# 企業濫用個人信息的法律應對

文立彬*

中共中央總書記習近平在中央政治局第九次集體學習上指出：“人工智能是新一輪科技革命和產業變革的重要驅動力量和戰略性技術，發展人工智能事關我國的科技革命和產業變革的戰略問題”。發展人工智能成為未來一段時期內中國科技革命和產業變革的重要目標。人工智能的核心在於預測，而預測準確度依賴於大量個人信息的搜集、處理和運用。個人信息作為信息化社會和數字經濟產業的生產力要素，個人信息的保護與流通已上升至國家安全的高度。

## 一、問題的提出

在數據產業發展規模和經濟效益持續向好的背景下，中國網絡黑產從業人員已超過 150 萬，數據黑產鏈條已經形成較大規模。個人信息作為數據黑產鏈條的核心，個人信息犯罪呈現逐年遞增、分佈集中、罪犯年輕、偏服務業的主要趨勢，並引發諸多二次犯罪。研究指出，企業濫用個人信息的刑事追訴率與自然人相比顯著偏低，企業濫用個人信息呈現“有恃無恐”的狀態，這不僅在互聯網企業中尤為突出，並且呈現愈演愈烈之趨勢。[1] 有數據表明，公安部“淨網 2018”專項行動共偵破個人信息類案件 5,000 餘件，抓獲犯罪嫌疑人 1.3 萬餘名。針對 APP 違法違規亂象，公安機關共清理 APP 3.5 萬餘款，依法查處相關企業 104 家。最高檢察院官網指出，2018 年全國檢察機關共起訴侵犯公民個人信息犯罪 5,271 人，同比上升 20.2%。中國消費者協會在 2018 年 11 月發佈的《100 款 APP 個人信息收集與隱私政策測評報告》中指出，有 91 款 APP 存在過度收集手機用戶個人信息的問題，其中以“位置信息”、“通訊錄信息”和“手機號碼”的過度收集或使用最為常見。由此可知，中國在治理個人信息違法犯罪問題上取得實質進展的同時，也反映出個人信息濫用行為的泛濫與嚴重。在互聯網、大數據和人工智能相互融合的背景下，有必要針對企業濫用個人信息防治問題展開深入的研究，為中國數據產業和人工智能技術的良性發展保駕護航。

* 法學博士、博士後，南寧師範大學法學與社會學院講師

## 二、人工智能時代企業濫用個人信息的防治困境

### (一) 中國人工智能發展與個人信息保護的內在關聯

人工智能高度依賴於數據儲量，個人信息的充分利用正是人工智能深入學習的關鍵環節。在網絡環境中，企業過度搜集、不當儲存、越界使用、相互交換個人信息的情況屢屢發生，顯著加劇了個人信息的侵害狀況。從《“十三五”國家信息化規劃》到《新一代人工智能發展規劃》，從《國家網絡安全戰略》到《網絡空間國際合作戰略》，這一系列政策戰略體現了中國關於個人信息保護的基礎立場，即發展與安全並重、保護與流轉並舉。個人信息作為信息化社會和數字經濟產業的生產力要素，個人信息的保護與流通已上升至國家安全高度。在維護個人信息安全的同時促進個人信息的流通，是發展人工智能的關鍵環節。在個人信息的安全保障層面，個人信息濫用是個人信息非法獲取、非法交易的本質原因，並且濫用個人信息是個人信息權遭受直接損害的環節。因此，治理個人信息濫用是中國治理個人信息犯罪問題的關鍵所在。在人工智能時代，個人信息濫用呈現出高科技犯罪、有組織犯罪、跨國家犯罪和多次生犯罪的主要傾向，提高了個人信息濫用刑事治理的難度。在個人信息流通層面，秉持刑法謙抑性原則，探討個人信息犯罪的單位監管責任和出罪化事由，將促進中國數據產業的行業自律和落實企業監管責任。從人工智能發展和個人信息保護的關係來看，中國人工智能及數據產業發展勢頭強勁受益於較為寬鬆的個人信息保護策略。此外，中國現行個人信息犯罪刑事立法參照歐盟立法將防治個人信息洩露作為重心，阻礙了中國個人信息犯罪的追訴與懲處，應予以修正。對此，基於域內外不同國情特點深入剖析濫用個人信息的防控對策，具有重大的現實意義。

