互聯網黑色產業鏈的概念界定與特徵分析——從刑法規制的視角

中國刑事警察學院遼寧網絡安全執法協同創新中心教授　秦玉海
中國刑事警察學院法律教研部教授　李　影
中國刑事警察學院法律碩士專業研究生　劉華森

【摘要】互聯網黑色產業鏈發展迅速且手段日新月異，不僅對互聯網安全帶來嚴重威脅，也對傳統的法學理論和實踐造成衝擊與挑戰，產生許多新型犯罪形態和一系列取證問題。面對這些新形態、新問題，法律規制存在諸多空白。對互聯網黑色產業鏈進行刑法規制的前提是明晰其概念並對其特徵進行分析。本文認為互聯網黑色產業鏈是指以網絡技術為基礎，多個部門之間緊密聯繫、互相配合從而謀取經濟利益的特殊關聯關係形態，具有以下五個明顯特徵：實施空間和場所虛擬化、隱蔽性極強；涉及領域新穎、處於法律模糊地帶；取證過程複雜、面臨障礙多；對從業人員的技術水平要求低；手段智能化、方式多樣化及國際化。

【關鍵詞】互聯網黑色產業鏈　概念　特徵

一、問題的提出

隨着互聯網的迅猛發展，網絡技術和服務不斷普及。“網絡技術直接作用於社會，造就了一個擁有網絡結構的社會”，[1]催生出阿里巴巴、京東購物、順豐速運等一大批新興產業，徹底改變了我們的生活方式。當然新興產業的出現也為各種違法犯罪活動提供了空間，形成諸多為違法犯罪活動提供網絡技術支持的行業。而且隨着時間的發展，這些行業在不斷升級演化，已經從過去的零散分佈發展成以產業鏈[2]的形式存在，表現出許多以往不曾有過的新型違法犯罪形態，由此對社會造成的危害也成倍擴大。但是由於相關法律規範的不健全和理論研究的滯後，這些危害並沒有得到有效的預防和懲治，從以下兩個案例當中，我們可以看出在對互聯網黑色產業鏈的打擊與防範中存在諸多問題。

案例一：某電子商務公司發現該公司武漢地區發生大額紅包套現案件，短時間內共計17,826個新註冊買家帳戶在該公司開展的購物促銷活動期間，領取小額活動紅包，並使用領取的紅包與21個公司平台的賣家帳戶進行虛假交易，然後將錢款轉入五個匯總支付寶帳戶後套取現金，涉案金額30餘萬元，該電子商務公司立即報案，公安機關隨後將鄭某抓獲。經審訊，鄭某交代了其作案細節。先是在網上大量購買公民個人信息，然後網上購買黑客軟件，繼而進行惡意註冊和虛假認證活動，最後通過虛假交易騙取電子紅包並提現，整個過程十分順利。由於手法新穎且涉及電子紅包的性質認定，檢察院最終對鄭某作出“無罪不捕”的決定。

案例二：2017年2月，某地公安分局抓獲一個利用社交軟件冒充好友實施代付詐騙的犯罪團伙。該團伙分工明確，頭目鄭某負責招募人員、培訓和購買作案工具，其他成員登錄各種社交軟件實施詐騙活動。在該團伙的電腦中，警方發現大量公民個人信息，其中一台電腦中存放有300多GB的個人信息，而且信息定位都很準確。根據主犯鄭某供述，這些信息是他以一組兩元左右的價格，花費40多萬元在互聯網上從吳某等人手中買來的，而吳某手中的信息來自一個黑客團伙。該黑客團伙利用“脫庫”[3]手段獲取大量信息後，以每10萬條數據50元到100元的價格賣給吳某等人。獲取數據後，吳某等人用“撞庫”[4]軟件將各類帳號與密碼匹配成功的帳戶以1.2元到兩元一個的價格，販賣給其他網絡團伙。在“撞庫”過程中，由於各網站設置了驗證碼檢驗程序，若要試出有效密碼，一般情況下需要人工識別並輸入驗證碼，黑客們通常將這一過程交給“碼奴”[5]完成。但是在本案中，警方發現拿到原始數據的數據商，通過某打碼平台進行加工。該打碼平台是瀋陽某網絡科技有限公司旗下產品，該公司經營範圍包括電腦科學技術研究、網絡工程設計等。調查發現，該平台專為互聯網黑灰色產業提供識別破解字符型驗證碼服務，打碼平台上有多種針對不同互聯網產品進行“撞庫”的軟件，接入該平台提供驗證碼識別服務的“撞庫”軟件有100多款，接入平台的用戶達1.1萬餘人，從2016年6月到2017年3月，平台資金進帳累計達1,650萬元，為國內已發現的最大“打碼”平台。 該打碼平台被調查的前三個月，已提供驗證碼識別服務259億次。不同於過去的人工打碼，該打碼平台使用人工智能程序，平均一秒可以識別出2,000個驗證碼，該程序由楊某設計。經訊問得知，該打碼平台收取的信息處理費用，50%分給“撞庫”軟件開發者，50%由楊某和平台開發商李某平分。短短一年內，平台牟利1,300多萬元，楊某分到300多萬元。本案涉及獲取公民網上數據、定位個人信息、個人信息倒賣、購買作案軟件、提供驗證碼識別服務、編寫智能識別程序、開展詐騙活動等多個過程，整個過程環環相扣，警方共抓獲159名嫌疑人。由於犯罪手法新穎、案情複雜、取證難度高，該案在進一步調查中。

