主题研讨

大数据时代个人信息保护的路径重构

范　为

内容提要:大数据分析的普遍应用给公民隐私带来严峻威胁,以“知情同意”为核心的传统个人信息保护架构日益捉襟见肘,既无法为公民隐私提供实质性保障,又成为制约数据价值开发的重要掣肘。各国纷纷重审既有法律制度以顺应时代发展需求,尤以美国《消费者隐私权利法案(草案)》及欧盟《数据保护通用条例》最为典型。欧美个人信息保护立法改革虽路径各异,然其最大亮点在于均不同程度地吸纳了国际主流的场景与风险导向的新理念。新理念以隐私风险作为衡量个人信息“合理使用”的指标,根据具体场景中的风险评估采取差异化保障措施,变信息处理前的静态合规遵循为信息使用中的动态风险控制,在提升个人信息保护实效性的同时大幅减轻企业负担,助力数据开发与数据保护的双赢。本文提出以基于场景的风险管理理念重构个人信息保护的新路径,以期为我国立法与实践提供参考借鉴。

关键词:个人信息保护　场景与风险评估　合理使用　消费者隐私权利法案　数据保护通用条例

范为,中国信息通信研究院互联网法律研究中心助理研究员。

一　“知情同意”为核心的传统架构面临的困境与抉择

信息技术的飞速发展深刻地改变了人们的生活,催生出新的经济增长模式,数据的创新应用更是激活了巨大的经济与社会价值。[1] 与此同时,大数据开发引发的一系列伦理问题也日益凸显,对公民隐私及权益造成的威胁尤为突出。在信息技术的冲击下,隐私威胁日益超越了传统个人信息保护机制的应对能力。如何在开发信息价值的同时保障个人

〔1〕 The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf,本文所有网络资料最后访问时间均为2016年9月6日。

信息的合理利用,有效平衡创新发展与隐私保护,业已成为当今时代最大的公共政策难题之一。[2]

(一)传统架构无法应对大数据时代的挑战

大数据时代,数据作为基础性的生产资料,日益成为企业提升竞争力的核心资产,海量信息尤其是个人信息的收集、多方流转、比对与再利用成为价值创造的源泉,同时也推动着个人信息生态系统(personal data ecosystem)[3]朝着去中心化的方向重构。用户面临的不再仅仅是与服务提供商直接、单一的联系,还要同时面对与数据中间商和数据后续利用者等多重主体的关联,[4]因而对自身信息的控制能力日益削弱。除此之外,大数据技术的创新应用在多重方面对个人隐私构成严峻冲击。无所不在的数据收集,对个人形成密集追踪,大量机器对机器的被动收集往往不为用户所知悉;个人信息的累积及分析、比对,构建出完整的人格图像,极易挖掘出个人不愿为他人知晓的敏感信息,为个人带来困扰、不安,引发寒蝉效应,乃至造成财产、人身损害,敏感信息用于求职、教育、信用评级等领域,极易使个人遭遇不公及歧视待遇。[5]

面对日益严峻的冲击,以欧盟《数据保护指令》(以下简称"指令")为代表的传统个人信息保护架构[6]日益捉襟见肘。传统机制建构在"知情同意"架构(notice-and-consent framework)的基础之上,要求机构在收集用户个人信息前,告知用户信息的处理状况,在网络服务的语境中通常表现为发布隐私声明,用户在阅读声明后作出同意的意思表示,作为对个人信息收集及利用的合法授权。然而,作为传统架构"立足之本"的"知情同意"机制在大数据时代遭遇严峻冲击。首先,知情同意机制为用户与机构均带来沉重负担。个人信息流转的多元复杂性为机构在隐私声明中清晰阐述带来严峻挑战,信息创新利用的目的也往往难以在收集时所预知,为遵循法律要求,机构往往列出冗长艰涩的隐私声明,也给用户阅读带来沉重负担,有研究表明,用户仅阅读一年中使用的网络服务的隐私声明就要花费 244 小时的时间。而现实中用户往往越过隐私声明直接点击同意,既不阅读更难以理解其内容,隐私声明沦为一纸空文,正如学者兰道(Susan Landau)所言,隐私声明

---

〔2〕 Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 Stan. L. Rev. Online 25, 26, 2013, http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-and-big-data.

〔3〕 The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.

〔4〕 See, e.g., The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 – 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

〔5〕 See generally Daniel J. Solove, The Future of Reputation: Gossip, Rumor and Privacy on the Internet (2007), http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text/futureofreputation-ch1.pdf.

