



元照出版提供 請勿公開散布

「秘密」搜索扣押第三方業者 數位證據 ——鬆動最高法院Hibox案基準

王 士 帆*

要 目

壹、前 言	參、搜索扣押第三人之被告程序保障
貳、最高法院Hibox案見解與分析	一、搜索扣押公開性
一、法律爭點	二、搜索扣押被告在場權與抗告權
二、Hibox案基準	(一)在場權
(一)秘密通訊自由之時間界限	(二)抗告權
(二)「過去已結束」之通訊內容	(三)搜索票和扣押裁定之應受送達人
三、搜索扣押電子郵件	三、「暫緩通知被告」之立法構思
(一)保全方式	(一)秘密鬆動Hibox案基準
(二)提出或交付命令	(二)德國2021年增訂「暫緩通知
(三)《刑事訴訟法》第133條之1	被告」規定
第1項目的性限縮	肆、結 論

DOI : 10.53106/102398202024030176002

* 國立臺北大學法律系副教授，德國慕尼黑大學法學博士。本文初稿發表於2023年1月11日《第78屆司法節學術研討會》。本文為行政院國科會補助專題研究計畫（NSTC 112-2410-H-305-004-MY3）成果之一。

投稿日期：一一二年二月二十七日；接受刊登日期：一一二年五月十五日

責任校對：鍾淑婷



摘 要

現代人手機不離身，暴露大量足跡於網際網路已屬常態，對偵查機關而言，掌握數位證據將提高犯罪追訴效率，具有高度調取價值。是以，傳統強制處分搜索扣押正面臨數位轉型，逐步從公開執行局部轉為秘密偵查。針對偵查機關於第三方業者處搜索扣押被告數位證據，最高法院106年度臺非字第259號刑事判決肯認被告之隱私權受到侵害，且將秘密通訊自由保障範圍限於過去已結束的通訊內容，對於調取通訊已結束之郵件內容，應適用搜索扣押規定。然而，依現行法規定，被告原則上有搜索在場權及受通知權，國家倘逕行「秘密」搜索扣押，將鬆動Hibox案判決基準。展望未來立法芻議，法規主管機關應兼顧保障被告救濟權與國家追訴犯罪之憲法任務，參酌比較法例，審慎思辨第三人受搜索扣押時的暫緩通知被告規定。

關鍵詞：秘密通訊自由、搜索、扣押、在場、訴訟權



壹、前言

臺灣今日生活，Email、Facebook、Instagram、LINE、WeChat、Google應用程式（雲端硬碟、日曆、地圖等）和物聯網裝置等，或許不是人人有帳號，但若說你我每天總會點選其中的幾種或幾次，實在再日常不過。新冠疫情肆虐期間因居家隔離，科技遠端互動更是加深人們網路浸漬感和依賴度。一份2022年3月的統計調查，「全台有2,172萬的網路用者，約佔91%人口數；而活躍的社群平台用戶則高達2,135萬，佔全台89.4%」、「國民每日平均聯網時間為8小時7分鐘，其中有4分之1的時間（2小時4分鐘）都用於社群媒體」¹。而國人普遍熟悉的LINE，該臺灣公司在2022年11月16日舉辦年度LINE CONVERGE行銷年會，公布「2022 LINE使用行為研究調查」，調查顯示目前臺灣2,100萬LINE用戶，一週使用率達93%，每位用戶平均使用6.1個LINE服務，最常用的LINE服務是即時通訊²。

這些由網路平台、網路內容或網路應用服務等網路服務提供者（Internet Service Provider, ISP）供應的軟體程式，成為智慧型手機的標配。不管是雲端硬碟、電子郵件或網路即時通訊，一般用戶必須藉助這些第三方業者的程式服務，才能享用網路去地域化和資訊數位化的科技便利。以全球超過18億用戶的Gmail為例，2022年7月在Google使用介面中整合Gmail、Meet、Chat（即時通）與

¹ 【2022台灣社群平台指南】社群行銷選平台，你該知道的重點數據！，TenMax，2022年3月18日，https://www.tenmax.io/tw/archives/56490?_trms=0282cf8891ce62c7.1672680802779，最後瀏覽日：2024年1月28日。

² LINE用戶一周使用率達93% 最常用這項功能，壹蘋新聞網，2022年11月16日，<https://tw.nextapple.com/gadget/20221116/38A632191C4167DB72E82753619BAEDF>，最後瀏覽日：2024年1月28日。



Spaces（聊天室）四項Workspace的產品³，企圖心之大，可謂囊括人們的平常網路溝通型態。況且，「隨著科技日新月異，手機之普及與便利已快速改變人類生活習慣，使其成為現代人與外界互動之重要媒介，廣泛形成手機如同其使用者之貼身物品」⁴，於是乎，現代人隨時、隨地使用手機，不僅是手機暴露的位置資訊，上傳或備份於網路服務提供者伺服器之電子資料等「數位證據」⁵。掌握這些數位證據，可能是澈底認清一個人的最佳方式，自然也具有追訴犯罪意義的調取價值。

偵查機關欲取得刑事被告在第三方業者處儲存的個人電子郵件、影音或文件等數位證據，事涉國家取證手段與被告和第三方業者之間基本權干預關係。於法律保留原則下，所涉基本權不同，干預手段自應有異，授權基礎亦應有別，並禁止對受干預人不利益之類推適用。所謂「強制處分法定原則」⁶，也應貫徹於科技偵查面向⁷。具體而言，當調取客體是秘密通訊自由保護的數位通訊內容，或不受秘密通訊自由保護，而屬資訊隱私權保障的影像或文

³ 工作效率大提升！Gmail整合郵件、Meet、Chat、Space更新優化搜尋，數位時代，2022年7月29日，<https://www.bnnext.com.tw/article/70938/gmail-web-update->，最後瀏覽日：2024年1月28日。

⁴ 最高法院110年度臺上字第4549號刑事判決。

⁵ 最高法院111年度臺上字第1021號刑事判決表示，數位證據指儲存於電磁紀錄載體，或是以數位方式傳送，於審判中得用以證明待證事實之數位資訊。而將該數位資訊內容，以機械、照相、化學、電子或其他科技方法，「準確重製」之產出物，乃原始證據內容重現之複製品，自與原始證據具有相同之證據能力，例如LINE對話內容紀錄畫面之翻拍照片，或列印成紙本文件。

⁶ 「強制處分法定原則」概念，參見如陳運財，GPS監控位置資訊的法定程序，台灣法學雜誌，293期，頁67-69，2016年4月14日。

⁷ 實例如最高法院106年度臺上字第3788號刑事判決（GPS偵查）、110年度臺上字第4549號刑事判決（M化車定位追蹤）。



件，會分流成需要不同干預授權基礎。前者應依侵害秘密通訊自由的干預授權為之，例如我國《通訊保障及監察法》，後者則是依循對資訊隱私權的干預授權規定，典型偵查方法是向受搜索扣押人實施公開的搜索扣押（參見刑事訴訟法第42條第4項、第125條、第139條第1項、第145條、第148條與第150條）。

以搜索扣押來說，當第三方業者提供網路服務給被告使用，偵查機關為了取得被告存放的數位證據，舉凡扣押第三方業者伺服器內儲存已讀取過的Email、遊戲網站聊天對話紀錄、社群帳號使用者資料或雲端檔案，對無犯罪嫌疑之第三方業者發動搜索扣押，同時會建立對被告——屬被告所有或與被告有關資訊或資料的——數位證據之受干預性（Betroffenheit）⁸。換言之，在這種情形，搜索扣押規定成為偵查機關干預及保全第三方業者處被告數位證據的法律授權基礎。2018年，最高法院106年度臺非字第259號刑事判決所謂Hibox案⁹，正是以調取被告存放第三方業者（中華電信公司）伺服器的已讀取之電子郵件，是否干預被告秘密通訊自由、應依什麼規定進行保全作為法律爭點，結論上，其樹立Hibox案基準：「過去已結束」的通訊內容，屬資訊隱私權，應回歸適用《刑事訴訟法》之搜索扣押規定。

數位證據所向披靡，無所不在，刑事訴訟的傳統強制處分和證

⁸ Vgl. BT-Drs. 19/27654 v. 17. 03. 2021, S. 61; *Becker/Dogan*, StV 2022, S. 461.

⁹ Hibox判決評釋，可參見李榮耕，犯罪偵查中通訊內容的調取，國立臺灣大學法學論叢，51卷3期，頁757-831，2022年9月；林恆吉，論新進通訊之正當法律程序——以Hibox為例，司法周刊，1924期，2-3版，2018年10月26日；黃朝義，網路通訊資料保障與網路通訊監察——以取得過去已結束通訊內容為主，中央警察大學法學論集，35期，頁45-89，2018年10月；薛智仁，2017年刑事程序法回顧：刑事救濟程序、證據法則與強制處分，國立臺灣大學法學論叢，47卷特刊，頁1924-1926，2018年11月。



據法則，不得不面臨數位轉型：雲端偵查（Ermittlung in der Cloud）早就示警刑事追訴迎接新挑戰¹⁰，域名扣押議題一語成讖¹¹；加密通訊手機當道，動用跨國木馬入侵實施監察，像2020年法國協同歐盟執法機構瓦解EncroChat案，成為國際合作打擊犯罪趨勢，但衍生跨國數位證據的證據能力適格性爭議¹²。搜索扣押從公開執行，局部轉變為「秘密」偵查措施，也是受科技偵查影響鮮明之例。承此背景，本文擬以搜索扣押第三方業者處被告數位證據為主題，先說明最高法院Hibox判決見解與本文分析（本文貳）。其次，本文嘗試論證依現行法，於第三方業者處搜索扣押被告數位證據時，應使數位證據所有人之被告知情，這是出於保障被告聽審權與救濟權之目的；若未通知被告，對被告而言屬「秘密」搜索扣押第三方業者，將鬆動Hibox案基準。展望未來立法芻議，建議法規主管機關充分檢討兼顧保障被告程序權利與國家追訴犯罪之憲法任務，參酌比較法例，審慎思辨第三人搜索扣押時的暫緩通知被告規定妥適性（本文參）。文末，以結論總結全文（本文肆）。

¹⁰ Vgl. *Obenhaus*, NJW 2010, S. 651ff.