### (二) 中國治理個人信息濫用的現狀分析

自 2009 年中國刑法增設侵犯公民個人信息犯罪至今，個人信息犯罪治理已經取得明顯成效。以刑事立法先於民事和行政立法對個人信息不法行為進行規制，是中國治理個人信息濫用的特點，故以刑法視角考察個人信息濫用現狀符合國情特點。近年來，隨着國家對於人工智能、大數據產業的重視，個人信息保護亦成為了各級公檢法機關依法懲處的對象，這從公安部組織的多次專項整治行動可以看出成效顯著。在 2009 年至 2015 年間，個人信息違法犯罪治理打擊的是出售、非法出售公民個人信息、非法獲取公民個人信息的案件。隨着 2015 年《刑法修正案(九)》修改和確立了侵犯公民個人信息犯罪，此類行為的刑事規制範疇得到了拓寬，並且就不同的法定情節設置了不同的量刑區間。2017 年“兩高”出台的《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》進一步明確了“情節嚴重”和“情節特別嚴重”的適用條件，加上公安部開展的專項整治行動，偵破了一批大案要案，因此該類犯罪案件在 2017 年至 2019 年間呈現顯著增長趨勢。從個人信息犯罪的發案地域來看，主要分佈在沿海區域。究其原因，新技術、新產業、新業態和新模式不斷湧現，沿海地區的人工智能產業具有較好的內部基礎和外部環境。在此背景下，個人信息灰黑色產業鏈條已經形成並逐步蔓延，個人信息犯罪呈現從沿海區域向內陸區域擴散的趨勢。研究指出，在個人信息犯罪中，自然人犯罪佔絕大多數，法人犯罪追訴較低，僅佔不到 1%。從司法判決中可知，服務型企業員工多為提升銷售業績而非法買賣和使用他人個人信息，而作為最終受益的企業則幾乎不需要承認責任。[2] 換言之，在員工案

發的情況下，企業往往將行為責任歸結於員工個人，這導致個人信息保護法人監管責任流於形式，故有必要深入探討企業個人信息安全監管責任之完善。

### (三) 中國治理個人信息濫用的困境剖析

其一，中國現行個人信息犯罪刑事立法參照歐盟立法，將防治個人信息洩露作為重心，阻礙了中國對個人信息犯罪的追訴與懲處。將個人信息洩露作為個人信息保護工作的重心，旨在從源頭嚴密保護個人信息安全。但對於一般的個人信息而言，收集和公開本身不會造成直接的損害，造成損害的多是後續的個人信息濫用行為。比如，在涉及到諸如垃圾信息、騷擾電話、身份假冒和濫用等最為突出的個人信息或數據濫用問題上，中國立法呈現斷層。這導致民眾將個人信息的濫用問題歸咎於個人信息的洩露或是公開，並把解決問題的希望寄託在嚴格的個人信息源頭保護之上。對此，立法完善的方向應是防治個人信息濫用，而不是一味加強個人信息的保密或收集工作。

其二，個人信息分類滯後、企業數據所有權未明確，以致阻礙了個人信息的流轉和利用。中國現行的個人信息保護立法多借鑑的是歐盟的立法模式，但對個人信息的分類標準仍停留在歐盟 1995 年制定的《歐盟個人信息保護指令》(下稱《95 指令》)，即將個人信息分為直接識別型和間接識別型。研究指出，即使是匿名化處理過的個人信息也能夠被用以識別具體個人，完全不可識別的個人信息僅存在理論可能，因此認為區分個人信息的可識別性意義不大。[3] 在歐盟的個人信息保護立法模式中，將個人信息自決權作為保護法益，強調個人對於其信息的控制權和政府對個人信息安全的保障。在美國的個人信息保護立法模式中，則將個人信息保護納入隱私權之中，在個人信息保護中強調政府干預的最小化，一方面通過公、私部門法律對個人信息保護加以規範，另一方面依靠行業自律實現個人信息的有序流轉。[4] 中國《網絡安全法》依據個人信息的可識別程度，將個人信息分為可識別信息和不可識別信息，立法思路來源於歐盟《95 指令》，重點防範個人信息的被識別。對企業而言，其無意收集高風險的可識別信息，通過對個人信息的收集、加工、使用形成的數據，才是企業的核心競爭力，因此立法重心應傾向於企業的數據確權與追責方式。此外，以強調個人信息控制為特色的歐盟模式在中國難以實施，本質原因在於與中國國情脫節，中國目前人工智能產業和數據產業得以迅速壯大的主要原因之一在於較為寬鬆的個人信息保護政策。在人工智能時代，控制信息的成本和信息傳播的成本是成反比的，換言之，信息傳播的成本相當低廉，而控制信息的成本則上不封頂。因此，以控制信息為宗旨的歐盟立法模式，在中國缺乏持續性和操作性。

其三，APP 濫用加劇了個人信息侵害狀況，相關的監管責任有待落實。在傳統經濟下，用戶有不同意的選擇，但在人工智能背景下，交易程序變成了一種“硬性規定”，若用戶拒絕某些權限的申請，應用程序則無法正常使用。對於用戶而言，以個人信息權換取便利屬無奈之舉。在 APP 濫用個人信息的背景，是網絡借貸、網絡詐騙等違法犯罪行為的陷阱。APP 濫用個人信息的背後，也反映出以國家規制為主的防治模式存在諸多弊端，進而有必要將單一的防治模式向多元化轉變。

