交大法学 SJTU Law Review
No. 3 (2018)

大数据语境下的个人信息合理使用原则

江　波*　张亚男**

目次

摘要　大数据时代，个人信息的合理使用原则具有正当性，其符合大数据时代的法律需求，是平衡个人和数据控制者利益的利器，对作为个人信息法律核心原则的同意原则形成补充，弥补同意原则在大数据背景下的局限性。合理使用原则的内涵可适当借鉴著作权法上的合理使用原则，并在现有制度体现的基础上，通过数据安全管理、经设计的隐私、个人信息风险评估、个人参与和控制等相关规则加以丰富。

关键词　个人信息保护　合理使用原则　同意原则

一、合理使用原则的提出

大数据产业发展伴随着诸多的挑战，法律对个人权利和数据控制者权利保护的缺位，乃至失衡，势必影响大数据产业的健康发展。面对这些问题，我们急需结合我国数据产业发展和个人信息保护现状，从法律层面理清个人信息保护与使用的关系，在现有以同意原则为核心的个人信息保护规则上，找到促进数据产业健康发展和保护信息主体权利的平衡点。从世界范围看，个人信息保护制度迎来新一轮改革，自2010年以后，欧盟、日本等各国个人信息保护立法和相关国际条

* 腾讯控股有限公司法务副总裁、法学博士。本文为国家社科基金项目（项目编号：18CFX068）成果。
** 腾讯控股有限公司法务。

约都进入修改和完善期，此前没有制定一部统一个人信息保护法的国家也在这个阶段颁布了统一立法。当前信息经济强势发展，个人信息的挖掘、分析呈现出规模化的利用趋势，制定一部统一的保护个人信息权利，促进数据使用、流动的法律的呼声越来越高，对个人信息收集、使用、存储等各环节进行规范是势在必行的趋势。个人信息主体权利与数据使用者的利益平衡需要在大数据时代的法律规则中得到反映。

在研究现有立法与行业实践的基础上，尝试以个人信息主体与数据控制者之间的利益平衡为切入点，剖析同意原则的理论基础及面临的现实困境，从大数据时代发展现实需求、法律借鉴等角度提出合理使用原则，具有正当性、合理性和理论、现实意义。透过欧盟等国家的现有法律制度分析数据使用的合法基础，不难发现有突破同意原则的现象，存在除同意以外的其他可以进行数据处理的合法事由，而解析诸多事由，均是出于合理使用之目的。而出于商业秘密等知识产权保护的顾虑，各国法律也从一定程度上对同意原则进行了减损。进一步地，笔者通过观察国际条约和各国法律提出的数据管理、个人信息风险评估/隐私影响评估、经设计的隐私、个人参与和控制等规则，探索和解读其对保护个人信息和数据使用正当利益所起的作用，理清合理使用原则与这些规则之间的关联关系，以期将合理使用原则构筑、充实成为保护个人信息权利，促进数据合理使用的基本原则。从大数据时代促进数据流动的制度构建出发，提出在对数据使用的场景进行充分风险评估后可无须经权利主体同意为之处理，此种处理也构成合理使用。

二、合理使用原则的价值

（一）时代价值

将合理使用原则应用于个人信息保护与数据使用领域，是大数据时代数据流通和使用的现实诉求，需要得到法律层面的反映。在大数据时代背景下，保护个人信息，不等于禁止个人信息的使用、开放和共享，在数据使用高需求的大数据产业背景下，禁止个人信息的使用、开放和共享无疑会扼杀信息社会进一步发展的可能性。个人信息保护法应然地具备保护个人信息的目的，除此之外，个人信息保护的目的还在于促进个人信息的合法流通和使用。〔1〕例如，台湾的相关立法就紧扣了时代主题，其《个人资料保护法》将保护个人信息和促进个人信息的合理使用、流通作为立法的双重目的。在人类逐渐步入大数据时代，理清个人信息保护与使用之间的关系，找到平衡两者利益关系的方法和原则，将影响整个信息社会发展的方向、深度和广度。保护个人信息主体之个人信息不受非法获取、使用的重要性自不待言，而从促进数据使用的角度看个人信息保护，也是从大数据时代的发展眼光去看待个人信息保护问题，是大数据时代个人信息保护立法的应有态度，即强调数据的合理使用。

（二）利益平衡与指导制度设计价值

个人信息主体与数据控制者间的利益关系，是在当前立法、司法中需要协调和平衡的核心法律关系，平衡核心法律关系的原则是知情同意。然而大数据时代的数据二次利用、多环节流转特点将使得知情同意原则发挥的作用越来越有限。合理使用原则的引入有利于上述现状及问题的解决，以该原则为基石构建的立法规则体系具有更强的实践价值。

观察欧盟和美国相关立法，个人信息保护的规则事实上都从规范数据控制者个人信息处理活

〔1〕 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》，载《苏州大学学报（哲学社会科学版）》2015年第1期。

动出发，换言之，实现保护个人信息的立法目的，很大程度上取决于对个人信息处理活动的规范，个人信息使用与以使用为目的的相关处理是否构成合理使用，是判断个人信息保护相关规则是否有效的重要原则，对大数据时代约束数据二次利用、多环节流转有重要的现实意义。欧盟的《一般数据保护条例》及其被遗忘权等系列案例都已体现或运用了合理使用的理念，《一般数据保护条例》规定了无须征求用户同意而进行数据使用的例外条款，数据控制者的商业秘密、知识产权等合法权利对个人信息权利可起到限制作用，无一不体现了合理使用的理念。更进一步地，将合理使用理念具化为原则，可对相关立法规则制定、司法判决起到更好的指导作用，实现个人信息保护与使用的利益平衡目的。

大数据产业健康发展离不开对数据相关权利主体利益的明晰和权利边界的划定，法律对各方主体、各项权利的充分保障起到至关重要的作用。数据权利保障是大数据产业有序发展的前提和基础，内含了保障个人信息权和数据相关权利之义，即保护个人信息主体和保护数据控制者利益。从当前立法和司法保护环境看，相关权利保护领域都产生了一些新变化和趋势。总体而言，立法、司法层面都越来越多地体现出对个人权利保护的重视，然而，遗憾的是，对数据控制者的数据相关权利保护仅仅体现在少量的司法判决中，立法保护鲜而有之。这不利于平衡个人和数据控制者利益关系，对个人的过重倾斜保护，可能导致阻滞大数据产业发展的严重后果。在这样的立法背景下，确立合理使用这一原则显得尤为必要。以下对相关立法背景进行具体分析。

