本論文獲得法務部司法官學院114年傑出碩博士犯罪防治研究論文獎

國立臺灣大學法律學院科際整合法律學研究所

碩士論文

Graduate Institute of Interdisciplinary Legal Studies
College of Law
National Taiwan University

Master Thesis

域名扣押—以停止解析為中心 (DNS RPZ)

Domain Name Seizure—Stop Resolution (DNS RPZ)

白凌瑀

Ling-Yu Pai

指導教授：林鈺雄 博士

Advisor: Yu-Hsiung Lin, Dr. jur.

中華民國 112 年 5 月

May 2023

doi:10.6342/NTU202302025

國立臺灣大學碩士學位論文

口試委員會審定書

域名扣押—以停止解析為中心（DNS RPZ）

Domain Name Seizure—Stop Resolution (DNS RPZ)

本論文係白凌瑀君（學號 R08A41023）在國立臺灣大學科際整合法律學研究所完成之碩士學位論文，於民國 112 年 5 月 5 日承下列考試委員審查通過及口試及格，特此證明

指導教授：林鈺雄

口試委員：林鈺雄

之中

溫祖德

謝　辭

2022-23 年，從跟老師討論題目、擬定大綱開始，一步一步的完成了論文走到現在，花了比想像中還要漫長的時間。過程中彷彿走進看不到盡頭的隧道，不曉得什麼時候會到終點，只能哭哭鬧鬧的、徬徨的在黑暗中摸索著緩慢前進，擦乾眼淚終究看到盡頭透進隧道的光。

謝謝我的指導教授林鈺雄老師，不只是學術上的討論，老師登山的心得分享、面對人生的態度或是平時的關心，對我來說都是成長養分，總覺得在老師身上學習到了好多。大學初接觸法律課程時便是拜讀老師的教科書，老師的文筆好流暢清晰，也因為這份崇拜，進入台大後幾乎每一個學期都會修老師的課，收穫滿滿，也很喜歡看老師講課時眼睛散發的光芒，很有魅力。

也要謝謝溫祖德老師與王士帆老師，願意撥空擔任學生的口試委員，仔細地指出論文初稿中的缺失與不足，並且在口試時溫柔的與我討論想法，提供了好多好有幫助的建議，協助我看破盲點，將論文進一步的修正。在滿滿摺痕的口試本中，可以感受到兩位老師的用心，也在口頭上給予了我好多的鼓勵，真的非常感謝！

決定以域名扣押為論文主題後，查找文獻時便參考了陳昱奉檢察官的文章，其後透過老師的引薦，告知陳檢察官我的論文題目後，學長也好熱心的提供了許多相關資訊。謝謝學長總是一有資訊便立刻通知我，也很樂於與我進行學術討論。完全可以感受到學長在網路犯罪方面的研究熱忱，我的心也因此被感染，期許自己的論文能夠有所貢獻，也可以在某天像學長一樣給予後輩幫助。

加入熊門後獲得了意料外的溫暖。謝謝奕崴帶我入門，認識了大家。也謝謝怡凡帶領著我口試，沒有你我不曉得論文還會拖拖拉拉多久才能完成。謝謝家維、昀霈在論發前主動詢問是否需要幫助，焦慮緊張的心緩了下來。論發時投影設備出問題，也因為有熊門大家的即時協助，才安穩順利的完成發表。謝謝珮群、友銓參加了我的口試，對我說我的題目很有趣，或是提出想法與我討論，這些都讓我感覺自

doi:10.6342/NTU202302025

己的論文似乎有點意義，也更有自信了。還有學長姐、學弟妹，聚餐時的鼓勵、加油、恭喜，這些點滴溫暖都在寫論文的階段拉了我一把，謝謝你們。

一直認為自己不算擅長交友的人，很慶幸在研究所階段，有一群科法所的好朋友在身邊，不論什麼辛苦的事、人生的煩惱、論文的抱怨，總是有人可以討論，或是一起面對。整個科法四年，每天跟你們待在研究室的時間比我待在家還多，也像家人一樣，會吵架，會不耐煩有話直說，但重要時刻總是可以獲得一個擁抱。謝謝家凱二話不說動用立法院資源幫我找了論文的重要資料，坐在隔壁組鋼彈也讓我可以專心的撰寫；謝謝厚宇在往返瑜伽課的路途中，會陪我討論論文、抱怨人生或單純的傾聽煩惱；謝謝俐蓉，光是坐在研究室漂漂亮亮的，就讓人心情很好，每次我提前離開時也都會移動步伐送我搭電梯；謝謝美國代表冠嫻，雖然感覺人都不在台灣，但會在奇怪的時間回群組訊息，釋放一些正能量，香香的。

寫論文期間的我低氣壓籠罩，初期對自己太嚴苛，只要沒達到每日目標就會心態崩，哭著騎車回家。謝謝運動夥伴兼人生導師冠琳，在這段時間成為了我極大的心靈支柱，大概只有妳會這麼不厭其煩的聽一個研究生反覆抱怨一樣的事，然後塞一些正向想法給我。此刻回想那段時間我們的聊天內容，都會覺得鬼擋牆的荒唐至極，謝謝你的包容。謝謝敦志，論文第二章技術的部分幾乎都是你教我的，謝謝你的耐心，我知道我不是一個脾氣太好的學生，也謝謝你隨時都會接聽我在路邊大哭的電話。在撐不住、慌張到不行的時候，知道你一定會接通電話這件事本身就讓我感到安心。謝謝允箴，我們聯絡的頻率不高，但知道彼此都在自己喜歡的地方各自努力，每隔一段時間的聯繫都會讓我的心滿滿的，知道你不論如何都會套上白白濾鏡盲目地為我加油。論發的時候是穿著你送的香水，信心滿滿地前往教室！還有好多好多朋友，就不一一列舉了，但我都記在心裡。小小的鼓勵、替我開心的笑臉、一些建議或是即時的協助，在寫謝辭的此刻，回想起這些瞬間，都會覺得我是個好幸運的人。軟弱迷茫時，身邊總是有人及時伸出援手，並讓我帶著期許推著自己進步。

doi:10.6342/NTU202302025

謝謝文謙，謝謝你大方的讓我壓榨幫我的論文校稿，也謝謝你陪我走過這段時間。撰寫論文的初期也是剛認識的時候，那時會在半夜閒聊，抒發論文或國考的煩惱，談話中也協助我釐清思緒。論文寫到後期時間壓力很大，常常在研究室待到半夜趕進度，要離開時抓著睡眼惺忪、為了等我而在研究室趴睡的你一起走，心裡感到很踏實。返家的路不再是一個人穿過黑暗的小徑，而是有人陪伴著。那些大大小小的煩惱你都願意聽我說，用擁抱來化解焦慮不安的情緒，讓我的心好安定，簡單的給了我力量。讓我可以無後顧之憂的投入寫作，自由的做喜歡的事，自信的完成論發與口試，也在後段衝刺期體會到了寫論文的成就感。那些貼心的、溫柔的小事我都記著，很慶幸有你在，也很謝謝你的照顧。

不知不覺把謝辭寫得好長。最後，好感謝我的家人，不僅是經濟上無虞，讓我能夠把心思專注於學業。在生活上也扶持著我，早上起床後爸總是會泡好熱茶放在我的書桌，擁抱送我出門；睡前也可以吱吱喳喳的跟姐姐分享亂七八糟的煩惱，抽塔羅牌當迷信少女；在任何一個無助的時刻，媽媽都會陪在身邊，務實的陪我思考解決方案，提供人生意見。雖然偶爾會覺得煩，但知道那其實都是關心。我愛你們，永遠永遠。

科法四年，變得更努力、更喜歡自己了，撐過了以為做不到的國考，也完成了比預期中更像個樣子的論文。接下來還要做更多的事！

白凌瑀

2023 年 7 月 21 日

法律學院霖澤館

doi:10.6342/NTU202302025

摘　要

在網路犯罪中，網域名稱（簡稱：域名）通常被用作指引非法網站，擴大犯罪規模之工具。若想要控制非法網站不被一般大眾造訪，除了關閉系爭網站外，也可以透過註銷域名，或是對域名「停止解析」來達成。停止解析能夠使我國網路使用者於上網時，無法享有正常的解析上網服務。是以，即便該網站架設於境外伺服器，或是網站域名註冊於境外，毋庸依賴司法互助，我國執法機關亦能夠透過停止解析，以一己之力及時阻止犯罪。

惟停止解析於我國刑事偵查程序的運用，實務尚未建立穩定之見解及程序，對於域名是否屬於扣押標的也存有疑惑，國內文獻亦較少就此討論。故本文以此為出發，欲透過美國與澳洲法之比較分析，嘗試建立我國處置非法網站域名之法制。並思考於現行法中，對域名發動扣押並以停止解析作為執行手段的合憲性。期許透過本文之討論，能讓科技手段合法且正當的成為我國執法助力。

關鍵字：網域名稱、停止解析、非實體扣押、網路犯罪、言論自由

doi:10.6342/NTU202302025

Abstract

In the realm of cybercrime, domain names are commonly used as guides for illicit websites, facilitating the expansion of criminal activities. To control access to these illegal websites by the general public, apart from shutting down the contested websites, domain names can also be canceled or subjected to "DNS RPZ". DNS RPZ prevents internet users in our country from accessing normal DNS resolution services. As a result, even if the website is hosted on a foreign server or its domain registered overseas, our law enforcement agencies can independently and promptly prevent cybercrime through DNS RPZ, rather than relying on international legal assistance.

However, the judicial practice hasn't built up the standard procedures of DNS RPZ. Additionally, whether domain names can be subjected to seizure is also arguable, for there is limited domestic literature focusing on this matter. Therefore, this paper aims to develop the legal framework for regulating the DNS by referring to American and Australian laws. Following that, the constitutionality for domain name seizure in the practicing laws will also be examined. Hopefully, this paper will be a proper proposal for the law enforcement to apply technological means legally and legitimately.

Keywords: Domain Name, DNS RPZ, Virtual Seizure, Cybercrime, Freedom of Speech

doi:10.6342/NTU202302025

簡　目

第一章 緒論.....1
第一節 緣起.....2
第二節 問題之提出.....11
第三節 研究目的.....21
第四節 研究方法.....22
第五節 本文架構.....23
第二章 停止解析技術分析.....25
第一節 名詞解釋.....25
第二節 技術優勢.....35
第三節 技術限制.....38
第四節 輔助制度—補足技術限制.....42
第五節 小結.....43
第三章 美國法.....45
第一節 美國扣押、沒收制度簡介.....45
第二節 美國域名扣押實務.....58
第三節 域名扣押合憲性審查.....64
第四節 分析與比較.....94
第四章 澳洲法.....98
第一節 澳洲法制簡介.....98
第二節 基本權.....105
第三節 授權依據合法性探討.....109
第四節 分析與比較.....115
第五章 我國法.....122
第一節 基本權限制.....122
第二節 法律保留.....127
第三節 比例原則.....134

doi:10.6342/NTU202302025

第四節 正當法律程序 139
第五節 其他 148
第六節 立法展望 151
第六章 結論 155
第一節 論文主軸與研究結果 155
第二節 停止解析的侷限與輔助措施 157
第三節 美國法域名扣押 158
第四節 澳洲法數據破壞令 160
第五節 停止解析於我國之合法性 162
參考文獻 165

doi:10.6342/NTU202302025

詳　目

第一章 緒論 1
第一節 緣起 2
第一項 安博盒子 3
第二項 關注 31 條網站 5
第三項 與楓林網之比較 9
第二節 問題之提出 11
第一項 停止解析之法律定性 11
第二項 問題意識 13
第三節 研究目的 21
第四節 研究方法 22
第一項 比較法研究 22
第二項 本國文獻回顧 23
第五節 本文架構 23
第二章 停止解析技術分析 25
第一節 名詞解釋 25
第一項 IP 位址 25
第二項 網域名稱（域名） 26
第三項 網域名稱系統（DNS）與解析 28
第四項 停止解析（DNS RPZ） 32
第二節 技術優勢 35
第一項 執行效果佳 35
第二項 與其他技術比較 35
第三項 小結 38
第三節 技術限制 38
第一項 直接輸入 IP 位址 38
第二項 透過快取資料上網 39
第三項 透過外國伺服器連線 39
第四項 重新申請域名 41
第五項 域名所有權移轉 41
第四節 輔助制度—補足技術限制 42

doi:10.6342/NTU202302025

第五節 小結 43
第三章 美國法 45
第一節 美國扣押、沒收制度簡介 45
第一項 刑事、行政與民事沒收 45
第二項 沒收程序比較 55
第二節 美國域名扣押實務 58
第三節 域名扣押合憲性審查 64
第一項 基本權干預 64
第二項 憲法上要求 66
第三項 比例原則 75
第四項 正當法律程序 83
第五項 司法管轄權 92
第四節 分析與比較 94
第一項 優勢 94
第二項 隱憂 95
第三項 我國法比較 96
第四章 澳洲法 98
第一節 澳洲法制簡介 98
第一項 澳洲法體系 98
第二項 網路管制手段 99
第三項 聚焦討論具體規範 102
第二節 基本權 105
第三節 授權依據合法性探討 109
第一項 1997 年電信法第 313 條第 3 項 110
第二項 2004 年的監視設備法之數據破壞令 112
第三項 小結 114
第四節 分析與比較 115
第一項 優勢 116
第二項 隱憂 116
第三項 我國法比較 118
第四項 我國法援引可能性 119
第五章 我國法 122
第一節 基本權限制 122

doi:10.6342/NTU202302025

第二節 法律保留 127
第一項 域名屬犯罪工具，得沒收 127
第二項 對「物」沒收 130
第三項 停止解析是否符合「扣押」定義？ 133
第四項 言論自由 134
第三節 比例原則 134
第一項 適合性—保全沒收必要性 134
第二項 必要性 137
第三項 相當性—狹義比例原則 138
第四節 正當法律程序 139
第一項 事前程序 139
第二項 事中程序 144
第三項 事後程序 147
第五節 其他 148
第一項 司法管轄權 148
第二項 輔助規範之建置 150
第六節 立法展望 151
第六章 結論 155
第一節 論文主軸與研究結果 155
第二節 停止解析的侷限與輔助措施 157
第三節 美國法域名扣押 158
第四節 澳洲法數據破壞令 160
第五節 停止解析於我國之合法性 162
第一項 法律授權依據 162
第二項 比例原則分析 162
第三項 程序正當性探討 163
第四項 管轄設計建議 163
第五項 未來修法與研究方向 163
參考文獻 165

doi:10.6342/NTU202302025

圖表目錄

圖 1 內政部警政署刑事警察局之網站查禁公告 10

圖 2 網址拆解 27

圖 3 DNS 的查詢順序 29

圖 4 國碼頂層網域之命名模式 30

圖 5 DNS 查詢流程 31

圖 6 國家型 DNS RPZ 架構 34

表格 1 美國法沒收制度比較 56

表格 2 試擬條文 154

doi:10.6342/NTU202302025

第一章 緒論

「安博盒子遭全面斷訊」的消息於 2021 年 12 月底時為各大新聞所播報，此新聞一方面宣示了我國執法機關保障智慧財產權之決心，另一方面也揭示了新興科技—「停止解析」運用於偵查之功效。現今世代的犯罪，大多利用網路作為載體，增加觸及並擴大犯罪規模，只要在網路上註冊一 IP 位址與網域名稱，即可將非法資料放置於網路空間並散佈於眾。

所謂「**網域名稱**」，下文簡稱域名，以台大法律學院官方網站為例，即「law.ntu.edu.tw」，一般人可以透過輸入域名而連結到網站。這段網址能夠輕易的被記憶，也可以從「law」推敲出本網站與法律有關。然而，域名並非網頁之真實所在位址，在電腦的識別系統中，台大法律學院網站之實際位址為 140.112.150.xxx，即 IP 位址，僅是一串數列，而不像域名可以讓人透過關鍵字等相關資訊與網站內容連結。由於事實上一般人並不會特別記憶網頁之 IP 位址，因此網路服務業者提供將域名轉換成 IP 位址之服務，這個讓使用者可以透過域名拜訪網頁的過程，稱為「**解析**」。

換句話說，在網路世界中，「域名」就好比地標名稱，如「台大法律學院萬才館」；而「IP 位址」則代表實際地址，如「台北市大安區辛亥路三段 30 號」。除非特別記住了地址，否則一般人想要造訪台大法律學院時，通常會以地標作為搜尋，而地標對應到實際地址的過程，即是上述之解析。

是以，若想要控制非法網站不被一般大眾造訪，以減少損害、嚇阻不法，除了關閉系爭網站，也可以透過對域名「**停止解析**」來達成目的。停止解析便是使我國網路使用者透過域名連結網站時，無法享有正常之解析服務。不論該網站係註冊於境內、外的域名註冊管理機構，停止解析可以讓我國之解析伺服器無法再提供正確

doi:10.6342/NTU202302025

的 IP 位址，而使我國網路使用者無法順利造訪非法網頁。蓋若域名註冊於境內之註冊管理機構，要使該機構配合註銷域名或停止提供域名使用服務，尚屬容易；若犯罪嫌疑人位於境內，要使其配合關閉境內網站，亦非不可行；但註冊於境外伺服器的域名，若沒有外國司法機關或該註冊管理機構之協力，對我國來說便成為執法困境，而停止解析則可以補足這個漏洞。

將新興科技運用於偵查，是近年被廣為討論的議題。科技便利了偵查手段，同時也可能擴大限制了人民的權利，若無與時俱進的法規範控制國家公權力，將會帶來疑慮。是故，本文以「域名扣押」為題，並討論其中的執行手段「停止解析」，處理此新技術在現行法下作為偵查手段運用，是否合適以及如何精進。期許透過本文之討論，能讓科技手段合法且正當的成為我國執法助力，不再讓偵查機關陷入「游泳追快艇」之窘境。

第一節 緣起

在近年網際網路之興起下，網路盜版侵權之法律議題甚囂塵上，各式各樣的影音串流平台流竄著侵權作品，不僅讓我國對著作權的保護蒙上一層灰[1]，並且此類網站使人人都可以輕易獲得盜版內容，更是擴大了著作權人的損害。而在疫情期間，人們使用網路的機會增加，也使得網路詐騙案例頻傳[2]，釣魚網站、一頁式網頁及彈跳視窗等。這些案例都再再顯現了網路安全保護以及管理之必要性。而國家可以透過什麼手段去避免非法內容於網路上流竄，同時保障人民權益又不至逸脫法治國原則，便是本文欲探討的主軸。

[1] 在美國商會 2021 年的台灣白皮書中，便提到「海外的盜版網站和侵權 APP 在 2020 年持續猖獗。目前仍然缺乏適當的法律制度和有效的政府行動來解決該問題，從而損害了著作權人的合法權益。」詳參台灣美國商會網站，https://amcham.com.tw/2021/06/2021-intellectual-property-licensing-position-paper/#tab-id-2（最後瀏覽日：09/30/2022）。

[2] 新冠肺炎大流行期間，依警察局之統計網路詐騙案件相較往年大幅度增加。詳參中央社（07/27/2021），〈疫情宅在家上網時間多 網路詐騙比去年同期增 9 成〉，https://www.cna.com.tw/news/asoc/202107270043.aspx。

doi:10.6342/NTU202302025

我國偵查機關打擊網路犯罪的技術也隨著犯罪手法日趨複雜而進步，不論是取消境內網站的域名註冊或是對境外網站為停止解析，都有辦法阻止我國大部分網路使用者造訪非法網站。然而，不可否認的，此作法也同時限制了人民自由上網、透過網路傳遞訊息及接收資訊等權利，有如國家在網路世界築起堡壘般，若技術遭惡性利用恐有生不當限制言論自由之情事。因此，如何在法秩序的維護以及人民自由間平衡，便成為新興偵查技術的難題。

本章節將透過近年我國的實際案例，觀察我國偵查機關針對非法網站的打擊手段，系爭手段是否符合法治國對於國家公權力發動的限制，以此作為本文的問題意識。並比較實務上面對註冊於境內與境外管理機構之域名，處理方法有何不同之處，且此差異是否造成法律上之落差。建立問題意識後，將參照美國及澳洲法進行比較法研究，並以之為鑑，盤點我國現行法，並討論我國法可能的修正、立法方向。

下文將以近期熱門案例介紹我國「域名扣押」概況，也可以發現域名扣押在我國發生的頻率日益漸增，成為實務重要議題。

第一項 安博盒子

安博盒子是一款多媒體影音機上盒，內建了部分的應用程式，利用這些應用程式及網路可以讓使用者收看不同來源的影音頻道。而其飽富爭議的理由在於安博盒子於系統上安裝的程式可以連線至其所屬之機房，而機房內提供了非常多免費但是侵害著作權的影音節目，使用者只要花小錢購買安博盒子[3]，就可以觀看無數影片，安博盒子毋寧是加劇了著作權的侵害。

在過去沒有停止解析技術時，執法機關面對境外註冊之非法網站，僅能在逮到犯罪網站的主嫌時，要求被告配合主動關閉網站[4]。但若找不到主嫌，而網站又是架設在國外無法關閉時，似乎就束手無策。雖然於規範上有司法互助的選項存在，

[3] 「安博盒子的硬體在中國製造後輸入我國，成本不到新臺幣一千元，售價高達四、五千元，這正是可收看侵權節目的加持，因為每一代安博盒子都綁定了收看盜版的軟體。」參中華民國衛星廣播電視事業商業同業公會（12/27/2021），〈安博盒子全斷訊 感謝政府執法決心—『拒絕盜版，支持正版』〉，http://www.stba.org.tw/news.aspx?id=20211228104126 &dd=20220106213208。

[4] 吳惠蘭檢察官接受中央社記者專訪時所表示。詳參中央社（05/02/2022），〈斷開與惡的連結 高檢署推動扣押域名首戰告捷〉，https://www.cna.com.tw/news/asoc/202202050094.aspx。

doi:10.6342/NTU202302025

但於實際情況，難以期待外國配合我國執法機關協助關閉網站[5]。是以，非法網站在此情形下也日益猖獗，只要將機台架設於國外，或是註冊國外的域名，便能輕易逃避法網。

安博盒子便是鑽此漏洞，台灣安博公司負責人向美國網際網路服務供應商承租網域及 IP 位址，設法使安博盒子連結到未取得版權的特定網址[6]，公開傳輸他人著作，侵害著作權。然而，將網站架設於國外之作法，似乎不再成為法律的化外之地。

於 2021 年 12 月，檢方針對安博盒子非法影像來源的 56 個網址向新北地方法院聲請域名扣押獲准，而財團法人台灣網路資訊中心（Taiwan Network Information Center，簡稱 TWNIC）配合扣押裁定，對系爭網域進行停止解析。雖無法關閉該外國網站，但可以使來自我國之連線連不上該非法網站。此時，位於台灣的安博盒子使用者，螢幕上僅會顯示「此網域已經遭到停止解析」的畫面，而沒辦法再觀看影片。如此之結果，對於台灣的民眾而言形同安博盒子全面斷訊，可謂即時且有效地防止著作權侵害擴大，補足前述法網之漏洞。

此例顯現出了停止解析對於打擊非法網站的效用，但也延伸出了許多法律問題。一、「域名」是我國刑事訴訟法之**扣押標的**嗎？依刑事訴訟法第 133 條第 1 項，我國扣押之標的為「物」，網域為無形的網路空間，與實體物之性質有所差異。二、而「停止解析」作為執行手段，與傳統的扣押於目的、效果、限制權利方面皆有所不同，可以援用刑事訴訟中扣押之規範作為法律保留之依據嗎？詳言之，傳統的扣押，其**意義**是為了保全證據或沒收，而暫時性的將物交由國家為占有[7]，使刑事訴訟程序得以順暢進行。而現今針對網域為停止解析，其目的則有部分是防止侵害擴

[5] 規範上存在國際刑事司法互助法，然而「觀察我國現有簽訂的條約協定，正式條約僅限與邦交國簽訂，惟對照歸納我國歷年來重大逃犯潛逃出境的可能去向大多為美國或中國，這些通常都不是我國友邦的國家，讓現有簽定條文的政治宣示功能比實用功能來得大。」黃姿蓉（2017），《我國刑事司法互助發展模式與困境之探討》，頁 85，中央警察大學外事警察研究所碩士論文。

[6] 聯合報（10/08/2021），〈藝人用安博盒子看盜版引風波 刑事局聯手新北檢全抄了〉，https://udn.com/news/story/7321/5802276。

[7] 林鈺雄（2022），《刑事訴訟法（上）》，11 版，頁 453。

doi:10.6342/NTU202302025

大、避免損害，防止損害是否為刑事訴訟程序目的，不無疑義；在**效果**方面，我國刑事訴訟上之扣押，係剝奪被告對扣押物之支配、處分權[8]。然而在實施停止解析時，犯罪行為人仍能透過不受我國司法管轄之境外域名註冊管理機構，繼續支配或處分該域名。更有甚者，對於境外註冊之域名，若於我國遭停止解析，也僅能阻擋我國之網路使用者之一般連線，外國使用者仍能連上該網站，此種情形難謂「剝奪」被告之支配與占有，與傳統扣押之概念並非完全相符；**限制權利**方面更是本文關注之重點，一般所認知的扣押，既然是由國家暫時性的占有物品，即限制物品所有人自由使用、收益該物之權利，為財產權之限制。然而，停止解析對於域名的限制使用，似乎不僅有財產權限制之面向。一方面，域名已被廣泛承認其具有財產價值，屬於財產之一種，而認停止解析干預了受處分人的財產權；另一方面，不容忽視域名的使用與言論自由息息相關。蓋不論是網站經營者張貼言論、造訪網站的人留言或接收資訊，這些都關係到人民言論自由之權利，而網站乘載的資訊之所以能進入言論市場，就是依賴域名與解析。準此，與傳統的扣押相比，對網域的扣押更多了言論自由之干預，惟仍援用原則上僅授權干預財產權之扣押規範作為法源依據，似乎有所不妥。綜上所述，停止解析之目的、效果、限制權利範圍，恐難完全等同於我國法上之扣押執行，其權利干預性質引發法律保留的疑慮。

此外，在所謂「安博盒子全面斷訊」後相隔不久，使用者們便發現安博盒子又能夠觀看影片了。雖原本的域名無法被我國使用者正常解析，但申請、變更域名並非難事，只要安博公司不斷地更換域名、搬動網站，且更換頻率相較我國執法機關聲請扣押的速度還快，那麼停止解析能發揮的實際效用似乎相當有限，在規範上是否容許其他輔助手段以補充停止解析之不足，也有討論之必要。

第二項　關注 31 條網站

與安博盒子之案例類似，關注 31 條網站的域名也成為行政沒入之標的，被移轉於國家公權力所控制。但關注 31 條網站遭關閉的理由與安博盒子不同，其涉及

[8] 法務部，行政院「網路不實廣告管理專案會議」有關議題之研析意見，頁 2-3。

doi:10.6342/NTU202302025

國安之危害。由此可見網路犯罪之危害層級逐漸上升，從侵權行為提升至國家安全問題，顯現出我國確實需要有效且即時打擊網路犯罪之手段，但同時該手段又必須符合法治國之要求與程序正當性。下文將介紹關注 31 條網站之案例，以之推導出域名扣押之存在必要性以及停止解析干預言論自由之面向不容忽視。是以，雖然有賦予國家將停止解析作為執法手段之必要，但手段的發動必須要通過謹慎、可供檢視的程序把關，以免對人民造成過大的權利侵害。

於 2018 年，中國推出惠台 31 條措施[9]，並在實施屆滿一年之際，以「31t.tw」註冊台灣域名，推出「關注 31 條」網站。該網站內容大多是惠台措施的相關資訊及報導。惟嗣後經由總統府發言人證實 31t.tw 此域名係由中國國務院台灣事務辦公室轄下的「北京海峽文化交流有限公司」所註冊，其註冊目的是為了在台灣從事具政治目的之宣傳，引發國安疑慮。該網站內容違反了兩岸人民關係條例第 34 條[10]不得為中共政治宣傳以及同法第 89 條第 2 項[11]得沒入該廣告之規定[12]，國家通訊傳播委員會於收到國防部之公文後，通知 TWNIC 註銷其域名[13]（即依行政手段沒入該域名）。

由於關注 31 條網站內容是在提供中國惠台 31 項措施的相關資訊，確屬有關「大陸地區」事項之廣告，該當兩岸條例之政治宣傳，應無疑義。但該條例所稱「得沒入」者為「廣告」，但域名只是一串網址，31t.tw 文字本身也難認為是有意義且可以作為政治宣傳的廣告。因此，便有論者拋出疑問，在本例中得否依該條例將域名認作廣告而沒入呢？就此而言，論者以為廣告一詞係指資訊的傳遞與提供，廣告

[9] 國台辦聯合其他等 29 個部門於 2018 年 2 月 28 日聯合發佈了「關於促進兩岸經濟文化交流合作的若干措施」，此又被台灣媒體稱作「31 條惠台措施」，其內容涵蓋了投資、金融、教育、文化、影視等多個領域。

[10] 台灣地區與大陸地區人民關係條例，第 34 條第 2 項第 1 款：「在台灣地區從事依該條例許可之大陸地區事項廣告播映、刊登或其他促銷推廣活動，不得為中共從事具有任何政治性目的之宣傳」。

[11] 台灣地區與大陸地區人民關係條例，第 89 條第 2 項規定：「委託、受託或自行於臺灣地區從事依該條例許可以外之大陸地區事項廣告播映、刊登或其他促銷推廣活動者，其廣告不問屬於何人所有或持有，得沒入之」。

[12] 蔡志宏（03/28/2019），〈『關注 31 條』網站域名下架，是台灣域名法學發展上的里程碑〉，《關鍵評論》，https://www.thenewslens.com/article/116230（最後瀏覽日：06/15/2022）。

[13] 公視新聞網（03/16/2019），〈國安疑慮 NCC 封鎖中國『關注 31 條』網站〉，https://news.pts.org.tw/article/425750。

doi:10.6342/NTU202302025

本身僅是一抽象之概念，難以進行沒入。所以，條例中所謂「沒入廣告」，於解釋上可以合理推論是指得沒入「廣告所在的載體」[14]。是以，域名乃該網站內容依附之傳遞工具，於本件得沒入之。

本案例相較於安博盒子，另外衍生之法律議題在於：一、本件沒入域名並未經過法院事前審查，而是行政機關逕行行文要求 TWNIC 協助註銷。行政程序不若司法審查嚴謹，且未經公正第三方審查即註銷域名，有程序保障不足之疑慮，何況現行域名註銷之過程也未見賦予相對人陳述之程序設計。甚言之，參酌 TWNIC 之政策，其停止解析網域的情形包括（一）依法院之判決或裁定、（二）依行政機關之命令、（三）犯罪防治緊急案件處理以及（四）網域名稱影響資安重大者[15]，後三者皆無司法審查，且所謂「犯罪防治緊急」及「資安影響重大」等用語模糊，由 TWNIC 自行判斷與決策即可發動停止解析，而無其他審查機制，容易淪為濫權之利器。由此可見，現行對於域名管理政策之規範尚為不足，程序保障問題亦在本件浮現。二、關注 31 條網站的出現，也彰顯了在資訊時代下，國家安全與網路自由之難題。面對網路戰，停止解析可以作為我國的防禦工具，確實是必要之手段。然而，一體兩面地，此種親中宣傳毋寧是一種政治性言論，依照釋字第 644 號，此亦為言論自由保障之範圍。進一步言，政治性言論在釋憲實務上通常被認作高價值言論，須給予更大程度的保障，不得任意限制之。相較於安博盒子案，本件所限制之言論，理應經過更高密度的審查，現實上卻並非如此。

或有認為，即便是傳統的扣押，若扣押之物為書信或其他表現言論之載體，也有可能涉及言論自由之干預，域名扣押在此並無特別關注之必要。然而，本文以為，針對扣押的域名並非僅僅是對於言論自由的輕度限制，基於現今社會對於網際網路之依賴，大眾已習慣於透過網路空間交流想法、發表言論。雖然網路空間是否構

[14] 蔡志宏，前揭註 12。
[15] 財團法人台灣網路資訊中心，https://www.twnic.tw/dnservice_argue_company.php（最後瀏覽日：06/15/2022）。

doi:10.6342/NTU202302025

成「公共論壇」尚屬爭議問題[16]，但此爭議也顯現出網路世界言論自由的重要性在現今社會逐日漸長，成為不容忽視的事實。另一方面，域名本身就是言論之載體，人們註冊域名就是為了傳遞資訊與發表意見；域名的價值也是隨著其知名度提高[17]，容易辨識與廣為人知的域名將成為網路使用者的優先選擇[18]，而越高的瀏覽數就代表越多人透過該網域接收資訊，域名的價值也隨之提升。換言之，相較於一般財產權，域名跟言論自由的相關性更為強烈。是以，域名扣押的討論無法與言論自由之干預脫鉤[19]，且相較於一般的書籍與信件，網域所涉之言論自由更為廣大。扣押網域不僅僅是網域註冊者之言論發表受到限制，還有於無數的網站留言者[20]，甚至「知的自由」也是言論自由之一環，故潛在的網路瀏覽者接收資訊的權利也將遭受影響。綜上，域名扣押對言論自由之干預，尤應有完整、嚴謹的程序把關，也應該與傳統扣押在此作出明確區別。

附言之，在關注 31 條網站此案例中，註銷域名也另外涉及比例原則之問題。如前所述，沒入域名係對人民權利干預之公權力措施，故除了前述的程序保障及法律保留之討論外，也應符合憲法上比例原則之要求。在本案例中，似乎欠缺沒入域名的必要。蓋真正涉及政治宣傳的是網站之內容，而非域名，故將網站中涉及政治宣傳之部分移除，即可以達到執法目的，中性的域名似乎並無一併註銷之必要。舉例而言，若將違法廣告寫在傳單上，沒入標的可以涵蓋與廣告不可分的傳單，但以電視進行違法廣告時，卻將電視台用以發送廣告的設備全數沒入，則明顯違反比例原則[21]。在個案中，若侵權之內容僅佔網頁一小部分，卻針對整個域名停止解析，

---

[16] 陳怡卉（2017），《公共論壇與言論自由—以美國法制為中心》，頁 122，東吳大學法律學研究所碩士論文。且有認為，網路空間無「稀缺性」之特徵，故無公共論壇理論適用之餘地，蓋公共論壇理論之前提係發表言論的空間有限，故國家有義務提供使人民放心討論的場域。Derek E. Bambauer, *Orwell's Armchair*, 79 U. Chi. L. Rev. 863, 912 (2012).

[17] 蔡志宏（2018），《全球域名法制之治理架構研究—以 ICANN 的組織原理及制度運作為中心》，頁 2，國立交通大學科技法律研究所博士論文。

[18] 同上註，頁 6。

[19] 「域名最初功能雖僅在於便利使用者記憶網路位址，但就因為域名可供人類辨識，而可以傳達思想，域名本身的存在以及使用之容許性，就與言論自由產生關連。排除禁用特定域名，可能就會有侵害言論自由之疑慮。」同上註，頁 8-9。

[20] 另有論者認為特定域名的的網站，也有匯集群聚持相同言論或意見者之功能，故認為停止解析亦涉及集會結社自由。同上註，頁 9。

[21] 蔡志宏，前揭註 12。

doi:10.6342/NTU202302025

也會遭逢比例原則相當性之問題。是以，公權力針對域名所為之限制，其涉及比例原則之疑義也在本案例中顯現。

第三項 與楓林網之比較

將安博盒子與關注 31 條網站案兩相比較，前者是「針對境外註冊之域名，運用停止解析執行扣押」；後者則是「針對境內註冊之域名，以取消註冊之方式執行沒入」。兩者的執行名義及方式迥異，除了違反法條不同外，另一值得注意的是執行標的之不同（分別是境內、外註冊之域名）所造成的執行差異。究竟註冊於境內或境外之域名註冊管理機構，於執行上有什麼不同，本文將以「楓林網」之案例詳細討論其法律意義。

國內最大影音盜版網站「楓林網」之負責人於 2020 年 4 月遭刑事警察局以違反著作權法為由遭逮捕，網站因此關閉，成為近年最令人矚目的網路治理案件，本案也同時被認為是國內司法實務首次對「域名」進行扣押的先例[22]。而本件使域名無法指向楓林網的實際方式，係由於警方逮捕了國內負責人，使其移轉域名控制權，變更電磁紀錄，使網址導向執法部門所設定的頁面（見圖 1）。

[22] 立法院， https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=195951（最後瀏覽日：6/16/2022）。

doi:10.6342/NTU202302025

圖 1 內政部警政署刑事警察局之網站查禁公告

資料來源：Newtalk 新聞（04/08/2020），〈盜版退散！警方查禁國內最大免費影片網站『楓林網』〉，https://newtalk.tw/news/view/2020-04-08/388156。

同樣是以侵害著作權法為由而遭域名扣押的安博盒子案，所運用的是停止解析之技術，使國內使用者透過搜尋連線安博網頁時，無法透過原本的域名連結至網站。而楓林網案則是由執法機關直接取得域名的控制管理權限，將其域名所對應的網頁，由楓林網轉至執法部門之頁面。兩案採取不同的執行方式，根本的理由在於安博盒子所註冊的是由美國管理的域名，非我國業者所得控制。而基於我國之國際情勢，司法互助並非通常存在的選項，因此僅有停止解析可以達到使國內使用者停止透過一般方式前往網頁的效果。但實際上該網頁、域名仍存在，境外使用者透過原域名、或是國內使用者透過其他手段繞過我國之 DNS 架構，實際上仍能造訪該網頁。反之，在楓林網案，由於是直接將域內註冊的域名移轉由國家控制，故不論世界各地的網路使用者透過域名搜尋，都無法再看到楓林網原本的頁面。透過兩案比較，可以察覺停止解析作為域名扣押執行手段之侷限。

「停止解析」雖然不如註銷域名、關閉網站來的有效，卻補足了過去執法機關對於境外域名束手無策的法網漏洞。而兩種執行方法對於受處分人以及一般網路

doi:10.6342/NTU202302025

使用者之權利干預與執行效果皆有所差異。很明顯的，停止解析僅是限制「國內使用者其中一種上網方式」，對於受處分人而言仍可以自由使用與處分域名，而網路使用者們也仍得透過其他手段造訪網站。停止解析對人民上網之權利干預較小，同時防止侵害的效果也較為不彰。另外，境外域名之註冊者通常是偵查機關難以追蹤、通知者，不若境內域名可以透過 TWNIC 協力提供註冊資料聯繫並通知受處分人。是以，針對境外註冊之域名該如何賦予受處分人便利且可行的救濟管道，以充實程序保障，亦形成實務難題。

綜上，停止解析作為執行方法，因技術限制執行效果有限，難以完全地阻止再犯，後文將討論如何配套措施以加強執法；另一方面，對於境外域名的停止解析於程序保障方面則有現實難題，該如何補足保障，此二問題亦將於後文更詳盡地討論。

第二節　問題之提出

透過上述案例之討論，可以發現停止解析運用於偵查之中，衍生出了許多爭議。而這些議題便是本文所欲探討者，故藉由前揭案例建立本文的問題意識。惟進入爭議探討之前，本文想先確立何以我國大多數的實務與學說對於**停止解析**之討論，皆將之定性為**域名扣押**之執行方式，而以傳統扣押與停止解析之區別作為討論重點。

第一項 停止解析之法律定性

按目前多數見解對於強制處分之定義，並不再固守過去以「強制力」作為區分的想法，而是採取「刑事訴訟上之基本權干預說」，以精確描述這種公法行為之特性，此亦較符合憲法對於基本權保障之理念[23]，近期之實務見解亦同此說[24]。故具備國家性之基本權干預措施，便需要受到刑事訴訟上的取證規範拘束，並通過干預正當性之檢驗。換言之，強制處分乃刑事訴訟程序中，國家機關為追訴犯罪、保全被告及蒐集證據，對受處分人施加的措施，而該措施干預了受處分人之基本權。查

[23] 林鈺雄，前揭註 7，頁 312-313。
[24] 最高法院 110 年台上字第 3858 號刑事判決；最高法院 110 年台上字第 4549 號刑事判決。

doi:10.6342/NTU202302025

停止解析乃偵查機關於刑事偵查之過程中，對於域名註冊人所為，**限制**其言論自由與財產權等**基本權**之國家公權力行為，故停止解析乃國家干預人民基本權之措施，為一強制處分，自無疑義。

而停止解析究竟是一個新型態的強制處分，抑或其屬於現行刑事訴訟中已規範者，則有討論之空間。惟若將之定性為新型態強制處分，則勢必會受到法律保留之限制，在立法者修法之前，無法將之作為合法之偵查手段。然修法曠日廢時，並非一蹴可幾，且若每一種新技術之出現都需要透過立法解決，偵查機關將永遠晚於犯罪者一步，難以有效追訴犯罪。故本文基於現實面之考量，認同在現階段於現行規範中尋求解答之作法[25]。是以，盤點現行刑事訴訟法所規範之強制處分，停止解析對於「域名限制使用」之性質，與「扣押及沒收針對財產權限制」較為相近，故接續以此二者討論。

於傳統的定義下，沒收係國家以判決**終局剝奪**人民之財產權，將系爭財產之所有權移置國庫；扣押則是對於可為證據或得沒收之物，使國家對其**暫時占有**之強制處分。而停止解析於效果上至多僅能達到讓使用我國伺服器上網之民眾無法透過解析服務連線上該網站，於效果上僅能論以「限制使用」，而不致終局剝奪並移轉所有權於國家之程度，與沒收之效果有較大的差距。而暫時性的限制域名的使用效果，與占有類似，皆是對於財產之所有權能的部分干預。準此，以「針對域名之扣押」來討論停止解析技術，毋寧較為相近。且在現今科技進步之下，對於沒收與扣押的定義也有所變化，不同型態的財產權干預，都有可能被認定屬於扣押之一環。

是以，就此確立了本文的討論方向，係將停止解析作為域名扣押此強制處分之執行方法。於此前提之下，接續案例討論，整理域名扣押、停止解析之爭議，建構本文之問題意識。

---

[25] 雖將停止解析定性為新型態強制處分，透過修法可以設置更加量身定作之規範，能夠更適切的考量其特殊性。然而此並非唯一的選擇，在修法緩不濟急之下，司法者透過合理解釋而使停止解析有現行施用之空間，亦非憲法所不許。「憲法上權力分立之架構，在立法與司法之間，應該是一種動態的平衡，在此議題，並不存在絕對性或先驗性非立法不可之領域，如此在立法動能尚未充足之情況下，司法依舊可以透過個案的裁判來解決社會問題。」蔡志宏（2022），〈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》，31 期，頁 226-228。

doi:10.6342/NTU202302025

附帶說明，本文並非全盤否認將停止解析運用於沒收之可能性。蓋囿於我國之境外執法侷限，實際上難以剝奪境外註冊的域名。故對於境外域名的沒收判決執行，以停止解析作為執行手段，乃現實上可行之作法。雖無法達到沒收剝奪的終局執行效果，但至少可以讓系爭域名在我國的使用受到干預，以及讓我國使用者搜尋不到系爭違法網站。

第二項 問題意識

於本項整理前述案例所提出之問題並梳理架構，以聚焦本論文之討論重點。**域名扣押，既然屬一強制處分**，則自然要受到法治國原則與正當法律程序之審視。故本文透過「基本權干預體系」之架構審查，在各個階層中整理域名扣押與停止解析可能遭遇之法律爭議，作為本文之問題意識。問題依序提出如下：

一、法律保留

（一）域名是否「可為證據」或「得沒收」？

按刑事訴訟法第 133 條第 1 項，可為證據或得沒收之物，得扣押之。是以，若欲針對域名扣押，必須先處理域名是否該當本條之得扣押標的。首先，於此類網路犯罪中，運用於刑事訴訟上之證據應係該非法網站本身，域名之存在理論上無法直接的證明犯罪事實，似無作為證據之意義[26]。退一步言，於某些情況或許域名有作為證據之可能，惟證據扣押與沒收扣押並非相斥之存在，本可分別或同時發動。是以，即便域名得作為證據亦不妨礙其遭沒收扣押之可能。而由於域名得否作為證據較有賴個案討論，故本文討論重點將置於**域名適用沒收扣押之可能性**。

在犯罪中，域名的使用有助於非法網站之傳播及散佈，對於犯罪結果有所助益，故應得將其認作犯罪工具。復依刑法第 38 條第 2 項，**供犯罪所用**之物且屬於犯罪行為人者，得沒收之。準此，既然域名為犯罪工具，似得依此進行沒收扣押。

[26] 詳言之，域名之於網站，相當於書目標籤之於書本。域名只是一中性的索引標籤，而無法說明網站之內容，無法證明犯罪事實存在。

doi:10.6342/NTU202302025

（二）域名得否作為扣押「物」？

惟查，此處仍存在另一爭議，即域名得否為得扣押之「物」，存有法條文義解釋之爭議，蓋域名的非實體性質，與有體物有所區別。然而，我國刑事訴訟法中扣押之規定僅將「物」作為標的，究竟無形的域名得否成為扣押標的，亦為問題。另外，域名之財產性質於實務及學說上也多有爭議，本文將一一探討梳理之。

（三）停止解析是否該當扣押執行手段？

再者，若是肯定域名得作為沒收扣押之標的，但停止解析是否屬於扣押執行之手段也非毫無爭議。停止解析之意義和效果皆與傳統的扣押有所區別，援引扣押之規範作為授權來源，尚有待釐清。雖本文於前段認為停止解析對於所有權能的部分干預，與傳統扣押對於財產占有的干預具有相似性，但不代表可以理所當然地將扣押從剝奪占有的概念轉化為其他性質的干預，故此爭議也具有討論之必要。

（四）對言論自由之限制，是否為扣押之授權範圍？

即便在前面的問題都獲得肯定域名扣押之答案，認可域名為我國刑事訴訟法之扣押標的，仍須注意法律解釋之界限，不得有背離規範目的之解釋結果。而刑事訴訟法關於扣押之規定，其意義係立法者透過事前權衡，授權偵查機關於特定情況下得限制人民財產權。換言之，域名扣押對於言論自由之干預面向，似乎並非原立法者已權衡，並授權予偵查機關者。

詳言之，傳統的扣押主要涉及人民財產權之干預，對於言論自由僅在部分案例中產生輕度限制。但域名扣押之目的本身就是在於限制不法言論被接觸及散佈，對於言論自由之干預不容忽視，在某些案例中更可能涉及到高價值的「政治性言論」。同時，域名也具有財產權之性質[27]，雖然其權利性質仍有爭議[28]，惟目前多數學說皆肯定其具有財產性質。尤其是現在網際網路的興盛，部分具識別性的域名被評估為高價值，蔚為網路世界之不動產。準此，域名扣押，相較於傳統扣押，其在財產權以外多干預了言論自由。財產權與言論自由雖同屬基本權，但在違憲審查上，司

[27] Alexis Freeman, *Internet Domain Name Security Interests: Why Debtors Can Grant Them and Lenders Can Take Them in this New Type of Hybrid Property*, 10 AM. BANKR. INST. L. REV. 853, 889 (2002).
[28] 蔡志宏，前揭註 25，頁 202-206。

doi:10.6342/NTU202302025

法實務對於言論自由之限制傾向採取較嚴格之審查[29]。蓋依司法院釋字第 509 號解釋，言論自由為人民之基本權利，憲法第 11 條定有明文。而國家應給予最大程度之保障，以利其發揮實現自我、溝通意見、追求真理及監督政府之功能，促進社會發展，屬於重要基本權。基此，由於域名扣押對於言論自由構成額外限制，且此限制不容忽略，若仍運用原本的扣押作為授權依據，是否能通過法律保留原則不無疑義。

法治國要求國家之公權力實施，若對人民之基本權構成限制，則需要符合「法律保留」及「比例原則」。在法律保留方面，上述域名扣押對於言論自由的額外限制即構成問題。而若通過法律保留之審查，域名扣押則進入下一階段—比例原則之檢視。

二、比例原則

域名扣押與停止解析所會遭遇之比例原則問題有二：其一，是立法通案性的討論，針對域名發動扣押，是否符合比例原則？以及使用停止解析作為執行手段，是否符合比例原則？其二，則是司法個案適用之問題，若網站中僅有部分內容非法，於個案中法官應如何操作比例原則，才不致過度侵害人民基本權？以及於個案中應如何依言論之類型調整審查基準？由於後者與強制處分之事前程序保障中，法官保留的層次有關，故本文將此個案性的討論置於後。而於此階層僅處理通案性的問題，即將停止解析作為域名扣押執行手段是否妥適。

比例原則的操作需要依序經過適合性、必要性及相當性（狹義比例原則）三階段的審查。在適合性階段，將遭遇的問題是，針對域名停止解析，似乎無助於後續的沒收執行。是以，停止解析似乎欠缺作為扣押手段的適合性。而在必要性階段，由於技術上存在其他使非法網站不被網路使用者造訪之手段，如：IP 位址過濾、

