Dispute Settlement 争议解决, 2023, 9(2), 514-520
Published Online March 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.92069

Hans汉斯

“去识别化”个人信息的刑法保护

孙　冕

华东政法大学，刑事法学院，上海

收稿日期：2023年2月3日；录用日期：2023年3月5日；发布日期：2023年3月16日

摘　要

司法解释将“去识别化”个人信息排除在刑法保护范围之外，但是个人信息彻底去识别化且达到无法复原的程度几乎不可能，只会导致大量形式上匿名化或者形式上已经去识别化的个人信息暴露于风险之中。“去识别化”个人信息的公共属性来源于其自身固有的流通利益，侵犯公民个人信息罪应坚守个人信息自决权的法益立场，因此“去识别化”个人信息的刑法保护具有正当性。“去识别化”个人信息有三方面刑法保护路径：修正对“识别”的理解以扩张本罪的保护对象；修正知情同意对个人信息再识别的效力规制；将“再识别”行为解释为“以其他方式非法获取”行为。

关键词

“去识别化”个人信息，个人信息自决权，再识别，知情同意，以其他方式非法获取

Criminal Law Protection of “De-Identified” Personal Data

Mian Sun

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

Received: Feb. 3rd, 2023; accepted: Mar. 5th, 2023; published: Mar. 16th, 2023

Abstract

The judicial interpretation excludes “de-identified” personal information from the scope of criminal law protection, but it is almost impossible to completely de-identify personal information to the extent that it cannot be recovered, which will only lead to a large number of formally anonymous or formally de-identified personal information being exposed to risks. The public attribute of “de-identified” personal information is derived from its inherent circulation interest, and the crime of infringement of citizens’ personal information should adhere to the legal benefit position of the right to self-determination of personal information, so the criminal law protection of “de-identified”

文章引用: 孙冕. “去识别化”个人信息的刑法保护[J]. 争议解决, 2023, 9(2): 514-520.
DOI: 10.12677/ds.2023.92069

personal information is justified. The criminal law protection of "de-identified" personal information has a three-pronged approach: amending the understanding of "identification" to expand the object of protection of this crime; amending the effect of informed consent to regulate the re-identification of personal information; and interpreting the act of "re-identification".

Keywords

"De-Identified" Personal Information, Right to Self-Determination of Personal Information, Re-Identification, Informed Consent, Otherwise Unlawful Access

1. 引言

随着《刑法修正案》对侵犯公民个人信息罪的不断修改完善，本罪的各项要件也不断成为刑法学界激烈讨论的焦点。可识别性是学界普遍认同的公民个人信息的基本要素，只有具有可识别性的信息才可以成为本罪保护的对象。这一点也获得了刑事司法的认可，两高联合发布的《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》(下文简称《解释》)第 3 条第 2 款也规定，经过处理无法识别特定个人且不能复原的个人信息不在本罪的保护对象之列。该条款的目的旨在平衡个人信息的利用利益与保护利益，具有可识别性的个人信息必须通过信息主体的知情同意方能交易流通，而对于已经去识别化的个人信息，则可以直接绕过信息主体的知情同意环节流入信息市场之中，为信息交换与互动提供素材。然而，该条款很可能只是司法解释者的美好愿景，原因在于随着科技的不断进步，几乎不可能出现个人信息彻底去识别化且无法复原的情况[1]。陈璐教授通过概述美国相关技术研究指出，任何程度上的“去识别化”信息(或称“匿名信息”)都不具有绝对的安全性，将去识别化个人信息与特定个人联系起来在技术上并非难事[2]。即使采用直接识别的方式无法复原个人信息，该类去识别化信息也可以通过间接识别的方式，将一定数量的去识别化信息进行相互结合，即能在茫茫人海中精准地指向信息主体[1]。因此，该条款在实践中的情况是，形式上匿名化或者形式上已经去识别化，但是依然存在再识别风险的个人信息，大量流通于信息市场。司法解释将这些信息排除在侵犯公民个人信息罪的保护范围之外，成为大量数据巨头非法利用该类个人信息的避风港。由于刑事法律并没有对去识别化信息做出明确的保护规定，相关法律也没有对去识别技术化构建起成熟的技术标准，则该类信息是否应当存在于本罪的保护范围之内，以及如何对其在现有的刑法教义学框架内进行保护，也成为了相当重要的问题。

