【文章编号】1002—6274(2020)04—003—12

《民法典》与信息社会^{*}

——以个人信息为例

王洪亮

(清华大学法学院,北京 100084)

【内容摘要】从信息社会的基本内涵、特征出发,处理个人信息时需协调个人信息保护与信息流动的关系,构建政府、信息处理者以及信息主体之间共生共存关系。首先,《民法典》第1034条规定了比较窄的个人信息范围,没有完全反映技术的发展,也没有完全覆盖信息主体的核心利益。其次,《民法典》将个人信息分为私密信息、公开信息以及一般个人信息,对于私密信息,通过隐私法与个人信息保护法双重保护,但双重保护会带来规则之间的冲突,也没有必要性。依据《民法典》,信息主体享有查询、复印、更正以及删除等权利。这些权利均不构成对信息的收集、处理与流动的障碍,属于信息主体的核心利益。最后,《民法典》第1035条规定了收集、处理个人信息应当遵循的原则。适用该规则的主体既包括信息收集者,也包括信息处理者,甚至包括信息处理各个环节的主体。信息处理者在收集、处理个人信息时,应当合法、正当、必要且最小够用。最为重要的是,信息处理者在收集、处理个人信息时,须取得信息主体的同意。知情同意是信息主体的核心利益,不可让渡。

【关键词】个人信息 信息主体 私密信息 信息控制者 信息处理者

【中图分类号】DF51 【文献标识码】A

当今社会,电子信息技术蓬勃发展,数据挖掘、处理能力极大地增长。基于信息技术的智能工具日益成为表征性的社会工具,信息产业成为基本社会产业,信息产品越来越成为表征性的社会产品,信息、知识成为重要的生产力要素,人类社会已经从工业社会转向信息社会。^[1]

信息技术处理的“原料”是数据、信息、知识,信息成为社会发展的基本资源,通过信息的创新、共享、传播和创造性使用,大幅度地提高知识生产率和生产力水平。^[2]一方面,传统产业经营者大量收集和处

理个人信息,以把握市场需求、提高生产能力、获得高额回报;另一方面,还出现了专门收集、处理信息的信息服务提供者。而信息资源主要来自于个人,个人信息对于社会发展、经济发展起到了基础性作用。

信息社会的核心价值理念是“自由、开放与共享”,^[3]其天然地要求个人信息向社会输出。但个人信息本身又是个人人格的组成部分,与人不可分离,

其本质要求封闭式的保护,最理想的保护模式就是隐私权保护模式。由此形成了个人信息保护与个人信息收集、处理与流动之间的矛盾。个人信息法的主要任务就是处理这一对矛盾。比较新近的欧盟《一般数据保护条例》在“鉴于条款”第2条就做了这样的规定:“本条例致力于实现自由、安全、公平和经济联盟,致力于经济和社会进步,加强并聚集内部市场的经济,实现个人的幸福”。《民法典》关于个人信息保护规则也是建立在个人信息保护与数据流动之间的平衡的基础之上。^[4]^{P203}

信息社会中,对于个人信息享有独立利益的主体日益多元化。信息业者在个人信息的收集与处理中享有巨大的商业利益,而国家也不是超然的法律规则制定者和执行者,同时也是个人信息最大的收集、处理、储存和利用者。^[5]政府之所以收集处理个人信息,一方面是为了社会管理与社会福利的增进,另一方面是为了提高行政能力与行政效率。有意思的是,

* 基金项目:本文系国家电网有限公司总部科技项目“电力数据权属和商业应用法律关键技术研究”(1200-2020057234A-0-0-00)的阶段性成果。

作者简介:王洪亮(1973-),男,黑龙江海伦人,法学博士,清华大学法学院教授、博士生导师,研究方向为民法学。

自然人个人、信息业者与政府之间,在个人信息收集、处理、利用方面处于共生关系之中,相互依存。个人信息的收集、处理、利用往往对彼此都有利。比如,企业收集处理数据,固然存在独立的经济利益,但个人也具有利用信息包括利用他人个人信息的需求。^[5]所以,在个人信息保护与利用方面,需要平衡个人对个人信息保护的利益、信息业者对个人信息利用的利益和国家管理社会的公共利益。个人信息保护法要保护各利益主体的核心利益,但相应地各利益主体也需要让渡其非核心利益。^[5]

《民法典》总则编中规定了个人信息保护的一般原则,与此同时人格权编第六章“隐私权和个人信息保护”中规定了个人信息保护的基本框架规则,具体包括个人信息的界定、个人信息处理的原则、个人信息保护的边界等。这些规范构建了未来个人信息保护法的制度框架与基础。不过,需要解释的是,在信息社会基本价值理念下,个人信息的范围有多大,个人信息中含有何种利益,其权利边界何在,对于个人信息的收集与处理的前提是什么。

一、信息社会中个人信息的界定

信息社会中,随着技术发展,越来越多的个人信息作为国家、社会与经济的原材料,^[6]而相应地,法律对于个人信息的界定也随之不断发展。比如,在房地产交易中,国家要求当事人进行网签,对于当事人的个人信息、交易信息乃至财产信息均予以采集、处理。在防疫阶段,社会组织也搜集了大量个人身份信息与个人行为轨迹。在经济上,国家电网通过用电量、用电习惯也可以进行精准分析个人消费习惯乃至进行环境保护分析。

(一) 个人信息内涵的沿革

早在2000年12月28日,全国人大常委会《关于加强网络信息保护的決定》第4条规定“非法截获、篡改、删除他人电子邮件或者其他数据资料,侵犯公民通信自由和通信秘密”可构成犯罪,其中仅列举规定了电子邮件和其他数据材料等个人信息,既不全面,也没有抓住个人信息内涵的本质。2012年全国人大常委会《关于加强网络信息保护的決定》第1条以抽象概括的模式规定了个人信息,即能够识别公民个人身份和涉及公民个人隐私的电子信息的权益。这一规定抓住了个人信息内涵的本质,但不完全。

2013年,《电信和互联网用户个人信息保护规

定》第4条采取了比较全面的列举与概括的模式规定了个人信息的内涵。所谓个人信息,是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。2017年6月实施的《网络安全法》第76条也采纳了这种定义的模式,其规定的个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息,包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。至此,现行法比较准确地界定了个人信息的内涵,并且基本上能够与现代信息技术的发展相适应。

(二) 《民法典》中个人信息的新发展

《民法典》第1034条规定“个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱地址、行踪信息等。”

