

网络空间个人信息安全刑法研究

吴雯婧

华东政法大学刑事法学院, 上海

收稿日期: 2023年4月6日; 录用日期: 2023年5月19日; 发布日期: 2023年5月26日

摘要

在大数据背景下侵犯公民个人信息的案件不断增加, 侵害方式呈现出多元化趋势, 在网络空间下公民个人信息的刑法保护更加刻不容缓。本文结合目前网络空间现状, 分析个人信息的法益与保护的不足之处, “经被收集者知情同意”条款的滥用侵害信息自决权, 缺失明确的个人信息法益定位。对此需要不断规范和完善公民个人信息的刑法保护体系, 不仅是维护公民的个人信息权利和社会公共秩序的需要, 也是对信息产业发展的指引与促进。

关键词

网络空间, 个人信息, 法益, 非法使用行为

Research on Criminal Law Protection of Personal Information Security in Cyberspace

Wenjing Wu

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

Received: Apr. 6th, 2023; accepted: May 19th, 2023; published: May 26th, 2023

Abstract

The cases of infringement on personal information of citizens are increasing in the background of big data, and the ways of infringement are becoming more and more diversified, so the criminal law protection of personal information of citizens in cyberspace is becoming more urgent. Using the method of literature analysis, combined with the present situation of cyberspace, the article analyzes the legal interests of personal information and the inadequacies of its protection, and the abuse of the clause of “Informed consent of the person being collected” infringes the right of self-determination of information, lack of clear legal positioning of personal information. To standardize and perfect the criminal law protection system of citizens' personal information is not on-

ly the need to safeguard citizens' personal information rights and social public order, but also the guidance and promotion to the development of information industry.

Keywords

Cyberspace, Personal Information, Legal Interest, Illegal Use

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

随着信息网络技术的迅速发展,各种手机应用、社交媒体和电子商务平台已成为日常生活中必不可少的一部分。从衣食住行到社交娱乐,成千上万的数据不断涌现,5G网络的进步,带来的不仅仅是更加便捷高节奏的生活方式,还有持续上升的个人信息被非法侵害的安全风险。2022年7月21日,滴滴全球股份有限公司因为违法收集、过度使用司机和用户信息等行为,违反《网络安全法》《数据安全法》《个人信息保护法》,被罚款80.26亿,再一次敲响了个人信息刑法保护的警钟。

2022年公布的《中国网民权益保护调查报告》揭示了大数据时代下公民的个人信息权益更容易遭到侵害:恶意软件、骚扰电话和网络弹窗层出不穷、信息知情选择权的丧失、个人真实信息遭非法泄露,被不法分子冒充银行、公安机关诈骗也时常发生。基于刑法的惩罚与教育功能,在大数据时代不断进步发展的今天,为了保障个人信息的安全性和流通性,完善个人信息刑法保护十分迫切。

2. 个人信息范围的立法演变

公民个人信息是指有关公民个人身份的信息,往往能直接或间接与公民的衣食住行、医疗教育、社交娱乐等各方面关联。因此在大数据时代,如何定义“个人信息”的范围和其保护权益具有极其重要的价值。

目前,我国对公民个人信息的刑法保护范围已经比较完备,其法律理念不断拓展,扩大了对个人信息的刑法保护范围。从2005年附属于金融管理秩序规定的从个人信用卡信息到个人信息的综合保护,这单是我国立法层面的进步,也是网络信息技术进步后的必然发展。

2.1. 个人信息范围的雏形

传统刑法对个人信息的保护缺乏精确的保护范围,而是将个人信息附属于刑法保护的其他合法权益之上,如2005年《刑法修正案(五)》增设的附属于金融秩序管理的窃取、收买、非法提供信用卡信息罪,该罪名从形式上来看存在对信用卡个人信息的刑法保护,但实质上其位于破坏金融管理秩序罪,立法宗旨是为了维护金融管理秩序。到2009年《刑法修正案(七)》新增了出售、非法提供公民个人信息罪和非法获取公民个人信息。虽然明确了对个人信息的刑法保护,但此时主体限定为特定行业的工作人员,并未明确个人信息范围,而是依附于公务、公共职能^[1]。