## 三、域外國家防治企業濫用個人信息的經驗與反思

### (一) 以刑事合規、行業自律為特點的美國治理模式

其一，建立企業個人信息監管刑事合規制度，從企業內部形成個人信息保護屏障。源於美國的企業合規制度旨在通過激勵性的內部監督來彌補外力監督的不足，其包含的犯罪預防措施、犯罪應對方法和報告程序已形成體系，被譽為“懲治經濟犯罪的刑法替代模式”。企業合規(Corporate Compliance)指企業遵守規範、合法經營。企業合規誕生與發展，均以企業自覺遵守法律法規為主綫。在美國，1929 年開始的大蕭條中頒佈的《國家工業復興法》促進了企業間的公平競爭，遵守法律法規越來越成為企業經營的普遍風氣，尤其是在證券投資領域。隨着 20 世紀 60 年代《反托拉斯法》政策實施的進程不斷推進，企業合規管理制度得到了普及。到了 20 世紀 90 年代，美國《聯邦量刑指南》的出台顯著促進了企業合規制度的實施。在該法案中明確規定，企業在組織正確實施了合規管理制度的情況下，可對罰金數量進行必要的減免。並且，若其他條件相同，則實施了合規管理的企業較未實施的企業須繳納的罰金額可能降低 30%至 83%。《聯邦量刑指南》在計算施加於企業的罰金時，將企業組織正確實施了合規管理制度納入考量的範疇之原因在於，注重企業的內部監管在預防犯罪層面的積極作用，通過制度激勵企業積極防範內部刑事風險，不僅可以降低企業陷入商業危機的概率，更能減少企業面臨刑事指控的風險。具體而言，某一企業是否正確組織實施了合規管理制度，主要從企業規模、經營性質和犯罪前科三個因素進行考察。就企業規模而言，規模以上企業一般需要明文規定合規管理的具體制度和操作流程。就經營性質而論，應就不同類型的企業設置不同的管理制度，做到量體裁衣。對於涉及個人信息相關的企業，在其合規治理制度中應明確規定個人信息的收集、使用和流轉制度，明確規定能落實至個人監管責任，以確保個人信息被用於合法合規的途徑。再就企業的犯罪前科而言，實質上是引導企業防範對於特定類型犯罪的預防，通過採取有效、合理的措施防治再犯。從美國的企業合規管理制度發展來看，企業的社會責任以及商業倫理已深紮企業管理，相應的合規管理制度已具備專業化、規範化和體系化。

其二，依靠行業自律，在不同行業間構建個人信息保護屏障，同時儘量避免國家公權力的介入。美國將市場經濟視為社會的重要基石，在此之上將個人信息安全保障依託於行業自律規範和技術保護，較少從國家立法層面尋求解決方案。在 2019 年公佈的世界五百強企業中，中國有 129 家企業上榜，美國有 121 家企業上榜。中國世界五百強企業中，國企佔八成，以能源型企業居多；而美國上榜企業全為私企，產業分佈較為均衡，體現出美國企業與市場經濟、全球貿易的緊密關係。美國奉行的行業自律制度，既有歷史因素的沉澱，又有市場經濟的依託，呈現可持續發展的狀態。美國在個人信息保護層面亦遵從行業自律，注重自律規範具有的靈活性和敏感性，允許並鼓勵涉及個人信息業務的企業就個人信息的流轉和保護尋求利益平衡機制。同時認為個人信息保護最為有效的方法不是嚴防死守個人信息洩露，而是放權給信息主體自行採取行動，在市場經濟中尋求個人信息利用和保護間的良性發展路徑。

### (二) 以嚴格立法、嚴密防控為特色的歐盟治理模式

其一，歐盟通過修訂立法，將嚴重的個人信息不法行為歸入法律規制範疇。基於個人信息自決權的理念，個人信息自決權在 1995 年《歐盟個人信息保護指令》中得以確立，並經由 2016 年《歐洲通用數據保護條例》(General Data Protection Regulation，GDPR)加以完善。歐盟的個人信息自決權源於人格權，是人格權在個人信息層面具體化的表現。歐盟治理模式對個人信息實施事前全面一體的保護，較為容易導致信息流通的障礙。[5] 以嚴格立法為主導介入個人信息保護，說明了歐盟治理模式異於美國，歐盟政府被視為信息個體的保護者，而非市場原理下的第三方。進而，在個人信息安全保護層面，歐盟政府多是承擔積極應對的角色。當信息保護擁護者認定個人信息自決權為公民的基本權利時，個人信息的流通價值和安全價值則較難協調，因此在歐盟模式下的個人信息保護立法呈現出規範詳細、保護嚴密和責任嚴格的主要特點。隨之而來的是個人信息商業價值利用率的降低和個人信息管理成本的上升。面對同樣問題，美國則傾向於採用成本效益的分析模式來尋求協調發展之策。總之，歐盟通過嚴格個人信息立法確保法律權威，促使企業認真遵循規範，倒逼企業重視個人信息處理方式的合法合規。

