國安法與科技中立之爭——香港數位權利的未來挑戰

鄺頌晴
對中政策跨國議會聯盟（IPAC）高級分析員
漢堡大學法律系博士候選人

摘要

自《港區國安法》通過以來，香港的公民社會和數位權利經歷了劇烈的變化。該法律不僅在現實中限制了公民的表達，還對數位空間中的言論自由帶來了前所未有的挑戰。煽動罪的定義被擴大，導致許多市民和活動人士因和平言論而遭逮捕、起訴和監禁，促使公民自我審查。

隨著第二十三條立法的推進，數位監控與限制將進一步加劇，資訊自由流通更加困難，公民在網絡上表達意見的恐懼感增強。本文通過探討煽動罪在網絡中的應用、網絡服務供應商的困境和網站封鎖案例，分析香港數位權利的侵害情況。

文章指出，《國安法》和《刑事罪行條例》對煽動罪的擴展與技術中立性原則產生衝突。例如，分享超連結的行為被視為煽動，違反了技術中立性，削弱了言論自由。案例如王浩鏘案和許佩怡案顯示，網絡用戶和平台管理者可能因用戶生成內容而被追究法律責任。

此外，政府對網絡供應商施加更多監管義務，要求其封鎖被視為威脅國家安全的內容，進一步違反技術中立性，削弱了網絡言論自由。立場新聞案的判決降低了煽動罪的定罪門檻，增加了網絡服務供應商的法律風險。

《維護國家安全條例》的通過擴大了政府對言論的控制，適用範圍涵蓋全球，對香港異議人士和跨國科技平台帶來更大限制。條例中模糊的定義使市民和企業難以判斷哪些行為可能觸法，加劇了自我審查和寒蟬效應。

台灣人權學刊 第七卷第四期
2024 年 11 月　頁 111~126

關鍵字

香港國安法、維護國家安全條例、數位權利、煽動罪、自我審查、技術中立、數位監控、網絡言論自由

自《港區國安法》通過以來，香港的公民社會及數位權利在短時間內經歷了急速轉變。這些法律不僅在現實空間中限制了公民的表達，也對數位空間中的言論自由帶來了前所未有的挑戰。尤其是《國安法》下，煽動的定義被擴大，導致許多香港市民和活動人士因為發表和平言論而遭受逮捕、起訴，甚至監禁。此外，這種法律實施推動了公民自我審查，以避免受到類似的懲罰。

隨著《維護國家安全條例》立法，數位空間中的監控與限制將會進一步加劇，信息在香港的自由流通將越來越困難，公民對網絡上表達意見的恐懼感也會持續增加。本文通過煽動案件、網絡服務供應商的困境及封鎖網站的實例，探討香港的數位權利如何受到侵害。

數位言論自由與煽動定義的擴大

《國安法》引入了「國家安全罪行」的概念，開啟了大規模的政治檢控。此類罪行涵蓋分裂國家、顛覆政權、恐怖活動及勾結外國勢力，並且可根據案件情況，將《刑事罪行條例》中的煽動罪視為「國安罪行」。[1] 這一寬泛的罪行定義導致當局有更大的調查權，並且案件由指定法官審理，保釋條件也更加嚴苛。2023 年，一位香港居民因為在日本留學期間在社交媒體上發表的言論，返回香港後被控以「煽動分裂國家罪」，這是國安法域外適用的第一案。這類案件凸顯了當局對公眾表達自由的打壓，並且在數位空間中的應用愈加明顯。

煽動罪在網絡表達中的具體應用

煽動罪的擴大主要體現在對網絡內容的監控和定罪上。根據《刑事罪行條例》第 9(1) 和第 10 條，發布、分發或展示任何具有「煽動意圖」的內容都是

1 2021 年，終審法院確立《刑事罪行條例》中的煽動控罪屬「國安罪行」。過去 3 年，當局頻繁使用其他條例作出「國安罪行」相關抓捕；當局在處理這類罪行時，有更大的調查權力，保釋條件嚴苛，並由《國安法》指定法官審理。

