大数据时代个人信息使用的合法利益豁免

谢 琳

摘 要: 在大数据时代,知情同意机制已无法有效应对大数据生态系统的多元性和复杂性,无需取得数据主体同意的合法利益豁免可成为大数据信息使用的另一重要合法依据,为大数据产业发展提供灵活空间。我国在个人信息保护的相关立法中可引入合法利益豁免机制。引入该机制时,对合法利益应采用广泛的定义,只要是未违法的使用利益均属合法利益。但数据控制者必须进行一个平衡测试,证明数据使用的合法利益高于数据主体的个人利益,方可适用合法利益豁免。平衡测试可采用个案分析方式,并遵循必要性原则、目的限定原则和比例原则。此外,数据控制者还应对平衡测试进行全程记录,以接受数据主体、政府数据保护部门和法院的监督。

关键词: 大数据时代; 个人信息保护; 合法依据; 知情同意机制; 合法利益豁免

随着大数据时代的到来,要求取得数据主体知情同意的信息使用机制已无法适应大数据二次利用产业模式的多元性和复杂性。合法利益豁免机制因无需取得数据主体同意而有可能成为大数据产业使用个人信息的重要合法依据。该机制有利于平衡个人信息保护和信息自由流动,因而已为世界主流立法所采用。近期欧盟还专门出台相关的指导意见,提高合法利益豁免机制的可执行性。遗憾的是,我国相关立法目前尚未引入合法利益豁免机制,这导致我国个人信息保护制度过于僵化,甚至有可能比一向主张严保护的欧盟相关立法更为严格。本文试图对合法利益豁免进行分析,为我国未来个人信息保护制度的构建提供借鉴。

一、合法利益豁免的适用意义

合法利益豁免指的是,当数据处理为实现数据控制者或第三方的合法利益所必需时,数据控制者可通过一个平衡测试证明其使用利益高于数据主体利益,使其无需取得数据主体同意也可对数据主体个人信息进行处理。合法利益豁免是处理个人信息的合法依据(legal ground)之一。

处理个人信息须有合法依据。以影响广泛的欧盟为例,欧盟相关立法规定了处理个人信息的六个合法依据: (1)取得数据主体的同意; (2)履行与数据主体的合同; (3)履行数据控制者应承担的法定义务; (4)保护数据主体或另一个自然人的重要利益; (5)执行公共利益所需或官方机构要求的任务; (6)实现数据控制者或第三方的合法利益。[①]除征得数据主体同意这一合法依据以外,第2-5个未经同意的合法处理依据所列举的情形是特定的,难以进一步扩大解释。但第六个合法依据"合法利益"则范围

作者简介: 谢琳,法学博士,中山大学法学院讲师、硕士生导师。

* 本文系国家社科基金青年项目"大数据时代个人信息保护的'场景风险监管'模式研究"(17CFX069)的阶段性成果。

① 欧盟《通用数据保护条例》(REGULATION (EU) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data,简称General Data Protection Regulation)第6(1)(f)条。早在1995年,欧盟的《个人数据保护指令》就已对合法利益豁免做出规定。

广泛,并引入了动态的平衡测试,通过个案衡量方式为数据保护留下了灵活的操作空间,是个人信息保护与促进信息流动之间的重要平衡器[1](P. 244 - 261)。在大数据时代,由于知情同意机制的局限性,合法利益豁免具有更广泛的适用意义。

(一)知情同意机制的局限性

传统个人信息保护制度以知情同意机制为核心。然而在大数据时代,大量的隐私协议导致数据主体无暇阅读,大数据技术的复杂性也导致数据主体无法真正理解其隐私风险而可能做出非理性选择[2]。数据控制者取得的用户同意往往不是真正的同意,知情同意机制沦为一纸空文。①

为此,欧盟 2018 年 5 月生效的《通用数据保护条例》(General Data Protection Regulation,GDPR)对知情同意机制进行了强化和修复,如要求在隐私条款中必须明确具体收集目的;用户如同意条款则必须明确做出主动性行为(如主动勾选而非默认勾选)等。我国相关部门监管实践②以及 2017 年 12 月颁布的首个关于个人信息保护的国家推荐性标准《个人信息安全规范》也同样试图通过提高获得同意的标准、细化征得同意的操作规定来增强点击同意的有效性。③ 然而,这些措施虽然在一定程度上缓解了知情同意机制的困境,但却不能从根本上解决问题。隐私协议的海量化和数据处理的复杂性仍是同意机制失效的症结所在。并且,由于多数情况下用户与数据控制者并非处于平等协商的地位,因此即使用户点击同意,也很难被认定为是真正意义上的自由选择[1](P. 257)。

再者,提高获取同意标准与大数据产业的发展趋势并不相符。大数据产业需要海量的数据分析,注重数据价值的二次利用。有专家便指出,强化知情同意机制要求收集目的明确具体,导致数据控制者不再能够通过列举广泛的收集目的方式来获取数据主体同意,大数据产业将无法获取足够的分析材料[3](P. 326)。且大数据二次利用模式的多元性和流转性也使数据控制者难以追踪回原数据主体并寻求他们的同意[4](P. 90)。在复杂的数据收集处理情形下,同意并非是最为合适的处理数据的合法依据。个人信息保护制度是为了在数据保护与使用之间取得平衡,而仅仅依靠同意机制是无法实现平衡各方利益的最终目的[1](P. 246 - 247)。

