中外法学 Peking University Law Journal
Vol.32, No.2(2020)pp.339－356

个人信息权利的反思与重塑

论个人信息保护的适用前提与法益基础

丁晓东*

摘 要 社会需要从隐私权保护过渡到个人信息保护,这已是共识,但学界缺乏对个人信息保护适用前提的研究。个人信息权利保护的适用前提是存在持续性的信息不平等关系,因此知情权、选择权、访问权、纠正权、删除权等权利不能针对信息能力平等的主体,也不能针对国家执法过程中产生的非持续性信息收集与处理行为。个人信息保护即信息隐私保护,区别于侵权隐私保护与执法隐私保护,其制度也不是传统部门法的简单叠加。此外,个人信息权利保护的法益基础具有多元性,有的信息权利可能对自身、他人、企业、市场与公众都有负面影响。因此,个人信息保护是为了实现"合理与正当的信息实践",应当在具体场景的信息关系中确定个人信息权利的边界。

关 键 词 个人信息 适用前提 法益 公平信息实践 不平等信息关系

一、问题的提出

个人信息保护在中国已经提上日程。2012年,全国人大常委会审议通过了《全国人民代表大会常务委员会关于加强网络信息保护的决定》,开启了个人信息的法律保护之路。2015年,《刑法修正案(九)》规定了侵犯公民信息罪,将"违反国家有关规定,向他人

* 中国人民大学法学院副教授。本文系国家社科基金一般项目"大数据背景下的个人信息保护与企业数据权属研究"(项目编号:18BFX198)的阶段性成果。

出售或者提供公民个人信息”的所有主体都纳入刑法调整范围。2016 年,《网络安全法》对个人信息保护作出了规定,规定网络运营者收集个人信息应当遵循合法、正当、必要的原则,而且应当获得个人的知情同意。2017 年,《民法总则》又在第 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。”2020 年,全国人大常委会将制定《个人信息保护法》,可以预见在不久的将来,就会有专门的《个人信息保护法》出台。

伴随着国家的立法进程,围绕着个人信息权利的理论探讨也成为热点,学术界从不同角度对其进行了讨论。例如就个人信息权是否成立的问题,有的学者主张个人信息可以成为一种权利;〔1〕有的学者认为个人信息是一种利益,不足以成为一种权利;〔2〕还有的学者则主张一种个人信息被保护权或个人信息相关权益被保护权,认为个人信息是一种保护相关权益的工具。〔3〕有的讨论则关注个人信息权利或利益的属性问题,例如有的学者认为个人信息所要保护的是个人的人格性利益,〔4〕有的学者认为个人信息所要保护的是个人的财产性利益,〔5〕有的学者则指出个人信息所保护的是个人的安全利益,〔6〕有的学者指出个人信息上还附着了他人利益与公共利益。〔7〕此外,还有的讨论则从部门法的角度对个人信息进行探讨,就部门法性质而言,有的学者主张个人信息权利是一种宪法性权利或基本权利,〔8〕有的学者则认为个人信息权利是一种私法性权利。〔9〕就部门法保护手段而言,有的学者重点从公法的角度

〔1〕 参见吕炳斌:“个人信息权作为民事权利之证成:以知识产权为参照”,《中国法学》2019 年第 4 期,第 44－65 页。

〔2〕 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;杨芳:“个人信息自决权理论及其检讨:兼论个人信息保护法之保护客体”,《比较法研究》2015 年第 6 期,第 22－33 页。

〔3〕 参见丁晓东:“个人信息的双重属性与行为主义规制”,《法学家》2020 年第 1 期,第 64－76 页。

〔4〕 参见张新宝:“《民法总则》个人信息保护条文研究”,《中外法学》2019 年第 1 期,第 54－75 页;房绍坤、曹相见:“论个人信息人格利益的隐私本质”,《法制与社会发展》2019 年第 4 期,第 99－120 页;高富平:“论个人信息保护的目的——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;叶名怡:“论个人信息权的基本范畴”,《清华法学》2018 年第 5 期,第 143－158 页。

〔5〕 参见刘德良:“论个人信息的财产权保护”,《法学研究》2007 年第 3 期,第 80－91 页;邢会强:“大数据交易背景下个人信息财产权的分配与实现机制”,《法学评论》2019 年第 6 期,第 98－110 页;谢琳、李旭婷:“个人信息财产权之证成”,《电子知识产权》2018 年第 6 期,第 54－61 页。

〔6〕 参见王德夫:“大数据时代下个人信息面临的新风险与制度应对”,《西安交通大学学报(社会科学版)》2019 年第 6 期,第 123－132 页。

〔7〕 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;高富平:“个人信息使用的合法性基础——数据上利益分析视角”,《比较法研究》2019 年第 2 期,第 72－85 页。

〔8〕 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》2016 年第 4 期,第 67－80 页。

〔9〕 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 119－129 页。

对个人信息保护进行阐述，〔10〕有的学者重点从私法角度对个人信息保护进行分析。〔11〕学者们的共识是：传统的隐私权已经不足以保护公民的合法权益，法律需要从隐私权保护转向个人信息权利或权益的保护。〔12〕

本文分享此种共识，并且从参与上述讨论获得了很多有益的洞见。但本文将关注一个更基础性的问题：个人信息权利保护的适用前提与法益基础。在本文看来，这一问题仍然讨论不足。尤其是个人信息权利保护的适用前提，尽管个人信息权利保护的中文文献已经浩如烟海，但中文文献对这一问题的讨论仍然处于空白。对这一问题不进行深入讨论，就可能造成对个人信息权利保护原理与制度的误解。

本文从个人信息权利保护的适用前提切入，指出全球通行的个人信息权利保护制度只能适用于具有持续性信息不平等的关系，个人信息权利只能针对商业性或专业性收集个人信息的主体。无论是欧洲、美国还是国际组织的个人信息权利保护制度，都排除了纯粹个人或家庭活动中的个人信息收集与处理，也排除了执法过程中的信息收集与处理。离开这一前提谈论个人信息权利保护，就无法正确认识个人信息权利保护的法益基础和基本原理，也无法正确设计个人信息权利保护的法律框架。

在此基础上，本文归纳了侵权隐私、执法隐私与信息隐私（个人信息保护）三种不同的法律框架，指出当前以公平信息实践为基础的个人信息保护框架不能应用于侵权隐私与执法隐私。个人信息保护实际上采取了一种二元治理的框架，将个人正当程序权利与合作治理方法结合起来。这种治理框架既区别于传统私法，也区别于传统公法。由于个人信息权利总是针对信息能力不平等的关系性主体，因此个人信息权利的法益具有多元性，分析个人信息权利，也必须将其还原到具体场景的信息关系中，在信息关系中确定个人信息权利的边界。

二、持续性不平等信息关系：个人信息权利保护的适用前提

在中文学术界，对于个人信息的保护往往会回溯和参照隐私保护的框架。众所周知，沃伦

〔10〕 参见周汉华：“探索激励相容的个人数据治理之道——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；高秦伟：“个人信息保护中的企业隐私政策及政府规制”，《法商研究》2019年第2期，第16－27页。