¹¹ 參見陳昱奉，網路犯罪與資訊安全的未來——從網域名稱扣押談網路治理，刑事政策與犯罪防治研究專刊，32期，頁219-290，2022年8月；蔡志宏，剝奪犯罪工具之數位轉型——域名之沒收與扣押，刑事政策與犯罪防治研究專刊，31期，頁197-237，2022年4月。

¹² Vgl. BGH, Beschl. v. 02. 03. 2022 – 5 StR 457/21; Böse, JZ 2022, S. 1048-1056; Derin/Singelnsteins, NStZ 2021, S. 449-454; Löffelmann, JR 2022, S. 454-460; Ruppert, NZWiSt 2022, S. 221-227; Weiss, ZfStW 2022, S. 427-438.



貳、最高法院Hibox案見解與分析

一、法律爭點

Hibox案是非常上訴判決，案情約略為：被告是六合彩組頭，提供電話予賭客傳真簽單，其等再將簽單傳真予上游組頭簽賭。被告租用中華電信Hibox服務，這項服務會將賭客的簽注單傳真電子化，即轉換成Email的附件，寄到組頭被告租用的Hibox信箱，這些簽注單的電子郵件遂成為被告涉犯賭博罪之關鍵證據。原確定判決維持第一審判決見解，認為Hibox數位傳真列印資料是由中華電信伺服器儲存傳真影像而傳送訊息，涉及通訊內容，應以《通訊保障及監察法》第5條「通訊監察書」方可取得，但偵辦檢察官以同法第11條之1「通信紀錄調取票」調取Email內容，違反同法第5條規定，依同法第18條之1第3項規定，調取之Email不得採為證據用途，因而維持第一審之無罪諭知，駁回檢察官上訴。

對確定判決之見解，檢察總長提起非常上訴，本案法律爭點是，當被告已讀取電子郵件，將郵件保留在中華電信Hibox的郵箱伺服器時，偵查機關欲保全該電子郵件，應適用《通訊保障及監察法》或依《刑事訴訟法》之搜索扣押？在此先指出Hibox判決的結論：偵查機關為犯罪偵查目的，需取得「過去已結束」之Hibox傳真通訊內容時，該通訊內容屬於被告之資訊隱私權範圍，應回歸適用《刑事訴訟法》，依刑事訴訟搜索、扣押相關規定為之¹³。

¹³ 最高法院106年度臺非字第259號刑事判決，行碼357-360。



二、Hibox案基準

(一)秘密通訊自由之時間界限

在Hibox案，保全被告在第三方業者處儲存的電子郵件，究竟應適用《通訊保障及監察法》或《刑事訴訟法》之搜索扣押，回答關鍵在於被告已讀取過的電子郵件，是否仍受秘密通訊自由保護。依德國法理解¹⁴，維護秘密通訊自由的宗旨，乃在保護人民免於遭受通訊過程脆弱性的特殊危險狀態。詳言之，在保護有空間距離的通訊雙方，當其仰賴通訊設備交流彼此訊息內容時，因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，亦即，通訊方使用他們無法支配的通訊媒體，這會比他們在場面對面直接溝通，更容易受到國家有心干預。所以，秘密通訊自由在對抗使用通訊設備所形成的侵擾秘密之特殊危險。鑑於使用通訊設備傳達訊息內容有此特殊危險性，故有特殊的保護必要性。在此宗旨下，秘密通訊自由應盡可能維護通訊雙方如同未使用通訊設備，彷彿親身在場般交流意見。否則，有空間距離的雙方，如忌憚脫離其支配的通訊設備，易受第三人或國家侵擾而不敢信賴使用，「寒蟬效應」將有害資訊傳遞和意見交流¹⁵。

在此認知下，秘密通訊自由的保障範圍，會隨訊息送達接收人及傳遞過程結束而終止。易言之，秘密通訊自由有保障範圍之時間

¹⁴ 以下說明參見王士帆，德國聯邦憲法法院BVerfGE 124, 43——扣押伺服器之電子郵件（上／下），司法周刊，1921/1922期，2/2-3版，2018年10月5/12日。Vgl. BVerfGE 124, 43, 54; Durner, in: Maunz/Dürig (Hg.), GG, 84. Aufl., 2018, Art. 10 Rn. 49f.; Kingreen/Poscher, Grundrechte. Staatsrecht II, 38. Aufl., 2022, Rn. 1043.

¹⁵ 蔡宗珍，電信相關資料之存取與利用的基本權關連性（上）——德國聯邦憲法法院BVerfGE 125, 260與BVerfGE 130, 151判決評析，月旦法學雜誌，274期，頁124，2018年3月。



界限（zeitliche Grenze des Schutzbereichs）¹⁶。當訊息抵達接收人，由於訊息已處於接收人的支配範圍，通訊因空間距離所出現的特殊危險狀態，不復存在。所以，「過去已結束」之通訊內容，若該通訊內容已處於接收人支配範圍，其得對已結束通訊過程之訊息內容，自行決定保護或刪除等處理，而非毫無支配可能時，通訊者即不再處於通訊過程脆弱性的特殊危險狀態，便失去秘密通訊自由所顧慮的特別保護需求。不過，收件人對該電子郵件仍得主張資訊隱私權。在干預基本權的審查順序上，秘密通訊自由相較於資訊隱私權具有特別性¹⁷，應優先於資訊隱私權而審查，然個案中若排除秘密通訊自由之保護，不等於一併排除資訊隱私權之保障¹⁸。結論簡言之，當通訊抵達收受人而處於其支配領域時，應由收件人自己採取保護措施對抗其不願發生的資料截取，此時再無因空間隔離，以致通訊有被侵害的特殊危險¹⁹。從而，「過去已結束」之通訊電子郵件，由於不再受到秘密通訊自由保護，所考量的干預授權基礎，不再是《通訊保障及監察法》，而是刑事訴訟之搜索扣押規定²⁰。

¹⁶ 最高法院106年度臺非字第259號刑事判決，行碼296-297。

¹⁷ 司法院釋字第631號解釋理由書：「憲法第12條規定：『人民有秘密通訊之自由。』旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一」。

¹⁸ Vgl. BVerfGE 124, 43, 57.

¹⁹ BVerfGE 115, 166, 184.

²⁰ BVerfGE 115, 166. 惟應注意，德國聯邦憲法法院認為，系爭存放在第三方業者之電子郵件仍受秘密通訊自由保護，但偵查機關得依一般之證據扣押規定（§ 94 StPO）取得電子郵件，參見王士帆，德國聯邦憲法法院BVerfGE 124, 43——扣押伺服器之電子郵件（上），同註14，2版。



(二) 「過去已結束」之通訊內容

以上德國學理見解，連同美國與日本相關見解，均被Hibox判決參酌採納²¹，其表示：「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。……。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」²²。

簡言之，依Hibox案基準，在第三方業者處之被告「過去已結束」的通訊內容，並非「現時或未來發生」之通訊內容，不受秘密通訊自由保護。進一步來說，既然不受秘密通訊自由保護，則調取被告在第三方業者處的已讀取電子郵件，不適用通訊監察書或通信紀錄調取票之取證程序（參見通訊保障及監察法第5條、第6條、第11條之1）²³。附帶一提，美國法有所謂「第三人理論」或稱「第三

²¹ 最高法院106年度臺非字第259號刑事判決，行碼329-331：「德國、美國及日本實務上，將『過去已結束』之通訊內容，有別於『現時或未來發生』之通訊內容，分別適用不同之審查方式，予以保障」。

²² 最高法院106年度臺非字第259號刑事判決，行碼202-220。

²³ 最高法院106年度臺非字第259號刑事判決，行碼345-357。



人原則」，大意是指用戶和第三方業者簽署服務條款，明訂業者為配合司法機關要求，可不經用戶同意而提供用戶資料，原因是用戶分享予第三方業者之個人資訊，乃屬自願揭露或自願交付之行為，用戶對於該等個人資訊，難以主張合理隱私期待²⁴。然而，第三人原則於今日之數位時代已有鬆動，美國聯邦最高法院已表示，隨著高科技發展引發的隱私權之高度風險，現代人使用網路服務進行諸多之通訊及網路活動，用戶個人經常提出敏感性資訊予第三方電信業者，對於交付之資訊，已無法逕自從個人自願分享之角度，一概否決對於用戶個人隱私資訊之保護²⁵。很顯然，Hibox判決在研析包含美國法在內之比較法經驗後，未採納第三人理論²⁶，否則Hibox判決無庸大費周章，詳細探究本案被告資訊隱私權受干預的法律授權基礎。

三、搜索扣押電子郵件

(一)保全方式

對「現時或未來發生」之電子郵件內容進行監察，由於其受秘密通訊自由保護，應適用《通訊保障及監察法》。那依Hibox案基準，不受秘密通訊自由保護的「過去已結束」的電子郵件，應依搜