(二)合法利益豁免的必要性

合法利益豁免可为传统同意机制与大数据产业之间的冲突提供一个平衡路径。在大数据时代,由于传统知情同意机制限制了大数据产业的发展,从收集阶段转向使用阶段的风险监管路径成为颇受提倡的个人信息保护新路径[5]。合法利益豁免无需取得用户同意,并通过使用阶段中的平衡测试进行风险监控,与风险路径的新保护理念相契合。就如同知识产权一般,个人信息保护权并非是一个绝对权,而是一个受限制的权利[6]。并非所有的数据使用都必须取得用户同意,当使用利益高于用户个人利益时,可以让渡用户利益。④

据此,英国信息专员公署(Information Commissioner's Office,以下简称 ICO)在 2017 年 9 月《大数据、人工智能、机器学习和数据保护》报告中便指出,鉴于大数据时代背景下取得数据主体同意存在某些困难,合法利益豁免可为数据处理提供另一种可供选择的路径,从而在商业和社会利益与个人权利之

① 欧盟 29 条工作组在其关于同意机制的意见中指出,同意机制已被滥用,应对其进行限缩解释。Article 29 Data Protection Working Party, *Opinion* 15/2011 *on the definition of consent*, WP 187 (2011).

② 2017 年下半年中央网信办等四部门联合对微信、淘宝等十款网络产品和服务的隐私条款进行评审,重点评估是否明确告知用户收集个人信息及收集使用方式等。2018 年 1 月支付宝年度账单事件中,支付宝与芝麻信用软件因用户信息流转通知不够清晰明确且未经用户选择同意的问题被网信办约谈整改。

③ 《个人信息安全规范》在《网络安全法》的基础上,规定了选择同意的示例,要求数据主体做出主动性选择的动作,并为破除一揽子授权的困境,建议区分核心功能和附加功能,要求使用附加功能需要二次授权。

④ 依据法经济学原理,当公共利益等所需时,需经权利主体同意的财产规则可转化为通过赔偿即可使用的责任规则。参见丁利、韩光明 "现状还是底线? ——征收拆迁中的补偿与规则适用",载《政法论坛》2012 年第 3 期。

间取得平衡[4](P.90)。有立法报告甚至主张,合法利益豁免可被视为大数据信息处理的默认适用路径。①

为提高合法利益豁免的可执行性,欧盟29条工作组2014年专门发布了关于合法利益的指导性意见(以下简称"29条工作组意见"),试图为合法利益豁免提供一个清晰可行的执行框架,以此减轻知情同意机制的实施压力。该意见明确了合法利益豁免的法律地位,指出合法利益豁免并非是同意机制的补充,而是并列选择,企业可以在同意和合法利益两个合法依据之中任选其一[7](P.3)。合法利益豁免突破了同意机制的固有限制,强调信息使用价值的实现。我国应引入该合法利益豁免,为大数据产业提供发展空间。

二、合法利益的界定

引入合法利益豁免机制应先对合法利益进行界定。欧盟将合法利益规定为"数据控制者或第三方的合法利益"。对于合法利益的范围,欧盟相关实践曾产生争议,有严格解释说和宽泛解释说两种路径。

(一)严格解释说:法定权利

严格解释说认为,合法利益仅限于法律上予以规定和认可的权利,即法定权利。当立法所赋予的数据控制者或第三方的法定权利与数据主体隐私权及个人信息保护权产生冲突时,有必要对其进行平衡。欧盟基本权利宪章也明确规定,对于数据主体的基本权利的限制须以另一个法律规定的权利作为依据[8](P.1-26)。

29条工作组意见将有可能与数据主体的隐私权和个人信息保护权产生冲突的权利归纳为:表达和信息自由、艺术和科学自由、访问资料权、人身自由与安全权、思想信仰和宗教自由、从商自由、财产权、获得有效救济和公正审判权以及无罪推定和抗辩权等[7](P.34-35)。

法定权利之间的冲突平衡已形成一系列的判例实践。例如2012年西班牙法院判决,言论自由是合法利益,公司有权公布涉嫌违法活动的教授在该公司网站上所注册的个人信息,教授个人信息的权利并没有高于公司的言论自由权利。② 欧洲法院2010年判决,基于透明性要求的公众知情权高于隐私权,③ 2014年判决为保护财产、健康和家庭生活可在房子周围安装监控摄像头。④ 在2014年29条工作组发布合法利益意见后,2017年欧洲法院在其代表性案件"拉脱维亚路交通事故案"中裁定涉案私人财产权高于个人信息权。该案中,一个计程车乘客打开车门造成巴士的损害,巴士公司向警方要求提供该乘客的姓名、ID号码和地址,但警方拒绝提供。欧洲法院认为保护私人财产是合法利益,并对该案进行利益平衡,指出财产损害赔偿的民事诉权应高于数据主体的个人信息权,警方应提供乘客个人信息。⑤

法定权利平衡已形成较为成熟的判例法,能够提供清晰的指引。主张法定权利说的学者担心,如若将合法利益扩大至其他非法定利益的情形将引起法律适用上的不确定性,造成立法漏洞[8]。

(二)宽泛解释说:未违反法律规定的利益

宽泛解释说则认为,合法利益不仅限于法定权利,还应包括法律上未规定的不违法的利益。大至公共利益,小至企业私人利益,只要不违反法律规定,均可属于合法利益。

1. 公共利益或广泛群体的利益

公共利益或广泛群体(wider community)的利益包括多个方面,例如进行历史、科学、统计、市场等研究,防范欺诈、服务滥用或洗钱,进行政治活动或慈善活动筹款,维护信息技术和网络安全,披露有关犯

① The Federation of European Direct and Interactive Marketing, *Data Industry Platform, Proposal for a balanced approach on consent*, Position Paper (20 Dec. 2011); Industry coalition for data protection, *Paper on Proposals for a new EU legal framework on data protection*, available at: www.bsa.org/~/media/Files/Policy/Security/DataBreach/eudataprotect.ashx, accessed Oct. 31, 2018.

