

Web3.0时代下侵犯公民个人信息罪的特征和法益明晰

李玮玮

华东政法大学刑事法学院，上海

收稿日期：2023年10月13日；录用日期：2023年11月9日；发布日期：2023年11月17日

摘要

随着科技的进步，已经迎来Web3.0时代。在Web3.0时代，存在一个由传统现实生活延伸出的包含衣食住行等日常生活的网络空间，在这一空间中充斥并流动着大量个人信息。Web3.0时代在实现足不出户完成工作、娱乐、生活，给人们带来便利的同时，侵犯个人信息犯罪也呈现高发的频率以及多变的形式。为了充分发挥Web3.0的优势，规避对公民个人信息可能带来的风险，为侵犯公民个人信息罪划定合理的犯罪圈，可以借鉴《欧盟基本权利宪章》和《欧盟运作条约》将个人信息保护权作为本罪的法益。在保护公民个人信息不受侵犯的同时，也促进个人信息进行有限制的流转利用，平衡保护个人信息与信息流转带来的社会效益，以期为人民提供更优质的服务，优化网络环境。

关键词

网络犯罪，个人信息，法益

Clarity on the Characteristics and Legal Interest of the Crime of Infringing on Citizens' Personal Information in the Era of Web 3.0

Weiwei Li

Criminal Justice College, East China University of Political Science and Law, Shanghai

Received: Oct. 13th, 2023; accepted: Nov. 9th, 2023; published: Nov. 17th, 2023

Abstract

With the advancement of science and technology, the Web 3.0 era has been ushered in. In the era

文章引用: 李玮玮. Web3.0 时代下侵犯公民个人信息罪的特征和法益明晰[J]. 争议解决, 2023, 9(6): 3162-3169.

DOI: 10.12677/ds.2023.96431

of Web 3.0, there is a cyberspace extending from traditional real life that includes daily life such as food, clothing, housing and transportation, and a large amount of personal information flows in this space. In the era of Web 3.0, while completing work, entertainment, and life without leaving home, and bringing convenience to people, crimes of infringing on personal information also show high frequency and changeable forms. In order to give full play to the advantages of Web 3.0, avoid the risks that may be brought to citizens' personal information, and delineate a reasonable criminal circle for the crime of infringing on citizens' personal information, the right to protect personal information can be referred to as the legal benefit of this crime in the EU Charter of Fundamental Rights and the EU Treaty on the Functioning of the European Union. While protecting citizens' personal information from infringement, it also promotes the limited circulation and use of personal information, balancing the protection of personal information and the social benefits brought by information flow, so as to provide citizens with better services and optimize the network environment.

Keywords

Cybercrime, Personal Information, Legal Interest

Copyright © 2023 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

科技在改变生活的同时，也对犯罪行为的形式产生了一定的影响，网络时代历经 Web1.0、Web2.0 再到如今 Web3.0，在此发展过程中也滋生了不同的犯罪形式。公民个人信息随着 Web3.0 时代的到来，被泄露和不合理使用的风险提升，需要特殊的规制。

2. Web1.0、2.0、3.0 时代侵犯个人信息犯罪的特征

(一) Web1.0 和 2.0 时代

瑞达网络公司的创始人诺瓦·斯皮瓦克(Nova Spivack)以 10 年为一个周期，将网络发展的第一个十年(1990~2000)作为“信息单向发布的 Web1.0 时代”，第二个十年(2000~2010)视为“互动参与的 Web2.0 时代”[1]。Web1.0 与 Web2.0 的主要区别在于网络内容的发出者是否包含普通网民。

在 Web1.0 时代，关键词是只读(only-read)，也被称为只读网络。网民对于网络上的信息只能读取，普通用户不能编辑修改，即网民只能单向、被动地浏览网站发布的信息。此时的网站更类似于电子报纸或者电子公告牌，上网相较于传统获取信息的方式而言，不过是一种电子化的延伸。在 Web2.0 时代，关键词是互动(interaction)，也被称为参与式社交网络。网络不再只是单纯地输出信息，网民也不再只被动地浏览信息，而是借由网站搭建的平台，实现互动交流，由被动地接收网络信息转变为可以主动创造网络信息。就如在新浪微博上既可以发表自己的观点，也可以评论别人的观点，还可以回复别人对自己观点的评论，社交媒体的产生与发展就是 Web2.0 时代最突出的成果。此时，网民在互联网世界除了承担阅读者的角色还要承担参与者的角色，由此不可避免地会留下个人信息。