一直到2011年《信息系统安全解释》第11条规定身份认证信息为:“用于确认用户在计算机信息系统上操作权限的数据。”此时对于个人信息的范围虽然局限于计算机信息系统领域的的数据,但确实是纳入刑法保护的个人信息搭建了一个框架雏形。

2.2. 个人信息范围的明确

2012年全国人大常委会通过了我国第一部关于网络信息保护的专门性立法,即《关于加强网络信息保护的決定》,其第1条规定了个人信息范围涵盖识别个人身份和涉及个人隐私的电子信息。2013年最高人民法院、最高人民检察院、公安部制定了《关于依法惩处侵害公民个人信息犯罪活动的通知》,在之前的基础上对个人信息范围进行了列举和进一步的明确,范围从电子信息扩展到了比电子信息范围更广的数据资料。这两个文件表现出在这一阶段,个人信息范围的涵盖标准为“身份识别性”和“个人隐私性”。

2.3. 个人信息范围的扩张

2016年全国人大常委会通过了《网络安全法》,其第76条第5项规定了个人信息范围变为了可识别自然人个人身份的各种信息,此时还包括了记录方式为电子记录或其他方式记录,识别类型为单独识别或与其他信息结合。总体来说此时个人信息范围的核心判断标准变成了“可识别性”,与之前的规定相比,删除了个人隐私。这是由于立法者对于个人隐私与个人信息的关系有了新的认识,认为两者之间存在重叠但不重合的关系,公民的个人隐私包括了隐私信息、隐私活动等。而公民个人隐私信息与个人信息可能重叠,但是其他隐私内容可能并不属于个人信息的范围。

2.4. 个人信息范围的归纳

2017年6月1日起实施的《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》基本延续了《网络安全法》个人信息范围的有关规定,但是在列举时增加了财产状况、行踪轨迹的内容,并在《民法典》第1034条继续沿用,将行动轨迹、财产状况、账号密码等本身虽不具有身份的可识别性,但可能影响人身和财产安全的具有活动反应性的个人信息纳入了保护范围。因此,学界展开了关于“行动轨迹能否纳入可识别的个人信息”的理论争议。

而至目前的《个人信息法》规定了“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,不包括匿名化处理后的信息。”这一范围只强调了个人识别性,没有再将活动反应性列举出来。这种改变意味着学界关于“行动轨迹不能纳入可识别的个人信息”的观点获得了一定认可,由于行动轨迹并不必然可以联系自然人的身份信息,若为了应对大数据时代风险,与其将行动轨迹纳入个人信息范畴,不如将行动轨迹与个人信息同等并列保护。

3. 个人信息的法益属性

在大数据时代,侵害个人信息犯罪的受害主体从过去的个体逐渐群体化,这决定了侵犯个人信息犯罪所需要保护的法益应当从个人法益逐步转向为个人法益和公共法益并存。但在立法中存在保护法益定位含糊不明的问题,因此需明确个人信息权益的法益属性,来完善后续立法[2]。

3.1. 个人法益属性

个人法益属性是人格法益和财产法益的集合。一方面,个人信息有其人格权属性,个人信息内容往往涉及公民个体的人格尊严和人格自由,同时其可识别性又导致公民与其个人信息紧密相连,这体现了公民的人格特征[3]。

另一方面,随着财产概念的不断扩大,虚拟财产、财产性利益都被包括其中,无论是网络社会的数据财产还是蓬勃发展的数字经济都逐渐被囊括在了财产概念之中,因此,个人信息开始被占有和分析,当信息处理者需要占有大量个人信息时,出于合法利用的需要,应当赋予相应的信息财产权。同时,这也为公民在虚拟财产被侵占,个人信息被违法利用开发之时,提供了其维护自身权益的法律依据。