② Audiencia Nacional, 11 April 2012 (JUR/2012/148319), quoted from Paolo Balboni, et al., *Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection*, *International Data Privacy Law*, vol. 3, no. 4 (2013), p. 251.

③ Volker und Markus Schecke and Eifert (C-92/09 and C-93/09, EU: C: 2010: 662, para. 77).

④ RyneŠ (C-212/13, EU: C: 2014: 2428, para. 34).

⑤ Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas paŠvaldības SIA Rīgas satiksme (Case C-13/16, ECLI: EU: C: 2017: 336).

罪活动或对官方机构造成安全威胁的信息等。举例而言,慈善组织可为了医学研究目的而使用病人信息,非营利组织可为了提高对政府腐败的认识而处理相关数据[7](P.35)。

同时私人商业活动也可能涉及公共利益,例如金融机构打击金融诈骗,服务提供商防止数据主体滥用服务(如版权盗版或逃避付款等)[7](P.35)。认可公共利益或广泛群体的利益有利于发掘大数据分析中的有价值的用途。当大数据分析用于以上用途时,则可适用合法利益豁免。

2. 私人利益

合法利益并不限于公共利益,数据控制者的私人利益也可包括在内,例如公司可以基于安全或管理的目的对员工进行监控,为评估员工表现而记录员工工作情况,为制作公司通讯录而使用员工的联络方式信息,也可直接利用客户数据分析预测有可能流失的客户量的总百分比;律所可以为提供客户账单并发放律师奖金而统计律师的工作小时等。

商业信用信息共享便曾被认定为私人合法利益豁免。如借贷公司向第三方信用评估机构提交客户的个人金融信息,以便评估借贷风险,意大利信息保护官方机构认为可属合法利益豁免。① 英国信息专员公署也认为,借贷方拥有了解情况后做出借贷决定的合法利益。② 该观点也获欧洲法院的间接认可。③ 再如谷歌分析用户信息进行服务维护升级和产品改进等,29 条工作组虽然认为谷歌未采取所有必要的保障措施,但仍认为服务维护升级等属于合法利益。④ 同样,德国相关个人信息保护部门主张,在侵犯公司利益的行为性质较为严重时,公司可适用合法利益豁免而设立检举揭发制度。⑤

直接营销也属私人合法利益。直接营销向数据主体发送商业广告,是常见的大数据商业利用模式。随着大数据技术的引入,数据控制者可以在了解顾客偏好的基础上,进行个性化推荐,为顾客提供更契合需求的产品和服务。欧盟《通用数据保护条例》绪言 37 条便明确指出直接营销也可视为合法利益。

(三)路径选择

相较于严格解释说,宽泛解释说更能发挥合法利益平衡机制的作用。由于合法利益豁免为目前惟一现行有效的灵活性平衡机制,若将其限定于法定权利将导致其适用范围过于局限,无法充分平衡数据保护与使用之间的冲突。

欧洲法院就曾表示不应对合法利益范围进行不合理的限制。在 2011 年 ASNEF 案中,欧洲法院判决,西班牙法律对合法利益豁免进行限制是违反欧盟指令的。⑥ 在 2016 年 Breyer 案中,欧洲法院认为,维护网页服务的顺利运行虽非法律规定的权利,但可属合法利益。⑦

为解决宽泛解释所带来的模糊性问题,欧盟 2012 年的立法提案曾采用较为僵化的界定路径,将合法利益豁免修改为列举式的情形,并附上了一个描述性的详细列表,全面列举了合法利益适用的具体情形。⑧ 该提案遭到产业界强烈反对,认为列举式模式将带来新技术和商业模式的悲剧。⑨ 欧盟数据保护

---

① Garante per la Protezione dei Dati Personali (Italian Data Protection Authority), *Balancing of interests: data collection by CRAs without consent* (Rome, 16 Nov. 2004).

② Information Commissioner Office, *Credit agreements – Data sharing* (6 Nov. 2006).

③ ASNEF and FECEMD v. Administración del Estado (Joined cases C – 468 & 469/10, ECLI: EU: C: 2010: 638).

④ Article 29 Working Party, *Letter from the Article 29 Working Party to Google in Relation to Its New Privacy Policy* (Brussels, 16 Oct. 2012).

⑤ Report of the Du¨sseldorfer Kreis, *Whistleblowing – Hotlines: Internal Warning Systems and Employee Data Protection*, p. 3, quoted from Paolo Balboni, et al., *Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection*, *International Data Privacy Law*, vol. 3, no. 4 (2013), p. 252.

⑥ ASNEF and FECEMD v. Administración del Estado (Joined cases C – 468 & 469/10, ECLI: EU: C: 2010: 638).

⑦ Breyer (Case C582/14, ECLI: EU: C: 2016: 779).

⑧ European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Rapporteur Albrecht*, *Draft Report on the proposal for a regulation of the European Parliament and the Council on the protection of individual with regard to processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 0011 – C7 – 0025/2012 – 2012/011 (COD), (Strasbourg, 17 Dec. 2012).

⑨ International Chambers of Commerce, *ICC Position on Legitimate Interests*, ETD/STM, 28 Oct. 2015, available at: http://www.iccgermany.de/fileadmin/user_upload/Content/Digitale_Wirtschaft/373 – 537legitimateint11 – 2015.pdf, accessed Oct. 25, 2018.