其二，GDPR 對個人信息處理者和控制者在處理數據全流程中均制定了安全保護防控措施的條款。在對數據處理前，要求企業進行相關的風險評估，已明確其着手數據之前發現處理內容存在哪些問題，進而進行有效的數據風險防控。同時，GDPR 規定企業應設立專門的監管人員負責監管個人信息利用行為，此項規定被學者認為是統一監管與自律監管的結合。[6] 在處理數據的過程中，GDPR 要求企業遵循數據匿名化和數據最小化原則等要求，以確保處理過程中的數據安全。數據經過匿名化處理，喪失了可識別性，企業可以依據自身意識來處理此類數據。數據最小化原則要求企業只收集並儲存達到其目標的最少量的個人信息，相反的，過多數量的數據量不僅會加重企業的信息管理成本，而且會提升企業數據洩露風險。在數據處理後的階段，GDPR 第 32 條規定了數據相關企業應具有數據恢復能力，一旦發生數據洩露事件，會有一套完整的應對方案，並且監管機構也會及時介入。GDPR 作為“最嚴數據法”，其防治個人信息濫用的方式將對世界主要國家的個人信息保護立法產生重要影響，該立法不僅喚醒了歐盟民眾對於自身個人信息流轉方式合法化的重視，而且對企業合規制度的實施和完善起到了強有力的推動作用。

### (三) 中國單位犯罪制度與域外經驗的比較

美國通過將個人信息安全監管義務上升至刑事注意義務，從而促使企業制定和落實內部管理制度，從而降低企業刑事風險和節約國家司法成本。歐盟通過立法詳細規定了個人信息全流程的操作要點和法律責任，倒逼企業重視個人信息處理方式的合法性。歐盟成員國在本國刑法中規定了企業濫用個人信息的犯罪。其中，法國較早和較為全面的規定了法人犯罪。如《法國刑法典》第 226-21 條規定了因數據收集或信息處理產生的人之權利罪[7]，另依據該法第 226-24 條之規定，上述犯罪可由法人構成。此外，該法還以專節三目 13 個條文明確規定了法人犯罪的刑事責任，因而在追究法人犯罪時，只要機關或代表是為了法人的利益實施犯罪，就要同時追究自然人正犯、共犯和法人的刑事責任。[8] 在刑責減免與企業合規的關係上，作為大陸法系國家的法國引入了美國式的暫緩起訴協議制度，並為企

業合規確立了刑法上的激勵機制。[9] 在德國，企業合規計劃在制裁裁量中發揮着關鍵的作用，有效的企業合規計劃能夠作為一個減輕情節在制裁裁量中加以權衡。[10] 需注意的是，德國法規定公司不能被處以刑罰，而只能被處以罰款，企業合規的意義在於減免刑事責任。[11] 在中國，個人信息犯罪立法制定具有先刑後民的特點，因此從刑法角度考察企業濫用個人信息狀況具有合理性。中國《刑法》規定的單位犯罪可由公司、企業、事業單位、機關、團體構成。個人信息犯罪是指《刑法》第 253 條之一規定的侵犯公民個人信息罪，該罪明文規定了可由單位構成。依據《刑法》相關規定，中國企業只能以作為方式構成個人信息犯罪，即同時要滿足兩點要求：一是侵犯公民信息行為是經單位全體成員或單位決策機構集體作出決定，排除了單位中的某個人以個人名義擅自作出決定的情形；二是侵犯公民個人信息所得非法利益歸單位所有。在司法實踐中，一些企業往往為牟利而放任員工實施侵犯他人個人信息的違法犯罪行為，在案發後多將行為責任歸結於員工個人，以致該罪適用於企業的情形甚少，未能起到有效預防單位犯罪的作用。中國現行個人信息犯罪立法受歐盟立法影響，重在防範個人信息洩露，這與國情需求差之甚遠。受益於較為寬鬆的數據政策，中國數據產業在近年來得以迅速壯大，而個人信息的過度搜集、越權使用成為了中國數據產業優化升級面臨的最大阻礙。對此，國內一些知名企業已在完善企業內部的個人信息保護細則，如騰訊公司在 2018 年發佈的《騰訊隱私保護白皮書》中指出其已經制定了隱私保護制度，並正將數據保護策略制度化、數據管理流程規劃化，通過數據加密、數據脫敏、去識別化等技術手段為企業數據安全提供全流程保障。處理好中國數據產業的優化升級，首要解決的是個人信息濫用的普遍性和嚴重性問題，對此應重點把控規模以上企業的數據安全風險，不僅在刑事責任分配上可以審慎借鑑美國經驗，將企業內部監管制度的制定和執行情況作為刑事責任有無及高低的標準，而且也可學習歐盟立法趨勢，落實數據處理原則和企業數據所有權。