在以上兩個案例中，我們可以看出互聯網違法犯罪形態不斷推新，暴露出法律概念模糊、證據標準不清晰等弊端，導致國家機關難以對其有效打擊。這些新型違法犯罪活動越來越猖獗，已經影響到國家正在建立的網絡徵信體系，危害互聯網及電子商務經濟的健康發展。

如在案例一中的黑色鏈條上，由網上個人信息銷售，至黑客軟件的製作販賣，再到騙取電子紅包並提現，涉及到電商平台帳戶的惡意註冊、虛假認證、虛假交易等行為的性質認定，電子紅包的屬性認定等。從目前司法機關查辦的網絡詐騙、網上盜竊、售假以及販毒販槍等犯罪案件看，幾乎所有案件都與網上虛假帳戶和虛假商業信用有關。這些惡意註冊的買家或賣家帳戶可以獨立成為詐騙犯罪甚至買賣暴恐物品等多種犯罪的工具；經過虛假認證的賣家帳戶往往利用大量惡意註冊的買家帳戶進行虛假交易來提高信用，利用“高信用”的賣家店舖吸引廣大網購消費者進一步實施詐騙、盜竊、售假、售賣違禁品、洗錢等犯罪活動。“從具體層面來說，網絡犯罪的危害已經被全世界所公認。”

電子紅包屬於網絡虛擬財產[6]，是信息化時代的產物。從物質形態來說，網絡虛擬財產是存在於特定網絡虛擬空間內具有一定現實經濟價值，可由網絡用戶依規則進行調用的具有專屬性的數據資料[7]。網絡虛擬財產的突出特徵就是價值不確定，對不同的網絡程序參與者而言其價值大小不一，對非特定網絡程序參與者而言可能沒有價值。[8]因此其與大眾認識中的財產存在顯著區別，但是現實中其確實在

發揮財產的作用。當公民的網絡虛擬財產受到不法侵害時，法律並沒有明確規定是否予以保護。

“自由、財產等法益受到刑法的保護，但是自由的內容、財產的內容則會隨着社會的發展而變化。”[9]如果將網絡虛擬財產界定為刑法中的“公私財物”，對價值如何認定，存在諸多問題。首先，目前我國還沒有相關的司法解釋對網絡虛擬財產的價值認定作出具體規定，人民法院在實踐中缺乏明確的認定標準。其次，從客觀意義上來說，網絡虛擬財產本身沒有普遍價值，其價值大小只是在特定網絡程序參與者交易時確定，而且對不同的參與者而言其價值存在差別。如果這些網絡虛擬財產被他人竊取，涉案金額如何確定還是空白。而且，如果行為人竊取網絡虛擬財產後，僅是供自己使用而沒有對外交易，該行為如何進行價值認定，目前法律也沒有具體規定。在2013年盜竊罪司法解釋[10]制定過程中，曾有將網絡虛擬財產納入盜竊罪犯罪對象的意見，但是最高人民法院沒有採納，認為將網絡虛擬財產解釋為盜竊罪的犯罪對象“公私財物”，超出了司法解釋的權限[11]。在實務中，根據網絡虛擬財產是電磁記錄這一屬性將其定義為電腦信息系統數據。這樣做雖然實現了對現實中此類犯罪行為的打擊，但是並沒有體現出法律對網絡虛擬財產屬於公民合法財產性利益的保護。