监督机构指出,合法利益豁免的意义在于提供一个灵活的平衡机制,如局限于特定的列举情形,将丧失了其本身的意义。①

欧盟29条工作组2014年意见最终未采纳该提案,仍保留对合法利益的宽泛解释,并针对宽泛解释说所带来的法律适用模糊性问题,专门出台相关的平衡测试操作指引。合法利益的宽泛界定可为大数据发展提供较为宽松的空间,符合大数据二次利用的产业趋势。

三、平衡测试的构建

欧盟没有在源头上对合法利益加以限制,而是通过平衡测试来限制合法利益豁免的适用。数据控制者必须进行一个平衡测试,证明其使用利益高于数据主体利益,方可获得合法利益豁免。平衡测试的可行性是落实合法利益豁免机制的关键所在。但在以往实践中,平衡测试的个案衡量方式因缺乏清晰的指引而未能得到有效适用[1](P.253)。29条工作组2014年专门出台的相关意见详细规定了如何进行平衡测试,并列举了一系列示例加以指引,值得借鉴。

(一)平衡测试的内容

29条工作组意见将平衡测试解构为:1.数据控制者合法利益的评估;2.对数据主体的影响;3.一般义务上的平衡;4.数据控制者为防止对数据主体造成过度影响而采取的额外保障措施。②

1.评估数据控制者合法利益。合法利益应是真实且现实存在的,而不是假设的;合法利益的陈述应足够清晰具体。合法利益的客观性要求是为了后续平衡测试能够对其进行准确评估[1](P.254)。在客观性前提之下,评估合法利益的性质和重要性。若合法利益重要性较高,如为公共利益所需等,则通过平衡测试的可能性较高;若合法利益重要性较低,如企业私人利益,则须对数据主体的影响很低时才有可能通过测试。

2.评估对数据主体的影响。"影响"是比"损害"更为广泛的概念。影响还包括情感上的影响,例如厌烦、害怕和沮丧等负面情绪。因为证明数据主体受到具体损害并获赔偿往往是比较困难,因此重点应是预防监管对数据主体的影响。衡量风险有两个方面:(1)引发风险的可能性高低。数据处理规模越大越容易引发隐私风险。并且,风险高低跟使用场景有关。如果使用场景是连接到互联网,与外部站点进行数据交换,与其他系统互连等,那都可能成为黑客攻击的漏洞,有可能增加因数据整合而产生负面影响的风险。相反,未与互联网相连的稳定系统中的数据整合风险则较低。(2)风险引发的后果的严重性。后果严重性可以是比较低的,如使数据主体产生心理上的不适;也可能是非常高的,如犯罪分子有可能利用个人的位置轨迹信息进行犯罪活动而导致受害者失去性命。③ 儿童数据及敏感数据引发的后果严重性也较高,应着重予以保护。在可能引起高风险的使用场景中可引入业已成熟的隐私影响评估机制(Privacy Impact Assessment)加以判断。

3.衡量是否已达到一般性义务上的平衡。④ 数据控制者须遵循一般性的数据保障义务,例如遵循比例原则和透明化原则,尊重数据主体的合理预期等。如数据控制者完全遵循了这些义务,则更有可能通过平衡测试。当然,遵循一般性义务并不意味着一定能够通过平衡测试,否则合法利益将会变成有机可乘的立法漏洞,导致个人信息使用的其他合法依据不再具有适用意义。

4.平衡存疑时,可考虑数据控制者是否采取了额外保障措施以减少对数据主体的影响。保障措施

① European Data Protection Supervisor, *Additional EDPS Comments on the Data Protection Reform Package* (Brussels, 15 Mar. 2013).

② Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP217 (2014), p. 25. 英国ICO《欧盟通用数据保护条例指南》则将合法利益测试(legitimate interests assessment)解构为:(1)确认合法利益;(2)证明数据使用的必要性;(3)与个人利益、权利和自由进行平衡。本文采用欧盟29条工作组建议的检验步骤。下文是对29条工作组意见的归纳和分析。

③ 我国2017年5月9日发布的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条也已专门将行踪轨迹纳入保护范围,目的在于防止绑架等犯罪活动。

④ 29条工作组表述为"临时平衡"。鉴于衡量的是在遵循一般性义务的基础上是否已经取得平衡,本文表述为"一般性义务上的平衡"。

可以是匿名技术、隐私增强技术、隐私设计、隐私影响评估、增加透明度、无条件退出机制等。依据个案情况,可采用相应的额外保障措施。例如为未成年人提供药品滥用、意外怀孕、酗酒等敏感信息咨询的非政府组织的网页搜集访客的信息后应立即进行匿名化处理,将个人信息转成统计数据。再如,各个医院为控制药品供应而共同建立了药品瘾君子的黑名单,由于毒瘾为个人敏感信息,医院应采取额外的保障措施,严格确保个人信息不会被泄露和不当利用。在科研方面,研究父母离婚失业对儿童教育所产生的影响及儿童肥胖症等,需要进行个人信息假名化处理和采取防止信息泄露的安全性保障措施。

(二) 平衡测试应遵循的原则

虽然工作组提出了平衡测试的内容框架,但仍需采用个案分析方式进行测试。个案分析方式无法预设结论,需依据案例情况的不同进行分析。总体而言,平衡测试必须遵循以下几个基本原则。

