因應對策—從通訊監察技術觀點出發，臺灣警察專科學校警專學報，第 7 卷第 6 期，2021 年 2 月，頁 39。

doi:10.6342/NTU202301879

國家最終通過立法之版本，均遭到捨棄。

分析本章所介紹之國家早年至近期之立法進程，英國、法國及荷蘭係先採行解密令狀之立法《如英國 2000 年 RIPA 之第 49 條通知、法國 2004 年刑事訴訟法第 230 條之 1、荷蘭 2012 年刑事訴訟法第 126m(6)條》，嗣後面臨單純解密義務仍不足以因應國安及執法困境時，方修法新增國家木馬授權規定，以補足單純仰賴解密義務規定之不足。澳洲的立法趨勢正巧相反，澳洲早年先採用國家木馬授權方式，而於近來 2018 年 TOLA ACT 法案強化通信服務商之協力義務。值得注意者是，澳洲、英國此波新法所定協力義務之內涵，已遠遠超越英、法、荷等國早年立法之「提供解密金鑰」或「協助轉換至可閱讀模式」之協力義務，澳洲 2018 年 TOLA ACT 與英國 2016 年 IPA 所規定通信服務商協力義務，均已擴大至要求特定通信服務商在產品或服務中加入新功能之技術能力通知，涵蓋義務型態可謂包羅萬象，大大擴張並強化業者協力義務範圍。反觀德國雖同樣有木馬授權及通信服務商協力義務之規定，然其協力義務僅係電信法及電信監察規則之一般性協力義務規範，並不包含提供「解密金鑰」，與英國、法國、荷蘭、澳洲等國之法定協助解密，甚至強制性地要求通信服務商在產品或服務中加入新功能之法定義務大有不同。

另外，本章所介紹之國家雖然清一色均有國家木馬授權規範，然立法方式確有明顯差異，德國及法國於法規範體系中針對木馬功能進一步區分並為相異之法律規範。德國法下之來源端通訊監察明確定性為傳統通訊監察之補充手段，扣緊「公共電信線路以加密方式所進行之傳輸過程原本即可監察與記錄」與傳統之電信監察具有功能等價，故實體及程序要件原則與傳統通訊監察相同，而對於資訊科技系統之內部儲存資料進行全面性地取證之線上搜索，德國法上以其侵害程度與大監聽相當，於實體及程序要件上不僅要求必須是相對於傳統搜索應具有補充性及最後手段性，列舉重罪部分更

doi:10.6342/NTU202301879

與住宅監聽同樣採取「特別重大犯罪」之門檻。法國刑事訴訟法亦針對遠端訪問「通訊內容」（法國刑事訴訟法第 706-95-1 條）以及秘密線上搜索（同法第 706-102-1 條）予以區分，有不同之法律授權規定。

相較於德國及法國立法模式將國家木馬依其功能及基本權侵害程度區分為來源端通訊監察及線上搜索，並依其基本權侵害程度賦予不同強度之實體及程序規範，英國、荷蘭及澳洲於近來之立法中，有關國家木馬之規定大多係以同一木馬授權規範囊括包含攔截通訊內容、遠端觀察、執行搜索等不同功能之木馬。比較上開兩種立法方式，德國及法國立法方式於執行面上國家必須有能力監督個案中木馬執行之功能與授權範圍相符，此亦應為採取此種立法方式時應予考量之先決要素，反面而論，若使國家木馬適用單一法律規範，可減輕執行及事後監督階段均需耗費大量功夫確定木馬僅在授權功能範圍內執行之問題。然而，從基本權干預角度而論，木馬程式功能強大，依其功能不同所干預基本權種類暨強度亦有極大落差，從較輕微的擷取指定種類、時間之資料，到最嚴重之取得設備或網路的控制權，開啟麥克風、鏡頭等進行監視，其基本權干預程度天差地遠，不僅是立法時之實體及程序要件，法官個案審核時之標準亦會不同，易言之，同一案件縱使能符合以木馬程式執行監聽，未必能符合侵害程度更高之秘密線上搜索。

有鑑於我國針對刑事訴訟干預處分，已建立基於干預之基本權利、干預程度予以不同層級之授權（詳本文第四章、第二節、第二項《我國刑事訴訟強制處分之層級化授權》），本文認為立法者於立法當時本應有責任就法律授權之木馬功能範圍有明確之立法決定，又因其干預程度落差甚大，不應強行適用單一法律規範，且依我國現行法各類刑事偵查干預處分，均係依照處分種類之性質適用不同之法定程序，與美國法上以搜索令(warrant)之概念涵蓋各類刑事干預處分之立法方式大有不同，德國法依其基本權干預程度予以細緻區分之方式，應屬較符合我國法制之立法方式。是以，於討論我國

doi:10.6342/NTU202301879

未來立法方式時，應有針對不同之科技偵查手段所干預之基本權為何進行細部區分及討論之必要，方能依其基本權干預種類及強度為程度相當之立法設計。

另外，英國 IPA 所創設針對通訊服務業者課予互聯網連接紀錄保留義務亦頗具參考價值，互聯網是由多項通信數據組成，記錄有關客戶在互聯網上連接到的服務（包含網站、應用程式等），互聯網連接紀錄雖不會顯示有關內容(例如:瀏覽網頁內容、在網頁上所做事情等)，但互聯網連接紀錄在諸多情形下對於執法很有幫助，例如：透過 IP 位置查知涉嫌人的身分、確認涉嫌人、被害人使用哪種通訊軟體進行通訊、確認利用網路進行犯罪之嫌疑人身分以及所使用之應用程式[386]，這些伴隨互聯網設備而產生之各種數位資訊，可用來分析犯罪者之數位足跡，藉此達到追查犯罪行為人身分，向上追溯共犯，甚至預測可能受害者之效果，對於打擊網路犯罪有極大功效，已逐漸在執法上受到重視。

本文認為，英國 IPA 所創設之「保留互聯網連接紀錄」之法定義務係因應互聯網時代來臨網路犯罪充斥之今日執法所不可或缺，具有其必要性，而在法律規範不夠明確時，當執法機關向通信服務業者要求業者留存客戶連接紀錄時，互聯網業者往往面臨客戶資料保密義務（可能為個人資料保

[386] 除互聯網以外，以物品與互聯網相結合之「物聯網」也與偵辦犯罪具重要關聯，如：2018 年美國更曾經發生新罕布夏州警方偵辦命案過程中，取得法院核發令狀要求 Amazon 公司交出旗下 Alexa 智慧音箱之錄音檔，因法院認定智慧音箱傳回物聯網業者之錄音紀錄，可能包含命案現場當時之錄音；嗣後 2019 年發生在佛羅里達州之命案，警方亦係透過法院令狀要求 Amazon 公司交出 Alexa 智慧音箱之錄音檔。Amazon 公司對於上開法院令狀，對外均以「除非得到“合法有效且具有約束力的命令”的要求，否則它不會交出客戶信息，並且拒絕“過分寬泛或其他不適當”的要求」。註參 Meagan Flynn, *Police think Alexa may have witnessed a New Hampshire double homicide. Now they want Amazon to turn her over*., The Washington Post, (November 14, 2018), at https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/, last visited 07/03/2023；RAFAEL OLMEDA, *Alexa, is he guilty of murder? Amazon device may have heard slaying, cops say, SOUTH FLORIDA SUN SENTINEL*, (OCT 31, 2019), at https://www.sun-sentinel.com/news/crime/fl-ne-amazon-alexa-murder-investigation-20191031-qccpvdl6kng5hcx3z6eusxa264-story.html, last visited 07/03/2023.

doi:10.6342/NTU202301879

護法或是契約義務)，以及配合司法、執法機關（可能為法定義務，甚至有違反法定義務之法律制裁）之兩難困境，若有法律明確規範業者保留(甚至提供)互聯網連接紀錄之法定義務，業者辦理相關事務能有所依據，方不至於違反法律所規範蒐集個人資料之規定以及對客戶所負之契約義務，業者之配合意願自會提升。而我國執法機關目前亦面臨追查相關犯罪時，電信事業及設置公眾電信網路者未留存互聯網連接紀錄之困境，致使執法機關在預防重大犯罪之發生以及有效追訴犯罪上遭遇困境。

有鑑於此，我國對此也開始推動立法，法務部前曾於 107 年 11 月 7 日預告之通訊保障及監察法部分條文修正草案中，其中第 14 條修正研擬新增電信事業保存網路流量紀錄(Netflow Log)法定義務[387]，此部分立法與英國 IPA 之「保留互聯網連接紀錄」規定具類似性，同屬針對非內容之連網紀錄課予業者保留義務，而值得注意者是我國草案與英國有關互聯網連接紀錄之保留義務雖都是針對電信事業，然英國 IPA 所規定之「保留互聯網連接紀錄」雖亦係電信事業，但英國電信事業之範圍尚包含於網路上提供服務之事業，亦即我國定義下之網路服務業，範圍顯較我國廣泛，而英國因應網路服務業範圍廣泛應如何執行之問題，係依照政府對特定業者有連網紀錄獲取需求時，循針對特定業者發出具強制力之保留通知之方式執行之，兩種立法方式各有其優劣，足以作為我國新增此部分規定之重要參考。

[387]參公共政策網路參與平台 2018 年 11 月 7 日預告之通訊保障及監察法部分條文修正草案，https://join.gov.tw/policies/detail/7660d6d4-ec2a-4052-a725-854cd4c3c1a8?fbclid=IwAR0XoYoJnfg9vDuOuHhZL2z5MIiygPvu80M1z5mPEhuOR6QkuQ9t0xMsD2o，最後瀏覽日 2023 年 6 月 24 日。

doi:10.6342/NTU202301879

第四章　科技偵查之基本權干預及我國法制現況

第一節 刑事訴訟干預手段之憲法誡命

刑事訴訟法屬「廣義公法」，為國家行使刑罰權時依憲法價值秩序所生之規範基準，因刑事訴訟程序中包含諸多針對人民憲法基本權之干預，自然應恪遵憲法基本權干預之法律保留原則、比例原則等憲法基本原則，予以檢視干預處分之合憲性。準此，刑事訴訟法規範及解釋可謂憲法基本權保障之具體實踐，故又有「憲法的測震儀（Das Strafverfahrensrecht als Seismograph der Verfassung）」之稱[388]。

傳統刑事訴訟干預處分所涉及之基本權干預，包含憲法第 10 條居住遷徙自由（如：限制住居命令）、憲法第 15 條財產權（如：搜索、扣押命令）、憲法第 12 條秘密通訊權（如：通訊監察），另伴隨當代基本權體系之擴張，發展出諸多非憲法明文揭示之基本權，如憲法第 22 條發展出之人格權，內涵包括資訊自決權、隱私權及一般行為自由權等等，傳統基本權保護領域及干預概念隨之擴大，致使法律保留原則適用範圍產生擴張，伴隨科技發展所帶來之犯罪手法日新月異及偵查手段之相對應調整，造成「干預無所不在」之現象。然而，依司法院釋字第 443 號解釋理由書揭示之「層級化保留原則」，不同基本權於憲法上所享有之保護位階具有層級化差異，例如憲法明文列舉之基本權與非列舉基本權其保護位階即有不同，準此，實務[389]及學說遂有層級化法律保留體系（System des abgestuften Vorbehalts）理論，輔以門檻理論（Schwellentheorie），用來解決上開法治國兩難之處[390]。

我國憲法第 23 條揭示「法律保留原則」及「比例原則」有關憲法基本

[388] Vgl. Roxin/Schünemann, Strafverfahrensrecht, 27. Aufl. 2012, S.9.
[389] 層級化法律保留可參司法院釋字第 443 號、第 614 號、第 658 號、第 765 號解釋等。
[390] 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，第 96 期，2007 年 4 月，頁 191-193。

doi:10.6342/NTU202301879

人權限制之兩大憲法誡命，歷來司法院釋字論及憲法基本權利之干預時，均引用憲法第 23 條「法律保留原則」作為依據，國內學說及實務亦普遍肯認只要是涉及憲法保障基本權之干預，均有法律保留原則之適用，剩下者僅係保留密度的問題[391]。憲法第 23 條雖未依基本權之性質或其影響程度建立不同層級之法律保留體系，然自司法院釋字第 443 號開始，明白揭示「層級化法律保留原則」意旨，將法律保留原則進一步區分為憲法保留（憲法第 8 條之人身自由權[392]）、絕對法律保留（又稱國會保留，憲法第 7 條、第 9 條至第 18 條、第 21 條及第 22 條之各種自由及權利[393]）、相對法律保留（又稱法律授權，有關其他人民自由權利之重要事項[394]）以及非屬法律保留之細節性、技術性事項[395]。而門檻理論則是依循層級化法律保留原則下所發展出，將刑事訴訟之基本權干預處分予以層級化區分，主張司法警察（官）為刑事追訴時所為之干預性活動，在一定干預門檻以下，可以援引法律的一般授權條款作為干預基本權之法律授權基礎[396]，門檻理論尤其適用於欠缺物理性強制的資訊干預，而所謂一般授權條款即係刑事訴訟法第 228 條至第 231 條有關司法警察調（偵）查權限的一般性規定，門檻理論認為司法警察（官）依法進行偵查犯罪時，對於因此所造成質量輕微之干

[391] 蔡宗珍，法律保留思想及其發展的制度關聯要素探微，臺大法學論叢，第 39 卷第 3 期，2010 年 9 月，頁 42-43。

[392] 參司法院釋字第 392 號解釋理由書：並非一切自由及權利均無分軒輊受憲法毫無差別之保障：關於人民身體之自由，憲法第八條規定即較為詳盡，其中內容屬於憲法保留之事項者，縱令立法機關，亦不得制定法律加以限制。

[393] 參司法院釋字第 443 號解釋理由書：「…憲法第七條、第九條至第十八條、第二十一條及第二十二條之各種自由及權利，則於符合憲法第二十三條之條件下，得以法律限制之。至何種事項應以法律直接規範或得委由命令予以規定，與所謂規範密度有關，應視規範對象、內容或法益本身及其所受限制之輕重而容許合理之差異：諸如剝奪人民生命或限制人民身體自由者，必須遵守罪刑法定主義，以制定法律之方式為之。」

[394] 參司法院釋字第 443 號解釋理由書：「…涉及人民其他自由權利之限制者，亦應由法律加以規定，如以法律授權主管機關發布命令為補充規定時，其授權應符合具體明確之原則。」

[395] 參司法院釋字第 443 號解釋理由書：「…若僅屬與執行法律之細節性、技術性次要事項，則得由主管機關發布命令為必要之規範，雖因而對人民產生不便或輕微影響，尚非憲法所不許。」

[396] 有反對門檻理論者認為：任務指示規定欠缺作為干預授權基礎之適格性，違反明確性原則及恐架空刑事訴訟法之特別授權等，詳參楊雲驊，通訊保障及監察法實施前電話監聽合法性及證據評價之探討，臺灣本土法學雜誌，第 57 期，頁 45 以下，2004 年 4 月。

doi:10.6342/NTU202301879

預(如跟監、盯梢),可以援引上開一般授權條款作為干預基本權的基礎[397]。

我國刑事訴訟法第 230 條、第 231 條是否屬於「一般偵查之概括授權條款」,仍存有不同見解,否定論者認為「刑事訴訟法第 230 條及 231 條第 2 項,應定位為『單純之任務分配規範』,司法警察必須有個別授權條款才能進行具基本權干預性質之偵查手段[398]」,否定論者主要認為「刑事訴訟法第 230 條、231 條對於調查手段之種類、 發動門檻、要件及程序均無明文規定,欠缺法明確性,而與法律保留原則不符,若將其解釋為偵查概括條款,恐造成擴大司法警察自動發動強制處分的權限,使偵查程序更趨於警察化」[399];肯定論者則認「刑法第 231 條第 2 項規定相當於德國刑事訴訟法第 163 條規定,該條規定在德國過去存有『任務指示說』及『一般授權說』之爭議,後來在 1999 年修法正式確立屬一般干預授權之性質,任務指示說也因此成為過去」[400]。

實務見解就此也有不同見解,最高法院 102 年度台上字第 3522 號判決係採肯定說,認為:「跟監」雖對被跟監者之隱私權、資訊自決權造成干預,然因不具強制力,性質上屬於任意偵查行為,僅依刑事訴訟法第 230 條第 2 項、第 231 條之一般授權條款,即可為之。最高法院 106 年度台上字第 3788 號判決則推翻以往見解,認為刑事訴訟法第 230 條第 2 項、第 231 條僅具有組織法意義,不得援引作為強制處分之法律依據。有鑑於刑事訴訟法第 230 條、第 231 條是否屬於我國法上「一般偵查之概括授權條款」之爭議未能停歇,有學者建議未來必定需要透過立法新增明確之概括偵查授權條款以因應恐科技偵查手段之發展,立法政策上無論定在刑事訴

