

編按：本文在“第十四屆海峽兩岸暨香港、澳門警學研討會”中獲選為現場發表論文，該次研討會的主題是“優化智慧警務效能與跨境警務合作”。

# 探討澳門電子商務領域的 犯罪型態及防治對策

澳門司法警察局副督察 劉敏玲

【摘要】受經濟全球化與社會資訊化的帶動，加上電子網絡技術日漸成熟，消費者消費觀念及消費模式逐漸轉變，使電子商務在全球貿易中的地位和作用日益彰顯。在新型經濟發展理念“互聯網+貿易”的態勢下，電子商務已成為經濟發展的一種新興業態。然而，由於各國及地區政策制度及法律法規的差異性和滯後性，在電子商務迅速發展的同時，電腦資訊技術這把“雙刃劍”也為一種新的犯罪——電子商務犯罪創造了條件，嚴重威脅着電子商務的交易安全。

本文將闡述澳門電子商務發展的情況，探討澳門電子商務領域的犯罪問題及成因分析，從而提出防治對策。

【關鍵詞】電子商務 電子支付 第三方支付 電子商務犯罪

## 一、前言

隨着網絡的普及應用，為企業帶來商機，許多經濟行為隨之改變，此股熱潮不僅對企業帶來衝擊和轉機，也引導使用者進入一個虛擬商城的購物世界。電子商務的運營方式不僅改變了企業的商貿方式，還完全改變了消費者的消費觀念及消費方式，這種沒有店面的網絡商店、沒有櫃台的網絡銀行、沒有營業場所的網絡證券商、沒有會場的網絡研討會、沒有紙張的電子書店和數碼化圖書館及博物館等等在互聯網世代十分普遍。

電子商務是建立在開放性數碼資訊網絡上的經濟活動，是在資訊基礎設施上建立起來的一種新的經濟模式，它不僅擴大一個國家或地區的網絡經濟市場規模，更成為新的經濟增長點和經濟轉型的引擎。電子商務是現代新技術集成的一種新型經濟運營模式，與傳統商務活動相比，由於網絡交易的虛擬性、隱蔽性、跨地域性，電腦資訊技術這把“雙刃劍”為電子商務領域的犯罪創造了條件，它不僅具有傳統

財產型犯罪的特徵，更成為資訊時代的一種特殊的社會現象。

在促進跨境經濟合作發展的態勢下，澳門特區政府透過多項政策制度促進跨境電子商務發展的廣度與深度。隨着電子商務的迅速發展，近年澳門地區涉及電子商務領域的犯罪呈上升趨勢。

## 二、電子商務發展概述

### （一）電子商務的含義與發展

電子商務的概念出現於1996年，當年IBM提出了Electronic Commerce (E-Commerce)的概念，其後又於1997年提出了Electronic Business (E-Business)的概念，兩個概念的內涵和外延不同，前者強調電子交易，後者強調電子商務。<sup>1</sup> 電子商務是指在網際網絡（Internet）、內部網絡（Intranet）和增值網（VAN, Value Added Network）上以電子交易方式進行交易活動和提供相關服務，是傳統商業活動各環節的電子化、網絡化，可讓買

賣雙方在互不謀面下進行各種商貿活動，例如：網絡購物、商戶之間的網上交易和線上電子支付，以及各種商務活動、交易活動、金融活動和相關的綜合服務活動的一種新型的商业運營模式。

電子商務經過多年的發展，其競爭日趨全球化和白熱化。過去幾年，全球電商銷售持續成長，市場研究機構eMarketer發佈的《2017全球電子商務平台》報告預估，全球零售電商銷售額將從2017年的2.29兆美元增長至2021年的4.479兆美元。而隨着大數據、人工智能、區塊鏈等數碼技術與電子商務加快融合，線上電子商務平台與線下傳統產業、供應鏈配套資源加快融合，將構建更加協同的數碼化生態；社交網絡與電子商務運營加快融合，將構建更加穩定的用戶關係；電子商務還將進一步促進內外貿市場融合，加快資源要素自由流動。

## （二）澳門地區電子商務的發展

透過電子商務，中小企業能夠以廉宜及迅速的方式與全球的貿易伙伴進行交易，締結強大的環球網絡伙伴關係。同時，中小企業可藉着網上無遠弗屆的廣泛宣傳，創造新的經營模式，開拓無限商機。2004年，內地跨境電商興起之初，澳門企業對電商還不太接受，很多人覺得做實體店已經足夠。直到2016年，隨着線上支付在澳門不斷普及，澳門電商才慢慢興起，不少澳門企業意欲染指跨境電商業務，但無奈在物流、通關等方面仍有不少制肘。

2016年初，澳門特區政府將發展電子商務正式列為“促進經濟適度多元”的施政重點之一，隨後推出“電子商務推廣鼓勵措施”及“中小企業和青年創業援助計劃”等一系列政策措施，扶持和鼓勵澳門各界企業和青年人利用互聯網技術發展電子商務。澳門特區政府經濟局於2017年推出“跨境電商一站式服務”，為澳門中小企業提供線上銷售、處理訂單、貨

表一：認可電子商貿營運商名單

認可電子商貿營運商	網站
阿里巴巴香港有限公司	www.alibaba.com www.alibaba.com.cn
eBAY香港有限公司	www.ebay.com.hk
香港貿易發展局「貿發網」	www.hktcdc.com
利達通黃頁有限公司	www.yip.com
焦點科技股份有限公司	www.made-in-china.com
環球資源	www.globalsources.com