20世纪末期，个人信息保护的问题开始受到国际组织关注，经济合作与发展组织（Organization for Economic Co-operation and Development，以下简称“OECD”）在1980年制定了《隐私保护与个人数据跨境流动的指导方针》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），旨在加强隐私保护，促进个人数据跨境流动，确立了隐私保护的八项原则，并为各国立法广泛采纳。亚太经合组织（Asia Pacific Economic Cooperation，以下简称“APEC”）在2004年通过了《隐私权保护纲领》（APEC Privacy Framework），旨在保护隐私、促进信息流动、建立全球化数据处理标准程序和促进执法，以推广亚太地区的电子商务。世界各国也逐渐意识到个人信息立法中平衡个人和数据控制者利益的重要性，纷纷开启立法篇章。〔2〕

1. 20世纪80年代—90年代，个人信息问题受到普遍关注，相关立法主要规范政府机构

在此阶段，美国、加拿大、澳大利亚、日本都制定了隐私法，除美国在金融、消费者保护、未成年人保护、网络隐私保护领域较早进行立法，规范商业机构数据处理行为以外，其他国家的法律均只规范政府机构对个人数据进行处理的行为。

2. 21世纪00年代—10年代，个人信息立法规范重心转向商业机构

1995年欧盟率先开始个人信息保护立法，我国台湾和香港地区也在同时期颁布了个人信息保护法，欧盟之下的德国和英国、法国、瑞典亦先后制定了数据保护法。〔3〕这些立法都适用于政府机构和商业机构，但有的国家在同一套法律体系中规定了分别适用于政府机构和商业机构的两套规则。上述已提及，加拿大、日本、澳大利亚的法律之前只规范政府机构对个人数据进行处理的行为，直到2000年左右，这些国家才重新立法，或在原有法律基础上扩展立法，将其适用于商业机构。

3. 2010年至今，大数据时代个人信息立法进入新一轮修法阶段

近几年，个人信息保护立法进入新的修法高潮，这一时期的立法更加与大数据发展的时代主

〔2〕 周汉华：《个人信息保护研究丛书之3：中华人民共和国个人信息保护法及立法研究报告》，法律出版社2006年版，第25～40页。

〔3〕 王利明：《隐私权概念的再界定》，载《法学家》2012年第1期，第108～120页。

题紧扣，并随着技术和商业发展设定了被遗忘权、数据可携权等新型权利。个人数据在经济、社会和生活中扮演越来越重要的角色，数据相关的技术促进经济增长、增进社会福祉。个人数据收集、使用和储存大量且持续地增长。利用数据洞察和分析个人行为、兴趣和活动越来越普遍。与此同时，人的行为大量、轻易地以数据的形式被记录下来，个人数据利用可能引发的隐私风险越来越大，〔4〕个人信息保护问题受到更为广泛的重视，因此，修订个人信息法律或国际隐私框架以顺应大数据时代发展，为 OECD 等国际组织和许多国家提上修法议程，并业已获得通过。

国际约定层面，OECD 在 2013 年修改了《隐私保护与个人数据跨境流动的指导方针》，引入隐私管理计划、违反安全信息通知、国家隐私战略、教育和宣导和国际协作等概念，跨太平洋伙伴关系协定（Trans-Pacific Partnership Agreement，以下简称“TPP”）在电子商务一章中专节规定了个人信息保护，就 TPP 各国如何进行个人信息保护、跨境数据传输和计算设施的存放安排等进行了规定。欧美之间在 2000 年达成的数据安全港协议更是被欧盟法院推翻，并在 2017 年达成新的欧美隐私盾牌协议（以下简称“隐私盾”），隐私盾对欧美之间跨境数据传输过程中的个人信息保护提出了更高的要求。

国家立法层面，欧盟在 1995 年颁布的《欧洲议会和欧盟理事会 1995 年 10 月 24 日与个人数据处理有关的个人保护以及此类数据的自由流动指令》（以下简称“欧盟 1995 年指令”）的基础之上，于 2016 年 4 月份，结束了长达四年之久对《一般数据保护条例》（General Data Protection Regulation）的起草审议，拔高了个人信息保护法律的层级，创设新型权利和制度规则，该立法受到极为广泛地关注，也备受争议。日本也在 2017 年通过了最新修订的《个人信息保护法》。新加坡在此前尚无一部统一的个人信息保护法，直到 2013 年《个人信息保护法》生效。

纵观各时期立法进程，围绕个人信息保护这一核心主题，各国个人信息立法在不同阶段有不同的保护重点。从规范主体上，由主要规范政府机构的行为转向同时规范政府机构和商业机构；从实现方式上，主要通过规范或限制个人信息控制者的个人信息收集、处理、储存等行为，以保证个人信息权利的实现，也通过对个人权利进行限制以保证数据自由流动和公共利益。〔5〕个人信息的信息本质决定了其法律规范的重心随着时代变化和技术发展而变化和更新。大数据时代的来临，数据挖掘、分析技术的迭代更新，数据商业化模式的逐步成熟，促使了个人信息的多元化应用。从这个意义上说，法律的滞后性在个人信息保护法律领域体现得尤为突出。法律需要不断地完善以调整随着大数据技术和应用进步而变化的法律关系，从世界范围的立法进程来看，各国法律和国际公约都试图从个人信息权利创设、管理机制创新等角度入手尝试调整现有法律制度，从中也可以看到立法者平衡个人信息主体和数据控制者两者间的利益关系的意图。〔6〕

世界范围内各国越来越重视个人信息保护问题，美国、欧盟、加拿大、韩国、日本、澳大利亚、新加坡、我国台湾、香港地区等国家或地区均通过立法赋予个人对其个人信息享有权利。目前，我国虽然尚未制定一部统一的个人信息保护法，但值得提出的是，《民法总则》在民事权利一章规定自然人的个人信息受法律保护。此外，《消费者权益保护法》明确消费者享有个人信息依法得到保护的权利。但法律并没有明确个人信息主体应当享有哪些具体的权利。

保障个人信息权利是个人信息保护立法的核心诉求和原则，但当对同一权利客体，有两个以

---

〔4〕 See Supplementary Explanatory Memorandum to The Revised Recommendation of The Council Concerning Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data (2013), p.10.