在案例二中涉及到網上個人信息的一系列操作，但是各個團伙之間並沒有共同犯罪的意思聯絡，相比過去犯罪團伙利用互聯網實施的共同盜竊、詐騙、製售假冒偽劣商品等犯罪而言，這是新產生的犯罪類型，是否構成共同犯罪有較大的討論空間。而且，我國《刑法修正案（七）》、《刑法修正案（九）》雖然先後增加、修改了非法獲取公民個人信息罪[12]，但對公民個人信息的概念沒有明確定義，該案中的信息買賣涉及多個環節，有些信息可以精確到具體公民，有些並不能，如何準確界定個人信息仍是公安機關面臨的棘手問題。除此之外，互聯網黑色產業鏈中涉及的證據，多數情況下是行為人所使用的電腦硬盤上的存儲文件、服務器上的歷史記錄等電子數據。由於這些電子數據是行為人通過鍵盤輸入的一種記錄，它很容易被複製、刪改，不像傳統犯罪痕跡那樣易於甄別，而法律對電子數據的採集、質證缺乏具體規定，由此在刑事訴訟實踐中產生許多不便。

二、互聯網黑色產業鏈的概念界定及表現形式

互聯網黑色產業鏈是從過去的黑客活動逐步發展而形成的。在上世紀60年代，美國首先出現了黑客（hacker）[13]一詞，過去互聯網空間的經濟效益表現得並不是很明顯，黑客利用技術手段入侵他人信息系統，或是為了炫耀自己的高超技術，或是為了實現其他不法目的，一般情況下不會造成嚴重的經濟損失。但是近年互聯網經濟迅猛發展，網絡空間的經濟效益越來越大，在巨大利益的驅動下，一些黑客開始利用技術優勢獲取他人有價值的數據信息，並在這群人周圍衍生出上下游產業，嚴重影響到互聯網經濟的健康發展。

目前，國內對互聯網黑色產業鏈沒有準確定義。筆者認為：互聯網黑色產業鏈是指以黑客技術為基礎，多個部門之間環環相扣、緊密配合從而謀取經濟利益的特殊形態。產業鏈中各部門分工明確，上下游之間形成一種供需關係與合作關係。產業鏈上游從業人員一般具有較高的網絡技術水平，主要負責一些技術性研究工作，包括最前沿的惡意軟件技術代碼、編寫木馬病毒、發現發佈網絡漏洞信息；產業鏈中游從業人員主要負責竊取個人信息、傳播病毒、發動網絡攻擊等；產業鏈下游從業人員主要負責販賣木馬病毒、個人信息資料、肉雞[14]以及洗錢等。此外，還有一些支撐整個黑色鏈條的周邊產業，如販賣身份證及銀行卡的部門或人員、專門實施黑客技能培訓的部門或人員以及在電子商務平台上進行惡意註冊、虛假認

證、虛假交易的部門或人員。上游與下游交易時並不知道對方的真實身份，整個過程借助互聯網完成，每一環節都有非法利潤可得，而且非法收益數目驚人。[15]處於黑色鏈條各個環節的不法份子緊盯大眾、企業、政府在信息安全方面的薄弱環節，通過一切可能的手段將虛擬世界的數字代碼變成現實世界的真金白銀。[16]

互聯網黑色產業鏈的表現形式有多種，根據手段方式的不同，大體上可以分為網絡技術類黑色產業鏈和社會工程學類黑色產業鏈兩大類型。網絡技術類黑色產業鏈是指利用網絡和電腦系統存在的安全漏洞或缺陷，竊取數據信息，或者對網絡和電腦系統發動各類攻擊，從而實現獲利的非法活動。[17]社會工程學類黑色產業鏈是指利用社會工程學原理[18]，針對受害者的心理弱點（如本能反應、輕信、粗心、貪婪、警惕性不高等），採取諸如欺騙、傷害等危害手段，來操縱受害者執行預期的動作或洩露機密信息，從而實現獲利的非法活動。[19]在互聯網黑色產業鏈實際運作過程中，二者總是綜合使用，以實現非法利益的最大化。