[397] 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,第 96 期,2007 年 4 月,頁 212-213。
[398] 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,第 235 期,2014 年 11 月,頁 241-243。
[399] 同上註,頁 243-254。
[400] 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,第 96 期,2007 年 4 月,頁 212。

doi:10.6342/NTU202301879

訟法或是其他專法裡都有其必要性[401]。

第二節 科技偵查與層級化授權

第一項　司法院釋字第 443 號解釋之層級化法律保留

有鑑於科技時代下各種偵查干預手段，因應科學技術之不斷更新，科技設備儲存及使用、運算方式更是日新月異，若依循傳統立法方式，以特定技術之干預方式作為授權標的，必定面臨立法（修法）速度趕不上犯罪手法及偵查技術之困境，司法院釋字第 443 號解釋理由書所揭示之公法上「層級化法律保留」之概念，可以將其運用在刑事訴訟之干預處分，干預處分之層級化授權理論也因此孕育而生[402]，以因應科技偵查手段不斷發展之立法難題。亦即，著眼於科技偵查法制之長遠發展，適合之立法方式可回歸基本權干預性質暨層級化法律保留原則之理論體系，依照干預處分所干預之基本權性質、程度，予以層級化法律授權暨程序保障，方謂現今科技時代下可長可久之立法方式。

干預處分之層級化授權，是依照干預處分所干預之基本權性質以及強度（包含蒐集資訊能力之強弱、時間長短以及被蒐集資訊之私密性強度等等），決定其層級化保留位階。最輕微者，得援引一般干預處分概括授權條款即可為之，反之，干預處分愈強者，則依其強度層級化之方式提升其授權層級及程序保障密度。

第二項　我國刑事訴訟強制處分之層級化授權

我國現行刑事訴訟法規範之各類干預處分，其實已可見層級化授權之體系架構，從規範最嚴格者依序往下大致可分為絕對法官保留、相對法官保留、檢察官保留及一般概括授權條款等不同層級。絕對法官保留者如羈

[401] 王士帆，科技偵查立法之可行性評估及建議方向（發言紀錄），檢察新論，第 27 期，2020 年 2 月，頁 179。
[402] 林鈺雄，刑事訴訟法（上冊），新學林出版股份有限公司，2019 年 9 月，9 版，頁 312。

doi:10.6342/NTU202301879

押、鑑定留置等對於人身自由侵害之強制處分；相對法官保留原則係指原則經法官同意才可為之，緊急狀況時檢察官可先行為之，事後報請法官核准，例如:干預人民身體、財產與居住自由等基本權之搜索[403]、干預秘密通訊權之通訊監察[404]；至於時間短暫或影響較為輕微之人身自由干預，如傳喚、拘捕、具保責付限制住居等，係採檢察官保留原則；質量輕微之跟監、盯哨等，則可援引一般偵查概括授權條款為法律依據。

另外，我國於民國 108 年 6 月 19 日修正公布之刑事訴訟法第 93 條之 3[405]有關限制出境、出海之法律規範設計，更是我國刑事訴訟法上首見以時間長短造成之干預程度不同而定有不同層級之授權，8 個月以內之限制出境、出海，可由檢察官為之，逾 8 個月者則應有法官核准。

第三項　層級化之基本權利

觀察我國現行刑事訴訟法強制處分體系下有關層級化授權立法脈絡，

[403] 搜索原則上，依刑事訴訟法第 128 條之 1 之規定：「偵查中檢察官認有搜索之必要者，除第一百三十一條第二項所定情形外，應以書面記載前條第二項各款之事項，並敘述理由，聲請該管法院核發搜索票。司法警察官因調查犯罪嫌疑人犯罪情形及蒐集證據，認有搜索之必要時，得依前項規定，報請檢察官許可後，向該管法院聲請核發搜索票。」有急迫情形者，依同法第 131 條第 2、3 項之規定「檢察官於偵查中確有相當理由認為情況急迫，非迅速搜索，二十四小時內證據有偽造、變造、湮滅或隱匿之虞者，得逕行搜索，或指揮檢察事務官、司法警察官或司法警察執行搜索，並層報檢察長。前二項搜索，由檢察官為之者，應於實施後三日內陳報該管法院；由檢察事務官、司法警察官或司法警察為之者，應於執行後三日內報告該管檢察署檢察官及法院。法院認為不應准許者，應於五日內撤銷之。」

[404] 通訊監察原則上，依通訊保障及監察法第 5 條第 2 項之規定「…通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面聲請該管法院核發」。有急迫情形者，依同法第 6 條第 1 項：「有事實足認被告或犯罪嫌疑人有犯刑法妨害投票罪章、公職人員選舉罷免法、總統副總統選舉罷免法、槍砲彈藥刀械管制條例第七條、第八條、毒品危害防制條例第四條、擄人勒贖罪或以投置炸彈、爆裂物或投放毒物方法犯恐嚇取財罪、組織犯罪條例第三條、洗錢防制法第十一條第一項、第二項、第三項、刑法第二百二十二條、第二百二十六條、第二百七十一條、第三百二十五條、第三百二十六條、第三百二十八條、第三百三十條、第三百三十二條及第三百三十九條，為防止他人生命、身體、財產之急迫危險；或有事實足信有其他通訊作為前條第一項犯罪連絡而情形急迫者，司法警察機關得報請該管檢察官以口頭通知執行機關先予執行通訊監察。但檢察官應告知執行機關第十一條所定之事項，並於二十四小時內陳報該管法院補發通訊監察書；檢察機關為受理緊急監察案件，應指定專責主任檢察官或檢察官作為緊急聯繫窗口，以利掌握偵辦時效。」

[405] 刑事訴訟法第 93 條之 3 第 1 項：「偵查中檢察官限制被告出境、出海，不得逾八月。但有繼續限制之必要者，應附具體理由，至遲於期間屆滿之二十日前，以書面記載前條第二項第一款至第四款所定之事項，聲請該管法院裁定之，並同時以聲請書繕本通知被告及其辯護人。」

doi:10.6342/NTU202301879

其最關鍵要素當屬受干預之基本權屬性。人身自由權拘束受到最高密度之保障，接續為秘密通訊權、財產權及居住自由權等，而基於人性尊嚴與個人主體性之維護所發展出之隱私權、一般人格權、資訊自主權，係源於憲法第 22 條概括性補遺條款發展出來，基本權位階應低於憲法明文揭示之基本權利，再加上隱私權、一般人格權、一般行為自由權，均有範圍廣泛，範圍幾乎涵蓋一切生活領域行為之特性，此部分亦有德國法上針對一般人格權保障發展出之「領域理論」[406]可為參考。

「領域理論」將隱私權以同心圓方式進行理解，關於人格權之保護依照涉及個人人格核心之親疏，區分為私密領域(Intimbereich)、私人領域(Privatbereich)與公開領域(Sozialbereich)等三大部分，同心圓中心之「私密領域」屬「私人生活核心領域(Kernbereich privater Lebensgestaltung)」，絕對不可侵犯，但私人領域與公開領域之則非絕對不可侵犯，須依照具體個案情況而定。因此，對於一般人格權而言，因社會環境變遷而被承認為新型態之一般人格權者，其大部分歸屬於公開領域之人格權，故承認其為基本權之最重要意義，主要是當其與其他權利發生衝突時，僅係未自始被排除在權利衝突相互權衡之列而已[407]。

第三節　科技偵查可能涉及之基本權干預

伴隨科技發展而生之新興偵查干預手段，其可能干預之憲法基本權，並不限於憲法明文揭示之固有基本權利，更多情形是涉及從憲法第 22 條所稱之「其他自由及權利」導出之隱私權、一般人格權、資訊自主權等等之干預，德國聯邦憲法法院 2008 年另發展出保障電腦資訊設備私密性及完整性之資訊科技基本權（即 IT 基本權）。

[406]張永明，一般行為自由與一般人格權作為憲法保障之基本權，司法院大法官 106 年度學術研討會-「憲法解釋與憲法上未列舉之權利」第三場報告，2017 年 12 月 2 日，頁 24。
[407] 同上註。

doi:10.6342/NTU202301879

第一項　隱私權及資訊自決權

司法院釋字第 588 號[408]解釋於真調會案中揭示「隱私權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。」

司法院釋字第 603[409]號解釋在按捺指紋案中，再從隱私權衍生個人資料之資訊自決權，揭示人民有決定其個人資料「於何時、何種方式、向何人揭露」之資訊及控制權，更指出政府大量蒐集人格資訊時，法律保留原則應明定其蒐集目的、目的與手段間符合必要性急關聯性、禁止目的外使用，主管機關更應配合當代科技採取必要之防護措施等。是以，從司法院釋字第 603 號解釋當可理解資訊自主決定權之保障內涵為，個人對其資料是否揭露以及如何使用，原則上有權自主決定，而當政府違反其意願將其資訊揭露於他人面前時，則可能構成資訊自主決定權之侵害。

司法院釋字第 689 號解釋在狗仔隊跟追案中，針對隱私權及新聞自由權利之基本權利衝突時，於解釋理由書揭示:「生活私密領域不受侵擾之自由及個人資料之自主權，屬憲法所保障之權利...現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或

[408] 司法院釋字第 588 號解釋：「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，而受憲法第二十二條所保障」

[409] 司法院釋字第 603 號解釋：「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。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。...國家基於特定重大公益之目的而有大規模蒐集、錄存人民指紋、並有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。主管機關尤應配合當代科技發展，運用足以確保資訊正確及安全之方式為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。」

doi:10.6342/NTU202301879

公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。」是以，司法院釋字第 689 號解釋理由書不僅確立個人人格自由發展、一般行動自由、資訊自決及隱私權等基本權利，更點出上開基本權利之侵害，隨著科技之發展，侵擾及保護之程度均應隨之增加。司法院釋字第 689 號解釋理由書所點出之科技發展下基本權利之侵害程度提升之問題，似已隱含承認科技技術對基本權之干擾恐因科技技術進步而「量變導致質變」之意思，然而，迄今我國大法官解釋尚未直接承認下述德國聯邦憲法法院 2008 年後所承認之 IT 基本權。

第二項　資訊科技基本權（IT 基本權）

德國聯邦憲法法院於 2008 年間自遠端搜索（即線上搜索；Online-Durchsuchung）之案件，發展出資訊科技基本權（即 IT 基本權），承認電腦資訊設備之私密性及完整性[410]（Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme）為過去其他基本權利無法涵蓋，而 IT 基本權即因此而生，用以補充其他基本權無法保護之人格高度風險[411]。

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之需求。鑑於不受阻礙之人格發展，人民對國家尊重資訊系統之私密性與完整性具有正當期待與信賴」、「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

[410] 資訊安全領域有所謂之「C.I.A 三原則」（CIA triad），即「機密性」(ConfId.entiality =Vertraulichkeit)、「完整性」(Integrity=Integrität)與「可用性」(Availability=Verfügbarkeit)，德國聯邦憲法法院裁判即意指前兩者(s. Paal/Pauly/Martini DS-GVO, 2. Aufl., 2018, Art. 32 Rn. 35)。並參照我國資通安全管理法第 3 條第 3 款:「資通安全:指防止資通系統或資訊遭受.....侵害，以確保其機密性、完整性及可用性」。註參施育傑，科技時代的偵查干預處分－兼論我國法方向，月旦法學雜誌，第 306 期，2020 年 11 月，頁 157 註 20。

[411] BVerfGE 120, 274.

doi:10.6342/NTU202301879

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；一旦儲存資料系統受到攻擊，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」[412]。

值得注意的是，德國聯邦憲法法院揭示：「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」、「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，將出現保護性漏洞，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」[413]，基此可知，德國聯邦憲法法院是將 IT 權作為補遺性基本權，相對於秘密通訊自由乃德國基本法第 10 條明定、住宅不可侵犯權乃德國基本法第 13 條明定，IT 基本權乃「補充性」之作用，只有在其他基本權保護範圍所不及時，才加以檢驗，以作為填補基本權保護之漏洞[414]。

IT 基本權其所代表之指標性意義，可以從德國法過去針對「來源端通訊監察」可否援引原本通訊監察之法律規定作為授權依據之爭議更清楚理解。德國法過去就上開爭議有肯定說與否定說之爭，肯定說認為「來源端通訊監察」之方式所截取之內容本屬通訊監察所保護之「通訊內容」，干預之基本權只有秘密通訊自由，並未逾越原本通訊監察規定之授權範圍；反對說則認為以「來源端通訊監察」之方式取得通訊內容，除了秘密通訊自由外，還包括電腦資訊設備之私密性與完整性，即屬於 IT 權保護範疇內之額外干預，故反對說論者認為不得援引過去通訊監察之法律授權作為「來源端通訊監察」之干預授權依據，由於德國聯邦憲

[412] BVerfGE 120,274,302；中譯參王士帆，網路之刑事追訴－科技與法律的較勁，政大法學評論，145 期，2016 年 6 月，351 頁。

[413] BVerfGE 120,274,308；中譯參王士帆，網路之刑事追訴－科技與法律的較勁，政大法學評論，145 期，2016 年 6 月，351 頁。

[414] 吳俊毅，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的困境，刑事政策與犯罪研究論文集（23），法務部司法官學院，2020 年，頁 470。

doi:10.6342/NTU202301879

法法院在 2008 年已經承認 IT 基本權，德國立法者為免有違憲爭議，故採否定說，另於刑事訴訟法增訂授權依據[415]。是以，從上開「來源端通訊監察」之立法發展亦能知悉，IT 基本權雖源於秘密線上搜索，但其實際適用範圍並不僅限於單一干預手段，隨著資訊科技之發展，當干預手段所侵害之範圍已觸及「保障資訊科技系統私密性與完整性的一般人格權」範疇時，則有以 IT 基本權之干預予以檢視之必要。

我國司法院釋字 603、631、689 號解釋雖確立了個人資訊自主決定權，然迄今並未承認 IT 基本權為我國憲法所保障之基本權[416]。就此，國內有學者認為，資訊科技設備之私密性與完整性（不可侵犯性）的基本權保障，恐係我國基本權體系與釋憲實務遲早要面對之問題 ，應與否定以一般傳統之通訊監察規定作為其授權依據，應另立授權規定及加強其技術性與程序性擔保[417]，亦有認為德國聯邦憲法法院將 IT 基本權之保護拉到對抗國家干預處分之思考，具有指標意義，因 IT 基本權往後不會僅適用在秘密偵查之議題，資訊科技未來會以何種樣貌深入個人生活領域，永遠無法預知[418]，本文對此亦贊同，隨著資訊科技之發展，個人生活早已與個人資訊設備緊密結合，個人資訊設備內儲存之資料，幾乎等同於具有高度個人人格性之資料庫，而逾越固有憲法基本權利之保護範疇。立法實務上，從法務部 109 年 9 月 8 日公告「科技偵查法」立法草案第三章「設備端通訊監察」之立法說明明白表示「設備端通訊監察是因應網路通訊軟體取代傳統電話通訊方式之變革，過去通訊監察之技術必須更新為在通訊之設備端進行訊息擷取，且此種干預方式除侵害『秘密通訊自由權』以外，另侵害『資訊科技基本權』，故無法援引現行通訊保障及監

[415] 林鈺雄，科技偵查概論：干預屬性及授權基礎(下)，《月旦法學教室》，第 221 期，2021 年 3 月，頁 48 至 49。
[416] 林鈺雄，侵入資訊科技系統之來源端通訊監察，月旦法學教室，第 223 期，2021 年 5 月，頁 18。
[417] 同上註，頁 19。
[418] 王士帆，網路之刑事追訴-科技與法律之較勁，政大法學評論，第 145 期，2016 年 6 月，頁 352。

doi:10.6342/NTU202301879

察法為授權依據，故有另行立法授權之必要性」，已可發現我國行政機關於草擬科技偵查手段相關法律規範時，已有意將德國法上「資訊科技基本權」之概念引進我國。

第四節　國家木馬可能涉及之基本權干預

第一項　來源端通訊監察（小木馬）

第一款　秘密通訊自由與資訊自我決定權之區分

「人民有秘密通訊的自由」為憲法第 12 條揭示之基本權利，人民使用電信通訊時，通訊內容及使用通訊時產生之狀態資料(如通訊參與者、起迄時間、通訊長度等)均屬憲法第 12 條秘密通訊自由權之保護範圍，業經司法院釋字第 631 號解釋中揭示「秘密通訊自由是憲法保障隱私權的具體態樣之一，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。為維護人性尊嚴、個人主體性及人格發展之完整，並未保障個人生活私密領域，免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利」。從而，以來源端通訊監察之干預方式取得進行中之加密之通訊內容及通訊相關狀態資料，核屬對憲法第 12 條秘密通訊自由權之干預。

又我國司法院釋字第 603、689 號解釋自憲法第 22 條之「其他自由及權利」概括性補遺條款發展出個人資訊自主決定權，我國最高法院針對秘密通訊自由權之保障範圍，係以「進行中通訊」為限，針對「過去已結束」之通訊內容，認非秘密通訊自由保護之客體，應僅受一般隱私權即個人資料自主控制之資訊隱私權所保護[419]。前開實務見解與德國聯邦憲法法

[419]「通訊隱私權保護之主要緣由，乃通訊涉及兩個以上參與人，意欲以秘密之方式或狀態，透過介質或媒體，傳遞或交換不欲為他人所得知之訊息。因其已脫離參與人得控制之範圍，特別容易受國家或他人之干預與侵擾，有特別保護之必要，故其保障重在通訊之過程。另上揭通訊之本質

doi:10.6342/NTU202301879

院判決認定受秘密通訊自由權保障者必須是進行中的通訊(die laufende Telekommunikation)之見解相同[420],惟德國聯邦憲法法院 2009 年針對已讀取而繼續保留在伺服器之電子郵件,認為仍受秘密通訊自由保護,惟得依扣押手段取得電子郵件[421]。

我國固有針對「通訊監察」干預手段是侵害秘密通訊自由權或是資訊自主決定權之區分方式,在網路通訊已改變過去傳輸方式之今天受到了挑戰。來源端通訊監察係針對加密之網路通訊內容,網路通訊之傳輸方式,有別於傳統電信,係透過去中心化之網際協議通話技術(VoIP),將語音切割成資料封包,不經中央伺服器,透過網路自行搜尋最近路徑,傳送至受話方,達成語音通話,這種以通訊參與者雙方為收受源的端點對端點傳輸[422]。而加密技術則是當發送端將資料傳給接收端時,資料於傳輸過程中經過複雜之密碼學進行加密,於缺乏金鑰且破解密碼實際可行性之狀態下,只能在通訊內容「加密前」或是「解鎖後」透過植入木馬程式之方式取得,因加密技術造成過去透過於傳輸過程中「截收」方式進行之通訊監察已無用武之地。

分析網路通訊之傳輸架構,大致可區分為「存儲狀態」以及「傳輸過程」二種情形,存儲狀態包含(通訊內容暫存於載體或網際網路應用服務供應商之階段)、傳輸過程則包含(從載體與網路應用服務供應商之傳輸,

係涉及兩個以上參與人間之意思交換之旨,故通訊隱私權實有別於一般隱私權,一般隱私權並不當然涉及個人以外之他人,即便僅個人一人,亦能主張此一憲法權利,如個人在住家之活動、身體之私密部位、書寫之日記,均為一般隱私權所保護之對象,然此皆與通訊隱私權無涉。秘密通訊自由所保護者,既係在於通訊參與人間之訊息得以不為他人知悉之方式往來或遞送之秘密通訊過程,其所保障之範圍,自應隨訊息送達接收方,傳遞過程結束而告終止,據此,通訊內容在傳遞過程中固為秘密通訊自由所保護之客體,如該通訊內容已處於接收方之支配範圍,接收方得對此已結束傳遞過程之通訊內容,自行決定留存或刪除等處理方式,則其秘密通訊自由之保障已經結束,換言之,所謂『過去已結束』之通訊內容,已非秘密通訊自由保護之客體,應僅受一般隱私權即個人資料自主控制之資訊隱私權所保護。」(最高法院 106 年度台非字第 259 號判決理由參照)

[420] BVerfG, Urt. V. 02. 03. 2006 – 2BvR 2099/04= BVerfGE 115, 166, 184.