首先,有疑问的是,个人信息的形式是否限于电子形式。全国人大常委会《关于加强网络信息保护的決定》中明确使用的是“公民个人电子信息”的概念,而《电信和互联网用户个人信息保护规定》则没有明确限制个人信息的表现形式,《网络安全法》更是明确了个人信息可以是电子或其他形式记录的。《民法典》第1034条也明确了个人信息可以是电子的,也可以是其他方式记录的。一些采用传统形式处理的有关个人的信息也应当在个人信息概念的涵摄之下,比如纸版呈现的个人信息。

其次,在个人信息列举的层面,与《网络安全法》第76条相比,《民法典》第1034条增加了电子邮箱地址和行踪信息两个新的类型。^{[41]P209}但该条并没有穷尽目前技术手段下可能的个人信息类型,比如IP地址等网络日志信息、手机广告标识符或者如mac等永久标识符等设备地址、浏览记录等无法直接识别用户身份,但可与其他信息结合识别用户身份的信息。根据欧盟《一般数据保护条例》第4条第1款的定义,个人数据是指关于已经识别或可识别的自然人(或称数据主体,Data Subject)的任何信息,可识别的个人是指可以直接或间接、特别是通过姓名、身份证

号码、位置数据、在线标识(Online Identifier)或身体、生理、基因、精神、经济、文化或社会身份之一或若干特定因素而可识别的人。相较于欧盟《个人数据保护指令》,^[7]《一般数据保护条例》关于个人信息的界定增加了个人位置数据、在线标识等具体的类型,反映了现实中信息技术发展带来的新问题,使得个人信息概念更加清晰、更加便于判断。

再次,“可识别”所指向的应当并非是非自然人的整体,而是针对自然人的身份或者某一身份要素,甚至针对的是用户所使用的设备标识。^[8]随着科学技术的发展,只要能通过大数据分析,识别自然人的某一身份,就可以带来巨大商业利益。从反面讲,也可能通过某一身份的识别对个人人格形成侵害。所以,《民法典》第1034条应当全面列举个人信息自然属性以外的精神、经济、文化以及社会等属性。^[9]欧盟《一般数据保护条例》第4条第1款即明确列举了身体、生理、基因、精神、经济、文化或社会等因素。

最后,个人的信息核心要件是个人信息的可识别性,^{[4]P209}对于不可识别的个人信息,并不受《民法典》中个人信息保护法的保护。

传统的保护隐私的方法是不允许第三人对外披露,但对于个人信息不能作如此简单的处理。在个人信息处理上,信息的流动带来了巨大的商业利益,并拓展了人类决策能力。将个人信息投入商业利用,就必须在一定程度上向第三人公开。而如果一旦向第三人公开,就有可能侵害个人信息自决权。所以,为了平衡个人信息的利益与商业利益,只有可直接或间接识别的个人信息才是确立法律保护个人信息。通过可识别性这一概念,兼顾了信息流动的好处和对个人信息的有力保护。

为了达到个人信息不可识别的目的,网络经营者要对个人信息进行匿名化处理,匿名化有助于在保护个人信息的同时,促进个人信息的自由流通。^[10]具体而言,匿名化是对个人数据的修改,匿名化后,该信息与个人就不再相关联。采用的具体手段有泛化、压缩、分解、置换以及干扰等。

除了匿名化方式,还有假名化处理方式。假名化是指不附加信息即无法将个人数据归属到特定数据主体,可以是以特定的标志替代姓名或其他特征。与匿名化的常用工具不同,假名化无需将个人数据移除或隐藏起来,更多地是将一个直白的文字转化为令人

无法理解的密码。例如:真实的个人数据是“王大明,65岁,糖尿病患者”,而假名数据可能是“00108,65岁,糖尿病患者”。^[8]而且,假名化需要额外的技术与组织手段保障。必须加密信息,并由少数人保有密匙。假名化下识别个人信息的风险要大于匿名化下识别个人信息的风险,因此,通常情况下,假名化的个人信息是可识别的,至少是可间接识别的。只有在假名构成通过技术保障数据适当方法使个人信息不可识别的情况下,假名化的个人信息才是不受保护的信息,不适用个人信息保护法下的各种规则。^{[11]P15}

值得注意的是,在计算机信息技术发达的社会,匿名化是相对的。在大数据时代,由于信息量庞大,通过再识别技术以及去识别化技术,将匿名的记录与外部信息相联系起来,即可以发现隐私数据,挖掘数据主体的真实身份。所以绝对的匿名化是做不到的,只能在一定程度上避免数据信息被特定到个人。^[12]

在个人信息的判断上,《民法典》采取了绝对标准与相对标准相结合的方式,如果数据本身即可以指向个人身份,即构成受保护的个人信息,即绝对性标准,只要任何人可能将处理的数据与个人联系在一起,即构成受保护的个人信息。^[13]除此之外,如果信息与其他信息结合可以识别自然人个人身份的各种信息,也是受保护的个人信息,而且,这里的其他信息未必是信息控制者或者处理者所占有的信息。对于可识别的个人信息,采取的是相对标准,即如果对控制人或处理人而言,基于其无须不成比例的努力可接入其他额外信息的机会,识别数据主体是可能的,那么就是可识别的数据,受保护的数据。综合来看,《民法典》保护的个人信息有两种:一种是通过该个人信息可以直接“认出来”自然人。另一种是,该个人信息要结合其他信息,间接地可以“认出来”自然人。进一步来看,认出来“自然人”的含义,主要是指“认出来”自然人身份,而且,未必是全面“认出来”自然人各种身份,也可以是“认出来”自然人社会、经济、文化等身份中的一个身份,甚至是设备终端。

在“北京百度网讯科技有限公司与朱烨隐私权纠纷案”中,百度网讯公司利用cookie技术收集朱烨信息,并在朱烨不知情和不愿意的情形下进行商业利用,问题的焦点在于,该个人信息是否具有可识别性。对此,二审法院认为:百度网讯公司在提供个性化推

荐服务中运用网络技术收集、利用的是未能与网络用户个人身份对应识别的数据信息,该数据信息的匿名化特征不符合“个人信息”的可识别性要求。^①不过,值得质疑的是,法院在这里使用的可能是直接识别的概念,若将个人信息保护范围扩展到间接识别的范畴内,法院的处理就不恰当了。在该案中,百度网讯公司可以精准销售,已经意味着间接识别到了原告的身份或使用的设备。

