

議題研析

一、題目：詐欺犯罪防制議題--新加坡防制網路犯罪危害之 法制簡介

二、議題所涉法規

詐欺犯罪危害防制條例草案¹（行政院研擬中）

三、背景說明

根據新加坡警察部隊（Singapore Police Force，SPF）公布的新加坡詐欺及網路犯罪 2022 年報指出：2022 年新加坡警方共接獲 31,728 起詐騙案，總計損失金額高達新加坡幣（下同）6.607 億元。其中最常見的 5 個詐騙類型分別是：網路釣魚、求職、電子商務、投資詐騙和假冒朋友電話詐騙²。鑒於詐騙案逐年呈現激增趨勢，新加坡政府於 2020 年 4 月成立打擊詐騙跨部門委員會（Inter-Ministry Committee on Scams），以督導政府的反詐騙工作並負責制定和執行全面的反詐騙策略³。2023 年 7 月 5 日經國會立法通過《網路犯罪危害法》（Online Criminal Harms Act

¹ 行政院刻正召集各打詐主責部會積極研擬「詐欺犯罪危害防制條例」（草案）內容，以「強化防詐作為、打擊詐欺集團與保護犯罪被害」三個重點進行立法，由內政部擔任領銜提案主責機關，通傳會（電信管理）、數位部（數位經濟管理）、金管會（金融機構管理）及法務部（刑度及刑罰執行）共同辦理機關，力求本（2024）年上半年送立法院審議。立法院議事暨公報資訊網站，行政院打擊詐欺辦公室「詐欺犯罪防制立法及各部會打詐機制盤點」公聽會書面資料，2024 年 3 月 14 日，網址：https://ppg.ly.gov.tw/ppg/SittingAttachment/download/2024030618/PPGB60500_4300_20769_1130313_0003.pdf，最後瀏覽日期：2024 年 4 月 28 日。

² 新加坡警察部隊網站，Annual Scams and Cybercrime Brief 2022，網址：<https://www.police.gov.sg/-/media/C23E61900EFD4BA99AA8117ABF2D937C.ashx>，最後瀏覽日期：2021 年 4 月 28 日。

³ 打擊詐騙跨部門委員會（簡稱 IMCS），由新加坡內政部主政，協同新加坡警察部隊（SPF）、通訊及新聞部（Ministry of Communications and Information, MCI）、新加坡金融管理局（Monetary Authority of Singapore, MAS）以及貿易和工業部（Ministry of Trade and Industry, MTI），並與新加坡銀行協會等私營部門合作，共同打擊詐騙，網址：<https://www.mha.gov.sg/mediaroom/parliamentary/ministerial-statement-on-strengthening-enforcement-and-public-education/>，最後瀏覽日期：2024 年 4 月 28 日。

2023，簡稱 OCHA)於同月 24 日經總統公布，並於 2024 年 2 月 1 日生效施行⁴。我國刻正研擬「詐欺犯罪危害防制條例草案」之打詐專法，謹就新加坡《網路犯罪危害法》等相關法制簡要概述，俾供參考。

四、探討研析

(一) 修訂相關反詐法令

自 2018 年以來，新加坡的詐騙案件增加了 5 倍多，超過人身犯罪案件的數量。網路詐騙案件屢見不鮮且迅速蔓延，對受害人造成精神與財物上的嚴重傷害。新加坡雖有《刑法》(Penal Code)等現行法律可用於打擊網路詐騙，但該等法律被認為屬於被動性質⁵。當局認為雖修法加重詐欺罪之刑責，卻難以對犯罪者產生震懾作用，主因是網路詐騙者大多數身處海外，他們也擅長利用科技來掩飾自己的蹤跡⁶。近來新加坡政府已採取進一步措施來阻止詐騙，2023 年 5 月 9 日通過修正《1992 年貪腐、販毒和其他嚴重犯罪問題（沒收所得）法》(Corruption, Drug Trafficking And Other Serious Crimes (Confiscation of Benefits) Act, 簡稱 CDSA) 和《1993 年電腦濫用法》(Computer Misuse Act, 簡稱 CMA) 等法案，使新加坡警方能夠更有效地對付錢驢(Money mule, 術語：車手)、遏制詐騙犯罪所得的轉移和濫用 Singpass(新加坡數碼個人身分)的犯罪活動⁷。CDSA 新增一些罪行，警方得以更容易認定構成洗錢罪要件，而 CMA 的修正則允

⁴ 新加坡共和國政府公報，Online Criminal Harms Act 2023 (No.24 of 2023)，網址：<https://so.agc.gov.sg/Act/OCHA2023>，最後瀏覽日期：2024 年 4 月 30 日。