[421] BVerfGE, 124, 43, 56.

[422] 王士帆,德國科技偵查規定釋義,法學叢刊,第 262 期,2021 年 4 月,頁 95。

doi:10.6342/NTU202301879

以及網路應用服務供應商間之資料傳輸階段）[423]，故秘密通訊自由權與資訊自我決定權之區分，係著眼於訊息若已達接收人可得支配範圍，通訊因空間距離出現特殊危險狀態（即「通訊設備之傳輸過程脫離通訊者的支配範圍，以致訊息內容之秘密性易受第三人或國家侵擾」）不復存在，故當「過去已結束」之通訊內容已處於接受人之支配範圍，其對於訊息內容已可支配，訊息不再處於通訊過程脆弱性之特殊危險狀態，也就失去秘密通訊自由權之特別保護必要[424]，而落入資訊自我決定權之保障範疇。

觀諸來源端通訊監察之干預手段介入之時間點，係為因應資料於傳輸過程中加密，提前或延後至「加密前」或是「解鎖後」之與通訊「開始」與「結束」幾乎同一瞬間發生之時點，解釋上可理解為與通訊「開始」與「結束」之時點同時發生，從而本文認為應仍符合秘密通訊自由權所欲保障之範圍內。

至於來源端通訊監察實務操作可能尚包含 2 種必定發生之特別情形，其一是木馬植入及啟動均需一定作業時間，而其所需期間更會依植入方式及順利與否而不一，從而實際執行時令狀開始時間至木馬程式實際啟動作用（即德國刑事訴訟法第 100a 第 1 項第 3 句規範情形）應存在一段時間落差；第二種情形是偵查機關實施傳統通訊監察後發現監察所得資料均經加密傳輸，偵查機關事後向法院取得令狀，針對「本來得以通訊監察手段」之資料為「假設替代干預」（hypothetischer Ersatzeingriff），以此方式取得「本來應該可以取得卻未取得之資料」[425]。而上開兩種特殊情形，均係針對通訊已結束而保留在通訊載體內之通訊內容，即為個人資料

[423] 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研究所碩士論文，2019 年，頁 75

[424]王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 92；張麗卿，監察網路通訊作為抗制犯罪手段之原則及界線，輔仁法學，第 57 期，2019 年 6 月，頁 180

[424] 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研究所碩士論文，2019 年，頁 75

[425]同上註，頁 87

doi:10.6342/NTU202301879

自主決定權即資訊隱私權所保護範疇，倘依照傳統通訊監察之區分方式，本應透過保全扣押之干預手段取得之範圍，然因保全扣押缺少秘密偵查及對抗加密之特性，故一併將其列為來源端通訊監察干預手段之射程範圍，應具有填補可能執法漏洞之意義。

第二款　資訊科技基本權

來源端通訊監察係透過植入國家木馬之方式進行干預，是除了傳統秘密通訊自由權以及個人資訊自主決定權以外，德國聯邦憲法法院在2008年間自遠端搜索（即線上搜索；Online-Durchsuchung）之案件，發展出資訊科技基本權（即IT基本權），承認電腦資訊設備之私密性及完整性為過去其他基本權利無法涵蓋，我國司法院釋字603、631、689號解釋雖確立了個人資訊自主決定權，然迄今尚未承認IT基本權為我國憲法所保障之基本權[426]。然而，觀察國內學界及立法實務之發展，不僅學界普遍認為資訊科技設備之私密性與完整性（不可侵犯性）的基本權保障，係我國基本權體系與釋憲實務遲早會面對的問題，不可援引一般傳統之通訊監察之法律規定作為來源端通訊監察之授權依據，應另立授權規定及加強其技術性與程序性擔保[427]，立法發展上，亦可從科技偵查法草案第三章有關設備端通訊監察之立法說明，立於設備端干預及其基本權干預屬性包含對資訊科技基本權之干預，故有另立授權依據之必要，應可推知我國學界及實務已逐漸往承認資訊科技基本權之方向靠近。

第二項　秘密線上搜索（大木馬）

在討論秘密線上搜索可能干預之基本權利之前，有鑑於本文前所介紹各國有關秘密線上搜索之規定，其授權國家木馬之功能範圍不盡相同，除了原始型「針對存儲內容取證（如電腦搜索檢視）」，尚有部分國家之秘

[426] 林鈺雄，侵入資訊科技系統之來源端通訊監察，月旦法學教室，第223期，2021年5月，頁 18。
[427] 同上註，頁19。

doi:10.6342/NTU202301879

密線上搜索包含「使用行為監察（如紀錄受干預人瀏覽之網頁）」與「外部行為監察（遠端打開麥克風、鏡頭等進行監察）」等不同模式、強度之干預[428]，再加上我國現行刑事訴訟制度，無論是法制面尚未肯認線上搜索之干預處分，實務面亦未使用秘密線上搜索之偵查手法，再討論秘密線上搜索可能干預之基本權之前，應先就本項探討之線上搜索干預處分之功能明確區分並予以界定。

第一目 德國刑事訴訟法第 100b 條線上搜索

德國刑事訴訟法第 100b 條線上搜索之範圍，以條文文義解釋，「由該系統取得資料」僅授權偵查機關可以透過植入木馬之方式秘密取得受入侵資訊科技系統之資料，並不允許以主動方式製造資料，例如：秘密啟動麥克風、攝影機等功能進行資料蒐集，易言之，只允許偵查機關以被動方式探知訊息，不得主動開啟受干預系統之功能[429]。申言之，若性質屬於「外部行為監察」之資料主動製造與取得，並不在德國刑事訴訟法第 100b 條線上搜索範圍內。至於介於其中之「使用行為監察」，則可依是否涉及傳輸通訊內容，可分為「單純使用行為監察（如瀏覽網頁監察）」或「傳輸過程來源端通訊監察」，依照德國刑事訴訟法第 100b 條立法理由中提及「線上搜索不僅得對於新產生之通訊內容進行監察，而更可以對於資訊科技系統內所有存儲內容與使用行為進行監察」[430]，應可認為「單純使用行為監察」以及「傳輸過程來源端通訊監察」，應屬德國刑事訴訟法線上搜索之授權範圍內。

第二目 英國調查權力法之設備端干預

[428] 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研究所碩士論文，2019 年，頁 230。
[429]王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月，頁 103
[430]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研究所碩士論文，2019 年，頁 235。

doi:10.6342/NTU202301879

不同於德國刑事訴訟法第 100b 條將線上搜索之授權範圍排除「外部行為監察」，英國調查權力法（IPA）第 5 部分之設備端干預「A Targeted Equipment Interference Warrant」以及第 6 部分第 3 章之「Bulk Equipment Interference Warrant」，依照 2018 年英國內政部公布之設備端干預操作規範（EQUIPMENT INTERFERENCE Code of Practice）[431]第 3.2、3.3 針對「設備端干預」之定義為「設備端干擾權限是使用一系列技術，以遠端或物理設備交換之方式，從設備端獲取通信內容（communications）、設備數據（equipment data）或其他訊息（any other information）。」、「設備干擾包含不同複雜程度之操作方式，低度為在無人看管的情況下秘密地從對象的設備中下載數據，或者使用對象之登錄憑證訪問其電子設備之保存數據。更複雜的設備干擾操作可能涉及利用軟體現有漏洞，以獲得對設備或網絡的控制權，以遠程搜索資料或監視設備的用戶。」是以，從英國調查權力法有關設備端干預之定義可知，其以單一授權方式包括大木馬、小木馬，更擴及德國刑事訴訟法第 100b 條線上搜索未允許之「外部行為監察」。

第三目　荷蘭第三部電腦犯罪法之國家木馬

荷蘭第三部電腦犯罪法修正刑事訴訟法第 126nba、126uba 及 126zba 節有關國家木馬之授權規定，該法授權執法機關基於調查嚴重犯罪之目的，可以合法透過遠端植入木馬之方式截取加密資訊，透過設備或相互連接之系統，以程式對犯罪嫌疑使用中之電腦數據（如電腦、手機、伺服器等）進行自動化處理，依照第三部電腦犯罪法解釋性備忘錄所載，新法施行後可以透過遠端打開麥克風、鏡頭等方式對特定使用者身分、系統進行監視，其授權範圍與英國調查權力法相同，均包含「外部行為監察」。

[431] UK Government Home Office, 'Equipment Interference Code Of Practice' (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, last visited 07/02/2023.

doi:10.6342/NTU202301879

第四目　秘密線上搜索可能干預之基本權

當秘密線上搜索之功能界定為「透過植入木馬之方式秘密取得受入侵資訊科技系統之資料」時，最至為相關之憲法基本權，當屬德國聯邦憲法法院在 2008 年間，自遠端干預（即線上搜索；Online-Durchsuchung）之案件，發展出資訊科技基本權（即 IT 基本權）。有關干預強度之部分，有鑑於個人資訊科技系統儲存所有來自使用者之多元資訊，而線上搜索得以輕易、暗中描繪資訊科技系統使用者的個人人格圖譜，任何資訊科技使用者均可成為國家科技偵查眼裡的透明人[432]，故秘密線上搜索應認為屬於對於人格權最為嚴重之干預手段。

當秘密線上搜索之功能包含外部行為監察(如英國、荷蘭之國家木馬）時，其不僅係秘密取得個人儲存於資訊科技系統內之資料，尚包含秘密對於可能隱私權最核心部位之私宅內進行監聽、監視，此種情形即可能該當隱私權核心領域之干預。

惟不論係功能僅限於「透過植入木馬之方式秘密取得受入侵資訊科技系統之資料」者，抑或包含「外部行為監察」之功能，前者之干預強度在德國法上已認與德意志聯邦共和國基本法第 13 條第 3 項住宅監聽相當[433]，屬現行德國法上強度最強之干預處分。又住宅監聽在德意志聯邦共和國基本法第 13 條第 3 項至第 6 項[434]有明文規定該有之程序保障，於德國

[432]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 12 月，頁 217。

[433]林鈺雄，科技偵查概論：干預屬性及授權基礎(下)，《月旦法學教室》，第 221 期，2021 年 3 月，頁 51；施育傑，數位、科技與刑事程序干預處分-資訊框架理論之建構，2020 年政治大學博士論文，181 至 184 頁；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 12 月，頁 198 至 215。

[434] 德意志聯邦共和國基本法第 13 條
第 3 項
根據事實懷疑有人犯法律列舉規定之特定重罪，而不能或難以其他方法查明事實者，為訴追犯罪，得根據法院之命令，以設備對該疑有犯罪嫌疑人在內之住所進行監聽。前開監聽措施應定有期限。前述法院之命令應由三名法官組成合議庭裁定之。遇有急迫情形，亦得由一名法官裁定之。
第 4 項

doi:10.6342/NTU202301879

採用最高層級之「憲法保留」之基本權保障。

第五節 我國科技偵查整體法制落後之困境

我國現行有關刑事訴訟干預處分之法律規定，均尚未有科技偵查相關立法，相較於本文第三章介紹之立法先進國家自 2016 年後紛紛推出新一波對抗加密之立法，以補足過去解密令狀或是國家木馬不足之處，我國甚至對於干預程度較國家木馬輕微之 GPS、M 化車等科技偵查方法，均尚未有法律明文規範，立法進度不僅未能跟上世界潮流，國內法制面與實際執法面之嚴重落差，更已 2 度經最高法院判決認定違反法律保留原則，並對立法機關發出嚴正呼籲。

第一項 GPS 案

我國最高法院 106 年度台上字第 3788 號判決[435]，認定司法警察 GPS

為防止公共安全之緊急危險，特別是公共危險或生命危險，唯有根據法院之命令，始得以設備對住所進行監察。遇有急迫情形，亦得依其他法定機關之命令為之；但應立即補正法院之裁定。

第 5 項

僅計畫用以保護派至住所內執行任務之人而為監察者，得依法定機關命令為之。除此之外，由此獲得之資料，只准許作為刑事訴追或防止危險之目的使用，唯須先經法院確認監察之合法性；遇有急迫情形，應立即補正法院之裁定。

第 6 項

聯邦政府應按年度向聯邦議會報告有關依前三項規定執行監察之情形。由聯邦議會選出委員會根據該報告進行議會監督。各邦應為同樣的議會監督。

[435] 「偵查係指偵查機關知有犯罪嫌疑而開始調查，以發現及確定 犯罪嫌疑人，並蒐集及保全犯罪證據之刑事程序。而偵查既 屬訴訟程序之一環，即須依照法律規定行之。又偵查機關所 實施之偵查方法，固有『任意偵查』與『強制偵查』之分， 其界限在於偵查手段是否有實質侵害或危害個人權利或利益 之處分而定。倘有壓制或違反個人之意思，而侵害憲法所保 障重要之法律利益時，即屬『強制偵查」，不以使用有形之強制力者為限，亦即縱使無使用有形之強制手段，仍可能實質侵害或危害他人之權利或利益，而屬於強制偵查。又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，自不得假借偵查之名，而行侵權之實。查偵查機關非法安裝 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 23 0 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，僅係有關偵查之發動及巡防機關人員執行犯罪調查職務時，視同刑事訴訟法第 231 條司法警察（官）之規定，自不得作為裝設 GPS 追蹤器偵查手段之法源依據。 而原判決復已依據卷證資料詳細說明警察職權行使法第 11 條第 1 項之規定，如何不得作為被告安裝 GPS 追蹤器偵查之依據 ，且被告事前亦未立案調查或報請長官書面同意，在無法律 授權下，擅自藉口犯罪偵查，自行竊錄蒐證，不能認為有法律上之正當理由。因認被告並無法律授權，即透過 GPS 追蹤器蒐集告訴人車輛位置等資訊，嚴重侵害告訴人之隱私權， 且無法律上之正當理由，業已構成刑法第 315 條之 1 第 2 款「 無故」之要件，核無不合。檢察官上訴徒憑己意，漫指安裝 GPS 追蹤器之作為，應屬偵查作為，屬於依法令

doi:10.6342/NTU202301879

追蹤器為犯罪偵查，將 GPS 裝設在犯罪嫌疑人車輛底盤，定位追蹤犯罪嫌疑人之位置，因缺乏法律授權，屬違法偵查不被允許，並於判決書末段對立法權做出呼籲「至 GPS 追蹤器之使用，確是檢、警機關進行偵查之工具之一 ，以後可能會被廣泛運用，而強制處分法定原則，係源自憲法第 8 條、第 23 條規定之立憲本旨，亦是調和人權保障與犯罪真實發現之重要法則。有關 GPS 追蹤器之使用，既是新型之強制偵查，而不屬於現行刑事訴訟法或其特別法所明定容許之強制處分，則為使該強制偵查處分獲得合法性之依據， 本院期待立法機關基於強制處分法定原則，能儘速就有關 GPS 追蹤器使用之要件（如令狀原則）及事後之救濟措施，研議制定符合正當法律程序及實體真實發現之法律，附此敘明」，為我國司法實務判決首次針對立法規範科技偵查手段以符憲法規範發出警告。

