# 大數據時代個人信息權的刑法保護

文立彬*

## 一、前言

個人信息之所以需要法律保護，特別是刑事保護，是因為現實存在着諸多侵害個人信息的嚴重行為，已造成了惡劣的社會影響。構成犯罪的侵害個人信息的行為可稱為“個人信息犯罪”，核心目的在於保護個人信息的安全。中國法律對於個人信息保護，採取了刑法先與民法提供法律保障依據的立法策略，集中體現了個人信息保護的急迫性和重要性，故以刑法保護視角考察中國個人信息的現狀和發展問題具有法律依據和司法數據的支持。

## 二、大數據產業與個人信息保護的聯繫

第四次工業革命正在發生，以大數據、雲計算、人工智慧為代表的科技變革正逐漸改變着我們的生活習慣與工作環境。在科技迅速發展的背影下，社會上滋生了較多的新型犯罪，如個人信息犯罪、環境污染犯罪等，相較於傳統犯罪而言，新型犯罪具有行為隱蔽、結果嚴重以及危害期長的特點。關注大數據產業發展背景下的個人信息保護問題具有重要的理論價值和實踐意義。出於行文便利，本文中的“個人信息”與“公民個人信息”屬同一概念，下文不再贅言。

### (一) 大數據的概念界定與技術特徵

中國《促進大數據發展行動綱要》明確規定了“大數據”的概念。[1] 大數據有四個典型特徵：數據量大(volume)、數據變化速度快(velocity)、數據內容龐雜(variety)、數據的精確(veracity)。[2] 在大數據背景下，個人信息所具有的人身屬性和財產屬性越來越重要。從立法層面考察，個人信息不僅體現為人格權的內容，更在新修訂的《民法總則》中明確規定為民事權利。[3] 據此，保護個人信息安全和懲處個人信息犯罪應當兩手抓且兩手都要硬。對此，打擊、懲處侵犯個人信息行為的刑事策略應當具有針對性、體系性和實效性。針對性是指依據個人信息犯罪的網絡依賴性和牟利性進行有效打擊；體系性是指根據侵犯個人信息的行為程度高低進行區別化的規制；實效性是從規制可行性和規制目的性來考察制度的設計是否實際發揮作用。在大數據時代下，民眾對於個人信息保護的訴求集中體現在安全保障和風險管控，進而要求立法及時性和保護實效性。

* 廣西民族大學法學院教師、法學博士

### (二) 大數據產業發展對個人信息安全的影響

個人信息是指能將個人直接或間接識別的一切信息，主要包括姓名、住址、身份證號、工作單位、通訊方式、血型、基因信息、股票交易賬號、信用卡卡號等。[4] 大數據背景下，個人信息具有的人身屬性和財產屬性凸顯，不法分子憑藉多種途徑倒賣個人信息牟取暴利，使得民眾對個人信息的安全感驟降。大數據產業的發展與個人信息的使用密不可分，大數據技術對個人信息的影響主要表現在以下三個方面：①大數據的技術特徵增加了個人信息洩露的風險。大數據儲存比傳統存儲方式數量更大、價值更高，更加容易遭到駭客和病毒關注。大數據的多樣性特點使得駭客的攻擊目標增多，高滙集度的海量信息不可避免地加大了個人信息的洩露風險，亦提升了遭受不法分子攻擊的可能；②個人信息收集和使用不當帶來安全風險。一方面，過度收集個人信息並進行二次開發利用的現象比較普遍。在信息社會，個人信息的電子化管理滲透到衣食住行玩等日常生活的方方面面。另一方面，對個人信息進行惡意使用、非法買賣之風愈演愈烈，甚至形成了灰色產業鏈；③個人信息洩露將造成嚴重後果。垃圾短信、垃圾郵件、行銷電話騷擾和微信朋友圈“殺熟”現象無休無止，令人煩不勝煩；網絡詐騙、電信詐騙花樣翻新，層出不窮，危及個人信息主體的財產安全。更有甚者，定點跟蹤、綁架、搶劫、強暴，嚴重危害個人信息主體的生命安全。因此，在大數據產業發展促進全球經濟增長的同時，部分民眾對於自身的個人信息安全感到擔憂和恐懼。