之所以将可识别性扩大到间接识别,主要原因在于:在现实中,如果需要的时间、成本与人力上花费不成比例的努力才可能识别个人数据的情况下,识别的风险似乎是微不足道的。^{[11]P12}因此,如果识别到个人所缺失的信息很容易获得的情况下,如在网络上或者商业信息服务中可获得或者很容易获得的情况下,即可以认定可识别的个人信息。所以,在确认可识别性上,首先考虑识别所需的时间与成本,除此之外还需考虑在处理时可能的技术以及技术发展,但并不要求控制与处理人在做出决断处理过程中考虑可预见的或可能的技术发展,只是对各种数据处理技术进行风险评级,定性定量;再次,需要考虑处理的目的,区分为了研究目的、商业目的以及某些具有恶意主观目的等;最后,还要考虑个人信息公开的范围,如果数据匿名化之后被公布,则除了数据控制者之外,还要考虑能够获得该数据的第三方,其所能够获得的数据资源、数据能力,以及在此基础上对匿名化数据重新恢复身份的可能性。^[8]

在信息透明的时代,匿名化有时也会带来人格权保护的窘境,比如匿名者或者假名者侮辱、诽谤他人的情况,匿名保护了匿名者或假名者自己的自由,却使得相对人无法追究匿名人的责任。^[14]通过可识别标准,保护信息主体的核心利益,而信息主体也让渡了不可识别的个人信息这一非核心利益。匿名化处理的个人信息,无法直接或间接地识别个人,所以就丧失了个人信息的最本质特征,因而也就已经不再属于个人信息。信息处理者即可以进行自由处理,包括不经信息主体同意而向他人提供(《民法典》第1038条第1款后段)。^{[4]P227}

二、信息社会中个人信息的赋权

在《民法典》制定过程中,个人信息是一种权利,还是一种权益,是一种什么样的权利,是一个争论最多的问题。肯定论者认为,个人信息是一种权利,而

且是一种具体人格权。^{[9][15][16]}个人信息权是指自然人依法对其本人的个人身份信息所享有的支配并排除他人侵害的人格权,包括保有、决定、知情、更正、锁定等权利内容。^{[17][18]P137}反对论者则认为,个人信息的若被界定为绝对权和支配权,会造成信息无法自由地流动,将每个人变成一座孤岛而无法进行正常的社会交往。^[19]而且,绝对权模式下无法承载不同价值和利益的平衡。

对此问题,《民法典》总则编第111条只是笼统地规定了个人信息受法律保护,没有具体规定“个人信息权”受法律保护。《民法典》人格权编第六章的标题是“隐私权和个人信息保护”,同样也没有规定个人信息权。由此可见,《民法典》的起草人经过研究比较,最终还是采用了个人信息保护的表述,这主要是因为个人信息的保护中要适当平衡信息主体的利益与数据共享利用之间的关系,并且不会形成绝对权的误解,从而有利于数据的共享、利用以及大数据产业的发展。^{[4]P213}

其实,个人信息到底是不是权利,涉及对权利的界定。权利既有利益的内容,也具有个人意志支配力量的内容。^{[20]P499}个人信息本身是符合权利这两个内涵的:其一,个人信息具有利益的内容,主要体现为个人自决的利益以及可被利用的利益;其二,个人信息中也含有支配的力量,《民法典》人格权编就规定了个人信息的查询权以及删除权等。所以,不可否认个人信息是一种权利。但这种权利,不同于私法上的权利。私法上权利,一经同意转让,即权利用尽,不能再请求返还或者更正,受让人再利用时,也无须在内容、范围、转让对象上受制于原权利人。但在个人信息权情况下,经过个人信息权利人同意而收集之人,再次利用或者扩大范围利用时,还是需要经过个人信息权人的再次同意,而且,个人信息权人一定条件下可以请求更正或者删除,甚至可以行使携带权。

另外,个人信息也不是一种人格权。对于人格权,一般认为是一种绝对权,具有排他性。^{[20]P512}个人信息权往往不具有排他性,民事主体可以收集、处理个人信息,但要经过个人信息权人同意,并遵守公开、合理等原则。而且,个人信息也不一定含有任意处分的内容,如对姓名、头衔、学历、家庭住址等个人信息,没有完全自决的可能性。^[21]另外,并非所有的违反个人信息保护法的信息处理行为都侵害了他人的人格

权,比如故意错误传递信用信息,并不会使信息主体的名誉当然受到侵害。^[21]个人信息只是中含有一定的利益,如知悉个人信息被处理的利益、个人信息正确和完整的利益、个人信息处理须符合特定目的的利益以及隐私利益,^[21]并含有查询、更正等法律之力。所以,个人信息权只能是一种独立的权利。

(一) 个人信息的分类保护

《民法典》中区分了一般个人信息、私密信息以及公开信息,对于私密个人信息加强保护,对于公开信息则采取了弱化的保护。

1. 属于私密信息的个人信息

在人格权保护体系思路下,《民法典》并列规定了隐私权与个人信息。《民法典》第1032条第2款将隐私区分为三类:私密空间、私密活动以及私密信息。而《民法典》第1034条第3款规定了“个人信息中的私密信息”,也就是说,有些私密信息可能属于个人信息,对于个人信息中的私密信息要特殊保护。

首先需要澄清的是,私密信息与个人敏感信息的关系是什么。《信息安全技术:公共及商用服务信息系统个人信息保护指南》区分了个人敏感信息和个人一般信息。而所谓个人敏感信息,是指一旦遭到泄露或修改,会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。^②对此,有学者认为,来自域外立法的敏感的个人敏感信息所包含的范围非常广泛,但其中很多不适合我国国情。^[22]还有学者认为,个人敏感信息界定为“会对个人信息主体造成不良影响”,过于宽泛,而且也折损了敏感信息与一般信息的区分意义。^[5]对于个人敏感信息的界定应考虑我国文化传统、社会普遍价值观、法律传统、风俗习惯等因素。所以,应将个人敏感信息限缩为“个人敏感隐私信息”,即关涉个人隐私核心领域、具有高度私密性、对其公开或利用将会对个人造成重大影响的个人信息,如有关性生活、基因信息、遗传信息、医疗记录、财务信息等个人信息。^[5]

2012年最高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第12条首次采用了个人隐私信息的思路,其规定网络用户或者网络服务提供者利用网络公开自然

人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息,造成他人损害,被侵权人请求其承担侵权责任的,人民法院应予支持。

