澳門刑事電子數據的留存、通訊截取與在線搜索制度研究——基於對歐盟法和德國法的考察

李哲　羅伯特・埃塞爾（Robert Esser）　歐陽楚欣

[摘　要] 澳門第 10/2022 號法律《通訊截取及保障法律制度》確立了通訊紀錄的數據留存及調取機制，並以通訊截取制度取代了原有的電話監聽制度，回應了網絡時代調取電子數據的需求。然而，該制度仍面臨諸多挑戰，包括數據留存制度的合法性質疑、加密通訊難以截取、跨境數據獲取的困難，以及雲端數據和網絡服務提供商處理的電子數據難以調取等問題。為應對這些挑戰，澳門可以借鑑歐盟和德國的經驗，重構通訊紀錄數據留存的程序，優化數據調取與權利保障機制，並增加來源端截取及在線搜索等偵查措施。在遵守比例原則及保障隱私權和數據權等基本權利的前提下，應進一步完善澳門有關電子數據保全及秘密獲取的相關規定。

[關鍵詞] 通訊紀錄　數據留存　來源端截取　在線搜索

一、澳門刑事電子數據秘密獲取的新制度與尚待解決的問題

根據 1997 年生效的澳門《刑事訴訟法典》，電話監聽是秘密獲取通訊內容的唯一手段，但隨着通訊技術的發展，通訊模式發生了根本性的變化，網絡化通訊成為主流，[①]僅規定電話監聽顯然已經無法滿足獲取網絡時代數據化資訊的需求。因此，澳門第 10/2022 號法律《通訊截取及保障法律制度》，廢除了澳門《刑事訴訟法》第 172 條至第 175 條的“電話監聽”制度，規定了“通訊紀錄”、“通訊使用者資料”等不同形式的電子數據，將原有的電話監聽制度修改為通訊截取制度，並規定了通訊紀錄的數據留存制度及其後可能的調取程序。

澳門在秘密獲取通訊數據的新措施為刑事偵查機關獲取網絡化通訊數據提供了可能，但也引發了巨大的爭論。不加區分地留存所有通訊使用者的通訊紀錄長達一年，是否是刑事偵查的必然需要？是否有違比例原則並導致對隱私權與數據權的侵犯？此外，上述立法沒有完全回應刑事偵查實踐的新問題，諸如加密數據的通訊截取問題，以及如何解決大多

作者簡介：李哲，澳門大學法學院副教授、博士；羅伯特·埃塞爾（Robert Esser），德國帕紹大學德國法、歐洲法和國際刑法講座教授（Chair of German, European and International Criminal Law, University of Passau）、博士；歐陽楚欣，澳門大學法學院博士研究生。

[①]澳門特別行政區政府《通訊截取及保障法律制度》公開諮詢，https://www2.fsm.gov.mo/ch/rjipc/qa.aspx，2024 年 8 月 5 日讀取。

數網絡服務提供商不在澳門境內所帶來的電子數據取證困難的問題等。

電子數據的留存與獲取，是近些年歐洲法院及歐陸各國的熱點問題。德國國內法在歐洲法院及歐洲人權法院諸多判例的影響下，對其電子數據留存制度，加密即時通訊的獲取制度，以及通過木馬程式進入被偵查對象的電腦系統以獲取電子數據的在線搜索制度等，作出了規定及修改，對我們探討澳門相關問題的解決提供了最新經驗與完善思路。本文將基於澳門的實際，結合在秘密獲取通訊數據領域經驗更為豐富的歐盟與德國的相關規定，分析澳門現行法中數據留存和通訊截取制度存在的主要問題，以期提出符合澳門電子數據體系的通訊截取、數據留存及在線搜索等秘密獲取刑事電子數據方式的完善方向。

二、數據留存與調取通訊紀錄

根據澳門《通訊截取及保護法律制度》第 9 條，數據留存是指電信營運者或網絡服務提供者應當在法律要求的範圍內，留存用戶在使用其服務過程中所產生的通訊紀錄。該措施從本質上屬於證據的保全措施，刑事偵查機關無權直接調取該被留存的數據。在刑事案件偵查過程中，需要依據法律規定的程序調取該被留存的通訊紀錄。為了確保刑事案件偵查的順利推進，尤其是那些需要通訊紀錄來確定行動軌跡、上網資訊及其他互聯網資訊的案件，數據留存作為一種保全性措施，是成功調取通訊紀錄的前提。

數據留存涉及所有使用通訊服務的主體，而不僅限於具有犯罪嫌疑的特定人，因此關係到公民隱私權和數據權等基本權利。那麼，是否可以長時間並且不加區分地留存所有通訊使用者的通訊紀錄呢？這一問題引發了廣泛的爭議。如果基於案件偵查的需要確實需要留存通訊紀錄，那麼留存的界限在哪裏？是否需要區分不同數據類型而適用不同的數據留存及調取程序，數據留存及其調取過程的事後權利保障及救濟如何構建，這些問題都需要進一步探討。

（一）澳門的數據留存制度及其爭議

澳門在 2022 年通過的《通訊截取及保障法律制度》中首次確立了數據留存制度，該法律第 9 條要求“電信營運者及網絡通訊服務提供者，須將於澳門特別行政區提供的通訊服務所產生的通訊紀錄或在外地向澳門特別行政區用戶提供通訊服務所產生的通訊紀錄，自完成通訊之日起計在澳門特別行政區至少保存一年；在該期間內須確保該等資料安全、保密和完整”。

數據留存是一種自動啟動的程序，只要在澳門特別行政區產生的通訊紀錄，包括電信號碼或其他呼叫識別標誌、通訊日期及時間、使用長度、互聯網協議地址、服務類型及電子信箱或位置資訊等通訊服務後所產生的各參與方的紀錄，電信營運者或網絡服務提供者就應當履行其數據留存義務，無需經過司法當局命令或通知被留存數據之所有人。

然而，該數據只是具有留存的屬性，並不能直接應用於刑事偵查。在某一具體刑事案

件的偵查過程中，如有理由相信通訊紀錄有助於刑事調查工作，有權司法當局可通過批示許可或命令調取電信營運商及網絡通訊服務提供者所留存的數據。當然，如果在情況危急時，刑事警察未經有權司法當局的預先許可亦可調取留存數據，但須在七十二小時內通知有權司法當局，否則該措施無效且刑事警察應當銷毀已獲得的留存數據。

