

论数据、信息与隐私的权利层次与体系建构

彭诚信 杨思益

摘要:我国法律中的隐私、个人信息具有各自独立的内涵,个人敏感信息的保护范围已由隐私所覆盖,不应成为与之并列的分类方式。个案中的隐私与个人信息应该存在一定的界限,对其厘定需要在个案中予以具体判断。信息、数据在信息学意义上的可分性不等于在法学上的可分性。在个人层面,个人数据就是个人信息,权利客体始终只有个人信息;在数据控制者层面,经过脱敏处理、无法识别或不能直接识别出信息主体的数据,才是财产权的客体。隐私、信息与数据的定性及其上权利定性与体系建构为整个数字社会的存在与发展创造了前提。

关键词:隐私;个人信息;数据;权利层次;权利体系

中图分类号: D920.1

文献标识码: A

文章编号: 1009-2447(2020)02-0079-11

一、问题的提出

文明源于记录,互联网的全面记录不仅造就了数字经济,而且开创了数字文明时代。^[1]在这个高透明度的新时代,再没有人是一座“孤岛”,每个人既在产生大量的信息、数据,也在利用信息、数据,相应的信息权、数据权对传统的权利领域造成了冲击,引发了激烈讨论。然而,若信息、数据的法律属性尚未明确,与既有隐私的关系尚无界定,其上的权利建构便只是空中楼阁;若仅仅关注个人或企业一方进行权利建构,则难免顾此失彼,无法形成统一的制度规范。司法实践中,信息、数据的权利保护更是面临诸多难题。

(一) 隐私、信息及数据的客体属性不清

1. 隐私与个人信息的范围不清

个人信息诞生之初,学界就对隐私与个人信息的关系进行过探讨,认为二者虽然存在重合,但根本上是两个独立的客体,能够进行界分:隐私强调

私密性,而个人信息注重身份识别性;隐私不限于信息形态,而个人信息则不然;隐私具有个体性,而个人信息则更易与国家安全相关。^[2]这种抽象的区分虽然为隐私、个人信息的关系认知勾勒出了框架,但其实用性有限,尚未与作为区分目的的差异性保护规则相对接,从而导致司法实践中对隐私、个人信息的判断甚为模糊。

两个概念内涵的模糊直接反映在《中华人民共和国民法典(草案)》(以下简称《民法典(草案)》)中,“人格权编”第一千零三十二条把隐私界定为,“自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”,而在第一千零三十四条个人信息的界定中又规定,“个人信息中的私密信息,同时适用隐私权保护的有关规定”。此处引发的问题是,“私密信息”到底是个人信息,还是隐私,何况法律也没有规定“私密信息”为何。在隐私与个人信息本来就界限模糊的情况下,再增加一个“私密信息”,使得理论与实践

基金项目: 国家哲学社会科学基金重大项目“大数据时代个人数据保护与数据权利体系研究”(18ZDA145)

作者简介: 彭诚信,男,山东嘉祥人,上海交通大学凯原法学院副院长,教授,博士生导师,民商法学科带头人,研究方向为民法原理、物权法、数据与人工智能;杨思益,女,湖北恩施人,上海玛娜数据科技发展基金会特约研究员,上海交通大学凯原法学院民商法学硕士,研究方向为民商法。

会更为复杂。“私密信息”概念的出现也是隐私与个人信息概念不清的一个明证。

两个概念内涵的界限模糊在司法实践中亦多有体现。如在“史玉田与平安保险案”^①中,史玉田以平安保险公司侵犯其个人信息权为由起诉至法院,但法院认为个人信息属于隐私权的客体之一,从而按照隐私权纠纷判断案件管辖,实际上是将个人信息划入隐私的范围进行保护。在“李蕾与上海映迪、中视创艺案”^②中,李蕾在“小小红领巾”微信号填写昵称、性别、手机号、照片等系列信息用于交友推广,而被告运营的网络平台擅自抓取、保存其个人信息并对外推送,法院认为上述行为既侵犯了李蕾的隐私,也侵犯了李蕾的个人信息。但在“陈瑞生与张卫国案”^③中,对于张卫国擅自在微信群公开原告照片、住址等个人信息的行为,法院认为侵犯了陈瑞生的隐私权或个人信息权,似将二者作为同义词使用。隐私、个人信息能否同时作为侵权客体,抑或只能二者择一,目前的学理区分尚没有为司法实践提供恰当的判断路径。

2.个人信息与数据的概念混淆

无论在学界还是司法实践中,信息、数据的概念都存在混合使用的现象,对二者应否区分产生了不同观点:主张同一说的学者认为,信息和数据并没有本质区别,两者可以互换使用;^④即便承认信息和数据是内容与形式的关系,也认为在大数据时代两者不可分离,需要进行统一理解;^⑤除了称个人信息、个人数据外,还有少数学者直接兼采二者,称个人数据信息、信息/数据。^⑥主张区分说的学者则认为,信息与数据化表达相互分离而独立存在;^⑦信息的外延大于数据,主张数据工具主义;^⑧或者认为信息和数据分属于内容层和符号层,主张严格区分个人信息与数据文件。^⑨这种概念纷争的现象受到了比较法上的影响,如欧盟、德国、法国、英国、新加坡使用数据的概念,^⑩加拿大、韩国、日本则使用信息的概念。^⑪概念不清会造成内涵不明,时常难以判断此学者所称“信息”是否等同于彼学者所称“数据”,由此产生的“信息权利”是否又等同于彼处的“数据权利”。信息、数据的法学规范意义和相互关系亟须厘清,这也是后续探讨对二者如何赋权的基础。

