

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

汪庆华

内容提要:《个人信息保护法》是数字时代个人信息保护的基本法。它采取了将个人信息权作为新兴公法权利的思路,确立了完整的个人信息权利保护体系,在个人信息保护问题上和《民法典》一起形成了公私法共同协力的进路。《个人信息保护法》以权利束的方式规定了个人信息主体的知情权、决定权、查阅权、复制权、更正权、删除权、可携带权和信息权利救济权等。《个人信息保护法》从立法依据、权利体系、条文设计和规制措施上都体现出鲜明的公法属性,这也可以从基本权利的双重面向和个人信息国家保护义务得到理论上的证成。这部法律是数字时代公法秩序的基石,它对公法边界的形塑仍需通过其实施来确立。

关键词:个人控制 个人信息权 国家保护义务 公法属性

汪庆华,北京师范大学法学院教授。

在《个人信息保护法》通过前,我国学界就个人信息保护达成了广泛的共识,但在具体进路上存在一定分歧。部分学者主张采取私法的模式,^[1]另有学者主张采取公法的模式,^[2]也有学者倡导公私法共同协力的综合进路。^[3]持私法保护进路的学者或主张将个人信息保护置于一般人格权之下,或认同个人信息商品化的实践将个人信息财产化,在救济方式上采取侵权救济的模式。这一观点最终为《民法典》所吸收,“人格权编”专章规定了“隐私权和个人信息保护”。持公法保护模式的学者认为,个人信息保护的私法模式存在困境,需借助公法机制才能够实现超越。个人信息保护的规范基础是“八二宪法”

[1] 参见王成:《个人信息民法保护的 mode 选择》,《中国社会科学》2019 年第 6 期,第 124 - 146 页;叶名怡:《个人信息的侵权法保护》,《法学研究》2018 年第 4 期,第 83 - 102 页。

[2] 参见丁晓东:《个人信息私法保护的困境与出路》,《法学研究》2018 年第 6 期,第 194 - 206 页。

[3] 参见程啸:《民法典编纂视野下的个人信息保护》,《中国法学》2019 年第 4 期,第 26 - 43 页。程啸指出,个人信息的民法保护具有重要意义,但个人信息保护需采取公法和私法并重的综合性方法。

确立的人格尊严条款。应确立公法意义上的个人信息权利,建立与数字时代发展相兼容的风险管理导向、激励相容的个人信息保护制度。^[4] 基于公法视野的个人信息权利,在救济模式上可以采取多元化的方式,在个案侵权救济之外,更需要结合风险规制的手段,综合采取行政执法、公益诉讼等其他方式。^[5] 此外,个人信息保护公法进路带来的最大意义在于,它不仅约束私人主体的信息处理行为,更进一步约束政府行为,从而构成个人信息保护的周密全面的体系。

一 个人信息权的宪法规范基础

中华人民共和国第十三届全国人大常委会第三十次会议于 2021 年 8 月 20 日通过了《中华人民共和国个人信息保护法》,在立法上对上述个人信息保护模式的争论进行了回应。《个人信息保护法》第 1 条规定,“……根据宪法,制定本法。”^[6]《个人信息保护法》的法源在于《宪法》,而并不在于《民法典》,^[7]这一条款是《个人信息保护法(三审稿)》增加进去的,《个人信息保护法》之前的《网络安全法》和《数据安全法》都没有采用这一表述。2021 年 8 月 13 日,全国人大常委会法工委发言人在介绍有关立法工作的记者会上详细说明了增加这一规定的理由:“我国宪法规定,国家尊重和保障人权,公民的人格尊严不受侵犯,公民的通信自由和通信秘密受法律保护。制定实施本法对于保障公民的人格尊严和其他权益具有重要意义。据此,拟在草案第一条中增加规定‘根据宪法’制定本法。”^[8]这一说明可以被理解成《个人信息保护法》第 1 条的原意解释。全国人大常委会法工委的上述说明明确了《个人信息保护法》的宪法规范基础:人权条款、人格尊严条款、通信自由和通信秘密条款。在法律性质上,《个人信息保护法》是公法。在法律位阶上,其为个人信息保护的基本法。^[9]这三个条款构成了公民个人信息权的规范基础,个人信息权也从未经列举权利成为实证法意义上具有基本权利属性的公法权利。^[10]在公法权利保护进路上,采取的是和宪法隐私权相区分的个人信息权保护模式。

(一) 人权条款是个人信息权作为公法权利的理论基石

“八二宪法”制定之时,将“公民基本权利和义务”一章提到“国家机构”一章的前面,

[4] 参见周汉华:《探索激励相容的个人信息治理之道——中国个人信息保护法的立法方向》,《法学研究》2018 年第 2 期,第 3-23 页。

[5] 关于侵权救济和风险自担规制关系的讨论,参见 Steven Shavell, *Liability for Harm versus Regulation of Safety*, 13 *The Journal of Legal Studies* 357, 357-374 (1984)。

[6] 关于这一表述的规范意涵的讨论,参见叶海波:《“根据宪法,制定本法”的规范意涵》,《法学家》2013 年第 5 期,第 20-33 页;杜苏:《“根据宪法,制定本法”:一个“中国特色”条款的起源、演进与分布规律》,《澳门法学》2021 年第 2 期,第 103-119 页。

[7] 关于个人信息保护的宪法基础,参见王锡锌、彭聿:《个人信息保护法律体系的宪法基础》,《清华法学》2021 年第 5 期,第 6-24 页。

[8] 张维炜、陈珊:《个人信息保护法草案等 15 部法律案将提请本次常委会会议审议》,http://www.npc.gov.cn/npc/kgfb/202108/de67efbe04e143e59a544f7e5ea9ad43.shtml,最近访问时间[2021-12-15]。

[9] 参见周汉华:《个人信息保护的法定定位》,《法商研究》2020 年第 3 期,第 44-56 页。

[10] 参见孙平:《系统构筑个人信息保护立法的基本权利模式》,《法学》2018 年第 4 期,第 67-80 页。

在公民基本权利保护问题上采取了列举式规定,规定了公民的平等权、言论自由、宗教信仰自由、人格尊严、人身自由、劳动权、教育权等具体权利。2004年宪法修改增加了“国家尊重和保障人权”的内容,人权条款入宪使得我国宪法公民基本权利保护从列举式的保护变成了“概括+列举式”的保护。人权是人之为人所应当享有的权利。从这一定义出发,人权条款具有自然法的意涵。尊重和保障人权成为宪法规范,则意味着人权的实证化。基于规范结构,除了《宪法》明确列举的权利之外,人权条款赋予了理论上主张宪法上未列举基本权利的空间。^[11]但是在主张宪法未列举权利或者新兴权利之时,需要在作为基本权利一般条款的人权条款之外,寻找其他的宪法规范基础。以人权条款作为未列举权利的单一基础,将使得人权条款的实质内容被抽空,从而失去其规范效力,导致权利泛化。^[12]而个人信息权的宪法规范除了人权条款之外,直接关联的条款是《宪法》第38条的规定。