違法的，這些條文涵蓋了網絡空間中的各類表達，包括個人社交媒體帳號、討論區、網上論壇及博客等。隨著網絡監控的加強，個人社交媒體貼文的內容也成為政府關注的重點，任何批評政府、司法或中國內地的言論都有可能被視為煽動。這對個人表達自由構成了嚴重威脅，因為批評政府、司法體系或中國內地的言論隨時可能被視為違法。模糊的煽動罪定義讓網民難以預測自己的言論是否觸犯法律，導致自我審查的普遍現象。

過去，社交媒體和討論平台被視為公民表達自由意見的重要渠道，但如今，這些平台成為政府監控和法律管制的重點領域。煽動罪的模糊定義使得個人用戶在表達批評意見時面臨巨大風險，特別是那些涉及政治敏感話題的內容。網民無法確定自己的言論是否會被視為違法，這導致了廣泛的自我審查現象。鄭麗琼案 (HCMP 1256/2020）、[2] 譚得志案（DCCC 930/2020、DCCC 927/2020、DCCC 928/2020）、[3] 鍾翰林案（DCCC 27/2021）、[4] 曹雪芯案（DCCC 767/2021）反映了煽動罪的廣泛適用和不確定性。[5] 越來越多的公民選擇在網絡表達時進行自我審查，以避免法律風險。許多人不再敢在網絡上公開討論政府政策、社會運動或中國內地的問題。尤其是在涉及反修例運動、香港獨立或民

2 鄭為香港中西區區議員，因轉發了一名警員的個人資料，並在社交媒體上表達對警方的不滿，遭到控告。她被控藐視法庭罪及煽動意圖。根據《刑事罪行條例》第 9(1)(a) 條，鄭麗琼的行為被法庭認定為「引起對香港政府的憎恨或藐視」。雖然她的行為是對警方行為的不滿表達，但法院認為她的言論具有煽動性，導致她被判刑 28 天，緩刑一年。

3 得志是香港社運活躍分子，因在街站集會和社交媒體上呼籲「解散警隊」及「光復香港，時代革命」等口號，被控「發表煽動文字」罪及「煽惑他人參與未經批准集結」罪，最終被判三年四個月監禁。法院認為譚得志的言論符合《刑事罪行條例》第 9(1)(a) 條中的「引起對香港政府的憎恨」和第 9(1)(b) 條中的「激起香港居民企圖不循合法途徑促致改變」。法院強調，譚得志的言論旨在動員民眾反對政府和警察，並鼓動他人參與非法集會。

4 鍾翰林，香港學生動源的成員，因其在社交媒體上多次發布涉及「香港獨立」的言論，被控「串謀發布煽動刊物」罪。該組織曾通過網絡發布了大量支持香港獨立和分裂國家的文章和材料。鍾翰林的言論被認為符合《刑事罪行條例》第 9(1)(e) 條中的「引起或加深香港不同階層居民間的惡感及敵意」，以及第 9(1)(g) 條中的「慫使他人不守法或不服從合法命令」。法院認為他的行為旨在鼓動分裂主義，威脅國家安全。鍾翰林案強調了《刑事罪行條例》和《港區國安法》對於涉及香港獨立或自決的言論零容忍的立場。

5 曹雪芯因在社交媒體上發表「香港人要獨立建國」等涉及香港獨立的言論，被控「串謀刊印、發布、分發、展示或複製煽動刊物」罪。最終，她被判 13 個半月監禁。法庭強調，曹雪芯的言論和行為涉及「引起憎恨或藐視香港政府」和「激起對香港政府的離叛」，因此符合《刑事罪行條例》第 9(1)(a) 條和 (b) 條中的煽動意圖。儘管她聲稱言論無直接煽動暴力，但法院認定其言論仍具政治危險性。該案再次強調，香港任何關於獨立或政治變革的公開討論，無論其是否涉及暴力，均可能被認為是具煽動性的行為。

主訴求的討論中，言論空間的萎縮尤為明顯。即使是個人在社交媒體上表達支持自決或獨立的意見，也可能面臨嚴重的法律後果。這促使許多市民對於在網上發表的內容進行高度自我審查，避免涉及敏感話題。

