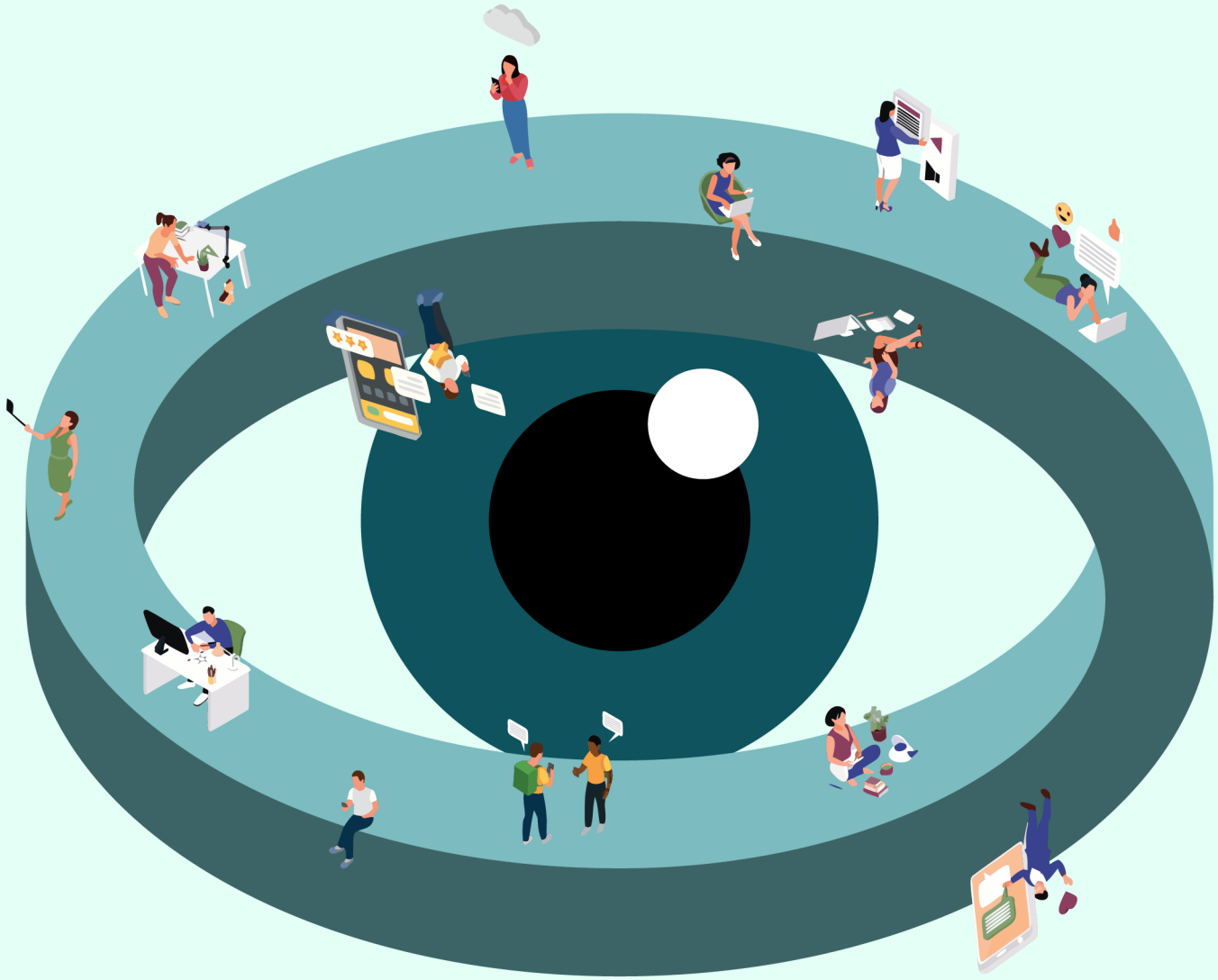
處變不驚

公民社會資訊安全韌性指南



聲明

本手冊之內容僅供教育用途。所有內容均可在網上查閱，並不構成資訊安全、法律或其他事項的專業意見。如有需要，請向相關專業人士諮詢，以獲取具體的行動建議。本手冊內容反映截至撰寫時的法律及技術環境，讀者宜定期查閱最新修訂。