2018 年 9 月，澳門特別行政區政府就《通訊截取及保障法律制度》展開公開諮詢，並首次公佈了數據留存的制度設想。這一制度是該法律草案中爭論最大的一個制度，數據留存這一方式的必要性、通訊紀錄的數據種類、數據留存的模式及調取通訊紀錄的程序是公眾重點關注的議題。根據公開諮詢的總結報告數據，涉及“保存義務”議題的意見有 119 條，其中，有 6.28% 的意見明確表明不贊成該制度，另有 27.23% 未有明確意見。[①]有人指出，澳門立法中不加區分，要求為期一年且全面留存數據的留存模式，加劇了對數據留存本身可能對隱私權和數據權等基本權利造成的侵害。[②]也有質疑者提出，澳門這一立法乃是參考葡萄牙第 32/2008 號法律（Lei n.º 32/2008）第 6 條，而該條法律的源頭 —— 歐盟第 2006/24/EC 號指令（Directive 2006/24/EC）已因侵犯隱私權和數據權被歐洲法院（European Court of Justice）認定無效。[③]德國科隆行政法院（Verwaltungsgericht Köln）[④]也認為，在德國不加區分地普遍保留通訊紀錄不符合歐洲法律的要求。[⑤]下文將結合歐盟的相關判決以及德國在歐盟判決基礎上的國內法演變，討論數據留存的必要性，並且在此基礎上進一步探討如何優化澳門數據留存及調取的相關制度。

（二）數據留存的必要性爭論

關於歐洲法院認定數據留存屬違法的判決，[⑥]澳門特區政府對此澄清稱，雖有數據留存屬違法的判決，但歐洲多國因偵查之需並未因此修法。[⑦]澳門特區政府表示上述解釋是歐洲法院在 2018 年作出的，自 2019 年開始，德國雖因為數據留存的人權爭議暫停了數據留存制度，[⑧]但到 2021 年通過了《電信與電子媒體資料與隱私保護法》（Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien, TTDSG），又重新啟動了強制數據留存的制度。

可以看出，是否可以在立法中確立數據留存制度問題，確實存在着巨大的爭議，在德國也經歷了從肯定到否定、再到部分肯定的過程。從歐盟第 2006/24/EC 號指令首次確立數

---

①澳門特別行政區政府司法警察局：〈《通訊截取及保障法律制度》公開諮詢總結報告〉，2019 年，頁 20－21，https://www2.fsm.gov.mo/ch/rjipc/pdf/relatorio_C2.pdf，2024 年 8 月 5 日讀取。

②〈立法表決通過犯罪類型擴至十二類　澳通訊截取法全世界最嚴〉，《澳門日報》（澳門），2022 年 7 月 23 日，版 A02。

③澳門特別行政區政府司法警察局：〈對《通訊截取及保障法律制度》保存通訊記錄的說明〉（新聞稿），2018 年 10 月 15 日，https://www2.fsm.gov.mo/ch/rjipc/pdf/20181015.pdf，2024 年 8 月 12 日讀取。

④科隆行政法院（Verwaltungsgericht Köln），2018 年 4 月 20 日判決，編號：9K3859/16；BeckRS2018, 9168。

⑤科隆行政法院（Verwaltungsgericht Köln），2018 年 4 月 20 日判決，編號：9K3859/16、BeckRS2018, 9168，頁 54；在此背景下還可參見 Rossnagel, Alexander. “Vorratsdatenspeicherung rechtling vor dem Aus? ” *Neue Juristische Wochenschrift,* vol. 70, no. 10, 2017, pp. 696-698.

⑥歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12。

⑦澳門特別行政區政府司法警察局：〈對《通訊截取及保障法律制度》保存通訊記錄的說明〉（新聞稿），2018 年 10 月 15 日，https://www2.fsm.gov.mo/ch/rjipc/pdf/20181015.pdf，2024 年 8 月 12 日讀取。

⑧德國聯邦行政法院（Bundesverwaltungsgericht），2019 年 9 月 25 日判決，編號：Urt.v.25.9.2019。

據留存制度，到德國一度擱置後，又在區分數據種類的前提下，縮短了留存時間，進一步限制了數據留存，數據留存的存立幾經波折。

歐盟第 2006/24/EC 號指令規定成員國應當規定管轄境內的公共電信提供商或公共網絡通訊提供商保留在通訊服務過程中產生的數據。[①]但在 2014 年，歐洲法院認為數據留存構成了對《歐盟基本權利憲章》（The Charter of Fundamental Rights of the European Union）第 7 條和第 8 條有關隱私權與數據權規定的特別嚴重侵犯。[②]法院在具體陳述中指出，第 2006/24/EC 號指令“超出了根據《歐盟基本權利憲章憲章》第 7、8[③]和 52(1) 條遵守相稱性原則所施加的限制”，[④]可能會使有關人員感到自己的私生活受到持續監視。[⑤]且由於該指令涉及範圍廣泛，可以保留所有類型的通訊紀錄，還適用於“沒有證據表明其行為可能與嚴重犯罪……有關”的人，[⑥]因此幾乎所有歐洲人的基本權利都將受到干涉。[⑦]

德國憲法法院（Bundesverfassungsgericht, BVerfG）自 2007 年在國內法引入數據留存制度開始，就收到了約 34,000 起相關的憲法申訴，[⑧]德國憲法法院更是在歐洲法院之前，就作出了數據留存違反《德國基本法》（*Grundgesetz*）的判決，法院在 2010 年 3 月 2 日的判決中指出，德國《刑事訴訟法典》第 100g 條第 1 款第 1 句、第 113a 和第 113b 條中收集留存數據的規定違反了《德國基本法》第 10 條關於確保通訊、郵件和電信隱私權的規定。[⑨]

德國北萊茵－威斯特法倫州高等行政法院（The Higher Administrative Court of North Rhine-Westphalia）在其 2017 年 6 月 22 日的臨時裁決中同樣指出，[⑩]德國《電信法》（Telekommunikationsgesetz, TKG）中關於強制存儲數據的法律不符合歐洲法院的判例，[⑪]

---

① “Directive 2006/24/EC of the European Parliament and of the Coucil of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC.” *Offical Journal of the European Union*, 13 Apr 2006, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, accessed 30 Aug 2024.

② 歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 37、69；Wolff, Heinrich Amadeus. “Anmerkung zum Urteil des EuGH vom 08.04.2014 zur Vorratsdatenspeicherung.” *Die öffentliche Verwaltung*, vom. 8, Apr 2014, pp. 608-612.

③ 歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12，頁 28；C-594/1215，頁 69、70。

④ 歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 69；Wolff, Heinrich Amadeus. “Anmerkung zum Urteil des EuGH vom 08.04.2014 zur Vorratsdatenspeicherung.” *Die öffentliche Verwaltung*, vom. 8, Apr 2014, pp. 608-612.

⑤ 歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 37；另見 Mansoor, Koshan. “Vorratsdatenspeicherung - verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung.” *Datenschutz und Datensicherheit,* vol. 40, Feb 2016, pp. 167-171.

⑥ 歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 58。

⑦ 歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 56。

⑧ Oehmichen, Anna, and Christina Mickler. “Christina Die Vorratsdatenspeicherung - Eine Never Ending Story?” *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht*, Jun 2017, pp. 298-299; Roßnagel, Alexander. “Die neue Vorratsdatenspeicherung.” *Neue Juristische Wochenschrift*, vol. 69, no. 8, 2016, pp. 533-534.

