第一常設委員會

第 1/VI/2020 號意見書

事由：修改第 11/2009 號法律《打擊電腦犯罪法》法案

I - 引言

1. 澳門特別行政區（下稱“澳門特區”）政府於二零一九年七月二十三日向立法會提交了修改第 11/2009 號法律《打擊電腦犯罪法》法案。立法會主席透過同月二十六日第 1016/VI/2019 號批示接納了該法案。

2. 上述法案於二零一九年十月十七日經全體會議一般性討論和一致通過。立法會主席於同日透過第 1371/VI/2019 號批示將上述法案分派給第一常設委員會進行細則性審議，並要求委員會於二零一九年十二月十七日前提交意見書。但由於種種原因，該期限延至二零二零年四月九日。

3. 委員會先後於二零一九年十月二十九日、二零二零年一月二十二日、二月二十七日和二十八日，以及四月八日召開會議，對本法案進行分析。政府代表列席了其中三次的會議。此外，為了在技術層

面上完善法案，立法會顧問團與政府代表亦舉行了一次技術會議。

4. 由於法案涉及修改程序性的規定，委員會認為有需要按照八月二十一日第 42/95/M 號法令第三十條第三款規定聽取澳門律師公會的意見。當年在立這部法律時亦曾要求該公會發表意見[1]。因此，委員會於二零一九年十一月一日致函律師公會並在同月十五日收到該公會的意見書[2]。

5. 因應在委員會會議上的討論和所提出的建議，提案人對已獲一般性通過的法案最初文本作出了相應的修改，並於四月七日提交了法案的最後文本。委員會亦按照立法會議事規則第一百一十九條製作了相關的意見書。

II - 提案

根據理由陳述，*本法案有四個明確的目的：*

- 新增一項罪狀，規定將使用電腦裝置和程式以及“sting ray”類型的專門器械操作（非法或未經授權的）流動電信模擬發射站的行為定為犯罪；

[1] 見第三常設委員會第 3/III/2009 號意見書第二頁 - https://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer_cn.pdf

[2] 見附件。

– 確保能更好地配合剛通過的第 13/2019 號法律《網絡安全法》，目的是對《網絡安全法》訂定的關鍵基礎設施營運者以及第 22/2000 號行政法規《中央人民政府駐澳機構履行職責的保障及有關豁免》中所訂定的中央人民政府駐澳機構（即現時的中央人民政府駐澳門特別行政區聯絡辦公室、外交部駐澳門特別行政區特派員公署、中國人民解放軍駐澳門部隊）所使用的電腦系統加強刑法保障；

– 明確規定允許對儲存於澳門特別行政區以外的電腦數據資料提取副本以作為刑事訴訟程序的證據，只要透過位於澳門特別行政區的電腦系統查閱或獲取該等資料屬合法；

– 將違反職業保密犯罪獨立成罪，而且刑罰加重。

針對第一個目的，提案人表示“近年來，利用電腦裝置和程式以及“sting ray”類型的專門器械操作偽基站的違法行為大幅增加”；“這類偽基站運作模式是使手提電話裝置將其識別為正當的電信基站（……）偽基站通常設置在人流集中或是流動頻繁的地點附近，例如在出入境口岸一帶，蓄意向途經的市民的手機發送滋擾信息，侵入他人的私人生活，並且散播或宣傳非法活動（賣淫、為賭博的非法貸款、詐騙形式的投注等等）不僅使該區居民、出入境市民及旅客大受滋擾，更導致罪案發生，亦造成市民損失，嚴重影響澳門特別行政區社會的法治及旅遊形象。”

還有"偽基站的打擊難度大，它不但是一種遠程無需人手控制的犯罪，而且其作案工具（個人電腦、電腦程式和"sting ray"類型器械等裝備）的體積較小，易於掩藏，多設置於住宅單位內，這將大大增加調查及搜證的難度。"

關於第二個目的，提案人表示"*擴大刑事保護有以下兩種方式：*

- 一方面，修改現行第 11/2009 號法律第十二條，除加重對公共實體所實施的電腦犯罪的刑罰，亦加重對關鍵基礎設施的私人營運者、對第 22/2000 號行政法規中所訂定的中央人民政府駐澳機構所實施的電腦犯罪的刑罰；

- 另一方面，修改有關告訴權的現行規定，即引入一新條文（第十二-A 條）以規範告訴權，並廢止現行法律中就有關方面的若干零散規定（第 11/2009 號法律第四條第三款、第五條第三款、第七條第五款及第十一條第四款）。

新的法律規範中，應加重以關鍵基礎設施營運者和上述重要實體為目標所實施的電腦犯罪的刑罰，並將這行為一律定為公罪，即無須告訴便可開展及進行刑事程序。"

針對修改第 11/2009 號法律第十六條第一款（六）項的第三個目的，提案人表示"*然而，澳門特別行政區單方面進行自我限制似乎太不合邏輯，因為國際上的一貫做法是，只要（跨境）查閱的數據資料*

屬可公開查閱或取得依法獲許可者的同意(但涉及未成年人或精神失常人士的個案時，應特別謹慎)，A 司法管轄區的司法當局便可查閱儲存於 B 司法管轄區的電腦系統中的電腦數據資料，並可在不侵害 B 司法管轄區的主權的前提下取得有關資料的副本。

因此，建議在法案中刪除現行法律中“位於澳門特別行政區”的表述，並允許司法當局對具體個案進行評估，以確定是否具有收集儲存於其他司法管轄區的電腦數據資料副本的正當性條件。

刪除有關表述後，澳門特別行政區的法例將有類似下列法律所主張的解決方案：

– 葡萄牙《網絡犯罪法》第十五條第五款；及

– 西班牙《刑事起訴法》第五百八十八 sexies 條。

當然，屬以下情況，澳門特別行政區司法當局繼續須訴諸國際司法互助機制：

– 不具備上述要件時（資料屬可公開查閱或取得依法獲許可者的同意）；或

– 所實施的並非單純查閱和取得已儲存資料副本的措施，而是諸如扣押數碼載體實體、實時截取數據及查閱路由數據資料等的其他措施時。"

至於最後的目的，提案人解釋稱"*上述條文列於《刑法典》第二卷第一編第七章中，該章明確規定受保護的私人生活的有關利益。然而，當關係到洩露電腦系統安全關鍵漏洞時，由於當中所保護的利益已提升到公共利益的層面，凌駕於涉事電腦系統擁有人的個人利益，而該等電腦系統乃通過網絡互相聯結，所以，當其中一個系統出現漏洞，可能會對整套系統、甚至整個社會造成負面影響。*

故此，本法案增加新條文（第九-B條），對存有任何不正當意圖，向他人透露在執行職務時或基於職務原因而獲悉的有關系統、裝置或電腦程式的安全關鍵漏洞，即使屬暫時性的漏洞，而足以造成有實施電腦犯罪的危險者，建議加重有關刑罰（處最高三年徒刑或科罰金）。"

III – 審議

A. 一般性審議

1. 現正修改的第 11/2009 號法律規定將特定的電腦犯罪刑事化及為方便調查該等犯罪訂定了相關的刑事程序，並且對透過電腦系統實施的犯罪作了刑事化規定，還規定在電子載體中搜集和保存有關實施任何犯罪證據的特別制度。

2. 電腦犯罪在全球迅速增長，發展越來越快，變化越來越大，犯罪手法也越來越複雜，所以有必要採取更有效的偵查及預防措施，以及加強對最近十年間在世界各地和澳門特區均有出現的新型犯罪行為的處罰。