自我審查的趨勢也導致了社交媒體上的討論內容趨向於非政治化，許多公民選擇避免涉及任何可能引起政府注意的話題，這使得香港網絡空間的言論更加單一、封閉。

國安法與技術中立性（tech neutrality）之間的張力

在香港，《國安法》和《刑事罪行條例》對煽動罪的擴展，與技術中立原則之間存在著顯著的張力。技術中立性強調，網絡平台或個人僅分享信息或提供超連結（hyperlink），不應被視為與內容創作相同的行為，因此不應承擔與內容創作者相同的法律責任。然而，香港的煽動罪擴大至網絡世界，導致即使只是分享超連結的行為，也可能被視為煽動。

在香港的司法實踐中，我們看到煽動罪的適用已經不僅限於傳統媒體上的發表行為，還涵蓋了社交媒體上的行為。例如，在涉及《羊村繪本》案和其他煽動案件中，當事人因在網絡上分享煽動內容的超連結或電子版資料而面臨起訴。這一趨勢反映了法律對網絡言論的擴大解釋，即使只是分享超連結，也可能被視為「煽動」。然而，這樣的做法與技術中立性產生對立。技術中立性是一種法律原則，認為互聯網技術應該是中立的，即無論技術是如何使用的，其本身不應被視為違法行為。例如，僅發布一個指向某煽動內容的超連結，並不應該被認定為與創作或發布該內容相同的行為。技術中立的核心在於，提供信息的技術本身（如超連結）與內容的創作和發布應有明確區分。

在多個國家和國際法框架下，技術中立原則通常得到尊重。歐洲法院（Court of Justice of the European Union，簡稱 CJEU）在許多判決中曾強調，分享或轉載他人內容的行為，特別是當該內容已經公開可獲取時，應與內容本身分開考慮。在這種情況下，提供超連結的人並不必然承擔與原始作者相同的法律責任，因為他們並未實際參與內容的創作或直接發布。

羊村王浩鏘案（WKCC93/2023）分享超連結的罪責

王浩鏘因在連登討論區分享有關《羊村繪本》的下載超連結而被控「做出一項或多項具煽動意圖的作為」。此案明確展示了政府將分享超連結等同於內容發布的趨勢，這不僅擴大了煽動罪的適用範圍，也模糊了分享行為與創作行為之間的界限。這樣的應用無視了技術中立原則，將網絡用戶的分享行為視為具有同等法律責任的行為，這對於公民自由交流信息的權利造成了極大的威脅。

先撇除《羊村繪本》在正常情況下不應被視為具煽動意圖，其超連結分享者不應該自動承擔與內容創作者相同的法律責任，特別是在技術中立性的背景下。根據歐洲法院的一些判例，特別是 Svensson Retriever Sverige AB (C-466/12) 案，當內容已經公開可獲取時，超連結分享者並不必然直接參與了侵權行為。因此，將超連結分享與原始內容的創作行為區分開來是合理的。在 Svensson 中，法院裁定，當超連結指向的內容已在另一網站上合法公開時，分享該內容的超連結行為不被視為向公眾傳達新內容，因此超連結提供者不需承擔法律責任。只要超連結的內容是合法公開的，超連結者不對原始內容負責。而在 GS Media BV v Sanoma Media Netherlands BV (C-160/15) 案中，法院進一步指出，如果超連結分享者知道或應該知道超連結指向的是未經授權的內容，則其可能承擔責任。然而，這主要適用於商業目的的超連結分享者，普通用戶分享超連結的行為通常不應被視為侵權。此類判例表明，歐洲法院在判定超連結分享的責任時，更多地考量了分享者的知情程度以及其是否具有營利目的。兩案確立了技術中立原則的應用——超連結本身並不應被視作等同於內容創作或發布行為。

這一點在涉及網絡煽動罪的案件中應具有重要意義。如果僅僅因為一個人分享了一個超連結就被指控煽動，那麼這不僅不符合技術中立原則，也對言論自由構成了嚴重威脅。因為許多網絡用戶可能根本無法完全了解所分享超連結中的所有內容，甚至有些超連結可能指向的是被動態修改的頁面。將超連結等同於內容本身，對公民在網絡上的信息分享行為產生寒蟬效應，進一步壓縮網絡言論空間。