〔11〕 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，第62－72页；王成：“个人信息民法保护的模式选择”，《中国社会科学》2019年第6期，第124－146页；宋亚辉：“个人信息的私法保护模式研究——《民法总则》第111条的解释论”，《比较法研究》2019年第2期，第86－103页；谢远扬：“《民法典人格权编（草案）》中‘个人信息自决’的规范建构及其反思”，《现代法学》2019年第6期，第133－148页。

〔12〕 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38－59页。为了文章简洁需要，下文将统称“个人信息权利”，而不再使用“个人信息权利或权益”的说法。

(Smauel Warren)与布兰代斯(Louis Brandeis)于 1890 年发表了《隐私权》,提出了隐私权的概念。〔13〕其后,这一权利分别被英美法系与大陆法系所继承和发展。在美国,威廉姆·普罗斯(William Prosser)在侵权法重述中进行了归纳,将隐私侵权归纳为四种类型:对于独处的侵犯(intrusion upon seclusion);未经他人同意公开私人事实(disclosure of private facts);公开扭曲他人形象致误解(false light);擅自利用他人姓名或肖像为自身牟利(appropriation)。〔14〕在德国、中国等大陆法系国家,隐私权被归入人格权的范畴,侵犯隐私主要以侵犯人格权的案由进行立案和救济。〔15〕

当个人信息权利保护被提上议程,很多研究自然而然地以侵权法的框架来分析个人信息权利保护问题,探讨个人信息的权利类型、法益基础与制度设计。但这里却实际上有个前提性问题需要我们思考:个人信息权利保护是否可以针对所有活动中的所有主体?分析这一问题,可以发现个人信息权利中的知情权、选择权、访问权、纠正权、删除权、携带权等权利,都只能对具有专业性或商业性收集能力的主体进行主张,这些权利既不能对日常活动中的个人信息收集与处理进行主张,也不能针对国家执法中的个人信息收集与处理进行主张。个人信息权利保护的这一前提性问题,至少可以从三个方面的论据进行证明。

第一,不同国家和地区的法律都表明了这一点。以欧盟《一般数据保护条例》为例,其适用首先排除了平等主体之间的信息收集与处理。第 2 条第 2 款(c)项规定:"自然人在纯粹个人或家庭活动中所进行的个人数据处理"不属于《一般数据保护条例》的调整范围。〔16〕《一般数据保护条例》"重述"进一步指出:"本条例不适用于自然人在纯粹个人或家庭活动中与专业或商业活动无关的个人数据处理。个人或家庭活动包括:通信和持有地址,或在此类活动范围内进行的社交活动和在线活动。"只有对于"为此类个人或家庭活动提供处理个人数据手段的控制者或处理者",《一般数据保护条例》才能适用。〔17〕其次,《一般数据保护条例》还将"有关主管部门为预防、调查、侦查、起诉刑事犯罪、执行刑事处罚、防范及预防公共安全威胁而进行的个人数据处理"排除在外,〔18〕此类个人数据或个人信息的收集与处理也受法律规制,但其规

〔13〕 See Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No.5, 1890, pp.193－220.

〔14〕 RESTATEMENT (SECOND) OF TORTS § 652A－E (1977).

〔15〕 See Paul M. Schwartz and Karl-Nikolaus Peifer, "Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?", *California Law Review*, Vol.98, No. 6, 2010, pp.1925－1987.

〔16〕 "欧洲一般数据保护条例",丁晓东译,http://www.calaw.cn/article/default.asp? id＝12864,最后访问日期:2019 年 12 月 15 日。

〔17〕 《一般数据保护条例》"重述"第 18 条,https://gdpr-info.eu/recitals/, 最后访问日期:2019 年 12 月 15 日。

〔18〕 《一般数据保护条例》第 2 条第 2 款(d)项。

制方式与《一般数据保护条例》以及通行的个人信息权利保护制度有很大区别。〔19〕因为此类个人信息收集的主体虽然和个人之间也具有不平等的信息能力，但二者不具有持续性的信息关系。

美国的个人信息权利保护法律制度同样表明了这一点。以美国的领域立法为例，美国的《家庭教育权利与隐私法》(Family Educational Rights and Privacy Act of 1974)的规制对象是公共机构，如潜在雇主、公共资助的教育机构和外国政府。〔20〕美国的《1974 年隐私法》(Privacy Act of 1974)的规制对象是美国联邦规制机构收集与处理个人信息，〔21〕美国的《健康保险可携带性和责任法》(Health Insurance Portability and Accountability Act)的规制对象是医疗保健提供方、提供或支付医疗费用的实体、医疗信息交换所、商业伙伴等实体。〔22〕美国的《儿童在线隐私保护法》(Children's Online Privacy Protection Act)的规制对象是在线收集儿童信息的网站等主体。〔23〕这些法律都将个人信息权利保护的范围限定在具有持续性不平等信息关系的主体之间，既排除了个人日常活动中的信息收集与处理，也排除了政府执法中的个人信息收集与处理。对于政府执法中的个人信息权利保护，美国法律和欧盟一样，都以特殊的法律框架来加以规制，例如以宪法第四修正案以及相关联邦立法来规制。〔24〕美国州层面的立法更说明了这一点，例如 2020 年 1 月 1 日生效的《加州消费者隐私法》，顾名思义其规制对象主要是信息能力不平等的商家或企业，这一法律赋予个人的信息权利，也属于针对商主体的消费者权利。事实上，《加州消费者隐私法》不仅排除了一般自然人的信息收集与处理活动，而且排除了小微企业的信息收集与处理活动。《加州消费者隐私法》将受管辖的企业范围限定在年收入超过 2500 万美元，或者为了商业目的而接受 50000 条以上个人信息或者年收入的 50％及以上为销售消费者个人信息所得的公司。〔25〕

第二，从个人信息权利保护的思想资源来看，也可以看到个人信息权利保护的适用前提。无论是沃伦、布兰代斯、普罗斯等人所提的隐私权，还是大陆法系基于人格权的隐私保护，都建

〔19〕 Directive (EU) 2016/680 of the European Parliament and of the Council.

〔20〕 20 U.S.C. § 1232g (2006).

〔21〕 5 U.S.C. § 552a (2006).

〔22〕 Pub. L. No. 104－191.

〔23〕 15 U.S.C. § § 6501 - 6506.

〔24〕 See Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven: Yale University Press, 2011, pp.93－154.

