網路爬蟲之刑事責任

劉 瑩*

目 次

關鍵詞：網路爬蟲、刑事責任、電腦犯罪、秘密、著作權

Keywords：Web Crawler, Criminal Liability, Computer Crime, Secret, Copyright

* 輔仁大學法律學院法律學系博士生。
投稿日期：2021 年 12 月 21 日；接受刊登日期：2022 年 8 月 10 日。

摘　要

在資訊化時代，網路爬蟲被廣泛應用於各個領域進行資料的挖掘與收集。網路爬蟲在展現出顯而易見的優勢同時，隨之而來的還有對秘密、財產、國家安全等法益侵害的可能性。法律無法僅將使用網路爬蟲視為中性之行為，必須對其作出適當的評價。只不過何種使用網路爬蟲行為應受刑法規制，以及應當承擔何種刑事責任尚無定論。

本文試結合網路爬蟲運作原理及實際案例，歸納當前不當使用網路爬蟲的行為態樣，分析其中需承擔刑事責任的行為類型，並通過相關犯罪構成要件的檢視，探討可適用之罪名，明確網路爬蟲「罪」與「非罪」的界限。考量到並非所有使用網路爬蟲行為都具有法益侵害性或刑罰必要性，以當前的刑事規範對其中的不法行為類型進行規制尚未出現明顯之缺失，故無需針對使用網路爬蟲行為進行專門的立法。

A Study of Criminal Liability about Web Crawler

Liu Ying

Abstract

In the information age, Web Crawler is widely used in various fields for data mining and collection. While Web Crawler shows obvious advantages, it also has the possibility of infringing on legal interests such as secrets, property and national security. Therefore, the law can not only regard the use of Web Crawler as neutral behavior, and it must be properly evaluated. However, what kinds of use of Web Crawler should be regulated by criminal law and what kinds of criminal responsibility should be borne are still inconclusive.

This article attempts to combine the operating principles of Web Crawler and actual cases to summarize the current behavior patterns of improper use of Web Crawler, and to explore which acts should undertake the criminal responsibility. It also discusses the applicable crimes through the analysis of relevant criminal constitutional elements, and clarifies the boundary between

the crime and non-crime of Web Crawler. Furthermore, considering that not all acts of using Web Crawler have legal interest infringement or penalty necessity, and there is no obvious deficiency in regulating the illegal acts with the current criminal law. Therefore, there is no need to legislate a special law for Web Crawler.

壹、前　言

網際網路自1969年誕生至今已逾五十年，其在飛速發展的同時產生了大量的資料（Data）[1]。這些豐富的資料不僅為人們提供了解世界之機會，亦提高了日常生活之效率。隨著大數據（Big Data）時代的到來，海量的資料在持續地產生、傳遞，資料之重要性及經濟效益日益凸顯，人們希望能夠從不同的網站獲取並分析資料。

與手動複製網站顯示的資料到本機儲存（Local Storage）這一枯燥且費時的傳統方法相比，「網路爬蟲」（Web Crawler）[2]得快速且準確擷取大量資料並儲存於電子表格或資料庫[3]。網路爬蟲之使用並非「高不可攀」，網站上不僅有免費的教學資源，還有許多已編寫好之爬蟲程式。任何稍具技術專長且能使用必要電腦資源的人，皆可使用網路爬蟲[4]。同時，網站對於用戶之易用性及可訪問性的關注，亦為爬蟲擷取資料提供便利[5]。網路爬蟲之高效性及較低技術門檻使其使用日漸頻繁，根據統計，當前網路上爬蟲所占的網際網路流量已達40.8%[6]。

近年來，與網路爬蟲相關之案件層出不窮，人們在享受網路爬蟲帶來之便利的同時，亦意識到其對電腦與資料的安全性以及個人隱私與財產等所生之威脅，進而

1　Data也有翻譯為「數據」。

2　網路爬蟲的英文名稱還有Web Crawling、Web Scraper、Web Scraping，此外文獻中還常使用Screen Scraping（螢幕擷取）、Data Mining（資料挖掘）、Web Harvesting（網頁收割）、Robot（機器人）、Automatic Web Browser（自動網路瀏覽器）、Spider（蜘蛛）、Search Engine（搜尋引擎）等術語來指稱網路爬蟲。陳會安，《Python從網路爬蟲到生活應用超實務：人工智慧世代必備的資料擷取術》，博碩文化股份有限公司，2020年12月，頁3-1；李周平，《網絡數據爬取與分析實務》，上海交通大學出版社，2018年9月，頁32；Andrew Sellars, "*Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*", 24 Boston University Journal of Science and Technology Law, Sept. 2018, pp. 381-382；Amber Zamora, "*Making Room for Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online*", 12 J. Bus. Entrepreneurship & L., May. 2019, p. 204; Myra F. Din, "*Breaching and Entering: When Data Scraping Should Be a Federal Computer Hacking Crime*", 81 Brooklyn Law Review, 2015, p. 410; Md. Abu Kausar/ V. S. Dhaka/ Sanjeev Kumar Singh, "*Web Crawler: A Review*", 63 International Journal of Computer Applications, Feb. 2013, p. 31; Ryan Mitchell, "*Web Scraping with Python: Collecting Data from the Modern Web*", O'Reilly Media Inc., Jun. 2015, p. 7.

3　S.C.M. de S Sirisuriya, "*A Comparative Study on Web Scrapin*g", Proceedings of 8th International Research Conference, KDU, Nov. 2015, p. 135.

4　Zachary Gold /Mark Latonero, "*Robots Welcome? Ethical and Legal Considerations for Web Crawling and Scraping*", 13 Wash. J. L. Tech. & Arts, Apr. 2018, p. 285.

5　Jeffrey Kenneth Hirschey, "*Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*", 29 Berkeley Tech. L.J., Apr. 2014, p. 904.

6　Bad Bot Report 2021,〈https://www.exclusive-networks.com/se/wp-content/uploads/sites/25/2020/12/Imperva-Bad-Bot-Report-2021.pdf〉, last visited Sept. 19, 2021.

引發了對於網路爬蟲合法性之討論。在刑法領域，則主要聚焦於何種使用網路爬蟲之行為應當承擔刑事責任以及可能適用之罪名，此為本文探討之主要內容。

本文先從網路爬蟲之概念、運作原理、應用及可能造成的法益侵害入手，再結合相關案例將不當使用網路爬蟲之行為依行為手段及所取得資料之性質予以區分，進行歸納與說明；接著，就不當使用網路爬蟲行為可能成立之犯罪進行分析；最後，從網路爬蟲之需求性與必要性及當前刑事規範對該行為之規制，來探討是否有必要對其進行專門之立法。

貳、網路爬蟲之解析

一、網路爬蟲的定義

網際網路是目前最大的資料庫，如將其比作一張巨大的蜘蛛網，爬蟲就是一隻小蜘蛛，沿著網路抓取自己的獵物（資料）[7]。網路上大部分資料皆為未按照特定的方式組織，亦未預先定義資料模型之非結構化資料[8]，網路爬蟲可以從網站提取此類資料，並將其轉化為可理解之結構化資料，以便儲存、分析[9]。無論是結構化資料還是非結構化資料，皆是網路爬蟲所擷取之對象，而所謂「網路爬蟲」，即指可以自動從網站擷取資料的一種程式[10]。

Web Crawler、Web Crawling、Web Scraper、Web Scraping 雖常被當做網路爬蟲的英文名稱，看似並無區別，然於電腦專業技術領域中，其內涵不盡相同。Web Crawling、Web Crawler 為遍歷網站上每一個頁面並擷取網站上所有資料之程式；Web Scraping、Web Scraper 則更專注於網站上特定資料之擷取[11]。無論是 Web Crawling、

7 趙廣輝，《Python 語言及其應用》，中國鐵道出版社，2019 年 7 月，頁 244。

8 Vandana Shrivastava, "*A Methodical Study of Web Crawler*", 8 International Journal of Engineering Research and Applications, Nov. 2018, p. 1.

9 S.C.M. de S Sirisuriya, supra note 3, at 135.

10 S.S. Dhenakaran/ K. Thirugnana Sambanthan, "*Web Crawler-An Overview*", 2 International Journal of Computer Science and Communication, Jun. 2011, p. 265; Vandana Shrivastava, supra note 8, at 1; Md. Abu Kausar/ V. S. Dhaka/ Sanjeev Kumar Singh, supra note 2, at 31-32; Myra F. Din, supra note 2, at 410-411; Ryan Mitchell, supra note 2, at 7；另有學者將其表述為一種資料擷取軟體、技術，本文認為網路爬蟲確實也是一種電腦技術或是軟體，然該技術與軟體的本質仍是電腦程式，故資料擷取之技術等應為網路爬蟲之廣義定義。Mini Singh Ahuja/ Dr Jatinder Singh Bal/ Varnica, "*Web Crawler: Extracting the Web Data*", 13 International Journal of Computer Trends and Technology, Jul. 2014, p. 132; Christopher Olston /Marc Najork, "*Web Crawling*", 4 Foundations and Trends in Information Retrieval, 2010, p. 176; 陳會安，前揭（註 2），頁 3-1。

11 Web Scraping vs Web Crawling: What's the Difference?, 〈https://www.parsehub.com/blog/web-scraping-vs-web-crawling/#:~:text=A%20Web%20Crawler%20will%20generally,or%20any%20other%20data%

Web Crawler還是Web Scraping、Web Scraper皆是自動訪問目標網站，擷取所需資料之程式，符合本文所討論之網路爬蟲的定義，故而無需對其詳細區分。

至於其他諸如Screen Scraping（螢幕擷取）、Web Harvesting（網頁收割）等各式各樣的名稱，但凡其本質上屬自動擷取資料之程式，均為本文所指之網路爬蟲。惟網路爬蟲需與搜尋引擎進行區分，網路爬蟲乃搜尋引擎之基礎[12]，為搜尋引擎抓取系統之重要組成部分[13]，二者不能等同。

二、網路爬蟲的運作原理

網路爬蟲運作之核心在於模擬人類瀏覽操作，並對獲取到的網頁進行解析，進而擷取所需資料[14]。網路爬蟲與一般使用者獲取網頁內容的路徑相同，皆需向伺服器發送存取請求（Request），伺服器則接收並對請求的有效性進行驗證，隨即向用戶端作出回應（Response），用戶端在接收到伺服器回應之內容後，將內容予以展示[15]。

超文字傳輸通訊協定（HyperText Transfer Protocol, HTTP），則定義了用戶端如何向伺服器請求，伺服器如何根據請求作出回應之規則[16]。當瀏覽器向網站伺服器發出訪問請求時，即將請求資訊打包成一個資料包，發送給伺服器。HTTP請求由三部分組成：請求方法URL（Uniform Resource Locator）[17]協議和版本、請求標頭（Request Header）、請求正文[18]。一般用戶在瀏覽器地址欄輸入URL並敲擊確認鍵，瀏覽器即用戶端就會向網站的伺服器發送請求，而爬蟲則需要用代碼來模擬此過程。

待伺服器傳回相應之內容，爬蟲即對網頁進行解析，蒐集其中有用的資料及URL，並將該URL加入待抓取之列表中，同時將有用的資料保存至電子表格、資料庫、文本文件等。而後，程式會一直重複上述過程，直到滿足所設定之條件方停止[19]。圖1為網路爬蟲的運作原理之簡單架構。

20sets.〉, last visited Sept. 19, 2021；徐寧，《論大數據時代資料蒐集之智慧財產法與競爭法爭議：以網路爬蟲技術為中心》，國立政治大學科技管理與智慧財產研究所碩士學位論文，2018年7月，頁11。

12 郭卡、戴亮，《Python數據爬取技術與實戰手冊》，中國鐵道出版社，2018年8月，頁2。

13 Mini Singh Ahuja/ Dr Jatinder Singh Bal/ Varnica, supra note 10, at 132.

14 郭卡、戴亮，前揭（註12），頁 2。

15 零一、韓要賓、黃園園，《科學運算：數據乃AI之基石：用Python爬蟲抓取大量資料》，深石數位科技股份有限公司，2018年11月，頁2-8。

16 肖盛文，《計算機網絡基礎》，航空工業出版社，2017年8月，頁135；Andrew Sellars, supra note 2, at 385-386.