版權



© 2026 韌性創新實驗室 Resilience Innovation Lab

除另有註明外，本手冊採用 Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International（CC BY-NC-SA 4.0，CC「署名－非商業性使用－相同方式共享」4.0 國際）授權條款發佈。

在遵守上述授權條款的前提下，任何人均可複製、分享、傳播及改作本書，惟必須清楚標示作者／來源，提供授權條款連結，並註明是否曾作修改；不得將本書用於商業用途；如改作、轉換或建基於本書創作，須以相同的 CC BY-NC-SA 4.0 授權條款發佈相關作品。

授權條款全文請見：https://creativecommons.org/licenses/by-nc-sa/4.0/

第三方版權材料除另有註明外，不受本書之 CC BY-NC-SA 4.0 授權涵蓋；使用者須就該等材料另行向相關權利持有人取得使用許可。

韌性創新實驗室
Resilience Innovation Lab

https://resilienceinnovationlab.org/
info.ril@proton.me

快 速 參 考

緊急情況清單

懷疑設備被入侵時：

1. 立即斷開網絡連接
2. 移除未知登入裝置
3. 更改所有密碼
4. 啟用封鎖模式（iOS）
5. 考慮重置設備

出入境前：

1. 備份所有重要資料至安全雲端
2. 清除設備敏感資料
3. 準備沒有連上個人資料的備用設備
4. 設定安全聯絡人
5. 確認 VPN 可用

推薦工具一覽

類別	推薦工具
密碼管理	KeePassXC, Bitwarden
雙重驗證	2FAS, Aegis（Android）, Yubico Authenticator
加密電郵	Proton Mail（僅限收件人寄件人同為ProtonMail帳戶）
即時通訊	Signal, Session, Wire, Delta Chat
VPN	Proton VPN, Mullvad VPN, Lantern VPN
檔案加密	Cryptomator, VeraCrypt
安全瀏覽器	Brave, Firefox, DuckduckGo

當前香港立法環境下的資訊安全威脅



概述

現行法律框架直接規範我們如何行使網絡自由，並劃定資訊安全的底線。本章重點探討三項法例：第一是《港區國安法》的四類罪行及其域外效力，第二是《國家安全法》第43條的實施細則（內容移除、資料提交、秘密監察），第三是2024年頒布的《維護國家安全條例》（SNSO）及其新增罪行。無論身在香港與否，理解這些法律的內容、檢控門檻與實施情況，都有助於評估自身風險並做出相應調整。章節依「罪行的定義 → 執法權力 → 新法例擴充 → 觀察與應對」的順序編排；讀完本章後，讀者將對當前法律紅線與執法工具有一幅較完整的圖像，並可在後續章節中結合技術與操作建議，制定保護資訊安全與身份的策略。

對於每一個居住或曾居於香港的人來說，自2020年起，理解這些條文不僅是法律層面的需求，更關乎日常生活與言行舉止。因此，以下盡量以條文與案例說明這些法律如何影響言論自由、資訊安全及個人安全，從而協助你在知情下確保自身權益與安全。

1 《港區國安法》四大罪行

本節說明《港區國安法》中與網絡言論最相關的四類罪行，以及「域外效力」如何令在境外發表的言論仍可能受香港法律追究。了解罪行的定義與既有案例，有助於判斷哪些網上行為可能被視為觸法。

域外效力（第36條）

第36條訂明：只要被指控的言論、行為或結果在香港境內出現，即使行為不在境內進行，亦屬犯罪。例如，若某些言論被指有意圖「引起境內香港市民對政府憎恨」或對政府機關施政造成干擾，即使發表者不在香港，亦可能被追究。

分裂國家罪（第20條）

四大罪行中，與網上言論最直接相關的是分裂國家罪，以下先看其定義與案例。任何組織、策劃或參與旨在分裂國家、破壞國家統一的行為，不論是否使用武力，均屬犯罪。

案件	案件編號	要點
唐英傑案	HCCC 280/2020	展示「光復香港，時代革命」標語，不需要運用武力，已足夠被裁定為有意圖分裂國家
黃煡聰案	DCCC 210/2023	警方監察「香港獨立黨」在 Facebook、Twitter、Instagram 發表鼓吹獨立的言論，追蹤到長居海外的被告為平台管理員，在他回港探親時將其拘捕檢控；被告其後被裁定罪成

