

Doi:10.11835/j.issn.1008-5831.fx.2021.04.004



欢迎按以下格式引用:刘利平.个人信息侵权法保护的价值与理据新论——基于大数据悖论的分析视角[J].重庆大学学报(社会科学版),2022(5):221-234. Doi:10.11835/j.issn.1008-5831.fx.2021.04.004.

Citation Format: LIU Liping. On the value and theory basis of personal information protection in tort law: Analysis perspective based on big data paradox[J]. Journal of Chongqing University (Social Science Edition), 2022(5): 221-234. Doi: 10.11835/ j. issn. 1008-5831. fx. 2021. 04. 004.

个人信息侵权法保护的 价值与理据新论 ——基于大数据悖论的分析视角

刘利平

(盐城师范学院 历史与公共管理学院,江苏 盐城 224007)

摘要:为有效应对信息科技发展引致的个人信息保护和信息产业发展的矛盾冲突,必须创新优化个人信息侵权法保护的制度设计,肯定个人信息受法律保护的同时又限制信息主体的排他性控制权,制衡“数据权力”以抑制个人信息处理者的恣意和滥权,谋求信息时代人权保护以及为信息产业内置发展空间的“双赢”。基于大数据透明化悖论、权力悖论、身份悖论的视角,个人信息处理事实上同时存在正负效应双重外部性,这决定了个人信息法律保护不能仅依赖“基于权利的方法”,还应直面大数据时代面临的认知和结构困境,并“基于风险的方法”对个人信息的法律保护进行路径重构。大数据悖论决定了个人信息侵权法保护的价值取向不能简单化、绝对化,其实质是要求在信息处理者秘密搜集处理信息与个人主张信息处理透明化、信息处理者的数据特权与个人对信息权利的“让渡”或“牺牲”、信息处理者识别个人身份与个人主张身份隐私保护等博弈关系中求得优解。为此,个人信息侵权法保护的价值既要定位于保护公民个人的人格尊严,保障数字时代人权,又要衡平信息有序流动、跨境交易以及信息产业发展中的各方利益。大数据悖论非但不应成为个人信息权利保护、政府信息治理权力、信息产业发展间“非零和博弈”的“共赢”目标之障碍,作为源流之诱因反而要求个人信息侵权法保护的价值不仅定位于救济信息主体遭受损害的权利和筑牢个人信息权利的边界,还在于制约公权力可能对个人信息的侵犯,对信息业者利用个人信息予以明确规范并提供“负面调整”的方向警示。个人信息侵权法保护的理据也因此不仅限于人权保护理论,还应从经济分析理论、危险控制理论、营业收益风险理论、企业社会责任理论等多维视角进行深度审视,籍以考索个人。

基金项目:江苏省教育厅高校哲学社会科学基金项目“大数据时代被遗忘权的制度建构与法律适用研究”(2017SJB1531);江苏省社科应用研究精品工程课题“新时代江苏防范塔西佗陷阱的路径对策研究”(18SYA-044)

作者简介:刘利平,盐城师范学院,Email:ljpy@126.com。

关键词:个人信息;侵权;价值;理据;大数据悖论

中图分类号:D913

文献标志码:A

文章编号:1008-5831(2022)05-0221-14

信息科技的迅猛发展和大数据时代的到来,网络的虚拟性以及信息主体的不对称地位使得个人信息不仅事实上面临国家公权力的侵害威胁,更面临着非公权力机构的信息业者各种新型侵害行为的吞噬,赋予个人信息侵权法保护地位已经成为对抗公权力侵犯和进行民事权利救济的必然要求。客观上,赋予信息主体以个人信息权,可以消除信息利用的“丛林法则”和“公地悲剧”^[1]。虽然对个人信息进行法律保护已成为世界上绝大多数国家的共识^①,但是不同国家对个人信息的侵权法保护持有不同立场,立法确认的进程也不一致。除了历史文化传统、社会现实的国别差异以及信息产业发展的不同程度等原因外,一个必须正视的缘由就是大数据悖论而致的个人信息处理面临正负效应并存的双重外部性^[2]。大数据悖论本身意蕴为少数主体占有、掌控大数据时的作用和效果大,不过当多数参与者都知晓、使用和分享后其效用就会消减,甚至会引发反向的破坏作用^[3],但从现实发展和数据利用视角看,其主要表现为透明化悖论、权力悖论、身份悖论^[4]。透明化悖论即信息主体的透明化要求与信息业者秘密搜集信息的悖论,可表现为数据的共享和隐私之间隐含分离和对立因素^[5],在人工智能领域,透明性可以帮助缓解公平、歧视和信任等问题,但信息透明度的增大会导致人工智能容易受到攻击而可能带来新的风险^②;权力悖论即权力走向呈现出话语权向社会弥散的去中心化与向新兴资本、知识和权力中心聚合的集中化悖论^[6],实践中表现为大数据资源作为改造社会强大工具的独享数据特权与广大的信息主体权利主张的矛盾;身份悖论即信息产业发展需要识别利用个人身份与信息主体主张身份隐私的矛盾与冲突^[7]。所以,当前对个人信息侵权法保护的价值与理据进行重新审视和深度分析,有助于拨开大数据悖论的理论迷雾,有利于探求个人信息权利保护与信息有序流动、跨境交易以及信息产业等多重博弈关系的优解。

一、问题的提出:大数据时代个人信息危机呼唤侵权法保护

(一)大数据时代个人信息安全面临严峻挑战

大数据时代的来临给人们带来极大便利,同时也给个人信息保护带来了严峻挑战。“大数据指的是大量的、多种类的、复杂的、长的和(或)分散的数据集,这些数据来源于各种传感器、电子交易、电子邮件、视频、点击流和(或)我们今天或以后可用的所有数字资源”^[8]。大数据具有海量性、时效性、多变性和可疑性等特征,其低成本和高效率的数据采集方式导致了数据体量的爆炸^③。在信息社会,企业往往通过对社会数据的分析研究,实现对网络用户的喜好、行踪、需求等分析预测,从而为企业创造更高的生产率 and 用户盈余,社会数据已成为网络时代的黄金^④。

①截至2017年,世界上已经制定个人信息保护法的国家达到120个,国际规则特别是区域性国际规则中也有关于个人信息保护的相关内容,对个人信息提供法律保护已经成为不可逆转的世界性潮流和趋势。参见:京东法律研究院著《欧盟数据宪章:GDPR评述及实务指引》(法律出版社,2018年版第2页)。

②Andrew Burt. The AI transparency paradox, Harvard Business Review, December 13, 2019. https://hbr.org/search?search_type=&term=AI+transparency+Paradox.

③Big data and privacy: A technological perspective. https://www.researchgate.net/publication/271967381_Big_Data_and_Privacy_A_Technological_Perspective.