2009 年，刑法修正案(七)新增第二百五十三條之一出售、非法提供公民个人信息罪和非法获取公民个人信息罪，首次将公民个人信息独立为刑法所保护的對象。在本次新增中，将出售、非法提供的主体限定为“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员”。此次增设的主要依据在于

国家机关以及相关单位通过掌管相关事务、经营垄断性业务掌握了大量公民的个人信息，因此针对这些特殊主体作出了刑法规制。但是在 Web2.0 时代，网民在各种网站搭建的平台上互动交流的同时，必然会留下一些仅为网站提供者、管理者所知晓的个人信息。同时，不满足特殊主体要件的普通公民也存在窃取或以其他方式非法获取上述个人信息的可能性。因此，刑法修正案(九)删除了特殊主体要件，这也为 Web2.0 的发展中可能面临公民个人信息受侵害的风险提供了刑法保护。

(二) Web3.0 时代

随着技术的进一步发展，互联网世界迎来了 Web3.0 时代。在 Web3.0 时代中，最直观的进步就是上网不再仅依赖于固定设备，而是出现并普及了移动终端，包括智能手机、平板电脑、笔记本电脑等。当我们有了移动终端的时候，就全面步入了万物互联时代^[2]。截至 2022 年 6 月，我国网民规模为 10.51 亿，互联网普及率达 74.4%。我国网民规模较 2021 年 12 月新增网民 1919 万，互联网普及率较 2021 年 12 月提升 1.4%；农村地区互联网普及率也进一步提高，达 58.8%；网民用于上网的工具按照使用频率分别为手机、台式电脑、笔记本电脑、电视和平板¹。上述数据表明 Web3.0 的网民相比前两个时代更多、人员组成更为复杂、上网方式更为多变。

Web3.0 的关键词本文认为是融合、一体化(integration)。截至 2022 年 6 月，我国短视频用户规模达 9.62 亿、即时通信用户规模达 10.27 亿、网络新闻用户规模达 7.88 亿、网络直播用户规模达 7.16 亿、在线医疗用户规模达 3 亿，较 2021 年的数据都有不同程度的增长(见 p. 3164 脚注 1)。上述数据表明 Web3.0 在 Web2.0 时代的互动性的特征下延伸出一个包含日常生活衣食住行的网络社会。简单来说，Web2.0 侧重日常生活之外的“娱乐消遣”互动，而 Web3.0 则是将许多传统线下的活动开辟了线上模式，除了满足人们的娱乐需求，已然还能满足大部分生活需求。

一方面，Web3.0 的发展给人们的生活带来了前所未有的便利，足不出户也能进行日常生活，另一方面，由于人们利用网络实现日常生活的频率很高，不免会在各个地方留下个人信息。Web3.0 时代作为 Web2.0 时代的迭代更新，也存在 Web2.0 时代侵犯个人信息犯罪的特征——犯罪主体组成复杂、犯罪行为方式丰富。同时也存在一些新的特征：首先是技术上的先进性，Web3.0 时代的侵犯个人信息犯罪以大数据和人工智能为犯罪的技术支撑；其次是犯罪对象的复杂性，Web3.0 时代的个人信息的内涵与外延需要进一步进行明确；最后是侵犯公民个人信息罪的法益的争议性更大，虽然侵犯公民个人信息罪的法益之争自此罪单独分立出来之后就一直存在，但是 Web3.0 时代有一个包含日常生活的延伸空间，在这个新背景下，侵犯公民个人信息罪的法益的研究有新的意义。

3. Web3.0 时代个人信息的内涵和外延

个人信息作为侵犯公民个人信息罪这一罪名的核心概念，明确个人信息的内涵和外延，是适用该罪的先决基础条件。

信息一词在我国历史上已存在了上千年，尽管历史悠久，但由于技术和社会的不断发展，至今信息仍没有一个具体明确的定义。按照语义解释，“信息”有如下三个含义：1) 音信；2) 信息论中指用符号传送的报道，报道的内容是接收符号者预先不知道的；3) 通信系统传输和处理的对象，泛指消息和信号的具体内容和意义。从语义的角度来说，“信息”的内涵应当是某件事物向外界发出的数据、符号等媒介上所包含的内容，人们可以通过对这些内容的获取而识别不同的事物^[3]。因此，个人信息的含义就是能够识别出的特定公民的外界的数据、符号等媒介上的内容。可识别性是从语义角度分析个人信息的关键词。