²⁴ 關於第三人原則的意涵與檢討，詳見溫祖德，偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查——從美國聯邦最高法院判決檢視我國法制，政大法學評論，167期，頁187-190，2021年12月；另參見李榮耕，同註9，頁785-788。

²⁵ 溫祖德，同前註，頁217。

²⁶ 看法相同，李榮耕，同註9，頁799：「第三人理論在涉及調取第三人所持有的本人通訊類型的案件中，沒有適用，或至少應該有所調整。亦即，在現今社會中，人們對於儲存在通訊系統上的訊息，仍享有合理隱私期待」。



索扣押保全，那該如何為之？²⁷一般來說，個人電子郵件會儲存在個人電腦、行動裝置或第三方業者伺服器。電子郵件是一種電磁紀錄，從物理性言，電子郵件非實體物，不能成為受扣押之「物」，但由於存在實體物件，偵查機關欲取得實體物的占有支配，應循搜索扣押規定，即扣押電子郵件所在的儲存載體，例如直接扣押個人電腦硬碟或第三方業者伺服器。

再者，執行扣押電磁紀錄載體應遵守比例原則。扣押儲存載體對持有人而言，未必是相較輕微的干預手段；設想一下，證券公司經理人涉嫌背信，檢調若扣押儲存與證券戶往來資料的全部硬碟，將損及公司的正常營運。準此，基於比例原則，偵查機關一方面應儘量避免檢視無關追訴犯罪意義的私密檔案。另一方面，扣押原因區分成「可為證據或得沒收之物，得扣押之」、「為保全追徵，必要時得酌量扣押犯罪嫌疑人、被告或第三人之財產」（刑事訴訟法第133條第1項、第2項），除非保全沒收（含追徵）執行之扣押，若僅是證據扣押²⁸，應採用較輕微的電子保全措施，通常選項是複製、列印或製作映像檔。在Hibox案的偵查程序，警察向中華電信所調取者，即是被告過去使用「Hibox」服務所接收賭客傳真簽單影像的列印資料。至於這些原物替代品的後續審判證據調查，只要

²⁷ 以下說明，參見王士帆，網路之刑事追訴——科技與法律的較勁，政大法學評論，145期，頁356-358，2016年6月。日本法方面，參見吳天雲，未經刑事司法互助跨國線上搜索扣押電磁紀錄之證據能力——以日本最高裁判所令和3年2月1日判決為中心，檢察新論，31期，頁299-300，2022年11月。

²⁸ 保全沒收扣押與證據扣押概念，可參見王士帆，犯罪所得沒收與追徵之保全扣押——談立法定位，載：沒收新制(二)——經濟刑法的新紀元，頁367-369，2016年9月；朱石炎，刑事訴訟法論，頁179-180，2022年9月，修訂10版；林鈺雄，刑事訴訟法（下冊），頁624-625，2022年9月，11版；林俊益，刑事訴訟法概論（上），頁389-390，2022年9月，22版。亦參見最高法院111年度臺上字第1345號刑事判決。



鑑定同一性無虞（驗真程序）²⁹，即對替代品之真實性不生懷疑時，則依物證性質，循（準）書證或合併勘驗方式調查。

（二）提出或交付命令

Hibox判決認為向第三方業者調取被告過去已結束的電子郵件，不涉及秘密通訊自由。最高檢察署非常上訴意旨同樣，也不認同原確定判決的干預秘密通訊自由見解，惟進一步主張根據「對於應扣押物之所有人、持有人或保管人，得命其提出或交付」（刑事訴訟法第133條第3項，舊法列第2項），可以向中華電信以提出或交付命令之函調方式取得被告電子郵件。最高檢察署說法未受Hibox判決青睞。

Hibox判決否定檢察官函調的結論，值得贊同。然其判決理由中，敘述交付命令通常伴隨後續之強制處分，即得用強制力扣押（刑事訴訟法第138條）的看法，似有待商榷³⁰。道理不難理解，因為當搜索扣押相繼納入（相對）法官保留原則（參見刑事訴訟法第128條、第133條之1），除非情況急迫或經相對人同意得無庸事先向法院請票外（參見刑事訴訟法第130條、第131條、第131條之1、第133條之1、第133條之2），檢察官已無搜索扣押核准權限。假如不服從檢察官的提出命令便自然伴隨後續強制處分之效果，或交付命令本身具有扣押強制力，那立法者設計搜索扣押法官保留豈

²⁹ 數位證據驗真，參見最高法院111年度臺上字第1021號刑事判決；李榮耕，證據驗真及其監管，台灣法律人，7期，頁79-100，2022年1月；沈冠伶，民事訴訟之數位證據與證據調查，月旦法學雜誌，330期，頁77-103，2022年11月；蘇凱平，數位證據如何分辨真偽？如何舉證？，月旦法學教室，233期，頁20-23，2022年3月。

³⁰ 最高法院106年度臺非字第259號刑事判決，行碼385-388：「提出命令，隱含後續之強制處分，受處分人如無正當理由拒絕提出或交付時，通常伴隨著後續之不利處分，即得用強制力扣押之（刑事訴訟法第138條）」。



不形同虛設？正確來說，檢察官的提出命令，正是因為沒有「合法」強制扣押效果，相對人也沒有因為面對交付命令而承受提出應扣押物之義務，偵查機關仍需要向法院聲請搜索票或扣押裁定，以發動搜索扣押。

總言之，現行法之提出或交付命令，並無課予相對人不服從之強制效果³¹。之所以有執行扣押時，立法者允許檢察官得先為提出或交付命令，乃兩全其美之道，因為提出或交付應扣押物後，已達成扣押目的，無庸強制扣押；另一方面，偵查機關在執行合法之扣押權限時，命令提出或交付是比強制扣押更為輕微的手段，在預期不妨害扣押成果時，例如相對人不會因被命提出或交付而預先湮滅證據，執行機關應先命提出或交付，相對人拒絕時再予強制扣押，始符合比例原則³²。

（三）《刑事訴訟法》第133條之1第1項目的性限縮

1. 2016年扣押修法缺失

回到搜索扣押脈絡，Hibox判決認為應依搜索扣押規定，向第三方業者調取被告過去已結束的電子郵件，也就是說，最終目的是扣押電子郵件。值得注意的是，Hibox判決特別提到《刑事訴訟法》第133條之1第1項之證據扣押，「基於維護人民一般隱私權、保障其訴訟權益及實現公平法院之憲法精神，應依目的性限縮，而認不及於『過去已結束』之通訊內容。是以，檢察官對於『過去已結束』之通訊內容之非附隨搜索之扣押，原則上應向法院聲請核發扣押裁

³¹ 立法設計可參考德國《刑事訴訟法》第95條交付義務（Herausgabepflicht）規定，參見林鈺雄、王士帆、連孟琦，德國刑事訴訟法註釋書，頁132-134，2023年6月，1版。

³² 林鈺雄，刑事訴訟法（上冊），頁457，2022年9月，11版。



定」³³。對於Hibox案法律爭點，最高法院法官們正確表示應依搜索扣押規定後，本可成功結案，為何還在判決理由尾聲，針對過去已結束的通訊內容之調取，以法官造法來目的性限縮解釋《刑事訴訟法》第133條之1第1項？這涉及2016年扣押修法的缺失。

扣押是國家對物管領占有，或對權利禁止變動的強制處分，乃是定暫時性權利狀態的保全追訴或執行措施³⁴。國家對扣押實體標的形成公法上的管領關係，得對原權利人主張暫時有權支配或排除其支配，無疑會干預人民基本權。扣押過去已結束之電子郵件方面，本來可以選擇扣押儲存之載體，倘基於比例原則，保全方式若是列印電子郵件內容，仍會侵害被告資訊隱私權³⁵。因此，扣押必須符合基於法律保留原則、比例原則所框定的法定要件。

依2016年大幅翻修的《刑事訴訟法》扣押規定³⁶，合法扣押應滿足實體要件與程序要件³⁷：扣押實體要件，指扣押應出於保全證

³³ 最高法院106年度臺非字第259號刑事判決，行碼413-417。

³⁴ 朱石炎，同註28，頁180。另參見最高法院103年度臺抗字第720號刑事裁定：「刑事訴訟法第133條所稱扣押者，係保全可得為證據或得沒收之物，而對物之暫時占有或對權利禁止變動之強制處分，解釋上除物以外，權利亦包括之，故凍結帳戶使受處分人對存款禁止提領亦屬之」。

³⁵ 參見本文貳、二與三、(-)。

³⁶ 立法過程可參見陳文貴，刑事訴訟法增訂保全扣押相關條文立法過程與簡釋，司法周刊（司法文選別冊），1805期，頁20-38，2016年7月1日。

³⁷ 以下說明，參見王士帆，借錢交付——保全追徵之扣押(-)，法務通訊，3016期，頁6，2020年8月7日。亦參見最高法院111年度臺上字第1345號刑事判決：「扣押通常雖係緊隨於搜索之後而來，然亦有獨立於搜索程序外之扣押，其型態若從用途或目的觀察，可分為保全證據之扣押與保全沒收或追徵之扣押；若從手段或方式觀察，則可分為附隨於搜索之扣押與非附隨於搜索之單獨或獨立扣押。關於非附隨於搜索之單獨或獨立扣押，觀諸刑事訴訟法第133條之1第1項規定非附隨於搜索之單純證據保全扣押、經受扣押標的權利人同意之扣押，以及同法第133條之2第3項規定有相當理由認為情況急迫而有