2. “去识别化”个人信息法益保护必要性之证成

对于“去识别化”个人信息的刑法保护必要性之所以存在争议，源于学界对侵犯公民个人信息罪的法益的误读。近年来，法益的功能逐渐从出罪化转向入罪化，抽象危险犯等预防性刑法规定在超个人法益的犯罪领域盛行[3]。对于已经去识别化的个人信息而言，其一方面体现为个人信息自决权，另一方面，个人信息的社会性和公共性在去识别化的过程中得到了加强，这一点主要表现为，该行为侵犯到不特定或多数信息主体的个人法益，这就危及到公共利益、信息秩序和信息安全[4]。因此，有不少观点认为，之所以需要对该种类型的信息进行刑法保护，归根到底是为了保护这些信息背后的社会秩序、国家信息

主权独立以及国家安全等超个人法益[4]。但是，通过《解释》的相关规定就可以看出，刑法对具有识别性的个人信息的保护完全优于对于去识别化个人信息的保护，认为“去识别化”个人信息不仅具有个人法益性质，而且具备社会乃至国家等超个人法益的性质的观点，无异于直接否定了现有实证法秩序对个人信息的态度，同时也并没有回答为何“去识别化”个人信息能够被直接认定为“公民个人信息”的问题[1]。因此，以保护超个人法益为理由来解释对“去识别化”个人信息的保护并非有力。本文认为，应当采本罪的保护法益为个人信息自决权的观点，才能凸显对“去识别化”个人信息刑法保护必要性的正确理解。

2.1. 公民个人信息公共属性之界定

公民个人信息具有公共属性，并不意味着在侵犯公民个人信息的同时也侵害到公共利益等超个人法益。基于超个人法益的概念，本罪的保护法益并不符合超个人法益的内涵特征。首先，学界普遍认为，超个人法益的特定利益应当由全部个体所共有，也无法还原为个人法益[5]。而个人信息具有强烈的财产属性，在一定情形下能给信息主体带来利益，显然并不能为社会共同体所共有且无法还原为个人法益。其次，在当前信息技术快速发展的大数据时代，信息主体的个人信息被暴露在公众目光之中，不同信息主体的大量信息都存在被侵害的风险，尤其是在窃取、出售、购买、交换个人信息等行为产业链化的当下，大量的个人信息被同时侵害是实践中的普遍现象。但被害者人数众多、侵害范围广泛，只是本罪情节严重的表现形式，凸显行为对传统法益的危险程度，达不到侵害人数众多、侵害范围广泛的标准也达不到本罪的入罪标准，并不能因此就判断本罪的行为方式侵害了超个人法益。有别于个人法益的集合体[6]，超个人法益在现代刑法的扩张中取得了独立于个人法益的地位[7]。

学者蔡桑指出，由于个人信息的价值产生于其流动的过程，因此个人信息公共属性的表现不是个人信息权集合而成的秩序、安全、信赖或对信息的排他性权利，或是与信息秩序有关的公共利益，而是信息本身所具有的利用利益[5]。本文赞同该观点。个人信息的公共属性是其本身所固有的属性，符合信息社会的共享特征，这一点与超个人法益论中的社会秩序、信息安全等不同，后者产生于单个的个人信息权并集合而形成[5]。同时，当某些行为重点在于保护个人信息的个人法益而忽视其利用价值时，一般并不会认为这是应当入罪的行为。例如严格规范利用已公开个人信息、对于形式上去识别化的信息纳入保护的范围而非放纵其在市场上流通，这些严格保护信息主体利益的做法实际上加强了其他主体尊重和保护信息主体个人信息的义务。这种安全感向信息主体个人倾斜的行为并不会被认为是违反刑法规定的，这是因为在大数据时代下，个人信息的滥用和泄露的风险加剧了普通数据主体的无力和不安，尤其是在政府、企业与个人的三方关系之中，个人处于绝对弱势的地位，一旦信息被泄露，就会造成不可逆的后果[8]。因此，去识别化个人信息的公共属性并不能等同于超个人法益。对于侵犯公民个人信息罪而言，应当肯定个人处于利益尺度的中心，而不是反射性的或边缘性的利益，其公共属性也仅具有附带性和衍生性的意义[5]。