具體表現為如下八種形式：

（1）電商平台黑色產業鏈。主要特點是運用各種自動化軟件，完成某些電子商務平台帳戶的批量註冊、虛假認證，從而違規開展惡意帳號買賣、虛假交易、炒信（編按：炒作信用）等活動，嚴重妨害了電子商務平台正常的經營秩序，不利於互聯網新興經濟的健康發展，不利於國家互聯網徵信體系的建立。該產業鏈上游涉及到惡意軟件編寫及買賣、個人信息採集、人工打碼等活動，下游涉及假冒偽劣產品銷售、網上詐騙等活動。在2017年6月，李某某因組織他人開展炒信活動，被浙江省某法院判刑。[20]

（2）暗鏈產業鏈。“暗鏈”是一種互聯網搜索引擎常用的優化技術，可以用來提高它所指向的網站搜索排名。“暗鏈”原則上對普通用戶是不可見的，在網頁頁面上極易被忽視，它能夠與網站“長期共存、共同發展”。黑產從業者通過技術手段任意設置暗鏈，欺騙搜索引擎，借此提升相關網站排名。只要這些暗鏈在一定時間內能夠提高網站排名，黑產從業者就可以從排名提高的網站經營者那裏獲得收益。

（3）流量劫持產業鏈。流量劫持指網上的流量被竊取、刺探或控制，在收到用戶的流量後，還可以分析獲取用戶隱私。黑產從業者通過技術手段，控制用戶的上網行為並讓用戶打開不想打開的網頁、看到不想看的廣告等，從而給流量劫持者帶來源源不斷的收入。例如，一個黑客劫持的流量如果是每天五萬個IP，合作90天，千次IP的價格是35元，那麼流量購買方支付給黑產從業者的費用就是157,500元，平均每月逾五萬元，何況出售流量的黑產從業者手中擁有的IP遠不止五萬個。[21]在流量劫持黑色產業鏈上還包括許多提供劫持技術的團隊，一些互聯網公司、路由器生產商都可能是流量劫持的操作者，目的不外乎廣告收入、網站點擊率以及採集用戶信息等。

（4）釣魚產業鏈。主要特點是通過網頁、短訊、電話等方式誘使用戶上鉤，並盜取用戶的個人信息、財產等。一些不法份子設立釣魚網站，或利用釣魚網站向受害者發送大量釣魚鏈接。這些鏈接主要偽裝成銀行、各大網站安全中心、郵箱安全驗證中心、電商服務平台等，以竊取用戶的各種信息或存款，如著名的“一元木馬”案[22]。根據2017年10月被舉報的釣魚網站排名，以“中國新歌聲”“蘋果公司”“10086”“奔跑吧兄弟”等為名義的釣魚網站最多。[23]而且有專門的黑產網站向會員出售木馬程序用於建立釣魚網站，並提供釣魚網站的維護、短訊群發、服務器出租等服務。

（5）網絡色情產業鏈。主要特點是通過網絡手段進行各類線上或線上線下結合的情色交易。與過去的淫穢色情網站相比，現在的網絡色情網站牟利方式已經發生了巨大變化，由過去的會員制收費發展成通過廣告牟利。如今，淫穢色情網站已經形成個人製作網站，流

量聯盟[24]推廣，廣告聯盟根據點擊率提供廣告費用返還的完整產業鏈，行為非常隱蔽。

（6）拒絕服務攻擊產業鏈。主要特點是運用DDOS/CC等技術手段，[25]黑產從業者將目標網站攻擊癱瘓，無法進行正常的服務，給目標網站造成損失，以此要挾或敲詐被攻擊者，獲得非法利益。我們可以把一個網絡應用（網站、APP、遊戲等）看成一個實體店舖，而DDOS/CC攻擊類似於突然之間派遣大量社會閒散人員去這個實體店舖，佔滿所有的位置，和售貨員聊天，在收費處排隊等，讓真正想購物的人沒法正常購物從而給店舖造成損失。一些商業類、遊戲類網絡公司遇到競爭時，往往通過非正規手段打擊競爭對手，DDOS攻擊是其中比較常用的一種手段。