〔5〕 齐爱民、李仪：《论利益平衡视野下的个人信息权制度》，载《法学评论》2011 年第 3 期。

〔6〕 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 40～60 页。

上主体同时对其拥有相应不同利益时，利益的平衡显得尤为重要，否则，偏重利益一方极有可能造成权利的滥用，形成权利优势一方的权利绿洲和权利弱势一方的权利荒漠，造成极不对等的权利格局。〔7〕更为直观的后果是，一边倒地保护个人信息，将使得依赖于此的大数据产业得不到发展，个人信息被束之高阁再无法发挥其应有的经济价值，信息社会发展将遭受停滞，个人信息主体无法享受数据产业发展带来的福祉。对我国来说，尤其是欧盟推崇的新型权利类型应当引起立法者警惕，被遗忘权、数据可携权等新型权利类型是否符合产业发展实际情况，值得深思。

在大数据时代，我国个人信息保护立法呈现较为严重的滞后性，在对数据控制者的权利保障方面的立法更是如此。数据对企业而言，是具有高价值的商业资源和核心竞争力。尽管个人信息保护成为舆论社会高度关注的焦点问题，但数据盗窃、非法获取现象仍是频发，个人信息主体和数据控制者的利益都因此遭受巨大损失，权利得不到充分保护。值得提出的是，一些立法、司法案例对作为数据控制者的企业拥有的数据享有正当利益进行了肯定，从独立的数据库权、著作权、不正当竞争、合同保护等角度对数据或数据集合进行保护。〔8〕从数据权的角度，欧盟和美国都做出了努力。欧盟和美国在1996年向世界知识产权组织（World Intellectual Property Organization，WIPO）提出过数据库保护条约的草案但未获通过。随后欧盟通过了《数据库保护指令》，创设了数据库权。美国国会也于同年度提出《数据库投资和知识产权反盗版法》，旨在创设类似于欧盟的数据库财产权，后续推出《信息集反盗版法》等多部数据库保护法案，遗憾的是均未获得通过。我国《民法总则》第127条明确规定，法律对数据、网络虚拟财产的保护有规定的，依照其规定。该法虽未对数据的权利主体及其法律地位予以明确，但对数据相关权利的认识有一定的前瞻性，提出将数据作为一种权利保护客体进行保护的可能性，也为后续立法埋下伏笔。从著作权保护的角度，如果数据通过汇编，其数据选择或编排具有独创性，形成具有独创性的数据集合或数据库，符合著作权保护的要件，应当可以获得著作权保护。我国有类似判决承认了权利人对具有独创性的数据库享有著作权。欧盟《数据库保护指令》规定具有独创性的数据库可以获得著作权保护。从商业秘密的角度，某项或某些数据，如果符合商业秘密的秘密性、价值性、实用性的构成要件，权利人应当可以主张其对相关数据享有商业秘密。我国2002年的衢州万联网络技术有限公司诉周慧民等人侵害商业秘密纠纷案，法院认为网站用户注册信息数据库是网站的核心资产，从而认定网站的经营者享有权利。从反不正当竞争的角度，北京知识产权法院亦认为作为企业对其付出劳动获得的数据应享有合法权利，近日在新浪微博诉脉脉非法获取、使用其用户数据案判决强调，数据对企业而言已经成为一种商业资本，是经营者重要的竞争优势和商业资源，微博可以就脉脉未按约定、未获授权、无正当理由使用其平台相关数据资源的行为主张合法权益。从合同基本理论的角度，只要合同没有无效或可撤销的情形，就应认可数据相关条款的法律效力。在*Ryanair Ltd v. PR Aviation BV*一案中，欧盟法院认为，不受著作权或者数据库权保护的在线数据库的所有人可以通过合同限制他人使用其数据库。我国法院也有判例认可通过合同约定数据使用方式的做法。尽管数据能通过现行法律体系获得某种程度的保护，但相关法律的缺位仍是不可否认的事实，这不仅导致个人信息得不到充分保护，也使得企业对其数据的法律地位呈现不明确的状态。

鉴于此，在尚无法律明晰数据控制者权利和个人信息权利的法律背景下，合理使用原则对平衡两种利益和指导相关制度设计意义重大，有必要通过法律明确数据控制者与个人信息权利人之

〔7〕 周汉华：《论互联网法》，载《中国法学》2015年第3期。

〔8〕 林华：《大数据的法律保护》，载《电子知识产权》2014年第8期，第81页。

间利益平衡的合理使用原则。

（三）对知情同意原则形成互补和限制

从当前的法律制度来看，知情同意原则对个人信息主体和数据控制者的保护越发捉襟见肘。

同意原则作为隐私法和个人信息法的理论基石，有着深厚的哲学、政治学、法理学渊源。从哲学的角度，同意原则是人的意志体现所在。黑格尔认为人作为单个的意志而存在，人有权把他的意志体现在任何物体中。但人们只有在做出决定后，才是现实的意志，才是特定个人的意志。〔9〕在论证政府权力的问题上，同意原则也是法理学名著聚焦的论证核心。洛克、卢梭、霍布斯等人都无一例外地论述个人同意让渡部分权利交给国家或政府，是政府权力合法性的基础。洛克在《政府论》中把同意作为政治权力具有合法性的一个核心因素，认为“一切自然人都是自由的，除他自己同意以外，无论什么事情都不能使他受制于任何世俗的权力”。〔10〕

英美法系将个人信息纳入隐私的范畴，将隐私法的理论扩张用于解决个人信息保护问题。隐私权是消极、被动的防御型权利，其权利的价值不在于主动去行使某项积极权能，而关乎个人对不愿被不特定多数人知悉的信息或内容，享有不被知悉、获取、公开等的权利。〔11〕未经个人同意，知晓、获取、公开隐私信息的行为，即构成隐私权侵权行为。反之，经过同意即不具备隐私权侵权的构成要件。对于同意的效力，有学者甚至认为“同意具有道德性魔力，只要受害人同意，盗窃就能变成赠与”。〔12〕倾向于对个人信息采取单行立法保护的大陆法系提出个人信息自决的重要性，强调个人有权决定其个人信息如何被利用、公开，个人信息自决权的内核也是同意，意即除非个人同意，任何人无权决定如何利用、公开其他人的个人信息。具体地说，收集、使用个人信息应当达到一定的透明度，透明度即是基于知情同意原则的要求，采取有效的方式方法，以明确向用户告知收集、使用其个人信息。OECD《隐私保护与个人数据跨境流动的指导方针》在其确定的基本原则中对透明度做出了框架性的要求，收集、超出之前明确的目的范围使用、披露都应当获得用户同意。美国 FTC 的《公平信息实践原则》详细地列举了应该告知或披露的事项，包括收集的主体、用途、潜在的数据接收方、收集的方式和采取的安全措施等。