[29] 雖然依司法院大法官解釋第 414 號及 445 號所闡釋言論自由之「雙軌、雙階審查」，對於非言論內容或低價值言論之限制，採取較寬鬆之審查，然而此為少數之案例。在多數關於言論自由之限制案例，通常仍採取中度以上之審查標準。且與之相對的財產權干預案例，實務上至多僅採取中度標準，討論也多聚焦於「正當程序」、「補償」，而非財產權限制本身。由此可知，財產權並不若言論自由般的不可限制，其所關注者在於制度的維持與公平性。

doi:10.6342/NTU202302025

URL 過濾。而選擇停止解析（DNS RPZ）作為扣押執行手段，是否為達到偵查目的所必要之最小侵害手段，則有待討論。最後，在相當性的階層，也要審查停止解析所追求的公共利益，是否與對於人民權利的干預衡平。

於通過法治國原則之審查後，強制處分尚須符合正當法律程序之要求。

三、正當法律程序

不論是憲法或是刑事訴訟法，皆有提及強制處分應循正當程序之要求。前者之依據係憲法第 8 條關於人身自由拘束之程序保障；後者則散見於刑事訴訟之條文中。不論如何，對於基本權之干預，應有正當之程序保障，並無疑義。而扣押之正當法律程序又可以區分為事前、事中及事後階段，以下分述。

（一）事前程序—法官保留

在此需事先說明，本文對於域名扣押的討論，限於**明網**內的域名犯罪。蓋暗網上的網站型態變化多端，有時需要有密碼始得進入暗網，或需要經由特殊的手段才能造訪其中特定的網站。若將此部分加入本文，會導致討論內容過於龐雜，故本文將域名扣押之討論限定於明網中，即一般大眾的上網方式。

扣押於我國刑事訴訟法上可以區分為「附隨於搜索之扣押」或「非附隨於搜索之扣押」。而在明網中的域名，係顯示於網址末段者，無需經過搜索即得確立標的（即欲扣押之域名為何者），故其適用之程序係後者。

復按刑事訴訟法第 133 條之 1 條第 1 項，除得為證據之物或經受扣押標的權利人同意外，應經法官裁定。另按同條第 3 項，該裁定需明定案由、扣押標的及得執行之有效期間等資訊，本條乃令狀原則之展現。令狀原則係學理上之名詞，其係在規範強制處分核發之事前程序，意義有二：其一，限制核發令狀權限之主體，應由獨立於偵查機關以外之有權機關事前審查，本條將此權限授予法官行使，相當於「**法官保留**」之概念展現。其二，令狀記載須符合明確性原則，透過於令狀上事前明確之規範，得以促使法官慎重審查；節制偵查機關，抑制權限濫用；使受處分人

doi:10.6342/NTU202302025

瞭解被侵害權利的內容及範圍，便於監督與救濟[30]。附言之，於第 133 條之 2 條第 3 項，設有緊急扣押之例外規定，容許事後陳報，依此可謂扣押係採取「相對法官保留」。

令狀記載明確性原則，於刑事訴訟法第 133 條之 1 條第 3 項已有明確之規範，運用在域名扣押上亦無爭議。且即便於域名扣押中，容易出現註冊人不明或難以確認之狀況，依同項第 2 款之但書，於應受扣押裁定人不明時亦得不予記載，於實務操作上並無疑問。

然而，在法官審查扣押聲請時，則有個案中應如何操作比例原則之疑慮，尤其域名扣押與傳統扣押於干預權利面向有所差異。法官於審查時該如何調控審查密度，具有討論空間。

1.審查密度調整

對於網站中僅部分侵權之案例，卻將其域名扣押，形同遮蔽整個網站，顯現出不符比例之疑慮，該如何在案例中操作比例原則也有待思量。另外，面對不同種類及價值之言論，其比例原則之操作是否也應該同違憲審查調整審查密度？

而停止解析作為其中一種執行手段，由於其並非將網域全然移除之狀態，技術上仍有造訪系爭網站之可能，故對於受處分人之限制較為輕度。基於停止解析於執行之特殊性，於法官裁定時，該如何將此納入比例原則之審查，是否以及該如何調整審查密度？

2.現行規章架空司法審查

前述為法官保留於扣押程序實際操作之討論。然而，於現行規範下，除緊急狀況得事後陳報外，尚容許其他未經法官保留即得停止解析域名之情況。如「關注 31 條」網站一案，透過行政處分即將網域沒入。且按 TWNIC 之 RPZ 治理機制（即停止解析之管理政策），得實施停止解析的情事，除了依法院之判決或裁定外，更包括依行政命令、因犯罪防治緊急案件處理以及當網域名稱影響資安重大者。此類

[30] 陳運財（2014），《偵查與人權》，頁 303。

doi:10.6342/NTU202302025

未經司法審查及法律授權之停止解析，其程序是否足夠嚴謹？蓋如前所述，停止解析運用於偵查中具有干預人民權利的性質，而刑事扣押及強制處分，原則上應適用令狀原則之規定[31]，在此被轉化運用於行政程序之扣留與沒入，似乎巧妙地迴避了令狀原則之要求，致有「刑事扣押遁入行政扣留及沒入」之疑慮[32]，故本文將分析現行域名管理政策之規範，思考執行停止解析之審查程序正當性。

（二）事中程序—裁定程序之參與及扣押流程

1.裁定程序之參與

按刑事訴訟法第 133 條之 1 條第 4 項，核發扣押裁定之程序，不公開之。其立法理由係為避免證物滅失或應被沒收財產之人趁隙脫產。然而，如前所述，域名通常無法作為證據，故無證據滅失之疑慮；至於脫產方面，域名確實可以於不同的註冊管理機構間移轉，或是變更所有權人，存在防止移轉之必要。惟此僅需透過扣押命令中禁止處分之效力便可以達成，而禁止處分實際的執行方式只要透過通知域名註冊管理機構協助配合即可，停止解析無法達到此防止脫產的效果。換言之，在扣押執行中，採用停止解析作為執行手段，似乎不存在秘密執行、程序不公開的理由，則受停止解析處分之人是否於裁定程序中有參與權呢？

2.扣押流程

扣押執行之流程，於刑事訴訟法已有完善規範。然而，現行的扣押之條文顯係針對有體物扣押所制定之程序規範，其是否適合套用於域名扣押？或是該如何就條文解釋使其符合域名扣押之特性，本文將於第五章我國法之章節討論。

（三）事後程序—受處分人及網路使用者之救濟與程序保障

與扣押之執行流程相同，對於扣押裁定之救濟程序，於刑事訴訟法中已有詳盡之規範，運用於域名之扣押似無疑義。然而，最常需要運用停止解析技術的案例，通常是犯罪行為人不在境內或是甚至無法追蹤的情況。就此，該如何踐行通知、賦

[31] 刑事訴訟法第 1 條第 1 項：「犯罪，非依本法或其他法律所定之訴訟程序，不得追訴、處罰。」
[32] 陳文貴（2017），〈行政檢查與令狀原則之界限探討〉，《中原財經法學》，39 期，頁 142-143。

doi:10.6342/NTU202302025

予陳述意見機會及提供救濟而滿足其程序保障，現行法之規範完整且足夠嗎？這些也都是討論之重點。

四、「停止解析」作為執行手段的特殊性

當域名扣押通過基本權審查架構檢視後，對於運用停止解析作為域名扣押之執行手段，尚有與傳統扣押不同之處需要考量。如「審判權過度擴張之疑慮」，雖刑事訴訟中本就偶有涉外因素，尤其在現今之網路世代，匿名性及跨域性更是網路犯罪之特徵，追訴之過程中亦頻繁與外國司法權有合作需求，惟此於停止解析之實施將更為明顯，需重新檢視現行法於司法權擴張之適用性。另一方面，停止解析並非萬能，其仍有技術上可突破之處，因此在域名扣押之實施中得否有其他輔助手段或司法外之制度，能夠協力保障網路安全，亦係本文所欲探究者。

（一）審判權過度擴張

對於同一事實，關係到複數國家之刑罰及刑事管轄權，在適用上發生競合時，為了調整及分配各國刑法的適用範圍，主要援用屬地主義、屬人主義、保護主義、普遍主義及船旗國主義各基準來決定[33]。我國刑法便是從此原則，判斷一案件是否為我國刑罰權效力所及，適用上以屬地原則為優先[34]。而程序法係為貫徹實體法的執行，故刑法適用法關於刑罰權之劃定，亦具有其程序法面向之意義。刑法對於刑罰權之效力範圍，亦得用以定我國刑事法院審判權之範圍，決定我國是否刑事法院是否得予審判、發動偵查[35]。

但網路犯罪能夠穿透實體的邊界，對於現行傾向以領土邊界作為司法管轄權劃分基礎的體制便形成困難。網路犯罪的特性，在於其雖實際存在一犯罪行為地，但犯罪之結果卻能遍佈全球，只要是能上網的地方，就有可能連結上該非法網站。在操作我國刑法第 3 條屬地原則時，所謂的領域內犯罪，依同法第 4 條只要犯罪行為地或結果地其中之一在我國領土內即屬之。就此，面對網路犯罪，所謂的「犯

[33] 魏靜芬（2001），〈國際法上管轄權之域外適用〉，《中央警察大學法學論集》，6 期，頁 388。
[34] 中華民國刑法第 3 條：「本法於在中華民國領域內犯罪者，適用之。在中華民國領域外之中華民國船艦或航空器內犯罪者，以在中華民國領域內犯罪論。」
[35] 最高法院 110 年度台上大字第 5557 號刑事大法庭裁定。

doi:10.6342/NTU202302025

罪結果地」該如何解讀，於學說上便出現爭議。若採廣義說，以「得於某地藉由電腦連結上該網頁」作為犯罪結果地，如此幾乎在世界各地均有可能成為犯罪地，此已涉及各國司法審判權之問題，且對當事人及法院均有不便；若採較狹義之說法，強調行為人之住、居所或網頁主機設置之位置等，似又過於僵化[36]。

在過去即便採取廣義說，而將與我國關聯性低之案件納入我國司法管轄，於偵查中也會遭遇我國欠缺司法互助之事實而難於實際上追訴。惟於現今，若在偵查案件中運用停止解析技術，便有可能實質的擴張我國強制處分的執行範圍，但這種擴張執行模式，是否會造成當事人之不便、我國司法系統之過重負擔以及與他國之管轄衝突，不無疑義。

在**國際管轄權**會生此問題，在**國內法院**之分工亦如是。我國刑事訴訟法第 5 條法院土地管轄中「犯罪地」之解讀，依實務見解[37]應參照刑法第 4 條之解讀。是以，也生網路犯罪之管轄法院是否採廣義說形成全國法院皆有管轄權，進而使法定法官原則之限定功能喪失之爭議。運用停止解析時也是，是否會因此造成受處分人救濟障礙或是程序之不便利。

綜上，停止解析之運用，某方面而言可以促進我國刑罰權之執行，另一方面也有將司法權實質擴張之疑問。停止解析在打破我國過去司法執行障礙的同時，也將網路犯罪的審判權界定問題引領到了需要被解決的層次。是以，本文亦將此作為問題之一環，探討域名扣押之國際、國內管轄，該如何規範並解決衝突。

（二）「停止解析」對於非法網站之打擊實際效果有限，該如何建立輔助規範？

停止解析仍有其技術上之侷限，無法阻止境內民眾透過域外連線、IP 位址搜尋等方式連結上網站，能發揮的實際效用似乎相當有限。在規範上該如何建立輔助制度，運用其他手段以補充停止解析之不足，也有討論之必要。並且，對於網路言

[36] 臺灣士林地方法院 110 年度易字第 187 號刑事判決。
[37] 最高法院 72 年台上第 8594 號判決。

doi:10.6342/NTU202302025

論之管制，除了司法機關外，學說上有提及運用行政管制及民間合作等方式者協力[38]，本文亦將討論該等說法之適切性。

第三節 研究目的

由於停止解析於我國刑事偵查程序的運用，尚未建立穩定之見解及程序，實務上對於是否運用扣押之方式進行網域之停止解析也仍有諸多疑惑。並且，國內學說上對於此議題之討論也較少，相關文獻不多。故本文之研究目的即為透過外國法制之比較分析，研究他國如何處理違法網站域名之議題。比較之對象以英美法系國家為主，即美國與澳洲，蓋兩者針對域名議題採取了截然不同之手段。針對美國所採取的域名扣押及沒收制度，本文將整理相關條文及代表性之案例，建立美國實務操作之架構；而澳洲所採者乃創立新興令狀，以授權偵查機關對域名發動停止解析，本文將整理其立法過程與學說討論，思考澳洲與美國模式對我國法制之可參考性，並盡可能的回應前文所提出之問題。

另外，由於世界上大多網域註冊於美國域名受理註冊機構[39]，故對於美國而言管理域名之方式較我國容易且便利。反之，我國在此之背景與美國不同，我國非域名註冊大國也欠缺國際司法互助之機制。就此差異，本文於進行比較法研究時，將對兩國之現實背景亦加以介紹，分析與我國之差異，並對我國現行制度提出比較與建議。

[38] 台灣網路講堂，https://www.twsig.tw/20201120/（最後瀏覽日：03/28/2023）。會議進行中有論者提及透過民間單位協力，或是以行政、民事之手段處理域名爭議。

[39] 「設立於美國加州的非營利法人機構—網際網路號碼與名稱管理機構（Internet Corporation for Assigned Numbers and Names，簡稱 ICANN），擁有主宰全球網際網路域名的權力。由於網際網路於國際上發展的先後，域名在國際上的持有分配即存在有極不平均的問題，而擁有最多域名註冊量者為美國。」蔡志宏，前揭註 17，頁 9-10。

doi:10.6342/NTU202302025

第四節 研究方法

承前述，本論文主要之研究方向為我國法與英美法系國家制度之比較，惟除此之外，仍有其他研究方法，以下說明之。本文將按照章節發展採取不同的研究方法，以期對於研究主題「域名扣押」及「停止解析」可以有更全面的掌握。首先，第一章的研究動機，係透過案例介紹與評析之方式，點出停止解析、域名扣押現階段所面臨的問題。接著透過文獻回顧之方式，建構出本文之問題意識與章節架構。而第二章之技術介紹，也是透過整理現有文獻及技術資料，去蕪存菁後將與停止解析相關之技術資訊，以簡易清楚的方式說明。第三至四章便是以比較法研究為主軸，依序為美國及澳洲法之現況簡介，嘗試梳理各國之實務判決與法制，並援用該國學者之文章及 ICANN 之治理規範與資料，概述各國對於違法網站域名之處理方式，並提出可供我國法參考之處。最終於第五章回歸我國法討論時，藉用既有的法律理論加以統合，回應問題意識，提出本論文之見解，並於第六章加以總結。

第一項 比較法研究

本論文之主要研究方法為比較文獻分析法，並以美國及澳洲法為比較對象。其中關於「域名扣押」制度的討論，主要係以相關法案、重點判決與先例之方式，採取歷史研究之演繹分析，整理其對於無形扣押之制度演變。而對於美國法上的「停止解析」，則主要以近期案例評析以及美國學者意見，點出相關討論。

而相較於採取扣押及沒收之美國，澳洲則非以扣押之脈絡，而是以創新令狀及網路管制之角度，切入非法域名管理之問題。本文亦將參酌思考，國家對於網路管理之界限，以及行政手段所可能引發之爭議，延伸討論非刑事手段於此議題之實踐可能性。

當然，比較法研究不可忽略者為比較法體系之異同，故於各國法制之介紹後，本文將對於美、澳二國與我國背景事實、法制及歷史等差異處，分析並評價得為我國借鑑之處。是以，將切割議題，以確保各該議題的不同面向皆經過充分比較，而非將某國的整個法制度搬運於我國。

doi:10.6342/NTU202302025

第二項 本國文獻回顧

由於停止解析係較新的技術與議題，故我國文獻中所得參考之資料較少。本文主要係以 TWNIC 舉辦之域名研討會資料，以及多位關注域名扣押及網路言論管制之學者文章，釐清思緒並提出問題。以蔡志宏博士所撰寫之〈剝奪犯罪工具之數位轉型—域名之沒收與扣押〉、〈全球域名法制之治理架構研究—以 ICANN 的組織原理及制度運作為中心〉此二篇文章為基礎，建立關於停止解析與域名扣押之問題意識及對於議題的介紹。而較多實務上之討論，則以陳昱奉檢察官所撰寫之〈網路犯罪與資訊安全的未來—從網域名稱扣押談網路治理〉、〈數位時代之犯罪偵查與網路自由及隱私權之保障—從網域名稱（Domain Name）之扣押、沒收談起〉等諸多文章探討網域扣押於我國實務可能遭遇之法學問題。至於前述文獻尚未解決之問題，本論文擬以法學理論，進行研究與推導。

透過閱讀網路資源、TWNIC 官方政策與契約以及研討會資料等方法蒐集域名扣押與停止解析之法律爭議。接著閱讀法學專書、期刊、學位論文，以刑事訴訟法中對於強制處分之審查建立本文的分析架構，並運用該審查架構省思現行法，在現行法下如何進行域名扣押，以及提出現行法有何不足，得到初步的結論並對現行制度提出具體建議。

第五節 本文架構

本文共分為六個章節，第一章是緒論，說明研究動機、問題意識、研究目的、研究方法以及本文架構。第二章為「停止解析」技術之介紹，包括名詞解釋、停止解析之運作方式、其運用於偵查之優勢以及技術限制，藉由本章之簡介使後續對於停止解析所牽涉法律議題之討論可以更加清晰。

第三章以美國法為主軸，依序討論美國實務如何面對「域名得否扣押之爭議」，以及其運用民事對物扣押制度來進行域名扣押之作法。並以美國文獻、學說對現行

doi:10.6342/NTU202302025

制度批評以及美國與我國國際地位之背景差距，來思考其現行制度對於我國法之參考性。

第四章則是以澳洲法為主，依序討論澳洲法制背景之特殊性，以及此特殊性導致該國立法者於面對「非法域名管制爭議」時，採取了與美國截然不同之作法。本文將以澳洲之立法資料、文獻、學說對其制度進行分析，思考其現行制度對於我國法之參考性，以及分析美、澳二國之策略選擇優劣。

第五章便回歸我國法之討論，在此本文欲以基本權審查架構做為本章之結構，依序探討域名扣押、停止解析所限制之基本權，並以我國現行法規範以及 TWNIC 治理規章，討論域名是否適用刑事訴訟法之扣押，是否符合法律保留原則、比例原則（本處之比例原則之操作客體為立法者通案性的將停止解析做為扣押手段）以及正當程序保障。並將正當程序原則拆分為事前、事中及事後討論。事前程序包括強制處分之令狀原則與法官保留（於此探討司法於個案中該如何操作比例原則，以及審查密度之調整）；事中程序則是關於令狀聲請之過程中，權利受干預者（受處分人與網路使用者）是否有程序參與及表達意見之機會；事後程序是關於權利救濟之面向，現行法中是否提供受干預者即時救濟之管道。

最後整理本文對於問題意識之回應，於第六章作出結論。除整理與總結外，將額外提及立法修正建議，盤點現行法之不足。並且提出面對停止解析之技術限制，規範上或制度面之解決之道。

doi:10.6342/NTU202302025

第二章 停止解析技術分析

本文於緒論簡要的說明了何為「域名」、「解析」以及「停止解析」，然而為詳細論述停止解析所遭遇的實務問題，有必要將其技術背景更加深入的介紹，使讀者得以掌握議題，故於本章詳盡說明之。

第一節 名詞解釋

第一項 IP 位址

IP 位址（Internet Protocol Address）代表著網路與主機之位址，而要與外部網路連接上網，每個主機都必須擁有一個獨一無二的 IP 位址以進行通訊，使其他電腦得藉由該 IP 位址尋找裝置並連線。換言之，欲參與網際網路並享受資訊瀏覽、檢索、通訊等服務，IP 位址是不可或缺的[40]。目前大部分的網際網路所使用的是 IPv4 協定[41]。IPv4 的 IP 位址，是利用 32 位元的數字所構成，將 32 位元以每 8 個位元切割[42]，每個部分以「.」作為區隔，共分成 4 個位元組，而每個位元組以一個介於 0 至 255 之間的十進位數字來代表。準此，IPv4 的 IP 位址其存在範圍便落在 0.0.0.0 至 255.255.255.255 之間。舉例而言，168.95.192.1 便是中華電信 DNS 伺服器的 IP 位址[43]。

---

[40] 小泉修（著），羅美華（譯）（2003），《圖解你不可不知的網際網路》，頁 132。

[41] 同上註，頁 153。後續亦發展出 IPv6 之協定，「惟至 2011 以來已面臨 IPv4 發罄危機。即使已有各種措施出現，但僅能作為能夠暫時減緩 IPv4 網路位置之耗盡，仍非釜底抽薪之計，故新一代分配方式即 IPv6 應運而生。IPv6 為 128 個位元組成，除了有更多的命名空間外，在規則上亦更有彈性，傳輸效能、安全性及方便性都勝出 IPv4。」簡菀菱（2017），《從法律經濟學與財產權理論之觀點探討新通用頂級域名分配機制》，頁 5，國立交通大學科技法律研究所博士論文。

[42] 同上註書，頁 169。

[43] 簡國璋（2015），《新世代網路概論》，修訂 1 版，頁 7-13。

doi:10.6342/NTU202302025

然而，主要設計給電腦識別與讀取的 IP 位址，係由一連串的阿拉伯數字所組成，對於人們來說繁雜且不好記憶。因此，後續發展出將 IP 位址代換成較易於識別並記憶的名稱管理方法，也就是網域名稱（Domain Name，以下簡稱域名），其常見的表現形式為 xxx.com.tw。而現今人們在使用網路資源時，多數係運用具有可讀性的域名去連接與存取網路資源[44]。

第二項 網域名稱（域名）

參見圖 2，以臺灣大學官方網站舉例說明之，一般習慣上所稱的網址，正式名稱為「經充分認證的網域名稱」（Fully Qualified Domain Name，簡稱 FQDN）[45]，而網址中段的 www.ntu.edu.tw.[46]，其中的 www 為主機名稱，而 ntu.edu.tw.則是網域名稱。我們可以從該網域名稱中解讀出，該網站與台大相關，蓋.ntu 為台灣大學的英文簡稱，而.edu 表示該網站係屬於教育機構，.tw 則代表了其係註冊於台灣的網域，與台灣有所關聯。相對於 IP 位址為一串數字，域名顯然是對於人們來說較方便理解、容易聯想的表現形式。然而，相反的，域名並非電腦主機進行連線時所得溝通的方式，電腦在進行通訊時，必須使用數字形式的 IP 位址才行。為了解決這個問題，便有了網域名稱系統（Domain Name System，簡稱 DNS）的出現[47]，該系統提供了 IP 位址與域名之間的轉換服務。綜上，不妨說網域名稱與 DNS 的出現，旨在提供一種簡單的分類法，以更方便、更有效率的方式指引主機 IP 位址和其他資訊[48]。

---

[44] 同上註，頁 10-1。
[45] 同上註，頁 10-3。
[46] 在頂級網域的上層是唯一且未命名的根，以「.」表示，以上述國立台灣大學之域名為例，其實 FQDN 的正式用法應該要將代表根的「.」加上，成為「www.nctu.edu.tw.」，但習慣上都會忽略，由系統自動補上協助電腦判斷。同上註，頁 11-3。
[47] 小泉修，前揭註 40，頁 132。
[48] NATIONAL RESEARCH COUNCIL, ET AL., SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION 45 (2005).

doi:10.6342/NTU202302025

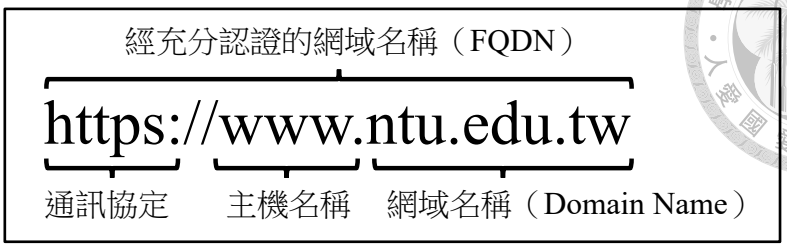

圖 2 網址拆解

資料來源：小泉修（著），羅美華（譯）（2003），《圖解你不可不知的網際網路》，頁 71。

在此需特別注意的是，DNS 並非以扁平化的方式將人類可理解的域名與電腦可識別的 IP 位址為一對一對應，而是以「階層化」的方式為之。若要類比，扁平化的對應就如同電話簿般，將 IP 位址與域名一一列上，在查詢電話號碼時只能夠依序查找電話簿上的所有名稱，直到找到完全對應的名稱為止。而此方法有其缺陷，每當新增一組號碼，為了維持這本電話簿的正確性，便必須麻煩的通知所有擁有電話簿副本之人，使其同步新增號碼。若電話簿上的人數寥寥無幾，此種紀錄方式尚不致產生問題。然而，現今所要面對的是無邊無際的網路世界，其牽涉範圍之廣大，此種電話簿式的對應模式將大幅提高維護資料庫正確性的行政成本，實際上也欠缺運作可能性。從而，面對「名稱」與「IP 位址」對應的問題，DNS 改以階層化之方式將名稱與 IP 位址分配，將管理電話簿的權限分散到網路上數如繁星的主機上，採取去中心化的分配方式，有別於過去的統一管理模式[49]。易言之，DNS 所採取的方式類似於中英字典。當我們查閱字典，尋找英文單字所代表之中文意義時，係將單字中的每個字母，按閱讀順序依次查詢，每找到一個字母，便在該字母之階層中尋找下一個字母，反覆為之，層次化的找到完整的單字，以及其所對應的中文意義[50]。而在 DNS 中，便是以此種階層式的結構管理並對網域命名。

[49] 簡菀菱，前揭註 41 碩士論文，頁 6。

[50] 舉例來說，欲尋找 Ant 此單字，翻閱中英字典時，會先翻閱到 A 的章節，在此尋找 An，再接續著在以 An 開頭的單字中找到 Ant。

doi:10.6342/NTU202302025

對應於階層式的管理，網域名稱的命名便是以「.」作為分段，由右向左區分層級為頂級域名、次級域名[51]。每一個層級的網域中，都有至少一台的名稱伺服器，負責管理該網域之域名。當要搜尋某一完整域名時，便是以此分層方式，由頂級域名開始，在相對應的網域層級中，詢問負責管理該層網域的伺服器，關於下一層級網域的名稱伺服器位址，依此順序從頂級到次級網域，層層搜尋與對應，直到找到完整域名以及其相對的 IP 位址，並將結果回傳給使用者之主機。上述尋找網域 IP 位址之過程即係所謂的「解析」。

第三項 網域名稱系統（DNS）與解析

承上言，域名之所以能夠在網路上產生定址之功能，是透過 DNS 將域名與相對應的 IP 位址經過一套技術設定予以解析轉換而成。DNS 是由擁有網域等資訊的**伺服器**[52]程式，以及可依使用者需求來要求伺服器程式解決問題，名為**名稱解析器**（Name Resolver）的系統常式（System Routine）所構成[53]。其中，可以將 DNS 伺服器區分為用戶端（Client）與伺服器（Server），由伺服器提供 IP 位址轉換、解析之服務，供用戶端使用。用戶端則是負責接受使用者之查詢，並將其需求轉知伺服器。在 DNS 伺服器中，便是由前揭名稱解析器擔任用戶端，負責接受使用者各類搜尋引擎、應用程式的呼叫，並將查詢要求提供給擔任搜尋工作的名稱伺服器，由名稱伺服器代替使用者，向各網域的主機遞迴查詢。

因此使用者在用戶端輸入網域名稱後，名稱解析器便會向伺服器要求提供所對應的 IP 位址，此稱為正向名稱查詢。而伺服器提供 IP 位址並回覆給用戶端之動作，則稱為正向名稱解析；反之，若是輸入 IP 位址要求對應域名，此為反向名稱查詢。伺服器解析後將域名提供予用戶，則稱為反向名稱解析[54]。

---

[51] 以圖 1 說明之，頂級域名為.tw，第二層域名為.edu，第三層域名為.ntu。後二者皆屬次級域名。

[52] 「伺服器（Server）一般是指提供網路服務的電腦，用來處理某些特殊的作業，舉例來說資料庫的檢索是負擔很重的作業，若交由伺服器來處理，就可以減少用戶端電腦的負荷。用戶端（Client）是指連結至伺服器，接受伺服器服務的電腦。」小泉修，前揭註 40，頁 19。

[53] 同上註，頁 132-133。

[54] 簡國璋，前揭註 43，頁 10-4。

doi:10.6342/NTU202302025

每一部電腦皆保有一份記錄相關的 IP 位址與域名對應的主機檔案(Host File)，當有需要查詢時，若係主機檔案或快取資料中已有記錄者，則不需經過 DNS 伺服器即得馬上透過主機檔案取得資料，可以減少查詢之時間。然若所查詢者於主機內沒有紀錄，便須經由 DNS 查詢。DNS 查詢的運作過程中，DNS 中的名稱伺服器對其他網域伺服器的查詢係採取「遞迴查詢」方式。亦即，當用戶端向本地伺服器要求查詢時，若本地伺服器有查詢到資料，便立即回覆用戶所對應的資料；若否，則繼續向外部伺服器求救，若外部伺服器有查到資料便會回覆給用戶；若皆搜尋不著，便會通知用戶無法解析（見圖 3 輔助說明）[55]，採用一種反覆、遞迴的詢問模式。

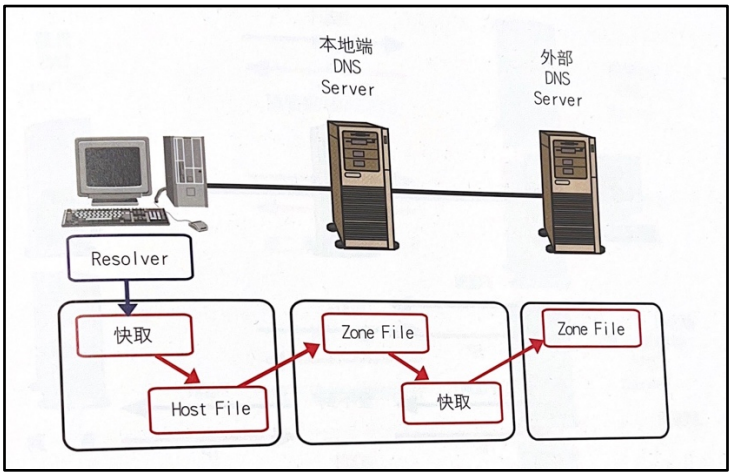

圖 3 DNS 的查詢順序

資料來源：簡國璋（2015），《新世代網路概論》，修訂 1 版，頁 10-13。

綜上所述，解析係按照層級化、遞迴式之方式搜尋資訊，可謂 DNS 係一階層式結構（Hierarchy）遞迴詢問之解析伺服器[56]。而欲以圖像化之方式理解之，得將 DNS 想像成倒立的樹狀分枝(見圖 4)。圖像最上方如同樹根的部分為根網域(Root Domain)，所有按規定正式註冊過的 DNS 名稱，都屬於根網域之管理範圍內。若在某一個網域（分支）中無法解析，便會一直向上尋求幫助，最終將到達根網域，再由根網域前往其他分支向下尋找。

[55] 同上註，頁 10-12, 10-13。
[56] 蔡志宏，前揭註 17，頁 42。

doi:10.6342/NTU202302025

根網域之下的第一層級網域，則稱為頂層網域（在此層級相對應的域名則稱為頂級域名）。頂級域名之取名有兩種類型，一種是以國家為區分[57]，另一種則是以單位性質命名[58]，而台灣係採取前者，即域名之最右端為國名之代碼「.tw」。下文以台灣所採取之國碼頂層網域之命名模式（ccTLD）接續說明之[59]，頂級域名之下一層級為第二層網域，第二層級之域名則係標示著單位之性質，如：教育機構為「.edu」、一般公司行號的營利機構為「.com」。再由此分支延伸，下一個層級為第三層網域，第三層網域之域名係單位名稱之簡稱、代號，如：台灣大學係「.ntu」、清華大學則是「.nthu」。從此模式，透過不同層級網域名稱的排列組合，組成一獨一無二的完整域名。

而完整域名中的每一個點，則形成每一層的分支，如前述亦是透過「.」將域名區分層級。當使用者於用戶端進行正向名稱查詢時，伺服器解析的過程便是從頂部樹根（頂級域名）向下搜尋，一一向下對應每一個層級的分支（依照順序，第二層對應二級域名、第三層對應三級域名……），直至找到完全相符合之域名為止[60]。

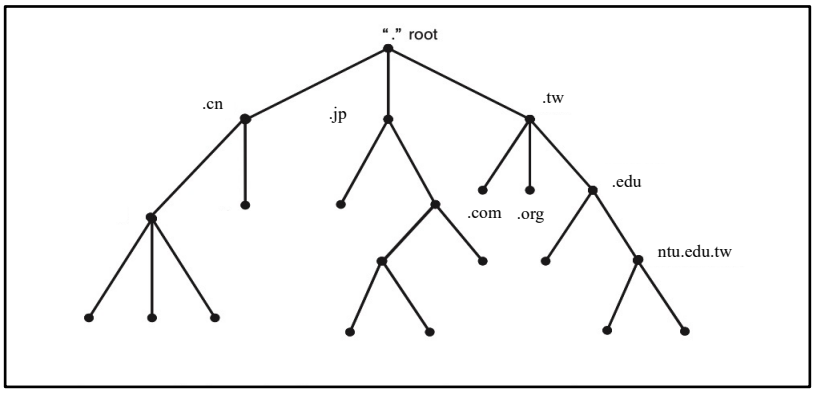

圖 4 國碼頂層網域之命名模式

資料來源：簡國璋（2015），《新世代網路概論》，修訂 1 版，頁 10-6, 10-7。

DNS 尋找的路徑，大致可以分為六個步驟（惟若主機檔案內有記錄資料，或是快取內有紀錄，則可以直接回傳主機資訊，得省略以下部分步驟）。（一）使用

[57] 稱為國碼頂層網域（Country Code Top Level Domain, ccTLD），如：台灣為「.tw」、日本為「.jp」。
[58] 稱為通用頂層網域（Generic Top Level Domain, gTLD），此多為美國所使用，如：「.com」是指一般公司行號的營利機構、「.edu」則是指教育單位。
[59] 若係 gTLD 之命名模式，則頂級域名係指涉單位之性質，第二層域名則是單位名稱。與 ccTLD 模式有一層之差別。為免於過度繁雜之說明，本文逕以台灣所採之 ccTLD 模式舉例說明。
[60] NATIONAL RESEARCH COUNCIL, ET AL., *supra* note 48, at 43.

doi:10.6342/NTU202302025

者在網頁瀏覽器中鍵入域名，並傳輸到網際網路中，DNS 伺服器之用戶端即名稱解析器，接收該查詢並將查詢要求轉知給名稱伺服器。（二）接著，名稱伺服器向 DNS 根伺服器請求查詢該網域頂級域名之伺服器位址。（三）根伺服器回傳相關頂級網域伺服器之資訊後，名稱伺服器再接著向頂級網域之伺服器發出請求，詢問次級網域伺服器之位址。（四）重複此詢問過程，最終查詢到實際上保留並負責處理該網域資源記錄的**權威伺服器**，並由其將該完整域名所對應之 IP 位址回傳給名稱伺服器。（五）最後，名稱伺服器藉由所查知之 IP 位址，將使用者之查詢傳送到該網域之伺服器。（六）名稱伺服器使用該網域的 IP 位址回應網頁瀏覽器，使用者之主機應而與該網站建立起連線，得以瀏覽網頁[61]。得參見圖 5 之說明。

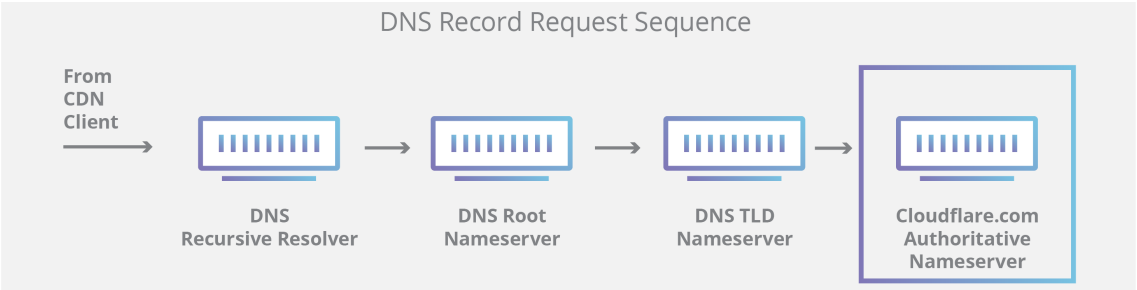

圖 5 DNS 查詢流程

資料來源：CLOUD FLARE，https://www.cloudflare.com/zh-tw/learning/dns/what-is-dns/（最後瀏覽日：07/10/2022）。

舉一實例說明以總結解析之過程。當使用者欲造訪台大法學院之網站時（網址為：http://www.law.ntu.edu.tw），其查詢之流程，是由使用者之主機先向伺服器內之主機檔案與快取資料進行查詢；若未能查到，則再向本地端伺服器查詢；再查不到，則向外部伺服器尋求幫助。而進行查詢時，係運用 DNS 之解析技術，由根伺服器詢問管理「.tw」域名伺服器之 IP 位址，根據所得到的答案，前往訪問「.tw」的域名伺服器，並接著詢問「.edu.tw」域名伺服器其所在 IP 位址。依此方式，由右向左的逐一確定域名「http://www.law.ntu.edu.tw」之所在 IP 位址，而加以造訪。

[61] CLOUD FLARE，https://www.cloudflare.com/zh-tw/learning/dns/what-is-dns/（最後瀏覽日：07/10/2022）。

doi:10.6342/NTU202302025

可以發現，解析的過程，需要許多伺服器分工協助，若該等伺服器之資料庫被改寫，而對某一特定域名提供修改過的解析資訊，則可以達到使使用者進行正向名稱查詢時，無法得知網站正確 IP 位址之效果，致其無法順利造訪該網站。此即下文欲介紹之「停止解析」技術概念。

第四項 停止解析（DNS RPZ）

一、技術內涵

DNS RPZ (Domain Name System Response Policy Zone)，即本文所欲探討的停止解析，顧名思義，便是使上述解析網域功能停止服務之技術。停止解析「是域名系統服務器上的一種自定義策略的機制，讓遞歸解析器返回可以修改解析的結果。通過修改結果，以阻止對相應主機的訪問，達到使民眾無法再透過平常上網的方式拜訪該惡意網站之效果。」[62]

簡單來說，DNS RPZ 是域名系統服務器提供的功能之一。由於，DNS 系統近年常遭遇惡性攻擊，為了避免使用者們不慎造訪不法網站，網域管理者得利用 DNS RPZ 之技術，針對已知的惡意網站域名，修正其解析之結果。例如：將使用者導向執法單位之網站 IP 位址，或是單純拒絕解析該網域。

由於 DNS 系統之資料庫是採取分散式管理之模式，因此並不存在一伺服器記錄著全世界之域名。準此，若想要修改某一特定網域解析之結果，發布一黑名單給全世界的伺服器，於技術面及現實執行面皆屬不可能。故 DNS RPZ 採取另一作法，其係將黑名單發佈於管理系爭網域之部分伺服器，而只要運用該存有黑名單之伺服器查詢網域，伺服器將會比對黑名單，若發現域名為惡意網站，便不會提供解析之服務，使用者即無法順利造訪網站。

然而，透過上述的說明可以發現，同一份黑名單要整合到所有的伺服器是不可能的事，因此使用者若是使用其他沒有該份黑名單的伺服器，仍然可以解析並連結上該網站，而這也是停止解析之技術限制。為了使停止解析在我國可以達到一定程

[62] TWNIC，https://rpz.twnic.tw（最後瀏覽日：07/02/2022）。

doi:10.6342/NTU202302025

度之效果，須盡可能地將同一份黑名單整合到提供我國大部分網路使用者服務的解析伺服器上，這也是 TWNIC 在我國停止解析執行中扮演重要角色之原因。

二、TWNIC

財團法人台灣網路資訊中心（Taiwan Network Information Center，又稱 TWNIC），是目前我國統籌網域名稱註冊及 IP 位址發放、超然中立之非營利性組織，為域名之**註冊管理機構**，提供國內完整之域名註冊及 IP 位址分配服務，同時也負責台灣國家網域名稱「.tw」的註冊與營運[63]。TWNIC 亦有將部分之域名註冊業務委託於其他法人組織，該等組織則被稱為域名之**受理註冊機構**，其基於契約有配合 TWNIC 管理之義務[64]。

按電信管理法第 71 條第 1 項，域名之註冊管理服務應由法人組織管理。故在交通部電信總局及中華民國電腦學會的共同捐助下，TWNIC 於 1999 年 12 月 29 日完成財團法人設立登記事宜，「財團法人台灣網路資訊中心」正式成立，主管機關乃交通部。復於 2017 年 12 月 22 日變更**主管機關為國家通訊傳播委員會**[65]（以下簡稱通傳會）。其捐助章程第 2 條揭示了 TWNIC 之服務宗旨[66]，包括：協助推展全國各界網際網路應用之普及，以及協調資訊服務之整合、交換，並支援政府辦理各項事務。

是以，TWNIC 實際上掌握了我國的網域管理，其與國內網路關鍵基礎設施提供者、網路服務供應商（Internet Service Provider，簡稱 ISP）等提供我國網路使用

---

63 TWNIC，https://www.twnic.tw/about.php（最後瀏覽日：07/05/2022）。

64 關於「註冊管理機構」與「受理註冊機構」之關係說明：「註冊管理機構（registry）負責域名之管理。而當註冊者（registrant）欲使用域名時，則需向註冊管理機構轄下之受理註冊機構（registrar）申購註冊服務，再由註冊管理機構依照 ICANN 之規定，予以分配域名。簡而言之，註冊管理機構就如同『批發商』，僅負責『批發』其所掌管之網域名稱，不直接面對消費者；而受理註冊機構就如同『零售商』，受理網域名稱使用者之申請，並提供註冊服務。」陳昱奉（2014），〈數位時代之犯罪偵查與網路自由及隱私權之保障—從網域名稱（Domain Name）之扣押、沒收談起〉，臺灣嘉義地方法院檢察署 102 年度自行研究報告，頁 12。

65 TWNIC，參前揭註 63。另參電信管理法第 2 條：「本法所稱主管機關為國家通訊傳播委員會」。

66 財團法人台灣網路資訊中心捐助章程第 2 條：「本中心為國家級網路資訊中心，其服務宗旨如下：一、非以營利為目的，以超然中立及互助共享網路資源之精神，提供註冊資訊、目錄與資料庫、推廣等服務。二、促進、協調全國與國際網際網路（Internet）組織間交流與合作，並爭取國際網路資源及國際合作之機會。三、協助推展全國各界網際網路應用之普及，以及協調資訊服務之整合、交換。四、協助或支援政府辦理各項事務，並推動網路資訊相關公益事務。」

doi:10.6342/NTU202302025

者上網服務之電信業者，共同合作建構全台 DNS RPZ 服務架構[67]。藉此國家型 DNS RPZ 架構，DNS RPZ 所限制接取之網域名稱不再限於「.tw」國家頂級域名，而得作為我國境內或境外惡意網域名稱的第一線防護措施。

三、國家型 DNS RPZ 之運作

DNS RPZ 採取主從式結構，當不當網域名稱或 IP 位址被寫入主節點 DNS RPZ，所有參與 DNS RPZ 的次級節點會同時限制接取此不當網域名稱或 IP 位址[68]（見圖 6）。

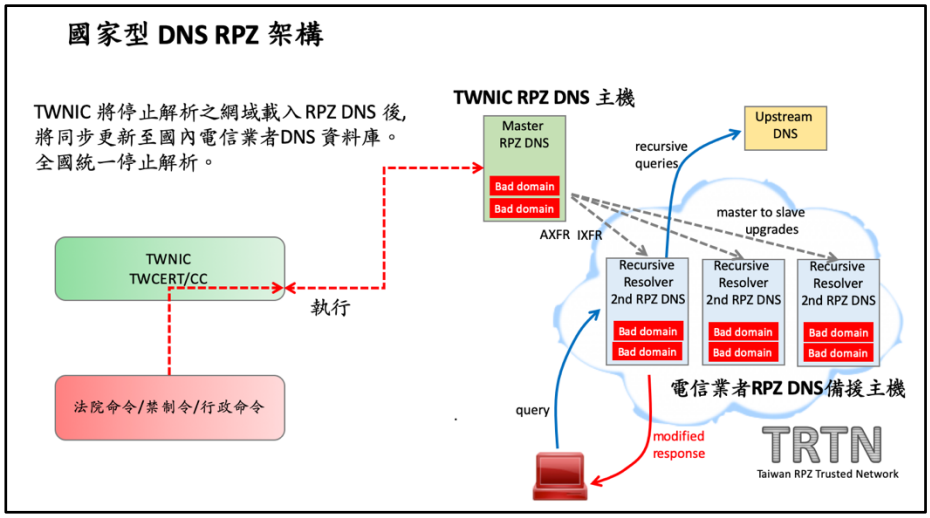

圖 6 國家型 DNS RPZ 架構

資料來源：黃勝雄（09/23/2020），〈DNS RPZ 摘要說明〉，TWNIC，https://blog.twnic.tw/2020/09/23/15311/（最後瀏覽日：03/28/2023）。

每當 TWNIC 將欲停止解析之網域名稱載入 DNS RPZ 後，將同步更新至國內 ISP 業者的 DNS 資料庫，達到全國停止解析之效果，此乃國家型 DNS RPZ 之運作方式[69]。

用前面黑名單之比喻來說，便是 TWNIC 擁有將黑名單傳送給我國 ISP 業者伺服器之能力。另外，ISP 業者亦得作為停止解析之主體，惟基於前述 TWNIC 的 DNS

---

[67] ISP 業者參與此架構並非強制性，故其配合停止解析係屬自願配合，而無國家強制之課予私法人義務之疑慮。

[68] 黃勝雄（09/23/2020），〈DNS RPZ 摘要說明〉，TWNIC，https://blog.twnic.tw/2020/09/23/15311/（最後瀏覽日：03/28/2023）。

[69] 同上註，圖 1。

doi:10.6342/NTU202302025

RPZ 政策，自動參與該政策之業者，並不會自行判斷網域違法，大多係通過 TWNIC 的通知而配合執行停止解析[70]。簡言之，透過國家型 DNS RPZ 之運作，只要是在系爭黑名單上的域名，使用我國業者提供之伺服器上網，便無法正確解析造訪網站。

了解停止解析之技術後，接著可以思考其實際執行之效果、優勢與技術限制。畢竟停止解析對於人民基本權之干預性質強烈已如前述，是否真的有運用此科技於偵查之必要，以及如何補足其技術限制，使得網域管理更加全面，有討論之必要。

第二節 技術優勢

第一項 執行效果佳

實務、學說上之討論，普遍肯認停止解析之實效性。停止解析在執行時可以有效地針對參與非法行為的網路資源。且執行上只需要政府與域名管理機構、受理註冊機構之間的合作，便可以完成扣押。此外，對於境外域名或行為人行蹤不明時，停止解析可以直接採取司法行動，而無需冗長的法律程序[71]。

第二項 與其他技術比較

除了 DNS RPZ 外，技術上存在其他手段可以達到限制網站瀏覽之目的。故於本項介紹其他可能之手段，並將其等與停止解析比較。

一、IP 位址過濾（IP Filtering）

IP 位址是電腦連線上網之過程中所必須存在、標示主機位址的一串數字。在討論停止解析時，亦有論者提及，可以設計 IP 位址之黑名單，透過封鎖黑名單上的 IP 位址，讓主機無法連線至特定 IP 位址。這種過濾 IP 位址之方式，亦得達到封鎖網域、阻擋使用者造訪非法網站之效果。

---

[70] 戴豪君、余啟民主持（2021），〈網域名稱涉有違反相關法律之實例研究及處置建議委託研究期末報告〉，國家通訊傳播委員會，頁 176。

[71] Aniket Kesari, Chris Hoofnagle & Damon McCoy, *Deterring Cybercrime: Focus on Intermediaries*, 32 Berkeley Tech. L. J. 1093, 1121 (2017).

doi:10.6342/NTU202302025

承接前述上網之過程，使用者於伺服器輸入域名後，網路服務提供之業者將協助解析，將域名轉換為 IP 位址。而知悉了所要造訪網站之地址，使用者之主機便可以透過網路連線服務，前往該 IP 位址，向該位址之主機發出連線、存取之訊息。在上網之後階段，將連線要求從使用者之主機傳遞至指定 IP 位址之過程，需要透過網路服務業者所提供之**路由器**進行。路由器，主要功能是連結不同的主機、裝置，其運作模式係讀取訊息、決定資料之傳輸順序、尋找最佳之傳遞路徑，將資料傳輸至指定之 IP 位址。

是以，只要在路由器上設定封鎖特定 IP 位址，於使用者透過我國業者提供之路由器上網，便沒有辦法順利抵達該主機之位址，即無法造訪系爭非法網站。此作法與 DNS RPZ 設置域名黑名單之作法有異曲同工之妙，但何以目前實務傾向使用 DNS RPZ 而非 IP 位址呢？

其主要原因係共享 IP 位址乃十分普遍之現象[72]，若是針對某一 IP 位址封鎖，則共享此 IP 位址之其他合法網域也將一同被封鎖，而有過度封鎖之疑慮。雖然過濾域名時亦有可能會同時將該網域之子域，以及網域中其他合法之內容一同封鎖，某種程度上也有過度封鎖之問題。惟此不如封鎖 IP 位址時明顯，故兩相比較之下，過濾 IP 位址無法精確執行之程度大於 DNS RPZ，較不可採。

尤其在扣押裁定之程序中，一域名下大約有多少之子域，係法官可審查與衡量者。縱使境外之域名註冊管理機構無法配合提供資訊，亦不難推論，針對越高層級之域名扣押，勢必會影響較多之網域，此乃程序中法官得審酌者。然而，一 IP 位址究竟與多少人共享，於形式上無法認定或推測，僅能依賴註冊該 IP 位址之人協助提供[73]。是以，過濾 IP 位址所產生的過度封鎖乃事前不可預期，難以期待法官正確衡量扣押所帶來的負面影響。

---

[72] Benjamin Edelman, *Web Sites Sharing IP Addresses: Prevalence and Significance*, https://cyber.harvard.edu/archived_content/people/edelman/ip-sharing/ (last visited Sept. 6, 2022). “Research by plaintiffs’ expert Michael Clark empirically confirms the prevalence of shared IP addresses. … at least fifty percent of domains shared an IP address with at least fifty other domains.” Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 618 (2004).