3.2. 公共法益属性

公共法益属性既包括了社会法益，也包括了国家法益。在大数据时代，无论个人、企业、社会还是国家都有可能成为个人信息侵害的施暴者和受害者，个人信息犯罪侵犯的也不仅仅是公民的人身权利和个人权利，还关乎了社会秩序与国家安全。信息主体与范围的不断扩大，这些反映了刑法所保护的个人信息需涵盖公共法益。从信息法益平衡的需要来看，大数据时代下个人信息的使用与流通不可避免，过于突出信息的个人法益，一味地强调对信息的保护而阻止信息的流动，不仅不利于目前数据经济发展，同时对于现代公民而言，信息流通对于他们的工作、学习与社交都有重要价值，出于兼顾信息安全与流动的需要，一个稳定安全的信息管理秩序将成为法治社会的重要组成部分。

因此，无论是个人法益说还是公共法益说都仅仅是从时代趋势上提取信息所附着的法益类型，而这些法益是否都值得刑法保护，是否符合刑法的谦抑性和其他原则标准，还有待筛选和考量。

同时，在大数据时代，可以被了解的个人信息不断增多，信息产业为了获得更多经济利益，往往对数据在合法获取的前提下过度分析。这导致个人信息的可识别性增加，每个人在大数据面前都将无处遁形，导致个人信息泄露风险也逐渐上升，不仅存在通过正当合法途径搜集获得，也存在通过不当违法途径如窃取、或是购买取得；既可能是本人主动提供，也可能是社交网络上的无心泄漏。因此，在大数据背景下个人信息的刑法保护存在许多不足。

4. 个人信息刑法规范与互联网产业发展趋势的矛盾

4.1. 个人信息刑法规范与信息产业发展趋势的矛盾

1) 滥用“经被收集者知情同意”条款

“知情同意”，指收集利用公民个人信息者应当明确告知信息权利主体有关情况并征得同意^[4]。这所带来的关于个人信息的权利保护和价值利用的讨论如硬币的正反两面，既互相对立，又统一于权利与义务的利益衡量之中。

首先，“经被收集者知情同意”条款有其作为出罪事由存在的必要性，它不仅推动了信息产业与网络时代的发展，同时也平衡了个人、互联网企业与国家之间的利益。之所以“知情同意”条款可作为出罪事由，是因为法律不可能单单强调对个人信息的严格保护，而是在信息权利主体与收集使用信息的网络服务提供者之间合理分配权利与义务，在法律框架内实现个人信息价值的有效利用，从而达成信息权利主体、网络服务提供者和国家之间的利益平衡^[5]。

其次，“经被收集者知情同意”条款的滥用，导致核心地位的信息决定权逐步丧失。这不仅是因为公民法律意识淡薄，也存在网络服务提供者的刻意引导。一方面，长篇累牍的专业化使用协议，使得大部分公民怠于了解自己的个人信息将会被如何搜集与使用；另一方面，如果公民不同意使用协议，往往无法正常使用对应的网络服务，如各类导航和外卖软件。

最后，随着近年过度收集使用用户个人信息的 APP，如“猎头搜”“今日头条”“天翼征信”引发的不正当竞争、隐私权、名誉权等民事纠纷案件的经常性发生，再加上被泄漏和滥用的个人信息逐步成为欺诈、敲诈勒索等犯罪行为的来源和逃避法律制裁的工具，“经被收集者知情同意”条款的滥用不仅使公民难以产生安全感与信任感，也将不利于功能各异的网络服务平台的长久发展。