許佩怡案 (DCCC177/2020) 平台與發布者同罪

在許佩怡案中，許佩怡作為網絡頻道的管理員被控「串謀煽動罪」，原因是該頻道中的用戶發表了煽動性言論。許作為 Telegram 頻道「阿囝搵老豆老母」的管理員，曾發布逾千名政見相反人士的資料，包括國家官員，而被告與頻道管理員的群組中亦有人提及製作汽油彈方法。被告作為群組管理員，有權刪除相關訊息，惟被告卻容許訊息存在。這一案件展示了另一個技術中立性問題，即網絡平台或頻道管理者是否應為用戶生成內容（User Generated Content，簡稱 UGC）承擔與發布者相同的法律責任。

歐洲法院在 YouTube 和 Cyando 案件（C-682/18 和 C-683/18）中，[6] 針對網絡平台和用戶行為的法律責任做出了關鍵裁決。法院指出，使用者在平台上分享或上載的內容，平台本身並不一定要負上法律責任，除非平台在非法內容的管理或促進方面有積極參與。在技術中立的框架下，平台或頻道管理者通常被視為中介，應保持其技術中立性。也就是說，他們提供的是一個表達平台，而非直接創作或發布內容。因此，許佩怡案中，雖然她作為管理員，理論上有能力控制頻道內容，但她並未親自創作或發表這些具煽動意圖的言論。這種情況下，將她定罪為「煽動」無疑是一種對技術中立原則的背離。

技術中立原則可以被視為保護這一權利的核心概念之一。它確保了用戶在互聯網上傳播信息時，不必為他人創作的內容承擔相同的法律責任，從而促進了信息的自由流動和交流。煽動罪的適用範圍擴大，將分享超連結視為與發布內容相同，已極大地打擊公民在網絡上分享信息的意願，並對言論自由造成持續的威脅。

技術中立性與言論自由密切相關。如果分享信息或提供超連結的行為被視為與內容創作或發布相同，那麼網絡上的信息流動將受到嚴重限制。根據國際公認的言論自由標準，分享和交流信息，尤其是在網絡空間中的信息，應當受到高度保護。聯合國公民與政治權利國際公約（The International Covenant on Civil and Political Rights，簡稱 ICCPR）第 19 條強調，每個人都有權享有言論

6 Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C-682/18) and Elsevier Inc. v Cyando AG (C-683/18)

自由，包括尋求、接收和傳播信息的權利。在當前法律框架下，煽動罪的適用與技術中立原則之間存在著明顯的張力。分享超連結和發布內容本身應被區分對待，否則將導致網絡上的言論自由受到不當壓制。政府和司法機構在應用煽動罪時，應當遵循技術中立原則，確保個人僅因分享信息或提供超連結而不會承擔與創作或發布相同的法律責任。

網絡技術和平台應保持中立

科技中立的原則強調，網絡技術和平台應保持中立，只提供技術性的支持，而不對內容的合法性進行審查。然而，香港《國安法》下的眾多案例，對此原則作出顯著的改變，對於網絡供應商（Internet Service Provider, 簡稱 ISP）和網路服務供應商（Online Service Provider, 簡稱 OSP）來說，有幾個方面的影響。

《國安法》下網絡封鎖義務的擴大

香港國安法要求網絡供應商根據政府要求，封鎖某些被視為威脅國家安全的網站或平台。這直接違反了科技中立的原則，因為 ISP 和 OSP 被迫在技術中立和審查政府要求之間做出選擇。自從「香港編年史」等網站被封鎖後，網絡供應商需履行更積極的審查義務，這增加了其法律風險和操作負擔。