〔25〕 按照加州《民法典》第 1798.140 节(c)的规定，《加州消费者隐私法》所指的“企业”是：“满足如下条件的个人独资企业、合伙企业、有限责任公司、公司、协会或其他法律实体：为其股东或收集消费者个人信息的其他所有者的利益或财务利益而组织或经营的，或代表其收集信息，并单独或与他人共同确定处理消费者个人信息的目的和方法的，在加利福尼亚州开展业务的，并满足以下一个或多个基本条件的公司：(A)根据第 1798.185 节第(a)小节第(5)段调整后，年总收入超过 2500 万美元。(B)为商业目的，每年单独或合并购买、接收、出售或共享 50000 条或更多消费者、家庭或设备的个人信息。(C)年收入的 50％或以上为销售消费者个人信息所得。”

立在侵权法的思想基础之上的，都预设了侵权方与被侵权方的防范关系与平等主体关系。但个人信息权利保护或所谓的信息隐私，其思想框架却起源于阿兰·威斯丁（Alan Westin）对于个人信息控制的主张。〔26〕这种主张具有明确的指向对象，明确了个人信息权利保护所针对的对象并非日常生活中的个体，而是具有专业性或商业性信息收集特征的主体，尤其是利用数据库等现代科技大规模收集个人信息的主体。〔27〕就此而言，尤其需要注意和澄清的是，虽然美国法上采取了“大隐私”的概念，将信息隐私也视为隐私保护的一种，但实际上美国的信息隐私与传统的侵权隐私具有结构性的差异。美国的信息隐私其实等同于欧盟和其他地区的个人信息权利保护，两者有着类似的针对对象和制度框架。

第三，从个人信息权利保护的制度框架来看，也可以看到个人信息权利保护的适用前提。全球通行的个人信息权利保护的制度框架起源于“公平信息实践”（fair information practices）原则，这一原则给个体赋予了一系列信息权利，给信息收集者与处理者施加了一系列义务。〔28〕但同样须注意的是，公平信息实践所处理的是不平等的信息关系，公平信息实践原则所规制的对象，要么是具有专业性信息收集能力的公共机构，要么是具有商业性或专业性信息收集能力的企业或类似主体。不可否认，欧盟和美国对于公平信息实践的继承和适用有一定的差异，例如欧盟《一般数据保护条例》以数据控制者和数据处理者的概念来概括政府、企业和专业信息收集者与处理者，而美国的《1974 年隐私法案》和《加州消费者隐私法》则对政府规制机构和企业进行区别立法。〔29〕但二者的差异并不妨碍其共同之处。无论是欧盟还是美国，都排除了纯粹个人活动中的信息收集与处理，同时以不同的法律框架来规制政府执法中的个人信息权利保护问题。

综上所述，个人信息权利保护只能适用于特定的信息关系，个人信息权利保护不能像隐私权保护那样，可以针对不特定的第三人。探讨个人信息的权利类型与法益基础，也必须从这个前提出发。不论将个人信息视为何种权利和类型，此类权利都只能针对形成持续性不平等信息关系的收集者与处理者。〔30〕在这个意义上，可以说个人信息权利保护中的相关权利既非传

〔26〕 See Alan Westin, *Privacy and Freedom*, New York: Atheneum Press, 1967, p. 7.

〔27〕 See D. J. Solove, “Public Records, Privacy and the Constitution”, *Minnesota Law Review*, Vol.8, No.6, 2002, p. 185.

〔28〕 参见丁晓东：“论个人信息法律保护的思想渊源与基本原理——基于‘公平信息实践’的分析”，《现代法学》2019 年第 3 期，第 96－110 页。

〔29〕 是否以及如何区分商业场景与公共机构场景中的个人信息保护，这也将是中国的个人信息保护立法或个人信息保护执法所面临的核心问题。

〔30〕 有的青年学者已经注意到个人信息保护法的适用范围问题，但将适用范围限定于个人信息自动化处理领域，这与本文所阐述的信息关系角度有一定的共同点，但也仍有一定的区别。从大部分国家和地区的立法来看，非自动化的个人信息收集与处理也仍然可能受个人信息保护法管辖，只要非自动化的个人信息收集与处理具有商业性或专业性。参见杨芳：“我国个人信息保护法适用范围之思考——隐私权救济困境下的个人信息保护法”，《社会科学家》2016 年第 10 期，第 112－115 页。

统民法权利，也非传统宪法权利。因为传统民事权利主要针对平等的民事主体，而传统宪法权利主要针对国家。但无论是个人信息权利保护中的知情权、选择权、纠正权、删除权，还是被遗忘权和携带权，都属于特定信息关系中的新型权利。如果将其纳入民法权利的范畴，也必须突破传统民法权利的平等法律关系，以不平等的民法权利关系来看待个人信息权利保护。如果将其纳入宪法性权利，则这种权利也只能针对专业收集个人信息的公共机构，不能针对偶尔或单次性获取个人信息的执法机构。

三、侵权隐私、执法隐私与信息隐私

个人信息权利保护为何只能针对信息不平等关系中的专业或商业信息收集者与处理者？回答这一问题，我们可以以侵权隐私、执法隐私与信息隐私的法律框架进行进一步分析，通过这三种法律框架的区分，我们可以更深入理解个人信息权利保护适用范围限定的原因，同时理解隐私与个人信息权利保护的整体图景。

首先，在侵权隐私的框架中，法律只对个人信息做非常有限的保护，而且依赖于侵权法这一被动性的保护方式。在美国，只有当相关主体侵犯了普罗斯所归纳的四种隐私侵权类型中的一种或多种权益时，而且只有当个人提起诉讼，此时法律才对个人信息进行保护。在大陆法系，只有当相关主体侵犯了人格权中的隐私权时，而且同样只有当个人提起诉讼，法律才对个人信息进行保护。对于纯粹个人活动或平等民事主体之间的个人信息收集与处理，国家主要采取以社会规范调整为主导的方式，只有在侵犯核心隐私而且公民提起诉讼时，国家法律才会介入。〔31〕

法律之所以对个人信息进行限定性保护与被动性保护，其原因在于个人信息具有很强的流通属性，在日常生活中，当我们打听他人的姓名、手机号、职业，甚至八卦他人的婚姻状况，都是非常常见的行为。如果赋予个人对于其信息的积极性权利，要求获取个人信息都必须获取个人同意，这将导致人们日常交往的失效与社会运转的失灵，导致打听他人信息也属违法的结果。个人信息的访问权、纠正权和删除权亦是如此，个人不可能要求访问他人所掌握的个人信息，也不可能要求纠正他人所掌握的个人信息，更不可能要求他人删除他人所掌握的个人信息。赋予个人以针对他人或平等主体的信息权利，既不合理，也不现实。〔32〕

其次，在执法隐私的框架中，个人信息权利保护框架也不能简单适用于作为公权力机构的执法机关。这其中的原因不仅在于公权力机构的执法目的是为了公共利益，因而区别于商业机构对于个人信息的收集和利用。更为重要的原因是，公权力机构在执法过程中和个体形成

〔31〕 Robert Post, "Rereading Warren and Brandeis: Privacy, Property, and Appropriation", *Case Western Reserve Law Review*, Vol.41, No.3, 1991, p. 647.