[73] *Id.* “One cannot determine with any certainty using technical means whether a given web site shares its IP address with another web site.”

doi:10.6342/NTU202302025

再者，過濾 IP 位址之效果反而較 DNS RPZ 不彰，蓋對於網站架設者，面對此種方式之解套手段，便是申請新的 IP 位址，其便利迅速之程度與註冊域名相同。而多數使用者上網所依賴使用的是域名而非 IP 位址，在域名沒有變動而 IP 位址更改的情況下。反而對於使用者而言，上網的過程不會遇到阻礙，仍能按照記憶中的域名去抵達新網站，難以達到減少網站流量之效果。

二、URL 過濾

URL（Uniform Resource Locator，中文稱為：統一資源定位符），其意義在於指定網際網路上資源的位置。它的表現形式與域名相似，都存在於常見的網址列中。舉例來說，在台大法學院官網院訊之頁面，它的網址是：「http://www.law.ntu.edu.tw/index.php/院訊」。與域名不同的是，URL 不僅可以指稱特定網站，更可以指向網站中的特定頁面、子頁。是以，如果過濾特定 URL，則可以控制只針對非法頁面停止解析，而不妨礙同一網站中其他合法內容。換言之，URL 過濾之執行精準度優於 DNS 過濾。

執行精準度較高，便可以降低過度封鎖所引發比例原則之疑慮。那麼，何以目前討論上傾向使用 DNS RPZ 而非 URL 過濾呢？理由在於使用 URL 過濾之技術成本過高[74]，實際上難以期待域名之受理註冊機構皆能夠花費高成本建制 URL 過濾的基礎設施。且不僅是設施、技術之本身成本高昂，如偵查機關欲使用 URL 過濾非法網域，則需在扣押聲請時鉅細靡遺的描述該特定頁面之位址。倘若系爭網站中有無數子頁皆涉及不法，但又參雜著合法頁面，此時光是描述扣押標的便必須花費無數時間與精力；而對於網站架設者而言，將內容搬運到同一網域的不同的頁面，更是簡單又輕鬆的舉動，過程中甚至不用重新註冊網域。是以，URL 過濾技術本身，以及作為扣押手段時，皆屬耗費過劇成本之方案，實際上難以運作與執行。

[74] *Id*, at 628-31. 另有論者認為，台灣之網路服務業者現階段沒有辦法實施 URL 過濾之技術。朱哲群，〈淺談網域扣押的司法困境〉，《法務通訊》no. 3097，第 5 版。

doi:10.6342/NTU202302025

第三項 小結

藉由上述 DNS RPZ 之說明，可以知悉 DNS RPZ 係以一種對於特定域名過濾（DNS 過濾）之方式，排除使用者對於該網域之造訪。其執行精準度大於 IP 位址過濾，然而沒辦法僅針對網域之部分頁面或內容停止解析，且層級較高的域名，旗下又有許多次級域名，亦有過度封鎖之可能。然而，可以做到精準執行之 URL 過濾，又因時間、金錢成本之現實考量，於現階段無法如 DNS RPZ 般創建國家型的設施。是以，要在短時間關閉非法網站，且該網站之係境外域名或網站架設者行蹤不明時，現時最可行的網站封鎖技術為停止解析，即本文探討之 DNS RPZ。

第三節 技術限制

雖然停止解析有成本低、迅速有效減低損失之優點，惟如前所述，停止解析所能達到限制民眾前往網站之效果與註銷網域之間有所差異，此落差係源於停止解析之技術限制。蓋停止解析並未能真正地將非法網站關閉，僅是技術上使利用我國伺服器上網的民眾，在上網的過程中無法解析該網站，而該網站事實上仍存在。以下提出幾項能夠規避停止解析之方式，並期許能夠發展出其他制度，與停止解析相互配合，補足法網漏洞。

第一項 直接輸入 IP 位址

既然停止解析之作用係變更電腦解析之過程，那麼若是使用者不使用解析之服務，而逕行輸入網站的 IP 位址，仍然能夠造訪該網站。是以，直接輸入 IP 位址便成為規避停止解析之方式之一。

惟此種手段之可實行性並不高，因此對於停止解析之應用尚難謂構成嚴重阻礙。蓋之所以發展出 DNS 系統，便是對於人們而言 IP 位址難以記憶。因此，可以想像，採取記錄某一特定網站之 IP 位址而得以繞過停止解析造成之障礙，此一情況應屬少數。

doi:10.6342/NTU202302025

第二項 透過快取資料上網

類似於上述直接輸入 IP 位址以繞過 DNS 伺服器之方式，透過主機所記錄之快取[75]資料來造訪網站亦屬可行之方法。在前揭 DNS 查詢順序之介紹，提及為了節省查詢時間，在透過 DNS 伺服器解析之前，若是系爭域名已被記錄於快取伺服器內，則使用者可以逕行透過該紀錄前往網站，而毋需經過 DNS 伺服器解析。亦即，縱使該網域被施以 DNS RPZ，使用者仍得透過主機內之快取而知悉該網域之位址，而不會被停止解析所影響。準此，透過快取資料上網亦屬一停止解析所無法限制之手段。

惟快取資料之特徵，即在於其僅負責短時間儲存紀錄，原則上受有儲存時間之限制，時間一到即會自動刪除並更新。縱使得以手動之方式儲存而免於自動刪除，只要電腦關機該紀錄仍會消失。是以，基於快取資料儲存時間之有限性，亦難認為此一手法對於停止解析之強制效果有削弱之嫌。遑論，於一般使用者而言，能夠手動儲存快取紀錄亦屬少見。

第三項 透過外國伺服器連線

另一對於使用者而言，可以規避停止解析而連結系爭網站之方式，便是透過未與 TWNIC 合作之 ISP 業者所提供之解析伺服器上網。只要該解析之過程，未經過我國國家型 DNS RPZ 架構，即未通過那些擁有我國域名黑名單之伺服器，那麼該網域則仍可以被正常解析，因此使用者仍能前往造訪系爭網站。

原則上我國網路使用者於上網時，其協助解析之預設伺服器係由我國之電信業者、ISP 所提供。換言之，在未變更解析伺服器之設定下，理論上我國境內之用戶皆會被停止解析所影響，而無法造訪系爭網站。然而，變更解析伺服器並不須花

[75] 快取伺服器不具有保存 DNS 資料庫之功能，僅提供輔助查詢之功能，以分擔解析伺服器的工作量。快取伺服器會記錄使用者過去查詢以及解析之流程，於未來使用者再度查詢同一網域時，便可以直接透過快取資料造訪網域。惟一但重新開幾，快取之所有資料便會被清除。簡國璋，前揭註 43，頁 10-11。

doi:10.6342/NTU202302025

費太大的力氣，只需要更改主機之 DNS 設定，將之設定為**外國伺服器**即可以不經過我國的 DNS RPZ 架構而完成解析。

更改主機的 DNS 設定，對於一般非資訊學科背景之民眾，或許並非得輕易思及並使用之手段。然而，大部人都耳聞甚至使用過的**虛擬私人網路（Virtual Private Network，以下簡稱 VPN）或代理伺服器（Proxy）**，便得採取相似之手法以繞過我國 DNS RPZ 架構，蓋 VPN 的虛擬主機位置係連線外國之伺服器解析、上網，代理伺服器亦如是。

是以，此一方法對於使用者而言，技術門檻不高，也有高度的實現可能性。若網路使用者欲透過此手法規避停止解析，確實有可能使停止解析之強制效果大為減損，此乃停止解析之技術限制。但根據一些威權國家使用規避軟體的經驗數據，其強烈的表明這種網路長城式的管制措施，即便存在 VPN 等規避軟體，在阻礙使用者造訪網站之效果仍是顯著的。蓋使用者已經習慣於「無摩擦」的上網環境，無法容忍獲取違法材料所需的額外步驟或較慢的速度。而停止解析會增加造訪網站的成本，是以，對於大多數的使用者來說仍是有效的防止手段[76]。

並且，隨著警察機關在停止解析之網域公告違法原因以及「此網域已遭停止解析之訊息」，使民眾得以知悉網域涉及非法事項，相信此舉能夠避免「誤認出現技術障礙而對網域內容違法不知情」之民眾前往系爭網站，某種程度上也具有嚇阻以及降低損害之功能。另觀刑事訴訟之強制處分，本就不在於完全地阻止犯罪、損害之發生，而是在於製造犯罪之阻礙，使犯罪變得困難，降低損害之發生。因此本文以為不得僅以停止解析得被 VPN 所破解，即反推此技術無成為我國強制處分手段之必要，只要其於程度上可以達到損害防止、減少之效果，便有將其作為我國偵查機關手段之意義。

上述三種方式是對於網路使用者而言可以採行之規避手段，下文將介紹對於網站架設者而言，其可能採行之作法。

[76] Derek E. Bambauer, *supra* note16, at 909.

doi:10.6342/NTU202302025

第四項 重新申請域名

對於網站架設者而言，在原有網域被偵查機關停止解析時，想要立刻使網站重新為人們所能造訪，簡單的方式便是重新申請註冊域名，透過一新的域名連接網站，而使用者們也可以透過該新申請的域名解析並連線該網頁主機。尤其申請域名並非難事，最快在一日之內[77]便能夠申請完成並開通使用。當申請域名之速度，高於偵查機關聲請令狀並且執行停止解析之流程所費時間，停止解析至多僅可達到暫時中止的效果，所能發揮之嚇阻效用似乎極為有限。

然而，本文以為，觀察 DNS 之發展，網域名稱相較於 IP 位址有「方便記憶」、「關聯性」、「可讀性」之特色。是以，對於網站架設者而言，雖然可以輕易地更換域名，但新的域名相較於原有域名，其知名度較低，也與原本網站造訪者之記憶有所落差，有阻擋部分使用者之效果。而對於關聯性而言，新註冊之域名是否如同原有域名，擁有與網站內容之高關聯性，而得以導引使用者前往瀏覽，不無疑問。在可讀性方面亦同，新註冊之域名其名稱是否可以達成與原有域名具有相同的可讀性與意義，於申請上也有其困難度。

準此，本文亦認為不得僅以網站架設者得變更域名即否認停止解析之實際效用。且若是從源頭控管，使域名註冊受理機關與偵查機關合作，針對相似於遭停止解析之域名，暫停該等域名之註冊，便可以某程度上的限制域名關聯性之優勢，達到嚇阻效果。因此，若於註冊階段引入**管制**，或許能夠彌補停止解析之技術限制。

第五項 域名所有權移轉

停止解析尚有一技術限制，即停止解析無法限制域名所有權之移轉。蓋停止解析只是在網路使用者上網連線時發動阻礙，但沒有辦法阻止域名註冊人使用域名，決定域名的指向、更新網站的內容等。因此，即便停止解析域名，域名仍有被移轉之風險，可能造成沒收之困難。

---

[77]「申請網域名稱所需花費之時間，只要依照申請流程儘速進行 E-mail 回覆確認及完成繳費程序，最快可於當日內完成。」TWNIC，https://www.twnic.tw/dnservice_reg isterqa.php（最後瀏覽日：07/11/2022）。

doi:10.6342/NTU202302025

惟本文以為透過核發扣押命令給 TWNIC 及域名受理註冊機構，對系爭域名產生**禁止處分**之效果，即能補足此缺漏。首先說明，觀念上存在「域名移轉」與「變更域名所有權人」兩種概念，前者係將域名移轉至不同的域名註冊單位；後者係向原本的註冊單位請求變更域名註冊人，由新的註冊人使用原本的域名。後者才是所謂域名所有權之移轉，而只要該註冊單位不同意註冊人之變更（即禁止處分該域名），域名之所有權便不會移轉。

附帶而論，或有疑惑，若是網站架設者更換網站之 IP 位址，此舉是否得規避停止解析呢？答案是否定的，理由在於更換了網站之 IP 位址，若其仍然使用原本的網域名稱，那麼使用者輸入該被停止解析之域名，仍然無法到達網站的新位址，因為系爭域名仍在黑名單上，不會因為更改 IP 位址而有所改變。是以，IP 之更改並非停止解析之技術限制。

第四節 輔助制度—補足技術限制

整理上一小節之結論，停止解析之技術限制有兩個方面，對於網路服務之使用者而言，便是透過境外之伺服器解析域名；對於網站架設者而言，則可以重新申請新的域名。

欲補足前者之缺口，所得依靠者為「使用者自律」以及「關閉網站」。蓋是否使用其他手段解析上網，此非政府所得控制，檢警機關所能做的僅有將系爭域名導引至警告頁面，告知、提醒使用者該網域內容涉及不法，若執意前往網頁亦有觸法之可能。除警告外，於政策上也可以多加宣傳，鼓勵使用者自律。另外，對於註冊於境內之域名，本就可以依註銷域名、停止服務等方式使該域名本身無法再被使用；對於境外之域名，除停止解析外，仍得同步向境外註冊管理機構或司法單位為協助執法之請求。是以，停止解析可以搭配同步進行清除該不法網站之程序。

而對於重新申請域名簡便之問題，本文以為可以於註冊域名之程序上添加限制。蓋域名除了成為解析之工具外，亦代表其品牌，或甚至與搜尋結果相關。若是

doi:10.6342/NTU202302025

讓該非法網站之架設者重新註冊相似的域名，則難以削弱該域名的記憶性與關聯性，非法網站春風吹又生，而使用者只要透過類似字彙即可造訪，網站流量不因原本域名之停止解析受重大影響。

是以，欲解決此問題，本文以為可以機關協力，向 TWNIC 請求暫停「相似詞彙、關鍵字」之域名註冊。而按 TWNIC 現行之業務規章[78]，此乃可行之作法。依規章第 10 條，域名之申請係採取先申請先發給原則，且原則上不得拒絕客戶申請網域名稱，除非客戶所申請之域名係已被 TWNIC 保留或限制者。換言之，若是於申請扣押時，亦請求其協助將相似域名列為保留，暫停相似域名之註冊，能夠補充原域名停止解析之效果。

或有認為，何不以「申請人」作為限制註冊之對象，而以「相似域名」為保留標的？蓋於現行業務規章上，TWNIC 不會基於「申請人」之資格而限制申請。更有甚者，按規章第 8 條，TWNIC 與受理註冊機構皆不負查證客戶所填具資料真偽之責任。準此，TWNIC 無針對申請人資格審查之義務，且若以申請人曾遭停止解析即一概拒絕其域名之註冊，有言論自由事前限制之違憲風險。而僅暫時保留相似域名之註冊，則申請人尚得註冊其他域名發表言論，又能兼顧停止解析之執行效果，應屬可行之方式。

最後，停止解析尚存在無法阻止域名移轉之技術限制。惟只要搭配扣押命令之禁止處分效力即得補足此漏洞，故此技術上之侷限不會對停止解析之執行效果構成太大的阻礙。

第五節 小結

本章節從技術面切入探討停止解析，首先針對本論文之專有名詞說明，尤其以「域名」及「解析」為中心。並以較為白話之方式介紹停止解析之技術內涵，使讀者得以掌握停止解析之概念，以利後續法律議題討論。而透過對於技術之理解，可

[78] TWNIC，https://www.twnic.tw/dnser vice_announce_announce_1.php（最後瀏覽日：07/09/2022）。

doi:10.6342/NTU202302025

以了解到一般使用者上網時，通常有使用 DNS 伺服器之需求；而 TWNIC 掌握了我國的網域管理，並與我國之電信業者合作創建了國家型 DNS RPZ 架構。是以，我國之偵查機關可以請求 TWNIC 協助，達到使境內使用者，使用我國業者所提供之伺服器上網時，無法解析網域之效果。

透過本節對於技術之介紹，可以得知停止解析乃我國目前針對網域扣押，乃成本低、效率高，且實際上可行之技術。雖存有技術限制，但透過制度上的輔助，於網頁公告停止解析事由、對註冊機關下禁止處分等，則可以某程度上補足漏洞。且上述之限制也無法否定停止解析具有提高犯罪成本、嚇阻不法之效果，故將此技術運用於偵查，有其意義。

而本文下一章節將以美國域名扣押、停止解析之法律實務探討問題意識所提出之爭點，了解美國法對此議題之處理，以及將我國與美國之法制、背景差異考量與比較，思考美國法之作法是否適合於我國援用，作為借鑒。

doi:10.6342/NTU202302025

第三章 美國法

本章節將介紹美國的扣押及沒收制度，尤其針對域名扣押之現況進行討論。DNS 過濾之技術已存在一段時間，過去大多是由網路服務業者運用於維護、管理上網服務者，而後則被美國作為網路言論之管制手段。美國對於域名之扣押已經行之有年，且對此具有豐富的文獻探討，故本文挑選美國法作為比較法之對象之一。雖然美國在網域管理方面所掌握之資源遠大於我國，而與我國有背景上之差異。惟在討論我國如何規範新興技術停止解析時，不妨先參考對此已行之有年之美國法，且美國法在我國刑事訴訟之發展上也具有影響力，在進行比較法分析時也可能遇上相同之爭點，得以參考美國做法，再思考我國是否適合援用。是故，本文以美國法作為比較法對象，下文介紹美國法上域名扣押之爭議。

於下一小節概略的介紹美國之扣押、沒收制度後，將以本文問題意識為架構，依序探討美國法對於域名扣押爭議之處理方式，於章節之末分析並與我國法背景比較。

第一節 美國扣押、沒收制度簡介

在談論美國法上域名扣押制度之前，須先了解該國沒收、扣押制度之特色，始得窺探議題全貌。

第一項 刑事、行政與民事沒收

美國法的沒收制度散落於各個不同的條文，並無統一之規定。然而隨著政府機關長年運用沒收制度打擊犯罪，其沒收制度已體制化發展[79]。在美國的聯邦法體系

[79] 楊雲驊、簡士淳（2015），〈刑事獨立沒收與追徵立法之必要—以德、美立法為觀察〉，《月旦法學雜誌》，241 期，頁 96。

doi:10.6342/NTU202302025

下，共有三種沒收型態，分別為行政沒收（Administrative Forfeiture）、刑事沒收（Criminal Forfeiture）及民事沒收（Civil Forfeiture），三軌並行之狀態。以下分別就各該制度簡介之。

一、行政沒收

行政沒收係由聯邦執法機關執行，過程中並無檢察官或法院的介入，未經由司法審查程序，故**不具備司法訟爭性**[80]。此乃行政沒收與民事、刑事沒收之間最大的差異。由於不需經由司法審查程序，簡便的行政沒收於聯邦政府之沒收案件中占了相當高的比例[81]。而行政沒收之另一特徵，係其與民事沒收同為**對物（*In Rem*）沒收**，換言之，行政沒收係聯邦執法機關針對「財產」所發動之程序，程序之相對主體乃財產，而非財產之所有人、權利人等，此種對物性質將於民事沒收中詳述。

（一）行政沒收之程序

首先，只要聯邦執法機關依**相當理由**（Probable Cause）認為系爭財產為行政沒收之標的，便可以向財產發現地或沒入程序地之聯邦地方法院**聲請扣押**[82]。依 18 U.S.C. § 981(b)(2)，此處之扣押以有令狀為原則，惟另外存在執法機關得逕為扣押，不用事先向法院聲請之例外情形[83]。

於扣押財產後，執法機關將會於官方網站刊登扣押資訊，或是書面通知系爭財產之所有人、相關權利人，若於法定期間內無人對系爭扣押物提出異議，執法機關

---

[80] Legal Information Institute, *Administrative Forfeiture*, https://www.law.cornell.edu/wex/administrative_forfeiture (last visited Sept. 15, 2022).
[81] 楊雲驊、簡士淳，參前揭註 79，頁 97。
[82] 同上註，頁 97。18 U.S.C. §981(c).
[83] 18 U.S.C. §981(b)(2):

> Seizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure, except that a seizure may be made without a warrant if—
> (A) a complaint for forfeiture has been filed in the United States district court and the court issued an arrest warrant in rem pursuant to the Supplemental Rules for Certain Admiralty and Maritime Claims;
> (B) there is probable cause to believe that the property is subject to forfeiture and—
> (i) the seizure is made pursuant to a lawful arrest or search; or
> (ii) another exception to the Fourth Amendment warrant requirement would apply; or
> (C) the property was lawfully seized by a State or local law enforcement agency and transferred to a Federal agency.

doi:10.6342/NTU202302025

便會做出與法院判決具有同等效力之沒收命令，進而發生行政沒收。此處顯現了行政沒收之優點，於無人異議之沒收，政府毋庸承擔司法訴訟之花費與負擔[84]。

另外，為保障財產權利人之正當程序權利，於 2000 年提出的民事沒收改革法案（Civil Asset Forfeiture Reform Act, 簡稱 CAFRA），要求執法機關於扣押後的 60 天內必須開啟沒收程序[85]。

倘若於扣押後有相關權利人提出異議，扣押機關則必須於 90 天內向檢察機關報告，由檢察機關決定是否提起司法沒收程序，即民事或刑事沒收。若扣押機關未如期提出報告或是檢察機關評估後拒絕提起沒收訴訟，即須返還系爭扣押財產[86]。

（二）行政沒收之標的

由於行政沒收不具有司法性，在程序要求較低之情況下，對於沒收之標的亦有所限制。參照 18 U.S.C. §985(a)以及 19 U.S.C. §1607(a)，行政沒收不得針對不動產、不動產相關權利、現金與金融票據以外價值超過 50 萬元美金的動產。故面對高價值之財產，若欲沒收僅得依循司法沒收程序，以免過度侵害人民財產權[87]。

二、刑事沒收

刑事沒收是對於被告刑事起訴的一部分，為刑罰之一部[88]。準此，刑事沒收之前提係被告有罪，倘被告之刑事案件被定罪，並且財產被認為可沒收，法院則可以發出沒收之命令[89]。換言之，刑事沒收必當附隨於刑事案件之起訴，只有被告於刑事訴訟程序之終結被定罪，才可能發生刑事沒收之法律效果。此乃以被告為訴訟主體，**對人（*In Personam*）**之訴訟，與前述之行政沒收乃對物程序有所不同。

---

84 Department of Justice, *Statement for The Record U.S. Department of Justice* (Apr. 15, 2015), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2015/10/06/doj_submission_for_the_record_re_asset_forfeiture_reform_act_15apr152_2_508_compliant.pdf, at 4.

85 楊雲驊、簡士淳，參前揭註 79，頁 97。18 U.S.C. §983(a)(1)(A)(i).

86 同上註，頁 97。18 U.S.C. §983(a)(3).

87 吳協展（2009），〈美國犯罪所得單獨沒收之法制研究〉，臺灣高雄地方法院檢察署，頁 9。

88 楊雲驊、簡士淳，參前揭註 79，頁 97。

89 The United States Department of Justice, *Types of Federal Forfeiture*, https://www.justice.gov/afms/types-federal-forfeiture (last visited Sept. 11, 2022); U.S. Department of The Treasury, *Forfeiture Overview*, https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/asset-forfeiture/forfeiture-overview (last visited Sept. 11, 2022).

doi:10.6342/NTU202302025

（一）刑事沒收之程序

承前說明，刑事沒收由於具有刑罰之性質，其程序必然係附隨於刑事訴訟。以下詳述：

1.審前保全措施

由於刑事沒收之成立前提乃被告成立犯罪，故其沒收之時點係發生於審判後階段。在此之前系爭應沒收之財產很有可能被移轉、脫產，而使得實際上難以達成沒收之效果。是以，於規範上存在審前保全措施，檢察機關可以於審判終結前聲請，以保全日後對沒收財產之執行。

(1)保全命令（Protective Orders）

按 21 U.S.C. §853(e)，於檢察官起訴前或起訴後至法院審理之前，法院得依檢察官之聲請向被告核發保全命令，確保沒收物在刑事訴訟程序終結前不致流失[90]。其中，保全命令又可以區分為「通常禁制令」、「暫時禁制令」兩種。前者之依據乃 21 U.S.C. §853(e)(1)(B)，法院可以核發通常禁制令，限制被告對於財產之處分、或是為一定的履約保證行為。此類禁制令之有效期間乃 90 天，且核發前必須事先通知相對人並由法院舉行聽證程序，以調查禁制令之必要性；而被告得於此程序中答辯或提出有利之證據[91]。相對於通常禁制令需經過聽證程序，暫時禁制令則不用此繁複之程序，由檢察官單方面向法院聲請即可。惟既然於程序上未能提供被告答辯之機會，為避免限制被告權利過劇，暫時禁制令之效期僅有 14 天。

(2)刑事扣押令狀（Warrant of Seizure）

依法院核發之刑事扣押令狀扣押財產，國家即得直接於刑事程序進行中占有系爭財產，且毋庸經聽證程序。相對於保全命令來說，程序上較為便利，故於實務上檢察機關亦較傾向以聲請扣押令狀之方式保全系爭沒收財產。按 21 U.S.C. §853(f)，法院於審查扣押聲請時，需審酌系爭財產是否具有合理根據，得認定其將

[90] 楊雲驊、簡士淳，參前揭註 79，頁 98。
[91] 同上註。

doi:10.6342/NTU202302025

來具有沒收之可能性，且僅依 21 U.S.C. §853(e)的保全命令將不足以保全財產。於此二要件皆該當時，法院始得核發扣押令狀。

2.起訴

由於刑事沒收係對人訴訟，而非針對財產單獨提起沒收，故須經由刑事起訴才得以執行。依據聯邦刑事訴訟程序[92]之規定，檢察官於起訴時便須將沒收客體載於起訴書中，且應盡可能的具體、明確描述，始得拘束法院於判決後之量刑程序中考量沒收之必要性[93]。

由於刑事沒收係從刑，被告須被判處有罪或認罪協商，才可開啟刑事沒收程序[94]。而開啟程序後，由於沒收乃法律效果，故應進入量刑程序，裁量是否沒收。是故，刑事沒收之舉證責任可以區分為兩階段，第一階段是定罪程序，就本案事實之證明，檢察官應舉證被告的犯罪嫌疑已到達無合理懷疑（Beyond Reasonable Doubt）的程度。第二階段是沒收程序，必須證明犯罪行為與沒收之間的關聯性[95]，而此關聯性之證明，檢察官僅需舉證至優勢證據（Preponderance of the Evidence）程度，則輪由被告舉反證。所謂的優勢證據，可以理解為「系爭財產與犯罪有關之可能性大於無關[96]」。

作成沒收判決後，即交由檢察長負責沒收財產，並由國家保管使用或出賣，再以賣出的金錢補償沒收程序產生的費用。

---

[92] Fed. Rule Crim. Proc. §32.2(a): "A court must not enter a judgment of forfeiture in a criminal proceeding unless the indictment or information contains notice to the defendant that the government will seek the forfeiture of property as part of any sentence in accordance with the applicable statute." 補充說明，在此也展現了被告在刑事沒收訴訟中，被告有受通知權（Right to Notice），另參 Fed. Rule Crim. Proc. §7(c)2, Notes of Advisory Committee on Rules—1972 Amendment.

[93] 楊雲驊、簡士淳，參前揭註 79，頁 99。

[94] 林志潔（2016），〈『沒收新制的挑戰』研討會會議紀錄〉，《沒收新制（一） 刑法的百年變革》，頁 274。

[95] 同上註，頁 276。

[96] "Preponderance of the evidence means that the evidence 'more likely than not' weighs in the government's favor—or, put differently, that there is a 51% chance the government is correct." Institute of Justice, *Standard of Proof*, https://ij.org/report/policing-for-profit-3/pfp3content/civil-forfeiture-laws-fail-to-protect-property-owners/2020-civil-forfeiture-law-grades/standard-of-proof/ (last visited Sept. 18, 2022).

doi:10.6342/NTU202302025

（二）刑事沒收之標的

按 21 U.S.C. §853(a)，刑事沒收之範圍，包括行為人直接或間接因犯罪所取得或由其所生之財產（Property）；以及，行為人用以、意圖用以從事或促進該犯罪之財產。其中，財產之概念包括不動產及其他有形或無形之財產，如權利[97]。

另外，由於刑事沒收屬對人訴訟，故當應沒收的財產已被移轉、消費或無法發現時，法院仍可命令被告支付相當之金額（Money Judgment）或沒收替代財產（Substitute Asset）[98]，類似於我國之追徵制度。此與對物沒收之性質相當不同，蓋對物沒收只能針對標的物發動，對人沒收的所關注的則是對行為人之懲罰，不因系爭應沒收之物消失不見即放棄沒收。在此層面之上，刑事沒收相較於對物沒收乃更為廣泛且有力的沒收機制。然而，從另一個角度觀察，基於刑事沒收的對人性質，刑事沒收只能對被告本人發動，若該物另屬他人所有，則無特別規定之下不得沒收之。此與對物沒收原則上不過問物之所有人為何，又有所不同。

三、民事沒收

民事沒收於美國實務上運用廣泛，且歷史悠久[99]。由於過去美國法上並無針對民事沒收為概括、準則性之規範，故於實際案例之操作下，民事沒收遭遇無數的違憲爭議與抨擊。是以，美國國會為健全沒收法制，建構更為公平且一致的對物沒收程序，於 2000 年通過民事沒收改革法案，進一步明確規範沒收之令狀原則、扣押等重要程序[100]，並回應了過往的批評。於下文透過程序介紹民事沒收之變革：

（一）民事沒收之程序

當政府機關執法時，於調查過程中有相當理由認為某財產依法應予沒收時，即可向法院**聲請扣押**[101]。而在有證據可信特定財產為犯罪所得，或是供犯罪所用時，

---

[97] 李榮耕（2015），〈犯罪所得資產的沒收—以美國民事沒收制度為借鏡〉，《輔仁法學》，49 期，頁 63。

[98] 楊雲驊、簡士淳，參前揭註 79，頁 100。

[99] 有認為美國民事沒收制度至少可以回溯至中世紀歐陸或英國普通法。李榮耕，參前揭註 97，頁 69，註腳 29。

[100] 同上註，頁 80。

[101] 民事沒收的審前保全程序：「為了確保民事沒收程序的順利進行，一般在沒收前會對可得沒收之物予以扣押。扣押程序可能是依照刑事程序進行，可能是單純為民事沒收而扣押。」楊雲驊、簡士

doi:10.6342/NTU202302025

政府機關可以分別依聯邦或州法規，**針對該財產提起民事訴訟**，予以沒收，此乃美國法的民事沒收制度。在此，民事沒收與刑事沒收相同，皆屬司法沒收。於訴訟程序中，財產之相關權利人可以提出抗辯，爭執沒收的合法性。然而因民事沒收乃**對物訴訟**，故該權利人雖有參與訴訟、表達意見之權利，卻並非訴訟當事人[102]。

由政府機關擔任原告之民事沒收訴訟，程序之開啟係由政府機關提出起訴書，表明系爭財產依照實體法之規定應予沒收。而對系爭財產主張權利者，則須在法定期間內提出異議，並回應原告起訴的沒收請求。爾後，該民事沒收案件依序進入證據開示、審前程序及審理程序[103]。

由於選用何種沒收方式，得由執法機關自行決定。是以，若於刑事案件之偵查、審理，同時開啟民事沒收訴訟，民事沒收之證據開示程序有可能影響檢察官於刑事案件之偵查優勢。故按 18 U.S.C. §981(g)，此時民事沒收法院可以暫停訴訟。

民事沒收訴訟經過司法審查後，若政府機關勝訴，則由國家取得財產的所有權（法制上亦有民事沒收財產利益分配之設計[104]）；政府機關敗訴時，則財產所有人保有其所有權。

關於民事沒收程序發動之時機，由於民事沒收之訴乃獨立訴訟，且不以刑事有罪判決為前提，故無論是在刑事案件之起訴前或起訴後，甚至未有任何刑事起訴時，皆得提起此訴訟[105]。另一方面，由於民事沒收不以刑事有罪為前提，政府機關的舉證責任相較於刑事沒收則大幅減輕。按 18 U.S.C. §983(c)，於民事沒收程序中，政府負有舉證「犯罪發生」、「系爭財產與犯罪存在關聯性」及「財產依法應予沒收」此三要件之責任[106]，惟其證明之程度皆僅需達到**優勢證據程度**。

淳，參前揭註 79，頁 108。扣押令狀原則上應向法院聲請，由法院開立，以符合憲法第四修正案禁止不法搜索扣押的精神。

[102] 同上註，頁 64。

[103] 吳協展，參前揭註 87，頁 11。

[104] 18 U.S.C. §981(e). 沒收轉讓財產制度，使協力機關間可以共享沒收利益，透過分享普遍的反應出機構對於沒收參與貢獻之程度。

[105] 楊雲驊、簡士淳，參前揭註 79，頁 100-101。

[106] 同上註，頁 101。

doi:10.6342/NTU202302025

（二）民事沒收之標的—兼論「對物」沒收

1.沒收標的

美國之沒收法並無概括、準則性的規定，而是透過長時間的案例發展，由國會先後針對各種不同的犯罪，制定相應的法規來規範沒收之客體，因此財產沒收的對象會因所適用之法規而有所不同[107]。歸納聯邦法規中有關沒收客體的主要規定[108]，大致上涵蓋：(1)列舉犯罪之犯罪所得[109]、(2)用以實施或幫助犯罪的財產（Facilitating Property），包括毒品、暴力犯罪、貪汙及兒童色情案件等[110]、(3)洗錢[111]、(4)犯罪組織運作期間賴以維持及取得的所有財產，以及被告在犯罪組織下所有的利益[112]、(5)計畫或從事恐怖活動者，其國內、外之所有財產[113]。

2.對物沒收之概念與範圍

對物沒收乃以「財產」為程序之主體，係聯邦政府機關以欲沒收之物作為訴訟之被告或程序之相對人。此種制度能夠解決一些因現實困難，如犯罪嫌疑人逃亡、死亡等，無法追訴行為人犯罪卻又有沒收必要之情形；也同時使得程序較為迅速，只需特定標的物，而不須事先特定並起訴相對人。於美國實務上也常以民事沒收作為事件之終結，而不以行為人被定罪為必要[114]（將重心置於查扣犯罪財產，而非犯罪追訴）。

基於民事沒收之對物性，若系爭財產不見了，則不得再對財產之所有人請求相當金額、沒收替代財產或追徵，故民事沒收之效力只及於該財產本身。另外，無論系爭財產是否為第三人所有，原則上均為民事沒收之客體。僅例外於該財產之權利

---

107 吳協展，參前揭註 87，頁 6。
108 同上註，頁 6-8。
109 18 U.S.C. §981(a)(1)(C); 18 U.S.C. §1956(c)(7).
110 18 U.S.C. §981(a)(1)(B); 21 U.S.C. §881(a); 18 U.S.C. §2254.
111 18 U.S.C. §981(a)(1).
112 18 U.S.C. §1963(a).
113 18 U.S.C. §981(a)(1)(G).
114 TWNIC，https://blog.twnic.tw/videosyt/域名之扣押與沒收-以司法實務操作為中心/（最後瀏覽日：09/15/2022）。

doi:10.6342/NTU202302025

人提出「無辜所有人抗辯」（Innocent Owner Defense）[115]，並舉證成功時，始得免於系爭財產之沒收。

（三）2000 年民事沒收改革法案之重點

在民事沒收改革法案出現之前，民事沒收已是美國執法機關長期運用於實務之工具。其程序簡便、快速之特色已如前述。然而，民事沒收的便利性實際上是由程序正當性換來的[116]，因此在實務上也遭逢不少質疑。

常見的爭議如：1.民事沒收是否為處罰，而受到處罰過度禁止的憲法誡命約束（美國憲法第八修正案[117]）？2.沒收係對人民財產權之限制，則是否符合憲法所要求之正當法律程序（美國憲法第五修正案）？詳言之，過去的沒收規範散見於各法案，法條卻未明確規範政府機關之舉證程度，故實務上亦不少僅舉證至相當理由程度即沒收之例，舉證責任為何無統一之規範。且對於未涉案之第三人，亦未明確規範其受通知權、程序參與權，有保護不周之嫌。3.民事沒收雖非刑事案件，無美國憲法第六修正案之適用，是否即無需保障財產所有人辯護權？詳言之，無資力、欠缺法律知識之財產所有人與握有公權力之檢察官，難認於訴訟上係處於對等、相當之地位，有武器不相當、不公平之疑慮。4.民事沒收程序中，搜索、扣押之執行，是否符合憲法對於非法搜索扣押禁止之規定（美國憲法第四修正案）[118]？5.民事沒收之運用範圍廣泛，若將財產所有人賴以維生之工具、房屋或一切財產沒收，將致其難以維生。倘將其生存之一切剝奪，有侵害人性尊嚴、生命權，而侵害過度之疑慮。

於 2000 年，美國國會提出沒收法之改革法案，正面回應上述爭議。改革法案最大的變革共有下列五點：

---

[115] 18 U.S.C. §983(d)(2); 18 U.S.C. §983(d)(3). 法條設計上，將無辜所有人抗辯區分為取得財產之時間為犯罪發生前，抑或犯罪發生後。前者抗辯之重點在於犯罪發生之時是否「知悉」犯罪行為，以及是否有「採取適當措施」防止該財產被用以為犯罪行為；後者之重點則在於聲明人是否為「支出對價的善意購買人」，以及「是否知悉其取得之財產是將被沒收者。」

[116] 楊雲驊、簡士淳，參前揭註 79，頁 112。

[117] U. S. Const., 8th Amend.: “Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.”

[118] 吳協展，參前揭註 87，頁 14。

doi:10.6342/NTU202302025

1.比例原則：依 18 U.S.C. §983(g)，異議者可以請求法院判決民事沒收是否過當（Grossly Disproportional）而違反美國憲法第八修正案，法院則需衡量財產沒收的範圍與犯罪嚴重性之間是否符合比例（罪刑相當原則）。若異議人抗辯成功，法院可就沒收數額予以酌減[119]。

2.正當程序：依 18 U.S.C. §983(a)，要求政府必須嚴格遵守特定的程序規範才能執行民事沒收。明確規定財產權利人之受通知權以及異議權，如：財產扣押之後，執法機關必須於 60 天內通知權利人，並將扣押資訊公告於網站上。並且，財產權利人得於扣押後 90 天內提起異議，若提起異議，則必須進入司法程序使得沒收，使財產權受干預者之程序權受到更妥適之保障。另依 18 U.S.C. §983(c)，亦明確規範政府機關須負證據優勢之舉證責任，解決了過往實務標準不一之問題。

3.辯護權保障：依 18 U.S.C. §983(b)，賦予異議者於無資力聘請律師且係善意提出異議時，有請求法院指定律師為其辯護之權利，充實其辯護權之保障。倘若異議有理由，依 28 U.S.C. §2465(b)將由國家負擔該財產權利人之律師費用[120]，作為國家對於人民財產權干預之補償。當然，為了避免濫行異議耗費司法資源，於賦予無資力異議者辯護權保障的同時，依 18 U.S.C. §983(h)對於輕率提起財產沒收異議者亦有制裁規定。

4.扣押程序：扣押作為保全措施，可以使政府機關在沒收判決之前先占有、管理系爭財產，然而對於財產的搜索、扣押，將限制人民之隱私權與財產權。因此，為避免對人民造成過度侵害，並且合乎美國憲法第四修正案禁止非法搜索扣押之原則。於 18 U.S.C. §981(b)設有民事沒收中扣押之規範。該條明定扣押乃採取令狀原則，若無法律明定之例外情形，則必須事先獲得法院核發之扣押令始得執行之。

其中，由於不動產屬高價值財產，且不動產涉及財產所有人之生活起居。若僅透過簡單的扣押程序即於沒收判決前由政府機關取得占有，恐過度侵害依賴其生

[119] 同上註，頁 47。
[120] 此與美國法上，訴訟當事人自己承擔法律費用（無論輸贏）的一般規則存在重大偏差。Department of Justice, *supra* note 84, at 6.

doi:10.6342/NTU202302025

存的不動產所有人。是以，於民事沒收改革法案 18 U.S.C. §985(b)明定，原則上不允許政府機關於沒收判決前扣押不動產，且縱要扣押亦應由所有權人占有。

5.窘困抗辯：依 18 U.S.C. §983(f)(1)，設有財產所有人之窘困抗辯。於本條所列之情形，財產所有人可以請求立即返還被扣押之財產，例如：「政府對該財產之占有可能使財產所有人陷入無法營業或無家可歸之生活困窘。」除非該財產為 18 U.S.C. §983(f)(8)的證據或違禁物，得不予返還。此抗辯之設計，目的係在於兼顧抗制犯罪的公益與人民的生活基本需求。蓋民事沒收的範圍相當廣泛，這固然使得偵查官員得以有效地根除不法活動的利益與所得，除去犯罪動機；但也可能使得財產所有人的生活陷入無以為繼的困境[121]。此項改革處理了民事沒收範圍過廣，於個案中有過度侵害人民生存權之疑慮。

第二項 沒收程序比較

於介紹美國之沒收法制後，本文根據前文，以表格 1 整理美國法上行政、刑事、民事沒收程序之比較，以利後續討論美國實務如何將沒收運用於非法域名。

[121] 李榮耕，參前揭註 97，頁 82。

doi:10.6342/NTU202302025

	行政沒收	刑事沒收	民事沒收
司法性	否	是	是
性質	對物程序	對人訴訟	對物訴訟
追徵、補繳	否	是	否
對第三人沒收	是	否	是
沒收標的	金額小:「50 萬美元以下之動產，以及現金或金融票據」。	與犯罪相關:「行為人直接或間接因犯罪所取得或由其所生之財產。以及,行為人用以、意圖用以從事或促進該犯罪之財產」。	範圍廣，由條文列舉：「犯罪所得、實施或幫助犯罪之工具、洗錢、犯罪組織財產、恐怖活動發動者之財產……等」。
證明度		兩階段： 犯罪事實—無合理懷疑 關聯性—優勢證據	優勢證據
程序發動時點	扣押後法定期間內	於刑事起訴書上記載請求沒收之意旨	針對扣押異議後之法定期間內。不與刑事案件程序掛鉤。
財產所有人之訴訟地位		刑事被告	程序參與人（異議者）

表格 1 美國法沒收制度比較

資料來源：筆者自製。

由表格 1 可知，行政沒收與民事沒收相比，雖然行政沒收之程序較為簡便，毋庸經過司法審查。然而，其沒收標的也相對較為狹窄。除金額限制（50 萬元美金以下）外，19 U.S.C. §1607(a)—關稅法案作為行政沒收之法源，其對於沒收客體本身亦有限制。不若民事、刑事沒收係以財產（Property）做概括之規範，19 U.S.C. §1607(a)則是列舉了與進出口相關之動產,「船隻、車輛、飛機、商品或行李（Vessel, Vehicle, Aircraft, Merchandise, or Baggage）」。準此，與關稅、進出口無關之域名，難認得作為行政沒收之客體,美國實務上亦無透過行政沒收手段沒收域名之案例。

doi:10.6342/NTU202302025

另一方面，行政沒收亦僅能接續於「未被提起異議之扣押程序」後實行。故行政沒收雖於程序上簡捷，但規範上同時透過客體限制，限縮其運用範圍。本文亦贊同美國實務未透過行政沒收處理非法域名之問題。蓋針對域名之沒收同時限制人民財產權與言論自由，且涉及敏感的網路言論管制問題，以程序保障之觀點觀之，若對於人民權利之限制較重，則自然必須透過更為嚴謹之審查程序，尤其應有司法審查之必要。是以，除上述文義限制外，本文透過程序保障之觀點，亦認同不宜以行政沒收手段沒收域名。

同樣具有司法性之刑事沒收與民事沒收程序，於實務上美國執法機關較**傾向運用民事沒收制度**。其理由有三：（一）民事沒收乃對物程序，刑事沒收則為對人程序。是以，舉凡犯罪行為人潛逃、死亡、失蹤，或是犯罪無法追訴之情形，刑事沒收都將因程序主體之不存在而無法發動。反之，對物程序的民事沒收則不受此限，不論財產所有人位於何處，可以直接針對物提起訴訟。（二）舉證責任之差異。雖由於刑事沒收屬刑罰，係於刑事案件之量刑程序審酌，故證明度僅須達優勢證據程度，檢察官在此所負之舉證責任似乎與民事沒收相同。惟查，刑事沒收係以被告有罪為前提，是以，對於犯罪事實之證明仍須達無合理懷疑之高舉證程度，才能發動刑事沒收。故於舉證責任上仍係民事沒收程序較輕。（三）沒收範圍之差異，此差異係源於對物與對人程序之不同。以人為程序主體的刑事沒收，當沒收財產被移轉、脫手，仍得向被告請求追徵、追繳財產價值。然而，若系爭財產屬第三人所有，由於刑事沒收僅能針對被告發動，此時則不得沒收。就此而言，尚難斷定刑事、民事沒收之範圍廣狹。然，另考慮到刑事沒收係依附於刑事案件，故沒收之標的亦須限縮於與本案具實質關聯者。縱使存在相關案件，惟只要他案尚未被定罪，則不得對他案之相關財產沒收。反之，民事沒收則不用被單一案件綑綁，只要與犯罪相關之財產皆得一次性的於民事沒收程序處理[122]。因此，考量到刑事沒收依附於刑事案件，需經過冗長訴訟程序之特性，其沒收執法效率較民事沒收低，實際上成功沒收財產

[122] 同上註，頁 66-68。

doi:10.6342/NTU202302025

之範圍亦較民事沒收窄。是故，在執法策略上，政府機關較偏好運用民事沒收，於域名之沒收亦同。可以發現美國實務上關於域名之扣押與沒收，皆係以民事對物沒收為手段。

下一節將介紹美國實務對於域名扣押與沒收之現況，以及民事沒收程序運用於域名時遭遇之爭議與難題。

第二節 美國域名扣押實務

2021 年，新冠肺炎（COVID-19）於美國境內肆虐，隨著疫情升溫，民眾對於疫苗的渴望也隨之提升。此時，便出現了利用大眾的渴望而為非法行為之人。其手法如設置販售疫苗之假網站，使人們透過點擊網址，藉機收集訪問網站的個人資料，並將資料用於惡意目的，包括詐欺、網絡釣魚攻擊或安插惡意軟體[123]。除了提醒民眾提高警覺不要點擊未知的連結外，美國馬里蘭州聯邦檢察署同時對相關的惡意域名聲請扣押。扣押後，當民眾造訪系爭網頁，頁面將顯示系爭域名已被聯邦政府機關扣押，若想要查看更多資訊，此網址將被導向其他網頁[124]。運用域名扣押作為網路犯罪抗制之手段，在美國已行之有年。近年更是被大量用於阻擋恐怖主義之宣傳[125]，以及防止新冠肺炎相關之假消息等。經統計，於 2017 年至 2018 年間，有超過一百萬個域名被刑事或民事扣押[126]。

欲了解域名扣押之所以於美國實務上被大量運用，可就其歷史發展探知。

一、域名扣押之發展歷程—Operation In Our Sites

---

123 *HSI Investigation Results in Seizure of 3 Domain Names Purporting to Be Biotechnology Company Websites With COVID-19 Treatments*, U.S. IMMIGR. AND CUSTOMS ENFORCEMENT (Apr. 7, 2021), https://www.ice.gov/news/releases/hsi-investigation-results-seizure-3-domain-names-purporting-be-biotechnology-company.

124 *Id*.

125 The United States Department of Justice, *United States Seizes Domain Names Used by Foreign Terrorist Organization*, https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-foreign-terrorist-organization (last visited Sept. 22, 2022).