〔6〕 传统个人信息保护架构最先由美国卫生及公共服务部(Department of Health, Education and Welfare)于 1973 年提出,宗旨是确保信息主体的信息得到公平的利用。1980 年经济发展合作组织(OECD)将其采纳入个人信息保护指南(OECD Guidelines),并发展为收集限制、信息质量、目的限定、利用限制、安全维护、公开透明、个人参与、责任明确八项基本原则。OECD 指南构成了国际上现行个人信息保护法的基础,建立在此原则基础上的欧盟《数据保护指令》是国际上最早的全面性立法,也是国际个人信息保护法的典范,因而本文主要以欧盟数据保护指令为例说明现行立法框架面临的困境。See Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

远非为人类使用而设计。[7] 其次,用户并无实际的控制权,且权利的行使日益困难。在网络语境中,为使用产品或服务,用户往往除点击同意之外并无其他选择,[8] 实质上架空了用户的权利;更重要的是,在个人信息密集收集与多方流转的生态系统中,用户在很多情况下对其信息的收集并不知情,难以对第一方收集者行使权利,更遑论向缺乏直接联系的第三方机构行使控制权。在大数据时代,用户对其个人信息面临全面失控的局面。总而言之,传统的知情同意框架在大数据时代面临穷途末路:一方面隐私保护效率低下,用户权利几近架空;一方面给企业造成沉重负担,严重阻碍数据流通及创新应用。

除知情同意机制失灵外,传统架构还面临全方位的适法性困境。[9] 首先,在个人信息定义方面,海量信息的收集比对及信息技术的发展,使信息对特定个人的辨识能力日益增强,传统个人信息的边界越发模糊,大幅扩张了个人信息保护法的潜在适用范围,也使得个人信息的有效匿名化日益困难;第二,在目的限定原则方面,个人信息的后续比对挖掘和价值开发成为创造价值的主要来源,收集的个人信息用于超出原初收集的、无法预知的目的,使传统"目的限定"原则遭遇前所未有的挑战,与此同时,信息日益成为生产资料与核心资产,传统"信息最小化"原则的合理性日益受到质疑;第三,在多方主体责任界定方面,在去中心化的个人信息生态系统中,多元信息处理主体的存在及与用户直接联系的缺失,使得对个人信息后续利用的第三方主体尤其是数据中间商的监管几近真空,数据中间商与第一方信息收集者的责任界定十分模糊,用户对后续流通环节的权利更是无从行使;第四,在数据跨境传输方面,全球经济的互联驱动信息跨国跨境流转,然而各国间个人信息保护法律制度存在相当的差异,个人信息跨境传输面临严峻的管辖权与适法性难题,信息的自由流通面临严重阻碍。

事实上,早在大数据分析盛行之前,欧盟指令已长期陷入严峻的执行困境,大数据时代的到来使得既有的困境更加严峻。传统个人信息保护制度架构已经远远落后于时代发展需求,既无法为用户隐私提供有效、实质意义的保护,同时又给企业带来沉重负担,成为数据经济时代开发数据价值、释放数据红利的严重掣肘。

(二)探索个人信息保护新路径的必要性

知情同意的传统架构遭遇严重冲击的根本原因在于,其根植于"前信息时代"的框架中,与大数据时代个人信息生态系统的新格局格格不入。经济合作与发展组织(OECD)指导原则及欧盟数据保护指令均制定于互联网尚未产生的年代,[10] 信息的收集比对及挖掘分析能力不可同日而语,更遑论当今盛行的云计算、大数据技术,因而已无法适应当今

〔7〕 Susan Landau, Control use of data to protect privacy, 347:6221 *Sci. Issue* 504,506 (2015).

〔8〕 Susan Landau, Control use of data to protect privacy, 347:6221 *Sci. Issue* 504,504 (2015).

〔9〕 Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 256 (2013). See also Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning*?, NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp.

〔10〕 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning*?, NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp.