### (三) 中國個人信息犯罪的現狀

從中國個人信息保護立法來考察，刑法先於其他部門法對個人信息提供法律保障，即 2009 年《刑法修正案(七)》的出台，首次將出售、非法提供公民個人信息的行為和非法獲取公民個人信息的行為明確規定為犯罪。據此，從個人信息犯罪的視角觀察中國個人信息保護現狀具有法律依據和實踐意義。通過查詢中國裁判文書網 2013-2016 年涉及侵害公民個人信息類刑事判決文書可知：①中國個人信息犯罪呈現上升趨勢，判決數量從 2013 年的 76 件上升到 2016 年的 437 件，上升幅度達 475%。個人信息犯罪案件數量的增長與公安部積極開展專項打擊行動、公民自我保護意識的提高具有密切關係；②個人信息犯罪主要集中於南方經濟發達省市，其中福建省的案件數量最多(235 件)，其次是上海市(201 件)和廣東省(182 件)。從案件分佈不難發現，侵害個人信息所實施的搜集、整理、利用行為主要依託繁榮的經濟市場，通過交易、交換等方式獲取高額利潤；③涉及個人信息的範圍較廣、種類繁多，洩露的個人信息包括身份信息、財產信息、通信信息、車輛信息、旅遊信息、住宿信息等。從被害人群體進行觀察，被害人多具有業主、考生、電商消費者、病人等身份。綜上，個人信息犯罪行為在中國愈演愈烈，目前的規制思路和制裁措施並未能有效的遏制此類犯罪，因此有必要精確分析中國現狀，反思現行立法策略與規制措施。

## 三、中國個人信息犯罪的法律特徵與立法策略分析

大數據環境下，個人信息具有的人身屬性和財產屬性備受重視，面對日益嚴峻的侵害個人信息行為的狀況，細緻分析中國個人信息犯罪的法律特徵和規制困境，將有利於個人信息保護的立法完善。

### (一) 個人信息犯罪的法律特徵剖析

德國社會學家烏爾里希·貝克曾預言的風險社會的到來，即人造風險將取代自然風險成為人類社會面臨的主要風險。[5] 大數據產業作為科技革命下的典型產物，亦體現了科技的兩面性，使用不當將危害整個社會。對於大數據時代下的個人信息犯罪而言，其法律特徵可概括為以下三點：①個人信息犯罪屬於法定犯[6]，在人類步入風險社會的當下，法定犯的增多成為了必然的趨勢，原因在於法定犯的設置是國家為了更好的把控經濟風險、保障社會安全，如《中國刑法》中規定的逃稅罪、走私罪、洗錢罪等；②個人信息犯罪侵犯的是無形財產，相較於土地、房屋、汽車等有形財產，個人信息、智慧財產權等屬於無形財產，無形財產具有非物質性、無消耗性和載體依託性的特徵。侵害個人信息的行為並不會導致信息本身的消耗，亦讓受害者難以察覺，進而造成刑事偵查、證據收集等方面的困難；③個人信息犯罪多以牟利為最終目的，實證研究數據表明，約五成的個人信息犯罪案件的行為人以出售個人信息牟利，約二成的行為人將個人信息用於業務推廣，約三成的行為人利用個人信息從事其他違法犯罪活動，如實施電話詐騙、信用卡詐騙、敲詐勒索等、偽造證件等。以打擊牟利為立法導向，或可通過沒收非法所得、提高罰金數額等針對性經濟制裁措施顯著提升個人信息犯罪的成本，積極實現刑法的一般預防和特殊預防。總之，個人信息犯罪具有法定犯、侵害無形財產、以牟利為目的的法律特徵，進而在規制措施的設計上應凸顯民事、行政與刑事法律規制的梯度銜接、保護手段上的科技依託以及懲罰方式上的成本增加，進而對個人信息進行科學立法、民主立法和有效保護。

