

论个人信息保护中责任规则与财产规则的竞争及协调

曹 博

内容提要:《民法总则》出台后,我国个人信息保护的法律规则初步实现了体系化。在法律救济层面,单行法及行政法规构建的财产规则与商业实践存在重大背离,《民法总则》第111条对此进行了一定程度的修正。通过对个人信息的定位和分类,将进一步明确其保护根据是利益而非权利,从而为责任规则与财产规则的竞争奠定基础。基于交易成本、估价成本、行为模式预期等经济效率的综合考量,应当重构我国个人信息保护的救济规则。对自然性个人信息适用财产规则,对社会性个人信息与复合性个人信息适用责任规则,并结合行业规则的逐步完善,建立去身份化的行为指引,实现理论构想、法律规范与社会实践的逐步统一。

关键词:个人信息 法律救济 卡-梅框架 责任规则 财产规则

曹博,重庆大学法学院讲师。

个人信息的权利属性在理论与实务中均面临较大争议,以权利模式构建保护体系的尝试难于实现。法律经济学中的“卡-梅框架”^[1]提供了从法律救济角度评判法益保护效果并决定规则选择的理论模型。具体而言,在利益归属明确的前提下,禁易规则不允许利益的转移,即使交易双方完全自愿;财产规则下利益的转移必须征得拥有者的同意并由其确定交易价格;责任规则是指如果相对方愿意支付一个客观确定的价格,无论拥有者是否同意,均可发生利益转移。^[2]通过对个人信息的重新界定与分类,结合财产规则、责任规

[1] 美国学者卡拉布雷西(Guido Calabresi)与梅拉米德(Douglas Melamed)提出从法律后果的角度对法律规则进行逻辑分类,并以财产规则(Property Rules)、责任规则(Liability Rules)和禁易规则(Inalienability)的划分形成了“卡-梅框架”(C & M Framework)。参见 Guido Calabresi & Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 *Harv. L. Rev.* 1089, 1089-1128 (1972)。中译本参见[美]吉多·卡拉布雷西、道格拉斯·梅拉米德著:《财产规则、责任规则与不可让渡性:“大教堂”的一幅景观》,凌斌译,载[美]威特曼主编:《法律经济学文献精选》,法律出版社2006年版。

[2] Guido Calabresi & Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 *Harv. L. Rev.* 1089, 1092 (1972)。

则与禁易规则的基本内涵和适用条件,将明确不同类别的个人信息应当选择何种救济规则,为个人信息保护提供一种可能的理论模型与制度构想。

一 现有个人信息保护法律规则的缺陷

将“卡-梅框架”投射到我国个人信息保护的体系之中,可以发现单行法及行政法规确立了以同意规则为表征的财产规则,《民法总则》第 111 条一定程度上调整了这一规则,使之具有了部分责任规则的特质,但商业活动中同意规则被架空,司法实务也并未采纳同意规则。

(一) 单行法及行政法规中关于个人信息保护的财产规则

个人信息保护立法始于全国人大常委会于 2012 年发布的《关于加强网络信息保护的決定》,该决定是为了因应日渐严重的收集、使用、泄露、倒卖个人信息的现象,^[3]并确立了收集、使用个人信息时应征得被收集者同意的规则。2013 年修订的《消费者权益保护法》第 29 条明确规定经营者收集和使用消费者个人信息必须经消费者同意。最高人民法院在 2014 年公布的《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》中试图将侵犯个人信息的行为作为独立的侵权类型,以责任例外的形式确认了同意规则。^[4] 2016 年颁布的《网络安全法》规定网络运营者收集使用个人信息也必须征得被收集者同意。^[5] 此外,在相关的行政法规、部门规章、部门规范性文件中亦以大体相同的表述确认了同意规则。^[6]

若以交易的视角考察前述法律规则,意味着网络服务提供者等主体要收集相关个人信息并进行使用、处理,必须通过自愿交易的方式,从公民处以其同意的价格或条件购买。这种特点符合“卡-梅”框架中对财产规则的基本界定。^[7]

[3] 据参与起草该决定的相关人员介绍:“随意收集、擅自使用、非法泄露甚至倒卖公民个人电子信息,网络诈骗、诽谤等违法犯罪活动大量发生,严重损害公民、法人和其他组织的合法权益……我国有关的法律规范还比较薄弱,必要的管理措施缺乏上位法依据,与信息化发展和维护人民群众在网络活动中合法权益的要求不相适应。”殷泓、王逸吟:《个人信息保护立法正当时——解读全国人大常委会关于加强网络信息保护的決定草案》,《光明日报》2012 年 12 月 25 日第 001 版。

[4] 该司法解释第 12 条规定,网络用户或者网络服务提供者利用网络公开相关个人信息造成他人损害应承担侵权责任,同时将经过自然人书面同意且在约定范围内公开作为侵权的例外情形,事实上确认了个人信息收集与使用的同意规则。

[5] 《网络安全法》第 41 条第 1 款:“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,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。”

[6] 例如,2013 年国务院发布的《征信业管理条例》第 13 条第 1 款规定:“采集个人信息应当经信息主体本人同意,未经本人同意不得采集。但是,依照法律、行政法规规定公开的信息除外。”2013 年工业和信息化部发布的《电信和互联网用户个人信息保护规定》第 9 条第 1 款规定:“未经用户同意,电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。”2013 年国家质量监督检验检疫总局、国家标准化管理委员会发布的《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 4.2 条 d) 项规定:“处理个人信息前要征得个人信息主体的同意。”

[7] 参见 Guido Calabresi & Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 *Harv. L. Rev.* 1089, 1092 (1972)。

(二)《民法总则》第 111 条对财产规则的调整

《民法总则》第 111 条规定：“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”该条并未承继“同意规则”，而是代之以“依法取得”的要求，二者的规范意旨存在明显区别。

回到卡-梅框架，《民法总则》第 111 条的规定已经不再是一个完全的财产规则，而是具有了责任规则的部分特质。该条的规范重点落在了对“依法取得”和“确保信息安全”的理解。就个人信息的获取而言，即便未获同意，若符合相关法律规定并确保信息安全，亦属于合法行为。从法律责任的角度考察，该条并未给出明确指引。如果违反该条规定后仅需承担损害赔偿赔偿责任，则无异于自然人对个人信息享有的是一个可以被他人以法定赔偿强行剥夺的有限权益，这符合责任规则的基本界定。^[8] 如果违反该条规定需承担停止侵害（禁令）的民事责任，甚至行政责任乃至刑事责任，则属于财产规则的范畴。《民法总则》第 120 条笼统地规定在民事权益受到侵害时，被侵权人有权请求侵权人承担侵权责任，而《侵权责任法》亦未明确侵害个人信息应当承担的民事责任类型。

《民法总则》第 111 条对于既有的以同意规则为表征的个人信息法律救济的财产规则进行了调整，使之具有了部分责任规则的特质，或者说消解了财产规则的合理根据，但由于法律责任条款的缺失，尚不能得出责任规则已经确立的结论。

(三)商业实践中财产规则被架空

从卡-梅框架来看，财产规则对权益的保护强度更大。但商业实践中同意规则被架空的现实，使其规范效果受到影响。

同意规则在比较法上早有先例，经济合作与发展组织（OECD）在 1980 年制定的《隐私保护与个人数据跨境流通指南》中，就针对数据主体的同意做出了规定，体现在收集限制原则与使用限制原则的具体表述之中。^[9] 1995 年，欧盟《数据保护指令》^[10] 及欧盟诸国有关个人信息保护的律^[11] 都明确规定了同意规则。已于 2018 年 5 月 25 日生效的

[8] 责任规则之下的利益转移不再取决于当事人之间的自愿定价，而是由法律设定价格，在实定法层面的例证有无因管理、不当得利、添附、法定许可等，其实质均是权利被剥夺时私人主体仅享有损害赔偿或法定补偿的请求权。参见凌斌：《法律救济的规则选择：财产规则、责任规则与卡梅框架的法律经济学重构》，《中国法学》2012 年第 6 期，第 9-10 页。

[9] *OCED Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 1980, Article 7 (Collection Limitation Principle) and Article 10 (Use Limitation Principle).