④Andreas Weigend, Data for the People. Basic Books, 2017.

由于商业机构相对于个人在信息持有上处于优势地位,商业机构获取用户信息的基本模式以及用户的“同意让渡”行为,使其在参与网络活动中事实上将个人信息商业化了。正是由于大量的相关资料交错分析得到的信息具有巨大的经济价值,所以对个人信息的控制已经变成一种所谓的“权力”。这种“权力”的滥用有可能使得科技发展越快、越有效,对个人信息的侵害就越大。因此而致的隐私泄露、生活安宁被打破乃至数据歧视等个人信息处理负外部性就会增强。

从安全视角看,个人信息保护关乎公众信息安全,关乎社会治理体系和治理能力的提升^[9]。大数据安全问题不仅威胁个人和企业,对社会安全和国家安全也可能构成危害和影响。虽然现代社会已经建立相应的规则体系保障个人信息安全,但大数据时代这些规则都有可能成为无用的“马奇诺防线”。更为严重的是,人们面临的危险不再仅仅是对隐私的泄露,通过数据分析,人们还可能被预测到生病、拖欠还款、犯罪等,这些预测会导致其无法购买保险、无法贷款,甚至在实施犯罪前就被“预先逮捕”。如同出版印刷行业的发展推动了国家立法保护言论自由一样,大数据时代也需要新的规章制度来保卫岌岌可危的个人信息权利堡垒^[10]。所以,对个人信息予以侵权法保护应当是保障信息安全和抑制信息处理负外部性的必然选择。

(二) 大数据时代个人信息危机危及信息主体权利

信息主体的人格独立和自由遭受侵害。由于信息业者利用互联网将个人信息以不同方式加以组合或呈现,经过数字化处理,对用户的思想、信仰、性向、嗜好等加以推测,并预测其行为模式、政治态度、消费习惯,从而重塑了自然人网络上的“虚拟人格”。这种“虚拟人格”不为信息主体意志所左右,所表现的个人形象可能与个人真实人格大相径庭。“虚拟人格”产生的影响不仅仅是对个人人格特质的掌握,真正的应用是对个人的行为预测,如果“虚拟人格”的控制者和干扰者之意图并非出于善意,则会对信息主体的人格与自由构成实质上的侵害。可见,信息主体对其“虚拟人格”的无自主性决定了将其命运寄托于信息控制者的善恶,显然是对信息主体人格独立和自由的挑战。

信息主体的生活安宁权遭受影响。当前,大数据技术的应用已经使网络世界里人们几乎成为一个“透明人”。信息时代各种移动终端、微处理器和传感器悄无声息地收集着个人信息,使人们感觉到时刻被“看不见的耳朵”倾听着,被“看不见的眼睛”注视着,个人的喜好嫌恶、思想倾向等不愿透露的信息被信息业者掌握无遗,个人随时面临着各种网络精准推销和无法回避的信息骚扰,大数据时代个人生活的安宁业已被打破,精神上的安全感随时有可能被摧毁。因此而致的信息处理负外部性效应完全要个人“忍耐”,显然与“数字时代第四代人权”^[11]保护目标不相适应。

信息主体的隐私权遭受侵害。大数据时代互联网用户的各种数据,包括一些微不足道的数据,以信息技术手段加以整合后可以从中推测出用户最有价值的私人隐秘信息,如通过社交网络行为数据有可能识别出个体的性取向、政治倾向、价值观等通常意义上更为“敏感”的个人信息。保护隐私权是世界各国侵权法的共识,如果因为信息产业发展的需要赋予秘密搜集信息不受信息主体透明化要求的制约,则大数据透明化悖论就不复存在,人类发展信息产业的初衷和目的就会因此被认为“非人道、失人性”,保障数字时代人权就会成为一句空话。

信息主体的个人信息财产权益遭受损害。2018年制定并于2020年1月1日生效的美国《加州消费者隐私法案》规定了如果个人同意公司交易其信息,可获得返券、折扣等经济利益,在法律上确认了个人信息的财产权价值^[12]。表面上看,信息主体通过获得返券、折扣将自己的个人信息“让渡”的行为符合契约精神要求,但实质上却是大数据“权力悖论”显现得最为隐秘的模式。因为商业

机构、公共服务机构从个人信息的收集、处理和使用中获得了巨大的现实或潜在的财富,返券、折扣只不过是其权力的工具和信息主体牺牲权利的代价。事实上,作为信息产业链中个人信息源头的信息主体并未得到其应有的份额,反而频频遭受个人信息侵权而致的财产损失风险。当前,越来越多的关注焦点锁定在个人信息财产利益风险的议题上,需要使之与当前科技的发展达到一种平衡^[13]。必须承认,大数据悖论并非指个人信息权利保护和信息产业发展二难选择的无所适从,其研究的意旨是要探寻如何平衡和定位权利保护的程度和方式,谋求个人信息权利保护和信息产业发展的“双赢”。

(三) 必须确立个人信息权公法、私法一体化保护体系

美国欧盟等国外立法及实践经验表明,建构个人信息权公法、私法一体化保护体系是有效应对个人信息危机,切实保护个人信息权利,谋求信息权利保护及信息产业发展“双赢”的必要条件和关键举措。鉴于信息社会的个人隐私保护与公权力行使紧密联系^[14],世界上不少国家已经制定专门的个人信息保护法,确立个人信息公法保护的基本框架,其中具有典型性和代表性的有1995年《欧洲数据保护指令》(简称《1995年欧盟指令》),2018年5月25日生效的《通用数据保护条例》(General Data Protection Regulation,简称“欧盟GDPR”)。

以美国为代表的英美法系国家,以尊重信息主体隐私权为前提,遵循“公平信息实践原则”的分散立法模式。该模式肇始于隐私权保护理念,从1888年Thomas Cooley法官提出“个人独处的权利”到1965年“Whale v. Roe案”(429 U. S. 589(1977)),美国法上的隐私权观念逐步扩张,并延伸至政府和企业对个人信息的收集、使用及传播上。而且,美国的州立法层面也在不断强化个人信息保护。例如,前述美国的《加州消费者隐私法案》就堪比“欧盟GDPR”,被称为美国“最严厉、最全面的个人隐私保护法案”。

关于我国个人信息的法律保护,在《民法典》颁行前学界认为对个人信息以宪法、行政法、刑法等公法保护为先导,逐步建立以《民法总则》为基础的私法保护体系已成大势所趋^[15]。“个人信息侵权的责任救济方面,我国首先采取的是刑法制度设计已经先行一步,行政责任与民事责任的建立健全在进行之中”^[16]。2017年《民法总则》第111条虽然作出个人信息民法保护的“权利宣言”,但由于并未规定违反该规定应负的民事责任,因而当时的个人信息侵权救济仍需结合原《侵权责任法》的相关规定进行处理。尽管2017年《网络安全法》第74条规定了“违反本法规定,给他人造成损害的,依法承担民事责任”,但《网络安全法》性质上属于公法,公法规定私法的民事责任存在体制不顺,且其不能涵盖救济私法领域的各种侵权责任,尚需后续个人信息保护法的补充和完善。