（7）遊戲私服產業鏈。“私服”[26]本質上屬於網絡盜版，其直接結果是分流網絡遊戲運營商的利潤。遊戲私服同官方服務器一樣，都是向遊戲玩家收取費用以獲利。私服雖然沒有官方服務器那麼上檔次，但發展速度之快、規模之大已經讓官方束手無策。如今，手遊私服已經形成產、供、銷完整的產業鏈，而開設一款私服的成本卻非常低。曾有報道揭秘月流水可破百萬的私服，成本僅需幾千塊錢。[27]

（8）掛馬產業鏈。主要特點是向用戶電腦或智能移動終端中植入病毒或木馬等惡意程序，從而盜取電腦或智能手機中存儲的信息，包括各種帳號密碼、網銀資料、信用卡信息、遊戲中的虛擬財產等，經過“脫庫”、“撞庫”後開展一系列的黑產活動。

三、互聯網黑色產業鏈的特徵分析

近些年，互聯網黑色產業鏈能夠迅速發展有其自身的特徵。

（一）實施空間和場所虛擬化，隱蔽性極強

人在網絡世界是匿名的，可以在不暴露行蹤的情況下更改、破壞他人的電腦信息系統及資料。具體表現：網上作案不受時間、地點限制，可以隨時隨地跨越國界；作案時間短，甚至瞬間完成，留下的痕跡極少且極易被擦除。以網絡色情產業為例，由於網絡信息傳播的跨地域性、隱匿性、瞬時性等特點，對網絡色情產業的查處要比對現實生活中色情活動的查處困難得多。[28]一些色情網站偽裝成普通論壇，將色情信息藏匿其中，在各大網絡社交平台（QQ、微信、貼吧、論壇等）中傳播。通過提示網民申請註冊會員，管理者會謹慎考察並將其升級為特殊會員後才開放色情板塊。一些色情團伙在視頻聊天室是否開展淫穢色情表演，也是由會員註冊年限、熟人介紹等方式決定的。此外，色情網站還會經常更換網站域名以逃避監管。[29]隨着網絡技術的不斷發展，網絡色情又發現了新領域，新興的雲盤、網盤、VR領域、直播平台都成了其藏身和傳播的地方。全國掃黃打非辦公室2015年6月公佈的五起網絡色情典型案例中，行為人通過360網盤進行淫穢信息的上傳、分享，將色情網盤帳號在網上秘密銷售，同時通過廣告盈利。微信、QQ群組等移動端APP都是淫穢信息傳播的重災區，網絡色情利用私人社交圈子進行傳播，不斷翻新其手段和方式。[30]

（二）涉及領域新穎，處於法律模糊地帶

法律具有滯後性，不可能將立法時尚未發生的行為完全規範進來。“這符合技術進步與制度發展的協調性原則，即技術進步帶來社會關係的不協調，再通過制度規範進行修補，以平衡技術進步與社會發展的關係。”[31]許多互聯網黑色產業鏈上的行為對象、手段方式都存在特殊性，與傳統法律條文所映射的行為存在顯著差異。對於這類行為，應該具體由甚麼法律規制或者是否需要法律進行規制，都需要根據黑色產業行為的特徵、社會危害程度以及通過現行行政、民事法律是否足以調整來綜合判斷。形形色色的互聯網黑色產業伴隨着網絡技術的快速發展，也在發生快速變化。此

外，互聯網和現實生活的不斷融合形成了全新的虛擬社會領域，虛擬社會領域中同樣存在社會秩序。傳統犯罪的客體是國家、社會的利益以及他人的生命健康權利、民主權利、財產權利等，這些客體都是人們在現實生活中能夠看得見、摸得着，從而被普遍接受的。[32]互聯網黑色產業除了侵犯上述人們所普遍認知的社會關係外，還能夠對虛擬社會秩序造成侵害，如各種搶購軟件、搶票軟件等。不斷變異的互聯網黑色產業相對於法律而言，具有鮮明的超前性，也正是由於這一突出特徵，司法機關遇到此類案件時總是很被動。