## 四、人工智能時代防治企業濫用個人信息的可行路徑

### (一) 確立個人信息權保護法益

建議將個人信息權作為侵犯公民個人信息犯罪的保護法益，且法益內容包括個人法益延和社會法益。個人信息權於刑事司法中的適用思路分解為三個層面：其一，在人工智能時代背景下明確個人信息保護的價值取向。風險社會理論為刑法前置化和實現積極預防提供了正當化事由，個人信息犯罪作為風險社會時代發展的產物，具有法定犯罪、新型犯罪等特徵，故個人信息犯罪所保護的法益應當契合風險社會的基本要求。風險社會理論認為風險已經逐步取代自然風險，成為威脅人類社會的主要災害，法益侵害危險應受到高度重視，進而主張風險管控和安全價值。以個人信息權為個人信息保護基礎，將個人法益和社會法益納入保護內涵，法益內涵的抽象化轉變基於個人信息犯罪危害的不確定性，且刑法對於社會法益的保護亦體現了風險社會的法益預防性和前置性要求，因此將個人信息權確立為個人信息保護法益契合現實需求。其二，在刑事立法層面以個人信息權為基點，優化個人信息類型劃分，在刑法規範層面為個人信息流動鏈條中的多方主體及其權利保護預留空間。個人信息的類型劃分實際上是對個人信息流動中所涉及的主體及其權利進行類型化，進而明確個人信息刑事保護的界限。

相反，個人信息缺乏科學的類型劃分，容易導致本罪保護範圍模糊和引起刑罰正當化缺失的質疑。司法解釋雖然個人信息進行了分類，並依據不同類別設置了程度不一的入罪標準，這是具有積極意義的刑事司法嘗試，但在企業個人信息監管失責層面仍需完善。其三，基於個人信息的專有權側面，在個人信息犯罪刑事追訴層面或可採用自訴與公訴相結合的制度。從比較法視野看，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。究其原因可歸結為兩點：一是基於個人信息權中的個人信息專有權，個人有權在一定範圍決定以何種方式實現法益保護和損害懲處；二是自訴案件的設置能緩解緊張的司法資源使用情況，並能促進多元法律制裁措施的制定和落實。

### (二) 細化個人信息處理規則，賦予企業數據所有權

人工智能技術的發展，促進生活便利的同時亦帶來信息過載、數據安全等問題。新技術、新科技帶來的人為風險危害已經超過自然風險危害，以制度形式把控新科技、新技術的負面效應刻不容緩。通過信息處理規則的細化、企業數據所有權的明確，引導數據產業朝着良性方向發展。在處理個人信息層面，企業首先應遵循數據最小化和數據匿名化原則，把握好用戶數據利用和保護之間的關係。數據最小化要求企業明確搜集和使用個人信息的界限。數據匿名化則要求企業實現數據的去識別性，降低企業的數據濫用風險和拓寬數據盈利空間，有助於“數據產權制度”的構建。在實踐中，企業應就自身的數據匿名狀況、數據交易方再度識別個人信息的風險進行第三方評估，以確保企業數據所有權的合法使用和數據交易風險的可控性。同時，公權力機關應重點監管和打擊個人身份再識別行為，即通過數據使用許可協議，限制個人信息的使用與披露，在發現違反使用許可協議時，依行為性質追究信息再識別行為人的法律責任。此外，面對 APP 濫用個人信息的嚴峻形勢，我們不僅應正視“知情—同意”原則的形式化弊端，而且應設置“知情—同意”原則的豁免規定。一方面，通過可期待性修正“知情—同意”原則，在立法上預留彈性空間，從而提升司法實踐的可操作性。[12] 簡言之，即使用戶閱讀並同意的 APP 的隱私協議，但 APP 運營商越權搜集和使用了用戶個人信息，屬違背用戶個人信息運用的合理期待，依然可以認定為侵犯個人信息行為並承擔相應責任。另一方面，推進數據活動正當性事由的多樣化。中國《信息安全技術：個人信息安全規範》第 5.4 條規定了在特殊情況下，可以不徵得同意即可合法收集個人信息，符合個人信息權法益的價值取向，體現了人工智能時代企業對智能產品深度開發和應用的真實需求，將有助於中國數據產業和工人智能技術的發展。然而，《信息安全技術：個人信息安全規範》規定的無需徵得同意的特殊情形讓較為有限，“知情—同意”原則過度限制了個人信息的利用，因此有必要逐步拓寬個人信息收集、使用和轉讓過程中的正當化事由。

企業在對搜集的個人信息進行上述處理後，可以豁免某些相關義務，這意味着擁有該些數據的企業不必再徵得用戶的同意，就擁有了佔有、使用、轉讓數據並從中收益的權利，即享有數據所有權。在人工智能時代，個人信息的廣泛搜集和深度發掘有利於實現更為精準的預測，這對於企業、甚至國家而言都是核心競爭力。個人信息權法益的確立，本質在於將個人信息所包含的人身權、隱私權和財

產權進行綜合保護，立法宗旨也從單一保護轉讓保護與利用兼顧。[13] 因此，賦予企業數據所有權，允許其利用和保護經合法處理的個人信息，在法律允許的範圍內實現個人信息經濟效益的最大化利用，這不僅有利於企業完善自身數據保護制度和技術，更利於數據的深度發掘和依法流轉，促進數據產業的良性發展。