(二)人格尊严是个人信息权作为积极权利的规范依据

“八二宪法”第38条规定了公民的人格尊严不受侵犯,这一条款是公民个人信息权的内在根据。在人权条款入宪之前,这一条也被认为具有宪法基本权利一般条款的地位,《德国联邦基本法》(Grundgesetz)人的尊严条款往往作为理解其在宪法基本权利体系所具有功能的参照。2004年人权条款入宪之后,“八二宪法”的人格尊严成为了具体的宪法权利,不再承担基本权利一般条款的使命。但这一宪法规范在数字时代具有了新的内涵和外延。由于个人信息可以直接或者间接辨识个人身份,其滥用和盗用将会对个人的人格形成极大的伤害,而生物特征信息、行踪信息、金融信息、敏感个人信息更是涉及个人的主体性的建构,对其保护必须要采取一种更为严格的模式。个人信息保护的客体是个人信息,但其目的在于实现基于个人信息建构的个人身份的自治、自主和自足。^[13]个人尊严作为个人信息权的规范依据,夯实了以个人数字身份建构社会秩序的宪法基础。^[14]

由于信息通讯技术的发展,个人信息被广泛地采集、利用、分析和共享,大规模的信息处理成为平台经济的日常实践,可以说整个互联网经济的运行模式就是建立在个人信息的商业化之上的。人们利用互联网或应用程序点播歌曲、观看视频、购买商品服务、刷朋友圈,日常生活普遍地嵌入到网络世界中。由于网络效应,用户越多的平台越能够吸引用户,而用户要退出平台则承担着巨大的不方便和不利益。^[15]在个人信息被商品化的同时,个人和平台之间的地位产生了极大的落差。^[16]

用户和平台之间存在着三个方面的“不均衡”:信息收集能力不均衡、信息处理能力

[11] 关于人权保障条款作为未列举宪法权利规范依据的综合性研究,参见余军著:《未列举宪法权利:论据、规范与方法》,中国政法大学出版社2017年版。

[12] 对各种权利入宪的批评,参见姜峰:《权利宪法化的隐忧》,《清华法学》2010年第5期,第51-63页。

[13] 参见陆青:《数字时代的身份建构及其法律保障》,《法学研究》2021年第5期,第3-23页。

[14] 参见付新华:《个人信息权的权利证成》,《法制与社会发展》2021年第5期,第129-131页。

[15] 参见冯恺:《个人信息选择退出机制的检视与反思》,《环球法律评论》2020年第4期,第148-165页。

[16] See Van den Hoven, Information Technology, Privacy, and the Protection of Personal Data, in J. Van Den Hoven and J. Weckert (eds.), *Information Technology and Moral Philosophy*, Cambridge University Press, 2008, pp. 301-322.

不均衡、社会影响力不均衡。^[17] 平台基于个人信息对用户进行画像描绘,并对个人进行个性化的商品、服务和新闻信息的推送,数据、算法和平台共同形塑了用户的认知,常规性、持久和普遍地影响用户的行为,平台成为了用户选择的架构,用户的自主性受到一定程序的限制和侵蚀。^[18]

大规模信息处理背景下个人和平台等信息处理者关系的不均衡是个人信息保护法要回应的基本事实。要打破个人和平台之间的这种不均衡,必须要恢复个人信息主体在信息关系中的能动的主体地位,使得个人在算法决策的时代能够具有自主性,而不是成为算法决策的被动对象。个人信息的处理必须要在个人信息主体知晓和控制的闭环中。《个人信息保护法》关于个人信息权的具体规定体现了个人对于信息的控制和自我决定,这使得个人信息权具有鲜明的积极权利的色彩。这一积极权利的向度无法单纯由民法保护的方式来实现,它决定了个人信息保护权的内在公法属性。

不宁唯是,在数字经济条件下,个人和平台的不均衡藉由以个人控制为中心的赋权体系仍嫌不足,需要在“个人—平台”之外增加政府的维度,由其直接介入个人平台的信息关系;个人信息权利不仅为个人信息处理者和控制者设定义务,而且从具有社会意涵的积极权利的功能出发,为国家设定了保护义务。^[19] 在国家保护义务理论之外,平台也被看成社会公权力的新兴形态,平台成为了政府监管的重要工具,获得政府的授权或委托,事实上行使着一定的公权力,监管平台并通过平台监管成为平台经济中的常态。此外,平台在资本、信息、资源等方面相对于用户的支配力意味着平台不能被看作一般意义上的私主体。^[20] 有必要重构传统的国家—个人二元的公法分析框架,形成“国家—个人—平台”这样的三维分析框架。更有学者认为,平台成为社会公权力主体,基本权可以对其发生直接效力。^[21] 这类理论假设具有非常重要的实践意义,对于数字领域的立法、数据要素市场的设立、知情同意的建构、个人信息保护的国家角色都将带来新的理解和突破。为了回应互联网平台的社会控制力和支配力,实现平台治理的有效性,《个人信息保护法》为大型互联网平台设定了个人信息保护的特别义务。^[22]

个人信息权具有两个层面的积极权利属性。道德哲学层面上,个人信息权属于伯林(Isaiah Berlin)的消极自由和积极自由划分中的积极自由。个人信息权源于个人成为自己主人的愿望。个人是个人信息的主体,而不是客体。个人信息主体受自身理性的、有意

[17] 从消费者保护角度出发,对这种不平等信息关系应进行公法规制的论证,参见应飞虎:《消费者立法中的信息工具》,《现代法学》2019年第2期,第119-136页。

[18] See Abbey Stemler, Joshua E. Perry, Todd Haugh, The Code of Platform, 54 *Georgia Law Review* 605, 625-633 (2020).

