Doi:10.11835/j.issn.1008-5831.fx.2020.05.002

欢迎按以下格式引用:刘双阳,李川. 大数据时代个人信息法益刑法保护的应然转向——以规制非法使用个人信息为重点[J]. 重庆大学学报(社会科学版),2022(6):231-242. Doi:10.11835/j.issn.1008-5831.fx.2020.05.002.

Citation Format: LIU Shuangyang, LI Chuan. The change of criminal law protection of personal information legal interests in the era of big data: Focus on regulating illegal use of personal information[J]. Journal of Chongqing University (Social Science Edition),2022(6):231-242. Doi:10.11835/ j.issn.1008-5831.fx.2020. 05.002

大数据时代个人信息法益刑法保护的应然转向
——以规制非法使用个人信息为重点

刘双阳[1],李 川[2]

(1.中国政法大学 刑事司法学院,北京 100088;2.东南大学 法学院,江苏 南京 211189)

摘要:我国《刑法》第253条之一侵犯公民个人信息罪规定的行为类型仅限于非法获取、出售或提供个人信息代表的转移行为,没有将非法使用个人信息行为纳入规制范围,造成刑事规制出现漏洞,体现了将个人信息自主片面地理解为转移自主、忽视使用自主的法益认识缺陷,进而仅以防范非法转移个人信息为入罪逻辑,使得个人信息法益刑法保护不周延。当前个人信息已然成为网络犯罪中的关键要素,非法使用个人信息现象愈演愈烈,侵犯公民个人信息犯罪已经逐渐形成"提供者—中间商—非法使用"的完整黑色产业链,各环节分工明确、组织严密,通过非法使用个人信息实施违法犯罪活动,进而变现牟利是诱发个人信息泛在泄露以及违法交易激增的根源,刑法单纯打击制裁非法转移个人信息行为只能是治标之策,导致侵犯个人信息犯罪刑事治理效果欠佳。随着进入大数据深度挖掘应用阶段,数字经济蓬勃发展背景下根植于个人信息的人身性、财产性、公共性等复合法益属性的使用价值日益凸显,使得个人信息使用自主相较于个人信息转移自主更具核心法益地位,个人信息刑法保护的重点理应从转移环节转向使用环节。非法使用个人信息属于下游行为,对公民的人身财产安全以及社会管理秩序造成极大损害或威胁,与处于上游的非法转移个人信息行为相比,非法使用个人信息行为具有更为严重的法益侵害性,表现为法益侵害的根源性、直接性和精准性。因此,刑事立法应以需求端为导向,有必要在遵循刑法谦抑性原则的前提下合理确定非法使用个人信息行为的入罪要件与出罪事由,即以未征得信息

基金项目:国家社会科学基金一般项目"网络智能时代个人信息泛在泄露与刑法有效保护研究"(19BFX076);南京市法学会法学研究课题"《个人信息保护法》视角下侵犯公民个人信息犯罪问题研究"(NJFX2022C02);中国政法大学网络法学研究院2019年度网络法治理论研究项目

作者简介:刘双阳,中国政法大学刑事司法学院,Email:948573989@qq.com;李川,东南大学法学院教授。

主体同意且情节严重为危害行为,以非经匿名化处理的个人信息为行为对象,以符合个人信息合理使用的情形为违法阻却事由,既从源头上规范个人信息使用行为,又限定非法使用个人信息行为刑事入罪的边界,在保护个人信息安全的同时促进个人信息有序自由流动、合理有效利用,平衡信息主体的使用自主利益与信息处理者的正当使用利益,为数字经济高质量发展提供强有力的刑事法治保障。

关键词:个人信息;非法使用;使用自主;法益侵害;入罪要件;出罪事由

中图分类号:D924.3 **文献标志码**:A **文章编号**:1008-5831(2022)06-0231-12

随着奠定数字社会基石的5G移动通信、大数据、物联网、云计算、人工智能等新兴网络信息技术的快速发展,数字化生存已然成为当下最活跃的社会生活方式,像空气和水一样自然,由此开启一个全新的"赋权"时代[1]。从原子到比特的数字化过程意味着利用数据量化一切,记录、分析和重组对客观事物的描述[2],其中能够识别或关联到特定自然人身份或活动情况的数据被称为个人信息,即个人生活在数据空间的镜像。大数据环境下,通过收集处理、深度挖掘记录自然人一言一行的个人信息,可以准确分析并勾勒出其在社会交往过程中形成的以数据为基础的公共形象如生物特征、健康状况、教育背景、经济能力、兴趣喜好等,即创建"数字化人格"[3],并以此作为高效分析社会需求、辅助业务决策的工具。个人信息的应用价值和商业价值使得其在社会治理乃至经济发展中的作用日益凸显,成为一座储藏于网络空间、被竞相开采的"富矿"。然而,法谚有云:"有利益的地方就有犯罪人。"个人信息不可避免地成为网络犯罪觊觎的目标,遭受不法侵害的风险陡然剧增。是故,"我们要坚持以人民安全为宗旨","完善国家安全法治体系"[4]。