[10] 该指令全称应为“欧盟议会与理事会 1995 年《关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC/号指令》”(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individual with regard to the processing of personal data and on the free movement of such data)，第 7 条规定了数据处理合法化的标准之一包括数据主体的明确同意。参见高富平主编：《个人数据保护和利用国际规则：源流与趋势》，法律出版社 2016 年版，第 147 页。

[11] 例如，德国《联邦数据保护法》(Federal Data protection Act)、法国《数据处理、数据文件及个人自由法》(Data processing, Data Files and Individual Liberties)、英国《资料保护法》(Data Protection Act)以及瑞典《个人数据法》(Personal Data Act)都确立了个人数据收集处理使用的同意规则。参见任龙龙：《论同意不是个人信息处理的正当性基础》，《政治与法律》2016 年第 1 期，第 127 页。

《通用数据保护条例》(General Data Protection Regulation, GDPR)再次确认了同意规则。^[12]美国联邦贸易委员会在1998年就已经将“同意”视为隐私保护中广为接受的核心原则之一。^[13]

按照同意规则,需要收集和处理个人信息的主体(例如网络服务提供商),制定了冗长的用户协议(服务条款或隐私声明),要求用户点击同意,体现出对同意规则的遵守,将可能的法律风险降至最低。然而,此类用户协议结构复杂、条款众多,阅读理解耗时费力,在移动互联网高度普及、对效率的期待与追求无所不在的时代,奢望用户详加关注太不现实。此外,为使用相应的网络产品或服务,用户在点击同意之外时常别无选择,^[14]交易地位的不对等使得同意的真实性与对隐私声明的知悉度都大打折扣。

(四)司法实践中并未采纳财产规则

实践中个人信息保护的诉求大多以隐私权、名誉权或一般人格权受到侵犯为由提起,法院亦只能在这一框架内进行裁判。总体上看,法院并不认可自然人与其相关的个人信息享有支配权和决定权,而是强调收集、使用个人信息的行为是否侵犯了某一具体人格权或一般人格权。

在杨某与熊某名誉权纠纷案中,法院虽然援引了最高人民法院的司法解释中有关个人信息保护的内容,^[15]但并未明确自然人对相应个人信息享有支配性权利,而是强调杨某的个人信息被熊某公开后招致了辱骂行为,从而产生了对其名誉的损害,进而造成对名誉权的侵犯。^[16]

在朱某与百度公司隐私权纠纷案中,二审法院援引《电信与互联网用户个人信息保护规定》^[17]中的“可识别性”标准,将百度公司利用 cookie 技术收集的搜索关键词排除在个人信息的范畴之外。^[18]但论者敏锐地指出,前述规定及《网络安全法》对个人信息的界定结合了直接识别说与间接识别说,二审法院认为只有直接识别的信息才构成个人信息,

[12] 值得关注的是, GDPR 对同意的认定提出了更高的要求, 施加了更为明确的限制: 一是由数据控制者证明数据主体已对处理个人数据的行为予以同意; 二是同意在形式上必须明显区别于其他事项并使用明了且容易获取的方式和清楚简单的语言; 三是数据主体有权在任何时候撤销其同意; 四是要考虑数据主体的同意是否基于自由意志做出, 特别是当包含服务条款的合同履行是以数据主体同意为条件的, 而该数据处理又不为履行合同所必需时。 Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016. Article 7; Conditions for consent. 中文译本参见高富平主编:《个人数据保护和利用国际规则:源流与趋势》,法律出版社2016年版,第225页。该书将 General Data Protection Regulation 翻译为《统一数据保护条例》,本文采用更为常见的译法,仍翻译为《通用数据保护条例》。

[13] U. S. Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), p. 8.

[14] 范为:《大数据时代个人信息保护的路径重构》,《环球法律评论》2016年第5期,第94页。

[15] 《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条第1款:“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。”

[16] 南京市中级人民法院(2015)宁民终字第322号民事判决书。

[17] 国家工信部《电信与互联网用户个人信息保护规定》第4条:“本规定所称用户个人信息,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。”

[18] 南京市中级人民法院(2014)宁民终字第5028号民事判决书。

背离条文文义和学理通说,成为判决的重大瑕疵。^[19]

在任某与百度公司名誉权、姓名权、一般人格权纠纷案中,二审法院认定原告要求删除的涉诉工作经历信息是客户或学生藉以判断的重要信息依据,也是作为教师诚实信用的体现,不应成为侵权保护的正当法益。^[20] 在该案中,原告要求删除的个人信息显然能够通过“可识别性”的检验,但法院并不认可原告对之享有支配性权利。

由此可见,虽然实定法层面给出了有关个人信息的定义,并且初步构建了财产规则,但在实践中个人信息的定性及其归属仍然具有极大的不确定性,且相关概念之间界限模糊,需要重新厘定个人信息的利益属性及其内涵。

二 个人信息的利益属性及其内涵

个人信息保护的依据从何而来,学界纷争不断,构建个人信息权制度的主张曾成为主流看法。《民法总则》出台后,有人断言我国正式在实定法层面确立了个人信息权。由于权利与利益在侵权法上区分保护已成共识,^[21]有必要对个人信息权这一说法及其争议进行评判,并以此为基础探求个人信息获得保护的根据。

(一) 个人信息权的争议及评判

《民法总则》第 111 条对个人信息保护进行了规定。该条的规范目的与基本含义,学界多有争议。有人认为本条已确立了“个人信息权”,包括个人信息自决权、查询权、选择权、保密权等内容。^[22]也有人认为该条一定程度上明确了“个人信息权”,既是宣示性规定,也是确权性规定。^[23]如此看来,个人信息似乎已在民事权利的谱系中谋得一席之地,虽未得“权利”之名,已获“权利”之实。

对《民法总则》第 111 条的文义解释和“民事权利”章的体系解释将阐明前述理解的偏颇之处。从字面含义出发,该条并未使用“个人信息权”,只是宽泛地指称“个人信息受法律保护”。仅因出现在《民法总则》“民事权利”一章,就必然获得权利身份?须知该章