第二項　M化車案

桃園地院 106 年度易字第 164 號[436]M 化車案件中，認定人民之一般行為自由、生活私密領域不受侵擾及個人資料之自主、隱私等權利，均屬憲

之行為云云 ，自與法律所規定得上訴第三審之理由不相適合。」（最高法院在 106 年度台上字第 3788 號判決意旨）

[436] 「使用「M 化車」之偵查作為造成基本權干預：依據前述「M 化車」之作用，可知其原理係利用「虛擬基地台」的方式，透過已知的 IMEI 或 IMSI，藉「M 化車」與目標設備之間的訊號連結，進而定位目標設備，藉此定位所欲偵查之對象。該定位科技方法，係藉訊號之強弱連結以探知資訊，其實際發動之時間乃取決於偵查機關，且不分目標係在何處（私人住宅或公開場所）而有異，因而導致目標設備、對象所在之位置資訊，不限時間、地點，均得由偵查機關透過「M 化車」之使用，持續達到定位追蹤以及蒐集、處理與利用該等資料之目的。縱不論上述偵查手段亦不可避免地必須將第三人系統內之識別資訊納入（但不會「連結辨識第三人資料」，且「於系統關閉後即自動清除」，如前所述），前述「M 化車」使用之結果，已對目標對象之前揭基本權，造成並非輕微的干預。」；「M 化車」使用的原理，係為定位追蹤，而藉由虛擬基地台與目標通訊設備之間的直接訊號強弱連結，據以特定目標對象位置。此科技偵查之干預措施，雖有「利用」通訊設備、技術，但並「非」國家介入通訊參與者之間「秘密通訊狀態（過程）」的干預處分。況且，「M 化車」之使用，既係以虛擬基地台「直接」連結目標　　對象訊號、即時性地定位追蹤，亦與向第三人即電信事業「調取」過去通聯紀錄的類型不符。準此，「M 化車」之使用，無從引用上述「調取通聯條款」作為授權依據。綜上，「M 化車」的干預處分，並無「法律」授權。」；「本案『M 化車』之使用，既然根本性地欠缺法律授權，則警方據此測點、獲知者（即偵查報告記載鎖定特定序號、門號的資訊），倘若作為證據使用，等同由本院認同違反法治國基本原則的干預處分（況本案警方出動「M 化車」本身，也沒有試圖、或實際取得任何檢方核准或法院令狀）。從而，依前述憲法、法律之相關說明，基於法治國、法律保留原則之誡命，本案因『M 化車』直接取得之證據（資訊）應認無證據能力，不得作為證據使用。」（桃園地方法院 106 年度易字第 164 號判決意旨）

doi:10.6342/NTU202301879

法第 22 條保障個人人格自由發展之基本權保護範圍，而 M 化車對於目標設備、對象所在之位置資訊，不限時間、地點，持續定位追蹤以及蒐集、處理與利用該等資料，係屬對於上開基本權之侵害，屬偵查干預手段，而 M 化車之相關使用規範僅有「執行 M 化定位勤務作業流程」，並無法律層次的規定，故認定「M 化車」的干預處分，並無「法律」授權，而該案中因「M 化車」直接取得之證據，則因違反法律保留原則，無證據能力。

本案上訴二審後，二審臺灣高等法院 109 年度上易字第 1683 號判決[437]推翻一審見解，認 M 化車僅具「訊號定位」功能，無法顯示地址或精確定位、亦無行為人行動影像或對話內容，並不會顯示與隱私有關的內容，警方基於保護公共利益之目的為之，依刑事訴訟法第 158 條之 4 規定予以

[437]「法的闡述與適用，不能僅有人權保障的廣度，也須同時把握憲法的高度。隱私權之保護並非絕對，仍須與憲法保護之其他權利、所欲追求的價值與公益要求等等，綜合判斷，合理權衡。一般人跟追行為，只要綜合考量跟追目的，行為當時之人、時、地、物等相關情況，以及對被跟追人干擾程度等因素，合理判斷具有正當理由者，即不被評價為違法。新聞採訪者於有事實足認特定事件之報導具一定公益性，而屬大眾關切並具有新聞價值者（例如：犯罪或重大不當行為之揭發…等）如須以跟追方式進行採訪，且跟追行為依社會通念非屬不能容忍，該跟追行為即具有正當理由而不受處罰。（3）綜上，司法院釋字第 689 號解釋正足以正當化警察機關接獲被害人報案，調取被害人使用門號與犯嫌所用人頭門號相關通聯紀錄、申登人資料，並於分析申登人申辦之所有門號、搭配使用之序號 IMEI 碼及通聯紀錄顯示之基地台位置之後，發現涉案門號通聯之基地台位置均位於特定幾個地址，於是將上述門號申登人申辦的門號及搭配使用的序號，鍵入「M 化車」在上述幾個特定基地台位置周邊測點，偵查犯罪，具有正當性；換言之，治安機關對於有事實足認有特定犯罪嫌疑之犯罪行為，因偵查犯罪之需要，而採用現代科技設備，如對隱私權並未構成重大、不合比例之侵害，也未逾越依社會通念所認不能容忍的界限，即屬該號解釋意旨所揭示：符合憲法第 23 條之比例權衡原則。」、「現今犯罪手法日益翻新、設備日新月異，檢警職司保護社會大眾人身自由財產安全，相較於作奸犯科的少數犯罪人，安分守己的社會多數大眾，應是期待偵查犯罪機關有足夠的能力、設備，打擊犯罪。本案查獲過程，並非僅只依靠 M 化車；其實是先依被害人報案、提供通訊電話資訊、調閱監視器、進行人臉辨識、查調通聯記錄、分析時間順序、基地台，然後才向市刑大及檢察官聲請調取票，才使用 M 化車配合偵查。並且 M 化車僅僅是以訊號定位，無法顯示地址，也無精確定位、並無行為人行動影像或對話內容，好比災難生存跡象搜索的訊號顯示，究其實質並無妨害秘密可言；何況，M 化車顯示龍潭中興路、國聯街附近訊號最強，警方並未因此逕行逮捕，因 M 化車並不顯示地址，警方是依訊號埋伏，發現上址有異常的大量餐盒進出、停放於該址附近之特定車輛駕駛進入上址，該車輛李姓車主曾涉及詐騙集團案件經移送偵辦，核屬員警依據專業判斷，認定此址是犯罪集團聚集管理的場所，因此聲請搜索票。取得搜索票之後，警方仍持續埋伏，發現多人進入、車輛聚集，依專業敏銳判斷時機已成熟，才進行搜索。查獲過程，M 化車的訊號定位系統只是將警方已知的犯罪地點加以限縮，並且如上述，M 化車定位並不會顯示與隱私有關的內容。新聞報導尚且得因特定事件報導、揭發犯罪行為，具有一定公益性，屬於大眾關切並具有新聞價值，即認具有正當理由；何況，警方使用 M 化車是為偵查已經發現的犯罪行為，保護公共利益，基於公益的合理權衡，依刑事訴訟法第 158 條之 4，應認 M 化車的偵查作為，具有證據能力。」（臺灣高等法院 109 年度上易字第 1683 號判決理由參照）

doi:10.6342/NTU202301879

權衡後，認定 M 化車的偵查作為，具有證據能力。本案嗣經被告提起上訴，最高法院於 111 年 11 月 17 日做出 110 年台上字第 4549 號判決[438]，再次推翻二審見解，認定 M 化車雖無取得手機使用者因通訊附隨產生之資料而無造成秘密通訊自由權之干預，然 M 化車所取得之手機識別碼及位置資訊，均係可連結辨識與該手機使用者相關個人資料之中介資訊，而屬憲法第 22 條所保障隱私權及資訊自主權之範圍，依憲法第 23 條所揭示之法律保留原則，「強制偵查」必須以法律或法律授權明確規定者，始得為之，執法機關僅依行政機關訂定之作業流程作為依據，非法律位階，難謂適法。

我國司法實務上針對司法警察機關使用科技偵查手段進行合憲性檢視之判決雖然不多，然隨著科技偵查手段使用之日益頻繁，其對於基本權干預之議題日益受到重視，應可想見未來在個案中遭受檢視之可能性將日益升高。而無論是最高法院在 GPS 判決中明示立法授權之必要性，抑或 M 化車是否對於隱私權造成侵害之爭議，均清楚可見科技偵查立法之必要性與急迫性，更遑論目前世界各國法律授權執法機關可使用之科技偵查手段，另包含來源端通訊監察、線上搜索等技術層級、權利侵害更重大且複雜之領域，未來科技偵查手段之合憲性爭議僅會更加頻繁及嚴重。然而，反觀我國之立法進度，法務部雖曾於民國 109 年 9 月公告科技偵查法立法草案，然因引發「政府擴權」、「全民監控」等爭議而予以暫緩。但是，無法迴避

[438] 「警方使用『M 化車』蒐證取得手機 IMEI、IMSI 及位置等資訊，並非手機使用者因通訊附隨產生之資料，而係手機與『M 化車』等科技設備間自動連結傳輸之技術訊號，該資訊均不具有人際間表達或交換意見等通訊應有之特徵…並非秘密通訊自由保障之範疇。惟『M 化車』所截收之 IMEI 及 IMSI 等識別碼，如同手機及門號 SIM 卡之身分證號碼，因電信業者有通訊使用者（即行動電話門號之申辦人）之資料，電信業者在行動通訊網路中即藉由該識別碼辨識通訊使用者之身分。而警方取得手機識別碼，既可依規定向電信業者調取該識別碼之電信門號及使用者資料，亦可藉由『M 化車』系統與該手機連結訊號之強弱而偵測該手機位置資訊，進而探知手機使用者所在位置，故『M 化車』所取得之手機識別碼及位置資訊，均係可連結辨識與該手機使用者相關個人資料之中介資訊，而屬憲法第 22 條所保障隱私權及資訊自主權之範圍。…內政部警政署刑事警察局雖已訂定『執行 M 化定位勤務作業流程』，作為執行操作之依據，惟該規定並非經立法機關授權所訂定，非屬法律層次之規定，亦不得作為本件『M 化車』強制偵查作為之法律授權基礎。是本件警方依該作業流程使用『M 化車』之強制偵查作為，欠缺法律授權基礎，違反法律保留原則，尚難謂適法。」（最高法院 110 年度台上字第 4549 號判決理由參照）

doi:10.6342/NTU202301879

之問題乃係無論是科學技術之發展或是人類生活（包含犯罪活動）跟隨科技進步之快速變化均從未停歇，世界各國針對科技偵查立法腳步持續進行，此從本文第三章所列舉世界多個先進國家有關科技偵查立法浪潮，已清楚可見，而加密技術發展對於國家犯罪偵查權行使之衝擊日益嚴重，科技偵查之立法，究屬擴權？亦或限權？實屬一體兩面，法治國原則下法律不僅係賦予權利，更係權力節制規範，倘若科技偵查係必然之趨，在法治國原則之下，當無不立法、不面對之選項。

第三項 科技偵查法草案介紹

我國最高法院 106 年度台上字第 3788 號判決本於憲法所揭櫫基本權干預應恪遵法律保留之基本原則，針對執法機關使用 GPS 進行犯罪偵查因屬於人民隱私權侵害之干預手段，欠缺法律明文授權之前係屬違法偵查不可使用開出示警第一槍後，媒體相繼報導上開判決未來恐影響辦案[439]，然而，轉眼多年已過，我國立法進程仍牛步，其中遭遇諸多立法障礙雖屬主要原因，然而觀察本文前面所介紹之英國、德國、法國、荷蘭、澳洲等國立法過程也不難發現，科技偵查因涉及國家對人民基本權利之干預，再加上網路自由、科技發展及秘密偵查等議題，均與民主法治國家所秉持之基本信念至為相關，不免牽動立法敏感神經，前開國家於立法過程中同樣遭遇諸多阻礙。

我國現行與科技偵查相關之立法進度，僅有法務部於 109 年 9 月 8 日曾公告「科技偵查法」立法草案，此乃我國首次針對偵查機關現行及未來可能實施之科技偵查干預處分嘗試透過立法方式明定授權依據及相關規範，可惜的是草案預告後隨即遭遇各界強烈批評及質疑，致使草案

[439] 裝 GPS 偵查犯罪 判侵害隱私，自由時報，2017 年 12 月 10 日，https://news.ltn.com.tw/news/focus/paper/1156843，最後瀏覽日 2021 年 12 月 28 日；驚！最高法院首度表態　用 GPS 辦案違法，蘋果日報，2017 年 12 月 10 日，https://tw.appledaily.com/local/20171201/RW5D6EQAY3GQIMUZRMXZ4OO5RI/，最後瀏覽日 2023 年 6 月 28 日。

doi:10.6342/NTU202301879

火速「進廠維修」持續研議中。

法律保留原則既為我國憲法第 23 條所揭示基本權干預之憲法基本原則，是以在法治國基礎上應予思考者應是，我國是否要讓執法機關使用科技設備或技術進行秘密偵查？倘若答案是肯定，則必然推導出進行科技偵查之立法為唯一途徑，第二層思考才會進入法律授權範圍應包含哪些科技偵查手段，此時常見之質疑包含「國家木馬是對人民進行監控？」、「科技偵查法是國家威權再現？」，然而，如同本文前述所介紹之諸多立法先進國家早已針對加密技術提出相對應之立法因應對策，在數位科技發展已徹底改變人類生活方式之今日，通盤抵制因應時代變遷之立法反而會促使國家遁入無「法」遵循之路。

再觀實務面，目前尚未有法律明文授權之科技偵查手段中，已有我國執法實務上已實際使用多年者，如被譽為「破案神器」之 M 化車，已多次因在社會矚目案件發揮關鍵功效而登上新聞，如：臺北市峨眉停車場雙屍命案陳姓槍手 2015 年在犯案後逃亡 14 日後，警方透過M化車定位之方式鎖定陳姓犯嫌所在地，成功逮捕逃亡中之陳姓嫌犯[440]；2020 年高雄 14 歲少女北上失蹤，警方亦是透過 M 化車定位之方式，終使失蹤少女成功獲救，防止憾事發生。媒體輿論面對社會矚目案件時，大多只問「破案」與否不問過程，媒體對於 M 化車「立功」多採正面肯定之報導，社會大眾也普遍贊同科技執法對治安帶來的正向效果，在此氛圍底下，社會大眾能否接受執法機關在維護治安之關鍵時刻，縱使擁有科技執法之工具及能力，卻以「缺乏立法授權」為由而拒絕使用？或是警方基於破案及輿論之壓力使用，卻要求執法人員應自行承擔後續可能之侵權後果？甚至因使用科技偵查技術影響證據能力進而導致個案無法實現司法正義？無論是上述哪

[440] M 化定位車立功　鎖定陳福祥上色情網站搭訕「正妹」，ETtoday 社會新聞，ETtoday 新聞雲，2015 年 1 月 15 日，https://www.ettoday.net/news/20150125/458423.htm#ixzz7FP2z8fri，最後瀏覽日 2023 年 6 月 30 日。

doi:10.6342/NTU202301879

一條路，想必都並非全民得以接受。準此，對於科技偵查手段立法予以明文授權並明定其要件及程序規範，身為民主法治國的我國，基於法治國原則下，已是必然之趨。

法務部於 109 年 9 月 8 日公告「科技偵查法」立法草案共有七個章節，包含：總則（草案第一章）、秘密監視、攝錄與追查位置（草案第二章）、設備端通訊監察（草案第三章）、數位證據蒐集與保全（草案第四章）、救濟（草案第五章）、罰則（草案第六章）及附則（草案第七章）。以下就科技偵查法草案說明如下：

第一款　秘密監視、攝錄與追查位置（草案第二章）

草案第二章之立法架構，係先以「隱私空間」及「非隱私空間」予以區分，依照草案第 2 條第 2 款及第 3 款之規定，隱私空間定義為「住宅、建築物、交通工具或其他具有隱蔽設施之地上物之內部空間，且具有隱私或秘密之合理期待者」；非隱私空間定義為「前款以外之空間」。屬於對於「非隱私空間」之秘密偵查行為（包含監看、與聞、測量、辨識、拍照、錄影）可依草案第 3 條之「一般基礎性規範」為之，又依草案第 3 條之立法說明「至於為治安或預防危害等目的進行之監看、錄影等作為，則係依警察職權行使法及其他法律規定為之」，是以，草案第 3 條可謂針對非隱私空間進行秘密偵查行為之一般授權規定。第 4 條相較於第 3 條規定，係針對「空中實施前項調查時」，依第 4 條立法理由可知，因高空實施監看、拍照、錄影之「無人機」、「空拍機」等，範圍較廣、長期實施基本權侵害程度也愈高，故認有另以第 4 條另立規範之必要。草案對於「長期」監看係以 30 日為區隔，30 日以內之高空監察，司法警察即可為之，累計期間逾 30 日者，應報請檢察官下許可後續行之。

草案第 5 條規定「實施位置追蹤調查」之科技偵查手段，依本條草案立法說明，本條規範之科技偵查手段包含目前常見之全球定位系統（GPS）、

doi:10.6342/NTU202301879

行動電話軟體定位、定位偵防車（M 化車）、物聯網等，然因科技日新月異，未來用於追蹤位置之設備或技術當不僅限上述幾種，故立法理由說明「本條係針對實施追蹤位置調查之程序，而非針對特定設備或技術進行規範」。依草案第 5 條之規定，「實施位置追蹤調查」之科技偵查係採檢察官保留原則，實施期間累計逾 2 個月應聲請法院許可。