[19] 参见王锡锌:《个人信息保护的国家义务》,《中国法学》2021年第1期。关于国家保护义务理论在德国法上经由判例和学说形成的历史、基本内容和构成要件的讨论,参见王进文:《基本权利国家保护义务的疏释与展开》,《中国法律评论》2019年第4期。

[20] See K. Sabeel Rahman, Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities, 2 *Georgetown Law Technology Review* 234, 242-246 (2018).

[21] 参见李海平:《论基本权利对社会公权力的直接效力》,《政治与法律》2018年第10期,第109-123页。

[22] 参见张新宝:《互联网生态“守门人”个人信息保护特别义务研究》,《比较法研究》2021年第3期,第11-24页。

识的目的驱动,而不是为影响到信息主体的外在动因所驱动。这一积极自由是个人自我实现、自我成就的权利,是个人信息权形塑人格的功能。^[23]此外,基于宪法权利分类上的自由权利和经济社会文化权利的二分法,个人信息权又接近于需要政府提供设施和支持框架的积极权利。

个人信息主体权利的实现必须要借助政府设定的网络信息法律架构。^[24]这是个人信息个人控制和社会控制争论的起源。^[25]在个人信息社会控制面向上存在两种观点:一种认为信息的价值在于流通,为此目的,在个人信息控制问题上,存在着个人和平台这两个主要的主体,要承认平台的控制权力以及这种控制所带来的商业上的价值。这仍然侧重于个人信息的财产权保护路径,只是在此基础上强调平台处理者对于企业数据的财产权拥有权利;另一种观点则认为基于大数据技术条件,个人对于数据的收集和利用无法有效实施控制,因此私法保护无法对其作出有效回应,应当由政府专门机构将个人信息作为公共物品来规制,其法律性质是公法而不是私法。^[26]个人信息个人控制更偏向于基本权利进路,社会控制则倾向于功利主义的市场进路。有学者认为应当根据数字技术的发展,超越这种二元主义的划分,提出基于风险的数据规则和场景化的企业合规规范。^[27]

(三) 个人信息权进一步丰富通信自由和通信秘密内涵

“八二宪法”第40条规定了公民的通信自由和通信秘密,这一条款为个人信息处理划定了外部边界和底线。通信包括邮政通信和电子通信,具体指书信、电报、电话、传真、电子邮件、即时通讯等。宪法上的通信最初仅限于邮政通信,并不包括电子通信。随着技术的发展,基于合目的性解释,通信自由和通信秘密所指向的通信权应当同时包括电子通信、即时通讯等当代最常见的通信方式。个人通信的内容信息,不仅作为一般私人主体的平台无权收集,即便是公权力机关也必须按照宪法明确的方式、由宪法指定的机构才可以进行检查。^[28]通信自由和通信秘密在我国宪法列举的公民基本权利中受高位阶的保护,对于公民通信自由和通信秘密的限制性措施属于特别法律保留。在宪法明确列举的基本权利中,如果只是泛泛地规定依据法律可以进行限制,属于一般法律保留。对于公民通信自由和通信秘密的限制,则是在宪法上明确了限制的主体、理由和方式,因此属于特别法律保留。除国家安全机关和公安机关为了国家安全或者追查犯罪的需要,依法对通信进行检查外,任何组织和个人不得以任何理由侵犯公民的通信自由和通信秘密。而在现实中,限制的主体、条件和方式这三个要件,有一个不能满足就有违宪之虞。“八二宪法”第40条的规定特别具体、明确,与宪法条款的普遍、抽象和概括形成了鲜明对比。

[23] 参见[英]以赛亚·伯林著:《自由论》,胡传胜译,译林出版社2003年版,第200、211-214页。

[24] 参见王锡锌:《个人信息保护的国家义务》,《中国法学》2021年第1期,第845页。

[25] 参见郭瑜著:《个人数据保护法》,北京大学出版社2012年版,第208页。

[26] 参见吴伟光:《大数据技术下个人数据信息私权保护论批判》,《政治与法律》2016年第7期,第116-132页。

[27] 参见谢尧雯:《基于数字信任维系的个人信息保护路径》,《浙江学刊》2021年第4期,第72-84页。

[28] 参见秦小建:《新通信时代公民通信权的实践争议与宪法回应》,《政治与法律》2020年第7期,第85-97页。

随着技术的发展,公民通信的样态已经发生了根本性的变化。智能手机是具有强大存储功能的微型电脑,对于手机的搜索扣押、电子取证必须要符合正当程序、比例原则等公法原则的约束。^[29]手机中的信息包含短信、彩信、通讯录、^[30]各种社交软件中的交流内容、相片、网络浏览记录、各种文件。对于手机存储信息的不当获取将会对个人的通信权构成极其严重的侵犯。宪法关于公民隐私权的规定如何回应新的技术发展,是各国宪法在新的信息通讯技术条件下面临的普遍问题。美国在卡朋特诉美国一案中认定,关于公民手机通话时的位置、通话次数、通话时长以及具体的通话时点等通讯记录属于美国宪法保护的隐私权的内容。^[31]而通话记录等元数据是否数据通信自由和通信秘密保护的范畴,在我国学界引发了一定的争论。^[32]由于通信元数据的信息要远远超过纸面信封所能提供的信息,通话记录本身就是通信内容的一部分,^[33]而手机实时定位信息^[34]是个人行踪信息的表现形式,它们都应当受通信自由和通信秘密的保护。^[35]

如果没有了信息安全的保障,通信自由和通信秘密都将无从实现,这一宪法基本权利将成为一种空洞的希望。在数字时代,信息安全是通信自由权得以实现的技术前提。尤其要关注个人信息安全已经跃迁到网络安全和算法安全,公民通信自由和通信秘密是在这样的三重安全架构之下展开的基本权。

二 个人信息权的确立与权利体系

《个人信息保护法》第四章专章规定了个人信息主体在信息处理活动中具有的各项具体权利,确立了完整的个人信息权利体系,个人信息权也从实然权利转变成应然权利,从背景性权利转变成制度性权利。^[36]《个人信息保护法》以权利束(bundle of rights)的方

[29] See Matthew DeVoy Jones, Cell Phones Are Orwell's Telescreen; The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information, 67 *Cleveland State Law Review* 523, 545-556 (2019).