基于上述考虑,《民法典》没有采纳个人敏感信息的概念,而是使用了“个人信息中的私密信息”这一表述。欧盟《一般数据保护条例》在明确区分二者的基础上,原则上禁止个人敏感信息的收集和处理,但《民法典》并无类似的禁止规则,只是在保护上可以适用隐私权法规则,以加强保护。^{[4]P213}《民法典》第1034条第3款规定:个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定。实际上将个人信息区分为私密信息的个人信息以及一般的个人信息。对于私密信息的个人信息,进行特别保护。首先,私密信息是一种隐私,受隐私法保护,其次,隐私法中没有规定的,而个人信息保护法中有规定的,对私密信息也适用,比如同意规则、公开、明示等规则以及查询权、更正权等规则。实质上,这类个人信息处于双重保护的地位。

在权利性质上,隐私权与个人信息权益都是一种个人自主决定权,都是自然人专属的权利,都是人格尊严和个人自由的体现。^{[5][15]}而且,二者的客体上有交叉重叠之处。某些未公开的个人信息可能属于隐私,比如个人家庭住址、银行账户等;反过来某些隐私也属于个人信息的范畴,如个人通讯隐私、谈话的隐私等,都可以通过技术的处理而被数字化。^{[5][15]}其实,隐私与个人信息的载体是不一样的,这会导致二者保护的对象是不同的,前者是不愿意为他人所知的事实,而后者针对的是可识别的数据。但同一侵权行为可能会同时导致对隐私权与个人信息权的侵害,比如,随意传播个人病历资料,既会造成对个人隐私权的侵犯,也会侵犯个人信息权。^[15]但在法律适用上,应区别适用,不应该将隐私权规则与个人信息保护规则同时适用于私密信息。

在规则适用上,如果同时适用隐私权规则与个人信息规则,会产生冲突,比如,经过匿名化处理的私密信息,在个人信息保护法上是不受保护的,那么在隐私法上,是否受保护呢?虽然别人无法识别到自然人个人,但该信息还是自然人的私密信息,如果因为个人信息保护法的原因,不保护,对隐私权规则是一个违反;反过来,若是保护,个人信息权利不就成为了绝

对性权利了吗。再如,个人信息收集时须经自然人同意,而且,若再次转让或者扩大范围使用时,也需要经过自然人同意。而对于私密信息之隐私权,经过同意而公开,则不构成侵权,而且,一旦公开,就没有二次利用的可能。此时,私密信息的同意规则是否适用于再次利用的情况呢?

另外,通过 cookie 等技术手段收集、处理未公开的隐私范畴的信息,只要遵循知情同意以及公开、合理使用都能规则,就不会构成隐私权的侵害。^[6]《民法典》第 1033 条在“权利人同意”之外补充了“法律另有规定”的例外条款,从而为其它法律基于公共利益等正当目的而处理“他人私密信息”提供了法律基础。按照这样的逻辑,在对私密信息进行收集、处理时,是无法适用隐私权法律规则的。

最后,有学者认为,个人信息是一种利益,在权利救济上,缺乏排除妨碍、消除危险或停止侵害等措施。^[6]而且根据《民法典》第 1033 条,处理他人的私密信息需要获得隐私权人的明确同意。在保护强度上,隐私权的保护更强一些。^[4]^[21]不过,如果注意到《民法典》中规定了信息主体的查询、复印、更正、删除等权利,就会发现,个人信息的保护有时要强于隐私权的保护。对于隐私权,可以准用“物上请求权”以及适用侵权法,进行双重保护,而对于个人信息,信息主体享有查询、复印、更正、删除等权利。对于妨害防止请求权这种物上请求权,必须存在具体的、有相当发生之可能的危险才能构成,而对于更正、删除等权利,只要具备抽象危险即可。而查询、复印等权利,则是隐私权人所不享有的。^[21]

所以,对于私密个人信息,应当分别适用隐私法与个人信息保护法,如果同一侵权行为或者妨碍行为同时构成对隐私权或者个人信息的侵害或者妨碍,则会出现请求权并存的现象,但由于二者保护的对象不同,仍然可以分别适用,只是在法律效果上,有可能出现侵犯隐私权的法律效果吸收侵犯个人信息的法律效果,如精神损害赔偿。

2. 公开的个人信息

《民法典》第 1036 条规定“收集、处理自然人个人信息,有下列情形之一的,行为人不承担民事责任:……(二)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,但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外。”该条规则来自于最

高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第 12 条。依据该条第 1 款第 4 项,如果网络用户或者网络服务提供者利用自然人自行在网络上公开的信息或者其他已合法公开的个人信息,诸如自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等,则不构成侵权行为。

首先,个人已经公布于众的信息,即使是私密信息,不管怎么被使用,都很难再援引隐私权加以保护。^[23]按照这样的逻辑,经过公开的私密信息,是不适用《民法典》第 1033 条关于私密信息适用隐私权法的规则的。

其次,经过公布的个人信息是否是受保护的个人信息。德国联邦宪法法院经个人信息保护扩展至公共空间,公共空间里的个人信息也受个人信息法保护。在车牌监控案中,德国联邦宪法法院强调,基本权保护并不会因为相关信息可被公开获取就必然落空。即使国家被允许获取个人信息并公开,但若进一步采取处理等措施,则会被评判为侵犯信息自决权,因为其严重影响了个人的隐私和行为自由。^[14]对该判决持反对意见者认为,将个人信息自决权扩展到公开信息,没有考虑到个人在公共场所交出个人信息时所抱有的合理的保护期待,也没有考虑到会增加政府对于收集、处理公共场所个人信息(如公共场所可辨识的视频监控)论证的义务,因为法律保留原则要求政府对个人信息权“干涉”作出规定或者法定理由。^[14]

根据《民法典》第 1036 条第 2 项,对于公开的个人信息,如果该自然人明确拒绝,数据处理者是不可以处理的,否则,应当承担民事责任。对于可以公开且必须公开的个人信息,自然人应当也有一定的控制权。例如,权利人有权知晓在多大程度上公开、向谁公开该信息以及他人会基于何种目的利用信息等等。^[15]

另外,如果处理该信息侵害自然人重大利益的,数据处理者也是不可以处理的。而所谓的处理该信息侵害自然人重大利益,是指处理将有害于自然人的生命、身体、自由、财产或其他重大利益。例如,通过对各种合法公开的信息的处理对自然人进行人格画像,区别对待,使自然人在接受商品或服务的过程中遭受种族、性别歧视等。^[24]