〔32〕 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 202 页。

的关系，并不存在持续性的信息关系。从信息收集与处理的关系类型来说，执法隐私所形成的个人与国家关系其实更接近于传统的侵权隐私中的个人与侵入者，二者都是某个主体对个人的隐私空间的一次性或多次性侵入。对于这种一次性的侵入，法律一般根据侵入的合理性来判断是否违法。套用卡拉布雷西的财产规则与责任规则的理论，就是法律仅仅为此类场景的个人信息设置责任规则而非财产规则。〔33〕

因此，个人相对于执法机构的权利仍然限定于传统核心隐私的范畴。在美国等国家和地区的司法实践来看，法院主要以“合理预期”的标准来确定执法机构是否侵犯公民的隐私，即政府执法过程的搜查或信息收集是否违反了一般理性人的合理预期。〔34〕对于政府在执法或搜查过程中所合法获得的个人信息，个人一般不具有知情选择权、访问权、纠正权、删除权等权利。这其中的道理不难理解。如果执法机构获取个人信息都需要获得个人同意，那么个人就会有足够的时间与机会藏匿或删除执法所需信息，同样，如果个人对于自身信息具有访问权、纠正权、删除权等权利，那么个人就能利用这些权利破坏执法所需要的信息与证据。无论是何种权利，都将从根本上破坏国家的执法能力。

最后回到信息隐私法即个人信息权利保护法的框架。从信息关系上来说，个人和信息收集者与处理者之间构成了一种持续性的信息不平等关系，区别于侵权隐私中的信息能力平等之间的关系，也区别于执法隐私中的非持续性信息关系。就此类关系的法律性质而言，此类关系更类似于劳动法与消费者保护法等社会法的关系。在社会法的关系中，劳动者与用人单位之间，消费者与商家之间都形成了一种持续性的不平等法律关系。个人信息权利保护中的关系亦是如此。个人信息的收集者与处理者介于公权力与私主体之间，与个人之间形成了一种不平等的持续性法律关系，这种关系既不同于平等主体之间的民事法律关系，也不同于个人与国家公权力之间形成的关系。〔35〕

对于这样一种关系，以公平信息实践为基础的个人信息权利保护制度采取了多种法律部门综合保护的进路。其中既包括了知情同意的民法框架，针对商家的消费者权利保护框架，还包括了对违反相关信息权利进行处罚的行政法框架。但需注意的是，这些综合性的法律框架并非移植或套用传统侵权隐私或执法隐私，也并非是不同部门法的简单叠加。相反，个人信息权利保护中的部门法之间相互交叉，使得每个部门法都区别于传统的部门法框架。

以个人信息的民法保护为例，个人信息权利保护制度更依赖于合同法保护，而对侵权法的进路相对依赖较少，因为传统侵权法所能发挥的作用有限，个人很难有动力、精力与把握去赢

〔33〕 See Guido Calabresi & A. Douglas Melamed, “Property Rules, Liability Rules, and Inalienability: One View of the Cathedral”, *Harvard Law Review*, Vol.85, No.6, 1972, pp.1089－1128.

〔34〕 See Katz v. United States, 389 U.S. 347, 360－61 (1967).

〔35〕 参见林嘉、邓娟：“论我国劳动法范式的转变”，《政治与法律》2009 年第 7 期，第 2－12 页；张守文：“社会法的调整范围及其理论扩展”，《中国高校社会科学》2013 年第 4 期，第 135－144 页。

得个人信息侵权的诉讼。〔36〕相较之下，合同法至少可以为个人提供更多的知情权和选择权，因而成为个人信息权利保护制度的重要组成部分。〔37〕但另一方面，即使信息收集者与处理者通过用户同意获得个人信息，而且完全满足合同法的要件，也并不能保证信息收集者与处理者对于个人信息的支配权。在个人信息被收集后，个人仍然拥有访问权、纠正权、删除权、信息安全权等多种不可让渡的权利。

以个人信息的消费者法保护为例，个人信息权利也区别于消费者法所赋予个人的消费者权利，一般消费者权利主要包括知情权、选择权，以及某些国家和地区所认可的“撤回权”或“后悔权”，〔38〕但个人信息权利保护中的相关权利则远远超出一般的消费者权利。〔39〕针对信息收集者，消费者不仅有知情权和选择权，还具有对个人信息的访问权、纠正权、删除权、携带权、信息安全权等多种权利，这些权利无论从类型的多样性，还是从权利主张的强度上来说，都远远超过一般的消费者权利。消费者在购买商品后，不可能要求查看或兑换支付的币种，或者对支付的金钱进行销毁和删除，但个人在同意信息收集者收集其个人信息并获得免费服务后，仍然有权利要求信息收集者纠正或删除个人信息。

最后以个人信息的行政法保护为例，个人信息权利保护也区别于一般行政规制中所采取的普遍规制的立场。在一般的行政法与行政规制中，法律与行政规章一般对被规制对象采取一视同仁的立场，施加相同的责任。但在个人信息权利保护中，法律对于被规制对象所施加的义务主要是程序保障责任，即要求信息收集者与处理者保障信息主体的相关权利得到正常行使。就这一点而言，个人信息权利保护法的行政法框架其实非常具有弹性。在个人信息权利得到充分保障和行使的前提下，信息收集者与处理者既可能因为个人的拒绝而完全无法收集与使用个人信息，也可能因为个人授权而获得宽泛的收集与处理个人的权利。

综合而言，个人信息权利保护法采取了一种马格卡·米尼斯基（Margot Kaminski）所谓

〔36〕 对于传统侵权法保护现代社会个人信息的有限性，See Diane L. Zimmerman, “Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort”, *Cornell Law Review*, Vol.68, 1983, p. 362; James Q. Whitman, “The Two Western Cultures of Privacy: Dignity Versus Liberty”, *Yale Law Journal*, Vol.113, 2004, p. 1151; Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information*, New York: New York University Press, 2006, pp.47－55.

〔37〕 当然这并不是说侵权法框架就无法对个人信息进行保护，传统侵权法经过改造，例如降低立案标准、倒置举证责任、降低证明标准、提高赔偿责任、设立公益诉讼，都可能使侵权法发挥更大作用。参见叶名怡：“个人信息的侵权法保护”，《法学研究》2018年第4期，第83－102页。

〔38〕 Eric Posner & Omri Ben-Shahar, “The Right to Withdraw in Contract Law”, *The Journal of Legal Studies*, Vol.40, No.1, 2011, pp.115－148.

〔39〕 有学者从理论上认为，不应设立过多的信息权利，应将个人信息权利作为普通类型的消费者权利，即个人只具有知情权和选择权。但是这种分析只是理论上的，全球通行的个人信息权利保护都认可了个人针对信息收集者与处理者的访问权、纠正权、删除权等个人信息权利。See Omri Ben-Shahar & Lior Jacob Strahilevitz, “Contracting Over Privacy: Introduction”, *Journal of Legal Studies*, Vol.43, No.S2, 2016, pp.1－11.

