編按：本文在第六屆“澳門．珠海警務論壇”中獲選為現場發表論文，是次論壇主題為“多元發展，創新融合——新時代澳門．珠海警務合作的新機遇”；此處刊出的是經作者修訂之版本。

犯罪行為網絡化的趨勢下跨境電子取證的思考

司法警察局首席刑事偵查員　李建章

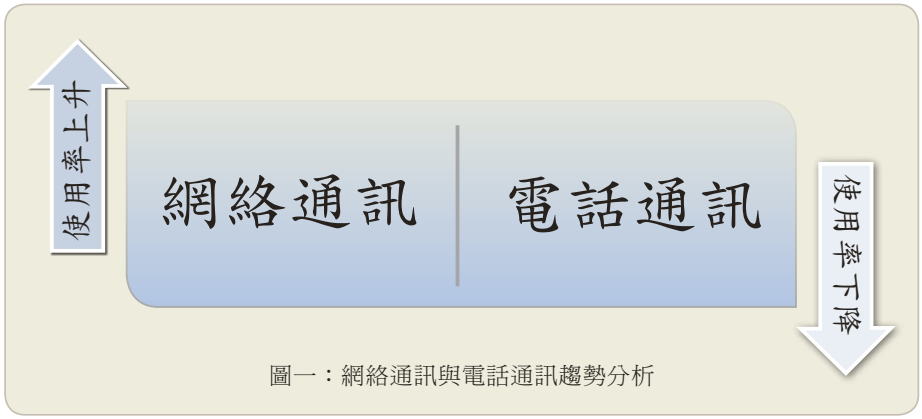
【摘要】現代社會通訊模式的急速轉變，智能手機普及率不斷提高，網絡通訊的快速興起，間接促使不法份子利用通訊軟件作為犯罪溝通工具及實施場域，犯罪行為網絡化已傾向常態性的發展趨勢，對傳統刑事偵查帶來深遠的影響。

本質上，網絡通訊是一種跨國界、跨區域的數據流動，單一地區的電子數據偵查取證措施難以滿足調查效率及跨境取證的需求。因此，本文建議粵港澳大灣區在保障公眾隱私及企業合法權益等前提下，參考歐洲聯盟的《歐盟數據提交令》及《歐盟數據保存令》等法令，運用粵港澳大灣區的政策優勢，共同制訂“大灣區數據自由流動框架協議”，從而確立數據主權範圍及網絡刑事管轄標準，完善跨境快捷電子取證的偵查程序制度。

【關鍵詞】犯罪行為網絡化、網絡通訊軟件、跨境快捷電子取證

一、前言

互聯網速度的大幅提升，促使人類社會通訊模式發生根本性的變化，由過往高度依賴電話語音及文字短訊進行溝通，逐步演變成以通訊軟件作為主要的溝通渠道。邁進第五代流動通訊時代（5G），網絡速度將呈現爆發性增長並更為穩定，自主性或人工智能化的網絡通訊，使用率將不斷提升，而電話通訊將日漸式微，甚至有可能最終被淘汰，網絡通訊及電話通訊的發展呈現出反比的趨勢（詳見圖一）。



圖一：網絡通訊與電話通訊趨勢分析

鑑於網絡世界“無國界”的特性，雲服務逐漸被市場認可和接受，數據儲存成本大幅度下降，促使網絡科技公司將大型伺服器數據中心設置於世界各地。網絡通訊實質是一種跨國界、跨區域的數據流動，在保障公眾隱私及企業合法權益等前提下，執法部門如何有效提升調查效率及滿足跨境電子數據取證的需求，

已經成為珠澳兩地執法部門在區域警務合作方面，需要共同面對的重大挑戰。

二、犯罪行為網絡化趨勢概述

順應網絡科技的發展，珠澳兩地均不斷優化各自的網絡基礎建設，讓市民得以在任何時間、任何地點均可以連接網絡，享受網絡帶來的便利，然而智能手機的全面普及，網絡通訊的快速興起，卻間接促使不法份子轉為透過通訊軟件進行秘密溝通，通訊軟件經常被濫用為犯案工具或犯罪實施場域；另一方面，新型的網絡犯罪不法份子亦頻繁策動釣魚攻擊、遠端存取攻擊等網絡攻擊行為，嚴重威脅珠澳兩地的公共關鍵基礎設施[1]的安全。