另外,值得思考的是,什么是合理处理?合理处理应当是指符合诚实信用、合比例地处理个人信息。

具体来讲,是指收集、处理、公开个人信息,应当在服务于法律规定合理使用所希望达到的目的范围内,且手段和方式没有超过为实现该目的而可以采取的最缓和的方式。^[24]比如,电商使用公开的电话等个人信息,不分昼夜地进行推销,即为不合理地处理个人信息。^{[4]P220}

合理处理的对象一般是自然人的个人信息,如果企业通过爬虫的方式爬取公开网页中的自然人自行公开的或者其他已经合法公开的信息,这种情况是否属于“合理处理”呢?对于自然人个人而言,应当属于合理处理,但对于公开自然人信息的网页,则有可能构成不正当竞争行为。

(二) 个人信息权益的权利内容

虽然立法起草人认为《民法典》没有将个人信息规定为权利,但吊诡的是,在《民法典》中,个人信息的信息主体拥有很多权利。

首先,自然人对个人信息的处理享有同意权(《民法典》第1035条第1项)。而且与此相关,根据《民法典》第1036条第2项,自然人还享有拒绝权,处理该自然人自行公开的或者其他已经合法公开的信息,行为人不承担民事责任,但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外。欧盟《一般数据保护条例》第21条也规定了拒绝的权利,但其范围更广泛,数据主体可以于任何时间基于个人原因拒绝个人信息被处理,除非数据控制者能够提供充分的法律基础证明对数据的处理超越了数据主体的利益、权利和自由。该条第2款规定了当对个人数据的处理出于直接营销目的时,数据主体有权拒绝个人信息被处理。此外,除非个人信息的处理对于公共利益而言是必要的,否则数据主体有权拒绝出于科学研究、历史学研究以及统计目的而对个人能信息的处理。这项权利应当在最初与数据主体沟通时进行单独告知,并提示数据主体注意。

其次,根据《民法典》第1037条,自然人享有查阅权,即个人信息权人对其个人信息被处理的情况享有进行查询的权利。查询权是后续自然人行使更正、删除权利的前提。^{[4]P223}

再次,自然人还享有更正权,即信息主体有权请求信息处理主体对不正确、不全面的个人信息进行补正与补充的权利,这里实质上包含了更正权、补充权以及更新权这样一些权利。在来源上,源自欧盟《一

般数据保护条例》第16条,我国《网络安全法》第43条也规定了这一权利。^{[4]P223-224}

具体在信息处理者处理个人行为不合法,信息处理者处理个人信息的目的已不存在、没有必要再保存个人信息,或者信息主体与信息处理者约定的处理期限已经届满等情况下,信息主体可以要求删除信息,值得注意的是,删除权不同于个人信息被遗忘权,《民法典》没有规定被遗忘权。^{[4]P224}

删除的责任主体主要是将个人信息发布到网络上的人,其功能主要在于强制要求责任主体删除违法传播的内容。而被遗忘权的责任主体不限于信息上传者,还包括搜索引擎服务商,因为违法的信息很可能出现在其他网站甚至外国网站,而这种不良信息的传播方式已经远远超出网络使用者和公众对信息的实际需要。在信息社会,被遗忘权会损及言论自由,并会导致信息资源减少、带来企业审查责任与成本等。^[25]

查询之后的复制权,在逻辑上,它是查询权的延伸,但在实际效果上,还可以达到携带权的效果。欧盟《一般数据保护条例》第20条规定,当以电子化方式并且以一种结构化和通用格式来处理个人数据时,数据主体有权利从数据控制者处获得个人数据的副本,以在不同服务提供者之间移转自身数据。^[26]可携带权是支持数据流动、减少垄断、并促进控制正竞争的重要工具。

有疑问的是,信息处理者的范围是什么。根据第1035条对信息处理的界定,“个人信息的处理包括个人信息的收集、存储、使用、加工、运输、提供、公开等”,这里的信息处理者是应当广义的,包括信息控制者与狭义的信息处理者。^[9]但是,信息处理者是否包括受委托处理个人信息的主体呢?在商业实践中,受委托处理个人信息的云计算平台,其客户运营了大量的网站、App,并收集了大量自然人的信息,云计算平台与其客户是一种合同关系。作为信息主体的自然人是否有权直接向云计算平台行使查询权、更正权以及删除权。根据欧盟《一般数据保护条例》,自然人是不可以直接向云计算平台行使查询权、更正权以及删除权等权利的。只是,如果自然人向云计算平台行使查询权、更正权以及删除权,云计算平台应负有转递的义务。

如上所述,在商业实践中,个人信息还包括IP地址等网络日志信息、手机广告标识符或者如mac等

永久标识符等设备地址、浏览记录等能够间接识别信息主体身份的信息,那么,信息主体是否可以请求信息处理者对这些信息形式查询权、更正权、删除权?个人信息的界定采取了列举加概括的模式,这些信息虽然没有被列举,但符合间接识别的要件,所以,也构成个人信息,那么在逻辑上,对于这些信息,自然人当然可以主张查询权、更正权、删除权。只是,对于信息处理者会带来运营成本的增加。而且实践中,数据处理者在数据库中存储用户的前述网络日志信息、设备信息基本是去标识化的数据,为避免与真实身份之间的关联,是单独保存的。那么,信息处理者为了履行自己的义务,需要专门做信息关联、识别用户身份,可能会增加隐私泄露风险。由此,也有可能用户恐慌。但是,对于这些间接识别信息,应当是在法律保护范围之内,在利益衡量上,相比于企业的成本以及泄露之风险,更应当受到保护。

在更正权、删除权的内容上,立法上并不是十分明确,比如,及时删除的内容是什么,如何删除,如果该数据已被数据控制者公开、数据主体要求删除的情况下,数据控制者是否有义务通知第三方删除任何该数据的链接、副本或者备份(比较《一般数据保护条例》第17条)。另外,采取更正等必要措施的内容,也无法从字面上确定。这样一来,企业合规操作时存在一定难度,难以有针对性地进行合规确认。

(三) 个人信息的财产利益内容

在现代信息技术条件下,数据有“内容层、代码层、物理层”等三个层面,个人信息是数据的内容层。在信息社会,尤其是在“大数据”场景下,个人数据可以成为构成大数据的“原始数据”。而原始数据是一种可交易的商品,是一种财产。那么,作为其基础的个人信息是否具有财产属性呢?