同时，随着大数据时代信息技术的发展，个人信息逐渐变成了一种商业资源，被过度分析，进行买卖。此时，被侵害客体的范围不断被扩大，如 Facebook 支付 6.5 亿美元的赔偿金，与 160 万名诉讼成员为人脸识别侵权集体诉讼达成和解。当被侵害客体涉及到 160 万公民，这早已不单单是对公民个人法益的侵害，而是一种对社会利益的侵害。

2) 个人信息保护法益定位不准确

《刑法》第 253 条的“侵犯公民个人信息罪”，是目前我国侵犯公民个人信息的主要刑法规制，位于分则第四章“侵犯公民人身权利和民主权利”，如果将该条文放在整个法律体系中来解释，可以理解为该罪名的主要客体定位于公民个人的人身自由权益。学界因此有将该罪视为仅对公民个人法益的侵害，而没有包括公共秩序或者社会利益。然而，诸多案例表明，该罪不仅侵犯了公民的个人法益，也对社会公共法益、甚至是国家法益存在着威胁。这种观点存在不足，侵犯公民个人信息罪虽然属于公民人身权利犯罪，但这只能说明被侵犯的主要客体是公民个人利益，而非只侵犯了公民个人利益，在司法实践中个案所侵犯的直接客体有可能多样化，因而并不能否认个人信息保护法益具有社会公共法益属性。

在司法实践中，个人信息保护法益突破公民个人利益的情况并不罕见。在抗击疫情期间，网络空间存在大量泄漏新冠肺炎患者个人信息的案例，确诊患者、疑似患者或密切接触者本人乃至其家庭成员的个人隐私被曝光，遭到了网民们的“人肉搜索”，如 2020 年 12 月确诊的成都女孩赵某，因为她的行动轨迹涉及多家酒吧，其个人隐私在多个社交平台被转发，有好事者甚至拨打其电话进行辱骂侮辱。这些案例在疫情期间频繁发生，所侵害的早已不单单是被侵害公民的个人法益，也包括了社会公共秩序法益，个人信息保护的公共安全与个人利益之间的矛盾冲突问题被不断放大。

4.2. 非法使用公民个人信息行为尚未纳入刑法保护

侵犯公民个人信息罪包含三种行为方式，即非法获取、非法出售和非法提供，但不论如何对这三种行为进行理解，大数据时代开始泛滥的恶意篡改毁损、冒用身份、非法加工、过失泄露等行为无法囊括其中^[6]。毫无疑问，并非所有未被侵害公民个人信息罪规定的行为方式都尚未纳入刑法保护，其中部分行为可以被主行为吸收，如盗窃罪，或是有妨害信用卡管理罪、信用卡诈骗罪、合同诈骗罪、使用虚假身份证件、盗用身份证件罪等专门罪名，但非法使用行为入罪存在其合理必然之处。

1) 增加个人信息犯罪行为方式的合理性

一方面，在多个前置性法律中，对于个人信息应当受到保护的行为类型，即《网络安全法》第 41 条、《民法典》第 1035 条、《个人信息保护法(草案)》第 4 条、《消费者权益保护法》第 29 条及《电信和互联网用户个人信息保护规定》第 9 条等都有提及“使用”这一行为。

另一方面，非法使用行为具有严重的法益侵害性。与目前法定的三种行为方式相比，由于公民个人信息的可识别性特征，非法使用行为能够更加直接精确地侵害到公民的个人信息。随着大数据时代信息泄露风险的增加，信息主体与被使用信息也更容易被一一对应，因此一旦信息被投入不法用途，即使不法分子能够被绳之以法，也难以立刻消除其带来的负面影响，无论是公民的名誉受到损害，亦或是信用利益受到侵害，都将影响到公民日常生活。

2) 增加个人信息犯罪行为方式的必要性

最根本的原因是除去上文提及的四个刑法中涉及到非法使用公民个人信息的主要罪名之外，仍存在大量目前刑法规定无法囊括的非法使用公民个人信息行为。

首先，存在没有合适罪名定罪的情况，现实中存在大量“合法获取，非法使用”行为。通过滥用“知情同意条款”收集到的信息，进行如广告轰炸等非法使用行为，造成严重后果时，既难以认定为非法获取，也无合适罪名^[7]。