1. 必要性原则

必要性原则是衡量可否对个人信息基本权利进行限制的基本原则。欧盟《通用数据保护条例》中的合法利益豁免条款明确规定,个人信息的使用程度必须是为实现合法利益所必需(necessary)。具体而言,必要性可归纳为两个规则。

首先,信息使用程度应以最小化利用为限。例如报纸可能有必要公布某些涉嫌参与腐败的高级政府官员的消费习惯细节,但不应该一揽子允许媒体公开所有不相关的公众人物私人生活细节。再如,APP 开发商希望能够收集其 APP 用户的整个通讯录,但收集通讯录上他人的手机号码一般需经号码本人的同意。对此 APP 可以采用对比后删除的方式,先获取用户的通讯录,以确定其他人以前是否已经授权 APP 开发商获取其手机号码,之后立即删除未征得同意的他人手机号码。该获取后立即删除的方式也体现了使用的程度仅以必要性为限的原则。

其次,处理个人信息的方式应是影响最低的方式。因此,衡量必要性还需考虑是否有其他影响更低的替代性使用方式。例如公司设置隐藏摄像头以监控员工和访客吸烟就违反了必要性原则,公司可采用更合适的方式,比如设置吸烟监测器和明显禁烟的标志来禁止吸烟。再如,为检查员工是否在工作时间内过度浏览无关网页,公司收集了其员工浏览网页和下载文件的记录信息。由于公司可以采用其他较为不侵犯隐私的方式(比如限制某些网站的访问权限)来达到管理目的,因此不太可能通过平衡测试。

在判例 Breyer 案中,虽然德国政府的网站拥有防止黑客攻击的合法利益,但是记录访客 IP 地址不一定是影响最低的使用方式,且没有在一定期限内删除所记录的 IP 地址,有可能违反必要性原则。①

2. 目的限定原则

工作组意见特别指出,平衡测试还需遵循目的限定原则[7](P.33)。目的限定原则是指,数据的后续使用方式应与原先的收集目的"相称"(compatible)。② 欧盟《通用数据保护条例》绪言第 50 条指出,衡量相称性应考虑后续使用目的与原先目的之间的关联性、数据收集的场景及该场景下的数据主体的合理预期、数据的性质、后续使用产生的后果及现有的保障措施等。可见,相称性是对以上因素进行综合考量后得出的判定结果。尤其是在大数据产业下,数据机构对数据的二次利用往往跟原先目的没有关联性,但这并不意味着一定不相称。后续使用方式如果符合用户的合理预期,则有可能符合相称性要求[4](P.37-39)。

用户合理预期是用户基于其与数据控制者之间关系所产生的预期。③ 该概念源于欧洲人权法院判例所确立的合理预期规则,④是隐私基本权利内涵的体现。在以往的实践中,用户的合理预期便是衡量

① Breyer (Case C582/14, ECLI: EU: C: 2016: 779).
② 欧盟《通用数据保护条例》第 5 条第 1 款第 b 项。
③ 欧盟《通用数据保护条例》绪言第 50 条。
④ Copland v. United Kingdom App No. 62617/00 (ECHR 3 April 2007), para. 42.

相称性的因素。为了回应平衡测试不清晰的问题[9](P. 321 - 352),欧盟新颁布的《通用数据保护条例》更是将"数据主体的合理预期"明确纳入立法之中。条例绪言第 47 条规定,平衡测试应将数据主体合理预期纳入考量范围之内。数据控制者除非能够证明其合法利益足够重要(compelling),否则应避免数据使用方式超出数据主体的合理预期。①

数据主体的合理预期应置于具体的使用场景中进行具体考量。29 条工作组意见对数据主体合理预期进行示例解释,指出竞选候选人使用公民注册时的资料发送其未来竞选活动的日程表,符合个人的合理预期;而某非营利组织通过收集用户浏览其网站的痕迹,例如点赞、分享或定期浏览该网站的某些类型的消息,然后根据用户的画像向用户发送与该类型相关的消息,则不太可能符合用户的合理预期,应征得用户同意更为合适。再如披萨零售店将其顾客的订单数据卖给保险公司,保险公司通过食品订单数据建立健康状况模型,以确定该顾客投保保费金额的高低,这显然超出了该顾客的合理预期[7](P. 31 - 33)。英国 ICO 大数据政府报告也指出,大数据分析能够对投保风险进行更精准的评估,但对于需要支付更高额保费的高风险投保人而言,这个评估过程意想不到且令其"毛骨悚然(creepy)",不符合用户合理预期[4](P. 19 - 28)。

总而言之,大数据分析有可能以数据主体意想不到的方式重新利用数据,使用复杂的算法,对数据主体进行特征分析,产生预期以外甚至是不良的影响。在大数据时代,数据机构仍需要考虑大数据应用中数据主体的合理预期[4](P. 19 - 28)。

3. 比例原则

合法利益豁免并非禁止对数据主体产生任何负面影响,而是应将产生的影响控制在符合比例的范围之内[7](P. 41)。直接营销便是体现比例原则的典型例子。由于直接营销属于私人商业利益,本身的重要性较低,使用所产生的影响是否符合比例对平衡测试的结果起着决定性的作用。

简单的直接营销可通过平衡测试。例如,披萨店储存了购买披萨顾客的地址和信用卡信息,向顾客家中信箱邮寄了披萨店类似商品的打折券,并提供了简易的拒绝营销的退出机制,符合比例原则[7](P. 31)。