[30] 通讯录、通讯记录应当构成“通信”,参见张新宝:《个人信息收集:告知同意原则适用的限制》,《比较法研究》2019年第6期,第4-5页。

[31] See *Carpenter v. United States*, 585 U.S. (2018) 17,关于该案的介绍,参见刘冷:《美国宪法第四修正案下隐私权保护规则的新发展——美国卡朋特诉合众国案评析》,《人权研究》第22卷,第335-353页。关于该案涉及的信息内容和元数据的讨论,参见朱嘉璐:《数字时代刑事侦查与隐私权保护的界限》,《环球法律评论》2020年第3期,第48-49页。

[32] 唐忠民认为当短信发出以后,在设备终端仍然存储通信内容属于违反《宪法》第40条的行为。参见唐忠民:《公民通信自由和通信秘密保护的两个问题》,《法学》2007年第12期,第13-17页。

[33] 关于通信记录不属于通信内容,不受《宪法》第40条保护的观点,参见杜强强:《法院调取通话记录不属于宪法上的通信检查》,《法学》2019年第12期。不同的观点,参见王锴:《调取查阅通话(讯)记录中的基本权利保护》,《政治与法律》2020年第8期;张翔:《通信权的宪法释义与审查框架——兼与杜强强、王锴、秦小建教授商榷》,《比较法研究》2021年第1期。

[34] 关于手机实时定位信息应受美国宪法第四修正案保护的讨论,参见 Matthew DeVoy Jones, Cell Phones Are Orwell's Telescreen; The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information, 67 *Cleveland State Law Review* 523, 545-556 (2019)。

[35] 关于通信秘密的构成,以及借助该条款保护死者个人信息的讨论,参见王琦:《网络时代的数字遗产·通信秘密·人格权——以社交、通信网络账户的继承为焦点》,《财经法学》2018年第6期,第84-101页。

[36] 关于应然权利和实然权利、背景权利和制度权利区分的讨论,参见 Ronald Dworkin, Hard Cases, 483 *Harvard Law Review* 1057, 1069-1070 (1975)。

式赋予个人信息主体对于个人信息的全面的控制权。就此而言,《个人信息保护法》是以个人控制为中心的立法。个人信息的合法利用则是建立在个人信息保护前提上的。^[37]

当然,个人信息控制模式、社会功能、正外部性的讨论并不会因为立法对这个问题予以回应就归于沉寂。有学者认为在“后《个人信息保护法》时代”,需要关注个人信息的社会性,数字社会的发展建立在个人信息自由流动的基础上。^[38]也有学者指出,个人信息除了个人控制、社会控制之外,还有更重要的资本控制,要关注资本控制之下的个人控制的变异。^[39]无论是个人控制、社会控制还是资本控制,个人信息的本质在于可以通过识别性和相关性关联到具体个人。所以在个人信息控制的位阶上,个人控制是原初的,社会控制是派生的,而资本控制是异化的。就此而言,并不存在从个人控制到社会控制这种直线演化的进路,但需要考虑个人信息上承载的其他利益。所有信息处理的主体,无论是私人性质的信息控制者,还是公权力性质的政府和公共企业,其处理个人信息的前提仍然主要是个人信息主体的知情同意。需要特别指出的是,基本权利的规范效力意味着对于它的限制不能简单地基于功利主义或管理便利的目的。^[40]《个人信息保护法》中的个人信息主体权利主要包括以下几个方面。

(一) 知情权、决定权是个人信息权的基础

知情决定是个人信息权的起点,其目的在于确立个人信息主体对于自身人格形塑的自主控制。知情决定意味着信息主体对个人信息的收集、使用、分析、共享、删除的全生命周期的把握、选择和决定。知情权作为个人信息权利体系的理论基础具有指向明确、功能清晰、权利内容完整等优势。^[41]德国联邦宪法法院在1983年数据保护判决中就曾指出,在一个法律秩序中,如果民众无法知晓其个人信息被何人知悉、为何被知悉,以及在何种情形下被知悉,这样的社会秩序以及其所赖以存在的法律秩序,将和个人信息自决的意旨相冲突。

个人信息保护法中的知情同意机制设计正是基于知情决定而生,将个人的同意作为信息流通和使用的合法性基础。就同意的实质意涵而言,用户的同意必须是在充分告知的前提下,自由、明确地作出的,是用户清楚而不含糊的意思表示。在移动互联网时代,用户在面对具有市场优势地位的应用程序,往往没有选择的余地,只能选择同意;而平台的隐私协议与用户规则繁琐不堪,用户往往不假思索地点选同意。信息过载和信息不对称是知情同意机制普遍面临的情形。为了让用户的同意变得具有实质意义,各国法律为知情设定了增强同意、书面同意与额外同意等情形。《个人信息保护法》对敏感信息的处理也采取了增强同意的立法思路,规定个人信息处理者处理敏感信息需要取得个人单独同意。《个人信息保护法》在个人知情同意机制的设计上体现了个人自治和政府规制相结

[37] 参见申卫星:《论个人信息保护和利用的平衡》,《中国法律评论》2021年第5期,第28-36页。

[38] 参见胡凌:《功能视角下个人信息的公共性及其实现》,《法制与社会发展》2021年第5期,第176-189页。

[39] 参见郑智航:《数字资本运作逻辑下的数据权利保护》,《求是学刊》2021年第4期,第113-126页。

[40] 关于基本权利规范效力的经典讨论,可以参见德沃金基于原则主张和政策主张而展开的辨析,Ronald Dworkin, Hard Cases, 483 *Harvard Law Review* 1057 (1975)。

[41] 参见赵宏:《从信息公开到信息保护:公法上信息权保护研究的风向流转与核心问题》,《比较法研究》2017年第2期,第32-36页。

合、强化个人信息处理者责任、兼顾事后风险防范的特点,形成了权利建构为主、行政监管协同的个人信息同意机制。^[42] 就此而言,知情同意不仅具有私法上的合意的效果,它更是一项个人信息保护的公法制度。^[43]

(二) 查阅权、复制权是个人信息权的核心

《个人信息保护法》第 45 条规定了个人信息主体对于信息的查阅权和复制权。这一权利的具体内涵仍有待立法机关的解释以及监管部门在执法中的进一步明确。查阅、复制权可以说是个人信息权利束的核心内容,是落实个人信息保护原则的重要手段。个人信息主体经由查阅复制权的行使可以清晰了解到个人信息控制者所掌握的数据是否满足了个人信息收集中的知情同意规则,可以衡量数据最小化、目的特定等个人信息保护原则是否得到了遵守。^[44] 查阅复制权具有核校数据处理者是否遵守了《个人信息保护法》所确立的系列原则的功能。

