Dispute Settlement 争议解决, 2023, 9(3), 831-837
Published Online May 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.93111

Hans汉斯

大数据时代个人信息滥用的刑法规制

许毅冰

华东政法大学刑事法学院，上海

收稿日期：2023年3月16日；录用日期：2023年5月9日；发布日期：2023年5月16日

摘　要

针对近年来侵犯个人信息案件频发的现象，我国制定了各类个人信息保护的法律法规，在公法和私法领域形成了一套个人信息保护模式。然而，刑法领域的个人信息保护仍存在许多漏洞，一则，非法转移的传统侵犯个人信息犯罪没有得到有效的遏制；二则，当下刑法忽视了“使用型”侵犯个人信息行为，在个人信息核心权能由转移演化成使用的社会现实下，更无力抵挡个人信息滥用的趋势。一方面，应遵循刑法谦抑性原则，减少对合理利用个人信息行为的干涉；另一方面，在信息化时代，个人信息安全将迎来更大的威胁，在前置法对滥用个人信息行为无法起到很好的遏制、惩罚作时，刑法作为“最后一道防线”，应该设置相应的措施来对此类行为进行规制。

关键词

个人信息，刑法保护

The Criminal Law of Personal Information Misuse in the Era of Big Data

Yibing Xu

School of Criminal Law, East China University of Political Science and Law, Shanghai

Received: Mar. 16th, 2023; accepted: May 9th, 2023; published: May 16th, 2023

Abstract

In response to the frequent occurrence of personal information infringement cases in recent years, China has established various laws and regulations on personal information protection and formed a set of personal information protection model in the field of public and private law. However, the protection of personal information in the field of criminal law remains a lot of loopholes, for one, the traditional crime of illegal transfer of personal information has not been effectively curbed; for

文章引用: 许毅冰. 大数据时代个人信息滥用的刑法规制[J]. 争议解决, 2023, 9(3): 831-837.
DOI: 10.12677/ds.2023.93111

another, the current criminal law ignores the "use-based" infringement of personal information, and under the social reality that the core rights of personal information have evolved from transfer to use, it is even more powerless to resist the trend of misuse of personal information. Therefore, the criminal law, as the "last line of defense", should set up appropriate measures to regulate the misuse of personal information when the previous law is unable to curb and punish the misuse of personal information. The criminal law, as the "last line of defense", should set up appropriate measures to regulate such behaviors.

Keywords

Personal Information, Criminal Law Protection

1. 引言

随着信息网络的全面覆盖，我们进入了大数据时代，数据信息成为了重要的生产资料。信息数据化在带给人们便利的同时，个人信息被泄露、被滥用的风险也日益提升。中国消费者协会 2018 年发布的《App 个人信息泄露情况调查报告》显示：有 85.2%的受访者个人信息曾被泄露，位列前三的信息泄露方式为骚扰电话或短信、诈骗电话和垃圾邮件，还有部分受访者的个人账户密码被盗[1]。除了以各种手段非法获取、泄露公民个人信息外，利用这些信息进行电话营销、精准诈骗等骚扰行为层出不穷，加之数据处理技术的发展，诸如针对个人信息分析加工而产生的 AI 换脸、“大数据杀熟”、数据画像、强制推送等非法利用个人信息的行为也严重影响了公民的正常生活和经济社会的稳定性。

我国对于个人信息的保护经历了由间接保护转向直接保护的过程，相继制定了各类个人信息保护的法律法规，在公法和私法领域形成了一套个人信息保护模式。但是出于种种原因，刑法领域的个人信息保护仍存在许多漏洞：随着个人信息价值提高，原有刑法规定不能满足保护个人信息的需求。尽管在几次法律修订中专门设立、修改了侵犯公民个人信息的相关罪名，且通过相关的司法解释明确与细化了侵犯公民个人信息罪的具体适用问题，但侵犯个人信息的行为仍屡禁不止。随着科技进一步发展，侵犯个人信息行为呈现出多样化、复杂化、隐蔽化的特征，打击侵犯个人信息犯罪陷入困境。