草案第 6 條規定許可書應記載事項，其中「使用之科技設備或技術」及「裝設前款科技設備或技術之方法」為許可書應記載事項，依草案立法說明「因追蹤位置之設備或技術眾多，許可書應將實施之特定設備或技術載明之」、「又為實施調查，可能有必要在特定場域裝置設備，例如汽車內，此時應由執行機關敘明須以此方式裝置設備或技術，經法院許可後，始可為之」。

草案第 7 條為「緊急實施位置追蹤調查」之規定，針對有必要實施實施位置追蹤調查且情況急迫時，草案規定得由司法警察逕行實施，並於 3 日內報請檢察官許可之。

草案第 8 條將「實施位置追蹤調查」事後通知之程序保障規範，延續第 5 條以 2 個月為法官保留之區分方式， 2 個月內之短期追蹤位置調查，依第 5 條之規定，係採檢察官保留原則，實施完畢後應陳報許可調查之檢察官，逾 2 個月之實施位置追蹤調查，採法官保留原則，結束後應陳報法院通知受監察人。

草案第 9 條至第 12 條為「對於隱私空間實施『非侵入性』之監看、測量、辨識、拍照、錄影等非聲音之調查」，隱私空間之定義依草案第 2 條第 2 款為「住宅、建築物、交通工具或其他具有隱蔽設施之地上物之內部空間，且具有隱私或秘密之合理期待者」，針對具合理隱私期待空間非聲音之調查，採法官保留原則，且限於「最重本刑 3 年以上有期徒刑」之罪始可為之，每次不得逾 30 日，偵查方式僅限非侵入性方式，例如以高倍數照相

doi:10.6342/NTU202301879

機、熱顯像設備等從外往隱私空間內部拍攝，並不包括侵入隱私空間之內裝設竊錄設備。具急迫情況時，依草案第 10 條可由檢察官、司法警察官先行為之，並於實施後 3 日內聲請法官許可之。草案第 11 條、第 12 條則規定許可書應記載事項、事後通知以及資料銷燬之規定。

第二款　設備端通訊監察（草案第三章）

草案內容與對抗加密有關之立法，僅有草案第三章「設備端通訊監察」，依照第三章「設備端通訊監察」立法說明，設備端通訊監察是因應網路通訊軟體取代傳統電話通訊方式之變革，過去通訊監察之技術必須更新為在通訊之設備端進行訊息擷取，且此種干預方式除侵害「秘密通訊自由權」以外，另侵害「資訊科技基本權」，故無法援引現行通訊保障及監察法為授權依據，故有另行立法授權之必要性，草案明確表明採「通訊保障及監察法不得作為設備端通訊監察法源依據」之立場。另外，草案因將設備端通訊監察定性為基於通訊方式變革所為之新興通訊監察手段，設計上原則援用通訊保障監察法所設定之基本原則架構，依草案第 14 條規定，要件包含通訊保障及監察法第 5 條第 1 項列舉重罪、危害國家安全、經濟秩序或社會秩序情節重大、相當性及最後手段性，法律授權之設計採相對法官保留原則，一般情形由法官授權，急迫情形得由檢察官許可先行為之，並於 24 小時內陳報法官許可之。

草案第 15 條比照通訊保障及監察法國安監聽規定，訂定綜理國家情報工作機關首長得核發設備端通訊監察書，然受監察人在境內設有戶籍者應經所在地之高等法院專責法官許可。草案第 16 條第 1 項規定實施設備端通訊監察之方式得以實施接觸、網路傳輸或其他必要方法侵入受監察人所使用之資訊系統或設備，將現行及未來可能之木馬植入方式均予以囊括。

又設備端通訊監察技術上必須侵入資訊系統或設備，執行上必會遭遇實際侵入時點與法院核准時點有長短不一之時間差，草案第 16 條第 2

doi:10.6342/NTU202301879

項係為明確設備端通訊監察得以取得之資訊時點，應以法院核准通訊監察之時間為準，而非實際完成資訊系統或設備侵入之時間點。草案第 16 條第 3 項則參考通訊保障監察法第 13 條規定，於與監察目的無關者不得作成書面紀錄且應即時銷燬。

草案第 17 條為技術性擔保規定，因設備端通訊監察是透過侵入資訊系統或設備之方式，故草案規定應於「技術可達成」之範圍內確保：「不得監察或取得通訊以外之資訊」、「對受監察人之資訊系統或設備僅進行取得監察資料所必須之變更」、「監察結束時，曾進行之變更應即時回復，曾植入之軟體應即時刪除」、「所採用之監察方法應防止第三人利用而入侵受監察人所使用之資訊系統或設備」，依照本條草案立法說明，技術性擔保是於「技術可達範圍內」，若屬現行科技水準下所產生不可復原、防止之事項，並非本條規定技術性擔保之範圍內。

草案第 18 條為準用通訊保障及監察法之規定，依本條規定，設備端通訊監察準用通訊保障及監察法實施期間、續行、停止程序、事後通知、報告與監督、統計資料年報、監察所得資料之保管、使用及銷燬、另案證據使用、違反之民刑事責任等等。依照草案第 18 條立法說明，設備端通訊監察並不準用通訊保障及監察法第 15 條第 5 項、第 6 項有關電信事業相關規範，以及同法第 11 條之 1 調取通信紀錄及通信使用者資料之規定。依照草案第 18 條規定準用通訊保障及監察法第 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；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。」及同條第 4 項「電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」。

然而，值得注意者是，草案課予「協力義務」之對象究係僅限電信事

doi:10.6342/NTU202301879

業，抑或包含通信服務業，從文義解釋來看，草案係透過準用通訊保障及監察法之方式，故協力義務之義務對象應僅限於「電信事業」，協助方式為固有之「設備（建置及維持）及人員之協助」，是否符合網路軟體通訊特性所需，尚屬存疑，本文將於後段《第二項 本文意見--對科技偵查法草案評析》討論。

第三款 數位證據蒐集與保全（草案第四章）

草案第四章之「數位證據蒐集與保全」，依立法說明，本章之性質屬於「現行刑事訴訟法電磁紀錄搜索、扣押之補充性、澄清性規定，並非獨立之強制處分」，從而，本章規定應是現行搜索、扣押強制處分之補充規定，性質上是在受干預人之狀況下為之，非屬秘密偵查，與一般科技偵查係屬秘密偵查性質，誠屬不同。

草案第 19 條為搜索範圍及於雲端之澄清性規定，立法明定關於雲端搜索扣押時，可及於「可讀取該電磁紀錄且與其在空間上分離之其他儲存設備方式」，以解決向來在雲端搜索扣押議題中存在之「雲端硬碟所在地」之爭議，草案採「硬碟延伸說」，欲透過立法方式明定搜索電腦設備可及於軟體入口之延伸儲存地，而並未採取「硬碟儲存地說」[441]。

草案第 20 條是參照刑事訴訟法第 144 條第 1 項「因搜索及扣押得開啟鎖扃、封緘或為其他必要之處分。」之規定，在執行搜索、扣押雲端儲存設備時，為避免犯罪嫌疑人或第三人透過遠端對證據進行湮滅、變更或移轉，故規定執行雲端搜索時，得針對物（行動裝置、儲存設備、電腦等）或人（被告、犯罪嫌疑人、設備或電磁紀錄之所有人、持有人、保管人或其他相關人）為必要之保全處分。

[441] 硬碟儲存地說認為若雲端搜索資料儲存範圍位於境外，應透過司法互助方式使得為之，詳參施弘文，以科技偵查跨境取得證據之研究-以美國法為中心（發言紀錄），檢察新論，第 27 期，2020 年 2 月，頁 202 至 207。

doi:10.6342/NTU202301879

草案第 21 條為針對已經合法扣押之電磁紀錄進行數位鑑識之相關規定，規定執法機關進行數位鑑識得為實施使用、操作、破解帳號密碼、複製、另存、復原、分析、比對、建置資料庫等處置，並於草案第 21 條第 2 項規定實施前開處置時，應於技術可達範圍內確保實施標的與實施前之完整性及同一性。

第六節 小結-（兼科技偵查法草案評析《以對抗加密之立法對策為中心》）

第一項　與我國現行法干預處分層級化授權體系之相容性

參考司法院釋字第 443 號揭示之「層級化保留原則」，不同基本權於憲法上所享有之保護位階具有層級化差異，而我國現行刑事訴訟法針對干預處分，亦已依其基本權干預屬性及強度發展出層級化干預理論。考量科技時代下之各種新興偵查干預手段，必定隨著科技不斷進步而日新月異，若依循傳統以特定干預手段為區分之立法方式，未來必定面臨立法（修法）速度趕不上犯罪手法及偵查技術之困境，故在科技偵查法制體系上，宜依「干預之基本權屬性」以及「干預強度」，建構層級化授權體系，並輔以概括授權條款，較能因應科技快速發展之特性。準此，在形塑我國作為對抗加密之立法策略時，亦應從基本權干預屬性及干預強度出發，檢視其可能干預之基本權，以及依其干預強度所應放置之授權層級，方能與我國現有之刑事訴訟法業已存在之干預處分層級化授權體系彼此相容。

準此，本文認為來源端通訊監察作為加密時代通訊監察之補充手段，當干預範圍及內容均緊扣原通訊監察得以取得之範圍時，應可採取與現行通訊監察相當之授權規定及程序保障規範，而我國未來增訂秘密線上搜索之法律授權時，則可能面臨到我國現行法律並無住宅監聽之刑事訴訟干預處分，憲法亦無相關規定，未來倘要以法律保留層級，而非憲法保留層級

doi:10.6342/NTU202301879

做為秘密線上搜索之層級化法律保留，與德國法之憲法保留位階將有所落差，可以預見未來恐出現是否能符合司法院釋字第 443 號解釋文所揭示之「層級化法律保留原則」意旨之合憲性質疑，此乃是我國推動秘密線上搜索立法恐須面對之一大課題。然而，探討此問題時仍應注意到我國與德國之憲法體制有根本不同，我國除憲法第 8 條揭示人身自由之憲法保留外，其他憲法保障之基本權均一概適用憲法第 23 條法律保留原則，而德國憲法並無如同我國憲法 23 條此類概括基本權限制條款，係依各基本權分別規定限制條件[442]，兩者有顯著不同，參考比較法時自不能忽略兩國憲政體制有此根本性不同。國內學者亦有指出我國大法官於司法院釋字第 443 號解釋理由書所揭示之「憲法保留」，並不是將保障之範圍保留給制憲者或修憲者，而應屬憲法優位之概念，限制立法者訂定法律有關人身自由之限制條件不得低於憲法規定，有特別法優於普通法之涵義[443]。準此，本文認為於我國憲法體制下，立憲者係以憲法第 23 條作為基本權限制之概括條款，於制憲者並未於憲法為「特別規定」時，仍應回歸憲法第 23 條法律保留原則之適用，屬於法律保留之範圍。

第二項　秘密線上搜索立法重要性

相較於本文第三章所介紹之英國、法國、德國、荷蘭及澳洲等國之立法，不難發現我國科技偵查法草案部分立法規範者（包含攝錄與追查位置（草案第二章）、數位證據蒐集與保全（草案第四章），均為上開國家早期已存在之立法規範，我國現階段可謂僅係嘗試追趕上開國家前一代之立法進度。草案第三章之設備端通訊監察，係唯一較符合近期世界各國對抗加密之立法，然相較於上開國家除以設備端通訊監察作為傳統通訊監察因應

[442] 蔡宗珍，法律保留思想及其發展的制度關聯要素探微，臺大法學論叢，第 39 卷第 3 期，2010 年 9 月，頁 44。
[443] 同上註，頁 45。

doi:10.6342/NTU202301879

網路通訊時代之立法對策外，大多另訂定秘密線上搜索授權規範，將傳統搜索扣押擴張至秘密線上搜索搜集證據，我國此次草案尚無秘密線上搜索相關規範，就打擊組織性、跨國性之網路犯罪而言，仍欠缺有利工具，然其可能原因，恐係因秘密線上搜索之基本權侵害程度嚴重，於德國視為與住宅監聽(即大監聽)相當，而我國現行刑事偵查干預處分相關法律規定，均尚未肯認執法機關可基於犯罪偵查之目的進行住宅監聽，故於立法策略上先予排除秘密線上搜索。

從立法推動策略而論，固可理解現階段先予排除秘密線上搜索，主要原因係考量我國目前科技偵查相關法制仍屬草創階段，若未來立法授權政府使用木馬技術，其技術、程序規範及監督機制均有賴一段時間之運作觀察，故從干預程度較輕微之來源端通訊監察著手，等到實務運行一段時間，再漸進式推動秘密線上搜索之立法，不可否認是較為穩健及保守之立法策略。

然而，本文認為秘密線上搜索已為現今數位時代下對抗組織性、跨國性犯罪不可或缺之必要手段，正如同本文第三章所介紹之英國、法國、德國、荷蘭及澳洲近來立法，均已見秘密線上搜索授權規範，足見於所有犯罪幾乎脫離不了網路犯罪之今天，秘密從電腦設備蒐集證據之方式，已係多國用來對抗重大犯罪所不能缺少之工具，草案內容未包括秘密線上搜索之偵查干預手段，甚為可惜。

或有認為我國現階段所面臨恐怖主義威脅風險相較於西方國家較為輕微，然而，我國特殊政治情勢，所面臨之國家安全威脅相較於其他國家更為嚴峻，我國近來積極增修國家安全相關犯罪之實體處罰規定，擴大國安犯罪類型，然而，無論是國家安全法第 2 條之發展組織罪，或是犯罪規模日益龐大，手段日漸兇殘之詐騙集團、洗錢集團及人口販運集團等，早已形成一條複雜、不法利益糾葛之跨國犯罪產業鏈，在欠缺有效之秘密蒐

doi:10.6342/NTU202301879

證偵查手段，要有效一網打盡此類犯罪組織，甚為困難。從犯罪偵查面而論，所面臨之困境在實務案件執行時，縱使係依現行刑事訴訟法執行搜索、扣押，實際上早已係以數位證據之搜索、扣押為中心，得以成功將犯罪定罪之關鍵證據往往都係在搜索電磁設備中查扣。

秘密線上搜索與傳統搜索雖然同樣是針對數位證據進行搜索及扣押，然最大差別在於「秘密」，現行法下之搜索電磁設備屬一次性搜索且不具秘密性，於執行搜索時往前以「回溯」之方式過濾證據資料，是否能成功獲取關鍵證物形同「開獎」，因案件已發動執行而曝光，若未能於當次搜索行動中查扣證物，未遭執法機關發現之證物往往也迅速遭到湮滅，未來亦難有其他新生犯罪事證，向上查緝集團上游等於跟時間賽跑，越高階層之犯罪者，在無法秘密進行電磁紀錄蒐證之情況下，往往有充裕的時間逃亡、滅證。申言之，在僅能透過現行法搜索扣押規定進行電磁紀錄搜索之情況下，因僅能在受搜索知悉之情形下為之，搜索當下等同將執法行動曝光，要以溯源斷根之方式將組織一網打盡幾乎不可能，執法困境如同「斬草不除根，春風吹又生」。

相反地，秘密線上搜索係透過秘密蒐證之方式長時間取證，往往可以待證據蒐集完備後一舉收網，有利於查緝集團型、跨國型之組織犯罪，將犯罪集團一次根除，此應為秘密線上搜索最有利於犯罪偵查之原因，也唯有透過秘密線上搜索之長期蒐證，方能將集團斬草除根。

另一個不可忽略的點是國內法對於跨國執法合作之重要性。從國際合作觀點觀察，國際上已見秘密線上搜索之立法趨勢以及實際的執法合作行動，本文前《見第一章、第二節、第四項「端對端加密技術對犯罪及執法之影響」》所介紹之 EncroChat 跨國執法行動事後於歐洲多國引起之執法合法性爭議，執法合作亦需以合於各國法律規範為前提，確保內國科技偵查法制與國際趨勢接軌，更係參與執法合作之基礎條件。

doi:10.6342/NTU202301879

第三項　兼採來源端通訊監察及業者協力義務之必要性

觀諸本文前所介紹之英國、法國、德國、荷蘭及澳洲等國之立法，因應加密通訊軟體之立法對策，均兼採解密金鑰、協力義務及國家木馬等多種方案，其原因不外乎係因面對技術門檻、跨國大型科技公司之商業利益以及企業責任等諸多面向之考量，倘採取單一立法方式，從外國立法例已清楚可見難以應付所有個案情狀，易言之，單採解密金鑰、協力義務方式，縱有違反義務之刑事處罰作為強制手段，仍難保得有效要求業者履行法定義務；反之，單採國家木馬者，在加密技術一日千里之今日，國家木馬技術之更新速度能否完全追上市場上所有科技產品所使用之技術等級，更屬一大變數，也因此本文所介紹之國家在立法策略上兼採解密金鑰、協力義務及國家木馬等立法，賦予政府於個案中選擇個案最適宜之方式，以此取得解密資訊。