資料來源：澳門貿易投資促進局

運物流及回收貨款等一站式服務，吸引眾多中小企業加入。<sup>2</sup>

澳門電子商務的發展相對鄰近地區而言起步較晚，但在政府政策大力支持下，近年發展迅速。截至2018年8月，澳門已有69家企業從事跨境電商，備案產品二千項，涉及伴手禮、化妝品、保健品、葡萄酒、沙丁魚及橄欖油等特色商品，累計銷往內地的產品貨值約六千萬澳門元。<sup>3</sup>而透過“電子商務推廣鼓勵措施”獲認可的電子商貿營運商至2018年共有六家（詳見表一），而獲認可的B2C電商平台則共有13家（詳見表二）。

除了澳門特區政府積極推動電子商務發展外，我們可見澳門居民的上網率、網民數目及消費模式的轉變，亦直接推動着電子商務的穩步發展。澳門互聯網研究學會發佈的《澳門居民互聯網使用趨勢報告2018》<sup>4</sup>指出，澳門居民的上網率從2001年的33%上升至2018年的84%，高於全球平均水平（54%）及亞洲平均水平（48%），與歐洲平均水平（85%）相若，在亞洲處於領先位置。澳門居民中，年齡由6至84歲的網民規模從2001年約13萬人穩步擴大，至2018年達50.9萬人。網民通過互聯網進行各類活動，以社交、溝通、資訊為主。而最多網民使用的社交網絡平台是微信及Facebook，當中微信使用率呈逐年上升趨勢，由2013年的46%，增長至2018年的74%；手機網民的微信使用率為92%。

在6至84歲居民中，90%為成年居民，成年居民的上網率為83%。而52%成年網民有進行網上購物。在有網購的成年網民中，55%會使用網上支付，當中54%透過信用卡 / 銀行卡進行網上支付，43%透過支付寶進行網上支付，28%會使用微信支付，20%會使用網上銀行，透過澳門錢包MPay、PayPal進行網上支付的比率較低，皆為5%。而手機支付方面，在有使用手機支付的成年網民當中，59%會使用微信支付，50%會使用支付寶、17%會使用網上銀行APP、14%會使用澳門錢包MPay APP、2%使用Apple Pay。

### 三、澳門地區電子商務領域的犯罪問題

從上述數據，不難看見澳門電子商務的發展已滲透到經濟、社會生活的各個方面；伴隨電子商務的發展，電子支付業務應運而生，面

對這些改變，政府機關將如何因應各種電子商務所引發的問題及糾紛，例如：電子交易安全的法律問題、電子合同的法律問題、第三方支付平台的法律問題、客戶的隱私權問題等等，而制定相應的法律法規及監管制度，從而保障電子商務市場的良好競爭環境，正是澳門特區經濟發展過程中無可避免的問題。基於網絡交易的虛擬性、隱蔽性、跨地域性，以及法律制度不完善、監管缺位等問題，導致澳門地區涉及電子商務領域的犯罪問題近年日見凸顯。

#### (一) 電子商務犯罪的概念與分類

電子商務犯罪不是刑法規範意義上的類罪名或個罪名，而是在資訊時代電子商務應用中出現的、具有某種共同特性的諸多犯罪的集合。<sup>5</sup> 電子商務犯罪因具有傳統財產型犯罪的特徵，卻借助互聯網技術發展及資訊科技創新而為犯罪提供了便利條件，因此，電子商務犯

表二：認可B2C電商平台名單

公司名稱	電商平台名稱	網站
易網零售有限公司	西洋街	www.macaumarket.com
澳之城有限公司	“澳之城網上跨境購物平台”	“m.macaueshop.com” 在微信中搜“macaueshop”或“澳之城”
澳門網絡傳媒發展有限公司	大眾點評澳門站	www.dianping.com/macau
買野有限公司	澳門買野網	www.mineyeah.com
淘寶中國控股有限公司	天貓國際	www.tmall.hk
澳門電訊有限公司	澳門好幫手 – 購物	https://shopping.macaugoodhands.com
廣東廣新貿易發展有限公司	國通達	www.gtdmall.com
澳門購科技有限公司	洋品味商城	www.yangpinwei.cn www.yangpinwei.com
指南科技有限公司	澳指南商城	mall.macaucentral.com
中國工商銀行（澳門）股份有限公司	融e購澳門館	http://channels1.mall.icbc.com.cn/ channels/pc/operation/macau/index.html
惠澳科技有限公司	優優站	www.113m.com
澳門世寶一人有限公司	澳門世寶網上商城	www.macaushibao.com
麥迪科技有限公司	澳門街	www.macauo2o.com

資料來源：澳門貿易投資促進局

罪是網絡犯罪的延伸，是網絡犯罪的最主要表現形式。

關於電子商務犯罪的概念，由於界定方法的不同，形成的概念也有差異。內地有學者認為所謂電子商務犯罪，從犯罪學意義上的定義，是指利用電子商務資訊系統特性危害電子商務正常秩序，具有嚴重社會危害性的行為。<sup>6</sup>亦有學者認為，從刑法學意義上，應該表述為以互聯網為平台，行為人利用電子商務電腦資訊系統的特性，在電子商務活動中嚴重危害電子商務秩序和安全，觸犯刑法，應受刑罰懲罰的行為。<sup>7</sup>