3. 鑒於這個現實和有需要將現在的法定制度與近期在立法會通過的《網絡安全法》加以配合，以及由於現行法律已實施超過十年之久，委員會非常樂見本法案的出現。儘管如此，委員會仍有針對某些修改建議提出問題和與提案人進行討論，以便從刑法保護的層面上能夠明晰對法案修改建議的理解，以及能夠在法律技術上完善一些規定。

4. 委員會的討論主要涉及：

a）對第 11/2009 號法律已訂定的犯罪，透過對第十二條的修改，擴大納入加重處罰的範圍；

b）同一法律第十六條（六）項所訂定的特別措施的執行範圍和方式；

c）新引入的第九-A 條和第九-B 條的罪狀所保護的法益、法律定義及適用範圍。

5. 按照現在第十二條的修改規定，只要犯罪的標的屬《網絡安全法》所規定的關鍵基礎設施營運者或屬中央人民政府駐澳機構在其業務中所使用的電腦數據資料或電腦系統時，第 11/2009 號法律所規定的刑罰就會加重。委員會希望知道該規定是僅包括第十二條所指屬公共實體和機構的關鍵基礎設施的營運者，抑或亦包括第 13/2019 號法律第四條第三款所指具私人性質的關鍵基礎設施營運者，以及希望知道這項修改的理由是甚麼。

6. 提案人解釋說"*關鍵基礎設施營運者已涵蓋關鍵基礎設施公共營運者和關鍵基礎設施私人營運者，而加重刑罰的目的是要加強對所有關鍵基礎設施營運者的刑法保障。因此，重點並不在於營運者屬公共或私人性質，而是其對於社會正常運作及大眾福祉的關鍵性。*"

7. 委員會強調，立法會第三常設委員會在細則性審議第 11/2009 號法律時所製作的意見書[3]中提到："*第十二條第一款規定，如犯罪行為涉及澳門特別行政區公共實體的電腦數據資料或電腦系統，則第四條至第十一條設定的電腦犯罪的刑罰加重。刑罰的加重是為了加強*

[3]第 3/III/2009 號意見書第 33 頁-https://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer_cn.pdf

對當局使用電腦的保護，即加強保護‘公共實體的電腦系統或電腦數據資料的保密性及完整性’。”而且，現在只要牽涉關鍵基礎設施營運者，不論涉及公共還是私人的營運者在其業務中所使用的電腦數據資料或電腦系統的非法行為，就會有加重處罰的情況，相關的案件亦會大大增加，因為所涉及的關鍵基礎設施營運者的數量遠比原本所規定適用的實體的數量多很多。[4]

8. 因此，委員會詢問提案人，既然是基於特殊預防需要而採取這一加重刑罰的刑法政策取向，而且考慮到第 13/2019 號法律第二條（三）項對關鍵基礎設施作出的定義，加重刑罰的重點是否應該是直接保護關鍵基礎設施，而非營運者。重要的是加強對關鍵基礎設施內電腦網絡和系統的刑事保護，這些設施一旦受到攻擊，就會直接對公共安全秩序和廣大市民的生活造成較嚴重的影響和損害。因此，需要更嚴厲地處罰針對此類關鍵基礎設施的犯罪。

9. 提案人回應稱，加重刑罰的範圍不會如此廣泛，因為澳門特區有數千家企業，其中關鍵基礎設施私人營運者僅佔很小的百分比。此外，加重刑罰取決於被害人的性質，即關鍵基礎設施營運者這一性質，不論是公共還是私人營運者，可有效保護其營運的關鍵基礎設施。委員會認為此解釋合理。

[4]除第 13/2019 號法律第四條第二款所規定的關鍵基礎設施公共營運者外，第一常設委員會第 3/IV/2019 號意見書第 10 頁指出“*政府向委員會指出，初步確定了 117 個關鍵基礎設施的私人營運者，主要集中的領域包括銀行、金融及保險業務等不同行業(共 64 個實體)*。”- https://www.al.gov.mo/uploads/attachment/2019-05/619955ceb9fb1538d9.pdf

10. 關於第 11/2009 號法律第十六條（六）項的修改，委員會討論過程中，首先要求提案人解釋，對某電腦系統進行初步搜索或進入電腦系統有何種法律和程序要求。其次，如何延伸搜索，延伸的範圍有多大，可查閱何種數據類型，透過何種法律程序為之，尤其當涉及的資料儲存於澳門特區以外的電腦系統中或相關地理位置不詳的情況下。

11. 經過討論，得以澄清，針對儲存在某電腦系統中的數據資料進行初步搜索或查閱時，根據第 11/2009 號法律第十四條，須考慮《刑事訴訟法典》有關搜索和扣押的規定。而（六）項規定的延伸搜索，前提是某設備在初步搜索中被扣押，而且要求待查找的新電腦系統或曾被搜索的初始系統中的不同部分必須可以透過初始系統進入，就是說必須可透過被扣押的設備進入。根據該法律第十六條第一款，延伸搜索須得到有權限司法當局的許可或命令。但如屬該條第二款規定的情況，即使未經有權限司法當局預先許可，也可由刑事警察機關執行〔即司法警察局，根據第 5/2006 號法律第七條第一款（十）項規定，司法警察局有專屬職權調查與資訊有關的犯罪〕。在此情況下，須立即將延伸搜索的實施通知有權限司法當局，並由其在最遲七十二小時內審查該措施，以便使之有效，否則該措施無效（第十六條第三款，該款未經任何修改，如同條第一款及第二款的序文）。刑事警察機關的介入屬例外性質，僅在緊急情況下或如有延誤將對具重大價值之法益構成危險時方可介入，這一點與《刑事訴訟法典》有關搜查及搜索（第一百五十九條第四款）及扣押（第一百六十三條第四款）的規定類似。

透過延伸搜索可查閱的電腦數據資料是內容數據，而非路由數據資料。路由數據資料的查閱及收集一直根據第 11/2009 號法律第十六條第一款（二）項的規定進行。

12. 委員會強調，（六）項規定的獲得此類證據的法定要求自第 11/2009 號法律生效以來從未改變，多年來從未受到過質疑，而根據上述解釋查閱此類數據不排除、也不取代《刑事訴訟法典》的規定，因為在獲得證據的方法、以及保障依法受保護的保密事實方面，《刑事訴訟法典》作為補充制度，仍然是必需參考的法規。

13. 法案建議刪除第 11/2009 號法律第十六條第一款（六）項中“位於澳門特別行政區”的表述，目的是允許獲取位於澳門特別行政區以外的（不論是位於某具體地區，還是雲端）儲存於另一電腦系統或初始系統的不同部分中的數據資料。就相關程序，提案人確認立法原意是構建一套與《網絡犯罪公約》（《布達佩斯公約》）第三十二條一致的法律制度，在符合法定前提下，允許跨境查閱或獲取電子證據。現行法律在該項中已對該法定前提作出規定，即有理由相信擬找尋的資料儲存在該電腦系統或其某部分內，且透過初始系統查閱或獲取該等資料屬合法。提案人指出，“*這意味着澳門特別行政區當局可取得的電腦資料包括公眾可查閱的資料（來源公開），或如屬公眾不可查閱的資料，則須取得能合法地透過該電腦系統發佈有關資料的人士的合法及自願同意才可獲得，通常是指資料持有人本身*”。提案人重申，如數據位於另一特定司法管轄區，由司法當局判斷是否使用澳

門特區現行的國際或區際司法協助機制。

14. 委員會認為，現今網絡犯罪絕非次要問題，是各國政府、社會及個人關心的主要問題之一。當今世界，每天有數以千計針對電腦系統的攻擊，由於電子證據的跨國性和不穩定性，快速獲得電子證據越發重要。