商业模式的发展需求。[11] 法律制度的设计与执行应建立在相应的技术发展水平的基础之上,面对信息技术的迅猛发展,“前信息时代”的制度、理论和经验都变得过时。知情同意架构的设计之初旨在保障用户对其个人信息的控制,然而大数据时代信息收集分析能力的飞跃使得用户陷入显著的不利局面,大大削弱了用户对其个人信息的权利,同时加重了用户及机构的负担,限制了个人信息的流通开发及创新应用,因此知情同意作为保障个人信息的基础性机制已经走向穷途末路。世界经济论坛(WEF)联合微软研究团队发布的一份研究报告[12]指出,由于缺乏实质意义上的用户控制及透明机制,传统个人信息保护架构在当下社会已经失灵。学者鲁宾斯坦(S. Rubinstein)则更进一步指出,知情同意机制在大数据时代已经“无可挽回地走向瓦解,超出了任何规制的修复能力”。[13] 因此,欲实现隐私保护与数据价值开发的共赢,亟需破旧立新,因势利导,跳脱传统知情同意架构的局限,转而探索顺应技术发展的新路径,构建个人信息保护的有效机制,以适应大数据时代的发展需求。[14]

面对大数据分析技术对个人信息保护的威胁,各国政府纷纷重新审视既有法律架构的有效性,不断强化个人信息保护力度,并将此提升至数据主权与国家安全的新高度。在探索适应时代发展的制度架构中,欧美采取了不同的路径与导向。美国通过颁布《消费者隐私权利法案(草案)》(Consumer Privacy Bill of Rights Act of 2015,CPBR),引入场景为主导的个人信息保护新机制,在国际上率先突破了既有的架构模式,在探索适应时代需求的信息保护路径方面做出良好表率。相较而言,欧盟在其改革草案《数据保护通用条例》(General Data Protection Regulation,GDPR)中增设数据外泄通知、隐私影响评估、第三方认证等新机制,突出了场景导向、风险评估等新理念,[15]然而在总体路径上依然延续了既有《数据保护指令》[16]的旧机制,继续强化传统的知情同意架构。[17] 众多学者认为,欧盟

〔11〕 See Fred H. Cate et al., *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (2013), http://op. bna. com/pl. nsf/id/dapn-9gyjvw/ $ File/Data-Protection-Principles-for-the-21st-Century. pdf.

〔12〕 The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3. weforum. org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014. pdf, p. 6 - 7.

〔13〕 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?* NELLCO Legal Scholarship Repository 2, http://lsr. nellco. org/cgi/viewcontent. cgi? article = 1359&context = nyu_plltwp, p. 6.

〔14〕 Fred H. Cate et al., *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (2013), http://op. bna. com/pl. nsf/id/dapn-9gyjvw/ $ File/Data-Protection-Principles-for-the-21st-Century. pdf, p. 9; The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3. weforum. org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014. pdf; Carolyn Nguyen et al., A User-Centered Approach to the Data Dilemma: Context, Architecture, and Policy, *in Digital Enlightenment Yearbook 2013: The value of personal data* (M. Hildebrandt et al. eds., 2013).

〔15〕 Gabriel Maldoff, *The Risk-Based Approach in the GDPR: Interpretation and Implications*, *available at* https://iapp. org/media/pdf/resource_center/GDPR_Study_Maldoff. pdf.

〔16〕 European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC (1995).

〔17〕 See, e. g., Viviane Reding, The European Data Protection Framework for the Twenty-First Century, 2 *Int'l Data Priv. L.* 119 (2012).

的此种路径无益于大数据时代挑战的有效应对。[18] 笔者以下以美国《消费者隐私权利法案(草案)》及欧盟《数据保护通用条例》为例,分析其对传统框架困境的应对及不足,进而探究大数据时代个人信息保护的路径重构。

鉴于商业机构在个人信息生态系统中的特殊影响力,本文研究对象仅针对进行"个人信息处理操作"的商业机构。为行文方便,下文简称商业机构为"机构"或"企业",称"个人信息主体"[19]为"用户",除特别区分外,简称"个人信息"[20]为"信息",特此说明。

二 场景与风险导向理念的内涵及建构

如前所述,欧美个人信息保护立法改革的最大亮点即为引入了"场景"与"风险管理"为代表的新理念。[21] 场景与风险的理念并非横空出世,而是有其深厚的根源,日益为国际社会所倡导与认同。

(一)欧美个人信息保护改革法案概述

2015 年 2 月,美国政府正式发布《消费者隐私权利法案(草案)》的政府讨论稿。[22] 由 2010 年提出框架蓝图,[23] 到 2012 年发布反馈意见[24](以下分别称"白宫白皮书"及"FTC 报告"),直至讨论稿的正式颁布历时五年,其间政府收集采纳了社会各界的意见及需求,社会参与度空前,堪称美国消费者隐私保护立法领域的集大成之作。该法案规范商业环境下的个人信息处理行为,旨在为消费者提供纲领性的隐私基本保障,以提升消费者信任及信心,同时确保充分的灵活性以促进数据的自由流动与开发。法案正文由"透明度"、"用户控制"、"尊重场景"、"集中收集与有责利用"、"安全维护"、"信息获取与信息质量"、"责任界定"七部分构成,并规定由业界根据此纲领性内容制定实施细则予以细化

---

〔18〕 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article=1359&context=nyu_plltwp.