根據不同的分類標準，學者把電子商務犯罪分為不同的種類。例如，有學者把電子商務犯罪分為屬於資訊的刑事犯罪及與資訊和通訊新技術相關的刑事犯罪。<sup>8</sup>根據攻擊對象進行的分類，可以分為針對用戶資訊進行的犯罪、針對商家和銀行進行的犯罪、針對認證中心進行的犯罪；而根據犯罪主體進行的分類，可以分為自然人進行的犯罪和單位犯罪。有學者把電子商務犯罪分為危害電子商務資訊系統的犯罪和以電子商務交易方式為作案工具的犯罪兩類，前者是以電子商務交易過程中的資訊、數據資源安全為攻擊對象，後者是以電子商務交易方式的跨國性、隱蔽性為掩護從事非法交易或其他破壞電子商務交易正常秩序的行為。

## （二）澳門地區電子商務領域的犯罪問題分析

以下將根據澳門司法警察局（以下簡稱司警局）有關資訊犯罪數據的統計（詳見表三），對利用電子商務交易方式來作案的犯罪<sup>9</sup>進行分析。

### 1. 透過電子郵件、互聯網及社交網站進行的詐騙

隨着互聯網的普及，資訊技術的不斷發展，電子郵件、各類社交網站、手機應用程式（APP）和電商平台等逐漸成為人與人之間資訊互動的媒介，更廣為商業界使用。根據司警局資料顯示，2016、2017、2018年期間涉及電郵、互聯網及社交網站進行的詐騙犯罪分別有

204宗、200宗及260宗。有關詐騙犯罪的主要方式及手法如下：

#### （1）假商務電子郵件詐騙

國內外公司或機構仍然習慣使用電子郵件與客戶聯繫，給予騙徒或詐騙集團可乘之機。這從司警局於2019年5月3日破獲的一宗發送假電郵要求受害人將貨款匯到澳門的案件中可見一斑。該案件發生於2017年，一家英國藥業公司舉報指懷疑有黑客入侵該公司電腦系統，監視運作及匯款程序。期間，該公司職員收到假電郵，並按指示匯出395,340美元（折合約308萬港元）至澳門某銀行帳戶。在匯款後，更遭對方勒索，要求購買六萬美元的虛擬貨幣，否則將公開公司內部資料。經調查，被捕香港男子在澳門開設從事批發的空殼公司，在某銀行開立了三個帳戶，用作接收詐騙款項。<sup>10</sup>

這類假商務電子郵件詐騙案件的犯罪手法主要有：

##### a. 假冒公司電子郵件

攔截被害人公司的交易電子郵件，申請與公司電子郵件地址所用字符相似度極高（如：以1代替l、以vv代替w等）的假電郵地址，再以此偽冒電郵地址與客戶聯繫，收件客戶一時不察，便會按指示把款項匯至騙徒所提供的銀行帳戶。

##### b. 假冒公司老闆電郵

騙徒假冒老闆電郵向公司會計人員要求匯款至指定的銀行帳戶。

##### c. 假冒客戶電郵

假冒客戶發出電郵要求變更匯款帳號，並要求公司匯款至該指定的銀行帳戶。

##### d. 入侵公司的電腦系統及電郵帳戶

入侵公司的電腦系統或公司負責人的電郵帳戶，訛稱銀行帳戶已變更，藉以詐騙被害人將公司款項匯至騙徒指定的銀行帳戶內，直至受款一方反映未收到貨款時才知悉受騙。

#### （2）透過互聯網及社交網站進行的詐騙

隨着互聯網時代的來臨，各類社交通訊程式推陳出新，人們透過社交網絡平台進行商業活動也越來越普遍。由於海峽兩岸暨香港、澳門地緣接近，運輸成本相對便宜，加上近年內地盛行以電子支付作為交易媒介，電子支付從

表三：資訊犯罪數據統計

案件類別	2016年			2017年			2018年		
	專案調查	要求調查	小計	專案調查	要求調查	小計	專案調查	要求調查	小計
詐騙（涉及電郵、互聯網、社交網站）	179	25	204	162	38	200	217	43	260
電腦詐騙（涉及POS機）	25	13	38	15	8	23	70	37	107
電腦詐騙（騙積分）	6	3	9	10	1	11	6	1	7
電腦詐騙（涉及銀聯卡、提款卡、信用卡）	79	8	87	77	6	83	233	4	237
假冒網站	2	3	5	9	3	12	7	2	9
干擾電腦系統（偽基站）	4	3	7	7	5	12	19	8	27
不當進入電腦系統、不當獲取、使用或提供電腦數據資料、干擾電腦系統、用作實施犯罪的電腦裝置或電腦數據資料	39	4	43	73	7	80	42	6	48
總數：	334	59	393	353	68	421	594	101	695

資料來源：澳門司法警察局

最初主要用作網上購物，逐漸滲透到居民生活的各個環節當中，諸如訂送外賣、“打的”出行、乘搭公共汽車、購買城軌車票、高鐵票及電影門票等等，各類型電商平台、電子支付平台及手機應用程式（APP）相繼出現。