17 URL即統一資源定位符，俗稱網址，是用來表示資源在網際網路上的地址。曾劍平，《Python爬蟲大數據採集與挖掘》，清華大學出版社，2020年3月，頁107。

18 李安，《語料庫語言學及Python實現》，山東大學出版社，2018年8月，頁92-93。

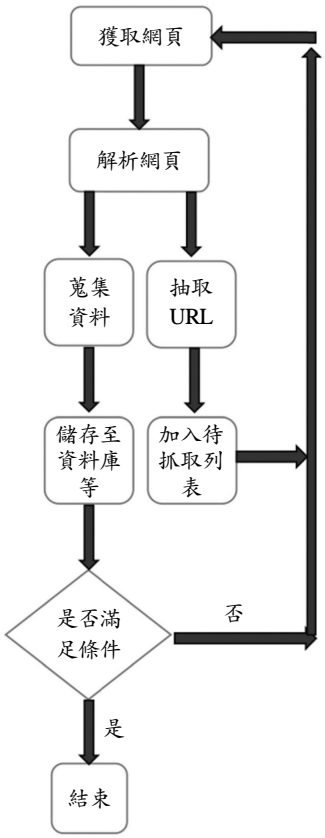

圖 1　網路爬蟲運作原理

資料來源：作者自行整理

三、網路爬蟲的應用

網路爬蟲在資料蒐集上具有精準、高效等顯而易見的優勢，其被廣泛應用於各個領域，其中最廣為人知的應用便是搜尋引擎。搜尋引擎使用爬蟲訪問數以萬計的網站，將其上之資料進行及時、全面的採集，並以易於閱讀之形式呈現給用戶[20]。例如谷歌搜尋引擎就是使用一個名為 Googlebot 的網路爬蟲從數十億個網頁中抓取資料。還有各種聚合器（aggregator），將從網路上獲取的網頁資訊進行整合，並呈現給用戶[21]。聚合器與搜尋引擎類似，但聚合器所蒐集和呈現的是特定類型之資料，例

19 范春曉，《Web 數據分析關鍵技術及解決方案》，北京郵電大學出版社，2017 年 8 月，頁 12；Md. Abu Kausar/ V. S. Dhaka/ Sanjeev Kumar Singh, supra note 2, at 32.

20 曾劍平，前揭（註 17），頁 11；Myra F. Din, supra note 2, at 412.

21 Sean O'Reilly, "*Nominative Fair Use and Internet Aggregators: Copyright and Trademark Challenges Posed by Bots, Web Crawlers and Screen-Scraping Technologies*", 19 Loy. Consumer L. Rev., 2007, p. 274.

如金融聚合器，用戶在一個地方即可查看自己所有的金融資料，而不必登入每個銀行的帳戶進行查閱[22]；新聞聚合器，從多個來源獲取新聞並在一個網站上顯示，如Google News、Yahoo！News[23]。

網路爬蟲常被應用於網路輿情監測，通過對特定網站中的頁面資料為提取、統計分析等，對輿情態勢做出合適研判[24]；網路爬蟲還被用於搜尋網路犯罪，即使是發生在普通搜尋引擎難以搜尋到的暗網（Dark web）上之犯罪活動，亦可藉由網路爬蟲予以監測、揭露[25]；企業還能透過網路爬蟲從論壇、博客、社交媒體等地方蒐集資料，對用戶偏好等進行分析[26]。

儘管上述各種應用所使用的爬蟲頗為複雜，專業性較強，但並不意味一般人就無法使用爬蟲。一般人完全可以自己編寫簡單的爬蟲程式或從網路上找到現成的爬蟲程式，進行文獻、案例、價格、書籍或電影評論之蒐集與分析等。

四、網路爬蟲可能侵害的法益

任何技術的使用都是雙面刃，網路爬蟲亦不例外。網路爬蟲之廣泛應用推動社會資訊的流動，使資料之共享與分析具有更多的可能性，但與此同時，法益侵害之可能性亦存在。

根據網路爬蟲運作之原理，使用網路爬蟲擷取資料可分為訪問與儲存兩個階段。在訪問階段，網站管理者出於維護網站運作或是資料安全之目的，抑或出於限制競爭之考量，常設置相應之安全防控措施，以阻止爬蟲向網站伺服器發送請求或讓伺服器停止回應。在儲存資料階段，雖然網路上的資料大多數皆為完全公開的資料，即任何人皆可自由獲取、分享及使用之資料，但除此之外，尚有限制儲存、限制重新使用、非公開之資料等。對於此類資料，資料主體並未放棄其保密性、獨占性、可使用性，故資料之蒐集、使用、處理自應受到保護。

在網路世界裡，孤立的資料尚不足以體現其價值，但若將其置於特定環境中，

22 Julia Alpert Gladstone, "*Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data*", 19 J. Marshall J. Computer & Info. L., 2001, pp. 315-317.

23 Kimberley A. Isbell, "*The Rise of the News Aggregator: Legal Implications and Best Practices*", Berkman Center Research Publication, No. 2010-10, Aug. 2010, p. 2.

24 曾劍平，前揭（註17），頁11；任書平，《基於人工智慧之輿情分析》，淡江大學資訊工程學系碩士論文，2020年6月，頁1-12。

25 Mandeep Pannu/ Iain Kay/ Daniel Harris, "*Using Dark Web Crawler to Uncover Suspicious and Malicious Websites*", Tareq Z. Ahram / Denise Nicholson ed., 782 Advances in Intelligent Systems and Computing, Springer International Publishing AG, 2018, p. 109-115.

26 Zachary Gold /Mark Latonero, supra note 4, at 278.

並經分析，則資料就變成人們所期望得到的、有價值之資訊[27]。換言之，資料不單單只是電腦中由「0」和「1」組成的編碼，在其之上還承載著有價值、有意義之資訊，二者呈現一體兩面關係，無電腦資料，則電腦資訊亦不復存在[28]。資訊所涉及之類型具有多樣性，蒐集特定類型資訊亦可能侵害相應之法益。

法益乃法律上所保護之生活利益，而所謂生活利益，則係社會多數人在日常生活中所接受之價值觀[29]。刑法保護法益之分類，雖有爭議，惟就現行刑法分則觀之，係採國家法益、社會法益及個人法益之三分法[30]。

就個人法益而言，網路爬蟲無視或破解網站所設之安全防控措施而訪問網站擷取資料之行為，可能對電腦及資料安全造成損害，即可能侵害個人財產、秘密等法益；若使用網路爬蟲擷取他人在社交媒體、論壇上發佈的訊息，與他人的互動等，此等資訊可能會涉及個人資料，或是揭示他人之政治、宗教及其他觀點[31]，獲取此類資訊，則有侵害他人隱私之嫌。另使用網路爬蟲將刊載於網站上之受著作權法保護之文字、影像、音樂等資料進行複製，或者使用網路爬蟲蒐集網站商品銷售價格、交易底價、成交數量等資訊，因此類資訊具有經濟價值，故獲取該資訊，亦可能侵害他人之財產。

就社會法益而言，若是使用網路爬蟲擷取客戶名單、人事管理、技術、方法等資訊，則有侵害社會秩序之可能。就國家法益而言，若使用網路爬蟲所蒐集之資訊為國家重大決策事項、軍事行動計畫、軍事部署、國防預算及統計等與國家安全、國防安全、軍事安全及公務相關之資訊，則有侵害國家存亡安全之虞。

參、不當使用網路爬蟲的態樣及實際案例

網際網路之本質就是以電腦為載體，進行資料之共享、流轉，為應對巨量的資料，自動化處理技術的發展必不可少[32]，而網路爬蟲作為一種電腦程式，本身並無好壞之區別，端視行為人如何使用。正當使用網路爬蟲即恪守法律規範及網站管理者關於訪問、擷取資料之要求，妥當擷取所需資料，此時擷取資料行為即為獲得授權之行為，自未侵害法益。而不正當使用網路爬蟲往往未遵守法律規範及網站之要求，

---

27 Ali M. Al-Khouri, "*Data Ownership: Who Owns 'My Data'?*", 2 International Journal of Management & Information Technology, Nov. 2012, p. 1.

28 蔡蕙芳，〈電磁紀錄無權取得行為之刑法規範〉，《中正法學集刊》，2003 年 10 月，第 13 期，頁 109-110。

29 靳宗立，《刑法總論 I：刑法基礎理論暨犯罪論》，自版，2010 年 9 月，頁 118。

30 甘添貴，《刑法各論（上）》，三民書局股份有限公司，2019 年 9 月，5 版，頁 4。

31 Zachary Gold /Mark Latonero, supra note 4, at 282.

32 付強、李濤，〈網絡爬蟲的刑法應對〉，《中國檢察官》， 2020 年 9 月，第 18 期，頁 20。

以不恰當之手段擷取資料或是擷取屬於受法律類型化保護的資料，則極有可能侵害法益，引起責任承擔之問題。以下結合實際案例從使用網路爬蟲的手段與取得資料的性質，具體說明不當使用網路爬蟲的態樣。

一、以不當使用網路爬蟲的手段來觀察

㈠違反網站管理規定

網站管理規定是網站管理者為保證網站的正常運行、維護資料安全及自身利益而設置的各種規則，其中自然也包括針對爬蟲的管控規則，大致上可將違反網站管理規定使用網路爬蟲分為以下三類：

1. 違反網站管理者所設條款

網站管理者所設的條款包括「使用條款」、「服務協議」、「用戶協議」、「法律聲明」等，這些條款通常被置於網站的下方，或在用戶首次訪問網站或進行註冊時以跳出對話框的形式呈現，並要求用戶點擊「同意」後才可進行後續操作。網站管理者若欲對爬蟲作出限制，則會在條款予以說明[33]。

違反網站所設置的條款使用網路爬蟲擷取資料，即違反網站管理者在「使用條款」等中關於禁止使用爬蟲之規定。例如【案例一】Outtask公司從FareChase公司處獲得爬蟲程式，其無視Southwest Airlines公司所經營網站之「使用條款」中禁止使用爬蟲程式之規定，而使用爬蟲擷取該網站上票價與時刻表資訊[34]。

2. 違反網站「爬蟲協議」

爬蟲協議，又稱機器人協議、機器人排除標準（Robots Exclusion Standard、Robots Exclusion Protocol、robots.txt），是網站管理者告知爬蟲訪問資料之權限與可擷取資料及禁止擷取資料之範圍，並以robots.txt命名置於主機的最上層目錄中的TXT格式文字檔[35]。爬蟲協議中設定了User-agent、Disallow、Allow值，User-agent用於標識爬蟲，Disallow與Allow用來設定不同的訪問許可[36]。如下圖2為Facebook網站部分爬蟲

---

33 「crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services without the prior consent of Twitter is expressly prohibited.」Twitter服務條款，〈https://twitter.com/en/tos〉, last visited Nov. 26, 2021；「非依臺灣證券交易所同意之方式或經臺灣證券交易所同意者，禁止透過包括但不限於自動化裝置、指令碼、自動程式、蜘蛛程式、爬蟲程式或擷取程式等方式下載本網站之軟體或資料。」臺灣證券交易所使用條款，〈https://www.twse.com.tw/zh/page/terms/use.html〉，最後瀏覽日：2021年11月26日。

34 Southwest Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435, 437-440 (2004).

35 韋世東，《偏不讓你抓：最強Python爬蟲vs反爬蟲大戰實錄》，深智數位股份有限公司，2020年7月，頁10-45。

36 曾劍平，前揭（註17），頁53-57。

協議，該協議顯示允許百度、蘋果、谷歌等大型企業使用爬蟲訪問並擷取部分資料，其他爬蟲則被禁止訪問與擷取該網站上的資料。

爬蟲協議與網站所設條款的區別在於，爬蟲協議專門針對爬蟲所設，使用程式可讀取的代碼語言編寫，且對於資料的訪問權限與可擷取範圍規定的較為細緻。違反爬蟲協議使用爬蟲，即不遵守爬蟲協議之限制，而使用爬蟲擷取資料。如【案例二】百度公司為限制奇虎公司的搜尋引擎抓取其網站上之內容，遂於網站之爬蟲協議中禁止奇虎公司爬蟲的訪問。然奇虎公司並未遵守該爬蟲協議，仍使用爬蟲擷取該網站上之內容提供給用戶[37]。

```
User-agent: Applebot
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/

User-agent: baiduspider
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/

User-agent: Bingbot
Allow: /*/videos/
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/
Allow: /watch

User-agent: facebookexternalhit
Allow: /*/videos/
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/
Allow: /watch/?v=*

User-agent: Googlebot
Allow: /*/videos/
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/
Allow: /watch

User-agent: LinkedInBot
Allow: /*/videos/
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/
Allow: /watch/?v=*

User-agent: teoma
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/

User-agent: Twitterbot
Allow: /ajax/bootloader-endpoint/
Allow: /ajax/pagelet/generic.php/PagePostsSectionPagelet
Allow: /safetycheck/

User-agent: *
Disallow: /
```

圖 2　Facebook 網站部分爬蟲協議

資料來源：https://www.facebook.com/robots.txt（截取日期：2021.11.21）

3. **違反網站管理者所發出的拒絕訪問通知**

拒絕訪問通知，係網站管理者就行為人未得同意而使用爬蟲擷取資料之行為，在事後向行為人作出停止使用爬蟲的通知。違反該通知，即爬蟲使用者在收到通知後並不執行通知之要求，仍然繼續使用爬蟲擷取網站上之資料。如【案例三】3Taps 公司使用爬蟲擷取 Craigslist 公司經營的網站上資料。Craigslist 公司向 3Taps 公司發出停止函，明確拒絕其出於任何目的而使用該網站，並封鎖與 3Taps 相關之 IP 位址。但 3Taps 公司並未遵守該停止函，而是使用代理伺服器隱藏其身分後繼續擷取資料[38]。

---

37 北京市第一中級人民法院 2013 年度一中民初字第 2668 號民事判決。

38 Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 966-970 (2013).