⑨ 德國憲法法院（Bundesverfassungsgericht），2010 年 3 月 2 日判決，編號：1BvR256/08; Rößner, Sören. “Vorratsdatenspeicherung in Deutschland - Ende des Umsetzungsdefizits in Sicht?” *Europäische Zeitschrift für Wirtschaftsrecht*, vol. 25, no. 4, 2014, pp. 134-138。

⑩ 北萊茵－威斯特法倫州高等行政法院（The Higher Administrative Court of North Rhine-Westphalia），2017 年 6 月 22 日判決，編號：13B238/17、NVwZ-RR2018，頁 43。

⑪ 北萊茵－威斯特法倫州高等行政法院（The Higher Administrative Court of North Rhine-Westphalia），2017 年 6 月 22 日判決，編號：13B238/17、NVwZ-RR2018，頁 43、45 及其後頁碼。

因此，在德國強制保留通訊紀錄違反了歐盟法律，必須暫停，直至具有法律約束力的主要訴訟程序結束。[①]德國政黨自由民主黨（Freie Demokratische Partei）還在 2017 年提交了一份廢除德國《刑事訴訟法典》和《電信法》中允許數據保留的相關條款的草案。[②] 2019 年 9 月 25 日，德國聯邦行政法院（Bundesverwaltungsgericht）請求歐洲法院作出初步裁決，以澄清德國《電信法》中的數據留存規定是否符合歐盟法律。[③]在此期間，德國暫停了強制數據留存。而在 2021 年，德國聯邦參議院為解決德國《電信法》、《電信媒體法》（Telemediengesetz, TMG）與《歐盟通用數據保護規則》（General Data Protection Regulation, GDPR）並行所致的適用困難，通過了《電信與電子媒體資料與隱私保護法》，以更好地保護網絡世界中的資料與隱私，平衡網絡服務使用者利益與公司經濟利益，並重新啟動了強制數據留存制度。

由此可見，雖然數據留存對隱私權與數據權的挑戰是不可迴避的，但德國在幾經搖擺後仍然選擇了數據留存制度。德國聯邦警察局（Bundeskriminalamt, BKA）時任局長霍爾格 • 明希（Holger Münch）指出，保留通訊數據對打擊犯罪發揮了重要作用，尤其是在調查兒童色情犯罪等嚴重犯罪方面。在一起案件中，由於保留了相應的通訊紀錄，當局能夠從 3,500 個使用德國 IP 地址的流覽器訪問中識別出幾乎所有的電話用戶。[④]在打擊和預防恐怖主義犯罪的過程中，位置數據留存為分析通訊過程的確切時間和移動電話的位置提供了可能。[⑤]因此，為提高破案率，數據留存顯然是必要的。[⑥]

歐洲法院在 2022 年 9 月 20 日作出的判決（C-793/19, 794/19 等）中確認，歐盟法律禁止普遍且不加區分地保留流量數據，除非在國家安全受到嚴重威脅時。然而，歐洲法院又在 2024 年 4 月 30 日（C-470/21）的裁決中放寬了留存 IP 地址的限制，即現在在歐盟，可以通過儲存 IP 地址以打擊各種的犯罪。

澳門特區政府就數據留存制度回應社會質詢時也強調，數據留存是刑事偵查的必要手段。數據的保存雖在過往立法中未有規定，但屬於電信業務者基於業務需要的慣常做法，新法並未變更原有留存的數據種類，只是明確規定了保存期限。[⑦]這一保存義務的目的是輔助刑事調查工作，以便有權限當局在有需要的時候可以查閱這些紀錄。數據留存對於維護特別重大的公共利益，如打擊犯罪和維護公共安全，是必要的、有用的和適當的。[⑧]

[①]北萊茵－威斯特法倫州高等行政法院（The Higher Administrative Court of North Rhine-Westphalia），2017 年 6 月 22 日判決，編號：13B238/17、NVwZ-RR2018，頁 43、54。

[②] Freie Demokratische Partei, Entwurf eines Gesetzes zur Stärkung der Bürgerrechte, BT-Drucks. 19/204, Dec 2017; Roßnagel, Alexander. “Erneute Diskussion um die Vorratsdatenspeicherung.” *Zeitschrift für Rechtspolitik*, vol. 51, no. 5, 2018, p. 125.

[③]德國聯邦行政法院（Bundesverwaltungsgericht），2019 年 9 月 25 日的判決，編號：Urt.v.25.9.2019。

[④] Münch, Holger. “Praktische Nutzung der Vorratsdatenspeicherung.” *Zeitschrift für Rechtspolitik,* vol. 48, no, 5, 2015, pp. 130-131.

[⑤] Münch, Holger. “Praktische Nutzung der Vorratsdatenspeicherung.” *Zeitschrift für Rechtspolitik,* vol. 48, no, 5, 2015, pp. 130-131.

[⑥] Münch, Holger. “Praktische Nutzung der Vorratsdatenspeicherung.” *Zeitschrift für Rechtspolitik,* vol. 48, no, 5, 2015, pp. 130-132.

[⑦]澳門特別行政區政府司法警察局：〈對《通訊截取及保障法律制度》保存通訊記錄的說明〉（新聞稿），2018 年 10 月 15 日，https://www2.fsm.gov.mo/ch/rjipc/pdf/20181015.pdf，2024 年 8 月 12 日讀取。

[⑧]澳門特別行政區政府《通訊截取及保障法律制度》公開諮詢，https://www2.fsm.gov.mo/ch/rjipc/qa.aspx，2024 年 8 月 5 日讀取。

實際上，歐洲法院與德國法院雖然都曾作出數據留存因嚴重干涉隱私權和數據權而違法的判決，但均是認定最初確立的、不加區分地全面留存這一留存模式屬於違法，並未完全否定數據留存這一制度本身的可行性。以下，本文將結合德國最新做法，具體分析澳門在數據留存的適當性、數據安全保障及調取通訊紀錄的規定是否符合比例原則的要求，以及應當如何進一步優化。

（三）基於比例原則的數據留存制度構建

既然數據留存對於偵查活動具有不可或缺的保全功能，而該制度的寬泛適用又極有可能牽涉甚至威脅、侵害公民的隱私權和數據權，該制度的設計就必須符合比例原則。考慮到數據留存的必要性、不可替代性，在數據留存制度的建構中須確保數據留存符合侵害與利益的相稱性、侵害最小原則與合目的性的要求。

澳門特區政府在立法會的細則性審議中指出，只有“不加區分地”保存澳門特別行政區所有使用者的通訊紀錄，通訊紀錄的保存才能發揮其效用，特別是考慮到在保存數據時尚無法判斷這些數據的可用性。因此，以籠統和不加區分的方式保存，這些數據才可能在犯罪發生後的偵查階段具有證據價值。[①]由此可見，澳門特區政府在立法之初就考慮過是否應當區分留存的問題，且在此問題上立場鮮明，認為出於偵查需要，必須不加區分地全面留存數據。