具有里程碑意义的是,我国《民法典》人格权编第六章对个人信息民事权利作出了明确规定,肯定了此前的基本共识即“将个人信息权作为一种具体的人格权加以保护”^[17],而且2021年11月1日我国《个人信息保护法》的施行,标志着体系上“形成了公私法共同协力的进路”^[18]。从个人信息侵权法保护的角度看,应着重在实践中运用好《民法典》侵权责任编的相关规定以及《个人信息保护法》第69条等规定,并与现行《网络安全法》《电子商务法》等公法规范一起系统编织个人信息公法、私法一体化保护制度体系。

二、大数据悖论视阈中个人信息侵权法保护的价值定位

大数据透明化悖论、权力悖论、身份悖论决定了个人信息侵权法保护价值取向不能简单化、绝

对化,其实质是要求在个人主张信息透明化要求与信息业者秘密搜集信息、信息业者的数据特权与个人信息权利的“让渡”或牺牲、信息业者识别个人身份与个人身份隐私等博弈关系中求得优解。也即,个人信息侵权法保护价值取向不能仅仅概括为救济个人信息权遭受的侵害,其价值取向悖论的理性定位必须务实多元。

(一) 尊崇人格尊严,保障信息时代人的全面发展

法律作为人类最伟大的发明,在实现人类自我控制的征程上,只有客观反映信息科技生产力最新变化的时代要求,着眼个人全面发展和自由个性的彰显,信息主体的人格尊严和信息产业的发展才能获得“双赢”的生命力。源自自然法传统的“人的尊严”所强调的个人皆为自主、自决独立个体的观念,在民法熏陶和洗礼的过程中使得与人本身不可分离的“天生权利”成为现实,客观上奠定了法治国家私法秩序的哲学基础。

当前,个人“信息化形象”亟需侵权法保护,也只有个人信息权的权利边界定位准确、合理,侵权责任落实到位,才能真正解决大数据“身份悖论”难题。因为,信息爆炸的大数据时代互联网能够连接全世界亿万网站信息,并且事实上广泛收集和存储各类信息^[19],个人在信息化时代都形成了“数字化人格”(computer persona)^[20]。或者说,“数字化人格”塑造了个人“信息化形象”,人们在信息社会中习惯于以这种“信息化形象”来指代现实中的个人。不幸的是,“数字化人格”的形成依赖“身份识别”,信息主体的“信息化形象”受他人操控,以致与本人的实际形象可能相差甚远,而且信息技术发展越快,个人对“信息化形象”的自主权丧失得也越快。“如果个人在网络中被随意监控、分析和操纵,个人作为人的完整性和主体地位都被控制,则个人就会演变为纯粹的‘个人数据客体’,个人独立人格和尊严将直接受到挑战”^[21]。因此,保障人格尊严和自由发展应当成为个人信息侵权法保护的首要目标。

以欧洲个人信息法律保护的价值取向为例,欧洲立法者总体上偏向于维护信息主体的人格尊严,禁止个人成为纯粹的“个人数据客体”。这与欧洲人权屡遭摧残的惨痛经历不无关系。根据1789年《法国人权宣言》第4条,“自由必须无碍他人的人格”,此后欧洲法律形成的传统是,与人格尊严等基本人权相悖的行为自由不受法律保护^[22]。《1995年欧盟指令》第1条规定了“自然人的人格尊严等基本权利”是其基本宗旨,该指令第9条明确了在此基础上才应在一定程度上保护信息自由流通。“欧盟GDPR”秉承了《1995年欧盟指令》保护人格尊严的理念,在第一章“一般规定”第1.2条中对自然人的基本权利和自由,特别是其个人数据保护权的保护作了明确的规定。

欧盟各成员国在各自的个人信息立法或规范中也宣示了相同的上述立场,几乎无一例外地采用统一的个人信息保护法模式。欧盟及其成员国的立法系统而全面地规定了信息主体对其个人信息享有的权利^[23]。事实上,欧洲对个人信息侵权行为的法律规制,保证了信息主体的人格尊严成为信息自由流通所不得触碰的“边界”。从现实角度看,信息时代人的全面发展的价值取向落实与否的一个重要标准就是信息业者侵犯信息主体人格尊严的侵权责任有否被实际追究。

(二) 强化责任担当,维护信息时代的公平正义

大数据“权力悖论”优解的路径之一就是信息业者不能藉口信息产业及社会发展需要恣意强化自身的“数据特权”,恰恰相反,信息产业以及信息社会健康发展需要仰仗信息业者的社会责任担当。然而,基于利益至上的本能,信息业者“数据特权”不大可能“自省自觉”地放下身段,必须要借助外力给这个特权套上制度的笼子。实践证明,给予个人信息侵权法保护是迫使信息业者展现其

社会责任担当的关键举措。事实上,互联网的开放性、数字化特征决定了其社会属性几乎是无边界的扩大,突破了地域、国家的限制,信息已经成为一种商业资本,可以创造新的经济利益,但同时也带来了更多的威胁:对个人隐私、网络行踪、生活安宁的侵害等。诸如用户信息泄露、网络黑客勒索和通讯信息诈骗等各种网络侵权现象的增多和网络安全的脆弱化,威胁着信息时代的公平正义。互联网企业需要遵守的重要底线就是要扛起法律要求其承担的社会责任。构建完备的个人信息侵权法保护体系,对作为信息控制者或处理者的互联网企业的权利边界进行勘定,对其应当承担的责任予以明确,不仅有利于强化其社会责任意识,而且有利于网络生态的健康、可持续性发展。

所以,大数据“权力悖论”优解的直接对策就是强化信息控制者和处理者等信息业者的权责一致性。大数据时代信息的财富价值决定了信息控制者和处理者在利益最大化的诱惑面前,势必对个人信息进行最大程度的利用和推进信息最快速地流通。信息主体对其个人信息无法掌控的现状和对权利保障的渴望,势必在个人信息权利宣言的基础上呼吁对信息控制者和处理者设定侵权行为边界和越界责任的承担。为了保障信息主体的权利,个人信息侵权法保护的价值取向应当明确信息控制者和处理者的权责一致性,即信息控制者和处理者在赢取利润的同时必须强化社会责任承担,守住法律底线。

(三) 衡平各方利益,实现个人权利与信息利用的“双赢”