澳門與珠海僅一關之隔，內地的電子支付方式亦影響着澳門居民的消費模式，越來越多澳門居民前往珠海開設銀行帳戶。正如上文所述，澳門網民在網上購物的比率及使用網上支付的比率均已超過五成，分別為52%及55%，而使用手機支付的成年網民當中，最多人使用的是“微信支付”及“支付寶”；亦因應內地旅客不斷增多，澳門商戶紛紛提供“支付寶”、“微信支付”和“MPay”等支付方式。這些購物網站、電商平台、手機應用程式（APP）等社交網絡平台不僅促進了電子商務發展，為人們生活帶來便利，與此同時，透過社交網絡平台進行各種涉及電子商務的電腦詐騙犯罪亦層出不窮。

根據警方資料顯示，澳門地區在社交網

站透過“支付寶”、“微信支付”等電子支付進行的詐騙類型主要有：購物騙案、繳交購物保證金、購買網絡遊戲卡騙案、冒認購物網站管理員要求匯款、代刷銷量獲回佣騙案、招工騙案、兌換貨幣騙案、代收商品騙案、冒認友人要求購買點數卡或充值卡騙案、性交易詐騙等，尤其透過手機聊天程式向被害人表示可提供性服務，從而要求被害人到便利店購買“支付寶”購物卡、遊戲點數卡或充值卡等的性交易騙案近年亦有所上升。<sup>11</sup>

## 2. 涉及銀聯卡、提款卡、信用卡消費的電腦詐騙

涉及銀聯卡、提款卡和信用卡消費的電腦詐騙犯罪，主要是犯罪集團從一些存有漏洞的網站或其他方式盜取銀行卡資料後，再以網上消費方式進行詐騙。這類案件多以團伙方式作案，成員不限於澳門居民。

根據司警局資料（詳見表三），2016年期間涉及銀聯卡、提款卡和信用卡消費的電腦詐

騙案件為87宗，2017年為83宗，2018年則大幅飆升至237宗。2018年10至12月期間，司警局更接獲多宗舉報，案中被害人均是在一間外國旅遊網站消費後，信用卡資料隨即被盜用。經調查後，司警局於2019年1月25日成功拘捕七名年齡介乎15歲至28歲的澳門居民。該犯罪集團主腦透過身處內地的上線成員獲取盜竊所得的信用卡資料，其後僱用其他成員利用盜取所得的信用卡資料，購買網上遊戲虛擬貨幣或道具，該團伙成員最少利用40張信用卡的資料進行超過300筆網上交易，涉案總金額逾17萬澳門元。警方證實該外國旅遊購物網站存有漏洞，而在拘捕行動中，警方檢獲多台存有涉案信用卡資料的電腦，同時亦發現由內地上線成員提供的開設帳戶、綁定信用卡等操作的教學視頻。<sup>12</sup>

### 3. 利用銀聯POS機刷卡消費的電腦詐騙

“銀聯”是內地銀行界的銀行卡清算機構的品牌，它是一個支付系統，亦是金融業的一種結算系統。“銀聯”標識推出的目的是：為各種自動櫃員機（ATM）和銷售點終端機（POS）受理各商業銀行發行的銀行卡提供一種統一的識別標誌，以便不同銀行發行的銀行卡能夠在帶有“銀聯”標識的自動櫃員機和銷售點終端機上通用，為廣大消費者提供方便、快捷、安全的金融服務。目前，銀聯卡已經走向世界，可以在20多個國家的POS機和40多個國家的ATM機使用。

2017年1月5日司警局與澳門金融管理局在一次聯合搜查行動中，首次搗破一個非法改裝銀聯POS機的地下工場，查封八間從事非法刷卡套現活動的店舖，查獲10部違規刷卡機和現金750萬港元，拘捕涉案人員23人。<sup>13</sup> 2018年，銀聯POS機在澳門非法刷卡套現的案件更高達107宗，相比2016年的38宗和2017年的23宗，有大幅上升。

有關不規則使用銀聯POS機的行為，除了對銀聯國際帶來直接經濟損失外，更將原本發生在澳門地區的交易繞過銀聯國際，逃避銀聯國際的港澳正規消費網絡。交易發生地區經技術轉變而被扭曲及變得不真實，使銀聯及發卡銀行在風險監控系統內設置的監控參數發揮不

到應有作用，提高交易風險。<sup>14</sup> 據警方調查，不排除有不法之徒利用郵寄等其他方式輸送刷卡設備來澳，藉以加大警方的追查難度。

### 4. 虛假網站詐騙

2016至2018年這三年內，這類假冒網站的詐騙案件合共26宗（詳見表三），主要有假冒銀行網站及博企網站這兩大類型。在假冒銀行網站的詐騙犯罪中，犯罪集團以澳門某銀行名義設立虛假銀行網站，並假冒銀行名義發送電郵給客戶，要求收件者瀏覽相關虛假網站，更新或核實網上銀行帳戶資料，藉以騙取收件人的銀行帳戶及登錄密碼。然後團伙成員非法登錄銀行帳戶，將帳戶內款項轉入其他團伙成員的銀行帳戶或信用卡帳戶內。經警方調查發現，非法登錄銀行帳戶的IP地址往往來自美、英及東南亞等國家，而策劃提款的團伙成員之聯絡電話則來自東南亞國家，負責取款的人是澳門居民。這種涉及多國或多地域的跨境犯罪，大大增加警方的追查及搜證難度。