同为英美法系和大陆法系个人信息权利体系构建的内核，以知情同意为基本框架的信息隐私权保护模式自 20 世纪 70 年代以来，基本上没有发生任何变化。〔13〕然而，通过同意赋予个人控制权以实现对个人信息的有效保护显得力有不逮，古老的知情同意原则面对现代信息社会的数据使用趋势，难以独立完成保护个人信息的目的。数据处理的复杂性使得满足告知并保证个人出于对其个人信息处分情况完全掌握的情况下做出同意选择，显得不切实际。而凡是个人对处分情况不完全理解情况下的同意，例如通过一纸隐私政策勾选授予的同意，并不能实现完全保障知情权前提下的同意。数据控制者往往费尽千辛万苦将数据处理的基本情况披露给个人信息主体，而个人信息主体却不愿意阅读或需要花费大量的时间成本去理解，使得双方都无从得知对方是否真正理解了对方的意图。也即是说，虽然数据控制者明确了数据处理的规则，而规则的复杂性使得个人信息主体不愿花费时间去详细阅读，导致在不完全知情的情况下做出同意，反过来，对基于此同意进行数据处理的数

〔9〕［德］黑格尔：《法哲学原理》，范扬等译，商务印书馆 2013 年版，第 52 页。

〔10〕见前注〔4〕，约翰·洛克书，第 28 页。

〔11〕张新宝：《隐私权的法律保护》，群众出版社 2004 年版，第 41 页。

〔12〕Steven L. Willborn，“Notice，Consent，and Non-consent：Employee Privacy in the Restatement”，100 Cornell L. Rev. 1423—1452(2015).

〔13〕徐丽枝：《个人信息处理中同意原则适用的困境与破解思路》，载《图书情报知识》2017 年第 1 期，第 106～113 页。

据控制者处理个人信息的定性处于不稳定状态，甚至饱受质疑。由于无法克服事实上的信息不对称，导致个人信息主体在被告知相关个人信息收集、处理情况，但却因自身原因在并不完全知情的情况下做出意思表示，使得具有坚厚的理论与历史基石的同意原则形同空中楼阁。

引入合理使用原则，基于该原则对相关法律制度进行一定解构和充实，强调个人信息使用行为的合理性，对个人信息使用行为本身做出规范，在满足法律规定的特定情形下可不经权利人同意，并按照法律规定为之使用，可一定程度上弥补同意与信息不对称的知情同意悖论，解决一揽子获取或滥用用户授权无法切实实现个人信息权利保护的问题。合理使用原则与同意原则并列，作为处理数据的正当性基础，满足大数据时代日益增长的数据使用高需求，在数据控制者与个人信息权利人之间寻求平衡，在即使不经权利人同意也不会影响其他合法权益的前提下，对个人权利进行一定的合理限制，实现促进数据使用的目的，保障数据流通、使用可控。

三、合理使用原则的制度内涵

合理使用原则，即在法律明确规定的合理的限度以内，可不经个人同意，按照法律规定对个人信息进行利用，但不应对个人信息、隐私造成侵犯，不应以影响数据安全的方式为之利用。该原则对于平衡数据控制主体利益和个人利益尤为重要，有的国家或地区甚至将促进数据合理利用作为立法目的，如我国台湾地区《个人资料保护法》明确规定将“促进个人资料之合理利用”作为与“避免人格权受侵害”并重的立法目的。〔14〕也有不少学者认为，面对数据经济发展的大局势，促进个人信息流通、使用，也应成为数据保护法律的立法目的或指导性原则之一。

（一）借鉴著作权法上的合理使用原则

合理使用原则是著作权法上的重要原则，意即出于合理的目的和用途，可以不经权利人许可使用其作品，是基于保护权利人和未经授权的合理使用人利益之目的发展演化出的保护垄断与保护公共利益的一项重要利益平衡原则。合理使用原则对平衡个人信息权利人利益和其他合理使用者利益同样有效，将该项原则借鉴到数据保护领域，具有正当性和合理性。该原则以公平正义为正当基础。美国学者威廉·F.帕提（William F. Party）将合理使用称作一项“理性主义的公平原则”，“该规则充满公平正义并具有弹性而无法定义”。〔15〕判断公平与否，一般是从社会正义的角度，以人们公认的价值观、是非观作为标准的，包括人们公认的经济利益上的“公正”“合理”。〔16〕公平正义观在数据保护法律制度中表现为一种均衡思想。正如，现代意义的著作权制度并没有拘泥于18世纪那种绝对的、放任的“个人本位”，而是在保护作者的著作权与限制作者的著作权中寻求平衡，即合理地消除作品创造者、作品传播者、作品使用者之间的冲突，力图实现在维护作者权益基础上的三者利益的均衡保护。〔17〕大数据时代的数据保护制度也不宜局限于绝对的“个人本位”，而应在保护个人的个人信息权与限制个人的权利中找到平衡，合理地消除个人、数据控制者、数据使用者之间的冲突，实现在维护个人权益基础上的利益均衡。实现这一平衡社会功能的法律调节器首选合理使用原则及其制度。

---

〔14〕 齐爱民：《拯救信息社会中的人格：个人信息保护法总论》，北京大学出版社2009年版，第34～58页。

〔15〕 William F. Party, *Fair Use Privilege in Copyright Law* (Washington, D.C. : Bureau of National Affairs, 1986), p.4 .

〔16〕 张新宝：《民事活动的基本原则》，法律出版社1986年版，第22页。

〔17〕 吴汉东：《论合理使用》，载《法学研究》1995年第4期。

从立法目的来看，各国著作权法立法目的通常都包括“促进科学和实用技术的发展”，也就是说，如果保护著作权人的权利的目的是为了促进科技发展，基于同样的目的进行的合理使用也具有正当性。在数据保护制度领域，合理使用的价值目标在于通过利益平衡的途径，促进数据流通、使用，从而促进数据科学、技术的发展和进步。数据保护法的立法目的通常包括保护个人信息和促进数据流通、使用的双重目的。类比著作权法的合理使用，为促进数据流通、使用，在保障使用安全且不对个人权利造成不利影响的前提下，满足特定情形即可不经个人同意进行合理使用，具有正当性，其正当基础来自对立法目的的解释。