（一）全球網絡通訊軟件使用情況統計

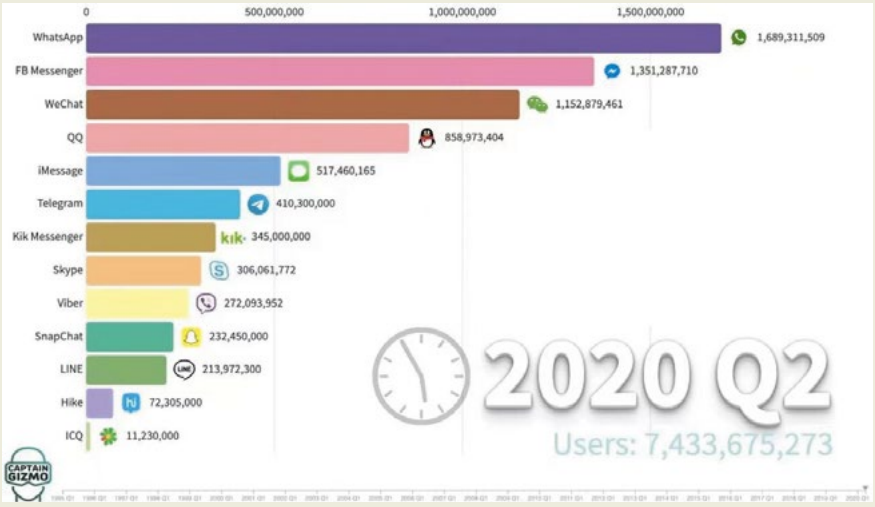
根據資料顯示，直至2020年第二季，全球網絡通訊軟件的用戶超過74.3億，而用戶人數最多的通訊軟件依次為“WhatsApp”、“FB Messenger”、“微信（WeChat）”、“QQ”、“iMessage”（詳見圖二）。

另外，根據第43次《中國互聯網絡發展狀況統計報告》及《澳門居民互聯網使用趨勢報告2018》顯示，內地與澳門的智能手機普及率均位居世界中、前列位置，當中內地手機網民的數量龐大，達8.17億人，位居世界第二，而中國內地與澳門習慣使用之通訊軟件則有所不同，相關統計數據如表一：

表一：內地與澳門通訊軟件使用情況

	手機網民	通訊軟件滲透率	最常使用的三款通訊軟件
中國內地	8.17億	95.5%	微信、QQ、陌陌
澳門特區	50萬	92%	微信、WhatsApp、FB Messenger

※相關數據可能因個別調查報告結果而有所出入。



圖二：截至2020年第二季的全球通訊軟件活躍用戶統計數據[2]

（二）犯罪行為網絡化趨勢的特點

除了滿足市民日常溝通的功能外，通訊軟件已經延伸至社交平台、電子支付、遊戲應用、移動教育、企業營銷、城市政務等多方面民生應用範疇，其影響力是不容忽視的。市民的日常生活離不開互聯網和通訊軟件，大量個人數據被儲存在網絡上；隨着通訊技術和電子支付的全面普及，不法份子利用人們在非接觸狀態下防範意識和辨識能力相對薄弱的特點，實施層出不窮的網絡犯罪。

從刑事偵查實務中，不難發現身處異地的不法份子刻意利用通訊軟件作為溝通工具及實施場域，顯示犯罪行為網絡化、跨境化、常態化的趨勢已悄然成形，伴隨着與日俱增的技術風險、人為風險與制度風險，改變了犯罪行為的不法屬性與不法程度，亦改變了珠澳兩地的犯罪基本態勢和結構，為刑事歸責及刑事調查工作帶來了諸多挑戰。以下為犯罪行為網絡化的四個概括特點：

1. 經濟犯罪呈現上升趨勢

在智能手機全面普及的環境下，海量的個人數據被存儲在網絡世界，大數據成為經濟犯罪的重要資訊來源。犯罪份子利用各種系統漏洞獲取個人資訊，實施網絡經濟犯罪，尤其以互聯網金融領域成為了經濟犯罪重災區。當中，通訊軟件、移動支付更是不法份子實施網絡詐騙的主要工具。

2. 犯罪份子低齡化與隱蔽化

近年，資訊科技在各行各業和各個領域被廣泛應用，網絡應用課程已經成為基礎教育的學科之一，年輕人有較強的求知慾和好奇心，接受能力強，能快速掌握各種網絡專業技術知識，但因為他們的社會閱歷不足，容易被不法份子利用或直接實施犯罪。另一方面，由於網絡自身具有開放性及虛擬性等特點，加上作案人本身具有高度反偵查能力，導致新型網絡犯罪技術手段日新月異，作案人的真實身份和IP位址也能完全隱蔽，增加執法部門防範和偵查取證的難度。

3. 犯罪行為跨區域化

無遠弗屆的網絡世界，沒有地域空間限制，具有壓縮時間與距離的特點，為網絡犯罪提供了無限的可能，不法份子只要擁有一台終端電腦，就能通過網絡利用遠端技術控制任何地域的其他終端電腦，犯罪的範圍亦可以無限擴張。

執法機關礙於管轄權及異地執法合作等問題，使偵查工作難以開展，導致多數犯罪行為不能及時得到懲處。相對而言，由於網絡犯罪成本低、傳播速度快、目標對象廣泛，亦助長犯罪份子的囂張氣焰，跨境犯罪活動亦顯得更加猖獗。