（三）取證過程複雜、面臨障礙多，查處難度大

互聯網黑產從業者在網絡環境中都是以虛擬帳號形式存在，並採取了偽裝措施。儘管偵查部門可以通過網絡IP地址等技術手段進行查詢，但並不是所有的IP地址、帳號等與黑色產業從業者完全捆綁，尤其是在盜用、冒用、黑客控制他人帳號或設備開展互聯網黑色產業時，行為主體的不確定是訴訟的一大障礙。網絡中存在着許多網絡代理服務，這對於隱藏個人真實身份更為便利。此外，互聯網黑色產業鏈的涉案證據多存儲在網絡服務器中，對涉案服務器的調查取證存在諸多障礙。如果採用物理手段，雖然偵查機關對涉案服務器硬盤進行一一取證和分析不存在技術問題，但是在具體案件中，服務器數量很多，且可能分散在全國甚至世界各地，如果逐一取證，需要花費的人力、物力將是巨大的，這會消耗大量的法律資源，況且服務器的所有權人或者租用人也未必同意；如果通過網絡手段調查取證，則需要取得進入服務器的權限，但是相關法律對此類問題並沒有具體明確的規定。[33]更重要的是，如果利用網絡技術調查取證，服務器中的相關數據資料存在着被即時更新的數據覆蓋的可能，難以保證證據的原始性和準確性，因此所取得的證據在證明力上存在瑕疵。此外，對服務器中的商業秘密、個人隱私進行有效保護還是個問題。

（四）對從業人員的技術水平要求低

過去電腦技術被視為一種新興高科技，從事互聯網產業的人員必須具備專業的網絡技術，如今這一情況正在改變。互聯網黑色產業不需要行為人具有多深的網絡專業背景，只需要具備基本的現代生活常識以及理解應用能力。一方面，網民的基本素質在不斷提高，而且智能移動終端隨處可見，人們或多或少都掌握一些軟件應用的操作技能。另一方面，互聯網的精神在於分享，[34]那些想要從事互聯網黑色產業的個人或群體，只要動動滑鼠就可以在網絡中找到木馬病毒、注入工具等黑客程序，並能夠根據社交平台或觀看視頻教程掌握具體操作方式。而且，根據中國互聯網絡信息中心（CNNIC）2017年7月發佈的第40次《中國互聯網絡發展狀況統計報告》顯示，截至2017年6月，我國網民仍以10至39歲群體為主，佔整體的72.1%：其中20至29歲年齡段的網民佔比最高，達29.7%，10至19歲、30至39歲群體佔比分別為19.4%、 23.0%。與2016年底相比，40歲及以上中高齡群體佔比增長1.7個百分點。[35]我國網民絕大多數屬於青壯年時期，潛在從業者非常多。這也是近些年互聯網黑色產業鏈迅速蔓延的原因之一。

（五）手段智能化、方式多樣化，且具有國際化趨勢

網絡技術在不斷進步，互聯網黑色產業採取的手段也在不斷升級、形式在不斷擴展，呈現出智能化、多樣化的特點。互聯網黑產從業者在不斷提高自身的技術水平，採用各種新技術、新手法突破網絡安防系統，包括解密用戶密碼、暴力破解密碼等。[36]例如，電商平台黑色產業鏈是伴隨着近幾年電子商務的陡然興起而出現的，涉及的惡意註冊、虛假認證及虛假交易過程均是運用自動化軟件完成的。虛假認證過程的驗證碼識別原來是通過“碼奴”識別並輸入的，現在隨着AI（人工智能）技術的興起，現實中已經出現了利用AI技術幫助識別破解字符型驗證碼的產業。此外，互聯網沒有國界，互聯網黑色產業鏈的國際化趨勢也越

發明顯。在2017年9月，國家互聯網應急中心檢測到的木馬或殭屍網絡控制服務器IP總數為7,976個，其中，境內木馬或殭屍程序控制服務器IP有2,416個，境外木馬或殭屍程序控制服務器IP有5,560個，主要分佈於美國、俄羅斯、中國香港等地區。[37]