但直接营销若涉及大数据分析的精准营销,对数据主体带来的负面影响程度有可能变高,则有可能不符合比例原则。例如某定向行为广告公司不仅仅使用顾客的地址和信用卡信息,还使用了披萨店近期的订单历史(例如过去三年)和该顾客在披萨店所属的总公司旗下其他在线超市商场的购买信息。该公司通过定期信件,电子邮件以及顾客登录的网站等线上和线下各种渠道发送基于顾客偏好而形成的各种广告。此外,公司还追踪顾客的位置信息,当顾客搬至富人区时则无法享受折扣优惠,导致顾客无法享有公平待遇。② 该定向行为广告公司在信息使用程度和规模上超过必要合理的限度,且违背公平对待原则,因此无法通过平衡测试[7](P. 32)。

直接营销能否通过平衡测试跟其使用的程度和规模有关。库勒(Kuner)教授指出,大规模的数据收集和使用不太可能符合比例原则[10](P. 1615 - 1619)。由于在线追踪有可能对隐私形成威胁,研究也表明人们普遍认为在线追踪过度侵犯用户的隐私,③欧盟不少专家认为,对于跨网页追踪用户浏览痕迹的定向行为广告不能适用合法利益豁免,单个网页内的定向行为广告才可适用,比如网上书店可使用用户在书店网页上的浏览记录推荐图书,但不能追踪用户在其他网站上的浏览记录进行综合推荐[11](P. 163 - 176)。

综上所述,是否通过平衡测试应具体情况具体分析,结合使用场景中的各个因素(如合法利益的重

① UK Information Commissioner's Office, *ICO Guide to the General Data Protection Regulation (GDPR)*, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/, assessed May 14, 2018.

② 大数据"杀熟"目前已成为热点议题。

③ European Commission, *Special Eurobarometer* 359: *Attitudes on Data Protection and Electronic Identity in the European Union* (2011), available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, accessed Oct. 31, 2018, p. 146.

要性、使用所产生的负面影响、可采取的保障措施等) 进行综合考量。数据使用程度应为实现其使用目的所必需,符合比例原则,并尊重用户合理预期。

四、平衡测试的监管

不少专家质疑,合法利益豁免有可能成为企业规避法律的漏洞[8]。合法利益豁免避开了取得用户同意的环节,将风险控制交由数据控制者负责,容易导致数据控制者的权限过大,滥用个人信息。该问题可以通过对数据控制者加以必要的监管来解决。

(一) 数据主体拒绝权和退出机制

合法利益豁免虽然不用经过数据主体同意,但并不意味着架空数据主体的选择权和控制权,用户可以通过行使拒绝权(即退出机制) 来监督数据控制者的数据使用。退出机制与同意机制的区别在于,同意机制采用择入(opt - in) 方式,在数据主体在点击同意后方可使用; 而退出机制采用择出(opt - out) 方式,在数据主体点击退出后才不可使用。

个人信息权是自主决定权,因此数据主体拥有拒绝使用其信息的权利。欧盟《通用数据保护条例》第 21 条确立了数据主体拒绝权,并在第 21 条第 1 款指出,数据主体对基于合法利益豁免的数据使用享有拒绝权。数据主体拒绝权主要体现在以下两个方面:

当使用利益属于足够重要的利益(如为公共利益或广泛群体利益所需),但数据主体提出拒绝时,数据保护机构或法院可以基于数据主体的拒绝理由对利益平衡进行重新评估。除非数据控制者能够证明其合法利益达到足够重要的程度(compelling) 且高于数据主体的利益,否则数据控制者不能再使用该数据。数据主体拒绝权是对平衡测试的再补充[7](P. 44 - 45)。

当使用利益属于私人商业利益等其他非重要利益时,数据主体可以无条件拒绝使用其个人信息。在这种情况下,数据控制者必须提供易于操作的用户退出机制。《欧盟通用数据保护条例》第 21 条第 2 款特别指出,当个人数据用于直接营销时,数据主体任何时候均可拒绝,其中包括数据主体画像的直接营销。直接营销属于私人利益,相较于公共利益,重要性较低。对于大数据营销,29 条工作组意见还特别指出,随着大数据带来的隐私风险的提高,数据控制者更加难以通过平衡测试。以数据主体画像为基础的大数据预测分析通过复杂的机器自动处理技术进行全面追踪和分析,容易纳入敏感信息,高度介入个人隐私。因此,平衡测试的天秤将往个人基本权利倾斜,数据控制者如要通过平衡测试则需有足够的保障措施以恢复天秤的平衡[7](P. 45 - 46)。因此当涉及商业营销时,数据主体可以无条件拒绝。

基于拒绝权的用户退出机制是大数据实践的重要保障措施。欧洲数据保护监督机构建议,在大数据利用的情形下,如果难以在机构的合法利益与数据主体的权益之间取得平衡,数据主体退出机制则可成为取得权益平衡的有效手段。① 29 条工作组意见也指出,除同意机制外,一个完善可行的退出机制也可在数据主体权利保障方面发挥重要作用。退出机制越容易操作,越有利于控制者通过平衡测试[7](P. 45 - 46)。此外,数据控制者还应遵循透明化原则,公布相关信息使数据主体能够清楚了解数据使用方式,保证用户退出机制的有效行使。

(二) 平衡测试的问责机制

平衡测试的判定方曾在欧盟各成员国形成不同的实践,或由控制者判定,或由国家监管机构判定[1](P. 249 - 250)。欧盟《通用数据保护条例》最终将平衡测试交由数据控制者执行。有专家担心,数据控制者为利益相关方而非中立方,不合适作为判定者,交由数据控制者执行将成为数据控制者规避监管的法律漏洞。且平衡测试需要专业的法律意见加以评判,有的数据控制者未必具有专业经验,由法院或政府官方机构判定更为合适[8](P. 19)。尽管如此,政府部门和法院实际上并无足够的精力一一审查。因此,

① European Data Protection Supervisor, *Meeting the Challenges of Big Data*, Opinion 7/2015. EDPS, 19 Nov. 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15 - 11 - 19_big_data_en.pdf, assessed Oct. 31, 2018.