[19] 李谦:《人格、隐私与数据:商业实践及其限度——兼评中国 cookie 隐私权纠纷第一案》,《中国法律评论》2017 年第 2 期,第 128-129 页。

[20] 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。

[21] 关于这方面的论述,可参见张家勇:《权益保护与规范指引》,《四川大学学报(哲学社会科学版)》2017 年第 1 期;方新军:《权益区分保护的合理性证明——〈侵权责任法〉第 6 条第一款的解释论前提》,《清华法学》2013 年第 1 期;于飞:《侵权法中权利与利益的区分方法》,《法学研究》2011 年第 4 期;曹险峰:《在权利与利益之间——对侵权行为客体的解读》,《当代法学》2005 年第 4 期。

[22] 参见中国审判理论研究会民事专业委员会编著:《〈民法总则〉条文理解与司法适用》,法律出版社 2017 年版,第 197-198 页。这种理解在《民法总则》出台之前也有诸多学者支持和倡导,参见王利明:《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》,《现代法学》2013 年第 4 期;齐爱民、李仪:《论利益平衡视野下的个人信息权制度——在人格利益与信息自由之间》,《法学评论》2011 年第 3 期;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》,法律出版社 2006 年版;谢远扬:《个人信息的私法保护》,中国法制出版社 2016 年版。

[23] 陈甦主编,谢鸿飞、朱广新副主编:《民法总则评注》(下册),法律出版社 2017 年版,第 785 页。

内容多为宣示性条款,且其中亦对不少民事利益提供保护。^[24] 法条之中未见权利字样,即推知已确认权利,突破了文义解释的基本要求。从“民事权利”章的体系考察,第109条至第112条的规定均是带有人格权性质的内容,第113条至第125条则是财产权内容,第126条至第127条为其他权利,第128条至第132条是关于权利取得、行使的规定。第109条和第113条扮演了“总则”,宣示性质和概括特点较强。^[25] 其后的规定则是具体化的权利类型,例如第110条就是关于生命权、身体权等人格权的规定,第114条至第124条则规定了物权、债权、知识产权等具体权利类型,在此之外是对尚有争议却值得保护的民事利益进行的列举。按照这种体系结构,只能得出个人信息并非具体化的人格权类型,但属于值得保护的民事利益这一结论。

按此,《民法总则》没有确立所谓个人信息权,其他法律规范中亦未见“个人信息权”,无法得出我国已确立个人信息权制度的认识,个人信息保护的依据只能是利益,其正当性及必要性值得进一步研究。

(二) 个人信息的定性及分类

《网络安全法》第76条将个人信息界定为:“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。”学界对个人信息的认识基本上与此相当,均强调“可识别性”。^[26]

《信息安全技术 公共及商用服务系统个人信息保护指南》^[27] 给出了敏感信息与一般信息的区分模式。学理上与比较法层面亦有直接个人信息与间接个人信息、公开个人信息与隐秘个人信息、专业个人信息与普通个人信息等多种分类。^[28] 这些做法都致力于为个人信息的收集和使用建立类型化的法律规则,普遍将权属配置给能够连接到的自然人个体,并采用了信息主体的说法。

有的分类采用了“P与非P”式的方法,依赖于对客观事物的完全或非完全列举,在内涵与外延上并不能形成自治,边界模糊;有的分类则尝试从行为结果出发进行反面定义,更增添了分类标准的不确定性。此外,这些分类的共同特点均是从个人信息反映的外部特征进行归纳,而外在形式的多样化决定了其对于解决个人信息的收集、使用、处理等问题起到的作用只能集中在某个方面。同时,信息主体的提法亦颇为不妥,这暗示了自然人

[24] 例如,《民法总则》“民事权利”章中关于无因管理、不当得利的规定,事实上只是确认了相关的民事利益。在知识产权客体的规定中,虽然涵盖了地理标志、商业秘密、集成电路布图设计等内容,但断不能得出《民法总则》已确认了“地理标志权”、“商业秘密权”、“集成电路布图设计权”的结论。

[25] 《民法总则》第109条规定:“自然人的人身自由、人格尊严受法律保护。”第113条规定:“民事主体的财产权利受法律平等保护。”

[26] 参见张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,《中国法学》2015年第3期,第38页;张平:《大数据时代个人信息保护的立法选择》,《北京大学学报(哲学社会科学版)》2017年第3期,第144页;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》,《现代法学》2013年第4期,第64页。

[27] 该指南由国家质量监督检验检疫总局和国家标准化管理委员会于2013年发布。

[28] 参见齐爱民:《大数据时代个人信息保护法国际比较研究》,法律出版社2015年版,第138-149页。

对个人信息的独占性与支配性,无异于创设了一项私有权利。

无论个人信息之上附着人格利益还是财产利益,其权属问题应经过正当性检验,从个人信息的来源进行考量更为可取。这种分类及定义力图对个人信息这一事物本质进行客观认识与描述,避免主观要素的干扰。2014 年世界经济论坛发布的报告《反思个人数据:加强信任的新视角》即是按照这一路径将个人数据区分为个人提供的个人数据(individually provided personal data)、被观测到的个人数据(observed personal data)及推测的个人数据(inferred personal data)。^[29]意大利学者马尔杰里(Gianclaudio Malgieri)根据个人与相应数据联系的紧密程度将个人数据区分为强关系数据(strong relationship data)、中级关系数据(intermediate relationship data)以及弱关系数据(weak relationship data),^[30]事实上也是按照个人信息的来源进行的分类。笔者借鉴这种思路,并采用更为直观和通用的词汇进行表述,按照个人信息的来源将其区分为自然性个人信息、社会性个人信息以及复合性个人信息。

自然性个人信息主要是相貌、指纹、血型、基因等与生俱来且无法轻易改变的身体属性;社会性个人信息包括姓名、身份证号、电话号码、电子邮箱、家庭关系、工作单位、网页浏览记录、购物消费记录等为了社会生活的便利由个人主动或被动地获取到的相应符号或信息;复合性个人信息的典型例证是个人画像^[31]信息,实际上是一种经过信息收集者分析处理之后得出的对个人行为趋向与潜在偏好的预测。从它们产生的过程来看,自然性个人信息内化于相应自然人的身体之中,应当归属于其个人进行支配;社会性个人信息的获得则颇为复杂,并不能轻易将其权属配置给具体的个人;至于复合性个人信息,收集者和处理者在此类信息形成的过程中投入了更多资金、技术和智慧,但由于其利用又时常直接与具体个人发生联系,^[32]故也不能轻易将其权属配置给收集者和处理者。

诉讼实践中已经出现了区分个人信息类别而确定其利益归属的考量。在汉涛公司与百度公司不正当竞争纠纷案中,法院认为大众点评网上的用户评论信息是汉涛公司付出大量资源获取的,具有很高的经济价值,是汉涛公司的劳动成果。^[33]此类用户点评信息虽然是个人在社会生活中形成的,但其权属不宜直接配置给相应个人。另外,在淘友天下公司与微梦科创公司不正当竞争纠纷案中,法院虽未明确新浪微博中的用户信息属于微

[29] World Economic Forum, *Rethinking Personal Data: A New Lens for Strengthening Trust*, (May 2014), p. 16.