《香港編年史》是第一個因《國安法》而被封鎖的網站。該網站記錄了 2019 年反送中運動過程中的事件，並公開了香港警員和官員的個人資料。根據《國安法》中的國家安全條款，香港警方要求網絡供應商（ISP）封鎖這個網站。這一舉動違反了科技中立的原則，因為 ISP 本應保持中立，僅提供技術服務，而不應負責內容審查和限制用戶訪問。2021 年 2 月，台灣促進轉型正義委員會的網站也被香港網絡供應商封鎖。這是一個與中國大陸政府的歷史、社會正義相關的台灣政府網站，其封鎖進一步顯示了香港國安法對網絡自由的打壓。香港的網絡供應商，包括數碼通、香港寬頻等公司，被要求對特定的政治內容進行屏蔽，這無疑將技術提供者置於被迫參與政府審查的地位，從而違反了技術中立的基本原則。此類封鎖行為不僅削弱了公眾對互聯網服務的信任，還阻礙了國際信息的自由流通。另外，香港近期封鎖了海外香港人媒體

《如水》網站，是香港境內針對海外媒體進行封鎖的首例。《如水》由流亡海外的香港社運人士創辦，主要發布關於香港的深度報道和評論，並維繫流散各地的香港社群。

香港的網站封鎖案例顯示，網絡供應商和平台被迫參與政府的內容審查，這違反了他們作為技術服務提供者應保持中立的原則。此外，煽動罪的擴展使得網絡言論自由進一步受限，許多用戶和平台管理者因為恐懼法律後果而進行自我審查，加劇了言論空間的萎縮。

立場煽動案（DCCC265/2022）對網絡供應商（Internet Service Provider）和網路服務供應商（Online Service Provider）的啟示

國安法賦予香港政府更大的權力要求 ISP 或 OSP 封鎖和移除某些被認為是「煽動」或「勾結外國勢力」的內容。如果服務提供商未能遵守，可能會面臨法律制裁，包括罰款或更嚴重的懲罰。這使得平台或供應商無法像過去一樣僅作為中立的技術提供方，而需承擔更多內容審查責任，這與國際上對科技中立性的通行標準背道而馳。上個月法庭頒下法場案的判詞，進一步確立《國安法》下，網路業者的法律責任包括審查用戶生成內容 (UGC)。

在立場一案中，法官推翻羊村案的判詞，頒布以下判詞：

> *183.* 經重新考慮後，本席認為適當的平衡是要求控方證明發布者在發布煽動刊物時具有第 9(1) 條的煽動意圖（蓄意煽動）、或證明發布者在發布煽動刊物時明知刊物具第 9(1) 條的煽動意圖，但他罔顧後果依然將它發布（罔顧煽動後果），發布者便可以被裁定罪名成立。本席亦重複 *Lai Man Ling* 案的判決，發布者不需要具有與煽動刊物完全相同的煽動意圖，只要有至少一項相同的煽動意圖便可。本席裁定，煽動罪是特定意圖的罪行，而特定意圖指發布者在發布煽動刊物時蓄意煽動、或罔顧煽動後果而明知犯險，他便需要承擔罪責。這準則既可有效維護國家安全，亦同時可適當保障言論及出版自由等基本權利。

立場案的判詞改變了煽動罪的定罪標準。過去法庭需要證明被告的具體意圖（如明確的煽動意圖），在此案後轉變為只需證明發布者在明知刊物可能具有煽動性後仍然發布。這實際上降低了對罪行認定的門檻，並將煽動罪的範圍擴大至不僅僅是故意的行為，還包括了魯莽和疏忽的行為。

對於 ISP 和 OSP 來說，這一標準的變化意味著它們在處理用戶生成內容（UGC）時的法律風險大幅增加。如果一個平台或服務供應商即便未主動創作煽動性內容，但仍然發布或未能有效阻止這些內容的傳播，可能會被視為「罔顧煽動後果」，從而承擔法律責任。這使得它們在管理和審查用戶內容時面臨更大的壓力，特別是在內容涉及政治敏感議題時。ISP 和 OSP 可能會因這一低門檻的責任標準而進一步加強自我審查，特別是針對政治相關的內容。由於沒有明確的具體意圖證明要求，服務提供商可能不得不採取更加保守的措施來避免可能的法律責任，這會對用戶的言論自由產生抑制作用，導致寒蟬效應。為了避免可能因「罔顧後果」而承擔的法律責任，ISP 和 OSP 可能需要投入更多資源在內容審查和過濾系統上，強化技術手段以自動篩查或阻止涉嫌煽動性的內容。這不僅提高了運營成本，還可能導致平台內容的審查過度，進一步壓縮用戶的表達空間。