一、问题的提出:个人信息使用自主刑法保护阙如

数字经济时代,作为个人信息载体的数据与土地、劳动力、资本、技术等一道被纳入生产要素的范畴,通过深化要素市场化配置,促进数据自主有序流动,提升数据资源的价值①。在此背景下,越来越多的市场主体参与大数据产业,投入巨额人力、物力、财力加工处理和分析应用个人信息,"它们的终点线是让所有收集到的数据产生业务价值,或者说商业利润"[5],个人信息主体成为被观察、分析和监测的对象。此外,网络空间信息流转的迅捷性和不可控性放大了个人信息遭受不法侵害的可能性,使得个人信息面临前所未有的泄漏与滥用风险。例如,为疫情防控、疾病防治而收集使用的密切接触者的姓名、电话、身份证号码、个人详细居住地址等信息在微信群组被不当传播扩散,产生超越时空的不良社会影响。在暴利驱动下,现实中已经形成一条分工明确、精细完整的数据交易黑色产业链[6],个人信息被明码标价,上游"中间商"负责非法获取、出售、提供个人信息,下游需求群体则购买并利用个人信息实施各种违法犯罪活动,诸如使用他人个人信息恶意注册互联网账号"刷单炒信"、冒用个人信息申请信用贷款或逃税、盗用个人信息破解生物识别身份认证系统、滥用个人信息拨打虚假营销类骚扰电话或定向推送有毒有害信息等现象愈演愈烈。以"侵犯公民个人信息罪""刑事案件""一审程序"三个关键词在中国裁判文书网上进行检索发现,2016—2020年侵犯公民个人信息的刑事案件分别为387件、1 323件、2 229件、2 159件、1 910件。当前侵害个人信息犯罪呈高发态势,其中不少案件涉及的个人信息数量惊人、影响范围甚广,引发的盗窃、诈骗等

①2020年4月9日,中共中央、国务院印发的《关于构建更加完善的要素市场化配置体制机制的意见》明确提出"加快培育数据要素市场"。

次生犯罪危害也日益严重。

从数据信息的流动链条和生命周期来看,获取、出售、提供都属于个人信息的转移方式,而转移个人信息的最终目的在于利用,如此才能创造价值或收益。非法使用个人信息牟利无疑是诱发当前个人信息泛在泄露以及违法交易激增的根源,已成为整个侵害个人信息犯罪产业链的核心环节。对个人信息深度挖掘应用所带来的侵害风险要求大数据时代个人信息保护的重点应从转移环节转向使用环节[7]。如何从需求端确保信息处理者遵循合法、正当、必要的原则,合规使用个人信息就显得尤为重要。我国涉及个人信息保护的民法和行政法规范中均有“不得非法收集、使用、出售、提供公民个人信息”的相关规定②,将个人信息的使用行为作为一种独立的行为类型与获取、出售、提供行为并列规定。然而,刑法分则中的侵犯公民个人信息罪却并未将非法使用个人信息行为纳入本罪的构成要件类型,仅仅是按照犯罪行为的自然延伸来解释,使得刑法保护个人信息法益不周延,并与其他部门法规范不协调。出现这一“真空地带”的主要原因在于立法者对侵犯公民个人信息犯罪所保护的法益——个人信息自主的理解不够全面,将保护个人信息自主简单地等同于保护个人信息转移自主,以防范非法转移个人信息为入罪逻辑,一定程度上忽视了对个人信息使用自主的保护。

以信息交换与共享为主要特征的互联网思维已深深嵌入当下社会生活的方方面面,人们在享受网络带来的便捷生活的同时,不得不让渡部分个人信息权益作为获得相关产品和服务的“对价”,“当网络化和数据交换不断扩大时,相应地,信息网络犯罪也侵入到更多区域”[8]。近年来,非法使用个人信息事件频频见诸报端,尤其是个体指向性较强的敏感信息的靶向使用[9],如利用个人身份信息实施精准电信网络诈骗,给公民的人身和财产安全造成严重威胁或损害,引起社会的普遍关注。中国通信研究院发布的《移动互联网应用个人信息安全报告(2019 年)》显示,有关个人信息使用问题的投诉已占网络不良与垃圾信息举报受理中心收到的用户 App 投诉数量的 21%。随着公众个人信息保护意识的觉醒与增强,对不法分子违规使用个人信息侵害用户权益的感受日益强烈,因此,个人信息使用自主作为信息社会产生的新价值形式亟需刑法的保护[10]。但需要格外注意的是,基于刑法保障公民权利自由的最后手段性定位,在通过入罪方式规范互联网经营者的个人信息使用行为时,须秉持刑法谦抑性原则,合理确定非法使用个人信息行为刑事规制的边界,审慎发动刑罚权,使信息主体与信息处理者的利益平衡映射在大数据时代的法律规则之中[11]。

二、复合法益语境下个人信息使用利益的界分

网络智能时代个人信息呈现泛在泄露的趋势,由非法使用个人信息所引发的社会问题层出不穷,法益保护链条不断拉长,从刑法层面规范个人信息使用行为、加强对个人信息使用自主的保护逐渐取得社会共识。刑法的谦抑性要求刑法只在必要性意义上制裁最危险、对法益容易造成最严重侵害的行为,因此在区分罪与非罪的界限的关键领域厘清个人信息的法益属性与权利边界是刑

②我国《民法典》第 111 条规定:“不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息。”《网络安全法》第 41 条规定:“网络运营者不得收集与其提供的服务无关的个人信息,不得违反法律、行政法规的规定和双方的约定收集、使用个人信息。”第 42 条规定:“未经被收集者同意,不得向他人提供个人信息。”《消费者权益保护法》第 29 条规定:“经营者不得违反法律、法规的规定和双方的约定收集、使用信息。经营者及其工作人员对收集的消费者个人信息必须严格保密,不得泄露、出售或者非法向他人提供。”《个人信息保护法》第 10 条规定:“任何组织、个人不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息。”