[30] Gianclaudio Malgieri, Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, *Privacy in Germany-PinG*, n. 4, 2016, 133 ff. <https://ssrn.com/abstract=2916058>, 最近访问时间[2018-05-11]。

[31] 在互联网领域,个人画像主要是指以真实用户群体为对象,以用户的静态属性(人口统计特征、空间和地理特征等)和动态属性(消费行为、使用行为等)数据为基础,通过定性或定量方法提取抽象出的具有显著特征的用户模型。参见亓丛、吴俊:《用户画像概念溯源与应用场景研究》,《重庆邮电大学学报(社会科学版)》2017年第5期,第82页。

[32] 例如,个人画像信息固然通过对数据挖掘等客观化的分析,反映了客户潜在的偏好和倾向,但却不一定能够代表客户的真实情况,甚至可能产生不公平的歧视。参见 Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *Machine Learning with Personal Data*, Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016, p. 6. <https://ssrn.com/abstract=2865811>, 最近访问时间[2018-05-11]。

[33] 上海知识产权法院(2016)沪73民终242号民事判决书。

梦公司的劳动成果,但强调这些数据信息是其拥有的重要商业资源。^[34] 这同样体现出此类社会性信息形成过程多主体参与的特性及其对利益归属产生的影响。

(三)作为一种民事利益保护的个人信息之甄别与筛选

《民法总则》中关于个人信息保护的规定被置于人格权的体系框架之中。根据民法学者的概括,《民法总则》第109条^[35]属于广义人格权之权利立法范畴,通过“人身自由”、“人格尊严”等彰显人格利益核心要素的表达,确立了一般人格利益的应受保护性,使其成为《侵权责任法》第6条第1款“民事权益”之中的法益,实现了权利立法与侵权法的结合,并形成了人格利益开放性保护的“中国模式”。^[36]

从这种立法安排来看,个人信息属于具体人格权范围之外被明确给予保护的一般人格利益,要进一步确定其作为一种民事利益的内涵,需要将其与已经类型化的具体人格权的保护对象进行比对,剔除重合的内容。既有的具体人格权中,隐私权与个人信息的关系最为密切。在比较法上,美国的隐私权概念相当宽泛,是调整所有精神性人格利益与部分物质性人格利益的权利,其作用类似于德国法上的一般人格权,个人信息可通过隐私权获得保护。^[37] 我国立法并未对隐私权进行明确界定,学界通常认为其内涵包括个人独处与对生活秘密的保有。^[38] 与此同时,论者亦时常将隐私信息的独享权或控制权纳入了隐私权的范畴之中,^[39] 它们又在通常意义上被个人信息的概念所涵盖。然而,《民法总则》将个人信息与隐私权分别规定,个人信息当中具备隐私性质的内容应由隐私权进行规范,与之同理,个人信息之中包含的其他具体人格权中的姓名权、名誉权、肖像权等性质的内容也应由相应权利进行规范。

社会性个人信息与复合性个人信息基本均是个人参与社会生活的过程中由行政机关认可或商业机构提供,借助信息媒介形成,个人并不能完全控制和支配,但这些个人信息中可能包含了人格利益和财产利益也是不争的事实。人格利益可以被隐私权、姓名权等内容涵盖,财产利益则不具有普遍性和直接性。一方面某些个人信息的财产价值只能由个别群体享有,^[40] 另一方面基于大数据分析进行的精准广告等商业行为建立在对海量信息与数据分析处理的基础上,单个信息的财产价值即使存在也并不显著。^[41] 由此,从正面尝试对个人信息保护的民事利益内涵进行精确界定并不现实,而从法律救济或侵权责

[34] 北京知识产权法院(2016)京73民终第588号民事判决书。

[35] 《民法总则》第109条:“自然人的人身自由、人格尊严受法律保护。”

[36] 参见叶金强:《〈民法总则〉“民事权利章”的得与失》,《中外法学》2017年第3期,第650页。

[37] 任龙龙:《个人信息民法保护的理论基础》,《河北法学》2017年第4期,第187页。

[38] 参见Richard A. Posner, *The Economics of Justice*, (Cambridge: Harvard University Press, 1981), pp. 272-273。

[39] 参见王泽鉴:《人格权的具体化及其保护范围·隐私权篇(中)》,《比较法研究》2009年第1期,第9页;另见范进学:《我国隐私权的立法审视与完善》,《法学杂志》2017年第5期,第44页。

[40] 例如,名人能够许可商家在商品或服务的宣传推销中使用其姓名及肖像从而获取商业利益,亦即其姓名与肖像本身内涵了财产利益,但这种财产性利益并不具有普遍性。参见郭明龙:《论个人信息之商品化》,《法学论坛》2012年第6期,第110页。

[41] 参见吴伟光:《大数据技术下个人数据信息私权保护批判》,《政治与法律》2016年第7期,第118页。

任法的角度进行规制成为最现实和理性的选择。^[42]

三 财产规则与责任规则在个人信息保护中的竞争

按照现有立法,尚不能明确侵害个人信息的行为将承担何种具体的侵权责任,这关系到法律救济层面财产规则与责任规则的选择问题,在同意规则于立法与实践中的渐遭诟病的情况下,责任规则具备了与财产规则竞争的前提条件。

(一) 责任规则与个人信息的共享属性及社会价值

个人信息的对象和范畴随着科技水平的提高不断扩展。例如血型、基因、虹膜等具有人身专属性的个人信息,虽内化于身体,但没有生物技术的发展,这些人身属性是无法被发现和认知并加以利用的;身份证号、交易记录、网页浏览记录、手机号码、电子邮箱等社会性个人信息是随着相关技术的普及利用才新增的个人信息类型;个人画像信息的出现和利用更是以大数据技术为基础,通过数据分析、算法应用等方式实现。

社会性个人信息多是个人参与社会生活取得,与其他主体提供的管理或服务具有密切关系。例如,身份证号是国家户籍管理机关依照身份管理与识别系统配置给每一个合法公民的个人识别符号;电话号码、电子邮件是自然人为了参与社会活动,以合同形式取得的一种对特定公共资源的个人使用;网上交易记录、电子支付记录则是在商业活动中留下的痕迹,其形成既体现自主选择,又有赖于交易相对方提供的交易机会、中介机构提供的购物媒介或支付媒介,以及基础网络运营商提供的服务。复合性个人信息的形成与收集者和处理者的关系更加密切,需要对社会性个人信息的集合进行分析处理,在利用过程中又将之与具体的个人联系在一起,有时甚至不需要结合自然性个人信息就能够识别到个人。

可见,社会性个人信息与复合性个人信息具有相当程度的共享属性,大数据技术的推广普及使得其蕴藏的公共管理和商业营销的巨大潜力得以显现。这种潜力建构在海量个人信息数据的基础之上,单独或少量个人信息数据的使用价值具有较大的局限性,同时个人信息的价值需要进一步的数据分析才能实现:“分析为大数据赋予生命力。设若没有分析,大数据可以被完全或部分地存储和检索,但这就使得其与最初的数据别无二致,包含了诸多计算技术的分析是大数据革命的助推器。正是分析使大数据集合产生了远胜于数据集合本身所带来的价值。”^[43]根据权威机构的研究结论,个人信息的收集和分析为公

[42] 民法学者将这种做法称之为“行为规制模式”,即从他人行为控制的角度,来构建利益空间,通过他人特定行为的控制来维护利益享有者的利益。参见叶金强:《〈民法总则〉“民事权利章”的得与失》,《中外法学》2017年第3期,第650页。此外,也有学者提出个人信息保护法防范的是一种因个人信息被滥用而可能产生的抽象的危险,这一危险可能现实化为隐私受侵害、名誉受损或者财产损失,遵守个人信息保护规则有助于避免这种危险。这依然是一种从他人行为控制的角度进行规范思路。参见杨芳:《个人信息保护法保护客体之辨——兼论个人信息保护法和民法适用上之关系》,《比较法研究》2017年第5期,第81页。

[43] President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, (May 2014), p. 24.