从公平原则出发,大数据悖论的优解应当跳出绝对化的藩篱,个人信息侵权法保护价值取向的理性定位需要围绕相关各方利益的衡平。个人信息合理使用是对自然人享有的作为人格权益的个人信息权益的限制^[24]。这决定了个人信息权利保护与信息的流动利用是对立统一的矛盾体。由于个人信息处理可能给个人带来危害,为了自保,个人会尽可能隐匿甚至伪造信息,或者减少信息产出;如果信息主体对其个人信息完全失控,势必导致信息的无序使用和质量下降,信息的真实性也难以保障,所以,必须要大力保障个人信息权益。但是,如果绝对化地强调个人信息权利保护,又极有可能使信息处理者在考量侵权与否的犹豫摇摆中影响信息流动和利用的效率。所以,法律上必须对权利保护和信息利用的“度”作出“衡平和定夺”,信息处理者作为个人信息利用的“既得利益者”,必须对其违反法律规定的侵害个人信息行为承担侵权责任。有学者甚至提出其还应对下游损害依不同情形承担连带责任、按份责任和补充责任^[25]。

事实上,个人信息的保护与利用之间存在着“零和博弈”关系,如果过于重视对个人数据信息安全的保护,则必然会影响对其在经济方面的利用,反之,如果过于重视对个人数据信息经济利益的开发,则又容易忽略对个人数据信息安全的保护^[26]。王利明教授在《民法典》颁布前就提出应当妥善平衡二者之间的关系,既要注重发挥个人信息的经济效用,也要注重保护信息主体的个人信息权利,不能因为过度保护个人信息等权利而限制了数据产业发展,也不能为发展数据产业而不考虑对个人信息等权利的保护^[27]。因此,在认定个人信息侵权行为时,应当兼顾信息主体与信息业者双方的利益。

从实证层面看,信息自由流动加速条件下,信息控制者和处理者往往会降低成本,这就意味着消费者可以得到更多更好的低价商品和服务。信息主体自身要从信息处理中受益就必须以“让渡”对个人信息控制程度为代价。事实上,这是信息流动的需要,但同时也存在信息安全的隐患。个人信息侵权法保护的制度价值既在于制裁信息业者侵害信息主体利益的行为以救济受到损害的权利,同时又在于藉此明确法律给信息自由流动利用界定侵权与否的“度”。总之,个人信息的个人价

值、社会(经济)价值和公共价值决定了我们一方面要保护个人权益,另一方面要促进个人信息流动和经济利用,以维护社会和公共利益^[28]。

在信息社会中,信息共享与开放是信息经济发展的大势所趋。著名社会学家杰里米·里夫金指出,新经济体制将应运而生,它就是协同共享,到2050年协同共享很可能在全球范围成为主导性的经济体制^[29]。依据“社区导向论”观点,“每个人都有独处与不受干扰的权利……但是将这种权利推演至极致时将导致社会义务的毁灭。这就决定了为了保障自由,在社群生活当中我们被要求放弃某些行为的自由”^[30]。所以,对个人信息的法律保护不能无条件、绝对化,应当在与公共利益的平衡中谋划和强化个人信息保护,“政策制定者在制定个人信息保护政策时,还需要考虑其他经济视角的价值,以及权衡经济视角之外的政治社会问题和消费者对隐私泄露的抗拒心理等”^[31]。根本上,个人信息值得保护的主要原因除了人格尊严的价值外,还在于其对社会存在有益性,保护个人信息理应更加有利于信息安全有序地流通,有利于构建秩序井然的网络信息社会。

根据亚里士多德“交换正义”或“矫正正义”理论,侵权法的责任和使命在于要求个人信息控制者和处理者在接受行业自律和法律规定的的前提下,加强与信息主体之间的互动合作,以对个人信息的充分保护“交换”个人信息的自由流通与利用,否则,个人信息控制者和处理者就会因为侵权行为接受“矫正正义”的审判。毕竟,信息社会背景下民主政治和“公意社会”目标实现的基础依赖于信息自由流动,个人信息保护作为基本人权的价值追求会不断强烈,成熟市场经济和完备信息社会中,“交换正义”或“矫正正义”都是包括个人信息在内的社会资源高效配置的必备手段和必要保障。

客观上,信息主体与信息业者双方利益均衡的调整和权利保障的满足是构建网络秩序的基本要素。信息社会条件下,强调利益均衡并不是要求对信息业者与信息主体之间的利益作均等化或同等化的配置,更不在于忽略或抹平相关各方之间的业已存在的利益差别与竞争,而是以利益冲突最低限度和谋求各方利益关系和谐共享为目标,在相关利益关系主体之间寻找博弈平衡点,在确保整个网络社会稳定和发展的大局下,以侵权责任制度作为“压舱石”,切实保障个人信息利益与公共利益的“双赢”。

(四)善用“负面调整”方法,寻求大数据“公权力悖论”优解

公权力悖论在于公权力“公属”性与“私掌”性的分离冲突、积极的无可替代作用和消极影响的共生并存。具体表现为公共权力的公共性与占有使用的私人性之间、中立性与决策的利益倾向性之间、公共性目标与强制性手段之间的矛盾^[32]。事实上,除了信息业者以外,政府等公权力机构是大数据“权力悖论”中掌握“数据特权”的重要一方,公法介入个人信息保护的必然性在于公权力机构必须建构“数据特权”自我约束的制度机制。客观上,信息社会中个人信息遭受来自公权力机构与非公权力之私主体的多重侵害,有必要从公法和私法两个维度对个人信息进行保护,两种保护途径殊途同归,尽管所使用的保护手段有所不同,但是其规范目的一致^[33]。

个人信息的公法保护既指国家公权力行使不能侵害个人信息权,也包含公权力机构应当积极保护个人信息。处理好个人信息与公权力保护的关系,一方面,基于“有限政府”的法治理念,政府作为权力最大的信息收集者,其掌控个人信息与介入个人隐私的权力应当受到必要的限制;另一方面,个人信息的保护客观上又需要政府的积极介入,以便其牵头组织对个人信息遭遇威胁的“系统防御”。同时,必须经由公权力针对个人信息保护进行立法,继而依法规制并通过司法权力进一步落实个人信息的法律保护。可见,大数据“权力悖论”绝不是一个伪命题,正如劳伦斯·莱斯格所言:“我们都渴望居住在

分离的群落里或分离的标准化空间中。隐私或对个人资料的控制能力支持这种渴望。这样有助于群体的多样性,不会使某个优势群体去规制和同化其他群体,使后者逐渐被人淡忘”^[34]。

私法是个人信息保护的权力宣言与行为规则。民法以对人的关怀作为其终极价值,其目标表现为对人格尊严及其个人自由发展、全面发展的维护,例如,德国民法体系实际上就是以人格尊严和自由作为中心而辐射的网状结构^[35]。民法对人的关怀在制度上体现为对民事主体的各项权利和利益的充分保障,对个人信息利益的保护主要通过权利模式和行为规制模式两种基本途径加以实现。个人信息侵权法保护的实质是私法保护的“负面调整”方法,在于以此划定公权力“数据特权”的权力边界,“负面调整”方法的落实是除公权力自我约束之外的大数据“公权力悖论”的另一优解。