坚持本罪个人法益的立场同样符合法秩序统一性原理的要求。我国《宪法》虽未明确列举完全基本人权，但是随着时代的变化发展，个人信息权也理应出现在《宪法》尊重和保障的人权之中。同时，《民法典》在人格权编第六章对公民个人信息的权属做出了专章规定，2021 年 11 月起保护公民个人信息的综合性法律规范《个人信息保护法》也正式实施。这些法律规范都充分表明，公民个人信息的重要性不在于对其公共价值的开发和利用，而在于保障公民个人信息的自然人之人格权益[9]。相应地，刑法作为宪法的下位法和整个社会的兜底性法律，其面对个人信息，应当首先着眼于对其本身的保护，谨防行为人利用信息的利用利益进行犯罪。

2.2. 个人信息自决权内涵之廓清

上文已论证，对于本罪的法益，应当坚守个人法益的立场，且无论是《民法典》亦或是《个人信息保护法》，都旨在强调保护个人信息权利。因此，刑法也应当坚守保护个人信息权之立场。不同于传统意义上的隐私权，个人信息权的权属范围更广泛，无论是愿意为人所知晓的一般个人信息，还是不愿为人所知晓的个人隐私，都属于公民个人信息的范围。从权利属性上看，个人信息权属于一种主动性权利，即使没有实际侵害的发生，也可以提前行使其同意权而同意信息的后续流通利用，而隐私权属于被动性权利，必须要求实际侵害发生时，才能主张防御。对这一保护范围更广泛的主动性权利进行保护，符合当前积极刑法观主张的刑法提前介入干预的刑事立法大趋势。但同时，基于刑法的谦抑性理念，《民法典》所确立的个人信息权是一种宽泛的信息权利，那么在侵犯公民个人信息罪的刑法保护法益上，个人信息权应当进一步限缩至个人信息权的核心：个人信息自决权[10]。

个人信息自决权是自我决定权在个人信息领域的具体化[11]。因此，该权利带有一般自我决定权的特征，其核心就在于知情同意，信息主体对个人的信息具有支配的权利，可以自我决定授权给他人使用、流转。作为一般人格权的一种，这项权利是旨在保护个人在数字时代自由发展其人格的“自主权”[12]。本文认为，个人信息自决权并非是一种绝对控制权和排他性支配权，该权利并不排斥国家以及公权力对个人信息的合法强制利用，也不排斥他人对自己信息的利用，权利人本身可以自愿将信息公开，同时权利人依然可以通过删除权、访问权等后续权能对信息进行的控制[13]。因此，为了保障信息主体自由发展的“自主性”，除了个人信息的支配权、知情权、同意权，同时也包括删除权、访问权等后续防御权能，在整个信息流通的过程中都能实现自我决定的自由意志。

2.3. 去识别化个人信息的法益关联性

本文认为，刑法应当将这类“去识别化”个人信息纳入保护的范围，这符合本罪的保护法益：个人信息自决权的要求。对于正常具有可识别性的个人信息，是否存在信息主体的同意或者重大公共利益等法定出罪事由是关注重点，而对于经过去识别化处理的个人信息来说，是否可以被“再识别”是被关注的重点。在个人信息去识别化之前，信息主体有权对其去识别以及去识别之后的合理使用赋权，这是在行使其同意和授权；当个人信息流入信息市场，若信息处理者擅自对信息进行再识别，识别而成与其他信息具有同样可识别性的个人信息，将其暴露于风险之中，本质上就是一种对该信息保护义务的违背，此时信息主体同样可以行使其删除和撤销同意的权利，在信息流动的整个过程中体现对其信息的自由意志。虽然“去识别化”个人信息被再识别是一种风险，并不是一种已出现的现实危害，但本文认为，对去识别化个人信息的保护，在根本上应当依托于对具有可识别性的公民个人信息的保护，是保护可识别性个人信息的辐射效果，在本质上应当被理解为一种“预防性举措”[1]。

3. 去识别化个人信息刑法保护路径

在新的司法解释出台或者相关的去识别化技术标准出台之前，对于“去识别化”个人信息的保护，则应当在遵守罪刑法定原则的前提下，在现有的刑法教义学框架内加强。

3.1. 对本罪保护对象的扩张解释：修正对“识别”的理解

3.1.1. 采用《个人信息保护法》的识别对象要求——广义的识别

“违反国家有关规定 ”是刑法明文规定的侵犯公民个人信息罪的构成要件之一。加上了“有关”二字的“国家有关规定”应从泛义层面来理解，即没有专门性明确规定、有一般性规定的也可以予以认定[14]。就本罪而言，最直接、最专门的明确性“国家有关规定”为《个人信息保护法》。因此，在识别对