法审慎介入保护个人信息使用利益的先决条件,有助于恰当处理个人信息保护与利用的冲突及协调问题。

(一)个人信息的复合法益属性

关于个人信息的法益属性,因对个人信息的内容范围和应用价值理解不同,学者们的观点存在诸多差异。当前学界主要有以人格权说[12](人格尊严与个人自由)、财产权说[13](经济价值与商业利益)为代表的个人法益论,以及以公共产品说[14](公共利益与社会秩序)为代表的超个人法益论,但都有失偏颇,未能全面阐释个人信息的法益属性。

当下,网络信息技术影响和改变着社会生活,个人信息逐步成为一种重要权利,所蕴含的权益内容也日益丰富,形成了包含决定权、保密权、访问权、更正权、可携权、封锁权、删除权和被遗忘权等一系列子权利的权利系统。同时,在个人信息的流动和使用过程中,初始权利主体逐渐不再拥有对个人信息的完全控制,信息权利主体也呈现多元化,从信息主体扩展至收集者、使用者及处理者。因此,个人信息权益内容呈现复合化特征[15],既包含个体的人格权及其衍生的财产权,又涉及公共利益、社会秩序和国家安全。人身属性、财产属性和公共属性共同构成个人信息的法律内核,这是由个人信息的不同内容及其作为特殊资源的使用价值所决定的。相应地,个人信息权利法律保护具有信息自由与信息安全的多元价值。例如,为了运用大数据联防联控新冠肺炎疫情,需要收集和使用有关确诊或疑似病患者及其他相关自然人的个人信息,这一过程是对公共安全与个人自由的利益衡量,公民的个人信息权利受到一定程度的限制,不可避免地要让渡部分个人信息使用利益,承担公共卫生安全保障义务和法律责任。数字化疫情防控背景下,被授权收集和利用个人信息的部门和机构拥有信息使用权,社会公众有获悉和分享个人信息的知情权,政府机关则行使披露和发布疫情公共数据的权力。

概言之,个人信息的法益属性具有复合性特征,不仅包括初始信息主体的权利自由,而且包括其他依法收集和使用个人信息的主体享有的信息权利;同时,个人信息安全也是个人信息权的重要内容,个人信息法益不仅包括公民个人信息安全,更涉及公共卫生健康安全乃至国家安全。个人信息刑法保护所追求的价值目标也有信息自由和信息安全两个方面:一是传统法益或个人法益,即公民个体的人格权和财产权,这是由个人信息来源于特定自然人所决定的;二是新型法益或超个人法益,即信息领域的国家和社会公共利益、安全或秩序,这来自个人信息广泛应用于商业经济、行政管理、教育科研等领域,为经济发展、社会治理、风险防控提供决策参考。

(二)个人信息承载的使用利益识别

个人信息法益识别包括两层含义:一是个人信息所承载的利益是否上升为法益;二是个人信息利益体现的是何种法益。个人信息承载的使用利益根植于个人信息法益所具备的人格利益属性、财产利益属性与公共利益属性并存的复合特征,保护个人信息法益首先须明晰各方主体的权利边界。具体而言,在信息流动不断加速的时代背景下,信息主体并不一定直接占有和控制其个人信息,信息主体和信息处理者相分离已然成为常态。因此,个人信息往往承载着两方面的使用利益:一是信息主体的使用自主利益,源于其与个人信息的人格关联,由个人信息的可识别性所决定;二是信息处理者的正当使用利益,其一定程度上代表的是社会利益,因为身处信息社会的任何组织或个人都有使用个人信息实现特定目的的需求,都可能成为掌握他人个人信息的信息处理者。平衡信息主体与信息处理者的使用利益是保护个人信息法益的应有之义。

1. 信息主体的使用自主利益

个人信息是指任何能够直接或者间接识别特定自然人身份特征或个人属性的信息。识别通常所依赖的是个人特有的或者能够标识个人特征的信息,如姓名、身份证号码、通信地址、联系方式、位置数据等,由信息本身的特殊性识别出特定自然人,而识别的目的是为了将特定主体与社会中的其他人区别开来。可以说,个人信息是个人社会性的延伸,既是个人标识自己的工具,也是他人辨识特定自然人的手段[16]。由于个人信息与人格尊严、自由发展关系密切,传统个人控制论强调个人信息的私人属性,通过将基本权利上的个人自治拓展至个人信息领域,从而推导出独立的个人信息自决权,即赋予信息主体独立自主决定如何处理其个人信息的权利。人作为独立的个体,只能是目的而不是达到任何目的的工具[17],凡是与个人人格形成、发展有关的事项都应当由本人自主决定。个人信息是人格的征表,只能自主决定而不能被他人决定,否则将损害自然人独享的人格尊严。随着计算机和网络技术的普及,个体在社会交往中提供的个人信息被自动记录、留存和分析应用,如果这些行为信息主体并不知情甚至违背其意愿,那么人就被当作客体对待,是对人格尊严和自由发展的侵犯。“个人有权拒绝仅基于数据自动化处理而不考虑信息主体本人意愿作出的结果的约束”是各国个人信息立法普遍遵行的基本原则,保护信息主体的个人信息自主即是为了防止将人格尊严当作客体“被处理”[18],以实现对个人自治等基本权利的保护。

由基本权利演化而来的个人信息自决权将个人信息处理纳入纯粹个人事务的范畴,认为自然人对其个人信息享有自主控制和自主决定的权利,包括对个人信息的转移自主和使用自主,超越了单纯防范非法转移个人信息的隐私权保护逻辑。个人信息相对于隐私的独立特性使得个人信息自决权的内涵也与隐私权产生明显差异。隐私权强调个人信息的私密性,是一种保护个人私密事项的防御性权利,主要是防范个人私密信息未经许可被权限外的主体知悉,造成隐私泄露。所以隐私权是一种防范个人信息被不当转移的消极权能。然而,网络时代个人信息由于公开分享和交换使用的特性,具有自主共享使用的积极权能,与隐私权形成鲜明对比。个人信息自主既包含对个人信息分享或传播等转移范围的自主限定,还包括对个人信息运用方式、程度的自主权利,强调信息主体按照自己的意志对个人信息的用途进行自主控制。因此,个人信息自决权以全面自主权能为核心,自然就超越了隐私权单纯的转移自主权能。随着个人信息使用价值的日益凸显,对个人信息使用自主的控制越来越成为个人信息权能的核心。欧盟个人数据立法措辞的变化明显地体现了这一点③。