的“二元治理”(binary governance)结构,它将个人正当程序权利与合作治理方法结合起来。[40]这种治理结构类似公共参与治理,一方面,它将个人针对国家的正当程序权利主张转嫁到针对信息收集者与信息处理者身上;另一方面,它借鉴了合作治理中的意思自治与国家监管。它和传统侵权隐私、执法隐私所适用的对象具有重大区别,在部门法的保护方式上,这种保护也区别于传统部门法的简单叠加。

四、个人信息权利保护的法益基础

在分析了个人信息权利保护的适用前提及其原因之后,现在可以进一步分析个人信息权利保护的法益基础或保护目的,此种分析将为我们思考个人信息权利保护的制度框架奠定基础。

首先,个人信息权利保护的法益包含了防御性隐私权益。相比传统侵权隐私,个人信息权利保护的适用对象虽然限缩了,但其法益却没有限缩,个人信息权利保护仍然包含了侵权隐私中所包含的法益。传统侵权隐私所包含的法益,仍然是个人信息权利保护的共识与起点。如果信息收集者与处理者在个人不知情的情形下收集和处理个人秘密或私密信息,此时个人既可以选择以个人信息权利保护法的框架进行救济,也可以选择传统侵权隐私法的框架进行救济。[41]正如我国《民法典人格权编(草案)》所规定的:“个人信息中的私密信息,同时适用隐私权保护的有关规定。”[42]

其次,个人信息权利保护的法益还包含了针对信息控制者与处理者的信息自主控制权益,例如本文一再提到的知情权、选择权、访问权、纠正权、删除权、反对用户画像与自动化处理权和携带权等权利。就部门法性质而言,此类积极性权利并非针对平等主体的传统民法性权利,也非针对国家执法的传统宪法性权利。就权益的类型分类而言,这些权利有的具有人格性权益,有的具有财产性权益,有的具有个人的安全性权益,有的具有个人的便利性权益,有的具有实现公共政策的目的。而在更多的情况下,这些权利往往是多种不同类型权益的集合。

例如在个人对于收集信息时的知情权和选择权中,就包含了个人的人格性权益、财产权权益与安全性权益。因为对个人进行告知,赋予个人选择权,这包含对个人人格的尊重,[43]也赋予

〔40〕 Margot Kaminski, Binary Governance: “Lessons from the GDPR's Approach to Algorithmic Accountability”, *Southern California Law Review*, Vol.92, No.6, 2019, p. 1529.

〔41〕 当此类信息收集侵犯了我国宪法上规定的通信自由和通信秘密等权利时,此时即使信息收集者获得了个人的知情同意授权,也仍然属于违法行为。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 1—20 页。

〔42〕 《民法典人格权编(草案)》第 1034 条第 2 款。

〔43〕 Denise Reaume, “Dignity, Choice, and Circumstances”, in Christopher McCrudden (ed.), *Understanding Human Dignity*, Oxford: Oxford University Press, 2013, p. 33.

了个人在很多场景下对个人信息的财产化利用，〔44〕同时使得个人能够在一定程度上防范和预期相关的风险。〔45〕在个人信息访问权与纠正权中，此类权利则包含了个人的人格性权益、安全性权益与便利性权益。因为此类权利有利于个人通过访问和纠正个人信息而保护自身的人格，也有利于个人防范相关风险，同时给自己带来相关便利。在个人信息的删除权、反对用户画像与自动化处理权中，此类权利包含了个人的人格性权益与安全性权益。因为此类权利有利于个人通过删除和反对用户画像与自动化处理而保护自身的人格，也有利于个人防范相关风险。〔46〕而在个人信息携带权中，个人除了可以通过携带信息而实现其人格性权益、财产性权益、安全性权益、便利性权益之外，还具有实现公共政策的功能，因为这一权利可能可以促进数据流动，在一定程度上抵消数字经济中的网络锁定效应，从而促进市场更充分的竞争。〔47〕

需要指出的是，相比起防御性的隐私权利，个人针对信息收集者与处理者的信息自决权更具争议性。这其中的原因有几点。第一，有些信息权利看起来有可能保护个人权益，但实际上个人却无法有效行使这些权利，造成个人信息相关权利保护的落空，或者给个人带来其他风险。以个人知情权和选择权为例，面对信息能力不平等的信息收集者与处理者，个人很难有足够的兴趣、时间、专业作出真正理性的选择。个人信息权利保护中的“告知—选择”框架和同意机制，很多时候不但没有带来真正理性的选择，反而变成了无知和恐慌状态下的武断选择，不利于个人信息相关权利的保护。〔48〕同时，由于此类武断选择，个人信息知情权和选择权也造成了企业与公共机构无法合理有效地收集与利用此类信息为个人提供服务，为个人提供更多的便利。另一个例子是个人信息访问权、携带权等权利，此类权利虽然赋予了个体以访问和获取相关信息的权利，有利于维护公民相关权利，但此类权利也同时给个体带来了很多风险。因为一旦他人或犯罪份子冒用个人身份，利用信息访问权和携带权获取个人信息，此时个人信息就会全部泄漏，对个人信息权利造成重大伤害。即使法律对个人身份的验证程序作出严格规定，此类风险也可能因为公民信息访问权、携带权的行使而加大。〔49〕

第二，有些个人信息权利可能影响他人的合法权益。权利的冲突是权利保护中经常出现的

〔44〕 例如《加州消费者法》和《加州消费者条例》明确赋予了企业可以因消费者披露、删除或出售个人信息而向消费者提供的程序、福利或其他优惠，包括向消费者付费。

〔45〕 当然，由于大数据时代个人信息引起风险的不确定性，这种预期也可能是非理性的，See Alessandro Acquisti & Jens Grossklags, “What Can Behavioral Economics Teach Us About Privacy?”, in Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis & Sabrina De Capitani di Vimercati (eds.), *Digital Privacy*, Auerbach Publications, 2008, p. 369.

〔46〕 参见丁晓东：“被遗忘权的基本原理与场景化规制”，《清华法学》2018 年第 6 期，第 94－107 页。

〔47〕 参见丁晓东：“论数据携带权：权利属性、竞争效应与中国应用”，《法商研究》2020 年第 1 期，第 73－86 页。

〔48〕 See Daniel J. Solove, “Introduction: Privacy Self-Management and the Consent Dilemma”, *Harvard Law Review*, Vol.126, No.7, 2013, pp.1880－1903.

〔49〕 See Peter Swire & Yianni Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare”, *Maryland Law Review*, Vol.72, No.2, 2017, pp.373－375.