⁵ 例如：涉嫌違反刑法第 411 條不實收受贓物罪，或第 415 條至第 420 條規定的詐騙罪（冒名行騙、以詐術誘使交付財產），依據罪行可處最高 3 年至 10 年徒刑和罰金。儘管如此，輿論仍舊批評政府對於網路詐騙採取被動的應對方式，只有受害人遭受損失並向警方報案後，才採取偵查行動。參閱 Bryan Tan, Eng Han Goh (2023,May 16). Singapore Tackles Online Criminal Activities with a Trio of Bills. 網址：<https://www.reedsmith.com/en/perspectives/2023/05/singapore-tackles-online-criminal-activities-with-a-trio-of-bills>，最後瀏覽日期：2024 年 4 月 29 日。

⁶ 新加坡內政部對國會關於審查詐騙相關犯罪量刑框架頻率質詢的書面答復，網址：<https://www.mha.gov.sg/mediaroom/parliamentary/written-reply-to-pq-on-the-frequency-of-reviewing-sentencing-framework-for-scams-related-crimes/>，最後瀏覽日期：2024 年 4 月 29 日。

⁷ 詳參新加坡《貪腐、販毒和其他嚴重犯罪問題（沒收所得）法》(CDSA) 和《電腦濫用法》(CMA) 修正案，網址：<https://www.police.gov.sg/Advisories/Crime/CDSA-and-CMA-Bill-Amendments>，最後瀏覽日期：2024 年 4 月 29 日。

許警方得以處置濫用 Singpass 憑證的個人，該兩法案的新修正條款於 2024 年 2 月 8 日生效。

(二) 《網路犯罪危害法》

新加坡國會 2023 年通過的《網路犯罪危害法》，是藉由立法手段，期以有效迅速的方式管制網路內容，打擊詐騙和惡意網路活動，為公眾打造更安全的網路環境，相關特點如下：

1. 主動預防詐騙及惡意網路活動，針對特定刑事犯罪發布指示

- (1) 該法第 6 條允許政府向任何可能進行犯罪活動的網路行為或服務發布「指示」(Direction)，並適用於法定的特定刑事犯罪類型，包括影響國家安全、民族和諧及個人安全並與網路有聯繫的刑事犯罪⁸。
- (2) 當**合理懷疑**某特定犯罪行為已發生且其任何網路活動都是為了協助犯罪 (**reasonably suspects** that a specified offence has been committed and that any online activity is in furtherance of the commission of the offence)，及**懷疑或有理由相信**任何網路活動正在準備或協助實施詐騙或惡意的網路犯罪時 (**suspects or has reason to believe** that any online activity is preparatory to, or in furtherance of, the commission of a scam or malicious cyber activity offence)，即可依據犯罪事實發布以下相關指示⁹：
 - ① 停止傳播指示 (Stop Communication Direction)：要求個人或實體停止向新加坡民眾傳播特定的網路內容(包括本質相似的內容)。
 - ② 禁用指示 (Disabling Direction)：要求網路服務供應業者禁止提供特定內容(如：貼文或網頁)，其中可能包含相同內

⁸ 例如：資助恐怖主義行為、煽動暴力、傳播性虐待兒童的內容、非法賭博.....等，參見新加坡內政部新聞稿附件 A，Introduction of the Online Criminal Harms Bill，2023 年 5 月 8 日。網址：<https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/>，最後瀏覽日期：2024 年 4 月 30 日。

⁹ 同註 4，Online Criminal Harms Act 2023 (No.24 of 2023)，PART 2 DIRECTIONS AGAINST OFFENCES，網址：<https://sso.agc.gov.sg/Act/OCHA2023>，最後瀏覽日期：2024 年 4 月 30 日。

容的副本。

- ③ 存取封鎖指示 (Access Blocking Direction)：要求網路服務供應業者阻止新加坡民眾對特定網路網域的存取。
- ④ 帳戶限制指示 (Account Restriction Direction)：要求網路服務供應業者停止其服務的帳戶在新加坡進行通訊和/或與新加坡民眾聯繫。
- ⑤ 應用程式移除指示 (App Removal Direction)：要求應用程式商店(App store)從其新加坡頁面中下架指定的應用程式，避免新加坡民眾繼續下載該程式。

(3) 與其他特定的刑事犯罪法令相比，本法明顯降低了取締網路詐騙的法律門檻，使政府能迅速採取行動，在詐騙和惡意網路活動傷害更多民眾之前即予以遏止¹⁰。

2. 網路服務供應業者須遵守業務守則，主動偵測可疑網路情況

新加坡政府另訂定一套業務守則 (Codes of Practices)¹¹，讓指定的網路服務供應業者遵守，與政府建立夥伴關係，共同合作打擊網路犯罪活動，主動偵測可疑情況，並與警方共用資料，減低用戶受騙或受害的風險（例如：打擊詐騙跨部門委員會推出的「電子商務平台交易安全評等」制度及供民眾下載的反詐騙應用程式 App「詐騙盾 ScamShield」等）¹²。