在這一問題上，歐洲法院的立場出現了前後矛盾，歐洲法院在 2016 年英格蘭與瑞典的 Tele2Sverige 和 Watson 案中認為數據留存應當區分進行，[②]強調規定普遍和不加區分地保留數據的國內法規已超出了嚴格必要的限度，但不應阻止成員國“通過立法，允許為作為打擊嚴重犯罪的目的的預防措施，有針對性地保留流量和位置數據，但在所保留數據的類別、受影響的通訊手段、相關人員和所採用的保留期限方面，必須限制在嚴格必要的範圍內”。[③]然而，歐洲法院在 2018 年的另一份判決書（C-207/16）中，與之前的判決持相反立場，認為不加區分地留存數據是合法的，在該判決中，法院認為在干擾並不嚴重的情況下，以預防、調查、偵查和起訴單純的刑事犯罪為目標，即可證明獲取數據是合理的。[④]在該判決中，涉案法院授權當局查閱電信營運商所保留的個人數據，用於識別 SIM 卡在 12 天內的所有者，但相關數據並不包括個人通訊內容，[⑤]當局無法收集到有關當事人的私人生活資訊，因此歐洲法院認為這種行為不會嚴重干涉數據相關者的基本權利。[⑥]

[①]澳門特別行政區政府《通訊截取及保障法律制度》公開諮詢，https://www2.fsm.gov.mo/ch/rjipc/qa.aspx，2024 年 6 月 18 日讀取。

[②]歐洲法院（European Court of Justice），2016 年 12 月 21 日判決，編號：C-203/15、C-698/15 - “Tele2Sverige 和 Watson”。

[③]歐洲法院（European Court of Justice），2016 年 12 月 21 日判決，編號：C-203/15、C-698/15，頁 108。

[④]歐洲法院（European Court of Justice），2018 年 10 月 2 日判決，編號：C-207/16（MinisterioFiscal），頁 56：“相比之下，當這種訪問所造成的干擾並不嚴重時，這種訪問能夠被預防、調查、偵查和起訴一般‘刑事犯罪’的目標所證明是合理的”。

[⑤]歐洲法院（European Court of Justice），2018 年 10 月 2 日判決，編號：C-207/16，頁 59。

[⑥]歐洲法院（European Court of Justice），2018 年 10 月 2 日判決，編號：C-207/16，頁 61。

德國在 2015 年通過《2015 年 12 月 10 日關於引入流量數據存儲義務和最長存儲期的法律》（Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten），[①]拋棄原定全面留存數據六個月的規定，區分數據類型留存並縮短了留存期限。修改後的數據留存制度區分了包含電信服務使用者終端設備位置的位置數據，與其他通訊紀錄兩種數據類型，並根據這兩種類型設立了不同的留存期限，規定電信服務提供者有義務將其他通訊紀錄保存長達十周，將位置數據保存四周，以便在檢察機關起訴“特別嚴重的刑事犯罪時”將其移交給檢察機關；或在個人健康、生命或自由面臨具體危險時，或在聯邦或其某個州的存在受到威脅時將其移交給預防機關。[②]在 2019 － 2021 年期間，因可能違反歐盟法律中對隱私權與數據權保障的要求，該法被德國聯邦行政法院決定暫時擱置。2021 年，德國通過制定《電信與電子媒體資料與隱私保護法》，基本重述了上述《2015 年 12 月 10 日關於引入流量數據存儲義務和最長存儲期的法律》所規定的數據留存模式，但是作出了非常細微的調整。

從歐洲法院及德國立法關於數據留存觀點的衝突與變化，可以看出，數據留存這種通訊紀錄的保全措施，是刑事偵查活動的重要證據來源，在各國的立法中都很難割捨。這也是澳門特區政府在回應有關數據留存制度的質詢時所持之立場。然而，還應當看到的是，數據留存應當遵循比例原則，區分不同數據類型的數據留存程序，並盡量縮短數據留存的期限。

根據澳門《通訊截取及保障法律制度》第 9 條，所有通訊數據的留存採用統一的程序，並沒有作出區分。通訊數據雖然都不涉及通訊的具體內容，但是不同類型的通訊數據對公民隱私權和數據權的影響仍然是不同的。例如，位置數據涉及更為敏感的隱私資訊，可能造成更大的隱私權侵犯。德國《電信法》第 176 條規定，位置數據只能留存四周，而其他通訊數據的留存時長為十周。為進一步確保數據留存的適當性，澳門應當調整數據留存的模式，根據數據的敏感度和對被調查對象個人隱私權與數據權影響的程度，區分位置數據與其他通訊紀錄的不同留存期限。特別地對位置數據這一類型設定較短的留存期限，在有效降低數據留存對隱私權干涉的同時，也兼顧了刑事偵查的需要。

此外，澳門目前的數據留存期限長達一年之久，也是值得商榷的。那麼，澳門是否應當借鑑德國的立法例子，規定位置數據的留存期限為四周，而其他通訊紀錄的留存期限為十周呢？本文認為，德國的規定時限與其在歐洲法院與德國法院等存在大量訴訟的情況有關。澳門地域細小，絕大多數的網絡服務提供商位於澳門境外，獲取電子證據的手段有限，過短的數據留存期限無法滿足澳門刑事偵查的需要。但是，數據相關權利人的隱私權與數據權也是需要考慮的重要因素。未來，澳門應當在堅持比例原則的基礎上，在區分不同數據類型的前提下，適當縮短留存期限。

[①] Schiedermair, Stephanie, Anna Mrozek. “Die Vorratsdatenspeicherung im Zahnräderwerk des europäischen Mehrebenensystems. ” *Die Öffentliche Verwaltung*, no. 3, Mar 2016, pp. 89-97.

[②] Schiedermair, Stephanie, Anna Mrozek. “Die Vorratsdatenspeicherung im Zahnräderwerk des europäischen Mehrebenensystems. ” *Die Öffentliche Verwaltung*, no. 3, Mar 2016, pp. 89-97; Mansoor, Koshan. “Vorratsdatenspeicherung - verfassungsrechtliche Rah-menbedingungen und rechtspolitische Verortung. ” *Datenschutz und Datensicherheit,* vol. 40, Feb 2016, pp. 167-171.