共管理与商业服务带来的积极效用至少体现在教育、交通、消费品、电力、油气、医疗保健、消费金融等七大领域。^[44]

从法律救济的规则选择出发,责任规则在体现个人信息的共享属性及发挥其社会价值方面具有更为积极的效果。试想,若坚守财产规则,则个人信息的收集、使用与分析均必须依照自愿交易的原则取得海量自然人主体的同意,与社会性个人信息的共享属性相悖,在实践中可能导致效率低下、大数据应用裹足不前。与财产规则相比,责任规则赋予了更多的行为自由,亦为技术创新和提高公共管理效率、增进商业服务质量保留了足够空间。^[45]

(二) 财产规则与个人的隐私利益及人格尊严

自然性个人信息属于与生俱来的身体特征,不当收集和使用产生的问题,通过隐私权等具体人格权保护通常可以解决。社会性个人信息与复合性个人信息由于其产生过程中参与主体复杂,不能径行分配给个人独享,具有一定的共享属性。但是,大数据技术对个人信息的深度挖掘和利用,也大大提升了侵害隐私的风险,甚至带来了人格尊严减损的潜在可能。

同个人信息的范畴随着时间的推移和技术的进步不断扩展一样,隐私利益之所以得到关切,一方面是人的主体观念与权利意识逐步觉醒的体现,另一方面也源自技术进步与传播媒介日渐丰富带来的消极影响。在美国学者沃伦与布兰代斯奠定隐私权概念基础的论文中就阐明了这一点:“快速照相和报社已经侵犯了个人和公民生活的神圣领地,许多机械设备的使用使我们面临着这样的威胁:隐秘空间内的喃喃私语也将被从屋顶上宣扬出去。”^[46]网络时代加剧了隐私风险,个体获得了相对匿名的身份状态,陌生的人际关系和相对隔离的时空状态带来一种脱离群体规范与熟人社会处事规则的行为自由,借助于互联网,更多的个人信息可能被公开和挖掘。当某个事件引起群体性的价值共识或情绪宣泄时,借助于过往形成的诸多痕迹,极易锁定相应个体,为隐私保护带来极大困扰。^[47]

与此同时,对个人信息的大数据分析和利用有可能使个人被贴上不同标签,带来一种新的身份歧视,对人格尊严的维护产生消极影响。复合性个人信息中的个人画像信息就是例证,此类个人信息以“行为定向”(behavioral targeting)和“画像”(profiling)为特点,最典型的的就是网络服务商对个人用户浏览记录和行为轨迹的追踪。这虽然有助于增加用户检索的精确性和推送广告的相关性,节约时间成本,但同时也可能产生“井蛙之见”(tunnel vision),使得用户的先前行为“一语成讖”,形成累积效应,将其框定在由商业机构业

[44] McKinsey Global Institute, Open data: Unlocking innovation and performance with liquid information, (October 2013), p. 2. <http://www.commit-nl.nl/sites/default/files/Samenvattingrapport.pdf>, 最近访问时间[2018-05-11]。

[45] 目前美国的做法更接近责任规则的基本架构,参见郑戈:《在鼓励创新与保护人权之间——法律如何回应大数据技术革新的挑战》,《探索与争鸣》2016年第7期,第83页。

[46] Samuel Warren & Louis Brandeis, The Right to Privacy, 4 *Harv. L. Rev.* 193, 194 (1890).

[47] 近年来“人肉搜索”的大行其道就是例证。有论者即敏锐地指出,作为社会实践的人肉搜索行为事实上先于网络时代的“人肉搜索”,互联网的出现不过增进了人肉搜索的技术条件。参见刘晗:《隐私权、言论自由与中国网民文化:人肉搜索的规制困境》,《中外法学》2011年第4期,第872页。

已给定的选择范围之内,反而进入了一种“自治困境”(autonomy trap)。^[48] 个人画像信息被出售给第三方之后,又极易形成新的歧视性做法,导致不同个体在获取教育和就业机会等方面受到不公平对待。

如何最大限度地防止对隐私利益的侵犯以及维护人格尊严? 财产规则似乎提供了较为满意的答案,即对于任何收集和使用个人信息的行为,均需征得相应个体的同意,毕竟个人的自主性即是正当,^[49] 理性人能够做出个人利益最大化的选择。试想,若在个人信息保护中采纳责任规则,无异于促成了个人信息的强制交易,使得个人更加暴露在网络时代的放大镜之下,隐私利益与人格尊严也变成了可以讨价还价的商品。较之于责任规则,财产规则在保障隐私利益和维护人格尊严方面显然能够起到更好的预防和警示功效。^[50]

(三) 个人信息保护中的利益平衡

个人信息保护不但涉及个人利益,也与产业发展、公共管理相联系。财产规则固然能够在形式层面为个人信息进行事前防护,但不利于商业化的信息数据开发和利用,且以同意规则为表征的财产规则实践效果不佳;采用责任规则能够最大限度地发挥个人信息的利用价值,提高商业服务的效率,但也增大了侵害隐私的风险和减损人格尊严的可能。对于个人信息保护的规则选择,涉及个人隐私与人格尊严、公共管理及商业利益的平衡,与特定国家在不同阶段的政策导向具有较为密切的关联。

就政府实施的公共管理而言,基于海量个人信息的收集和使用,政府机构有能力创建大规模数据集,催生新的科研成果、为公共政策的制定提供决策参考,推进经济增长。^[51] 此外,对个人信息的获取与分析在反恐与治安等方面亦将发挥重要作用,个人信息的跨境传输对开展国际合作与维护国家安全也具有不容忽视的效果。^[52]

商业机构收集使用、分析处理个人信息的行为受到法律限制的多寡与面临的法律风险高低,甚至可能对整个产业的发展前景产生重大影响。在大数据时代,数据已成为最有价值的无形资产,从国际竞争的格局来看,如果不能赶上科技发展的潮流,在全球化的洪流中再强大的个人信息保护规则也只能停留在纸面上,个人不但无法从中得利,反而将由行业先行者掌握话语权,在事实层面遭遇不公待遇。^[53]

[48] Ronald Leenes, Do They Know Me? Deconstructing Identifiability, 4 *U. Ott. L. T. J.* 135, 145 (2007).