### (二) 個人信息保護立法的歷史沿革與規制困境

1979 年和 1997 年刑法沒有專門規定侵犯公民個人信息的犯罪，2008 年《個人信息保護法(草案)》呈交國務院審議，至今尚未頒行。有學者指出，中國現行法律規定的犯罪，雖存在個別罪名廢除與否的爭議，但主要的問題是犯罪化。[7] 即根據社會情境變遷，適時設置新的犯罪構成，進而預防犯罪和規制行為。2009 年《刑法修正案(七)》首次將個人信息納入刑法保護，規定了相應的犯罪構成。2014 年《刑法修正案(九)》的出台，一方面擴大了個人信息犯罪的主體範圍，另一方面增設了出售或者非法提供公民個人信息的犯罪。2017 年《關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》的出台規定了侵犯公民個人信息罪入罪要件的“情節嚴重”、明確了設立網站侵犯個人信息可構成非法利用信息網絡罪、破解了公民個人信息數量“計算難”等問題。

就中國個人信息犯罪規制困境而言，可歸納為以下三方面的問題：①立法策略有待轉變，大數據產業的發展離不開信息的自由流通，在信息洩露愈發嚴重的當下，國家對信息主權的宣導、民眾對信息安全的訴求都預示着立法有必要着眼於個人信息的安全保障與風險管控；②個人信息保護立法體系仍待構建，即中國個人信息保護的民事法律、行政規章並未與刑事規定形成有層次的規制體系，《個人信息保護法》的缺失，使得個人信息相關的重要概念未得以明確，規制的範圍亦呈現模糊狀態[8]；③規制措施尚有完善空間，即現行的刑事規制手段未足以遏制個人信息犯罪行為的發生與蔓延，從本質上來看，是犯罪成本與犯罪收益之間缺失恰當比例，以致刑法的預防作用收效甚微，更多的行為人選擇以身試法。

### (三) 域外個人信息保護立法的相關經驗

第一，制定專門的個人信息保護立法，形成個人信息保護的規制體系，如英國《數據保護法》和

日本《個人信息保護法》。英國《數據保護法》屬於附屬刑法，即在民事法律中規定了刑罰條款，有利於法條的有效銜接和靈活應對犯罪變化。[9] 日本《個人信息保護法》則主要就個人信息獲取、利用目的、安全管理措施、從業者監督等事項進行了規定。對於個人信息犯罪，日本《刑法典》第 134 條規定了洩漏秘密罪、第 246 條第 2 款規定了使用電子電腦詐騙罪。綜上，英國與日本採取了個人信息保護專門立法的策略，雖然在附屬刑法的設置層面有區別，但兩國均對個人信息保護設置了體系化立法，從民事賠償到行政處罰再到刑事責任，形成了梯度化的個人信息保護。

第二，對個人信息業務相關的主體設置了較高的注意義務。德國、日本和台灣地區的刑法均針對不同的個人信息侵犯行為規定了詳細的主體範圍。[10]

第三，個人信息保護呈擴張趨勢。隨着大數據產業的深入發展，侵犯個人信息的行為呈現多元變化，民眾對個人信息安全的意識亦逐漸提升。在此背景下，域外立法多以增加罪狀和增設罪名的方式加以規制。如台灣地區《刑法典》規定了妨礙秘密罪，以保護公民的秘密權，並且在附屬刑法中設置了較多的侵犯個人信息及隱私的犯罪。此外，面對侵犯對象日益複雜多樣的現狀，域外立法多以擴大解釋方式周延保護個人信息。[11]

## 四、大數據環境下中國個人信息保護立法的優化路徑

通過研究域外立法對個人信息的保護，不難發現立法有所側重、刑法介入多節點、保護範圍擴張以及刑法二次規範性等主要特點。必要且適當的法律移植將有助於中國個人信息保護的立法發展和完善，因此在既充分吸收先進經驗，又不盲目照搬的基礎上，提高法律移植的適用性對中國而言具有頗多益處。