其次，没有合适罪名将难以为公民提供有理有据的法律支持，当公民面临“轻微侵害个人信息的刑事案件”时，将处于难以找到法条支持的境地。在大数据背景下，个人信息被获取后被非法使用，如注册空壳公司，注册电话卡等类似行为日益增多。一方面公民本人难以发现自己的个人信息被非法使用，

发现了也难以靠刑事自诉获得救济，另一方面非法使用个人信息进行诈骗，利用他人个人信息往往被视为一个手段行为，但在实际情况下，没有利用他人个人信息注册公司仍然可以使诈骗行为顺利进行，与其说这两个行为之间存在牵连关系，不如说这是为了逃避法律制裁的一个单独行为。此时，若司法机关只是对最终犯罪结果予以定罪，而忽视信息主体的权利，即使行为人受到法律制裁，受保护的是宏观经济秩序和社会秩序，而信息主体的名誉和人格利益却没有得到保护。

5. 网络空间侵害个人信息的刑法保护对策

5.1. 完善个人信息刑法保护的导向

公民个人信息的法益属性体现了完善个人信息刑法保护导向应当综合考虑个人法益与公共法益。将对公民个人信息的保护转变为不仅要能够平衡公民个人的信息自决权和“知情同意”条款之间的关系，[8]在完善个人信息刑法保护的基础上，促进信息产业的进一步发展，还要明确刑法保护的个人信息法益，保障刑法的惩罚和教育功能[9]。

第一，平衡“知情同意”与信息自决，近年来，出于信息网络发展的需要，越来越多的网络服务提供平台开始作出改变，但是仍然存在一键式授权隐私政策，一揽子协议强迫用户同意的现象，这需要增强有关的国家政策和法律规范的约束，一方面，法律法规和行业规范需要对滥用“知情同意”条款制定合理规范，对“知情同意”条款的告知方式和获取提醒提出明确性和规范性的要求[10]。同时在获取用户同意时，从原来的默认勾选同意条款到要求用户主动做出明确肯定性授权，实现在个人信息保护方面由“推动”到“自发”的转变[11]。另一方面，需要更加明确知情同意原则，在保护公民个人信息的基础上，协调公民个人法益和社会法益，在个人信息的权利主体与使用主体之间取得平衡，使得民法、行政法和刑法在个人信息保护互相衔接协调，在刑法的法益保护功能和人权保障功能的基础上，把持好“最低入罪门槛”[12]。因此，对于规范了知情同意条款的行业规范，比起作为直接判断刑事违法性的根据，更适合作为界定网络服务平台是否侵害个人信息法益的前置性依据，避免造成打击范围过大，阻碍了信息产业的进一步发展。

第二，完善侵犯个人信息犯罪的法益，一方面确定其公共法益，司法实践中的大量案例表明，侵犯个人信息犯罪涉及的信息数量和造成的影响已经不断扩大至在实质上早就超越了“个人法益”的范围，同时侵犯信息犯罪的对象逐渐呈不特定化趋势，可能危害社会公共安全、乃至于是国家安全。但从另一方面说，如果过于强调个人信息的公共利益，将会面临公共利益与个人利益相冲突的情况，因此，需要限制刑法对公共法益保护的力度，当民法、行政法等其他部门法能够通过相关规定予以保护的时候，不必通过刑法予以保护，使得对刑法予以保护的个人信息逐步完善，平衡个人利益与公共利益，以个人法益为基础，以公共法益为补充。