从合理使用的立法模式来看，各国著作权立法模式存在一定的差异，主要有以下三种。第一种是美国法上的“fair use”模式，其最大的特点是保持完全的开放性，法官不受立法所列举的“合理使用”类型的限制。第二种是除美国之外的版权体系国家采用的“合理利用（fair dealing）”模式，该模式对合理利用行为进行了目的限定。英国《版权法》即采用这一模式。第三种是作者权体系采用的“著作权例外（exception of copyright）”模式。此表述暗示了著作权的享有是原则，而著作权的受限是例外。〔18〕第一种立法模式对合理使用不做任何限制，最大限度促进合理使用从而实现促进科技发展的立法目的，第三种立法模式则最大限度保护著作权人利益，合理使用仅在满足特定的例外情形时才适用。若将合理使用原则引入数据保护领域，需考虑借鉴哪一种立法模式。个人信息权是一项具有人身属性的私权，与所有权、著作权等所有私权一样，只有在例外的情况下才受到限制和剥夺，而又与著作权主要是一项财产性权利的权利属性不同，个人信息权主要是一项精神性权利，在合理使用的借鉴上更应重点关注该原则对这一个人精神性权利可能产生的不利影响。事实上，上述三种立法模式的“合理使用”都是采用原则和例外的模式。参照《伯尔尼公约》首先创立继而为后来的国际条约所沿袭的约束各国著作权限制的原则“三步检验法”是：第一，使用属于特殊情况；第二，使用与作品的正常使用不相抵触；第三，不得不合理地损害作者的合法利益，〔19〕个人信息合理使用原则可包含以下要素：第一，使用属于法律明确规定的特殊情况；第二，不能以影响数据安全的方式进行使用；第三，使用不得不合理地损害个人信息权利人的合法权益。笔者认为选择第三种立法模式更有利于保护个人权利，即通过法律明确列举正当合理使用事由，并对合理使用进行目的限制，以防止司法适用上做扩大解释，不利于保护个人权利。第三种立法模式对什么情况下构成合理使用具有明确的可预见性，但是法律弹性和灵活性不足，可能导致立法的僵化。从司法适用的角度，无法解决一种行为具有极强的正当性，但不符合立法规定的权利限制条件时的合理使用认定。所以在采用该种立法模式的基础之上，还应增加目的限制的概括性规定，法官可基于该目的限制的规定做出较为灵活的解释。

从合理使用的适用来看，合理使用需要通过个案加以适用，这通常体现在司法认定中。在著作权法学者的著述中，合理使用通常归入“侵权抗辩”部分，可见合理使用与司法认定有着内在的逻辑联系。〔20〕在著作权法上，判断某项使用是否能构成合理使用，法官通常会考虑使用的目的、作品的性质、使用或引用的数量 、使用对作品价值的影响等因素。〔21〕除前述考量因素，美国最高法院著名大法官及学者都认为作者的作品与其隐私之间存在密切联系，斯坦福学者斯蒂芬（Stephen）甚至认为在合理使用的判定标准上应引入隐私保护。沃伦（Warren）和布兰代斯

〔18〕 李琛：《论我国著作权法修订中“合理使用”的立法技术》，载《知识产权》2013年第1期。

〔19〕 见前注〔18〕，李琛文。

〔20〕 见前注〔18〕，李琛文。

〔21〕 Stephen B. Thau，“Copyright Privacy and Fair Use”，24 Hofstra Law Review 185（1995）.

(Brandeis)在论证隐私权的誉世名篇《隐私权》一文中提出当代鲜为提及的著作权具有保护作者隐私的功能。霍姆斯(Holmes)大法官在20世纪初,*Bleistein v. Donaldson Lithographing Co.*[22]一案中说道:"个性总是包括一些个人的唯一特质。这种唯一的特质甚至体现在个人的作品中。"鉴于此,斯坦福学者斯蒂芬进一步论述,在认定著作权的合理使用时,还应将对著作权权利人的隐私保护作为合理使用的判断因素之一。尤其是当作品强烈地体现作者的隐私时,应当严格限制合理使用原则的适用范围。当作品中大量内容体现作者隐私的时候,法官在平衡权利保护和合理使用时,需更多考虑隐私的重要性,而更少地考虑法官常用的判断构成合理使用时的经济利益要素。[23] 这也意味着,当作者的作品与其隐私毫无关联时,判断其他人对作品的使用是否构成合理使用时,应主要聚焦经济利益要素,而非隐私要素。同上述,隐私因素对判断是否构成著作权合理使用有重要影响,这主要是因为著作权同时包含了财产性权利和精神性权利,隐私因素与著作权中的精神性权利存在内在的逻辑联系,例如,包含作者隐私的作品,作者可能通过主张或不主张发表权,以决定是否公开包含其隐私的作品。在数据使用领域,因为隐私与个人信息的合理使用存在更为密切的联系,合理使用的客体本身就是个人隐私或信息,隐私或个人信息这一因素对判断某一数据控制者是否合理使用了个人信息主体的信息显得更为突出且有意义。合理使用原则在个人信息保护领域的适用应主要考虑数据使用行为对个人信息或隐私的影响。在基于合理使用原则构建的相关规则层面,虽然有不少学者认为个人信息也具有财产属性,但个人信息权仍然主要是一项精神权利,在合理使用的界定及规则设计上更应慎重、严格。如上述提及,相关的合理使用配套规则宜采用第三种例外模式,通过列举正当理由的形式对那些特定情形下可以进行合理使用的予以明确规定。在司法认定或事前合规评估层面,如果某些数据的隐私属性弱,那么在认定合理使用时,可不必警惕数据使用对隐私或个人信息保护的影响。当达到一定极值,即隐私影响为零时,可不考虑这一因素,即使不经过个人同意直接使用,也不宜认定为侵权,即符合合理使用原则的适用条件,可认定为合理使用。反之,如果某一或某些数据的使用将对个人隐私造成严重影响时,此种使用构成合理使用的概率将大大减少。

从合理使用的法律属性来看,合理使用在著作权法上一般被认为是对著作权的限制。美国学者约翰·S.劳伦斯(John S. Lawrence)等人认为:"基于使用者利益的立场出发,合理使用是对版权的一种最重要的限制,它不是对这种独占权利的一种排除,而是对侵权诉讼的一种抗辩。"[24]我国大多数学者也认为,作者的专有权利不是绝对的,而要受到种种限制。但对合理使用的法律属性存在一定争议,《版权本质:使用者权利的法律》一书便提及:"必须区别版权的利用与版权作品的利用的两者界限。""合理使用规则并不表现为是对版权作品的个人使用,而是确认后任作者对一部作品的版权进行合理的利用,即意味着他是在行使某种权利。"[25]著名知识产权学者吴汉东在《论合理使用》一文中认为合理使用是对他人著作财产权的一种利用。[26] 对应地,数据保护法上的合理使用也需要区别是对数据的利用,还是对数据权的利用。笔者认为,数据保护领域的合理使用也应当是对他人个人信息权中财产权部分的利用,表现为使用人对他人的数据所享有的不经

---

〔22〕 See *Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239 (1903).