4. 網絡犯罪黑產化

傳統犯罪加速向網絡空間蔓延，形成龐大的地下黑產化犯罪鏈，持續為網絡犯罪提供“模組化”工具，已經成為該類犯罪高發的重要原因。網絡犯罪已經形成較為固定的犯罪利益鏈：上游為犯罪團伙提供技術工具、收集個人資訊等；中游實施詐騙或開設賭場等網絡犯罪；下游利用電子支付平台“洗白”資金。

（三）傳統犯罪的網絡化趨勢

網絡技術的高速發展深刻影響着社會發展，與此同時，犯罪活動日益向網絡空間滋生蔓延，為國家安全、經濟發展和社會穩定帶來新一輪挑戰。近年，除了個別偶發性的侵害人身案件外，傳統上既有的案件類型，均已滲進各種網絡元素。網絡詐騙、網絡賭博案件持續高發，網絡犯罪黑產業生態圈逐步形成並持續發展等，已經成為執法部門當下犯罪風險管控，以至整個社會治理所面臨的突出問題。

1. 中國的相關情況

根據我國最高人民檢察院統計數據顯示，於2020年，全國檢察機關起訴涉嫌網絡犯罪（包括利用網絡實施的犯罪及其上下游關聯犯罪）14.2萬人，同比上升47.9%。數據顯示，網絡詐騙、網絡賭博成為網絡犯罪主要類型，於2020年已佔網絡犯罪總數的64.4%。網絡詐騙犯罪具有非接觸特性，例如新冠肺炎疫情期間部份市民或欲購口罩無從、或遭遇裁員打擊，犯罪份子便利用受害人渴求防疫物品或求職心切而實施犯罪；有些犯罪集團藉開發境外賭場或賭博網站，誘使內地居民參與非法博彩，致使網絡賭博及相關的犯罪大幅增多。

此外，網絡犯罪集團化、跨境化的特徵相對突出。犯罪份子在網絡黑產業的“支援”下，已逐漸告別“單兵作戰”的模式，更多以團伙或集團形式作案，佔全國網絡犯罪的涉嫌人總數的83%。另外，不少犯罪份子為逃避監管打擊，將犯罪窩點、通訊工具等向境外轉移，有目的性地針對我國公民實施跨境網絡犯罪，網絡犯罪中跨境實施佔13%；當中，暗網和境外通訊軟件在網絡犯罪中的應用亦明顯增多。

2. 澳門的相關情況

2019年，澳門的出入境總人數和旅客量再創新高，各出入境口岸共錄得1.94億人次，入境旅客超過3,940萬人次，進一步確立澳門作為“世界旅遊休閒中心”的地位。澳門每天接待來自世界各地的大量旅客，亦面臨着複雜多變的犯罪新型態。

2019年11月25日，澳門保安司司長黃少澤舉行治安簡報會，介紹2019年首三季的罪

案統計及執法數字。據統計資料顯示，本澳電腦犯罪案件錄得較為明顯的升幅，更首次出現不法份子運用GoIP網絡電話設備[4]實施跨境詐騙的新模式，反映出傳統犯罪網絡化的形勢與全國趨向一致，澳門成為犯罪份子設立犯罪窩點、轉移通訊工具的目的地之一。

2019年5月，澳門司法警察局聯同珠海市公安局，首次破獲以住宅單位用作發出詐騙電話的傳輸“窩點”，並拘捕一名來自台灣地區的詐騙集團骨幹成員。犯罪集團利用珠澳兩地地理位置毗鄰，可以接收到內地電訊網絡訊號的特點，利用內地智能電話卡和設備，在外地透過電腦遠端操作，通過互聯網轉換和傳輸，最後透過澳門“窩點”發出訊號，營造出詐騙電話在內地撥出的假象，誤導警方調查方向。

該詐騙犯罪集團以台灣地區居民為骨幹成員，且分工細密，透過設置在外地的網絡電話伺服器，將VoIP語音[5]轉入互聯網，由互聯網接入澳門兩個“窩點”內的GoIP網絡電話設備，將一些數碼訊號轉變成語音訊號，再經過流動電話提供者撥打詐騙電話尋找詐騙目標。在現時技術層面，犯罪集團更無須在GoIP語音網關設備插入智能電話卡，有關傳輸設備也能運作，其隱蔽化及跨區域的特性，進一步增加執法部門調查取證的難度。

（四）新型網絡犯罪的“落地”趨勢

隨着經濟全球化程度的加深，跨境網絡犯罪亦日漸猖獗，近年不法份子針對電腦資訊系統的攻擊從未間斷，網域名稱系統（Domain Name System，簡稱DNS）作為互聯網的關鍵基礎資源，長期面臨分散式拒絕服務攻擊（Distributed Denial of Service，簡稱DDoS）、緩存中毒、中間人攻擊等形式的安全威脅。

近年，市民大眾使用智能手機接入互聯網的比率不斷提高，智能手機作為可隨身攜帶的“移動電腦”，絕大多數使用者會在手機上進行與金錢有關的操作或處理敏感性數據，但一般市民對手機的防護安全意識薄弱，往往沒有為手機安裝適當的防毒軟件，促使不法份子頻繁地透過通訊軟件或手機應用程式，進行釣魚攻擊、遠端存取攻擊、魚叉式釣魚、惡意軟件等網絡攻擊，當中大多與不安全的網絡連結瀏覽有關，為新型網絡犯罪提供“落地”至線下的機會。