在假冒博企網站的案件中，犯罪集團盜用澳門一些附有博彩場所的著名酒店或渡假城的名稱、商標、圖片及客戶服務專線作誤導，並設立虛假博彩網站進行網上博彩，甚至以欺詐手法套取個人及信用卡資料來實施詐騙犯罪。為了有效打擊這類博彩犯罪，司警局主動查核及分析假冒澳門博企的名義設立虛假網站進行網上博彩或實施詐騙等犯罪，要求外地相關網域註冊公司或伺服器寄存公司對464個存在詐騙成份的博彩網站採取屏蔽措施或將之“下架”，至2018年底成功停運其中361個相關網站，防止網民因登入虛假博彩網站墮入詐騙陷阱。<sup>15</sup>

### 5. “偽基站”詐騙

偽基站設備是指未經監管部門許可的非法無線電通訊設備，能夠搜尋一定範圍內的流動電話號碼，例如IMSI（International Mobile Subscriber Identity，國際移動用戶識別碼），並可虛構任意電話號碼，例如他人的電話號碼或公用服務號碼向流動電話用戶發送各類短訊，經常用於詐騙和商業宣傳等。<sup>16</sup>

由於偽基站可向一定範圍內的流動電話發送任意號碼及任意短訊內容，犯罪份子利用偽基站結合傳統犯罪進行各式各樣的新型犯罪。

以澳門發生的偽基站案件為例，自2014年接獲首宗偽基站案件舉報至今，由最初犯罪份子主要利用偽基站向關閘入境旅客發送含有不法賭博或偽冒賭博網站網址的短訊進行詐騙，至現時偽基站窩點已逐漸向澳門各區蔓延開來。

在近年破獲的偽基站案件中，警方甚至可在關閘廣場、皇朝區、新口岸、外港碼頭及路氹城區一帶的豪宅單位內搜獲多套偽基站設備；而由犯罪集團經營的偽基站，過往主要招募內地人士負責操作，現時則是招募心智未成熟的澳門青年及外地家傭參與經營和操作偽基站。

2016年11月，警方更首次破獲由澳門居民操縱的偽基站犯罪集團，該集團勾結內地犯罪集團干擾電訊營運商通訊網絡，向旅客和居民發放網上博彩宣傳短訊。犯罪集團除了經常轉移偽基站點來逃避警方偵查外，亦有發現利用私家車、行李箱、背包等裝載設備來運作的流動偽基站。

2018年6月，司警局與珠海警方以“12.04跨境賣淫專案”開展聯合調查，至2019年5月15日採取行動，共同瓦解一個利用偽基站設備向旅客或賭場人士“招嫖”的有組織跨境賣淫犯罪集團，該集團操控多名內地男女及俄羅斯女子賣淫，涉及不法利益三千萬港元。珠海警方分別在湖南、湖北、昆明、重慶和中山的犯罪窩點內拘捕32名男女嫌犯和搜獲五十多萬人民幣贓款及汽車等作案工具。澳門警方則搜查澳門和氹仔19個住宅單位，拘捕23名嫌犯及搜獲大量作案工具。<sup>17</sup>

## 四、電子商務領域犯罪高發的成因

### （一）商務模式的轉變

#### 交易安全問題突出

電子商務主要在網絡虛擬環境中進行，與傳統商務模式相比有極大轉變，從昔日的直接面對面交談和金錢交易等方式，轉變為以網絡、通訊程式、流動電話、電商平台等非直接接觸的聯繫模式。交易環境與交易主體虛擬化、交易產品的數碼化、資訊化，交易支付手段電子化和高度信用化，交易範圍跨時空性甚至全球化，交易成本低而交易機會效率高<sup>18</sup>是電子商務的獨有特性。然而，目前網絡安全成

全球關注問題，防火牆、加密技術、網絡連接端口和節點控制等存在不完善之處，而電子支付、票據轉帳等則在網上完成，大大增加了交易安全的風險，這些客觀因素，為犯罪提供了便利條件，而安全技術控制和管理缺位，導致交易安全存在問題，成為涉及電子商務領域犯罪的直接原因及條件。

### （二）被害人防範意識薄弱

#### 不經意把個人資料外洩

資訊技術日新月異，使利用網絡技術及社交通訊平台進行的詐騙犯罪日漸高發，究其原因，是被害人自身的防範意識薄弱、辨別真偽能力較低、存在僥倖心理，以及貪圖方便快捷等，這些因素讓犯罪份子有機可乘。例如：在目前資訊科技發達的年代，人們日常各種活動中，很多時候參加旅遊報團、培訓活動、辦理銀行業務等，都需要提供身份證、回鄉卡、銀行存摺和水電費單等文件副本，而遞交方式從過往親身遞交，到現在普遍改為把對方要求提供的文件直接拍照或截圖上載至即時通訊程式社交平台，在目前透過各種釣魚工具、病毒程式進行網絡攻擊高發的情況下，人們的不經意及貪圖快捷方便的行為往往成為洩露自己個人資料的“元兇”，使騙徒總能隨之而更新騙術，而且常騙常有。被害人防範意識薄弱，成為助長犯罪的原因之一。

### （三）電子商務犯罪隱蔽性高

#### 電子證據取證難

電子商務犯罪是利用網絡為載體的其中一種電腦犯罪的表現形式，不僅具有跨地域性、隱蔽性高等特徵，在偵查涉及電子商務領域的電腦犯罪中，獲取、分析與保全電子證據至關重要。電子證據對電腦犯罪案件偵查及犯罪事實起着關鍵作用，然而電子證據具有多樣性、易破壞性、易偽造性和取證困難等特點，導致電子證據具有的證明力容易受到質疑。