據或保全沒收（含追徵）執行之原因，或兩者競合，亦即，應具備「可為證據之物」、「得沒收之物」或「為保全追徵」之扣押原因（參見刑事訴訟法第133條第1項、第2項）。其次，扣押程序要件，以系爭扣押是否附隨於搜索作為後續程序判準：於「附隨搜索」之扣押，應依搜索規定——含有票搜索及無票搜索規定在內——審查扣押合法性，且搜索合法與否，會影響附隨扣押之合法性；於「非附隨搜索」之扣押，原則上應有法官之扣押裁定（刑事訴訟法第133條之1第1項），除非符合法定例外之無令狀扣押，即單純證據扣押、同意扣押或緊急扣押（參見刑事訴訟法第133條之1第1項與第2項、第133條之2第3項）。

扣押程序要件以是否附隨搜索而區分不同程序流程，是2016年立法者扣押修法的傑作之一。當年修法，未明顯從搜索與扣押各自獨立干預基本權角度，例如以德國扣押法（§§ 94ff., 111bff. StPO）作為借鏡之一，去積極構思跳脫搜索法的扣押法獨立體系，卻選擇以發現扣押物與搜索的時序先後關係，設計出「附隨於搜索」或「非附隨於搜索」之扣押程序要件，這實在是太過直覺的思考，引發物議³⁸。另一令人費解的傑作是，《刑事訴訟法》第133條之1第1項規定「非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定」，依立法理

立即扣押必要所為之逕行扣押（下或從學理名為『緊急扣押』稱之）等情形即明」。

³⁸ 批評如林鈺雄，同註28，頁628-629：「新法仍遷就舊法混淆搜索扣押之立法例，據此而區別了『附隨於搜索之扣押』、『非附隨於搜索之扣押』這兩種程序，前者仍依附於搜索令而無須獨立之扣押令，後者則明定採相對法官保留原則；於比較法上，這可以說是我國立法者兄弟個人獨獲之創見，進而衍生諸多解釋論上的困擾，令人不解」。



由所示³⁹，對於不涉及保全沒收扣押的單純證據扣押，竟然構成法官扣押裁定之例外。這樣的獨特例外，益見2016年扣押修法的中心價值飄忽不定。因為一來，證據扣押與保全沒收扣押同樣干預人民財產權，但是「基於偵查的有效性，得為證據之扣押不適用法官保留」⁴⁰，「以方便檢警辦案需要」⁴¹，使前者逕自免除法官保留監督，差別對待的立法正當性不足。二來是干預體系紊亂，因為單純證據扣押之搜索原則上應有搜索票，適用相對法官保留，那為何單純證據扣押完全不受法官保留監督？搜索以發現應扣押物為目的時，搜索本身只是手段。當立法者直觀地以扣押附隨於搜索與否，區分扣押不同程序要件，則於附隨搜索之扣押，在搜索法方面，也未同時以所應發現之扣押物，若單純屬證據扣押便改變成無票搜索，以對應非附隨搜索之單純證據扣押免除扣押裁定，換言之，搜索以扣押單純作為證據之物，以有搜索票或無搜索票之相對法官保留為原則，獨立扣押單純作為證據之物，則概括免除法官扣押裁

39 立法理由：「現行法關於搜索，原則上，應依法官之搜索票為之，即採法官保留原則，附隨搜索之扣押亦同受其規範。非附隨於搜索之扣押與附隨搜索之扣押本質相同，除僅得為證據之物及受扣押標的權利人同意者外，自應一體適用法官保留原則。爰參考本法第128條規定，德國刑事訴訟法第98條第1項、第111e條第1項，及日本組織犯罪處罰及犯罪收益規範法第22條第1項、第42條第1項之立法例，增訂本條第1項。至於同時得為證據及得沒收之物，仍應經法官裁定，以免架空就沒收之物採法官保留為原則之立法意旨，併此敘明」。

40 余麗貞，刑法沒收新制介紹，檢察新論，20期，頁118，2016年7月。

41 陳文貴，同註36，頁27：「本條在委員會協商時，法務部代表主張維持目前刑事訴訟法制度，檢察官對保全證據之扣押，毋須適用法官保留與令狀原則，以方便檢警辦案之需要，僅關於保全沒收、追徵之扣押，同意改採法官保留與令狀原則，因獲多數委員支持而將司法院版第1項規定修改為『非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定』」。



定，立法考量失之均衡。因此，《刑事訴訟法》第133條之1第1項將非附隨搜索之證據扣押自始排除法官扣押裁定，亟待立法匡正⁴²。

2. 目的性限縮解釋

焦點拉回Hibox判決。Hibox判決認為偵查機關取得「過去已結束」之電子郵件時，應回歸適用《刑事訴訟法》，依搜索扣押相關規定為之。是以，依現行搜索扣押體系，如系爭電子郵件是附隨於搜索之扣押，則依搜索規定。若是非附隨於搜索之扣押，則「該『過去已結束』之通訊內容，如同時得為證據及得沒收之物，依第133條之1第1項之立法理由，仍應經法官裁定」⁴³。

假如「過去已結束」之通訊內容僅單純作為證據扣押標的，直接適用規範欠妥的《刑事訴訟法》第133條之1第1項，將得出偵查機關無須法官扣押裁定，便可強制扣押的不當後果，這和檢察官得以函調取得電子郵件命令的不當主張殊無二致。所以，Hibox判決鑑於「如比較『通信紀錄或通信使用者資料』對個人隱私權之侵害程度相對於『過去已結束』之通訊內容較為低，立法者既將前者以法官事前審查核發之令狀（調取票）為原則，後者至少亦應以法官事前審查核發之令狀為原則，才屬妥適」⁴⁴、「人民對於『過去已結束』之通訊內容，既享有一般隱私權，且通訊內容往往含有與本案無關之大量個人私密資訊，比其他身體、物件、處所、交通工具等之搜索，其隱私權之保障尤甚」⁴⁵，《刑事訴訟法》對第133條之1第1項規定「得為證據之物」之扣押客體，應進行目的性限縮解釋，不及於「過去已結束」之通訊內容，「檢察官對於『過去已結束』之通訊

⁴² 相同批評，王兆鵬、張明偉、李榮耕，刑事訴訟法（上），頁319-320，2022年3月，6版；薛智仁，同註9，頁1926。

⁴³ 最高法院106年度臺非字第259號刑事判決，行碼394-396。

⁴⁴ 最高法院106年度臺非字第259號刑事判決，行碼360-364。

⁴⁵ 最高法院106年度臺非字第259號刑事判決，行碼369-372。



內容之非附隨搜索之扣押，原則上應向法院聲請核發扣押裁定」⁴⁶。
《刑事訴訟法》第133條之1第1項的證據扣押除外規定殊欠妥適，
Hibox判決在法律爭點範圍內進行目的性限縮解釋，立論值得推崇。

參、搜索扣押第三人之被告程序保障

一、搜索扣押公開性

Hibox案基準劃出秘密通訊自由的時間界限，僅限於「未來及現在」的通訊內容，而不及於「過去已結束」的通訊內容，當再就第三方業者儲存的被告「過去已結束」的通訊內容，屬於被告資訊隱私權，偵查機關對之干預，應依搜索扣押規定行之。Hibox判決公布後，保全第三方業者儲存的被告數位證據問題，望似河清海晏。然而，刑事實務遇到第三方業者處搜索扣押時，若從依法應通知被告執行搜索扣押一事，不論通知方式是通知被告在場（刑事訴訟法第150條）或送達裁判書（刑事訴訟法第227條），脫法轉變成爲對被告之「秘密」搜索扣押，不但會顛覆搜索扣押的法律基調，Hibox案區分「秘密」通訊監察和「公開」搜索扣押的基準亦隨之鬆動。何以如此？

⁴⁶ 最高法院106年度臺非字第259號刑事判決，行碼415-417。反對意見參見薛智仁，同註9，頁1926：「本法的搜索扣押客體限於『可為證據之物』，但是『物』的概念自始就無法包含無形的通訊內容，在立法者配合當代科技發展彌補此一規範漏洞之前，基於法律保留原則，『過去已結束』之通訊內容也理應不得適用搜索扣押規定才對，根本沒有透過目的性限縮才能排除適用的餘地。最高法院無視法條文字的障礙，是因為其向來就在『可得沒收之物』的解釋上涵蓋『權利』在內，連帶地在『可為證據之物』的解釋上包含無形的通訊在內，自始就毀棄了法律保留原則」。



首先應確立的關鍵是，我國刑事訴訟搜索扣押的設計，乃以公開性為基調。有別於通訊監察、GPS定位偵查、臥底偵查等「秘密」偵查措施，搜索扣押之「公開」，指受干預人知悉搜索扣押之執行⁴⁷，揭載於現行《刑事訴訟法》，如「經搜索而未發見應扣押之物者，應付與證明書於受搜索人」（第125條）、「扣押，應制作收據，詳記扣押物之名目，付與所有人、持有人或保管人」（第139條第1項）、「法官、檢察官、檢察事務官、司法警察官或司法警察執行搜索及扣押，除依法得不用搜索票或扣押裁定之情形外，應以搜索票或扣押裁定示第148條在場之人」（第145條）、「在有人住居或看守之住宅或其他處所內行搜索或扣押者，應命住居人、看守人或可為其代表之人在場；如無此等人在場時，得命鄰居之人或就近自治團體之職員在場」（第148條），並應命在場之人於搜索扣押筆錄簽名、蓋章或按指印（第42條第4項）。

整體以觀，我國《刑事訴訟法》搜索扣押的圖像，與德國法強調搜索扣押公開性（*Offenheit*）⁴⁸相同，乃是偵查人員以公職外觀出現在搜索扣押地點，且讓受搜索扣押人知悉搜索。執行搜索扣押時，視個案之情形，受干預人可能選擇主動交付應扣押物，以避免被搜索，甚至當欠缺搜索扣押要件時，可加以阻止。再者，受干預人於搜索扣押完畢後，得請求發給搜索證明書或扣押收據，而欲做此書面請求的前提是，其及時受通知有進行搜索扣押一事，以藉此獲得指摘搜索扣押合法性的救濟機會⁴⁹。搜索扣押一旦未落實上述公開性配套，即會使受干預人失去防禦可能性，任何「秘密」搜索扣押基於本身所升高之干預強度，乃成為一種有別於傳統搜索扣押

⁴⁷ Gallus/Zeyher, NStZ 2022, S. 464; Joecks/Jäger, StPO, 5. Aufl., 2022, § 95a Rn. 1.