四、結語

互聯網黑色產業鏈發展迅速，已經侵害到公民的合法權益，構成犯罪的應當受到刑法的規制。本文對互聯網黑色產業鏈的概念作了初步界定，並就我們經常遇到的一些互聯網黑色產業鏈進行了介紹。針對這些犯罪新形態，筆者認為應當採取立法與司法解釋相結合的方式，進一步完善我國的刑事法律制度。例如在案例一中，面對“電子紅包”定性不明的情況，可通過刑事立法的方式，將其納入財產性權益的範疇，以詐騙罪追究騙取電子紅包的行為人責任，以有效地維護網購消費者及電商平台的合法權益；案例二中，可以通過司法解釋的途徑，重新解釋共同犯罪的成立條件，將網絡環境中多方操作個人信息的行為視為共同犯罪，從而更有效地維護公民隱私權益。此外，在分析互聯網黑色產業鏈特徵的基礎之上，我們還要制定相應的刑事證據規則，為實務部門有效打擊該類犯罪活動提供便利。總之，我們要不斷完善刑事法律規則，加快與互聯網科技的融合，切實維護公民的合法權益，保障互聯網經濟健康快速發展。

註：

1. 張康之：〈論社會的網格結構〉，《理論學刊》，2008年第三期，第72至77頁。
2. 產業鏈是產業經濟學中的一個概念，是各個產業部門之間基於一定的技術經濟關聯，並依據特定的邏輯關係和時空佈局關係客觀形成的鏈條式關聯關係形態。
3. “脫庫”是指網絡黑客通過運用超級SQL注入工具、網站漏洞掃描軟件，批量掃描網站程序漏洞，非法獲取網站後台用戶註冊數據的行為，獲取的數據大多是網站後台中存儲的用戶帳戶及密碼信息。
4. “撞庫”是指網絡黑客通過收集互聯網已洩露的用戶和密碼信息，生成對應的字典表，嘗試批量登陸其他網站後，得到一系列可以登錄的用戶。很多用戶在不同網站使用的是相同的帳號密碼，因此黑客可以通過獲取用戶在A網站的帳戶從而嘗試登錄B網址，這就可以理解為“撞庫”攻擊。
5. “碼奴”是專門通過識別驗證碼圖像、輸入正確的驗證碼，從而幫助完成網上信息註冊的打碼工作者，這一過程被稱為“打碼”。根據驗證碼的複雜程度和輸入的準確率，打1,000個驗證碼會掙到一元至25元不等，每天工作12小時，最多可以輸入兩萬個驗證碼，掙到300多元。打碼平台的使用者通常是網絡詐騙人員、“羊毛黨”、搶票的“黃牛”、論壇刷帖“水軍”等。
6. 2009年6月4日施行的《文化部、商務部關於加強網絡遊戲虛擬貨幣管理工作的通知》對網絡遊戲虛擬貨幣作出了界定：“是指由網絡遊戲運營企業發行，遊戲用戶使用法定貨幣按一定比例直接或間接購買，存在於遊戲程序之外，以電磁記錄方式存儲於網絡遊戲運營企業提供的服務器內，並以特定數字單位表現的一種虛擬兌換工具。網絡遊戲虛擬貨幣用於兌換發行企業所提供的指定範圍、指定時間內的網絡遊戲服務，表現為網絡遊戲的預付充值卡、預付金額或點數等形式，但不包括遊戲活動中獲得的遊戲道具。”
7. 吳佳穎：〈論網絡虛擬財產的屬性及其民法保護〉，載《湖南行政學院學報》（雙月刊），2017年第五期。
8. 許多網絡遊戲玩家會花費千元從其他玩家手中購買遊戲裝備，但是這些遊戲裝備對於不玩網絡遊戲的人來說卻一文不值。
9. 張明楷：〈網絡時代的刑事立法〉，《法律科學》（西北政法大學學報），2017年第三期。
10. 即2013年最高人民法院、最高人民檢察院發佈的《關於辦理盜竊刑事案件適用法律若干問題的解釋》。
11. 胡雲騰、周加海、周海洋：〈“關於辦理盜竊刑事案件適用法律若干問題的解釋”的理解與適用〉，《人民司法》，總第698期。

註：

12. 《刑法修正案（七）》第七條規定：在刑法第二百五十三條後增加一條，作為第二百五十三條之一：“國家機關或者金融、電信、交通、教育、醫療等單位的工作人員，違反國家規定，將本單位在履行職責或者提供服務過程中獲得的公民個人信息，出售或者非法提供給他人，情節嚴重的，處三年以下有期徒刑或者拘役，並處或者單處罰金。

“竊取或者以其他方法非法獲取上述信息，情節嚴重的，依照前款的規定處罰。

“單位犯前兩款罪的，對單位判處罰金，並對其直接負責的主管人員和其他直接責任人員，依照各該款的規定處罰。”