欧盟最终规定,平衡测试由数据控制者进行记录和证明,并由法院或政府数据保护机构加以监管。

谷歌 2012 年便是因不当适用合法利益豁免而被 29 条工作组要求整改。谷歌为维护升级系统而使用个人信息。29 条工作组认为谷歌无法通过平衡测试,理由如下:(1)谷歌并未尽充分告知义务,未告知用户其信息使用的目的和类型;(2)谷歌将各类服务的数据进行合并处理,但未能证明收集如此大的数据库是为其使用目的所必需的,且未能符合比例原则;(3)谷歌未能提供其收集的数据的保留期限,未能在一定期限内删除该数据。29 条工作组就此要求谷歌进行整改,采取一系列的额外保障措施。①

由政府部门和法院加以监管的方式与现行实践较为契合,也是欧盟数据保护核心原则"问责原则"的体现[1](P.261)。在问责原则的规范下,数据控制者负有举证责任证明其操作符合规定,否则将受到相关处罚和承担赔偿责任。② 因此,相较于知情同意机制,合法利益豁免并不是一个相对轻松的选择,在未获得数据主体同意的情况下,意味着数据控制者应承担更多的责任,数据控制者需对使用和评估过程进行全程记录[4](P.34)。

英国 ICO 大数据政府报告指出,大数据机构需要有一个合法利益的基本价值框架表,形成评估方法,并定期对信息处理过程进行再评估。当接受政府监管部门检查或受到数据主体质疑时,大数据机构应能够提交这些评估过程记录予以证明,产生争议时可由政府监管部门或法院判定是否通过平衡测试[4](P.34)。

五、对我国的启示

我国目前并未对个人信息保护进行系统立法,关于个人信息保护的相关规定散见于各种法律法规及部门规章之中。基于大数据信息使用的多元性和复杂性,各国近年来都陆续制定通过个人信息保护法,我国制定个人信息保护法的需求也迫在眉睫。在未来制定系统的个人信息保护法时,我国应引入合法利益豁免。

(一)明确立法目的和构建基本原则

制定个人信息保护法首先应明确立法目的。个人信息保护法的根本立法目的应为,实现个人信息保护与信息自由流转之间的平衡,而并非单一地保护个人信息本身[12]。我国之前相关规定一直未明确该立法目的,例如 2012 年《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》及 2017 年《网络安全法》均未对平衡信息流转价值进行规定。这导致我国在强调个人信息的人格权保护时,往往忽略了信息流转的价值。未来应明确利益平衡的立法目的,这样才能形成整体统一的系统性立法架构。

其次,应确立相应的个人信息保护基本原则。我国《网络安全法》第四章仅规定了"合法、正当、必要的原则"。2017 年《个人信息安全规范》对个人信息保护基本原则进行了较系统的规定,认为包括:a)权责一致原则;b)目的明确原则;c)选择同意原则;d)最少够用原则;e)公开透明原则;f)确保安全原则;g)主体参与原则。其中,权责一致原则即是"问责原则",也是合法利益豁免中数据控制者负责证明通过平衡测试的依据所在。最少够用原则即为必要性原则,数据使用应以最小化利用为限。

除上述原则以外,我国还应引入比例原则。比例原则是实现"平衡数据保护与流转"立法目的的重要平衡工具,旨在"在社会共同利益与保护个人基本权利之间寻求合理平衡"。③ 比例原则是个人信息保护新理念"风险路径"的基本原则。风险路径提倡信息监管应由收集阶段转至使用阶段。依据比例原则,可确立相应场景下合理使用的判定规则,以判定使用阶段中数据使用是否合规。

再者,我国可考虑引入改进后的目的限定原则。目的限定原则为传统个人信息保护的基本原则,但

① Article 29 Working Party, *Letter from the Article 29 Working Party to Google in Relation to Its New Privacy Policy* (Brussels, 16 Oct. 2012).

② 关于数据控制者的规管模式研究,参见谢琳"香港资料处理者的个人资料保护责任问题研究",载《当代港澳研究》2013 年第 3 期。

③ Soering v. United Kingdom, 11 ECtHR (ser. A) at §89 (1989).

由于受到原先收集目的的限制,与大数据二次利用模式格格不入,受到风险路径支持者的强烈批评[5]。对此,可对目的限定原则进行改造,不必要求后续使用目的必须与原先目的具有关联性,只要尊重用户的合理预期,即可符合目的限定原则。这也是相应场景下合理使用规则的体现,尊重数据主体合理预期的使用才属于合理使用。

(二)引入合法利益豁免机制

在确立立法目的和基本原则的框架下,我国应引入合法利益豁免机制。《网络安全法》仅规定了收集利用个人信息须经数据主体同意,但未对无需数据主体同意的例外情况进行规定。这导致了我国个人信息保护有可能比采用严保护的欧盟立法更加严格。为解决这个问题,国家推荐性标准《个人信息安全规范》5.4 条规定了十个信息处理的例外情况,例如国家安全、重大公共利益、犯罪侦查等,在一定程度上弥补了《网络安全法》过于僵化的缺陷。但由于《网络安全法》规定的框架所限,安全规范只能采用列举性规定,未能在整体上引入合法利益豁免,无法代替合法利益动态平衡机制所带来的灵活性。①