由于侵犯公民个人信息罪的刑法条文中两处表述有“违反国家有关规定”，因此在探讨个人信息的

¹ 参见中国互联网络信息中心(CNNIC)发布的第 50 次《中国互联网络发展状况统计报告》。

具体含义的时候也需要将视野投入到其他部门法的视角。关于公民个人信息的具体内涵,在其他部门法中有一些不同的判断标准:《中华人民共和国民法典》(以下简称《民法典》)中将隐私权与个人信息保护合并为一个章节,对个人信息定义为“是以电子或者其他方式记录的能够单独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的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等”,不同于英美法系侧重从隐私的角度来定义个人信息[4],我国民法典沿袭了大陆法系的规定,侧重于从可识别性这一特征来划定个人信息的范围——无论是从“识别”这一词语还是从这一章将隐私权和个人信息保护分立开的规定都可以看出。2021年11月1日生效的《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》)中则将个人信息定义为“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,不包括匿名处理后的信息”。略微区别于《民法典》突出可识别性标准,《个人信息保护法》还加上了关联性标准,这实际上扩大了个人信息的范围,将那些虽然不能直接识别但是经过技术处理与个人能产生关联的信息也纳入保护范围。本文认为加上关联性这一标准是对《民法典》只强调可识别性的优化与改进,因为随着时代的发展,对于一些虽然不可识别但是经过特殊处理与公民有密切关联的信息,如果单独适用可识别性标准,是不会被认定为公民个人信息的,这样会不利于保护公民的合法权益。

我国刑法对于公民个人信息的内涵和外延还没有作出明确界定,但是在最高人民法院、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》(以下简称《解释》)中指出刑法第二百五十三条之一规定的“公民个人信息”是指“以电子或者以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,包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等”。与前两部法律中的定义进行比较分析,可以发现《解释》侧重于可识别性标准,即只有能够直接或者间接识别身份或者反映活动情况的才属于刑法所保护的个人信息。《解释》中的这一条款很有可能是出于谦抑性原则的考量。如前所述,对于某些不能识别但是经过特殊技术处理与公民存在密切关联的信息,如果不将其认定为公民个人信息,是不利于保护公民的合法权益的。但是这并不表示要将这种关联信息纳入刑法规制的范围,不仅因为刑法谦抑性的要求,还因为如果在现阶段将关联信息纳入刑法规制的范围会出现许多的问题。首当其冲的就是何为“关联”,将在现阶段尚未得到明确解释的“关联”这一指向模糊的词语适用于刑法条文会导致法官自由裁量权的滥用。在 Web3.0 时代,衣食住行、工作、就医都开辟了线上通道,随着网络社会空间的出现,生活变得越来越便利的同时,个人信息也不可避免地被大量需要,如果关联一词定义不明,不仅会阻碍技术的进步和发展,也会给人们的生活带来极大的不便。上述的可识别性在司法实践中应当按照社会一般人的标准来进行判断,因为随着时代和技术的发展,可能对于一些碎片化无法识别的信息,如果在数量足够多的情况下,的确能识别出特定的公民身份,但是如果按照木桶短板效应中的最短板即只要有人能够通过技术汇聚足够多条信息来对收集、使用公民个人信息的行为进行规制,无疑是因噎废食,不仅对于相关技术人员和单位需要投入的成本过高,同时也不利于信息的合理收集和利用来为用户提供更好的使用体验。由于《民法典》和《个人信息保护法》规定的差异,本文认为对于那些经过技术处理与公民有密切关联的信息是否构成民事违法行为可能尚有争论,但是不适合纳入刑法规制的范围。

通过上述对个人信息的内涵和外延的比较分析,对于在 Web3.0 时代常见的浏览记录等是否属于个人信息或者分析公民的浏览习惯和喜好进而精准投送公民可能喜欢的内容是否属于侵犯个人信息的行为等问题不难回答:从《解释》的“可识别性”标准而言,这些反映了网民的浏览习惯和喜好的信息在社会一般人看来是不能识别出特定公民身份的,故而不属于个人信息;从《个人信息保护法》中个人信息的