我國草案目前係單採國家木馬之立法，再以草案第 18 條規定準用通訊保障及監察法第 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；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。」及同條第 4 項「電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」之方式課予電信事業有關設備（建置及維持）及人員之協助義務，然此協力義務之內涵僅限於人力、物力之協助，且主體範圍僅限「電信事業」，礙於我國現行對於電信事業範圍之定義甚為狹隘，僅限於第一類、第二類電信事業，不包括「通信服務商」，將無法涵蓋網路應用服務業、網路平台服務業等未提供電信設備為基礎之網路服務業者草案以準用通訊保障及監察法之方式所規範之協力義務，其主體跟義務內容均過於狹隘，恐無法因應政府面對數位加密時代之所需。

doi:10.6342/NTU202301879

當然，無論是網路應用服務業、網路平台服務業，與電信事業在提供國家「監察」之協力義務上，均有著先天性的差別，電信事業有國際標準組織所建立之通訊監察標準，例如：美國電信行業解決方案聯盟/電信行業協會（ATIS/TIA）、有限電視網路纜線實驗室（Cable Labs）、歐洲電信標準協會（ETSI）以及第三代合作夥伴計畫（3GPP）等[444]，因為通信事業基本上有著國際通用之基本架構，各國執法機關也得以基於上開特性，透過法律規定要求電信事業將通訊監察功能放置於其中。然而，網路應用服務業、網路平台服務業等與電信事業不同，不僅不是特許事業，也無全球幾乎一致之基本架構為框架，各家業者使用之技術不盡相同，系統、版本更是推陳出新，執法機關已無法仰賴配合納入監察功能換取特許執照之方式，要求業者於所提供之產品、服務納入監察功能。然而，協力義務在本文所介紹之立法例中，不僅未被捨棄，更有澳洲 2018 年 TOLA ACT 與英國 2016 年 IPA 擴大至要求特定通信服務商在產品或服務中加入新功能之技術能力通知，可以看出部分國家仍嘗試透過立法之方式給予業者壓力，課予程度不一之協力義務。

本文認為，政府面對加密衝擊雖應首重強化國家本身之技術能力，而協力義務作為國家所技術有其限制或不足時之另一種權宜方式仍有其必要性。而在決定協力義務之範圍及種類時，應當注意兼顧打擊犯罪以及數位產業發展之利益權衡，現階段如技術能力通知之協力義務，雖已有英國、澳洲之立法例可供參考，然從英國、澳洲所公布之相關報告中亦發現實務運作上均還是透過非強制力，亦即與業者溝通協調之方式來達到目的，高強度且具強制力之技術能力通知恐仍需更多國外實證經驗來驗證其可行性，相較之下，立法例中早已普遍存在之解密令狀，於不違反不自證己罪

[444] 林國翔、沈士豪、李鎮宇，取得加密通訊內容因應對策—從通訊監察技術觀點出發，臺灣警察專科學校警專學報，第 7 卷第 6 期，2021 年 2 月，頁 28。

doi:10.6342/NTU202301879

原則及法定拒絕證言權之限度下，針對已有破解加密保護措施之密碼、方法及技術之自然人、法人適度課予其解密之協力義務，當可與設備端通訊監察及秘密線上搜索等規定相輔相成，提供更完整之執法因應對策。

doi:10.6342/NTU202301879

第五章　立法建議

2019 年德國最大的刑事訴訟法註釋書 Löwe-Rosenberg, StPO 在刑事訴訟法第 94 條前段前言部分提到一句話「偵查機關的科技武器平等」[445]；國內學者亦有以「不能讓被告上太空，偵查人員還在殺豬公」呼籲立法者應重視犯罪者使用科技犯罪，然執法者還僅能使用傳統工具追緝犯罪之問題，儘速立法提供追訴人員能夠和犯罪行為人匹敵的科技偵查手段，否則將有害刑罰權之實現[446]，科技偵查之立法，並非要在人權的道路上走回頭路，而是要在偵查機關的科技武器平等原則下，堅守法治國原則，給予明確之授權及規範，使干預處分之執行受到法律明確之規範及監督。

當我們正視現今人類之生活方式，早已隨科技發展與科技緊密結合，犯罪工具及手法亦是如此，無論是傳統通訊方式早已被加密通訊軟體取代，一般人慣用軟體即時通話取代門號撥號，或是資料早已從紙本轉換成雲端儲存，加密技術更是電磁資訊儲存、傳輸之基本配備等，都清楚可見過去之通訊監察、搜索等干預處分已不足以因應現今犯罪模式，而當傳統通訊監察、搜索等方式因數位加密時代之道來已無用武之地，不給予執法機關相對應之執法武器，等同在科技時代中要求犯罪偵查機關倒退至石器時代。

有鑒於此，為因應數位加密技術對我國執法所生衝擊，本文認為應立法明定設備端通訊監察、秘密線上搜索以及解密命令之法律授權依據暨程序保障規定，使執法者能有明確之遵循依據，並建構完整之程序保障規範及監督機制。本文謹嘗試於最後提出建議之草案條文，期能拋磚引玉，提供立法者參考。

第一節 國家木馬

[445] 王士帆，科技偵查立法之可行性評估及建議方向（發言紀錄），檢察新論，第 27 期，2020 年 2 月，頁 179。

[446] 王士帆（發言紀錄），科技偵查立法藍圖-刑事訴訟目的之試金石（上），月旦裁判時報，第 103 期，2021 年 1 月，頁 111。

doi:10.6342/NTU202301879

第一項　設備端通訊監察及秘密線上搜索之立法芻議

有鑑於秘密線上搜索已為當今執法機關對抗組織性、跨國性犯罪不可或缺之必要手段，此從本文介紹之立法先進國家之立法例即可知悉，況資通時代之來臨，組織型、資通型、跨國型犯罪無一不需要跨國執法合作來達成查緝犯罪集團之目標，與世界先進國家法律規範之落差將造成我國未來與他國進行執法合作之阻礙，是以本文認為我國應於國家木馬之立法上，採取與世界各國相同之標準，不僅增定僅針對通訊內容之設備端通訊監察，亦應有能針對儲存於資訊設備之電磁紀錄進行遠端秘密搜索之秘密線上搜索干預手段授權，方能有效遏止犯罪。

在規範要件設計上，我國現行刑事訴訟干預處分均係緊扣基本權干預強度而為層級化授權，考量設備端通訊監察與秘密線上搜索所干預之基本權有重大差異，自應有授權以及程序保障密度不同之設計。設備端通訊監察作為以植入木馬程式方式取得傳統通訊監察通訊內容及使用通訊時產生之狀態資料之新興科技干預手段，在擷取之時間及內容均有嚴格限制，亦即在擷取之時間與內容均緊扣「傳統通訊監察原本即可監察與記錄之通訊內容」之前提下，當可理解與傳統通訊監察功能等價，性質上屬於因應加密通訊軟體時代來臨替代傳統通訊監察之干預手段，故其基本上仍屬秘密通訊自由權之偵查干預手段，僅係為對抗加密，故干預方式係在資料存在設備端時進行擷取，而非通訊傳輸期間，而性質上亦屬於資訊自主決定權之干預手段。本文認為，此部分可參考德國法刑事訴訟法立法方式，採用與現行通訊監察相似之實體及程序要件，選擇相對法官保留原則之授權層級。

秘密線上搜索相較於設備端通訊監察，其干預之範圍擴及受干預對象使用電腦設備儲存、傳輸、瀏覽之任何資訊，在每個人之個人生活與電磁設備高度結合之今日，秘密線上搜索可謂對於人格權最為嚴重之干預

doi:10.6342/NTU202301879

手段，授權密度自有較設備端通訊監察再予提高之必要性。基此，本文建議參考德國刑事訴訟法第 100b 條秘密線上搜索之規定，採合議庭 3 位法官保留之授權密度，並就執行期間已達 6 個月者，提高為高等法院合議庭核准，希冀透過法官保留之強化，以確保合於法律授權範圍內之執行。

另外，著眼於不論係設備端通訊監察，抑或秘密線上搜索，其所使用之木馬程式均係干預個人電腦設備，基於保護受干預人資訊科技設備私密性與完整性之特性，應增訂必要之程序規範（例如木馬技術性擔保、執行完畢後移除並回復原狀等），並強化於技術層面確保木馬僅在法律授權範圍內執行功能更為重要，故可著重「技術性擔保」及事前事後監督機制等程序保障，以確保技術性擔保事項能夠有效被落實並受到適當監督。基此，本文認為有關於國家木馬之法律授權，除應搭配事前審查與事後監督雙軌審查、建置機關應與執行機關應予區分等程序規範以外，木馬程式之開發或採購、驗收以及日後之定期功能檢測，均應有具有技術能力之第三方獨立機關（構）進行檢測及審核，方能有效確保木馬技術係在法令授權範圍內執行，以完備法治國原則下，國家使用木馬所不可或缺之監督機制。

第二項　設備端通訊監察及秘密線上搜索建議條文

第一條　（設備端通訊監察）

有事實足認被告或犯罪嫌疑人涉有通訊保障及監察法第五條第一項各款所列罪嫌，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得以科技方法實施設備端通訊監察。

前項情形，應由檢察官或由司法警察官報請檢察官同意後，以書面聲請該管法院核發設備端通訊監察書。

有事實足認被告或犯罪嫌疑人涉有通訊保障及監察法第六條第一項所列罪嫌，為防止他人生命、身體、財產之急迫危險；或有事實足認有其他通

doi:10.6342/NTU202301879

訊作為第一項所列罪嫌之連絡而情形急迫者，得由檢察官或司法警察官報請檢察官許可後，通知執行機關先予實施設備端通訊監察，並於二十四小時內，由檢察官或由司法警察官報請檢察官同意後，聲請該管法院補發設備端通訊監察書。

第二條（設備端通訊監察書）

前條聲請書應記載第二項設備端通訊監察書應記載事項，並檢附相關資料，釋明有相當理由可信其通訊內容與本案有關，且曾以其他方法調查仍無效果，或以其他方法調查，合理顯示為不能達成目的或有重大危險情形。

設備端通訊監察書應記載下列事項：

一、案由及涉嫌觸犯之法條。

二、監察對象。

三、監察通訊種類、行動通訊設備號碼或使用之卡片卡號等足資識別之特徵。

四、監察理由。

五、監察期間及方法。

六、聲請機關。

七、執行機關。

八、建置機關。

前項第七款之執行機關，指蒐集通訊內容之機關。第八款之建置機關，指單純提供通訊監察軟硬體設備而未接觸通訊內容之機關。

核發設備端通訊監察書之程序，不公開之。

法官並得於設備端通訊監察書上對執行人員為適當之指示。

第三條（法院受理聲請之程序）

doi:10.6342/NTU202301879

檢察官受理第一條聲請案件，應於四小時內核復；如案情複雜，得經檢察長同意延長四小時。

法院受理第一條聲請案件，應於四十八小時內核復。

聲請不合法定程序、不備理由、未經釋明或釋明不足者，法院應予駁回。其聲請經法院駁回者，不得聲明不服。

第四條(監察期間)

設備端通訊監察期間，每次不得逾三十日；其有繼續監察之必要者，應釋明具體理由，至遲於期間屆滿之二日前，提出聲請。繼續監察期間逾一年者，執行機關如認有繼續監察之必要者，應重行聲請。

監察期間屆滿前，偵查中檢察官認已無監察之必要者，應即停止監察。

第五條 （秘密線上搜索）

有事實足認被告或犯罪嫌疑人涉有下列犯罪嫌疑重大，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其使用之資訊系統或設備有製造、傳輸、接收或儲存與本案有關內容，且不能或難以其他方法蒐集或調查證據者，得使用科技方法執行秘密線上搜索。

一、最輕本刑五年以上有期徒刑之罪。

二、組織犯罪防制條例第三條第一項、第四條或第六條之罪。

三、刑法第一百條至第一百零一條內亂罪、第一百零三條至第一百零九條或第一百十一條外患罪。

四、刑法第三百三十九條之四之加重詐欺取財罪。

五、國家安全法第七條第一項至第三項、第八條第一項至第三項之罪。

六、國家機密保護法第三十二條第一項、第二項、第五項、第三十三條第一項、第二項、第五項、第三十四條第一項至第三項或第五項。

doi:10.6342/NTU202301879

七、洗錢防制法第十四條或第十五條洗錢罪。

前項情形，應由檢察官以書面聲請該管法院合議庭核發秘密線上搜索票。聲請書應記載第六條秘密線上搜索票應記載事項，並檢附相關資料釋明有相當理由可信其使用之資訊系統或設備製造、傳輸、接收或儲存之內容與本案有關，且曾以其他方法調查仍無效果，或以其他方法調查，合理顯示為不能達成目的或有重大危險情形。

第六條 （秘密線上搜索票）

秘密線上搜索票應記載下列事項：

一、案由及涉嫌觸犯之法條。

二、受搜索之被告、犯罪嫌疑人。但被告或犯罪嫌疑人真實身分不明時，得以其他方式特定之。

三、受搜索之資訊系統或設備。

四、有效期間，逾期不得執行搜索及搜索後應將搜索票交還之意旨。

法官並得於搜索票上，對執行人員為適當之指示。

核發搜索票之程序，不公開之。

第七條(秘密線上搜索期間)

秘密線上搜索期間，每次不得逾三十日；其有繼續監察之必要者，應釋明具體理由，至遲於期間屆滿之二日前，提出聲請。但繼續秘密線上搜索期間，不得逾六個月，執行機關如有繼續執行秘密線上搜索之必要者，應向該管高等法院合議庭重行聲請。

秘密線上搜索期間屆滿前，檢察官認已無繼續搜索之必要者，應即停止。

第八條（法院受理秘密線上搜索之程序）

doi:10.6342/NTU202301879

法院受理秘密線上搜索聲請案件，應於四十八小時內核復。

聲請不合法定程序、不備理由、未經釋明或釋明不足者，法院應予駁回。

其聲請經法院駁回者，不得聲明不服。

第九條 （實施設備端通訊監察及秘密線上搜索之科技方法）

實施設備端通訊監察，得以實體接觸、網路傳輸或其他必要方法，侵入受監察人所使用之資訊系統或設備，查看、截取、紀錄、複製監察期間之通訊內容及通訊紀錄。核准設備端通訊監察之後，開始實施設備端通訊監察之前已結束者，亦得為之。

實施秘密線上搜索，得以實體接觸、網路傳輸或其他必要方法，侵入受搜索人使用之資訊系統或設備，查看、截取、紀錄、複製系統或設備所製造、傳輸、接收、存取或以網路相連之其他儲存媒體所存取之電磁紀錄。

實施秘密線上搜索可查看、截取、紀錄、複製通訊內容及通訊紀錄，無庸另行聲請設備端通訊監察書。

執行設備端通訊監察及秘密線上搜索所得內容顯然與原聲請目的無關，且法律明定不得作為他用者，應即時銷燬之。

第十條 （技術擔保）

實施設備端通訊監察及秘密線上搜索，應於科技技術可達成之範圍內，確保下列事項：

一、不得查看、截取、紀錄、複製法律授權範圍以外之資訊。

二、資訊系統或設備僅進行執行所必要之變更。

三、執行完畢時，曾進行之變更應即時回復，曾植入之軟體應即時刪除。

四、所採用之科技方法應防止第三人利用而入侵受監察人所使用之資訊系統或設備。

doi:10.6342/NTU202301879

第十一條 （技術擔保監督委員會）

本法主管機關應設置技術擔保監督委員會，監督查核本法所使用之科技技術，於開發、採購、審驗、使用階段符合前條規定。

前項監督委員會之人員，不得為建置機關或執行機關之人員。

技術擔保監督委員會應定期透過現地查核或使用電子監督設備之方式，為第一項所列事項之監督。

第一項委員會之組成、運作、委員之資格及其他相關事項之辦法，由主管機關訂定之。

第十二條（指定之通信服務事業之協力義務）

指定之通信服務事業應協助執行機關執行設備端通訊監察及秘密線上搜索。

前項協助內容包括下列事項:

一、提供必要設施及人員協助。

二、提供必要技術協助。

三、提供必要資訊。

因執行前項協助所生之必要費用，於執行後，得請求執行機關支付。

指定之通信服務事業如有正當理由無法履行應協助事項，應以書面方式說明理由復知執行機關。

第一項所稱指定之通訊服務事業之範圍，由法務部會同中央目的事業主管機關報請行政院指定。

第十三條（指定之通信服務事業違反協力義務之處罰）

前條指定之通信服務事業未履行前條協助事項者，處以新臺幣五十萬以上

doi:10.6342/NTU202301879

二百五十萬以下罰鍰;經中央目的事業主管機關限期履行,屆期未履行者,按日連續處罰,並得限制、停止營業、或為剝奪或消滅資格、權利之處分。

第十四條(程序保障-期中報告)

執行機關應於執行設備端通訊監察以及秘密線上搜索期間內,每十五日至少作成一次以上之報告書,說明執行情形以及有無繼續執行之需要。檢察官或核發設備端通訊監察書或秘密線上搜索票之法官並得隨時命執行機關提出報告。法官依據經驗法則、論理法則自由心證判斷後,發現有不應繼續執行之情狀時,應撤銷原核發之設備端通訊監察書或秘密線上搜索票。

第十五條(程序保障-事後通知)