根據第43次《中國互聯網絡發展狀況統計報告》指出，中國內地於2018年的網絡安全事件報告累計多達十萬宗，較2017年增加3.1%，互聯網平均每秒就會誕生四個新的惡意軟件，全國77%組織至少經歷過一次基於DNS的網絡攻擊，有23%的DNS網絡攻擊會對目標群組織的聲譽產生明顯影響。

據360互聯網安全中心發表的《2018年網絡詐騙趨勢研究報告》指出，中國內地於2014年至2018年期間所攔截的釣魚網站多達4,500萬個，透過調研和分析後，發現境外彩票類釣魚網站為第一大釣魚網站類型。由於釣魚網站平均只會存在四至五個小時，而被釣魚的用戶亦只有17%會報告相關攻擊，反映新型網絡犯罪已趨向常態化發展，釣魚攻擊依舊被視為最易成功、犯罪風險成本較低的攻擊方式之一。該份報告預測，由於暗網上不斷湧現新的釣魚攻擊方式，於2020年會出現高級釣魚攻擊工具包，利用這些工具包，即使只具備最基本的電腦知識的人也能夠進行釣魚攻擊，釣魚攻擊的危險性及影響程度將會與日俱增。

公安部第三研究所網絡安全法律研究中心與百度於2019年12月13日聯合發表《2019年網絡犯罪治理防範白皮書》，指出2018年每分鐘因網絡犯罪導致的經濟損失高達290萬美元，顯示全球網絡黑產的總體規模極為龐大（詳見圖三）。

三、歐洲聯盟的跨境電子取證措施

隨着大數據時代到來，運用大數據進行的偵查措施已成為執法部門偵查案件的利器，單一地區的電子數據實在難以滿足大數據對海量數據的要求，擴大跨境電子取證的適用範圍可謂大勢所趨，如何在保障公眾隱私及企業合法權益等前提下，平衡偵查的需要，亦不損害網絡服務提供者的基本權益，從而遏止犯罪行為網絡化，成為世界各地執法部門亟待解決的問題。

圖三：2018年全球網絡黑產總體規模

近年，歐洲聯盟在充分考慮公民的基本權利下，透過制訂適當的保護措施及監管機制，使跨境電子取證的發展能夠有序進行，此做法對於內地與澳門執法部門在解決相應問題方面起到示範作用。

（一）保障個人數據的國際趨勢

大數據涉及的全面監察措施會干預公民的基本權利，例如：隱私權、資訊自決權、資訊科技權、秘密通訊自由和一般行為自由；引申而言，相關的寒蟬效應[6]還會干預公民的宗教自由、集會遊行自由、居住遷徙自由等其他基本權利。

因此，為防止偵查機關濫權，各國均就個人數據的保護政策先後進行立法或修例，從而有效平衡憲法對公民基本權利的保障和偵查部門對犯罪偵查的需要。據騰訊研究院專家王融等人在《迷霧中的新航向——2018年數據保護政策年度觀察》中的歸納分析，2018年數據保護政策時間軸如表二所示：

2018年5月，歐盟生效的《通用數據保護條例》（下稱GDPR），被稱為史上最嚴格的國家數據保護法，直接適用於所有歐盟成員國，各成員國須自行修訂國內法，並使之與GDPR保持一致。GDPR給予歐盟用戶權力去掌控、得知自己的網絡數據如何被搜集、使用與儲存，並要求網絡公司須清楚告知用戶，自己使用用戶個資的方式與目的，用戶也可以直接要求網絡公司修正不正確的個人資訊，網絡公司也得負責用戶個人資訊的儲存安全。

GDPR本身還處於探索塑造期，需要大量解釋和細則予以澄清。截至2018年，歐盟數據保護機構EDPB已發佈共20項、約15萬字的指南，以回應各方關切的問題，指南涉及的項目包括：數據保護官、數據保護影響評估、識別主導監管機構、行政處罰、充分保護認定、有約束力的公司規定（BCR）的基本原則等，監管內容十分廣泛。