[49] 参见金观涛著:《历史的巨镜》,法律出版社 2015 年版,第 13 页。

[50] 目前欧盟的相关立法更符合财产规则的基本架构。例如法国有非常严格的隐私权保护法,任何人未经允许在网络上发布他人(包括自己的未成年子女)的照片,都可能面临最高一年的监禁和 35000 英镑的罚款。<http://www.dailymail.co.uk/news/article-3472292/Children-SUE-parents-future-breaching-privacy-uploading-photos-Facebook.html>,最近访问时间[2018-05-11]。

[51] 参见 John Carlo Bertot:《大数据与开放数据的政策框架:问题、政策与建议》,郑磊、徐慧娜、包琳达译,《电子政务》2014 年第 1 期,第 6-7 页。

[52] 日前,国家网信办已经发布《个人信息和重要数据出境安全评估办法(征求意见稿)》,主要内容包括:个人信息出境的同意规则、行政机关对其业务范围内的数据出境状况进行安全检查的机制、网络运营者的自评估机制、安全评估的重点内容、禁止数据出境的情形。http://www.cac.gov.cn/2017-04/11/c_1120785691.htm,最近访问时间[2018-05-11]。

[53] 谷歌在搜索引擎、大数据处理和人工智能方面的压倒性优势,及其对欧亚各国公民个人数据的实际控制就是一个鲜活的例子。参见郑戈:《在鼓励创新与保护人权之间——法律如何回应大数据技术革新的挑战》,《探索与争鸣》2016 年第 7 期,第 84 页。

从实现个人隐私利益、维护人格尊严的角度考察,个人信息的收集使用带来的更多只是一种侵害的风险和可能性,在实践中广遭诟病的电话营销、垃圾短信、电信诈骗等现象亦可以通过既有的隐私权制度和相应的刑事法律规范加以解决,而“行为定向”和“画像”等复合性个人信息的生成和利用对人格尊严的减损还只是一种担忧。

(四) 责任规则在我国立法中的实现路径

责任规则在与财产规则的竞争中具有一定优势,立法中如何实现需要进一步阐述。

比较法上,美国的经验值得关注。美国卫生、教育及福利部早在1973年的报告《记录、计算机与公民权》(Records, Computer, and the Rights of Citizens)中就针对数据库问题对个人信息的利益内涵及其归属进行概括:“包含个人信息的数据库往往反映并协调个人和机构之间的关系,这种关系对双方都有益,而且它往往是为了机构和个人的共同目的被创造出来的。”^[54]因此,美国将个人信息保护的重心投向对收集者和使用者行为的规制,强调对个人信息被滥用的风险进行事先防控。^[55]这实际上可以理解为以义务的形式事先设定了有关个人信息的使用、处理和交易的法定条件,因而符合责任规则的基本界定。

对于自然性个人信息,由于其具有较强的人身专属性,理应由相应个人享有权利,并通过具体化的人格权寻求保护。社会性个人信息与复合性个人信息属于一种值得保护的民事利益,由于其产生于多方主体共同参与,在利益归属层面也不能由个人独占,但理论上的共享在实践中难于操作。可供选择的立法模式应当是为个人信息的收集者和控制者、处理者设置相应义务,只有履行了义务,才能实现对个人信息的交易,这符合责任规则的界定。因此,立法对责任规则的实现就是如何确定合理可行的义务规范,使得按此行事的相应主体能够实现对个人信息的合法收集与后续利用,这实际上就是一个市场定价的过程,对于违反这种义务的行为则由行政机构施以处罚或由个人依据相应的请求权寻求救济。

《消费者权益保护法》《网络安全法》以及行政法规、部门规章、司法解释中对个人信息的收集与使用都是以同意规则为中心展开的,只要满足形式上的同意要件,后续的使用和处理行为似乎当然免除了法律责任,因而在未来的“个人信息保护法”中确立个人信息保护的责任规则是更为现实的立法选择。具体而言,可以借鉴美国的行为规制模式,为信息控制者和处理者设置义务,以行业自律的方式进行事前规范。^[56]如果违反义务,主管部门可施以相应处罚,个人也可寻求司法救济。与此同时,亦应保障个人针对信息处理行

[54] Records, Computer, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, (July 1973). <https://epic.org/privacy/hew1973report/>, 最近访问时间[2018-05-12]。

[55] 美国消费者隐私保护立法采纳的场景风险规则即是例证,2015年发布的《消费者隐私权利法案》草案(Consumer Privacy Bill of Rights Act)第103节规定,经营者在场景一致的情形下,可以进行数据的收集处理。在场景不一致的情形下,经营者应当通知,以使个人决定是否减少数据的披露来降低隐私风险。对场景风险规则的相关介绍与评价可参见金耀:《消费者个人信息保护规则之检讨与重塑——以隐私控制理论为基础》,《浙江社会科学》2017年第11期,第66页。

[56] 例如,在中央网信办、工业和信息化部、公安部和国家标准化委员会的倡议下,国内十家互联网企业于2017年9月共同签署了《个人信息保护倡议书》,参见媒体报道,“个人信息保护倡议书签署仪式举行 公布隐私条款专项工作评审结果”,http://www.cac.gov.cn/2017-09/25/c_1121715816.htm, 最近访问时间[2018-05-12]。

为的选择退出权利,具体包括知悉权、更正请求权、封锁请求权和删除请求权等。^[57] 这些权利没有实际的财产利益,依然体现为相应个人信息收集者和处理者未能满足法定义务时需要承担的法律责任,是一种法定的交易条件,与责任规则的内涵相一致。

综合看来,在个人信息法律救济规则选择的利益衡量中,产业发展应占据优先地位,而公共安全与隐私利益及人格尊严的维护则应相对劣后。从立法论的视角出发,责任规则具有实现的可能性。但具体的规则选定需要回到卡-梅框架的理论预设,通过效率比较决定不同的个人信息类型应当适用何种救济规则。

四 个人信息保护中财产规则与责任规则的协调

卡-梅框架的重要目标之一就是在确定了相关权利或利益的归属之后,为不同规则的选择提供相应理论依据。卡、梅二人提出的评价标准是经济效率(economic efficiency)、分配偏好(distributional preferences)和其他正义考量(other justice considerations)。^[58] 由于分配偏好与正义考量的不确定性,后继学者将关注点投向了经济效率。

起初,这种分析从科斯经典的交易成本理论^[59]获得启发,提出当交易成本较高时,责任规则比财产规则更为可取的论断。^[60] 有学者将交易成本论进一步概括为两个准则:当交易成本较低时,使用财产规则(否则使用责任规则);当损害能够被合理精确地计算,则使用责任规则(否则使用财产规则),后者又被称之为“估价成本”(assessment costs)。但论者敏锐地指出当交易成本和估价成本均较高时(这在现实中较为常见),对财产规则与责任规则的取舍将陷入循环往复的相互推诿之中,无法形成有效结论。^[61] 由此,又有学者尝试从事前出发衡量经济效率,亦即考察具体规则对相关主体未来行为模式产生的影响,这种影响包括可能产生的过度投资或投资不足、逆向选择(adverse selection)以及道德风险(moral hazard)等问题。^[62] 综合看来,对于责任规则与财产规则在相应权益保护问题

[57] 参见杨芳:《个人信息保护法保护客体之辨——兼论个人信息保护法和民法适用上之关系》,《比较法研究》2017年第5期,第81页。

[58] Guido Calabresi & Douglas Melamed. Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 *Harv. L. Rev.* 1089, 1093 (1972).