2. 信息处理者的正当使用利益

传统个人控制论建立在 20 世纪七八十年代计算机和信息网络发展的初期阶段即 Web1.0 时代,计算机和互联网尚未普及,网民以及网络平台数量较少,个人向特定主体提供少量单一的个人信息即可获得相应的产品和服务,个人信息尚未被大规模收集和使用,信息主体对个人信息的披露和用途具有一定的控制力。进入依托网络平台实现人与人双向交换分享信息的 Web2.0 时代,互联网社交活动日益频繁,网络空间留存了大量可识别个人特征的数据信息,这些个人信息大部分并非由个人主动提供或公开,而是由无处不在的网络系统、智能设备或传感器实时记录、自动处理后关联到特定自然人,同时能够识别个人特征的信息类型也日趋多样化,个人信息的收集和使用环境已

③欧盟 1995 年制定的《个人数据保护指令》第 1 条第 1 款规定:“成员国应当依据本指令保护自然人的基本权利和自由,特别是有关个人数据处理中的隐私权。”2018 年实施的《一般数据保护条例》第 1 条第 2 款规定:“本条例旨在保护自然人的基本权利和自由,尤其是个人数据保护的权利。”显然,最新立法以“个人数据保护的权利”替代了“个人数据处理中的隐私权”。

发生根本性变化。再到万物互联、智能匹配、个性化定制的Web3.0时代,信息的实时交互性和快速流动性使得信息主体与信息处理者日渐分离,对于海量多样的个人信息,信息收集者往往无法事先作出准确判断并告知被收集者特定的使用目的及方式。大数据、云计算、人工智能等算法技术的运用显著增强了信息处理者对个人信息的采集加工与分析应用能力,个人在网络空间的任何"蛛丝马迹"都无所遁形,信息主体对个人信息陷入失控的境地,个人控制论赖以存在的社会基础被摧毁。由此,个人信息保护理论开始从个人本位向社会本位转变,社会控制论应运而生,强调个人信息所蕴含的利益应由全社会共享。

网络时代数字化生存越来越依赖信息的全面交换和分享,基于个人控制论的个人信息私权化与信息社会个人信息社会化利用之间的冲突加剧。深度挖掘与自动处理技术提升了信息处理者对个人信息的分析应用能力,个人信息被广泛用于创新市场营销、改进产品和服务、防范安全风险、完善公共治理、深化学术研究等用途,创造出更大的经济价值与社会效用[19],保护个人信息自主权利的同时促进个人信息在更大范围内流动利用的观点得到广泛认同。个人信息本身只是可以识别某个人的事实或记录,本质上不具有排他性或者排除他人使用的成本很高,并不当然由个人拥有或控制,其不仅直接关涉信息主体的人身和财产权益,而且也关系他人利益以及社会利益[20]。社会控制论认为,个人信息与个人的人格关联性不足以使其成为私人控制的客体,就个人信息的超个人法益属性而言,个人信息被视为一种处于公共领域的社会资源,应由社会共同决定如何使用。虽然个人信息自决权赋予信息主体自主决定如何使用个人信息的权利,但个人信息兼具的社会公共性要求个人信息自主不能等同于物权、人格权等支配权,有必要防止个人信息自主宽泛化、绝对化。比如,欧盟《一般数据保护条例》承认数据主体对个人数据收集、处理、流动、使用的控制权,并不认可个人享有绝对的排他性支配权,必须遵循比例原则,考虑个人数据在社会中的作用,并与其他权利协调平衡。概言之,个人信息不仅涉及信息主体的自主使用利益,同时也承载着商业经营者、公共机构等信息处理者的正当使用利益,应当在此基础上进行利益衡量,制定包括刑法规范在内的、符合各方利益的个人信息使用规则。

三、非法使用个人信息行为刑事规制的边界

深度挖掘信息效用、重构信息应用价值是大数据产业最新的发展方向。大数据时代以实现信息资源的经济效益与社会效益为逻辑起点,个人信息同时承载着信息主体和信息处理者的使用利益,保护个人信息使用自主法益并不等于禁止个人信息的流动利用。域外个人数据保护规范普遍将保护信息主体的基本权利与促进个人信息合规使用助力社会经济发展作为立法的双重目的。例如,印度《个人数据保护法》指出:"数字经济的发展进一步拓展了数据作为人与人之间的重要沟通手段的运用,有必要通过数字治理和数字融合,营造一种尊重个人信息隐私,确保赋权、进步和创新的整体文化,以促进自由和公平的数字经济。"这对于我国个人信息保护立法具有很强的借鉴意义,应从源头规制个人可识别信息的潜在非法使用行为并给予救济,而不是限制创造效益的转移行为或正当使用行为。

(一)非法使用个人信息行为具有严重的法益侵害性

在强调个人信息安全流动与有效利用的背景下,个人信息的使用价值凸显使得个人信息使用自主逐渐成为个人信息权能的核心。法益侵害是建构刑事不法的根基,非法使用个人信息行为的