126 *Over A Million Websites Seized in Global Operation*, U.S. IMMIGR. AND CUSTOMS ENFORCEMENT (Nov. 26, 2018), https://www.ice.gov/news/releases/over-million-websites-seized-global-operation.

doi:10.6342/NTU202302025

回首過去，美國的執法機關開始大量運用域名扣押係自 2010 年開始，美國國土安全部（Department of Homeland Security）轄下的移民及邊境執法局（Immigration and Customs Enforcement，以下簡稱 ICE）及相關執法機構發起了 Operation In Our Sites 行動。該行動主要係針對販售仿冒品及侵害著作權的網站，包括：精品、藥品、盜版影音網站[127]，加強執法、展開全面性的打擊[128]。且行動大多在重大節慶前發起，如感恩節、黑色星期五等，蓋彼時購物需求增加，仿冒品也同時的大量流通於市場，在此時發動執法可以有效減少損害發生。在執法行動中，執法機關將系爭網站之域名作為行為人侵害智慧財產權時所使用之犯罪工具，因而透過民事對物沒收的方式，對域名發動扣押，並隨後開啟沒收程序。

Operation In Our Sites 為跨國行動，不僅針對境內註冊之域名，亦致力於防止來自境外之侵害。然而，架設於境外伺服器的非法網站非屬美國之管轄，理論上需仰賴外國政府之協力與配合執法，造成執行方面之困擾。而美國政府機關最終取巧地突破了境外執法的限制。

其原理在於，透過扣押令，請求位於美國境內之域名註冊管理機構，註銷、移轉系爭網站之域名。故雖該網站架設於境外伺服器，惟透過其註冊於美國的域名，美國執法機關便得使該網域無法與原本的網址連結，進而達到限制連結網站之效果。換言之，美國政府機關係透過**域名作為扣押與沒收執法之管轄聯繫因素**。此作法之所以在美國奏效，係因大多的域名註冊管理機構皆設立於美國境內[129]。

二、美國於域名管理之優勢—ICANN

美國之所以在域名之管制佔據地利優勢，可以從設址於美國加州的 ICANN 略知一二[130]。

---

127 陳昱奉（2019），〈跨境電腦犯罪偵辦之未來走向—從『電腦犯罪公約（Convention on Cybercrime）』暨『In Our Sites 行動』出發〉，《台灣國際法學刊》，15:2 期，頁 100。

128 陳昱奉，參前揭註 64，頁 10-11。

129 陳昱奉（2022），〈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》，32 期，頁 267。

130 蔡志宏，參前揭註 17，頁 9-10。

doi:10.6342/NTU202302025

從第二章技術章節之說明可以發現，域名係現今上網過程中所不可或缺者，雖事實上存在其他替代域名之連線方式，但皆不如域名擁有大眾的信賴，而成為通用之網路語言[131]。換言之，掌握了域名的管理，即成為網路管制之重要角色，此即現今 ICANN 之地位。

網際網路號碼與名稱管理機構（Internet Corporation for Assigned Numbers and Names，簡稱 ICANN），係一非營利私法人機構，負責網際網路公共資源統籌管理和網際網路標準制定。是故，全球域名法制亦係由 ICANN 所主導治理，有謂網路世界之制憲機關[132]。表面上 ICANN 係一與政府無關之機構，惟實際上至 2016 年 ICANN 始脫離美國之監管[133]。

在域名管理受美國監管之特殊架構之下，加上美國的網際網路技術發展較早。故在域名市場中，係由美國之公司佔據一席之地，亦非難以理解。域名市場中，可以區分為經營域名之「域名註冊管理機構（Registry）」，及提供註冊域名服務之「域名受理註冊機構（Registrar）」概念。而許多常見的、使用人數眾多的頂級域名，如.com、.org、.tv 和.net，即係由設立於美國境內之域名註冊管理機構所管理。

是以，以域名作為管轄權聯繫因素的觀點之下，國際上應屬美國享有網路執法之最大優勢[134]。蓋大多的域名註冊管理機構與受理註冊機構系設立於美國境內，只要該等機關之配合，美國政府在網路犯罪之執法上將無往不利。

在確立了美國對於域名之管制能力後，接著將探討實際上以域名作為執法手段時，程序該如何進行。

---

131 同上註，頁 6。

132 劉靜怡（2001），〈從 ICANN（the Internet Corporation for Assigned Names and Numbers）的成形與發展看網際網路公共資源分配和標準制定統籌管理機制的政策與法律問題：一九九八至二○○一年的國際趨勢觀察和省思〉，《國立臺灣大學法學論叢》，30 卷 6 期，頁 98。

133 蔡志宏，參前揭註 17，頁 35；愛范兒（10/04/2016），〈全球網路的新『波瀾』：美國正式交出域名管理權〉，《數位時代》，https://www.bnext.com.tw/article/41205/icann-domain（最後瀏覽日：09/23/2022）。

134 同上註網頁。

doi:10.6342/NTU202302025

三、域名扣押之程序

（一）美國法規範

如前所述，美國實務上目前多數採用民事沒收作為沒收域名之工具。而在沒收判決前，為即時阻止犯罪損害持續發生，在沒收判決前亦通常伴隨著扣押之發生。以下就域名扣押之程序介紹之。

依 18 U.S.C. §981(b)(1)得沒收之財產，除非有 18 U.S.C. §985 不得扣押之情形（如：不動產），原則上皆得扣押之。而扣押採取令狀原則，原則上係由法官保留，由法院裁定是否核發扣押令，並且令狀須明確、具體記載扣押標的以及搜索地點。法官保留之例外則係來自合法搜索、逮捕之扣押、當事人同意、緊急情況等符合美國憲法第四修正案[135]之情況。

按 18 U.S.C. §981(b)(2)民事對物扣押之程序適用聯邦刑事訴訟法之規定，故 ICE 等執法機關於搜集相關證據後，載明犯罪事實並詳列證據，得向管轄法院聲請針對域名之扣押[136]；而其舉證責任僅需達相當理由之程度，以量化的方式表現，美國學者與實務大多將相當理由定位為接近百分之五十之心證門檻。另外，聲請扣押之機關依據美國憲法第四修正案尚須具備宣誓書（切結書）或以代誓宣言保證。

若系爭違法網站係使用**註冊於美國境內**管理機構之域名，於法院核發令狀後，執法機關將持該扣押令向美國境內之註冊管理機構或受理註冊機構請求，將系爭域名所登記之 IP 位址導向美國政府，以達到扣押、沒收該域名之目的。域名被扣押之後，造訪該網站之網路使用者，將會看到網頁被轉址至執法機關的網站，並得透過網頁知悉原網站之域名已遭扣押。基於扣押之聲請係屬於**單方程序**（*Ex-Parte* Proceeding），故在聲請過程中，執法機關**無須**向法院證明該網站確有侵害他人權

[135] U. S. Const., 4 Amend.: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[136] 戴豪君、余啟民主持，參前揭註 70，頁 125-126。

doi:10.6342/NTU202302025

利或者違反刑事法規；而遭扣押之域名所有人，即網站經營者，並無事先就侵權與否或有無扣押域名之必要等，向法院表示意見之機會[137]。

舉實例說明之，管理.com 和.net 頂級域名的註冊管理機構為 VeriSign 公司[138]；管理.org 的註冊管理機構為 The Public Interest Registry（PIR）公司[139]。二者皆設立於美國境內。準此，ICE 便可以持扣押命令，向該等公司請求協助執行網址結尾為.com、.org 和.net 等網站之扣押，公司便會將系爭域名重新導向至美國執法機關網頁，並告知造訪網站者該網站已被扣押。以上之流程不必經由國際司法互助或者於境外提起訴訟程序，便能夠完成[140]。

（二）ICANN 域名扣押指引

另補充說明，ICANN 有以技術人員之現場經驗，出版一域名扣押指引，系爭指引主要取材於美國法院之判決。其中，臚列了對於域名註冊管理機構請求協力者所需提供之資訊，以便利該等機關順利執行。本文就系爭指引摘要如下：1.需提供請求人之聯繫資訊。2.區分請求依據為「法院判決」或「第三人請求」，若係後者則另外需要提供相關可供驗證之證據。3.表明扣押、執行期間。4.明示需要域名管理機構協力變更之域名資訊為何，或是該提供何種協助（停止解析、阻止域名移轉、刪除域名或域名轉址等）。5.告知負責域名資訊查詢之 WHOIS 系統，該顯示何種資訊，以及是否有保密需求[141]。

上述指引供請求執行域名扣押者，於請求前可以自我檢視是否提供完足資料；亦使域名註冊管理機構、受理註冊機構等，於配合執行時有所憑依，清楚該檢驗何種資料，以及執行時該注意之細節。

---

137 陳昱奉，參前揭註 64，頁 10。
138 同上註，頁 11，註 39。
139 同上註，頁 11，註 40。
140 戴豪君、余啟民主持，參前揭註 70，頁 125-126。
141 ICANN, *Guidance for Preparing Domain Name Orders, Seizures & Takedowns*, 6-11 (2012), https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.

doi:10.6342/NTU202302025

四、對於境外域名之處置

至若違法網站之域名係註冊於美國**境外**之域名註冊管理機構，則難以適用上開扣押及沒收程序。蓋既然屬於境外機構所管理之域名，除司法互助之情形下，境外司法機關或是註冊管理機構是否願意配合執行域名之轉址，並無法保證；且溝通過程亦將耗費大量時間成本。就此，對於境外域名似乎存在執法困境。

本論文研究之過程中，致力於查找美國法上對於境外域名扣押之處置方式，惟卻尋找不到相關資料。梳理資料後，本文以為理由有二：（一）美國境內本就掌握了大多數的域名管理[142]。如前所述，大眾常見的頂級域名.com、.org 等都係屬於美國境內之註冊管理機構，故對於美國政府而言，註冊境外域名之非法網站應屬少數，並無並無特別關注之必要。且縱有需求，依美國之國際地位，司法互助仍屬於一有效選項[143]；另外從 ICANN 之發展史中，也可以發現其與美國政府關係之密切，若從 ICANN 與境外域名註冊管理機構之契約著手，亦有可能達到限制系爭網站使用域名之目的。（二）從法制面上觀察，也可以發現民事對物沒收訴訟之**審判權**不及於域名註冊於境外機構之情形，既然境外域名不屬於得沒收者，自然亦不得扣押。依 15 U.S.C. §1125(d)(2)(A)[144]，在商標侵權、搶註之訴訟中，具有民事對物沒收訴訟審判權之法院，限於「註冊或分配域名的註冊管理機構或其他域名管理機構所在地」以及「當足以確立對域名註冊和使用處置的控制和授權的文件已交存於法院之情形」。換言之，在美國法上對於境外註冊之域名於對物訴訟中並無審判權（即不在其司法管轄範圍）。

---

142 蔡志宏，前揭註 17，頁 9-10。

143 可以從「ThePirateBay.cr」此域名之爭議探知。PirateBay 是著名的著作權侵權網站，而此域名係註冊於哥斯大黎加的註冊管理機構，美國透過駐當地的大使館對該機構不斷施壓，雖最終該機構調查後認為無需扣押該域名。惟從此案中可以發現兩個重點，一是美國雖然於技術上可以做到停止解析，惟停止解析只是扣押的執行手段，當於法律上沒有扣押境外域名之權力時，美國也只能採取施壓的方式請求他國協力執法；二者則是美國在國際地位上佔盡優勢，其施壓的過程中甚至有以商業利益威脅關閉機構作為手段，確實造成了註冊管理機構的壓力，與台灣的國際聲量明顯不同。故基於美國的國際地位，透過司法互助將域名管制擴及於境外亦非不可能。Andy Maxwell, *US Embassy Threatens to Close Domain Registry Over "Pirate Bay" Domain*, https://torrentfreak.com/us-embassy-threatens-to-close-domain-registry-over-pirate-bay-domain-170620/ (last visited Oct. 27, 2022).

144 15 U.S.C. §1125(d)(2)(A): "The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if…."

doi:10.6342/NTU202302025

不過，由於我國不若美國在域名管理享有優勢，因此於我國而言，網路犯罪中使用境外域名之犯罪網站反而是常態。此背景差異乃後續進行比較法研究時所需注意者，我國於域名扣押之法制，不宜將審判權同美國之作法限縮於境內註冊之域名。而在扣押之執行面上，不同於美國可以透過直接通知境內域名管理機構協力轉址、更改域名登記，我國則如前言所述有仰賴停止解析技術之必要。

另需注意，由於美國法上民事對物沒收之打擊範圍係限於境內註冊之域名，故理論上美國實務執行域名扣押時，並無迂迴的使用停止解析技術之必要，而可以透過境內註冊管理機構之協力直接暫停係爭域名的使用。而實際上，本文也未查詢到美國法上有將停止解析運用於扣押或刑事偵查之案例。然並非謂美國於網路言論管制上並無使用停止解析作為執行手段，例如：於著作權侵權之民事訴訟中，亦有原告請求法院向 ISP 業者核發禁制令（Injunction Order），而該禁令之執行方式即是禁止 ISP 業者對系爭侵權網站之域名提供解析服務[145]；在 ICANN 的扣押指引中也有提及法院可以於令狀中註明扣押之執行過程中，是否一併請求管理機構協力停止對於系爭域名的解析[146]。是以，於法律層面上，本文所著重者乃域名得否扣押之問題。惟於實際執行上，也會一併關注停止解析是否為妥適之域名扣押執行技術。故於下方針對域名扣押進行合憲性審查時，也會進一步討論停止解析的作為扣押執行手段的相關爭議。

第三節 域名扣押合憲性審查

第一項 基本權干預

扣押，是一為保全證據、得沒收之物及追徵的強制處分。也就是國家取得相對人的財產，以避免證據滅失，或使後續的沒收程序得以執行的處分[147]。在美國法之觀點下，早期認為扣押所限制之基本權係**財產權**。是以，當時對於「扣押標的範圍」

[145] United King Film Distribution Ltd. v. Does 1-10, 21 Civ. 11025 (KPF) (S.D.N.Y. Apr. 26, 2022).
[146] ICANN, *supra* note 141, at 5.
[147] 王兆鵬、張明偉、李榮耕（2022），《刑事訴訟法（上）》，6 版，頁 315。

doi:10.6342/NTU202302025

採取單純證據法則作為認定標準。亦即，對於單純的證據，國家並無高於行為人之財產利益，因此不得扣押，至多僅得向其請求提出。然而，到 1960 年代，刑事訴訟法的思潮已將搜索、扣押規範的保障核心置於**隱私權**之影響。在此想法下，扣押單純證據或得沒收之物對於行為人的隱私侵害程度應無差異，因此國家為了追訴利益之實現，符合法制時自然都可以扣押[148]。

在後續學說討論中，也有關注到扣押財產對於行為人之行動自由、工作權之限制，蓋若系爭財產係行為人賴以為生的營業、交通工具，扣押所限制的將不僅僅是財產權、隱私權[149]。另外，針對猥褻書籍的扣押[150]也曾升起扣押與言論自由關係之討論。綜上，犯罪偵查的過程中以及強制處分的運用，本來涉及的基本權就不會僅有單一面相，故本文於審查域名扣押之合憲性時，不會僅專注於第四修正案中扣押之規定本身，亦將關注其他基本權干預之憲法要求。

在域名扣押中，除財產權之干預外，美國法上討論的另一重點便是扣押與美國憲法第一修正案所保障之**言論自由**[151]，兩者間之緊張關係。不論是停止解析，還是移轉、註銷域名登記，都是對行為人的網路言論進行限制。既然確立了域名扣押涉及複數基本權限制，且其中尤以財產權及言論自由為主要限制，將接續討論此限制之合憲性。

附言之，域名扣押所涉及之言論，通常係與犯罪相關，如兒童色情或侵害著作權之影音。而在美國憲法上，誘導、促進犯罪之言論是否為言論自由之保護領域，有所爭議。有一說認為此類言論不受憲法保障，故政府自得限制之，無違反第一修正案之問題。惟另有認為，此仍屬於第一修正案所保障之言論，只是保障密度較低[152]。惟不論如何，即便域名扣押所限制者大多屬非受憲法保障之言論，但不容否認於個案中終究會存在是否為受保障言論之邊界案例，以及於執行時基於技術之侷

---

148 同上註，頁 315-316。

149 Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, Stanford Tech. L. Rev. 40, 59 (2008).

150 Quantity of Books v. Kansas, 378 U.S. 205 (1964).

151 Alex Abdo, *Why Rely on the Fourth Amendment To Do the Work of the First?*, 127 Yale L. J. Forum 444, 444 (2017).

152 ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 1018-19 (4th ed., 2011).

doi:10.6342/NTU202302025

限，也勢必會對其他合法言論造成干預。是以，本文以為在此仍有針對言論自由之干預之進行合法性審查之必要。

第二項 憲法上要求

由於美國法屬英美法系，其法律制度之概念上並無所謂法律保留制度。是以，即便屬於立法者未事前授權之偵查手段，只要其對於基本權之干預符合憲法上之要求，即屬於合法之公權力行為。

一、財產權干預—第四修正案扣押規範

首先，如果政府有目的地干擾個人對其私有財產的控制權，即構成了所謂的「扣押」。但凡該當扣押行為，則必須符合美國憲法第四修正案之要求，即扣押執法機關須具備發動扣押之相當理由，附上宣誓書（誓言或代誓宣言）向法院聲請扣押令狀，且該令狀必須具體的說明搜查地點和扣押物。

透過上文所說可以知悉，美國法是將暫停域名解析之行為置於扣押之下討論，且已經由實務長年運作。然而此技術運用究竟是否該當「扣押」，於過去並非毫無疑義。尤其，若認為確實屬於第四修正案所指之扣押行為，則偵查機關必須遵守令狀原則，其於發動偵查前所需聲請之令狀，也需要符合聯邦法上（美國法典，United States Code）扣押、沒收之規定，始得聲請之。換言之，聯邦法之規定乃第四修正案之具體化規範，故下文亦將以此作為爭議討論之主軸。

探查美國法上扣押與沒收之相關規範，皆未明確將域名列為執法標的，民、刑事沒收之標的僅以概括的財產（Property）表示。究竟此種通知域名註冊管理機構協助轉址、變更域名登記人之執法手段，是否符合「扣押」之定義，以及域名是否屬於「扣押標的」，以下詳述之。

（一）域名為實施或幫助犯罪之財產，得扣押及沒收

美國法典上得沒收之財產，包括用以實施或幫助犯罪者（Facilitating Property）[153]，而域名之使用有助於該等犯罪之規模擴大或是遂行。是以，域名乃一對於不法

[153] 18 U.S.C. §981(a)(1)(B).

doi:10.6342/NTU202302025

行為有所助益之工具，於實體法上屬於得沒收之財產。而既然得沒收，依 18 U.S.C. §981(a)亦得扣押之。

實體法上屬於得扣押之犯罪工具，惟程序法上域名是否屬於扣押標的？

（二）域名是否為「扣押標的」？

蓋傳統扣押之標的大多為實體物，惟隨著科技進步與犯罪型態之改變，有越來越多的財產是以無形的型態存在，然此類無形物、權利，是否屬於扣押之標的不無疑義。如今，與網路犯罪習習相關，以一串網址作為表現形式的域名，亦存在相同的困擾，其是否可以作為得扣押之「財產」尚待釐清。

1.否定說—域名之使用乃與註冊服務密切關聯之契約

較早期之美國實務見解係採取否定之見解。美國維基尼亞州最高法院於 Network Solutions Inc. v. Umbro International, Inc.[154]案（以下將 Network Solutions Incorporation 簡稱為 NSI 公司）中，認為域名並非與著作、專利權等相同概念之無體財產權；且亦非於強制執行程序中屬於債務人、可供扣押、並由第三人向債務人負有責任之財產（Garnishable Property）。是以，於本案認為域名**非**屬於得扣押、執行之標的。

其中，後者所謂可供扣押且由第三人向債務人負有責任之財產，依先例係將系爭財產限縮於「可以完全不顧第三人意願，而由法院逕為扣押並公開拍賣者」，故向來將「服務給付契約」排除於可供扣押之範疇。本案原因事實係 Umbro 公司請求扣押並強制執行註冊於 NSI 公司之侵權網站域名，法院已認定存在侵權事實，且 Umbro 得向侵權人之財產強制執行以取得損害賠償。惟多數意見認為，侵權人與 NSI 公司之間的域名契約，域名使用之權益與域名註冊服務密不可分；從而，域名契約非屬得不顧第三人意願便加以扣押、拍賣、取償之財產。是以，雖然 NSI 公司對侵權人負有給付域名使用服務之債務，但 Umbro 不得扣押系爭債權[155]。

---

[154] Network Solutions Inc. v. Umbro International, Inc., et al, 529 S.E.2d 80 (Sup. Ct. Va., Apr. 21, 2000).
[155] 蔡志宏，參前揭註 25，頁 202-203。

doi:10.6342/NTU202302025

本案見解認為域名不具有易於確定之價值，且與無體財產權之性質不相似，故將域名之財產性質定性為「提供域名使用之契約」，再另外以域名使用權與註冊服務之不可分，認為域名非屬扣押標的。

但域名使用權與註冊服務是否為密不可分，不無斟酌餘地。於本案中便存在不同意見，認為域名契約中，域名受理註冊機構與域名註冊人之間不存在特殊配對關係，故扣押域名時，無考慮受理註冊機構意願之必要。準此不同意見推論出，域名乃可供扣押、拍賣之財產。於此時便開始有見解傾向認同域名得作為扣押標的。

嗣後漸漸的有法院嘗試以不同視角切入此議題，其等將域名定性為財產權，以財產權而非契約之觀點討論。此轉變係源於兩個理由：1.早期域名系統發展時，域名的申請與發給無須繳納費用。故於此類案型中域名使用人難以主張存在契約權利。2.在英美侵權法中，對於侵奪他人財產之侵權型態有賴以侵占（Conversion）作為訴因來請求，而契約權利並非侵占訴因。是以，若於個案將域名定性為契約，則會使得域名使用人無法主張權利之窘境，難認公平。故法院為避免權利保障落空，後續傾向將域名作為財產權保護[156]。

2.肯定說—域名為財產權

(1)無體財產權說—Kremen v. Cohen

在 Kremen v. Cohen 案中，掀起爭議的域名，便是前述免費註冊之情形。本案之原因事實係 Kremen 在 NSI 公司註冊了一域名 sex.com，嗣後 Cohen 卻以一封偽造的郵件假冒 Kremen，以此請求 NSI 公司變更域名註冊人為 Cohen，Cohen 便因此取得 sex.com 的域名使用權。

Kremen 在訴訟中主張，NSI 公司未向其確認便直接移轉域名的行為，乃構成侵權行為，使其受有喪失域名使用之損害。法院在此面臨的主要問題便是，Kremen 免費註冊域名，是否可以認定 Kremen 與 NSI 公司間有契約存在？又當認為兩人間

[156] 同上註，頁 203-204。

doi:10.6342/NTU202302025

不存在契約時，系爭域名使用權可否認定為財產權，而得作為侵占訴因，使 Kremen 順利向 NSI 公司請求損害賠償？

就此，法院認為免費註冊域名的行為難認 Kremen 與 NSI 公司間存在默示契約合意，因而 NSI 公司並不負有持續給付 Kremen 使用域名之義務。但法院不否認 NSI 公司之不當行為確係造成了 Kremen 喪失域名使用之損害。在此，本案認為所謂財產係一廣泛之概念，包含「每一種無形的利益和易於擁有或處置的特權」。並引用三階段測試來判斷域名是否屬於財產權：1.存在能夠精確定義的利益 2.必須能夠獨占或控制 3.所有人得以建立排他性。

首先，許多註冊人會投入大量時間與金錢來開發、推廣使用域名的網站，網站的流量及知名度等都可以用於衡量域名之價值。換言之，域名是一種可以明確定義的利益，雖然欠缺實體，但就像就像公司股票一樣，可以透過市場行情、投資與獲利程度定義價值。再者，域名註冊人可以透過域名的使用與控制，決定域名所導向之網站 IP 位址，且理論上只有註冊人可以決定域名之指向。是以，可謂註冊人能獨佔與控制域名。最後，由於每一個域名在網路世界中都是獨一無二的，因此只有註冊人可以使用及移轉特定域名，域名的使用是具有排他性的。綜上，法院於操作三階段測試後，認為域名滿足上述標準，因此肯定域名乃一無體之財產權[157]。

於認定域名為無體財產權後，法院另外透過解釋論，認為域名乃一電子文件，以此認定域名符合侵占訴因中無體財產權須與有體物合併或聯繫之要求[158]。是以，由於域名屬於個人的財產且有受保護之必要，並具備與有體物之聯繫，最終法院認為本案 Kremen 得向 NSI 公司請求損害賠償。

雖然上述案例與域名之扣押看似無關，惟本案實際上確立了域名之法律地位為無體財產權。是以，將案例置於本處討論之意義，係在於肯定域名作為財產之一種，在運用扣押規範時，自然也得以此概念認為域名屬於扣押標的。

---

[157] Kremen v. Cohen, 325 F.3d 1035 (9th Cir. 2003).

[158] 傳統之侵占訴因，只包含有體財產權。但隨著無體財產權概念之擴大，此標準也漸漸鬆動。大多的美國法院承認無體財產權在與有形物體具有聯繫時（如以書籍形式表現的著作權），亦得作為侵占訴因。更有甚者直接認定無體財產權與有體財產權於侵占訴因之討論上無須特別區分。

doi:10.6342/NTU202302025

然而，另有一見解乾脆的將域名建構為有體財產權，而直接的肯定域名得作為侵占訴因以及財產法中得移轉之標的。

(2)有體財產權說—Jubber v. Search Mkt. Direct, Inc. (*In re* Paige)[159]

在 Kremen 案中，以無體財產權結合有體物，建構侵占訴因來解決域名遭到不法侵奪之問題。在侵占訴因要求必須以有體財產權為限時，便會再度遭到問題[160]。此即在 Jubber v. Search Mkt. Direct, Inc.中猶他州法院所面臨的困境。由於 Kremen 案是維吉尼亞洲之法院判決，並不構成猶他州法院之前案；且依猶他州財產法之規範，即是將侵占訴因限制於有體財產權。為了解決問題，在本案法院便採取域名為有體財產權之說法。

本案之原因事實係，破產者 Paige，於申請破產後將其註冊之域名移轉登記給他人。因而負責管理破產財團之破產管理人向受移轉人提請訴訟，主張申請破產後之財產移轉行為無效，該受移轉人應返還域名予破產財團，以便債務之清算。並認為 Paige 移轉域名乃不當行為，使財團受有域名之損失，故向其請求侵權行為之損害賠償。

如上述，本件又遭遇了域名是否為侵占訴因之爭議，並且基於猶他州法律之規定，只有將域名認定為有體財產權，原告才有請求損害賠償之餘地。在此，法院以下列理由建構了域名之有體財產特性：A.域名是物理上存在的，其透過編碼實體的儲存於電腦之記憶體與硬碟中。B.且域名的存在可以由感官感知，並非單純存在於他人腦海中的思想。C.現實上域名也能夠以密碼或其他加密手段排除他人使用。

據此，本案法院認定在 Paige 申請破產後，依法便喪失對於屬於破產財團之財產處分權。因此，其移轉域名即屬符合侵占訴因之侵權行為，受移轉人應將系爭域名返還於破產財團之破產管理人[161]。

159 Jubber v. Search Mkt. Direct, Inc. (*In re* Paige), 413 B.R. 882 (Bankr. D. Utah 2009).
160 蔡志宏，前揭註 25，頁 204。
161 同上註，頁 205。

doi:10.6342/NTU202302025

學說上有肯定本案法院結論者，但認為其說理有誤。有論者指出法院將域名與網頁之概念混淆了，域名與網頁就如同索書號與書本之對應關係，然實體存在者係書本，而非索書號；網頁確係實體存在於電腦硬碟中，但域名只是索引網頁過程中之指引，法院將其作為物理性之存在實屬有誤[162]。學說透過其他方式說理何以域名應歸類為有體財產。

論者不否認域名係無形之存在，但其認為應將域名作為有體財產權看待之理由有三：A.首先，域名與有體財產權具有較多相似之處。蓋域名與一般的無形資產不同，它具有固有、內在之市場價值，即便域名經過移轉，被指向不同的網站，仍然有自己獨立於網站的價值，與股票價值係附隨於公司之營運、營收有所不同。另外，域名權利之存在是被公開的，可以隨時透過 WHOIS 系統[163]查詢域名之註冊狀態；反之，論者認為大部分的無體財產之存在是非公開、不易確認的。因此，域名相較於無體財產，與有體財產具有較多相似的性質[164]。B.透過反網路搶註消費者保護法（Anti-cybersquatting Consumer Protection Act，ACPA）對物訴訟之管轄規定[165]，係以域名之註冊管理機構所在地為管轄，而非所有人所在地。此特徵亦與不動產等有體財產之管轄設計相似，可見立法者亦有意將域名作為有體財產[166]。C.最後，基於公共政策之考量，若將域名定性為有體財產權，則可以使各州的侵占訴因判斷趨於一致，以免形成部分地區成為人民規避域名侵權之勝地[167]。

本文對於域名本身之財產性質為何亦有個人見解，惟筆者之論點係以我國法之財產概念思考域名定性之問題，故將此議題置於第五章第一節討論。不論域名係有體或無體之財產概念，只要屬於財產，便是肯定它得作為扣押之標的，因此，在後續域名扣押開始盛行後，可以想見美國法院之主流見解係採取域名扣押肯定說。

---

162 Daniel Hancock, *You Can Have It, But Can You Hold It?: Treating Domain Name As Tangible Property*, 99(1) Kentucky L. J. 185, 200-02 (2010).

163 WHOIS 是一種網際網路協定，用來查詢域名註冊人的相關資料，註冊人、聯絡方式、域名建立的時間等。而網路上也有許多 WHOIS 資料庫可供查詢。

164 Daniel Hancock, *supra* note 162, at 203-05.

165 15 U.S.C. §1125(d)(2)(A).

166 Daniel Hancock, *supra* note 162, at 205-07.

167 *Id*, at 208.

doi:10.6342/NTU202302025

3.全面肯定—Operation In Our Sites 行動

在前面提過由 ICE 發起的數次 Operation In Our Sites 行動中，各法院並未將域名排除於扣押、沒收客體之外，而拒絕核發扣押令狀[168]。該行動自 2010 至 2014 年間已扣押了 2,700 多個域名，足見自 Operation In Our Sites 行動發起後，各地的聯邦法院廣泛的肯認域名乃得扣押、沒收之客體，乃對域名作為扣押標的之全面肯定。

在美國法院普遍承認域名為「財產」之概念，而屬於得扣押之標的。此時生出另一疑問，此種請域名註冊管理機構、受理註冊機構協助將域名轉址、變更註冊人為國家，使原註冊人無法繼續正常使用域名之手法，似乎與傳統的扣押意義不同，是否符合扣押之定義呢？

（三）是否符合「扣押」定義？

如上所述，針對域名的扣押執行，「移轉域名」係將域名登記之 IP 位址，更改為美國聯邦政府網頁，並在網站上宣示網頁因涉違法行為而扣押其域名；「停止解析」則是使網路使用者無法正常的解析到非法網頁 IP 位址。此種現實上，沒有實體物之占有移轉是否可以稱為扣押？並非無疑。

如前所述在 1960 年代後，美國實務將扣押與搜索之重點置於隱私權之限制，然而，此類見解在針對無實體物之扣押（無形扣押）時，卻又矛盾的將焦點重新關注於財產實體之剝奪。例如，在 United States v. Jacobsen 一案中[169]，便對扣押之意義進行闡釋。本案法院認為，所謂扣押，係指「國家對於系爭財產的個人**占有**利益，有意義地加以干涉」[170]。系爭見解仍將扣押與財產之「占有利益」併同討論，但這種觀點遇上無形財產時，便會出現問題。

舉例而言，便有法院認為複製文件並未干預行為人對於文件原本的占有，因此不屬於扣押[171]。雖然在這類案件中，通常可以運用取得資料的前行為乃「侵害合理隱私期待的非法搜索」來排除證據。但隨著科技進步，越來越多的資訊、數據取

---

168 陳昱奉，參前揭註 129，頁 232。
169 United States v. Jacobsen, 466 U.S. 109 (1984).
170 *Id*, at 113. “Some meaningful interference with an individual’s possessory interests in the property.”
171 United States v. Chapman, 559 F.2d 402, 407-08 (5th Cir. 1977).

doi:10.6342/NTU202302025

得不需要經過搜索才能達成，此時在未侵害隱私與財產占有利益的偵查行為，便會構成問題[172]。

政府對於「域名之移轉」或「停止解析」便屬一例。對於前者，透過美國境內的註冊管理機構移轉域名登記給國家，並將域名轉址至執法網站，此時或許還能稱為對於域名「占有」的干擾，而認屬於扣押行為。蓋所謂占有係指「對於財產的實際控制」，而將域名指向何處、以及如何移轉，都是實際上控制域名的行為；然而對於後者，則似難認該當占有利益的干預。蓋停止解析並無限制註冊人對於域名的使用，仍然可以將域名指向其指定的網站，在沒有禁止處分命令時，也仍然可以任意移轉域名登記。然而，若將占有之概念擴大，其實對於財物使用效果的干預，某種程度上也構成了對所有權人對於財物支配與控制的減損。是以，在此觀點下，套用 Jacobsen 案之標準，也應認停止解析該當扣押。

附帶而論，學說上也有對於上述 Jacobsen 案標準之質疑，認為美國憲法第四修正案所保障之權利範圍既然不限於財產權與隱私權，也因此，應該將扣押的定義從「占有之干預」修正為「任何第四修正案保障之權利受到干預」；並亦將關注焦點從「人民財產受限制」轉移到「政府的強迫與管制行為」[173]。

而停止解析係對於域名使用效果的干預，且該干預引發了言論自由的侵害，乃對於財產的使用利益、言論自由之限制。並且，該限制乃國家違反域名註冊人之意志所為的強制干預手段。是以，在前述學說的觀點下，停止解析亦該當對於域名的扣押。就此，停止解析一方面符合「扣押」執行之定義，另一方面也須遵守憲法、法律對於扣押之程序規定。

二、言論自由干預—第一修正案

認定域名得作為扣押標的，且現行之執行技術該當扣押定義後，則尚須注意一問題，即域名扣押對於言論自由的特殊干預。與傳統扣押不同，針對域名的扣押權利侵害重點在於言論自由，而不僅僅是財產權與隱私權。

---

[172] Paul Ohm, *supra* note 149, at 46.
[173] *Id*, at 57-59.

doi:10.6342/NTU202302025

在美國法體系下，言論自由是被高度重視之基本權利，此點可由美國憲法第一修正案「禁止美國國會制訂任何法律剝奪言論自由」觀察出。且言論自由與民主實踐之關係緊密，也因而政府對於言論之管制，於美國憲政上也時常引發爭議。然而，言論自由並非全然不可限制之權利，美國法上通說對於言論自由干預合憲性之審查，係以利益權衡為依歸，應就「政府限制該言論所維護之利益」與「憲法保障該言論所帶給個人及社會的利益」兩者權衡[174]。

由此可知，美國憲法上干預言論自由之合憲性審查，與第四修正案扣押之合憲要求，有明顯之差異。兩者之審查方式不同、對於權利之保障密度亦有所區別。

美國法上便有論者提出，不應該將第四修正案對於搜索、扣押之規範，用以授權對於言論的限制。蓋在美國法上，後期多數論者主張第四修正案主要保護的法益是隱私權。而在實務操作下，保障言論自由的第一修正案，對於政府利益之要求（審查標準）通常高於第四修正案；且第四修正案往往只關注對於個人權利的侵害，而不若第一修正案的審查會關注對於**整體社會的影響**與**微小侵害的累積效應**[175]。因此，論者以為域名扣押對於言論自由的干預，有違反第一修正案之虞。退一步言，即便認同對於言論得發動扣押，於比例原則及正當法律程序的審查上仍應該符合保障言論自由的第一修正案標準。

而基於美國實務上已廣泛的承認以符合第四修正案之方式發動對域名的扣押，可見其多數見解係認為無庸於全盤否認扣押對於言論自由的干預可能性。惟美國法上亦存在案例，對於涉及言論自由干預的扣押要求較嚴謹之程序者[176]。是以，美國法上對於言論所發動的扣押，多數見解係置於程序保障之層次討論，尚認為域名扣押並無逾越扣押之範疇。

---

[174] 張陳弘（2012），〈去類型化猥褻性言論之理論建構—美國法之比較研究〉，《臺北大學法學論叢》，83 期，頁 51。

[175] Alex Abdo, *supra* note 151, at 444-45; Arthur L. Burnett, *Obscenity: Search and Seizure and the First Amendment*, 51(1) Denver L. Rev. 41, 67-69 (1974).

[176] 如：A Quantity of Copies of Books, et al. v. Kansas 案，本文將於後續正當法律程序之小節介紹此案例。

doi:10.6342/NTU202302025

就此，域名得成為扣押及沒收之標的，且 DNS 過濾之使用也屬於扣押之一環，對於言論的干預亦非不得置於扣押概念下討論者。是以，以下將進一步探討涉及言論自由干預之扣押於美國法上之發展。

第三項 比例原則

本處所要討論的是，於通案性的立法層次上，利用停止解析技術對域名發動扣押，以即時減損網路犯罪損害，是否為符合比例原則之手段。本文此處將區分兩個面向討論。首先，延續上一項所提及的言論自由干預及第一修正案之議題，下文將以美國法上利益衡量之觀點，審查域名扣押對言論自由干預之面向；再者，本文將關注停止解析作為域名扣押執行手段之妥適性。如前所述，於美國法上對物扣押、沒收之標的，主要係針對境內註冊域名，只需要請求美國境內之註冊管理機關協力配合域名轉址即可完成，故本文未能搜尋到於刑事犯罪偵查中實施停止解析技術之案例。惟於網路管制法案之爭議，則有法院曾探討過停止解析、IP 位置過濾與 URL 過濾等手段間選擇與必要性之議題，故將以此案例作為美國法對於停止解析技術之比例原則分析。

域名沒收與傳統上犯罪工具之沒收，差別僅在於域名為無形財產，僅有在執行方法上可能有所差異。是以，財產權干預之面向上，針對域名發動的扣押與傳統的犯罪工具扣押，於比例原則審查階段並無特殊性，故本文不另外處理。另一方面，由於第四修正案對於扣押之發動僅以相當理由、令狀原則作為門檻，雖比例原則也應被考量，惟在域名扣押之議題上，爭議之處仍是在於執行手段之選擇，即 DNS 過濾是否為最適切之手段，此為本項所探討的第二個問題。

一、言論自由干預之審查

承上言，域名扣押與傳統扣押明顯差異之處，係在言論自由之干預面向。然而，進一步思考，其實過去也不乏有案例於扣押時涉及言論自由干預。是以，扣押言論素材並非新興議題，也不是域名扣押所單獨面對的。因此，本文在此欲援引相關爭議之案例，處理域名扣押之比例原則審查問題。

doi:10.6342/NTU202302025

在美國法上關於涉及言論的扣押已有諸多案例發展，以下整理美國法院判決，對於「涉及言論干預之審前扣押」，於合憲性審查上所持有之態度。

首先釐清，檢警針對言論素材發動扣押之目的，係為留作證據亦或阻止言論發表。若係前者，雖仍屬於對於言論自由之干預，惟其並非對言論內容之審查，且作為證據僅需要留存單一複本，並無禁絕言論進入市場之特性，對言論自由之干預較輕微，且目的係為達成國家追訴犯罪之重大公益，通常此類型扣押於比例原則之審查上較無爭議。而後者則於美國實務上有眾多討論，蓋其係針對言論內容所為之審查，且目的是阻止言論進入市場，有國家選擇言論之特徵，容易引發寒蟬效應，對言論自由屬於較大之干預手段。

本文所探討之域名扣押，其實就是國家依據言論之內容，阻止該言論進入大眾視野之手段，**目的並非在於留存證據**，蓋若欲留存證據有其他更輕微之手段，如網頁截圖、保存造訪網頁之路徑等。且國家所扣押之域名，通常是系爭言論之唯一載體，是以，域名扣押所涉及的是上述後者，即國家於針對「言論內容」審查並禁止。此種針對言論內容發動之審前扣押，於美國法上之主要爭議，係是否構成言論之事前限制（Prior Restraint）[177]？蓋此涉及審查標準之擇採，若是屬於事前限制，通常國家之管制行為會被推定違憲（採取嚴格審查，目的須是追求迫切之政府利益，且手段與目的間須符合嚴密剪裁[178]），政府必須提出具有正當性之管制理由[179]。

（一）言論之事前限制？

關於對言論素材發動審前扣押與沒收，是否會造成言論之事前限制之爭議，首要處理的是「事前限制」之定義為何？事實上，事前限制之定義是模糊的，難以簡單的用「事前審查」或「事後處罰」來區分。畢竟不論是審查或處罰，都是在言論發生之後才會發動；且審查或處罰之法規範，都是在言論發生前即存在，並對言論之發生產生嚇阻作用。

177 ERWIN CHEMERINSKY, *supra* note 152, at 980.
178 *Id*, at 986.
179 *Id*, at 978.

doi:10.6342/NTU202302025

在美國法上對此較為清晰的定義，係於 Alexander v. United States 案，「對於言論自由之『事前限制』，係政府以行政或司法命令，在言論發生前事先禁止」[180]。而美國法院實務也通常將「阻止言論發表之扣押」，以事前限制論[181]。常見之案例事實舉例：檢警於審判前對言論素材（書籍、報章雜誌）的大量複本發動扣押與沒收[182]。

然而，在 Alexander 案，雖操作相同之標準，卻認為沒收電影放映商之色情電影係事後對於違法言論載體之剝奪，而非言論發生前之禁止，故不屬於事前限制。可見即使有上述定義，但言論「發生」之時點，仍難以判斷。而也可以發現，於部分案例法院之所以傾向將言論載體之扣押與沒收，判定非屬言論自由之事前限制，係為避免提高審查標準，因而必須將政府之管制行為推定違憲。

惟此並非解決問題之根本之道，即有論者質疑，是否有必要將言論之事前限制，採取如此高的審查標準。其分析了主張事前限制為對言論自由較嚴重侵害之論點，並一一提出論理不足之處。首先，人們通常認為事前限制會使表達於有機會被聆聽、進入言論市場前，即被排除在外，將使言論市場之想法縮減。然而，論者認為當事後之懲罰足夠嚴厲時，也會導致相同之情形，人們的言論同樣不敢表達，無法進入言論市場。反之，審查制度為人所之時，反而會讓聽眾於聆聽消息時抱持懷疑態度，創造想法[183]。再者，有認為事前限制比起刑事定罪更容易發動，因此有較多的濫用疑慮，故應該對事前限制採取較嚴格之審查。此說或有道理，比起程序簡便的司法、行政命令，刑事起訴、審判、處罰之過程緩慢。然而，此說法未注意到，光是對於言論發表者發動刑事程序本身便是一種處罰，具有威嚇效果，且漫長的程序亦耗費心神、時間成本，而起訴的發動不若審判程序嚴謹，亦有被濫用之可能[184]。綜上，

[180] *Id*, at 979; Alexander v. United States 509 U.S. 544 (1993).
[181] *Id*.
[182] Quantity of Copies of Books v. Kansas, 378 U.S. 205 (1964).
[183] Martin H. Redish, *The Proper Role of the Prior Restraint Doctrine in First Amendment Theory*, 70(1) Virginia L. Rev. 53, 59-60 (1984).
[184] *Id*, at 61-63.

doi:10.6342/NTU202302025

論者以為，從根本上就不應該將「事前限制」採取推定違憲之高標準，而是回歸政府所追求之利益，與個案所限制之權利間，是否衡平[185]。

是以，撇除事前限制推定違憲之高審查標準，純粹回歸「事前」之判斷標準，審前扣押、沒收表達性材料，其目的即是在於阻止特定言論向外界的傳遞、發表。而當言論接收者無法取得相關資訊時，即是對於言論發表之限制，故應屬於所謂的言論事前限制。

如前文所述，本文以為域名扣押與表達性材料之審前扣押與沒收屬於相當類似之概念，故將表達性材料的審前扣押，作為討論與比較分析之對象。而下文將延續表達性材料扣押之事前限制議題，爬梳美國法院在此議題所採取之審查標準。

（二）表達性材料扣押案例之發展

Marcus v. Search Warrant 案[186]，其案例事實係一名警察於審判法庭宣誓，聲稱雜誌、報紙和書籍的批發商以及零售報攤，出售「猥褻」出版物。其經由單方程序向法院聲請令狀，法院在沒有被扣押人參與程序，甚至沒有看到任何相關出版物之情況下，簽發了搜索令，授權警察搜索被告的住所並沒收所有猥褻出版物。且系爭令狀並無指明扣押標的，而是交由警察判斷何為猥褻物，並逕自全數沒收。

於 Marcus 案中，最高法院指出扣押言論素材時，必須採用「嚴格」之程序，保障相對人之正當程序，且法院須考慮對言論自由限制之效果，始得為之。而在相似案例事實之 Quantity of Copies of Books v. Kansas 案[187]及 Heller v. New York 案[188]，最高法院則更進一步的指出所謂嚴格程序，係須於扣押前經過「對抗性聽證（Adversary Hearing）」程序，即於扣押前要使相對人有於法院提出抗辯之機會，並經由司法裁決。本案更將對言論素材所發動之審前扣押與沒收作限縮，其目的僅能是為了調查猥褻與否之爭議。

---

185 *Id*, at 99-100.
186 Marcus v. Search Warrant, 367 U.S. 717 (1961).
187 Quantity of Copies of Books v. Kansas, 378 U.S. 205 (1964).
188 Heller v. New York, 413 U.S. 483 (1973). 本案之事實係被告於其電影院放映色情電影，而於起訴前其影片即被沒收。

doi:10.6342/NTU202302025

在 Lo-Ji Sales, Inc. v. New York 案[189]，其案例事實係法官簽發扣押所有電影及書籍之令狀。而經由最高法院審查後，另外提出，當扣押標的涉及表達性材料，即應**推定**該材料受到第一修正案之保護，則法院不得僅以第四修正案授權扣押之。

由以上案件可以發現，對於表達性材料之審前扣押，法院於審查時，沒有特別提及言論自由之事前限制，以及其於比例原則上所採之嚴格標準，故本文在此無法援引判斷美國法上對於域名扣押之比例原則操作，是否係以言論自由之事前限制，採取嚴格審查標準。

惟可以發現，美國法院處理表達性材料扣押時，係將焦點置於程序參與之保障。該等判例認為，依據第一修正案，對於言論自由之事前限制需要有正當程序保障，始符合憲法保障言論自由之精神。而透過上述判決之整理，其於表達性材料之扣押與沒收，所要求之程序有「對抗性聽證程序」，即被扣押人有於扣押前參與程序、表達意見之機會；以及「司法裁決」，即透過中立、客觀之法院，審查並決定是否扣押。此程序保障於域名扣押中是否是於套用以及如何實踐，將於正當法律程序之層次詳加討論。

而本段落之下文將處理比例原則層次之第二個問題，即實施 DNS 過濾作為域名扣押之手段，是否符合比例原則？

二、DNS 過濾

利用停止解析作為網路言論管制手段將有可能引發違反比例原則之問題。蓋依本文第二章的技術介紹，曾提及存在其他技術亦可以達到防止使用者造訪網站之效果，則美國法上便有案例探討採取 DNS 過濾是否為對人民權利最小侵害的手段；以及相較於對於人民權利之限制，手段是否符合相當性等問題。

（一）Center for Democracy & Technology v. Pappert 案

2002 年 2 月，美國賓夕法尼亞州通過了網路兒童色情法案（Internet Child Pornography Act）。該法案要求 ISP 業者協力阻止「使用其網路連線服務者」造訪

[189] Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979).

doi:10.6342/NTU202302025

兒童色情網頁，即在檢察總長通知 ISP 業者須禁止訪問之網頁後，ISP 業者須於五日內阻止該網頁之連線服務，若否，ISP 業者將受到刑事起訴，此為美國網路管制中著名之 Center for Democracy & Technology v. Pappert 案[190]。

此法案於實施上有幾個困難及爭議之處，首先，並非所有的 ISP 都是一樣的，有的 ISP 係提供網站託管服務，人們可以將網站架設於該業者之平台，而使他人可以造訪網站，但有的 ISP 僅僅是協力提供網路連線、訊息傳遞。即使是前者，其限制訪問特定網頁的能力也是有限的，遑論後者。是以，網路上絕大多數網站不在 ISP 業者的控制之下，任何一個單獨的 ISP 都沒有能力或權力要求另一個 ISP 從其服務器中刪除禁止的內容或阻止特定網站的訪問。是以，此法案毋寧是課予了 ISP 業者難以實踐之義務。而實際上在法案生效後不久，多個 ISP 業者向檢察總長辦公室報告，難以遵守法院命令之擔憂，尤其刪除期限僅有僅僅五天。

再者，依法案之規定，檢察官可以單方地向法院聲請刪除命令。法院核發命令之過程，是在 ISP 業者及個人網站不知情的情況下進行的。且核發命令後，僅 ISP 會收到通知，協助執行命令並關閉網站之訪問，而毋庸使網站架設者知悉。換言之，網站的架設者和那些意外被封鎖的人始終不知情其等的網站已被限制訪問，事後也無法質疑該行為，程序保障似有不足。