⁴⁸ BGHSt 51, 211.

⁴⁹ BGHSt 51, 211, 213 Rn. 6.



的獨立新性質之秘密強制處分⁵⁰。

據此，於第三方業者處搜索扣押被告數位證據，受搜索人或受搜索處所是第三方業者，依前述規定，第三方業者於搜索處所享有在場權，「避免產生爭端，減少違法搜索情事」⁵¹，又可增加爾後爭執時的證明管道⁵²，並有權要求出示搜索票或扣押裁定，及付與搜索證明書或扣押收據。坦白說，搜索扣押無犯罪嫌疑的第三方業者，例如Hibox案的中華電信公司，基本上沒有避免第三方業者妨害偵查策略的考量，也就是沒有鬼崇搜索扣押的必要，客觀上也難以想像在業者的偌大廠房設備，偵查機關若無業者在場協助，如何順利取得扣押物。因此，**搜索扣押第三方業者，通常會滿足搜索扣押使第三方業者知悉的公開性要求。**

然而問題是，對第三方業者處搜索扣押被告數位證據，既然同時會建立對被告資訊隱私權之干預性，如同Hibox判決已明白肯認，則現行法對身為數位證據受扣押干預人的被告，是否提供程序保障、如何的規範機制，方使被告得以有效監督搜索扣押執行及訴訟救濟，司法實務又有無確實依法踐行，殊值觀察。

⁵⁰ BGHSt 51, 211, 215 Rn. 10.

⁵¹ 最高法院103年度臺上字第159號刑事判決：「搜索處分，以有無搜索票為準，可分為有令狀搜索（有搜索票）與無令狀搜索（無搜索票），而基於『法官保留原則』，固以有令狀搜索為原則，無令狀搜索為例外，惟無論何類搜索，為避免產生爭端，減少違法搜索情事，除在政府機關、軍營、軍艦或軍事上秘密處所內行搜索或扣押者，應通知該管長官或可為其代表之人在場外，在有人住居或看守之住宅或其他處所內行搜索或扣押者，應命住居人、看守人或可為其代表之人在場；如無此等人在場時，並得命鄰居之人或就近自治團體之職員在場，此觀刑事訴訟法第148條、第149條之規定即明」。

⁵² 林鈺雄，同註32，頁446。



二、搜索扣押被告在場權與抗告權

(一) 在場權

觀察我國現行法，於第三方業者處搜索扣押被告數位證據，例如本文評釋的Hibox案，被告同樣享有在場權與抗告權。

先說明被告搜索扣押在場權。《刑事訴訟法》第150條明文規定，「（第1項）當事人及審判中之辯護人得於搜索或扣押時在場。但被告受拘禁，或認其在場於搜索或扣押有妨害者，不在此限。（第2項）搜索或扣押時，如認有必要，得命被告在場。（第3項）行搜索或扣押之日、時及處所，應通知前二項得在場之人。但有急迫情形時，不在此限」，據此，無論於偵查中或審判中搜索扣押，除非在場有妨害搜索扣押，否則被告原則上有在場權，必要時甚至得命被告在場，辯護人則是審判中之搜索扣押始有在場權⁵³。另外，為了促成在場權之行使，司法機關除非急迫情形，應預先通知被告和辯護人搜索扣押時間和地點。因此，除非發生法定例外事由，現行法乃賦予被告在場權並受通知權，其規範目的在監督及適時指摘搜索扣押不當執行，故應等待被告到場，方得開始實施搜索扣押；若允許執法機關僅通知被告，便得不待被告到場即行搜索扣押，將架空被告在場權規範目的。綜合而言，依立法者構想，並不區分執行搜索扣押是對被告或第三方業者為之，一律賦予被告在場權，「使其目睹搜索或扣押之情形，以減少不必要之爭論」⁵⁴。被告搜索扣押

⁵³ 建議應放寬成辯護人於偵查中搜索扣押亦有在場權，林永謀，刑事訴訟法釋論（上），頁461，2010年12月，改訂版：「限之於『審判中』之辯護人，而不及於偵查中者，立法理由係以偵查中之搜索，重在證據之蒐集，必須迅速即時為之，如許辯護人在場，非特影響及此，且有損於偵查不公開云云，惟衡諸同法第245條第2項規定，如此之理由，尚不足以服人」；林鈺雄，同註32，頁447。

⁵⁴ 程元藩、曹偉修，修正刑事訴訟法釋義（上冊），頁273，1969年6月，修正



在場規定是執行搜索扣押的重要程序，規範目的在賦予被告監督搜索扣押之權利，故屬強制規定，而非可由偵查機關隨意處置的訓示規定（Ordnungsvorschrift），偵查機關有無遵守這些執行規定，將左右搜索扣押合法性的判斷⁵⁵。也就是說，違反被告搜索扣押在場權所取得之證據，縱使是有票搜索或執行扣押裁定，仍可能依《刑事訴訟法》第158條之4規定宣告證據使用禁止⁵⁶。

（二）抗告權

在被告就搜索扣押訴訟救濟權方面，對第三方業者搜索扣押，既然同時會建立對被告數位證據權利的受干預性，基於「有權利即有救濟」的憲法原則⁵⁷，被告享有訴訟救濟權乃法理當然。現行法固然有將搜索、扣押列為抗告清單（刑事訴訟法第404條第1項第2款），但問題是，於第三方業者之搜索扣押，被告也是第三方業者受搜索扣押時之抗告權人嗎？

根據《刑事訴訟法》第403條規定，「（第1項）當事人對於法院之裁定有不服者，除有特別規定外，得抗告於直接上級法院。（第2項）證人、鑑定人、通譯及其他非當事人受裁定者，亦得抗告」，答案是肯定的。被告是《刑事訴訟法》所稱當事人（參見刑事訴訟法第3條），而在第403條第2項之非當事人受裁定者為抗告權人的情

再版。

⁵⁵ BGHSt 51, 211, 213-215 (Rn. 6-8).

⁵⁶ Tsambikakis, in: *Becker/Erb/Esser/Graalman-Scheerer/Hilger/Ignor* (Hg.), *Löwe/Rosenberg StPO Großkommentar*, Bd. 5/2, 27. Aufl., 2018, § 106 Rn. 15. 朱石炎，同註28，頁190-191；林永謀，同註53，頁461：「若無法定例外情形，而未依法通知當事人及辯護人，使其有到場之機會者，所踐行之訴訟程序自有瑕疵，其依此搜索所扣押之證物，應認屬因違背法定程序取得之證據」。另參見最高法院94年臺上字第4929號刑事判例。

⁵⁷ 參見如憲法法庭111年度憲判字第7號判決。



形，當事人如因其與本案具有利害關係，縱非受裁定之人，依第403條第1項，當事人對於法院之裁定不服者，除有特別規定外，得抗告於直接上級法院，故被告「仍屬有抗告權，並不以其本身所受之裁定為限」⁵⁸，只不過被告仍應有抗告利益，始可合法提起抗告⁵⁹。

由此觀之，偵查機關向第三方業者執行搜索扣押被告數位證據，受搜索處所或受扣押裁定之人是第三方業者，第三方業者屬於非當事人之受裁定者，依《刑事訴訟法》第403條第2項得提起抗告，而扣押物之所有人則是被告，其資訊隱私權因第三方業者伺服器遭搜索扣押受有侵害，故具有抗告利益，亦得依第403條第1項，本於當事人地位提起抗告。

(三) 搜索票和扣押裁定之應受送達人

肯認被告於第三方業者受搜索扣押時，亦有抗告權後，不禁令人疑問的是，被告是針對第三方業者搜索扣押之搜索票或扣押裁定的應受送達人嗎？答案必然是肯定，理由之一是，被告若不知悉資訊隱私權受侵害，無從提起抗告救濟。理由之二是「抗告期間，除有特別規定外，為5日，自送達裁定後起算，但裁定經宣示者，宣示後送達前之抗告，亦有效力」（刑事訴訟法第406條），裁定若未經合法送達於抗告權人，抗告期間將無從起算。

再者，《刑事訴訟法》第227條規定，「（第1項）裁判制作裁判書者，除有特別規定外，應以正本送達於當事人、代理人、辯護人及其他受裁判之人。（第2項）前項送達，自接受裁判原本之日起，至遲不得逾7日」，同樣可說明搜索票或扣押裁定應向身為當

⁵⁸ 程元藩、曹偉修，修正刑事訴訟法釋義（下冊），頁970，1969年6月，修正再版；相同見解，林永謀，刑事訴訟法釋論（下），頁185，2010年11月，改訂版。