法益侵害性较之非法转移个人信息行为更为严重。首先,非法使用个人信息行为的法益侵害具有根源性。个人信息使用自主是个人信息转移自主的目标和落脚点,经营者对个人信息使用价值的追逐成为当前非法转移个人信息行为高发的深层次诱因。例如,在个人信息黑色产业链中,下游利用个人信息恶意注册网络账号、实施网络诈骗等违法犯罪活动并从中获利的非法需求,加剧了上游非法获取、出售或提供等个人信息转移行为的滋长。其次,非法使用个人信息行为的法益侵害具有直接性。转移个人信息行为本质上只是个人信息自身的物理流转和空间变换,从信息主体转换至信息处理者,由一个空间转移至另一个空间,不管变换如何频繁,非法转移行为始终只是形式上的侵害,并未直接侵害实质的法益[21]。易言之,非法转移个人信息行为仅具有间接的法益威胁或者法益侵害的抽象危险。而个人信息的非法使用将这种法益侵害可能性变成具体化、可视化的现实损害,如身份证件等个人信息被他人冒用在网络平台办理借贷逾期不还,会给信息主体的征信记录带来负面影响,甚至造成重大财产损失。再者,非法使用个人信息行为的法益侵害具有精准性。个人信息能关联到特定自然人的可识别性特征使其与信息主体呈现一一对应的涵摄关系,不法分子利用个人信息实施违法犯罪往往令人防不胜防,受害人一步步落入事先设计好的陷阱,信以为真,造成严重损失,如损害后果严重的电信网络诈骗犯罪大部分都是“精准诈骗”,诈骗分子在摸清目标受害人基本情况后进行针对性的“私人订制”。

基于以上特点,非法使用个人信息行为无疑会对信息主体的隐私、财产、名誉等方面以及社会管理秩序造成严重损害或威胁。刑法通过入罪施加刑事责任的方式规制最为严重的法益侵害行为,因此有必要在刑法上对非法使用个人信息行为予以单独评价,实现对个人信息法益的周延保护。而且,非法使用个人信息行为的法益侵害性与非法转移个人信息行为相比有过之而无不及,举轻以明重,如果不以需求端为导向从源头规范个人信息的使用行为,单纯打击制裁非法转移个人信息行为只能是治标之策,无法有效应对个人信息遭受侵害愈演愈烈的严峻形势。

(二)非法使用个人信息行为的入罪要件与出罪事由

在个人信息使用价值凸显的背景下,对个人信息权益关注的重点必然从转移环节转向使用环节,规范个人信息使用行为,管控个人信息规模化利用带来的法益侵害风险成为网络刑法的重要任务。但是,“刑罚之界限应该是内缩的,而不是外张的,刑罚是国家为达其保护法益和维持法秩序的任务时的最后手段”[22],作为刑事规制的关键步骤,将个人信息使用自主纳入刑法的保护范围并对相应的非法使用个人信息行为进行入罪规制,必须遵循刑法谦抑性原则,明确非法使用个人信息行为的入罪要件与出罪事由,防止过度犯罪化损害刑法作为保障公民权利自由的最后手段的职能定位。

1.危害行为:未征得信息主体许可使用且情节严重

从周延个人信息法益刑法保护出发,应将个人信息使用自主作为个人信息法益的核心内容,相应地,应以非法使用个人信息行为作为侵犯公民个人信息罪的关键构成要件类型,完善该罪的危害行为体系。在确定非法使用个人信息行为入罪门槛时,基本原则是与侵犯公民个人信息罪已规定的非法转移行为的入罪标准保持相对一致,并根据非法使用行为的特殊性质进行适度调整。侵犯公民个人信息罪具备典型的法定犯属性[23],法定犯的刑事可罚性最终取决于行政法规范的规定。

现行侵犯公民个人信息罪以“违反国家有关规定”④作为客观构成要件要素之一,换言之,违反国家法律、行政法规和部门规章是非法转移个人信息行为入罪的必要前置条件,因而非法使用个人信息行为在入罪时也应当遵循这一标准,与转移型侵害个人信息行为保持相同的违法性前提。具体而言,我国《网络安全法》第41条、《个人信息保护法》第13条、《消费者权益保护法》第29条、《全国人大常委会关于加强网络信息保护的决定》第2条,以及《电信和互联网用户个人信息保护规定》第9条等强制性法律法规均明确要求信息处理者使用个人信息前应征得信息主体的同意。因此,以实现自己的特定目的[24],未征得信息主体许可而使用他人个人信息的行为违反国家有关规定,构成非法使用个人信息。知情同意原则作为个人信息使用的正当性基础建立在个人信息自决权之上,而非隐私权,个人信息不要求具有隐私的秘密性特征[25],那么即使是已经公开的个人信息也应当征得信息主体的许可后才能商业化使用,未经授权同意擅自对从网络上搜集、整理的他人个人信息加以利用的行为同样属于非法使用。在徐某诉芝麻信用管理有限公司个人信息纠纷案中,杭州互联网法院认为,被告采集并利用其他渠道已合法公开的原告系被执行人的信息是基于双方签订的“芝麻信用”服务协议,表明原告已授权同意被告可以对其个人征信数据进行合理化的商业使用。刑法理论上,个人的知情同意通常可以被看作是一种被害人同意或承诺,具有一定的出罪功能,信息主体知情同意可能成为排除或降低刑事违法性的事由,以此作为阻却或减轻非法使用个人信息行为刑事责任的根据。