〔19〕 European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC (1995), Article 2(b). 本文采欧盟数据保护指令的表述方式,以"处理"指代对个人信息进行的收集、加工、利用、传输、留存、删除等一切操作。

〔20〕 European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 95/46/EC (1995), Article 2 (a).

〔21〕 "场景与风险管理理念"之称法为笔者个人提出,在国际学说中,仅有"风险导向的理念"(risk-based approach)或"场景导向的理念"(contextual approach)之说。鉴于二者密不可分的关联,为兼顾此两方面要素,笔者在此暂采"风险"与"场景"并列的称法,融合两方面学说,俾供探讨批判。

〔22〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

〔23〕 F. T. C., Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers-Preliminary FTC Staff Report (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

〔24〕 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 - 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. See also F. T. C., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

实施。该法案草案的颁布引发了社会各界广泛反响,部分人士认为其有望开启消费者隐私保护的新纪元;批评人士则认为,草案既未能提供行业可遵循的明确性标准,又未能对消费者隐私提供充分有效的保障。

同于2012年,欧盟委员会发布了《数据保护通用条例》草案,对1995年颁布的《数据保护指令》做出大幅改革,以应对大数据时代的发展需求。该草案历经多轮讨论修订,于2016年4月获最终通过并正式颁布,[25]将于2018年5月开始生效。《数据保护通用条例》最终文本由11章、99条构成,通过提高用户同意的要求及新增被遗忘权、数据可携权等规定强化了数据主体的权利,为数据控制者增设了数据泄露告知、任命数据保护官员(DPO)、进行隐私影响评估(DPIA)等义务,与此同时大幅扩展了条例的适用范围,加大对违法行为的惩处力度,强化对数据保护的监管及起诉机制。可以预期的是,该条例必将在国际社会产生深远影响及示范效应,对于条例内容,各界评价褒贬不一,笔者将在下文的对比与分析中对个人看法逐一阐述。

(二)"场景与风险管理"理念的内涵

大数据时代,个人信息保护的目标是防范个人信息的滥用,同时倡导个人信息的合理使用。如何界定"合理使用"的情景,即构成了个人信息保护的边界。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、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。大数据时代,个人信息的使用场景纷繁复杂,超出立法所能规范与预见的能力,以用户为中心、结果为导向进行动态界定的思路由此日益为国际上所倡导,其核心在于考察个人信息的处理行为给用户带来的后果及隐私影响。个人信息处理是否合理,取决于引发的影响能否为用户所接受,或是否符合用户的"合理预期"。影响用户接受程度[26]或对个人信息利用的敏感程度的因素即统称为"信息场景"(data context)或"场景"(context)[27]。"场景"一词源于美国教授尼森鲍姆(Helen Nissenbaum)的"情境脉络完整性"理论,[28]指个人信息原始收集时的具体语境应得到尊重,其后续传播及利用不得超出原初的情境脉络。场景导向路径,即认识到个人信息保护的合理程度要置于其所处的环境中具体审视,避免脱离场景做抽象式的预判。鉴于场景构成要素的多元性,对个人信息利用的合理性应综合多种因素进行"程度性"判断。跳脱传统架构中二元化的"全有全无"式评判,在具体场景中综

---

〔25〕 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 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri = CELEX:32016R0679&from = EN.

〔26〕 欧盟《数据保护通用条例》中同样强调了用户的接受度。See 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 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri = CELEX:32016R0679&from = EN, Recitals (32).

〔27〕 The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf, p.4.