（四）留存數據的調取：條件、程序與數據刪除

數據留存作為一種保全措施，是為了滿足偵查中調取通訊紀錄的需要。沒有留存，就無法做到事後的調取。但是，在不加區分地留存了所有通訊使用者的通訊紀錄後，為防止數據濫用，就更加需要制定嚴格的通訊紀錄調取程序，以及被留存數據的事後刪除程序。

德國法院在其作出的違法認定判決中強調，為刑事起訴、安全和危險防禦以及情報部門的目的而毫無根據地將數據保留六個月本身可能不會自動違憲，[①]但是立法者必須通過一項法律，制定嚴格而明確的規則，以確保數據的安全性和完整性，限制數據的使用，制定透明的規則，並保證充分的法律保護。[②]同樣地，歐洲人權法院（The European Court of Human Rights）在其 2018 年 9 月 12 日對申請人提出的、從通訊服務提供者獲取通訊數據的制度違反了《歐洲人權公約》中關於隱私權規定的判決中指出，國內法應要求各制度將獲取數據的目的限制在打擊嚴重犯罪上，而且當這些制度允許當局獲取通訊服務提供者留存的數據時，獲取數據必須有嚴格的程序限制，例如經過法院或獨立行政機構的事先審查。[③]歐洲法院也指出，在第 2006/24/EC 號指令中並沒有體現對所保留數據的保障，應制定關於保留數據的敏感性、非法獲取數據的風險以及對有關數據的保護和安全的管理方面的內容，以確保這些數據的完全完整性和保密性。[④]同時，數據留存者在數據留存期結束時能夠對數據進行不可逆轉的銷毀，也對確保數據安全非常重要。[⑤]

綜合歐洲法院與德國法院的判決來看，妥善處理數據留存中的人權保障，一大關鍵就在於必須對調取留存數據作出具體和嚴格限制，包括對調取的適用條件以及調取的程序作出嚴格規管，還需要設立一些規定以確保到期數據得到妥善處置。

澳門現行法律也規定了調取通訊紀錄的程序，但是並未有根據不同的通訊紀錄的類型規定不同的調取條件及程序。根據《通訊截取及保障法律制度》第 10 條，如有理由相信通訊紀錄有助於刑事調查工作，有權司法當局得以批示許可或命令電信營運者及網絡通訊服務提供者提供數據，或者在法律規定的特別情況下由警察機關先予執行並在 72 小時內得到司法當局的確認。這一規定過於籠統，因此，澳門特區政府可以考慮區分不同的數據類型、規定不同的調取條件，在適用條件以及適用程序上予以完善。

在這個問題上，德國的經驗可以借鑑。德國將被調取的留存數據分為位置數據和其他通訊紀錄，同時對位置數據中的無線電基站（radio cell）數據又作出了特別規定。適用條件最為寬鬆的是其他通訊紀錄，當涉嫌使用電信手段進行犯罪時，須滿足調取對偵查有必要且沒有其他可能實現偵查的手段；當涉嫌犯罪係德國《刑事訴訟法典》第 100a 條中列明

[①]德國憲法法院（Bundesverfassungsgericht）, 2010 年 3 月 2 日判決，編號：1BvR256/08；Rößner, Sören. “Vorratsdatenspeicherung in Deutschland - Ende des Umsetzungsdefizits in Sicht?” *Europäische Zeitschrift für Wirtschaftsrecht*, vol. 25, no. 4, 2014, pp. 134-138.

[②]德國憲法法院（Bundesverfassungsgericht）, 2010 年 3 月 2 日判決，編號：1BvR256/08；Roßnagel, Alexander. “Die neue Vorratsdatenspeicherung.” *Neue Juristische Wochenschrift*, vol. 69, no. 8, 2016, pp. 533-534.

[③]歐洲人權法院（The European Court of Human Rights），2018 年 9 月 13 日判決，編號：58170/13、62322/14、23960/15，頁 467。

[④]歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 66。

[⑤]歐洲法院（European Court of Justice），2014 年 4 月 8 日判決，編號：C-293/12、C-594/12，頁 67。

的目錄犯罪（包括未遂、預備以及實施其他犯罪以達成目錄犯罪）時，僅須滿足調取對偵查有必要的通訊紀錄。更為嚴格的適用條件所針對的對象是位置數據，僅在涉嫌罪名為第100g 條中列明嚴重罪名（包括未遂、預備以及實施其他犯罪以達成目錄犯罪）時，並需要滿足調取對偵查有必要且無其他可能方式時可調取位置數據。而最為嚴格的，是有關無線電基站的位置數據的調取，適用的犯罪進一步限縮，除了要滿足位置數據的條件，還需滿足所涉罪名為第 100a 條列明的目錄犯罪。在將來的立法中，澳門特區政府也可以進一步考慮對通訊紀錄作出類型區分及程序細化。

與此同時，為更加完善地保障被留存數據所有人的權利，還應當建立類似德國所規定的到期數據刪除制度。根據德國《電信法》第 176、203 及 228 條的規定，電信營運商與網絡通訊服務商在留存期限屆滿時最遲一周內應當不可逆地刪除到期的留存數據，並且規定未履行該刪除行為時，將構成行政違法，最高可處以 50 萬歐元的處罰。澳門應當效仿德國採取的到期數據刪除的做法，規定電信營運者與網路通訊提供者在留存期限屆滿時銷毀留存數據，確保留存數據到期後得到妥善處理，避免到期數據無人管理而洩漏的風險。

三、澳門通訊截取的空白：加密通訊截取

加密通訊是指運用了端對端加密技術的通訊，通訊方須通過密鑰方可獲取通訊內容，大型加密通訊軟件 WhatsApp 稱，WhatsApp 通過端對端的加密技術，確保通訊內容僅有通訊雙方可知悉，用戶可通過密碼鎖定聊天介面，軟件亦提供所謂“閱後即焚”的功能，通訊內容經過一定時間即自動刪除，即使是服務商即 WhatsApp 本身也無從知曉。[①]隨着公眾對網絡中隱私與資訊保障的需求不斷強化，加密技術在通訊中的使用越發普遍，不僅出現了以加密通訊為核心功能的加密通訊軟件，且越來越多的通訊軟件中也提供加密通訊的功能。[②]

澳門《通訊截取及保障法律制度》中沒有對加密通訊截取作出直接規定，有關監聽、截收、錄音、錄影、複製等截取方式均難以獲悉加密後的通訊內容，只能獲取未經加密的通訊數據。澳門在加密通訊的截取方面，仍然處於空白狀態。

（一）逆向還原是否能夠解決加密通訊的截取問題？

在澳門特區政府 2018 年的公開諮詢會上，回應加密技術是否會阻礙通訊截取的實現問題時，澳門特區政府表示，當局有辦法逆向還原加密通訊為可識別內容。[③]但是，逆向還原並不能完全解決加密通訊的截取問題，逆向還原有可能需要花費大量的時間，還可能面臨破解時內容滅失的情況。[④]例如，在“閱後即焚”類型的通訊截取上，因為通訊內容

[①] “Privacy.” *WhatsApp*, https://www.whatsapp.com/privacy, accessed 19 Aug 2024.