有学者认为,在信息时代,个人信息具有潜在的商业价值,故而应该受到财产权的保护。另有学者区分基础数据与增值数据,个人数据属于基础数据。基础数据具有流通功能,并与现实经济活动结合而演变为企业数据、行业数据、政府数据和国家数据等各种形式的数字资产,从而个人数据具有经济属性,所以,应赋予个人基础数据以所有权。

不过,应当看到,单个自然人的个人信息的财产价值是微乎其微的,只有形成大数据,才可以进行收集、分析与创造。而且,《民法典》并没有赋予个人信

息可转让性,而是将之界定在人格权的范畴。从人格权的特性来看,其内容可以具有财产价值,但不能脱离人而被移转。所以,就目前立法现状来看,并不存在独立的个人信息财产权,但并不否认个人信息的财产价值。对于个人信息可以商业化利用,对于个人信息因此产生的财产利益,法律应予以保护。

三、信息社会下个人信息处理的准则

《民法典》第1035条规定了收集、处理个人信息应当遵循的原则。在赋予信息主体法定权利的基础上,划定了信息处理者收集处理个人信息的边界。这一边界的划定对信息处理者是比较有利的,疏通了信息收集及流动的渠道。

(一) 义务主体问题

首先,有疑问的是,谁是遵循《民法典》第1035条所规定的原则的义务主体。《民法典》第1035条的核心概念是“处理”,而处理的内涵包括收集、存储、使用、加工、传输、提供、公开等。从这一立法体系可以推知,个人信息处理者,应当包括数据控制者与数据处理者。此外,从《民法典》第1037条、第1038条中“信息处理者”的表述来看,并没有区分“数据控制者”、“数据处理者”与“受委托处理者”,而是笼统地赋予其各种义务。《民法典》第1038条将“信息处理者”作为个人信息安全保障义务的责任人,涵盖了“信息收集者、控制者”。

再有,根据《消费者权益保护法》第29条以及《网络安全法》第41条第1款、第42条第1款,任何方式的信息处理行为均须获得信息主体之同意,那么,这就意味着,信息控制者与信息处理者收集与处理信息均需事先获得信息主体的同意。从知情同意的本质来看,是个人信息决定权的体现,信息主体对收集信息的同意,并不意味着对处理的同意,所以,信息收集的知情同意规则应当适用于所有个人信息收集与处理行为。^[27]所谓的数据控制者是独自或者共同确定个人数据处理目的和方式的法人、政府机关或者其他单位。^{[11]P17}数据控制者不仅会处理数据,而且最重要的是对数据的决定权。这种对数据处理的决定权可能是来自明示或默示的法律职责,或者对处理方法与目的事实上影响。^{[11]P19}所以,《民法典》第1035条适用于数据控制者是没有问题的。

数据处理者是一个独立于控制者的主体,其代表数据控制者处理数据,其典型活动是提供IT解决方

案,包括云存储。数据控制者与数据处理器之间必须通过合同约定数据处理者的职责,未经数据控制者事先特别或一般书面授权,数据处理器不能引入另一个数据处理器。在一般书面授权的情况下,如果数据处理器增加或替换其他数据处理器,还需要通知数据控制者(《一般数据保护条例》第28条)。通常,数据控制者与数据处理器之间存在一个合同关系。数据控制者作为“受委托处理个人信息的主体”,一般不与信息主体接触,也不会具体收集个人信息。数据处理器具体从事“处理行为”时,往往事先无法取得自然人的同意,也无法向信息主体公开处理规则、明示处理目标、方式、范围。根据欧盟《一般数据保护条例》,作为“受委托处理个人信息的主体”,处理个人数据时,无须取得自然人的同意,也不需要履行公开与明示等义务,最关键的是要取得数据控制者的授权。

在个人信息收集、处理中,同意是最核心的要件,在技术上,要求所有主体的同意,是没有问题的,这与《民法典》第1038条规定的数据处理者的侵权责任,也是相适应的。事实证明,信息社会的高级段智能社会已经到来,在收集、处理信息的各个环节取得信息主体同意,在技术上是可行的。另一方面,所有的信息处理器处理个人信息都需要经过信息主体同意,不会增加成本,也不会形成数据流动的障碍。

在司法实践中,法院也认为,在Open API场景下,对于个人信息收集、利用,应遵循“三重授权原则”,即平台方收集、使用用户数据需获得用户授权,第三方通过开放平台Open API接口间接获得用户数据,需获得用户授权和平台方授权。^③

(二) 合法、正当、必要且最小够用

根据《民法典》第1035条,收集、处理个人信息需要“合法、正当且必要”,不得过度收集、处理。所谓合法,是指所有对个人信息的收集和处理的活动的都要符合我国的法律规范,这里的法律规范不仅是指《民法典》中的相关内容,还包括其他部门法对个人信息保护有所涉及的内容,如《电子商务法》、《网络安全法》以及最高人民法院、最高人民检察院的相关司法解释等。所谓正当,是指进行信息收集和处理的目的是手段要正当,正当的含义不仅仅是指手段目的要合法,更要求手段目的要符合诚实信用的基本原则,并且尽量满足透明的要求,以便当事人能够充分

了解相关情况,行使相应权利。^{[4]P217}所谓必要,是指所收集和处理的个人信息应当限于实现正当目的所必须之部分,与实现所涉目的无关的个人信息不能收集和处理的。^{[4]P217}尤其是社会公众在使用APP时,大部分APP会向用户开通访问通信录和位置信息的权限,但部分APP的实际功能与这些信息并无直接关联,这就属于《民法典》中个人信息收集行为的非必要,亦是过度收集个人信息行为。

根据《民法典》第1035条,信息处理器不得过度处理,《网络安全法》第41条也规定,网络运营者收集、使用个人信息,应当遵循合法、正当、必要的原则,并且遵循最小够用原则。而所谓最小够用原则,是指除与个人信息主体另有约定外,只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后,应及时根据约定删除个人信息。

(三) 同意

《民法典》第1035条第1项要求收集、处理自然人个人信息,必须征得该自然人或其监护人同意。有学者认为,个人信息不应由个人控制,而是应由社会控制、社会决定,个人信息是社会的共同资源。据此,对于个人信息的收集和使用,应“以一般允许为原则,以个人控制(同意决定)为例外”。只有个人敏感信息的收集和使用,才需要个人的同意。^[28]

对此,笔者持不同意见。知情同意是个人信息权的核心,暗含着法律认可个人信息由个人支配或控制,个人享有个人信息的使用决定权,包括是否允许他人使用、如何使用等决定权。^[28]信息主体本人的知情同意是对信息进行收集、处理和使用的的基础。原则上,没有当事人的知情同意,除非法律强制规定的情况以外,任何的收集行为都是没有合法性基础的。