2. 个人信息的内涵

2.1. 个人信息的定义

首先，“可识别性”是个人信息区分于其他信息的关键。2017 年 5 月 8 日颁布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称《解释》)第 1 条对公民个人信息下了定义：侵犯公民个人信息罪中的“公民个人信息”是指，以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。而在 2021 年颁布的《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第 4 条第 1 款则明确，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。尽管以上两个条款对个人信息的定义存在一定分歧，但实际上两者并不矛盾：无论是《解释》还是《个人信息保护法》，“可识别性”都是个人信息的核心要素，即个人信息能够与特定信息、特定自然人相关联，能够通过个人信息识别、确定特定人的身份或活动情况。

其次，个人信息权益常与隐私权是容易被混淆的两种概念，事实上法律对于个人信息的保护也由隐私权保护衍变而来。但是个人信息并不等同于隐私，针对二者法律所应保护的应是不同的法益。隐私权因强调信息的私密性而是一种以秘密保护为内涵的防御性权利，其权能核心是个人对其未公开的秘密信息所进行的范围控制，主要是防范个人私密信息未经许可被向权限外的主体不当转移，造成信息被公开扩散披露[2]。而个人信息内涵多种法益，可以被公开、转移、共享，且不影响其本身价值。对于个人信息的保护不仅是信息转移方面：信息使用的自主性应逐渐成为现今个人信息保护的重点。

2.2. 个人信息权能核心的转变

随着大数据时代的来临，个人信息不再只属于个人，具有个人和公共的双重属性，其公共属性随着数据信息共享的发展而不断增强。个人信息共享的趋势日益强烈，其流转速度也会随之提高。与隐私权不同，个人信息存在主动共享使用的积极权能。且个人信息的使用强调信息主体本身的自主控制，而不是以私密性为核心，自主使用成为现今个人信息权能的核心。

一方面，信息数据化的时代，个人信息一定程度上脱离了主体掌控，即使未经权利人同意，也能被转移和适用，出现了信息主体和控制主体分离的现象。个人信息逐渐同隐私权分离，其特征由秘密性转变为非独占、易转移、难控制，信息主体对个人信息的自主使用、控制收到影响。公开的个人信息虽不具有私密属性但也应属于法律保护范畴：在一定范围公开个人信息不意味着其允许信息被任意使用，信息控制主体对于信息超范围的利用存在着侵犯信息主体个人权益的问题。

另一方面，科技发展提高了个人信息的使用价值，特别是在大数据时代，各类信息被明码标价，高额利润驱动了个人信息的共享使用，个人信息权能超越了精神人格属性，使用价值凸显出来，进一步同隐私权分离开。

与此对应，当下刑法由隐私权(信息私密性)出发、以规制信息转移为重点的个人信息保护模式应该作出调整。刑法既要加强对个人信息的保护以实现对人格的尊重和自由的保障，又需要促进个人信息的合理流动以维护公共性和社会性[3]。

3. 滥用个人信息的刑法规制及漏洞

3.1. 个人信息的刑法保护

纵观世界各国对于个人信息的立法保护模式，主要分为专门立法保护(即个人信息保护法)，或是通过不同法律来保护个人信息(分别立法模式)。我国关于个人信息的立法存在着“先刑后民”的立法状态，缺乏前置法的刑法规制虽然一定程度上缓解了法律惩治需求，但是个人信息本身的具体概念内涵，抑或是所需保护的法益内容都没有前置法的具体规定，刑法作为最后一道防线，既无法处理情节较轻的违法行为，又无法涉及个人信息的细枝末节，难以有效遏制侵犯公民个人信息行为。再者，法律的稳定性和罪刑法定的原则使得现有的刑法规制难以适应大数据时代飞速发展的个人信息犯罪种类和手段，产生了无法被规制的侵犯公民个人信息的“灰色地带”。

具体分析公民个人信息的刑法保护，呈现出直接化与专门化的趋势：由最初的附属其他权利进行保护再到专门立法进行专属保护。我国《刑法》对于个人信息的保护模式可以溯源至对隐私权的保护，并由此衍生，一系列的修改都与隐私权保护的思路相类似，围绕的核心也是重视个人信息的转移，即保护信息的非公开性、私密性。这是由于在网络信息还不发达的时代，个人信息电子化程度不高，个人信息主体和控制人并未分离，信息主体对信息的可控性高，个人信息处于相对私密的状态，即个人信息与个人隐私之间的差异不大。然而随着信息数据化，个人信息的共享性和公开性大大增强，这种类比隐私权的保护模式已不适应大数据时代的要求，滥用个人信息行为伴随个人信息应用价值和商业价值的飞速提