情形，〔50〕在个人信息权利的行使中，这种冲突更为明显。个人信息虽然关乎个人，但常常包含他人信息，当个人行使个人权利时，就很可能会影响到他人的信息权利。以访问权为例，当个人行使访问权获取个人信息，此时个人很可能就获取了第三方的信息。而当个人将个人通讯录信息或个人相册信息从一个平台转移到另一个平台，此时他人的通讯录信息或相册信息甚至可能面临核心隐私被侵犯的风险。〔51〕因为在个人行使访问权或携带权之前，个人信息可能位于陌生人的场景，很难被陌生人识别；但在个人行使访问权或携带权之后，个人信息就转移到了熟人或半熟人的场景，比较容易为熟人或半熟人识别。〔52〕

第三，有些个人信息权利可能给企业施加不合理的影响，影响企业的正当权益。以个人信息访问权、纠正权、删除权为例，个人信息一旦被合法收集，就可能在企业内部流转和分析，此时如果个体可以行使针对企业绝对性的访问权、纠正权、删除权等权利，那将意味着企业需要在所有的信息储存和分析部门都给予个人以访问、纠正和删除的权利。即使企业对于相关信息已经进行了匿名化处理，或者仅仅是在数据集合与统计中分析个人信息，个人也可以要求获取和纠正此类信息，在数据分析中删除此类信息。因为此类信息仍然可以重新识别和结合其他信息重新识别个人，因而属于个人信息的范畴。〔53〕在欧盟等地区，此类个人信息或个人数据权利等行使已经给企业造成了很多的不合理负担，因为企业不但面临普通个人的访问权、纠正权、删除权请求，而且可能面临社会组织、竞争对手所提起的大量请求。企业除了为个人寄送大量的个人信息，满足个人的信息访问权之外，还需要面对个人行使纠正权和删除权所带来的信息分析结果随时调整的风险。

第四，有些个人信息权利可能影响市场机制，损害平台经济和数字经济的发展。个人信息权利保护以信息的“识别”性作为保护前提，包括个人信息的已识别性与可识别性，〔54〕但在大数据的背景下，绝大部分信息都可能被纳入个人信息的范围，因为绝大部分信息都可能因为和其他信息结合而识别个人。〔55〕因此，个人信息权利保护的相关权利很可能导致市场中的信息流通与共享受到很大限制。从市场经济的基本原理来看，市场之所以能够有效运转，就在于市场中的信息流通与共享使得市场中的主体能够及时有效地进行自我调节。市场中消费者的用户需求、价格偏好、消费习惯、消费预期，都需要通过个人的相关信息汇总而获得，离开了对于

〔50〕 See Mary Ann Glendon, *Rights Talk : The Impoverishment of Political Discourse*, New York: The Free Press, 1991, pp.1－3.

〔51〕 See James Grimmelmann, “Saving Facebook”, *Iowa Law Review*, Vol.94, 2009, p. 1193.

〔52〕 内容社区和关系社区的区别，对于理解很多个人信息与数据保护问题具有重要意义，参见“内容社区和社交的关系”，https://www.jianshu.com/p/8b93bbc70486，最后访问日期：2019 年 12 月 20 日。

〔53〕 See Paul Ohm, “Broken Promises of Privacy”, *UCLA Law Review*, Vol.57, 2010, p. 1701.

〔54〕 See Paul M. Schwartz & Daniel J. Solove, “The PII Problem, Privacy and a New Concept of Personally Identifiable Information”, *NYU Law Review*, Vol.86, 2011, p. 1814.

〔55〕 See Nadezhda Purtova, “The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law”, *Law Innovation and Technology*, Vol.10, No.1, 2018, pp.40－81.

此类个人信息的收集和分析，市场就不可能有效运转。而在平台经济与数字经济中，这种信息的对称性尤其重要。无论是双边市场中所强调的平台的媒介功能，〔56〕还是长尾理论所强调的平台的去中心化功能，〔57〕都依赖于平台对于市场经济主体的相关信息进行合理收集和利用。就此而言，个人信息权利中的反对用户画像与自动化处理权等权利，如果上升为一种适用于所有场景的绝对性权利，未必有利于市场机制的正常运转。离开了用户画像等个性化推荐的能力，不仅个人可能无法在市场中获取有效信息和个性化服务，而且小微企业也可能会失去市场机会。只有大型企业、商场或商家才有可能在线上购买广告投放流量，或者在线下占据人们的注意力市场。

第五，有些个人信息权利还可能影响公共利益。个人信息的合理使用首先对于公权力机构具有重要作用，特别是对于一些具有公共治理功能的公权力机构，个人信息的收集与处理是其治理能力的基础。离开了对个人信息的合理收集与利用，公权力机构就不可能有效地征税，有效地扶贫，有效地制定相关政策或对国家进行“数字化管理”。此外，很多场景下的个人信息收集与流通其实具有公共功能，允许个人对于个人信息行使纠正权、删除权等功能，会极大地妨碍个人信息的合理流通与公众的知情权。这一点最为明显的是针对谷歌、百度等搜索引擎和网站的纠正权和被遗忘权。〔58〕试想，如果个人有绝对权利可以修改自己在百度词条和维基百科上的信息，或者可以删除自己在百度和谷歌搜索中的搜索结果，那么很多关于个人的负面信息都可能从这些网站上消失，因为没有人会希望自己的负面信息在公共领域流通。〔59〕对于公众的知情权而言，这种删除权的任意行使会造成信息的真空，甚至造成信息的失真。

综上所述，个人信息权利保护的法益既包括防御性的隐私权益，也包括人格尊严、财产权益、安全权益以及增强个人便利或个人信息能力的信息控制权。但信息控制权只能针对信息收集者与处理者，而且此类权利面临更多争议。也因此，个人针对信息收集者与控制者的信息控制权必然无法成为绝对性的权利，或者至少面临很多例外。例如《一般数据保护条例》已经对知情权和选择权规定了同意之外其他合法处理个人信息的机制。〔60〕访问权、纠正权、删除

〔56〕 See David S. Evans and Richard Schmalensee, “Matchmakers: The New Economics of Multisided Platforms”, *Harvard Business Review Press*, 2016, pp.15－117.

〔57〕 See Chris Anderson, *The Long Tail: Why the Future of Business is Selling Less of More*, Oversea Publishing House, 2006, pp.1－10.

〔58〕 See McKay Cunningham, “Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten”, *Buffalo Law Review*, Vol.65, No.3, 2017, p. 495.

〔59〕 Jeffrey Rosen, “The Right to be Forgotten”, *Stanford Law Review Online*, Vol.64, 2012, p. 88.

〔60〕 参见《一般数据保护条例》第 6 条第 1 款。除了(a)款的同意机制外，其他五种合法处理个人信息的类型分别为：“(b)处理对于完成某项数据主体所参与的契约是必要的，或者在签订契约前基于数据主体的请求而进行的处理；(c)处理是控制商履行其法定义务所必需的；(d)处理对于保护数据主体或另一个自然人的核心利益所必要的；(e)处理是数据控制者为了公共利益或基于官方权威而履行某项任务而进行的；(f)处理对于控制者或第三方所追求的正当利益是必要的，这不包括需要通过个人数据保护以实现数据主体的优先性利益或基本权利与自由，特别是儿童的优先性利益或基本权利与自由。”

权、反对用户画像与自动化处理权和携带权等其他权利亦是如此，在法律规定与实践执法中，这些权利实际上都受到了各种条件和例外的限制。

五、在具体场景与信息关系中思考信息权利

个人信息权利保护的法益基础之所以如此复杂，而个人信息权利又可能和如此多的利益相冲突，根本原因在于个人信息权利保护高度依赖于具体场景中个人与信息收集者与处理者之间的关系。当我们谈论一般性权利，例如财产权、人身权甚至隐私权，这些权利即使有争议，也大致有一个共识性的范围。即使在不同的场景中，这些权利的范围也大致确定。但在个人信息权利保护的问题上，个人信息权利及其保护的根源就在于不平等不合理的信息关系。因此，分析与界定个人信息权利的边界，就必须把个人信息重新放置在信息关系中加以思考。