⁵⁹ 林永謀，同前註，頁185-186。



事人之被告送達。筆者以德國法為例。依德國《刑事訴訟法》第35條，法院於受干預人（*betroffene Person*）在場時作出之裁判，以宣示方式通知受干預人，其他裁判則以送達方式通知，據此，德國搜索和扣押裁定，縱使是對第三人伺服器搜索扣押，亦應送達受干預人⁶⁰。如果是自願交付扣押物，由於沒有法院之搜索或扣押裁定，則無庸送達⁶¹。在檢警之無令狀緊急扣押，檢警應於3日內陳報法院補發令狀，確認扣押合法性（§ 98 II S. 1 StPO），並向受干預人通知法院該決定⁶²。另一方面，於無令狀扣押，受干預人得隨時聲請管轄法院裁判，執行扣押機關負有此權利救濟告知義務（§ 98 II S. 2, 5 StPO），但檢警於第三人扣押聲請暫緩通知被告時，免除此告知義務（§ 95a III StPO）。倘法院已因檢警聲請而補發令狀確認，受干預人又聲請法院裁判，其聲請將轉變成請求撤銷補發之扣押裁定⁶³。受干預人對法院補發之扣押裁定不服或聲請法院裁判被駁回者，均得向上級法院提起抗告⁶⁴。

裁判送達，規範目的的一方面是訴訟證明功能，即證明應受送達人收受法院文書，使之發生一定效力⁶⁵，這事涉訴訟流程是否依法進行，攸關法定期間之起算，所以受干預人不得自由放棄受送達權利⁶⁶。另一方面，送達使應受送達人有知悉訴訟文書的機會，也在

⁶⁰ Vgl. Menges, in: Becker/Erb/Esser/Graalman-Scheerer/Hilger/Ignor (Hg.), Löwe/Rosenberg StPO Großkommentar, Bd. 3/1, 27. Aufl., 2019, § 94 Rn. 14.

⁶¹ Köhler, in: Meyer-Goßner/Schmitt (Hg.), StPO, 65. Aufl., 2022, § 95a Rn. 4.

⁶² AaO., § 98 Rn. 17.

⁶³ Joecks/Jäger, aaO. (Fn. 47), § 98 Rn. 16; Köhler, aaO. (Fn. 61), § 98 Rn. 19.

⁶⁴ Joecks/Jäger, aaO. (Fn. 47), § 98 Rn. 23; Köhler, aaO. (Fn. 61), § 98 Rn. 31; Zeyhe, JuS 2022, S. 637.

⁶⁵ 朱石炎，同註28，頁79。

⁶⁶ Weißer/Weßlau, in: Wolter (Hg.), Systematischer Kommentar zur StPO, Bd. 1, 5. Aufl., 2018, § 35 Rn. 2.



保障受干預人之聽審權⁶⁷。於德國法，為了保障受干預人刑事程序之聽審權，法院裁定、判決或處分等所有決定，不問是偵查程序、審判或執行程序，均應通知受干預人，使其有機會評估是否採取進一步訴訟措施，特別是提起訴訟救濟⁶⁸。簡單來說，凡受到法院裁判干預之人，就必須向其通知裁判。否則，受干預人無從實現可能的訴訟行為要求，也無法有效思考是否對系爭裁判採取訴訟救濟手段。因此，為了確保受干預人之聽審權，立法者規定法院裁判如何使受干預人知悉之規定，誠所必要⁶⁹。

在刑事訴訟之基本權干預脈絡，送達另有於比例原則誡命下，使受干預人得以和執法機關合作，緩和干預強度的功能。不過，在秘密偵查措施，例如通訊監察，不可能事先或於執行期間通知受干預人，故德國另外就秘密偵查措施設計執行完畢後之通知義務（§ 101 IV StPO）⁷⁰。而依德國法理解，搜索扣押相較於秘密偵查措施而言，是受干預人知情的公開偵查行為。故德國在2021年修法引進第三人扣押之暫緩通知被告規定（§ 95a StPO）前，德國法院最遲於搜索扣押開始時，應通知被告於第三方業者伺服器受搜索扣押一事，執行搜索扣押後才通知被告即屬違法，縱使是擔心通知被告會妨害其他同步秘密偵查成果，本來亦無例外⁷¹，這直到2021年修法才改觀。

⁶⁷ *Schneider-Glockzin*, in: *Barthe/Gericke* (Hg.), *Karlsruher Kommentar zur Strafprozessordnung*, 9. Aufl., 2023, § 35 Rn. 15; BGHSt 27, 85, 88.

⁶⁸ AaO., § 35 Rn. 1f.

⁶⁹ *Claus*, in: *Satzger/Schluckebier/Widmaier* (Hg.), *StPO*, 5. Aufl., 2023, § 35 Rn. 1; *Weißer/Weßlau*, aaO. (Fn. 66), § 35 Rn. 3.

⁷⁰ *Weißer/Weßlau*, aaO. (Fn. 66), § 35 Rn. 1; 說明參見王士帆，德國科技偵查規定釋義，法學叢刊，66卷2期，頁124-128，2021年4月。

⁷¹ BGH, *Beschl. v. 24. 11. 2009 – StB 48/09 (a)*, Rn. 19; *Weißer/Weßlau*, aaO. (Fn. 66), § 35 Rn. 1.



綜合上述，於第三方業者搜索處扣押被告數位證據，不管依理論或我國法現行構造，被告也是搜索票或扣押裁定的應受送達人，否則無從行使抗告救濟權，以維護其數位證據內的資訊隱私權。

三、「暫緩通知被告」之立法構思

(一)秘密鬆動Hibox案基準

走筆至此，對於在第三方業者處搜索扣押被告數位證據，應通知被告在場，並將搜索票或扣押裁定送達被告的說法，實務人士可能質疑不切實際，因為打草驚蛇，妨害偵查目的。但反過來思考，假如使被告一概不在場、不通知、不送達，這一來不符合《刑事訴訟法》第150條、第227條及第403條規定的基本理念。第二，第150條的在場權例外和受通知例外規定，原始適用範圍有限，程序規範密度嚴重不足，例如不妨害搜索扣押，但妨害通訊監察或其他偵查作為，便不構成在場權例外或受通知例外；即便依法得不通知被告搜索扣押時地（「急迫情形」），仍不等於可永久免予通知被告受搜索扣押干預，更不因此成為裁判送達例外。第三，偵查目的絕對優先的主觀念頭，導致被告資訊隱私權受到侵害，抗告救濟權同時一併埋葬，違反有權利即有救濟的憲法原則，這樣的刑事偵查救濟權缺失，無疑又成為憲法法庭判決認證的敗訴教材。

於第三方業者處搜索扣押被告數位證據之搜索票或扣押裁定，法律解釋論下，我國司法機關應無使被告一概不在場、不通知、不送達的便宜行事空間。一旦概括不在場、不通知、不送達，依Hibox案基準，「過去已結束」之通訊內容屬於隱私權保護範圍，而非秘密通訊自由，本來應依搜索扣押公開取得，將質變成「秘密」搜索扣押第三方業者的被告過去所有電子郵件。不妨設想一下，如果允許對第三方業者處被告電子郵件實施連續密集之「秘



密」搜索扣押，形式上雖稱系爭搜索扣押僅干預隱私權，實際上則是發生持續秘密侵害秘密通訊自由之效果，卻不受《通訊保障及監察法》之重罪原則等要件拘束（通訊保障及監察法第5條），調取範圍通常也超出30日乃至1年的通訊監察期間（通訊保障及監察法第12條），這尤其發生在被告為隨時查閱，不刪除業者電子郵箱信件，長年累月當作雲端硬碟用途，甚至會一併剝奪抗告權。總言之，實務在無法律明文允許下，若實際「秘密」搜索扣押第三方業者之被告數位證據，將釀成秘密鬆動Hibox案基準的法治災難，混淆搜索扣押與通訊監察之基本權干預界限與法律保留要件，又違反有權利即有救濟之憲法原則，後果不容輕忽。

(二)德國2021年增訂「暫緩通知被告」規定

在立法論上，對第三方業者搜索扣押，若確實存在暫緩通知被告的偵查意義，立法芻議規劃是有前例可循的，即《刑事訴訟法》第135條第2項「為前項扣押者，應即通知郵件、電報之發送人或收受人。但於訴訟程序有妨害者，不在此限」⁷²，但一般認為該條文已被《通訊保障及監察法》取代，不得再行適用⁷³。在外國比較法例，美國執法機關得向法院聲請核發命令，法院認為通知將造成對他人生命或身體危險、逃亡、偽造或變造證據、威脅或恐嚇證人，或嚴重危害偵查或審判遲延者，得命令暫時不通知通訊內容受有調取

⁷² 程元藩、曹偉修，同註54，頁262：「所謂訴訟程序有妨害者，例如扣押之郵電足供拘捕被告之線索，或恐通知後促使被告又復他逃，此際即可不予通知，是否有妨害於訴訟程序，由實施扣押處分之公務員憑客觀上之事實決之」。

⁷³ 王兆鵬、張明偉、李榮耕，同註42，頁330-331：「對於信件的扣押已經構成了通訊監察，通保法針對書信的監察已經設有相對應的條文，是故應認為書信的扣押不得再適用本條規定」。