在《个人信息保护法》立法的过程中,有学者建议采用个人信息访问权来代替个人信息查阅权和复制权,但最终的立法仍然保留了原来的措辞。比较而言,个人信息访问权更符合数字经济条件下信息主体对个人信息获取的方式。从解释论的角度,个人信息查阅权和复制权其实质就是个人信息访问权。查阅权、复制权文义上充满了前互联网时代的意涵,信息主体并不会像查阅账簿一样去信息处理者那里查看自己的个人信息,一般情形下也不存在请求信息处理者向其提供关于其个人信息的复印件的需求。如果采取这样的解释,个人信息主体行使这一权利的方式成本高昂、费时较长,为权利义务双方都施加了数字时代所不必要的麻烦,从而使这一权利失去实际意义。

就规范效力而言,这一权利等同于欧盟《一般数据保护条例》(*General Data Protection Regulation*)所规定的访问权。个人信息主体基于这一权利可以发起获取个人信息的请求,信息处理者应当提供结构化的、机器可读的通用格式的个人数据包,并提供下载工具。除此之外,个人信息主体也可以请求纸质版本,并承担因请求纸质版本而产生的合理费用。对个人信息查阅、复制权的这种解释才使得个人能够及时、便捷、数字化地获取个人信息。在《加州消费者隐私法》(*California Consumer Privacy Act*)下,个人信息主体行使访问权的方式就包括获得邮寄纸本或者数字版本的个人信息,而且个人信息控制者和处理者应当免费提供,个人信息主体在一年内可以行使两次请求权。这可以作为解释《个人信息保护法》查阅、复制权的一个参考。个人信息查阅、复制权作为请求权基础,其指向的不仅是一般的私人信息处理者,也可能是国家机关。在刑事诉讼领域,司法信息化浪潮之下辩方的阅卷权受到冲击,个人信息查阅、复制权为取代阅卷权提供了可能性,可以从这一权利行使的方式、权利的限制等方面入手,实现该权利与刑事诉讼制度的协调。^[45]

[42] 参见丁晓强:《个人数据保护中同意规则的“扬”与“抑”——卡-梅框架视域下的规则配置研究》,《法学评论》2020年第4期,第139-141页。

[43] 参见韩旭至:《个人信息保护中告知同意的困境与出路——兼论〈个人信息保护法(草案)〉相关条款》,《经贸法律评论》2021年第1期,第47-59页。

[44] 参见张新宝:《个人信息处理的基本原则》,《中国法律评论》2021年第5期,第18-27页。

[45] 参见郑曦:《超越阅卷:司法信息化背景下的刑事被告人数据访问权研究》,《河南大学学报》2020年第2期,第59-65页。

(三) 可携带权是个人信息自决的保障

个人信息可携带权为各国立法所普遍确认。欧盟、美国、印度、日本、新加坡等法域都引入了数据可携带权,它已经成为各国民众普遍享有的一项个人信息权利。例如2021年美国《通过促进服务转换实现兼容性和竞争性法案》(*Augmenting Compatibility and Competition by Enabling Service Switching Act*)规定,由该法所调整的平台应保持一套透明的可由第三方访问的接口(包括应用编程接口),以便能够安全地将数据传输到另一用户,或经用户的明确同意,在用户的指示下,以一个结构化、常用的、机器可读的、符合该法发布标准的可读格式传递给第三方商业用户。^[46]在《个人信息保护法》通过之前,我国在规章和规范层面已经建构了数据可携带权的雏形,在携号转网中形成了数据可携带权的实践。《个人信息保护法》在三审稿的基础上最终确立了可携带权,响应了个人信息保护立法的世界性趋势,使得我国个人信息保护的水平和个人信息保护高水位的法律区域不相上下。

个人信息可携带权的确立有利于数据竞争,在实质意义上实现个人的信息自决。《个人信息保护法》第45条第3款规定,“个人请求将个人信息转移至其指定的个人信息处理者,符合国家网信部门规定条件的,个人信息处理者应当提供转移的途径。”但这一权利对于互联网产业的影响巨大,出于审慎的考量,立法者增加了个人信息主体行使该权利需要符合国家网信部门规定的条件,因此在《个人信息保护法》生效之后,需要网信办出台个人信息可携带权行使的细则,明确其范围、行使方式和实施的条件。

欧盟《一般数据保护条例》尽管规定了个人数据可携带权,但对其进行了一定程度的限制,主要包括以下三个方面:可携带权在个人数据权利束中优先性靠后;对个人数据可携带权的范围进行了限定;关于平台互操作性仅仅是予以鼓励,而不是课加强制性义务。

监管部门在落实个人信息可携带权的细则时,应当考虑我国数字经济发展的实际,在上述问题上作出不同于欧盟的规定,明确个人信息可携带权相对删除权的优先性,对于不同领域平台之间的互操作性予以差别化的规定:对于政府等公共服务平台,互联互通是其法定义务;对于电商类平台、社交类平台,可以基于平台性质而在互联互通要求上有所区分,以拆除互联网世界花园的高墙(walled garden)。^[47]国家市场监督管理总局2021年10月发布的《互联网平台分类分级指南(征求意见稿)》可以作为这种差别化互操作性规制的参考。

(四) 删除权体现了个人数字人格的完整性

《个人信息保护法》确立了个人信息主体对于错误信息的更正权以及删除权,这是为了保证个人信息的完整性和个人数字人格的整全性。^[48]《征信业管理条例》对征信领域的删除权予以了具体化,明确规定征信机构采集的个人不良信息的保存期限为自不良行

[46] See *Augmenting Compatibility and Competition by Enabling Service Switching Act*, <https://www.congress.gov/bills/117/congress/house/bills/3849/text>, 最近访问时间[2021-11-10]。

[47] See Whitney Nixdorf, *Planting in a Walled Garden: Data Portability Policies to Inform Consumers How Much (If Any) of the Harvest Is Their Share?* 29 *Transnational Law & Contemporary Problems* 135, 147 (2020).