相比理论界,我国司法实践中对其的称谓更是五花八门,绝大多数法院并未有意识地规范使用信息、数据的术语,除了个人信息、个人数据外,还有私人信息、用户信息、用户数据、数据信息、资料数据、数据资源等表述。如在“微博与脉脉案”^⑫中,法院就曾表述:“获取用户信息时网络运营者不得收集与其服务无关的个人信息,收集信息限于为了应用程序运行及功能实现必要的用户数据。”同一判决书同时使用用户信息、个人信息、用户数据来指代同一对象。这些随意的称谓使得信息、数据的概念使用生活化,理论界和实务界缺乏对基础概念的统一理解,甚至导致当下无法在共同的话语体系下探讨信息、数据的相关法律问题。

(二)信息、数据上的权利性质不明

不同于美国的“大隐私权”概念,我国民法将隐私权作为一项具体人格权予以保护,^⑬对隐私权的人格权法律定性几乎没有任何争议。与隐私不同,信息、数据所蕴含的经济利益为其权利性质蒙上了一层神秘面纱,致使立法上尚未明确其权利性质。但权利性质决定救济途径,立法上的踌躇迫使学界和司法实践进行了多种尝试。

1.关于信息权利性质的争议

学界对信息权利的关注早于数据权利,有学者将有关个人信息权利的观点整理为宪法人权说、一般人格权说、隐私权说、财产权说、新型权利说和独立人格权说;^⑭之后又有学者总结出个人信息法律属性的八种观点:个人信息权否定说、基本权利和自由说、物权说或所有权说、隐私权说、一般人格权说、人格权兼财产权说、框架权说和具体人格权说。^⑮总体来看,理论上主要存在两种观点:一是财产权说,认为个人对其个人信息享有财产权,个人信息是一种有价值的商品,应当能够在自由市场上进行交换,^⑯二是人格权说,主张个人信息是人格自由和尊严的体现,至于以何种途径保护这一人格利益,又存在一般人格权说、隐私权说和具体人格权说的分歧。

由于缺乏明确的权利定性,司法实践中的个人信息保护常常陷于混乱的境地。有法院运用一般人格权保护个人信息:如在“任甲玉与百度案”^⑰中,法院认为任甲玉诉请的对其特定个人信息的

“被遗忘权”不能归入我国现有类型化的人格权保护范畴,只能从一般人格权的角度寻求保护。有法院藉由隐私权的路径保护个人信息:如在“庞理鹏与东航案”^⑧中,庞理鹏委托朋友在东航为其订购机票,所留联系方式为朋友的手机号,但却在自己的手机上收到了航班取消短信。法院认为姓名、手机号属于个人信息,在传统时代下不构成隐私信息,但因为大数据时代匹配能力和风险的大大提高,姓名、手机号和行程信息综合形成的整体信息就具有作为个人隐私保护的必要。还有法院单独适用个人信息权进行判决:如在“丁芝玲与汪锡奎案”^⑨中,汪锡奎未隐去丁芝玲的信息,将与丁芝玲纠纷的判决书张贴在小区报刊栏、发布在公众号等平台。法院认为,判决书上的个人信息仅是丁芝玲身份证上载明的基本信息,且已公开,不构成对其隐私权的侵犯,但构成对公民个人信息权的侵犯。可见,个人信息权利的性质不清,与隐私权的界限不明,导致司法实践对相应的侵权认定亦难有明确的判断基础。

2.关于数据权利性质的争议

随着数据价值的不断凸显,学界逐渐关注到数字经济背景下的数据权利问题,称谓上有企业数据、网络商业数据等。关于数据权利的法律属性,物权说认为,数据是一种特殊类型的物,^[1]数据处理者可对数据享有所有权;^[4]新型财产权说认为,数据财产是信息社会的基础资源,^[5]数据控制者对数据集合享有的对世性的财产权,^[6]应将其作为绝对权保护,^[7]可以原始取得;还有学者将其细分为类似专项经营权的数据经营权和作为归属财产权的数据资产权。^[8]权利性质决定保护方式,数据权利性质不明使得数据主体的利益处于悬而未决的状态,数据控制者对何种数据享有权利、该权利与个人信息权的关系为何仍缺乏探讨。

上述理论争议导致了司法实践对数据权利定性的回避,实际判决几乎全部走上了反不正当竞争的解决道路:如在“百度与大众点评案”^⑩中,法院认定用户评论信息是大众点评的劳动成果但不属于法定权利,虽不属于法定权利,但信息的价值远超以往,市场主体的使用要遵循商业道德、限于合理范围。在“大众点评与爱帮案”^⑪中,法院认为

大众点评对其吸引用户注册、评论而收集、整理的信息享有合法权益,应受法律保护,但并未明确这是何种权益。无独有偶,在“腾讯与抖音、多闪案”^⑫中,法院认可腾讯对其收集并进行商业性使用的用户数据整体享有合法权益,但同样未指明是何种权益。可以看到,法院对于数据权利有着明确的利益保护倾向,但碍于数据权利性质尚未法定,只能迂回地运用反不正当竞争法予以保护。作为资源配置的前提,数据权利的性质及归属亟待确定。

因此,本文试图对现有的隐私、信息和数据概念进行澄清,明确其规范含义,界定并厘清分别以三者为客体的不同权利性质与层次,并构建相应的权利体系。

二、数据、信息及隐私的属性界定

作为客体的隐私、信息及数据在法律上的厘清,是确定其上权利为何以及具体权利属性的前提。

(一)隐私、信息的界定与厘清

《中华人民共和国民法总则》(以下简称《民法总则》)和《民法典(草案)》均同时规定了隐私和个人信息,这说明我国法律中的隐私含义应该是狭义的,至少在理论上它不应该与个人信息存在交叉与相互包容。