### （四）法律制度不完善

涉及電子商務領域的犯罪具有傳統財產型犯罪的特徵，借助互聯網技術發展及資訊科技創新而為犯罪提供了便利條件，因此電子商務

犯罪是網絡犯罪的延伸，是網絡犯罪的最主要表現形式，其特徵與電腦犯罪有密切關係。

在1996年生效的現行澳門《刑法典》並沒有制定電腦犯罪的相關罪名，只在澳門《刑法典》第187條“以資訊方法作侵入”及第213條“資訊詐騙”<sup>19</sup>規定了與電腦及資訊有關的犯罪行為。直至2009年8月6日起正式生效的第11/2009號法律《打擊電腦犯罪法》規定了八個新罪名<sup>20</sup>來規範電腦犯罪行為。

在制定第11/2009號法律時，立法者認為“電腦犯罪可被理解為：利用電腦系統來達到犯罪目的的行為或此犯罪行為的對象就是電腦系統。根據上述的定義，可通過確定兩大類的罪來界定現著手進行立法的事宜的範圍，有關的犯罪涉及電腦系統：第一類，以電腦系統為犯罪工具，第二類，電腦系統是犯罪對象。”然而，立法者認為：“在澳門《刑法典》及刑事單行法律中所規定的大多數罪狀，對於科技而言均以中性的方式訂定，即犯罪行為得以任何方式作出，包括利用電腦系統的方式。”“就這些沒有針對科技而制定的法律，利用電腦系統作為犯罪工具在刑事上是沒有意義的，且可與利用任何其他工具實施犯罪相提並論。”“由於上述作為犯罪的手段在刑事上是沒有意義的，因此，該等犯罪不會納入電腦犯罪的範圍內。即使是利用資訊工具實施犯罪，但受保護的法益仍維持不變，因此，無需為實質回應該新模式的犯罪設定新的罪狀。”<sup>21</sup>正是由於當時立法者的這種觀念，在目前司法實踐中，這些利用“電腦系統作為犯罪工具”的犯罪，例如：利用電子郵件、互聯網及社交網絡、手機應用程式（APP）、電商平台進行的各類詐騙，倘若作案人沒有入侵或干擾電腦系統，又或沒有介入、輸入、更改、刪除或消除電腦數據資料，則因其行為未符合第11/2009號法律第11條“電腦詐騙”所指的犯罪要件，只能以澳門《刑法典》第211條的普通詐騙罪論處。

而在資訊技術日新月異的年代，使利用網絡技術進行的傳統犯罪發生了異化，原有的定量標準難以對新的犯罪方式進行定量分析。定量標準的實體要求是足以反映行為的社會危

害性或者法益侵害性和主觀惡性，程序要求是在司法實踐中依據現有的資訊技術等取證條件具有可操作性。<sup>22</sup>目前，不管是《刑法典》第211條“詐騙”罪，還是《打擊電腦犯罪法》第11條“電腦詐騙”罪的處罰刑幅大致相同，並且兩條罪均是非經告訴不得進行刑事程序，<sup>23</sup>即俗稱半公罪的案件，警方必須找到被害人，而且被害人同意作出檢舉時，相關的刑事程序才可開展。傳統的詐騙犯罪，作案人與被害人之間可能只是“一對一”的關係，即只有一名作案人或一個犯罪團伙詐騙一名被害人，對比利用網絡或電腦進行的詐騙犯罪，作案人只需簡單地按一下鍵盤，各類虛假訊息便可即時迅速廣泛傳播，而部份被害人很可能由於沒有受騙或金錢損失不大而沒有報案，然而，這類案件的社會危害性及法益侵害性卻比傳統詐騙犯罪的影響更大、範圍更廣。資訊時代對利用網絡技術進行傳統犯罪的定量問題提出了挑戰，警方在互聯網世界難以準確追查犯罪行為次數及行為對象數量，因此，即使這兩條法律規定“犯罪未遂，可處罰之”，但前提也得要先有被害人作出檢舉，刑事程序才可開展。

法律制度是警方執法的重要依據，現有法制存在的灰色地帶讓犯罪人得以規避應有的制裁，不單阻礙警方把不法份子繩之以法，亦會助長犯罪人的犯罪意圖。

### （五）監管措施尚須完善 刑事執法存在困難

在一國兩制下，國家大力支持和推動澳門的經濟建設和社會發展，旅遊博彩業的發展定位使澳門特區與內地、台灣地區及香港特區形成經濟、文化、社會發展等方面緊密交流的繁榮景象。在促進區域共同合作發展的同時，目前跨境、跨地域的各類電腦犯罪已成為客觀存在的現實情勢，大多數犯罪份子已將傳統犯罪轉移到網絡平台上實施，他們利用網絡的開放性、無邊際性、虛擬性及隱蔽性危害電子商務電腦資訊系統的安全，各類諸如詐騙、盜竊、金融詐騙及清洗黑錢等電腦犯罪及網絡安全問題亟待解決，尤其電子商務的核心之一是電子支付過程中的交易安全問題，然而，本地區監管機構無法對境外支付機構進行監管<sup>24</sup>，加上

各地法律制度的差異、執法及司法上存在灰色地帶，無疑加速了犯罪的衍生。

## 五、澳門電子商務領域犯罪的防治對策

在海峽兩岸暨香港、澳門地區多年來所建立良好警務合作的基礎上，針對跨境電子商務迅速發展，而本地區的監管機構無法對境外支付機構進行監管的現實情勢下，筆者從刑事偵查的角度，提出預防及打擊電子商務領域犯罪的建議：