象的要求上，若《个人信息保护法》具有明确规定，则《刑法》理应沿用。相较而言，《解释》将个人信息的识别对象规定为“自然人身份”，而《个人信息保护法》将个人信息的识别对象规定为“自然人”。前者实际上是指“你是谁”，指向具有身份标识的显名的个人，而后者是指“你是某个谁”，指向符号化的隐名的个人[15]。因此，对本罪而言，识别的对象不仅包括识别到特定个人的身份，同时还应包括特定自然人的特征、活动等关联信息。正如高富平教授将标识符分为直接标识符和间接标识符，无论是前者还是后者都可以做到指向特定个人。简言之，标识符具有直接识别出个人的能力，而这里的个人时常被解释为不明身份的个体，是一个抽象的“人”[16]。这虽然在一定程度上扩张了公民个人信息的范围，但是符合当前对于个人信息保护的需要。这是因为，在刑法意义上，当行为人获得的个人信息能够关联到特定自然人，其所实施的出售、提供行为即具有侵犯个人法益的潜在危险，而无需精准到该特定自然人的身份，即无须达到身份识别性的程度。否则，公共场所偷拍、手机定位等具有一定社会危害性的行为，却由于涉及到的个人信息并没有识别出特定个人的身份而只能被刑法排除出保护的范围[17]。因此，采用广义识别的要求更容易实现对个人信息的充分保护，不存在保护上的漏洞。而《解释》第 1 条[1]也恰恰证实了“可识别性”不是狭义的身份识别性，同样包括个人特征、活动等关联识别性。

采用广义识别对象的标准并不会导致本罪的保护范围不当扩大。表面上看，采用广义识别的对象标准似乎有将本罪的保护对象无限扩张之嫌。但是本文认为，由于“可识别性”并不是本罪的唯一构成要件要素，其只是构成要件要素之一，成立本罪还需要满足其他的构成要件，如“情节严重”此类罪量因素，因此将可识别性的程度适当扩张并不会造成本罪的泛滥。根据《个人信息解释》第 5 条[2]，可见对后面这一类信息的数量要求比第 3 项涉及的信息数量更高，表明对这些信息本身的可识别性要求并没有达到身份识别性的程度，正是因为如此，司法解释者才会在情节严重这一构成要件上对其要求更严格，使其整体上的可罚性与前一款相当。

3.1.2. 控制间接识别情况下识别节点的数量

既然当前对于去识别化信息而言，可以无限通过间接识别的方式不断精确到信息主体，那么必然会出现识别节点过多的问题，导致再识别行为的无限递归。纵使某些与特定个人相关联的信息的识别性越来越弱，但也无法否认其能够与其他信息结合从而具有识别能力的可能性。由此将导致大量信息都能够成为法律保护的对象[18]。本文认为，该界定思路会导致识别节点无限增多，识别的标准被泛化，也就完全不可能存在真正意义上的“去识别化信息”。尽管现实中尚不存在“不能复原”的去识别化技术，但“不能复原”的严苛要求在文义上显然能够被理解为个人信息去识别化的程度应当达到相当的程度和标准[1]。因此，控制识别节点的作用也是控制去识别化的程度和标准。任何需要经过若干技术程序或转换才能被识别或定性为特定自然人的信息，都不应被视为“可识别为特定自然人”，否则信息利用利益和信息保护利益之间的平衡就会被打破[19]。其次，在肯定识别标准为广义识别的情况下，识别到特定个人的特征、活动情况时，需和个人的其他法益具有强关联性，才能作为本罪的保护对象。个人的行踪轨迹、活动情况、健康信息、手机定位等，属于人的隐私信息，也属于本罪的保护范畴。正如周光权教授指出，应当强调这一信息对于个人行动自由的重要性与关联性，弱化可识别性[19]。

3.2. 修正知情同意对个人信息再识别的效力规制

上文已述，个人信息自决权以知情同意为核心。除了公共利益等法定出罪事由，无论是国际规范还

[1]《解释》第一条规定：刑法第二百五十三条之一规定的“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”。

[2]《解释》第 5 条第 1 款第 3 项涉及“行踪轨迹信息、通信内容、征信信息、财产信息”四项信息，要求犯罪数量达到 50 条属于情节严重，第 4 项规定的“住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息”，犯罪数量要求达到 500 条属于情节严重。