在分类场景与信息关系中思考个人信息权利保护，这与个人信息权利保护的很多前沿研究是一致的。例如以国内学界越来越熟悉的海伦·尼森鲍姆（Helen Nissenbaum）的场景理论为例，场景理论的核心就是批判脱离场景与信息关系谈论个人信息权利保护。〔61〕在其研究中，尼森鲍姆列举了场景（context）、行为者（actors）、信息种类（information type）、传输原则（transmission priciple）等要素，以此说明个人信息权利保护在不同场景与信息关系中的不同规则。以场景为例，公共领域与私人领域划分是场景划分的一种，对于位于公共领域的个人信息，法律赋予给个人的信息权利要远远小于私人领域的个人信息。但尼森鲍姆也指出，公私领域的划分只是场景分类的一种。场景公正理论假设了更为多元的社会场景，每一种场景都需要不同的规则来确定个人信息权利保护的边界。〔62〕就信息角色而言，尼森鲍姆指出，对于不同的信息的发送者、接受者以及信息主体，法律赋予给个人的权利或个人信息流通的规则也不同。〔63〕例如在医疗场景中，医生收集病人信息与一般医疗化验人员收集信息就非常不同，医生收集病人信息并不需要时刻征询病人同意，但医疗化验人员则要受到更多知情同意的约束。就信息种类而言，尼森鲍姆指出，敏感信息与非敏感信息是个人信息分类的一种，但在不同场景与不同的信息关系中，此类分类完全可能会转化。〔64〕例如，脸部识别信息在线下场景的信息收集中，可能是非敏感信息甚至是公开信息，但在线上场景，此类信息就可能成为敏感信息。就传输原则而言，不同的场景与信息关系也非常不同。〔65〕例如医生与病人之间的信息传输原则，招聘场景中的雇主收集求职者信息的传输原则，就非常不同于商业场景中的网站收集消费

〔61〕 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, pp.140－160.

〔62〕 Ibid., p.141.

〔63〕 Helen Nissenbaum, supra note 61, pp.141－143.

〔64〕 Helen Nissenbaum, supra note 61, pp.143－145.

〔65〕 Helen Nissenbaum, supra note 61, pp.145－147.

者信息的信息传输原则。

再以近年来兴起的个人信息的信义法(law of fiduciary)、[66]保密关系法(law of confidentiality)[67]保护为例,此类研究的共同点,也是将个人信息权利保护还原到具体场景与信息关系中进行保护。例如,就个人信息的信托法保护而言,此类研究者的关注点在于,信息收集者与处理者与个人之间形成了非常不平等的信息关系,而且此类关系是持续性和互相依赖性的。对于这样一种关系,赋予个体以对抗性的信息权利,很难对个人信息形成有效保护,也难以对信息收集者与处理者施加应尽的义务,提供信息收集和使用的有效空间。因此,信托法保护的路径主张对个人和信息收集者与处理者分别施加信息信托权利与信息信义义务。相比起传统的个人信息权利,信息信托权利常常需要结合场景与信息关系来确定权利的边界。个人信息的保密关系法保护具有同样的特点,也强调在具体场景与信息关系中确定个人信息权利的边界,而非事先确定个人信息的权利边界,然后再将其应用在具体场景中。

在具体场景与信息关系中思考权利关系,这不仅是前沿理论的共识,也是不可避免的实践真理。在个人信息权利的确立中,最为形式化的信息权利宣示当属欧盟的法律框架。欧盟首先在《欧盟基本权利宪章》第8条以基本权利的形式规定了个人信息或数据的被保护权、访问权与纠正权,[68]其后又在《一般数据保护条例》第12条到第22条用大量的篇幅规定了不同类型的个人信息权利或数据权利。但在实际执法中,这些权利的边界仍然处于待定状态,仍然需要欧盟数据保护委员会(European Data Protection Board)等机构提供场景化的指引,特别是需要执法案例与司法案例来最终确定各类权利的边界。

在这个意义上,个人信息权利保护必须回到公平信息实践的"初心",反思当前个人信息权利保护制度是否实现了公平信息实践所预期的目的。从形式上说,当前欧盟等国家和地区的个人信息权利保护制度很好地继承了"公平信息实践"所开创的制度,因为"公平信息实践"的最初版本中,的确包含了大量的个人信息权利。公平信息实践诞生之初,其核心的原则与制度就与当今各国普遍采用的个人信息制度类似。例如1973年版本的"公平信息实践"原则规定:①所有的个人信息记录系统都不得是秘密的;②个人必须有途径知晓其哪类信息记录在案以及其是怎么被运用的;③在未经个人同意的情况下,个人必须有途径阻止其被收集的信息不会被用于其他目的;④个人必须有途径对可识别的个人信息进行纠正或修改;⑤任何创设、保存、

〔66〕 See Jack M. Balkin, "Information Fiduciaries and the First Amendment", *U.C. Davis Law Review*, Vol.49, No.4, 2016, p. 1183.

〔67〕 See Neil M. Richards & Daniel J. Solove, "Privacy's Other Path: Recovering the Law of Confidentiality", *Georgetown Law Journal*, Vol.96. No.2, 2007, p. 123; Woodrow Hartzog, "Reviving Implied Confidentiality", *Indiana Law Journal*, Vol.89, 2014, p. 763.

〔68〕《欧盟基本权利宪章》第8条第1款规定,"每个人的个人数据都有权得到保护",第2款规定"这些数据必须在有关人员同意或法律规定的其他合法基础上,为特定目的公平处理。每个人都有权访问收集到的有关他或她的数据,并有权纠正这些资料。"

使用、散播个人可识别数据的机构在因为特定目的而使用数据时，都必须确保数据的可靠性，必须采取措施避免数据被滥用。〔69〕就当前全球各个国家和地区的个人信息权利保护法而言，这些法律与制度都继承并且强化了“公平信息实践”中的信息权利。除了“公平信息实践”中所规定的知情权、选择权、访问权、纠正权之外，欧盟等地区的个人信息权利保护法还规定了反对用户画像和自动化处理权、〔70〕携带权等权利。

但从个人信息权利保护的“初心”或预期目的来说，当前很多个人信息权利保护制度对于“公平信息实践”的继承仅仅是形式性的，这些制度是否能够真正实现“公平信息实践”的初心，即实现的是信息收集者或处理者与个人之间的公平或合理的信息关系，仍然取决于相应制度是否能够在具体场景与信息关系中确立个人信息权利的合理边界。而要实现这一点，首要的任务就在于破除脱离具体场景与信息关系的权利思维和形式主义思维。这种思维可能可以大致应对某些权利问题，但对于个人信息权利保护而言，却可能导致各种不合理的信息实践。

