



## 理由陳述

# 修改第 11/2009 號法律《打擊電腦犯罪法》 (法案)

### 1. 目的

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；
- 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。



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
行政長官辦公室  
Gabinete do Chefe do Executivo

此外，基於第 13/2019 號法律已規定在第 11/2009 號法律內新增一章（第三-A 章，包括第十六-A 條及第十六-B 條），並考慮到現新提出的修改，建議重新公佈《打擊電腦犯罪法》，以便更好保障法律的穩定性，以及讓市民更容易瞭解相關法律。

## 2. 將偽基站定為犯罪

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，並與之連接。從技術層面而言，當手提電話裝置與此類基站連接時，並不能確定基站是否正當；而手提電話裝置的設計是為了優化通訊，故會自動搜尋並連接最接近的電信基站，因為通常基站越近，訊號越強。

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）。

此等行為不僅使該區居民、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。



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
行政長官辦公室  
Gabinete do Chefe do Executivo

鑑於上述情況，司法警察局持續打擊與偽基站有關的犯罪活動，自二零一四年十一月起至二零一七年八月中旬，共採取十七次打擊偽基站的行動，搗破八十六個偽基站，並將六十六名涉嫌人移交檢察院。

然而，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。

另外，與偽基站有關的犯罪（即利用虛假電信基站為作案工具的犯罪）的涉嫌人大多為內地居民，因此，根據澳門現行的法律規定，倘有關犯罪可處的徒刑最高為三年，便無法對上述人士採取羈押措施；目前，大多數情況是將相關人士驅逐出境，並對其採取禁止入境措施。

再者，對於操作偽基站的人士，他們可辯稱他們沒有犯罪（詐騙、不法賭博等等），只是單純操作未經授權的基站，而根據澳門法律的規定，這一事實本身只屬行政違法而非構成犯罪，根據第7/2002號行政法規《經營地面流動公共電信網絡及提供公用地面流動電信服務》第二十六條的規定，科處澳門幣十二萬至一百萬元罰款及立即關閉設施。

綜上所述，目前的法律並不利於打擊操作偽基站此等既讓犯罪分子攫取豐厚利潤、又對市民生活和澳門特別行政區形象遺害深遠的違法活動。



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
行政長官辦公室  
Gabinete do Chefe do Executivo

此外，亦曾嘗試根據第 11/2009 號法律第八條規定遏止這種行為，但沒有取得成功，故司法機關認為犯罪分子不會干擾合法網絡營運者發射訊號的正常運作。

故此，本法案規定在第 11/2009 號法律內新增一項條文（第九-A 條），將使用與發射器械有關的電腦裝置及程式以模擬地面流動公共電信服務站的行為列為危險犯罪（不論具體損害結果為何），可處以最高三年徒刑。

— 就該行為的社會危害性而言，倘若在某些情節中顯示其具有更高的可譴責性及客觀嚴重性時，刑罰幅度應為一年至五年，且大體上允許採取羈押措施。這些具更高譴責性的情節尤其包括以下三種：如行為人意圖從偽基站獲利；如行為人使用偽基站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、賣淫或不法賭博活動；又或如設置偽基站係用於預備、便利或實施另一犯罪。

最後應強調一點是，本次修法並非擬將設置未經授權的電信基站此一行為定為犯罪，以保護無線電頻譜的完整性及專屬性的法益，而是將以不正當的方式隱蔽地使用與發射器械有關的電腦裝置及程式以模擬電信基站的行為定為犯罪，從而保護市民的隱私，防止不法分子使用該等偽基站作為犯罪工具。



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
行政長官辦公室  
Gabinete do Chefe do Executivo

### 3. 加強對關鍵基礎設施營運者和其他重要實體的電腦系統的刑法保障

隨着政府、企業、機構及市民對互聯網絡的依賴程度越來越高，針對電腦系統的攻擊亦逐漸增多。二零一七年五月和六月，“Wannacry”及“Petya”兩波勒索病毒攻擊席捲全球，澳門亦有部分電腦系統遭到入侵。

雖然兩次攻擊均未波及澳門基礎設施的電腦系統，但鑑於網絡攻—防不勝防，一旦此等系統遭到惡意攻擊，可能會嚴重干擾電訊網絡及其他主要服務的正常運作，甚至會出現公共服務癱瘓的情況，危及社會穩定。因此，我們必須居安思危，未雨綢繆，正如各地政府亦注意到這種新型犯罪的演變趨勢並有採取預防措施。

故此，澳門特別行政區適宜藉着修法，擴大對關鍵基礎設施營運者電腦系統的刑事保護，而不論其屬公共或私人性質，一如第 13/2019 號法律所規定的。

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。

#### 4. 提取澳門特別行政區以外的電腦數據資料副本作為刑事訴訟程序的證據

隨着雲計算服務的普及，網絡資訊跨越地域界限及不同司法管轄區，成為了刑事調查的重大法律障礙；在某些情況下，這些障礙甚至可使調查中斷，導致不能作出處罰。

根據第 11/2009 號法律第十六條第一款（六）項規定，司法當局可“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。”

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。



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
行政長官辦公室  
Gabinete do Chefe do Executivo

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。

某程度上，這個解決方案亦跟比利時法律所採用的相似。比利時  
— 《刑事訴訟法》第三十九 *bis* 條規定，只要懷疑資料並非儲存在比利時，便可將電腦檢索的範圍擴展到其他司法管轄區，不論其所在地為何，而資料僅會被複製而不會被刪除，並在可辨識相關國家的情況下，由司法部長將有關事宜通知被檢索的國家（實際上，似乎從未發生此等情況）。

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。



## 5. 將違反職業保密犯罪獨立成罪

正如一般規則的危險罪，《刑法典》第一百八十九條規定，違反職業保密者，處最高一年徒刑，或科最高二百四十日罰金。另外，第一百九十條亦規定，利用因自己的身分、工作、受僱、職業或技藝而知悉的有關他人的商業、工業、職業或藝術等活動的秘密，而造成他人或澳門特別行政區有所損失者（如毀損罪），處同等刑罰。

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係統、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）。