〔23〕 [英]约翰·洛克:《政府论(下篇)》,叶启芳等译,华夏出版社2013年版。

〔24〕 John S. Lawrence, *Fair Use and Free Inquiry: Copyright Law and the New Media* (Ablex Publishing Corporation, 1989).

〔25〕 L. Ray Patterson, *The Nature of Copyright: A Law of User's Rights* (University of Georgia Press, 1991).

〔26〕 见前注〔17〕,吴汉东文。

同意，而加以使用的某种利益。合理使用应当视为一种利益，即非个人信息权人依法享有的某种利益。这种利益应当得到法律确认，但前提是不得损害权利人的其他合法权益。从立法目的的角度，数据保护法以权力本位为基础，以保护个人权益为核心，因此，立法语言可将非个人信息权人享有的合理使用利益表述为“个人信息权的限制或例外”。

（二）合理使用原则的制度体现

事实上，个人信息的合理使用原则在一些国家的具体法律制度中已有体现。一些国家的个人信息保护法律对个人的同意与控制权进行了一定程度的减损，以实现对个人信息流通、使用的保障。〔27〕究其实质，其实是以合理使用原则为出发点，以利益平衡的目的，对个人信息保护相关制度、规则进行修正。

1. 合理使用是进行数据处理的法律基础

一般而言，各国法律将同意原则作为数据处理的一般合法基础，也规定了可不经个人信息主体同意的例外事由，这些例外事由基本归纳为可不经个人信息主体同意的合理使用。以欧盟为例，欧盟在《一般数据保护条例》第 6 条中规定了除同意以外，可被认定为合法处理的其他五种情形，满足任意一项即可被认定为合法处理。其一，个人数据的加工是作为合同一方的数据主体履行合同所必需的或是为了满足数据主体订立合同前或订立合同时的要求；其二，数据控制者履行法律义务必须进行个人数据加工；其三，为了保障数据主体的重大利益而进行的个人数据加工；其四，在不侵犯数据主体（尤其是未成年人）更重要的基本权利及自由的前提下，控制者的合法利益需要通过保护个人数据而实现的，且数据控制者追求其合法权益是必要的，则所述加工行为可以被认定为合法。〔28〕

我国已经发布并即将生效的国家标准《信息安全技术 个人信息安全规范》也明确了收集个人信息无须征得个人信息主体同意的例外情形，包括用于维护所提供的产品和服务的安全和合规所必需的；与国家安全、公共利益有关的；犯罪侦查、起诉、审判和判决执行等有关；出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；已合法公开披露的信息；学术研究机构基于公共利益开展统计或学术研究所必要等情形。

可见，欧盟和我国的法律、国家标准的相关条文都明确了可不经个人同意的例外情形，从核心思想上，符合合理使用原则的基本要求，从规范模式上，符合本文第二部分阐述的合理使用原则的第三种立法模式，是对合理使用原则的制度体现。

2. 构成商业秘密的合理使用可免于披露

同意原则并不意味着披露尽可能多的信息。虽然，各国法律都倾向于向个人信息主体披露更多的信息，欧盟和英国法律要求数据控制者不仅应披露数据收集、使用等情况，还应当披露收集、使用的逻辑和方法。如欧盟 1995 年《个人数据保护指令》在前言（41）中写道，个人数据权利包括获取数据的权利和获取自动数据处理（至少是自动处理产生与数据主体有关的数据的决定）的逻辑的权利。英国的《数据保护法》（1998）第 7 条第 1 款（d）规定，为评估数据主体的工作表现、信用、责任或行为等目的进行的个人数据自动化处理，构成或可能构成显著影响个人自身的基础，那么该个人有权被告知数据控制者做出决定的逻辑。但同时也做了例外规定，即不能对数据控制者的商业秘密造成影响，保障同意原则的隐含前提是要在个人信息权利保护和数据控制者商业秘密权

〔27〕 刁胜先：《论个人信息权的权利结构——以“控制权”为束点和视角》，载《北京理工大学学报（社会科学版）》2011 年第 3 期，第 92～96 页。

〔28〕 参见《欧盟一般数据保护条例》。

利保护之间做出平衡，构成商业秘密的合理使用及使用逻辑可免于向个人信息主体进行披露。

（三）合理使用原则的关联规则

1. 个人信息风险评估

在进行数据处理、使用前，应进行个人信息风险评估。个人信息风险评估的意义主要在于在使用数据前对使用行为的合法性、合理性进行判断，这也是事后认定是否构成合理使用的重要依据。有学者认为，在具体实践中，应弱化对用户同意的过度依赖，规定“合理使用”的场景，且对信息处理行为进行影响评估，在信息处理行为构成“合理”或带来的风险在“可预期”的范围之内时，免予取得用户同意，减轻其为机构及用户自身带来的负担。〔29〕这一观点具有一定的可操作性和现实意义，可对现有的规则体系起到有效的补充作用。现有的规则体系以同意原则作为核心的个人信息保护和合法使用基础，但如上所述，基于这一原则并不能实现对数据主体权利的有效保护。客观上最有能力判断某项使用行为是否对个人信息主体权利造成影响或侵犯的是数据控制者。在尚未获得同意或难以获得同意，而又需要对相应的个人信息进行处理和使用时，对个人信息利用的合法性、正当性、必要性进行隐私/个人信息风险评估，如果相关的个人信息处理行为对个人权利无影响或影响极小，且符合法律规定的满足合理使用的条件时，可进行相应的信息处理。合法性、正当性、必要性等因素即是合理使用原则的延展，即是说，当对某些个人信息的使用经过充分合法、正当、必要等条件的预判和使用结果的影响分析，发现影响在可接受的范围内时，即构成合理使用，此种使用可不经过权利主体同意。