15. 因此，委員會讚許政府關注到澳門特區的法律須符合國際法，尤其是《歐洲理事會網絡犯罪公約》(《布達佩斯公約》)，但強調現時對第 11/2009 號法律第十六條（六）項所引入的修改，並沒有就《公約》中對一方未經他方許可，跨境查閱儲存於他方境內的電腦數據資料訂定的限制作出明確規定，根據第三十二條，這些限制有：a)這些已儲存的電腦數據資料屬公眾可查閱的資料(來源公開)，不論這些數據所在的地理位置為何；b)一方取得能合法地透過該電腦系統發佈有關資料的人士的合法及自願同意；如不屬上述情況，《布達佩斯公約》只是規定相關的搜尋及查閱是透過互助(國際合作)進行。

16. 委員會關注到刑事司法協助針對雲端的情況難以進行，且程序複雜、成本高及效率低，導致很多國家都採取《布達佩斯公約》以外的單邊解決方法，與現時藉此修改擬在澳門特區規定的解決方法相似，而多年來，歐洲理事會網路犯罪公約委員會（T-CY）的雲端證據小組就此問題的討論從未停止。該組織 2016 年 9 月 16 日的報告建議為《布達佩斯公約》制定附加議定書，以加強法律互助，簡化與位於其他司法管轄區的服務供應商的直接合作模式，創造條件保障現有的

跨境獲取數據資料的方式，並確定數據保護的要件[5]。

17. 對這方面進行討論後，委員會最終結論是，《布達佩斯公約》第三十二條所訂定的限制，雖然沒有明確寫在條文中，但都存在於第十六條(六)項規定對延伸搜索所要求的法定前提中，因為要查閱的資料必須是透過初始系統查閱或獲取屬合法的，這意味著在已扣押一裝置的前提下，澳門特區當局要查閱的電腦數據資料必須屬公眾可查閱的資料(來源公開)，或取得能合法地透過該等裝置的電腦系統發佈相關資料的人士的合法及自願同意，通常是指資料的持有人本身。

18. 因此，委員會認為，綜上所述，不建議對第 11/2009 號法律第十六條第一款新的（六）項所建議的行文作任何修改。

19. 就第九-A 條新增的罪狀，其名稱為“使用電腦裝置以模擬流動電信服務站”，委員會認同有必要在電腦犯罪方面訂定此新的法定罪狀，因為模擬流動電信服務站尤其是在口岸出現得越來越頻繁，這些站利用電腦裝置連接到入境本澳的人士的手提電話，並藉此發佈及鼓勵作出與賣淫、色情及不法賭博有關的活動，從而使與該等活動有關的犯罪發生的可能性更大，影響澳門特區的法治及旅遊形象。

20. 在此主要應受譴責及懲罰的行為是模擬流動電信服務站，按提案人所述即“*使用電腦裝置和電腦程式，與其他工具或器械組合，*

[5] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168806a495e

連接市民的手提電話裝置，再向他們發送涉及各種不法行為的訊息”，因此，委員會認同在第一條僅處罰透過使用電腦程式及裝置，與其他工具或器械組合，純粹模擬流動電信服務站的危險犯，而在第三款(作為加重的犯罪)，則規定一些反映有關行為具更高不法性的可變更刑罰的情節，以要求更高的可譴責性及一種較重的刑罰，可以適用羈押，因為羈押可以是一種對這類犯罪具阻嚇性的防範性措施。

21. 關於第九-B條規定的新罪狀，其名稱為“不正當揭露電腦安全嚴重漏洞”，委員會與提案人一樣，都認同有必要保障一般電腦系統的安全，以免其關鍵漏洞被揭露，因為電腦系統是通過網絡互相聯結，所以必須保障因作出本法規定的電腦犯罪及發佈這些關鍵漏洞而可能受到損害的社會及個人的利益。

22. 委員會想知道是否擬增設一種職業保密，以及可能實施該罪的行為人的涵蓋範圍，也就是說，只是指公務員或在公共組織或機構任職的人，抑或還擬涵蓋其他人員，例如銀行職員。

23. 提案人解釋並非擬增設一種違反職業保密罪，而是一項“*違反職務保密罪*”，因為當查閱載於第 13/2019 號法律第十二條(二)項及第十四條第二款所指的網絡安全報告所包含的資訊時，可能會因而獲悉他人的資訊。而對於這些人，當然不可以確實地斷言他們就是某一職業的從業員，因此，“*擬涵蓋所有在執行(專業、機構、政治、或只是諮詢)職務時，或基於職務原因而獲悉某一特定電腦系統存在關鍵漏洞的人*”，他們將有關漏洞向他人透露，而足以造成有實施電

腦犯罪的危險。“*因此，其所指職務涵蓋任何職業(如銀行職員)或其他職務，包括政治職務*”。

24. 委員會明白安全的電腦系統的必要性，以及這些系統的關鍵漏洞可能對個人、公共部門及機構造成的影響，故對可能實施該罪及因為執行職務或基於職務原因而須受這項保密義務約束的行為人的概念範圍表示認同。

25. 關於第十二-A條，該條的名稱為“告訴”，增加該條導致在法案第三條廢止第11/2009號法律第四條第三款、第五條第三款、第七條第五款及第十一條第四款，委員會注意到，我們面對的只是改變制定該法律時所採用的立法技術(當時立法者選擇對上述條文中規定須經告訴的各個犯罪作出明確規範)，且現時將所有該法規定的犯罪的刑事程序非經告訴不得進行的情況集中於一條條文內。

26. 由於在該法的多項規定中均有提及關於須經告訴的要求，而且，這項立法技術在《刑法典》相似情況中均有被使用，例如在侵犯性自由及性自決罪(第一百七十二條)，以及侵犯名譽罪(第一百八十二條)，因此，委員會認為適宜作出有關廢止及增加第十二-A條，以便在單一條文中規定所有非經告訴不得進行刑事程序的情況，以及避免相同的內容在這些條文中每條作重複規定。

27. 關於第五條，該條規定法律的生效日期，曾經討論另訂一個新的日期，因為最初建議的日期已經過去，而委員會建議採用最初訂

定一個具體日期的方法，因為這樣能夠更肯定法律產生效力的日期，市民亦能夠更清楚地知道該日期。

28. 律師公會的意見書不僅涉及本法案的修改，還涉及《打擊電腦犯罪法》的整體內容。委員會與提案人一樣，認為涉及該法整體內容的意見應留待在將來全面檢討該法時仔細考慮。

B. 細則性審議

29. 委員會除了就法案進行上述的一般性審議工作外，亦已根據《立法會議事規則》第一百一十九條的規定，就法案所採納的具體解決方案與法案的立法原則的符合性作出審議，以及完善法案在法律技術方面的內容。

30. 第一條（**修改第 11/2009 號法律**）

本條對第 11/2009 號法律第十二條及第十六條作出修改。

31. 關於第十二條（刑罰的加重），其第一款現規定，當第四條至第十一條所定的電腦犯罪的標的為下列兩類實體在其業務中所使用的電腦數據資料或電腦系統，則該等犯罪的刑罰的最低限度及最高限度均加重三分之一（一如之前所規定般）：

a）第 13/2019 號法律《網絡安全法》所規定的關鍵基礎設施營

運者；

b）第 22/2000 號行政法規《中央人民政府駐澳機構履行職責的保障及有關豁免》第一條所訂定的中央人民政府駐澳機構。

32. 提案人希望藉此加強對《網絡安全法》所訂定的關鍵基礎設施營運者的電腦系統的刑事保護，而不論其屬公共或私人性質，因為關鍵基礎設施對社會的正常運作十分重要，故對其所作出的攻擊可產生重大影響，並直接對公共安全、公共秩序及大眾福祉造成損害；同時，亦為中央人民政府駐澳機構（包括中央人民政府駐澳門特別行政區聯絡辦公室、外交部駐澳門特別行政區特派員公署及中國人民解放軍駐澳門部隊）在履行職責方面提供更大保障。