網絡安全啟示：在海外管理社交媒體專頁發表的言論，同樣可能構成分裂國家罪。

顛覆國家政權罪（第22條）

涉及通過武力或其他非法手段推翻政權機關，或嚴重干擾政府機構依法履行職能的行為。

案件	案件編號	要點
47人案（民主派初選案）	HCCC 69 & 70/2022	判詞指被告人協定若當選為立法會議員，將無差別投下反對票，被視為會嚴重干擾政府履行職能的「其他非法手段」

網絡安全啟示：在網上討論或協調政治行動的紀錄，可能成為檢控證據。

恐怖活動罪（第24、27條）

涵蓋以實現政治主張為目的，組織或威脅實施恐怖活動的行為。第27條特別針對宣揚和煽動使用武力行為。

案件	案件編號	要點
港大學生會評議會案	DCCC 917/2021	學生在社交平台直播的會議上發表同情使用武力的意見，被控宣揚恐怖主義。律政司最終改控「煽惑他人有意圖而傷人」罪

網絡安全啟示：被告人不需要有具體的暴力行為，發表同情使用武力的政治言論已可入罪；而直播內容同樣可作為檢控證據。

勾結外國或境外勢力罪（第29條）

涉及與外國或境外勢力串謀，請求對中國或香港進行制裁。

案件	案件編號	要點
黎智英案	HCCC 51/2022	檢控證據大部分來自接受訪問的言論及政論文章

網絡安全啟示：網上發表的言論、接受訪問的內容、管理的應用程式、手機通訊內容，都可能成為「勾結」的證據。

2 第43條實施細則（2026年修訂）：執法權力

除「何種行為構成犯罪」外，同樣重要的是了解執法機關以何種權力執行國安法。2026年修訂後的第43條實施細則賦予國安處多項擴大的權力，以下涵蓋五個與網絡自由、資料保護及通訊保密最直接相關的附表。

附表1：裝置存取與解密協助

當局可即場要求指明人士提供密碼、解密方法及其他與裝置或電子資料相關的必要協助。拒絕配合或提供重大失實、誤導性回應，可能觸犯刑事罪行。 修訂同時收緊法律專業保密權（LPP）的程序，增加被捕人法律團隊在搜查或檢取期間爭議物料的程序要求。

資訊安全啟示：要求裝置解密不同於一般監管查問。當事人在查問現場等候法律意見的空間有限，有機會需要即場解鎖提供儲存在設備上的資料。此外，現行法例下，搜查住所無須事先取得法院手令；執法人員在逮捕時往往已備妥搜查令，可即時對住所及設備展開搜查。宜檢視設備是否儲存必須或過多的資料，亦請參考第七章出入境安全。

附表2：行動限制

接受國安調查的人士如不遵從交出護照要求或行動限制，須承擔明確的刑事後果，由過往民事層面升級至刑事責任。

附表4：內容移除

國安處可將視為危害國安的訊息加以限制、停止或刪除，令有關內容不能再在網上傳播。2026年修訂進一步強化當局在通訊鏈不同層面的執法能力，涵蓋出版商、平台、寄存服務及網絡供應商，即使他們並非有關物料的作者或擁有人。

- 在法庭裁定有罪之前，國安處已可向服務供應商作出要求
- 服務供應商包括：社交媒體平台、網站主機公司、網絡商、電訊公司
- 移除內容的決定無需向公眾公布

受影響網站案例：香港監察、支聯會、香港編年史等網站或專頁被封。

附表5：資料要求

當局可強制要求當事人在指定時間及地點答覆問題、提供資料或提交物料。修訂同時引入保密相關限制，可能影響受查人員向內部管理層或法律顧問盡職匯報的能力，令機構在資訊不完整的情況下須作應對決策。

資訊安全啟示：組織紀錄資料（會議紀錄、財務資料、成員名單）都可能被要求提交；而保密限制可能令管理層無法及時掌握完整事實。

案件	案件編號	要點
華人民主書院	—	組織代表接受傳媒訪問時表示，需披露過去七年舉辦過的所有活動資料，包括時間、地點、人物、開支等詳情
支聯會案	WKCC 3633/2021	常委拒絕提交資料被檢控，案件上訴至終審法院得直
J及其他人訴警務處處長案	HCCM 191/2021	國安處要求信託人提交管理帳目、交易記錄、捐贈者資料及受惠者詳情；法庭認為偵測及檢控嚴重罪行的公眾利益較私隱權重要