㈡非法使用訪問權限

網站通常以登入控制機制實現訪問權限之控制，需用戶輸入特定之帳號與密碼等予以登入，此意味著只有具有該帳戶特殊權利之用戶，才被授權訪問網站，無法滿足身分驗證要求之用戶則被排除訪問權限[39]。

非法使用訪問權限擷取資料有兩種形式，其一，使用他人帳號密碼，亦可是Cookie[40]，亦即將以騙取、竊取等方式而知悉他人帳號密碼寫入爬蟲程式中，使其得以訪問網站擷取資料；其二，超越權限使用本人之帳號密碼，即超越原預設自己帳號僅可瀏覽或僅可儲存部分資料等之權限，而擷取資料。此與申請多個本人帳號之情形不同，前者違反帳號訪問權限，後者僅違反帳號管理規定，所申請之多個帳號仍然具有訪問網站之權限。如【案例四】TomorrowNow公司使用Oracle公司客戶之帳號密碼，從而使用爬蟲大量擷取Oracle網站上的文檔及軟體[41]。又如【案例五】余○濤在淘寶公司工作期間，將自己內部論壇帳號的Cookie寫入爬蟲程式中，超越自己帳號只能查詢、瀏覽員工資料的權限，擷取員工個人資料2萬餘筆[42]。

㈢破解訪問限制

1. 破解登入機制訪問網站

登入機制是網站控制用戶訪問權限的主要手段，帳號密碼係當前登入機制中最常見之方式，其他還有如指紋、臉部識別等。破解登入機制即以破譯密碼之方式、破壞登入控制程式而使登入機制失效之方式、利用漏洞繞過登入機制之方式使不具有訪問權限之爬蟲能夠訪問網站擷取資料。如【案例六】張○等人利用具有破解安全防控措施及自動擷取資料功能的「淘小米」、「林某2」等軟體，對已註冊過淘寶網站的電子信箱帳號進行篩選，並以撞庫攻擊、忘記密碼等方式破譯密碼，大量擷取淘寶、支付寶帳號內之姓名、身分證號等資料[43]。

---

39 Orin S. Kerr, "*Norms of Computer Trespass*", 116 Columbia Law Review, 2016, p. 1171.

40 Cookie是網頁伺服器儲存在個人電腦硬碟上的一個文本文件，裡面包含有用戶名、密碼、用戶設定、IP等信息。對於使用Cookie的網站，Cookie被放在向網站伺服器發送的訪問請求中，以減少用戶訪問時反復輸入登入資訊。Michael R. Siebecker, "*Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*", 76 Southern California Law Review, May 2003, pp. 896-898.

41 TomorrowNow, Inc., Sentenced on Computer Intrusion and Copyright Infringement Charges,〈thttps://archives.fbi.gov/archives/sanfrancisco/press-releases/2011/tomorrownow-inc.-sentenced-on-computer-intrusion-and-copyright-infringement-charges〉, last visited Oct. 2, 2021; SAP to Pay $20 Million Criminal Fine in 'Web Scraping' Case,〈https://1.next.westlaw.com/Document/I228cb70af0ec11e08b05fdf15589d8e8/View/FullText.html? transitionType＝FolderItem&contextData＝(cid.cb7d7a7b2e6d47c391aa7f1b19cb0b9d*oc.Default)〉, last visited Oct. 2, 2021.

42 浙江省杭州市中級人民法院2018年度浙01刑終第441號刑事裁定。

43 浙江省紹興市越城區人民法院2016年度浙0602刑初第1145號刑事判決。

2. **破解 UA 驗證訪問網站**

UA 即 User-Agent，是一種向訪問網站提供所使用的瀏覽器類型及版本、操作系統及版本等資訊的標識[44]。網站可通過識別 UA 值來辨別用戶身分，以達到限制爬蟲訪問之目的。

破解 UA 驗證，即更改爬蟲程式代碼中的 UA 值，將其偽裝成任意瀏覽器繞過 UA 驗證[45]。如【案例七】上海晟品網絡科技有限公司主管人員張○禹等指使郭○使用偽造的 UA 及 IP 繞過北京字節跳動網絡技術有限公司伺服器訪問頻率之限制，對儲存於其中之影片資料進行抓取[46]。

3. **破解 IP 封鎖訪問網站**

為確保電腦在通訊時能互相識別，每臺電腦都必須用一個唯一的位址來標識，該標識位址即 IP 位址（Internet Protocol Address）。IP 位址可分為動態 IP 位址與靜態 IP 位址[47]。網站管理者可通過封鎖向網站發送異常訪問請求之 IP 位址，阻止爬蟲訪問網站。

IP 封鎖是對付爬蟲的常見手段，其破解也極為容易。如【案例八】Facebook 網站為阻止 Power 公司使用爬蟲擷取資料，向其發送停止函，並對其 IP 位址進行封鎖。然而 Power 公司使用代理伺服器，更換新的 IP 位址繼續訪問 Facebook 網站[48]。

4. **破解驗證碼機制訪問網站**

驗證碼（Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA）是全自動區分人類與電腦的圖靈測試（Turing test），當用戶通過測試時，便被認為是真正的人，而不是機器[49]。其原理為：人類有主觀意識，能夠根據要求執行操作，而電腦卻不能[50]。驗證碼之類型多樣，有基於文本、圖像、音訊、影片及謎題的驗證碼[51]。爬蟲可以使用圖像識別驗證碼等方式通過驗證碼測試[52]。如【案例九】李○環使用爬蟲，以自動識別驗證碼等方式，突破系統安全保護措施大量爬取各地車輛管理所公告的車牌資料[53]。

44 李周平，前揭（註 2），頁 40。

45 韋世東，前揭（註 35），頁 4-6。

46 北京市海淀區人民法院 2017 年度京 0108 刑初第 2384 號刑事判決。

47 毛錦庚、鐘肖英，《新編電子商務概論》，中山大學出版社，2018 年 9 月，頁 74。

48 Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1027-1038 (2012).

49 Ved Prakash Singh/ Preet Pal/ Pushpendra Kumar Pateriya, "*Web Security using Transparent Image Captcha (TIC)*", 5 International Journal of Computer Science and Information Technologies, 2014, p. 3089.

50 韋世東，前揭（註 35），頁 9-1。

51 Ved Prakash Singh/Preet Pal/Pushpendra Kumar Pateriya, supra note 49, at 3089.

52 曾劍平，前揭（註 17），頁 210。

53 四川省德昌縣人民法院 2018 年度川 3424 刑初第 169 號刑事判決。

5. **破解加密參數訪問網站**

爬蟲在向網站伺服器發起訪問請求時需編寫必要的參數，有些網站會對參數進行加密，使得爬蟲無法獲得正確參數，因而無法順利訪問網站。常見的加密方式有MD5、AES、RSA等等，但無論何種加密方式都是使用一定的計算規則將一串字元轉化成「不讀取」的另一串字元[54]。故破解加密參數即需對計算規則進行推理分析，以獲得正確之參數，而後將其寫入爬蟲程式中，進行資料的擷取。如【案例十】邵○霜等為提高公司開發的智慧公車APP「車來了」的用戶量及資訊查詢準確度，指使員工張翔○等破解加密算法，編寫爬蟲程式，大量爬取穀米公司開發的智慧公車APP「酷米客」的即時數據，每日約300萬至400萬筆[55]。

㈣破解儲存限制

1. **破解文字加密、混淆措施儲存資料**

文字加密、混淆措施可以有效避免爬蟲獲得網站上重要文字資料，通常網站所採取的加密、混淆方法有CSS偏移、SVG對映、圖片偽裝、字型加密等[56]。其原理都是對文字進行相應的處理，使其既不影響用戶閱讀，又讓爬蟲無法擷取到正確文字。破解此類措施主要是通過探尋其原理，用程式實現對應的演算法或邏輯，或者是藉助字元識別以獲得正確資料[57]。

2. **破解禁止複製、下載措施儲存資料**

網站為保護文字、圖片、影片等資料而禁止使用快速鍵或是滑鼠右鍵進行複製，或者是未設置下載之選項，使得用戶無法儲存資料。爬蟲則可直接通過訪問網站HTML[58]頁面獲得網頁上所顯示的文字、圖片或者影片鏈結，進而將其儲存至電腦。

㈤以異常的次數或頻率訪問網站

因網站伺服器的頻寬及系統資源有限，故對於訪問請求的處理均有一定上限。但網路爬蟲為追求擷取資料的效率以及為保證資料的時效性，會對目標網站的伺服器同時發起大量訪問請求，或以多線程（Multithreading）、高頻率之方式訪問網站，較之一般用戶，其消耗更多系統資源[59]，以致伺服器無法回應與處理其他正常的訪問

---

54 韋世東，前揭（註35），頁10-1-10-27。

55 廣東省深圳市南山區2017年度0305刑初第153號刑事判決。

56 韋世東，前揭（註35），頁6-1-6-47。

57 韋世東，前揭（註35），頁6-58。

58 HTML（Hyper Text Markup Language，超文本標記語言）是用來描述網頁的一種語言，一個網頁對應一個或多個HTML文檔，瀏覽器讀取HTML文檔後將其以一般用戶所見的網頁形式顯示。曾劍平，前揭（註17），頁29。

59 Daniel Kearney, "*Network Effects and the Emerging Doctrine of Cybertrespass*", 23 Yale Law & Policy Review, 2005, pp. 317-318.

請求。如【案例十一】日本愛知縣一男子，在 2010 年 3 月到 4 月間，使用自製爬蟲程式擷取岡崎市立中央圖書館新書清單，其在 14 天內共複製資料 3.3 萬次，致使其他使用者無法閱覽[60]。又如【案例十二】楊○明授權公司員工張○棟開發的「快鴿信貸系統」軟體，於 2018 年 5 月 2 日 10 時至 12 時，以每秒 183 次之頻率對深圳市居住證系統進行訪問，致使深圳市居住證系統伺服器無法正常運行[61]。

二、以網路爬蟲不當取得資料的性質來觀察

㈠擷取秘密

1. 擷取他人個人資料

個人資料係指可以識別特定自然人身分之資料，包括其姓名、地址、電話、電子郵件、職業、病歷等。數以億計的人們在網際網路上從事日常活動，在當前的技術配置下，會產生非常細緻的個人資料[62]。網路爬蟲持續、系統的搜尋能力，極大增加了個人資料被發現與利用的機會[63]，如【案例十三】周○使用自己編寫的爬蟲程式進入學校教務管理系統，擷取學生照片、姓名、身分證號碼等資料 4 萬餘筆[64]。又如【案例十四】Yahoo 奇摩網站的爬蟲曾擷取臺北市政府資訊局負責的「薪資發放管理系統」中 7 萬多名公務員的姓名、銀行薪轉戶帳號等資料[65]。

2. 擷取他人營業秘密

隨著科技的演進，愈來愈多的營業秘密被以電磁紀錄的形式保存於電腦中，營業秘密的資訊化給企業經營帶來便利之餘，也讓企業面臨較高的資訊安全風險[66]。網站上的用戶資訊、商品售價、交易底價，甚至保存於網站上的技術、配方等各類與網站的經營狀況、策略相關之具有經濟價值的資訊，皆有可能被網路爬蟲擷取。

3. 擷取國家機密、國防秘密、軍事機密、公務秘密

國家機密、國防秘密、軍事機密、公務秘密係指與國家安全、國家防衛、軍事作戰、公務相關，應當保密之資訊。雖然這些秘密資訊通常只保存於政府內部網路

---

60 〈ホームページへの大量アクセス事件 岡崎市立中央図書館の弁明に異論相次ぐ〉，〈https://www.j-cast.com/2010/09/02074918.html?p=all〉，最後瀏覽日：2021 年 10 月 7 日。

61 廣東省深圳市南山區人民法院 2019 年度粵 0305 刑初第 193 號刑事判決。

62 Paul M. Schwartz, “Internet Privacy and the State”, 32 Connecticut Law Review, Jan. 1999, p. 815.

63 Zachary Gold /Mark Latonero, supra note 4, at 284-285.

64 湖北省懷化市鶴城區人民法院 2019 年度湘 1202 刑初第 530 號刑事判決。

65 〈北市資訊局：薪資報表暫存檔遭「爬蟲」程式「爬走」〉，蘋果新聞網，2017 年 1 月 10 日，〈https://tw.appledaily.com/life/20170110/CQCDYJCGOUKCJICHGBIKUMP3IM/〉，最後瀏覽日：2021 年 10 月 9 日。

66 廖淑君，〈網路數位時代下之營業秘密保護探討：從美國白宮減少營業秘密竊盜管理策略談起〉，《科技法律透析》，2014 年 4 月，第 26 卷第 4 期，頁 34-35。

中，但使用爬蟲仍然有可能擷取到此類資訊。如【案例十五】愛德華・約瑟・斯諾登（Edward Joseph Snowden）使用網路爬蟲進入美國國家安全局內網，擷取了儲存在其中的約170萬份文件，其中很大一部分涉及美國軍事行動等資訊[67]。

㈡擷取著作

網路爬蟲還常擷取網站上具有著作權之圖片、小說、影片、音樂等以及相應資料之鏈結。【案例十六】劉○遜等使用網路爬蟲，自動抓取他人發布於YouTube或Dailymotion平臺上之影片鏈結，將其置於自己開發之APP內，使不特定公眾可通過該APP連結至YouTube或Dailymotion平臺，觀看此影片[68]。

㈢收集情報資訊

網路上的公開資訊浩如煙海，一般而言，公開於網路上之新聞、照片、言論等等，任何人皆可輕易獲取，並不屬於應當保密之資訊，然而當使用爬蟲收集此類資訊的人為他國之間諜時，此等資訊則可能變成有價值之情報。美國的情報小組就曾依據ISIS成員發布於社群網站上之自拍照，確定其指揮部位址，將其炸毀[69]。從公開的資訊中還能輕易得知各國政治、外交的動態以及影響社會穩定之重要輿情等。

肆、不當使用網路爬蟲之刑事責任分析

網路空間的原始結構決定了其存在天然之自由價值[70]，然網際網路的價值也依賴法律與技術框架的存在，該框架允許用戶在一定範圍內建立一個不受他人干預之隱私與安全區域[71]。故刑法在適用於網路空間時就不得不面臨兩種價值之間的衝突與平衡。對於網路爬蟲，如何確定「罪」與「非罪」之界限及所應當承擔之刑事責任，方可在保障網路之自由、公開性與維護電腦安全、個人隱私等利益之間保持平衡，則成為應著重討論與亟需釐清之問題。

一、概說

針對不當使用爬蟲擷取已類型化保護的資料之行為，境外通常依據資料之性質，適用相應之法規進行處置，較無疑義。例如前述【案例四】美國法院就判定Tomor-

67 Snowden Used Low-Cost Tool to Best N.S.A.,〈https://cn.nytimes.com/world/20140210/c10snowden/dual/〉, last visited Oct. 9, 2021.