升而大量出现，以隐私权保护角度出发的、重点在于规制信息转移的刑法法规不能产生足够的预防、惩罚作用。应当在侵犯公民个人信息罪的行为类型构造、规范射程等多方面进行调整，将犯罪的规制链条向全场景延伸[4]。

3.2. 滥用个人信息行为的刑法规制缺漏

我国《刑法》所规定的侵犯公民个人信息罪并未将“合法获得，非法使用”个人信息的行为纳入该罪的规制范围，对通过合法手段获得个人信息而后非法使用的行为无法以此罪名追究刑事责任，而是得判断是否符合其他罪构成要件，如无合适的条款，这种滥用行为甚至不构成犯罪。在非法转移的传统侵犯个人信息犯罪没有得到有效的遏制的情况下，现今刑法又忽视了“使用型”侵犯个人信息犯罪，在大数据时代个人信息核心权能由转移演化成使用的社会现实下，更无力防止个人信息滥用愈演愈烈的困境。

3.2.1. 刑法对“合法获取”的个人信息滥用行为规制不足

侵犯公民个人信息罪可以通过合法获取或“自愿”授权等形式进行规避。以公开的个人信息为例，在大数据时代，信息共享融入生活，大众不满足于对信息的简单获取，而是产生了愈发高涨的信息分享热情以及利用需求，群众的日常生活与网络融合的更加紧密，自愿、自发公开个人信息以实现某种目的的情形日渐成为一种常态。此类被公开的信息是行为人出于自愿而发布，他人将这类公开的信息进行收集，并不构成侵犯公民的合法权益。

再如，商业主体滥用个人信息的方式通常表现为概括同意式的“合法”获取后的不当利用，侵害个人信息的方式也从传统的获取型侵犯转化成使用型侵犯[5]。

具体而言，除个人信息价值提升带来的资本逐利引发的滥用个人信息行为泛化外，公民对于个人信息的保护意识不足也是个人信息被广泛不当利用的重要原因。“隐私换便利”是如今较为流行的一种说法，实际上，这里的“隐私”并不仅涉及隐私权方面的内容，也涉及了用户“公开”的个人信息：人们为了享受大数据时代下更为优质便捷的数据信息服务，愿意将自身的相关信息提供给各个平台机构，或主动或被动，个人信息在信息主体与各种中介中转移、共享，个人信息的社会流动已成为常态。可以发现，日常生活中多数 app 如果不进行数据授权则无法正常使用，而这类授权条款一般并不会被仔细阅读，一些关于信息使用的授权便隐藏在这类条款之中。即使大多数人知道这样做会泄露个人信息，甚至信息有被不当利用的可能，为正常使用软件也不得不“被同意”、“被授权”。现今授权常态化的情况下，许多服务方常常通过设置强制性条款抑或把条款细节隐蔽化的手段诱导获取用户授权，以获取最广泛的用户信息，成为个人信息的控制主体。如此一来，再将个人信息作为资产供给第三方使用，获得商业性套利。这类行为在外观上获取了用户的广泛授权，符合“合法获取”的情形，其使用无论合法与否不受刑法规制，个人信息被第三方获取适用也无法追究“中间商”即信息控制主体的信息泄露责任，个人信息安全进一步受到了威胁。

这类对“合法获取”的信息进行不当使用的行为，根据现行刑法并不能直接通过侵犯个人信息罪规制，而是要通过涉及的其他法条进行处理。利用他人信息进行诈骗等可被归纳为其他犯罪的行为，尚可以通过预备犯、帮助犯等犯罪状态、共犯理论来进行制裁，但实践中，合法获取后滥用个人信息的行为很大部分是为满足开展非犯罪活动的需求，例如加强监管、运营决策等商业性运作行为。对此类行为本身，无法通过刑事手段加以制裁，就无法有效规制滥用个人信息行为。而通过用户条款获得使用“授权”的信息控制者，则可以有效规避前置法的相关规定，这样一来，各类商家利用所掌握的用户个人信息进行高频率的广告推送等滥用行为没有得到有效的法律约束，用户受到的信息骚扰频频出现。