[48] 关于数字人格的理论建构,参见朱程斌:《论数字人格》,《学习与探索》2021年第8期,第82-90页。

为或者事件终止之日起 5 年。个人不良信息保存期限届满,征信机构应当将个人不良信息在对外服务和应用中删除;作为样本数据的,应当进行匿名化处理。

删除权的规定使得个人信息权的体系和信息生命周期得以匹配、同步保障。删除权体现为个人信息主体对于信息控制者的请求权,用户对于数据控制者所控制和处理的非必要、不相关和过时的个人信息可以行使该请求权。删除权确保个人在线下线上线一体化的数字化生存中可以避开“凝视的目光”。这也是它有时又被称为被遗忘权的原因。它是个人信息在信息社会自由流动中的终止,是个人从信息社会中抽离的权利机制。^[49]

被遗忘权在权利建构、公共人物的例外情形、请求权的形式以及个人信息处理者的响应等方面仍然需要在司法实践中进一步明确。^[50] 个人信息的公共维度在删除权的行使中表现突出,个人信息主体对删除权的行使可能会妨碍具有同样重要性的言论自由、新闻自由等权利,这时就需要进行利益衡量。在欧盟的司法中,已经有相关案例对这一问题作出回应。删除权的行使应注意和言论自由等其他权利之间的相互性。^[51]

《个人信息保护法》中并没有规定《加州消费者隐私法》中的退出信息处理权。这一权利实际上可以被删除权所吸收和涵盖,实定法上的删除权包含了个人信息处理者得以请求退出信息处理的权利。在实践中,个人账户的注销可能只是切断其他用户的检索,相关信息并没有从数据库中删除,甚至也未必作了匿名化的处理。主动注销的条件严格,而被动注销形同虚设,账号注销成为难题。^[52] 这些《个人信息保护法》实施中的问题仍然需要从规制上予以有效回应。

《个人信息保护法(三审稿)》中还增加了一个条款,“个人信息处理者拒绝个人行使权利的请求的,个人可以依法向人民法院提起诉讼”。这一条款最后成为第 50 条第 2 款。这使得个人信息主体在基于《个人信息保护法》所享有的列举权利受到侵害时可以依照该法而获得救济,无需借助其他的规范。在实践中,信息处理者的何种行为构成拒绝,还需要进一步的明确。这个条款强化了《个人信息保护法》作为数字时代个人信息基本法的法律地位,在实体法上和救济功能上具有一定的自足性,但在涉及民事侵权时,仍然需要转接到《民法典》中关于侵权行为及侵权责任的一般性规定。这体现了我国个人信息保护在宪法规范统摄下的公私法协同进路。在诉讼类型上,要根据信息处理者的身份来决定这一诉讼是民事诉讼还是行政诉讼。如果信息处理者是国家机关,这一诉讼属于行政诉讼;如果信息处理者是平台一类一般民事主体,则属于民事诉讼。

个人信息权作为数字时代的人权,是人权观念在数字时代的丰富。《个人信息保护法》建立了一个广泛而全面的权利体系,而各项具体权利的结构、行使方式、信息控制者和处理者的义务、义务未履行的责任、相关诉讼的案由仍有待执法机构和司法部门通过立

[49] 内维尔(Andrew Neville)认为,被遗忘权是一项人权。See Andrew Neville, Is It a Human Right to Be Forgotten? Conceptualizing the World View, 15 *Santa Clara Journal of International Law* 157, 158-171 (2017).

[50] 参见郑志峰:《网络社会的被遗忘权研究》,《法商研究》2015 年第 6 期,第 55-60 页。

[51] 刘文杰认为资料存档的公共价值应优先于个人被遗忘,参见刘文杰:《被遗忘权:传统元素、新语境与利益衡量》,《法学研究》2018 年第 2 期,第 35-36 页。

[52] 从个人信息删除权角度对用户账号注销的体系化构建的讨论,参见赵精武、唐浩隆:《从注销到删除:“账号注销权”的体系定位与制度建构》,《重庆邮电大学学报(社会科学版)》2021 年第 6 期,第 70-81 页。

法解释和司法个案的方式予以明确。人民法院应当通过司法解释进一步明确个人信息权利司法救济的条件、程序和方式方法。

三 《个人信息保护法》与《民法典》的衔接

(一) 几个概念的厘清:数据、信息与隐私

欧盟无论是在立法还是在理论上,一般并不严格区分数据和信息这两个概念。欧盟《一般数据保护条例》中的“数据”完全可以用信息替换。而美国的立法目前呈现出个人信息和数据的区分,《加州消费者隐私法》采用了个人信息的概念,在功能上和我国的《个人信息保护法》相近,区别在于加州的这一立法是在消费者隐私权保护框架下进行的,美国联邦层面的《澄清境外数据合法使用法》[*The Clarifying Lawful Overseas Use of Data (CLOUD) Act*]则采用了数据的概念,我国《数据安全法》的域外效力条款与该法接近。但在美国学者的研究和通常的讨论中,并不作数据和信息的区分。^[53] 我国的个人信息和数据区分保护的思路在《民法总则》中得以确立,《民法总则》第111条规定,自然人的个人信息受法律保护。第127条规定,法律对数据、网络虚拟财产的保护有规定的,依照其规定。个人信息和数据二分的做法为此后立法所遵循,《数据安全法》和《个人信息保护法》前后出台就延续了这一思路。在数据安全法的立法框架中,如果个人信息处理者处理个人信息达到一定数量,就会转化成数据安全问题。当然,个人信息数据是网络数据的一种形式,网络数据还包括企业数据、政府数据。实际上,需要在理论上进一步厘清算算法技术条件下的个人信息安全、网络安全和数据安全。隐私和个人信息有重叠之处,比如个人病例、^[54] 行踪轨迹、网络浏览记录,既属于个人隐私、也属于个人信息。《民法典》将个人信息分为隐私信息、公开信息和一般信息,对隐私信息采取隐私权和个人信息权的双重保护,但这一区分实非必要,反生困扰。^[55] 隐私强调的是个人生活安宁不受打扰、个人私密情形不被披露,是一种消极的不被侵扰、不被公开的权利,而个人信息的核心在于可以经由信息识别到个人。^[56] 有些隐私并不属于个人信息,比如《宪法》第37条规定的个人住宅不受侵犯的权利,即属于隐私权的一种表现,但这一权利却与个人信息无关。个人的姓名、工作单位属于个人信息,但它不具有隐私的成分。所以隐私和个人信息既有重合的地方,但又有不相隶属的成分。在美国法上有信息隐私的概念,^[57] 究其实质,它指向的是个人对于信息的知情控制权,类似于《个人信息保护法》中的知情、决定权。

[53] 实际上,美国学者在他们的研究中很少将数据和信息的概念进行区分,参见 Paul M. Schwartz, Property, Privacy and Personal Data, 117 *Harvard Law Review* 2056, 2057-2128 (2004)。