68 最高法院110年度台上字第8號刑事判決。

69 〈炫耀食惡果！ISIS天兵聖戰士玩自拍害總部被美軍轟炸〉,〈https://www.setn.com/News.aspx?NewsID=79191〉，最後瀏覽日：2021年10月10日。

70 Lawrence Lessig, "*Code: version 2.0*", Basic Books, Dec. 2006, p. 3.

71 Orin S. Kerr, "*Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statues*", 78 New York University Law Review, Nov. 2003, pp. 1649-1650.

rowNow公司的行為違反美國法典（United States Code）第18章第1030條與第17章第506條，屬未經授權訪問他人網站及侵犯著作權之行為，應承擔相應之刑事責任。【案例十三】中行為人使用爬蟲擷取個人資料的行為，被認定構成侵害公民個人資訊罪。

對於手段不當之各類使用爬蟲行為，境外主要使用電腦犯罪相關條款予以處罰。實務上，美國主要以「電腦詐欺及濫用法案」（Computer Fraud and Abuse Act, CFAA）對網路爬蟲進行規制[72]，通過把不當使用網路爬蟲的行為認定為「未經授權」（accessed a computer without authorization）訪問電腦擷取資料之行為，適用美國法典第18章第1030條之規定，承擔相應的刑事責任或民事責任。該條中「受保護的電腦」最初只是涉及「聯邦利益的電腦」，但在20世紀90年代末，當法院考慮將CFAA用於規制網路爬蟲時，受保護的電腦則擴張為大多數連接網路的電腦[73]。

然而美國法典第18章第1030條中「未經授權」此一規範性要素並未作明確之界定，故存在採寬廣解釋還是嚴格解釋之爭議，進而影響網路爬蟲刑事責任之認定。21世紀初期，美國法院對「授權」採極為寬廣之解釋，諸如違反使用條款、保密協議等網站所顯示出的任何對爬蟲不滿之信號，都會導致使用爬蟲行為被法官認定為「未經授權」[74]，如在前述【案例一】法院即認為違反「使用條款」而使用爬蟲程式擷取資料屬「未經授權」之行為[75]。到後來法院傾向以技術措施、拒絕訪問通知，作為「未經授權」判斷標準[76]，如【案例三】中法院認為違反網站管理者發出的停止函與所採取的技術措施而使用爬蟲才屬「未經授權」之行為[77]。直至現在，為倡導資訊的自由流動與共享，避免造成資訊壟斷損害公共利益，法院認為可以技術措施為判斷標準，同時加入行為是否有益公眾之審查[78]。如在hiQ公司與LinkedIn公司訴訟案

---

72 Kathleen C. Riley, "*Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases*", 29 Fordham Intell. Prop. Media & Ent. L.J., Feb. 2019, p. 266.

73 Andrew Sellars, supra note 2, at 375.

74 Andrew Sellars, supra note 2, at 394.

75 Southwest Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435, 439-440 (2004).

76 Andrew Sellars, supra note 2, at 396-401. 以技術措施或撤銷訪問通知作為「未經授權」的判斷標準也獲得了不少學者的支持。David J. Rosen, "*Limiting Employee Liability under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"*", 27 Berkeley Technology Law Journal, 2012, p. 766; Patricia L. Bellia, "*A Code-Based Approach to Unauthorized Access under the Computer Fraud and Abuse Act*", 84 George Washington Law Review, 2016, pp. 1475-1476; Orin S. Kerr, supra note 71, at 1651; Myra F. Din, supra note 2, at 439-440; Lee Goldman, "*Interpreting the Computer Fraud and Abuse Act*", 13 University of Pittsburgh Journal of Technology Law and Policy, Dec. 2012, p. 34.

77 Craigslist, Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 968-970 (2013).

78 Andrew Sellars, supra note 2, at 396-415.

中，美國聯邦法院認為LinkedIn網站對爬蟲擷取公開資料之限制可能形成不利於公眾利益的資訊壟斷，故認定地區法院之初步禁令是合適的[79]。

儘管上述網路爬蟲案件大多在民事背景下產生，但由於CFAA在規定電腦犯罪的同時也規定了民事上的損害賠償，故一個行為既是民事責任之基礎，又是構成刑事責任的基礎[80]，所以對於「未經授權」的判斷應採同一之標準。雖然目前「未經授權」的判斷標準仍在不停地調整，但從前述不斷變遷的實務觀點仍然可以看出，「未經授權」的判斷標準趨向嚴格解釋，此即意味著以電腦犯罪規制網路爬蟲的入罪門檻不斷提高。

中國大陸近年來在強化資料安全的理念下，對爬蟲的規制展現出日漸嚴厲的趨勢，逐步由民事領域轉向刑事領域[81]。涉及刑事責任時，中國大陸主要以其刑法第285條第2款非法獲取計算機信息系統數據罪與第286條第1款破壞計算機信息系統罪[82]作為處罰依據。在實務上，法院傾向認為網站所採取的任何技術措施都體現了網站管理者對資料的「強」保護意願，對其迴避或突破都屬於「未經授權」訪問，該觀點獲得大多數學者的支持[83]。如前述【案例七】行為人對於UA驗證與IP封鎖的破解以及【案例九】行為人對驗證碼機制的破解都被認為是強行突破電腦安全防護體系之入侵行為，從而構成非法獲取計算機信息系統數據罪。

境內雖然也有網路爬蟲相關之案件，但並未針對使用網路爬蟲之行為本身予以評價，而係以爬蟲所擷取資料之後續使用對法益造成之侵害來確定其刑事責任。如前述【案例十六】行為人使用爬蟲擷取電影鏈結後置於自己開發的APP內，被認為是幫助侵害他人著作權之行為。

誠然，以使用爬蟲擷取資料之後續行為，來區分行為之合法與否及認定其所承擔的責任自然可行，但若僅把網路爬蟲之使用當作完全中性之行為，而將目光聚焦

---

79 hiQ Labs, Inc. v. LinkedIn Corp., 938 F. 3d 985, 1004-1005 (2019).

80 Patricia L. Bellia, supra note 76, at 1472.

81 楊志瓊，〈數據時代網絡爬蟲的刑法規制〉，《比較法研究》，2020年6月，第4期，頁186。

82 「中華人民共和國刑法」第285條第2款「違反國家規定，侵入前款規定以外的計算機信息系統或者採用其他技術手段，獲取該計算機信息系統中存儲、處理或者傳輸的數據，或者對該計算機信息系統實施非法控制，情節嚴重的，處三年以下有期徒刑或者拘役，並處或單處罰金；情節特別嚴重的，處三年以上七年以下有期徒刑，並處罰金。」；第286條第1款「違反國家規定，對計算機信息系統功能進行刪除、修改、增加、干擾，造成計算機信息系統不能正常運行，後果嚴重的，處五年以下有期徒刑或者拘役；後果特別嚴重的，處五年以上有期徒刑。」

83 楊志瓊，前揭（註81），頁195-196；陳軍標、楊蘭，〈「網絡爬蟲」技術的法律規制〉，《上海法學研究》集刊，2020年8月，第12卷，頁14；游濤、計莉卉，〈使用網絡爬蟲獲取數據行為的刑事責任認定：以「晟品公司」非法獲取計算機信息系統數據罪為視角〉，《法律適用》，2019年5月，第10期，頁6-7。

於所取得資料之非法使用，實難以令法益得到有效的保護，也無法對使用網路爬蟲行為作出適當的評價。因此，有必要審視不當使用爬蟲擷取資料行為本身可能對法益造成的侵害及違法性，只是基於刑法謙抑之思想，在刑法的解釋及適用上需格外謹慎，是以，究竟不當使用網路爬蟲的行為是否需承擔刑事責任以及承擔何種刑事責任，尚需進行詳細之論證。

二、手段不當的可能刑事責任

㈠入侵電腦罪

1. 入侵電腦罪之成立要件

刑法第 358 條入侵電腦罪之行為乃入侵他人電腦或相關設備，入侵的方法包括輸入他人帳號密碼、破解使用電腦之保護措施、利用電腦系統之漏洞。另有學者主張，從本罪保護的法益考量，任何危害電腦系統安全性之入侵行為，皆應為本罪處罰的對象[84]。但就立法理由所述，該條係針對情節重大之無故入侵行為[85]，應是為避免僅具輕微法益侵害性之行為入罪。是以，基於罪刑法定原則，入侵電腦之方式只能限於此三種類型。

其次，對於破解電腦保護措施有認以物理力或非物理力為之皆可[86]，亦有認為行為攻擊之對象係電腦中的登入控制機制或保護機制（一種電腦程式）[87]，故對電腦保護措施之破解不是物理力可以實現。

本文認為，據立法理由所述，「系統遭惡意入侵後，系統管理者需耗費大量之時間人力檢查，始能確保電腦系統之安全性」[88]，而以物理力破壞外在硬體保護措施並不需要大費周章即可發現，也不會直接導致電腦系統安全性受損，故以上三種方式應是專門針對「電腦系統安全軟體保護措施」所為。而此種保護措施，須是為防止入侵電腦而設，即該措施可阻止外人入侵或使其入侵有相當困難[89]。從立法理由「本條之入侵行為是以盜用他人帳號密碼或破解相類似保護措施或利用電腦系統漏

84 柯耀程，〈刑法新增「電腦網路犯罪規範」立法評論〉，《月旦法學教室》，2003 年 9 月，第 11 期，頁 127；蔡榮耕，〈Matrix 駭客任務：刑法第 358 條入侵電腦罪〉，《科技法學評論》，2008 年 4 月，第 5 卷第 1 期，頁 126-127。

85 立法院公報處，《立法院公報》，2003 年 5 月 28 日，第 92 卷第 29 期，頁 140。

86 甘添貴，前揭（註 30），頁 425。

87 王皇玉，〈選課風波〉，《月旦法學教室》，2010 年 6 月，第 93 期，頁 18；李茂生，〈刑法新修妨害電腦使用罪章芻議（中）〉，《臺灣本土法學雜誌》，2004 年 2 月，第 55 期，頁 246-247。

88 立法院公報處，《立法院公報》，2003 年 5 月 28 日，第 92 卷第 29 期，頁 139-140。

89 許澤天，《刑法分則（下）：人格與公共法益篇》，新學林出版股份有限公司，2020 年 7 月，2 版，頁 306。

洞的方式為之」[90]亦可知悉，所破解的電腦保護措施對電腦系統起到的保護效果需與帳號密碼相差無幾，而利用電腦系統漏洞所繞過的保護措施亦是如此。

本罪在主觀上要求行為人對於客觀構成要件的實現具有故意。此外，本罪同侵害電磁紀錄罪均強調需滿足「無故」之要件。「無故」在實務與學理上多認為係指無正當權源或正當事由，即行為人不具任何阻卻違法事由，若有正當理由或經法律授權，則不具違法性[91]。

2. **非法使用訪問權限**

非法使用訪問權限之形式有兩種，其一，對於使用他人帳號密碼之行為，既是將騙取、竊取等方式而知悉之帳號密碼寫入爬蟲程式中以訪問網站，當然符合「輸入他人帳號密碼」之方式。另因Cookie中所包含的資訊較多，若其含有用戶帳號密碼資訊，而將其寫入爬蟲程式，自與前述情形無異。倘若Cookie只是用來記錄用戶瀏覽習慣、電腦設定等資訊，則寫入Cookie不屬於本罪所指之「輸入帳號密碼」。其二，對於超越權限使用本人帳號密碼之行為，因所使用者乃本人之帳號密碼，自不符合「他人」之要件。且行為人所使用之帳號密碼，具有訪問權限，只是儲存資料之權限受限，所以並無需以「破解使用電腦之保護措施」與「利用電腦系統漏洞」之方式訪問網站，故不成立入侵電腦罪。