首先,在逻辑上,同意的前提一定是告知,否则,信息主体无法判断是否同意,同意什么。那么,告知的内容是什么呢?针对不同类型的信息,是否告知的内容与方式有所不同呢?《民法典》第1035条没有明确告知这一前提,而且也没有区分普通个人信息与敏感个人信息或隐私信息进行分别处理。2020年版的《信息安全技术:个人信息安全规范》区分了普通个人信息与敏感个人信息,对于普通个人信息,收集个人信息,应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则。收集个人生物识别信息前,应单独向个人信息主体告知收集、使用个人生

物识别信息的目的、方式和范围,以及存储时间等规则,并征得个人信息主体的明示同意。而且,信息处理者收集、处理个人信息的行为受制于最初告知的目的。《电信和互联网用户个人信息保护规定》第9条规定“电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的。”

值得注意的是,在告知的方式上,一般需要向个人信息主体告知。只有在产品或服务仅提供一项收集、使用个人信息的业务功能的情况下,个人信息控制者可通过个人信息保护政策的形式,实现向个人信息主体的告知。而《民法典》第1035条将公开处理信息规则以及明示处理信息的目的、方式与范围作为两项原则,在逻辑上,可以适用于任何形式的个人信息。不过,从更有利保护个人信息的角度来看,向信息主体告知乃至单独告知应是告知的一般形式,只有在信息处理者仅提供一项收集、使用个人信息的业务功能的情况下,才可以以公开或明示信息保护政策的形式告知。在告知之后,处理个人信息还需要数据主体的同意或者法律准许。值得思考的是,同意的方式有哪些。是否区别不同个人信息类型,采取不同的同意方式。

2020年版《信息安全技术:公共及商用服务信息系统个人信息保护指南》第5.4条要求,处理敏感个人信息与生物信息,需要个人信息明示同意,依照反面解释,处理普通个人信息征得个人信息主体的默示同意即可。所谓明示同意,是指个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明,或者自主作出肯定性动作,^[4]对其个人信息进行特定处理作出明确授权的行为。而所谓默示同意是指,在个人信息主体无明确反对的情况下,即可认为个人信息主体同意。

《民法典》第1037条没有明确区分敏感信息与一般信息,但《民法典》第1033条第5项规定,任何组织或者个人未取得权利人明确同意,不得处理他人私密信息。所以,对于私密信息,应当是要明示同意的。^[4]^{P216}进一步值得思考的是,如果网络运营者将收集的信息授权转给第三人,是否还需要经过个人信息主体的同意?在2016年“脉脉”非法抓取使用“新浪微博”用户信息被判不正当竞争案中,涉及一个争议问题,即新浪未经用户同意将个人信息数据授权给脉

脉的行为是否合法?法院认为:微博确实是通过了用户的授权许可能够抓取这些信息,但是抓取以后对外使用的时候,还应该给用户再次选择权和知情权,两个被告公司他们经过和微用公司之间的合作确实获得了授权,但是他这种授权是没有再次经过用户同意的。^[5]在这种情况下,影响了用户的知情权和选择权。所以可以认为,对于个人数据,已经获得授权的网络经营者再次转让或再次利用时,仍需要用户的同意。

有争议的是,这种授权对象是对第一个数据控制者的授权,还是需要对受让人或共享人的授权,授权的内容是同意使用,还是转让授权。根据《信息安全技术:公共及商用服务信息系统个人信息保护指南》第5.3条b款规定,间接获取个人信息时,应要求个人信息提供方说明个人信息来源,并对其个人信息来源的合法性进行确认;应了解个人信息提供方已获得的个人信息处理的授权同意范围,包括使用目的,个人信息主体是否授权同意转让、共享、公开披露等。如本组织开展业务需进行的个人信息处理活动超出该授权同意范围,应在获取个人信息后的合理期限内或处理个人信息前,征得个人信息主体的明示同意。所以,授权的内容应当是同意使用。《民法典》第1036条对知情同意例外条款的适用范围做了必要的限缩,即便是获得权利人同意或者是已经公开的个人信息,依然需要在“合理”范围内使用,信息处理者方可免责。

最后,值得反思的是,在云计算、大数据、物联网环境下,个人知情同意模式已经无法起到保护个人数据的作用。一方面,明示收集、使用信息的目的、方式和范围的格式条款冗长而艰涩,无法阅读;另一方面,在网络语境中,为使用产品或服务,用户往往除点击同意之外并无其他选择,而且,用户在很多情况下对其信息的收集并不知情,向信息处理者行使权利,无从谈起。^[29]

在原因上,告知同意原则之所以时常失灵,可能不仅仅因为技术原因,更多的是各主体之间欠缺信赖,而风险控制本身也缺乏客观性。^[30]为此,有学者提出通过动态、考虑多种因素的场景理论替代同意规则,主要将个人信息处理置于其所处的环境中、具体审视考察个人信息的处理行为给用户带来的后果及隐私影响。^[29]具体通过隐私风险评估,来判断信息处理行为是否合理,其导致的风险是否在可预期的范围

内,如果结果是合理,则可以免予取得用户同意,减轻为机构及用户自身带来的负担。如果不合理,则可以采取适当的手段降低风险。^[29]

四、结论

信息社会需要信息流动,个人信息的挖掘使得个人信息保护更为突出。《民法典》中的个人信息保护规则已经充分考虑到这一对矛盾关系,并构建了国家、信息处理者、信息主体的共生、共存关系。

在个人信息范围界定上,《民法典》第1034条的规定是比较狭窄的,没有考虑技术发展的需要,虽然增加了电子邮箱和行踪信息等类型,但没有穷尽目前技术手段下的既存类型。在可识别对象方面,指向自然人个人,而没有指向社会、政治、经济等身份属性以及设备终端。在本质上,个人信息的核心内容是可直接、间接识别性。通过可识别标准,保护信息主体的核心利益,而信息主体也让渡了不可识别的个人信息这一非核心利益。

虽然法律条文上没有明确个人信息的权利属性,但从内容上,个人信息符合权利的特征,其中含有利益,也具有法律之力。《民法典》中区分了私密信息、公开信息以及一般个人信息,对于私密信息,通过隐私法与个人信息保护法双重保护,但在保护上会出现规范与价值冲突,在具体处理上,还是应该分别适用隐私法与个人信息保护法,只是要解决竞合的问题。《民法典》赋予了个人信息主体查询、复印、更正以及删除等权利,这些权利的内容需要结合《信息安全技术:公共及商用服务信息系统个人信息保护指南》予