“负面调整”方法之所以具有独特的生命力,在于民法是围绕着“权利、义务、责任”而展开的,民事法律关系的内容包含民事法律关系主体双方之间的权利义务关系和权利责任关系,两种关系是有序性的,实际上,总是先有权利义务关系,后有民事责任关系;后者相对于前者而言,只是一种可能性;这是由于前者对应的是原权利,后者对应的是救济权^[36]。救济权是指权利人享有的基础性民事权利受到侵害或有受到侵害的危险时,用以救助基础权利的权力;救济权的功能在于救助受损害的基础权利,是保护性的权利^[37]。通常情形下,民法在确认民事权利的同时,须配套相应的救济措施。“民事权利之所以有法律上之力,皆因有民事责任之故。民事权利因与民事责任结合,因此获得法律上之力”^[38]。

所以,民法在对民事权利进行正面法律宣示的同时,需要运用作为法律的“负面调整”方法的民事责任制度对遭到侵害的民事权利进行救济,即相对于民事权利在私法中的确认,侵权法保护是私法保护的“负面调整”方法^[39]。尽管解决大数据悖论的路径对策多元、多维,但运用上述“负面调整”方法解决信息社会中纷繁复杂的个人信息网络侵权问题,依靠个人信息侵权责任制度以切实改变信息主体的个人信息遭受侵害时难以有效维权问题,不仅有利于实现从保护个人信息到保护个人信息权的“飞跃”和升华,更在于为公权力“数据特权”划定了权力边界,为大数据“公权力悖论”寻得优解。

三、个人信息侵权法保护理据的多维审视及深度分析

国外学者一般认为大陆法系国家个人信息法律保护的理论基础聚焦于人权至上、伦理道德、公共舆论保护等方面^[40],美国个人信息权理论基础在定位于保障言论自由和表达自由的前提下,从信息隐私权角度强调个人信息法律保护^[41-42]。虽然保护人权是美欧个人信息法律保护的共同理论基础,但其具体表现、价值侧重存在思路和模式上的差异。例如,欧盟强调个人信息“自决”保护和“善”之基础,而美国则主张个人信息的“自决”不是重点,重点在于如何控制个人信息的使用,如何平衡信息“自决”与国家安全、公共利益之间的关系。我国学者论及个人信息权理论基础时大多也是从法哲学^[43]、伦理学^[44]等学科理论基础角度强调天赋人权、人本主义、人性尊严。笔者认为,大数据悖论的现实和信息产业发展的潮流决定了将个人信息权之理据仅建立在人权保护理论之上是不够的,基于数字时代人权的新特性及其信息社会的现实基础,必须恰当考量个人信息侵权法保护的“度”,在人权保护理论之外探寻个人信息侵权法保护的新理据。

(一) 个人信息侵权法保护的法经济学分析

“经济分析理论”肇始于19世纪的美国,20世纪以来该理论集大成观点见之于芝加哥大学波斯

纳教授的《法律的经济分析》,该著作运用简明经济学探讨法学领域中的特殊问题^[45]。汉德法官是采纳该理论进行裁判的著名法官,其最大的贡献在于通过1947年“United States v. Carroll Towing Co. Ltd 案”将侵权的损失通过“汉德公式”进行量化计算。“汉德公式”将侵权责任中的过失量化为数学公式,用经济分析的方式来判断行为人是否存在过失。为达到社会总成本的最低化,如果行为人为人付出的预防成本比预期事故发生的损害要低,则法院就会认定行为人应当承担采取预防措施的责任。实践中这种认定可以促使人们的行为方式朝着预防损害发生的方向转变。相反,如果行为人为人付出的预防成本高于预期事故发生的损害,则行为人会选择向受害方支付赔偿款,而不是采取预防措施。无论采取何种处理方式,都可以促使与该事故有关的社会福利达到最大化。据此,行为人是否承担侵权责任,以及如何承担责任最终取决于成本与损害孰轻孰重,这种侵权责任分配规则能够促使行为人最终选择风险与安全有效平衡配置的状态,因而在此基础上能够建构最具有法律效率与法律激励作用的侵权责任制度。可见,“经济分析理论”之核心在于确立“成本—效益”分析模式,其实质在于通过考察和减少“损失”强调社会成本控制,即“过去的事情已无法复原,我们作出是转移损失还是将损失留在原处这一决定应当考虑该选择可能导致的后果”,“正确的责任规则应当是那些可以实现最大限度地减少损失的规则”^[46]。

针对个人信息侵权的责任认定,从成本控制角度看,信息技术提供者相较于可能作为个人信息侵权的受害人而言成本更低,个人信息的控制者和处理者具有明显的成本优势,因此其应当承担相应侵权责任^[47]。客观而言,如果防止个人信息侵权最为经济有效的措施是让网络控制者或处理者承担责任,那么法律在制度设计时让其担责就是可取的^[48]。作为一个顺其自然的结论,“法律经济分析理论”中蕴含着行为人为投入的成本如果比获取的利益少,则可以增进社会的总体福利,减少社会的总损失,也即,要求信息控制者或处理者承担侵权责任是一个符合“成本—收益”分析模式的最为经济、最有效率的制度设计。

首先,应当明确私权保护比公法监控更符合信息保护的“成本—效益”原则。客观上,法律应否保护涉及个人信息的特定活动取决于两个因素:一是信息的本质与来源;二是交易成本。例如,假设窃听和其他监控形式被法律普遍允许时,人们在彼此通讯时就会考虑可能有人窃听而使得谈话小心翼翼,这样就需要付出更多成本,且更无效率。所以,为私人通讯提供私权法律保护比允许无条件的公法监控行为更加符合“成本—效益”原则。但是,如私人通讯涉及非法行为时,通常将会造成社会的成本损失,则例外允许对非法行为进行监控^[49]。

其次,应最大化地实施个人信息流动、利用及交易的成本控制。一方面,要控制个人作为信息主体参与网络活动的成本:(1)作为信息业者提供服务的对价而提供个人信息;(2)为获得更好的服务而允许信息业者记录、存储及使用自己的个人信息;(3)为获得必需的信息服务而允许信息业者收集个人信息建档;(4)选择高度保护自己的个人信息隐私可能需额外支付的费用。另一方面,要控制个人信息管理者采取事前预防措施的成本:对安全设备、安全软件的投入,因培训员工与监督措施产生的成本,信息主体因拒绝提供某些个人信息而导致的可能损失。事实上,信息业者具有强大的网络技术团队,对信息的发布、传输、监控、过滤、删除、屏蔽及断链的处理流程最为熟悉,而且技术控制区域相对集中,对网络上的各种个人信息侵权行为更容易发现与控制,并能及时组织力量有效地采取必要措施阻止侵权行为的发生或损害后果的扩大,与网络用户的侵权防控能力相比,信息业者无疑是能以最小的社会成本控制侵权损害发生的最合适的主体。