之人⁷⁴。

無獨有偶，德國2021年7月1日生效《刑事訴訟法》第95a條新增條文，允許第三人搜索扣押之「暫緩通知被告及揭露禁止」（Zurückstellung der Benachrichtigung des Beschuldigten; Offenbarungsverbot），這是基於偵查策略考量，以扣押被告存放於第三方業者的數位證據為主要適用案例，諸如扣押Email、聊天內容、雲端資料或網路服務用戶使用者資料⁷⁵。該條文之增訂是出於《刑事訴訟法進展與其他條文修正法案》（Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften）⁷⁶，整部法案核心宗旨是「刑事程序應順應持續變化的社會和科技整體條件，並顧及刑事司法為保護人民，得以在合乎司法形式與以發現真實為目的之程序，實踐憲法根本任務，即澄清犯罪、偵查犯罪行為人、認定其罪責與處罰及對無辜之人為無罪宣告。為實現此一宗旨，首要需求是使偵查程序諸多規定現代化」⁷⁷。德國《刑事訴訟法》第95a條即是德國立法者的偵查現代化作品之一，於第三人處之扣押，除了經法官同意得暫緩通知被告外，亦得課予第三人禁止揭露義務。

本文基於寫作定位，對於德國《刑事訴訟法》第95a條之利

⁷⁴ 李榮耕，同註9，頁775；黃朝義，同註9，頁70：「可另聲請法院命令禁止網路服務業者通知顧客或用戶。倘法院認為通知用戶會導致『負面後果』，例如危及個人生命或身體安全、有逃亡、湮滅、偽變造證據、脅迫證人或其他嚴重危及偵查或過度遲延審判時，可依聲請核准延遲通知。得延遲通知顧客之時間，係以『法院認為適當之延遲通知時間』」。

⁷⁵ BT-Drs. 19/27654 v. 17. 03. 2021, S. 63f.; Ladiges, GSZ 2021, S. 204; Mosbacher, GA 2022, S. 492.

⁷⁶ BGBl 2021, S. 2099ff.

⁷⁷ BT-Drs. 19/27654 v. 17. 03. 2021, S. 1. 新法簡要說明，Ladiges, aaO. (Fn. 75), S. 203-209.



弊⁷⁸，留待日後評論，在此僅指出其條文內容供作參考：

I. 法院對非由被告持有之物核發或補發扣押命令，於以下情形，如通知受扣押干預之被告將危及調查目的者，得暫緩通知被告：

1. 有事實懷疑被告以正犯、共犯、未遂犯或預備犯之地位，犯個案中犯罪情節重大之犯罪，尤其是第100a條第2項所列犯罪，並且
2. 以其他方法調查犯罪事實或探查被告所在地有顯著困難或預期無結果。

II. ^[1]第1項之暫緩通知被告，僅可由法院命令之。^[2]暫緩不得逾6個月。^[3]暫緩通知之要件繼續存在時，法院得命令延長暫緩，每次延長不逾3個月。

III. ^[1]扣押無犯罪嫌疑之人所持有之物，非由法院命令為之時，於扣押3日內，如聲請法院補發扣押命令及依第1項之暫緩通知被告，得免予對受扣押干預之被告踐行第98條第2項第5句之權利告知。^[2]於第98條第2項之程序，法院無須事先聽詢被告意見（第33條第3項）。

IV. ^[1]不危及調查目的時，應立即通知依第1項被暫緩通知之被告。^[2]於通知，應告知被告有依第5項事後權利保護之可能性與該規定之期限。

V. ^[1]被告亦得於第1項暫緩通知結束至依第4項通知後之2週內，向核發扣押之管轄法院聲請審查關於扣押、扣押執行方式與暫緩通知之合法性。^[2]對法院之決定，得提起立即抗告。^[3]已提起公訴並已通知被告者，由本案審理法院受理被告聲請，並於終局裁判對聲請作出決定。

VI. ^[1]法院依第1項命令暫緩通知被告時，在考慮個案中所有情況

⁷⁸ Vgl. *Becker/Dogan*, aaO. (Fn. 8), S. 459ff.; *Beulke/Swoboda*, *Strafprozessrecht*, 16. Aufl., 2022, Rn. 389a; *Gallus/Zeyher*, aaO. (Fn. 47), S. 462ff.; *Roxin/Schünemann*, *Strafverfahrensrecht*, 30. Aufl., 2022, § 36 Rn. 6; *Vassilaki*, *MMR* 2022, S. 103ff.



並權衡相關人利益後，得同時命受扣押命令之人於暫緩通知期間內，不得向被告與第三人揭露扣押、扣押之前有依第103條、第110條之搜索或第95條之交付命令。^[2]若依第3項免除權利告知且聲請法院補發扣押命令及暫緩通知被告者，於遲延即生危險時，檢察官與其偵查人員（法院組織法第152條）得準用第2項為第1句之禁止揭露命令。^[3]檢察官或其偵查人員命令禁止揭露時，應於3日內聲請法院認可之。

VII. 違反第6項禁止揭露命令者，準用第95條第2項規定。

肆、結 論

「隨著科技日新月異，手機之普及與便利已快速改變人類生活習慣，使其成為現代人與外界互動之重要媒介，廣泛形成手機如同其使用者之貼身物品」（最高法院110年度臺上字第4549號刑事判決），現代人隨時、隨地使用手機，上傳或備份於網路服務提供者伺服器之電子資料等「數位證據」。掌握這些數位證據，可能是澈底認清一個人的最佳方式，自然也具有追訴犯罪意義的調取價值。數位證據所向披靡，無所不在，刑事訴訟的傳統強制處分不得不面臨數位轉型。

偵查機關欲取得刑事被告在第三方業者處存放的電子郵件、影音或文件，事涉國家取證手段與被告和第三方業者之間基本權利干預關係。以搜索扣押來說，當第三方業者提供服務給被告使用，偵查機關為了取得被告存放的數位證據，舉凡扣押第三方業者伺服器內之儲存已讀取過Email、聊天內容、社群帳號使用者資料或雲端檔案，對無犯罪嫌疑之第三方業者伺服器發動搜索扣押，同時會建立對被告數位證據之權利的受干預性。最高法院106年度臺非字第259號刑事判決所謂Hibox案，正是以調取第三方業者處被告已讀取之電子郵件的法律爭點，其樹立Hibox案基準：「過去已結束」的



通訊內容，屬資訊隱私權，應適用《刑事訴訟法》搜索扣押規定。

Hibox判決認為秘密通訊自由的保障範圍，會隨訊息送達接收人及傳遞過程結束而終止，易言之，秘密通訊自由有保障範圍之時間界限。從而，「過去已結束」之通訊電子郵件，由於不再受到秘密通訊自由保護，偵查機關欲取得「過去已結束」之電子郵件時，應依搜索扣押規定為之。是以，依現行搜索扣押體系，如系爭電子郵件是附隨於搜索之扣押，依搜索規定調取。倘若是非附隨於搜索之扣押，鑑於「該『過去已結束』之通訊內容，如同時得為證據及得沒收之物，依第133條之1第1項之立法理由，仍應經法官裁定」。另一方面，鑑於「人民對於『過去已結束』之通訊內容，既享有一般隱私權，且通訊內容往往含有與本案無關之大量個人私密資訊，比其他身體、物件、處所、交通工具等之搜索，其隱私權之保障尤甚」，Hibox判決對《刑事訴訟法》對第133條之1第1項規定「得為證據之物」之扣押客體，進行目的性限縮解釋，不及於「過去已結束」之通訊內容，「檢察官對於『過去已結束』之通訊內容之非附隨搜索之扣押，原則上應向法院聲請核發扣押裁定」。由於《刑事訴訟法》第133條之1第1項的證據扣押除外規定殊欠妥適，Hibox判決在法律爭點範圍內進行目的性限縮解釋，立論值得推崇（本文貳）。

最後，於第三方業者搜索處扣押被告數位證據，不管依理論或我國《刑事訴訟法》第150條、第227條和第403條，被告也是搜索票或扣押裁定的應受送達人，否則無從行使抗告救濟權，以維護其數位證據內的資訊隱私權。一旦使被告概括不在場、不通知、不送達，依Hibox案基準，「過去已結束」之通訊內容本來應依搜索扣押公開取得，將質變成「秘密」搜索扣押第三方業者的被告過去所有電子郵件，甚至剝奪被告抗告權。如果司法機關對第三方業者處被告電子郵件實施連續密集之「秘密」搜索扣押，形式上雖稱系爭搜索扣押僅干預隱私權，實際上則是發生持續秘密侵害秘密通訊自



由之效果，卻不受《通訊保障及監察法》之重罪原則等要件拘束（參見通訊保障及監察法第5條），調取範圍通常也超出30日乃至1年的通訊監察期間（參見通訊保障及監察法第12條），這尤其發生在被告為隨時查閱，不刪除業者電子郵箱信件，長年累月當作雲端硬碟用途。實務若在無法律明文允許下，「秘密」搜索扣押第三方業者之被告數位證據，將釀成秘密鬆動Hibox案基準的法治災難。

展望我國刑事訴訟未來立法芻議，建議法規主管機關充分檢討基於兼顧保障被告救濟權與國家追訴犯罪之憲法任務，參酌比較法例，例如德國2021年7月1日生效的德國《刑事訴訟法》第95a條新增條文，規定第三人搜索扣押之暫緩通知被告及揭露禁止（*Zurückstellung der Benachrichtigung des Beschuldigten; Offenbarungsverbot*），審慎思辨第三人受搜索扣押時的暫緩通知被告規定妥適性（本文參）。