在此法律背景下，責任鏈可能會延伸至更多技術平台，無論是 ISP 還是 OSP 都需要更謹慎地處理第三方發布的內容。從法庭判決來看，無論是否直接參與內容創作，只要明知有煽動風險而繼續發布，都可能會觸法，這無疑使平台承擔更大風險。

這一低門檻的標準與國際上常見的技術中立原則相悖。在美國，《通訊規範法》第 230 條賦予互聯網平台強有力的保護，規定 ISP 和 OSP 對於用戶發布的內容不承擔責任，這反映了技術中立性的重要性。該法律保護平台不因用戶生成的內容而被視為「發布者」或「發言者」。例如在 Zeran v. America Online, Inc.（1997）案中，第四巡迴法院裁定，AOL（當時最著名的網路服務平台之一）不應為第三方用戶在其平台上發布的誹謗內容承擔法律責任，強調了技術中立原則，即平台對用戶內容不負責。

該案源於一個匿名用戶在 AOL 上發布了誹謗性內容，誤導其他用戶去聯絡和騷擾 Zeran。這些騷擾電話對 Zeran 造成了極大的困擾和情緒損害。Zeran 隨後起訴 AOL，要求該平台對該用戶的誹謗性帖子負責。案件的關鍵問題在於：互聯網平台是否應對用戶在其平台上發布的內容負責？ 在判決時美國法院援引了《通訊規範法》第 230 條，該法律明確指出，互聯網平台不應被視為第三方內容的「發布者」或「發言人」。第四巡迴法院在裁決中明確指出，依據第 230 條，AOL 作為服務提供商不需要為其他人發布的誹謗性內容負責，除非平台本身參與了內容的創作或積極修改。這一裁決鞏固了「技術中立」原則，即平台僅作為信息的中介，而不對用戶生成的內容負責。這為互聯網平台和服務提供商提供了法律保護，允許他們專注於技術支持，而不需要對所有用戶行為進行監控或負責。Zeran 案凸顯了技術中立原則，即互聯網平台應作為中立的技術提供者，而不應對用戶內容承擔相同的責任。

在香港，立場案後，煽動罪的認定標準已從具體意圖擴展到包括「魯莽」和「疏忽」的情形，這意味著只要 ISP 或 OSP 沒有及時阻止可能違法的內容，就可能承擔法律風險。這無疑擴大了 ISP 和 OSP 的法律義務，可能會導致與國際網絡治理標準的衝突，也增加了跨國公司在香港運營的法律風險。煽動罪定罪門檻降低，使得 ISP 和 OSP 的責任範圍大大擴展，不僅僅是對違法內容的發布承擔責任，甚至包括了對煽動性內容的發布者無心或無意識的行為也要負責。這意味著，只要平台「罔顧後果」或無法阻止這類內容的傳播，便可能被追究法律責任，即便平台本身未必完全知曉或故意違法。這樣的標準與歐盟法院確立的技術中立原則存在明顯衝突。

雖然歐洲的 Delfi AS v. Estonia 與英國的 Godfrey v. Demon Internet 兩案表明在某些情況下，技術平台（如新聞網站）必須為用戶生成的內容負責，但兩案涉及的是誹謗性內容及仇恨言論，與香港以政治言論入罪的社會現狀情況截然不同。