3.2.2. 刑法规定难以适应不断变化的滥用个人信息行为

公民个人信息刑法保护的现实困境不仅来自于刑法本身规范的缺陷与不足，更深层次的原因在于对于大数据时代下个人信息法益的核心转变认识不足，无法理清刑法规制侵犯个人信息犯罪的法益出发点为何[4]。

客观现实上，刑法较为稳定，难免因科技发展等产生法律滞后性：现有的个人信息相关的刑法规定，对于滥用个人信息的行为，或只能因涉及相关罪名定罪处罚(如惩治“呼死你”程序案以涉嫌破坏计算机信息系统罪或是非法利用信息网络罪处理)，或运用犯罪形态、共犯理论来作为其他犯罪的预备犯或者共犯进行处理。加之随科技发展，各类新事物纷纷涌现，滥用个人信息的行为种类多样化、手段复杂化，无法被刑法规定的常见情形所涵盖，许多滥用个人信息的行为甚至因找不到相对应的处理规定而不构成犯罪。

主观逻辑上，刑法对个人信息的保护思路未能适时而变。就个人信息权内部权能关系而言，转移权能是个人信息使用权能的基础，但使用权能是转移权能的目标和落脚点，决定了转移权能的行使动机和行使方向，因此使用权能居于个人信息权更核心的地位[6]。刑法对于个人信息的保护仍旧延续同保护隐私权一样的思路，即注重保护信息的非公开性，主要惩罚转移信息型侵害行为，这导致了没能有效规制滥用个人信息行为。

大数据时代网络化发展，个人信息价值的不断增高，信息利润驱使着不法分子以各种手段获取、转卖、利用个人信息，个人信息安全问题将愈发突出和复杂化，公民对于个人信息的使用甚至是日常生活、工作都会受到严重影响，个人信息不被滥用的刑法保护具有紧迫性和必要性。刑法在滥用个人信息行为方面的缺失不仅涉及法理意义上的逻辑缺陷，更对实践中的个人权益保护造成了困难。一旦个人信息的自助处理无法顺利进行，会严重影响到这类有价值的信息的共享适用，从而无法真正发挥个人信息的使用价值。

4. 滥用个人信息行为的刑法规制完善

刑法不应只聚焦于个人信息的转移部分，更应关注个人信息的使用方面。区分隐私权与个人信息权能，独立处理侵犯个人信息的行为。沿用隐私权保护的以规制信息转移为核心的刑法个人信息保护逻辑，忽视了日渐重要的个人信息的使用权能，必然产生对于滥用个人信息行为无法规制或规制不到位的情况。立法者对于刑法规定中对滥用个人信息行为的规制漏洞应当积极回应。

4.1. 完善刑法规制的必要性

4.1.1. 法益保护的需求

信息共享在大数据时代具有重要意义，个人信息主体与控制主体随信息共享转移而分离，公民个人信息有较高的商业价值和应用价值，在实践中滥用公民个人健康信息案例频频发生而技术手段难以防范，刑法其他罪名越来越无法如传统时代一般能够对滥用公民个人信息行为进行附带性评价时，刑法应当适时介入并且提出有效的规制方式[7]。

滥用个人信息行为的大量出现显示了现行刑法对于“合法获取”型侵犯个人信息行为难以有效规制的现实，个人信息自主使用无法得到较好的保护。个人信息侵害已经不单单是通过非法获取来简单利用，更典型的体现为通过利益诱导、批量广泛授权、第三方接转等隐蔽临界手段合法大量取得个人信息的并加以大肆滥用的情形[8]。在侵害个人信息现象频发、侵害行为日益复杂化的情况下，合理运用刑法手段规制个人信息滥用行为，发挥刑法的保护、预防、惩罚功能显得尤为重要。

4.1.2. 刑法与前置法的协调(刑事规制的必要性)

《民法典》《个人信息保护法》中个人信息保护条款的颁布，为刑法规制非法滥用个人信息行为提供了依据，刑法打击合法获取后非法使用的侵犯个人信息的行为并未脱离前置法的规定。但是民法和行