附表6：秘密監察（截取通訊）

國安處人員可繞過法庭，只需向特首申請命令，便可對特定目標進行監視。監察授權範圍包括：電話勾線、電話短訊、電訊商紀錄的網絡活動、在指定位置設置監察器材。

值得留意： 如當局認為律師或其相關人士會構成危害國安的威脅，
可申請授權監聽律師與客戶的通訊，令法律諮詢保密權利不再是絕對權利。

附表7：物料提交與LPP主張程序（2026年修訂）

國安處可向法庭申請手令，要求組織或團體提交任何與調查案件有關的資料。2026年修訂新設第3部LPP主張程序，當事人須以原訟傳票及誓章提出，並在嚴格時限內以足夠具體方式識別受保密權保障的資料，包括日期、作者、收件人及用途等詳情。

3 《維護國家安全條例》（SNSO）

2024年3月生效的《維護國家安全條例》（俗稱「廿三條」）在國安法之外，進一步擴充國家安全相關的刑事規定，並將「境外勢力」「特區居民」等定義寫入法例。

境外勢力定義

「境外勢力」範圍廣泛，包括： - 外國政府或部門 - 境外的政黨或政治組織 - 境外情報組織或情報蒐集機構（不限政府性質，包括私人公司）- 國際組織 - 上述組織的關聯實體或個人

特區居民定義

包括獲發身分證但沒有居留權的人，即在香港工作的外籍人士亦受規管。

新煽動罪（第23條）

煽動罪近年成為香港的「口袋罪」，一些不涉及使用武力的政見表達，都可能被視為具有煽動意圖。

轉變	內容
加重刑罰	舊法例最高刑期兩年，新法例最高七年
降低檢控門檻	明確訂明控方「無需證明煽惑擾亂公共秩序或煽惑暴力的意圖」

相關案例：「快必案」、「羊村案」、「立場新聞案」，以及多宗針對社交平台帖文、YouTube 評論、直播等網上言論的案件。

間諜活動

範圍非常廣泛：

- 管有對境外勢力有直接或間接用處的任何資料或物品
- 將這些資料傳達給任何其他人
- 勾結境外勢力向公眾發佈虛假或具誤導性的事實陳述

網絡安全啟示：一些簡單取得的資料，甚至公開資訊，都有可能構成間諜活動。

境外干預

構成罪行需具備三個元素：

1. 有境外勢力參與（包括「代」境外勢力作出）
2. 使用不當手段
3. 帶來干預效果

「不當手段」包括：明知而作出關鍵失實陳述；威脅對任何人使用暴力或損毀財產；使任何人蒙受財政損失；使任何人名譽受損或受到心理傷害。

「干預效果」包括：影響政府執行政策或任何其他決定；影響立法會議員或法官執行職能；影響他人行使投票權；損害中國或港府與其他地區的關係。

網絡安全啟示：網上批評政府官員的言論、呼籲制裁官員的意見，
都可能被認定為「不當手段」。

4 觀察與趨勢

綜觀上述法例與實施情況，可歸納出以下觀察；本節並簡要列出可與後續章節配合的應對方向。

香港的言論自由空間正在逐步收窄：

- 網絡言論的監控將變得更加嚴格
- 可能出現更多對網絡平台的審查和監控配套措施
- 自我審查將越來越普遍

應對建議：

轉變	內容
了解法庭案例	理解哪些言論可能觸犯法律
保護電子資料紀錄	加密敏感資料，定期清理不必要的紀錄
分離身份	將政治活動與個人身份分開
使用安全工具	VPN、加密通訊、匿名瀏覽
預備支援渠道	預先協定內部法律分流程序，避免前線成員在管理層或法律支援介入前，獨自面對當局的即場要求

檢查清單

- □ **了解《港區國安法》四大罪行的定義和案例**
- □ **理解第43條實施細則（2026年修訂）賦予的執法權力**
- □ **認識《維護國家安全條例》的新增罪行**
- □ **評估自己的網上活動是否存在法律風險**
- □ **制定保護電子資料紀錄的策略**

RESILIENCE
INNOVATION
LAB