33. 至於第十六條（特別措施），修改了其第一款（六）項的規定，以便在刑事調查中，澳門特區司法當局能透過將初步搜索延伸至特定電腦系統來查閱儲存於澳門特區境外的電腦系統的數據資料，或非儲存在任何具體地方的數據資料（因相關數據資料在“雲端”流通），又或儲存在初步調查所針對的電腦系統的不同部分的數據資料。

34. 搜索的延伸的前提條件與法律之前所規定的相同（即當有理由相信擬找尋的電腦數據資料有助刑事調查工作，而該等資料儲存在其他電腦系統內或初始系統的不同部分，且透過初始系統查閱或獲取該等資料屬合法），這意味著，當扣押一電腦裝置時，有權限當局透過延伸搜索所查閱的電腦數據資料必須是公眾可查閱的資料（來源公

開），或須取得能合法地透過該電腦系統發佈有關資料的人士的合法及自願同意（通常是指資料持有人本身）所獲得的資料；如非屬以上所述的情況，則應將問題提交司法當局，由其評估是否使用現行的國際或區際司法協助機制。

35. 委員會希望，將來當局根據有關解釋來適用（六）項的規定，並建議在查閱有關跨境數據資料時，如能明確識別儲存擬查閱的資料的所在地，則刑事警察機關應優先採用國際或區際合作機制為之，以避免地域或管轄權衝突。

36. 此外，委員會亦希望在執行查閱有關資料的程序時，刑事警察機關應考慮資料保護的相關規則及《刑事訴訟法典》關於保密的各項規定[6]，以保障個人權利。

37. 第二條（**增加第 11/2009 號法律的條文**）

透過本條，在第 11/2009 號法律增加了三條新條文，其中兩條，即第九-A 條及第九-B 條，規定了兩項電腦犯罪方面的新罪狀；而另外一條，即第十二-A 條，則涉及該法律第四條第一款、第五條、第七條第一款及第二款，以及第十一條第一款及第二款規定的犯罪的相關刑事程序。

[6] 如《刑事訴訟法典》第一百二十二條、第一百二十三條和第一百二十四條保護的職業秘密、公務員之保密和澳門特別行政區機密。

38. 第九-A 條規定了“使用電腦裝置以模擬流動電信服務站”罪，當中所保護的法益為流動電信服務及工具的安全性及可靠性。此為故意犯罪，不能以過失實施。

39. 一如在一般性審議部分所指出，第一款僅處罰使用電腦程式和電腦裝置與其他工具或器械組合來模擬流動電信服務站（作為抽象的危險犯），而第三款（作為加重犯罪）則規定了一些反映有關行為具更高不法性的可變更刑罰的加重情節，因而在刑罰方面要求更大的可譴責性。

40. 因應委員會的建議，第三款由最初文本包含的兩項規定改為三項規定，首兩項規定僅僅是將原來（一）項的內容分拆開來，因所涉及的是與行為人不同意圖有關的加重情節，而（三）項，即原來的（二）項，則與客觀行為本身特點及其結果具較高可譴責性有關。

41. 在法案最初文本中，該項[即原(二)項]規定了“*有關行為包括傳輸任何受法律禁止的廣告，及／或傳播、發佈或以任何形式煽動他人作出、支持或觀看色情資訊、賣淫或不法賭博制度規定的刑事或行政不法行為*”的情節。

委員會強調，無需要將色情、賣淫或不法賭博資訊的傳播和發佈加以區分，因兩個詞語意思相同。委員會曾詢問提案人，在刑法的保護層面，是否有必要將煽動他人作出上述任一行為從煽動他人支持該等行為獨立開來，因為支持可被視為與作出或觀看任一該等活動有

關，即作出或觀看這些活動的人是因為他們支持有關活動。

42. 委員會亦強調，在《刑法典》所規定的其他較嚴重的犯罪[例如犯罪集團罪（第二百八十八條）或煽動以暴力變更已確立之制度罪（第二百九十八條）]，或第 3/2016 號法律《預防及遏止恐怖主義犯罪》所規定的犯罪中，也沒有規定支持這種行為方式。

43. 在法案的最後文本中，提案人對該項進行調整，修改其行文，並刪除“傳播”活動以及“支持”行為。委員會對此表示贊同。

需強調在中文最後文本將原來“賣淫”一詞改為“性交易，兩者同義，因此葡文維持“prostituição”不變。

44. 第九-B 條，現以“不正當揭露電腦安全嚴重漏洞”為標題，規定了一種違反職務保密罪，即當該等違反足以造成有實施法律規定的任一電腦犯罪的危險時，則構成該犯罪。提案人擬藉此保障電腦系統的安全，避免暴露其關鍵或嚴重漏洞；同時，由於電腦系統透過網絡進行互動，故亦擬藉此間接地保護社會及個人的利益免受因透露該等漏洞而可能導致電腦犯罪實施的影響。當中，行為人必須是在執行本身職務（不論是專業、機構、政治或單純諮詢職務）時，或基於職務原因，獲悉某一特定電腦系統存在嚴重漏洞，並將之公開的人。

45. 該條在最初文本採用“安全關鍵漏洞”的表述，與現正審議的最後文本第一款的內容相對應。委員會認為，為了對此一新罪狀中

所定的行為進行定罪，如法律中載有安全關鍵漏洞的定義，則法律將會更清晰明確，從而讓市民能從客觀上得知行為人不能公開的信息內容。

46. 因此，委員會建議將法定罪狀改由第一款訂定，而為適用第一款的規定，建議增加第二款來規定安全關鍵漏洞的定義，一如《澳門刑法典》針對其他法定罪狀所規定的行文，例如酷刑及其他殘忍、有辱人格或不人道之待遇罪（第二百三十四條）、劫持航空器、船舶或火車又或使之偏離路線罪（第二百七十五條）或參與武裝騷亂（第二百九十二條）。提案人接納該等建議，此外還將“關鍵漏洞”的表述改為“嚴重漏洞”，兩者同義。

47. 關於這一罪狀，委員會亦曾就“存有任何不正當意圖”這一表述提出質疑，認爲用該表述來表達行為之不法性這一犯罪構成要素不適當，並以不確定的內容傳達行爲人的特定意圖，即所謂的“特定故意”。

48. 委員會一直知道，正如提案人所言，第 11/2009 號法律第四條及第五條所規定的犯罪亦採用相同的表述，且在適用該法律時一直沒有受到法院的質疑。然而，在那些犯罪中，亦使用了“未經許可”的表述，使每一罪狀所規定的行爲具有不法性，但現時的第九-B 條所規定的犯罪則並非如此。

委員會強調，“意圖的不正當性”最終是一種規範罪狀的要素，用以整體考量行爲的不法性，因此，“任何不正當意圖”最後只是用作體現行爲的不法性”，即用作強化行爲違反法律的這個意思。

49. 為了從法律技術層面完善法案，委員會就該表述提出了不同的建議，最後的建議是，參照《刑法典》第一百八十九條（違反保密）及第一百九十條（不當利用秘密）兩項犯罪中所採用的“未經同意”的表述，但建議不獲提案人接納。

50. 委員會最後接受了提案人的抉擇，但認爲對本條第一款所載“存有任何不正當意圖”的表述是純粹用作賦予相關行爲不正當或不法的性質，並不要求行爲人必須具有特定意圖或特定故意。因此，從主觀要素或故意的層面而言，不論形式為何，只要存在一般故意便足以構成犯罪。爲構成犯罪，只要行爲人以不正當的方式，向他人透露在執行職務時或基於職務原因而獲悉的安全嚴重漏洞，而足以造成有實施本法律規定的犯罪的危險。