政法中关于个人信息滥用的规定多为原则性的规定，如“禁止非法使用”，但对何为非法使用？使用程度如何等并没有作出进一步具体的阐述，缺乏针对性规定和具体的适用标准，这使得滥用个人信息的行为无法有效遏制，难以追究滥用信息行为人的责任。比如上文中提到的网络服务商“宽口径授权”问题：获取用户信息的同时在合同中附加“使用”的要求，而信息主体为了正常使用网络服务及产品不得不进行“授权”，此类行为是否能被归为民法、行政法中的“非法使用”也无法被明确。

通过现有的法律体系，传统“移转型”的侵犯个人信息行为能够通过刑法及相关前置法的共同规范实现相对有效的遏制作用，然而，“使用型”侵犯个人信息行为的危害已然超越了“转移型”，信息使用作为转移信息的主要目的却被法律规制“忽视”了。当前刑法对于个人信息的保护框架缺乏对合法获取后滥用行为的必要规制。非法获取、转移个人信息的行为固然值得处罚，滥用个人信息的行为同样需要刑法来给予处罚。

刑法作为“法律的最后一道防线”必须严格遵循罪刑法定原则进行入罪处罚。对于滥用个人信息的行为，现今除了有涉及刑法分则相关具体罪名的情况，都只能在行政法或民法范围处理，但是由于前置法规定出台较晚，且相关处罚也不够完善，大多情况下不能真正保护受害者的法益。这要求我们在保护公民个人信息法益的同时，也要为社会信息的共享适用留下充足的空间，以期实现个人利益与社会公共利益的平衡。

4.2. 具体刑法规制完善及入罪边界

在规制的重心上，我国刑法主要关注的是对非法获取信息行为的处罚，但数据流动中真正有危害的其实是对数据的非法滥用，所以有必要实现从非法获取的行为到滥用行为的转变[9]。关于非法使用个人信息的行为刑法具体应如何规制，存在着观点展示：

其一，将“合法获得，非法使用”的行为最妥当的入罪方式是调整《刑法》第 253 条之一第 2 款的规定。该款规定了在履行职责或提供服务时获得公民个人信息的行为属于合法获取，这符合本文所讨论的“合法获取后非法使用”中“合法获取”的行为方式。再者，该款规定对于合法获取的个人信息非法出售或者提供的行为需要从重处罚，与第 1 款对比可以发现，立法者对于行为人合法获取个人信息后实施侵犯公民个人信息的行为持更为严厉的打击态度。非法使用个人信息的行为确实会对个人信息的安全造成更大的侵害，因而将“合法获取后非法使用”的行为归入第 2 款的规定，对非法使用个人信息的行为从重处罚，并无不妥[10]。

其二，认为应比照《刑法》第 253 条之一的第一款规定设置构成要件，将使用列入罪名中，与“出售、提供、窃取”等信息转移行为并列进行定罪处罚，入罪及处罚标准与其相当。无论是归入哪一款规定进行制裁，这样的调整符合刑法稳定性的要求，相关刑法条款的变动仅是小范围的略微调整。

根据刑法谦抑性，滥用个人信息的行为入罪也应达到“情节严重”的程度，“情节严重”具体应如何判断也是我们应该思考的。但实际上犯罪构成要件中“情节严重”是一种较为模糊的概念，其判断很大程度上是司法裁量的过程，直接、单一条件很难判断行为人的行为是否构成“情节严重”。但模糊不意味着含糊，“情节严重”影响因素众多，可以从多个角度采用多种标准来分析，如犯罪行为的客观危害、是否造成严重后果、行为人的主观恶性、犯罪数额大小。具体分析，同一种滥用公民信息的行为，在不同情况下、对不同的人都有可能产生截然不同的结果。

《解释》中的“情节严重”采用多种标准[1]，即类型、数量、违法所得数额、与其他犯罪关系、前科。其中，笔者认为，应当避免将违法所得数额作为认定滥用个人信息行为“情节严重”的决定性因素。违法所得数额大小并不影响是否造成法益侵害，它不表征法益侵害程度，存在侵犯公民个人信息类型严重、