[54] 关于个人健康信息应用基于个人信息权的讨论,可以参见李帅:《电子病历应用中个人信息权的谦抑与扩张》,《情报杂志》2021年第7期,第201-206页。

[55] 参见王洪亮:《〈民法典〉与信息社会》,《政法论丛》2020年第4期,第3-13页。

[56] 参见高富平:《论个人信息保护的目的一以个人信息保护法益区分为核心》,《法商研究》2019年第1期,第93-104页。

[57] 关于信息隐私权的定义,该文中将隐私分为信息隐私、访问隐私(accessability privacy)和表达隐私,参见 Judith Wagner DeCew, Privacy and Information Technology, https://wmich.edu/sites/default/files/attachments/u58/2015/ethics-privacy_info_tech.pdf,最近访问时间[2021-10-26]。

《个人信息保护法》采取了一般信息和敏感信息的分类,将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹、未满十四周岁未成年人的信息认定为敏感个人信息。数据处理者必须是为了特定目的、充分必要而且采取保护措施的前提下才能处理敏感个人信息。敏感个人信息更容易和隐私重叠,但仍然无法完全等同。在司法实践中,个人信息和隐私重叠,处理个人信息侵犯信息权和侵犯隐私权竞合时,个人信息主体可以选择基于个人信息权还是隐私权提起诉讼,从而解决部分个人信息兼具敏感个人信息和隐私二重性的问题。

(二)《个人信息保护法》与《民法典》在个人信息保护中的适用

《个人信息保护法》是个人信息领域的基本法,个人信息主体权利构成的解释、信息权利受到侵犯时所需的救济都应当以《个人信息保护法》为出发点,该法关于个人信息权的规定超越了私法意义的权利或者刑法上的法益,它是具有宪法规范基础的新型公法权利。

《民法典》无法作为《个人信息保护法》的一般法基础。个人信息除了个人维度之外,还具有公共的维度,个人信息并不会因为使用者的增加而受到损害,也不会因为被使用频次增加而受到损害。^[58] 个人信息主体同时面对公私两种信息处理主体,信息处理者和信息主体在信息能力上高度不对称。所以,无论是从个人信息法的属性、权利构成、调整关系,还是从回应社会的能力等方面来说,《民法典》人格权编都无力单独承担这一使命。从经验的角度而言,在《个人信息保护法》通过之前,通过侵权救济的方式在司法中回应 APP 过度索权、超范围索权等已经呈现出明显不足。

《民法典》并不必然构成《个人信息保护法》的先前理解。就民法和宪法的一般关系而言,我国的民法并不是在社会发展演进中先于宪法而形成的调整市民关系的一般准则,它是我国近代国家建构的一部分。虽然我国《民法典》的通过在时间上先于《个人信息保护法》,对后者的制定产生了重要的影响,促进了个人信息保护单独立法的共识,但《民法典》并不是《个人信息保护法》的一般法。^[59] 它也不必然成为《个人信息保护法》的前理解;它是构成《个人信息保护法》前理解语境中的一个因素,但同样重要甚至更重要的是时间上早于《民法典》、立法对象上更具重合性、交叉性的《网络安全法》。

《民法典》和《个人信息保护法》规定不一致时,应当优先适用《个人信息保护法》。例如,两部法律在个人信息定义的问题上就有所不同。《民法典》第 1034 条规定,个人信息是以电子或者其他方式记录的能够单独或者和其他信息结合识别特定自然人的各种信息,其判断标准为“可识别”。^[60] 而《个人信息保护法》第 4 条规定,个人信息是以电子或者其他方式记录的与已识别或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。《个人信息保护法》的规定更为周延,将匿名化信息排除在保护范围之外。但其采取的是“可识别”加“相关性”的标准,个人信息的指向范围更广,个人信息处理者对此应先

[58] 参见梅夏英:《在分享和控制之间——数据保护的私法局限和公共秩序构建》,《中外法学》2019 年第 4 期,第 845-870 页。

[59] 参见周汉华:《个人信息保护法的法律定位》,《法商研究》2020 年第 3 期,第 44-56 页。

[60] 参见苏宇、高文英:《个人信息的身份识别标准:源流、实践与反思》,《交大法学》2019 年第 4 期,第 54-71 页。

予遵守。监管部门需要在这两个标准的基础上对个人信息进行分级分类的风险规制,确保个人信息的范围不因为过于宽泛而无法落到实处,同时为数字产业的发展提供有效激励。^[61]

(三)《个人信息保护法》的行政执法体系

《个人信息保护法》在一定程度上吸收了之前个人信息保护行政执法政出多门的局面,确定了国家网信部门统筹协调个人信息保护工作和相关监督管理工作,国务院有关部门依法在各自职责范围内负责个人信息保护和监督管理工作。《个人信息保护法》在此基础上建立了完整的行政执法监管体系,对企业设定了约谈、申诫、财产罚、行为罚等一系列行政处罚机制。对违法处理个人信息的应用程序,责令暂停或者终止提供服务,对于违法处理个人信息情节严重的,吊销许可证或者吊销营业执照,禁止相关责任人员在一定期限内担任相关企业的董事监事等高级管理人员和个人信息保护负责人。

在行政监管体系之外,《个人信息保护法》还建立了个人信息保护公益诉讼制度。《个人信息保护法》建立了以事前事中执法为主、以公益诉讼和私人侵权救济为辅助的体系完整的救济机制。

四 《个人信息保护法》对公私主体的适用

个人信息主体在面对不同性质的信息处理者时,处于不同的法律地位。当他面对私人主体的时候,同意机制可以作为重要的保障当事人自主的合意机制;当处理者是政府的时候,一般意义上的同意机制可能并不够充分。有学者提出,个人信息保护立法应当采取“总分总”的模式,总则部分明确基本概念、基本原则等,一体适用于公私领域。继而分别规定国家机关和非国家机关在个人信息收集、存储、处理和利用等方面的处理规则,最后规定统一的法律救济模式。^[62]

我国《个人信息保护法》采取的是一种统合型的立法模式,比上述“总分总”的建议更能体现《个人信息保护法》适用的整体性。《个人信息保护法》规定,国家机关处理个人信息的活动适用该法,同时考虑到国家机关处理个人信息的特殊性,在第二章第三节对此进行了特别规定。对于特定领域的个人信息处理活动,比如档案、刑事诉讼等领域,应当有符合其特点的规则,实现个人信息保护和档案利用、刑事司法的衔接。基于《个人信息保护法》规范的体系分析,《个人信息保护法》的公法性质毋庸置疑。