我国法律中隐私的应有之义可从以下角度理解:第一,隐私的权利主体只能是自然人,其他主体如法人、非法人组织等都不能成为隐私的权利主体;第二,隐私的客体主要是关涉个人自然存在与社会存在之自由与尊严方面不愿为他人所知的信息,如基因、疾病医疗、性取向等信息;第三,隐私原则上不能自由交易和处分,隐私权作为人格权,在我国理论界和实务界都几乎没有争议,隐私意味着纯粹的人格属性,而不具有财产属性。

我国法律下个人信息的应有之义可从以下角度理解:第一,个人信息的权利主体不仅包括自然人,还可能包括企业、非法人组织等,所有的民事主体皆可为信息主体,这一点并未被现有法律所排除;第二,自然人主体的个人信息,应当是独立于隐私之外、作为单独客体保护的部分;第三,个人

信息的法律属性尽管有争议,但从个人信息作为主体的社会属性及其对主体社会存在的影响上来看,将其认定为人格利益更符合法律的本质要求。但作为人格利益的个人信息中也包含一定的财产利益,只不过该财产属性并不能直接为他人利用。个人信息的人格定性决定了对个人信息的利用需征得权利主体的同意,只不过具体的同意方式(明示、默示等)还可针对具体的利用方式进行细化研究。征得主体同意后,方可把具有人格属性的个人信息通过商品化权或公开化权的方式转化为财产价值予以转让与利用。^[9]

我国狭义的隐私内涵至少在法理上能够与个人信息界分清楚,隐私保护的是主体不愿为人所知的部分信息,而个人信息保护的是主体愿意为人所知,但不愿为人所滥用的部分。由此决定了隐私的保护目标应是禁止任何意义上的公开或侵入,确保隐私不为人所知,而个人信息的保护目标则是保障个人意愿的自由,实现个人对相关公开、利用、处理行为的知情和控制,确保个人信息不为人所滥用。

由于隐私在本质上就是信息,只不过此类信息过于隐秘而主体不愿意为他人所知,法律才将其命名为“隐私”并刻意予以保护。这也引起了实践中往往将隐私和个人信息相混淆的现象,典型的表现就是将个人信息分类为个人敏感信息与一般个人信息,从而带来隐私与个人敏感信息关系之疑惑。从现有规定来看,隐私是指“自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”^③,个人敏感信息是指“一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息”^④。如果个人信息与隐私分别为独立的客体,那么信息再敏感,也不会包含隐私,但上述定义中,“一旦泄露可能危害人身和财产安全,易导致个人名誉、身心健康受到损害或歧视性待遇等”的类型显然包含了隐私在内。此点亦可从《民法典(草案)》第一千零三十四条个人信息中明确包含“私密信息”中看出。《民法典(草案)》试图把隐私与个人信息界分清楚,而实际规定和表述上又模糊不清,原因就在于两者没有在概念内涵上厘清。

其实,如果采用本文的界定,两者在理论上泾

渭分明。但这仅是在概念上,或者在纸面上的界分清楚。而在实践中,仍然难以把隐私与个人信息清晰辨别,尤其对信息利用主体来说更是如此。这是由于隐私的主观性使然。同样的信息泄露,对不同主体产生的影响大不相同。不同的主体对相同信息的珍视与重视程度亦不一样。在此意义上,隐私的界定清楚,除了某些共识性的类型,如性取向、基因信息等之外,其他隐私内涵仅仅停留在法理概念上。而在实践中,隐私的具体范围远非确定,此为不同主体的个体差异性与主观性所决定。

这就要求企业在利用个人信息时,必须设立专门对个人信息予以评估与评判的机构,对哪些信息可能会被信息主体作为隐私对待,哪些信息会被信息主体作为隐私之外的一般个人信息而允许他人利用,事先做出一定的预判。在此意义上,《个人信息安全规范》对个人敏感信息与非敏感信息的分类,可以作为预判隐私与一般个人信息的参考标准^⑤,但它并不影响隐私与个人信息的基本分类,而仅是作为前置预判的操作性标准而已。实际上,现有的个人敏感信息、私密信息,都不是与隐私、个人信息相同意义下的分类,而仅是限于在预判操作、描述意义上的运用。

预判的一般步骤为:先判断某项信息是否为隐私,如可能是,则企业不能为商业利用,如果为了国家安全、社会安全等(如为了抵抗全国范围内的新冠肺炎而使用特定主体的医疗信息)也须依法使用;如否,则适用一般个人信息的保护规则。适用一般个人信息保护规则时,核心前提是如何征得信息主体的同意。同意规则应是确立隐私、信息与数据的客体范围及法律属性后最为重要的制度,也是信息利用的其中一个前提性制度。^⑥经过对隐私与一般个人信息个案预判后的信息利用未必没有争议,因为预判并不能完全代替具体信息主体对其信息的个人判断与个人感受。而一旦发生争议,隐私与个人信息的最终评判还是会经由司法予以判断,这就又回到最初有关隐私与个人信息界定的基本理论,作为司法裁判的参考标准。

(二) 信息、数据的界定与厘清

1. 信息学意义上的信息和数据

信息(Information)、数据(Data)并不是法

学领域的专有名词,学界对信息和数据的定义主要受到信息学、符号学的影响,尤其是持区分说的学者,往往依据其定义的不同,认为二者是内容与形式或内容层与符号层的关系。

信息和数据是否可分?在信息学意义上,数据(Daten)是以0和1的二进制单元表示的信息,这种表示方式以被表示的信息能够从数据中重新还原为前提。因此,数据是表示(Repräsentation)信息并用于处理目的的符号,数据要再现为信息,需要经过抽象化(Abstraktion)的过程。^[10]国际标准化组织(ISO)同样是在信息学术语下进行定义:数据是以适合通信、解释或处理的形式表现的可复译的信息;信息是在特定上下文中具有特定含义的关于特定对象(例如事实、事件、事物、过程或想法,包括概念)的知识。^[11]在知识管理领域,存在着数据、信息、知识和智慧的四分法,数据是对客观事物感知形成的原始记录,对数据进行加工处理、建立联系就形成了信息,对数据和信息的应用提炼出知识,而智慧是在知识基础上的创新性、前瞻性发展,从数据到智慧反映出从低级到高级的认识阶段。^[12]可见,数据既是为特定目的而被改变了形式的信息,也是信息得以形成的基础。因此,在信息学或计算机科学的意义上,信息和数据可以且应当予以区分。