51. 第十二-A 條規定，“如屬第四條第一款、第五條、第七條第一款及第二款，以及第十一條第一款及第二款規定的犯罪，非經告訴不得進行刑事程序，但屬第十二條規定的加重刑罰，不在此限。”即這些犯罪屬準公罪。此舉，將原

來分散於不同條文內涉及這些犯罪的刑事程序規定，集中在單一條文內規範。

52. 第三條(**廢止**)

本條規定廢止一些原來載於第 11/2009 號法律中與現時第十二-A 條所規定犯罪刑事程序類似的條文。

53. 第四條(**重新公佈**)

本條規定，經加入本法律及第 13/2009 號法律通過的修改，以附件形式重新公佈第 11/2009 號法律。透過重新公佈該法律的更新版本，可讓法律適用的一般對象，以及負責執行該法律的人員能更好地了解和認識法律被修改的內容。

54. 第五條(**生效**)

本條規定法律的生效日期爲二零二零年七月一日。

採用一個固定的日期比用“法律自公佈後滿 XX 日起生效”的表述方式更爲清楚，儘管後者是本地法規常用的行文，但中文與葡文的表述之間卻存在差異。

後者的葡文表述方式源自葡萄牙的法例，當地仍然使用

該表述，其意思是有關法規於某一日的零時零分起生效。因此，從葡文的角度而言，如果規定法規於公佈三十日後生效(o diploma entra em vigor 30 dias após a sua publicação)，則意味着該法規在第三十日的零時零分起生效。

這與中文要求該法規滿三十日起生效的理解不同，換言之，法規只在第三十日的二十四小時過後才生效。一日有二十四小時，葡文的生效起點爲某日的零時零分，而中文則是同一日的二十四小時後。

因此，固定日期能讓中文文本及葡文文本中的法律生效及效力產生的開始時刻更具確切性和更清晰。

IV - 結論

委員會經細則性審議及分析修改第11/2009號法律《打擊電腦犯罪法》法案後認為：

（一）法案的最終文本具備在全體會議作細則性審議及表決的所需要件；

（二）有必要邀請政府委派代表列席為細則性表決法案而召開的全體會議，以提供必要的解釋。

澳門，二零二零年四月八日。

委員會

何潤生

（主席）

馬志成

（秘書）

區錦新

李靜儀

宋碧琪

葉兆佳

邱庭彪

馮家超

林倫偉

王世民

附件

澳門立法會前地

立法會大樓

立法會第一常設委員會主席

何潤生先生：

公函編號: 2136/19

事由: 修改第 11/2009 號法律《打擊電腦犯罪法》- 聽取澳門律師公會的意見及評論

按照貴會本月一日來函的要求，經聽取本公會律師對於上述法案的意見後，現將經澳門律師公會理事會通過的意見書呈交閣下。

如有需要請隨時聯絡本會。

順致問候

理事會

Álvaro Rodrigues

二零一九年十一月十五日

意見書

事由：修改第 11/2009 號法律《打擊電腦犯罪法》

立法會要求澳門律師公會就上述法案發表意見。

按照五月六日第31/91/M號法令核准的"律師通則" 第三十條第三款的規定[1],"關於規範司法組織、從事律師業、民事訴訟及刑事訴訟法規之提案或草案，必須聽取澳門律師公會之意見。"雖然沒有訂定諮詢的期間或階段，但慣常做法是法案提交予立法會前的初步階段便諮詢澳門律師公會的意見，也有在法案提交予立法會審議後才諮詢的。

要提醒的是，儘管第三常設委員會編製的關於《打擊電腦犯罪法》法案的第 3/III/2009 號意見書曾提到，委員會於二零零九年四月六日曾向澳門律師公會發出公函，要求就相關法案發表意見，但是由於我們沒有收到該公函的記錄，因而當時未能回應有關請求。

本公會現就有關事宜聽取了及收到了各會員和律師的意見，並把相關意見反映在澳門律師公會的意見書內。

在法案分析(第一文本)的基礎上，並經整理和編排所收到的意見後，澳門律師公會編製了本意見書，內容涉及整個《打擊電腦犯罪法》，而非只針對法案修改的部份。

基於系統編排原因，首先呈上引言，接著是針對第 11/2009 號法律的細則性分析，包括法案的修改，最後是結論。

[1] 經八月二十一日第 42/95/M 號法令修改後並重新公佈的現行文本。

I

引言

法案的理由陳述說明須達致四個明確的目標：

a) 新增一項罪狀，把操作（非法或未經授權的）流動電信模擬發射站定為犯罪；

b) 配合第 13/2019 號法律《網絡安全法》，對中央人民政府駐澳機構所使用的電腦系統加強刑法保障；

c) 規定對儲存於澳門特別行政區以外的電腦數據資料提取副本以作為刑事訴訟程序的證據；及

d) 將違反職業保密犯罪獨立成罪，而且刑罰加重。

鑑於這些目的，且基於對條文的分析，我們將在意見書內就一些內容的行文提出完善建議。

在細則性分析方面，我們也指出哪些規定是我們認為必須重新考量，以便與現行法律體系相協調。

為使到對我們就每一專門規定所持的立場更一目了然，以下是有關的細則性分析。

II

細則性審議第 11/2009 號法律《打擊電腦犯罪法》及法案所載的修改

1. 法案第一條 - 修改第 11/2009 號法律 – 第十二條第一款（二）項 – 各項的排序

顧名思義，第 22/2000 號行政法規《中央人民政府駐澳機構履行職責的保障及有關豁免》第一條所指的就是中央人民政府的機構，其位階高於第 13/2019 號法律《網絡安全法》規定的關鍵基礎設施營運者，因此，從系統編列上建議將之置於第（一）項。

另一方面，考慮到當犯罪標的為某些實體使用的電腦數據資料或電腦系統時將加重刑罰，我們認為應嚴格界定法律適用的主體範圍，因這牽涉到權利、自由和保障。

需指出，列舉關鍵基礎設施的公共及私人營運者但省略中央人民政府駐澳機構的做法，於第 13/2009 號法律第四條（適用的主體範圍）亦曾使用過。我們認為，在網絡安全層面上不提有關機構，但在電腦犯罪層面上則有所提及，不是最理想的立法技術。既然理由陳述強調法案的其中一個目的是"確保能更好地配合第 13/2019 號法律《網絡安全法》"，不明白為何有此立法取向，建議重新考慮。

2. 法案第一條 - 修改第 11/2009 號法律 – 第十六條第一款（六）項 – "在有理由相信擬找尋的資料儲存在初步調查所針對的電腦系統的不同部分或其他電腦系統內，且透過初始系統查閱或獲取該等資料屬合法的情況下，迅速搜索或以類似搜索方式進入該等不同部分或其他電腦系統。"

第 11/2009 號法律第十六條第一款（六）項規定：

"一、當有理由相信某電腦數據資料有助刑事調查工作，則有權限司法當局可透過批示許可或命令採取以下措施，並應儘可能由該司法當局主持：

（……）

（六）在有理由相信擬找尋的資料儲存在位於澳門特別行政區的某電腦系統或其某部分內，且透過初始系統查閱或獲取該等資料屬合法的情況下，迅速搜索或以類似搜索方式進入該電腦系統。"

雖然法案沒有修改第一款的序文，但我們認為"儘可能"的表述意思十分含糊，應先釐清在法律使用該詞的原因，然後正確地界定並列出所考慮的例外情況，盡量減少現有行文不清晰之處。

法案擬刪除第十六條第一款（六）項中"位於澳門特別行政區"的表述，內容改為*"在有理由相信擬找尋的資料儲存在初步調查所針對的電腦系統的不同部分或其他電腦系統內，且透過初始系統查閱或獲取該等資料屬合法的情況下，迅速搜索或以類似搜索方式進入該等不同部分或其他電腦系統。"*