某一行为成立法定犯要求其既违反行政法规范,同时又违反行政刑法规范中的特别要件,即“情节严重”,这一构成要件具有界分违法行为与犯罪行为的重要功能。《侵犯公民个人信息罪司法解释》第5条对非法获取、出售或者提供个人信息构成“情节严重”的具体情形作了相对明确的列举式规定,意在根据个人信息与信息主体的关联程度将其区分为敏感信息、重要信息和普通信息,进而实行分类、分级保护[26]。对不同类型和等级的个人信息设定差异化的入罪门槛,除了对象数量标准之外,还设置了其他类型化的定量标准如信息用途、违法所得数额、主体身份、再犯记录等,这些标准也可以为判断非法使用个人信息行为是否构成“情节严重”提供参考。但非法使用行为与非法转移行为相比,在行为属性上还有一些独特之处,非法使用行为主要以行为恶劣程度来区分与一般不当使用行为的界限,在解释“情节严重”时应加入行为性质标准,选择特定的类型化行为如恶意滥用、欺诈冒用、擅自允许第三方参与使用、改变目的或方式使用等,基本涵盖影响侵犯个人信息权益严重程度的情节因素,明晰个人信息合规使用的界限。此外,非法使用个人信息相较于非法转移个人信息,对法益的实质损害更为严重,在情节严重程度相近时,刑事处罚的量刑也应更重一些,才能体现以规制非法使用个人信息为重点的侵害个人信息犯罪治理思路。

2. 行为对象:非经匿名化处理的个人信息

与自然人人格不可分离的可识别性是个人信息区别于其他信息的本质特征。各国个人信息保护规范在定义“个人信息”时,均明确以可识别性作为个人信息的核心特征。个人信息应用实践中,越来越多的经营者在使用个人信息时开始重视对其进行“脱敏”,即去标识化或匿名化处理。数据脱敏技术运用加密算法、替换算法或生成算法将个人信息中标识个体特征的识别符(identifier)隐

④“两高”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》第2条规定:“违反法律、行政法规、部门规章有关公民个人信息保护的规定的,应当认定为刑法第二百五十三条之一规定的‘违反国家有关规定’。”

藏、替换或删除,即去除个人信息的可识别性且不能恢复,将个人信息转化为匿名信息,一定程度上切断了个人信息与特定自然人的关联可能性。匿名化处理在保留个人信息特定经济、社会用途价值内容的同时,也降低了该信息一旦泄露或滥用可能对信息主体的合法权益造成威胁或损害的风险。经匿名化处理去除可识别性的信息因无法指向特定自然人身份且不能恢复,就不再纳入个人信息的范畴,亦不适用个人信息保护规则。印度《个人数据保护法》界定"匿名化"系指将个人数据转换或者转化为数据主体无法被识别的形式的不可逆过程且符合保护局规定的不可逆标准。我国《网络安全法》也明确将个人信息匿名化处理载入立法,在第 42 条确立了使用个人信息征得信息主体同意的例外情形"经过处理无法识别特定个人且不能复原",即不可逆的匿名使用规则。遵循前置法规定,匿名信息不属于侵犯公民个人信息罪的行为对象,无须经信息主体同意即可合规使用。

当然,匿名信息是相对的概念,不存在绝对匿名的信息。在数据样本总量足够巨大的情况下,借助越来越强大的智能算法技术,任何信息片段都可能通过与外部信息关联比对后重新识别(Re-identification)出特定个人,经匿名化处理的个人信息同样存在重新识别出自然人特征的可能性。因此基于平衡个人信息安全保护与信息资源应用价值获取的考量,应当在法律层面确定合理的匿名信息判断标准。对此,欧盟采取"所有合理可能性标准"⑤,要求对信息处理者和任何其他人而言均不具有识别的合理可能性的信息方为匿名信息。也就是说,存在两种类型的匿名信息,一种为完全不能揭示原始识别信息的匿名信息,另一种为需要不合理的努力方能实现识别的匿名信息[27]。美国则针对个人健康信息匿名化创设了"专家标准"和"安全港标准"⑥。我国应当在《个人信息保护法》或侵犯公民个人信息罪相关司法解释的修订中对匿名信息作出明确界定,欧美国家关于匿名信息的判断标准可资我国借鉴。

3. 违法阻却事由:符合个人信息合理使用的情形

违法阻却事由是对违法性的否定,但以符合构成要件该当性为逻辑前提,从而在客观上限定了成立犯罪的范围[28]。违法阻却事由之确立作为一种出罪机制,"有如在不法阶层里创设另一个消极之不法要件,倘若此消极要件存在,行为人行为即被法律所容许"[29]。在认为刑法的机能之一在于法益保护的结果无价值论看来,不违反法益保护目的是违法阻却的一般原理,而优越利益保护原则是其第一下位原理。具体而言,当某一行为该当于构成要件时,便发生了法益遭受侵害这一有害于社会的结果;但在某些情况下,同一行为同时也具有保全其他法益这一社会有用性,在保全法益优于侵害法益之时,从社会功利主义的观点看,可以将该行为整体上正当化[30]。就个人信息保护与利用而言,经利益衡量后,为保全更重要的法益,特定情形下允许信息处理者无须征得信息主体同意即可在适当限度内使用个人信息的方式被称为"合理使用"。当满足个人信息保护规范预设的合理使用条件时,未经信息主体授权许可的个人信息使用行为不构成侵权。信息处理者未征得信息主体许可使用非经匿名化处理的个人信息且情节严重的行为,因符合构成要件该当性而推定具有形式违法性,但如果该使用行为构成合理使用就可以阻却实质违法性。这与著作权法上通常将合

⑤欧盟《一般数据保护条例》"鉴于条款"第(26)项指出:"为判断自然人身份是否可识别,需要考虑所有可能使用的手段,比如控制者或其他人来直接或间接地确认自然人身份。为判断所使用的手段是否可能用于识别自然人,需要考虑所有客观因素,包括确认身份需要花费的金钱和时间,同时考虑现有处理技术以及科技的发展。"