最后,社会总成本最小化应当作为个人信息侵权责任追究的终极“控制阀”。对于个人信息侵权责任承担的“成本—效益”分析而言,在成本、损失以及获利的比较过程中,个人信息管理者控制损害的发生所要付出的成本最小,实际上也对双方最为有利。个人信息管理者因预防信息泄露所采取的安全保障措施通常只需付出简单人力成本,而对于受害人而言,如果个人信息被泄露或滥用,所付出的不仅仅是财产损失,还有可能是人格权、知识产权的损失,个人信息管理者简单的人力成本无法与受害人的损失划等号。

所以,信息业者承担网络侵权责任的缘由,归根结底是其忽视管制成本或是管制成本小于侵权造成的损害。作为个人信息控制者或处理者,基于商人利益最大化原则其通过获取目标客户信息实现精准营销等市场目的时,主观上本来不愿主动保护信息主体的个人信息隐私,但是,“法律经济分析理论”的原理促使其充分认识到,如果其不采取事前保护措施可能会造成更大的损失,大数据透明化悖论在这里表现得尤为明显。所以,信息业者要获得利益最大化,基于“成本—效益”原则应当选择积极保护个人信息隐私权。

(二)个人信息侵权法保护之“危险控制理论”及“营业收益风险理论”分析

“危险控制理论”是伴随工业文明大发展,工业性灾害事故频发的时代背景而产生的。该理论认为,诸如高空、高压、高速、高辐射等活动属特殊的危险活动,由于这些技术活动为现代社会文明发展所必需,因而该危险在特定范围内为法律所允许。但是,从事这些特殊危险活动的人是“危险源”的肇始者和控制者,其对“危险源”具有一定的控制能力,“即使行为人毫无过错可言,也缺乏道德上的可非难性,但是基于分配正义的要求,仍需承担损害赔偿赔偿责任”^[50]。“营业收益风险理论”由法国的萨莱伊和约瑟兰德所倡导,是在“危险控制理论”基础上发展起来的针对企业经营者责任的理论。该理论认为,由于营业或物件的管理人从营业或物的积极作用中获得了利益,基于从其营业及物件中所获得利益的抵偿原理,法律要求产生危险的营业或物件管理人就其经营营业及管理物件所导致的损害后果承担侵权责任^[51]。

可见,作为企业经营者之所以要承担侵权责任的基础原因是基于其开启或维持了“危险源”,更为重要的是,从“危险源”中获得了利益是其应当担责的根本原因,根据收益与风险对等的原理,由在经营中获得利益的一方承担相应营业风险天经地义。从客观上看,适度加重其责任符合公平正义要求。事实上,掌握大数据运用能力与算法技术的商业组织是一种“准公共权力”性质的机构^[52]。从宏观层面上讲,让这些经营者承担损害赔偿的经营风险也会改善消费环境,提高参与消费人群的消费热情,使作为一个整体的经营者群体在长远利益上更容易获得更大的营业收益,最终仍然是有利于经营者群体的,也符合“矫正的公平正义”要求^[53]。因此,“营业收益风险理论”推动了经营者的安全保障义务得以最终确立。

客观而言,大数据社会是以一种更加巧妙、柔和、不会引起疼痛的方式将人类个体置于其统治之下,自然人所拥有的认知水平与迅猛发展的信息科技之间的鸿沟越来越难以逾越,信息富有者和信息贫乏者之间存在着日益分化并不断扩大的“数字鸿沟”(Digital Divide)^⑤,这事实上导致了信息社会中的“信息侵害危险源”比“工业性灾害危险源”可能有过之而无不及。所以,无论是基于分配

^⑤数字鸿沟是指拥有信息工具人与未曾拥有者之间存在的鸿沟,这个概念最早是1999年“美国国家远程通信和信息管理局(NITIA)”在其发布的《在网络中落伍:定义数字鸿沟》报告中提出的。

正义还是矫正正义,以个人信息侵权责任控制“信息侵害危险源”十分必要。

当前,客观上隐藏着诸多“危险源”的大数据技术事实上已经成为信息时代决策的有力武器,特别是在公权力利用“危险源”侵害个人信息权的场合,更需要以个人信息侵权责任制度划定公权力的“边界”。另外,信息业者的安全保障义务之所以不能因为网络的“虚拟性”也跟着“虚拟”,根据“营业收益风险理论”的重要缘由,就是他们从中获取的利润有时呈突变几何级数增长。例如,在美国2008年大数据这个词才刚被收录进词典,全球数据交易额就达到了89亿美元,此后每年以40%的速度递增,2016年已超过了240亿美元^[54]。

所以,以“危险控制理论”和“营业收益风险理论”作为大数据时代个人信息侵权法保护的理据缘起于分配正义的要求,赓续于矫正正义的嬗变,博弈于大数据悖论的现实优解。大数据时代,控制“信息侵害危险源”不仅在信息安全技术上是必要的,而且在信息社会的法律规制上也是必须的,获取营业收益与承担安全风险本来就是公平正义的题中应有之义。

(三) 个人信息侵权法保护的“企业社会责任理论”分析

“企业社会责任理论”认为,保障服务对象利益是信息企业社会责任应有之义。因为现代企业的经济力量存在的重要价值就在于其本身蕴含社会义务,现代企业既是一个谋求利润的利益聚合体,同时又是一个承载解决社会问题,保障服务对象利益的力量贡献体。企业主体从客体获得利益就必须承担与之对应的义务,企业履行其社会责任具有正当性与该当性^[55]。所以,信息企业作为最具有代表性和未来性的现代企业,其所有者与经营者不应仅仅将谋取股东利益最大化作为企业的唯一目标,为了担当企业社会责任,除了增进股东利益之外还应当最大限度地保护包括职工利益、消费者利益、债权人利益、环境利益、社区利益、社会弱者利益在内的多种利益以及整个社会公共利益。必须围绕个人信息的利用行为构建信息处理者与信息主体之间的权利义务关系,防范个人信息处理行为侵害主体权益的风险,并在侵害行为发生时予以纠正和救济^[56]。