3. **破解訪問限制**

使用爬蟲破解訪問限制進而訪問網站是否成立入侵電腦罪，最重要者乃判斷訪問限制措施是否屬本條之「電腦系統安全軟體保護措施」。顯而易見，各項訪問限制措施均為系統內含之軟體保護措施，至於其是否屬於電腦系統安全保護措施，尚需視其是否為防止侵入而設及保護系統安全之效果是否與帳號密碼相類似。

第一，UA驗證：依爬蟲運作之原理，編寫合適的UA值讓網站難以辨別來訪者之身分，此乃爬蟲最基本之技術要求。網站管理者也必然知曉僅靠UA驗證並非阻止爬蟲訪問網站之有效措施。所以，UA驗證實際上所起到的保護效果相當有限，根本無法與帳號密碼保護措施相提並論。

第二，IP封鎖：因IP位址通常為動態分配，經常變化，只要重啟數據機或更換上網地點，IP位址都會改變[92]，常用方式乃使用代理伺服器掩蓋發送請求的真正IP位址[93]。但無論哪種方式，一旦爬蟲的IP位址改變，網站管理者即不能阻止爬蟲之

90　立法院公報處，《立法院公報》，2003年5月28日，第92卷29期，頁140。

91　臺灣臺中地方法院108年度易字第3898號刑事判決；最高法院107年度台上字第2197號刑事判決；最高法院108年台上字第1026號刑事判決；林山田，《刑法各罪論（上）（修訂五版）》，北京大學出版社，2012年1月，頁390；甘添貴，前揭（註30），頁424。

92　How to change you IP address,〈https://whatismyipaddress.com/change-ip〉, last visited Oct. 15, 2021.

93　Daniel Kearney, supra note 59, at 318.

訪問。換言之，IP 封鎖措施對電腦系統的保護是以排除來自特定 IP 位址的訪問來實現，而難以實際禁止使用該 IP 位址的人訪問，此與直接排除未得授權之人對電腦訪問之帳號密碼保護措施在效果上不可同日而語。

第三，驗證碼機制：驗證碼機制與帳號密碼保護措施不同，網站會主動告知所有人應輸入之內容，其邀請所有人進入[94]。故設置驗證碼機制更重要之目的在於防止電腦程式自動、大批地訪問網站[95]，以減緩訪問速度，減輕伺服器負擔。因此，不能將其視為防止入侵電腦所設之保護措施，而是維護電腦正常運作之措施。

第四，參數加密：參數加密確能對爬蟲訪問網站造成一定程度之困難，只是是否符合「相當困難」之要求，則與網站管理者所採用的加密方式相關。如此則會造成同一網站，當採用簡單的參數加密方式時，使用爬蟲對其訪問不構成犯罪；當採用複雜的參數加密方式時，對其訪問則可成立犯罪，實難謂之合理，故不宜將參數加密當作為防止入侵而設之電腦系統安全保護措施。

第五，登入機制：登入機制通過排除未登入者之訪問授權，以保護電腦系統之安全。然登入機制或是為方便管理、記錄用戶瀏覽習慣、落實實名驗證之目的而設[96]，似難謂其係防止入侵而設之措施。但實際上，此僅係設置登入機制之次要目的，亦可通過其他方式實現，其主要目的仍係排除未經授權者對網站之訪問，且該措施確實能起到保護電腦系統安全之效果。因此，毫無疑問，登入機制屬於「電腦系統安全保護措施」。

綜上，由於驗證碼機制、參數加密措施皆不屬於為防止侵入而設置之保護措施，UA 驗證、IP 封鎖對電腦系統安全的保護效果與帳號密碼措施相去甚遠，惟登入機制才屬本條之「電腦系統安全保護措施」。是故，當行為人使用爬蟲以他人之帳號密碼或存有帳號密碼資訊的 Cookie 訪問網站，屬於「輸入他人帳號密碼」而入侵電腦之行為；若是以使網站之登入機制失效的方式而訪問網站，則屬於「破解使用電腦之保護措施」而入侵電腦之行為；若是利用電腦系統存在的漏洞而繞過網站的登入機制訪問網站，則屬於「利用電腦系統之漏洞」而入侵電腦之行為。以上行為在不具阻卻事由時，可成立入侵電腦罪。

㈡侵害電磁紀錄罪

1. 侵害電磁紀錄罪之成立要件

刑法第 359 條之侵害電磁紀錄罪的客體為「他人電腦或其相關設備之電磁紀

94 Orin S. Kerr, supra note 39, at 1169.

95 付強、李濤，前揭（註 32），頁 20-21。

96 薛智仁，〈無故取得電磁紀錄罪之解釋及立法〉，《政大法學評論》，2014 年 3 月，第 136 期，頁 83；劉艷紅、楊志瓊，〈網絡爬蟲的入罪標準與路徑研究〉，《人民檢察》，2020 年 8 月，第 15 期，頁 29。

錄」，電磁紀錄是提供電腦處理之用的數位資料，至於其內容是否涉密，可否視為準文書，皆在所不問[97]。然有學者指出應將「電磁紀錄」限定為已設定儲存權限或加密之敏感資訊[98]。但本罪既設結果要件，應是以此來限定電磁紀錄內容及形式，既如此，在對行為客體的解釋上自無需附加法條所無之其他限制[99]。本罪的行為乃「取得、刪除或變更」，且行為必須是「無故」始具違法性。本罪之結果乃「致生損害於公眾或他人」，只因本罪所保護的法益莫衷一是，故對此具體損害之內容也存在不同的解釋[100]。

本文認為，就本罪設計為告訴乃論之罪而言，應是傾向於個人法益之保護。若認為本罪保護的法益為社會法益，則無法適用被害人同意阻卻違法。因被害人同意之內容必須是其能處分之個人法益，對國家、社會法益，抑或同時含有個人法益之情況，均無適用被害人同意之可能[101]。事實上對「無故」之解釋，即包括未得被害人同意，故本罪保護的法益應認定為個人法益更為妥當。又電腦使用安全在本罪中主要是電腦資料的安全，而電腦資料之非法使用行為對資料主體所享有之處分權造成了極大危害，實難以財產法益所能概括，故以資料私密性、完整性與可使用性等新型法益及財產、名譽、秘密等傳統法益作為本罪之保護法益較為合適，而具體損害即為個人財產、名譽、秘密等遭受實際的損害。

本罪之主觀構成要件為故意。行為人使用爬蟲擷取資料，應對爬蟲程式之運作方式有所認識，是以，行為人是否認識到自己係擅自擷取他人電腦上之資料並決意為之，在認定上並無疑義。

2. **違反網站管理規定**

與物理世界不同，網際網路的開放屬性，使得訪問網站即默認為經過授權之行

97　林山田，前揭（註91），頁392。

98　蔡蕙芳，前揭（註28），頁160-162。

99　薛智仁，前揭（註96），頁90。

100　在學理上對本罪的法益有社會法益、個人法益、社會法益兼及個人法益之爭議，相應就具體損害的內容則有社群成員對電腦安全系統的信賴程度減少，財產、名譽、秘密等受損，被害人全部財產的客觀市場價值減少等觀點。許恆達，〈資訊安全的社會信賴與刑法第三五九條的保護法益：評士林地方法院九十九年度訴字第一二二號判決〉，《月旦法學雜誌》，2011年11月，第198期，頁245-246；李茂生，前揭（註87），頁254-256；甘添貴，〈虛擬遊戲與盜取寶物〉，《臺灣本土法學雜誌》，2003年9月，第50期，頁184-185；蔡蕙芳，前揭（註28），頁156-168；薛智仁，前揭（註96），頁86-96。實務上則普遍認可本罪保護的法益為社會法益及個人法益，損害之結果則不限於經濟上損害，但需對公眾與他人產生具體的侵害，另也有認為只需足以導致電腦使用人發生損害即可。最高法院108年度台上字第4114號刑事判決；最高法院101年度台上字第5295號刑事判決；臺灣臺北地方法院106年度訴字第567號刑事判決；臺灣高等法院110年度上訴字第271號刑事判決。

101　陳子平，《刑法總論》，元照出版有限公司，2017年9月，4版，頁299。

為[102]。換言之，一般情況下，網路爬蟲訪問網站擷取資料，為默認得到他人同意之行為，自不該當「無故取得」之要件，不具違法性。所以，若要說明爬蟲擷取資料為「未經授權」之行為，必先判斷網站管理者是否已作出足夠明確的不同意爬蟲訪問之意思表示，並將該意思準確傳達給爬蟲使用者。

就網站所設條款來看，首先，網站管理者並未以鼓勵用戶閱讀的方式清楚地展示條款內容[103]；其次，無論以何種方式展示條款，通常皆不以詳細閱讀作為訪問網站、擷取資料之必備前提；最後，這些條款是網站管理者基於自身利益所作之單方面意思表示，其可以隨時更改條款，而不提供更改通知。故此類具有不確定性的且未予以明確告知的條款難以充分表示網站管理者不同意爬蟲訪問並擷取資料之意思。

爬蟲協議亦是如此。爬蟲協議雖然稱為「協議」，但其實與民法上的協議有很大的區別，其與權利義務無關，只是一種被用於電腦網路通信中的規則[104]，有效性完全依賴爬蟲使用者對於爬蟲協議的尊重[105]。如此網站管理者就很難依靠爬蟲協議而將此種禁止或許可爬蟲訪問之意願有效傳達給爬蟲的使用者。況且，爬蟲協議之內容常不具平等性，背後隱藏著大型網際網路企業壟斷資料之目的[106]。如圖 2、圖 3、圖 4 所示，網站管理者利用爬蟲協議對爬蟲設置了不同的權限。此舉為資料的流動創造了壁壘，與爬蟲協議引導爬蟲更有效抓取有用的資料，從而更好的促進資訊共享之初衷相違背，其本身之合理性受到質疑[107]。

拒絕訪問通知，雖符合明確傳達意思之要求，然而其受質疑之處在於，此舉係以網站管理者的單方意思來劃定犯罪行為範圍、決定刑罰權的發動與否[108]。實並非所有的私領域皆值得或必須以刑法加以保護，尤其在本身具有開放、共享特性之網路空間，行為人將其私領域置於一個公開的或是不設防的環境中，即表示此處的隱私利益對行為人來說無關緊要[109]。因此，除了網站管理者明確的意思表示及有效的傳達外，還需網站管理者設置能夠對電磁紀錄之取得造成實質性阻礙之保護措施。

顯然網站的管理規定，只是單純以單方意思表示提醒訪問者注意訪問權限，並

102 Orin S. Kerr, supra note 39, at 1161-1162.

103 Kathleen C. Riley, supra note 72, at 302-303.

104 寧立志、王德夫，〈「爬蟲協議」的定性及其競爭法分析〉，《江西社會科學》，2016 年 1 月，第 1 期，頁 163。

105 Daniel Kearney, supra note 59, at 317-318.

106 石經海、蘇桑妮，〈爬取公開數據行為的刑法規制誤區與匡正：從全國首例「爬蟲」入刑案切入〉，《北京理工大學學報（社會科學版）》，2021 年 1 月，第 23 卷第 4 期，頁 157。

107 北京市高級人民法院 2017 京民終 487 號判決。

108 Orin S. Kerr, supra note 71, at 1651; Facebook, Inc. v. CONNECTU LLC, 489 F. Supp. 2d 1087, 1091 (2007)；蔡榮耕，前揭（註 84），130 頁。

109 徐育安，〈資訊風險與刑事立法〉，《臺北大學法學論叢》，2014 年 9 月，第 91 期，頁 145。

不能對爬蟲取得資料造成實質性的阻礙，更何況網站設置的條款及爬蟲協議尚且無法清楚傳達網站管理者的意思，是以，違反網站管理規定，並不該當於「無故取得」之要件，不成立侵害電磁紀錄罪。

```
User-Agent:Googlebot
User-Agent:Bingbot
Crawl-delay:0.1
Disallow: /cart/
Disallow: /checkout/
Disallow: /buyer/
Disallow: /user/
Disallow: /me/
Disallow: /order/
Disallow: /daily_discover/
Disallow: /mall/just-for-you/
Disallow: /mall/*-cat.
Disallow: /from_same_shop/
Disallow: /you_may_also_like/
Disallow: *-i.*/similar?from=flash_sale
Disallow: /find_similar_products/
Disallow: /top_products
Disallow: /search*searchPrefill
Disallow: /index.html

User-Agent:*
Crawl-delay:1
Disallow: /cart/
Disallow: /checkout/
Disallow: /buyer/
Disallow: /user/
Disallow: /me/
Disallow: /order/
Disallow: /daily_discover/
Disallow: /mall/just-for-you/
Disallow: /mall/*-cat.
Disallow: /from_same_shop/
Disallow: /you_may_also_like/
Disallow: *-i.*/similar
Disallow: /find_similar_products/
Disallow: /top_products
Disallow: /search*searchPrefill
Disallow: /index.html
```