⑥美国《健康保险流通与责任法案》第 164.514 条第 b 款第 1 项规定:"经专家判断认为信息不能具识别性则不属于法案规制的可识别健康信息。"该款第 2 项规定:"删除 18 种识别符的健康信息不是可识别健康信息。"

理使用归入侵权抗辩事由在思路上一脉相承。概言之,个人信息的合理使用制度处于保护与限制个人信息权利的平衡点,通过适度限制信息主体的权利促进信息资源的流动利用,调节信息主体与信息处理者之间的利益均衡,实现保护个人信息权益与增进社会公共福祉的双重目的。

合法利益豁免为个人信息合理使用提供了正当性基础。欧盟最早在1995年的《数据保护指令》中引入个人数据处理无须征得数据主体同意的合法利益豁免机制,随后在《一般数据保护条例》中继承并完善了这一制度⑦。合法利益判断并不限于公共利益,也包括信息处理者的正当使用利益。对于何为合法利益?美国隐私保护法采取"合理预期标准"⑧,以社会一般公众对于涉案信息是否持有合理的隐私期待来界定隐私的保护范围。即使没有信息主体的明确许可,只要信息处理者的相关使用行为符合信息主体在此情形下的主观心理预期,且这种期待客观上被社会一般公众认为是合理的,那么就可以认定信息处理者的使用利益是正当的。但合法利益豁免并非不受任何限制,某一个人信息使用行为即使通过"合理预期"规则被认定为属于正当利益,还必须进行一个符合权利限制比例原则的"平衡测试"[31],证明信息处理者的正当使用利益高于信息主体的使用自主利益,即只有优越利益才能够适用合法利益豁免机制。

个人信息合理使用强调使用行为的合理性,包含三个要素:一是属于法律规定的特殊情形;二是不影响个人信息安全;三是不损害信息主体的合法权益。个人信息合理使用制度从信息处理者享有的正当使用利益出发,强调特定情形下信息处理者可以不经信息主体许可而使用个人信息,但不得损害信息主体享有的其他权利。目前,我国在《民法典》第1036条将"合理处理该自然人自行公开的或者其他已经合法公开的信息"和"为维护公共利益或者该自然人合法权益,合理实施的其他行为"纳入侵犯个人信息权益的免责事由。同时,分别在最新修订的《个人信息安全规范》(GB/T 35273—2020)第5.6条和《个人信息告知同意指南(征求意见稿)》6.1条详细列举了信息处理者使用个人信息时免于告知同意(征得授权同意的例外)的十余种情形,涵盖履行强制性法律义务、保障国家安全与公共安全、保护公共利益、维护个人生命财产重大权益,以及开展公益性学术研究等方面。由此可见,我国现有的合理使用制度在设计上侧重于以社会公共利益来限制个人信息使用自主、阻却行为违法性,未来应更进一步将信息处理者利用个人信息追求正当且必要的经济利益纳入合理使用的范畴,但生物特征、行踪轨迹、通信内容、财产状况、14岁以下儿童信息等个人敏感信息除外。

四、结语

寻找社会利益与个人自由之间的平衡点是刑法学永恒的追求[32],个人信息刑法保护规范承载着保护个人信息法益与促进信息资源有效利用的双重使命。网络时代发展到大数据深度挖掘应用阶段,个人信息自主的内涵更加丰富,不仅包括以获取、出售、提供为代表的转移自主,还包括使用自主。个人信息使用价值的日益凸显使得使用自主相较转移自主具有更核心的法益地位,个人信

⑦欧盟《一般数据保护条例》第6条规定:"有下列情况之一,数据处理视为合法:……(e)处理是为了执行公共利益领域的任务或行使控制者既定的公务职权之必要;(f)处理是控制者或第三方为了追求合法利益之必要,但此利益与数据主体的利益或基本权利自由相冲突的除外,尤其是数据主体为儿童的情形。"

⑧美国《消费者隐私权利法案》第103条(b)款规定:"当机构处理行为在相应场景中合理时,无需经过用户同意或满足其他要件而自动获得合法性授权。"

息法益刑法保护的重点从转移自主转向使用自主是大数据时代的必然要求。然而,当下侵犯公民个人信息罪只保护个人信息转移自主,没有涉及个人信息使用自主,由此产生刑法规制漏洞,无力应对非法使用个人信息行为愈演愈烈、法益侵害严重这一现实而紧迫的问题。因此有必要在遵循刑法谦抑性原则的前提下合理确定非法使用个人信息行为的入罪要件与出罪事由,厘清个人信息使用自主刑法保护边界,平衡信息主体的使用自主利益与信息处理者的正当使用利益,在保障个人信息安全的同时推动大数据产业健康可持续发展。

参考文献:

[1]尼古拉·尼葛洛庞帝.数字化生存[M].胡泳,范海燕,译.北京:电子工业出版社,2017:232.
[2]维克托·迈尔-舍恩伯格,肯尼思·库克耶.大数据时代:生活、工作与思维的大变革[M].盛杨燕,周涛,译.杭州:浙江人民出版社,2013:104.
[3]齐爱民.拯救信息社会中的人格[M].北京:北京大学出版社,2009:31.
[4]习近平.高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告[N].人民日报,2022-10-26(04).
[5]涂子沛.数文明[M].北京:中信出版社,2018:36.
[6]操秀英.网络黑产"魔高一尺" 严刑重典才能"道高一丈"[N].科技日报,2019-12-31(4).
[7]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.
[8]埃里克·希尔根多夫.德国刑法学:从传统到现代[M].江溯,黄笑岩,译.北京:北京大学出版社,2015:382.
[9]高楚南.刑法视野下公民个人信息法益重析及范围扩充[J].中国刑事法杂志,2019(2):87-96.
[10]乌尔里希·齐白.全球风险社会与信息社会中的刑法[M].周遵友,江溯,译.北京:中国法制出版社,2012:308.
[11]江波,张亚男.大数据语境下的个人信息合理使用原则[J].交大法学,2018(3):108-121.
[12]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].政治与法律,2017(2):46-55.
[13]刘德良.个人信息的财产权保护[J].法学研究,2007(3):80-91.
[14]靳宁.大数据背景下个人信息刑罚治理的合理边界:以侵犯公民个人信息罪的法益属性为例[J].黑龙江社会科学,2018(3):28-32.
[15]刘一帆,刘双阳,李川.复合法益视野下网络数据的刑法保护问题研究[J].法律适用,2019(21):109-117.
[16]高富平.个人信息保护:从个人控制到社会控制[J].法学研究,2018(3):84-101.
[17]康德.实践理性批判[M].韩水法,译.北京:商务印书馆,2015:95.
[18]宋亚辉.个人信息的私法保护模式研究:《民法总则》第111条的解释论[J].比较法研究,2019(2):86-103.
[19]温昱.个人数据权利体系论纲:兼论《芝麻服务协议》的权利空白[J].甘肃政法学院学报,2019(2):84-96.
[20]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.
[21]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.
[22]林山田.刑罚学[M].北京:商务印书馆,1983:128.
[23]刘艳红."法益性的欠缺"与法定犯的出罪:以行政要素的双重限缩解释为路径[J].比较法研究,2019(1):86-103.
[24]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,2018:172.
[25]喻海松.网络犯罪二十讲[M].北京:法律出版社,2018:214.
[26]刘宪权,房慧颖.侵犯公民个人信息罪定罪量刑标准再析[J].华东政法大学学报,2017(6):107-115.
[27]韩旭至.个人信息的法律界定及类型化研究[M].北京:法律出版社,2018:233.
[28]陈兴良.教义刑法学[M].北京:中国人民大学出版社,2014:370.
[29]余振华.刑事违法性理论[M].台北:元照出版有限公司,2001:14.
[30]西田典之.日本刑法总论[M].王昭武,刘明祥,译.北京:法律出版社,2013:102.
[31]谢琳.大数据时代个人信息使用的合法利益豁免[J].政法论坛,2019(1):74-84.
[32]欧阳本祺.论网络时代刑法解释的限度[J].中国法学,2017(3):164-183.

The change of criminal law protection of personal information legal interests in the era of big data: Focus on regulating illegal use of personal information

LIU Shuangyang[1], LI Chuan[2]

(*1. School of Criminal Justice, China University of Political Science and Law, Beijing 100088, P. R. China; 2. School of Law, Southeast University, Nanjing 211189, P. R. China*)

Abstract: The type of behavior stipulated in Article 253 of the Criminal Law of China on the crime of infringing on citizens' personal information is only limited to the transfer behavior represented by illegal acquisition, sale or provision of personal information, and the illegal use of personal information is not included in the scope of regulation, resulting in loopholes in the criminal regulation, which reflects the defects in understanding the legal interests of one-sided understanding of personal information autonomy as transfer autonomy and neglect of use autonomy. And then only preventing illegal transfer of personal information is taken as the logic of criminalization, making the criminal law protection of personal information legal interests incomplete. At present, personal information has become a key element in network crimes. The phenomenon of illegal use of personal information has become increasingly fierce. Crimes against citizens' personal information have gradually formed a complete black industrial chain of "provider-middleman-illegal use". Each link has a clear division of labor and strict organization, and illegal and criminal activities are carried out through illegal use of personal information. And then the realization of profits is the root cause of the widespread disclosure of personal information and the proliferation of illegal transactions. The criminal law can only crack down on the illegal transfer of personal information, which can only be a temporary solution, leading to poor criminal governance of crimes against personal information. As we enter the stage of deep mining and application of big data, the use value of personal, property, public and other composite legal interest attributes rooted in personal information has become increasingly prominent in context of the vigorous development of the digital economy, making the autonomy of personal information use more of a core legal interest status than the autonomy of personal information transfer. The focus of personal information criminal law protection should be shifted from the transfer link to the use link. The illegal use of personal information belongs to the downstream behavior, which causes great damage or threat to the personal and property safety of citizens and the social management order. Compared with the illegal transfer of personal information in the upstream, the illegal use of personal information has a more serious legal interest infringement, which is manifested in the root, directness and accuracy of legal interest infringement. Therefore, criminal legislation should be demand-oriented, and it is necessary to reasonably determine the incriminating elements and causes of decriminalization of illegal use of personal information on the premise of following the principle of modesty of the criminal law, that is, taking serious cases without the consent of information subject as harmful behavior, taking personal information that is not subject to anonymous treatment as the object of conduct, and taking the situation that conforms to the reasonable use of personal information as the cause of illegal obstruction. It not only standardizes the use of personal information from the source, but also limits the criminal boundary of illegal use of personal information. While protecting the security of personal information, it promotes the orderly and free flow, reasonable and effective use of personal information, balances the independent use interests of information subjects and the legitimate use interests of information processors, and provides a strong criminal rule of law guarantee for the high-quality development of the digital economy.

Key words: personal information; illegal use; use autonomy; infringement of legal interest; elements of incrimination; cause of decriminalization

(责任编辑 胡志平)