针对信息控制、处理、利用的信息企业而言,承担侵权责任是实现其社会责任“矫正正义”的关键。从长期战略出发,企业承担社会责任的收益远大于其投入,由此积累的声誉能够形成企业无形资产,使企业维持长久的竞争优势,并在市场中占据有利的竞争力地位^[57]。信息企业在提供社会公众服务时,其服务内容作为促进社会利益与人民福祉的重要组成部分,其不应当具有对信息主体造成利益损害的服务缺陷,亦负有对个人信息所涉及的合法权益提供安全、可靠保障的义务。如果信息企业存在侵害信息主体利益的行为,则不仅需要及时纠正其社会责任主体意识的认识不到位,更要通过让其承担个人信息侵权责任来实现“矫正正义”,以确保与企业社会责任相称的社会利益保护真正落到实处。所以,这就决定了实践中需要发挥侵权法的利益协调作用,平衡个人信息保护与信息产业发展的需要^[58]。

从发展趋势看,提供网络服务的中间服务商逐渐成为信息社会的核心圈企业,影响人类社会生产与生活的方方面面,社会利益与人民福祉对这些网络企业的依存度越来越高,信息企业的社会责任也随之越来越大,尤其是对网络安全、网络秩序、网络文明、网络维权的社会责任会处于更加突出的位置。当前,个人信息权利保障问题比以往任何时代都更为突出,必须着力强化信息业者的社会责任意识,完善其承担社会责任的法律制度设计,落实其个人信息侵权责任承担,确保个人信息保护成为互联网企业社会责任的“头等大事”。

四、结语

人的本质是各种社会关系的总和,大数据时代个人信息不仅是社会关系的纽带,而且是互联网空间的重要资源。构建我国更加完备的个人信息保护的民事法律体系,一方面使个人的信息权益得到充分的保护,另一方面使个人信息在数字经济中的意义得以充分体现^[59]。实践证明,大数据悖论不应成为个人信息权利保护、政府信息治理权力、信息产业发展间“非零和博弈”的“共赢”目标之障碍,作为源流之诱因反而要求对个人信息侵权法保护的价值及理据进行重新审视和深度分析。个人信息侵权法保护的价值不仅在于救济信息主体遭受损害的权利和筑牢个人信息权利的边界,还在于制约公权力可能对个人信息的恣意和滥用,对信息业者利用个人信息予以明确规范和提供“负面调整”的方向警示。

个人信息侵权法保护理据的多维分析显示,人权保护理论是个人信息侵权法保护的基石,必须强化以数字人权为标志的“第四代人权”,个人信息侵权责任制度能够担纲个人信息私权保护的“压舱石”;经济分析理论、危险控制理论、营业收益风险理论、企业社会责任理论又赋予了个人信息侵权责任制度在大数据时代个人信息权、政府公权力、信息产业相关方之间进行利益衡平的新使命。应当围绕实现公法和私法路径个人信息保护功能的充分发挥目标,协调二者角色定位,避免冲突和内耗^[60]。事实上,个人信息侵权责任制度完善与否已经成为衡量个人信息公法、私法一体化保护制度体系和治理能力现代化的重要标尺,个人信息法律保护对数字时代人格尊严的终极关怀必将在大数据悖论不悖之时、个人信息相关方博弈优解之际迎来真正的权利春天。

参考文献:

- [1]申卫星.论个人信息权的构建及其体系化[J].比较法研究,2021(5):1-13.
- [2]胡朝阳.大数据背景下个人信息处理行为的法律规制:以个人信息处理行为的双重外部性为分析视角[J].重庆大学学报(社会科学版),2020(1):135-145.
- [3]王骥.新未来简史:区块链、人工智能、大数据陷阱与数字化生活[M].北京:电子工业出版社,2018:18.
- [4]RICHARDS N M, KING J H. Three paradoxes of big data[J]. Stanford Law Review, 2013, 5.
- [5]闫坤如.大数据的共享-隐私悖论探析[J].大连理工大学学报(社会科学版),2020(5):15-20.
- [6]叶娟丽,徐琴.去中心化与集中化:人工智能时代的权力悖论[J].上海大学学报(社会科学版),2019(6):1-12.
- [7]张道坤.浅谈大数据时代的三大悖论[J].电子世界,2014(19):184.
- [8]卢西亚诺·弗洛里迪.第四次革命[M].王文革,译.杭州:浙江人民出版社,2016:15-16.
- [9]潘静.个人信息的声誉保护机制[J].现代法学,2021(2):155-170.
- [10]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,2013:22.
- [11]张文显.无数字,人权:在2019年5月25日“知识产权与相关权利的法理”学术研讨会暨“法理研究行动计划”第八次例会上的致辞[EB/OL].(2019-05-26)[2020-03-08].<http://www.aisixiang.com/data/116468.html>.
- [12]DETERMANN L. Analysis: The California Consumer Privacy Act of 2018[EB/OL].(2018-07-02)[2020-03-12].
<https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/>.
- [13]翁逸泓,廖福特.私生活之权利[M].台湾:新学林出版股份有限公司,2014:3.
- [14]王秀哲.信息社会个人隐私权的公法保护研究[M].北京:中国民主法制出版社,2017:1.
- [15]叶名怡.个人信息的侵权法保护[J].法学研究,2018(4):83-102.
- [16]刁胜先.个人信息网络侵权归责原则的比较研究:兼评我国侵权法相关规定[J].河北法学,2011(6):92-98.
- [17]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(4):62-72.
- [18]汪庆华.个人信息权的体系化解释:兼论<个人信息保护法>的公法属性[J].环球法律评论,2022(1):69-83.