[59] 参见 Ronald Coase, The Problem of Social Cost, 3 *J. L. & Econ.* 1, 1-44 (1960)。

[60] 波斯纳最早提出这种主张,并将其表述为“当交易成本较高时,能最大限度发挥价值的资源配置方式是否否认权利所有人的禁令救济而代之以损害赔偿”。(where transaction costs are high, the allocation of resources to their highest valued uses is facilitated by denying property right holders an injunctive remedy against invasions of their rights and instead limiting them to a remedy in damages.) 参见 Richard A. Posner, *Economic Analysis of Law* (1st ed. 1972), p. 29。转引自 James E. Krier & Stewart J. Schwab, Property Rules and Liability Rules: The Cathedral in Another Light, 70 *N. Y. U. L. Rev.* 440, 456 (1995)。

[61] 参见 James E. Krier & Stewart J. Schwab, Property Rules and Liability Rules: The Cathedral in Another Light, 70 *N. Y. U. L. Rev.* 440, 456-457 (1995)。其他有关交易成本论的批判与争议,可参见 Louis Kaplow & Steven Shavell, Property Rules Versus Liability Rules: An Economic Analysis, 109 *Harv. L. Rev.* 714, 714-790 (1996)。

[62] 参见 Ian Ayres, Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade, 104 *Yale L. J.* 1027, 1027-1117 (1995); Jack M. Balkin & Ian Ayres, Entitlement as Auction: Property Rules, Liability Rules, and Beyond, 106 *Yale L. J.* 703, 703-750 (1996); Carol M. Rose, The Shadow of the Cathedral, 106 *Yale L. J.* 2175, 2175-2220 (1997)。

中的选择,应综合考量事前效率与事后效率,成本最低、收益最高、私人行为最符合社会期望的规则更具优势。^[63]

(一) 事后效率的衡量

按照前述归纳,事后效率的衡量主要通过通过对相应规则产生的交易成本和估价成本进行比对,交易成本较高时,选择责任规则更有效率;估计成本较高时,选择财产规则更有效率。

就个人信息而言,财产规则和责任规则之下形成的交易成本具有显著差别。按照财产规则的基本要求,要达成对社会性个人信息以及复合性个人信息的交易,必须征得自然人的同意,且交易价格由其确定。这对于交易相对方,也就是试图收集、使用、分析个人信息的网络服务提供商或者其他主体而言,成本颇高。试想,不同自然人由于职业、年龄、学识等因素的影响,其对个人信息的感知与理解存在重大差别,预期的心理价位并没有可资参照的对象。对于个人信息被收集和利用的后果进行大致准确的预判是确定交易价格的基本前提,但个人理性在这一问题上缺乏基础。^[64] 个人的预判更多是一种粗糙的感性认知,并且极易受到大众传媒与社会舆论的左右,混淆正当行为与违法乃至犯罪行为的界限,使得其对交易价格的确定更加难以捉摸。此外,个人信息的商业价值只有建立在对海量个人信息进行大数据分析的基础上才能显现,单个信息只是潜藏了一定的商业价值,但并不显著。

责任规则下的交易价格由法院确定,这就产生了估价成本的问题。^[65] 法院的考量因素涉及做出价格评估所需的搜寻成本或管理成本,由此提升的发生错案的预期成本、选择不同规则的管理成本、延缓其他案件审理的机会成本,甚至律师代理的成本等等。^[66] 就个人信息而言,目前实践中发生的诉讼多以侵犯隐私权或名誉权为案由进行,法院判决的损害赔偿亦多为精神损害赔偿,^[67] 真正涉及到个人信息使用产生财产性收益的赔偿问题较为罕见。^[68] 这一方面印证了个人信息中内含的财产价值并不显著且个人难以主张的事实,也表明个案中的估价成本相对偏低。

如此,就事后效率而言,责任规则较之于财产规则更为优越。

(二) 事前效率的比较

事前效率的比较主要涉及采用财产规则或责任规则对于相关主体未来行为模式可能

[63] 参见凌斌:《规则选择的效率比较:以环保制度为例》,《法学研究》2013年第3期,第25页。

[64] 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118页。

[65] James E. Krier & Stewart J. Schwab, Property Rules and Liability Rules: The Cathedral in Another Light, 70 N. Y. U. L. Rev. 440, 440-483 (1995).

[66] 参见凌斌:《规则选择的效率比较:以环保制度为例》,《法学研究》2013年第3期,第23-24页。

[67] 例如,在刘馨予与乐视网隐私权纠纷中,法院认定乐视网将属于刘的个人信息秘密公开的行为对其隐私权造成了侵犯,判定乐视网向刘支付精神损害赔偿金1万元,参见北京市一中院(2016)京01民终3257号民事判决书。类似案件可参见浙江省杭州市中级人民法院(2016)浙01民终7399号民事判决书;四川省成都市中级人民法院(2015)成民终字第1643号民事判决书。

[68] 在上海汉涛信息咨询公司与百度公司有关使用大众点评用户评价信息的不正当竞争纠纷案件中,法院在一定程度上认可了汉涛公司对用户点评信息享有的权益,并判令百度公司赔偿其经济损失300万元。该案是直接涉及财产性收益赔偿问题的个人信息案件,但诉争主体是网络服务提供商,个人用户处于缺位状态,且事实上也难以主张相应权益。参见上海知识产权法院(2016)沪73民终242号民事判决书。

产生的影响。相应规则如果可能导致相关产业的投资不足或者过度投资、反向选择的出现(亦即,市场上相关产品或服务的质量普遍下降,产生劣币驱逐良币的负面效应),或者对个体行为产生不良的道德导向,都意味着对社会福利的增进没有裨益,因而不值得选择。

从个人信息的收集、利用以及分析处理来看,与之直接相关的是互联网及大数据产业。对互联网企业而言,数据的价值不言而喻,大量的数据进行不断融合交汇再产生新数据,导致数据边际成本越来越低,边际效应越来越大,从而催生新的经济形态。^[69] 可见,大数据价值的发挥很大程度上以对个人信息的收集和使用为起点,只有拥有足够多的个人信息,才能使数据分析的样本更为全面,数据处理的结果才能更有说服力和针对性,从而形成对未来的精准预测,提高商业活动与社会管理的效率,更进一步促进互联网与大数据产业的发展,最终增进人类社会的整体福利。因而,财产规则与责任规则对事前效率影响的优劣判断,最直接的标准就是哪种规则更有利于实现海量个人信息的集合。设若采用财产规则,且不论私下谈判产生的高额成本,将涉及个人信息收集、存储、处理、交易的决定权完全交由自然人主体,海量个人信息的集合将难以实现,对于整个数据产业造成的负面影响显然更大,资本的投向发生动摇,投资不足的问题将会显现。