### (一) 價值取向：強調個人信息的安全保障和風險管控

自由價值與安全價值的博弈是立法長期的狀態，根據經濟發展、社會狀況、民眾需要而適時變化。以大數據為代表的風險社會下，人造風險已逐步取代自然風險成為了威脅人類生存的主要風險，進而如何管控風險和保障安全成為了現代社會的主要矛盾。從刑事立法演進來看，刑法介入提前化表明刑法不再恪守以結果為核心的追責方式，而是在堅持刑法謙抑性的基礎上提早干預行為，如將具有重大危害可能性的飆車行為、醉駕行為、環境污染行為、個人信息侵害行為納入犯罪。以安全價值為導向的立法理念，在宏觀上提倡對個人信息保護法律的頒行、政府監管部門協同機制的出台以及企業自律規範的制定，實現法制完備、有法可依；在微觀上，設置層次分明、程度不同的法律責任承擔方式。如對於情節輕微的個人信息犯罪者，可使用短期自由行、罰金刑和社區矯正，旨在盡快恢復受損的社會關係；對於情節嚴重的犯罪者，可判處自由刑的同時科以罰金刑和資格刑，進而實現法的引導作用和預防作用。

### (二) 立法策略：個人信息保護立法的有機銜接與體系優化

在安全價值引導的個人信息保護立法策略層面，目前世界各國對於個人信息保護的立法模式大致可分為兩大模式，即分散立法模式和統一立法模式。分散立法模式以美國為典型，即在公領域採取分

散立法模式，逐一在各個領域立法；在私領域，主張實行行業自律，通過行業組織的內部規範保護個人信息。統一立法模式以德國為代表，即通過制定一部完整的個人信息保護法律，進而規範公領域和私領域的個人信息收集、處理和利用等行為，並以信息自決權和一般人格權作為起權利基礎，對個人信息進行統一保護。就中國現狀而言，在查閱相關文獻的基礎上，建議或可採取以統一立法模式為主並佐以行業自律制度的折衷模式。目前個人信息保護的國際立法趨勢表明，已由原來偏重行業自律模式逐漸轉向統一立法模式加上行業自律模式的折衷模式轉變。在中國，隨着大數據戰略的深入實施，個人信息的批量處理和極速傳輸已成常態，說明中國已全面進入信息化社會。個人信息作為無形財產兼具人身屬性，給民眾帶來具有經濟價值的利益，並且對於整個社會的發展及科技創新愈發重要。統一式立法的不足在於，政府的立法可能過分束縛個人信息的自由流通，不利於中國未來信息產業的健康發展。分散式立法模式的弊端表現為，一些公司不參與《安全港協議》[12]，不法從事個人信息業務，或雖參與《安全港協議》，但缺乏自我監管，在從事個人信息業務過程中發生侵害信息主體人格利益的事件。因此，以中國國情為基礎，建議採取統一立法模式為主且佐以行業自律的個人信息保護立法策略。理由在於，第一，如前所述，調和各種保護模式的特點來保護個人信息將成為立法趨勢，中國或可順應該趨勢；第二，中國的隱私權一般制度尚未完整確立，對個人信息的保護難以借助已有的法律制度；第三，中國應注重與域外立法規範接軌，努力符合國際社會對個人信息保護的一般要求；第四，中國信息產業的行業力量仍待壯大，企業組織的控制力還有待加強，完全依賴行業自律難以實現個人信息的保護，因此依靠政府力量實現個人信息的安全與保障具有重要的現實意義。

### (三) 罪名增設：將非法侵入個人信息系統之行為納入犯罪

鑒於非法刺探、非法獲取、非法利用他人個人信息的行為是對他人人格權、個人信息權的侵害，因此在提升個人信息刑事保護力度之時，有必要將非法侵入個人信息的行為規定為犯罪。從犯罪階段來看，侵入公民信息系統罪是侵害公民信息罪的預備狀態，侵入公民信息系統的行為在很大程度上將引發二次犯罪，如電話詐騙、網絡詐騙、入戶盜竊、入室搶劫等。對於個人信息犯罪與二次犯罪的緊密關係，是對中國多地已經發生多起案件進行的規律總結。進而將侵入公民信息系統的行為獨立成罪，既有利於構建個人信息犯罪刑事規制體系，形成體系化規制、針對化打擊，更有助於發揮刑法的自由保障機能。