《維護國家安全條例》進一步損害科技中立

《維護國家安全條例》的通過亦對 ISP 和 OSP 的營運施加了額外的法律壓力，該法例對於 ISP 必須確保平台上沒有違法的言論或內容，否則可能面臨法

律責任，進一步迫使平台加強監控和內容審查，進一步限制了用戶在互聯網上的自由表達，並加劇了自我審查的寒蟬效應。

《維護國家安全條例》是香港在 2024 年推出的立法之一，引起了國際社會的高度關注。根據該條例，涉及「國家安全」的罪行定義非常廣泛，並且多數條文模糊不清，使得香港市民的言論自由受到前所未有的威脅。從數位權利的角度來看，這些模糊的條款和嚴厲的刑罰會直接影響到網絡言論自由。根據條例，任何人意圖引發對政府的「憎恨」或「藐視」行為，無論是否存在實際擾亂公共秩序或暴力，都可能構成煽動罪。這種模糊的定義和條款的應用，不僅打擊了傳統媒體的自由，也使得網絡上的個人和公眾平台，特別是社交媒體上的言論，受到更大的監控和壓制。

除了科技平台的責任增加，該條例的適用範圍涵蓋全世界任何地方的香港居民和企業，這意味著全球範圍內的香港異議人士在社交媒體或其他數位平台上的言論也會受到限制，跨國平台亦被《維護國家安全條例》制肘。香港大學法律學者陳文敏指出，該條例中的「憎恨」和「藐視」等條款定義模糊，缺乏明確標準，使得普通市民和企業難以判斷哪些行為會觸法，這進一步加劇了法律的不確定性。

無論香港居民身處世界何地，他們在社交媒體或其他數位平台上發表的言論都可能受到該法的限制。如果這些言論被認定為具有「煽動意圖」，例如被視為煽動對中國或香港政府的「憎恨」或「藐視」，則有可能面臨刑事指控。此外，該法的域外適用對跨國科技平台也產生了重要影響。跨國平台如 Facebook、Twitter 等全球社交媒體公司，可能會因為香港政府的要求，而被迫刪除被認為違反國家安全法的內容。此舉對於這些平台的內容審查政策以及全球用戶的言論自由帶來了前所未有的挑戰。跨國公司可能會面臨兩難處境：一方面要遵守香港的法律，另一方面又要維持全球範圍內的言論自由和用戶權利，這可能會導致它們在法律義務與言論自由保障之間的平衡變得更加複雜。這種不確定性不僅限於香港本地，還會對相關的技術平台產生寒蟬效應，導致他們對言論和數位權利進行更加保守的管理。跨國平台若因應香港政府的要求進行內容審查，也可能會削弱其用戶對平台言論自由保護的信任。

總結：香港數位權利的未來

香港數位權利的未來受到多重法律框架的影響，特別是在《國安法》、《維護國家安全條例》之下，這些法案對數位權利帶來了深遠的負面影響。

自《國安法》生效以來，大幅擴展了政府監控和干預的範圍，企業和技術平台不僅僅是提供中立技術服務，而是必須與政府合作，提供數據、網絡架構等詳細信息，甚至可能被要求安裝監控軟件以便政府進行實時監控。科技平台不再是中立的媒介，而是被強制要求參與到政府的審查和監控機制中。香港新法規中的責任機制，特別是對網絡服務提供商的加強監管，違背了國際公認的技術中立原則。科技平台被迫承擔更廣泛的審查責任，進一步削弱了數位言論自由和信息流通的可能性。

香港數位權利的未來面臨著更巨大的挑戰。政府準備於 2024 年內通過《加強保護關鍵基礎設施電腦系統安全》法案。該法案要求所有「關鍵基礎設施營運商」（CIO），包括可能涵蓋網絡服務供應商（ISP）和網路服務平台（OSP），對其系統的安全和數據流負責，並向政府通報任何的安全事件。這意味著，網絡服務供應商（ISP）和網路服務平台（OSP）可能會被納入「關鍵基礎設施營運商」的範疇，並因此承擔更多的法律風險。另外，法案對「第二類」營運商的定義模糊，涵蓋了「維持重要社會和經濟活動」的基礎設施，如科研園區或大型活動場所。這樣的模糊定義使得許多企業，特別是中小企業，可能突然被要求承擔法律責任，而無法預見或準備好應對這些責任。法案亦要求營運商與政府分享關鍵系統的設計和運營細節，這可能包括大量的商業機密。法案賦予政府廣泛的監管權力，包括直接介入私人企業的電腦系統，並在其中安裝監控軟件。