定义条款来说,明确排除了“匿名化处理后的信息”,上述信息属于匿名化处理后的信息,因此不属于公民个人信息。因此从这两方面都能得出确定的结论,即这些浏览记录不属于侵犯公民个人信息罪中的个人信息,因而不构成侵犯公民个人信息罪。

4. Web3.0 时代侵犯公民个人信息罪的法益明晰

明晰侵犯公民个人信息罪的法益,有利于划定合理的犯罪圈,一方面可以限制法官恣意行使自由裁量权,另一方面可以让普通民众了解罪与非罪之间的界限,在保护公民个人信息的同时推进科技进步,做到双赢。对于侵犯公民个人信息罪,在刑法理论界,对于侵犯个人信息犯罪存在一些争议,主要有以下两种法益观:

(一) 个人法益说

1) 隐私权说:持此观点的学者认为,刑法修正案(七)中,立法者将新增的侵犯个人信息行为置于《刑法》第二百五十三条之后表明了立法价值取向是保护公民的隐私权。这种观点认为只有体现了隐私权的那部分个人信息才是刑法所保障的公民个人信息[5]。这一观点可能存在的问题在于在《民法典》中已明确将隐私权和个人信息保护分开了,且《民法典》中有条款表明“个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定”,这说明个人信息包含私密信息和非私密信息,因此将个人信息保护等于隐私权保护不利于保护公民的个人信息。隐私信息侧重于公民不愿为人知晓的私密信息,以 Web3.0 从手机解锁到手机支付等普遍会用到的人脸识别为例,人脸信息是客观存在并暴露在外,很难说属于隐私信息,但是按照前述社会一般人可识别性的标准,显然是属于个人信息的,如果将侵犯公民个人信息罪限定为体现隐私权的那部分信息,不利于保护公民的个人信息。

2) 人格权说:持此观点的学者认为侵犯公民个人信息罪所保护的法益是人格权,具体包含人格尊严和个人自由[6]。这个结论的得出是结合了刑法分则的体系条文排列和比较分析了国际社会个人数据保护的基本规律,认为我国对个人数据的保护也应当建立在宪法所保护的公民基本权利之上。对于这个观点,本文认为刑法第二百五十三条“侵犯通信自由罪”所保护的法益是公民的通信自由和通信秘密,的确属于人格权利的保护范围之内,但是首先规定在某一条款之后是否一定能说明两个罪的保护法益类似?例如分则第二百二十四条合同诈骗罪和第二百二十四条之一组织、领导传销活动罪,两者的保护法益虽然都属于市场秩序这个大类,但是保护的法益实际是有差别的;其次就是如果将侵犯公民个人信息罪保护的法益认定为是人格权利,由于隐私权属于人格权利,仍然存在会不当缩小犯罪圈的问题[7]。

3) 个人信息自决权说:这也是我国刑法学界的主流观点。个人信息自决权的核心内容是公民个人有权决定其个人信息是否公开、何时公开、对谁公开、怎么公开以及公开到何种程度。在民法领域,有学者对个人信息自决权作了更加深入的阐释,认为“个人信息权的内涵是自然人对于自己的个人信息,自我占有、自我控制、自我支配,他人不得非法干涉和非法侵害。因而个人信息权是排他的自我决定权,是绝对权”[8]。个人信息自决权这个概念起源于德国,侧重于强调个人信息作为一种排他的绝对权,其获取和使用应当以所有者的同意为前提。这种观点认为,如果所有接触到个人信息的平台和个人都能在未经用户同意的情况下随意自由收集和处理公民个人信息,那么在当今个人信息使用频率过高的时代公民的隐私将无处遁形。在 Web3.0 时代,如前所述,几乎在各个领域到开辟了线上模式,如果将侵犯公民个人信息罪的法益定位为个人信息自决权,的确能加强对公民个人信息的保护。但是,该种学说由于将个人信息权定义为一种私有的绝对权,赋予了公民对个人信息的过大控制权,也存在一定的弊端,仍然不是一种最完美的法益观。首先,在 Web3.0 时代,每个网民每天会使用数个手机软件,几乎所有软件在注册之初会有一行小字在页面中:是否同意用户协议及隐私政策并完成注册?对此,武汉大学网络治理研究院副院长袁康所在的联合调研组于 2021 年对 1036 人进行调查访谈的结果显示,77.8%的用户在安装