（二）《歐盟數據提交令》及《歐盟數據保存令》概述

近年，歐盟刑事取證的司法合作已經成為

表二：2018年全球數據保護政策時間軸

3月	美國總統特朗普簽署《澄清合法使用海外數據法》（CLOUD法案）；歐盟隨即提出《歐盟數據提交令》和《歐盟數據保存令》立法計劃。
5月	歐盟《通用數據保護條例》（GDPR）經過兩年準備期後落實執行。
8月	中國《電子商務法》頒佈，對於“數據殺熟[7]”問題也首次嘗試做出回應。
9月	中國《民法典》各分編公佈草案，其中《人格權編》系統加強有關隱私權與個人資訊保護的條文。
10月	歐洲議會通過《非個人數據在歐盟境內自由流動框架條例》，旨在廢除歐盟各成員國的數據本地化要求，釋放非個人數據經濟潛能。
11月	澳大利亞和台灣地區加入亞太跨境隱私規則機制（CBPRs）。在APEC的21個經濟體中，包括美國、日本、加拿大、韓國、新加坡等八個經濟體加入CBPR體系，代表着美國主導下的以自律為主的數據跨境流動機制取得實質進展。
12月	澳大利亞政府通過備受爭議的《加密法案》，強制要求科技公司在訪問加密資訊時提供三種層級的“協助”，預示着加密數據領域安全將面臨前所未有的立法衝擊。

跨境刑事司法合作領域中一大研究熱點。從理論層面而言，歐盟刑事司法合作由傳統的相互協助機制逐步過渡到相互承認原則，能夠更加適應快速打擊跨國犯罪的需要。

2018年4月，歐盟委員會宣佈計劃制訂《歐盟數據提交令》（European Production Order）和《歐盟數據保存令》（European Preservation Order），兩項法令均著眼於跨境電子取證的重要制度。需要注意的是，歐盟官方表示作為該法義務主體的“服務”，並不要求在歐盟境內設立機構，即使未在歐盟境內設立機構，但向歐盟境內提供相關服務的，也將受該法的約束。

該法令的主要內容包括針對電子取證的特點加速刑事司法協助、在歐盟整體層面完善並規範跨境遠端取證制度、增進與服務提供者自願合作的同時轉向跨境數據的強制披露等三方面，相關細節如下：

1. 建立《歐盟數據提交令》制度

歐盟成員國的執法或司法當局可直接向在歐盟境內的服務提供者請求提交電子證據，無論數據存儲地位於歐盟境內還是境外。同時，提交令亦要求服務提供者必須在10天內對數據提交令作出回應；在緊急情況下，服務提供者在6小時內須做出回應。

2. 建立《歐盟數據保存令》制度

歐盟成員國的執法或司法當局可強制要求歐盟境內的服務提供者保存特定數據，以便主管當局能夠獲取該數據。

3. 指定法定代表措施

歐盟委員會要求服務提供者在歐盟境內指定一名法定代表，以負責接收、遵守和執行成員國主管當局為收集刑事訴訟中的證據而發佈的決定和命令。

4. 保障和補救措施

歐盟委員會將規定《歐盟數據提交令》和《歐盟數據保存令》只能在刑事訴訟框架內發佈，並受到所有刑事訴訟程序的保障。

5. 提交數據類型

服務提供者應執法或司法機關的要求可能需提交的數據類型包括使用者數據、訪問數據、業務數據等非內容數據及內容數據，具體規則如表三所示。

綜觀上述條文內容，歐盟並不要求在歐盟境內設立機構，至於那些未在歐盟境內設立機構、但向歐盟境內提供相關服務的，也會受該法的管轄。我國作為數據大國，數據總量於2020年預計將達到8,060個EB，佔全球數據總量的18%，相關法令勢必對我國帶來影響。

表三：服務提供者應提交的數據類型及具體規則[8]

數據類型	定義	獲取規則
用戶數據（Subscriber data）	用於識別用戶的數據，例如姓名、出生日期、郵寄地址、帳單、付款數據、電話號碼或電子郵件地址。	A國的檢察官／法官（Prosecutor/judge）可以直接要求B國的服務提供者或其法定代表提供電子證據。 如果請求來自警方，則警方在向服務提供者或其法定代表發佈執法要求之前，須獲得A國檢察官或法官已批准的命令。
訪問數據（Access data）	數據本身不能識別用戶，但對於識別是必要的，包括用戶訪問服務的數據。例如使用日期、登錄和注銷服務時間以及IP地址。	A國的檢察官／法官可以直接要求B國的服務提供者或其法定代表提供電子證據。 如果請求來自警方，則警方在向服務提供者或其法定代表發佈執法要求之前，須獲得A國檢察官或法官已批准的命令。
企業數據（Transactional data）	與服務提供有關的數據，例如信息的來源和目的地，與設備位置、日期、持續時間、格式、使用的協議、壓縮類型等相關的數據。	A國的法官可以直接要求B國的服務提供者或其法定代表提供電子證據。 如果請求來自警方或檢察官，則其在向服務提供者或其法定代表發佈執法要求之前，須獲得A國法官已批准的命令。
內容數據（Content data）	用戶訪問數據或企業數據以外的，利用數字格式存儲的任何數據，例如文本、語音、視頻、圖像和聲音。	A國的法官可以直接要求B國的服務提供者或其法定代表提供電子證據。 如果請求來自警方或檢察官，則其在向服務提供者或其法定代表發佈執法要求之前，須獲得A國法官已批准的命令。