亦即，法案擬擴大刑事警察機關的行動範圍，讓這些機關能查閱位於澳門特別行政區以外的其他伺服器的數據，甚至可包括雲端資料。

按理由陳述[2]所指，*"屬以下情況，澳門特別行政區司法當局繼續須訴諸國際司法互助機制：*

- 不具備上述要件時（資料屬可公開查閱或取得依法獲許可者的同意）；或

[2] https://www.al.gov.mo/uploads/attachment/2019-07/692345d3ab6588a0ba.pdf

- 所實施的並非單純查閱和取得已儲存資料副本的措施，而是諸如扣押數碼載體實體、實時截取數據及查閱路由數據資料等的其他措施時。"

理由陳述指出了一些在國際法律秩序中慣常採用的實務性理據，並列舉葡萄牙、西班牙及比利時的一些同類規定作為例子。

然而，有必要注意的是，葡萄牙的相關規定明顯有別於第 11/2009 號法律第十六條的內容。

接下來，我們將指出一些制度上的差異，以便理解澳門特別行政區現行的制度，以及瞭解修改建議的實際重要性。

首先，第 109/2009 號法律（**葡萄牙**的《網絡犯罪法》）第十五條規定允許在他人之電腦系統進行搜索/搜尋。

該條第一款規定："如在訴訟程序進行期間，為查明事實真相而有需要調查證據，而取得存於某一信息系統內之特定電腦資料，則有權限之司法當局以批示許可或命令在該信息系統內進行搜尋，但應盡可能由該司法當局主持。"

在**澳門**，不同的是第 11/2009 號法律第十六條中已有由有權限的司法當局核准的一系列更廣泛措施的規定（對此，其有義務主持該措施）。即：

（二）即時查閱及收集涉嫌人所使用的通訊或服務的路由數據資料，而該等通訊或服務是與透過澳門特別行政區內某電腦系統所傳送的特定通訊有關；

（三）命令某人將其持有或由其控制的電腦數據資料交出，而該等數據資料是儲存在某電腦系統內或某電腦數據資料儲存載體內；

（四）命令某互聯網服務提供者將其持有或由其控制的關於其互聯網

服務的登記用戶的基本資料交出；

（五）命令某互聯網服務提供者採取迅速移除或阻止他人查閱特定及不法的電腦數據資料的措施；（第 11/2009 號法律第十六條第一款）

在澳門特區，另一個不同的是，"*當刑事警察機關基於有依據的理由相信某電腦數據資料與犯罪有關而可作為證據，且如不採取措施將有可能失去該電腦數據資料，或如延遲採取措施可對具重大價值的法益構成嚴重危險，則即使未經有權限司法當局預先許可，亦可採取上款所指的措施。*"。也就是說，警察當局在未經法院預先許可的情況下，可以進入例如一台電腦或智能手機，以及查看、複製和監察該等數據，只要有充分理由認為數據資料與犯罪有關而可作為證據並有緊急性去取得。

即使如此，須立即將所實施的措施通知有權限司法當局，並由其在最遲七十二小時內審查該措施，以便使之有效，否則該措施無效（第 11/2009 號法律第十六條第三款）。

例如，屬即時查閱及收集涉嫌人所使用的通訊或服務的路由數據資料，而該等通訊或服務是與透過澳門特別行政區內某電腦系統所傳送的特定通訊有關的情況，及後，由於顯示出構成實施犯罪的根本證據的數據可能丟失的緊急性，故緊急地將收集所涉數據擴展至被針對人的個人電腦，因為所需的資料可能載於該電腦系統內。

要注意的是，在這種情況下，初步調查是得到了批准的，而續後調查則沒有批准。

在**葡萄牙**，有關制度規定僅在下列情況下才可未經有權限司法當局預先許可進行電腦搜尋："a）獲可處置或控制該等數據的人自願同意，只要該同意以任何方式記錄於文件上"〔第 109/2009 號法律第十五條第三款 a）項〕；僅在懷疑有恐怖主義、暴力犯罪或有高度組織的犯罪的情況下，方可

排除其同意〔第3）項〕。在任何情況下，都需要有權限的司法當局事後確認其有效性。

然而，**葡萄牙**刑事警察機關的這項權力，並沒有延伸至**葡萄牙**《網絡犯罪法》第十五條第五款所規定的程序，而這一規定正是澳門第11/2009號法律第十六條第一款（六）項的淵源。

也就是說，未經法官許可，不得使用葡萄牙《網絡犯罪法》第十五條第五款規定的手段。

在**澳門**，刑事警察機關未經有權限司法當局事先批准，得進行澳門第11/2009號法律第十六條第一款(六)項所規定的擴大搜索。

而上述第十六條並沒有提及在未經有權限司法當局事先批准的情況下，被針對者的同意是實施上述措施的要件。也就是說，在澳門，未經有權限司法當局的預先核准及被針對人的許可，仍可實施有關措施。

儘管如此，我們認為，為了維護居民的權利和保障，應透過第11/2009號法律第十四條的準用，適用《刑事訴訟法典》第一百五十九條及續後各條規定的搜查及搜索制度。

可得出的結論是，按葡萄牙《網絡犯罪法》第十五條所規定的制度，除上述的情況外，法律文義上禁止在沒有得到有權限司法當局的許可下進行遙距監視（隱蔽的，即不需要刑事警察機關身處電腦實際所在的地方）。

此外，葡萄牙《網絡犯罪法》第十九條明確指出隱藏的行動，並引用了葡萄牙第 101/2001 號法律（為預防及調查犯罪而隱藏的行動的法律制度），但第二款規定："如有需要使用電腦工具及裝置，在適用之情況下，須遵守為截取通訊所定之規則。"

關於此問題，須指出的是，葡萄牙《網絡犯罪法》第十八條規定了通

訊截取制度，規定"僅在有理由相信該措施對發現事實真相屬必要，又或以其他方式無法取證或取證非常困難時，才可透過預審法官具理由説明的批示及由檢察院聲請，許可在偵查期間截取及記錄發送的電腦數據資料。"(該條第二款)

此外，"截取可以是記錄與通訊內容有關的數據資料，或僅收集和記錄路由數據資料，而上款所指批示應按照調查的具體需要，詳細説明相關範圍"。(該條第三款)

因此，在利用電腦工具進行刑事調查的實際操作方面，葡萄牙法律本身已有明確的劃分和規範。

在**澳門**，有疑問的是，擬修改的第 11/2009 號法律第十六條第一款(六)項規定的進入私人電腦系統的範圍，根據法案的規定，是否指在現場對電腦系統進行調查，且被調查對象是知悉的，抑或相反，是指除了適用搜查及搜索制度外，還會進行遙距監控，尤其是為了查閱澳門特別行政區境外的數據資料。

第一種情況是刑事警察機關現場進入電腦系統，查閱和收集數據資料作為證據，因此，該立法取向是為了加快刑事調查，及避免因法律程序的延誤導致失去重要的犯罪證據。

但須指出，在這種情況下所進行的是搜索，故本法理應有一條規定，準用經適當配合後的《刑事訴訟法典》第一百五十九條及續後數條規定的搜索制度。

雖然有一條一般規定準用《刑事訴訟法典》所載的規則(《刑事訴訟法典》第十四條)，但與扣押電子郵件的做法(第十五條第五款)有所不同，沒有一條規定將該搜索等同於訴訟法現有的搜索制度。

而準用該制度的話，就可以說，例如"*如搜索律師事務所或醫生診所，搜索須由法官親自在場主持，否則無效；如有代表該職業之機構，則法官須預先告知該機構之主持人，以便其本人或其代表能在場。*"(《刑事訴訟法典》第一百六十二條第三款)。