圖 3　蝦皮購物網站爬蟲協議

資料來源：https://shopee.tw/robots.txt（截取日期：2021.11.21）

```
# robots.txt file for YouTube
# Created in the distant future (the year 2000) after
# the robotic uprising of the mid 90's which wiped out all humans.

User-agent: Mediapartners-Google*
Disallow:

User-agent: *
Disallow: /channel/*/community
Disallow: /comment
Disallow: /get_video
Disallow: /get_video_info
Disallow: /get_midroll_info
Disallow: /live_chat
Disallow: /login
Disallow: /results
Disallow: /signup
Disallow: /t/terms
Disallow: /timedtext_video
Disallow: /user/*/community
Disallow: /verify_age
Disallow: /watch_ajax
Disallow: /watch_fragments_ajax
Disallow: /watch_popup
Disallow: /watch_queue_ajax

Sitemap: https://www.youtube.com/sitemaps/sitemap.xml
Sitemap: https://www.youtube.com/product/sitemap.xml
```

圖 4　YouTube 網站爬蟲協議

資料來源：https://www.youtube.com/robots.txt（截取日期：2021.11.21）

3. **非法使用訪問權限**

網站所設置登入機制對一般人而言並不陌生，當需用戶進行登入時，即可知悉網站管理者排除不具有登入帳號密碼者的訪問授權之意思。且如前文所述，網站的登入機制為「使用電腦之保護措施」，其為資料之取得造成實質性阻礙。故以他人之帳號密碼訪問網站擷取資料，屬於未經授權之行為，該當「無故取得」之要件。而以本人之帳號密碼訪問網站，該訪問網站的行為雖獲得授權，但若其超越網站所賦予該帳號主體儲存資料之權限而擷取資料，仍屬未得同意之行為，同樣該當「無故取得」之要件。上述行為若造成個人秘密、財產、名譽等具體的損害即可成立侵害電磁紀錄罪。

4. **破解訪問限制**

網站所設各項訪問限制措施均能對爬蟲擷取資料造成一定程度之阻礙。但並非所有的措施均有效、明確表示及傳達網站管理者不同意爬蟲擷取資料之意思。網站管理者對 UA 值的限制一般以爬蟲協議來體現，但如前所述，爬蟲協議不具有強制力，並不足以傳達網站管理者之意思，故依賴於爬蟲協議之 UA 驗證同樣難以有效傳達網站管理者拒絕爬蟲訪問之意思。

對於 IP 封鎖措施，布雷耶（Charles R. Breyer）法官認為該措施傳達了一個明確的信號，即使用該 IP 位址者不再被授權訪問該網站[110]。然而經常變動的 IP 位址與使用者之間的難以建立穩定之聯繫，如前所述，該措施針對的只是特定之 IP 位址，而非實際使用者。故而，IP 封鎖只能表示網站管理者對該 IP 位址訪問授權的排除[111]，很難直接推論出不同意該 IP 位址的使用者訪問之意思。驗證碼機制雖然表面上看起來是為區分爬蟲與正常用戶而設，但如前述，實際上該機制更重要之目的在於降低訪問速度，以保障伺服器正常運作。故驗證碼機制亦不能清晰明確的表明網站管理者禁止爬蟲訪問的意思。而參數加密措施也只是加大爬蟲擷取資料的難度，從而避免大量爬蟲訪問網站而影響伺服器之運作，同樣無法準確傳達網站管理者拒絕爬蟲訪問之意思。

只有登入機制作為電腦系統安全保護措施，清楚明確傳達網站管理者不同意未經授權者之訪問。因此，以破解登入機制的方式使用爬蟲擷取資料，即為未得授權之「無故取得」行為，若對他人之秘密、財產、名譽造成實際損害，且無其他阻卻事由時，則可成立侵害電磁紀錄罪。

5. **破解儲存限制**

---

[110] Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178 ,1186 (2013).

[111] Orin S. Kerr, supra note 39, at 1168-1169.

儲存限制措施是專門針對資料的儲存而設，其中文字加密、混淆措施同前述參數加密措施類似，都是通過加密方式，使得爬蟲無法順利擷取資料。同樣，該措施也只是加大爬蟲擷取資料的難度，避免網站資料被輕易爬取，但無法確切知悉網站管理者是否具有不同意爬蟲擷取資料之意思。而禁止複製、下載措施，則主要是對正常用戶儲存資料的行為作出限制，該措施對於從網站 HTML 頁面上獲得資料的爬蟲而言並無實際的限制之效果。所以，該措施一樣難以明確表示網站管理者之意思。

㈢干擾電腦罪

1. 干擾電腦罪之成立要件

刑法第 360 條干擾電腦罪之行為係以電腦程式或其他電磁方式干擾他人電腦或其相關設備。干擾電腦的行為需符合「致生損害於公眾或他人」之結果要件，始能成罪。本罪之主觀構成要件為故意。此外，本罪之成立同樣需滿足「無故」之要件。

本罪中「干擾」一詞具有模糊性，意義並不明確[112]。學理及實務上則多認為需實際上造成電腦或其相關設備暫時性的使用不能[113]，以及降低其效能，方可謂之「干擾」[114]。然本文認為，根據法益保護原則，立法者在設計犯罪構成要件時，該行為事實需對法益至少造成危險才可為之[115]。單從「干擾」這一用語不易確定本罪的行為之程度，但從本罪透過對法益造成實害之結果限縮處罰範圍可知，構成要件行為之「干擾」的解釋應非局限於對電腦的運作造成實際影響之行為。換言之，凡事實上造成與有可能造成電腦或相關設備使用不能或效能降低之行為，皆為本罪所指之「干擾」行為。如寄發病毒郵件，妨害電腦運作的危險性較高，即屬於本罪之「干擾」行為[116]。

2. 以異常次數或頻率訪問網站之「干擾」的認定

使用網路爬蟲以異常的次數或頻率訪問網站，從而導致網路及系統資源消耗殆盡，屬於前述「致使電腦使用不能」之「干擾」行為無疑。只是如何判斷使用爬蟲之行為屬降低電腦系統效能，抑或是可能使電腦使用不能或降低其效能之「干擾」

112 李茂生，〈刑法新修妨害電腦使用罪章芻議（下）〉，《臺灣本土法學雜誌》，2004 年 3 月，第 56 期，頁 208-209；廖宗聖、鄭心翰，〈從網路犯罪公約談我國妨害電腦使用罪章的修訂〉，《科技法學評論》，2010 年 12 月，第 7 卷第 2 期，頁 81-82；徐育安，前揭（註 109），頁 147-148。

113 柯耀程，前揭（註 84），頁 125；林山田，前揭（註 91），394 頁。

114 鄭逸哲，〈吹口哨壯膽：評刑法第三十六章增訂〉，《月旦法學雜誌》，2003 年 11 月，第 102 期，頁 111；蔡蕙芳，〈妨害電腦使用罪章：第一講：保護法益與規範功能〉，《月旦法學教室》，2013 年 3 月，第 126 期，頁 68；甘添貴，前揭（註 30），頁 430；盧映潔，《刑法分則新論》，新學林出版股份有限公司，2021 年 8 月，17 版，頁 836；臺灣高等法院 95 年度上易字第 255 號刑事判決；臺灣花蓮地方法院 96 年度簡上字第 39 號刑事判決。

115 靳宗立，前揭（註 29），頁 118。

116 李茂生，前揭（註 112），頁 208。

行為，則不無疑問。

美國在實務中曾把導致網站的伺服器負載達到總負載 1.11%-1.53% 的爬蟲行為認定為對伺服器存在干擾[117]。中國大陸「數據安全管理辦法（徵求意見稿）」第 16 條規定，超過網站日均流量三分之一，即為嚴重影響網站運行之行為。二者認為占用系統資源達一定程度即可推定該行為屬於影響電腦系統正常運作之「干擾」行為。

有學者主張可以從網站伺服器的處理能力及平均每日流量，爬蟲是否同等對待每個網站，以及爬蟲之目的進行綜合考量，以確定爬蟲是否對系統造成干擾[118]。然而，網站伺服器的處理能力並不相同，何以要求爬蟲同等對待不同的伺服器？且不同時間段，網站訪問人數存在極大的差異，伺服器所承受的壓力亦不一致，實難以平均每日流量作為衡量基準。

因此，本文認為，既然本罪中「干擾」包括實際和可能影響電腦系統的正常運作之情形，那麼以系統資源的占用比例來推定行為對電腦系統之影響確有其可行性，只是不宜以固定數值作為衡量標準。可以考慮以爬蟲訪問網站時間段的日常流量並結合網站伺服器的正常處理能力作為衡量基準，來綜合判斷使用爬蟲的行為是否確實有可能導致抑或是已經致使伺服器無法運作、回應速度減緩、處理能力減弱等情況，以此作為「干擾」之認定標準。

3. **以異常次數或頻率訪問網站之「故意」的判斷**

使用爬蟲擷取資料不同於分散式阻斷攻擊（DDOS），後者以攻擊電腦為目的，其對自己行為會干擾電腦系統正常運作及造成損害具明確之認知且有意使其發生；而前者之目的僅在於擷取資料，只是其運作方式有可能造成網路及系統資源的損耗。是以，行為人使用爬蟲擷取資料在主觀上最多僅認識到行為有干擾電腦正常運作之可能，而非具有確定其發生之認識。

間接故意與有認識的過失在認識要素上並無差別，皆需認識到行為有導致犯罪實現之可能，只是前者具有實現該認識內容之意思，後者則欠缺該意思[119]。行為人是否具有實施干擾電腦系統，損害公眾與他人利益的行為之決意可以從以下兩個要素進行分析：其一，爬蟲程式所設定的訪問次數及頻率：若是爬蟲程式設定的訪問次數及頻率異於常態，則應肯定行為人具有實現構成要件犯罪事實之意思，如【案例十二】爬蟲以 1 秒 183 次的頻率訪問網站，顯然具有影響電腦運作之故意。其二，行為人是否持續性對網路爬蟲的運行狀態進行監控、修正[120]：若在使用爬蟲過程中，

---

117 eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1064-1072 (2000).

118 廖先志、陳鐘誠，〈論搜尋引擎以程式在網路上自動抓取資料時可能面臨之法律問題及其解決之道〉，《圖書館學與資訊科學》，2007 年 4 月，第 33 卷第 1 期，頁 9。

119 陳子平，前揭（註 101），頁 188-192。

行為人能主動、及時修正爬蟲不適當之運行狀態，則不應認為其具實施干擾電腦系統行為之決意。

綜上，使用網路爬蟲故意以異常的次數或頻率訪問網站，從而致使或有可能致使電腦使用不能或使其效能降低，且對公眾或他人造成具體損害，在無其他阻卻事由時，則可成立干擾電腦罪。

三、不當取得資料的可能刑事責任

㈠擷取秘密

1. 個人資料

在現代電腦技術之條件下，個人資料的發掘與儲存變得非常便捷，大量個人資料基於商業使用或是建構個人資料庫之目的而被秘密蒐集[121]，僅保護隱私領域尚不足以確保人格的自由發展，對非隱秘的、公開的數據儲存，亦可導致對公民自由的威脅[122]。是以，對個人資料的保護便以「資訊的自主決定」為出發點[123]。

個人資料保護法第 41 條規定違法蒐集處理利用個人資料罪，本罪之行為係違反所列舉之規定蒐集、處理、利用個人資料；本罪為具體危險犯，行為人所為之行為需足生損害於他人；本罪主觀要件為故意，且需為自己或第三人不法之利益或損害他人之利益的意圖。其中「意圖」要素所指之利益，素有限縮於財產上的利益與及於所有利益之爭。後經最高法院刑事大法庭作出裁定，統一見解，參酌舊法之「意圖營利」要件及其他法規用語，「意圖為自己或第三人不法之利益」應限於財產上之利益，而「意圖損害他人之利益」則考量立法目的，應及於所有利益[124]。

另基於對個人決定權之尊重與對公共利益之維護，容許特定條件下合理利用個人資料[125]。就使用爬蟲擷取（個人資料保護法所稱蒐集、處理）資料之合理利用個人資料情形中，最為常見及所需進一步說明者為使用爬蟲擷取「當事人已自行公開」及「取自一般可得之來源」之個人資料。自行公開之個人資料係當事人對不特定人

120 付強、李濤，前揭（註 32），頁 22。

121 Alexander Tsesis, "*The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*", 49 Wake Forest L. Rev., 2014, p. 441.