最後，基於網路無國界的特性，ISP 業者於執行法院命令時，無法將網站的遮蔽僅限於賓夕法尼亞州之公民，也會產生管轄、審判權越權之問題。另一方面，ISP 業者通常係使用 IP 過濾和 DNS 過濾來執行命令，而基於固有的技術限制，也導致了大量無辜和無關的網站遭限制，構成過度封鎖。此也使 ISP 業者擔心，如果他們在沒有適當權限的情況下不慎阻止網站的訪問或刪除了網站，要對客戶承擔法律責任。

基於上述問題，本法案被聲請釋憲，爭論的主軸係法案是否構成了對言論自由的非法限制，蓋雖法案的目標是對兒童色情言論之管控（此言論於美國法上屬於不

[190] Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606.

doi:10.6342/NTU202302025

受憲法保障，或僅受到低度保障者[191]），然而在實施法案時，事實上同時壓制了其他言論之表達，故法院處理時著重於執行手段之選擇。

（二）各式手段分析

由於法案並未特別指定 ISP 業者於執行命令時，要採取何種手段來阻斷網站之造訪，故法院分別討論了前述之三種技術，即 IP 過濾、DNS 過濾以及 URL 過濾。

於技術章節已經就三者之技術內涵為簡介，故就此僅將法院之結論節錄。IP 過濾最大的問題就是過度封鎖之疑慮，單個 IP 位址可以由許多不同的網站共享。有許多公司提供虛擬託管之服務，換句話說，個人用戶可以將自己的內容放置於公司網站之子頁面。因此，如果被阻止的 IP 位址是提供託管服務的 IP，不論是否涉及非法言論，所有子頁面也將一同被阻斷。而在大型託管服務的情況下，被阻止的站點數量可能會達到數千個。此外，IP 位址可以在不更改 URL 的情況下定期更改，因此阻斷特定 IP 對網頁造成的阻斷效果也不甚明顯。

DNS 過濾的主要問題亦如前述，網路使用者有多種方式可以繞過境內 ISP 業者的 DNS 解析，且由於域名可以更改，卻缺乏通知新域名所有者之程序，此舉可能導致無涉非法、新建立的網站，也一同被封鎖。

URL 過濾本身有被某些 ISP 業者運用，作為提供「家長管控孩童瀏覽」之服務。然而其難以按照賓夕法尼亞州法案所需的龐大規模進行 URL 過濾。工程師證稱，在整個網路空間內實施 URL 過濾將需要耗費數年時間，且 URL 過濾將使 ISP 業者之系統帶來龐大壓力，需要購買大量設備來擴展網路，成本極其昂貴[192]。換言之，在經濟上無法購置基礎設備時，ISP 業者僅能犧牲大量性能來實施 URL 過濾，這將使得網路連線速度大量下滑。而網路連線之速度通常是網路使用者們決定服務提供商的關鍵因素，實施 URL 過濾將使 ISP 業者之競爭力下降。

---

[191] 美國法上對於言論自由之保障，學說上「絕對保障論」、「利益衡量論」模式，前者係將言論區分為是否受到憲法保障，後者則是認為言論接受到憲法保障，僅是有保障密度高、低之落差。是以，低價值言論是否受到憲法保障於美國法上有所爭議。詳參張陳弘，同前揭註 174，頁 50-52。

[192] 據該案之證人工程師，其稱高達建置成本或可高達數百萬美元。

doi:10.6342/NTU202302025

將言論管制之重擔置於提供言論流通之平台業者，對政府而言，是一個以最小成本，對言論進行最大管控的方式，蓋只要中介商協力阻斷，言論就無法自由的流通，此種管控方式國家甚至不用確認言論發表者、接收者分別為何人。從執法面來看，此舉確實是有效阻斷網路犯罪之方式，尤其網路世界的匿名性，不從中介商切入限制，檢警機關實際上難以追訴犯罪。然而，此舉卻不是對無辜企業與個人最低程度之干擾，尤其當立法者試圖通過法律強制使用從經濟或技術角度來看都不可行的技術來幫助執法時，問題就開始了。

在 United States v. Playboy Entertainment 案中，1996 年《電信法》第 505 條要求有線電視運營商以加擾或其他方式阻止色情頻道之播放。否則，節目必須限制在未成年人不太可能看電視的深夜放映。由於加擾技術並不完美，偶爾會發生信號洩漏，使非訂閱者能夠在幾分鐘內看到成人頻道的圖片或聽到音頻。是以，基於技術和經濟的限制，有線電視業者大多選擇時間限制之方案。

在此案中，法院深入探討了加擾技術與第一修正案之關係，明確指出立法機關不能要求業者耗費巨額資金去使用特定技術，以致破壞行業競爭。當國家和公民個人可以使用其他侵入性較小的控制方法時，尤其如此。綜上，美國法院的立場是立法者不得全面禁止色情內容，也不能在存在較小限制手段的情況下使用過度影響人民權利之技術，尤其是該言論的管制可以由用戶端自行管控時（如家長可以自行管理兒童觀看之頻道），更是不得逕將壓力轉嫁予中介者。

總而言之，本案認為 URL 過濾雖較為精準、對人民權利影響較小，但難以期待，立法者也不得要求業者付出高額成本執行，而妨礙產業之市場競爭；而 IP 過濾、DNS 過濾皆有過度封鎖之疑慮，其中又以 IP 過濾較為嚴重。DNS 過濾（停止解析）雖是其中較佳之手段，但以當時的技術，實施該等過濾仍會對合法言論產生過多之額外限制，整體而言對於法案欲達成保障兒童免於色情接觸之目標，不符比例，故法院最終認為系爭法案違憲。

doi:10.6342/NTU202302025

三、小結

在比例原則層次之討論，觀察美國實務見解，於涉及表達性材料之扣押，是否涉及「言論之事前限制」有所爭議，惟即便認為屬於事前限制，也未以推定違憲之嚴格標準操作比例原則之審查，而是將審查重點置於程序保障之充足與否討論。故本文以為在犯罪預防、偵查時，由於所涉言論通常是非受憲法保障者，故即便是為阻斷言論發表所為之強制處分，也不會採取嚴格標準之比例原則審查。而是在法院處理言論是否應扣押之爭議時，應讓受處分人有表達意見之機會，以更公正地達到確認言論受憲法保護與否。是以，在美國法上，扣押表達性材料通常並無引起比例原則之爭議。反而較易引起爭議者係前階段之國家立法，即國家將特定言論列為犯罪之行為。故依實務見解，域名扣押於美國法上是一符合比例原則之強制處分。

進一步討論的是，以何種手段作為執行域名扣押之方式，始符合比例原則。在 Pappert 案中，認為 URL 過濾之精準度最為妥適，但立法者不得要求 ISP 業者負擔高額成本執行 URL 過濾。而 IP 過濾及 DNS 過濾，以當時的技術而言，其過度封鎖的比例太高，若以此作為執行言論管制之手段，即有違反比例原則之風險[193]。不過，本文在此須提醒，Pappert 案之時空背景為 2004 年。於將近 20 年後之現在，技術已有大幅之進步（詳參本文第二章之技術討論），故同樣屬於 DNS 過濾的停止解析（DNS RPZ）其過度封鎖之程度已大幅下降，不可以此案之結論即跳躍式的否定停止解析之使用，在此援引本案僅是為參酌法院之論理。

第四項 正當法律程序

透過上述案例，可以知悉美國法上對於涉及言論之扣押，係著重於程序保障之充實與否，作為是否違憲之論據。故本文接續前揭討論，於本項探討域名扣押之正當法律程序，以及其於美國法上所面臨之爭議。

[193] 法院指出，為了遮蔽不到 400 個的兒童色情網站，使用當時的技術卻可能同時關閉了超過 100 萬個無辜的網站。

doi:10.6342/NTU202302025

在 Pappert 案[194]中，法院認為僅有通過對抗性聽證程序的司法裁決才能確保裁判對言論自由的充分考量，是以，只有透過司法裁決的程序才足以充實國家對言論自由施加**終局**限制之合法性。正如 Quantity of Copies of Books v. Kansas 案及其後續之判決，皆明確的表示，在國家行為涉及言論之事前限制時，政府必須符合最低限度之正當法律程序，即「必須於事前向受影響的一方發出通知，並讓公正的第三方有機會發表意見」。

且不僅僅在言論自由之干預面向有正當法律程序之要求，依據美國憲法第十四修正案第一款，「不經正當法律程序，不得**剝奪**任何人的生命、自由或財產」，故本案法院在財產權干預之面向上，亦認為對於域名使用之剝奪，未經過聽證程序，亦違反憲法上正當法律程序之要求。

是以，本文透過整理美國法院之實務見解，對於涉及言論自由之限制，於程序上所要求者有二，「聽證程序」及「司法裁決」，下文將分別介紹之。另外，由於聽證程序實質上是扣押審查程序之參與，故本文將之置於事中程序之層次討論。而所謂司法裁決之要求，即類似法官保留之概念，要求於干預前須經過公正第三方之司法機關個案審查，故本文將之置於事前程序討論。

併予敘明，本文於初始閱讀 Pappert 案時，曾錯誤的理解該案法院所採之見解係指凡涉及言論素材之扣押，即須採取事前對抗式聽證之司法裁決程序，始得充足對於言論自由以及財產權之保障。惟查，對於言論自由之保障，案例中提及之司法裁決要求係專指涉及**終局**限制時，例如沒收，而並未將此要求擴張至暫時性質的扣押保全程序；於財產權保障觀點，第十四修正案所要求的正當法律程序，亦係僅在**終局**剝奪財產時，始有聽證程序與司法性之要求。就此辨明之，下方將進一步細談案例結論。

[194] 在此需注意，Pappert 案所爭議的「檢方對 ISP 業者發出刪除通知」，並非對人的刑事程序。故在此處僅是援引法院對於言論自由事前限制程序保障之探討，並非逕自將案例用於刑事偵查扣押之討論。

doi:10.6342/NTU202302025

一、事前程序—司法裁決

在 Pappert 案中，賓夕法尼亞檢方在執法掃蕩兒童色情網站時，最初是向法院聲請令狀，以法院命令之方式要求 ISP 業者配合關閉網站。之後則發展出，未聲請令狀，直接以非正式的通知向 ISP 業者提出請求，完全的繞過法院。前者的疑慮在於，核發命令之程序未通知相對人參與；後者的問題則更為嚴重，直接省略司法審查之階段。是故，上述執法都被認為不足以保障相對人之憲法權利。

至於為何法院認為需透過**司法裁決**[195]始足以滿足對言論素材扣押之正當程序，在 Pappert 案或是其他相關案例，都沒有詳述其理由。本文認為可以從兩個面向切入討論。一者是關於民事扣押本身便有相對法官保留之規範（財產權干預觀點），二者則是國際上對於網際網路中介者責任之規範準則—馬尼拉中介者責任原則（Manila Principles on Intermediary Liability，下稱馬尼拉原則）。

首先，如前所述，在美國實務上通常是以民事沒收、扣押之方式處理非法網站之域名，而依 18 U.S.C. §981(b)(2)之規定，扣押係採取相對法官保留。原則上扣押前須先向法院聲請令狀，僅有例外情形得無令狀扣押。可以發現，在單純針對財產干預時，於程序上即有司法審查之要求。而在域名扣押時除了財產權外，更是對於言論自由之限制。在干預的權利更多，且所涉權利更為敏感時，將程序之要求提高至法官保留，似乎並不難理解。尤其，言論之表達有其時效性，一時的限制便有可能導致嚴重的後果，不若財產權於嗣後較容易回復原狀。再者，言論自由不僅僅是個人權利，更是關係到整個社會之溝通、交流，比起單純對財產權的干預更有可能對整體社會造成影響。最後，言論是否屬於應扣押者，比起單純的財產是否涉及犯罪，更容易在個案中產生爭議，更有必要經過公正客觀之司法判斷。是以，對於表達性材料發動扣押，本文贊同美國法院見解，認為在無例外緊急情況時，有一律經過司法審查、裁決之必要，惟此司法審查仍屬於扣押單方程序，而無需將此審查拉升至刑事裁決程序之高密度保障。

---

[195] 法院僅言「某種司法裁決」，並未指明審查程序必須為刑事、民事或行政等。是本文在此處解讀本案法院所稱之「司法裁決程序保障」，僅是認為於言論素材扣押前，應經過第三方的司法審查。

doi:10.6342/NTU202302025

馬尼拉原則是由美國著名的非政府組織電子前哨基金會（Electronic Frontier Foundation，簡稱 EFF）所領銜倡議的網際網路中介者責任之最低標準。此原則係於 2015 年 3 月由 EFF 等其他國際非政府組織所公布之民間框架倡議文件。其主要目的係在提供各國政府對於訂定網路中介者相關責任之法規或政策時有所指引或參考。馬尼拉原則之主要精神在於保障網際網路之開放與自由，並以中介者免於為網路使用者產生之內容負擔責任[196]。

其中，馬尼拉原則便有提到，除非要求下架網路內容之一方為獨立且公正之司法機關，中介者不得在未取得系爭內容上架者之同意前，對內容限制之命令或請求有任何作為[197]。是以，從此專門針對網路內容管制所訂定之原則觀察，也可以發現政府對網路言論之內容限制，亦要求於管制前須先經過司法審查。

二、事中程序—聽證程序

（一）言論自由面向

在 Pappert 案中，法案要求 ISP 業者對於網域發動過濾，即便係以執法機關向法院聲請命令之方式其程序上也欠缺使網站架設者（即被遮蔽網站之相對人）參與程序、發表意見之機會，他們無法告訴法官為什麼他們的網站不應該被封鎖，也沒有任何明確的程序可以對這樣的決定提出上訴。是以，於執法機關之通知後，系爭域名即被終局性的封鎖，是本案法院認為此欠缺「對抗式聽證」屬於違反正當法律程序之要求。惟在本案所援引之判例，Freedman v. Maryland, 380 U.S. 51 (1965)，其中有額外提及，於言論的事前審查中，進行終局性司法裁決程序之前，若進行迅速、短期、以維持現狀為目的之暫時限制，非無不可。是對域名的暫時性扣押，於言論自由保障面向，並無踐行聽證程序之要求。

故在美國法上，原則上扣押之聲請係屬於單方程序（*Ex-Parte* Proceeding），在聲請過程中，執法機關無須向法院證明該網站確有侵害他人權利或者違反刑事

196 戴豪君、余啟民主持，參前揭註 70，頁 53。

197 Jeremy Malcolm, Gus Rossi & Mitch Stoltz, *Which Internet Registries Offer the Best Protection for Domain Owners?*, https://www.eff.org/files/2017/08/02/domain_registry_whitepaper.pdf, 7.

doi:10.6342/NTU202302025

法規；而遭扣押之財產所有人，即網站經營者，並無事先就侵權與否或有無扣押域名之必要等，向法院表示意見之機會[198]。

然而，在 A Quantity of Copies of Books, et al. v. Kansas 案，最高法院則有提出特別的限制，即針對「大量」的「書籍」扣押，應經過**聽證程序**（Pre-seizure Adversary Hearing）始得核發扣押令，使受處分人有抗辯之機會，以符合第一修正案對言論自由之保障。惟需注意，於單件的書籍、期刊之扣押，則無此要求。理由主要是肯定刑事追訴過程有防止證據滅失之需求，故對於涉及不法言論之物自然也得作為扣押之標的；惟為避免以此架空第一修正案，造成言論的事前限制、過度限制，故禁止大量扣押同一標題之書本。

而將此概念延伸至域名扣押作類比，可以發現「大量」與否的判斷亦可援用，蓋該判決係針對同一標題之複數書本被大量扣押，即同一言論依附於複數實體之情形。只扣押單一書本，若其他同標題之書本仍能流通，則對於言論發表的影響較輕微且可忽視；於現實網路生態而論，網路言論通常並不只會依附於一個網頁、域名，此也是造成現行使用停止解析技術時，執法效果不顯著之問題來源。如第一章所提及之安博盒子案，即是在執法不久後便搬運網頁內容至其他的域名，基於域名註冊之便利性，或是殭屍網路技術等，可以大量、輕易地將同一言論內容反覆轉載於網路上。是以，對其中一個域名的停止解析，而非運用技術大量的封鎖相關域名，其實對於言論發表的影響也不大。因此，針對單一域名進行過濾並不足以達到封閉特定言論，使其無法進入市場流通之效果。故本文以為若將 A Quantity of Copies of Books 案之概念援引至域名扣押，於法院為封鎖言論而審查扣押命令時，也同樣須考慮是否構成大量扣押，導致言論阻絕之效果，才去思考是否應賦予相對人程序參與權，以確保言論自由之保障。

因此，於一般情況下，域名扣押中未進行對抗式聽證程序，並不理所當然的構成第一修正案所保障言論自由的違憲限制。

---

[198] 陳昱奉，參前揭註 64，頁 10。

doi:10.6342/NTU202302025

類似之案例如 Fort Wayne Books, Inc. v. Indiana[199]，執法部門根據 Racketeer Influenced and Corrupt Organizations 法案（簡稱 RICO），從一家成人書店沒收了大量材料猥褻書籍與雜誌。初審法院舉行了單方聽證會，並下達了一項命令，允許扣押被指控者的所有出版物和個人財產以及封鎖、關閉商店本身。本案進入最高法院後，最高法院維持了被告適用 RICO 指控，但認為其扣押程序是違反正當法律程序的。具體而言，最高法院認為，拿走其中一部分的資料以確認系爭標的是否屬於猥褻出版物，是被允許的，但禁止在審前「大規模」扣押表達性材料。簡言之，最高法院裁定可以扣押特定材料的單個複本，但**未經司法審查、聽證程序**而大規模沒收或銷毀材料是違憲的。法院明確表示，雖然針對違禁品通常可以在無令狀的情況下發動沒收，但這並不一定授權執法部門判斷什麼是猥褻或什麼屬於違禁品，「僅僅有可能的理由相信發生了違法行為並不足以阻止書籍或電影之流通」，需要透過相對人之說明與辯證，法院始能盡可能地瞭解事實，在資訊充足、聆聽雙方說法的情況下，審查並確認系爭表達是否屬於應禁止之猥褻品。蓋違禁品與猥褻、色情物在法律上應屬可區別，但並非一目瞭然、乍一看便能分類。

因此，綜合前述案例之討論，可以整理出結論如下：於表達性材料之審前「扣押」，只要不是對同一言論內容發動大量的扣押，即無需踐行對抗式聽證程序，僅要司法審查即可確保程序正當性；而表達性材料之「沒收」，由於沒收乃終局性的銷毀言論，故需要經過較為嚴謹之程序，需使相對人有參與程序、表達意見之機會，並且同樣要經過司法審查。

（二）財產權面向

另一方面，依美國憲法第五及第十四修正案[200]，也有對財產權之干預做出限制，即廣為人知之正當程序條款，「禁止未經**正當法律程序**而剝奪任何人的生命、自由

[199] Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46 (1989).
[200] 此二修正案皆有提及正當法律程序之要求，差異在於第五修正案之規範主體係國家；第十四修正案之規範主體係州政府。

doi:10.6342/NTU202302025

或財產。」是以，即便純粹以財產權剝奪之觀點探討域名扣押，也同樣面臨了正當法律程序之要求[201]。

較為經典之案例如在 Fuentes v. Shevin[202]案，該案主要之爭執規範係關於一方當事人得單方面向法院以簡易程序聲請扣押令狀，程序上僅需繳雙倍保證金或是出示財產價值宣誓書即可，而毋庸通知另一方當事人參與程序或發表意見。最高法院在本案認為，根據第十四修正案，系爭條款是無效的，因為它們未經正當法律程序即剝奪人民財產上之權利。

在本案中法院確立了財產剝奪之正當法律程序，當從占有人手中剝奪動產時，除非有緊急情況，否則需賦予其事前參與聽證之機會。單方面聲請之法院令狀無法替代剝奪財產前之聽證程序。

在此反映出了第五及第十四修正案的精神，即保障個人有在不受政府干預的情況下享受自己財產之權利。憲法之所以將「發表意見」作為剝奪人民財產時正當法律程序之一環，此一方面確保了財產制度中個人抽象、公平的競爭，另一方面，也宣示財產權所保障個人對財產之使用與占有不受任意侵犯的權利。而唯有在干預權利前，賦予受干預者發表意見之機會，才能夠實踐上述不任意侵犯、遵循公平決策的財產權保障目的。

是以，如果政府在沒有司法程序的情況下，將現實世界中的實體店面或住宅上鎖，依本案所建立之原則，將是違反正當法律程序的。而與域名限制之情形類比，前述行為並不會因為發生於網際網路世界，即從非法轉為合法。

一旦執法機關發現了某些網站包含兒童色情或涉及其他犯罪行為，即向法院聲請扣押令狀，並進而通知 ISP 業者協助過濾、停止解析域名、關閉系爭網站，使網路使用者無法訪問網站，此舉實際上造成了域名之使用目的不達，干預了相對人

[201] 對於適用第四修正案所授權之扣押正當程序後，民事扣押、沒收是否還須遵守第五修正案，非無爭議。惟最高法院已作出決定，認為扣押仍有遵守一般正當法律程序規定，固仍須符合第五修正案之要求。李榮耕，參前揭註 97，頁 74。

[202] Fuentes v. Shevin, 407 U.S. 67 (1972).

doi:10.6342/NTU202302025

之財產權。雖然並非物理上的扣押電腦設備或是網站上的圖像、資訊，但當網頁之內容是被禁止而無法使一般使用者造訪時，事實上造成相同的阻斷效果。

就關閉網站而言，形同終局的剝奪了該域名之使用，故依據上述案例對於採產權剝奪之正當法律程序要求，有賦予相對人於程序中表示意見之必要。惟就停止解析而言，若係以扣押目的發動，而只是暫時性的干預域名使用，則無必要於事前賦予聽證程序。

是以，現行實務上，美國執法機關在進行此類域名扣押或管制行為時，雖大多係向法院單獨聲請令狀而行動，惟扣押程序上並無賦予受處分人發表意見之聽證程序。雖於學說上頗有微詞之處[203]，惟以現況而言似未違反前述憲法上正當法律程序之要求。

本文以為，考量到扣押的暫時性，以及偵查程序中之秘密性要求。未賦予事前聽審程序實乃符合現實犯罪偵查需求之作法，且難逕認違憲，蓋此處立法者已經於扣押程序之規範設計中詳細考量。且在此域名扣押之目的為刑事犯罪偵查程序以及即時管制犯罪規模，相較前述案例之民事私人紛爭，域名扣押具有較高之公益目的，且也有緊急處置之必要。因此在憲法上進行利益衡量時，犧牲部分正當法律程序並非毫無可能之價值權衡，且在民事沒收之規範中，即設有受干預者得即時異議之規範，概念上僅是將聽證程序從扣押前延至後續的沒收審查程序中補足。是本文以為無法逕自推論域名扣押欠缺事前聽審程序即屬違憲，惟於個案中的言論自由爭議或有可能對社會造成巨大影響，本文認為於此類言論敏感或高度爭議之案例，踐行審前對抗式聽證程序乃較保障人民權利者。

三、事後程序

於域名扣押中，事後程序較無特殊之處，仍係依據聯邦法中扣押與沒收之規範。即受處分人或受影響之第三人，可以於程序中提出異議或即時抗辯，如：財產權受

[203] Agatha M. Cole, *ICE Domain Name Seizures Threaten Due Process and First Amendment Rights* (June 20, 2012), https://www.aclu.org/news/national-security/ice-domain-name-seizures-threaten-due-process-and.

doi:10.6342/NTU202302025

干預者可以提出善意不知情之抗辯[204]（如在非法行為發生時擁有財產權益者或在非法行為發生後才獲得其財產權益者，可以主張對於對於非法行為之發生不知情）或沒收不成比例之抗辯[205]（財產所有人得以沒收之數額過多為由；或沒收數額與犯罪行為之嚴重程度不合比例等提出異議）。由此可見，在域名扣押與沒收方面，由於其係依據已長期發展之聯邦法其中關於沒收之規範，事後救濟程序之規範較為完整，此部分較無爭議。

在域名扣押實務中，額外被提及於事後程序有所欠缺之處，係其於規範上與技術上皆缺乏有效的方法**來監控被封鎖網站的後續變化**。**規範面**而言，有時政府之命令並沒辦法明確的預期、指示執行封鎖之期間，此類扣押或監管行動將會給註冊管理機構帶來長期的行政責任。而規範上又缺乏課予註冊管理機構長期監督或於執行後定期檢查域名封鎖狀態之義務。且現今存在演算法可以自動生成域名，註冊管理機構便需要通過相對應之算法，配合域名生成的頻率阻止這些域名的註冊。惟演算法生成的域名也可能與已註冊的域名相衝突，此時註冊管理機構亦將陷入應保障合法註冊人權益抑或執行法院命令之衝突，然此部分缺乏程序規範，註冊管理機構是否有就此決策之權力亦付之闕如。

在**技術方面**，如前所述，違法網站架設者得以殭屍網路透過演算法自動生成大量域名，反覆的將違法內容張貼於不同的網域上。雖此形式上並不妨礙原被沒收域名之判決執行，然而實質上已將域名沒收以阻絕犯罪言論之目的架空。是以，要達到沒收目的，註冊管理機構必須同樣的使用演算法，依其生成域名頻率阻止之。但如果註冊管理機構未能識別或阻止其中一個域名，就可能讓一個成功遏制數月的殭屍網路重新復活，於技術上阻擋方總是只能被動的防堵、追趕，而沒辦法終局、持續性的將系爭違法內容移除。

綜上，目前域名扣押大多依附於民事沒收程序，依現有聯邦法之扣押規範進行。然而基於域名扣押本身之特殊性，有將程序調整之必要，以更符合憲法對於正當法

[204] 18 U.S.C. § 983(d).
[205] 18 U.S.C. § 983(g).

doi:10.6342/NTU202302025

律程序之要求。觀察美國實務，對於涉及表達性材料之扣押，於事前程序中要求司法裁決，即法官保留之概念；於事中程序則有多起判決提起「對抗式聽證」之必要性，強調大量扣押表達性材料以阻絕特定言論時，有事前給予相對人參與程序與發表意見之機會；於事後救濟程序中，雖聯邦法中已有詳盡之規範，惟對於新興科技來說仍有未盡之處。該如何監督域名扣押之執行情況，於法律上及技術上皆仍欠缺解決方案。前述為正當法律程序之討論，除此之外，域名扣押於美國法上另有掀起爭議者，為管轄擴張之疑慮。

第五項 司法管轄權

在美國法上，學者對於域名扣押現制之批評，有一部分便是點出管轄過於擴張之疑慮。雖如前述美國法上所發動扣押者係域內註冊之域名，惟實際上全球多數域名皆係註冊於位於美國境內之註冊管理機構。換言之，以「物之所在地」作為民事沒收管轄權之界定，套用於網路空間之域名，便會發生美國法院可以扣押世界各地人民所註冊域名之現象，而此將生弱化管轄限定效力之嫌。下文簡介管轄之意義，並詳述域名扣押於此所生之爭議。

一、管轄權規範

管轄之設計，除了涉及政府分配事務之系統利益，另外也關係到私人利益，例如：個人參與程序所花費之時間、勞力及費用等成本，關係到程序的公平性。除此之外，由於不同的轄區法律規範不同，透過管轄之劃定也可以使人民防止繁重且不可預見之訴訟，有助於穩定商業活動之發展[206]。

國際上管轄權之劃分，一般係以領土為劃分依據，諸如：發生於領土內的行為、國民之行為、涉及重大域內利益等，美國法亦遵循此原則。比較特別的是，除了一般常見的對人訴訟外，美國法上另外存在以物為程序主體的對物訴訟，如：民事沒收。其中，對物訴訟之管轄規定，係以「國家對物有控制權」或「沒收根據發生地」為管轄法院。

---

[206] Michael Xun Liu, *Jurisdictional Limits of in rem Proceedings Against Domain Names*, 20(2) Michigan Telecommunications & Tech. L. Rev. 467, 476-77 (2014).

doi:10.6342/NTU202302025

然而，隨著時代演變，跨域的活動發生的越發頻繁，而國家也發展出多種手段可以對「物」享有控制權，例如：透過司法互助或公私協力等方式，國家便可以透過第三人的手，去控制系爭財產，進而對物享有控制權。然而，在此種發展下，便會隨著管轄界線的鬆動，降低人民對於外地訴訟的預見可能性，反而使得管轄劃分之效果弱化。

是以，為了避免管轄擴張造成之負面效果，首先在 International Shoe v. Washington 案[207]中法院便提出了管轄需要與當事人具備**最低接觸要求**，以符合正當法律程序。又為了避免法院在對人管轄不符合最低接觸要求時，轉而尋求以對物管轄規避，於 Shaffer v. Heitner 案[208]認為應將對物管轄限縮於「司法管轄權之利益足夠大於個人利益時」，始構成有管轄權之狀態。

二、域名沒收之管轄

美國實務上對於域名即係採取前述對物性質之**民事沒收**模式[209]，故在域名的沒收，也會遇上前述管轄權之爭議。蓋只要域名是註冊於美國境內之註冊管理機關，則透過管理機關之協力，美國政府可以輕易地控制該域名，此時將造成與美國關聯性甚低的案件，卻仍然受美國司法管轄。且依據 15 U.S.C. § 1125(d)(2)，此來自 ACPA 法案之條文，更是明定了在商標侵權案件中，若商標所有人無法獲得對註冊人的個人管轄權，則其可以在「註冊或分配域名的域名註冊商、註冊管理機構或其他**域名管理機構所在**的任何司法管轄區」獲得提起對物訴訟的權利。

有論者以為，此種管轄權之設置乃過度擴張而違憲的。一方面，從實際的角度觀察，註冊機構的位置在域名使用上並沒有意義，「.com」、「.org」等通用頂級域名係亦被公認為獨立於任何地理區域。即使主張註冊人在註冊域名時應可以設

---

[207] Int'l Shoe Co. v. State of Wash., Office of Unemployment Comp. & Placement, 326 U.S. 310 (1945).
[208] Shaffer v. Heitner, 433 U.S. 186, 207 (1977).
[209] 美國實務上對於域名之扣押係採取所謂民事沒收之模式，該制度之特徵即其程序具「對物性」。簡單來說，對物沒收係以「財產」為程序之主體，執法機關以欲沒收之物作為民事沒收訴訟之被告。此種制度能夠解決一些因現實困難，如犯罪嫌疑人逃亡、死亡等，無法追訴行為人犯罪卻又有沒收必要之情形；也同時使得程序較為迅速，只需特定標的物，而不須事先特定並起訴相對人。於美國實務上也常以民事沒收作為事件之終結，而不以行為人被定罪為必要（將重心置於查扣犯罪財產，而非犯罪追訴）。TWNIC，https://blog.twnic.tw /videosyt/域名之扣押與沒收-以司法實務操作為中心/（最後瀏覽日：09/15/2022）。

doi:10.6342/NTU202302025

想到註冊機構位於美國，然而實際上註冊機構所在地與網域線上活動之間缺乏關聯，註冊人不應僅僅因為其域名以「.com」結尾而預期須負擔在外國訴訟之成本。另一方面，過度擴張的國際管轄權，將造成與他國司法權之衝突。可能發生判決矛盾，也可能削弱他國法院監管其境內行為的能力，轉而成為國際間緊張關係[210]。

是以，亦有主張於適用 15 U.S.C. § 1125(d)(2)時，應將本條的對物管轄限縮適用於「惡意註冊」域名之情形，而不應該擴及所有的域名侵權爭議，對法院域名扣押之管轄權為限縮之解釋。

第四節 分析與比較

本章整理了美國法之沒收、扣押制度，以及探究美國法域名扣押之實務現況。並以基本權干預之觀點，整合美國之憲政實務，審查美國域名扣押現制之不足與爭議，以完整的分析「使用對物沒收作為域名管制手段」之優劣。下文將分析美國之作法，並與我國之法制背景比較，探究此是否適合援引至我國。

第一項 優勢

參見表格 1，民事對物沒收相比起刑事對人沒收，有沒收範圍較廣、程序證明度低、以及毋庸與刑事訴訟程序掛鉤之便利性等優勢。以偵查機關之觀點而言，此乃有效打擊、嚇阻犯罪之利器，且甚至不用經過繁雜之起訴程序。尤其運用於域名之沒收，更可以即時處理匿名性、跨國性的網路犯罪，於令狀上無需記載相對人，此乃過去對人沒收所無法突破之窘境。

是以，美國採用民事對物沒收作為違法域名之下架手段，其優勢乃程序上**有效率、打擊範圍廣**，可以即時的封鎖違法域名，且無論系爭網站之架設者是否位於美國境內。

[210] Michael Xun Liu, *supra* note 206, at 485-93.

doi:10.6342/NTU202302025

第二項 隱憂

美國法之作法，將民事沒收用於新興網路犯罪，毋寧是將重點置於執法之實效性。以迅速且程序簡便之方式，剝奪涉及不法之域名。以執法效能之觀點，可謂有效之犯罪防制手段。

然而，講究快速、簡易之程序，反過來以受處分人之觀點思考，則不免有程序保障不足之疑慮。在程序上，執法機關得以單方程序向法院聲請扣押令狀，而相對人無事前參與、發表意見之機會，此即遭受了不少學說質疑。尤其域名扣押額外產生之言論自由干預，觸動了美國憲法第一修正案之敏感神經。參照過去之憲政實務，最高法院便認為涉及表達性材料之大量扣押，應有聽證程序之保障。另一方面，終局剝奪的域名沒收，依據第五修正案，為符合財產剝奪之正當法律程序，也應舉行事前聽證程序。

另一問題在於，民事沒收採取較低之證明度要求，執法機關僅須證明至優勢證據之程度，即得發動沒收。相較於採刑事定罪為前提之刑事沒收，民事沒收之證明顯然較為輕鬆。在證明度相對低要求之情況下，偵查機關較偏好採取民事沒收，反而架空了刑事沒收制度。且雖程序不同，但無法否認民事沒收亦帶有懲罰之性質，卻毋庸經過嚴謹之刑事訴訟程序，且檢方所負之說明責任亦較低。為了執法的實效而減損了執法機關之責任，是否為妥適、衡平之政策，亦非無疑。

尤其域名的扣押與沒收，相較於傳統實體扣押，額外產生了言論自由的干預，卻容許檢方以較低之說明義務發動言論之審查與限制，更是提高了證明度爭議之疑慮。

除了上述程序保障、民事沒收之固有問題，非實體的域名扣押，還帶有網路執法無國界之特色，蓋依據現行技術以及美國於域名管理之優勢地位，即便是美國境外之行為人所架設之網站，只要系爭網站註冊於美國境內之註冊管理公司，美國亦能取得對其之管轄。而此會發生之疑慮有二，一者為對於境外行為人之程序保障難題；二者則是與他國管轄衝突之負面效應。

doi:10.6342/NTU202302025

第三項 我國法比較

一、域名註冊背景差異

透過上文對於美國域名扣押現制之分析，本文思考該民事沒收制度是否適於援引至我國，或截長補短，將其優勢之處擇採並融合至我國法制。

首先，分析我國與美國之背景差異，首要之差異在於域名管理之地位落差，國際上多數域名係註冊於美國境內之註冊管理機構，且 ICANN 也於此具有管理優勢地位，故於美國而言，大部分的網站犯罪皆係註冊於其境內之域名。故在立法上，僅將沒收標的限於境內域名，於美國執法上並無障礙。

惟於我國則有巨大之不同，註冊於我國境內之域名不若美國多，且以犯罪為目的之網站架設者，若為避免 TWNIC 之管制，其所註冊之域名也將以境外為主。是以，對於我國而言，若欲達到防堵犯罪之目的，於管轄設計則需注意不應逕援引美國法，扣押標的應擴及於境外註冊域名。然而，將標的擴張後，管轄擴權之問題又更加明顯了，何以我國得針對外國管理之域名執法，其聯繫因素有再思量之必要。

二、民事沒收與我國法制之差異

我國於民事程序中欠缺沒收制度之設計，基於前述民事沒收於執法上之便利性，不乏有學者主張我國有採行民事沒收之實際需求，其理由為我國沒收刑事法規範之不足以及與國際接軌之必要[211]。惟須注意，於 2016 年我國沒收新制正式實施後，是否還有此需求，則非無討論之空間。

於沒收舊法脈絡下，認為我國刑事沒收制度規範不足，係因於被告逃亡、無法起訴、證據不足等情況，一般情形下皆無法發動沒收。蓋舊法僅就特殊情形有單獨沒收之設計，缺乏總則性之規範。而所謂與國際接軌之需求，亦係關於呼籲非基於定罪之沒收有存在必要之公約簽署[212]。

---

[211] 李榮耕，參前揭註 97，頁 86-87。

[212] 立法院於 2015 年 5 月正式通過了聯合國反貪腐公約施行法。依據該公約第 54 條第 1 項：「考慮採取必要措施，以利在犯罪人死亡、潛逃或缺席而無法對其起訴或其他適當情形，允許不經刑事定罪，即予沒收此類財產。」

doi:10.6342/NTU202302025

惟於沒收新制，刑法第 40 條第 3 項，即建立了一般性的獨立沒收制度，明文規範於事實上不能或法律上不能追訴犯罪時，得單獨宣告沒收。是以前述二者提倡我國有建立民事沒收制度之理由，似不存在。

然而，仔細將美國民事沒收與我國刑事單獨沒收制度兩相比較，仍有關鍵性之不同。首先，美國法民事沒收本質上係對物程序，其發動前提不以未能追訴犯罪行為人為必要；反之，我國刑事沒收原則上仍為對人程序，僅有於構成 40 條第 3 項之情形，始得以客體（對物）之方式發動沒收，且檢察官有舉證說明構成單獨沒收之義務[213]。我國法上單獨沒收之發動具備位性，不若美國法制較不受限。

再者，美國民事沒收制度與我國刑事沒收最大之差異之處在於「證明度」之要求。後續有論者於域名扣押制度再次提及我國有參酌民事沒收制度之需求[214]，即以證明度之差異做為論述核心。美國法上民事程序中對證明度僅要求至「優勢證據」。反之，我國刑事訴訟法對於犯罪事實之證明度則要求至「確信」[215]。雖依據我國沒收新制建立時之討論，單獨沒收制度之建立即係為處理難以追訴犯罪之情形，故一般認為是否該當沒收之要件僅需採取自由證明即可，而無需採取嚴格證明法則，以法定證據方法、法定調查程序為之。然而，採取自由證明並不代表證明度即會因此調整，是以，在我國法上仍維持刑事程序之證明度要求[216]，不若美國民事沒收寬鬆。由此觀之，在執法實效上，民事沒收較低之證明要求或有其優勢。但同時，低證明度、程序保障不足也是民事沒收制度，於人權保障觀點下為人批評之處。

在此本文無法決定民事沒收制度是否適於我國所採行，僅能做出其與我國法制之比較分析，供讀者思考制度之取捨。

---

[213] 按刑事訴訟法第 455 條之 35 第 4 款：「前條聲請，檢察官應以書狀記載下列事項，提出於管轄法院為之：四、構成單獨宣告沒收理由之事實及證據。」

[214] 台灣網路講堂，https://www.twsig.tw/20201120/（最後瀏覽日：03/28/2023）。

[215] 參司法院釋字第 582 號主文。

[216] 此處另有疑問者係，依司法院釋字第 582 號，需形成確信心證者為犯罪事實存在。然而沒收已是獨立於刑罰之法律效果，其對於證明度之要求為何，實務、學說上皆無特別討論。故本文仍以刑事訴訟程序之一般要求，討論美國法上民事沒收與我國沒收證明度落差之概況。

doi:10.6342/NTU202302025

第四章 澳洲法

第一節 澳洲法制簡介

本文挑選澳洲作為比較法對象之一，一方面是希望能將同為英美法體系（普通法體系）之國家共同討論與比較，以探究於相似之法概念下，不同地點及不同的社會脈絡所造就管制手段之不同；另一方面澳洲是一個穩定、多元文化和民主的社會[217]，在重視言論自由的社會氛圍下，卻有不少以強制性的手段管控網路言論之立法[218]，令人意外的態度，也值得參酌其於言論自由與網路管制間之拉扯與平衡。

澳洲過去為英國殖民地，其司法制度係繼受於英國法制，於現今法治發展也仍受英國法院判決所影響。然其也同時一定程度的受加拿大及美國法影響[219]，於英、美等國之間斟酌損益，發展出自己的特色[220]。本節將簡介澳洲法體系，並詳述澳洲對於網路非法言論之管制手段。

第一項 澳洲法體系

澳洲係採取聯邦政府之體制，設有六州與兩個特別行政區，澳洲憲法中訂有聯邦與地方政府之分權規定。其中，聯邦國會立法權之範圍係涉及全國或國際性之事務，包括商貿、檢疫、貨幣、關稅、專利、國防以及社會福利等。其剩餘權限（Residual Power）則歸於各州，各州可對憲法未列舉之其他領域立法。除此之外，州議會尚有概括權限，只要是為了州的福利或利益，可對任何事務訂定法律。換言之，各州

[217] National Report Submitted in Accordance with Paragraph 15 (A) of the Annex to Human Rights Council Resolution 5/1, UN Doc A/HRC/WG.6/10/AUS/1 (Nov. 5, 2010), ⁋7.
[218] 於 2000 年，Electronic Frontiers Australia （簡稱 EFA）試圖引入「強制審查並過濾網路內容」，以杜絕兒童虐待、兒童色情之內容於網路上傳遞。此強制過濾之措施於 2012 年始被國會正式宣告停止實施。ITNEWS, *Australia's Mandatory ISP Filtering Plan Axed*, https://www.itnews.com.au/news/australias-mandatory-isp-filtering-plan-axed-322353 (last visited Dec. 13, 2022).
[219] 楊崇森（2016），〈澳洲法律制度運作概觀〉，《法令月刊》，67 卷 8 期，頁 34。
[220] 同上註，頁 26。

doi:10.6342/NTU202302025

所立之法只要不抵觸聯邦法，即可對任何事務設立規範。在立法範圍上，州法之打擊範圍較廣，惟州法與聯邦法相抵觸時，則以聯邦法為優先[221]。

在本文之討論上，雖然各州對於網路內容管制之立法略有不同，惟本文為避免討論範圍過廣而失焦，將專注於優先適用、級別較高之聯邦法為討論主軸，且聯邦法亦彰顯了澳洲國會在管制網路言論上一致性的觀點。

第二項 網路管制手段

在美國法上的討論，係將網域名稱作為標的發動對物沒收，以達到下架非法網站之效果，而我國學者亦大多將停止解析置於扣押與沒收之下審酌。雖然於澳洲之法制中亦存在便利、舉證責任低的民事沒收，且於沒收法中也發展出各式大膽、創新之令狀[222]，在剝奪犯罪工具之效率上不遜於美國法，惟澳洲政府針對非法網路言論之網站則未以沒收作為管制手段[223]，而係另外創設可以請求 ISP 業者提供技術協助、刪除非法網路內容之規範，或課予 ISP 業者義務、施以處罰之方式處理非法網站議題。

以下以管制手段作為區別，介紹澳洲涉及網路內容管制之聯邦法案：

一、非法院之通知

在廣播服務法案（Broadcasting Services Act 1992）中，授權澳洲通信與媒體管理局（Australian Communications and Media Authority，簡稱 ACMA）有審查網路

---

[221] 同上註，頁 29-30。

[222] 在澳洲的民事沒收法制發展中，較為著名的是新南威爾士州（NSW）於 1990 年訂立的 Criminal Assets Recovery Act（通稱為 CARA 法案），在此法案中設有 Restraining Order, Asset Forfeiture Order, Proceeds assessment Order （收益評估令，法院可以下令被告提供財產資訊）。另外在聯邦法的犯罪所得法（POCA 2002）也設置有 Automatic Forfeiture（自動沒收令，省略司法審查，涉及嚴重犯罪時行政機關可以直接發動沒收）, Pecuniary Penalty（罰款令，將犯罪所得利益以罰款之方式返還給國家）等特殊之令狀。Australian Government, *Confiscation of The Proceeds of Crime: Federal Overview*, https://www.aic.gov.au/publications/tcb/tcb1 (last visited Dec. 14, 2022). 在澳洲的民事沒收中，也常見舉證責任倒置，由被告自證財產來源合法之情形，蓋財產所有人對於財產之來源資訊較具有優勢。比起美國檢察官所負擔的優勢證明責任，澳洲法中檢方的舉證責任更低。

[223] 雖然於 POCA 2002 以及各州的沒收法中，皆將沒收之標的與美國法同用語，皆為作為促進犯罪或至犯罪所得之財產（Property），在此用語之下似乎也無法排除將域名作為財產扣押與沒收之可能性，惟本文於資料搜集及撰寫之過程中，皆未搜尋到澳洲將非法網站域名作為沒收或扣押標的。David Lusty, *Civil Forfeiture of Proceeds of Crime in Australia*, 5(4) J. Money Laundering Control 345, 348-49 (2002).

doi:10.6342/NTU202302025

內容之權利，將網路之內容分類管理，禁止項目包括：歸類為「絕對禁止」者、「未設計成人驗證之成人內容」或「網路霸凌」等。網路使用者可以向 ACMA 投訴涵蓋前述內容之網站，而 ACMA 審查後，若是網站內容被認為是禁止的，其有權向架設於澳洲境內之網站發出刪除通知，而網站根據該通知必須刪除系爭違法內容。若未依循通知刪除網站內容，將可能面臨高額罰款。且不僅限於澳洲境內之網站，若系爭網站架設於境外伺服器，該網站之 URL 或域名也將被加入 ISP 業者之黑名單中，而遭到阻擋，澳洲境內之用戶將無法依正常之解析造訪網站。此乃非源於法院之刪除通知。

除此之外，在 1997 年電信法（Telecommunications Act 1997）第 313 條第 3 項，也規範了 ISP 業者有配合政府（包括聯邦及州政府）機關之通知，採取措施阻擋網站之義務。若係涉及本國及外國刑法之執行、公共利益之維護以及國家安全之保障，政府機關即可向 ISP 業者請求合理、必要之幫助，協力阻擋網路使用者對於非法網站之訪問。附言之，雖本法於 1997 年即訂立，惟以本條作為授權依據下架網站之想法，係至 2014 年由時任通訊部長所提出，並於該年度提交委員會審查以本條干擾網路服務之可能性。本條之運用範圍極廣，幾乎所有涉及犯罪者或是基於公益目的，政府即得以此中斷網路服務，毋庸經過司法審查，也沒有搭配透明度之報告，因此也引發了許多的擔憂與質疑。

二、法院命令

法院也能夠發布刪除命令予設置網站者或是 ISP 業者，請求其等依據法院之命令下架網站非法內容。在**民事**方面，著作權法 2015 年之修正法案中（Copyright Amendment Bill 2015），即新增了網路侵權之相關規定，允許權利人向法院聲請命令，要求 ISP 業者協助阻止架設於澳洲境外之侵害著作權網站之造訪[224]。

而在**刑事**方面，根據 2004 年的監視設備法（Surveillance Devices Act 2004），設有「數據破壞令（Data Disruption Warrant）」的令狀，澳洲聯邦警察（Australian

[224] Australian Government, Department of Parliamentary Services, *Copyright Amendment (Online Infringement) Bill 2015*, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/3830145/upload_binary/3830145.pdf;fileType=application/pdf.

doi:10.6342/NTU202302025

Federal Police，簡稱 AFP）可以基於網路犯罪預防、阻止之目的，向法院聲請數據破壞令，並請求 ISP 協助執行，阻止用戶對非法網站的訪問，將域名轉址或直接刪除系爭犯罪內容，以挫敗嚴重犯罪的實施[225]。此令狀之特色在於，其有別於處罰之事後觀點、亦非保全刑事追訴的程序目的，它是基於**事前預防**之概念去介入犯罪。畢竟，網路犯罪具有擴散性、難以被遺忘之特性，一旦非法的內容被上傳到網路上，若無法及時下架內容，該非法言論將被廣泛的傳播，即便原始網站關閉，也在網路上流傳著複數備份，而加重了被害者之損害或是增加了民眾接觸不法內容之機率。是以，數據破壞令在此預防觀點下油然而生。

三、施以處罰

2019 年，紐西蘭基督城的兩座清真寺發生大規模的槍擊事件，且槍手在發動恐怖攻擊時亦同時在臉書上發起直播，並在槍擊後發佈線上宣言。這段槍擊直播影片隨後被紐西蘭及澳洲的 ISP 業者刪除，但在網路上仍然留下許多的備份，影像的流傳對社會造成了負面影響。

依此事件，澳洲亦提出了刑法修正案，增訂了 ISP 業者、網路平台服務者之作為義務。它要求提供託管服務的網站「確保迅速刪除」由被告或其共犯所製作的暴力影像或紀錄，並且須在合理時間內，識別此類內容並向當局報告。其中的暴力紀錄係指含有「令人憎惡的暴力行為」內容之影像、錄音檔，包括：恐怖行為、謀殺、謀殺未遂、酷刑、強姦或綁架。若未能即時移除這些內容，該網站營運者或負責人，將負擔刑事責任，可能面臨高額罰款與徒刑。且無論系爭內容是否架設於澳洲境內的伺服器上，該法律均有適用。