〔28〕 See generally Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Wash. L. Rev.* 119 (2004). 此外,"场景"一词由英文"context"而来,又译"语境"、"环境"、"情境"等等,"情境脉络完整性"等翻译参见刘静怡:《社群网路时代的隐私困境:以 Facebook 为讨论对象》,《台大法学论丛》第41卷第1期,第1-70页。

合考量多元因素,是场景理念区别于传统机制的最大特征。场景导向的路径近年来日益受到广泛认同与提倡,世界经济论坛的报告便提出建立场景为核心的个人信息保护新路径;[29]白宫白皮书也显示,美国诸多机构及学者均表达了对场景理念的大力倡导。[30]

影响用户对个人信息处理接受度的核心衡量标准即为对用户造成的"隐私损害"或"隐私风险"。防范个人信息的滥用,尤其应警惕个人信息处理行为给用户带来的损害或负面影响。降低隐私损害至用户可接受的合理程度即为个人信息保护的目标。关于隐私风险或隐私损害的具体内涵,国际上尚无统一定论,然而尤为可贵的是,欧盟《数据保护通用条例》及美国《消费者隐私权利法案(草案)》中均强调了防范个人信息处理对个人造成的"负面后果",并对此做出了建设性尝试。欧盟《数据保护通用条例》认为隐私风险源自"可能给数据主体造成身体、物质或非物质层面损害的个人信息处理行为,尤以下列情况最为典型:个人信息的处理可能引发歧视待遇、身份冒用或欺诈、财产损失、名誉损害、机密的泄露、化名信息未经授权的披露,以及造成信息主体经济和社会方面的其他重大不利局面时;用户被剥夺既有的控制权时;信息用以揭示种族来源、政治观点、宗教或哲学信仰、商业联盟成员状况、处理基因信息、有关健康状况、性生活及犯罪状况等信息时;信息被用以分析或预测个人的工作、经济状况、健康状况、个人偏好或兴趣、可靠性或行为、位置或行动,以构建或使用个人资料时;处理儿童等弱势群体的信息时;处理大量的个人信息且影响大量的用户时"。[31] 类似地,美国《消费者隐私权利法案(草案)》也将隐私风险定义为"信息本身或与其他信息比对时,对用户造成精神压力、人身、财产、职业或其他损害的可能性",[32]二者皆较好地归纳了主流观点,为风险评估及管理理念在立法中的构建奠定了初步基础。

"隐私风险评估"[33](Privacy Impact Assessment, PIA)是衡量隐私风险的有效工具,实践中已发展为标准化操作流程,成为国际上日益认同的理念与最佳实务。风险导向的理念,即舍弃传统路径中全有全无的"二元化"判断,转而进行"程度性"评估,以个案分析的精神,在相应场景中具体地评估数据处理行为的风险,根据风险等级采取相应程度的管理措施,是一种贯穿数据处理生命周期全程的动态控制,直指将隐私风险控制在可接受范围内的最终目标。相较于传统框架,风险理念的目标并非消除或最大程度地降低隐私风险,而是承认隐私风险的必然存在,并将隐私风险控制在可接受之范围,风险导向的理念

---

〔29〕 The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.

〔30〕 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 - 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, p. 110.

〔31〕 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 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri = CELEX:32016R0679&from = EN, recital (75).

〔32〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, ec.4(g).

〔33〕 See, e.g., Information Commissioner's Office, *Privacy Impact Assessment Handbook (Version 2.0)*, http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

跳脱日益失效的知情同意这一中间环节,提升用户信息保护的有效性与实质意义,同时因承认合理风险的不可避免性,能够大幅减轻企业的合规压力,从而为数据流通减少不必要的障碍。[34]

(三)欧美改革法案中"场景"与"风险"导向的路径建构

如前所述,美国《消费者隐私权利法案(草案)》的最大亮点即在国际立法中率先构建了场景与风险理念为核心的架构。其中规定,机构"只能通过相应场景中合理的手段收集、留存及利用个人信息",以"在相应场景中合理"的标准作为个人信息处理行为的合法性授权,界定了合理使用的动态边界,为整部法案奠定了基调。其规定,若个人信息的处理"在相应场景中不合理",机构需要"进行隐私风险评估",并"采取适当的手段降低风险",包括但不限于"提供增强性披露及用户控制机制"。机构须告知用户场景中不合理的事项,并以合理的方式为用户提供是否要承担风险以及是否希望降低风险的选择机制。由此可见,该草案建立了以场景为基础、增强用户控制为补充、风险评估为手段、风险控制为目标的架构,即个人信息处理在相应场景中合理,或虽不合理但为用户提供了增强性控制机制时,均构成个人信息的合理使用,从而跳脱了以用户同意作为主要合法事由的传统知情同意架构。