《刑法修正案（九）》第十七條對本條作了修改。

13. 趙丹：《黑客》，作家出版社，2011年。
14. “肉雞”也稱傀儡機，是指可以被黑客遠程控制的機器。黑客可以隨意操縱它並利用它做任何事情。
15. 2015年，廣東警方破獲一起特大黑客團伙案，該案主犯為年僅18周歲的黑客葉某。他利用自編的黑客軟件，通過互聯網批量提取客戶銀行卡信息，警方在其一部涉案電腦中查獲160萬條公民個人信息和銀行卡帳號，可直接盜刷的銀行卡信息及其密碼多達19萬條，可提現金額高達14.98億元。載http://gd.sina.com.cn/zh/news/2015-01-21/071524531.html，訪問日期：2017年11月14日。
16. 李剛、馮雪竹：〈直擊黑客地下產業鏈〉，《中國信息安全》，2014年第二期。
17. 任彥君：《犯罪的網絡異化與治理研究》，中國政法大學出版社，2017年。
18. 羅玉梅：〈網絡安全中的社會工程學應用研究〉，《無線互聯科技》，2015年第16期。
19. 米特尼克（Mitnick, K. D.）（美）、西蒙（Simon, W. L.）（美）著，潘愛民譯：《反欺騙的藝術》，清華大學出版社，2014年8月。
20. 陳東升、王春：《全國刷單炒信入刑第一案宣判》，載http://news.xinhuanet.com/legal/2017-06/21/c_1121180917.htm，訪問日期：2017年11月15日。
21. 許連連、吳雨欣：《流量劫持灰色產業鏈：劫持五萬IP　月入至少三萬》，載http://tech.sina.com.cn/it/2016-04-05/doc-ifxqxcnp8584192.shtml，訪問日期：2017年11月14日。
22. 王春、周德峰：《警方揭秘一元木馬網絡犯罪　專騙遊戲愛好者》，載http://tech.sina.com.cn/i/2016-06-21/doc-ifxtfrrc4018136.shtml，訪問日期：2017年11月22日。
23. 取自“12321網絡不良與垃圾信息舉報受理中心”，訪問日期：2017年11月14日。
24. “流量聯盟”是一個提供廣告服務的註冊平台，一旦在平台註冊成功，就可以在平台後台拿到該平台的鏈接並掛在自己的網站上，如果該鏈接被點擊一次，平台就會按照事先商量好的比例成倍地返還點擊率。
25. 劉會霞：《網絡犯罪與信息安全》，電子工業出版社，2014年。
26. “私服”是指未經版權擁有者授權，非法獲得服務器端安裝程序之後設立的網絡服務器。
27. 《手遊私服已成產業鏈5,000元就可開一個私服》，載http://www.sohu.com/a/66696616_116126，訪問日期：2017年11月18日。
28. 季岩硯、胡磊、高迎：〈中國網絡色情治理的難題及應對：政府公共權力運行的視角〉，《電子商務》，2015年第八期。
29. 張小川：〈當前網絡色情活動的新特點及防偵要略〉，《雲南警官學院學報》，2008年第二期。
30. 段文博：〈我國網絡犯罪的新情況及應對之策〉，《山東警察學院學報》，2015年第四期。
31. 張巍：《涉網絡犯罪相關行為刑法規制研究》，法律出版社，2015年。
32. 鄭志平：《國家與社會關係視角下的中國虛擬社會治理方式創新研究》，湘潭大學2016年博士學位論文。
33. 蔣慧嶺：《網絡司法典型案例》（刑事卷），人民法院出版社，2016年。
34. 胡啟恒：〈互聯網精神〉，《科學與社會》，2013年第四期。
35. 中國互聯網絡信息中心：《中國互聯網絡發展狀況統計報告》，載http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/t20170803_69444.htm，訪問時間：2017年11月12日。
36. 葉碧蝦：〈計算機網絡犯罪的偵查與防控探究〉，《山西師範大學學報》（自然科學版），2015年第三期。
37. 國家互聯網應急中心：《CNCERT互聯網安全威脅報告—2017年9月》，載http://www.cert.org.cn/publish/main/upload/File/2017monthly09.pdf，訪問日期：2017年11月15日。