此係將相關業者之作為義務刑罰化，以課予處罰之方式，使該等網站營運者、服務者，協力將違法內容刪除，達到網路管制之效果。

---

[225] Australian Government, Department of Home Affairs, *Data Disruption Warrants*, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021/data-disruption-warrants (last visited Dec. 15, 2022).

doi:10.6342/NTU202302025

四、課予 ISP 業者主動審查義務

在處罰以外，澳洲也曾討論過引入網路強制審查制度，以法案要求 ISP 業者配合全面性的網路審查，使其負有過濾不當內容的義務。此提案被外界稱為澳洲版的「網路長城」，備受爭議。尤其強制過濾的網域黑名單，主要是依據外國或第三方通報的兒童色情名單所構成，有責任轉移之嫌疑[226]；且技術的透明度不足，外界難以監督；過濾的標準模糊，可能遭到技術濫用扼殺政治性言論等，在國民的大力反對以及輿論壓力下，最終澳洲政府放棄實施網路的強制過濾與審查。值得注意的是，放棄強制審查的同時，亦是通訊部長提出將 1997 年電信法第 313 條第 3 項用以管制網路言論可能性之時機。可見 1997 年電信法第 313 條第 3 項彈性的用語與寬泛的授權，於網路管制方面可能成為政府有力之手段。

第三項 聚焦討論具體規範

縱覽上述澳洲與網路言論相關的立法，可以簡單的將之區分為「課予 ISP 業者主動介入審查的義務」以及「政府機關核發令狀或通知，ISP 業者被動配合」此二類。由於本論文所關注的重點是來自國家強制下架涉及刑事不法言論之手段，故在本章節澳洲法之比較分析，亦會將重點置於後者，即 2004 年監視設備法的數據破壞令及 1997 年電信法第 313 條第 3 項。

一、2004 年監視設備法的數據破壞令

所謂數據破壞是指**添加、複製、刪除或更改電腦中所保存的數據**。此令狀之授權目的僅能用以破壞犯罪、減少犯罪損害。而為了協助阻止犯罪，本令狀同時可以授權其他便利破壞犯罪之行為，例如：進入指定場所、從場所移走電腦、複製已取得之數據以及向技術人員要求提供合理與必要之協助等。另外，數據破壞令允許隱藏檢警機關之行動，以秘密的方式執行令狀。對於涉及外國之數據，經適當的外國官員同意，亦得作為數據破壞令之執行標的。

[226] Derek E. Bambauer, *Filtering in OZ: Australia's Foray into Internet Censorship*, 31(2) U. Pennsylvania J. Int'l L. 493, 496-97 (2009).

doi:10.6342/NTU202302025

（一）令狀之聲請

1.實體要件

聲請令狀者必須具備合理懷疑，正在、即將或可能發生違法行為，且該行為涉及保存於電腦中的資訊數據，而中斷、破壞該數據很有可能幫助阻止犯罪。該犯罪行為必須是聯邦或與聯邦有關的州、領地犯罪，並且可判處最低 3 年以上有期徒刑。

授權令狀者於核發令狀時，則必須確信該聲請所附理由已達合理懷疑，且數據中斷是合理、必要且相稱的手段。除此之外，核發令狀時須同時考量以下事項：(1)犯罪行為的性質與嚴重性、(2)是否存在其他阻止犯罪的替代手段、(3)對第三方的影響及影響之程度及(4)新聞自由，若是中斷數據令執行將影響記者等專業職業，須考量核發令狀的公共利益是否超過保護新聞來源身份或新聞報導的公共利益。

2.程序要件

聲請令狀之身份須為 AFP 之警察或澳洲刑事情報委員會（Australian Criminal Intelligence Commission，簡稱 ACIC）之官員。聲請前須獲得授權官員之批准，始得向法院聲請令狀。所謂的授權官員係由 AFP 之專員或 ACIC 之首席執行官任命，其必須具有足夠高的級別，並且必須滿足特定的培訓、技能和經驗要求。接受聲請、授權令狀者為法官或受指定之行政上訴法庭（Administrative Appeals Tribunal，簡稱 AAT）成員。

簡言之，數據破壞令之聲請，原則上聯邦警察須先獲得機關內部之授權官員同意，始得向法院提出聲請，並由法官或 AAT 之成員審酌上述實體要件後核發。惟例外於緊急情況[227]時，也可以由 AFP 或 ACIC 內部先行核發、授權破壞數據，嗣後再向法官或 AAT 之成員補足令狀聲請程序。相當於「相對法官保留」之規定。

（二）令狀之執行期間

授權破壞數據之執行期間最長期限為 90 天，最多可以再聲請延長 90 天。

[227] 緊急情況係指存在對人造成嚴重暴力或對財產將造成重大損害的急迫危險。

doi:10.6342/NTU202302025

（三）其他特色

原則上數據破壞令不得用以授權對合法使用電腦的人造成損害，除非合理、必要及合乎比例性，且造成損害後執行機關必須在 7 天內通知聯邦監察員。若於執行令狀時對第三人造成未經授權的損害，則受損人有權請求賠償。

數據破壞令授權執法機關刪除網路上的內容或將域名轉址等變更電腦資訊之行為，以防止犯罪損害的擴大，並及時阻止犯罪。舉例而言，機關可以將含有兒童虐待之內容刪除、停止該網站之域名解析，或將域名轉址等，來防止不法內容的傳播。在有技術協助需求時，執法機關也可以向法官或 AAT 成員尋求協助令，要求具備技術知識者提供協助，以執行數據破壞令。

由此可知，「停止解析」與「域名轉址」皆屬本令狀所得以授權之行為，不僅僅是阻擋非法內容、下架網站，數據破壞令更是得以授權政府機關竄改電腦之數據資訊，換言之，政府機關可以依此主動積極的創造假資訊。其對於言論自由之限制，與純粹的阻擋言論相比，難以判斷孰輕孰重。

另一個特色是，數據破壞令之條文中即明確**表示令狀之目的在於預防、阻止犯罪，而非以起訴蒐集證據為目的**。此種「創新令狀」的方式，處理了過去強制處分之目的通常被限縮於蒐集證據、保全審判程序以及後續執行之問題，正視了執法機關預防犯罪，減少損害之需求。此種新思維也是我國法中思考停止解析於刑事訴訟之定位以及規範模式時，所得以參考者。

二、1997 年電信法第 313 條第 3 項

相較於數據中斷令規範詳細，1997 年電信法第 313 條第 3 項則是一個相對模糊的授權依據。條文內容僅泛稱提供電信網路或設施之營運商、提供者，於某些情境下有向聯邦、各州及領地的政府官員提供合理、必要之協助。條文內卻沒有明確訂立請求協助之程序、如何監督本條之使用以及救濟程序，一切付之闕如。依文義觀之，似係只要政府機關有需求，即可以向 ISP 業者發出通知，請求轉址域名或刪除內容，而該通知毋庸經過司法審查，也無發出請求之主體限制，只要是政府官員皆得發出斷網命令。

doi:10.6342/NTU202302025

而上述所謂 ISP 業者有義務提供協助之情況包括：(1)執行刑法和處以罰款的法律、(2)協助在外國執行刑法、(3)維護公共利益及(4)保障國家安全。其中「公共利益」之用語亦屬模糊，政府機關之行動皆可以寬泛地認為是為了國家公益所為。模糊的文義、缺乏的程序要件，使本條使用上相當便利，也富有彈性，即便是 21 世紀發展出的新興技術都可以在此文義下套用，以本條作為授權依據；然而，也顯現出其被濫用的風險，透明度不足、監督單位不明，且即便人民受有損害也無法救濟，是否能發現系爭損害係源於政府依本條所為亦屬難事。

於澳洲法上，上述二規範皆可能作為停止解析之授權依據，但「創新的令狀」與「模糊的授權」這兩種針對新興科技偵查之立法模式，也有其各自要面對的法律爭議。雖然普通法體系之國家，不若大陸法系有所謂的法律保留，可以透過立法事前控制公權力行為之合法性。惟普通法系中仍有針對國家干預行為合法性之司法審查機制，下文以澳洲法制審查其域名干預措施之合法性，並整理澳洲立法例中可供我國參考之處，以及我國援引時所需注意之處為何。

第二節 基本權

欲探討於澳洲法制上運用停止解析、域名轉址等技術，其合法性爭議之前提，係該等刑事犯罪偵查之公權力行為干預或限制了澳洲人民之權利。是故，此處須先確認究竟斷網技術之使用，對澳洲人民之何等權利造成影響。

而本節最大之爭議，亦屬澳洲憲法最大的特色，就是澳洲並未於憲法中設置權利法案（Bill of Rights）的章節[228]。換言之，澳洲並沒有於憲法中明文規範人民之基本權利。在討論停止解析干預言論自由與財產權時，需要將此特殊背景列入考量。

一、澳洲憲法特殊背景

之所以澳洲憲法中並未將基本權章節列入，有一說是認為，透過立法權、行政權及司法權等機關之間的權力分立運作，所建立起互相監督、制衡權力之制度，已

[228] 楊崇森，同前揭註 219，頁 35。

doi:10.6342/NTU202302025

足夠保障澳洲人民之權利；亦有認為憲法中沒有列入基本權章節，是因為制憲者認為這些基本權利已經受到普通法的充分保護。[229]後者認為，雖然澳洲憲法沒有明文保障基本權，但在長期歷史發展之下，澳洲的法院也普遍承認**言論自由、財產權**屬於基本的普通法權利。

除了普通法外，在言論自由方面，高等法院也從憲法第 7 條及第 24 條「要求國會成員由人民直選」之規定，推導出憲法隱含著保護政治性言論之自由，蓋要使人民得以依自己的意志行使選舉權，必須使其可以自由獲取相關的政治資訊，此為民主國家之基石。是以，政治性言論之自由在澳洲法上通常被認為是憲法所隱含保障之權利，國家對此干預時，必須是出於維護憲政秩序之合法目的（Legitimate Objective），始得以合理、適當之方式為之；而在財產權方面，澳洲憲法第 51 條第 16 項則明文規範「禁止聯邦政府以非公正之方式干預財產」，雖然是限制政府權力之條款，但通常被認為是憲法明文保障財產權之依據。

另一方面，澳洲也是身心障礙者權利公約（Convention on the Rights of Persons with Disabilities，簡稱 CRPD）和公民與政治權利國際公約（The International Covenant on Civil and Political Rights，簡稱 ICCPR）之締約國，從公約可以推導出澳洲有保障人民言論自由之義務。雖 ICCPR 沒有明確保護財產權之條文，但世界人權宣言（Universal Declaration of Human Rights，簡稱 UDHR）另有每個人都有單獨擁有財產權利之規範。是以，在國際法之層面，言論自由、財產權也是被廣泛承認的，基於澳洲國際法上之地位以及公約之簽署，也具有維護之義務。惟基於國際條約不可凌駕於內國法之原則，於審查政府干預基本權之行為時，法院通常不會以公約上之權利作為干預審查之標的，而是僅在法律解釋時援引使用公約，加強論點。

綜上所述，在澳洲法體系中討論停止解析、域名轉址等網路管制之公權力行為時，首先要注意的是，言論自由與財產權之保障法源為何，蓋不同法源對於干預合法性之審查模式亦有所不同。

---

[229] 同上註；Lasa Sun, *Freedom of Speech, Democracy and Cyberspace: Lessons from Australia, Singapore and India*, 43 (2016), https://doi.org/10.25949/19427480.v1 (last visited Dec. 19, 2022).

doi:10.6342/NTU202302025

附帶而論，普通法解釋原則中的「**合法性原則**」在澳洲被認為是「普通法版本的權利法案」，長期以來被澳洲之司法機構用作加強人權保障之工具。合法性原則（The Principle of Legality）係指於法律解釋時，當法規沒有明文或是明確暗示的情況下，國會會被推定無意限制以下的權利或自由：人身自由、行動自由、言論自由、信賴原則（不得追溯變更權利和義務）、公平審判等，此類權利已經在普通法中被廣泛承認[230]。本文以為，合法性原則之概念與法律明確性原則相當類似，蓋合法性原則之法理系當法律用語模糊時，由於人民無法事前理解、預見規範效果，法院於法律解釋時也應傾向保障人民之態度，以符合法治。是以，縱使澳洲憲法內未設有權利法案，澳洲法制仍存有人民權利不得任意限制之想法，若干預普通法所承認之基本權利，則必須存在立法者之明確授權。併予敘明者，觀察所謂普通法基本權，其權利內涵與美國憲法修正案所保障基本權之內容大同小異。

二、現制批評

然而，此種未於憲法中明文基本權保障，而是將基本權規範於普通法內之制度，是否於人民權利保障方面毫無落差，尚存有爭議。澳洲國內學者也有正、反兩方意見。

反對論者認為，缺乏憲法層級的權利法案對於人民基本權利之保障仍屬不足，蓋若沒有明文的法律保障，權利很容易被政府所侵蝕，尤其在處理言論自由的法律中，更可以觀察出政府對於保障權利、促進自由發展相比，更關心如何控制言論的議題。另一方面，明文規範基本權可以賦予人民行動、實踐權利之路徑，可以合法的挑戰權力；並能夠加強少數族群的保護，相較於不平等的多數決政治，對影響力較小的少數族群而言，明文規範的基本權是確保不被多數犧牲之堡壘。最後，若於憲法制定權利法案，將可以促使澳洲與世界接軌，保障普世人權，履行澳洲之國際義務[231]。

[230] *Id*, at 43-44.
[231] *Id*, at 45.

doi:10.6342/NTU202302025

支持現行制度者，則是認為人民權利在澳洲已經獲得足夠的保障，政治制度本身就是澳洲最好的權利保障。倘賦予非民選的法官有推翻國會的權力反而是違反民主政治的，且可能導致龐大數量的訴訟，使訴訟成本大增[232]。此外，將權利保障明文化，定義權利之過程反而是對權利的一種限制與窄化，增加權利法案章節是否能夠確實的增加權利的保障，亦存有疑義。

三、小結

在上述爭議未決之下，本文難以判斷將基本權規範於憲法內是否為較佳之保障模式。惟觀察澳洲政府現行對於網路言論之管制政策，可以發現其相較於美國、加拿大此種憲法明文保障言論自由之國家，傾向採取較嚴厲而對言論自由干預較大手段，蓋其立法受到的憲法限制較小，政策受到的司法審查較少[233]，有較大的空間可以將政府管制的手伸入網路世界。

而回歸本文審查重點，停止解析、域名轉址等網路管制措施，所涉及之基本權為言論自由及財產權。此於澳洲檢警機關所使用之技術探討上亦同，雖不一定同樣的使用 DNS RPZ，但刪除網頁上的特定內容，或是讓使用者無法造訪網站等，皆屬於類似的干預。主要差別係在於澳洲法上對基本權保障及司法審查模式之差異。

於**言論自由**方面，憲法僅暗示政治性言論自由之保障，廣泛的言論自由則是屬於普通法權利。由於本文所討論之網路管制不僅僅針對政治性言論，且澳洲憲法並非旨在賦予個人權利，而是著重於對立法權力之限制。故本文討論主軸將置於**普通法上的言論自由**，進而討論普通法上言論自由干預之審查。而雖 CRPD 第 21 條與 ICCPR 第 19 條等國際公約有提及言論自由之保障，但國際公約於澳洲實務上，通常僅有於法律解釋時會被法院所援引，而無法逕自作為保障權利之法源，故國際公約亦非下文所深究者。

以澳洲現行制度觀之，普通法下對於言論自由之保護領域，與美國、我國對於言論自由之理解相差無幾，即任何形式之意見發表不受干預之自由。是以，停止解

232 *Id.*
233 Derek E. Bambauer, *supra* note 226, at 502-03.

doi:10.6342/NTU202302025

析或其他斷網措施之施行，亦是對言論發表者與一般民眾形成言論自由之干預[234]，則根據上文必須遵守**合法性原則**，以明確文義授權該等措施之實施。且對於權利有重大影響者，國會亦不得任意委派立法，應以「法律」層次之規範始得授權之[235]。

於**財產權**方面，則是憲法、普通法及國際公約都有提及之權利，但也皆同時提出財產權並非不得限制之觀點。蓋在概念上，財產權利之存在被認為係與法律制度相輔相成[236]，故其權利本質上就須受到規範之限制。在憲法上，國家可以透過立法以公正（On Just Terms）的方式取得財產權[237]；在普通法上也認為，只要對財產的干預不是任意的（Arbitrary），且有合理補償，並遵守合法性原則，即屬於合法之干預。

而對於域名、網域是否屬於財產（Property）之概念，其討論與美國法並無太大區別，蓋在澳洲法上對於財產之認定，亦認為財產涵蓋實體物以及非實體之權利[238]。是以，停止解析等干預網域自由使用之措施，其對於財產權之干預，下文將與言論自由之干預併同討論合法性原則，以及其是否屬於普通法上「非任意」之干預。至於澳洲憲法上對於國家取得財產「公正」之限制，其所指涉者並不包括純粹干預財產使用之情形，故於本文並不多加著墨此部分。

第三節 授權依據合法性探討

澳洲法上國家運用公權力將網站停止解析或是刪除內容，是對於人民言論自由（普通法權利）及財產權（憲法、普通法權利）之干預，授權此等干預之依據是

---

234 Australian Government, Attorney-General's Department, *Right to Freedom of Opinion and Expression*, https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/right-freedom-opinion-and-expression#what-is-the-right-to-freedom-of-opinion-and-expression (last visited Dec. 19, 2022).

235 Australian Government, Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws (ALRC Report 129)*, https://www.alrc.gov.au/wp-content/uploads/2019/08/alrc129finalreport.pdf (last visited Dec. 30, 2022).

236 *Id*, at 459.

237 *Id*, at 477.

238 *Id*, at 460.

doi:10.6342/NTU202302025

1997 年電信法第 313 條第 3 項和 2004 年的監視設備法之數據破壞令，本節即欲探討此等授權依據於澳洲法上之合法性。

透過上文可以得知，在缺乏憲法明文保障言論自由之背景下，澳洲的立法者於管制言論之政策制定上，具有較大的空間，也較容易發展出強硬的管制手段。是以，在對權利重大影響時，所要求「法律」層級授權之原則，可以預期不會遭遇太大的困難，蓋澳洲賦予立法者較多的權限去制定干預人民之規範，立法者也不會吝於授權干預。

而停止解析、網站阻擋等技術措施，於聯邦法上的授權依據為 1997 年電信法第 313 條第 3 項和 2004 年的監視設備法之數據破壞令涵蓋，二者皆屬於國會層級所設立之法規範，屬於最高層級之議會授權。政府為此類干預網路言論及域名財產權之行為時乃有所本，此點較無疑義。較有疑問者係上述授權依據本身是否符合合法性原則及比例原則之要求，以下分別討論之。

第一項 1997 年電信法第 313 條第 3 項

如前所述，電信法第 313 條第 3 項寬泛的提及政府機關於刑事追訴目的或國家安全維護時，得以請求 ISP 業者配合、協力斷網或是刪除網站內容等。本條於形式上給予了政府機關很大的權力，似乎只要有公益目的，國家便可以向 ISP 業者請求協力執法。

雖條文中有設定 ISP 業者所提供者乃限於「合理、必要」之協助。然而，本條之審查、運作程序及救濟方式等相關配套措施，於法皆未明文。是以何為所謂合理且必要之協助，於實際運用本條時，似乎僅需政府機關自行認定請求合理且必要，即得據此向 ISP 業者提出要求，實務上也未有事前向司法提出審查之案例。

學說上便對執法機關以本條逕行請求停止解析網站之作法，有所批評。反對論者主要提及之觀點有四：一、本條立法空洞，應引進令狀原則，經由司法事前個案具體審查。二、本條欠缺透明、公開的問責制度，容易有濫用之風險，也欠缺監督。三、救濟制度缺乏，一者是本條未規範執法機關之通知義務，故很可能發生人

doi:10.6342/NTU202302025

民根本不知曉自己的網站被關閉一事；二者即便發現了，因欠缺救濟程序之相關規範，也會形成有權利受干預卻無救濟管道之窘境。四、現行技術仍有所限制，無法百分之百精準執法，法規上卻又欠缺補償制度之設計，也有手段不合乎比例之疑慮。澳大利亞電子前沿（Electronic Frontiers Australia，簡稱 EFA）便舉出早期澳洲證券投資委員會曾使用電信法第 313 條第 3 項封鎖超過 250,000 個網站的例子，其中包含了許多非法的附帶損害[239]。

透過前述之批評，結合澳洲法上對基本權干預之合法性審查分析之。本文以為將文義寬泛、概括的電信法第 313 條第 3 項作為停止解析發動之授權依據，此作法未能通過合法性原則以及比例原則之審查。

首先，停止解析限制了網路言論之發表、接收，也使域名之使用效果不達，構成了普通法上所保障之言論自由以及憲法所保障之財產權的干預。政府之公權力行為構成普通法與憲法權利之干預，須通過普通法上合法性原則之審查，且該干預行為須為適當、合乎比例。另外，針對財產權之限制普通法上另外提出了干預非任意之要求。須通過上述原則之審查，始得謂合法之干預。

而**合法性原則**如前所述，其意義乃當法規沒有明文或是明確暗示的情況下，於法律解釋時將推定國會無意限制系爭權利，類似於我國法律明確性之概念。而電信法第 313 條第 3 項僅泛泛地指稱電信業者於特定情況下有協力執法機關為必要行為之義務，對於何謂「必要」行為，以及協力義務之範圍等，皆無進一步之解釋。此時，其實難以逕自認為停止解析乃此處被認為必要之協力行為，條文過於寬鬆，於法律解釋時難以推定國會有授權此技術運用之意。且如前述反對論者之批判，本條之執行程序、救濟方式、事後監督等皆於法無明文，難以推論國會有以此空洞條文授權網路言論管制措施之意，故本文以為本條未能通過合法性原則之審查。

---

[239] Electronic Frontiers Australia, *Submission Regarding the Inquiry into the Use of Subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operation of Illegal Online Services*, https://www.aph.gov.au/DocumentStore.ashx?id=14651c8e-5461-4ceb-b511-59a4c1566fed&subId=299629 (last visited Apr. 5, 2023); Bruce Baer Arnold, *Inquiry into the Use of Subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operation of Illegal Online Services, Submission 10*, https://www.aph.gov.au/DocumentStore.ashx?id=e8908f46-9df3-44a7-acd7-8d7588b02066&subId=299370 (last visited Apr. 5, 2023).

doi:10.6342/NTU202302025

而在**比例原則**方面，多數論者所關注之重點與美國法類似，即斷網之技術手段選擇。EFA 之報告便提出不宜透過 IP 過濾之手段進行斷網，蓋 IP 過濾過度封鎖之比例過高，容易構成違法執法。而雖停止解析屬於尚可接受之手段，但於個案中仍有造成附帶損害之風險，應於規範上併同設計補償措施，並且隨時注意技術之進展，盡可能地提高執法精準度。若否，仍於個案中有違反比例原則之風險。

至於對人民財產之干預，普通法上要求須為非基於任意者。而停止解析特定違法網站，乃對於域名財產使用之干預，惟此干預乃針對特定涉及違法之域名，並非執法機關任意挑選者，故就此原則較無疑慮。

綜上，依據電信法第 313 條第 3 項對違法網站實施停止解析，干預了普通法上言論自由與憲法上、普通法上所保障之財產權，條文卻過於空洞而未能符合合法性原則，技術實施上也有違反比例原則之風險，故本文以為，不宜以本條作為授權依據實施斷網措施。而實際上本條亦大有被濫用之風險，且現行制度上亦有其他詳盡規範之授權依據可以達到預防網路犯罪擴大之效果，故亦有論者主張從根本上應廢除電信法第 313 條第 3 項。

而澳洲政府雖未逕將本條廢除或停用，但後續便有針對電信法第 313 條第 3 項提出指導方針，增添了發動本條之限制（如：應將發動本條之案件限於涉及最高刑期為至少兩年以上之犯罪，以免執法機關針對小罪即發動斷網，反而違反比例原則），並建議執法機關於運用本條請求電信業者協助時，所需注意之程序要件（如：優先考慮其他執法工具的可行性，而將本條置於備位發動），以及事後應提出透明度報告，受第三方監督[240]。

第二項 2004 年的監視設備法之數據破壞令

透過上文之敘述，澳洲政府所提出電信法第 313 條第 3 項的指導方針，便將本條作為備位性之條文，當有其他規範得以作為授權依據時，便應以其為優先適用。

[240] Australian Government, Department of Communications and the Arts, *Guidelines for the Use of Section 313(3) of the Telecommunications Act 1997 by Government Agencies for the Lawful Disruption of Access to Online Services*, https://www.infrastructure.gov.au/sites/default/files/australian_government_guidelines_for_use_of_section_313_-_june_2017_0.pdf (last visited Apr. 5, 2023).

doi:10.6342/NTU202302025

而 2004 年的監視設備法所創設的「數據破壞令」，便是在阻止網站訪問此技術之實施中，較為具體之規範。

所謂數據破壞是指添加、複製、刪除或更改電腦中所保存的數據，並且按照澳洲政府機關對於數據破壞令適用之舉例說明，便包括了政府機關刪除網站上虐待兒童素材的內容、轉址或阻止對該網站的訪問等情形[241]。是以，於文義上很明顯的立法者授權了政府機關運用停止解析、域名轉址等技術斷網之行為，並無文義模糊之嫌，乃**符合合法性原則**之要求。

惟在**比例原則**方面，除卻技術手段之選擇問題，數據破壞令更是掀起了新的擔憂。在此區分必要性與相稱性討論。首先，在**必要性**方面，所涉問題係將數據破壞令廣泛的適用於任何類型之犯罪，是否有其必要。就此，由於數據破壞令除了單純的阻止網域之造訪外，更包括了對數據的變更、刪除，且容許秘密進行之。此比起單純的停止解析，對於民主政治抑或言論自由之影響，更為嚴重。故於討論上學說傾向採取嚴格之審查標準[242]。而規範上數據破壞令得廣泛的適用於三年以上之犯罪，學說上便認為，有些犯罪根本無須動用數據破壞令，性質上也不適合，例如：單純的財產犯罪。是以，應將數據破壞令之發動門檻嚴格化，應將之限於最嚴重的犯罪，且應同時考慮犯罪之類型、現行執法手段是否不足，以及是否為匿名犯罪而存在執法障礙[243]。

在**相當性**方面，學說上則是點出了由於數據破壞令之發動，係於犯罪早期即介入，其目的在於破壞犯罪，而非蒐證。是以，其發動門檻之要求頗低，僅須對犯罪存在或即將發生犯罪具備合理懷疑。然而，他的手段卻相當嚴厲，雖站在犯罪預防的角度，此乃及時有效之執法手段；但反過來說，在犯罪存在與否仍屬不明確之階段，卻授權政府以高破壞性的手段介入，有不相當之嫌。且於實務上可能變為偵查

241 Australian Government, Department of Home Affairs, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021/data-disruption-warrants (last visited Apr. 5, 2023).
242 Francis Maxwell, *When Good Is Not Good Enough: Evaluating the Proportionality and Necessity of the Australian Government Hacking Warrants*, 34(2) Criminal Justice 136, 148 (2022).
243 *Id*, at 143-44.

doi:10.6342/NTU202302025

機關用以規避較嚴格的證據搜查程序之利器，或甚至是用作犯罪誘捕使用。畢竟執法機關究竟於什麼時間點、變更了何種數據，事後難以檢驗與分辨。是以，學說上對此有主張，認為應提高數據破壞令法庭監督、審查之標準，且應避免秘密蒐證，或是於事後須向被告說明數據變更之細節，以免造成被告與執法機關之間於訴訟上的權力不對等[244]。故核發令狀之過程應採取嚴格審查，並且於核發時應同時將執法過程中對合法用戶的干擾也列入考量。

另外，在**正當法律程序**層面，亦有學者指出現行制度之不足，進而提出修正建議。於**事前程序**中，學說便對將令狀發動標準設定在合理懷疑有所質疑，認為在這麼低的發動門檻下，將使法官審查的程序流於制式化，反而架空法官保留之目的。而法官是否具備足夠的技術知識可以於令狀做出明確指示，並且斟酌使用特定技術對網路使用的影響，亦非無疑。故學者建議可以將此核發令狀之過程，多增設專家意見，以供法院諮詢。

而在令狀執行後的**事後程序**，雖規範上訂有執法機關之報告義務，惟報告上卻不會紀錄所取得之數據資料是否有供外部機關使用，對於越權、違法執法也未設有處罰之規定，難以嚇阻違法取證[245]。故學者主張應於規範上明定執法後的應報告事項，以及數據之銷毀與處理過程，並增訂懲處規範，以免執法機關濫用權力。

第三項 小結

澳洲法上對於網路言論的管制措施有多種途徑，而本文所關注的係政府機關主動發出命令，請求電信業者及 ISP 業者配合之命令。規範上有二者，一為 1997 年電信法第 313 條第 3 項，本條乃寬泛的課予電信業者協力義務，換言之，政府機關得以不拘形式的通知，命令其配合執法；二者則是 2004 年的監視設備法之數據破壞令，執法機關得向法院聲請此令狀，逕而請求電信業者執行數據破壞。

停止解析似乎皆得被兩者之條文涵蓋，惟電信法第 313 條第 3 項之文義過於寬鬆與模糊，難以直接觀其文義便推導出停止解析之授權，故本文以為其未能通過

[244] *Id*, at 148.
[245] *Id*, at 147.

doi:10.6342/NTU202302025

合法性原則之要求。而於實務上，政府機關也對本條之運用作出限制，認為應將本條作為備位性質，於有其他具體之執法工具時，應優先適用其他條文。

故就此，執法機關欲使用停止解析技術時，理論上應先向法院聲請數據破壞令。此乃創新之令狀，有別於美國法將停止解析套用於扣押、沒收之作法，澳洲採取新立法之方式解決網路犯罪、違法域名之問題。數據破壞令之文義清晰，符合合法性原則。且其程序規範嚴謹，設計了相對法官保留與事後報告義務等，但學說上仍有指出其不足之處。在比例原則層面，由於數據破壞令之破壞力極強，不僅僅可以斷網，甚至可以更改目標電腦內的數據、或是刪除資料等，可以涵蓋多種駭客技術；然而，本令狀的定位卻非犯罪偵查與蒐證，而是在犯罪前期介入，破壞犯罪之遂行或是迅速降低犯罪損害。故學說認為在犯罪是否存在仍屬不明朗的狀態，於核發令狀之審查上應從嚴，且於授權技術使用時也必須將對公眾的影響等皆納入考量，不宜任意的使偵查機關發動威力如此大的武器。而在正當法律程序上，也應該進一步的於核發令狀階段納入專家意見，並於規範上詳列執法後應報告之事項，以利事後之監督與咎責。

綜上，數據破壞令乃停止解析合法之授權依據，惟其於個案運用中有違反比例原則、正當法律程序之風險，並考量其手段之嚴厲性，應於核發令狀之審查時從嚴。

第四節 分析與比較

本章整理了澳洲法之網路管制制度，其面對新興的網路犯罪議題，選了跟美國法不同的路徑，並非在既有的規範中尋求適合的授權依據，而是以創新令狀之方式面對問題。並且以概括式的條文作為備位依據，當現行規範中無法找到適合者，則可以援引電信法第 313 條第 3 項，請求電信業者配合政府機關執法、斷網。

本文另探究了澳洲法制背景的特殊之處，即其憲法中並未設有權利憲章，即憲法中未保障基本權。雖其於普通法以及簽署之國際條約中，仍有保障人民權利之義務，惟可以發現，澳洲的立法往往更激進，以達到執法目標為優先考量，對於人民

doi:10.6342/NTU202302025

權利之保障則較為忽略。而此背景另造就了審查條文合法性之差異，對於普通法權利之干預，所應符合者乃合法性原則，此亦與美國法或我國法之干預合法性審查有所不同。

本章分別以合法性原則、比例原則、正當法律程序之要求，檢驗了澳洲現行實務上運用數據扣押令之不足與爭議，並提出學者建議之修改方針或實務操作之應注意事項。下文將分析澳洲之作法，並與我國之法制背景比較，探究此類「寬鬆備位性的授權」與「創新立法」之方式是否適合援引至我國。

第一項 優勢

1997 年電信法第 313 條第 3 項的優勢，在於其文義上富有彈性，即便技術一直更動，也幾乎會被文義所涵蓋。在科技日新月異的現代，此類寬泛的授權依據，足以避免立法緩不濟急之窘境。且本條對於通知電信業者之程序無特別的要求，於執法上而言，可以有效率的達到打擊犯罪之效果，而不用耗費大量的時間成本。

2004 年的監視設備法之數據破壞令，則是具體、創新的立法。其於文義上具體化、更貼切的描述了技術的內容，可以讓受規範者預見執法機關所可能使用之技術為何。相較於美國以扣押、沒收之方式處理停止解析之問題，這種創新立法的方式較不會遇上文義解釋衝突，也能夠明確立法者授權之範圍。且針對特定技術創立令狀，更能夠考量到技術之特殊性，為其量身打造條文，而不會造成規範上容許，實務上卻難以操作之問題。

第二項 隱憂

1997 年電信法第 313 條第 3 項的隱憂，則同樣源於其寬泛、概括式的文義。法條涵蓋的範圍廣泛，卻同樣的導致了讓受規範者無法預見之情形。似乎任何與犯罪偵查、國家公益有關的事項，政府機關皆得以此請求電信業者協力，斷網抑或刪除網站內容等等，法條中並未具體化「發動要件」、「授權技術範圍」及「請求協力之程序」等要件，對於司法審查與事後監督等制衡機制也付之闕如，此在學說上被大肆批評，認為本條有極大的濫用風險，且對於電信業者而言也難以解釋何以負

doi:10.6342/NTU202302025

有此協力義務，以及該配合政府執法至何種程度，是否導致消費者的不信任等等，故有論者主張本條應刪除。

面對新興科技的發展，在政策上究竟要採取以新立法的方式去創設授權依據，抑或在現有條文中尋找相似性的規範，並無絕對的答案。在立法量能足夠時，本文以為自然是新創設之立法能夠較為貼切且精準的授權，去考量技術的特性而設計出完整的規範，立法者也可以將技術對人民權利所造成的干預全面性的思考，斟酌配套措施。然而，此種作法最大的問題就在於立法效率，科技進步日新月異，若每一次發展出新的技術都必須重新立法，很可能發生立法速度追不上科技發展的情形。且每一次重新立法也都必須花費大量的時間、成本；而針對特定技術的立法，其授權範圍亦較狹窄，文義有所侷限，未來的新技術不一定可以援引此時的立法作為依據。是以，澳洲所採取創設新令狀的方式，本文以為最大的隱憂，以及對我國來說難以效仿的癥結，或許便是立法緩不濟急之問題。

除了立法時間與成本的考量外，澳洲 2004 年的監視設備法之數據破壞令，另一個特殊之處在於其與傳統的強制處分目的不同，一般刑事偵查程序中的強制處分，發動目的係在於保全訴訟程序之進行（保全人、證物於訴訟程序中存在），數據破壞令則是於規範上便開宗明義，其令狀核發之目的係為了破壞、預防犯罪。是以，只要合理懷疑有犯罪存在，且透過變更數據可能阻止犯罪遂行，或是減少犯罪損害，便得以核發數據破壞令。

刑事訴訟中的強制處分，大多是為了保全證據所存在；惟在警察法中，其實為預防犯罪而對人民施加處分，並非少見。是為預防目的施以國家公權力，並不是數據破壞令為人所詬病之處。其問題在於，數據破壞令所授權之行為，對於人民的隱私、IT 基本權及言論自由等基本權干預至深，容許國家秘密的駭入人民的電腦更改數據。如此嚴厲的強制手段，卻只需要對犯罪存在具備合理懷疑，便得以發動，有輕重失衡之嫌。學說上便有認為，出於預防觀點發動之處分，應該要比犯罪追訴

doi:10.6342/NTU202302025

目的有更高規格的要求[246]。發動門檻應提高，於核發令狀之審查程序也應該採取嚴格標準，謹慎地將對人民權利的影響全面性的考慮。

另一方面，數據破壞令之存在也造成了新聞媒體業的隱憂。蓋數據破壞令賦予了執法部門秘密訪問電腦上保存的數據以進行破壞活動（添加、刪除、複製或更改數據）的權力。通過這種方式，數據破壞令有能力對媒體的工作產生獨特的影響。舉例而言，執法部門可以利用數據破壞令以刪除或更改傳遞給記者的消息來源訊息、刪除記者持有的數據，甚至在新聞報導發布之前刪除或更改整個新聞故事，製造假消息。因此，數據破壞令不僅有能力阻礙記者和消息來源之間的訊息自由傳遞，並且還可以用來審查向公眾傳播的資訊[247]。

而此類在記者、消息來源或媒體組織不知情的情況下，秘密進行的數據破壞令，不僅有能力阻礙媒體的日常運作，更可能破壞新聞自由和獨立媒體的本質。即使相關受令狀影響之各方於事後意識到數據破壞令的存在，新聞自由也已經受到干擾，而且將來可能會繼續受到干預[248]。縱使該數據破壞令事後被認定為無效，損害也已經造成了，尤其在講求時效性的新聞產業中更可能產生難以回復之損害。

第三項 我國法比較

澳洲法與我國法制之主要差異有二：一、程序嚴謹程度不同，二、立法量能差異。關於前者，可以分別從基本權保障以及澳洲法條文設計二種角度觀察。就基本權來說，如前所提及，澳洲憲法之特殊之處在於欠缺權利憲章之設計。雖然其後透過普通法解釋以及國際條約之簽署，言論自由與財產權在澳洲仍是受到保護者，惟不難想見其保護程度與源於憲法的保障有所落差。而從澳洲法制之條文觀察，本文於查找文獻之過程中，也發現雖然澳洲同為民主自由之國家，但其很容易創設限制人民基本權利之公權力措施。於條文設計上，澳洲之立法者傾向採取嚴厲、強烈的

246 *Id*, at 140-41.
247 Sarah Kendall & Dominic Frost, *Network Activity, Account Takeover and Data Disruption Warrants: How Novel Law Enforcement Powers Impact Media Freedom*, 28(2-3) Australian J. Human Rights 249, 262 (2022).
248 *Id*, at 263-64.

doi:10.6342/NTU202302025

干預手段，（如：澳洲國會過去曾討論要創設澳洲版的網路長城[249]，對網路進行強制審查過濾）卻通常並未將處分發動之事前審查、依循程序以及事後救濟等保障措施列於條文中。此部分與我國刑事訴訟法將強制處分以及救濟方式完整訂定於法條之方式不同。是以，在比較澳洲法時，本文較難逕將澳洲對於網路管制之作法援引至我國刑事偵查程序之立法。惟並非毫無參考之處，於撰寫本論文之過程中，本文反思雖我國目前係採取如美國作法之域名扣押模式，然對於言論自由之保障，是否有必要同美國一樣採取如此高規格之保障密度，非無討論之空間。反觀澳洲，便並未將言論自由保障置於如此崇高之地位，卻不一定導致對人民權利之過度侵害。是以，在後續我國法討論之章節，本文將會就此議題重新思考，言論自由保障與刑事追訴公益之調和。

而關於立法量能差異之部分，則是造就了在比較澳洲法時，本文認為創新令狀之模式難以為我國所採用。雖立法論上非不得討論，但若欲解決現況非法域名之問題，在我國現行之刑事訴訟法中尋找解答，是較為可行之作法。故澳洲 2004 年的監視設備法之數據破壞令，或許能供我國未來立訂新法時，做為參考。惟於立法時仍需注意在預防犯罪目的下，於犯罪前階段施加之處分，不宜對人民權力過度干預之問題。在手段方面要重新設計破壞性較低者，或是再增添更高規格的事前審查機制，如絕對的法官保留。

第四項 我國法援引可能性

在網路言論管制的規範面，除了刑事訴訟之偵查手段外，法制上也有從網路平台、電信業者及 ISP 業者之中介者義務切入者，惟此二者乃得以同時存在而不衝突的，合先敘明。是以，澳洲法中關於中介者義務之設計，或如澳洲電信法第 313 條第 3 項被動的協力義務，或有我國得參酌之處。且我國也於近年有關於網路平台業者之義務討論，如數位中介法草案第 5 條，便提及為了犯罪之偵查或追訴，政府

[249] Chris Williams-Wynn, *The Great Firewall of Australia: The Political Concerns*, 26(1) Policy Magazine 33, 33 (2010).

doi:10.6342/NTU202302025

得以限制中介者提供數位服務[250]。是若援引澳洲法，於法制上課予 ISP 業者或電信業者協力執法之義務，並無不可。惟於條文設計上仍須注意，應就協力義務之範圍界定清楚，於何種特定情形，政府機關應通過何種審查、通知程序，以及協力執法之程度為何，後續應如何持續配合維護等，這些都應該清楚明定，而不可像電信法第 313 條第 3 項僅以模糊的條文為之，以免造成業者過大的負擔，使其無所適從，只能全面、無篩選地配合政府機關而造成濫權危機。

而在政府機關主動發出命令之情形，澳洲法所採取的兩個方式，創新令狀並搭配寬鬆的備位條款，於我國是否有採用之可能，存在討論空間。首先關於新立法之部分，本文以為以我國立法之量能與速度，有所困難。此也是導致本文與我國學說上，目前對於停止解析的討論，大多聚焦在是否合於扣押、沒收之條文。蓋創新立法毋寧是於法律保留層面較不致遭遇瓶頸之作法，惟以我國現況推論，立法緩不濟急之情形在所難免。為了及時地解決現有、近幾年內的網路犯罪問題，先以現有的規範應急，於我國而言屬於較為實際的選項。然而，一邊以現有的規範授權執法，一邊於法規範面重新設計妥適的條文，似乎是能夠衡平「立法時間」與「精準授權」的作法。

再者，關於寬鬆的備位條款，本文則以為我國法非不得援引或採用。雖寬鬆的授權依據有上述種種之疑慮，且有容易造成法律明確性原則之違反。惟若將之作為備位性之條款，僅在現行規範無法尋覓到適合者時，才作為臨時性、應急的授權依據，似乎可以解決未來若碰上無法對應到現有條文的新技術時，所面臨之窘境，此即學說上所提「門檻理論[251]」之概念。蓋於我國之法制下，國家公權力對人民所為之基本權干預措施，仍須遵守法律保留原則。但須注意，此類一般授權條款，文義上未能特定干預措施，對於人民而言可預見性較低，故僅能用作輕微干預之授權。

[250] 數位中介法草案第 5 條第 1 款第 3 目：「提供數位中介服務，除依法律規定且符合下列事項者，政府不得限制之：一、符合下列目的之一：（三）犯罪偵查或追訴。」

[251] 關於門檻理論之理論基礎與內涵，詳參林鈺雄（2007），〈干預保留與門檻理論—司法警察（官）一般調查權限之理論檢討〉，《政大法學評論》，96 期，頁 189-232。

doi:10.6342/NTU202302025

若新興技術對於人民之基本權干預並不輕微，仍不應引用本條作為授權依據，以免侵害人民權利過劇。

doi:10.6342/NTU202302025

第五章 我國法

本章將探討，將我國刑事訴訟法的扣押針對域名發動，並且於境外註冊之域名以停止解析之方式執行，此強制處分措施是否通過基本權干預合法性之審查，以及各個階層的審查中，目前遭遇之法學爭議，參考比較法制並於本章一一探討，期許透過本章之論述，能加強我國實務使用域名扣押之正當性以及論理依據，並於後思考以刑事訴訟作為網路言論管制之手段，現行法是否有不足之處；或是參考比較法制，思考強制處分以外的管制模式，進行立法論之探討。

第一節 基本權限制

關於域名扣押對於基本權的限制，上文已經多次提及與言論自由、財產權有關。惟於說明上無較細緻之討論，故將於本節以我國對於基本權之理解，進一步探討。另外，由於扣押對於財產之使用干預，並不僅僅限於此二者，故本文在此將稍微深入的說明與其他基本權之問題。

一、言論自由

首先，在言論自由方面，其實不無質疑，網站之內容是否屬於言論？以及下一個層次的問題，若網站內容屬於言論，則違法之言論是否屬於憲法言論自由之保障範圍？若以本文緒論提及之侵權網站為例，集合侵害著作權影片之網站，其單純的集合著作似未含思想之表達，則是否可以將之歸類為言論，或有討論之空間。

依據國內學者整理網路不當資訊的類型，包括：妨礙名譽（如：在網路上公然侮辱他人）、侵犯他人隱私（如：未經同意公開他人個人資料）、侵害著作權（如：販賣或散佈盜版影片或文字等）、網路色情（如：張貼色情圖片、提供空間供不特定使用者張貼、散佈或討論性交易訊息等）、煽惑他人犯罪、販賣違禁品（以網路

doi:10.6342/NTU202302025

為媒介，販買管制毒品或醫生處方藥）或散佈足以使人反感、噁心或驚懼的資訊（如屍體、合成靈異照片或血腥圖片等）[252]。

而上述類型之網站，不當或甚至構成違法之網頁內容是否屬於言論與表達，則涉及何謂「言論」之探討。所謂的言論，其範圍可以說是相當廣泛，凡是透過言語、寫作、行動或其他具有表達或溝通功能的方式，展現或表達個人內心的想法與意見，或藉以達成說服人的目的，都屬於言論之一種[253]。而在前述不當網站之類型，大多數皆含有思想的表達，如：色情內容、煽惑犯罪或販賣違禁品等，較有爭議者或許是侵害著作權之網站，其形式上看起來僅是在蒐集作品，且建立網站者之目的亦非在於透過作品傳遞思想，而是為盈利之目的。惟仔細探究之，即便其網站創立目的是為了營業，在作品中插入廣告內容，抑或是純粹提供盜版片源之行為，其實都隱含了思想之傳遞。如常見的廣告一般，於釋憲實務上也將其認定為商業性言論，僅保護層級較低，卻不會逕行將之劃定為「非言論」。學理上，凡是個人自主的表現與言論皆屬於憲法言論自由所欲保障者[254]。

是以，不論是否僅是單純的資料搜集或整理，僅僅的分享行為也是所謂的意見與思想之表達。是就此確認了網站之內容亦該當「言論」。

確認上述內容皆屬於言論之範疇後，則進一步討論，言論自由之基本權射程範圍，是否包括涉及違法之言論？若包含，則當國家進行干預時，必須符合法治國原則。就此，涉及言論自由之理論基礎探討。學理上認為言論有民主自治、真理追求、自我實現與社會安定等多元價值[255]；我國釋憲實務上也大多採取綜合理論之見解，認為言論自由有助於實現自我、溝通意見、追求真理及監督政治[256]。其中，「自我實現」之理論，即認為言論是否受到憲法保護之判斷標準，並不在於該言論是否對

[252] 許育典（2004），〈臺灣學術網路的教育性及其不當資訊管制規範：兒童與少年人格開展的保護觀點〉，《教育政策論壇》，7 卷 2 期，頁 213。
[253] 劉靜怡（2004），〈『言論自由』導論〉，《月旦法學教室》，26 期，頁 74。
[254] 林子儀（1988），〈言論自由之理論基礎〉，《國立臺灣大學法學論叢》，18 卷 1 期，頁 266。
[255] 賴祥蔚（2011），〈言論自由與真理追求—觀念市場隱喻的溯源與檢視〉，《新聞學研究》，108 期，頁 104。
[256] 司法院釋字第 509 號解釋主文。

doi:10.6342/NTU202302025

他人（聽眾）有功用，而是在於該言論是否為**表意人自主的表現**。如為表意人自主的表現，即應予以保障[257]。

是以，在此基礎下，我國學者對於言論自由之保障範圍，普遍傾向從寬認定之見解。先將言論劃入憲法所保障之範圍，再決定保障之程度高低，考量限制之方式[258]。而回歸本文關注的違法網站，其網站內容依前所述，於我國上仍屬於言論自由之保障範圍，只是此保障非屬絕對，非不得限制之。故政府透過技術管制該等內容之傳遞，仍屬於對言論自由之干預行為，由是，將於後討論該管制措施對言論自由干預之合法性。

二、財產權、營業自由

我國釋憲實務中，與財產權相關之解釋為數眾多，惟卻少見對於財產權之內涵與其保護領域之正面定義。司法院大法官第 400 號解釋曾簡要揭示，「憲法第十五條關於人民財產權應予保障之規定，旨在確保個人依財產之存續狀態行使其自由使用、收益及處分之權能，並免於遭受公權力或第三人之侵害，俾能實現個人自由、發展人格及維護尊嚴。」此定義近似於所有權保障之概念。惟隨著實務長期發展，後續之解釋已不必然跟隨著此定義發展。故有學者透過整理釋憲實務軌跡，試圖描繪財產權之保障內涵，其中，動產、不動產、債權、無體財產權皆已被認定屬於憲法財產權之保障範圍內[259]。是以，雖域名之財產性質有所爭議，惟不論如何定性（無體財產權或債權），其都是我國憲法上所保障之財產權範疇。