是大多数国家的个人信息保护法，知情同意都是信息持有者处理信息最核心的正当出罪事由。因此，了解同意对去识别和再识别个人信息的影响至关重要。由《解释》第 3 条第 2 款可以看出，已经去识别化的信息绕过了个人知情同意这一环，直接赋予其在信息市场流通的权利。可以认为，此处默认信息主体对于该类已经去识别化的个人信息进行流通是知情且同意的。只是，这种默认的同意并不包括对后续再识别以及再识别后使用、处理的同意。在此，或许可以参考已公开个人信息利用合法化在实践中的普遍标准：二次授权原则。二次授权原则的实质在于区别评价已公开个人信息的获取行为和再次提供行为，对与前者，默认信息主体对信息的流通已经知情同意且授权，对于后者，则需要获得信息主体的二次授权，否则该行为属于违反国家有关规定的行为，有可能构成侵犯公民个人信息罪[20]。该原则可以为“去识别化”个人信息的再识别行为规制提供参考。与已公开个人信息相类似，对“去识别化”个人信息也应当区别评价去识别行为以及再识别行为，获取已经去识别化的个人信息不再需要征得信息主体的同意，剩下的问题是将再识别行为定性为刑事犯罪，此处包括是否该行为已经获得了信息主体的二次授权和同意。行为人获取、处理该去识别化信息应当在合理限度之内，而再识别行为已经完全使得个人信息暴露于风险之下，超出了应有的合理限度，侵害了信息主体的重大利益，因此再识别行为同样需要信息主体的二次授权。信息主体的知情同意也只是对于信息去识别化处理以及处理之后的流通利用的同意，并不包含对于去识别后再识别行为的同意。因此，在其他主体对于去识别化信息进行再识别之前必须再次获得信息主体的知情同意，此时的再识别行为方具有正当性。

当然，在知情同意实施过程中会出现各种问题，例如基于信息壁垒，信息处理者难以尽到告知义务，即使其履行了告知义务，信息主体也很难全然了解其告知的内容。同时算法的出现也加剧知情权保障的难度，很多信息处理者反客为主，让“同意协议”成为自己的“保护伞”，主张其已经通过告知条款使信息主体知晓并同意，无需为对方受到的不利后果担责[21]。因此，传统的知情同意框架架空了信息主体的权利。本文认为，在既保护公民个人的信息自决权的同时，又不能忽视去识别化信息本身所忠实的其流通利益，对于该“再识别”行为的知情同意应当分类讨论，以更契合网络时代的共享和开放特征[4]。对于需再识别到个人身份的信息，应当采取明示识别的方式，而对于仅需识别到个人特征、个人活动情况的个人信息，可采用默示识别的方式。但由于默示同意存在一定程度上的困难，必须谨慎把握其使用限度。张勇教授提出，默示同意制度作为一种明示同意制度的补充性制度，应当默示授权内容、程序等完全合法时才能加以使用。默示同意的格式文本在同意之前就应当向信息主体出示，信息的收集也必须受到严格限制，同时信息的再识别主体也必须在后续流转信息的过程中严格审查该信息的用途是否超越了原有授权范围[4]。

3.3. 将“再识别”行为解释为“以其他方式非法获取”行为

我国侵犯公民个人信息罪的刑法条文只规定了“窃取”和“以其他方式非法获取公民个人信息”两种行为方式。对于“再识别”行为，似乎刑法及相关司法解释并没有做出明确的规制，这也刚好给了行为人游走在本罪边缘的机会。若要对此进行规制，则“再识别”行为必须满足上述两种行为方式的要求。而根据《解释》，“以其他方式非法获取”只包括“购买、收受、交换等方式或者在履行职责、提供服务过程中收集”几种方式。本文认为，“再识别”行为应当被解释为“以其他方式非法获取”行为，以弥补刑法保护的缺漏。

首先，根据“有关国家规定”，《网络安全法》也是刑法泛意义上的前置性法律，具有一定的参考根据。《网络安全法》第 41 条将“非法获取公民个人信息”的行为划分为违反“法律、行政法规的规定”和违反“双方的约定”两种情况，这表明，不仅违反强制性法律法规的行为属于“非法获取”行为，而且未达成合意的具有民事违法性的行为也属于“非法获取”行为。上文已述，根据二次授权原则，再识