（三）歐盟數據的跨國、跨域存儲的概況

隨着雲計算技術的飛速發展，相當部份電子數據實際上是存儲於境外的。即使犯罪行為本身並不涉及境外因素，但由於特定數據存儲於境外，導致刑事調查取證工作出現跨越國境的情況。網絡服務提供者的數據對偵查工作起關鍵作用，若不加以有效規範，警方電子取證工作將受到極大限制。

據網絡科技雜誌《Tech Orange》報道，現時世界上最流行的網絡通訊軟件WhatsApp及FB Messenger，均由臉書（Facebook）所持有。臉書在全球共有14座數據中心，經常用戶達22.3億，當中有多達40%位於亞洲，也是成長速度最快的市場。因此，臉書於2018年9月宣佈將投資超過10億美元，在新加坡建立首個亞洲數據中心，預計於2022年開始營運。另外，臉書在美國、愛爾蘭和瑞典皆擁有多個數據中心，並且正在丹麥建設另一個設備中心，科技巨擘壟斷海量數據的優勢越發明顯。

以歐盟為例，愛爾蘭被譽為歐洲數據中心，美國的微軟、臉書、谷歌、蘋果等科技巨擘的歐洲總部都設於該國；WhatsApp在美國建有龐大的數據中心，同時因應業務發展需要，亦在愛爾蘭設立歐洲總部數據中心。愛爾蘭憲法明文規定，對通訊服務商而言，電子數據監控附加的行為協助義務和設備設置義務，不會干預其營業自由權和財產權。由此觀之，數據儲存的伺服器所在地法律，往往成為能否順利開展刑事司法協助的關鍵。

歐盟成員國眾多，各國之間的刑事司法合作從傳統的刑事互助請求方式，逐步發展到《歐盟數據提交令》和《歐盟數據保存令》等域外刑事取證方式，體現了通過法治化的刑事司法合作理念來實現歐盟建立“自由、安全與司法的區域”的目標，也體現了實現歐盟“刑事一體化”的理念。統一的域外刑事取證機制的形成將會彌補不同成員國之間法律體系的差別，進一步推動歐盟刑事司法合作向縱深方向發展。因此，準確把握當前歐盟在刑事取證司法合作領域的發展動向，對於完善我國的刑事司法合作制度建設具有積極意義。

四、珠澳兩地共同簽訂大灣區數據自由流動框架協議的構想

2019年2月，中共中央、國務院印發《粵港澳大灣區發展規劃綱要》，表明“合理運用經濟特區立法權，加快構建適應開放型經濟發展的法律體系，加強深港司法合作交流”。粵港澳大灣區是我國開放程度最高、經濟活力最強的區域之一，在國家發展大局中具有重要戰略地位。建設粵港澳大灣區，既是新時代推動形成全面開放新格局的新嘗試，也是推動“一國兩制”事業發展的新實踐。隨着粵港澳大灣區的進一步融合，人員的自由流動在帶來經濟發展的同時，令打擊跨國犯罪活動的難度也不斷加大，與歐盟的情況不謀而合。

借鑑《歐盟數據提交令》和《歐盟數據保存令》制度的經驗，珠澳兩地應考慮構建以“相互承認原則”為基礎的區域刑事司法合作機制，作為粵港澳大灣區區域刑事司法合作的先行者，共同簽訂“大灣區數據自由流動框架協議”，並透過本地立法工作，構建快捷跨境取證協作機制。

（一）中國刑事司法合作制度概述

2018年10月，第十三屆全國人民代表大會常務委員會第六次會議通過《中華人民共和國國際刑事司法協助法》，標誌着我國在國際刑事司法合作制度建設方面邁出了重要一步。《中華人民共和國刑事訴訟法》關於刑事司法協助的原則僅見第十七條，具體條文為“根據中華人民共和國締結或者參加的國際條約，或者按照互惠原則，我國司法機關和外國司法機關可以相互請求刑事司法協助。”《中華人民共和國國際刑事司法協助法》第三條也指出：“執行外國提出的刑事司法協助請求，適用本法、刑事訴訟法及其他相關法律的規定。”然而，有關刑事司法合作的規定方面，兩者是一般法與特別法的關係，《中華人民共和國刑事訴訟法》作為上位法，應當設置專章對刑事司法合作的原則、內容、具體措施等細化規定，並適度引入人權保障原則、一事不再理原則、雙重犯罪原則等內容，讓我國的刑事司法合作進程逐漸步入規範化軌道。

在區域刑事司法合作方面，《中華人民共和國國際刑事司法協助法》尚未包含區域刑事司法合作的內容，亦未訂定對外刑事司法合作中國家和各個法域相互之間的關係處理，導致我國的區域刑事司法合作仍然欠缺規範化。現時，珠澳兩地的刑事調查取證工作，主要通過執法或司法機關之間的個案協查、情報交流及聯絡機制等方式進行，呈現出調查取證效率未能配合調查進度，數據欠缺全面性等不足之處。