法案賦予政府廣泛的權力，允許其對私人企業的關鍵電腦系統進行監控，甚至可以安裝程式以收集資訊。這樣的措施直接威脅到公民和企業的隱私權，特別是商業機密和數據保護。這種政府對數據和系統的干預，極大地削弱了數碼權利中核心的數據隱私，同時也會產生寒蟬效應，使企業和公民擔心自身的數據和通信被政府監控。該法案要求網絡供應商和在線平台進行更多的監控和報告義務，這打破了技術中立原則，迫使這些技術平台參與到政府的審查活動

中。這將導致數字空間的進一步封閉，使得言論自由受限。據法案內容，政府可以基於安全理由封鎖或限制公眾對某些網站或數據的訪問權。這會影響公眾的資訊獲取權，特別是在一些與公共利益相關的議題上，如社會運動或政府透明度等問題。當政府有權隨時封鎖某些資訊時，這會對社會的資訊流通產生不利影響，並可能導致自我審查現象的加劇。

由於國際社會未能對中國和香港特別行政區的人權侵犯行為採取有效行動，香港的網絡用戶和公民被迫依靠自身力量來應對日益嚴峻的數位監控和壓制。國際機構雖然多次發出譴責聲明，但缺乏具體行動和制裁，使香港市民在面對政府的數位壓迫時陷入孤立無援的局面。

香港的數位權利和言論自由空間大幅縮減，網民們不得不進行自我審查，甚至尋找更為隱秘的數位技術工具來保護自己的隱私和言論。例如，越來越多的香港人選擇使用虛擬私人網絡（VPN）或加密通信軟件，儘管這些技術的使用也存在法律風險。隨著國際社會無法提供有效援助，香港公民只能依賴自我保護的技術手段來捍衛其基本數位權利。在香港的數位言論環境更加不安全和不可預測的背景下，香港市民只能依靠自身努力抵禦數位權利的侵犯，這也加重了公民社會的壓力和孤立感。

National Security Law and Technology Neutrality: The Future Challenges of Digital Rights in Hong Kong

Chung-ching Kwong
Senior Analyst, Inter-Parliamentary Alliance on China (IPAC)
PhD Candidate in Law, University of Hamburg

Abstract

The passage of the Hong Kong National Security Law (NSL) and the Safeguarding National Security Ordinance (SNSO) has led to significant erosion of digital rights and civil liberties in Hong Kong. These laws have not only expanded the definition of incitement, resulting in the prosecution of individuals for peaceful online speech, but have also driven widespread self-censorship among citizens.

With the advancement of Article 23 legislation, digital surveillance and restrictions are expected to intensify, further hindering the free flow of information and amplifying citizens' apprehension of expressing opinions online. This article analyzes the erosion of digital rights in Hong Kong by examining the application of sedition charges online, the dilemmas faced by internet service providers (ISPs), and cases of website blocking.

The article highlights that the expansion of sedition under the National Security Law (NSL) and the Crimes Ordinance conflicts with the principle of technological neutrality. For instance, the act of sharing hyperlinks is considered seditious, violating technological neutrality and thereby undermining freedom of expression. Cases such as those of Ho-cheong Wong and Pui-yee Hui demonstrate that both users and platform administrators may face legal liability for user-generated content.

In addition, the government has imposed heightened regulatory

obligations on ISPs, requiring them to block content deemed a threat to national security. This further infringes on technological neutrality and weakens freedom of expression online. The ruling in the Stand News case has lowered the threshold for sedition convictions, thereby increasing the legal risks for ISPs.

The enactment of the Safeguarding National Security Ordinance (SNSO) has extended governmental control over expression, with its scope now covering a global audience, thereby imposing greater restrictions on Hong Kong dissidents and multinational technology platforms. The vague definitions within the ordinance make it difficult for citizens and businesses to judge what actions may violate the law, intensifying self-censorship and the chilling effect on expression.

Keywords

Hong Kong, National Security Law, digital rights, technological neutrality, freedom of expression, incitement, online censorship, self-censorship, extraterritorial jurisdiction, internet service providers, virtual private networks (VPNs), user-generated content, civil liberties, surveillance, privacy.