基于公法理论,宪法的规范对象一般为公权力行为,它调整是国家机关之间、国家机关与公民之间的关系,只在例外情形下才调整私法领域平等主体之间的关系。宪法在私法领域中的效力被称之为宪法第三人效力。^[63] 宪法基本权利既有防御权功能,还蕴含着客观法价值,目的在于通过强化基本权利的作用,完成客观价值秩序的建构。这一价值秩

[61] 参见谢琳:《大数据时代个人信息边界的界定》,《学术研究》2019年第3期,第69-75页。

[62] 参见蒋舸:《个人信息保护法立法模式的选择》,《法律科学》2011年第2期,第120页。

[63] 参见许瑞超:《基本权利第三人效力的范畴与本质》,《交大法学》2021年第1期,第46-59页。

序就是将个人自治、人格自由发展、促进和实现作为社会共同体的核心价值,并将其适用于所有法律领域。基本权利的双重性质,即面对国家的防御功能以及面对社会权力时国家的保护义务,成为了个人信息权利国家保护的理论基础和基本框架。

宪法基本权利规范中,有一些规范采取的是绝对权的表述,比如作为个人信息权直接宪法基础的“人格尊严”条款就属于这类表述。《宪法》第 38 条规定,“中华人民共和国公民的人格尊严不受侵犯”。这意味着它不仅直接约束公权力行为,也约束私人行为。这一条款为国家设定的保护义务意味着,国家在立法、行政、私法三个向度上对基本权利主体形成了公法上国家和个人信息主体的给付关系。

就国家保护义务而言,“公民人格尊严不受侵犯”的表述,从文义解释的角度可以看成个人信息权利受国家保护的规范来源。^[64] 基于国家保护义务,国家需要以一定的方式介入私人领域。^[65] 但国家介入的具体方式是由一国的宪法体制、国家机构之间的权力配置及其具体权限而定。我国人大制度的政体以及宪法解释权专属全国人大及其常委会的制度安排,决定了法院不能直接适用这些条款,仍需借助全国人大及其常委会基于基本权利条款,通过具体化的立法来落实基本权利保护的目标。对此,全国人大及其常委会具有立法形成自由。全国人大基于宪法基本权利条款进行的立法,可以采取公法保护模式,也可以采取私法保护模式,对于个人信息保护则兼采公私法协同模式,分别体现在《个人信息保护法》和《民法典》。《个人信息保护法》确立了个人信息保护的一般性规则,是个人信息保护的基本法,而《民法典》是私法领域的基本法,就个人信息保护而言,并无优先适用的问题。^[66] 从基本权利第三人效力理论出发,立法者制定民法上的概括性规定,以实现保护义务,法官在具体案件审理中参考国家保护义务之目的,适用该法规定,这是基本权利之间接第三人效力,实际上属于国家保护义务理论适用的具体情形。

五 余论:走向个人信息权利的时代

信息技术的发展,推动了社会生产力的发展,也深刻地改变着生产关系。由于信息技术的广泛运用以及对生产生活的深刻影响,我们的时代又被概称为大数据时代、人工智能时代或算法时代。我们需要从宪法时刻的视角^[67]和公民权利的双重面向^[68]构建个人信息保护的法治框架,让人的尊严和人性自主的价值引领技术发展。《个人信息保护法》的公法属性、立法宗旨、权利体系、规制措施都体现了这一价值目标,其是数字时代公法秩序变迁的重要产物,^[69]它对公法边界的塑造仍需通过其实施来确立。

[64] 参见李建良:《基本权利与国家保护义务》,载《宪法理论与实践(二)》,我国台湾地区新学林出版股份有限公司 2007 年版,第 61-125 页。

[65] [美] Peter E. Quint:《宪法在私法领域的适用——德、美两国比较》,余履雪译,《中外法学》2003 年第 5 期,第 606-630 页。

[66] 参见周汉华:《平行还是交叉——个人信息保护与隐私权的关系》,《中外法学》2021 年第 4 期,第 1167-1187 页。

[67] 参见余成峰:《信息隐私权的宪法时刻》,《中外法学》2020 年第 3 期,第 32-56 页。

[68] 参见[日]山本隆司、王贵松:《客观法与主观权利》,《财经法学》2020 年第 6 期,第 98-111 页。

[69] 参见季卫东:《数据保护权的多维视角》,《政治与法律》2021 年第 10 期,第 2-13 页。

[**Abstract**] The development of information technology not only promotes the development of social productive forces, but also profoundly changes the relations of production. Due to the wide application of information technology and its profound impact on production and life in the era of big data, we need to build a legal framework for personal information protection from the dual perspectives of constitutional law and civil rights, so that the development of technology can be guided by human dignity and the value of human autonomy. The Personal Information Protection Law is the basic law on the protection of personal information in China in the digital age. The human rights clauses in the constitution are the theoretical cornerstone of the right to personal information as a right in public law, and human dignity is the normative basis of the right to personal information as a positive right. The Personal Information Protection Law adopts the proposition that the right to personal information, as a new right in public law, establishes a complete legal protection system. In China, Personal Information Protection Law and Civil Code form a public-private law hybrid approach to personal information protection. The right to personal information further enriches the connotation of freedom and privacy of communication. Among the bundle of personal information right established by this law, the right to informed consent is the foundation, the right to access is the core, the right to portability is the guarantee of personal information self-determination, and the right to deletion embodies the integrity of digital personality. The adoption of the law transforms the right to personal information from a right ought to be to an actual right. In the relationship between the Civil Code and the Personal Information Protection Law, the construction of the right to personal information and the remedies for its infringement should take the Personal Information Protection Law as their starting point. The personal information right established by this law transcends the right in the private law sense or legal interests in criminal law. It is an emerging public law right with a constitutional normative basis, aimed at guiding the development of technology by the value of human dignity. The Personal Information Protection Law embodies the distinctive public law attribute in terms of legislative basis, rights system, and article design. This can also be theoretically explained from the dual perspectives of a fundamental right and the state's obligation to protect personal information. As the cornerstone of the public law order in the digital age, its function of shaping of the boundaries of public law still needs to be established through its implementation. The Personal Information Protection Law has established an extensive and comprehensive system of rights, and the structure of various specific rights, the way of their exercise, the obligations of information controllers and processors, the liabilities for failing to fulfill their obligations, and the causes of relevant actions still need to be clarified by law enforcement agencies and judicial departments through legislative interpretation or judicial cases.