2.法学意义上的信息和数据

信息学意义上的可分性是否意味着具有法学意义上区分的必要性?显然,将其他学科话语体系下的概念直接移植为法律概念并不谨慎。法学意义上信息和数据的关系可以从个人与数据控制者两个层面考察。

从个人层面来看,两大法系均是把法律本质上的个人信息作为权利客体,无论采用个人信息或个人数据的称谓,其含义基本相同。如:欧盟《一般数据保护条例》(GDPR)规定,“个人数据(personal data)是指与已识别或可识别的自然人相关的任何信息(information)”^⑦;德国《联邦数据保护法》(BDSG)规定,“个人数据(personenbezogene Daten)是指所有与已识别或可识别自然人有关的信息(Informationen)”^⑧;美国的许多联邦法律和州法律使用了个人数据

(personal data)的定义,但在美国被广泛接受的概念是PII,即个人可识别信息(personally identifiable information),这两个概念可以互换使用。^[13]我国立法也普遍采用了个人信息的概念。^⑨司法实践中尽管用语较为混乱,但也有规律可循:以“微博与脉脉案”^⑩为例,法院虽然使用个人信息、用户数据信息、用户数据等说法,但在以个人为主体时,其落脚点都在信息,意在强调用户个人的隐私权、知情权、选择权等,只有在指代经处理被提交给企业的信息时,才会混入数据的称谓;而在以企业为主体时,法院多用数据的说法,认为其为商业资本、经营资源、数据资源,主要强调其经济价值。可见,实践中对信息、数据的称谓并不以区分为目的,而是使用习惯使然,是对信息、数据的阶段化理解,人们倾向于在个人掌握阶段称其为信息,在企业掌握阶段,鉴于经过电子化处理、形成数量集合,倾向于称其为数据。

其实,法律对人格权利、知识产权中内含的个人信息保护早已存在,数据所带来的只是个人信息传播形式的变化,单独的、承载着个人信息或隐私的个人数据仍然没有独立价值;即使有一定的潜在价值,通过个人信息、隐私保护也已经足够,没有将其独立为新的权利客体的必要。据此,从法学规范意义的角度来看,在个人层面,信息就是数据,作为法学权利客体的始终只有一个,个人信息与个人数据没有区分的必要性。在国内外立法中,无论使用个人信息或个人数据的表述,其实质都是指个人信息,以0和1的二进制单元定义的数据并不具有法律意义。因此,为在法律意义规范统一表达,建议最好统一使用个人信息(而非个人数据)概念。

从数据控制者的层面来看,无论其使用原始数据还是衍生数据,目的都是获取信息,否则他们与第三方之间的交易就是掩耳盗铃,甚至在数据侵权的情况下,第三方通过网络爬虫等方式抓取数据的目的也是获取信息。大数据时代,真正具有市场价值的仍是信息,但与个人信息有所不同,数据控制者层面的信息往往是一种大数据集合,是对个人信息进行收集、脱敏、整理、加工后形成的海量数据,其与个人信息主体的直接关联往往已经切断,

完全成为外在于人的存在物,甚至负载着加工者、整理者的劳动、智慧。如果数据没有经过脱敏处理,尚能识别出信息主体,在法律上仍需适用隐私、个人信息保护规则处理。只有经过脱敏处理,无法识别或不能直接识别出信息主体的数据,才是真正在法律意义上讨论的数据。由此可见,数据控制者(多为企业)尽管拥有的海量数据在本质上多为他人信息,但为了与个人信息(即信息主体对自身信息所拥有)相区别,本文称之为数据或企业数据。

我国法律中数据的应有之义可从以下角度理解:第一,数据的权利主体主要是对个人信息进行收集、整理、加工等操作的法人(企业)、非法人组织和个人;第二,数据的客体属性本质上仍是信息,通常是批量信息的汇集,这种信息经过脱敏技术处理,切断了与信息主体的关联;第三,数据的法律属性表现为纯粹的财产属性,其转让、利用的自由程度最高。

综上所述,隐私、信息和数据三者作为法律关系客体的特征主要表现为:隐私属于严格意义上的人格利益且不包含任何财产属性,信息主要亦应归属于法律上的人格利益但其中包含着一定的财产属性,数据则仅有财产属性,而无人格属性。^[14]

三、数据、信息及隐私上的权利性质

清楚了隐私、信息及数据的客体法律属性,便可判断存在其上的隐私权、个人信息权及数据权利的法律属性。由于隐私权的人格法律属性已是法律的基本常识,为理论与实践所公认,这部分主要讨论个人信息及数据权利的法律属性。

(一) 个人视角下的信息权利

关于个人信息权利的法律属性,我国学界已多有著述,人格权说相对于财产权说得到了更多学者的赞同,在目前的立法进程中也占据着优势。在清楚界分隐私和信息的基础上,将个人信息权界定为具体人格权相对更为合理,理由包括:

第一,从立法结构来看,《民法总则》虽未明确称个人信息权,但将“自然人的个人信息受法律保护”置于民事权利一章,紧接着一般人格权、具

体人格权的规定,并与隐私权区分开来;^③《民法典(草案)》直接将“隐私权和个人信息保护”并列于第四编的第六章,并对个人信息的范围和保护方式做出了细化,甚至在该章的八条中,六条都用于规定个人信息保护。^④这在一定程度上都体现出将个人信息权独立为具体人格权的意味。

第二,从实际效果来看,肯定个人信息权的人格属性是对人在数字社会存在样态的尊重,同时也有利于个人信息在被充分尊重的前提下得到合理的开发。某种程度上来说,信息是人的社会存在形态,是人的社会属性的碎片,种种信息共同拼凑出数字社会中完整的人。人格要素中最基本的自由和尊严,是人在数字社会中的存在基础,也是个人信息权中最为核心的要素。将个人信息权作为人格权也并不影响个人信息的利用,不同于禁止为商业利用的隐私,个人信息可以被有限地利用,不但是为了发挥其中蕴含的财产利益,更是为整个数字社会尤其是其中人工智能的发展奠定基础。只不过信息的人格权属性决定了信息不能被直接利用,而是须将个人信息中的财产利益属性通过商品化权或公开化权的方式转化为财产利益或价值后,才可为自己或他人予以商业使用。^[15]

第三,从发展趋势来看,对于个人信息和数据,《民法总则》和《民法典(草案)》均已将其纳入权利保护客体的范围,只是尚未明确使用“权”的表述^⑤,但这种较为保守的立法进路与我国“隐私权”的发展路径十分相似。隐私权的保护也是经历了通过名誉权保护隐私权、将隐私作为独立的人格利益、立法明确承认隐私权为独立人格权三个阶段。^[16]既然个人信息权与隐私权在权利主体、客体、属性方面均能明确界分,其作为独立于隐私权的具体人格权进行保护,亦可谓水到渠成。需要指出的是,权利的定性未必一定意味着仅是对义务主体的限制,有时也是对权利主体的限制,这需要法律针对具体的权利形态予以具体规定。权利主体拥有漂亮的私人花园,并不能排斥路人对它的欣赏,只要路人未对该花园造成损害与妨害;尤其是当权利主体的建筑物被定性为文物予以保护时,建筑物所有权人获得相应权利的同时,其对建筑物的使用、处分等也将受到更多的法律限制;同理,

权利主体拥有电话号码、姓名、肖像等信息,并不意味着对他人的绝对排斥,有时反而恰是为了他人使用与认知。

(二) 数据控制者视角下的数据权利

数据控制者层面的数据,是在大数据时代背景下产生的新的权利客体。数据因其稀缺而具有了价值,成为诸多企业视若珍宝的经营资源。数据通过技术手段而可为某一主体所独占,但数字社会的存在样态决定了只有数据共享才能发挥数据的更大价值,也才能为人工智能的发展提供决定其生存的前提,也是保证其健康发展的前提,因为人工智能的发展须臾离不开数据,数据越丰富,其发展越迅速、越有效。数据可以共享,在有合理限制的条件下也应该共享,但这并不意味着数据已成为公共资源。除了一国范围内或全球性的公共数据之外,企业数据或个体数据等皆非公共资源,而是私有财产,否则数据爬取便成为悖论。企业或个人数据的私有财产属性决定了,其主体可以一定的价格将其让渡给他人,贵阳大数据交易所、上海大数据交易中心、武汉东湖大数据交易中心等便是在数据交易的需求下应运而生。数据控制者对数据所享有的财产权,在很大程度上是个人信息权的下游问题,但与此同时,数据也是算法加工、人工智能得以存在和发展的起点。本文关注的重点是,数据控制者可以对哪些信息形成的数据享有权利,数据财产权如何与个人信息权的保护规则相对接。

数据控制者得以建立数据财产权的客体,必须是健康的数据,即一定不能包含侵害他人隐私的数据,一定要经得信息主体知悉同意并有效脱敏的加工数据。^[17]经过信息主体同意而无需脱敏的加工数据的流转仍应依据个人信息保护规则,尤其是其中的同意规则,而不属于在此处讨论的数据利用规则。本文中的数据,是指与信息主体的人格利益联系已被切断的财产性信息,一般包括两类:一种是信息本身就几乎不含有格利益,如用户在大众点评网站上发表的评论;另一种则是经过去标识化处理,如软件安装信息、cookie技术下形成的网络行为轨迹等。

有学者认为,再识别(reidentify)和去匿名化(deanonymize)导致个人能被轻易识别,所谓的匿

名化成为了个人信息利用的避风港。^[18]本文区分匿名化和去标识化,根据《个人信息安全规范》的规定,匿名化(anonymization)要求个人信息主体无法被识别或者关联,且处理后的信息不能被复原。去标识化(de-identification)则是采用假名、加密、哈希函数等技术手段替代对个人信息的标识,达到的结果只是在不借助额外信息的情况下,无法识别或者关联个人信息主体。^[3]因此,去标识化的信息仍有被间接识别的可能性,标准匿名化的信息则往往难以再有可能被识别出来,因此去标识化的信息仍属于个人信息,匿名化的信息则是非个人信息。目前,技术上尚不能对匿名化作出绝对的保障,但去标识化的手段已经比较完善,将其作为数据处理的基本要求也较为合理。

去标识化应当成为数据财产权客体的最低标准,也是处理数据财产权与个人信息权关系的关键。如果数据控制者收集、利用的信息被判断为隐私,则数据控制者无论如何均不能侵犯,更不可能在他人隐私上形成自己的数据财产权;如果数据控制者经信息主体知情并同意收集、利用信息,但未进行去标识化等脱敏处理,而是直接利用,则数据控制者只能获得相应的使用权,无从形成数据财产权;只有剥离他人隐私,经由信息主体知情同意(或其他合法性事由),且已去标识化的数据,才有可能成为数据财产权的客体。