### (三) 引入企業刑事合規制度，激勵企業強化內部管理

域外的企業合規管理制度源於風險社會理論，旨在降低企業管理風險和積極影響刑事責任承擔，最終作用於企業商業價值的提升。相較於傳統的犯罪治理模式，企業刑事合規制度體現的“合作治理”模式，意味着企業內部自我管理與外部治理的合作，將責任落實至個人，克服傳統單一的外部規制效率低下的弊端，有益實現刑法積極預防。從立法實踐來看，中國《刑法》第 286 條之一規定的拒不履行信息網絡安全管理義務罪，說明了立法者認可採取刑法手段推動企業內控的方式，反映了刑事合規的部分理念。在國家管理者看來，企業刑事合規制度的實施意味着司法效率的提升。《網絡安全法》的頒佈施行，為網絡服務商提供了行為指引和責任分配，但行政處罰責任的威懾力限制了其預防個人信息濫用作用的發揮。因此，有必要通過刑事立法方式有效促進企業履行內部管理義務。具體而言，企業刑事合規與責任承擔、注意義務違反等問題存在內在關聯，以刑罰激勵企業自我規制是可行路徑。簡言之，通過管理過失和刑罰激勵，賦予特定人員保證人義務等方式，對企業合規管理實現縝密規劃。[14] 企業落實合規管理，舉證說明自身已經盡到了合理的注意和結果迴避義務，進而不僅可以作為刑罰減輕的依據，還可以作為阻卻刑罰的事由。

企業刑事合規制度在本土化路徑上還應當注意以下三點：其一，企業是否落實合規管理，可以作為減輕或阻卻刑罰的依據，但不應當成為加重刑罰的根據。前述提及，規制規模以上企業濫用個人信息是目前問題治理的核心。中國小型企業眾多，公司治理水平參差不齊，將企業合規管理的有無作為加強刑罰的法定事由很可能造成不公。其二，從中國現行的法律規範來看，企業合規制度尚未被明確規定為一項普遍的公司義務。如僅規定了金融機構和上市公司的董事具有法定的內部控制義務，而實踐中董事內部控制義務存在着操作性弱等諸多問題。對此，需要律師團隊進駐企業，與企業的董事會、高級管理層、審計部門以及各種業務部門進行通力合作，在全面掌握企業的具體情況後建立切實有效的合規制度。在企業面對調查和起訴時，律師團隊除了提供應對服務之外，還可就企業違法違規、風險分佈和合規漏洞的問題提出完善建議。從域外立法看，這將有益於企業降低刑事責任風險以及防範再犯。其三，在刑法典中完善單位關於減輕或加重法定量刑情節的規定。中國對單位犯罪採取單罰制，即僅規定了可以對單位判處罰金，沒有規定相應的刑罰裁量制度。就現行的單位罰金刑而言，有研究指出，全球範圍內的罰金刑適用差異較大，中國的問題在於罰金刑執行率偏低，有超過三分之二的罰金刑得不到執行。[15] 對此，或可借鑑法國刑法典關於法人量刑和執行制度的經驗。如在刑法典中規定法人成立累犯的條件和情形、法人適用緩刑的條件和效力、法人犯罪的刑罰消滅。只有在刑事法中明確規定單位犯罪的法定減輕和加重處罰情節，包括企業合規在內的措施才有機會納入量刑裁量的考察範疇。總之，相較於域外經驗，企業合規管理制度在中國處於初級階段，刑法立法將企業合規作為一種激勵機制促使企業遵循規範、合法經營，不失為應對企業濫用個人信息的可行對策。

### (四) 侵犯公民個人信息罪中信息條數認定的司法規則優化

雖然 2017 年《最高人民法院與最高人民檢察院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》(以下簡稱“《解釋》”)對於個人信息條數的計算和認定出台了相關的規定，但司法實踐中仍對該問題有着不同的看法。關於公民個人信息數量的認定標準，存在着“主觀說”和“客觀說”的爭議，在查閱相關文獻資料的基礎上，建議採用“主客觀結合說”。首先，“主觀說”認為，應當以行為人主觀意欲出售或者提供的方式來認定公民個人信息的條數。換句話說，行為人將多條特定個人信息進行統一編輯，其主觀目的在於出售或提供編輯完畢的個人信息。其次，“客觀說”主張，應依據涉案公民個人信息客觀可能侵害的法益進行認定。即行為人將他人個人信息按照人身信息、財產信息等分類編輯成一條信息，但該條個人信息在客觀上卻指向被害人的多項法益，應當在數量上認定為多條個人信息。在研究中發現，司法實踐多採用“主觀說”，即對於查獲的個人信息在排除重複、不真實的信息後予以直接認定。[16] 主觀說的優勢可概括為兩點，其一是能節約有限的司法資源且提高辦案效率，其二是司法機關認定的依據是行為人編輯的原始數據且異議可能性較小，進而案件質量較有保證。然而在司法實踐中，個人信息犯罪的信息條數根據信息類型的不同而劃分為不同的入罪門檻。因此採用一刀切的方式或適用“主觀說”或適用“客觀說”，並不能有效的解決實踐中的信息條數認定困難。因此，建議採用“主客觀結合說”。詳言之，其一，在信息數量直接影響罪與非罪、犯罪情節輕重判斷的情況下，以客觀說為依據，仔細甄別信息涉及的保護法益，並依據所侵犯的法益數量評價犯罪構成及罪數情況。其二，在個人信息條數達到一定規模時，且信息數量的認定不會影響罪與非罪、法定刑檔次的選擇時可以採用主觀說。採用主客觀結合說，既能確保個人信息犯罪中的正義實現，又能較好的解決司法資源緊張的問題。