122 Ulrich Sieber 著，周遵友、江溯等譯，《全球風險社會與信息社會中的刑法：二十一世紀刑法模式的轉換》（Criminal Law in the Global Risk and Information Society: The paradigm shifts of the 21st century），中國法制出版社，2012 年 1 月，頁 294。

123 劉靜怡，〈不算進步的立法：「個人資料保護法」初步評析〉，《月旦法學雜誌》，2010 年 8 月，第 183 期，頁 151；范姜真媺，〈個人資料自主權之保護與個人資料之合理利用〉，《法學叢刊》，2012 年 1 月，第 225 期，頁 73-76。

124 最高法院刑事大法庭 109 年度台上大字第 1869 號裁定。

125 范姜真媺，前揭（註 123），頁 77-78。

或特定多數人揭露之資料[126]。故當資料主體自行將個人資料置於網站上，無論該網站是任何人皆可訪問的網站抑或是需以特定帳號密碼才可訪問的網站，只要其資料可為多數人所見，此即意味著該資料對當事人而言無不受他人無端侵擾與自主控制個人資料的「隱私之合理期待」[127]，因而對該資料的擷取則屬合理利用之情形，不成立違法蒐集處理利用個人資料罪。

若非資料主體自行公開之資料，而是來自於「一般可得之來源」，即透過網際網路、政府公報等及其他一般人可得知悉或接觸而取得個人資料之管道[128]，如普通的個人資料被置於任何人皆可訪問之網站上，則對該資料的擷取通常也不成立本罪；但若當事人已明確禁止處理該資料，或該資料為病歷、基因等特殊個人資料，則對該資料的擷取不屬於合理利用之情形。若是個人資料被置於需特定帳號密碼才可訪問的網站，則只限於特定人可知悉而取得資料之管道，故擷取此類資料也不屬於合理利用之情形。

因此，當使用爬蟲擷取個人資料，不符合合理利用之情形，且蒐集、處理個人資料之行為有造成他人損害的具體危險，行為人亦具有違反個人資料保護法規定而足生損害他人之故意，同時該行為是為自己或第三人財產上之利益或是為了損害他人之利益而為之，則可成立違法蒐集處理利用個人資料罪。

2. **營業秘密**

營業秘密與企業的經營生存密不可分，是企業競爭力的保證，對營業秘密的保護既是對個人財產之保護，也是對社會競爭秩序之維持。針對侵害營業秘密的行為，營業秘密法第 13 條之 1 規定了相應的刑事責任。

首先，侵害營業秘密罪之客體為營業秘密，所謂營業秘密除包括技術性之資訊，如與特定產業研發或創新技術有關之機密，尚包括商業性資訊，如企業之客戶名單、經銷據點、商品售價等與經營相關之資訊[129]，且需符合秘密性、具有經濟價值、採取合理保密措施之三個要件。秘密性係指除一般公眾所不知者外，相關專業領域中之人亦不知悉[130]。經濟價值，指持有該營業秘密之企業較未持有該營業秘密之競爭者，具有競爭優勢或利基[131]，除金錢收入之實際經濟價值外，尚包括市占率、研發

126 個人資料保護法施行細則第 13 條第 1 項。

127 邱忠義，〈談個人資料保護法之間接識別〉，《月旦裁判時報》，2014 年 12 月，第 30 期，頁 96-97；張陳弘，〈個人資料之認定：個人資料保護法適用之啟動閥〉，《法令月刊》，2016 年 5 月，第 67 卷第 5 期，頁 92。

128 個人資料保護法施行細則第 28 條。

129 最高法院 110 年度台上字第 3903 號刑事判決。

130 最高法院 110 年度台上字第 3193 號刑事判決；最高法院 107 年度台上字第 2950 號刑事判決。

131 林洲富，〈營業秘密之理論與實務交錯〉，《中華法學》，2017 年 11 月，第 17 期，頁 235。

能力、業界領先時間等經濟利益或競爭優勢之潛在經濟價值[132]。合理保密措施則係指營業秘密所有人按其人力、財力，依其資訊性質，以社會通常所可能之方法或技術，使他人無法輕易地取得、使用或洩露該秘密資訊[133]。

其次，本罪的行為有四種類型，以擅自重製的方式而取得營業秘密、未經授權或逾越授權範圍而重製所知悉或持有之營業秘密者屬之。對於本罪中的「重製」之定義，依法規範一致性的解釋，著作權法第3條關於「重製」之定義亦可適用於本罪[134]。再者，本罪的主觀要件為故意，且需具有為自己或第三人不法之利益，或損害營業秘密所有人之利益的意圖。

至於使用爬蟲擷取產業研發或創新技術與商業性資訊是否成立侵害營業秘密罪，需先判斷該資訊是否屬於營業秘密。資訊的經濟價值認定較為容易，無需贅言，而秘密性與保密措施二者互相連動，則需深入探討。因網路空間已成為大眾可輕易進入之公共空間，若無採取保密措施，一般不特定人皆能輕易獲得置於網路上之資訊，該資訊自無秘密性可言[135]。只是即使採取保密措施，亦非皆屬「合理」，需達到使不特定多數人無法輕易取得資訊之效果方可謂合理之保密措施。

網站管理人所設置的管理規定無實際阻礙他人取得資訊之效果。訪問限制措施與儲存限制措施，皆對爬蟲取得資料造成或多或少的阻礙，只是訪問限制中的UA驗證、驗證碼機制、參數加密措施，以及儲存限制措施中的文字加密、混淆措施係專門針對爬蟲所設之措施，而IP封鎖則是以阻止來自該IP位址的訪問之方式防止資料被取得，皆無阻止不特定多數人知悉秘密之效果。禁止複製、下載措施乃限制資料之取得方式，並未對資料起到保密之作用，亦不屬於合理之保密措施。登入機制則有保密資訊之效果，但仍需進一步區分。若為任何人皆可註冊並得以訪問與取得資訊之網站，則登入機制不具有保密資訊之效果；若僅限定特定權限者才被允許訪問、知悉、取得資訊，則登入機制即為合理之保密措施。採取該保密措施之資訊自不為一般公眾與專業領域之人所知悉，具有秘密性。如此，則可認為該產業研發或創新技術與商業性資訊屬營業秘密。

因使用爬蟲擷取資料的過程本身就伴隨著資料的重製，故當行為人使用爬蟲破解前述之登入機制或擅自使用他人的訪問權限而取得營業秘密，則為未得他人同意

---

132 最高法院107年度台上字第2950號刑事判決；智慧財產法院103年度民營上字第3號民事判決。

133 智慧財產法院107年度刑智上訴字第14號刑事判決；智慧財產法院105年度刑智上訴字第11號刑事判決；最高法院102年度台上字第235號民事判決。

134 王皇玉，〈論侵害營業秘密之犯罪行為〉，《月旦法學雜誌》，2021年10月，第317期，頁76。

135 曾勝珍，〈資訊時代中營業秘密保障之探討〉，《智慧財產評論》，2009年4月，第7卷第1期，頁64-66。

而重製之擅自重製營業秘行為；若行為人擁有登入帳號密碼，卻突破該帳號密碼之權限範圍，進而擷取營業秘密，則屬未經授權或逾越授權範圍而重製營業秘密之行為。當其具有擅自或未經授權、超越授權重製營業秘密之故意，且存在為自己或第三人不法之利益或損害營業秘密所有人之利益的意圖時，則可成立侵害營業秘密罪。

3. **國家機密、國防秘密、軍事機密、公務秘密**

依國家機密保護法第 2 條規定，所謂國家機密係指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，依法核定機密等級者。國防秘密與軍事機密則依「軍事機密與國防秘密種類範圍等級劃分準則」所定之標準核定，主要係與國防安全、軍事秘密相關並被依法核定密級之文書、圖畫、消息、電磁紀錄或物品。公務秘密係指國家安全法第 2 條之 1 所稱「公務上應秘密」者，但其具體範圍並未有明確規定，缺乏法律明確性[136]，實務上認為所有與外交、財政、經濟、內政、監察、考試、交通、司法與國家政務、事務或人民權益具有利害關係不得洩漏於外之機密均屬之[137]。

一般主體使用爬蟲擷取符合上述定義之資料，擷取行為符合法規範中所指之「收集」，即係一切取得秘密之行為[138]，且行為人主觀上具有收集國家機密、國防秘密、軍事機密、公務秘密之故意，則以資料所屬之秘密類型可成立國家機密保護法第 34 條之收集國家機密、準國家機密罪、刑法第 111 條之收集國防秘密罪、國家安全法第 5 條之 1 第 3 項之收集公務秘密罪、國家情報工作法第 30 條第 2 項之收集秘密資訊罪；若使用爬蟲的主體為現役軍人，則可成立陸海空軍刑法第 22 條之收集軍事機密罪；另行為人若為從事間諜行為而故意收集以上各類秘密資訊，則可成立國家情報工作法第 30 條之 1 第 2 項為從事間諜行為而收集秘密資訊罪。

前述秘密之間雖各有界限，卻又相互關聯，尚非概屬相斥，可謂藕斷絲連[139]，所以在適用法規時，可能存在競合，此時，屬特別刑法之陸海空軍刑法應優先適用，而其他附屬刑法與普通刑法則需基於「窮盡判斷原則」，逐一檢驗，倘認識上均符合其犯罪要件者，再判定是否成立「法條競合」[140]。

㈡**擷取著作**

在網路時代，大量的著作被數位化而置於網路上，著作的重製也變得輕而易舉。針對著作的重製行為，著作權法第 91 條第 1 項規定擅自重製罪予以規制。本罪的客

136 蔡震榮，〈間諜罪防制修法之探討〉，《臺灣法學雜誌》，2019 年 7 月，第 371 期，頁 29-30。

137 最高法院 109 年度台上字第 2793 號刑事判決。

138 靳宗立，《刑法各論 I：國家・社會法益之保護與規制》，自版，2011 年 9 月，頁 113。

139 謝添富、趙晞華，《陸海空軍刑法論釋》，自版，2010 年 7 月，頁 618。

140 靳宗立，前揭（註 138），頁 55。

體為著作，需符合著作權法第3條第1項第1款及第5條第1項所規定之形式要件與具有「原創性」之實質要件[141]。即使是違反善良風俗之色情作品，只要符合「著作」的要件，亦受該法之保護[142]。本罪的行為為擅自重製他人著作；本罪是故意犯罪，行為人需具有擅自重製他人著作之認識與意欲。

其次，考量個人利益與公共利益之間的平衡，在禁止侵害著作權人獨占的著作利用法益外，著作權法尚訂定合理使用規定，故存在「允許重製」之特殊的規範常態[143]。但就本法所規定之合理使用係屬阻卻構成要件該當性還是阻卻違法性之事由存在爭議。有認從著作權法第65條第1項之「不構成著作財產權之侵害」之表述可知合理使用無著作權之侵權，即無法益之侵害性，故應將其視為阻卻構成要件該當性之事由[144]。有認擅自重製即對著作權人專屬權利造成侵害，只是基於利益衡量之考慮，肯定優先保護公益之必要，故而限制著作人於規範上具獨占性格的重製利益，因此，該項規定應為阻卻違法之事由[145]。

本文認為後者觀點較為合理，為保護著作權人之創作成果，著作權法賦予其專屬的著作財產權，除著作自身之價值外，更多指向著作利用所產生的相關經濟利益，所以，著作權人有權決定他人能否利用著作。合理使用的各種情形係對個人著作財產權的限制而非排除，即肯定擅自重製行為對法益存在侵害的前提下，例外允許在未得著作權人同意之情況下利用著作。且從「不構成著作財產權之侵害」的表述，亦無法得出其等同於「根本不存在法益侵害」之論斷，換言之，完全可以將其理解為係因阻卻違法性而無著作財產權之侵害。

雖然網路具有公開之屬性，但對著作而言，數位化與否只是在著作之載體形式上有所區別，不影響其本身作為原創性智慧成果所應受到的保護。使用爬蟲重製他人著作，必須得到著作權人的同意或授權方能為之，否則即為擅自重製之行為。且該同意或授權需行為時即已取得，事後之同意或授權不包括在內[146]。由於爬蟲可自動大量擷取資料，行為人在使用爬蟲擷取資料時，對其擅自重製他人著作的情況未必存在明知。然行為人既使用爬蟲程式理應對其運作原理有所了解，即應當對爬蟲

141 最高法院106年度台上字第455號刑事判決；古承宗，〈重新檢視擅自重製罪之解釋與適用〉，《東吳法律學報》，2012年1月，第23卷第3期，頁90-91。

142 智慧財產法院101年度刑智上易字第74號刑事判決；智慧財產法院109年度刑智上訴字第30號刑事判決。

143 古承宗，〈論刑法上的間接侵害著作權〉，《月旦法學雜誌》，2021年5月，第312期，頁118-122。

144 蔡蕙芳，〈著作權法第九一條擅自重製罪之刑法架構分析〉，《臺灣本土法學雜誌》，2007年11月，第100期，頁64-65。

145 古承宗，前揭（註141），頁108-109。

146 蔡蕙芳，前揭（註144），頁68。

可能擅自重製他人著作之情況有所預見，換言之，行為人對擅自重製之行為具不確定的故意。所以只要行為人使用爬蟲未得到同意或授權而擷取網路上受著作權保護的著作，即符合擅自重製罪之構成要件。若無本法所指之合理使用情形及其他阻卻違法事由，同時符合有責性之要件則可成立擅自重製罪。

㈢收集情報資訊

使用爬蟲在網路上蒐集匯總各類資訊，除屬於上述秘密類型的資訊外，大部分皆為公開的資訊。對於情報工作而言，公開資訊的蒐集、研析、處理與秘密資訊的蒐集同樣重要，蓋「公情」與「秘情」相互參照，始足確保其正確性，且基於現行公開資訊蒐集的方便與必要，各國情報機構無不擴大其「公情」蒐研機制[147]。若收集之情報資訊屬秘密之情報資訊，自有前述各項罪名之適用；然若為此處所指公開之情報資訊，因彼之「情報工作」，我方乃視之為「間諜行為」，是以，當為從事間諜活動，而使用爬蟲收集公開資訊時，則有可能成立相應之間諜犯罪。