### （一）完善電子商務企業的電子身份證管理制度

電子商務企業電子身份證管理制度是電子商務資訊管理制度的重點，它通過電子商務認證機構來完成。電子商務認證機構是電子商務體系中的重要部門，其作用是解決電子商務交易方的身份和資訊認定，以維護交易活動的安全。<sup>25</sup>

規範澳門特別行政區電子文件及電子簽名的第5/2005號法律於2005年9月7日生效，其範圍包括了電子文件的法律效力、證明力，以及合格電子簽名、認證業務、義務和責任、認可等等。該法是澳門電子政務和電子商務得以堅實發展的基石。<sup>26</sup> 澳門郵電局作為首個及唯一獲澳門特區政府認可的相關服務認證實體，2006年1月23日開始提供電子認證服務。該服務旨在為個人、機構或政府部門提供身份認證服務，以及執行法律所述的有關業務，確保具有法律效力的電子交易安全地進行。為此，澳門郵電局還於2009年成功加入“Microsoft Root Certificate Program”（微軟“根證書”項目）成為其成員之一。2009年7月22日，澳門郵電局根據第261/2009號行政長官批示，開始提供“電子認證郵戳公共服務”<sup>27</sup>。然而，法律沒有強制從事電子商務的企業必須獲認可實體確認其電子身份，而有關電子認證“雲簽”服務亦是一項收費服務<sup>28</sup>，多年來有關服務的應用範圍尚未普及。

電子商務認證是電子商務的關鍵，沒有電子商務認證，就無法消除交易雙方互不見面、互不瞭解而產生的憂慮，因此建議加強對電子

商務企業的電子身份證管理，完善相關制度，便可最大程度上確保交易雙方的電子身份，切實維護電子交易安全。

### （二）加快修法進程

#### 制定電子商務法律制度

隨着資訊與網絡技術的發展，越來越多利用電腦網絡進行的犯罪正不斷發生，而涉及電子商務領域的犯罪，更是網絡犯罪的一種主要形式。因應網絡犯罪的手法和方式不同於傳統犯罪，且電腦網絡的便利性更可讓犯罪不受時空所限，無論何時、何地皆可發生。正如上文所述，在資訊時代對利用網絡技術進行傳統犯罪的定量問題提出了挑戰，這類案件比傳統犯罪的社會危害性及法益侵害性更大、範圍更廣，而現行法律制度尚未能予以有效打擊。

《打擊電腦犯罪法》修改法案正由澳門立法會審議中，由於法律相當複雜，加上近年電腦犯罪模式變化很大、而且很快，譬如偽基站持續出現，預計該法案仍需一段時間才獲審議通過和正式生效。筆者期望修法程序能儘早完成，藉以有效預防及打擊各類電腦犯罪，從而為電子商務發展提供一個良好、安全的網絡環境。

此外，由於本澳的監管機構無法對境外支付機構進行監管，澳門特區必須首先完善自身地區相關的法律法規，加強監管，建議參考內地於2019年1月1日施行的《中華人民共和國電子商務法》，以及台灣地區於2015年5月3日正式生效、並於2018年1月31日修正公佈的《電子支付機構管理條例》，從而制定本澳的電子商務法律制度。

### （三）提升數碼偵查能力

#### 加強專業技術隊伍建設

當大數據、人工智能、區塊鏈等數碼技術與電子商務加快融合，線上電子商務平台與線下傳統產業、供應鏈配套資源加快融合，將構建更加協同的數碼化生態。在電腦資訊技術這把“雙刃劍”助長電子商務領域犯罪高發的態勢下，偵查人員除了必須掌握刑事法律知識外，還要對各種新型資訊網絡技術、各地金融體制及法律制度、電子商務運營方式、第三方支付運作模式等有一定的瞭解和認知，而在電

子證據容易被篡改及流失的情況下，數碼證據的採用與真實性備受質疑，因此，須特別強化偵查人員的數位偵查能力，加強對案發現場電子證據的獲取、保存、檢驗、分析及呈現的能力培訓，從而推動專業技術隊伍的建設。

## 六、結語

澳門特區政府2019年財政年度施政報告中明確指出，澳門特區積極參與“一帶一路”並融入粵港澳大灣區的發展大局，其中鼓勵中小企創新發展，利用跨境電商開拓商機，支持商會推行“跨境電商一站式服務”等，支援創業、創新的經濟政策將持續優化，未來跨境電子商務在澳門地區經濟發展中的重要性將日益明顯。

電子商務是現代新技術集成的一種新型經濟營運模式，與傳統商務活動相比，其獨有的虛擬化、數碼化、電子化、信用化、全球化，以及交易成本低、交易機會高及快捷等特性，容易為電子商務領域的犯罪創造條件，這類犯罪不僅具有傳統財產型犯罪的特徵，更成為資訊時代的一種特殊的社會現象。電腦資訊技術這把“雙刃劍”，既促進經濟飛躍發展，同時又助長電子商務領域犯罪頻生，因此，加快《打擊電腦犯罪法》的修法進程、制定電子商務的法律制度、完善電子商務企業的電子身份證管理制度、提升數碼偵查能力，以及加強專業技術隊伍建設，將能更好地預防和打擊涉及電子商務領域的犯罪，維護電子商務的交易安全，為促進區域經濟發展提供一個良好的網絡營商環境。