手机软件时“很少或从未”阅读过隐私协议，69.69%的用户会忽略手机软件隐私协议的更新提示²。一方面，有记者对手机应用市场里下载量过亿次的社交、游戏、短视频、购物等软件选择了5款进行查看，发现平均每款App需要用户“阅读并同意”的内容约2.7万字，如此长篇大论的文字已经远远超出普通民众耐心阅读的字数区间，普通民众难以阅读完这些眼花缭乱的专有名词，就算阅读完毕，也很难在阅读完的一种疲累的状态下做出最佳选择。另一方面，虽然《个人信息保护法》第十六条明确规定“个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外”，但是何种个人信息属于提供产品或者服务所必需的信息是由信息平台提供者自行决定的，因此这个条款对于公民来说其实是没有办法拒绝的，同意的所谓隐私协议也更像是一份放弃个人信息自决权的声明。如果将侵犯公民个人信息的法益定位为个人信息自决权，可能会导致信息平台 and 软件开发者投入大量心血到隐私和信息条款的制定，这从长远来看不利于保护个人信息[9]。

(二) 超个人法益说

持此观点的学者认为，侵犯公民个人信息罪的法益并非公民的人身权益，而是社会的公共信息安全。个人信息的法律保护体系应当遵循先民后刑的原则，即对侵犯个人信息的行为，区分有无对社会造成较大危害来选择是适用民事制裁手段还是刑事制裁手段。

但是如果将本罪的法益定义为公共信息安全会存在一些问题。首先，如此定义不符合分则的体系结构排列。公共信息安全应当归属于公共安全，因此应当属于分则的第二章，而立法者将其放置于分则第四章侵犯公民人身权利、民主权利的部分，显然与超个人法益说的体系相悖。其次，按照超个人法益说，如果没有对社会造成较大的危害，就不构成侵犯公民个人信息罪，这与《解释》第五条第二款第四项存在矛盾，该项规定“造成被害人死亡、重伤、精神失常或者被绑架等严重后果的”属于“情节特别严重”的情形，但是这种特别严重的情形并不属于公共安全的范畴，如果坚持超个人法益说，那么此类情形会由于没有对社会造成较大危害而出罪，显然不合理。

(二) 个人信息受保护权

如前所述，虽然个人法益说存在许多的问题，但是对比超个人法益说，本文更倾向于认为侵犯公民个人信息罪的法益定位为个人法益是更合适的。首先，本罪属于分则第四章侵犯公民人身权利、民主权利之下，且结合《解释》中情节严重和情节特别严重的一些表述，将本罪的法益定位为个人法益是更符合立法者本意的；其次，如果将本罪的法益定位为公共安全，会导致犯罪圈的不当缩小，导致没有危害公共安全但是对个人法益造成严重损害的情形不当被认定为犯罪。

本文认为可以借鉴《欧盟基本权利宪章》和《欧盟运作条约》中的个人数据受保护权为本罪的法益。

《欧盟基本权利宪章》和《欧盟运作条约》中的基本权利在欧盟法律体系中的地位相当于我国中宪法规定的基本权利[10]。个人信息受保护权是在批判个人信息自决权之后成为欧盟立法的选择的。相较于信息自决权，个人信息受保护权一词摒弃了个人独占、控制信息的倾向，不以个人信息本身为对象，而是指向个人在信息处理过程中应当获得的保护。具体如何获得保护，则取决于国家履行对该项基本权利的保护义务[11]。此外，希腊、墨西哥、阿尔及利亚都将个人信息保护权明文规定为宪法权利³。

Web3.0时代，在现实世界延伸出来的网络空间里，充斥着大量的个人信息，这些个人信息不可避免地具有流动性、公共性，个人信息自由流动尽管应当受到一定的限制，但是由于其流动运转具有巨大的

² 参见人民网：《我已阅读并同意”？你没读过的App用户协议有哪些“坑”？》，<http://finance.people.com.cn/n1/2022/0315/c1004-32375044.html>。

³ 《希腊宪法》第9条规定：“任何人就其个人信息的收集、处理和使用，尤其是通过电子手段为之的，受到法律保护”；《墨西哥宪法》第16条规定：“所有人都享有个人信息受保护以及访问、更正和删除此类信息的权利。”《阿尔及利亚宪法》第46条规定：“所有人在其个人信息被处理时受到保护是法律保障的一项基本权利。”