執行機關於執行設備端通訊監察或秘密線上搜索結束時,應即敘明下列事項通知受監察、搜索之人。如認通知有妨害監察、搜索目的之虞或不能通知者,一併陳報法院。

一、受監察、搜索之人。

二、設備端通訊監察書、秘密線上搜索票核發機關及相關文號。

三、實施期間。

四、有無獲得監察、搜索目的之資料。

五、救濟程序

檢察官逾一個月未為前項陳報者,法院應於十四日內主動通知受監察、搜索人。但不能通知者,不在此限。

法院對於前項陳報,除有具體理由足認通知有妨害監察、搜索目的之虞或不能通知之情形外,應通知受監察、搜索人。

前項不通知之原因消滅後,執行機關應報由檢察官陳報法院補行通知。原因未消滅者,應於前項陳報後每三個月向法院補行陳報未消滅之情形。逾

doi:10.6342/NTU202301879

期未陳報者，法院應於十四日內主動通知受監察、搜索之人。

第十六條（程序保障-年報）

執行機關、技術擔保監督委員會每年應製作該年度工作及相關統計資料年報，定期上網公告並送立法院備查。

前項年報應包含下列事項：

一、聲請及核准之案由、對象數、案件數。

二、設備端通訊監察、秘密線上搜索執行方式之種類及數量。

三、停止執行案件，其停止情形。

四、依第十五條之通知或不通知、不通知之原因種類及原因消滅或不消滅之情形。

五、技術擔保監督委員會監督執行情形。

六、自動化資料留存執行情形

七、依第十二條請求指定之通訊服務事業協助之種類及數量

八、資料銷燬執行情形。

第十七條(程序保障-立法院監督)

法務部每年應向立法院報告設備端通訊監察及線上秘密搜索執行情形。

立法院於必要時，得請求法務部報告並調閱相關資料。

立法院得隨時派員至建置機關或協助執行通訊監察之機關、事業及處所，或使用電子監督設備，監督設備端通訊監察及線上秘密搜索執行情形。

本法未規定者，依立法院職權行使法或其他法律之規定。

第十八條(程序保障-所得資料之留存及銷毀)

執行設備端通訊監察及線上秘密搜索所得資料，應以適當方式保存資料之

doi:10.6342/NTU202301879

真實性，防止遭到增、刪、變更，除已供案件證據之用留存於該案卷或因其他原因有長期留存必要者外，執行機關於執行結束後，保存五年，逾期予以銷燬。

前項得資料全部與執行設備端通訊監察及線上秘密搜索目的無關者，執行機關應即報請檢察官許可後銷燬之。

前二項資料銷燬時，執行機關應予以紀錄，並報請檢察官機關首長派員在場。

第十九條（程序保障-自動化資料留存）

建置機關應設置自動化傳遞至第三方設備之方式留存執行設備端通訊監察及秘密線上搜索之下列資訊，並以連續流程履歷紀錄方式記錄之。

一、 科技方法名稱。

二、 執行期間全部登入紀錄。

三、 對資訊系統或設備所為暫時性及非暫時性變更。

四、 對資訊系統或設備所為回復或軟體移除。

五、 執行機關及人員。

建置機關應以適當方式確保上開資料之真實性，並防止遭到增、刪、變更。

第一項紀錄自執行完畢時起，應至少保存五年。

第二十條（禁止目的外使用及另案陳報）

前二條資料，除符合原執行目的或其他法律另有規定者外，不得提供與其他機關（構）、團體或個人。

執行設備端通訊監察及線上秘密搜索期間取得與原執行目的無關之內容，然涉及其他法定允許執行設備端通訊監察或線上秘密搜索之不法犯罪者，應於發現後七日內補行陳報法院。

doi:10.6342/NTU202301879

第二十一條(罰則)

除第一條第三項情形外，公務員未經法院許可實施設備端通訊監察或秘密線上搜索者，處五年以下有期徒刑。

公務員或曾任公務員之人無故洩漏職務上知悉、持有或取得依本法實施設備端監察通訊或秘密線上搜索所得應秘密資料者，處三年以下有期徒刑。

第二十二條(損害賠償)

因故意或過失違法執行設備端通訊監察、線上秘密搜索，或洩漏、提供、使用執行設備端通訊監察、線上秘密搜索所得資料，而侵害他人權利者，負損害賠償責任。

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。

前項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第二十三條(損害賠償計算方式)

前條之損害賠償總額，按設備端通訊監察、線上秘密搜索日數，以每人每日新臺幣一千元以上五千元以下計算。但能證明其所受之損害額高於該金額者，不在此限。

前項日數不明者，以三十日計算。

第二十四條(請求權時效)

損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者亦同。

doi:10.6342/NTU202301879

第二十五條(國家賠償)

公務員或受委託行使公權力之人，執行職務時，因故意或過失違反本法或其他法律之規定侵害人民自由或權利者，國家應負損害賠償責任。

依前項規定請求國家賠償者，適用第十九條第二項、第三項及第二十條之規定。

第二十六條(適用民法及國家賠償法)

損害賠償除依本法規定外，適用民法及國家賠償法規定。

第二節 解密命令

第一項　　兼採國家木馬及解密義務之必要性

觀察本文所介紹之外國立法例之發展歷程及趨勢可以發現，各國在立法進程上，澳洲係先採取木馬授權，於近期立法加重業者之協力義務，而英國於早年之調查權規範即有第 49 條解密通知，後於 2016 年調查權力法同時擴大國家木馬授權以及業者協力義務，且無論其先後順序為何，本文第三章所介紹之英國、法國、荷蘭、澳洲等國，均清一色採取「國家木馬」及「業者協力義務」兩者兼採之立法方式，一方面立法授權並規範政府發展及使用木馬，另一方面保留甚至加重通信服務商程度不等之協力義務，或透過加重違反義務處罰之方式強化其效力。

隨著科技發展，於特定領域擁有領先技術之大型通信服務商往往佔據市場領先地位，科技產業早已走向大者恆大之路，以美國 5 大科技巨星（蘋果、微軟、谷歌、亞馬遜與臉書）為例，為履行其企業責任或是不得不因應於全球服務必須面對之各國執法機關需求，然又必須符合公司應

doi:10.6342/NTU202301879

與準據之該國法律，基此，此等跨國大型科技公司往往訂定自己公司協力執法之規則，此從目前實務上執法機關向跨國企業調取資料之運行方式可謂一人一把號各吹各的調，執法機關於執行犯罪偵查時，不僅應遵循內國法定程序規範外，更「不得不」必須依照各該公司自己訂定之資料調取規範，方能順利取得所需資料。此種現象從傳統國家以立法權訂定法律對人民發生拘束力之觀點，或有些許諷刺，然從另一方向觀察及解釋，此乃公私協力及企業責任之具體展現，何以此類大型跨國企業需要訂定自己協力執法之規則？不難發現此與世界各國針對企業協力義務之立法有著密切關連性，企業面對商業利益、公司政策、契約責任、法律義務及社會責任多面向之調和，與其說企業不欲立法者立法課予義務，應更不願國家在沒有法律依據之情況下強行要求企業配合。或有論者認為，以我國外交、商業、市場規模等處境來看，縱使立法明定通信服務商之協力義務，目前市佔率較高之通信服務商大多為外國公司，難以發揮實際效用，惟本文認為我國為既係民主法治國家，立法明定通信服務商之合理範圍內之協力義務，不僅是與業者洽談之基本籌碼，更是法治國之根本要求，或可白話的說，立法明定業者協力義務之同時，也同時給予業者無法履行對客戶義務之法律上正當基礎。

再者，更實際的是，在科技技術快速發展之時代，單純仰賴政府機關一己之力發展木馬或解密技術，不僅耗費鉅額時間及費用成本，更未必能保障能永遠即時跟上日新月異之科技發展腳步，更何況立法例上英、法、德、荷及澳洲等國均採用國家木馬以及業者協力義務之雙重立法以資周全，我國應有必要在國家木馬方案以外，立法明定通訊服務商一定程度之協力義務。

至於協力義務範圍，立法例上有德國之「電信法及電信監察規則之一般性協力義務」、法國、英國及荷蘭早年立法之「提供解密金鑰」義務，

doi:10.6342/NTU202301879

強度最高者有如澳洲 2018 年 TOLA ACT 以及英國 2016 年調查權力法要求特定通信服務商在產品或服務中加入新功能之技術能力通知，義務範圍相差甚大，若從澳洲 2018 年 TOLA ACT 施行後澳洲議會委員會 2021 年 12 月所出具之審查報告可發現，澳洲此次修法不僅擴張通信服務商之協力義務外，亦新增政府進入電腦令以及擴大搜索令，然新法施行後之審查報告各界之反對意見仍集中於擴大業者協力義務之部分，且從審查報告之統計數據可發現，新法施行後之案件均仍係透過不具強制力之「技術協助請求」完成，操作方式上是機關與通信服務商彼此協商結果，透過類似契約協議之方式使通信服務商獲得法律責任之豁免，具強制力之技術協助通知及技術能力通知截至審查報告公布之日為止仍未動用。觀察澳洲經驗，在期待通信服務商給予必要協助乙事上，若義務已超越企業所認合理範圍，縱有法律為後盾，實踐上也將是困難重重。

基此，本文認為政府對抗加密衝擊首應積極發展國家之技術能力，然協力義務作為國家技術有其限制或不足時之另一種補充措施，仍有其必要性。立法政策上應注意兼顧打擊犯罪以及數位產業發展之利益權衡，現階段課予類似澳洲、英國立法例之技術能力通知，恐不利國內產業發展，且尚需更多外國立法例之實證經驗用以驗證其效益暨可行性，相較之下，外國立法例早已普遍存在之解密令狀，於不違反不自證己罪原則及法定拒絕證言權之前提下，針對已知悉或持有破解加密保護措施之密碼、方法及技術之自然人、法人適度課予其協助解密之義務，應可與設備端通訊監察及秘密線上搜索等規定相輔相成，提供執法機關與業者溝通協調請求解密協助之依據，更可進一步提供業者於提供政府協助時，作為可能衍生賠償責任之豁免依據。

第二項　　解密義務建議草案條文

第一條（解密命令）

doi:10.6342/NTU202301879

檢察官、檢察事務官、司法警察官或司法警察依法執行通訊監察、搜索、扣押或其他合法方式取得之電磁設備或紀錄受加密保護者，得逕予破解加密保護措施。

前項情形，檢察官、檢察事務官、司法警察官或司法警察不能或難以破解加密保護措施，且有相當理由可信特定對象有解密之密碼、方法或技術者，檢察官得以書面向該管法官聲請核發解密命令，命其於一定期限內提供密碼、方法、技術或執行操作，破解加密保護措施或將受加密之標的轉為得以理解之形式。司法警察官得報請檢察官許可後，向該管法院聲請核發解密命令。

前二項解密命令之解密義務之相對人，不得為本案被告、犯罪嫌疑人或刑事訴訟法所規定得拒絕證言之人。

若解密之密碼、方法或技術為法人所有或持有者，應以該法人暨其法定代表人為解密命令之相對人。

第二條（解密命令聲請書）

解密命令聲請書應記載下列事項:

一、案由。

二、解密標的。

三、取得解密標的之原因事實、程序或法律依據。

四、解密義務相對人。

五、有相當理由可信解密義務人有解密密碼、方法或技術之原因。

六、解密期限。

七、聲請機關。

第三條（解密命令應記載事項）

解密命令應記載下列事項:

doi:10.6342/NTU202301879

一、案由。

二、解密標的。

三、解密義務相對人。

四、解密期限。

五、聲請機關。

六、違反解密命令之法律效果。

第四條（法院受理聲請解密命令程序）

法官受理聲請核發解密命令程序，得命聲請機關或解密義務相對人提出說明。

核發解密命令之程序，不公開之。

聲請經法院駁回者，不得聲明不服。

第五條（保密義務及罰則）

解密義務相對人或其他參與解密程序之人，就解密過程所知悉之偵查內容，應予保密。公務員於執行解密命令過程中知悉解密義務相對人之解密密碼、方法或技術者，亦同。

前項之人無故洩漏前項應保密之秘密者，處二年以下有期徒刑，拘役，或新臺幣五十萬元以下罰金。

第六條（違反義務之刑事處罰）

明知解密密碼、方法或技術而不履行解密命令者，處二年以下有期徒刑，拘役，或新臺幣伍佰萬元以下罰金。

法人暨其代表人為解密義務之相對人，而其代表人違反前項犯罪者，除處罰行為人外，對該法人並科以該條所定十倍以內之罰金。

doi:10.6342/NTU202301879

第六章 結語

數位時代的來臨，加密技術帶來人類使用數位科技時之資訊安全保護，但也同時造成執法機關查緝不法犯罪之嚴重阻礙，過去能透過通訊監察、搜索等法定程序蒐集到的犯罪證據，於加密時代來臨後，上開犯罪偵查方式已逐漸無用化，執法機關犯罪偵查之能力受到嚴重挑戰，而此情形已普遍存在於世界各國，亦已受到國際組織之重視。

面對加密技術對於查緝不法犯罪甚至國家安全所造成之衝擊，諸多法制先進國家紛紛透過立法方式做出對策，分析世界上常見之立法對策大致可分為「解密令狀」以及「國家木馬」2 大類別，解密令狀是透過政府發出具強制力命令之方式強制持有解密金鑰之人交出解密方法貨協助解密，此種方式通常搭配違反解密命令之刑事處罰賦予其強制力；國家木馬則是透過內國法立法授權國家於符合一定程序、要件之情形，得以合法對特定對象所使用之資訊設備植入木馬，以取得國家所需之資訊。觀察英國、法國、德國、荷蘭及澳洲之立法歷程，可以發現上開國家早年分別有採用解密令狀或國家木馬之立法，然有鑑於舊法不足以因應加密技術對於執法及國安所帶來之強大衝擊，紛紛於 2016 年開始接連發動修法，強化國家基於執法及國家安全之目的對抗加密之措施。

英國 2000 年立法制定之調查權規範(RIPA)，係以解密為規範中心，明定法院、國務大臣可依 RIPA 第 49 條規定發出解密令狀強制特定人針對受加密保護之電磁紀錄，交出解密金鑰或協助解密，然 RIPA 自 2007 年施行後，履行第 49 條通知之狀況不佳，違反第 49 條解密義務並依同法第 53 條規定受到刑事處罰之比例甚低，第 49 條解密義務無法有效發揮預期功效，因此英國國會 2016 年又制定調查權力法(IPA)，擴大政府調查權，同時引進司法監督。2016 年調查權力法重點包含:(1)創設電信事業保留互聯網連接紀錄之法定義務，授權國務大臣得以發出互聯網連接紀錄保留通知，強制特定電信事業

doi:10.6342/NTU202301879

保留互聯網連接紀錄、(2)擴大原本 RIPA 之第 49 條解密通知，將原本之解密客體自通訊內容擴大到元數據、(3)創設「技術能力通知」，明定國務大臣得向電信商發出技術能力通知，要求電信商或郵政運營商提供有關授權事項有關之任何協助、(4)創設「設備端干預」之國家木馬，並區分為「目標型」(執法目的)以及「大量型」(國安目的)，以此方式從設備端取得通訊內容、設備數據或其他資訊。另外，為平衡諸多政府調查權力之擴大，調查權力法創設司法審查制度，由總理任命現任或前任法官出任司法委員乙職，職司調查權力法之個案審查及通案監督。

法國刑事訴訟法早於 2004 年即有關於解密命令相關規定，2015 年法國巴黎發生恐怖攻擊之後，法國國會展開修法，於 2016 年 6 月 3 日修正刑事訴訟法第 706-73 條以下「特殊偵查技術」相關規定，強化執法機關對抗組織犯罪、恐怖主義、資助恐怖主義犯罪之調查權，其中包括增訂刑事訴訟法第 706-95-1 遠端訪問通訊內容之規定(小木馬)以及同法第 706-102-1 秘密線上搜索規定(大木馬)，透過國家木馬之授權，補足原先立法之不足。

德國在 2017 年修正刑事訴訟法，新增「來源端通訊監察」及「秘密線上搜索」2 種新興干預手段，「來源端通訊監察」作為傳統通訊監察之補充手段，將來源端通訊監察所能取得之資訊，緊扣於傳統通訊監察所能監察之通訊內容，定位上係與傳統通訊監察之功能等價；而「秘密線上搜索」可取得之資訊範圍及於設備內儲存之所有資料，惟禁止主動製造資料，亦即並未授權開啟麥克風、攝影機等功能蒐集資料，於立法方式上將木馬依其功能區分為大、小木馬，並依其基本權干預程度而異其程序規範。

荷蘭早於 2002 年情報安全法即可見政府木馬及解密令狀相關規定，復於 2018 年公布第三部電腦犯罪法，增訂「解密令狀」、「國家木馬」及「下架（刪除移轉）權」3 大授權。第三部電腦犯罪法修訂刑事訴訟法第 125k 條，授權執法機關得對於擁有加密技術之法人發出解密令狀，強制相對人提出解

doi:10.6342/NTU202301879

密金鑰或解密後之資料，然相對人不可為受到不自證己罪原則保護之犯罪嫌疑人。第三部電腦犯罪法另修訂刑事訴訟法第 125nba、第 125uba 及第 125zba 條有關國家木馬之授權規定，授權國家可以透過植入木馬之方式取得相關資訊，甚至可以透過打開麥克風、鏡頭等方式特定使用者身分或進行系統監視。此外，荷蘭是少數針對「設備位置所在地不明」訂有管轄權特別規定之國家，明定可以針對刻意隱匿而使所在位置不明之設備植入木馬，執行後倘發現設備所在地屬其他國家司法管轄，後續應透過司法互助方式為之，然若向該國提出司法互助請求，他國並未回復，仍可繼續執行。