现今越来越多的学者及机构倾向认为，隐私及个人信息保护的边界并非固定的、僵化的，而是主观的、动态的，并受多重因素影响，何以构成个人信息的合理使用，在不同的场合均不尽相同。〔30〕这就需要对个人信息处理进行个案的风险评估。赋予数据控制者进行风险评估、结果判断、做出使用决定的权利是有很大风险的，正义的规则要绝对避免既做裁判员，又做运动员的情况，将判断是否使用个人信息的权力交给会使用该信息的数据控制者，无疑触犯了数据控制者既做裁判员，又做运动员的禁忌。避免权利滥用的有效方法莫过于对权利的行使增加条条框框，建立规范性准则。只有当数据控制者按照规范性的个人信息风险评估程序进行评估时，得出的评估结果才可能是公正、不失偏颇的。从这个意义上说，建立个人信息风险评估规范性、监督性程序及个人控制的权利约束机制显得尤为重要。

数据控制者最有能力判断数据使用对个人信息主体造成的影响，因此，在使用个人信息前，进行个人信息风险评估，能有效地起到保护个人信息的作用。这是个人信息风险评估能为个人信息保护水平较高国家或国际组织普遍倡导的一项个人信息管理解决方案的原因。例如，OECD《隐私保护与个人数据跨境流动的指导方针》规定数据控制者应当准备一个隐私管理计划，基于隐私风险评估提供合适的安全措施。〔31〕我国个人信息安全和保护方面的国家标准也积极推动建立个人信息安全风险评估体系，比如《信息安全技术个人信息安全规范（草案）》对数据控制者开展个人信息评估提供了一些实操性较强的指引，要求定期进行评估，并在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生个人信息安全事件时，重新进行个人信息安全

〔29〕 范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016年第5期，第92～115页。

〔30〕 See Steven L. Willborn, supra note〔12〕.

〔31〕 A data controller should: a) Have in place a privacy management programme that: iii. provides for appropriate safeguards based on privacy risk assessment. See Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, 0829/14/EN WP216 (Adopted on 10 April 2014).

风险评估。

规范有序地开展个人信息风险评估固然重要，但对权利的监督也并不可少。因此，需要建立相应的监督和权利约束机制。各国的相关规定不仅需要对个人信息风险评估的流程、环节进行规定，也应制定评估有效性的监督机制，比如要求评估结果报告向社会公开，特定的个人信息处理评估需报政府部门知悉、备案，甚至审批。

2. 经设计的隐私

判断数据控制者某种使用行为是否尽到了合理使用的注意义务，需考量数据控制者在收集、使用数据的过程中是否将个人信息保护作为数据合规流程和管理机制的重要一环。从公司产品和流程设计的前端产品开发到后台数据管理，都将个人信息保护作为重要原则融入收集或处理个人数据的产品、服务的设计和运作过程中，即经设计的隐私（Privacy By Design，以下简称“PbD”）。

PbD 理念为欧盟和美国法律和执法机构认可。目前，PbD 已成为欧盟数据保护的基本原则，将隐私放在了优先位置并加以重点保护。2014 年 10 月澳大利亚隐私和数据保护委员会（CPDP）正式决定采用 PbD 作为加强其公共部门信息隐私管理的核心政策。美国联邦贸易委员会（以下简称 FTC）的报告（staff report）建议公司将实质性的隐私保护融入其实践当中，建议公司进行全面的数据管理。FTC 对 PbD 的态度也体现在相关的执法案件中。例如 FTC 在结束对谷歌街景案调查的信件中强调其采取一些实践，包括任命隐私工程管理总监，对核心员工进行核心隐私培训，在新产品设计过程中引入隐私审查；采取了合理的程序，如仅收集提供服务所必需的信息，目的完成即删除数据，从而认为谷歌街景保证了收集和存储数据的隐私和安全。各大公司也将 PbD 作为重要的个人信息管理机制。微软的安全开发生命周期（Security Development Lifecycle，以下简称“SDL”）是目前最著名的例子。SDL 的目的在于将隐私和安全原则融入软件开发生命周期，每个开发周期（产品需求、设计、完善、验证和发布）都包括了隐私指南，从强制性的到推荐性的，从程序性的到技术性的。每个项目都有隐私影响等级，这些等级决定合规的具体设计要求。其软件和服务开发隐私指南对 SDL 做出了进一步补充，这些指南在美国《公平信息保护实践》和相关的美国隐私法律的基础上界定了基本概念和定义，分析了在具体情形下产生的不同类型的隐私控制和特殊因素考量。对九款具体的软件产品和网站开发情景列举了详细的指南。对每种场景，指南定义了告知和同意、安全和数据完整性、消费者获取、使用 cookie 及其他控制相关的要求性和推荐性实践。

数据合规流程应涵盖前端产品开发到后台数据管理，在公司产品和流程设计中将个人信息保护的重要原则融入收集或处理个人数据的产品、服务的设计和运作过程中。数据控制者可借鉴优秀的实践，将 PbD 的理念融入前端软件开发活动和后端数据管理实践中。前者是针对面向消费者端产品、服务的设计过程，即与消费者通过下载软件、使用网站服务、分享个人数据或创造用户内容等交互。后者在于数据管理程序和实践中确保信息系统内部使用或分享给关联方、合作伙伴和供应商等行为遵守隐私法、隐私政策和消费者设置的隐私偏好。在软件开发周期致力于确保产品和服务设计过程中，考虑消费者隐私期待，赋予用户控制其个人数据的权力。同时，最小化隐私风险，如秘密收集数据、未经授权的使用、转移、披露和安全违规。在数据生命周期管理中，关注公司是否符合个人信息保护要求地研发和运营信息系统，并在公司雇员获取、使用、披露和删除个人数据时考虑到个人信息保护因素。

3. 安全管理措施

匿名化、去标识化技术既为个人信息利用开辟道路，又为个人信息保护保驾护航，是确保数据合理使用的重要安全管理措施。匿名化是指一种移除识别性信息，可达到使剩下的信息无法识别

到特定个人的信息处理技术。根据欧盟第二十九数据保护工作组官方意见，匿名化技术主要包括两种，随机化（Randomization）和泛化（Generalization）。随机化是为移除数据与个人之间的强联系而改变数据真实性的技术集合。泛化是匿名化处理的另一种主要方式，其通过改变数据量级的规模或次序来泛化或稀释数据主体的属性。〔32〕在实践中，企业往往还会采取其他额外的技术来确保无法从这些数据之中识别到个人，这些技术主要包括噪声添加（Noise Addition）、排列（Permutation）、差分隐私（Differential Privacy）、加权（Aggregation）、K-匿名化（K-anonymity）、L-多样性（L-diversity）、T-密闭（T-closeness）等。〔33〕去标识化是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。去标识化建立在个体基础之上，保留了个体颗粒度，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。由于去标识化后的信息仍具有识别个人身份的可能性，因此去标识化后的信息仍然是个人信息。