5.2. 增加个人信息犯罪的行为方式

目前，侵犯个人信息犯罪的法定行为只有三种：非法获取、非法出售和非法提供行为，在大数据时代，通过合法采集、购买等方式获取个人信息后进行的诈骗、逃避打击等非法使用个人信息的行为日益增多，这些行为对个人造成损害的严重性不亚于目前三种法定行为方式，但在司法实践中公民个人很难进行维权，维权的成功率极低，因此，需要增加个人信息犯罪的行为方式。

毫无疑问，无论是司法实践中的案例，还是法学理论界的争议，都有承认非法使用个人信息入罪的必然性，不过是否需要增加其他行为方式仍需进一步考虑，如信息篡改、损毁、过失泄露等。近年来这些犯罪行为不断增加，在司法实践往往认定为破坏计算机信息系统罪，但随着公民对个人信息保护意识的增强与国家法律系统的完善，法律中规定侵犯公民信息的方式也势必会制定的更加全面[13]。

6. 结语

在大数据时代背景下,有关人工智能、大数据、信息经济等各种话题越来越受到大众的关注,这既存在着大数据信息带来的无限商机,也面临着公民个人信息被侵害的巨大风险。随着信息技术的不断发展,个人信息所具备的经济价值与社会价值越发凸显,对个人信息的开发和利用也已是社会发展无法避免的趋势。而同时我国目前个人信息刑法保护存在一定的不足,“经被收集者知情同意”条款的滥用侵害信息自决权,缺失明确的个人信息法益定位。

因此,在这个日新月异的时代,对我国公民个人信息进行更全面的保护已经成为我国刑事立法的新挑战和新目标,因此刑事立法和司法都应当具备基于理性思考的前瞻视野^[14],这一方面,需要刑法发挥其惩罚和教育功能,对侵害公民个人信息的犯罪予以适当的刑事处罚,而另一方面,也需要刑法维持其明确性和谦抑性^[15]。大数据时代的到来是当今时代发展不可逆转的趋势,如何正确合理的引导,将成为促进信息产业乃至整个社会发展的重要一环。

参考文献

- [1] 于冲. 侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界[J]. 政治与法律, 2018(4): 15-25.
- [2] 皮勇, 王肃之. 智慧社会环境下个人信息的刑法保护[M]. 北京: 人民出版社, 2018: 69-71.
- [3] 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.
- [4] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
- [5] 方军. 被害人同意: 根据、定位与界限[J]. 当代法学, 2015, 29(5): 41-53.
- [6] 于志刚. “公民个人信息”的权利属性与刑法保护思路[J]. 浙江社会科学, 2017(10): 4-14+155.
- [7] 彭辅顺. 非法使用公民个人信息行为的刑法规制[J]. 中国刑事法杂志, 2023(1): 107-124.
- [8] 万方. 隐私政策中的告知同意原则及其异化[J]. 法律科学(西北政法大学学报), 2019, 37(2): 61-68.
- [9] 敬力嘉. 大数据环境下侵犯公民个人信息罪法益的应然转向[J]. 法学评论, 2018, 36(2): 116-127.
- [10] 张勇. APP 个人信息的刑法保护: 以知情同意为视角[J]. 法学, 2020(8): 113-126.
- [11] 李延舜. 我国移动应用软件隐私政策的合规审查及完善——基于 49 例隐私政策的文本考察[J]. 法商研究, 2019, 36(5): 26-39.
- [12] 田宏杰. 窃取 APP 里个人信息的性质认定——兼及个人信息与个人隐私的界分[J]. 人民检察, 2018(7): 27-31.
- [13] 刘仁文. 论非法使用公民个人信息行为的入罪[J]. 法学论坛, 2019(6): 118-126.
- [14] 王肃之. 从回应式到前瞻式: 网络犯罪刑法立法思路的应然转向——兼评《刑法修正案(九)》相关立法规定[J]. 河北法学, 2016, 34(8): 155-164.
- [15] 高富平. 论个人信息保护的目的一一以个人信息保护法益区分为核心[J]. 法商研究, 2019, 36(1): 93-104.