與之不同的情況是，有關搜索是對進入他人電腦系統的電腦進行的，而刑事警察機關無需前往該電腦系統具體所在的地方。

這一問題變得重要，同樣是因為葡萄牙的法律與法案的修改有另一個不同之處，就是在葡萄牙該行為被稱為搜尋，並將搜尋等同於搜索(《葡萄牙網絡犯罪法》第五條及第六條)，而澳門則沒有規定何謂第 11/2009 號法律第十六條第一款(六)項所指的"*搜索或以類似搜索方式進入*"，也沒有像前面所說的那樣，將其等同於《澳門刑事訴訟法典》的搜索制度。

有疑問的是，"*以類似搜索方式進入*"是否屬於一種隱蔽式監察，因而，根據第 11/2009 號法律第十六條第二款的規定，可以在未經預先許可下進行(但亦須由有權限司法當局在採取該措施後的七十二小時內追認其效力)。

也就是說，倘若當第十六條第一款(六)項提到搜索"*其他電腦系統*"，而該搜索是未經預先許可進行時(第二款)，是否僅指在該電腦設備(例如，涉嫌人的電腦)所在的地方進行的搜索，抑或是，還可以透過電腦設備及裝置進行隱蔽行動(遙距進行的電腦措施)。

此外，若我們理解，一方面，法律希望搜索是僅指進入現場的電腦系統，而另一方面，應根據本法律第十四條的規定，適用訴訟法的搜查及搜索制度(正如立法會關於第 11/2009 號法律的第 3/III/2009 號意見書[3]所指出的那樣)的話，那麼，便會有疑問，當法律提到"*以類似搜索方式進入……*

[3] https://www.al.gov.mo/uploads/lei/leis/2009/11-2009/parecer_cn.pdf

其他電腦系統"時想指的是甚麼，尤其是這些數據資料可能不在澳門特區。

然而，在**澳門**，儘管本法的規定有其特殊性，但本法只作出一次準用一般制度。

在此還要分析，第 11/2009 號法律第十六條第一款(六)項提出的修改如何允許取得儲存在雲計算服務的數據資料，因為基於上述所言，可以用電腦設備進行刑事調查。

以下是適用《修改第 11/2009 號法律〈打擊電腦犯罪法〉》法案中修改的第十六條第一款(六)項的實例：

"*在瀏覽嫌疑人的電腦後，發現只有極少資料有重要證據價值，但有線索表明重要的資料儲存在雲端。而在查閱該電腦的互聯網瀏覽器書籤後，確實發現該雲端儲存服務的連結。在選擇該連結後，發現登入碼已被記錄，因而只需按下登入就能查閱所需的資料。*

當檢察院準備根據《網絡犯罪法》第十五條第五款的規定，許可將搜尋延伸至該用戶在雲端的帳號時，卻發現該雲端的總伺服器在德國，其他伺服器在荷蘭、比利時和愛爾蘭。有人問：是否可以合法地按下登入，以查閱及扣押儲存在其他國家的資料?抑或是有關搜尋及扣押是被禁止的，否則會侵犯被搜尋國家的主權，所以必須透過現有的司法協助機制進行?若果要找尋的資料可能在黑暗網站(Dark web)，無法確定是儲存在哪一個國家，那該如何?若果資料是同時儲存在不同的國家，是否會進行複製、拆散? 問題並不容易解決"[4]。

這裏需要釐清的是，對進入位於澳門特別行政區以外的數據資料，如

[4] 上述例子載於"O DOMÍNIO DO IMATERIAL: PROVA DIGITAL, CIBERCRIME E A TUTELA PENAL DE DIREITOS INTELECTUAIS (非物質領域：電子證據，網絡犯罪及知識產權的保護)"研究第 57 頁, http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_ProvaDigital.pdf

何能有效地進行管控。"位於澳門特別行政區的電腦系統"是目前實施第11/2009號法律第十六條第一款（六）項的主要要件，如將此要件刪除，則澳門特別行政區的刑事警察機關確實可以進入技術上儲存在另一司法管轄區內的電子數據。

在實踐中，要查找雲計算服務提供者的所在地，以及知道其是否擁有國家伺服器，在大多數情況下往往難以滿足迅速取證的需要。

因此，關於為獲取儲存在其他國家主權領土內的數據而要求提供司法合作的通知義務，實際上有可能不被尊重。還有可能出現的情況是，與相關國家之間沒有任何法律和司法互助的條約或類似的協定。

在學術討論上，一直以來均認為有必要透過司法互助來查閱儲存在不同司法管轄區的數據，但仍然有實務操作是反其道而行的。司法當局在行動時認為這類侵犯主權的情況不會造成任何損害，故認為這類違反屬微不足道，且由於證據會快速損毀，有必要介入國外的數碼環境以獲取其內儲存的數據。

歐洲委員會的 *Transborder Group* 發表了如下聲明："*As noted by the T-CY previously, given these limitations and in the absence of a clear, eficiente and feasible international legal framework, governments increasingly pursue unilateral solutions in practice. It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud services accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country*"[5]

[5]網絡犯罪委員會，*Criminal Justice Access to electronic evidence in the cloud: Recommendations for*

關於理由陳述中提出的第一種需訴諸司法互助的情況，即"*不具備上述要件時(資料屬可公開查閱或取得依法獲許可者的同意)*"，需要指出的是，在第 11/2009 號法律中沒有任何必須獲得被針對人同意的規定（與前述的葡萄牙制度相反）。

然而，雖則沒有直接準用（與扣押電子郵件的情況相反，第 11/2009 號法律第十五條規定，對扣押電子郵件適用經必要配合後的《刑事訴訟法典》第一百六十四條及第二百三十五條所載的制度），但根據立法會第 3/III/2009 號意見書（關於第 11/2009 號法律）的內容，對於有關的搜索同樣應適用《刑事訴訟法典》第一百五十九條及續後數條有關搜查及搜索的一般制度〔尤其是第一百五十九條第四款 a）項、b）項及 c）項的前提〕，故必須得到被針對人的同意。

雖然如此，當有關查閱是以"*類似方式*"進行，且數據不在澳門特別行政區內時，同樣會對這一點產生疑問。

至於可公開取得的數據，則不存在任何問題，因為任何人都可輕易取得而無須任何許可。

另外，理由陳述中提到，當"*所實施的並非單純查閱和取得已儲存資料副本的措施，而是諸如扣押數碼載體實體、實時截取數據及查閱路由數據資料等的其他措施時*"，便需要司法互助。

然而，不知道何謂"*單純查閱和取得已儲存資料副本*"。問題是：查閱在雲計算服務中的數據是否被視為單純查閱？當打開嫌疑人的電腦，並因密碼已事先儲存而自動輸入後，任何持有該電腦的人士只需單純點擊一下

---

consideration by the T-CY，史特拉斯堡，歐洲委員會，二零一六年九月，載於以下網址：https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentJd=0900001 6806a495e

就可以進入雲計算服務，這就是單純查閱嗎?