另一個問題是，作為犯罪工具使用、用於違法用途之域名，是否仍屬於憲法財產權保障範疇？蓋或有認為，財產權乃制度性之權利，其權利係透過立法創建財產制度而生，則其本身即蘊含了社會義務。人民自應於合乎規範之範圍內享受權利時，若用以違法用途，則該權利是否仍受憲法、財產制度所保障，則非無疑。

---

[257] 林子儀，參前揭註 254，頁 262。

[258] 在美國憲法上確實有部分言論被劃定為不受憲法所保障者，惟此並非恆古不變之標準，在社會觀念之流動下，亦有過往被認為不受保障者，轉化為受憲法保障之言論。劉靜怡，參前揭註 253，頁 82-83。而在我國關於言論自由的釋憲實務上，雖在審查模式上常見參考美國作法，惟對言論自由射程範圍，則大多採取寬鬆認定，而不會在前階段即排除言論受保障之可能性。

[259] 蔡維音（2006），〈財產權之保護內涵與釋義學結構〉，《成大法學》，11 期，頁 38-41。

doi:10.6342/NTU202302025

我國學說上對於犯罪物沒收之性質，係將之定性為獨立於刑罰、保安處分以外之法律效果，而其發動基礎則係源於犯罪行為人「濫用財產權」，使國家有正當性而得沒收犯罪物。此論述之前提，即係該物之所有人對於沒收標的之財產權，仍受憲法所保障，故國家才需額外具正當性之理由始得發動沒收干預。準此，即便是用以促進犯罪之工具，其仍屬於受憲法所保障之財產權，僅是因為其與犯罪有所連結，國家為預防社會危險或遏止行為人利用同一工具再犯，得為追求此公益，於符合法律保留、比例原則之情況下限制行為人之財產權[260]。是以，在域名沒收與扣押，即便域名是用以違法用途之犯罪工具，國家對其停止解析，仍構成對人民之財產權干預，需檢驗干預合法性。

併予敘明，其實某部分的域名扣押另外會涉及營業自由之干預，例如，販賣違禁品、媒合性交易等網頁，國家對此類網站發動扣押，此乃對於網站架設者營業方式、營業活動自由之限制。按司法院大法官第 514 號解釋，人民營業之自由為憲法上工作權及財產權所保障。其中，在此亦生類似之爭議，即違反法令之工作、營業是否仍受憲法所保障？此即工作權是否存在「內在界線」之爭議。而本文在此認為，內在界線將使基本權之保障範圍過於限縮，國家為促進公共利益，非不得以合乎比例之手段限制之，不需要於基本權保障範圍界定之審查初階段，即逕行將之排除。是以，基於各種不同類型之網頁，偵查機關發動扣押時，所干預之權利亦將有部分差異，惟通案性的說，大部分的案件仍是以言論自由、財產權為主要干預者，而部分案例中對於營業自由、工作權的干預，則可以將之納入審查標準調控之因素之一。

三、IT 基本權？

過去刑事訴訟的單一強制處分通常只涉及個人的某一基本權，但在現今社會中，對電腦或網路發動偵查，則可能涉及複數基本權。尤其在今日社會，電腦龐大的運算能力與儲存空間，提供個人社交管道、線上儲存隱私資料，人們生活已離不開網路世界。而電腦與手機也無時無刻記載著人們的電子足跡，什麼時間點使用了

[260] 陳建廷（2022），《犯罪物沒收》，頁 72-73，國立臺灣大學法律研究所碩士論文。

doi:10.6342/NTU202302025

何種應用程式、瀏覽了什麼網頁、與誰電子通訊或甚至是該通訊內容為何等，皆非技術上所不得破解者。是以，若將電腦稱為帶有高度人格內涵的個人資料庫，並不為過[261]。

如前所述，對於網路之使用發動強制處分，可能導致複數基本權之干預。且隨著科技進步，並非每一種強制手段之發動，都可以將其干預套用於現行傳統基本權之概念下。換言之，現今社會中人們對於網路之使用有高度之依賴性，同時也難以接受網路遭到國家無端的管制，惟卻囿於無法於傳統基本權找到受干預者，而無法檢視、監督國家之公權力行為，有保護不周之疑慮。

是以，學說上有參酌德國法院之實務見解，創建了一新興基本權概念，即「IT 基本權」。IT 基本權，完整稱作**資訊科技基本權**，其所保障者乃資訊科技系統的私密性與完整性，文獻另有稱之為「電腦基本權」。其保障基礎係基於資訊科技之使用，與人格發展及人格之危害具緊密連結，因此德國聯邦憲法法院認為有以基本權保障之需求。且通訊秘密保障自由、隱私權並沒辦法完整的涵蓋 IT 基本權之概念，單純侵入手機或電腦的行為，卻未進一步干預通訊，也未截取之個人隱私資料，尚難構成前述權利之侵害。但此舉已足以使人民感到不安，並對資訊科技不信賴，故有前置保障此資訊科技完整性之必要[262]。

IT 基本權的保護範圍係利用資訊科技系統製作處理、儲存資料的私密性。一旦資訊系統受到攻擊，以致他人可未經本人同意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。另應注意，德國聯邦憲法法院是將 IT 基本權當作人格權範疇內的一種補遺性基本權，只在其他特別基本權保護範圍所不及時，才加以檢驗。換言之，IT 基本權是一**前置性保障與補遺性之基本權**，受干預者如無其他一般基本權可資主張時，至少還有 IT 基本權可作為防禦權利的最後一道防線[263]。

[261] 王士帆（2016），〈網路之刑事追訴—科技與法律的較勁〉，《政大法學評論》，145 期，頁 343。
[262] 同前註，頁 345。
[263] 同前註，頁 345-346。

doi:10.6342/NTU202302025

而國家發動域名扣押、停止解析時，是否構成 IT 基本權之干預，而有加以檢驗之必要呢？本文以為，雖停止解析之發動，將干預網路使用之效能，使他人無法正常解析、造訪網頁。然而卻不會產生使他人得使用網站系統之效能與運算，或甚至窺探、儲存網頁內容之效果，似未妨礙資訊系統之私密性。於系統完整性而言，則似有構成干預，蓋人們使用網路時，係預設使用未受政府審查與干預之系統。而停止解析造成了網路系統之可使用性遭受限制。由於此基本權之保護領域上處於發展階段，是否構成干預尚不明確，惟基於 IT 基本權僅是補遺性權利之觀點，既然域名扣押已明確構成前述言論自由及財產權之干預，則似乎無特別援引此備位性且尚有待實務發展之新興基本權。

總結，本文於我國法之討論，仍將域名扣押所干預之基本權，關注於言論自由與財產權之限制，而就此為干預合法性之審查，以及爭點討論。

第二節 法律保留

按刑事訴訟法第 133 條第 1 項，可為證據或得沒收之物，得扣押之。故在法律保留層次，需討論之問題乃本條是否得作為對域名發動扣押之法律授權基礎。本節將就法條之各個要件一一拆解討論。

另外，於問題意識之章節已說明，由於域名之存在本身無法用作犯罪事實之證明，或縱於個案中域名得作為證據，亦不妨礙其遭沒收扣押之可能，兩者並不相斥。因此本文於域名扣押之討論方向上，乃針對為保全沒收所發動之扣押。基此，首先須先討論域名是否屬於刑法上得（或應）沒收者。

第一項 域名屬犯罪工具，得沒收

在現行我國之沒收法制下，依照其標的，可以將沒收區分為兩種類型：「犯罪物沒收」與「犯罪利得沒收」，其分別之依據為刑法第 38 條與刑法第 38 條之 1。其中，後者之沒收標的為因犯罪行為人的犯罪而有利得，如：為了犯罪而獲取的報

doi:10.6342/NTU202302025

酬或產自犯罪之利潤[264]。惟查，在各式網路犯罪中，域名乃犯罪行為人向網域註冊管理者付費所申請，用於系爭非法網站之經營與傳播。是以，域名並非犯罪行為人產自犯罪的利潤或為了犯罪而得到的報酬，而是使用於犯罪的財產。故討論方向上撇除犯罪利得之沒收，而是以**犯罪物沒收**之審查體系思考域名之沒收議題。

我國刑法第 38 條將犯罪物沒收體系，區分為「違禁物」、「供犯罪所用或犯罪預備之物（即犯罪工具）」與「犯罪所生之物」沒收，此體系與所繼受的德國法有所不同[265]，也造成了我國犯罪物沒收一些實務操作上之困難[266]。此處暫且放下學說上對我國犯罪物沒收體系所提出之疑慮，以我國現行法制思考對域名發動沒收之依據。

於犯罪物沒收之審查順序，應**優先思考**是否構成刑法第 38 條第 1 項之違禁物沒收[267]。學者認為此處所謂的違禁物，係指依法令禁止私人製造、持有或使用之者[268]。蓋自違禁物沒收之目的以觀，其係基於維護社會秩序與公共安全的預防考量，故判斷依物本身的物理性質與狀態具社會危險性者，即得發動沒收。換言之，只需單純的持有便會成立犯罪者，始為此處所稱之違禁物。查域名本身僅是中性之存在，於日常生活中網路之使用，人人皆得使用域名以導引他人造訪網頁，域名之存在本身不具社會危險性，故並非刑法第 38 條第 1 項之違禁物，須接續審查是否屬於犯罪工具或犯罪所生之物。

而第 38 條第 2 項中所謂犯罪所生之物，係指產自犯罪之物，例如偽造之文書及貨幣，而此亦非一般網路犯罪中域名之角色。

是以，剩下可能討論的是第 38 條第 2 項前段「供犯罪所用或犯罪預備之物」，此主要是指犯罪工具而言。「供犯罪所用之物」是指該物實際上在犯罪流程中供犯

---

[264] 林鈺雄（2022），《新刑法總則》，10 版，頁 721。

[265] 德國法上是將犯罪物沒收區分為「犯罪工具」、「犯罪產物」與「犯罪客體」。我國法上獨有的違禁物沒收，定義不清，且容易與其他犯罪物概念重疊或沒收競合。林鈺雄（2020），〈初探犯罪物沒收—最高法院相關裁判之綜合評釋〉，《法學叢刊》，65 卷 3 期，頁 9。

[266] 林鈺雄（2023），《沒收新論》，2 版，頁 50-52。

[267] 林鈺雄，同上註，頁 61-63；王士帆，參前揭註 261，頁 57。

[268] 李聖傑（2016），〈犯罪物沒收〉，《月旦法學雜誌》，251 期，頁 69。

doi:10.6342/NTU202302025

罪之用；「犯罪預備之物」係指該物依行為人之犯罪計畫，準備用以犯罪而言[269]。而對於犯罪工具是否須以該物「專供」犯罪所用為必要，過往實務、學說上則有所爭議[270]。108 年度第 4 次刑事庭會議採取「專供說」，認為毒品危害條例第 19 條第 2 項「供犯罪所使用之交通工具」須與犯罪具「直接關連性」[271]，並依社會通念具有促使該次犯罪行為實現構成要件者，始得認定為犯罪工具而得沒收。若採此見解，則於個案中可能無法對域名發動沒收。蓋同一組域名的使用，或許不僅用於系爭違法網站，也可能曾經作為其他網站的指引，而非專門用以該次犯罪。

惟專供說於我國實務上之操作並固定標準，在相似的案例下，不同法院仍時常做出不同的判斷。且學說上對此說亦有所質疑，首先，所謂的工具蘊含著「便利」、「幫助」之意，而非以「不可或缺」、「唯一手段」為概念內涵[272]。再者，物與犯罪之間的關聯性，乃高、低之程度差異，而非僅是零或一的問題。故是否對一物發動沒收，應以其對於犯罪促進的貢獻度高或低來判斷。

是以，在學說之理解下，犯罪工具泛指用以或準備用以**促進犯罪的幫助物**，包含積極促進犯罪實現或消極排除犯罪障礙，只要對於構成要件實現有某種關聯性或貢獻度即可，不以其「專門」用作犯罪使用為必要。而本文亦較贊同此說法，蓋一物是否專門用於犯罪並不重要，重點仍在於該物對犯罪遂行的幫助程度，是否達到剝奪其財產權之必要，以預防該物再度被用於犯罪。且採取專供說將使得犯罪工具之沒收容易規避，只要犯罪行為人於犯罪前將物用作其他用途，就能夠輕易規避專供說之下的犯罪物沒收。

而域名之存在之於前述網路犯罪（散布猥褻影像、公開傳輸他人著作、發表危害國家安全之言論等），大多係扮演協助「散布」、「公開」及「發表」之工具，

---

[269] 林鈺雄，參前揭註 264，頁 730。
[270] 林鈺雄，參前揭註 266，頁 64-69。
[271] 在此需注意，毒品危害防制條例乃刑法之特別法，依刑法第 38 條第 2 項乃優先適用。而前述所提之實務見解「專供說」，係對於毒品危害防制條例第 19 條第 2 項之見解。是實務上並未逕自對刑法第 38 條第 2 項之犯罪工具做如此限縮之解釋。惟不論是否為特別法，其對於犯罪工具沒收之法理乃相同者，皆是著眼於工具對於犯罪之促進。故明明是基於相同之法理，過往實務對毒品危害防制條例的犯罪工具沒收所為之限縮解釋，仍有討論之意義，故就此仍對此議題稍加著墨。
[272] 李聖傑，參前揭註 268，頁 65。

doi:10.6342/NTU202302025

且域名非僅僅在犯罪過程中偶然存在，其對於網路犯罪之實現乃具有「工具性」的存在，有助於網路犯罪規模的遂行及擴張。是以，域名於上述網路犯罪中，其定性上屬於犯罪工具，若屬於犯罪行為人所有或第三人無正當理由提供或取得者，得沒收之。

是以，在此確立了在刑事實體法上，域名屬於得沒收之犯罪工具後，於程序法上即得接續討論，針對犯罪工具之沒收保全所發動的扣押。在法律保留層次所探討的爭點便是圍繞著扣押的授權依據，刑事訴訟法第 133 條第 1 項，「可為證據或**得沒收之物**，得扣押之。」作為討論核心。

第二項 對「物」沒收

此處存在法條文義之解釋爭議。域名的非實體性質，與有體物有所區別。然而我國刑法中犯罪物沒收與刑事訴訟法中扣押之規定僅將「物」作為標的，究竟域名得否透過法律解釋成為扣押標的？

此處所涉之問題有二，一者是域名本身之權利性質定性，係債權、無體財產權抑或有體財產權？二者則是我國法刑法上供犯罪所用之「物」與刑事訴訟法上扣押「物」之解釋，是否包含無體物？以下分述：

一、域名權利定性

域名具有經濟上之價值，惟其於我國法制中，究竟屬於何種財產，則有待推求。我國民法侵權行為之請求權，依通說所採之差別保護說，所受損害係債權利益或物權將有請求上的區別。然而，對於有、無實體之物於我國法制上則無保護差異。是以，與美國法不同，我國學說於討論域名之財產性質時，大多正視域名的非實體性，討論上僅區分為「債權」或「無體財產權」此兩種見解，而不若英美法系國家發展出有體財產之見解。

（一）債權

有認為，網域名稱之取得係來自於註冊人與管理局間所簽訂之網域名稱註冊協議，而並非來自特定「法律」。此種註冊協議係有償取得使用權之繼續性契約，

doi:10.6342/NTU202302025

類似於租賃。此說認為，域名技術上專用而具有事實上唯一之性質，無法推導出域名具有物權般排他的對世效[273]；再者，基於我國採物權法定主義，於法無明文下無法將域名認作物權，且域名尚缺乏一般人之確信，亦不該當習慣法物權[274]。

（二）無體財產權

我國實務採此說，臺灣高等法院 91 年上字第 357 號民事判決與台北地方法院 98 年訴字第 1190 號民事判決，認為「網域名稱使用權為當事人間私法契約所賦予，屬於註冊人之無體財產權，具有讓與性」[275]。

而學說上也有論者認為，由於網域名稱使用權本質上具有**事實上的唯一性、變價性與可交易性**等智慧財產權之特徵[276]，即便缺乏法律明文，亦應以無體財產權或類似準物權來加以保障。

（三）本文見解

對於有體財產權說，有論者指出法院將域名與網頁之概念混淆了，域名與網頁就如同索書號與書本之對應關係，然實體存在者係書本，而非索書號；網頁確係實體存在於電腦硬碟中，但域名只是索引網頁過程中之指引，法院將其作為物理性之存在實屬有誤[277]。並且，於我國法上，對於有體、無體財產並無保護差異，是以毋庸同美國實務見解忽略域名「非實體」之性質。準此，本文以為有體財產權之說法不可採。

至於契約說，由於早期大多採用免費註冊域名之模式，採取契約說確實會遇上受理註冊公司是否有「給付域名使用」義務之障礙。且現行域名制度，域名註冊人可以隨時移轉域名至其他受理註冊公司，與契約相對的概念不符。且事實上唯一性與物權之排他、對世性，於現實效果上並沒有區別，故本文較認同無體財產權說之說理。

---

[273] 王奕華（2013），《網域名稱爭議處理—以統一網域名稱爭議解決政策（UDRP）為中心》，頁 11-12，國立臺灣大學法律學研究所碩士論文。
[274] 同上註，頁 10。
[275] 簡菀菱，參前揭註論文 41，頁 5。
[276] 陳劍釗（2009），《TWNIC 網域名稱爭議處理機制與我國民事訴訟制度之比較研究》，頁 17-18，國立高雄第一科技大學科技法律研究所碩士論文。
[277] Daniel Hancock, *supra* note 162, at 200-02.

doi:10.6342/NTU202302025

另參酌民法上對於「物」之定義，係指人體以外，人力所能支配，具有獨立性，能滿足社會生活需要的**有體物或無體物**[278]。查域名於現代科技下，透過域名註冊管理機構之技術，得由人力控制、儲存、及運用；且以社會經濟價值與效用判斷，單一域名即得獨立發揮引導網站、產生經濟效用者，具有獨立性。準此，於此觀念下，域名應屬「無體物」。

二、犯罪物沒收是否包括無體物？

將域名定性為無體物後，遭遇到的另一問題即是，刑法第 38 條第 2 項供犯罪所用之物與刑事訴訟法第 133 條第 1 項所謂得沒收之物，是否僅限於有體物？

就此，本文先討論沒收層面之問題，蓋必須是得沒收之物，才有討論沒收扣押之必要。此處域名是否屬於犯罪物沒收之標的，存有爭議。蓋即便在沒收新制後，立法者僅就犯罪利得之沒收擴張及於無體物，卻未對於原舊制遺留之犯罪物沒收進行進一步之解釋。是以，在法條文義之解讀下，或仍認為第 38 條第 2 項之犯罪物限於「實體」[279]，而域名自不在此行列。

惟不乏有主張對本條「物」之解釋應採取從寬認定者，以避免無法沒收之法律漏洞，並且在新法對於犯罪利得沒收標的已經擴張至非實體之權利下，更無區別對待之理由[280]。且本文亦認為，並無將本條限於實體物之必要。理由有二：（一）以文義觀之，「物」於法體系上的定義，本就不限於實體存在，如參酌前民法對於物之解釋，學者亦認同物係包含無體物之概念。（二）而以犯罪工具沒收之目的觀之，亦無將沒收標的限於實體物之必要，無論是實體物、無體物抑或權利，只要是對於犯罪之遂行有所促進且貢獻度高，便有預防再度被用以犯罪，或是制裁該財產權濫用行為之必要。而實務上也有肯定得沒收之財產不以有體物為限，尚包括無形之財產上權利[281]。

---

[278] 陳聰富（2019），《民法總則》，3 版，頁 165。
[279] 李聖傑，參前揭註 268，頁 69；薛智仁（2018），〈刑事沒收制度之現代化：2015 年沒收實體法之立法疑義〉，《國立臺灣大學法學論叢》，47 卷 3 期，頁 1071；陳建廷，同前揭註 260，頁 91-92。
[280] 陳建廷，同前揭註 260，頁 92-93。
[281] 蔡彩貞（2016），〈我國刑事沒收特別程序之建制與淺析〉，《司法週刊》，1805 期，頁 16。

doi:10.6342/NTU202302025

是以，本文認為作為無體財產權之域名，乃犯罪物沒收之標的，為得沒收之犯罪工具。

三、扣押標的是否包括無體物？

確認域名為得沒收之物後，接續討論，刑事訴訟法第 133 條第 1 項所謂得沒收之物，是否僅限於有體物？

既然無形財產權得沒收，對於刑事訴訟法第 133 條第 1 項得扣押之「物」之解釋亦無理由僅限縮於實體物。且觀察我國實務，亦時常發生無形扣押，例如以股票為標的。是以，本文認為**域名作為無體財產權亦屬於扣押標的**。從法條體系上觀察，第 133 條第 5 項，也對債權之扣押執行方式進行規範。若是同條第 1 項的扣押標的未及於「權利」，何以體系上會矛盾的出現關於權利的執行方式呢？

是以，本文以為無體物、無體財產或權利，皆屬於我國扣押之標的，而域名乃我國刑事訴訟法上得扣押之物。

第三項 停止解析是否符合「扣押」定義？

承第一章問題意識所述，域名扣押時，犯罪行為人仍能透過不受我國司法管轄之境外域名註冊管理機構，繼續支配或處分該域名；對境外註冊之域名發動停止解析，也只能阻擋我國之網路使用者之一般連線，外國使用者仍能連上該網站，此種情形與傳統意義上的扣押—即暫時「剝奪」被告之支配與占有，有所落差。故下文將討論停止解析是否仍該當「扣押」。

我國法上，有學者提及，參諸我國刑事訴訟法第 133 條之修法理由：「關於不動產、船舶、航空器之保全方法，不限於命其提出或交付」，足見扣押之方式，**已不限於現實上移轉占有**的情形，也包括以其他方式**對物之支配權干預**的情形[282]。是以，不論參酌美國法之解釋，亦或我國立法者之想法，停止解析干預域名使用之性質，於現行法對於扣押之理解，仍符合我國扣押之定義。

[282] 陳昱奉，參前揭註 129，頁 247。

doi:10.6342/NTU202302025

第四項 言論自由

法律保留層次中，尚存有一疑惑，即言論自由是否為我國扣押之規範所授權干預者？過去我國實務上不乏出現對於誹謗性雜誌、書籍等扣押，且在犯罪追訴過程中，亦無特別規定不得扣押文件、書籍等與言論相關之物。若作否定解釋，將使任何與言論發表有關之犯罪，皆難以保全證據與沒收。因此，本文以為尚無法排除立法者在此有授權對於言論干預之意，無須在法律保留階段即否定域名之扣押。惟不容否認，域名扣押相較於傳統扣押，在財產權以外有不容忽視的言論自由干預。而財產權與言論自由雖同屬基本權，但在違憲審查上，司法實務對於言論自由之限制傾向採取較嚴格之審查。因此，本文以為，關於言論自由之干預疑慮，可以於個案比例原則之審查及正當法律程序之階段，提高審查標準處理。

第三節 比例原則

通過法律保留之審查後，強制處分之實施，尚須符合比例原則。在本小節本文所欲探討者通案性的比例原則問題（**立法層次**），即選擇以停止解析作為域名扣押之執行手段，是否符合比例原則？

第一項 適合性—保全沒收必要性

進行沒收扣押時，除須標的據扣押客體適格，尚須具備「犯罪嫌疑之存在」、「沒收判決之可預測性」與具備「保全必要性」[283]。前兩者較容易於實際個案出現爭議，惟本文之前提係假設網路犯罪已存在，故就此不贅言。此處有疑義的是，針對域名停止解析，是否有助於沒收之保全，而具備扣押適合性？

傳統的扣押，係為保全證據或得沒收之物，而對其暫時占有之強制處分。針對前者所發動之扣押，其目的在於證據之保全，以利追訴並且防止證據湮滅；後者之

[283] 潘怡宏（2020），〈保全扣押之發動要件與扣押競合之處理〉，《沒收新制（五） 沒收實例解析》，頁 362-365。

doi:10.6342/NTU202302025

目的則是在於確保將來沒收之執行[284]。但偵查機關將網域停止解析，並不能達到保全證據之功能，蓋將網域停止解析，只能夠使一般使用者無法造訪網站，系爭網站之控制權仍屬犯罪者所有，網站之內容是否被變更、刪除，皆非停止解析所能防免者。退一步言，為達保全證據之目的，運用網頁截圖之方式也能夠達到，實無使用停止解析之必要，故就此方面言，難認有將停止解析運用於證據保全之需求。

而針對後者，停止解析與保全沒收**似**亦欠缺關聯性。以下區分註冊為境內、外之域名討論。

若欲沒收者為**境外**註冊之域名，真正要達到剝奪網域的沒收終局效果，於實際上仍須透過司法互助，請求外國政府或域名註冊、管理單位協力註銷域名[285]，使犯罪行為人喪失使用該域名之權限。是以，於我國對該域名施以停止解析**似乎**並無助於該沒收程序之保全，蓋施以停止解析與否，與境外單位是否協力無關[286]。然而，囿於我國之境外執法侷限，當外國執法機關不願協助執行我國沒收判決時，將停止解析作為沒收執行之手段，乃現實上可行的作法。雖無法達到沒收剝奪的終局執行效果，但至少可以讓系爭域名在我國的使用受到干預，以及讓我國使用者搜尋不到系爭違法網站。此乃**執行程度**之問題，雖停止解析無法做到百分之百的沒收，但至少可以發揮一定的效果。是以，停止解析亦有作為沒收執行手段之可能，故將其用於扣押，亦該當保全沒收之手段。

至於，若欲沒收者為我國**境內**註冊之域名，透過 TWNIC 等註冊管理單位之協力，偵查機關即得註銷該域名之註冊，並將系爭域名之管理權限移至國家管理，達到沒收剝奪財產之目的，請求於沒收執行上並無困難，**似乎**無特別發動扣押保全之必要。

---

[284] 林鈺雄，前揭註 7，頁 453。

[285]「對於境外域名沒收，除了考慮請求域名之頂域註冊管理機構（Registry）或域名註冊商（Registrar）所在國之政府協助執行外，其實也可以直接商請各該頂域註冊管理機構或域名註冊商，自願配合協助執行我國域名沒收裁判」。參蔡志宏，前揭註 25，頁 215。

[286] 當然，境外單位協助與否乃實然面之問題，與是否應為沒收裁定之應然面無關。理論上若剛當沒收要件，即便於執行上存在困難，法院仍應為沒收裁定。而本處之討論建立於境外域名沒收裁定存在之前提，施以停止解析也無助於沒收之執行。同上註，頁 214。

doi:10.6342/NTU202302025

雖之於境內註冊域名，停止解析無法達成傳統扣押之目的，惟將其作為偵查工具運用仍有別於其他強制處分之意義。如第一章所述，我國執法單位過去往往對境外註冊域名之非法網站束手無策，實際上難以沒收。而停止解析則可以達到即時防止利用我國伺服器之網路使用者連結該網站之功能。對於賭博、釣魚網站之停止解析，可以保障我國社會法益與國民之個人法益受損；對於充斥侵害著作權內容之網站，也可以及時有效降低著作權人之損失，限制犯罪規模的膨脹。網域扣押對於犯罪預防、保障法益有所助益[287]，且向國外請求司法互助不僅緩不濟急、處理量能亦有限。相比之下，停止解析面對跨域性及隱匿性的網路犯罪，係一成本低且效率高之手段，無需等待漫長的資訊往返、交流，毋庸顧慮台灣之國際情勢，也不需要在偵查階段即確認網路犯罪之行為人。

或有認為，偵查程序之功能應係在於蒐集證據、保全刑事追訴之過程，犯罪預防、刑事政策等則應由行政權而非司法權所管轄。惟本文以為保全證據與犯罪預防間本就存有灰色空間[288]，且現行強制處分中亦不妨存在以預防為目的者，如：預防性羈押、犯罪物沒收[289]，於偵查程序中發揮犯罪預防之效果（惟仍須注意手段是否符合法治國原則），自無不可。

更進一步言，犯罪物沒收係為了剝奪犯罪工具以遏阻再犯，其中更蘊含了對於財產權濫用之制裁意義。而域名能夠助長網路犯罪之規模，對犯罪有所促進，係一犯罪工具。對於域名的停止解析與犯罪物沒收屬類似之概念，停止解析雖無法達到終局「剝奪」域名之程度，然得限制、干預域名之使用，也有犯罪預防、限制犯罪行為人財產權之制裁效果。

準此，本文認為雖停止解析於效果上不若沒收，無法終局剝奪財產權，但於現實上難以執行域名註銷時，不妨將停止解析作為替代手段，將沒收判決執行到某種

---

[287] 聯合報（12/22/2021），〈防網路犯罪 檢設台版防火牆〉，https://udn.com/news/stor y/7321/5978966（最後瀏覽日：03/28/2022）。

[288] 林鈺雄，參前揭註 7，頁 461-462。

[289] 刑法第 38 條第項立法理由：「三、犯罪行為人所有供犯罪所用、犯罪預備之物或犯罪所生之物（如偽造之文書），係藉由剝奪其所有以預防並遏止犯罪，有沒收之必要。」

doi:10.6342/NTU202302025

程度。故在此可將停止解析認作沒收之執行手段，於扣押實施行亦有助於沒收之保全；而將停止解析施用於境內註冊之域名時，其於意義上不若傳統之扣押，以保全證據或沒收程序之進行為目的。惟不妨將停止解析認定為「犯罪物沒收」之輔助措施，其存在意義係為了於現實上難以執行沒收時，即時制裁並控制犯罪規模，使犯罪工具沒收之目的能夠更迅速的達成。故於解釋上，也能將停止解析解讀為沒收保全之輔助措施，**具有保全沒收之必要**，而可以認定為有助於扣押目的達成之適合手段。綜上，本文以為停止解析作為扣押執行手段，有助於沒收之保全，具備手段適合性。甚至於某些情況下，更可以作為沒收之執行手段，現實上處理我國對於境外域名的執法難題。

第二項 必要性

必要性原則係指國家機關未達所企求之公法目的而採行之手段，惟當已無其他同樣有效且對基本權侵害更少的方法時，採行該項手段才被視為必要[290]。而停止解析是否為網域扣押時所必要採取之手段，存有疑義。

蓋如前所述，技術上存在其他使非法網站不被網路使用者造訪之手段，如：IP 過濾及 URL 過濾。而如本文第二章之技術分析，URL 過濾與 DNS 過濾，皆有過度封鎖之問題，相比此二者，URL 過濾乃對人民權利干預較小者。惟不論是其基礎建設之建置花費、或是檢警機關特定 URL 之時間成本，都過高而現實中難以期待以此方式達到網域扣押之目的。故以現行技術而言，DNS RPZ 乃能夠發揮扣押實效，且在相同有效之方法中，相較於 IP 過濾乃對基本權侵害較小之手段，故符合必要性之檢測。

併予敘明，於美國法章節中，曾提及美國最高法院於 2004 年之 Pappert 案，認為 DNS 過濾的過度封鎖太過嚴重，與所追求之遮蔽網站利益不成比例，故認為當時立法要求 ISP 業者執行 DNS 過濾乃違憲之法案。惟據本文了解，於將近 20 年後的現在，DNS 過濾的技術已大幅發展，其中 DNS RPZ 便為其中之一，雖同樣採

[290] 林鈺雄，參前揭註 7，頁 326。

doi:10.6342/NTU202302025

取過濾 DNS 的方式，但其額外加上了遞迴解析器等技術，可以讓使用者在沒有額外的設定下阻止其連結到惡意網站，同時也可以 Zone Transfer 的機制同步更新 RPZ 的內容，減少維護域名黑名單的成本[291]。換言之，相較於過去域名的黑名單需要有人員手動更新、定期維護，此時的技術已經得以成本低之方式，自動快速的將黑名單更新到所有參與國家型 RPZ 之 ISP 業者，而得即時的封鎖特定域名，而較不會發生錯誤或過舊的名單，導致過度封鎖之問題。

綜上，現行技術中，於我國而言，將停止解析運用於域名扣押，乃一符合必要性之手段。

第三項 相當性—狹義比例原則

國家機關運用強制處分為手段時，目的與手段間尚須符合狹義的比例原則，即具備相當性之關係。據此，限制基本權的手段強度，不應超過達成目的所需的範圍，同時因其限制所造成之不利益，不得超過其所欲維護之利益[292]。

首先，停止解析的手段強度並未過度。可以從其僅是阻礙國內使用者解析觀之，其並**未全面性的關閉網站及禁絕言論**。該網頁實際上仍存在，網路使用者能過其他並不算太困難的手段接觸言論，停止解析充其量僅是增加接觸系爭言論之成本。且於我國扣押之規定中，法官得於裁定中明定扣押實施之時間，故停止解析之實施也僅是暫時性的。是以，透過停止解析干預「範圍」與「時間」的有限性，本文以為此並非過度之手段。

再者，停止解析所欲維護的利益，不僅僅是在智財案件中對於著作權人個人私益的保障，更是蘊含了預防犯罪、限制犯罪規模的國家公益，乃重要之政府利益；相比之下，其所限制的言論係涉及刑事犯罪的低價值言論[293]，且由於網路論壇無稀缺性之特徵，不適用公共論壇理論[294]，無須對網路言論予以特別保障。縱使認為停

---

[291] TWNIC，參前揭註 62。
[292] 林鈺雄，參前揭註 7，頁 326。
[293] 戴豪君、余啟民主持，參前揭註 70，頁 221。
[294] 有認為，網路空間無「稀缺性」之特徵，故無公共論壇理論適用之餘地，蓋公共論壇理論之前提係發表言論的空間有限，故國家有義務提供使人民放心討論的場域。Derek E. Bambauer, *supra* note 16, at 912.

doi:10.6342/NTU202302025

止解析不僅干預犯罪行為人對於發表言論的自由，更限制了網路使用者對於言論接收之自由[295]，然而對於一般民眾，也難認有接觸非法言論的合法利益[296]。準此，本文認為停止解析作為強制處分得通過狹義比例原則之審查。惟認定屬於合法干預之處分後，強制處分尚須符合正當法律程序之要求。

第四節 正當法律程序

第一項 事前程序

扣押於我國刑事訴訟法上可以區分為「附隨於搜索之扣押」或「非附隨於搜索之扣押」。而於**排除暗網**之情形下[297]，域名乃無需經過搜索即得確立之標的（透過 WHOIS 系統查詢），故其適用之程序乃後者。後者之條文依據係刑事訴訟法第 133 條之 1 第 1 項，原則上扣押前應經過法官裁定，乃採取相對法官保留原則。

惟於法官審查扣押聲請時，則有個案中應如何操作比例原則之疑慮，尤其域名扣押與傳統扣押於干預權利面向有所差異，法官於審查時該注意哪些事項，具有討論空間。是以，在本項將處理兩個問題，一者乃法官審查令狀之程序中，審查密度該如何擇採，二者則是現行 TWNIC 的域名爭議處理機制，是否符合扣押相對法官保留之原則。

一、審查密度調整

首先，針對強制處分「相當理由」之審查，美國法上普遍肯定，當扣押涉及言論自由之限制時，此時必須較嚴格的審查相當理由具備與否[298]。本文呼應前文所述，

---

[295] *Id*, at 919. “First Amendment intervention on behalf of information consumers typically requires special conditions, such as resource scarcity, difficult-to-reach populations, or **quasi-state functioning by private actors who block access to speech.**”

[296] 陳昱奉，參前揭註 282，頁 266。

[297] 由於有時僅僅是要進入暗網，就必須具備特定的密碼。於暗網中之情形較為複雜，並不一定域名都是顯而易見的，故於暗網中的域名扣押則可能涉及前階段的搜索行為，或是其他的偵查行為。是以，為免本文討論範圍過於擴張，且暗網並非目前一般大眾所經常造訪者，故本論文對於域名扣押之討論限定於明網中。

[298] Arthur L. Burnett, *supra* note 175, at 67.

doi:10.6342/NTU202302025

亦認為對於言論的限制，由於具有整體社會影響與寒蟬效應之考量，於強制處分審查上應提高標準。

另外，於法官保留之審查中，將操作司法個案性的比例原則審查，故法官於裁量時也應該審查停止解析於個案運用的適合性、必要性，以及比例相當性。適合性較無疑義，強制處分的發動必須是於追訴個案有所助益；關於必要性，則有提出應**優先考慮其他侵害較小**之方式，如先行通知（透過 WHOIS 系統查詢註冊人）行為人配合刪除內容，如無法聯繫或於限期內無回應者，再行採取停止解析、暫停域名使用服務之方式[299]，而移除、註銷域名乃屬最後手段[300]。

至於比例相當性之審查，與傳統扣押有所不同的域名扣押，應基於其額外干預言論自由之性質，調整審查基準。因此本文在此提出於個案審查時應注意之事項。

（一）言論類型

首先，域名扣押係屬於對於言論之事前抑或事後限制，於我國法上並非毫無爭議。就此，有論者採取與美國法類似之觀點，認為此種對於言論素材之大量扣押，屬於「言論自由之事前限制」[301]，其想法是基於「於確定判決前所為的限制皆屬於事前限制」。然而，本文以為此想法與我國釋憲實務之觀點不符，我國釋憲實務僅在「言論發表前之審查」採取事前限制之嚴格審查模式。是以，本文在此認為，於我國釋憲實務之脈絡下，域名扣押乃言論發表後之懲罰性質，屬於基於言論內容涉及不法的事後限制。

將域名扣押定調為言論內容之事後審查後，進而參考我國釋憲實務對於言論自由的審查模式，普遍係參酌美國法雙軌、雙階之模式以定審查密度。是以，本文以為法官於裁定停止解析時，應考量並區分言論的類型。雖然大致上涉及刑事扣押

[299] 蓋停止解析之實施並非將網域全然移除之狀態，技術上仍有造訪系爭網站之可能，網站也還存在，故對於受處分人之限制較註銷域名為輕，於註銷前應優先考量之。
[300] 戴豪君、余啟民主持，參前揭註 293，頁 202。
[301] 參吳巡龍（2009），〈誹謗性雜誌之扣押〉，《月旦法學雜誌》，78 期，頁 24-25。

doi:10.6342/NTU202302025

者屬於犯罪性或商業性之低價值言論，然而實務上也有出現對於政治性言論扣押之案例[302]，因此本文認為有於審查時區分言論價值，調整審查密度之必要。

（二）違法情節

為避免「大砲打小鳥」，於個案中發生侵害權利大於所追求利益之情形。於裁量強制處分時本應考量違法情節。其中在域名扣押中，較容易發生的是非法部分於網站中所佔比例甚低之情形。此時若對之為停止解析，形同遮蔽整個網站，顯現出不符比例之疑慮。是以，在難以精準移除系爭域名之濫用部份時，例如：網路討論區等情形，應謹慎考量過度限制對社會造成的負面影響。

二、現行 TWNIC 規章架空司法審查？

參考美國法上針對域名扣押的處理，其主要是透過具備司法性質之民事扣押與沒收，以向法院聲請令狀並提起對物訴訟的方式為之。即便法制上存在行政沒收，實際上亦無運用於域名扣押之例，一方面是基於行政沒收的標的限制[303]，另一方面只要扣押後有權利人提出異議，則法規上明定需進入司法程序[304]。換言之，美國法上對於域名之扣押基本上採取司法審查之方式。

反觀我國現況，在網路世界蓬勃發展下，所衍生的網路犯罪及糾紛日益漸增，致使我國政府相關單位，例如行政院公平交易委員會、地方政府、內政部警政署等單位常以網域名稱註冊人違反公平交易法、菸害防制法、著作權法、刑法等法律或為偵查犯罪所需，要求 TWNIC 對該有違反法律之虞之網域名稱進行必要之處置[305]。

然而，參電信管理法第 71 條第 2 項及第 3 項，通傳會對於 TWNIC 之監督，僅係 TWNIC 應訂定業務規章供通傳會查核，較類似對於社團法人之低度監管模式

[302] 如「關注 31 條網站」之沒入即屬一例。參蔡志宏，前揭註 12 網站。
[303] 由於行政沒收不具有司法性，在程序要求較低之情況下，對於沒收之標的亦有所限制。參照 18 U.S.C. §985(a)以及 19 U.S.C. §1607(a)，行政沒收不得針對不動產、不動產相關權利、現金與金融票據以外價值超過 50 萬元美金的動產。故面對高價值之財產，若欲沒收僅得依循司法沒收程序，以免過度侵害人民財產權。參吳協展，參前揭註 87，頁 9。
[304] 18 U.S.C. §983(a)(1)(A)(i).
[305] 戴豪君、余啟民主持，參前揭註 293，頁 156。

doi:10.6342/NTU202302025

[306]。是以，原則上通傳會無權要求註冊管理機構就個案移除不法內容或取消網域名稱等必要處置，而其他機關、單位也不宜以機關協力之名義即向 TWNIC 為上述請求，而應有賴各機關於主管法規中明定授權基礎。

另依據 TWNIC 之規章，除緊急狀況得事後陳報外，尚容許其他未經法官保留即得停止解析域名之情況。按 TWNIC 之 RPZ 治理機制，得實施停止解析的情事，除了**依法院之判決或裁定**外，更包括**依行政處分**、**因犯罪防治緊急案件處理**以及當**網域名稱影響資安重大**者。此類未經司法審查、法律授權之停止解析，其程序是否足夠嚴謹？以下逐項討論之：

（一）行政處分

蓋如前所述，停止解析運用於偵查中具有干預人民權利的性質，而刑事扣押與強制處分，原則上應適用令狀原則之規定[307]，在此被轉化運用於行政程序之扣留或沒入程序，似乎巧妙的迴避了令狀原則之要求，致有「刑事扣押遁入行政扣留」之疑慮[308]。並且，違法行政法規定之言論，相較於犯罪言論更可能屬於高價值言論。是以，在行政程序較簡易、迅速之情況下，本文以為停止解析此種涉及言論管制之新興技術不適合直接作為行政手段運用。不過，若立法者於**法規明定**得停止解析域名之情事，則得以說明其已事先考量事件之特性及程序正當性之平衡。

現行法中訂有行政機關得限制接取、瀏覽或移除相關網頁內容者，僅有兒童及少年福利與權益保障法第 46 條第 3 項[309]以及動物傳染病防治條例第 38 條之 3 第 3 款[310]。除此二者外，本文以為不宜由行政機關逕自作成停止解析之行政處分。於未來立法上，或許各主管機關得考量違法態樣、公益性、比例原則等決定是否於主

306 同上註。
307 刑事訴訟法第 1 條：「犯罪，非依本法或其他法律所定之訴訟程序，不得追訴、處罰。」
308 陳文貴（2017），〈行政檢查與令狀原則之界限探討〉，《中原財經法學》，39 期，頁 142-143。
309 兒童及少年福利與權益保障法第 46 條第 3 項：「網際網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康或違反前項規定未採取明確可行防護措施者，應為限制兒童及少年接取、瀏覽之措施，或先行移除。」
310 動物傳染病防治條例第 38 條之 3 第 3 款：「網際網路內容涉及境外應施檢疫物之販賣至國內、輸入或其他檢疫相關事項，經輸出入動物檢疫機關公告者，其廣告刊登者、平臺提供者、應用服務提供者或電信事業，應依輸出入動物檢疫機關之公告，採取下列措施：一、加註有關宣導防疫或檢疫之必要警語。二、保存刊登者、販賣者或訂購者個人資料，或定期提供予輸出入動物檢疫機關。三、限制接取、瀏覽或移除相關網頁內容。」

doi:10.6342/NTU202302025

管法規中明文授權機關得採取限制接取、瀏覽，移除之措施，以建立對於域名管制作出行政處分之法源依據[311]。

（二）因犯罪防治緊急案件處理

依照 TWNIC 之 RPZ 處理流程，其指出由調查局、刑事警察局等單位，可以提出涉嫌犯罪之網域名稱資訊與公文，向 TWNIC 提出停止解析申請，而 TWNIC 則有審核人員審查並決定是否對系爭域名停止解析。且於緊急情況時，檢警單位更是可以先申請，之後再補上公文。

惟查，學說上有認為，依照網域名稱註冊管理機構業務規章之規定，客戶與受理註冊機構間非關網域名稱註冊事宜，與 TWNIC 無關，且 TWNIC 亦不負查證客戶所填具資料真偽之責任；此外，依網域名稱申請同意書第 7 條規定，TWNIC 於「接獲相關機關通知」後，得視情況暫停所註冊之網域名稱或為其他合理之處置。由此可推知，TWNIC **並非網路內容或使用者行為適法性之認定單位[312]**。

本文亦認為此種模式架空了扣押令狀原則，雖然有經過 TWNIC 作為第三方的獨立審查，但關於犯罪與否應屬法律爭議，由非法律專業的 TWNIC 審查犯罪資料乃對於受停止解析者之程序權干預。且 TWNIC 是否屬於偵查不公開之主體也存有疑義[313]，於偵查階段即由其介入並決定處分，似有不妥。

是以，本文以為應將本項**限縮解釋**，僅有在構成刑事訴訟法第 133 條之 2 緊急扣押之情形，檢警機關使得無令狀以犯罪防治緊急案件處理為由，向 TWNIC 請求協助停止解析。

311 戴豪君、余啟民主持，參前揭註 293，頁 155。
312 同上註，頁 160-161。
313 TWNIC 是否屬於刑事訴訟法第 245 條第 3 項「其他於偵查程序依法執行職務之人員」，本文以為於文義上有些模糊。蓋 TWNIC 是否為依法律規定、或是屬於偵查程序中執行職務者，皆有討論空間。

doi:10.6342/NTU202302025

（三）網域名稱影響資安重大

本項所謂「影響資安重大」係指「技術濫用[314]」之情形，是以，此非針對網頁內容之審查，由具備資訊科學專業性之 TWNIC 為審查機關似無不妥。惟即使屬於非言論內容之審查，其適用結果仍然有對於言論自由限制之效果。是以，本文建議仍宜於法律或命令中明定 TWNIC 得以資安影響為由為停止解析之處分，而非僅透過內部的治理機制規範。

第二項 事中程序

一、裁定程序參與權

在美國法之判例，於扣押「大量」「同書目」之書籍時，要求於扣押程序中須賦予受處分人程序參與權。反之，若係單一書籍的扣押則不需要。

而我國法中之扣押程序，採取與美國法類似之程序，皆係由檢察官單獨向法院聲請令狀，而被告原則上並無參與程序之權利。按刑事訴訟法第 133 條之 1 第 4 項，核發扣押裁定之程序，不公開之。其**立法理由係為避免證物滅失或應被沒收財產之人趁隙脫產**。然而，如前所述，域名理論上無法作為證據，故無證據滅失之疑慮；而對於脫產方面，域名確實可以於不同的註冊管理機構間移轉，或是向機構申請變更所有權人，有防止移轉以利刑事程序進行之必要。惟此僅需透過向域名註冊管理機構核發禁止處分之命令即可，停止解析無法達成此目的。換言之，於決定是否實施停止解析扣押域名時，似乎就不存在裁定程序不公開之理由，則受停止解析處分之人是否於裁定程序中有參與權呢？

---

314 「針對網域技術濫用依網域名稱濫用框架（DNS Abuse Framework）已針對網域濫用定義五種類型包含：一、惡意軟體（Malware）；二、殭屍網路（Botnets）；三、網路釣魚（Phishing）；四、偽冒嫁接（Pharming）；五、以垃圾郵件之形式達成以上濫用之行為（Spam）。」戴豪君、余啟民主持，參前揭註 293，頁 11。

doi:10.6342/NTU202302025

誠然，以停止解析扣押域名時，似乎不存在上述保全犯罪追訴利益之情事。是以，於立法目的論上，若單純欲實施停止解析，自無不可於處分前賦予受處分人受通知、參與裁定程序及發表意見之機會[315]。

然而，本文基於以下考量，認為於現階段**不宜**賦予受停止解析處分者，於扣押令狀審查之程序中參與並發表意見之機會。首先，最直觀的想法便是，欲將停止解析套用於現行法中扣押之執行，則必然要符合於現行法的框架，即同一般扣押裁定採取秘密審查模式。若非如此，則又會回到法律保留層次，即扣押規範得否作為停止解析法律授權依據之討論。或有認為，於現行法之架構下，非不得將刑事訴訟法第 133 條之 1 第 4 項為目的性限縮解釋，將本條解釋為「於有證物滅失」或「應沒收財產之人脫產」之情形，得不公開裁定程序，以此解決前述之疑慮。惟即便解釋論上現行法可以賦予受處分人程序參與權，實際上法院該如何於審查程序中通知受處分人，其程序進行方式現行法並未規範，法院未通知時該如何救濟亦付之闕如。故在現實考量以及現行法框架下，停止解析作為扣押執行方式，亦應符合現行法於扣押裁定採取之秘密審查模式，而不宜額外賦予受處分人事前的程序參與權。

再者，從對受處分人的權利限制觀之，扣押僅是**暫時性措施**，其對於正當程序之保障，相對於終局性之沒收，自無庸採取同樣的高規格。一方面可以參考美國法，除了在「大量」扣押書籍之情況下，基本上由於扣押並非終局性處分，無於事前踐行聽證程序之必要。而套用同樣的標準，由於網路言論的發表通常不會僅依附於單一域名，而可以透過複數通路傳遞，故針對單一域名的扣押並不至禁絕言論之程度，而亦無必要於事前供相對人表達意見。另一方面，從我國扣押法規範觀察，也可以發現我國立法者在此暫時性之處分，亦認為事後沒收程序，或是對於扣押之救濟程序中，所賦予相對人之程序參與權，已經足夠補足扣押之程序正當性。故我國立法