别行为并未获得信息主体的授权同意，则信息处理者擅自对其再识别属于违反双方约定的行为。因此，将“非法获取”行为扩大解释为再识别公民个人信息，并不违反有关国家规定，符合体系解释的原理。其次，我国刑法规定非法获取这种行为方式，其关注的重点绝非行为人从何处取得个人信息，而是行为人占有个人信息是否合乎国家有关规定[1]。再识别行为与出售、购买、交换这三种《解释》明文规定的非法获取行为具有相当性，都具有获得本不属于自身之物之意。出售、购买、交换重在从他人处获取，而再识别则重在通过信息技术获得该信息上自己本没有的他人信息，强调从自己处获取[1]，无论是从他人处获取还是从自己处获取，都强调从无到有的过程，属于“获取”的一种行为类型，该过程侵犯了信息主体自我决定权。因此，将“再识别”行为解释为“以其他方式非法获取”行为符合体系解释的规定以及罪刑法定原则的要求，并无类推解释之嫌。

4. 总结

“去识别化”个人信息重在保障信息的利用利益，但是当前刑法对于公民个人信息的保护较为浅显与粗疏，其他法律对于公民个人信息的保护也呈现出碎片化问题，为此，法律对于大数据时代信息主体的保护必须持谦卑而谨慎的态度，不能为了信息的流通而忽视了对其保护。本文对于“去识别化”个人信息的刑法保护提出了粗浅的个人见解，但更需要的是学术理论的不断深入和不断被验证的实践标准。

参考文献

[1] 李昱. “去识别化的个人信息”不受刑法保护吗? [J]. 刑事法评论, 2019, 44(1): 656-692.

[2] 陈璐. 个人信息刑法保护之界限研究[J]. 河南大学学报(社会科学版), 2018, 58(3): 72-78.

[3] 何荣功. 预防刑法的扩张及其限度[J]. 法学研究, 2017, 39(4): 138-154.

[4] 张勇. 个人信息去识别化的刑法应对[J]. 国家检察官学院学报, 2018, 26(4): 91-109+174.

[5] 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.

[6] 马永强. 侵犯公民个人信息罪的法益属性确证[J]. 环球法律评论, 2021, 43(2): 102-118.

[7] 王永茜. 论集体法益的刑法保护[J]. 环球法律评论, 2013, 35(4): 67-80.

[8] 劳东燕. 疫情防控中个人信息的刑法保护[J]. 清华法律评论, 2021, 10(1): 42-56.

[9] 程啸. 论我国民法典中个人信息权益的性质[J]. 政治与法律, 2020(8): 2-14.

[10] 刘艳红. 民法编纂背景下侵犯公民个人信息罪的保护法益: 信息自决权——以刑民一体化及《民法总则》第 111 条为视角[J]. 浙江工商大学学报, 2019(6): 20-32.

[11] 张忆然. 大数据时代“个人信息”的权利变迁与刑法保护的教义学限缩——以“数据财产权”与“信息自决权”的二分为视角[J]. 政治与法律, 2020(6): 53-67.

[12] 孔祥稳. 个人信息自决权的理论批评与实践反思——兼论个人信息保护法第 44 条决定权之适用[J]. 法治现代化研究, 2022, 6(4): 78-97.

[13] 蔡星月. 数据主体的“弱同意”及其规范结构[J]. 比较法研究, 2019(4): 71-86.

[14] 曲新久. 论侵犯公民个人信息犯罪的超个人法益属性[J]. 人民检察, 2015(11): 5-9.

[15] 杨君琳. 论北斗时代的个人位置信息法律保护[J]. 法学杂志, 2021, 42(2): 34-45.

[16] 高富平. 个人信息流通利用的制度基础——以信息识别性为视角[J]. 环球法律评论, 2022, 44(1): 84-99.

[17] 晋涛. 刑法中个人信息“识别性”的取舍[J]. 中国刑事法杂志, 2019, 5(5): 63-76.

[18] 黄事攀. 侵犯公民个人信息罪犯罪对象的识别性研究[D]: [硕士学位论文]. 兰州: 兰州大学, 2022.

[19] 周光权. 侵犯公民个人信息罪的行为对象[J]. 清华法学, 2021, 15(3): 25-40.

[20] 王华伟. 已公开个人信息的刑法保护[J]. 法学研究, 2022, 44(2): 191-208.

[21] 江书晔. 个人信息保护中知情同意规则有效实施的路径选择[J]. 信息安全研究, 2023, 9(2): 154-161.