就反向选择而言,从目前数据产业及互联网行业的发展来看,个人信息的收集使用提供了巨大的生活便利,产品和服务的个性化效果更加突出,大大提高了个人用户的选择效率和生活质量,^[70] 改变了搜索信息的方式。海量个人信息的集合才能够最大限度地发挥大数据的技术优势与实际价值,如果采用财产规则,意味着在这个集合之中形成了无数个分散的权属,极有可能形成“反公地悲剧”(The tragedy of the anticommons)。^[71] 个人信息的海量集合难以形成,基于大数据研发的产品和服务无法正常推出,更了解用户需求、更高效、更优质的产品和服务的市场价值无法彰显。

至于道德导向的问题,采用责任规则确实有可能产生个人信息被滥用的倾向,甚至出现一些倒卖个人信息的不法现象。但出于最大化个人信息利用价值的利益考量,具有技术实力进行大规模个人信息集合处理的互联网巨头公司依然有足够的动力采用积极的技术措施(如数据加密、物理隔离、内容识别等),确保海量个人信息及数据处理结果始终处于其掌控之下。此外,如果对个人信息保护采用财产规则,其造成的危害甚至更为严重。试想,如果将交易中的定价权配置给拥有个人信息利益的自然人,必然有很多收集和处理

[69] 上海社会科学院信息研究所信息安全研究中心主任惠志斌在“数据开放与发展纵横谈”论坛上的发言,2016年,北京。转引自张平:《大数据时代个人信息保护的立法选择》,《北京大学学报(哲学社会科学版)》2017年第3期,第143页。

[70] 按照美国学者的说法,“我们将自己的数据拱手交给企业,因为这样做所带来的结果是能提高我们的生活质量”。[美]马克·罗腾博格、茱莉亚·霍维兹、杰拉米·斯科特主编:《无处安放的互联网隐私》,苗淼译,中国人民大学出版社2017年版,第166页。

[71] 迈克尔·赫勒将“反公地悲剧”概括为“当太多人拥有一件东西时,就没人能够使用它了”(when too many people own pieces of one thing, nobody can use it.)参见 Michael Heller, The Tragedy of the Anticommons: A Concise Introduction and Lexicon, 76 *Mod. L. Rev.* 6, 6 (2013)。

行为在短期内无法通过正常途径和合理价格达成交易,面对巨大的利益诱惑,非法窃取个人信息的现象可能将更加严重,甚至催生出有关个人信息交易的“黑市”。此外,在采用财产规则时,许多合法的个人信息收集行为反而有可能成为后续非法交易的助推器。例如,诸多小型互联网公司以及其他实体机构虽然有机会以合法形式收集到相当数量的个人信息,但由于其不具有大数据处理的技术能力,或者并不以数据处理和交易作为主营业务,保障个人信息的安全并对之进行控制并不能为其产生更多经济效益,而以交易的方式将之分享给出价更高的市场主体却能够获取可观收益。因此,以财产规则抑或责任规则对个人信息进行保护,事实上都难以避免可能产生的个人信息滥用和非法交易的情形,但财产规则的适用带来的低效和黑市交易的可能性反而使得相关的互联网企业或意欲从事这一行业的经营者陷入道德危机,形成消极的行为指引。

因此,就事前效率的分析,责任规则依然优于财产规则。

(三) 个人信息保护中责任规则与财产规则的配置

通过事后效率与事前效率的分析比对,社会性个人信息与复合性个人信息救济规则的配置更应采纳责任规则,而非财产规则。虽然前文已经分析指出,自然性个人信息的保护基本上通过既有的隐私权等具体人格权制度可以解决,不应再作为个人信息指称的具体对象,但由于现实中对个人信息的传统认识,立法上亦暂未调整,故依然将自然性个人信息涵盖在讨论范围之内。

由于自然性个人信息具有人身专属性,交易定价权应归属于具体的个人,亦即采用财产规则。只有征得当事人的同意,相关主体才能够收集、使用和分析处理此类个人信息。实践中依然可以延用同意规则,违反该规则承担的具体法律责任将包括停止侵害、损害赔偿、惩罚性赔偿、行政责任乃至刑事责任。此外,由于可能具有的伦理特性,对于个别自然性个人信息的保护亦有必要采用禁易规则,不允许对某些特定信息开展交易。

对社会性个人信息而言,由于其具有共享属性和社会价值,在其利益内涵中牵涉到个人隐私利益和人格尊严、公共安全以及商业价值,基于交易成本和行为导向的分析,应当采用责任规则。即相关主体在收集、使用和分析处理个人信息时可以不征求具体个人的意见,而赋予其通过损害赔偿请求权取得交易对价的救济方式,由法院确定具体的价格。

对复合性个人信息而言,从其形成过程和利益归属的角度分析,显然收集者和处理者更有理由享有支配性权利,但由于此类个人信息在使用过程中同时结合了自然性个人信息和社会性个人信息,并且无法进行严格意义上的区分,使得这些信息的使用有可能识别到具体的个人。如果据此做出的行为预测存在歧视等问题,则有可能进入隐私权保护的领地,应当适用财产规则加以处置。当然,这种情形更有待于行业规则的建立,通过匿名化的处理方式降低个人信息使用的隐私风险。^[72]

[72] 关于个人信息去身份的价值和方式及其立法论意义,可参见金耀:《个人信息去身份的法理基础与规范重塑》,《法学评论》2017年第3期,第120-130页。

五 结 语

我国《民法总则》将个人信息确定为一种民事利益,并在相当程度上弱化了既有立法中以同意规则为表征的财产规则,为责任规则的适用提供了可能。结合我国力促大数据产业发展的现实需求,以及个人信息的特点和基本分类,通过卡-梅框架提供的理论工具,进行效率比对之后,个人信息救济规则的基本原则得以形成。在未来“个人信息保护法”的立法过程中,应体现这种更为理性客观的态度和立场,防止对个人信息定位的失当,以免权利虚置并对个人信息的正当使用和大数据产业的健康发展产生不应有的障碍。

[本文为作者参与的重庆市社会科学规划项目“互联网背景下数据财产交易的法律规制”(2017QNF45)的研究成果。]

[**Abstract**] With the promulgation of the General Provisions of the Civil Law, China has realized the preliminary systematization of the rules on the protection of personal information. At the level of judicial remedy, Article 111 of the General Provisions of the Civil Law rectifies to a certain extent the serious deviation of property rules, which have been constructed by separate laws and administrative regulations, from business practice. Through the positioning and classification of personal information, China will further clarify the basis of protection of personal information as interest rather than right, thus laying the foundation for the competition between liability rules and property rules. Based on the comprehensive consideration of such factors of economic efficiency as transaction cost, assessment cost, and behavior expectation, China should restructure the judicial remedy for the violation of personal information; apply property rules to natural personal information and liability rules to the social personal information and compound personal information; and, in the process of progressive elaboration of industry rules, establish the guidelines on the removal of the identity of personal information, so as to realize the gradual unification of theoretical conception, legal norms and social practice.

(责任编辑:支振锋)