詳言之，若行為主體為現職或退（離）職之情報人員，使用爬蟲為外國勢力、境外敵對勢力或其工作人員從事情報工作而收集公開資訊，則可成立國家情報工作法第 31 條收集非秘密資訊罪；若行為主體為現役軍人，出於有利敵人之意[148]而在我方使用爬蟲從事收集情報之間諜活動，則可成立陸海空軍刑法第 17 條為敵人從事間諜活動罪；若行為主體為一般人民，於「與外國開戰期內」或「將開戰期內」，隱匿其為敵國服務之身分，在我方領域內進行有助於敵國之資訊收集行為[149]，則可成立刑法第 107 條為敵國間諜助敵罪；同時，一般人民若於「戰時」而為之，亦可成立陸海空軍刑法第 17 條為敵人從事間諜活動罪。

四、小結

雖然不當使用網路爬蟲之態樣眾多，但通過對爬蟲運作原理及各罪成立要件之分析，可知並非所有不當使用網路爬蟲的行為均可構成犯罪。對於手段不當之使用爬蟲行為，一方面，應以登入機制構建網路公開領域與私人領域之間的屏障，以阻止不必要的訪問與資料的擷取，維護電腦與資料的安全及隱私。另一方面，則需關注爬蟲對電腦系統運作之影響，對干擾電腦運作之使用爬蟲行為作出限制。是以，非法使用訪問權限中非法使用他人帳號密碼之行為可成立入侵電腦罪（刑法第 358 條）及侵害電磁紀錄罪（刑法第 359 條），超越授權範圍使用本人的帳號密碼則可成立侵害電磁紀錄罪；破解訪問限制中唯有破解登入機制之行為可成立入侵電腦罪

147 陳重見，〈國安三法修正評釋〉，《臺灣法學雜誌》，2019 年 7 月，第 371 期，頁 17。

148 謝添富、趙晞華，前揭（註 139），頁 150。

149 靳宗立，前揭（註 138），頁 104。

及侵害電磁紀錄罪；而以異常的次數或頻率訪問網站可成立干擾電腦罪（刑法第360條）。

從不當取得資料之性質來看，刑法對於各種秘密類型資料與智慧財產都已建立較為完整的保護體系，應不至於出現處罰之間隙。使用爬蟲擷取個人資料可成立違法蒐集處理利用個人資料罪（個人資料保護法第41條）；擷取營業秘密可成立侵害營業秘密罪（營業秘密法第13條之1）；擷取公秘密則可成立收集國家機密、準國家機密罪（國家機密保護法第34條）、收集國防秘密罪（刑法第111條）、收集公務秘密罪（國家安全法第5條之1第3項）、收集軍事機密罪（陸海空軍刑法第22條）、收集秘密資訊罪（國家情報工作法第30條第2項）、從事間諜行為而收集秘密資訊罪（國家情報工作法第30條之1第2項）；擷取著作則可成立擅自重製罪（著作權法第91條第1項）；收集情報資訊可成立收集非秘密資訊罪（國家情報工作法第31條）、為敵人從事間諜活動罪（陸海空軍刑法第17條）、為敵國間諜助敵罪（刑法第107條）。

伍、代結論

一、網路爬蟲在資訊化時代的需求性與必要性

在資訊化時代，隨著資訊通信技術的不斷進步，各種各樣的資料以數位化的形式保存於網路空間。這些海量的資料，構成新的社會資源，新資源的利用正在改變著社會結構與運行方式[150]，可以說，資料就是資訊時代的石油。資料的流轉、匯集、共享、分析及應用離不開網路爬蟲，網路爬蟲在資訊化時代具有舉足輕重的地位。網路爬蟲不僅讓資料的蒐集變得更有效率，還讓資料的流轉、共享、應用更具多元化。網路爬蟲的廣泛使用開創了新的商業模式，為企業創造了更多經濟效益，同時利用該技術構建的各種網站或應用程式也在漸漸融入人們的生活，並且變得越來越密不可分。在資訊化時代，人們對網路爬蟲的需求性持續提高。

從必要性角度考量，網路爬蟲是搜尋引擎的核心，搜尋引擎是伴隨著網際網路而產生的，是其不可或缺的一部分。若無網路爬蟲，網際網路的使用必將變得非常困難，而且網路空間上的資料亦無法充分的流動與互相的連接，如此，互通、共享的網路空間將不復存在，而建立於大數據基礎上的人工智慧等研發亦將陷入困境。概言之，若是沒有網路爬蟲，那麼網際網路、科技、社會的發展都將停滯不前。因此，網路爬蟲在如今的資訊化時代具有必要性。

150 高富平，〈數據經濟的制度基礎：數據全面開放利用模式的構想〉，《廣東社會科學》，2019年9月，第5期，頁6。

二、網路爬蟲行為本身尚不具備入罪化之條件

儘管資訊化時代對網路爬蟲具有極高的需求性及必要性，然而其也帶來了不容小覷的風險。由於自古以來諸法合體，民刑不分的立法體系，刑罰萬能化之思維深入人心，故面對新事物、新技術所引發的風險，人們更傾向求諸於刑事法律來保護自己的權益及實現公平正義的期待。然而，刑罰作為最為嚴厲的制裁措施，其使用必須慎之又慎，在現代刑法理念中，檢討一行為是否應當動用刑法予以規制，所需考量的層面極廣，其中最為重要者在於法益保護原則及刑法謙抑思想[151]。

在刑法論述場域中，法益具有解釋犯罪成立諸項要素與劃定入罪化的處罰界限雙重功能[152]，保護法益安全是刑法的主要任務，亦是刑法規範之目的。法益保護原則要求立法者若欲處罰某一行為，則該行為需侵害法益，即造成法益損害或具損害法益之可能性，否則即不得動用刑罰加以制裁。換言之，「法益侵害性」是入罪化之必要條件，同時，「法益侵害性」還是「刑罰必要性」之前提，若是行為未侵害法益，則自然無需論及「刑罰必要性」[153]。

在一行為滿足法益侵害性之條件後，則需考慮刑法的謙抑性問題。基於憲法比例原則的要求，在國家權力機關所欲達成目的中所採取之手段，須係限制人民基本權利最少者，始得為之[154]。換言之，若是依民法或行政法即足以遏制不法行為或維持社會之公平正義時，則無需將該行為規定為犯罪，而施以刑罰處罰[155]，意即該行為並無「刑罰必要性」。

是以，對於網路爬蟲行為是否應入罪化，亦即制定「網路爬蟲罪」專罪，首先需審視該行為是否具有「法益侵害性」。按網路爬蟲作為一種自動擷取資料的程式，網路爬蟲行為是否侵害到法益不能一概而論，端視其使用方式之性質如何為斷：倘若是行為人遵守各項法律規定、行業準則或依網站管理者或資料主體所訂定之規則而使用網路爬蟲，那無論對網站的訪問，還是對資料的取得，皆為已得授權之行為，此種正當使用之行為並未對法益造成侵害，自無需加以刑事制裁；惟若係前述各種不正當使用網路爬蟲的行為雖具有侵害秘密、財產、國家安全等法益之可能，惟現行刑事規範已定有相關犯罪類型予以保護，亦無另定「網路爬蟲罪」之必要。

---

151 靳宗立，前揭（註 29），頁 132。

152 許恆達，〈刑法法益概念的茁生與流變〉，《月旦法學雜誌》，2011 年 10 月，第 194 期，頁 135。

153 陳志龍，〈刑法的法益概念（中）〉，《國立臺灣大學法學論叢》，1988 年 6 月，第 17 卷第 2 期，頁 118。

154 靳宗立，前揭（註 29），頁 132。

155 甘添貴，〈刑法之謙抑思想〉，《月旦法學雜誌》，1997 年 5 月，第 24 期，頁 50。

三、不當使用網路爬蟲行為現行刑事法制尚未出現明顯缺失

從美國及中國大陸的實踐經驗可知，二者皆未針對網路爬蟲進行專門之立法，而是一方面通過對網路爬蟲行為態樣之分析，並對相關電腦犯罪之構成要件進行解釋，使其可用於評價不當使用網路爬蟲之行為；另一方面，則是根據網路爬蟲所擷取資料的性質，視其是否為法律已類型化保護之對象，從而適用相關法規予以規制。

境內對於電腦及資料安全，早已訂定相應之電腦犯罪予以保護；對個人隱私、財產、國家安全法益，亦有專門之個人資料保護法、營業秘密法、著作權法、國家機密保護法等可以適用。只是能否將現有之刑事規範適用於不當使用網路爬蟲之行為，還需檢視該行為事實是否合於犯罪之成立要件。

依本文之研究結果，不當使用網路爬蟲之行為態樣可以使用爬蟲之手段及爬蟲所擷取資料之性質作區分。依手段之不同又可細分為違反網站管理規定、非法使用訪問權限、破解訪問限制、破解儲存限制、以異常的次數或頻率而使用網路爬蟲擷取資料五大類別；依資料之性質可分為使用爬蟲擷取秘密、擷取著作、收集情報資訊三種類型。

通過對電腦犯罪的構成要件之解釋，其可涵攝於部分手段不當之使用網路爬蟲行為，詳言之，非法使用訪問權限與破解登入機制而使用爬蟲擷取資料，屬無故入侵他人電腦及無故取得他人電腦之電磁紀錄行為，可成立入侵電腦罪、侵害電磁紀錄罪；以異常之次數或頻率使用爬蟲訪問網站，則屬無故以電腦程式干擾他人電腦之行為，可成立干擾電腦罪。又經分析可知，使用爬蟲擷取秘密，可構成蒐集處理利用個人資料罪、侵害營業秘密罪、收集國家機密罪等；使用爬蟲擷取著作，可構成擅自重製罪；使用爬蟲收集情報資訊，可成立收集非秘密資訊罪、為敵人從事間諜活動罪、為敵國間諜助敵罪。

惟手段不當類型中的違反網站管理規定、破解 UA 驗證、破解 IP 封鎖、破解驗證碼機制、破解加密參數以及破解儲存限制而使用爬蟲擷取資料之行為，因難以符合「破解使用電腦之保護措施」、「無故取得」等要件之故，在當前之刑事法制下不成立犯罪。且網站管理者於公開之網路上設置管理規定、UA 驗證等僅具提示訪問權限或減緩訪問速度作用之措施，意味此時電腦與資料安全之利益已不甚重要，故違反或破解 UA 驗證等措施而使用爬蟲擷取資料之行為，亦難謂其具法益侵害性。自啟蒙時代以降，刑罰已不再是嚴酷而無限制的處罰與制裁，僅嚴重的侵害行為方適用之[156]。是以，對於此類不當使用網路爬蟲行為並無動用刑法規制之必要。茲就

156 許恆達，前揭（註 152），頁 139。

本文研究分析之「不當使用網路爬蟲具體態樣」及其可能適用之現行刑事責任，彙整如表 1。

表 1 不當使用網路爬蟲態樣及可能刑事責任

不當使用網路爬蟲態樣			現行可能刑事責任
依手段區分	違反網站管理規定	違反管理者所設條款	無
		違反網站「爬蟲協議」	無
		違反拒絕訪問通知	無
	非法使用訪問權限	使用他人帳號密碼	入侵電腦罪、侵害電磁紀錄罪
		超越權限使用本人之帳號密碼	侵害電磁紀錄罪
	破解訪問限制	破解登入機制	入侵電腦罪、侵害電磁紀錄罪
		破解 UA 驗證	無
		破解 IP 封鎖	無
		破解驗證碼機制	無
		破解加密參數	無
	破解儲存限制	破解文字加密、混淆措施	無
		破解禁止複製、下載措施	無
	以異常的次數或頻率訪問網站		干擾電腦罪
依資料的性質區分	擷取秘密	擷取他人個人資料	違法蒐集處理利用個人資料罪
		擷取他人營業秘密	侵害營業秘密罪
		擷取國家機密、軍事機密、國防秘密、公務秘密	收集國家機密、準國家機密罪、收集國防秘密罪、收集公務秘密罪、收集秘密資訊罪、收集軍事機密罪、為從事間諜行為而收集秘密資訊罪
	擷取著作		擅自重製罪
	收集情報資訊		收集非秘密資訊罪、為敵人從事間諜活動罪、為敵國間諜助敵罪

資料來源：作者自行整理

綜上所述，當前之刑事法制尚足以應對不當使用網路爬蟲之行為，並未出現明顯之缺失，故而無需特別針對網路爬蟲設立專法或增設專門的刑事處罰條款。其實不僅是網路爬蟲，隨著科技的不斷發展，新的事物、技術、社會關係必將不斷湧現，由此引發的事實層面之行為在進入法學領域時，定將受到法律規範之價值評價。如何對廣泛存在的與計劃中的技術進行法律評價，同時及早說明可能存在的違法，以便在技術發展中進行修正，是我們所需面臨之挑戰[157]。

[157] Eric Hilgendorf 著，江朔、黃笑岩譯，《德國刑法學：從傳統到現代》（Die deutsche Strafrechtswissenschaft: Tradition und Moderne），北京大學出版社，2015 年 8 月，頁 378。