### 註：

1. 李琪、張維群、趙鯤鵬等著：《基於商務鏈的網上網下交易欺詐比較研究》，北京，電子工業出版社，2014年，第1頁。
2. 詳見網址：<http://www.chinanews.com/ga/2018/12-18/8705479.shtml>。
3. 詳見網址：[http://www.sofreight.com/news\\_30545.html](http://www.sofreight.com/news_30545.html)。
4. 《澳門居民互聯網使用趨勢報告2018》是關於澳門互聯網使用的年度報告，它是“澳門互聯網研究計劃”過去18年來持續對澳門居民的互聯網應用，以及資訊傳播科技環境進行監察的一個綜合成果。這研究計劃由澳門互聯網研究學會管理，易研網絡研究實驗室及澳門大學研究人員合作執行。
5. 皮勇主編：《電子商務領域犯罪研究》，武漢大學出版社，2002年，第1頁。
6. 同上，第20頁。
7. 彭遠春：《論電子商務犯罪的刑事法預防》，湖南大學碩士學位論文，2010年，第8頁。
8. (法)達尼埃爾·馬丁·弗德黑·馬丁著，盧建平譯：《網絡犯罪——威脅、風險與反擊》，北京，中國大百科全書出版社，2002年，第10頁。
9. 由於未有把危害電子商務信息系統的犯罪分別計算，即在表三中所指的不當進入電腦系統、不當獲取、使用或提供電腦數據資料、干擾電腦系統、用作實施犯罪的電腦裝置或電腦數據資料的犯罪中哪些是僅涉及電子商務領域的犯罪沒有區別開來，因此，本文僅對以電子商務交易方式為作案工具的犯罪進行分析研究。
10. 詳見網頁：<http://www.macaodaily.com/html/2019-05/03/content1349952.htm>。
11. 劉敏玲：〈利用第三方支付平台進行的犯罪問題及防治對策〉，發表於《第十屆海峽兩岸暨香港、澳門警學研討會》，2015年，第380-381頁。
12. 詳見網址：<http://www.macaodaily.com/html/2019-01/25/content1327134.htm>。
13. 詳見網址：<https://kknews.cc/society/bxz366m.html>。
14. 同註11，第380頁。

## 註：

15. 詳見網址：<https://www.gss.gov.mo/pdf/talk20190226b.pdf>。
16. 郭瑋熹：〈淺談偽基站設備法理鑑證〉，《刑偵與法制》，澳門司法警察學校出版，2016年6月第二期（總第72期），第3頁。
17. 詳見網址：<http://www.imastv.com/news/Macao/2019-05-16/319715.html>。
18. 唐先鋒：《電子商務法律實務》，北京，清華大學出版社，2014年，第4-5頁。
19. 澳門《刑法典》第213條“資訊詐騙”已被第11/2009號法律《打擊電腦犯罪法》廢止。
20. 2009年8月6日起正式生效的第11/2009號法律《打擊電腦犯罪法》中第4條“不當進入電腦系統”、第5條“不當獲取、使用或提供電腦數據資料”、第6條“不當截取電腦數據資料”、第7條“損害電腦數據資料”、第8條“干擾電腦系統”、第9條“用作實施犯罪的電腦裝置或電腦數據資料”、第10條“電腦偽造”及第11條“電腦詐騙”共八個罪名。
21. 澳門特別行政區立法會第三常設委員會第3/III/2009號意見書——《打擊電腦犯罪法》法案，第7-9頁。
22. 于志剛、郭旨龍著：《信息時代犯罪定量標準的體系化構建》，中國法制出版社，2013年，第254頁。
23. 按澳門《刑法典》第211條及220條、第11/2009號法律《打擊電腦犯罪法》第11條的規定，若損失金額在三萬澳門元以下，均為半公罪，即非經告訴不得進行刑事程序的案件。
24. 同註11，第383-387頁。
25. 同註5，第268-269頁。
26. 詳見網頁：<https://www.esigntrust.com/cn/legal.html>。
27. “電子認證郵戳公共服務”技術可保證郵戳發出日期、時間的確定性，保證電子文檔內容的完整性。該技術遵循了萬國郵政聯盟電子認證郵戳標準S43（Universal Postal Union Electronic Postal Certification Mark Standard, S43）和互聯網工程任務組的電子時戳標準RFC3161（Internet Engineering Task Force — Internet X.509 Public Key Infrastructure Time-Stamp Protocol, RFC3161）。這是一種由澳門郵電局為電子文檔蓋上可信時戳的服務。時戳相應的證據將被保存，以便為未來可能發生的法律糾紛提供相應的證據。電子認證郵戳不僅可蓋在用以存檔供參考及保證不被改動的電子檔上，也可蓋於提交給某機構的電子檔上，以顯示真確提交日期及時間。具有獲時戳認證的電子檔，可以充分應用在各種行業上，如私營企業競投政府招標時間提供財貨及勞務的報價書、政府部門對市民發出的通知書、律師寄送法庭的答辯狀等等。詳見網址：[http://www.thams.com.cn/post\\_005.php](http://www.thams.com.cn/post_005.php)。
28. 詳見網頁：[https://www.esigntrust.com/cn/serv\\_esignclouduserprice.html](https://www.esigntrust.com/cn/serv_esignclouduserprice.html)。