從構成要件分析，非法侵入個人信息系統罪的主體是一般主體，範圍涵蓋自然人和單位。該罪的保護客體是個人信息系統的安全，所謂個人信息系統是指儲存了大量且敏感的個人信息，還可能儲存了數量較大的虛擬財產的組合體系。此罪的主觀要件為故意，即行為人明知侵入行為公民信息系統的行為會危害個人信息權，並追求該種危害後果的發生。行為人在故意的主觀意識下，實施危害公民信息系統的行為，亦體現了行為的規範違反性和主觀的反社會性。本罪的客觀要件包括兩個方面，一是以侵入方式進行犯罪，二是以個人信息系統為侵入對象。具體而言，“侵入”是指非法用戶利用技術手段或者其他手段突破或者繞過系統安全保護機制“訪問”公民個人信息系統的行為。通常情況下，出於維護信息系統的安全，防火牆等安全保護機制均已建立。該機制可以鑒別訪問者是否具有存取權限，對於不具有存取權限的請求，系統會拒絕其訪問。對於將“侵入”行為歸入犯罪，如《刑法》第 285 條規定了非法侵入電腦信息系統罪。個人信息系統的範圍直接影響了罪與非罪、此罪與彼罪的分割界限，因此有必要進行明確。從電腦犯罪的規定來看，刑法保護的系統信息或數據是電腦數據庫中

產生的保存的數據，包括數據庫的完整性、可靠性、系統靈活性等。公民信息系統的保護範圍目前宜採用以上的保護範圍。但值得注意的是，大數據帶來的科技變革，諸如網頁瀏覽痕迹、下載記錄、關鍵字搜索等信息，一方面不屬於儲存於信息系統的信息，另一方面該些信息可反映使用者的生活規律、消費習慣和經濟狀況，刑法是否應將該些數據作為個人信息的保護對象？[13] 從立法的發展和保護的需求來看，將刑法保護的範圍延伸至上述信息必然是立法的趨勢，符合對大數據本質要求動態性和數據流程系統的描述，但從目前的狀況來看，切實保護信息系統中的信息或數據更為關鍵。公民信息系統的關鍵在於儲存着敏感的、大量的個人信息。相較於現行立法對於電腦系統的保護，個人信息系統的保護側重於個人隱私和個人信息的安全。具體而言，第一，公民信息系統不僅包括電腦系統、網絡設備、通信設備、自動化控制設備等，還涵蓋網絡雲端的公民信息系統，避免了對雲端個人信息犯罪行為的規制不能；第二，與電腦犯罪強調國家安全、國防安全不同，侵入公民信息系統罪設立的初衷在於保護個人信息安全，強調個人的合法權利不受非法侵犯，因此在刑罰量刑的設計上，建議採用短期自由刑結合財產刑，降低入罪門檻；在刑事追訴程序的啟動上，建議採取以自訴為主、公訴為輔的方式；第三，侵害公民信息系統罪的增設，將充分發揮法律的行為指引、行為評價作用，明確告知社會公眾公民的信息系統受法律保護，非法的侵入行為將導致嚴厲的法律責任。

### (四) 規制措施：個人信息犯罪追訴機制轉變與制裁方式優化

針對個人信息犯罪的法律特徵，或可將該類犯罪設置為“告訴才處理”的犯罪，以應對程度不同的個人信息犯罪行為。[14] 從比較法看個人信息犯罪的追訴程序的設置，英美法系的英國、美國以公訴為主，大陸法系的德國、日本則規定為以自訴為主。詳言之，對於情節輕微的個人信息犯罪行為，適用自訴程序，即公權力機關是否追訴行為人的責任取決於當事人的刑事起訴行為。對於達到情節嚴重的個人信息犯罪行為，則規定為公訴案件，以國家強制力保障法律的落實和民眾信息安全。之所以將部分的個人信息犯罪設置為自訴，主要鑒於以下三方面因素：①自訴案件的設置能緩解緊張的司法資源使用情況；②將個人信息犯罪設置為自訴案件有利於被害人獲取足以彌補損失的民事賠償，同時利於降低刑事懲罰的適用範圍，為營造較好的社會歸複氛圍奠定基礎；③自訴案件的設置將促進多元法律制裁措施的制定和落實。侵害個人信息行為依據民事法律、行政規章和刑事法律予以制裁，形成有層次、有梯度的法律制裁體系，對於不同的犯罪行為人適用有區別的懲治措施。總之，自訴為主、公訴為輔的追訴方式與中國現狀契合，並且能促進社會矛盾在較短時間內化解。