对于合法利益豁免的规定,应借鉴欧盟的灵活路径,对合法利益应采用宽泛解释,将其解释为未违反法律规定的利益,并通过平衡测试的个案分析来限制合法利益的适用。构建清晰可行的平衡测试操作指引是落实合法利益豁免机制的关键所在。我国数据保护部门(如网信办)可制定详细清晰的平衡测试指引,并出台一系列示例,进行类型化分析,为个案分析方式的不确定性提供一定的参考依据。

相较于欧盟的严格规定,我国平衡测试的平衡重心可相对向数据控制者倾斜。欧盟尽管已采用合法利益宽泛解释说的路径,但平衡测试的衡量标准仍过于严格。例如在 2014 年被遗忘权判例中,谷歌在搜索结果显示相关个人信息报道链接被认为不能适用合法利益豁免。② 该案的判决受到不少欧盟学者和我国学者的反对。对新技术采用过于严格的限制有可能不利于其发展。

纵观欧盟近年来的立法实践,欧盟过于强调大数据隐私风险的提升,而未充分考虑如何实现大数据的流转价值,对现行过于严格的标准也未适当放宽。这也是目前众多专家学者批评欧盟立法限制大数据产业发展的原因。譬如,在大数据营销中,欧盟一直关注的是大数据营销所带来的隐私风险的提高,而忽略了大数据产业自身的发展需求。大数据营销虽已被欧盟《通用数据保护条例》规定为合法利益,但却无法通过平衡测试。虽然欧盟在立法层面上已规定了可供执行的灵活的合法利益豁免机制,但却由于其对数据产业的数据保护要求过高,该机制在实际适用层面上仍具有较大的局限性,未能成为产业普遍适用的数据处理依据。

欧盟个人信息的严格保护模式有其自身历史成因和产业发展水平的考量[13](P.68-70)。由于我国的隐私文化和数据产业发展水平与欧盟不同,我国目前正处于大数据产业快速发展的上升期。因此,我国在平衡测试中可采取相对宽松的标准,将平衡测试的天秤向数据控制者适当倾斜,以促进大数据产业的发展。

参考文献:

[1] Paolo Balboni, *et al.*, *Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection*, *International Data Privacy Law*, vol. 3, no. 4 (2013).

[2] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).

[3] Viktor Mayer-Schanberger & Yann Padova, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, 17 Colum. Sci. & Tech. L. Rev. 315 (2016).

[4] UK Information Commissioner's Office, *Big Data, Artifi-*

① 《个人信息安全规范》起草者洪延青博士也指出,由于安全规范只能在网络安全法框架下制定,例外情况只能列举,不可能代替合法利益所给予的灵活性,参见"《个人信息安全规范》史上最内行解读",来源:南方都市报 2018-02-06,http://toutiao.3g.oeeee.com/mp/toutiao/BAAFRD000020180205669l1.html,最后访问日期:2018-03-13。

② Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez (Case C-131/12, EU:C:2014:317).

cial intelligence, *Machine Learning and Data Protection* (2017).

[5] 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。

[6] 谢琳、李旭婷 "个人信息财产权之证成",载《电子知识产权》2018 年第 6 期。

[7] Article 29 Data Protection Working Party, *Opinion* 06/2014 *on the notion of legitimate interests of the data controller under Article* 7 *of Directive* 95/46/*EC*, WP217 (2014).

[8] Federico Ferretti, *Data Protection and the Legitimate Interest of Data Controllers: Much ado about Nothing or the Winter of Rights?*, Common Market Law Review, vol. 51, no. 4 (2014).

[9] Irene Kamara & Paul De Hert, *Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground*. In Evan Seligner, Jules Polonetsky & Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge: Cambridge University Press (2018).

[10] Christopher B. Kuner, *Proportionality in European Data Protection Law and Its Importance for Data Processing by Companies*, Privacy & Security Law Report, vol. 7, no. 44 (2008).

[11] Frederik J. Zuiderveen Borgesius, *Personal Data Processing for Behavioural Targeting: Which Legal Basis?*, *International Data Privacy Law*, vol. 5, no. 3 (2015).

[12] 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",载《法学研究》2018 年第 2 期。

[13] 龙卫球 "数据新型财产权构建及其体系研究",载《政法论坛》2017 第 4 期。

Legitimate Interests Exemption for Personal Data Processing in the Big Data Era

Xie Lin

Abstract: In the big data era, the notice and consent mechanism is unable to effectively deal with the diversity and complexity of the big data ecosystem, and legitimate interests exemption which does not require the consent of the data subjects can be an important alternative legal basis for big data information processing, and provide big data industry flexible development space. China may introduce legitimate interests exemption mechanism in the relevant legislation on personal information protection. When introducing this mechanism, a broad definition of legitimate interests should be adopted, as long as it is a non - illegal use of interests, it belongs to legitimate interests. However, the data controller must conduct a balance test to prove that the legitimate interests of data use override the personal interests of the data subject, in order to apply legitimate interests exemption. The balance test can be carried in a case - by - case way and should follow the principles of necessity, purpose limitation, and proportionality. In addition, data controllers should document the balance test, in order to be monitored by data subjects, government data protection authorities, and courts.

KeyWords: Big Data Era; Personal Data Protection; Legal Basis; Notice and Consent Mechanism; Legitimate Interests Exemption

(责任编辑 寇 丽)