个人信息权与数据财产权的关系架构在实践中已经有所体现,如在“淘宝与安徽美景案”^[3]中,法院的判决思路已经在对个人信息、个人信息直接转化的原始数据、网络运营者加工形成的数据产品进行分别评价。个人信息权与数据财产权并不矛盾,前者以保护个人信息权中的人格利益为重点,个人信息中的财产属性利用则是个人信息权中的衍生利益或衍生价值。因个人信息中具有不同程度的财产利益属性,由之产生的数据便成为数据财产权中类型多样的“原料”。数据财产权以数据控制者为主体,可以是企业、机构或个人等。由于须经去标识化处理方可利用与转让,此时的数据已不再蕴含具体主体的人格利益,而仅有纯粹的财产价值,从而成为数据财产权的核心。需要注意的是,数据在本质上毕竟是个人的信息的综合,即使已去标识化,也

并非与信息主体绝对不能关联，一旦被标识，则又要返回到隐私或个人信息的法律规则予以处理。

四、数据、信息及隐私上的权利层次与体系

明确了数据、个人信息与隐私的法律客体特征及其上的权利属性，相应的权利层次划分和体系建构便也有了法律根基。

数据、个人信息和隐私在本质上都是信息，即使是同一条信息，也可能在不同的情形下成为数据、个人信息和隐私的客体。以电话号码为例，一般而言只是个人信息，在主体将其用于社会联络和交往时就更是如此；但是，若该电话号码属于工作带有保密性质的人员，或是专用于同家人联系的号码，便有可能属于隐私；而当电话号码被去标识化，无法与主体直接联系时，就会成为数据。因此，隐私权、个人信息权和数据权，实际上是在权利主体信息之上依据权利主体对该信息内在感受的私密程度以及该信息对权利主体外在表征的紧密程度，所形成的层次性保护，并共同构筑起对信息保护的体系。结合图1，在信息之上存在的权利层次及体系详述如下：

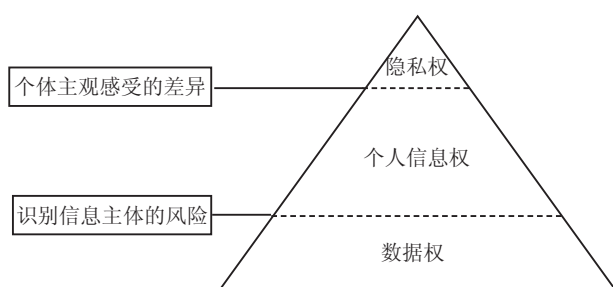


图1 信息之上的权利层次性与保护体系

首先是在隐私信息之上存在的隐私权。由于权利主体对隐私信息最为敏感且不欲为外人所知，而且此类信息对权利主体的外在表征也最为强烈，即他人往往对该信息也较为敏感而关注，法律对于隐私权的保护最为严格。隐私权是作为人之社会存在并体现着权利自由与尊严的最为重要的要素之一，因此是最为典型的一种人格权。有关隐私权的具体内容，法律可以直接明确规定的仅有性取向、艾滋病等特定疾病信息、基因信息等为民众普遍认同的

部分信息，但隐私信息强烈的主观性决定了其难以被法律全面规定。这给企业对信息的利用者带来极大困难，也是隐私信息给信息利用者带来的天然难题，需要企业正确而理性地面对。一方面，企业利用个人信息时要时刻警醒头上悬着的隐私之剑，不要触碰；另一方面，对于实践中有关隐私引发的争议最终只能交由司法予以判断。了解了隐私权的这些特点，便可知隐私处于信息之上权利体系的金字塔尖，但其范围与内容较其他信息来说，往往最稀少，这也决定了隐私权作为保护信息内容的一种权利，尽管其客体内容最少，但恰恰是最显性的权利，唯此才能强调与强化对隐私的保护，因此它位于信息之上三种权利的最顶端。

其次，是在个人信息之上存在的个人信息权。权利主体对该部分信息尽管也较为关注和关心，但毕竟不如隐私信息那么敏感，此类信息权利主体的外在表征也非常强烈，他人对该信息也比较敏感而有兴趣予以关注。以此类信息为客体的个人信息权，便也因为该信息外在体现出的权利主体的社会属性以及权利主体对该信息的敏感性而具备了明显的人格属性。但是，毕竟此类信息并非权利主体不欲为人所知而刻意掩藏或掩盖的信息，因此可以为他人商业利用，只不过须征得权利主体的同意。当下企业利用个人信息面临的矛盾主要是个人信息主体同意的方式到底如何确定，以及从人格属性的个人信息权到财产属性的商业利用，中间的具体环节应如何设定。而且，决定上述难题最为核心的问题还在于企业与个人信息提供者之间的利益分配仍未有效解决。清楚了个人信息以及个人信息权的这些属性便清楚，应然意义上的个人信息权是不包括隐私的信息权。此类信息的范围远大于隐私范围，从而也决定了个人信息权的范围也远大于隐私权的范围。由于隐私与个人信息并非泾渭分明，这也决定了隐私权与个人信息权也会存在模糊空间。而在社会的显性存在样态上，法律并没有像隐私权保护那样单一而严格，个人信息权的权利属性与存在样态也较为多元：即个人信息权尽管属于人格权利，但其中也包含着财产属性，而且这种财产属性可为企业等外在主体利用。在权利保护强度上，该权利位于信息之上三种权利的中端。