[②] 吳俊毅：〈刑事訴訟上的線上搜索（Online-Durchsuchung）與源頭通訊監察（Quelle-TKÜ）—— 引進的必要性及實踐上的困境〉，《刑事政策與犯罪研究論文集（23）》，台北：“法務部”司法官學院，2020 年，頁 461 － 484。

[③] 〈通訊“加密”、“閱後即焚”如何截？司警：有方法識別加密內容〉，https://aamacau.com/?p=50944，2024 年 6 月 30 日讀取。

[④] 林鈺雄：〈侵入資訊科技系統之來源端通訊監察〉，《月旦法學教室》（台北），總第 223 期，2022 年，頁 16 － 19。

存在的期限通常都僅為幾分鐘甚至幾十秒，即使獲取破解密碼，也無法獲取內容；再如，在語音通訊的截取上，當通訊結束時不會存儲通訊內容，也無從逆向還原通訊內容。另一方面，傳統的通訊截取有賴於服務提供者的合作，但在加密通訊中，服務提供者自身也無法獲取實質的通訊內容，又或是服務提供者可能出於技術專利保護和商業利益拒絕當局的解密的要求。

顯然，截取加密通訊有賴於立法引入針對性的新截取方式，授權偵查機關採取一些特別的方式以獲取加密通訊內容，但澳門《通訊截取及保障法律制度》對加密通訊仍處於空白狀態，鑑於偵查的需要與目前方式的不足，對其特定立法顯然是必要的。

（二）德國截取加密通訊的應對：來源端通訊截取方式與截取定義拓展

為應對加密通訊帶來的偵查問題，在 2016 年，德國向歐盟提出議案，稱 WhatsApp、Telegram 等手機通訊應用程式的加密功能使執法部門難以監控可疑恐怖分子。為加強反恐工作，要求歐盟委員會草擬法例，強制程式開發者於恐怖活動調查中解密信息。[①] 隨後在 2017 年 8 月 24 日，德國生效了《德國關於更有效、更實用的刑事訴訟法案》（Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens），修改原德國《刑事訴訟法典》第 100a 條關於通訊截取的規定，引入了來源端通訊截取（Quellen-Telekommunikationsüberwachung）這一針對加密通訊的截取新方式，明確規定允許以技術手段干擾有關人員使用的計算機資訊系統的截取方式，並允許截取通常可在公共電信網絡的正常傳輸過程中截獲並以加密形式紀錄存儲的通訊內容。

來源端通訊截取指偵查機關利用國家監控軟件（“國家木馬 National Spy Program”）侵入通訊發出方或接受方（即所謂來源端）的計算機資訊系統，以獲取在通訊內容加密前或通訊內容解密後的通訊內容，避免了對加密通訊的解密問題。[②]特別地，根據德國《刑事訴訟法典》第 100a 條第 5 款，當通訊通過公共電信網絡加密傳輸過程原本就可以被截取時，這種方式也可以被用來監察和紀錄侵入系統中儲存的通訊，但僅以截取被獲准後發生的通訊為限。

這種為了避免解密問題的加密通訊截取方式在德國通過後引發了巨大爭議，尤其是關於這種方式對於截取定義的挑戰問題。根據德國《刑事訴訟法典》第 100a 條中的解釋，截取指截獲被調查對象正在發送或接收的通訊內容，其明確限定適用的階段為通訊正在發生時，而來源端通訊截取則也適用於獲取儲存的通訊內容，這超越了截取的定義範圍。有學者指出，這種對原先截取定義的超越意味着其對數據權更強烈的侵犯，不僅侵犯了數據保密的權利，還侵犯了保證資訊科技系統的機密性和完整性的基本權利。[③]此外，關於“國

[①]程玉然：〈德法聲稱難監控恐怖分子　要求歐盟立法迫加密通訊軟件“開後門”〉，關鍵評論，2016 年 8 月 29 日，https://www.thenewslens.com/article/47845，2024 年 6 月 30 日讀取。

[②]（德）維爾納・薄逸克（Warner Beulke）、（德）薩比娜・斯沃博達（Sabine Swoboda）著；程捷譯：《德國刑事訴訟法教科書》，北京：北京大學出版社，2024 年，頁 269。

[③] Singelnstein, Tobias, Benjamin Derin. “Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens.” *Neue Juristische Wochenschrift*, vol. 70, no. 37, 2017, pp. 2646-2651.

家木馬”這種程式是否在實踐中僅僅只截取被允許範疇之內的通訊，也存在一定的質疑，擔憂者提出木馬程式本身存在技術漏洞，可以被利用來秘密獲取不在允許範圍內的公民隱私資訊。[①]

德國立法則希望通過對適用的限制，來確保來源端截取僅適用於實際上符合截取定義的即時通訊，根據德國《刑事訴訟法典》第 100a 條第 5 款，來源端截取適用非常嚴格的補充性原則，只有在其他方式“無法獲取”通訊內容時才可使用。如果其他方式的取證手段只是“難以獲取”通訊內容時，並不能採用該手段（在一般性通訊截取的適用條件上，立法用詞為“無法獲取或難以獲取”）。在截取的時候，應當使用最新的保護技術，以防止未經授權的系統訪問；在獲得數據的複製方面，也需要採取最新的保護技術，以防數據被修改，或者未經授權的刪除或訪問。此外，在措施結束後需在技術允許的範圍內自動移除被侵入系統中的國家木馬程式。對於“國家木馬”可能存在技術漏洞的質疑，德國不僅自己研發了國家木馬，據稱還專門地向木馬程式科技公司購買了相關程式，以盡可能確保在技術上的安全。[②]

（三）澳門加密通訊截取之確立

從上文的分析可以看出，僅靠“逆向還原”是無法實現所有通訊截取的需求的，其技術局限及現實困境要求我們尋求更為有效的、應對加密通訊的即時截取方法。確立澳門加密通訊截取制度，應當以澳門現行通訊截取制度為基礎，針對加密通訊的特性，引入來源端通訊截取。

首先，應當對加密通訊截取之“截取”作出特別規定，例外地允許對已經儲存的數據進行“截取”。也就是說，在本來通過截取手段可以獲得即時通訊的內容，但由於加密技術的適用而導致即時通訊無法獲取時，在接收端或者發送端的設備上所提取之內容，視為即時通訊的內容。其次，對加密數據的提取方式在法律上作出明文規定。加密數據的源端提取，需要植入木馬程式，這一做法已經超越了目前《通訊截取及保障法律制度》第 4 條所規定的“監聽、截收、錄音、錄影、複製”等截取方式，因此必須有明確的法律授權。在使用的條件和程序上，加密通訊除了滿足《通訊截取及保障法律制度》第 3 條所規定的在涉嫌本條所列明犯罪、且有必要和其他手段無法或難以實現偵查目的時，經由法官批示命令或許可方可實行通訊截取的條件外，考慮到來源端通訊截取更強烈的人權干涉風險，應進一步限定其補充性條件，規定在僅有此種方式可獲知通訊內容時方可進行。