[315] 蔡志宏，參前揭註 25，第 225 頁。作者認為，「於域名扣押之操作實踐初期，域名扣押較佳之執行時機應是於域名沒收裁判確定後，經請求被扣押域名所屬境外域名註冊管理機構或域名註冊商自主配合協助執行無效果後」。

doi:10.6342/NTU202302025

者在此已作出利益衡量之價值取捨，為了刑事訴訟程序保全之便利，在暫時性質之扣押程序中，無需賦予相對人事前之程序參與。

最後，考量到實務上聲請扣押時，並不一定會僅聲請停止解析域名，有時亦會併同其他處分一同聲請[316]，而其他處分之執行或許仍有裁定程序不公開之需求，故為了整體追訴程序之順利進行，並考量到偵查階段之秘密需求，本文認為停止解析作為扣押執行手段，於扣押審查決定實施時，無需事前賦予相對人裁定程序參與權。

二、執行流程

其中域名扣押較特別之處，應在於如何實踐「扣押之公示原則」？按刑事訴訟法第 139 條第 2 項，扣押物應加封緘標識、蓋印；以及第 145 條，執行扣押時應以扣押裁定提示在場之人之規定，此乃此乃公示原則之規範。公示原則能向一般大眾宣示系爭標的已置於國家公權力之支配之下，其意義不僅象徵程序依法可供大眾檢視，並便於受處分人救濟，亦得展現司法權，達到一般預防、警告財產權濫用行為之目的。

而域名之扣押亦應有公示原則之適用。學說上有提及，考量到域名之無體性，得透過將扣押資訊置於所扣押域名之網頁，或是將網域導向檢警機關之扣押頁面，並於頁面上記載扣押意旨、扣押機關、扣押裁定之摘要[317]。本文贊同此見解，實務上目前針對域名扣押亦大多採此作法[318]。此舉一方面可以使造訪網頁之大眾了解，網頁停止解析並非單純之技術障礙，而是有觸法事由遭到扣押，警告大眾該網頁不適宜造訪；另一方面亦有使域名註冊人瞭解該域名已經遭到扣押之事實，若有不服能夠提起抗告及準抗告（同法第 404 條及第 416 條）。

併予敘明，為便利域名註冊管理機構執行，ICANN 建立了一扣押指引，提及執行令狀宜記載，聲請單位、聯絡人、執行日期、執行方式（刪除域名、轉址或停止解析）、域名紀錄應如何變更以及是否需要同時取得域名之相關資訊等，以符合

316 戴豪君、余啟民主持，參前揭註 293，頁 71。
317 蔡志宏，參前揭註 25，頁 225。
318 見本文第 9 頁之圖 1，楓林網之域名於扣押後，其網域便顯示已遭停止解析之畫面，並提及其所涉著作權侵害之事實。

doi:10.6342/NTU202302025

實務執行需求[319]。此部分也可以為我國執法機關所參考，以利實務上執法之遂行，與 ISP 業者溝通順暢，降低執法成本。

第三項 事後程序

前有提及，對於扣押裁定之救濟程序，於刑事訴訟法中已有詳盡之規範，即第 404 條之抗告與第 416 條之準抗告，運用於域名之扣押似無疑義，透過事後救濟程序之賦予，也能夠補足扣押程序之正當性，彌補相對人之程序參與權。然而，最常需要運用停止解析技術的案例，通常是犯罪行為人不在境內或是甚至無法追蹤的情況。就此，該如何踐行通知、賦予陳述意見機會、提供救濟而滿足其程序保障，本文以為現行法之規範尚不完整。

於現階段將停止解析作為扣押手段使用，是一不得不之解套方式。但若是日後有機會，採取以立法的方式對停止解析授權，便得針對其特殊性建立程序規範，補足境外救濟保障不足之部分。另外，美國法上也有學者對於涉外性質的域名扣押提出管轄過於擴張之質疑，其文內提到了此種管轄擴張對於境外受處分者有程序不公平（對境外人士而言乃救濟繁重、事前不可預見之干預處分）的疑慮[320]。

簡單的說，若要將停止解析運用於境外域名，將管轄權擴張至涉外事項，則勢必會伴隨著境外人員程序保障之減損以及救濟負擔。於我國而言，對境外域名之停止解析有需求及必要，因此，立法上則有應盡可能去補足上述保障不足之處，以維公平（至於國際管轄權擴張之爭議則於下一章節討論）。

併予敘明，目前實務上於實施停止解析時，亦會盡可能的透過 WHOIS 系統查詢域名註冊人之聯絡資料，通知其域名之執法狀態。即使是境外之域名註冊人，亦將通過 ICANN 等境外機構協力通知，以盡可能維護受處分人之救濟。

---

[319] ICANN, *Guidance for Preparing Domain Name Orders, Seizures & Takedowns*, 6-11 (2012), https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.
[320] Michael Xun Liu, *supra* note 206, at 486-88.

doi:10.6342/NTU202302025

第五節 其他

第一項 司法管轄權

在第一章問題意識之章節有提及，依我國刑法第 3 條，我國之刑事管轄權係以屬地原則為主，其中包括犯罪行為地與結果地。惟此於網路犯罪將遭遇困難，蓋網路犯罪具有跨域性的特徵，即便是在境外的主機上進行犯罪行為，該犯罪結果也將遍佈全球，凡是能連接上網路的地方，皆可能受到該犯罪之影響。是以，很容易演變成任何一個網路上的犯罪，都可以納入我國管轄。

但是，若將與我國關聯性低之案件納入我國司法管轄，並運用停止解析技術，實質的擴張我國審判權。如此，雖可以達到真正預防網路犯罪之效果，卻很有可能造成當事人之救濟不便、我國司法系統之過重負擔以及與他國之管轄衝突等，形成兩難。

一、國際管轄

我國刑事訴訟之審判權範圍，應跟著我國刑事實體法的效力範圍決定。是以，以下討論國際管轄之範圍時，將回歸刑法之規範。

關於我國刑法第 3 條，於網路犯罪時所謂的「犯罪結果地」該如何解讀，於學說上便有不同見解。有採廣義論者，以「得於某地藉由電腦聯繫上該網頁」作為犯罪結果地；亦有採狹義解釋者，認為應強調行為人之住、居所或網頁主機設置之位置。

本文以為在此應採取廣義之說法，一方面是狹義說太過僵化，很容易形成規避，行為人只要把主機架設於國外、或是逃往外國，就可以輕易地達到犯罪目的又不用被處罰；另一方面，網路犯罪跨域性的特徵，也恰恰說明了凡是可以上網的地方，都有可能受到該犯罪之影響，於我國也不例外。於網站上散佈危害國家安全、侵害著作權、兒童色情相關的資訊，也很有可能影響我國的國家或社會法益，而我國也有採取應對措施之必要。

doi:10.6342/NTU202302025

於我國法上關於停止解析之討論，便有不少人質疑「基於管轄因素，我國無法針對.tw 以外之域名扣押[321]」，然本文以為此應屬誤解。在技術上 DNS RPZ 可以對境外域名停止解析；於法律上，只有在前述爭議中採取狹義說，才會衍生出管轄受限之問題。換言之，無論如何目前我國法對於域名之管轄規定，都不是以註冊於「境內或境外註冊機構」作為劃分，此與美國法不同。

是以，基於本文採取廣義說，以及回應我國實際執法上之需求，應有將 DNS RPZ 運用於境外域名之必要，且法律上亦不排斥此做法。然而，雖有實施技術必要，並不代表便要捨棄被告之權利。準此，連結本文關於停止解析正當法律程序之討論，本文以為應於扣押境外註冊之域名時，於法制上考量其實際救濟之困難，賦予更強的程序保障。學說上也有主張，實施停止解析時**應盡一切合理可能通知**域名註冊人[322]。並且，或許可以參酌美國法上最低接觸要求，對於我國管轄權為限縮，排除與我國關聯性甚低之案例，以免發生過度擴張之負面效應。

二、國內管轄

在國際管轄權會有上述界線模糊之問題，在國內法院之分工亦如是。我國刑事訴訟法第 5 條第 1 項「案件由犯罪地或被告之住所、居所或所在地之法院管轄。」其中「犯罪地」之解讀，依實務見解應參照刑法第 4 條之解讀。是以，也生網路犯罪之管轄法院是否採廣義說形成全國法院皆有管轄權，進而使法定法官原則之限定功能喪失之爭議。運用停止解析時也是，可能會因此造成受處分人救濟障礙或是程序之不便利。

本文以為，為符合法律解釋之一致性，此處犯罪地之中的「犯罪結果地」自應同刑法國際管轄採取同樣的廣義解釋。只是為同時衡平犯罪行為人之程序利益，也為避免國內法院難以分工，導致行政上之困難，或許運用本條分配管轄時，應以「犯罪行為人之住、居所」為原則，而僅在例外犯罪行為人不在境內或所在不明時，才例外以「犯罪地」進行操作。

---

321 陳昱奉，參前揭註 282，頁 247-248。
322 蔡志宏，參前揭註 25，頁 222。

doi:10.6342/NTU202302025

而以「犯罪地」進行國內法院分配時，則應優先以犯罪「行為地」之法院為原則。理由上與行為人之住、居所乃類似之衡平利益想法，蓋若行為人可以抵達該行為地實施犯罪，則對其而言或許也不是太難以抵達、而有諸多程序不便之地。

實在連犯罪行為地也無法判斷，而需要以犯罪「結果地」進行分配時，由於此時全國各地法院都將落入管轄範圍，本文在此建議，或許於實務上可以設立專職網路犯罪之偵查機構，於前階段之分配順序中都無法處理之案件，由該專職機構處理偵查與追訴事項。

另外，域名之沒收也常常會面臨到行為人行蹤不明或犯罪事實無法追訴之情形，而需要發動獨立沒收。依刑事訴訟法第 455 條之 34「單獨宣告沒收由檢察官聲請違法行為地、沒收財產所在地或其財產所有人之住所、居所或所在地之法院裁定之。」本條文反而無前述「結果地」之爭議，實務操作上應不會產生疑慮，故在此依原始條文進行管轄分配即可。

第二項 輔助規範之建置

附帶而論，本文係以刑事訴訟法上扣押之規定深入探討停止解析、域名爭議之議題。然討論上也有不少主張以「非司法」之模式處理，可以更有效率、更快的預防損害。尤其是我國不若美國法設有民事沒收此種證明力[323]要求較低之方式，皆以刑事扣押、沒收處理，難認可以追趕過行為人違法的速度。

學說上有提及運用行政管制、**民間合作**等方式者協力[324]，後者如網路內容防護機構（Institute of Watch Internet Network，簡稱 iWIN）以第三方民間機構之身份，專責處理網路內容涉及侵害兒少身心之申訴及後續通報，不僅可以促進業者自律，並使得民眾之反應可以迅速獲得解決，有良好得成效[325]。本文亦肯認若有司法外之手段可以協力網路之管制，係屬於可行之政策。

---

323 美國法上民事沒收之證明度僅需達**優勢證據程度**。與之相較，我國刑事沒收至少在「刑事不法之存在」、「沒收物存在」需要證明至無合理懷疑之確信。

324 台灣網路講堂，域名之扣押與沒收—以司法實務操作為中心，https://www.twsig.tw/20201120/。會議進行中有論者提及透過民間單位協力，或是以行政、民事之手段處理域名爭議。

325 戴豪君、余啟民主持，參前揭註 293，頁 11。

doi:10.6342/NTU202302025

第六節 立法展望

雖於本文第四章澳洲法制之章節，本文將澳洲法與我國法進行比較分析時，認為基於我國立法量能不足之現實，難以期待以創新令狀之方式處理非法域名爭議。然而，能夠以貼切的文字，針對技術本身量身打造條文，本文以為毋寧是較佳之作法，對於可以增加人民對於干預的可預見性，也能夠避免既有的扣押文義解釋問題。是以，本文在本小節嘗試擬定條文，作為未來立法之展望。試擬條文之發想，主要係以澳洲法之數據破壞令作為參酌對象，並就受有爭議之部分去蕪存菁。另一方面，亦參考**我國科技偵查法草案**對於新興技術之授權條款以及**刑事訴訟法**上關於搜索、扣押之規範作為**試擬條文架構**。

試擬條文	說明
第 1 條 為規範科技偵查，以保障人權，並有效追訴、預防犯罪，或減少犯罪損害，確保國家安全，維護社會秩序，特制定本法。	一、本條係參考科技偵查法草案第 1 條，就立法目的為說明。本法之目的在於平衡追訴犯罪之公益以及人權保障，確保國家運用科技技術時不會過度侵害人權，並有授權依據。 二、本文於原科技偵查法草案之條文中增加了「預防犯罪」及「減少犯罪損害」之目的，蓋偵查犯罪之過程係浮動的，預防與保全追訴交錯。本文為避免強制處分之發動受限於保全程序目的，故明文肯定預防作為發動處分之要件。 三、但相較於僅將目的限於預防之澳洲數據破壞令，本試擬條文亦就此做調整，承認其他偵查目的作為發動要件的可能性。

doi:10.6342/NTU202302025

第 2 條 本法名詞定義如下： 一、停止解析：修改資訊系統或設備上，對標的網域名稱解析之結果。 二、網域名稱權利人：實際使用標的網域名稱、網域名稱註冊人與相關權利人。	就本法重要名詞之意義進行定義，以資簡潔並避免爭議，茲說明如下： 一、針對域名的解析過程進行干預，所運用的技術其實不限於 DNS RPZ，故本文在此為定義時，不以列舉技術之方式，以開放相似技術之授權。 二、由於域名註冊人並不一定是實際使用域名者，故實施停止解析時，所影響到的也包括域名使用人，以及對系爭域名有其他財產上權力者。
第 3 條 對於涉及犯罪之網域名稱，必要時得停止解析之。 停止解析應經法官裁定。裁定應記載下列事項： 一、案由。 二、應受停止解析之網域名稱，以及網域名稱權利人。但網域名稱權利人不明時，得不予記載。 三、實施期間，逾期不得實施之意旨。 四、使用之科技設備或技術。 五、法官並得於裁定中，對執行人員為適當之指示。 核發第二項裁定之程序，不公開之。 授權停止解析之執行期間最長期限為 90 天，得聲請延長一次。但經法院判決確定應永久停止解析者不在此限。	一、由於停止解析相較於傳統的扣押，更有言論自由之干預，且於執行上亦與扣押有不少差異，故有立法之必要。 二、本條第 1 項係對停止解析發動之實體要件進行規範。由於澳洲數據破壞令之發動乃採取「合理懷疑」之低門檻，引發不少爭議。故本文在此仍採取我國刑事訴訟法對扣押的門檻，以存在「相當理由」以及「有停止解析必要」作為要件。另外，本條另一特點係參考美國法對物程序之作法，以「涉及犯罪之域名」為令狀主體，以掙脫網路犯罪中難以確定被告的困境。 三、如前文所述，基於馬尼拉原則的國際準則，以及我國「非附隨於搜索之扣押」，原則上係採取法官保留，故於本條第 2 項亦明定應經法官裁定。並將應載事項明列，包括停止解析之執行方式與期間，以及法官額外之指示，將澳洲法執行方式不明確導致難以監督的缺點改進。但同時參考澳洲法中明文授權法官要求技術人員協助之優點，充分考量新興技術實際上執行之難處。 四、基於偵查秘密性之要求，於本條第 3 項裁定程序不公開之。 五、第 4 項參考澳洲法，對於數據破壞令執行期間的規範。另外考量我國目前對於境外域名沒收執法需求，永久實施停止解析得作為沒收執行之替代方案，故於但書另外設計要件為法院判決確定，補足基本權干預之程序正當性。

doi:10.6342/NTU202302025

第 4 條 偵查中檢察官認有實施停止解析之必要時，應以書面記載前條第二項第一款、第二款之事項，並敘述理由，聲請該管法院裁定。 司法警察官認有有實施停止解析之必要時，得依前項規定報請檢察官許可後，向該管法院聲請核發裁定。 檢察官、檢察事務官、司法警察官或司法警察於偵查中有相當理由認為情況急迫，有立即實施停止解析之必要時，得逕行執行。 前項之執行，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，應即停止實施。 第一項及第二項之聲請經駁回者，不得聲明不服。	一、本條係對停止解析之聲請主體為規範，係參考刑事訴訟法第 133 條之 2 的主體設計。以檢察官為聲請主體；而司法警察則可以在報經檢察官許可後向法院聲請。 二、本條第 3 項及第 4 項，則是於情況緊急時，創設法官保留之例外，以免於特殊狀況緩不濟急。但當事後向法院補行陳報，若法院不允許，則必須立即停止實施。
第 5 條 停止解析執行起，應即向網域名稱權利人通知第三條第二項之事由，但通知有妨害調查目的之虞或不能通知者，不在此限。 對於審判長、受命法官、受託法官、檢察官或司法警察所為停止解析處分有不服者，受處分人得聲請所屬法院撤銷或變更之。處分已執行終結，受處分人亦得聲請，法院不得以已執行終結而無實益為由駁回。	一、本條第 1 項係對受停止解析處分所影響之相關權利人，執法機關通知義務之設計。充足程序正當性，並使相對人知悉干預而有提起救濟之可能性。 二、本條第 2 項係救濟條款之設計，乃參考刑事訴訟第 416 條第 1 項準抗告之規定。另回應學說呼籲，本條新增「司法警察之處分」為得救濟之對象，以填補現行刑事訴訟法對於「司法警察之處分」無救濟管道之法律漏洞，

doi:10.6342/NTU202302025

第 6 條 實施停止解析，於技術可達成之範圍內，確保下列事項： 一、所採用之停止解析方法應防止影響合法網站之正常解析。 二、執行停止解析時，對資訊系統或設備之變更，僅在預防、阻止或偵查犯罪之必要範圍內。 三、執行停止解析期間結束後，曾進行之變更應即時回復。	一、本條係參考科技偵查法草案第 17 條，所為之技術確保條文。蓋停止解析之實施，以現行之技術尚有可能影響其他合法網站，惟此應盡可能的避免之，若否將有干預正當性不足之違憲疑慮。 二、在澳洲數據破壞令，對於處分實施之事後監督程序不足，也為人所批評。故本文在此增添執行機關的回復原狀義務，以及確保僅在犯罪阻止之必要範圍內實施技術。

表格 2 試擬條文

資料來源：筆者自製。

上述試擬條文，本文僅是拋磚引玉，援引澳洲法創新令狀之優點，並盡可能以符合我國法制，以及適合停止解析之方式立法。或有不周全之部分，尚有待發展。

doi:10.6342/NTU202302025

第六章 結論

在近年網際網路之興起下，網路犯罪之法律議題甚囂塵上，線上盜版影片、兒童色情影音、詐騙網站、假消息流竄等，都再再的顯現出網路管制之必要性。但同時，當國家出手限制、斷網時，又會引起言論自由干預之爭議。而國家可以透過什麼手段去避免非法內容於網路上流竄，同時保障人民權益又不致逸脫法治國原則，便是本文欲探討的主軸。

而前述提及的網路犯罪類型，其所涉及之保護法益、實體法規範皆有所不同，於處罰方面各有各的議題，此非本文所欲討論者。本文所想探討的，是偵查機關是否有通案性的手段，可以即時的阻斷各式各樣的網路犯罪，減少損害、避免犯罪規模擴大，此即本論文之主題—「停止解析」之角色。

作為新興技術，停止解析於我國刑事訴訟上所遭遇的問題便是，其定位為何？是否為強制處分？若是干預人民基本權之強制處分，其是否能通過法治國原則對於干預合法性之要求？本文依此架構依序的處理停止解析於我國偵查實務運用時，其法律定位與合法性之議題。

第一節 論文主軸與研究結果

在本論文的**第一章**，介紹了安博盒子、關注第 31 條網站以及楓林網這三個案例。安博盒子案為本論文的緣起，也是偵查機關首次運用停止解析的實例；而關注第 31 條網站則是彰顯了網路犯罪的危害，除了私人之間的權利侵害，網路犯罪更可能涉及國家安全問題；楓林網則是作為安博盒子案的對照組，在楓林網一案中，偵查機關最終關閉網站的作法是請求犯罪行為人之配合。但現實中更常見的是犯罪行為人不明之情況，由此可以彰顯出，將停止解析作為我國偵查手段的現實需求。

doi:10.6342/NTU202302025

而透過前述案例討論，本文以為，實施停止解析使網路使用者無法造訪系爭非法網站，將造成受處分人的域名無法照常使用，也沒辦法將網站內容與資訊透過域名，引導大眾觀覽、接受，是以停止解析構成受處分人域名**財產權**與**言論自由**之限制。而我國實務與通說見解，皆認為所謂的強制處分，係指國家為追訴犯罪而干預人民基本權之行為，不以該行為具強制力為必要。故停止解析在此想法下，定性上該當刑事訴訟上之強制處分，需符合**法律保留原則**、**比例原則**以及**正當法律程序**等法治國原則之要求，始為合法之偵查手段。本文便圍繞這三個原則，探討我國現行實施停止解析之合法性。

由於停止解析屬於新興技術，將新的技術援用於我國法制時，先參考、借鑑他國的法制乃常見之作法。可以透過他國經驗之學習，尋找出更適合我國之模式。故本論文採取了比較法研究以及文獻探討的方式，來處理前述提及各個原則中，停止解析所遭遇的爭議。

由於我國學說上對於域名扣押之討論重點，大多置於停止解析之法源基礎，即爭議集中於法律保留層次。於立法論上，本處有兩種想法，一者是尋找現存的規範是否有近似而得用以授權者，二者則是乾脆的訂定新法。故在比較法的選擇上，本文於挑選外國法制作為研究參考之對象時，便找了分別採取不同手段的兩個國家—美國與澳洲。美國法係以原有的扣押、民事沒收規範處理域名爭議，澳洲法則是新創設了「數據破壞令」用以授權偵查機關使用斷網技術，並另以概括式、寬鬆文義的電信法第 313 條第 3 項，課予電信業者協力政府機關執法之義務，作為備位性的法源。

本文認為，由於我國立法效能不足，但現階段又有使用停止解析技術之需求。在現實考量下，美國以既有的扣押規範授權處理非法網站之作法，有我國援用之可能性。而澳洲創新令狀搭配備位性的概括授權，則可以作為我國未來立法展望之參酌對象。

doi:10.6342/NTU202302025

第二節 停止解析的侷限與輔助措施

本文於**第二章**就使用者連接網路時所需經過的解析過程詳盡解釋。簡要的說，由於電腦之間要相互連結，其溝通的語言是由一串數字所組成的 IP 位址；但這種形式對於人類來說太難記憶，因而發展出以單字所組成的域名，作為網站的導引。在上網的過程中就需要經過將人類輸入的域名轉譯成電腦可讀的 IP 位址這個過程，稱為解析。停止解析便是干預了正常的解析過程，阻止域名的轉譯，或甚至改變轉譯的結果，而將使用者導引至其他網站。

綜上所述，停止解析有**便利執行**的優點，只要知道非法網站的域名（此在明網中通常是顯而易見的，存在於網站的網址列），而無庸鎖定犯罪行為人，或是實際的知悉網站架設位址等，都可以直接的使系爭網站暫時無法為大眾所搜尋。且相比於其他斷網技術，停止解析取得了**執行精準與耗費成本的平衡**，乃同等有效手段中侵害最小者。

但是，停止解析也存有其**技術上的侷限**，從上方的說明可以知悉，其實上網的過程中域名的存在並非必要，只要網站的 IP 位址有被人類或電腦記憶的話，其實也可以透過此方式直接的連線至系爭網站。是以，本文整理出幾種網路使用者規避停止解析之方式，有「直接輸入 IP 位址上網」、「透過快取資料上網」以及「透過外國解析器上網」。不過，經過本文的分析，前兩者分別因記憶困難及快取暫存的有限性，可實行性不高，因此不至於削弱停止解析的效果。但後者卻並非如此，常見的「使用 VPN 上網」便是透過外國解析器連線的一種模式。這種大眾能輕易操作的手法，確實足以使得停止解析的效用大幅降低。然而，基於現代網路使用者皆已習慣「無摩擦」的上網環境，停止解析的實施能夠增加造訪非法網站的時間成本，從而製造犯罪的阻礙，達到某種程度的犯罪損害防止效果。是以，雖停止解析有此技術上的侷限，卻仍有其犯罪防止之意義。並且，透過改變解析路徑，將使用

doi:10.6342/NTU202302025

者導引至檢警機關設計的違法提醒頁面，也可以達到嚇阻不法之效果，輔以「使用者自律」以及終極的「關閉網站」，仍能達到減少犯罪損害的效果。

而對於網站架設者而言，停止解析無法阻止他們「重新註冊新的域名」而將違法網站轉載，也無法阻止「域名所有權的移轉」。惟對於前者而言，本文以為重新註冊新的域名，其知名度相較於原本的域名較低，導引的功能較弱，故停止解析仍有發揮其削弱再犯的功效。再者，本文認為偵查機關可以與域名註冊管理機構合作，於註冊階段引入管制措施，當核發扣押令時，可以一併下達暫時相似詞彙域名的註冊，以更進一步的降低與原域名的關聯性。至於後者，由於域名所有權的移轉程序上，需要域名註冊管理機構的協力。故僅要將扣押命令一併發送給註冊機構，請求其等協力執行，暫停系爭域名的權利移轉即可防免。此僅需透過扣押命令本身帶有的禁止處分效力便可以補足停止解析本身無法阻止域名移轉的技術限制。

第三節 美國法域名扣押

本文於**第三章**對美國法上的扣押與沒收制度進行介紹，以及美國域名扣押的現制分析，探究域名扣押制度在美國法上的合憲性以及爭議，並就其制度與我國法進行比較，思考供我國參考的可能性。

美國法上的沒收共有三種，行政、刑事與民事沒收。**行政沒收**的程序簡便，執法機關扣押後倘若無人異議，便可以逕行沒收，而無庸經過司法審查。但相對的行政沒收之標的則相當侷限，只能夠針對小額的財產；**刑事沒收**在定位上則是相當於刑罰，故其程序上是附隨於刑事起訴，乃定罪後的法律效果，屬於對人以及具備司法性的程序。但因必須依附於刑事案件程序，過程冗長且繁瑣，以結果來論刑事沒收的效率不彰；是以，在大部分的案件，偵查機關習慣採用的是**民事沒收**。對於沒收標的物，執法機關可以以物為被告，向法院聲請民事沒收。由於所採取者乃民事程序，執法機關的舉證責任較輕，且係對物訴訟，在行為人不明或失蹤的情形，亦

doi:10.6342/NTU202302025

不妨礙程序的進行。故有便利執行的優點，民事沒收在美國實務上也被廣為使用。對於非法域名的處置，也大多是採用民事扣押與沒收。

而美國法上域名扣押的大量實行，緣起於 2010 年的 Operation In Our Sites 執法行動。執法機關於行動中，為了打擊盜版影音網站，將系爭網站的域名作為犯罪工具，對其發動民事沒收與扣押，下架非法網站。實際執行方式，是執法機關請求設立於美國境內的域名註冊管理機構，協力將域名註銷或移轉給國家。且此行動所針對的網站，不僅針對來自境內的侵害，亦包括架設於境外伺服器者。而此作法之所以在美國格外奏效，係因**美國在域名的管制佔據地利優勢**。不論是負責統籌全球網際網路公共資源的 ICANN，或是負責常見頂級域名（如：.com）註冊的公司，皆位於美國境內，故有配合美國執法之義務，也造就了美國在網站取締之國際優勢。惟此部分導致美國於網路犯罪上可以近乎全球執法之結果，亦有論者主張應就域名扣押之管轄規範做限縮解釋，以免**弱化管轄事前劃分之限定效力**。

雖然域名扣押於美國實務上被廣為運用，但其於法律上非毫無爭議，本文對其為合憲性審查，並整理美國法上之實務與學說見解。首先，執法機關請求註冊管理機構移轉或停止解析域名之行為，是否該當「扣押」，而需符合**美國憲法第四修正案的扣押規範**？就此，美國實務上認為域名屬於對犯罪有所促進之工具，且屬於得沒收之財產，故該當得扣押之標的。其中，對於域名之財產定性，則有所爭議，分別有契約說、有體財產權說及無體財產權說。但無論如何，都認定**域名為扣押標的**；至於停止解析以及移轉域名是否屬於「扣押行為」？美國實務對於扣押的定義，係採取 Jacobsen 案標準，認為扣押乃「國家對於財產的個人占有利益，有意義地加以干預」。而將域名移轉給國家，便包含了對域名占有的干預，自然該當扣押。停止解析則是對域名使用效果（引導搜尋網站）的干預，本文認為財產使用的效果亦屬於占有處分之一環，故在此實務見解之下，**停止解析該當扣押行為**。是以，對域名停止解析需遵守美國憲法第四修正案的扣押規範，具備相當理由與符合令狀原則。

doi:10.6342/NTU202302025

另一方面，本文亦關注到了域名扣押對於言論自由造成的限制，故亦就**第一修正案對於言論自由**之保障為討論。在美國釋憲實務上，對於表達性材料之扣押，雖會將之視為「**言論的事前限制**」，但在比例原則之操作並不會特別拉高基準，故在此層次通常不會遭遇違憲風險，在此議題上通常係將審查重點置於程序保障方面。在涉及言論素材之扣押，**事前有司法裁決**之要求（即法官保留）；至於程序進行中中，僅有在涉及「大量」「同標題」之書籍扣押，即封鎖特定言論時，需進行聽審程序，賦予相對人事前發表意見之機會。但在域名扣押本文以為網路言論不至於導致言論禁絕，故原則上**無庸進行聽證**；**事後救濟**的部分則同原扣押之規範，受干預者可以於事後提出抗辯，此部分較無疑義。

最後，本文分析美國民事沒收與我國 2016 年上路的沒收新制具有類似性，皆是獨立以物為主體發動之程序；惟二者也存在相異之處，美國法上之民事對物沒收於證明力之要求較低，且其制度設計目的係重於犯罪利益之剝奪與預防犯罪，而不以犯罪起訴為必要。反之，我國沒收仍須依附於原始案件，思維上仍將犯罪之偵查、起訴作為關注重點。本文無法評論執法效率高、但程序保障相對低的民事沒收制度，是否適於套用於我國法制。惟美國法的扣押、沒收制度與我國仍具一定之相似性，故於思考如何以我國現有強制處分處理非法網站之域名時，本文亦係以美國法之思維，以扣押、沒收規範分析之。

第四節 澳洲法數據破壞令

本文於**第四章**對澳洲的網路管制手段進行介紹，並分析其是否適於我國援引、參考。澳洲的網路治理手段，主要可以區分為四種類型—「非法院之通知」、「法院命令」、「施以處罰」以及「課予 ISP 業者主動審查義務」。由於本文所關注的重點是國家強制下架涉及刑事不法言論之手段，故聚焦討論 2004 年監視設備法的數據破壞令及 1997 年電信法第 313 條第 3 項。

2004 年監視設備法的數據破壞令，其**令狀授權行為**係執法機關可以添加、複製、刪除或更改電腦中所保存的數據，依此文義包括對域名進行停止解析之行為；

doi:10.6342/NTU202302025

而**令狀授權目的**是為了破壞犯罪及減少犯罪損害，以預防而非追訴犯罪為導向；**令狀聲請的要件**係具備「合理懷疑」，「正在、即將或可能發生違法行為」，而授權「破壞數據很可能幫助阻止犯罪」，就此實體要件學說上不乏批評令狀發動門檻過低，只要合理懷疑便可以授權高破壞性的國家干預行為，有比例不相當之嫌；**令狀聲請程序**則是聯邦警察須先獲得機關內部之授權官員同意，復向法院提出聲請，僅例外於緊急情況時可以於事後再向法院補足令狀聲請程序，相當於「相對法官保留」之規定。此種「創新令狀」之方式，優點在於文義上可以具體、貼切的描述技術的內容，而不用如美國作法將停止解析套用於扣押與沒收之下，而遭遇文義解釋之衝突。但面對科技不斷地進步，此種模式會造成立法時間與成本的負擔，亦須考量現實層面立法量能是否充足之問題。

1997 年電信法第 313 條第 3 項，則是一個相對**模糊的的授權依據**，條文內容泛稱提供電信網路或設施之營運商、提供者，於某些情況下有向聯邦、各州及領地的政府官員提供合理、必要之協助。對於請求協助的程序、請求的主體限制、協助方式、事後監督以及救濟程序皆付之闕如，也欠缺司法審查之要求。文義上似得涵蓋執法機關逕向 ISP 業者要求停止解析域名之行為。惟基於前述，本條過於寬泛，且有過多之缺漏，不宜任意的為執法機關所用而作為授權基礎，故澳洲實務上係將本條作為**備位性的條款**，僅在現行法無法涵蓋的行為時，始得以本條作為臨時性的授權，處理問題。是以，回歸停止解析之授權討論，澳洲現行之作法係優先由執法機關向法院聲請數據破壞令，再依此向 ISP 業者請求協力執行，而非逕以電信法第 313 條第 3 項向相關單位為請求。

澳洲法對我國而言，背景差異過大，不僅僅是我國**立法速度**之問題，還有澳洲**憲法上欠缺基本權保障**之設計，此也使澳洲於立法上通常勇於嘗試較具侵略性、嚴厲的手段進行管制，與我國政策取向不同。且考量到現實層面我國立法量能不足，本文認為現階段在我國欲使用停止解析技術，較為可行的作法是於現有規範中尋找授權依據，即主要以美國法作為參考對象。不過，澳洲法中備位性、概括條款的設計（電信法第 313 條第 3 項），本文以為我國非不得參考其作法，如**門檻理論**之

doi:10.6342/NTU202302025

思維，設計一用以授權輕微干預之新興科技的規範，以面對科技進步伴隨的法律爭議。且課予 ISP 業者協力義務，與刑事偵查發動強制處分，兩者乃不相衝突得同時並存之管制手段。而就我國**立法展望**的部分，則可以參酌澳洲創新令狀之作法（數據破壞令），用清晰、可預測的文字，就新興科技為明確的授權，也得以就事前、中、後之程序對技術量身打造審查、監督及救濟規範。

第五節 停止解析於我國之合法性

於**第五章**進入我國法探討時，本文係以基本權干預合法性之審查架構，依序探討對域名發動停止解析，所可能遭遇之法律議題。首先，對域名實施停止解析，將阻礙網路言論發表以及造成域名使用受限，干預了受處分人的**言論自由與財產權**。故本文認為偵查機關於犯罪追訴過程中發動停止解析，乃一強制處分。再者，依本文第二章對於停止解析技術原理之解說，可以知悉停止解析的效果是「阻礙網路使用者依域名造訪網站」，主要影響的是域名的使用效果，與扣押是對於「財產所有權能的部分干預」雷同，故定性上將停止解析作為對域名扣押之執行手段討論。

第一項 法律授權依據

於法律保留層次，我國法上首要的爭議是關於刑訴法第 133 條第 1 項之扣押標的僅限於「物」，似不包含非實體之權利。本文透過法律解釋以及基於現階段執法需求之考量，認為**域名**屬於無體財產權，**具備扣押標的適格**；而停止解析對於域名使用之干預符合扣押之描述；最後，扣押所生**言論自由的限制，尚難謂立法者未授權干預者**，故通過法律保留之審查。惟此乃相對於傳統扣押之額外限制，則需要在個案法官審查核發令狀時，納入審查考量，並加強程序保障。

第二項 比例原則分析

於比例原則層次，本文以為停止解析乃**有助於達成犯罪物沒收預防目的**之手段，且相較於 IP 位址過濾與 URL 過濾，DNS 過濾屬於**同等有效手段中侵害較小**

doi:10.6342/NTU202302025

者。基於犯罪追訴公益之追求，對於犯罪言論的限制乃**符合手段相當性**原則。是以，停止解析乃符合比例原則之強制處分。

第三項 程序正當性探討

於正當法律程序，本文將之區分為事前、事中、事後三個階段探討。首先事前程序乃法官保留原則以及令狀原則之討論，本文認為**TWNIC 的 RPZ 治理政策中，有部分規定違反法官保留之意旨**，宜採取限縮解釋或立法補足之。且在此階段，由於涉及言論自由之域名扣押，本文以為應考量此方面之權利侵害，並參考我國釋憲實務，以較嚴格的審查基準裁量。而在事中核發令狀之程序，雖有論者主張考量到域名扣押對言論自由的干預，應賦予受處分人裁定程序之參與權。惟本文則認為基於**偵查階段扣押秘密性的需求**，在將停止解析套用於扣押執行之概念下，應符合我國法之既有規範，**無需事前通知**受扣押人**參與核發令狀之程序**，事後救濟之賦予已足夠確保程序之正當性。而於事後救濟之階段，本文則建議立法上宜考量停止解析之跨域特殊性，輔助境外救濟。

第四項 管轄設計建議

最後，基於停止解析突破傳統國界疆域之執行模式，本文雖認為**對境外註冊的域名停止解析，並不違反現行我國國際管轄**（刑法第 3 條前段及第 4 條，凡是於我國上網可以觀看之網站，我國即該當「犯罪結果地」）之規定，惟肯認有加重境外救濟程序保障之必要。而在國內法院之分工，本文則認為可以依序以「被告之住所、居所或所在地」、「犯罪行為地」及「犯罪結果地」為管轄之安排，於前階段之分配順序中都無法處理之案件，本文**建議設立專職網路犯罪之機構**，由該專職機構處理偵查與追訴事項。

第五項 未來修法與研究方向

停止解析的出現，為我國過去面對非法網站束手無策的實務窘境，亮起了一盞明燈。但同時，在立法緩不濟急的情況下，要如何合法的使用技術，則是本文欲處理之問題。綜上討論，本文擬以美國、澳洲法制為參考，詳盡分析其等之作法是否

doi:10.6342/NTU202302025

適於我國援用，並就我國現行將停止解析套用於扣押與沒收法制下所碰到的問題，提出本文的建議與解決方案。期許本文的研究，能讓實務運用停止解析時，能同時充實人民基本權之保障。

doi:10.6342/NTU202302025

參考文獻

一、中文文獻

（一）專書

1. 小泉修（著），羅美華（譯）（2003），《圖解你不可不知的網際網路》，世茂。
2. 王兆鵬、張明偉、李榮耕（2022），《刑事訴訟法（上）》，6 版，新學林。
3. 林鈺雄（2022），《刑事訴訟法（上）》，11 版，新學林。
4. 林鈺雄（2022），《新刑法總則》，10 版，元照。
5. 林鈺雄（2023），《沒收新論》，2 版，元照。
6. 陳運財（2014），《偵查與人權》，元照。
7. 陳聰富（2019），《民法總則》，3 版，元照。
8. 簡國璋（2015），《新世代網路概論》，修訂 1 版，上奇。

（二）期刊論文

1. 王士帆（2016），〈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。
2. 朱哲群，〈淺談網域扣押的司法困境〉，《法務通訊》no. 3097，第 5 版。
3. 吳巡龍（2009），〈誹謗性雜誌之扣押〉，《月旦法學雜誌》，78 期，頁 24-25。
4. 吳協展（2009），〈美國犯罪所得單獨沒收之法制研究〉，臺灣高雄地方法院檢察署。
5. 李聖傑（2016），〈犯罪物沒收〉，《月旦法學雜誌》，251 期，頁 60-72。
6. 李榮耕（2015），〈犯罪所得資產的沒收—以美國民事沒收制度為借鏡〉，《輔仁法學》，49 期，頁 55-97。
7. 林子儀（1988），〈言論自由之理論基礎〉，《國立臺灣大學法學論叢》，18 卷 1 期，頁 227-275。

doi:10.6342/NTU202302025

8. 林志潔（2016），〈『沒收新制的挑戰』研討會會議紀錄〉，《沒收新制（一）刑法的百年變革》，頁 274-284，元照。
9. 林鈺雄（2007），〈干預保留與門檻理論—司法警察（官）一般調查權限之理論檢討〉，《政大法學評論》，96 期，頁 189-232。
10. 林鈺雄（2020），〈初探犯罪物沒收—最高法院相關裁判之綜合評釋〉，《法學叢刊》，65 卷 3 期，頁 1-37。
11. 張陳弘（2012），〈去類型化猥褻性言論之理論建構—美國法之比較研究〉，《臺北大學法學論叢》，83 期，頁 43-98。
12. 許育典（2004），〈臺灣學術網路的教育性及其不當資訊管制規範：兒童與少年人格開展的保護觀點〉，《教育政策論壇》，7 卷 2 期，頁 205-228。
13. 陳文貴（2017），〈行政檢查與令狀原則之界限探討〉，《中原財經法學》，39 期，頁 129-186。
14. 陳昱奉（2014），〈數位時代之犯罪偵查與網路自由及隱私權之保障—從網域名稱（Domain Name）之扣押、沒收談起〉，臺灣嘉義地方法院檢察署 102 年度自行研究報告。
15. 陳昱奉（2019），〈跨境電腦犯罪偵辦之未來走向—從『電腦犯罪公約（Convention on Cybercrime）』暨『In Our Sites 行動』出發〉，《台灣國際法學刊》，15:2 期，頁 95-105。
16. 陳昱奉（2022），〈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》，32 期，頁 219-290。
17. 楊崇森（2016），〈澳洲法律制度運作概觀〉，《法令月刊》，67 卷 8 期，頁 26-66。
18. 楊雲驊、簡士淳（2015），〈刑事獨立沒收與追徵立法之必要—以德、美立法為觀察〉，《月旦法學雜誌》，241 期，頁 88-124。
19. 劉靜怡（2001），〈從 ICANN（the Internet Corporation for Assigned Names and Numbers）的成形與發展看網際網路公共資源分配和標準制定統籌管理機制的

doi:10.6342/NTU202302025

政策與法律問題：一九九八至二○○一年的國際趨勢觀察和省思〉，《國立臺灣大學法學論叢》，30 卷 6 期，頁 95-163。

20. 劉靜怡（2004），〈『言論自由』導論〉，《月旦法學教室》，26 期，頁 73-81。
21. 潘怡宏（2020），〈保全扣押之發動要件與扣押競合之處理〉，《沒收新制（五）沒收實例解析》，頁 355-372。
22. 蔡志宏（2022），〈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》，31 期，頁 197-237。
23. 蔡彩貞（2016），〈我國刑事沒收特別程序之建制與淺析〉，《司法週刊》，1805 期，頁 4-19。
24. 蔡維音（2006），〈財產權之保護內涵與釋義學結構〉，《成大法學》，11 期，頁 31-74。
25. 賴祥蔚（2011），〈言論自由與真理追求—觀念市場隱喻的溯源與檢視〉，《新聞學研究》，108 期，頁 103-139。
26. 戴豪君、余啟民主持（2021），〈網域名稱涉有違反相關法律之實例研究及處置建議委託研究期末報告〉，國家通訊傳播委員會。
27. 薛智仁（2018），〈刑事沒收制度之現代化：2015 年沒收實體法之立法疑義〉，《國立臺灣大學法學論叢》，47 卷 3 期，頁 1053-1123。
28. 魏靜芬（2001），〈國際法上管轄權之域外適用〉，《中央警察大學法學論集》，6 期，頁 387-404。

（三）學位論文

1. 王奕華（2013），《網域名稱爭議處理—以統一網域名稱爭議解決政策（UDRP）為中心》，國立臺灣大學法律學研究所碩士論文。
2. 陳怡卉（2017），《公共論壇與言論自由—以美國法制為中心》，東吳大學法律學研究所碩士論文。
3. 陳建廷（2022），《犯罪物沒收》，國立臺灣大學法律研究所碩士論文。

doi:10.6342/NTU202302025

4. 陳劍釗（2009），《TWNIC 網域名稱爭議處理機制與我國民事訴訟制度之比較研究》，國立高雄第一科技大學科技法律研究所碩士論文。
5. 黃姿蓉（2017），《我國刑事司法互助發展模式與困境之探討》，中央警察大學外事警察研究所碩士論文。
6. 蔡志宏（2018），《全球域名法制之治理架構研究—以 ICANN 的組織原理及制度運作為中心》，國立交通大學科技法律研究所博士論文。
7. 簡菀菱（2017），《從法律經濟學與財產權理論之觀點探討新通用頂級域名分配機制》，國立交通大學科技法律研究所博士論文。

（四）網路資源

1. 黃勝雄（2020），《DNS RPZ 摘要說明》，載於：https://blog.twnic.tw/2020/09/23/15311/。
2. 愛范兒（2016），〈全球網路的新『波瀾』：美國正式交出域名管理權〉，《數位時代》，載於：https://www.bnext.com.tw/article/41205/icann-domain。
3. 蔡志宏（2019），〈『關注 31 條』網站域名下架，是台灣域名法學發展上的里程碑〉，《關鍵評論》，載於：https://www.thenewslens.com/article/116230。

二、外文文獻

（一）專書

1. CHEMERINSKY, ERWIN (2011), CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES, 4th ed.
2. NATIONAL RESEARCH COUNCIL ET AL. (2005), SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION.

（二）期刊論文

1. Abdo, Alex (2017), *Why Rely on the Fourth Amendment To Do the Work of the First?*, 127 YALE LAW JOURNAL FORUM 444-457.

doi:10.6342/NTU202302025

2. Bambauer, Derek E. (2009), *Filtering in OZ: Australia's Foray into Internet Censorship*, 31(2) UNIVERSITY OF PENNSYLVANIA JOURNAL OF INTERNATIONAL LAW 493-531.
3. Bambauer, Derek E. (2012), *Orwell's Armchair*, 79 UNIVERSITY OF CHICAGO LAW REVIEW 863-944.
4. Burnett, Arthur L. (1974), *Obscenity: Search and Seizure and the First Amendment*, 51(1) DENVER LAW REVIEW 41-74.
5. Freeman, Alexis (2002), *Internet Domain Name Security Interests: Why Debtors Can Grant Them and Lenders Can Take Them in this New Type of Hybrid Property*, 10 AMERICAN BANKRUPTCY INSTITUTE LAW REVIEW 853-889.
6. Hancock, Daniel (2010), *You Can Have It, But Can You Hold It?: Treating Domain Name As Tangible Property*, 99(1) KENTUCKY LAW JOURNAL 185-209.
7. Kendall, Sarah & Dominic Frost (2022), *Network Activity, Account Takeover and Data Disruption Warrants: How Novel Law Enforcement Powers Impact Media Freedom*, 28(2-3) AUSTRALIAN JOURNAL OF HUMAN RIGHTS 249-265.
8. Kesari, Aniket et al. (2017), *Deterring Cybercrime: Focus on Intermediaries*, 32 BERKELEY TECHNOLOGY LAW JOURNAL 1093-1134.
9. Liu, Michael Xun (2014), *Jurisdictional Limits of in rem Proceedings Against Domain Names*, 20(2) MICHIGAN TELECOMMUNICATIONS & TECHNOLOGY LAW REVIEW 467-496.
10. Lusty, David (2002), *Civil Forfeiture of Proceeds of Crime in Australia*, 5(4) JOURNAL OF MONEY LAUNDERING CONTROL 345-359.
11. Maxwell, Francis (2022), *When Good Is Not Good Enough: Evaluating the Proportionality and Necessity of the Australian Government Hacking Warrants*, 34(2) CRIMINAL JUSTICE 136-154.

doi:10.6342/NTU202302025

12. Ohm, Paul (2008), *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, STANFORD TECHNOLOGY LAW REVIEW 40-59.
13. Redish, Martin H. (1984), *The Proper Role of the Prior Restraint Doctrine in First Amendment Theory*, 70(1) VIRGINIA LAW REVIEW 53-100.
14. Williams-Wynn, Chris (2010), *The Great Firewall of Australia: The Political Concerns*, 26(1) POLICY MAGAZINE 33-35.

（三）網路資源

1. Arnold, Bruce Baer, *Inquiry into the Use of Subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operation of Illegal Online Services, Submission 10*, https://www.aph.gov.au/DocumentStore.ashx?id=e8908f46-9df3-44a7-acd7-8d 7588b02066&subId=299370.
2. Cole, Agatha M. (2012), *ICE Domain Name Seizures Threaten Due Process and First Amendment Rights*, https://www.aclu.org/news/national-security/ice-domain-name-seizures-threaten-due-process-and.
3. ICANN (2012), *Guidance for Preparing Domain Name Orders, Seizures & Takedowns*, https:// www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.
4. Malcolm, Jeremy et al., *Which Internet Registries Offer the Best Protection for Domain Owners?*, https://www.eff.org/files/2017/08/02/domain_registry_whitepaper.pdf.
5. Maxwell, Andy, *US Embassy Threatens to Close Domain Registry Over "Pirate Bay" Domain*, https://torrentfreak.com/us-embassy-threatens-to-close-domain-registry-over-pirate-bay-domain-170620/.
6. Sun, Lasa (2016), *Freedom of Speech, Democracy and Cyberspace: Lessons from Australia, Singapore and India*, https://doi.org/10.25949/19427480.v1.

doi:10.6342/NTU202302025