对于很多法律人而言，在具体场景与信息关系中思考个人信息权利，看上去与法治的基本原理背道而驰。因为法治的基本原则恰巧要求普遍性的规则之治，〔71〕要求脱离人为关系来设计规则。〔72〕但需要指出的是，在关系中思考个人信息权利，并不排斥类型化的个人信息权利主张与规则治理，只是这种权利主张与规则治理更多依赖于从具体场景出发，通过自下而上的规则制定来勾勒和确定权利与规则。同时，这种类型化的规则治理更多从信息关系出发，通过信息关系中的合理信息实践或信息伦理来确定权利与规则。事实上，在现代法治实践中，这种基于具体场景和个案演化的规则制定方式并不少见，例如在行政规制中，很多前沿学术研究已经认识到，基于具体情境的正当性判断，反而比形式主义法治更可能符合法治的基本精神。〔73〕而在竞争法研究中，反垄断判断必须基于理性规则（rule of reason）来进行理性判断，

〔69〕 U.S. Dep't. of Health, Educ. & Welfare, Sec'y's Advisory Comm. on Automated Personal Data Sys., Records, Computers, and the Rights of Citizens (1973), https://aspe.hhs.gov/report/records-computers-and-rights-citizens, last visited 18 December 2019.

〔70〕 这一权利有时候也被称为“算法解释权”，对这一权利是否存在的讨论，参见张吉豫、丁晓东编：《人工智能的法律研究》，法律出版社 2019 年版，第 52－75 页；沈伟伟：“算法透明原则的迷思——算法规制理论的批判”，《环球法律评论》2019 年第 6 期，第 20－39 页；Sandra Wachter & Brent Mittelstadt & Chris Russell, “Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR”, *Harvard Journal of Law & Technology*, Vol.31, No.2, 2017, pp.3－71.

〔71〕 See Brian Z. Tamanaha, *On the Rule of Law: History, Politics, Theory*, Cambridge: Cambridge University Press, 2004, pp.1－3.

〔72〕 See Paul Kahn, *The Reign of Law: Marbury v. Madison and the Construction of America*, New Haven: Yale University Press, 1997, pp.1－8.

〔73〕 王锡锌：“行政正当性需求的回归——中国新行政法概念的提出、逻辑与制度框架”，《清华法学》2009 年第 3 期，第 100－114 页；Adrian Vermeule, “Our Schmittian Administrative Law”, *Harvard Law Review*, Vol.122, 2009, p. 1095.

而不能依赖规则本身(rules per se)进行判断,这也已经成为学界共识。〔74〕与个人信息权利保护类似,这些法律部门所遇到的问题更难以标准化,更依赖于具体情境中的相关因素,也因此更需要在场景与具体关系中进行判断。一旦脱离具体场景与信息关系,相关的个人信息权利主张就可能丧失正当性基础,蜕变为形式主义。

六、结语:重构大数据时代的个人信息权利保护

2020年,伴随着《加州消费者隐私法》的生效,面对欧盟以《一般数据保护条例》为代表的个人信息保护制度的强大影响,〔75〕信息隐私的两位学者伍德罗·哈特佐格(Woodrow Hartzog)与尼尔·里查德(Neil Richards)大声疾呼,当前正是美国信息隐私重构的宪法性时刻。〔76〕因为欧盟的个人信息权利保护制度未必适合美国,而美国自身的个人信息权利保护又面临种种不足,美国必须在这历史的关键时刻制定更为合理的个人信息权利保护制度。就此而言,中国面临着相同的挑战,面对欧美个人信息权利保护制度的竞争压力,是否能够走出一条独特的个人信息权利保护道路,对于中国而言既是挑战,也是机遇。而将挑战转化为机遇的前提是,我们对于个人信息权利保护的基本原理应当有清晰的认识。特别是对于个人信息权利保护的适用前提与目的,应当尽快走出相关认知误区。

正如本文所表明的,分析个人信息权利保护首先应当认清其适用前提。首先应当区分侵权隐私、执法隐私与信息隐私,对于现行以公平信息实践为基础的个人信息权利保护,应当明确这种保护只能针对具有持续性信息不平等关系的信息收集者与处理者,即只能应用在信息隐私的情形中。如果将个人信息权利保护制度适用于侵权隐私或执法隐私,那将误解个人信息权利保护的前提性问题,造成法律适用上的混淆。

其次,正如"公平信息实践"一词所表明的,保护个人信息的目的在于实现信息的合理实践;或者如同尼森鲍姆所指出的,个人信息保护的目的在于实现信息的合理流通。在这个意义上,当我们分析与探讨个人信息的相关理论时,必须认识到确立个人信息被保护的权利,其目的在于通过这类权利的确立来实现个人的相关权益、他人的相关权益、企业的相关权益、市场的相关权益以及公共利益。因此个人信息权利不是绝对性权利,不能用静态的形式主义的观念去理解和确定个人信息的边界。相反,我们应当在具体场景和信息关系中重新勾勒和确定个人信息权利。

在大数据时代,这一任务变得更为繁重。因为在大数据时代,形式主义的个人信息权利保

〔74〕 See Bus. Elecs. Corp. v. Sharp Elecs. Corp., 485 U.S. 717, 726(1988).

〔75〕 Paul M. Schwartz, "Global Data Privacy: The E.U. Way", *NYU Law Review*, Vol.94, 2019, pp. 3—31.

〔76〕 Woodrow Hartzog & Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection", *Boston College Law Review*, Vol.61, 2020, p.79.

护已经更加难以保护个人的相关信息权益，同时保证他人、企业、市场与公众对于信息的合理需求。在大数据时代，以识别为基础的个人信息范围大大扩展，造成了个人信息权利保护管辖范围变得非常宽泛；同时，大数据与人工智能发展的需要又使得数据的二次利用成为必要，对个人信息权利保护中的“目的限制”“信息最小化”等原则也形成挑战。解决此类问题，更需要我们突破传统强化个人信息赋权的进路，从信息信托、代表制等公私法混合的思路重新设计个人信息权利保护制度。只有如此，我们才能避免个人信息权利保护制度的异化，追寻个人信息权利保护的初心。

Abstract: It has become a consensus that modern society needs to transition from the protection of privacy right to the protection of personal information. However, there is a lack of research on the premise of personal information protection. The premise of the application of the personal information protection system is the asymmetric information relationship. Therefore, the right to informed consent, the right to access, the right to correction, the right to delete and other personal information rights cannot be aimed at the subjects with equal information capacity, or the non-sustainable information collection and processing behaviors generated in the process of governmental law enforcement context. Personal information protection is equal to information privacy protection, but different from infringement privacy protection and law enforcement privacy protection. Its system is not a simple aggregation of traditional branches of law. Meanwhile, the purpose or legal basis of personal information protection is diverse. Some personal information rights may have negative effects on the information subjects themselves, other people, enterprises, markets and the public. Therefore, the protection of personal information protection is to realize fair information practices. The boundary of personal information rights should be determined in contextualized information relationship.

Key Words: Personal Information; Applicable Premise; Legal Interest; Fair Information Practice; Unequal Informational Relationship

（责任编辑：章永乐）