參考文獻

一、中文

1. 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，頁339-390，2016年6月。
2. 王士帆，犯罪所得沒收與追徵之保全扣押——談立法定位，載：沒收新制(二)——經濟刑法的新紀元，頁355-374，2016年9月。
3. 王士帆，德國聯邦憲法法院BVerfGE 124, 43——扣押伺服器之電子郵件（上／下），司法周刊，1921/1922期，2/2-3版，2018年10月。
4. 王士帆，借錢交付——保全追徵之扣押(一)，法務通訊，3016期，頁6，2020年8月。
5. 王士帆，德國科技偵查規定釋義，法學叢刊，66卷2期，頁85-132，2021年4月。
6. 王兆鵬、張明偉、李榮耕，刑事訴訟法（上），6版，2022年3月。
7. 朱石炎，刑事訴訟法論，修訂10版，2022年9月。
8. 余麗貞，刑法沒收新制介紹，檢察新論，20期，頁101-121，2016年7月。
9. 吳天雲，未經刑事司法互助跨國線上搜索扣押電磁紀錄之證據能力——以日本最高裁判所令和3年2月1日判決為中心，檢察新論，31期，頁295-314，2022年11月。
10. 李榮耕，證據驗真及其監管，台灣法律人，7期，頁79-100，2022年1月。
11. 李榮耕，犯罪偵查中通訊內容的調取，國立臺灣大學法學論叢，51卷3期，頁757-831，2022年9月。
12. 沈冠伶，民事訴訟之數位證據與證據調查，月旦法學雜誌，330期，頁77-103，2022年11月。
13. 林永謀，刑事訴訟法釋論（下），改訂版，2010年11月。
14. 林永謀，刑事訴訟法釋論（上），改訂版，2010年12月。
15. 林恆吉，論新進通訊之正當法律程序——以Hibox為例，司法周刊，1924期，2-3版，2018年10月。
16. 林鈺雄，刑事訴訟法（上冊），11版，2022年9月。



17. 林鈺雄，刑事訴訟法（下冊），11版，2022年9月。
18. 林鈺雄、王士帆、連孟琦，德國刑事訴訟法註釋書，1版，2023年6月。
19. 林俊益，刑事訴訟法概論（上），22版，2022年9月
20. 陳文貴，刑事訴訟法增訂保全扣押相關條文立法過程與簡釋，司法周刊（司法文選別冊），1805期，頁20-38，2016年7月。
21. 陳昱奉，網路犯罪與資訊安全的未來——從網域名稱扣押談網路治理，刑事政策與犯罪防治研究專刊，32期，頁219-290，2022年8月。
22. 陳運財，GPS監控位置資訊的法定程序，台灣法學雜誌，293期，頁59-74，2016年4月。
23. 程元藩、曹偉修，修正刑事訴訟法釋義（上冊），修正再版，1969年6月。
24. 程元藩、曹偉修，修正刑事訴訟法釋義（下冊），修正再版，1969年6月。
25. 黃朝義，網路通訊資料保障與網路通訊監察——以取得過去已結束通訊內容為主，中央警察大學法學論集，35期，頁45-89，2018年10月。
26. 溫祖德，偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查——從美國聯邦最高法院判決檢視我國法制，政大法學評論，167期，頁171-256，2021年12月。
27. 蔡志宏，剝奪犯罪工具之數位轉型——域名之沒收與扣押，刑事政策與犯罪防治研究專刊，31期，頁197-237，2022年4月。
28. 蔡宗珍，電信相關資料之存取與利用的基本權關連性（上）——德國聯邦憲法法院BVerfGE 125, 260與BVerfGE 130, 151判決評析，月旦法學雜誌，274期，頁105-132，2018年3月。
29. 薛智仁，2017年刑事程序法回顧：刑事救濟程序、證據法則與強制處分，國立臺灣大學法學論叢，47卷特刊，頁1881-1929，2018年11月。
30. 蘇凱平，數位證據如何分辨真偽？如何舉證？，月旦法學教室，233期，頁20-23，2022年3月。

二、外 文

1. Barthe, Chrisptoh/Gericke, Jan (Hg.), Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl., 2023.



2. *Becker, Christian/Dogan, Zehra Baser*, Zwischen TKÜ und heimlicher Beschlagnahme – Neues zum Zugriff auf beim Provider gespeicherte E-Mails, StV 2022, S. 459-463.
3. *Becker, Jörg-Peter/Erb, Volker/Esser, Robert/Graalman-Scheerer, Kristen/Hilger, Hans/Ignor, Alexander* (Hg.), Löwe/Rosenberg StPO Großkommentar, Bd. 5/2, 27. Aufl., 2018.
4. *Becker, Jörg-Peter/Erb, Volker/Esser, Robert/Graalman-Scheerer, Kristen/Hilger, Hans/Ignor, Alexander* (Hg.), Löwe/Rosenberg StPO Großkommentar, Bd. 3/1, 27. Aufl., 2019.
5. *Beulke, Werner/Swoboda, Sabine*, Strafprozessrecht, 16. Aufl., 2022.
6. *Böse, Martin*, Der Auslandsbeweis im deutschen Strafprozess – die Encrochat-Entscheidung des BGH im Spiegel der Lehre von den strafprozessualen Verwertungsverboten – Besprechung von BGH, Beschluss vom 2. 3. 2022 – 5 StR 457/11, JZ 2022, S. 1048-1056.
7. *Derin, Benjamin/Singelnsteins, Tobias*, Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat), NSTZ 2021, S. 449-454.
8. *Gallus, Nico/Zeyher, Lukas*, § 95a StPO als „Rettungsanker“ für die heimliche Beschlagnahme von E-Mails beim Provider?, NSTZ 2022, S. 462-466.
9. *Joecks, Wolfgang/Jäger, Christian*, StPO, 5. Aufl., 2022.
10. *Kingreen, Thorsten/Poscher, Ralf*, Grundrechte. Staatsrecht II, 38. Aufl., 2022.
11. *Ladiges, Manuel*, Neue Eingriffsbefugnisse durch das Gesetz zur Fortentwicklung der Strafprozessordnung, GSZ 2021, S. 203-209.
12. *Löffelmann, Markus*, Verwertungsverbot bei Datentransfer aus dem Ausland – Besprechung von BGH, Beschluss vom 2. 3. 2022, 5 StR 457/21, JR 2022, S. 454-460.
13. *Maunz, Theodor/Dürig, Günter* (Hg.), GG, 84. Aufl., 2018.
14. *Meyer-Goßner, Lutz/Schmitt, Bertram* (Hg.), StPO, 65. Aufl., 2022.
15. *Mosbacher, Andreas*, Fünf Jahre Reform des Strafverfahrens – Ein kritischer Überblick, GA 2022, S. 481-497.



16. *Obenhaus, Nils*, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, S. 651-655.
17. *Roxin, Claus/Schünemann, Bernd*, Strafverfahrensrecht, 30. Aufl., 2022.
18. *Ruppert, Felix*, Erheben ist Silber, Verwerten ist Gold? Verwendbarkeit und Verwertbarkeit von Daten ausländischer Ermittlungsbehörden im Lichte des Grundrechtsschutzes – EncroChat, NZWiSt 2022, S. 221-227.
19. *Satzger, Helmut/Schluckebier, Wilhelm/Widmaier, Gunter* (Hg.), StPO, 5. Aufl., 2023.
20. *Vassilaki, Irini*, Heimliche Beschlagnahme von digital gespeicherten Informationen – Auf dem Weg zu einer neuen Ermittlungsmaßnahme, MMR 2022, S. 103-105.
21. *Weiss, Alba Hernandez*, Gegenseitige Anerkennung als „Joker“ bei transnationalen Ermittlungen? Einige Überlegungen zu dem Rechtsstreit Berliner Gerichte im Fall „EncroChat“, ZfStW 2022, S. 427-438.
22. *Wolter, Jürgen* (Hg.), Systematischer Kommentar zur StPO, Bd. 1, 5. Aufl., 2018.
23. *Zeyhe, Lukas*, Rechtsschutz gegen strafprozessuale Zwangsmaßnahmen im Ermittlungsverfahren, JuS 2022, S. 636-640.



“Secret” Searches and Detains Digital Evidence from Third-Party Providers: Loosening the Benchmark in the Supreme Court’s Hibox Case

Shih-Fan Wang^{*}

Abstract

With the increasing attachment to mobile devices in modern times, it has become a norm for the public to expose a significant amount of footprints on the Internet. For the investigating authorities, the availability of digital evidence will increase the efficiency of crime prosecution and have a high value for investigation. As a result, traditional compulsory search and seizure is undergoing a digital transformation, gradually moving from public enforcement to covert investigation. Regarding the search and seizure of digital evidence by investigating agencies from third parties, the Supreme Court, in its 106th Judgment No. 259, affirmed that the defendant’s right to privacy had been violated and limited the scope of the protection of the freedom of secret communication to the contents of past communications and

^{*} Associate Professor of Law, National Taipei University; Dr. jur. Munich University, Germany.

Received: February 27, 2023; accepted: May 15, 2023



that the search and seizure requirement should apply to the retrieval of the contents of closed emails. However, under the current law, the defendant has the right to search in the presence and to be notified of the search in principle, and if the state should seize the “secret” search, it would loosen the basis of the Hibox decision. In the future, the authorities should consider the constitutional mandate to protect the defendant’s right to remedy and the state’s right to prosecute crimes, and carefully consider the provision of a temporary stay of notice to the defendant in the event of a search and seizure of a third party, taking into account comparative legislation.

Keywords: Freedom of Confidential Communication, Search, Seizure, Presence, Right of Remedy