最后,是在数据信息之上存在的数据权。由于本文界定的数据是狭义上的数据,仅指经去标识化等脱敏手段无法识别具体信息主体的信息。此类信息既然不再跟具体信息主体关联,信息主体对该信息也不再关心、在意,更谈不上敏感。因此,数据上的权利不再具有任何人格属性,而仅具有财产属性,是一种纯粹的财产权利。此类权利仅对数据拥有者有意义,而不再直接对信息主体有价值。严格来讲,此类权利已经从具体信息主体的信息权利中剥离,而转变为独立的财产权利。它位于整个信息之上三种权利的底端。该权利可自由转让,自由交易。之所以其在图表中仍跟个人信息权没有绝对分离,原因就在于,脱敏等技术手段的运用仍然存在再次识别信息主体的风险。而一旦主体被识别,相应的信息便从数据中抽离,重新返回到隐私权或个人信息权的保护范围,并适用相应的保护规则和救济途径。

可见,实践中的隐私权、个人信息权和数据权的客体范围并非泾渭分明,许多信息都处于图1所示的虚线上下,个体主观感受的差异带来隐私与个人信息之间相互游离的可能性,识别信息主体的风险则导致数据可能回溯成为个人信息甚至隐私。但是,依托于具体情境和个案判断,任何发生争议的权利属性即便不能直接依据法律的规定而判明,最终也将通过司法裁判而确定。建立在信息之上三个层次的权利,共同构筑了保护各类信息的严密权利体系。从隐私权、个人信息权到数据权利,既注重了信息主体对其信息内在主观感受的敏感与关注程度,也注重了各种信息对信息主体外在表征的紧密程度。信息之上所形成的数据权、个人信息权及隐私权层次分明的权利保护体系,为理解信息、研究信息、利用信息提供了理论前提与法理基础。

五、结语

隐私、信息与数据的厘清及其上权利定性与体系建构是在为整个数字社会的运转搭建法律基础。只有把隐私、信息与数据的权利定性与客体属性在法律上界分清楚,我们方可知信息是整个数字社会的存在基础,它既是数字社会的土壤(脱敏后的信

息)而为任何主体拥有甚至交易,也可成为数字社会中的氧气(如公共信息)为任何人所吸取(利用)。数字社会中的主体(自然人)仍有不为任何利益所触动的自由与尊严需求,那就是人的隐私;数字社会中个人信息的人格属性也决定了其不能为他人直接利用,须转化为财产利益后方可交易,而且须以信息主体的同意为前提。

隐私、信息与数据上的权利定性也为信息主体的同意规则研究创造了前提。同意是个人信息利用的核心,但一对一(信息主体、网络平台、信息利用者)相互之间采用传统意思表示的同意规则(如三重授权规则)应该并不适合数字社会中的信息利用方式。目前同意规则或是对信息主体而言是掩耳盗铃式的存在(其不得不同意),对信息主体起不到任何保护作用,或是阻止其进入网络领域的实际伤害(若其不同意的话)。这就要求我们必须采用开放性思维寻求契合数字社会的信息利用同意模式。

隐私、信息与数据的权利定性也为个人信息的定价或价格创造了前提,个人信息中包含的财产属性决定了个人信息中的财产属性可以为他人利用并带来财产价值。但符合数字社会的思维模式是,个人信息中财产属性的利用并不能采用线下传统社会一般财产的交易模式,否则无论是对企业还是对具体信息主体都难以操作,且也没有效率。这就要求我们必须采用开放式思维,着眼于具体信息主体的利益保护并非数字社会应然的思维模式。数字社会应然思维模式应该以数据控制者或数据利用者为思考问题的着眼点,首先,肯定数据利用者对整个数字社会的构建所做出的贡献,没有这些平台或企业,数字社会便不会存在;其次,也要对数据利用者对数据的利用进行限制,必须要依法利用,底线是不能侵害信息主体的隐私;最后,数据利用者也要为初始信息的获取付费,只不过该付费未必是直接交由信息主体,而可由国家专门建立的税收、基金、信托等部门代为收取,然后再将该费用服务于信息主体;等等。隐私、信息与数据的厘清及其上权利定性与体系建构仅是步入数字社会的门槛,但其已开启以人工智能所引领的多元与精彩之数字社会发展的序幕。