個人信息犯罪滋生於科技發展的時代，此類犯罪的實施高度依賴於互聯網絡，因此在制裁手段層面應適時革新。“刑罰輕重的相互協調是根本性的，因為預防重罪要優先於預防輕罪，預防破壞社會秩序的犯罪應多於預防對社會危害較少的犯罪。”[15] 具體而言，第一，以互聯網為核心，對業務涉及個人信息的主體提高較為嚴格的注意義務，降低個人信息洩漏的人為因素。在制裁手段上表現為將不作為的行為納入法律責任範疇；第二，以信息牟利為導向增加犯罪成本，即通過適用高額罰金、限制或剝奪相關的從業資格等方式，顯著增加犯罪成本，明確告知犯罪人和潛在犯罪人觸法的後果必然是弊大於利；第三，刑事和解制度的深入開展。即加害人通過談判、悔過、社區矯正等多種方式，清楚瞭解自己的惡性行為及嚴重結果，促使其積極恢復所破壞的社會關係。相關司法數據表明，個人信息犯罪人多判處短期自由行且緩刑概率較高，因此採用多元法律制裁手段將對規制此類犯罪具有積極的現實意義。此外，對於個人信息犯罪取證難的問題，或可在一定條件下適用舉證責任倒置，即由法

院責令侵權人提交其沒有侵權的證據，若侵權人無法證明，則承擔相應不利的法律後果。

### (五) 個人信息保護：構建綜合保護體系，發揮政策引導及道德規範雙重作用

在個人信息權模式下，法律保護系統構建應具有科學性和前瞻性。科學性要求立法者運用科學的手段、方法和技術進行立法活動，使最終的立法兼具科學與合理要素。前瞻性是指立法者立足現實並具有遠瞻視野，尤其在互聯網環境下，侵害個人信息行為層出不窮，新技術的廣泛運用亦帶來了法律挑戰和監管困境。

就個人信息保護法律體系構建而言，首先應在憲法層面明確公民個人信息權利依法受法律保護，並規定國家在部門法律中明確個人信息權的保護方式和責任形式；其次在民事法律中規定個人信息權相關的概念、範圍與責任；再者在行政法律層面規定公權力的行使限度，防範公權力對個人信息權的侵害，並且規定侵害個人信息權的行政違法責任和行政救濟途徑；最後於刑法層面，將個人信息權規定為保護法益，明確個人信息保護的刑法範疇，並制定相應的刑罰措施。民事、行政和刑事層面的個人信息保護條款，應形成相互銜接、層次遞進的有機整體，為個人信息保護提供明確的行為規範和責任依據。

在個人信息保護的政策層面，應積極發揮社會政策的導向作用，實現社會秩序的長期穩定，滿足民眾對秩序和安全的需求。德國刑法學者李斯特曾指出，最好的社會政策即最好的刑事政策。刑法學界認識到在預防犯罪方面起到關鍵作用的不是刑法而是刑事政策。在個人信息保護的刑事政策層面，刑法仍應作為法律的最後一道防綫，並且刑法的適用亦應建立於人權保障和弘揚法治的價值之上。以政策引導民眾正確對待個人信息，企業正確使用個人信息，在制裁個人信息侵害行為之時亦注意防範制裁措施本身的風險，切不可以犧牲社會及其成員權益、喪失人權保障來維護個人信息安全。