（二）刑事司法協助對跨境電子取證工作的影響

根據傳統國際法原則，刑事管轄都是以屬地原則作為最為基本的依據。由於刑事管轄乃是國家主權的重要體現，因此一旦跨越國境施展包括偵查在內的刑事司法活動，原則上都屬於侵犯他國主權的表現。同理，從傳統的國際法框架出發，根據數據的物理存儲位置進行管轄，突出的優點就在於尊重國家主權。因此，為免在傳統的國際法框架下侵犯他國主權，各國慣常的做法仍是需要通過刑事司法協助機制收集存儲於境外的電子數據。

然而，這種機制發展至今已經表現出很多的問題，例如被請求方可能持漠不關心的態度，又或雙方的法律制度不同而導致程序十分複雜且漫長，以歐盟國家通過司法協助程序向美國司法部請求收集電子數據為例，即使協助流程順利開展亦需要大約十個月時間方能完成，這種情況與追求調查取證效率的偵查工作實為背道而馳。更為棘手的是，大多數的刑事司法協助請求事項，都會因為政治因素、不符合國際法上的“雙重犯罪原則”（Principle of Double Criminality）或不符合被請求國的相關法律，而經常遭到被請求國拒絕，這種冗長複雜的機制早已不適應數碼化時代電子取證的需要。

在相關背景下，由一國偵查機關單邊開展的跨境遠端取證及面向網絡服務提供者的跨境數據披露制度應運而生，希望以更快捷的方式取代刑事司法協助機制。

（三）“大灣區數據自由流動框架協議”的可行性方向

為確保“框架協議”切實可行，建議引入三階式的規管門檻，將數據提取的要求分級提高，分為註冊資料數據、通訊記錄數據和科技監控數據三大類，且必須具備正當、充足的理據，譬如請求地區必須在當地已開立刑事卷宗，偵查案件的關鍵電子證據被儲存在被請求地區等，作為數據移交的必要條件（詳見圖四）。

與此同時，建議粵港澳大灣區各個執法部門共同構建用於發佈和數據交換的加密平台，透過法官審查形式要件後，如果符合相關法律規定，不存在法律規定所拒絕執行的事由，就應當指令當地的網絡服務提供者配合請求地執法部門開展跨境遠端取證工作，從而快速有效地獲取刑事電子證據，並充分發揮先行先試作用，逐步推廣至全國，以至全球各國，讓跨境刑事司法合作機制在符合法律規定下有序發展。

圖四：“大灣區數據自由流動框架協議”訂定的數據規管門檻

（四）以智慧警務理念落實大數據偵查的未來展望

2017年12月8日，中共中央政治局就實施國家大數據戰略進行第二次集體學習，習近平總書記在主持學習時強調，“以數據集中和共享為途徑，推動技術融合、業務融合、數據融合，打通信息壁壘，形成覆蓋全國、統籌利用、統一接入的數據共享大平台，構建全國信息資源分享體系，實現跨層級、跨地域、跨系統、跨部門、跨業務的協同管理和服務。要充分利用大數據平台，綜合分析風險因素，提高對風險因素的感知、預測、防範能力”[9]，一針見血地指出了數據一體化建設已成為未來社會安全和經濟發展的重要基礎。

展望未來，本澳與各個城市、以至區域落實“數據自由流動框架協議”後，區域警務合作可透過建立類似現時廣東省“全省打擊治理電信網絡新型違法犯罪工作聯席會議制度”的方式，組織各地網絡營運商及科技公司建立線索輸出機制，對涉案資訊進行梳理，並匯入共同構建用於數據交換的加密平台，從而有效運用跨行業、跨區域的大數據資源，實現警務數據互聯互通、實時共用的願景。結合大數據偵查的智慧警務概念，對大數據的內涵、特徵、思維方式、技術方法進行歸納和總結，將進一步推進快捷跨境取證的建設工作，達至事後偵查導向事前偵查轉型，被動偵查導向主動偵查轉型，單線偵查導向協作式偵查轉型，粗放式偵查導向集約式偵查轉型。