以确定,这些权利均不构成对信息的收集、处理与流动的障碍,属于信息主体的核心利益。值得注意的是,复制权可否扩大解释为可携带权,可携带权可以大大促进数据流动、制衡企业垄断数据。

《民法典》第1035条规定了收集、处理个人信息应当遵循的原则。适用该规则的主体既包括信息收集者,也包括信息处理者,甚至包括信息处理各个环节的主体,在司法实践中,法院也认为,信息的收集、处理各个环节,都需要信息主体的同意。信息处理者在收集、处理个人信息时,应当合法、正当、必要且最小够用。最为重要的是,信息处理者在收集、处理个人信息时,须取得信息主体的同意。

知情同意是信息主体的核心利益,不可让渡。同意的前提是告知,收集一般个人信息,应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则。收集个人生物识别信息前,应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围,以及存储时间等规则,并征得个人信息主体的明示同意。信息处理者收集、处理个人信息的行为受制于最初告知的目的。告知的方式上,一般需要向个人信息主体告知。只有在产品或服务仅提供一项收集、使用个人信息的业务功能的情况下,个人信息控制者可通过个人信息保护政策的形式,实现向个人信息主体的告知。处理敏感个人信息与生物信息,需要个人信息明示同意,依照反面解释,处理一般个人信息征得个人信息主体的默示同意即可。即便是获得权利人同意或者是已经公开的个人信息,依然需要在“合理”范围内使用,信息处理者方可免责。

注释:

- ① 参见南京市中级人民法院(2014)宁民终字第5028号民事判决书。
- ② 参见《信息安全技术:公共及商用服务信息系统个人信息保护指南》第3.7条。
- ③ 参见北京市知识产权法院(2016)京73民终588号民事判决书。
- ④ 肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。
- ⑤ 北京市知识产权法院(2016)京73民终588号民事判决书。

参考文献:

- [1] 钟义信. 信息社会:概念、原理与途径[J]. 北京邮电大学学报(社会科学版) 2004 2.
- [2] 孙伟平. 信息社会及其基本特征[J]. 哲学动态 2010 9.
- [3] 孙伟平. 信息社会的价值理念与信息社会的构建[J]. 哲学研究 2016 6.
- [4] 黄薇. 中华人民共和国民法典人格权编解读[M]. 北京:中国法制出版社 2020.
- [5] 张新宝. 从隐私权到个人信息——利益在衡量的理论与制度安排[J]. 中国法学 2015 3.
- [6] 程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学 2019 4.
- [7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of person data and on the free movement of such data, OJ L 281, 23. 11. 95.
- [8] 王融. 数据匿名化的法律规制[J]. 信息通信技术 2016 4.

- [9] 齐爱民. 个人信息保护法研究[J]. 河北法学 2008 4.
- [10] Mario Martini , big data als Herausforderung fuer den Persoenlichkeitsschutz und das Datenschutzrecht , DVBI , 2014.
- [11] Paul Voigt , Axel von dem Bussche , The EU General Data Protection Regulation(GDPR) , Springer , 2017.
- [12] Paul Ohm , Paul Ohm , Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization , 57 UCLA L. Rev. 1701 (2010) .
- [13] Herbst , NVwZ 2016 , 902 , 904.
- [14] [德]肖弗里德里希·肖赫. 信息社会背景下的信息自决权[J]. 北京航空航天大学学报(社会科学版) 2015 6.
- [15] 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.
- [16] 张里安 韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛 2016 3.
- [17] 杨立新. 个人信息: 法益抑或民事权利——对《民法总则》第 111 条规定的“个人信息”之解读[J]. 法学论坛 2018 1.
- [18] 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.
- [19] 丁晓东. 个人信息私法保护的困境与出路[J]. 法学研究 2018 6.
- [20] 朱庆育. 民法总论[M]. 北京: 北京大学出版社 2016.
- [21] 杨芳. 个人信息保护法保护客体之辨[J]. 比较法研究 2017 5.
- [22] 周汉华. 《中华人民共和国个人信息保护法(专家建议稿)》及立法研究报告[M]. 北京: 法律出版社 2006.
- [23] 郭瑜. 个人数据保护法研究[M]. 北京: 北京大学出版社 2012.
- [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.
- [25] 丁晓东. 被遗忘权基本原理与场景化界定[J]. 清华法学 2018 6.
- [26] 李蕾. 数据可携带权: 结构、归类与属性[J]. 中国科技论坛 2018 6.
- [27] 王利明. 数据共享与个人信息保护[N]. 北京日报 2019-4-29(14).
- [28] 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.
- [29] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论 2016 5.
- [30] 姚佳. 知情同意原则抑或信赖授权原则——兼论信用时代的信用重建[J]. 暨南学报 2020 2.

The Civil Code of China and the Information Society

——Taking Personal Information as an Example

Wang Hong - Liang

(Law School of Tsinghua University , Beijing 100084)

【Abstract】Starting from the basic content and basic characteristics of the information society , this article finds that when dealing with personal information , it is necessary to handle the relationship between personal information protection and information flow , and it is also necessary to build a symbiotic relationship between the government , the information processors and the information subjects. Firstly , Article 1034 of the Civil Code stipulates a relatively narrow range of personal information , which does not fully reflect the development of technology , nor does it fully cover the core interests of information subjects. Secondly , the Civil Code distinguishes personal information into private information , public information , and general personal information. The private information is dually protected by the privacy law and the personal information protection law , however the dual protection will bring conflicts between different rules and seems not necessary. According to the Civil Code , information subjects enjoy the rights of inquiry , copying , correction , and deletion of his own personal information. These rights do not constitute obstacles to the collection , processing and flow of information , and belong to the core interests of the information subject. Finally , Article 1035 of the Civil Code stipulates the principles to be followed in the collection and processing of personal information. Subjects to which this rule applies include information collectors , information processors , and even entities involved in all aspects of information processing. When the information processor collects and processes personal information , it shall be lawful , justifiable , necessary , and minimum sufficient. The most important thing is that the information processor must obtain the consent of the information subject when collecting and processing personal information. Informed consent is the core interest of the information subject and cannot be assigned.

【Key words】personal information; information subjects; private information; information controllers; information processors

(责任编辑: 孙培福)