注释

- ① 参见吉林省四平市中级人民法院(2018)吉03民辖终31号民事裁定书。
- ② 参见上海市青浦区人民法院(2017)沪0118民初6453号民事判决书。
- ③ 参见广东省珠海市香洲区人民法院(2018)粤0402民初7843号民事判决书。
- ④ 参见王融:《大数据时代:数据保护与流动规则》,人民邮电出版社2017年版,第19页;郭瑜:《个人数据保护法研究》,北京大学出版社2012年版,第127-128页。
- ⑤ 参见程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018年第3期,第105页。
- ⑥ 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117页;胡凌:《商业模式视角下的“信息/数据”产权》,《上海大学学报(社会科学版)》2017年第6期,第3页。
- ⑦ 参见陆小华:《信息财产权——民法视角中的新财富保护模式》,法律出版社2009年版,第277页。
- ⑧ 参见梅夏英:《数据的法律属性及其民法定位》,《中国社会科学》2016年第9期,第168、181页。
- ⑨ 参见纪海龙:《数据的私法定位与保护》,《法学研究》2018年第6期,第72-76页。
- ⑩ 欧盟《一般数据保护条例》(General Data Protection Regulation),德国《联邦数据保护法》(Federal Data Protection Act),法国《数字共和国法案》(Digital Republic Law),英国《2018年数据保护法》(Data Protection Act 2018),新加坡《个人数据保护法》(Personal Data Protection Act)。
- ⑪ 加拿大《个人信息保护法案》(Personal Information Protection Act),韩国《个人信息保护法》(Personal Information Protection Act),日本《个人信息保护法》(Act on the Protection of Personal Information)。
- ⑫ 北京知识产权法院(2016)京73民终588号民事判决书。
- ⑬ 参见《中华人民共和国民法总则》(以下简称《民法总则》),第一百一十条;《中华人民共和国民法典(草案)》(以下简称《民法典(草案)》),第九百九十条。
- ⑭ 参见张里安、韩旭至:《大数据时代下个人信息权的私法属性》,《法学论坛》2016年第3期,第124-127页。
- ⑮ 参见叶名怡:《论个人信息权的基本范畴》,《清华法学》2018年第5期,第145-146页。
- ⑯ See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1246(1998);陆小华:《信息财产权——民法视角中的新财富保护模式》,法律出版社2009年版,第87页。
- ⑰ 参见北京市第一中级人民法院(2015)一中民终字第09558号民事判决书。
- ⑱ 参见北京市第一中级人民法院(2017)京01民终509号民事判决书。
- ⑲ 参见四川省德阳市旌阳区人民法院(2017)川0603民初4743号民事判决书。
- ⑳ 参见上海知识产权法院(2016)沪73民终242号民事判决书。
- ㉑ 参见北京市第一中级人民法院(2011)一中民终字第7512号民事判决书。
- ㉒ 参见天津市滨海新区人民法院(2019)津0116民初2091号民事裁定书。
- ㉓ 参见《民法典(草案)》第一千零三十二条。
- ㉔ 参见《信息安全技术 个人信息安全规范》(GB/T 35273-2020),第3.2条。
- ㉕ 参见《信息安全技术 个人信息安全规范》(GB/T 35273-2020),附录B。
- ㉖ 限于其重要性及复杂性,拟专文研究。
- ㉗ 参见欧盟《一般数据保护条例》(General Data Protection Regulation),第4条第1款。
- ㉘ 参见德国《联邦数据保护法》(Bundes daten schutzgesetz),第46条第1款。
- ㉙ 参见《民法总则》第一百一十一条、《电信和互联网用户个人信息保护规定》第四条等。
- ㉚ 参见北京知识产权法院(2016)京73民终588号民事判决书。
- ㉛ 参见《民法总则》,第一百零九至一百一十一条。
- ㉜ 参见《民法典(草案)》,第一千零三十二至一千零三十九条。
- ㉝ 参见《民法总则》,第一百一十一条、第一百二十七条;《民法典(草案)》,第一千零三十四条。
- ㉞ 参见《信息安全技术 个人信息安全规范》(GB/T 35273-2020),第3.14条、第3.15条。
- ㉟ 参见浙江省杭州市中级人民法院(2018)浙01民终7312号民事判决书。

参考文献

- [1] 涂子沛. 数文明: 大数据如何重塑人类文明、商业形态和个人世界[M]. 北京: 中信出版社, 2018: 229.
- [2] 王利明. 论个人信息权的法律保护[J]. 现代法学, 2013(4): 66-67.
- [3] 沈德咏主编. 《中华人民共和国民法总则》条文理解与适用(下)[M]. 北京: 人民法院出版社, 2017: 66.
- [4] 丁道勤. 基础数据与增值数据的二元划分[J]. 财经法学, 2017(2): 5.
- [5] 齐爱民, 盘佳. 数据权、数据主权的确立与大数据保护的基本原则[J]. 苏州大学学报(哲学社会科学版), 2015(1): 69.
- [6] 许可. 数据保护的三重进路[J]. 上海大学学报(社会科学版), 2017(6): 23.
- [7] 纪海龙. 数据的私法定位与保护[J]. 法学研究, 2018(6): 83.
- [8] 龙卫球. 数据新型财产权构建及其体系研究[J]. 政法论坛, 2017(4): 74-76.
- [9] 彭诚信. 数据利用的根本矛盾何以消除[J]. 探索与争鸣, 2020(2): 80-82.
- [10] Vgl. Heinz-Peter Gumm, Manfred Sommer. Einführung in die Informatik[M]. 10. Auflage, Oldenbourg Verlag, S. 4.
- [11] ISO/IEC 2382: 2015 (en) Information technology - Vocabulary: 2121272 data, 2121271 information [EB/OL]. [2020-04-08]. <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:vl:en>.
- [12] 荆宁宁, 程俊瑜. 数据、信息、知识与智慧[J]. 情报科学, 2005(12): 1786-1790.
- [13] See Paul M. Schwartz, Daniel J. Solove. Reconciling Personal Information in the United States and European Union[M]. 102 Calif. L. Rev. 877, 878-879 (2014).
- [14] 彭诚信. 数据利用的根本矛盾何以消除[J]. 探索与争鸣, 2020(2): 82-84.
- [15] 彭诚信. 数据利用的根本矛盾何以消除[J]. 探索与争鸣, 2020(2): 82.
- [16] 程啸. 侵权责任法[M]. 北京: 法律出版社, 2015: 165-166.
- [17] 彭诚信. 数据利用的根本矛盾何以消除[J]. 探索与争鸣, 2020(2): 84.
- [18] See Paul Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization[M]. 57 UCLA L. Rev. 1701, 1701-1704 (2010).

On the Right Levels and System Construction of Data, Information, and Privacy

PENG Chengxin YANG Siyi

Abstract: Privacy and personal information have separate connotations in Chinese laws, where the protection range of sensitive personal information has been fully entailed within that of privacy; therefore, they should not be parallel categories. Privacy and personal information should share a border line which needs to be specifically defined in individual cases. The division between information and data in informatics does not equal that in law. On the person level, personal data is personal information, so right objects possess personal information only; while on the data controller level, the object of property right refers to the desensitized data that is unidentified, or cannot be directly identified with its information subject. Thus, defining privacy, information, data, and the rights attached to them, as well as constructing the system, created presupposition for the existence and development of the whole digital society.

Key words: privacy; personal information; data; right level; right system