註：

1. 中國內地和澳門特區對於“公共關鍵基礎設施”的概念有所不同。在中國內地，根據《關鍵信息基礎設施安全保護條例（徵求意見稿）》第三章關鍵信息基礎設施範圍第十八條規定：“下列單位運行、管理的網路設施和信息系統，一旦遭到破壞、喪失功能或者資料洩露，可能嚴重危害國家安全、國計民生、公共利益的，應當納入關鍵信息基礎設施保護範圍：（一）政府機關和能源、金融、交通、水利、衛生醫療、教育、社保、環境保護、公用事業等行業領域的單位；（二）電信網、廣播電視網、互聯網等信息網絡，以及提供雲計算、大數據和其他大型公共信息網絡服務的單位；（三）國防科工、大型裝備、化工、食品藥品等行業領域科研生產單位；（四）廣播電台、電視台、通訊社等新聞單位；（五）其他重點單位。”在澳門方面，根據第13/2019號法律《網絡安全法》第二條第一款（三）項規定，關鍵基礎設施是指對社會正常運作具有重要意義，且一旦遭到擾亂、破壞、數據資料洩漏、停止運作或效能大幅降低，可能嚴重危害社會福祉、公共安全、公共秩序或其他尤為重要的公共利益的資產、資訊網絡和電腦系統。
2. 圖片源自YouTube頻道“Captain Gizmo”影片“Most Popular Instant Messengers 1995–2020”，2020年5月5日，＜https://www.youtube.com/watch?v=yJ3TTV0Il4o＞。
3. 手機網民指於過去六個月內曾使用手機接入互聯網的滿六周歲或以上的居民。
4. GoIP網絡設備是一種用於連接電訊營運商訊號與互聯網位址的通訊工具。
5. VoIP（Voice over Internet Protocol）指透過互聯網傳送的語音訊號。
6. 寒蟬效應（Chilling Effect）是法律用語，是指當下對言論自由的“阻嚇作用”——即使是法律沒有明確禁止的。
7. 數據殺熟：同樣的商品或服務，老客戶看到的價格反而比新客戶要貴出許多的現象。
8. 公安部第三研究所網絡安全法律研究中心：〈歐盟醞釀電子證據跨境獲取新規則〉，《安全內參》，2018年4月18日，＜https://www.secrss.com/articles/2368＞。
9. 〈習近平主持中共中央政治局第二次集體學習並講話〉，《中華人民共和國中央人民政府》，2017年12月9日，＜http://www.gov.cn/xinwen/2017-12/09/content_5245520.htm＞。

參考資料：

1. 王燃：《大數據偵查》，清華大學出版社，2018年。
2. 國家互聯網信息辦公室：《關鍵信息基礎設施安全保護條例（徵求意見稿）》，2017年7月10日。
3. 澳門特別行政區第13/2019號法律《網絡安全法》。
4. YouTube頻道“Captain Gizmo”影片“Most Popular Instant Messengers 1995–2020”，2020年5月5日，＜https://www.youtube.com/watch?v=yJ3TTV0Il4o＞。
5. 〈最新網際網路研究報告 這國家平均每天上網超過10小時〉，《XFastest》，2019年1月31日，＜https://news.xfastest.com/others/58695/worldwide-internet-report/＞。
6. Statistics of Internet users(2005-2019), The International Telecommunication Union (ITU), 18-01-2021, ＜https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx＞.
7. 中國互聯網絡信息中心：第43次《中國互聯網絡發展狀況統計報告》，2019年2月28日。
8. 澳門互聯網研究學會：《澳門居民互聯網使用趨勢報告2018》，2018年6月。
9. 360互聯網安全中心：《2018年網絡詐騙趨勢研究報告》，2019年1月15日。
10. 〈本局與內地警方聯手偵破電話詐騙集團 拘一名骨幹成員〉，《司法警察局》，2019年5月6日，＜https://www.pj.gov.mo/Web//Policia/201905/20190507/8704.html＞。
11. 公安部第三研究所網絡安全法律研究中心、百度：《2019年網絡犯罪治理防範白皮書》，2019年12月13日。
12. 最高人民檢察院：〈最高檢披露2020年國內網絡犯罪大數據〉，《安全內參》，2021年4月7日，＜https://www.secrss.com/articles/30331＞。
13. 梁坤：〈歐盟跨境快捷電子取證制度的發展動向及其啟示〉，《中國人民公安大學學報（社會科學版）》，2019年第1期。
14. 吳夢：《歐盟偵查令制度研究》，山東大學法律碩士學位論文，2018年。
15. 薛大政：《非內容性電子數據監控與基本權利保護研究》，天津商業大學憲法學與行政法學碩士學位論文，2018年。
16. 王融：〈迷霧中的新航向——2018年數據保護政策年度觀察〉，《搜狐》，2018年12月29日，＜http://www.sohu.com/a/285519767_455313＞。
17. 梁根林：〈傳統犯罪網絡化：歸責障礙、刑法應對與教義限縮〉，《法學》，2017第2期。
18. 公安部第三研究所網絡安全法律研究中心：〈歐盟醞釀電子證據跨境獲取新規則〉，《安全內參》，2018年4月18日，＜https://www.secrss.com/articles/2368＞。
19. 〈臉書首個亞洲數據中心放棄設點台灣，改砸300億台幣投資新加坡〉，《Tech Orange》，2018年9月7日，＜https://buzzorange.com/techorange/2018/09/07/fb-singapore/＞。
20. 李泓澤：〈“互聯網+”環境下網絡犯罪形勢及防範機制研究〉，《河北公安警察職業學院學報》，2019年第1期。
21. 賽博研究院：〈歐洲政策研究中心報告：歐盟刑事事項和電子IT數據司法合作手冊〉，《安全內參》，2020年4月15日，＜https://www.secrss.com/articles/18674＞。
22. 〈習近平主持中共中央政治局第二次集體學習並講話〉，《中華人民共和國中央人民政府》，2017年12月9日，＜http://www.gov.cn/xinwen/2017-12/09/content_5245520.htm＞。