[①]黃河：〈論德國電信監聽的法律規制 —— 基於基本權利的分析〉，《比較法研究》（北京），第 3 期，2017 年，頁 88 － 101。

[②]林鈺雄：〈國家木馬與國家安全 —— 以德國法發展趨勢為借鏡〉，《最高檢察論壇》（台北），創刊號，2023 年，頁 2 － 22。

四、在線搜索：澳門獲取電子數據的最後一根稻草？

在澳門目前的刑事偵查實踐中，如果需要獲取網絡服務提供商所存儲的電子數據，是非常困難的。澳門對已經存儲的電子數據的獲取，只能適用第 11/2009 號法律《打擊電腦犯罪法》第 16 條所規定的傳統的搜索、扣押或責令所有人提交的方式。由於當下主要的網絡服務提供商都不在澳門境內，也不會在澳門境內設立分支機構，因此在許多國家可以適用的諸如向網絡服務提供商調取電子數據的方式，在澳門幾乎無法使用。因此，是否應當考慮引入新的調取電子數據手段，以適應澳門偵查網絡犯罪或利用網絡實施的犯罪的需要？德國在 2017 年 8 月 24 日生效的《德國關於更有效、更實用的刑事訴訟的法案》規定了秘密利用國家監控軟件（“國家木馬”）獲取存儲在計算機資訊系統中的刑事電子數據的在線搜索制度，雖然這一制度引發了激烈的爭論，但仍然因為其在偵查中的重要作用而被立法採納。澳門是否可以借鑑這一制度，以及應當如何構建？本部分將予以討論。

（一）德國關於在線搜索的正當性爭議

根據《德國關於更有效、更實用的刑事訴訟的法案》，德國所規定的在線搜索，是指國家出於執法目的，在特定時間內秘密進入計算機資訊系統，以監測其使用情況，並記錄和傳輸其存儲的內容。具體而言，即偵查機關對調查對象計算機資訊系統植入木馬程式，秘密入侵其系統，通過木馬程式對資訊系統的儲存資料進行搜索，只要被調查對象使用該被植入了木馬程式的設備上網，木馬程式所搜尋的資料即會被秘密複製並傳送到偵查機關。[①]

在線搜索這一方式的爭議同樣是巨大的，一方面是這種方式嚴重干涉了隱私權與數據權，另一方面，則是在線搜索的搜索邊界因計算機資訊系統的發展而不斷變化，極容易引發超出偵查需要的過度數據獲取。

雖然刑事電子數據的秘密獲取方式總是伴隨着人權上的爭議，但這一爭議於在線搜索制度上更為嚴厲。通訊截取通常被認為是對隱私權的嚴重干預，但是在線搜索的干預程度尤甚。在線搜索可獲取被植入木馬程式的計算機資訊系統上的全部存儲數據，而通訊截取只能獲取特定時間內的即時通訊內容。

在線搜索有賴於計算機資訊系統進行，技術的發展拓展了在線搜索可獲取的數據範圍，這引發了對在線搜索可能造成的突破原定偵查範圍的強烈擔憂。德國立法中的“計算機資訊系統”是指能夠通過互聯網協議地址進行通訊的各種技術設備，它包括無線局域網接入點、衛星、移動電話、電腦、無線局域網接收器甚至智能家居設備。[②]例如，“無線局域網接收器”這種設備，它可以掃描所有集成在無線局域網系統中的所有設備，從而獲取

[①] 王士帆：〈偵查機關木馬程式：秘密線上搜索 —— 德國聯邦最高法院刑事裁判 BGHSt 51, 211 譯介〉，《司法週刊》（台北），總第 1779 期，2015 年，頁 2 － 3。

[②] Blechschmitt, Lisa. “Strafverfolgung im digitalen Zeitalter.” *Multimedia und Recht*, vol. 21, no. 6, Jun 2018, pp. 361-365.

在該無線局域網中所有資訊技術設備的數據；類似地，當局可打開安裝在設備上的麥克風和攝像頭，從而對用戶進行聲音和光學監控，[①]私人住宅監控系統的音頻和視頻數據也會匯聚到被截獲的系統中。[②]然而，關於是否允許在住宅區採取這種大範圍的監控措施，這些措施目前在德國面臨着法律上的不確定性。[③]根據德國《刑事訴訟法典》第 100b 條的措辭，“搜查”措施顯然僅限於在被侵入的計算機資訊系統中收集或儲存的數據，而不包括正在發生的通訊。

因為這些爭議，德國也出現了對在線搜索的憲法申訴，2018 年 4 月由聯邦資訊技術安全和數據保護協會（Der Bundesverband IT-Sicherheit e.V.）和 2018 年 8 月由德國政黨自由民主黨都提出了針對在線搜索的憲法訴訟。[④]申訴者認為，這種秘密措施明顯侵犯了關於計算機資訊系統的保密性與完整性的基本權利，且規定可適用該手段的罪行目錄過於廣泛，違背了侵害相稱性原則。此外，申訴人還提出，對在線搜索的立法程序過於匆忙，阻礙了對這一問題的公開辯論和民主程序的進行，[⑤]由此，申訴者認為在線搜索的正當性並不明確。

儘管存在這些爭議，但德國面臨着嚴重的恐怖主義犯罪威脅，出於偵查之需要，目前立法依然認為在線搜索是必要和合法的，[⑥]立法方通過對在線搜索嚴格的程序構建，以平衡偵查需求與隱私權、數據權等基本權利保障的關係。

（二）德國在線搜索的適用程序

正是因為在線搜索對隱私權與數據權等基本權利的持續干涉，及其可獲取的數據範圍之廣，在線搜索被視為“最為嚴重的刑事偵查手段”，[⑦]為確保在線搜索被恰當地使用，德國對在線搜索的適用條件、程序以及延長實施的程序作出了嚴格限制。根據德國《刑事訴訟法典》第 100b 條，只有在滿足必要性與補充性原則下，即在有足夠懷疑且涉及罪行嚴重，加之沒有其他可能手段或其他手段實現偵查目的之前提下，才能實施在線搜索。

在線搜索適用非常嚴格的補充性原則，要求僅當在線搜索是獲取證據的唯一方法時方可使用。當局在實施在線搜索之前，必須考慮德國《刑事訴訟法典》第 100b 條第 1 款第 3 句規定的低強度干擾手段，即該法典第 100a 條第 1 款第 2 句規定的來源端通訊截取、第