澳洲之立法趨勢不同於上開國家，其原本即有國家木馬相關規定散落於不同法令中，2018 年大規模修正電信和其他法律修正(協助和訪問)法(TOLA ACT)，兼採鼓勵及強制之方式，授權澳洲執法機關、情報機關可以透過發出請求（不具強制力），或是通知（具強制力）之方式要求通信服務商解密、提供技術協助甚至開發新技術、或對於產品或服務加入新功能，其大致分為(1)技術協助請求（不具強制力）、(2)技術協助通知（具強制力）及（3）技術能力通知(具強制力)3 種類型，其中技術能力通知之協力義務已包羅萬象，可強制業者在切實可行及技術可達之範圍以內，開發新技術以協助政府取得加密資訊。值得注意的是，上開 3 種授權之程序監督均僅限行政權內部，並無司法審查權之設計。TOLA ACT 亦有電腦訪問令之規定，授權執法機關得以透過木馬方式執行遠端搜索，其授權範圍包括攔截通訊對話內容，無庸另外取得攔截令。

相較於上述英國、法國、德國、荷蘭及澳洲等國針對加密技術對於執法之衝擊均積極透過立法反制，我國迄今科技偵查法立法仍牛步，連技術層級較低、干預程度相對輕微之全球定位系統（GPS）、國際行動用戶識別碼截收器（IMSI-Catcher）之立法均尚未完成，更遑論技術問題更為複雜，干預程度遠高於前開科技偵查手段之國家木馬。然而，在面對犯罪者已「受惠」於加

doi:10.6342/NTU202301879

密技術逐漸逃脫法律制裁之同時，吾人不能否定國家負有打擊犯罪、保護人民之重要義務，在犯罪者「科技化」之同時，科技執法已係時代趨勢。「要馬兒好，不能要馬兒不吃草」，此乃每個人都能理解之基本常理，我國倘不能於科技偵查立法議題上理性思考，不僅將於科技偵查之立法腳步上落後，更無法於臺灣這塊土地上遏止犯罪增長。加密技術所建構之網路安全機制，帶給個人於網路使用上最基礎之保護，故所謂「對抗加密」之立法，絕不是用來反對或阻礙加密技術之發展，而係在鼓勵加密技術發展之前提下，基於國家保護人民、追訴犯罪之義務下，不讓犯罪者因而受惠。在各類犯罪均與電腦、網路脫不了關係之今日，犯罪行為也受到加密技術之掩護而輕易逃避國家對於犯罪之查緝，此非人民之福。國家面對加密技術所帶來之執法衝擊時，應積極以技術反制，以履行國家查緝不法犯罪以保護人民之義務，而非消極坐視犯罪問題日益氾濫；另一方面，更應恪遵憲法保障人民基本權所揭示之各項原理原則，遵循法治國原則下對於人民基本權利之干預均須有民主正當性的法規為基礎之憲法誡命，而國家唯有於技術及法治兩者發展均能跟上時代趨勢，方可謂盡到國家對於人民應盡之責任及義務。

本文盤點及分析比較法上立法對策後，結論上認為，英國、法國、德國、荷蘭及澳洲等國無論其立法發展歷程為何，最終均清一色兼採國家木馬以及業者協力義務 2 種立法對策，一方面授權並規範國家使用木馬，另一方面加重甚至擴大業者之協力義務，此種「兼採」之立法模式確有其必要性，在科技技術發展一日千里之時代，吾等雖不可否認國家木馬係最有效之因應對策，無庸以刑事制裁手段對解密技術持有人苦苦相逼，立法例上亦已可見英國、法國過去單採解密令狀之立法方式，顯然無法達到預期功效，然而，反面而論，倘若全盤捨棄「業者協力義務」單單仰賴「國家木馬」一種方式，亦未必能確保我國木馬技術隨時能更上科技發展的腳步，再者，企業在面對商業利益、公司政策、契約責任、法律義務及社會責任之多面向考量下，與其說

doi:10.6342/NTU202301879

業者不欲立法者立法課予協力義務，應係更不願政府在沒有法律依據之情況下強行要求企業配合，在法治國原則下，立法課予業者一定程度合理之協力義務，應係與企業洽談之基本籌碼，也給予企業提供協助之合法性基礎，基此，本文認為兼採國家木馬以及業者協力義務之雙重立法有其必要性。

在國家木馬之立法抉擇上，英國、法國、德國、荷蘭及澳洲等國之國家木馬功能均包括設備端通訊監察（小木馬）以及秘密線上搜索（大木馬），而我國之科技偵查立法決策上，究竟是否要兼採大木馬及小木馬，確實面臨兩難抉擇，本文固不否認在立法推動策略上，若兼採大木馬在立法過程中恐面對更大阻礙，然而，執法機關面對打擊具組織性、跨國性、資通性之犯罪，倘無秘密線上搜索作為偵查手段，實難以期待能針對組織犯罪一網打盡，更遑論從 EncroChat 行動後續在歐洲多國引發之法律爭議可知，未來在跨國執法合作上，亦需要具備與其他國家程度相近之法律規範，作為執法合作之基礎，具有經得起後續司法檢視之執法依據，也才能使查緝不法犯罪成果得以維繫。是以，本文認為我國除有立法增訂「設備端通訊監察」之必要性以外，亦應同時增訂「秘密線上搜索」之國家木馬授權。

他山之石，可以攻錯，本文透過國際立法趨勢之介紹，作為我國立法正當性之佐證，並進一步提出設備端通訊監察、秘密線上搜索以及解密令狀之立法方向及建議草案條文，期盼能為我國面對加密科技發展所帶來之執法衝擊提出法制面之立法建議，並期盼立法者早日完成立法，使第一線執法者有「法」可循，才能有效履行人民所賦予之查緝犯罪、追訴不法之國家使命。

doi:10.6342/NTU202301879

參考文獻

一、 中文文獻

（一） 專書及期刊論文

1. Prof. Dr. Mark A. Zöller，譯者王士帆，來源端電信監察與線上搜索-德國刑事追訴機關之新手段，司法新聲，第 130 期，2019 年 4 月。
2. Prof. Dr. Arndt Sinn，譯者黃則儒，新的秘密偵查措施-來源端通訊監察及線上搜索，檢察新論，第 27 期，2020 年 2 月。
3. 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，司法週刊，第 1779 期，2015 年 12 月。
4. 王士帆，網路之刑事追訴－科技與法律的較勁，政大法學評論，第 145 期，2016 年 6 月。
5. 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 12 月。
6. 王士帆，德國科技偵查規定釋義，法學叢刊，第 262 期，2021 年 4 月。
7. 王士帆，科技偵查立法之可行性評估及建議方向（發言紀錄），檢察新論，第 27 期，2020 年 2 月。
8. 朱富美，國安偵查與基本權保障-「科技偵查法」草案「設備端通訊監察」章評析與建議，法學叢刊，第 260 期，2020 年 10 月。
9. 朱富美，黑暗將至？論網路偵查因應加密科技之立法新架構，法學叢刊，第 266 期，2022 年 4 月。
10. 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。
11. 何賴傑，論德國刑事訴訟程序「線上搜索」與涉及電子郵件之刑事處分，月旦法學雜誌，第 208 期，2012 年 9 月。
12. 吳俊毅，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的困境，刑事政策與犯罪研究論文集（23），

doi:10.6342/NTU202301879

法務部司法官學院，2020 年。

13. 林鈺雄，刑事訴訟法（上冊），新學林出版股份有限公司，2019 年 9 月，九版。
14. 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，第 96 期，2007 年 4 月。
15. 林鈺雄，科技偵查概論：干預屬性及授權基礎(下)，《月旦法學教室》，第 221 期，2021 年 3 月。
16. 林鈺雄，侵入資訊科技系統之來源端通訊監察，月旦法學教室，第 223 期，2021 年 5 月。
17. 林國翔、沈士豪、李鎮宇，取得加密通訊內容因應對策—從通訊監察技術觀點出發，臺灣警察專科學校警專學報，第 7 卷第 6 期，2021 年 2 月。
18. 施育傑，科技時代的偵查干預處分—兼論我國法方向，月旦法學雜誌，第 306 期，2020 年 11 月。
19. 施弘文，以科技偵查跨境取得證據之研究-以美國法為中心（發言紀錄），檢察新論，第 27 期，2020 年 2 月。
20. 陳芊儒，通訊軟體加密技術下個隱私與國家安全保護之平衡，科技法律透析，第 31 卷第 9 期，2019 年 9 月。
21. 高儀庭、金孟華，以木馬程式作為我國科技偵查手段之研究，萬國法律，第 240 期，2021 年 12 月。
22. 張麗卿，監察網路通訊作為抗制犯罪手段之原則及界線，輔仁法學，第 57 期，2019 年 6 月。
23. 張陳弘，美國聯邦憲法增修條文第 4 條搜索令狀原則的新發展：Jones, Jardines & Grady 案為例，《歐美研究》第 48 卷第 2 期，2018 年 6 月。
24. 黃銘輝，淺談當前課予通訊服務業者協力義務的困境與突破（下），桃律通訊，第 22 期，2021 年 3 月 1 日。
25. 楊雲驊，通訊保障及監察法實施前電話監聽合法性及證據評價之探討，臺灣本

doi:10.6342/NTU202301879

土法學雜誌，第 57 期，2004 年 4 月。

26. 蔡宗珍，法律保留思想及其發展的制度關聯要素探微，臺大法學論叢，第 39 卷第 3 期，2010 年 9 月。

27. 薛智仁，司法警察之偵查概括條款？-評最高法院 2013 年度台上字第 3522 號判決，月旦法學雜誌，第 235 期，2014 年 11 月。

（二）學位論文

1. 施育傑，數位、科技與刑事程序干預處分-資訊框架理論之建構，政治大學法律學系博士論文，2020 年。

2. 陳俞伶，網路搜索之法規範研究-以雲端硬碟搜索及線上搜索為核心，國立清華大學科技法律研究所碩士論文，2018 年 7 月。

3. 秦裕國，行動即時通訊軟體安全設定認知之研究—以 LINE 為例，東吳大學商學院資訊管理學系碩士論文，2016 年 6 月。

4. 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院碩士在職專班科技法學組碩士論文，2005 年 6 月。

5. 黃逸玲，行動通訊 APP 偵查與對策之研究，中央警察大學刑事警察研究所碩士論文，2018 年。

6. 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論文，2019 年。

（三）其他中文資料

1. 王晴玲，對已具加密功能之通訊軟體之通訊監察之理論與實務，出國報告（出國類別：研究），2015 年 11 月 20 日。

2. 何煒華 秦裕國，行動通訊軟體 LINE 的安全設計探討，2016 年第十屆資訊科技國際研討會/第六屆臺灣網路智能學會學術論壇，2016 年 4 月 23 日。

doi:10.6342/NTU202301879

3. 廖有祿、張維平、蘇莞筑、劉怡汎，網路平台業者紀錄保存規範之研究，2013年犯罪偵查學術與實務研討會，2013 年 5 月 30 日。
4. 張永明，一般行為自由與一般人格權作為憲法保障之基本權，司法院大法官106 年度學術研討會-「憲法解釋與憲法上未列舉之權利」第三場報告，2017年 12 月 2 日。

二、 外文資料

1. Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for –2012 – 2013（2013）.

2. Annual Report of the Chief Surveillance Commissioner to the Prime Ministe r and to the Scottish Ministers for –2013 – 2014（2014）

3. Annual Report of the Chief Surveillance Commissioner to the Prime Ministe r and to the Scottish Ministers for –2014 – 2015（2015）

4. Annual Report of the Investigatory Powers Commissioner 2019 (2020).

5. Annual Report of the Investigatory Powers Commissioner 2020 (2022).

6. Bill to Combat Organized Crime, Terrorism, and Their Financing EHRR4.

7. Bill to Combat Organized Crime, Terrorism, and Their Financing (No.3515) Amendment No.221, (Feb.25, 2016).

8. Bhairav Acharya, Kevin Bankston, Ross Schulman, and Andi Wilson Thomp son, Deciphering the Encryption Debate in Europe: France, Open Technolog y Institute 2017b, (July 2017).

doi:10.6342/NTU202301879

9. Bauer, S. and Bromley, the Dual-Use Export Control Policy Review: Balanci ng Security, Trade and Academic Freedom in a Changing World. Non-Prolif eration Papers by the EU Non-Proliferation Consortium. No. 48. (March, 20 16).

10. Beatrix Immenkamp, Review of dual-use export controls, EPRS | European Parliamentary Research Service, (July 2021).

11. Carlos Liguori, Exploring Lawful Hacking as a Possible Answer to the "Goi ng Dark" Debate, 26 MICH, (2020.)

12. Coalition Against Unlawful Surveillance (CAUSE), 'A critical opportunity: br inging surveillance technologies within the EU Dual-Use Regulation', (June 2015).

13. C Barker, M Biddington and H Portillo-Castro, Telecommunications and Oth er Legislation (Assistance and Access) Bill 2018, Bills digest,49, 2018–19, P arliamentary Library, Canberra, (3 December 2018).

14. Daniel Severson, the Encryption Debate in Europe, Jean Perkins Foundation Working Group on National Security, Technology, and Law (Hoover Instituti on), Aegis Series Paper No. 1702 (March 21, 2017).

15. David. Anderson QC, David. Anderson: The Investigatory Powers Bill is stil l a work in progress, TheTelegraph (March. 2, 2016)

16. Department of Home Affairs, Telecommunications (Interception and Access) Act 1979 Annual Report 2018-2019.

doi:10.6342/NTU202301879

17. Department of Home Affairs, Industry assistance under Part 15 of the Telecommunications Act 1997(Cth): Administrative Guidance for Agency Engagement with Designated Communications Providers, Document.
18. Department of Home Affairs, Surveillance Devices Annual Report 2018-19.
19. Fact Sheet, Investigatory Powers Bill: Internet_Connection_Records (ICRs)
20. Gemma Davies, Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers, Journal of Criminal Law 84 (407), (Oct. 2020).
21. H Abelson et al, the risks of key recovery, key escrow, and trusted third-party encryption, Columbia Academic Commons, (June 28, 2010).
22. Home Department, Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny, Cm 9219 40–41 (2016).
23. International Statement: End-To-End Encryption and Public Safety, October 11, (2020).
24. Independent National Security Legislation Monitor (INSLM), Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters (TOLA Act Report).
25. IACP summi Report, Privacy and Public Safety: A LAW Enforcement Perspective on the Challenge of Gathering Electronic Evidence (2015).
26. J Potapchuk, 'A Second Bite at The Apple: Federal Courts' Author- ity to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data, Under The AlI Writs Act' （2016）.
27. Joint Committee Report on the Draft Investigatory Powers Bill, HL Paper 93, HC 651 79 (2016).
28. Lorna Woods, the Investigatory Powers Act 2016, 3 EUR. DATA PROT. L.

doi:10.6342/NTU202301879

103-104 REV. (2017).

29. Joshua Eaton, With or Without Evidence, Terrorism Fuels Combustible Encryption Debate, Christian Sci. Monitor (Mar. 28, 2016).
30. Law Council of Australia, Review of the amendments made by the Telecom munications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth).
31. Letter from G.A. Van der Steur, Minister of Security and Justice, and H.G.J. Kamp, Minister of Economic Affairs, to the PresId.ent of the House of Re presentatives of the States General regarding the Cabinet's View on Encrypti on, No. 708641 (Jan. 4, 2016).
32. Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluati on and Comparison of Practices Study, European Parliament,（March. 2017）.
33. Manhattan District Attorney's Office, Report of the Manhattan District Attorn ey's Office on Smartphone Encryption And Public Safety (2015).
34. M Fidler, Regulating the Zero-Day Vulnerability Trade: A Prelimi- nary Ana lysis' (Social ScienceResearch Network 2015).
35. Marczak, B. et al., Pay No Attention to the Server Behind the Proxy: Mapp ing FinFisher's Continuing Proliferation. Munk School of Global Affairs. (20 15).
36. Machiko Kanetake, the EU's Export Control of Cyber Surveillance Technolo gy: Human Rights Approaches', Business and Human Rights Journal, Vol. 4 (1), (2019).
37. NCMEC's Statement Regarding End-to-End Encryption, (October 3, 2019)
38. OS Kerr and B Schneier, Encryption Workarounds, 106 Georgetown Law Jo urnal, (2018).

doi:10.6342/NTU202301879

39. Overview of France's Intelligence Legal Framework, Félix Tréguer, (Decemb er 2021).
40. Parliamentary Joint Committee on Intelligence and Security, Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, (DEC 2021).
41. Policy Department for Citizens' Rights and Constitutional Affairs, Pegasus a nd surveillance spyware, (May 2022).
42. Regulation of Investigatory Powers Act 2000, c. 23, introductory text (U.K.).
43. Surveillance Devices Annual Report 2019-20.
44. Thiago Moraes, Sparkling Lights in the Going Dark: Legal Safeguards for L aw Enforcement's Encryption Circumvention Measures, 6 EUR. DATA PRO T. L. REV. 41 (2020).
45. The Independent National Security Legislation Monitor (Dr James Renwick CSC SC), Report on Telecommunications and other Legislation Amendment (Assistance & Access) Act and related matters, (June 30, 2020).
46. Telecommunications and Other Legislation Amendment (Assistance and Acce ss) Bill 2018, Revised Explanatory Memorandum UNESCO, Human Rights a nd Encryption, UNESCO.
47. The Wassenaar Arrangement – On Export Controls for Conventional Arms a nd Dual-Use Goods and Technologies.
48. UK Government Home Office, Equipment Interference Code of Practice (201 8).
49. UK Government, Operational Case for Bulk Powers.
50. WePROTECT Global Alliance, 2019 Global Threat Assessment.

doi:10.6342/NTU202301879