匿名化技术对个人信息的保护作用在欧盟、美国以及我国都得到法律认可，匿名化后的数据使用可不受相关个人信息保护规则的限制。欧盟相关立法规定，如果对个人信息进行匿名化处理，使得通过该数据已无法识别出个人身份，对这种数据的处理就不受到个人信息保护规则的约束。〔34〕换言之，匿名化后的数据处理不必再考虑是否构成个人信息的合理使用的问题。我国《网络安全法》已借鉴欧盟将匿名化明确载入立法，明确了通过技术实现个人信息保护和使用利益均衡的态度，值得肯定。但应该进一步指出的是，在明确具体的匿名化规则时，我们需要推动匿名化国家标准的形成，使得匿名化规则的制定符合产业实际和技术现状，不过于严格地要求达到过高的匿名化程度，导致匿名化这一平衡商业利益和个人利益的利器丧失原本的价值和意义。我们也应当认识到，通过匿名化等隐私增强技术确实能从一定程度上保护个人信息，但越来越多的研究表明技术对个人信息的保护作用是有限的。如果缺乏社会规则和法律框架，仅仅技术本身无法保护隐私。因此，一方面，为保证匿名化处理后的数据仍然有较高的价值，应当认识到对匿名化标准的认定不应过于绝对，而应当是随机、动态变化的。既然没有绝对的匿名化，个人信息风险评估和PbD理念在数据应用实践中的运用就显得尤为重要，三者相互配套作用始能充分保护个人信息主体权利。另一方面，仅仅是匿名化技术，难以独立担负保护个人信息的责任，从国家规范层面，匿名化技术需与法律保护框架相结合，以实现个人信息的配套约束。从企业层面，匿名化技术需与企业内部数据管理规则相结合，从多维度保护个人信息，实现企业内部数据安全。

可见，一套明确的匿名化、去标识化的安全管理规则有助于将个人信息安全地运用于商业化，实现个人信息保护和商业运作双赢。〔35〕鉴于经匿名化处理后的信息无法识别主体身份，因此对于满足匿名化要求的信息，可不经个人信息主体同意直接使用，无须考虑是否符合合理使用原则。而去标识化后的个人信息，虽然不能达到匿名化后完全无法识别个人信息主体的程度，但是比去标识化前的识别个人信息主体的难度大很多，因此，使用去标识化后的个人信息更安全，判断构成合理使用所需履行的相关安全义务更低。

---

〔32〕 See 0829/14/EN WP216, supra note〔31〕.

〔33〕 Walden I.,"Anonymising Personal Data",10(2) International Journal of Law & Information Technology 224-237(2002).

〔34〕 GDPR详述(26)中指出，假名化的数据能够与其他数据结合来识别个人，其可被视为与一个可识别的自然人相关的信息。数据保护原则不适用于与该自然人无关或无法被识别的匿名化的数据，该条例因此不适用于对匿名化数据的处理行为。

〔35〕 张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015年第3期，第38～59页。

4. 个人参与和控制

个人参与和控制是实现个人信息保护的途径，是知情同意原则的延伸，能有效地对数据处理、使用行为进行约束，通过个人参与和控制检视数据使用的合法性、合理性。

国际条约和各国立法也将个人参与和控制作为个人信息保护的基本原则。OECD《隐私保护与个人数据跨境流动的指导方针》将个人参与原则作为八大基本原则之一，明确个人应当有权从数据控制者获得与其相关的数据，或要求数据控制者确认其是否有该个人的数据，有权就与其数据相关的问题与数据控制者联系，如果请求被拒绝，数据控制者应当提供理由。个人有权提出异议，如果异议成立，数据控制者应当对数据进行删除、修改、完善等相关处理。〔36〕用户参与不仅意味着用户可以查询数据，并且应当有权验证其准确性。美国 FTC 的《公平信息实践原则》描述了选择/同意、获取/参与原则，网络环境下的选择和同意意味着为用户提供控制其数据的选择。

个人参与和控制也是个人信息主体约束数据控制者使用数据的有效权利约束机制。赋予数据控制者权利，就应赋予个人信息主体参与和控制其个人信息处理的权利。权利与权利之间相互制约，始能达到个人信息保护与利用之平衡状态。此外，赋予个人参与和控制的权利也能实现对上述个人信息风险评估的有效约束。基于“个人信息风险评估可作为免于同意的条件”，评估结果若为个人信息处理对信息主体的影响在可控制的范围内，即可不经个人信息主体同意为相应的使用，这样的使用构成合理使用。前述也提及赋予数据控制者较大权利的个人信息风险评估流程需要通过规范性、监督性的程序加以约束。但是即使受到程序性的约束，还是不能实现个人权利的有效保护，因为该规则跳过了个人同意环节。如果说“个人信息风险评估可作为免于同意的条件”这样的机制的前提在尚未获得同意或难以获得同意，而又需要对相应的个人信息进行处理或使用，那么事后权利补授权环节或用户参与控制环节则必不可少。即使在影响较小的方案中实施个人信息处理，也应当保留主体参与相关处理流程的规则和余地，实现权利制衡。

四、结　　语

在大数据语境下，个人信息立法不仅以保护个人信息主体权利为单一目的，同时应承载促进数据使用、流动的立法目的，合理使用原则作为平衡两种利益关系的调节器，将起到重要作用。

我国在个人信息立法进程中，应廓清以同意原则为核心构筑起来的个人信息保护法律对双重立法目的实现之有效性，引入合理使用原则，允许基于保护数据使用方利益（如商业秘密）的角度对同意原则进行一定程度的减损。借鉴欧盟等国立法确立以合理使用原则和制度为数据使用的合法基础，吸纳场景理论的合理内核，侧重从个人信息风险评估的角度保护个人信息，当评估结果为对个人信息造成影响极小时，可不经个人同意为相应处理。当个人信息经匿名化处理后，不再是个人信息，亦可不经同意进行处理，且不受个人信息法律约束。此外，合理使用的认定上需通过是否进行个人信息风险评估、是否采取去标识化等安全措施、是否保障了个人参与和控制的权利等事项加以丰富。概括而言，合理使用个人信息的数据控制者应有良好的风险控制制度，在后台运营和前端应用等场景设计、开发时充分考虑个人信息保护，采取适当的技术手段保证使用过程中的信息安全，赋予个人信息主体一定程度的自主控制权利。

（责任编辑：徐彦冰）

〔36〕 参见 OECD《隐私保护与个人数据跨境流动的指导方针》第 7 段、第 10 段。