- [19] THOMAS D, LOADER B. Cybercrime[M]. London and New York: Routledge, 2000: 10.
- [20] 齐爱民. 拯救信息社会中的人格: 个人信息保护法总论[M]. 北京: 北京大学出版社, 2009: 32.
- [21] 郭瑜. 个人数据保护法研究[M]. 北京: 北京大学出版社, 2012: 83-84.
- [22] WHITMAN J Q. The two western cultures of privacy: Dignity versus liberty[J]. The Yale Law Journal, 2004, 113: 1151-1221.
- [23] 张才琴, 齐爱民, 李仪. 大数据时代个人信息开发利用法律制度研究[M]. 北京: 法律出版社, 2015: 34-35.
- [24] 程啸. 论我国民法典中的个人信息合理使用制度[J]. 中外法学, 2020(4): 1001-1017.
- [25] 谢鸿飞. 个人信息处理者对信息侵权下游损害的侵权责任[J]. 法律适用, 2022(1): 23-36.
- [26] 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(4): 91-109, 174.
- [27] 王利明. 数据共享与个人信息保护[J]. 现代法学, 2019(1): 45-57.
- [28] 高富平. 论个人信息处理中的个人权益保护: “个保法”立法定位[J]. 学术月刊, 2021(2): 107-124.
- [29] 杨培芳. 挽在一起的手: 协同互利新经济哲学[M]. 北京: 人民邮电出版社, 2016: 7.
- [30] NIZER L. The right of privacy: A half century's developments[J]. Michigan Law Review, 1941, 39(4): 526.
- [31] 李三希, 武琦璠, 鲍仁杰. 大数据、个人信息保护和价格歧视: 基于垂直差异化双寡头模型的分析[J]. 经济研究, 2021(1): 43-57.
- [32] 张振华. 公共权力: 悖论、异化与制约[J]. 云南行政学院学报, 2004(3): 34-37.
- [33] 迪特尔·施瓦布. 民法总论[M]. 郑冲, 译. 北京: 法律出版社, 2006: 67.
- [34] 劳伦斯·莱斯格. 代码2.0: 网络空间中的法律[M]. 李旭, 沈伟伟, 译. 北京: 清华大学出版社, 2009: 237.
- [35] 王利明. 民法的人文关怀[J]. 中国社会科学, 2011(4): 149-165, 223.
- [36] 丁海俊. 论民事权利、义务和责任的关系[J]. 河北法学, 2005(7): 118-121.
- [37] 韩松. 民法总论[M]. 3版. 北京: 法律出版社, 2017: 257.
- [38] 梁慧星. 民法总论[M]. 5版. 北京: 法律出版社, 2017: 85.
- [39] 李显冬, 杨怀智. 论消费者权益保护法之本质[J]. 海峡法学, 2011(1): 46-52, 74.
- [40] Van DIJCK J. Facebook as a tool for producing sociality and connectivity[J]. Television & New Media, 2012, 13(2): 160-176.
- [41] SCHWARTZ P M. The EU-U. S. privacy collision: A turn to institutions and procedures[J]. Harvard Law Review, 2013.
- [42] REIDENBERG J R. Resolving conflicting international data privacy rules in cyberspace[J]. Stanford Law Review, 2000.
- [43] 张莉. 个人信息权的法哲学论纲[J]. 河北法学, 2010(2): 136-139.
- [44] 陈仕伟, 黄欣荣. 大数据时代隐私保护的伦理治理[J]. 学术界, 2016(1): 85-95.
- [45] 张玲燕, 陈红兵, 甘德怀. 法律的经济分析理论探析[J]. 法制现代化研究, 1999: 667-689.
- [46] 格瑞尔德. J. 波斯特马. 哲学与侵权行为法[M]. 陈敏, 云建芳, 译. 北京: 北京大学出版社, 2005: 229.
- [47] 吴汉东. 论网络服务提供者的著作权侵权责任[J]. 中国法学, 2011(2): 38-47.
- [48] 万柯. 网络等领域垄断看门人的替代责任[J]. 环球法律评论, 2011(1): 23-37.
- [49] 谢永志. 个人数据保护法立法研究[M]. 北京: 人民法院出版社, 2013: 31.
- [50] 熊进光. 侵权行为法上的安全注意义务研究[M]. 北京: 法律出版社, 2007: 201.
- [51] 张民安. 法国侵权责任根据研究[M]//吴汉东. 私法研究(第3卷). 北京: 中国政法大学出版社, 2003: 345-376.
- [52] BALKIN J M. Free speech in the algorithmic society: Big data, private governance, and new school speech regulation[J]. SSRN Electronic Journal, 2017.
- [53] 张新宝. 侵权责任法原理[M]. 北京: 中国人民大学出版社, 2006: 273.
- [54] 马尔克·杜甘, 克里斯托夫·拉贝. 赤裸裸的人: 大数据、隐私和窥视[M]. 杜燕, 译. 上海: 上海科学技术出版社, 2017: 8.
- [55] 彭慧茹. 经济法视野下企业社会责任探究[J]. 经济师, 2021(4): 81.
- [56] 高富平. 个人信息处理: 我国个人信息保护法的规范对象[J]. 法商研究, 2021(2): 73-86.
- [57] 张月玲, 邓永杰, 王晴. 企业社会责任、媒体关注与企业竞争力[J]. 山东科技大学学报(社会科学版), 2021(2): 51-61.
- [58] 陈吉栋. 个人信息的侵权救济[J]. 交大法学, 2019(4): 40-53.
- [59] 乔榛, 蔡荣. 《民法典》视域下的个人信息保护[J]. 北方法学, 2021(1): 38-45.
- [60] 杨帆, 刘业. 个人信息保护的“公私并行”路径: 我国法律实践及欧美启示[J]. 国际经济法学刊, 2021(2): 48-70.

On the value and theory basis of personal information protection in tort law: Analysis perspective based on big data paradox

LIU Liping

(*School of History and Public Administration, Yancheng Teachers University, Yancheng 224007, P. R. China*)

Abstract: In order to effectively deal with the conflict between the protection of personal information and the development of information industry, which caused by the development of information technology, we must innovate and optimize the system design of personal information protection in tort law, affirm the right of personal information to be protected, limit the right of exclusive control of the information subject, check and balance the “data power” of information processors, so as to restrain the arbitrariness and abuse of power of personal information processors, and seek for the “win-win” for the protection of human rights in information era and the built-in development space for the information industry. From the perspective of big data transparency paradox, power paradox and identity paradox, as a matter of fact, there are both positive and negative externalities in personal information processing. It determines that the legal protection of personal information should not only rely on the “rights-based approach”, but also directly face the cognitive and structural difficulties in the era of big data, and reconstruct the path of the legal protection of personal information by using the “risk-based approach”. The big data paradox determines that the tort law protection value orientation of personal information should not be simplified and absolute. Its essence is to seek an optimal solution in the game relationship between the secret collection and processing of information by information processors and the personal assertion of information transparency, the data privilege of information processors and the “transfer” or “sacrifice” of personal information rights, the identification of personal identity by information processors and the privacy protection of personal identity. Hence, the value orientation of personal information protection in tort law should not only be to maintain the personal dignity of citizens and guarantee human rights in the digital age, but also be to balance the orderly flow of information, cross-border transactions and various interests in the development of information industry. The big data paradox should not become an obstacle to the “win-win” goal of the “non-zero sum game” among the protection of personal information rights, the power of government information governance, and the development of the information industry. As an inducement of the source, it requires that the value orientation of personal information protection in tort law lies not only in the relief of damage suffered by information subject and the strengthening of boundaries of personal information rights, but also in restricting the possible infringement of personal information from public power, and clearly regulating the use of personal information by information operators and providing direction warnings of “negative adjustment”. Therefore, the theory reasons for the protection of personal information in tort law are not limited to the theory of human rights protection, but also from multi-dimensional perspectives such as economic analysis theory, risk control theory, business income risk theory and corporate social responsibility theory. From the perspective of the above theories, the personal information tort liability system should become the “ballast stone” of personal information private law protection in the era of big data. In fact, the perfect system of personal information tort liability should be an important yardstick to measure the personal information integration protection system using public and private law at the same time and the modernization level of its governance ability.

Key words: personal information; infringement; value; theoretical support; big data paradox

(责任编辑 胡志平)