然而，我們認為對電子函件（電子郵件或同類文檔）的查看及複印並不屬單純查閱，因為法律已訂定了專有的制度（第 11/2009 號法律第十五條第六款）。

這些都是在未經有權限司法當局預先許可的情況下進行的活動所要面對的一些重要問題，即使有關司法當局隨後否定由刑事警察當局根據第 11/2009 號法律第十六條第二款規定提出的理由，但可以肯定的是，活動當中已對一名居民存放於外國管轄區的個人資料進行了電腦搜尋。

如遵循《刑事訴訟法典》中有關搜查及搜索制度及其他規定，則無需對該居民作任何彌補，但如有關措施可能基於其技術元素而不等同於該制度時就另當別論了。

還須注意的是，第十六條的第一款（六）項的特別措施，似乎可與第一款其餘各項所規定的措施一併實施。

最後須說明的是，修改第 11/2009 號法律的法案並沒有從根本上改變現行的框架。然而，這次對法案的分析中，我們認為將之與葡萄牙的制度進行比較分析可使我們對刑事調查中的電腦搜索和搜尋範圍有更清晰的認識和思考，同時能瞭解到經是次修改後，因應透過電腦進行刑事偵查的範圍擴大，相關行動在實務上可達到什麼程度。

3. 法案第二條—增加第 11/2009 號法律的條文—第九-A 條—使用電腦裝置以模擬流動電信服務站

這一新規範使到有需要對罪狀作出清晰和明確的定義，因此，我們認為有需要定義何謂“流動電信服務站”。

例如，第 32/2000 號行政法規《發出公共地面流動電信服務臨時牌照的程序》第二條，當中準用國際電信聯盟所確立的含義來定義該行政法規所使用的概念。

有見及此，倘認為在行政法規中所採用的這種準用不是最理想的技術，那麼，考慮到針對同一法律現實需作統一規範的這個原則，且對於現時正分析的有關行文，我們認為最重要的是在法律中作出有關定義，原因是由此所衍生出的是刑罰而不僅僅是行政違法。

扼要而言，"非法的"偽基站是使用未經批准以從事電信活動的電信設備，透過如發送信息等的電話通訊途徑進行犯罪（尤其是詐騙）。

在澳門特區一直以來都有很多投訴是針對這個使用相對原始電信途徑進行的犯罪活動，而將之納入在第 11/2009 號法律內，是因為無法透過法律規定的其他罪狀對該行為予以處罰，但我們想強調的是，有關的刑罰必須透過一個清晰的定義予以支持。

4. 法案第二條—增加第 11/2009 號法律的條文—第九-A 條—使用電腦裝置以模擬流動電信服務站的第三款（一）項 "屬下列任一情況，刑罰為一年至五年徒刑：（一）行為人意圖營利或其目的為預備、便利或實施另一犯罪"

我們認為上述規範的下劃線部分是很難證明的，況且所涉及的是嫌犯的假定意圖，故適用該規定時可能會出現僅僅基於懷疑存有的意圖便作出的控訴和判刑，而這應該避免出現在刑法規範內。

5. 法案第二條—增加第 11/2009 號法律的條文—第九-B 條—不正當揭

露安全關鍵漏洞—"存有任何不正當意圖，向他人透露在執行職務時或基於職務原因而獲悉的有關系統、裝置或電腦程式的安全關鍵漏洞，即使屬暫時性的漏洞，而足以造成有實施本法律規定的犯罪的危險者，處最高三年徒刑或科罰金。"

經分析這條規範後，且考慮到有關的下劃線部分，我們認為這會令到該規定的適用是建基於嫌疑和意圖之上。

與此同時，除了向第三人透露事實這一點以外，整個規範都不具有任何客觀準則，這會使到出現基於懷疑存有的意圖而作出的控訴和判刑。

可以認為有關的規範是針對危險犯，故無需要實際上作出有關犯罪。

考慮到所有罪狀對於未遂都是可予以處罰的，那麼，針對共犯的情況，這一個罪狀如何與其他的罪狀相配合？倘"告密者"被證實為犯罪首腦或教唆犯，他會否因這一條的犯罪且基於另一個被實施的犯罪而以數罪併罰的形式被判刑？

6. 第十六-A 條"保存及提供網絡地址轉換紀錄"

這條規定是透過第 13/2019 號法律第二十六條而增加到第 11/2009 號法律的，當中規定的"網絡地址轉換(...)的紀錄"[6]是一個沒有被定義的技術用語。

我們認為應該將有關定義加入到條文內，以使法律字面含意更加清晰

[6] 我們認為立法者想表達的是英語所指的"*network address translation*"。這個概念亦名為 *masquerading*，指的是使用雜湊表來自我重寫的技術，即來源 IP 地址封包通過路由器或防火牆令內部網絡的電腦得以連線至外部或全球資訊網。

和避免出現錯誤解讀。

7. 法案第四條—重新公佈—"(...)加入本法律及第 13/2019 號法律《網絡安全法》通過的修改"

從立法技術而言，將多個針對同一個法規進行的立法修改統一集合在一個文件內，這是一個很好的做法，因此，我們同意重新公佈法律。

8. 法案第五條—生效—"二零一九年十二月二十二日"

對於將法案生效日期定於十二月二十二日以便其與第 13/2009 號法律《網絡安全法》同時生效，我們對這一做法予以肯定和認同。

III

結論

經對各條規定作出闡述後，我們總體的結論如下：

a）**國際協調的需要**

從第 11/2009 號法律的現行條文以及法案所作的修改來看，沒有任何篇章或規定專門用於處理國際合作。

對比葡萄牙的《網絡犯罪法》，葡萄牙的法律就這一事宜訂定了一個共有七條條文的完整篇章。

另外，還應考慮《刑事訴訟法典》第六條（刑事訴訟法在空間上之適用）的規定。該條規定："刑事訴訟法適用於整個澳門特別行政區，且在適用於澳門特別行政區之國際協約及屬司法協助領域之協定所定之範圍內適用於澳門特別行政區以外。"

由歐洲委員會成員國及其他締約國於 2001 年 11 月 23 日在布達佩斯共同簽署的《網絡犯罪公約》不適用於澳門。根據《網絡犯罪公約》解釋報告第三部份第 16 點的規定，該公約的主要目標是：

- 使國家的刑事實體法領域內有關違法行為的元素與網絡犯罪有關的規定相協調；
- 按域內《刑事訴訟法典》的規定，針對有關違法行為、透過電腦系統作出的其他的違法行為以及與該等違法行為有關並以電子方式存在的證據，訂定調查及提起刑事程序的必要權力；
- 創建快速有效的國際合作制度。

因此，對於國際合作作出適當考慮屬必要的，我們認為只有這樣，打擊電腦犯罪的法律才能取得成功。

我們認為，為了使國際合作有效，且有鑑於布達佩斯《公約》是由包括歐洲委員會成員國在內的多個國家簽訂，特區政府應在域內法的層面上採取方案並在必要時作適當調整。

b) **對第十六條第一款(六)項**的修改不是根本性的修改，只是革新了刑事警察機關可把搜查延伸至澳門特別行政區司法管轄權以外雲計算服務中保存的數據。這不是一種新的，亦不是一種非一般的做法。

然而，不妨礙上述所作的闡述，我們還想強調的是，《修改第 11/2009 號法律〈打擊電腦犯罪法〉》法案內，沒有明確在跨境網絡方面第十六條規定的特別措施是怎樣實施，但相信總是要配合《刑事訴訟法典》規定的證據制度來處理。

c) **我們認為應考慮對第 11/2009 號法律作更深入的修訂。**有鑑於現實狀況及電腦領域的科技發展，立法者應更加關注比較法方面的立法演進，以保障這領域的法規適時及有效，因此，應考慮採用其他國家的解決方案。

d) 另一方面，藉由澳門的法例與其他司法管轄區的法律**相協調**，能避免有人利用漏洞實施越趨複雜的國際犯罪。我們建議把《網絡犯罪公約》的標準視為立法目標。因此，我們認為，澳門特區政府應努力採取布達佩斯《公約》所載的一系列解決方案，當然要作出必要的調整。

由於時間所限，這是我們提交立法會第一常設委員會考慮的意見。

澳門律師公會理事會二零一九年十一月十四日會議通過

(簽名見原文)