¹⁰ 新加坡警察部隊網站，Introduction To OCHA, 網址：<https://www.police.gov.sg/Advisories/Online-Criminal-Harms-Act/Introduction-to-OCHA>，最後瀏覽日期：2024年4月30日。

¹¹ 法令規定新加坡政府將發布業務守則，對那些評估為具有重大詐騙或進行惡意網路活動風險的指定網路服務供應商（如：社交媒體平台）採取措施，以降低有關風險。雖然業務守則不具有法律約束力，但主管機關有權向任何不遵守的業者發出糾正通知書，並強制要求遵守。參閱新加坡內政部網站，Online Criminal Harms Bill—Wrap-Up Speech by Mrs Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs, 2023年7月5日，網址：<https://www.mha.gov.sg/mediaroom/parliamentary/online-criminal-harms-bill/>，最後瀏覽日期：2024年4月30日。新加坡資通訊媒體發展局於2023年7月18日發布有關網路安全的業務守則，新加坡資通訊媒體發展局網站，Code Of Practice For Online Safety, 網址：<https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/codes-of-practice/codes-of-practice-media/code-of-practice-for-online-safety.pdf>，最後瀏覽日期：2024年5月1日。

¹² 詳參新加坡內政部網站，電子商務交易市場安全評等 E-commerce Marketplace Transaction Safety Ratings, 網址：<https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings>，以及新加坡國家預防犯罪委員會網站 National Crime Prevention Council, 關於詐騙盾 About ScamShield, 網址：<https://www.ncpc.org.sg/scamshield/>，最後瀏覽日期：2024年4月30日。

3. 未遵守指示或業務守則者將面臨處罰

《網路犯罪危害法》適用於個人及企業，包括新加坡境內外的指定網路平台及網路服務供應業者，主管機關發現指定網路服務供應業者不符合業務守則者，可以向業者發出**糾正通知書**（Rectification Notice），要求其限期改正，若業者對於業務守則、糾正通知書及指示仍未遵守，主管機關可進一步發出**命令**（Order）¹³，限制存取該服務或部分服務，並可對業者祭出最高100萬元之罰款；至於違反前述指示的個人，最高可處2萬元罰款，或科或併科2年以下有期徒刑，屢犯者更處以額外懲罰¹⁴。

4. 救濟途徑

（1）對指示與命令有異議：

① **再議**（Reconsideration）：個人、網路位址所有人以及網路活動發起人若對指示或命令有異議，得向原發出指示或命令之官員（新加坡警察部隊警官）**申請再議**（Application for Reconsideration）。網路服務供應業者則可向主管機關申請再議。

② **上訴**（Appeal）：個人或網路服務供應業者之再議申請遭駁回，可向**複審法庭提出上訴**（Appeal to Reviewing Tribunal），要求更改或取消該指示或命令，複審法庭成員由總統根據內閣建議任命的地區法官或治安法官組成，複審法庭的程序視為司法程序。

（2）**對業務守則有異議**：指定網路服務供應業者對業務守則有異議，可以向新加坡內政部長提出上訴（Appeal to Minister），部長對任何上訴的決定均為最終決定¹⁵。

（三）結語

¹³ 同註 4，Online Criminal Harms Act 2023(No.24 of 2023) PART 6 ORDERS AGAINST NON-COMPLIANCE，最後瀏覽日期：2024年4月30日。

¹⁴ 同註 4，Online Criminal Harms Act 2023(No.24 of 2023) Part 11 OFFENCES, PENALTIES AND DEFENCES，最後瀏覽日期：2024年4月30日。

¹⁵ 同註 4，Online Criminal Harms Act 2023(No.24 of 2023) PART 5 APPEALS ARISING FROM PART 4，最後瀏覽日期：2023年4月30日。

新加坡政府透過修法與加強立法，積極防制網路犯罪危害問題，此外，電子商務交易市場安全評等制度，也有助於監管平台業者在防範詐騙方面的表現。然而強制網路服務供應業者及社交媒體平台移除詐欺內容，同時引發社會對於政府侵犯個人隱私權及網路言論自由權的批評。《網路犯罪危害法》甫於今(2024)年2月1日生效施行，尚需一段時間方能評估成效，然該法內容對應我國研擬制定打詐專法草案時，如何強化行政管理上的責任與作為，頗值借鏡。

撰稿人：林華彬