---

① Blechschmitt, Lisa. “Strafverfolgung im digitalen Zeitalter.” *Multimedia und Recht*, vol. 21, no. 6, 2018, pp. 361-365.
② Blechschmitt, Lisa. “Strafverfolgung im digitalen Zeitalter.” *Multimedia und Recht*, vol. 21, no. 6, 2018, pp. 361-365.
③ Barthe, Christoph. *Karlsruher Kommentar zur Strafprozessordnung: StPO*. C.H.BECK, 2023, pp. 554-556；不同的是，Bertram, Schmitt, Köhler Marcus. *Strafprozessordnung: StPO*. C.H.BECK, 2024, §100b, p. 2，他認為這一措施是以“主動”監視來定義的，而德國《刑事訴訟法》第 100b 條只允許“被動”搜查。
④ 參考德國憲法法院（Bundesverfassungsgericht）編號：2BvR897/18、2BvR1797/18、2BvR1838/18、2BvR1850/18、2BvR2061/18；另見德國憲法法院（Bundesverfassungsgericht）2019 年概覽：https://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2019/vorausschau_2019_node.html; https://www.zeit.de/digital/2019-03/verfassungsschutz-staatstrojaner-horst-seehofer-gesetzesentwurf-ueberwachung-bnd，2024 年 8 月 31 日讀取。
⑤ “Bundestag gibt Staatstrojaner für die alltägliche Strafverfolgung frei.” 22 Jun 2017, HeiseOnline, https://www.heise.de/newsticker/meldung/Bundestag-gibt-Staatstrojaner-fuer-die-alltaegliche-Strafverfolgung-frei-3753530.html, accessed 31 Aug 2024.
⑥ Mark A. Zöller 著，王士帆譯：〈來源端電信監察與在線搜索 —— 德國刑事追訴機關之新手段〉，《司法新聲》（台北），總第 130 期，2019 年，頁 106 － 123。
⑦ Singelnstein, Tobias, Benjamin Derin. “Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens.” *Neue Juristische Wochenschrift*, vol.70, no. 37, Sep 2017, pp. 2646-2651.

102 和 103 條規定的對嫌疑人和他人進行搜查，或第 94 條及其後條款規定扣押物品等是否能夠實現獲取證據證據的目的，只有在上述手段均無法奏效時，才可以考慮適用在線搜索。

即便滿足補充性原則，在線搜索也未必可以適用，還必須滿足有足夠懷疑及所涉嫌的罪名極為嚴重的條件。根據德國《刑事訴訟法典》第 100b 條的規定，必須有某些事實證明有理由懷疑某人犯有特別嚴重的罪行，且涉嫌第 100b 條中列明的目錄犯罪時，才可以考慮適用在線搜索。此類犯罪必須大大超出平均犯罪的嚴重程度。[①]

在線搜索的續期程序也較通訊截取更為嚴格，根據德國《刑事訴訟法典》第 100e 條第 2 款，在線搜索每次可延長期限為一個月，且須經由檢察院向所在高級區地區法院分庭申請後，方能下令採取。在緊急情況下，主審法官也可以下達命令。如果命令的期限總共延長了六個月，則須經由地區高等法院決定是否進一步延長命令。

（三）澳門在線搜索之確立必要性與方案

在線搜索確實是一種非常有效的獲取已存儲電子數據的重要手段，尤其在那些犯罪性質及犯罪情節極其嚴重，其他偵查手段無法奏效的情況下，在線搜索就成了破獲刑事案件的唯一希望。這也是德國在巨大爭議下仍堅持推出這一措施並拒絕廢除的原因。

那麼，澳門是否需要引入在線搜索制度呢？本文認為，還是非常有必要的。首先，澳門毗鄰中國內地、香港及東南亞地區，加之澳門地區經濟活躍，利用加密技術、雲端技術等新興網絡技術進行的跨境犯罪多發，跨境電子數據調取需求旺盛。與此同時，由於澳門細小的司法管轄範圍，大型主流網絡通訊服務提供商並不位於境內，也不在境內開設分支機構，難以通過向網絡服務商提出數據需求以實現對存儲的電子數據的獲取，而僅靠扣押被調查對象設備，顯然也無法滿足獲取加密過的，又或是儲存在雲端的電子數據。因此，通過嚴格控制下的植入木馬程式進行在線搜索，就成為偵破某些嚴重犯罪或跨境犯罪的重要手段。

必需強調的是，基於在線搜索對隱私權和數據權強烈干涉的風險，如若在澳門設立此制度，應當十分謹慎，將其作為一種僅適用於特別案件的特殊偵查手段，在符合必要且沒有其他手段可獲取所需數據的情況下方可使用。

總體來說，可以對照目前《通訊截取及保障法律制度》中有關通訊截取的相關規定，作更為嚴格的程序設計。在適用的證據條件上，通訊截取的條件為有理由相信涉嫌犯罪，啟動在線搜索的證據條件應當更為嚴格，可以考慮適用與羈押這種強制措施相同的標準，即有強烈跡象涉嫌犯罪。在適用前提上，應當明確採用嚴格的補充性原則。通訊截取的適用前提或者是對偵查必要，或者是其他手段不能或難以實現；而在線搜索的條件應為對偵查必要，且無其他手段可實現。在適用的犯罪範圍上，在線搜索應僅適用於恐怖犯罪、洗錢犯罪、危害國家安全犯罪、有組織犯罪、不法生產和販賣麻醉藥品與精神藥物犯罪、禁

[①] Bertram, Schmitt, Köhler Marcus. *Strafprozessordnung: StPO*. C.H.BECK, 2024, §100b, p. 4; Satzger, Helmut, Wilhelm Schluckebier. *StPO Strafprozessordnung mit GVG und EMRK*. Carl Heymanns, 2022, pp. 544-550.

用武器犯罪、販賣人口、外貿犯罪、賄賂犯罪等性質特別嚴重的犯罪。而本來可以適用通訊截取的犯罪，例如最高刑三年的犯罪、電腦犯罪以及通過電信實施的侮辱罪、恐嚇罪、脅迫罪、侵犯住所罪或侵入私人生活罪等，則因為其犯罪性質不夠嚴重，應當排除在線搜索的適用。在適用的程序設計上，在線搜索適用的具體期限可與一般通訊截取相似，為三個月，但對其續期之程序應當更為嚴格，須規定可續期的一般上限，並增加審核程序。

五、結語

通過歐洲法院觀點上的搖擺以及德國多次的修法可以看出，如何在秘密獲取電子數據並平衡偵查需求和隱私權、數據權的保障，在德國乃至與整個歐盟尚未形成一個所謂完美的方案。澳門《通訊截取及保障法律制度》雖然已經回應了網絡化時代下通訊數據的截取以及通訊紀錄的留存和調取問題，但通訊紀錄的數據留存及調取程序尚需完善，澳門現有的偵查手段無法回應加密通訊的截取以及跨境調取雲端數據的需求，這些挑戰在澳門特殊的區位地理環境，以及欠缺對網絡服務提供商所控制的電子數據的調取手段的情況下顯得尤為突出。本文基於歐盟和德國的經驗，提出澳門在秘密獲取刑事電子數據上可能的完善方向，例如對數據留存的程序重構、留存數據調取的程序優化、引入來源端監聽及在線搜索手段等，但限於篇幅，本文僅作出原則性、方向性探討，具體的程序建構尚需進一步的分析論證。

〔責任編輯　　陳超敏〕
〔校對　宋永豪　何仲佳〕