社会价值,因此无法也没有必要让公民本人掌握个人信息的绝对排除权利。因此,Web3.0时代关于侵犯公民个人信息罪的法益相关的最重要的问题其实是如何平衡公民个人信息保护以及信息保护自由流转所带来的巨大社会利益。解决这一问题的路径设想就是把公民对个人信息的自决权转移为国家有关机关的保护权。根据《个人信息保护法》第六章的规定,国家网信部门和县级以上地方人民政府相关部门均具有个人信息保护和监督管理职责。因此,在司法实践中,大部分情况下可以推定某一行为在履行个人信息保护职责的部门的监管下是不构成犯罪的,这样有利于发挥Web3.0时代下个人信息在正常社会和商业流转中的巨大价值,同时由于为公民本人提供了更优质的服务也不会违背公民本身的意愿;但是如果某一行为逃避国家监管部门的监管,经国家监管部门的判断会侵犯公民个人信息保护权的,应当被认定为构成侵犯公民个人信息罪;如果某一信息属于《个人信息保护法》第二十八条规定的敏感信息⁴,相关部门如果在具有特定的目的和充分的必要性的前提下确要使用,不仅要在国家有关部门的监管下采取严格的保护措施,还应当按照第二十九条的规定,应当取得个人的单独同意;若有特殊规定还应当取得书面同意;最后,如果履行个人信息保护职责的部门玩忽职守或者滥用职权,不履行或者未能适当履行监管职责,按照刑法分则的有关规定定罪处罚。

个人信息保护权说一方面可以尽量清楚明确本罪的犯罪圈。将判断标准交给国家有关部门进行判断,既专业又足以使得民众信服;另一方面,还能平衡个人信息保护与信息保护自由流转所带来的巨大社会利益。

5. 结语

Web3.0时代,由于兼具1.0和2.0时代特征以及同时呈现出的融合性特征,使得公民个人信息在延伸的网络社会空间大量充斥并进行流转。Web3.0时代下的侵犯个人信息犯罪,基础核心概念还是个人信息的内涵与外延。对此,要遵循社会一般人的可识别性标准,只有社会一般人能够识别出特定公民的个人信息才是刑法所保护的个人信息。明确了个人信息的含义,在侵犯公民个人信息犯罪的研究中第二个比较重要的问题就是本罪保护的法益。学界的通说个人信息自决权说不宜成为本罪的法益,目前来说,公民的自决权利有名无实,并且赋予公民这项权利虽然短期看有利于保护公民的个人信息,但是长远来看既阻碍了科技的发展,又不利于保护公民的个人信息。借鉴欧盟的立法将个人信息保护权作为本罪的法益不失为一种合适的解决路径,将公民的自决权交由国家代为行使,对于国家有关机关来说,既是权利,又是义务。

参考文献

- [1] 刘琼,任树怀.论Web3.0下的信息共享空间[J].图书馆,2011(2):83.
- [2] 刘艳红.Web3.0时代网络犯罪的代际特征及刑法应对[J].环球法律评论,2020,42(5):104.
- [3] 李裕川.数据化时代侵犯公民个人信息罪法益的重新厘定[D]:[硕士学位论文].长春:吉林大学法学院,2022:9.
- [4] 蔡金燕.论侵犯公民个人信息罪之“公民个人信息”[D]:[硕士学位论文].杭州:浙江大学光华法学院,2018:7.
- [5] 蔡军.侵犯个人信息犯罪立法的理性分析——兼论对该罪立法的反思与展望[J].现代法学,2010,32(4):108.
- [6] 高富平,王文祥.出售或提供公民个人信息入罪的边界——以侵犯公民个人信息罪所保护的法益为视角[J].政治与法,2017(2):48-49.
- [7] 皮勇,王肃之.大数据环境下侵犯个人信息犯罪的法益和危害行为问题[J].海南大学学报(人文社会科学版),2017,35(5):116-117.
- [8] 杨立新.个人信息:法益抑或民事权利——对《民法总则》第111条规定的“个人信息”之解读[J].法学论坛,2018,

⁴《个人信息保护法》第二十八条:敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。

33(1): 41.

- [9] 欧阳本祺. 侵犯公民个人信息罪的法益重构: 从私法权利回归公法权利[J]. 比较法研究, 2021(3): 59.
- [10] 蔡培如. 欧盟法上的个人数据受保护权研究——兼议对我国个人信息权利构建的启示[J]. 法学家, 2021(5): 17.
- [11] 王锡锌. 个人信息国家保护义务及展开[J]. 中国法学, 2021(1): 150-153.