在個人信息保護的道德層面，應充分發揮道德的教育作用和規範作用。一方面持續培養民眾良好的道德意志和得到行為，樹立正確的個人信息使用觀念，提升對自身信息的保護和防範認識；另一方面促進單位、企業加強個人信息的自我管理和監督，逐步制定相應的個人信息保護規定和應對機制，防範內部人員的作案風險。

## 五、結語

人類步入風險社會，人造風險逐步取代自然風險成為威脅人類社會的主要風險，正如人類站在現代文明的火山之上。[16] 在大數據環境下，個人信息犯罪的產生和演變無不依賴科技發展、市場經濟，對此我們有必要轉變理念、優化現行立法體系和革新法律制裁手段。強調安全、把控風險逐漸成為了國家要務和輿論重心，審慎借鑒域外相關立法經驗可較快推進中國立法進程，通過對個人信息犯罪的立法價值和立法策略轉變、罪名和規制措施更新，將促進中國刑事立法在大數據時代下的積極應對，並且推動中國大數據立法體系的構建。

**註釋：**

[1] 大數據是以容量大、類型多、存取速度快、應用價值高為主要特徵的數據集合，正快速發展為對數量巨大、來源分散、格式多樣的數據進行採集、存儲和關聯分析，從中發現新知識、創造新價值、提升新能力的新一代信息技術和服務業態。

[2] 馮登國：《大數據安全與隱私保護》，載於《電腦學報》，2014 年第 1 期。

[3] 見《民法總則》第 111 條規定，“自然人的個人信息受法律保護。任何組織和個人需要獲取他人個人信息的，應當依法取得並確保信息安全，不得非法收集、使用、加工、傳輸他人個人信息，不得非法買賣、提供或者公開他人個人信息。”

[4] 王作富：《刑法分則實務研究》，北京：中國方正出版社，2010 年，第 963 頁。

[5] [德]烏爾里希・貝克：《風險社會》，何博聞譯，南京：譯林出版社，2004 年，第 2 頁。

[6] 法定犯是意大利犯罪學家加羅法洛最早提出的一種相對於自然犯的犯罪類型，是指侵害或者威脅法益但沒有明顯違反倫理道德的現代型犯罪。

[7] 陳興良：《刑法哲學》，北京：中國政法大學出版社，2004 年。

[8] 吳萇弘：《個人信息的刑法保護研究》，上海：上海社會科學院出版社，2014 年，第 157 頁。

[9] 如英國《數據保護法》第 5 條規定了禁止未經登記許可掌握私人數據罪，第 15 條規定了電腦服務未經授權的數據披露罪，第 20 條設置了替代責任和法人責任。

[10] 如台灣地區《刑法典》規定侵犯個人信息的犯罪主體既包括公務機關，也包括非公務機關，強調行為人的目的和動機和信息來源係其工作或職責所得，對一般主體實施的嚴重侵犯公民個人信息的行為也予以制裁。此外台灣地區《刑法典》第 316 條規定了“洩漏業務上知悉他人秘密罪”，是指醫師、藥師、藥商、助產士、心理師、宗教師、律師、辯護人、公證人、會計師或其業務上佐理人，或曾任此等職務之人，無故洩漏因業務知悉或持有他人秘密者，處一年以下有期徒刑、拘役或五萬元以下罰金。

[11] 以美國為例，其針對身份信息犯罪所保護的個人信息範圍從原來的姓名、社會保障卡號、信用卡號等內容延伸至任何能獨立識別、或與其他信息一起用於識別某一特殊個體的姓名或數位。

[12] 安全港協議(Safe Harbor)，是指 2000 年 12 月美國商業部與歐盟建議的協議，旨在調整美國企業出口和處理歐洲公民的個人數據。

[13] 黃曉亮：《從虛擬回歸真實：大數據時代刑法的挑戰與應對》，載於《中國政法大學學報》，2015 第 4 期。

[14] 劉憲權、方晉曄：《個人信息刑法保護的立法及完善》，載於《華東政法大學學報》，2009 年第 3 期，第 127 頁。

[15] [法]孟德斯鳩：《論法的精神》，許家星譯，北京：中國社會科學出版社，2007 年，第 191 頁。

[16] 同註 5，第 11 頁。