關於公民個人信息犯罪中“批量信息”的理解與適用，我們認為應以涉案個人信息數量達 5,000 條為標準。《解釋》第 11 條規定，對批量公民個人信息的條數，根據查獲的數量直接認定，但是有證據證明信息不真實或者重複的除外。為準確適用《解釋》，應着重把握以下三點內容。其一，結合《解釋》關於個人信息類別的劃分及犯罪情節設定，“批量公民個人信息”宜認定為數量在 5,000 條以上的公民個人信息。對於未達到此數量標準的個人信息，前述提及建議採用客觀說對“敏感”個人信息和“重要”個人信息進行逐一甄別，避免國家刑罰權力的濫用。其二，控方運用抽樣檢測辦法驗證信息真偽。部分生效判決中未寫明涉案個人信息鑑定的程序與結果。《解釋》規定對於批量個人信息可以查獲的數量直接認定，但缺乏證明標準和證明程序，很可能導致司法不公的情況出現。對此，建議推廣適用抽樣取證的辦法，即通過抽樣檢測以表明涉案個人信息為真的高度蓋然性，從概率上建立起基礎實施和推定事實之間的常態聯繫。其三，保障犯罪嫌疑人的反駁權利。《解釋》規定，對於犯罪嫌疑人能夠舉證證明信息重複或者不真實的，不計入涉案個人信息。對於批量個人信息數量的計算，控方只需要對基礎事實提出證據加以證明即可完成舉證責任，而犯罪嫌疑人則需要提供反駁、反證使控方的主張或事實處於真偽不明的狀態。[17] 犯罪嫌疑人擁有的反駁不僅是刑事訴訟中辯護權的延伸，而且是刑事訴訟推定證明中法律賦予被告人的舉證負擔。因此要求犯罪嫌疑人要以積極刑事進行辯護，若單純以沉默、言語進行反駁，缺乏具有說服力的證據支撐，則無法達到無罪辯護或罪輕辯護的效果。

### (五) 侵犯公民個人信息犯罪刑罰適用的完善思路

第一，側重一般預防的需求，規範罰金裁量的適用標準，逐步設立罰金緩刑制度和罰金替代制度和。刑罰應當具有正當性，並根據罪行的不同適用不同的刑罰思想。對於少發、偶發的犯罪，往往側重於特殊預防的需要；對於多發、常發的犯罪，則側重於一般預防的需求。刑法對於個人信息犯罪的干預應當秉承謹慎與寬和的態度，重視刑罰措施的輕緩性、多樣性和實效性。

針對罰金刑數額差距大的問題，在查閱相關文獻資料的基礎上，建議可在個人信息犯罪案件庭審中探討建立相對獨立的量刑程序。具體而言，在法庭調查階段，法官先就犯罪行為的定罪事實和相關證據進行調查，此後就涉案的量刑事實和相關證據進行調查。在法庭辯論階段，應保障訴訟雙方能就涉案的量刑問題展開充分的辯論。在判決書撰寫過程中，法官應明確寫明量刑的事實與依據，尤其是具有法定情節的法律事實，實現“看得見的正義”。

針對單處罰金適用率較低且罰金執行率較低的情況，一方面應逐步避免非必要的短期自由刑，擴大罰金刑的適用範圍，另一方面可借鑑德國刑事立法經驗，增設罰金緩刑制度。中國刑法中對性質較重的自由刑和財產刑都規定了緩刑的適用條件，然而對於性質較輕的罰金刑卻無緩刑的適用空間，不符合“舉重以明輕”的法理和邏輯。值得注意的是，罰金緩刑制度的適用應受到嚴格限制，並設置相應的考驗期限。就個人信息犯罪而言，建議將罰金緩刑的適用條件設定為最高罰金數額 10 萬元，以兩年作為考驗期限，並規定累犯、主犯不得適用。

針對個人信息犯罪罰金執行難的問題，亦可借鑑德國關於罰金替代制度的規定，即罰金無法執行的情況下，可以自由刑替代罰金刑、以義務勞動間接替代罰金刑。罰金替代制度的目的在於實現刑法的平等適用，讓所有的個人信息罪犯受到應有的懲罰，杜絕作為懲罰和預防輕罪重要手段的罰金刑淪為擺設。進而，對於因生活困難無力繳納罰金、有能力卻拒絕繳納罰金的個人信息罪犯，可以通過建立自由刑替代或以社區義務勞動等社區服刑方式替代罰金刑的制度，確保罰金刑能夠得到有效執行，實際發揮刑罰的應有作用。