[1]最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释，第五条。

数量众多违法所得数额却较少的情形。实践中由于个人信息数量众多难以查清真伪进而剔除，往往使用违法所得数额情节入罪，这存在较大的人权保障风险[11]。

笔者认为，通过数额认定来认定犯罪情节的方式适用于财产犯罪，而个人信息则具有财产和人身的多种属性，侵犯个人信息罪的保护法益是复合法益，仅以违法所得数额并不能完全评价侵犯个人信息行为的情节，只能作为一种考量因素。以“简历监控”事件为例：用人单位通过从数据平台或购买系统获取员工的简历动态等工作信息，以监控员工动态，筛选、辞退员工。用人单位利用“监控”获取信息来筛选、处罚员工，对劳动者的求职自由、以及正常工作的权利产生了威胁，是对员工个人信息的滥用。这种情况下，如果对于信息使用者的处理限于获利数额，而很难界定用人单位的行为是否达到入罪标准，因为公司监控员工的行为公司获得的并非是直接的经济利润，而是在企业运营中的“隐形利益”，而员工的合法权益也确实因此受损。仅以违法所得的数额多少来评价情节严重与否、侵犯个人信息行为是否入罪，实际是混淆了侵犯公民个人信息罪的法益，亦违反了罪刑法定原则。

5. 结语

在信息网络全面融入社会生活的大背景下，数据共享无论是对社会生活还是专业工作等场合都能带来巨大的便利，如果仅仅立足于信息泄露的风险而限缩各类信息的共享适用，甚至用刑法进行严格规制，只会阻碍社会经济发展，进而损害公共利益。然，现有刑法的规定主要围绕个人信息的转移保护，对与个人信息的使用问题没有形成专门对策，难以起到合理保护作用，如此一来，可能发生公民个人信息自主使用受限、个人信息权益无法保障的情况，进一步威胁个人信息的整体秩序。大数据时代信息共享的重要性和个人信息的价值属性决定了保护个人信息合理使用的必要性，要在使个人信息主体不受侵犯的情况下，发挥个人信息的应用价值，实现个人信息的高效利用。

在遵循刑法谦抑性原则、减少干涉个人信息合理利用的前提下，在民法、行政法等前置法对于滥用个人信息行为无法起到很好惩治作用的时候，刑法应发挥“最后一道防线”的作用，将“使用性”侵犯个人信息行为纳入刑法规制范围，以期构建合理的个人信息的刑法保护体系。

参考文献

[1] 澎湃新闻. 中消协发布 App 个人信息泄露报告, 超八成受访者有相关遭遇[EB/OL]. https://baijiahao.baidu.com/s?id=1610102259010218436&wfr=spider&for=pc, 2018-08-29.

[2] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(4): 62-72.

[3] 陈国军. 论大数据时代个人信息的私法保护与共享[J]. 河南师范大学学报(哲学社会科学版), 2022, 49(1): 66-73.

[4] 李怀胜. 公民个人信息保护的刑法扩展路径及策略转变[J]. 江淮论坛, 2020(3): 114-122.

[5] 龚珊珊, 李韬. 滥用公民个人信息行为的刑法保护路径研究——以个人健康信息为例[J]. 北京航空航天大学学报(社会科学版), 2022, 35(6): 64-71.

[6] 李川. 个人信息犯罪的规制困境与对策完善——从大数据环境下滥用信息问题切入[J]. 中国刑事法杂志, 2019(5): 34-47.

[7] 张明楷. 《刑法修正案(十一)》对司法解释的否认及其问题解决[J]. 法学, 2021(2): 3-18.

[8] 弗兰克·帕斯奎尔. 黑箱社会: 控制金钱和信息的数据法则[M]. 赵亚男, 译. 北京: 中信出版集团, 2015: 88.

[9] 劳东燕. 个人数据的刑法保护模式[J]. 比较法研究, 2020(5): 35-50.

[10] 刘宪权, 何阳阳. 《个人信息保护法》视角下侵犯公民个人信息罪要件的调整[J]. 华南师范大学学报(社会科学版), 2022(1): 141-154+207-208.

[11] 蔡燊. 侵犯公民个人信息罪的保护法益及其运用——从个人信息的公共属性切入[J]. 大连理工大学学报(社会科学版), 2022, 43(3): 74-83.