第二，明確緩刑適用的前提要件和實質要件。個人信息罪犯適用緩刑的前提要件是指“犯罪情節較輕”，應側重考慮刑罰的報應因素。司法實踐中法官普遍將“犯罪情節較輕”理解為罪行整體較輕，進而對社會危害性相對高的罪犯不適用緩刑。法官從“犯罪情節較輕”整體性進行緩刑適用考量具有一定的合理性，但涉及的情節過多會導致規範冗餘且緩刑制度內外衝突。因此，在查閱相關文獻的基礎上，建議對“犯罪情節較輕”的考量應着重於“人身危險性較輕”與“再犯罪危險性較輕”。個人信息罪犯適用緩刑實質要件是指“沒有再犯罪的危險”，應側重考慮刑罰的特殊預防因素。由於“沒有再犯罪的危險”缺乏具有操作性的評估工具，以至於目前此項評估工作多依據法官自身的辦案經驗，會造成較大的個體差異。因此，應篩選出合適的再犯罪危險預測因素，如取保候審、自首、年齡、共同犯罪、前科、罪數等，進而設計再犯罪危險評估工具，並且整合緩刑執行資源，建立審前調查隊伍，為法官的緩刑裁量提供諮詢。此外，要真正實現緩刑制度的科學適用，應是逐步轉變“裁判結果中心主義”，即只要法官不存在違法職業倫理規範的行為，就不應以判決不當或判決有誤來追究法官的責任。

## 五、結語

從國家一系列政策戰略體現出中國關於個人信息保護的基礎立場，即發展與安全並重、保護與流轉並舉。人工智能時代下，企業濫用個人信息加劇了數據黑產鏈條的複雜狀況。通過對國情狀況和域外經驗的深入分析可知，治理企業濫用個人信息問題，一方面應轉變單一的國家規制模式，轉向由國家與企業共治的防治模式，就單位犯罪的減輕和加重處罰情節作出明確規定，確立企業刑事合規制度的配套規則；另一方面應細化個人信息處理規則，賦予企業數據所有權。個人信息處理規則的細化，旨在明確個人信息保護的邊界，有助於規範數據產業亂象。賦予企業數據所有權，使得企業能投入更多的資源用於提升數據的利用率和安全性，促使數據產業和人工智能技術朝着良性的方向發展。

**註釋：**

1 喻海松：《侵犯公民個人信息罪的司法適用態勢與爭議焦點探析》，《法律適用》2018 年第 7 期，第 10-11 頁。

2 文立彬：《侵犯公民個人信息罪刑事判決實證研究——以 2015-2018 年 335 份相關生效判決為樣本》，《重慶郵電大學學報(社會科學版)》2019 年第 1 期，第 22-23 頁。

3 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, vol. 57, 2010, pp. 1701-1777.

4 張薇、池建新：《美歐個人信息保護制度的比較與分析》，《情報科學》2017 年第 12 期，第 116-117 頁。

5 齊愛民、張哲：《識別與再識別：個人信息的概念界定與立法選擇》，《重慶大學學報(社會科學版)》2018 年第 2 期，第 119-123 頁。

6 項定宜：《比較與啟示：歐盟和美國個人信息商業利用規範模式研究》，《重慶郵電大學學報(社會科學版)》2019 年第 4 期，第 48-50 頁。

7 《法國刑法典》第 226-21 條規定，掌握個人數據信息的任何人，在其記錄、分類、傳輸或其他各種形式的信息處理過程中，擅自改變法律、條例或者國家信息技術與自由委員會批准信息處理之決定對信息規定之用途的，或者擅自改變處理前預先聲明之信息用途的，處 5 年監禁並科 300,000 歐元罰金。

8 黃曉亮：《論我國"單位犯罪"概念的摒棄——以域外比較為切入點》，《政治與法律》2015 年第 3 期，第 38 頁。

9 陳瑞華：《企業合規制度的三個維度——比較法視野下的分析》，《比較法研究》2019 年第 3 期，第 69-70 頁。

10 李本燦：《刑事合規理念的國內法表達——以"中興通訊事件"為切入點》，《法律科學(西北政法大學學報)》 2018 年第 6 期，第 99 頁。

11 [德]烏爾里希·齊白：《全球風險社會與信息社會中的刑法》，周遵友、江溯譯，北京：中國法制出版社，

2012 年，第 252 頁。

[12] 林洹民：《個人信息保護中知情同意原則的困境與出路》，《北京航空航天大學學報(社會科學版)》2018 年第 3 期，第 17-19 頁。

[13] 文立彬：《大數據時代下侵入公民信息系統罪的設立》，《理論月刊》2017 年第 10 期，第 101 頁。

[14] 同註 11，第 102-103 頁。

[15] 熊謀林：《我國罰金刑司法再認識——基於跨國比較的追蹤研究(1945-2011)》，《清華法學》2013 年第 5 期，第 110-111 頁。

[16] 張勇、江奧立：《侵犯公民個人信息罪中的信息數量及認定規則》，《上海政法學院學報》2018 年第 1 期，第 23-24 頁。

[17] 付玉明：《侵犯公民個人信息案件之“批量公民個人信息”的數量認定規則》，《浙江社會科學》2017 年第 10 期，第 28-29 頁。