无独有偶,倡导基于具体场景的风险评估同样是欧盟《数据保护通用条例》的抢眼之处。相较于该条例草案于 2012 年最初颁布的版本,[35] 正式颁布的版本特别强化了场景与风险理念的重要性,搭建起了风险管理的初步框架。如第 22 条"数据控制者(机构)义务"中强调,机构应"根据其个人信息处理行为的性质、范围、场景、目的及影响公民权利的可能性、敏感度等"承担相应责任,又如规定在职场、个人或家庭目的利用或"引发高风险的行为"等等不同场景中的处理方式,将风险按大小分为高、中、低三个等级,为"可能引发高风险的行为"规定了额外的增强性义务,如就数据处理行为事先征询数据保护监管机构,进行数据保护影响评估,发生数据泄露事件除告知监管机构外还需通知数据主体等。与此同时,为风险低的数据处理行为豁免部分义务,如发生数据泄露时可免予通报监管机构,外国的数据控制者可免予任命代表等。然而必须指出的是,《数据保护通用条例》虽然规定在具体场景中评估机构的相应义务,但并未从最重要的用户角度强调尊重用户在相应场景中的合理期待,更未将"风险程度低"作为个人信息处理的合法授权,而是在传统的合法授权事由框架下,进一步提升了用户同意的形式要求,继续强化传统知情同意的框架。因此可以说,该条例对场景理念的引入只停留在碎片化的初步阶段,未能有效处理风险导向的理念同传统制度的关系,因而未能建构起风险管理为核心的系统框架,

---

〔34〕 风险管理的理念近年来日益为机构学者所大力提倡。See e. g. Centre for Information Policy Leadership at Hunton & Williams LLP, *Protecting Privacy in a World of Big Data*, Paper 2: The Role of Risk Management (DISCUSSION DRAFT 16 February 2016), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_ big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf. See also Christopher Kuner et al, Risk management in data protection, *International Data Privacy Law*, Vol. 5, No. 2 (2015). 另参见洪延青:《"以管理为基础的规制"——对网络运营者安全保护义务的重构》,《环球法律评论》2016 年第 4 期。

〔35〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

最终无法突破传统路径的困境与局限。

就欧美立法的对比而言,美国《消费者隐私权利法案(草案)》侧重“场景”为核心,而欧盟《数据保护通用条例》则更强调“风险”为导向。“场景”与“风险”理念虽是有所区分的两个侧面,然而基于前述分析可知,二者在本质上密不可分,均服务于为用户个人信息提供合理保障之最终目标。场景是出发点,风险管理是实现手段,风险管理基于相应的个人信息处理场景,即风险评估与控制必须在相应的场景中进行,场景的构成要素同时也是风险评估的具体操作指标。因此,笔者在本文中将两个要素融为一体,并暂命名为“场景与风险导向的理念”。

综上所述,场景与风险导向的理念秉持个案分析的精神,转变传统框架中知情同意的固化思维,认识到个人信息合理使用的判断标准取决于是否符合用户的合理隐私期待,以及是否造成了不合理的隐私风险,而并非僵化审视是否取得了当事人的同意。

场景与风险导向的新思路认识到,大数据时代纷繁复杂的个人信息处理场景中,前端的、静态的遵循知情同意的框架已经不足以应对严峻的隐私挑战,必须及时扭转思路,在个人信息处理所处的具体场景中进行动态的风险控制,即变僵化的合规遵循为灵活的风险管理,促进个人信息的“合理使用”,重点规制个人信息的“不合理使用”行为。场景与风险导向的理念能够显著提升个人信息保护的有效性及实质性,同时大幅减轻企业不必要的合规负担,是协调隐私保护与数据价值开发的必由之路。

三 欧美法案的新理念对传统困境的应对及不足

基于前述欧美法案中场景与风险导向的基本框架,笔者以下试从传统架构困境的视野出发,对美国《消费者隐私权利法案(草案)》与欧盟《数据保护通用条例》的应对传统困境的效果及不足加以逐一审视。

(一)个人信息的定义及法案适用范围

个人信息的定义在传统架构中面临边界模糊、界定困难的困境。欧盟《数据保护通用条例》除了对匿名、化名信息及特殊种类的信息有新增规定外,基本延续了传统指令“能够直接或间接识别特定自然人”的定义,依然未能摆脱传统框架的困境。相较而言,美国《消费者隐私权利法案(草案)》的定义则呈现出更为可观的改善,其中将个人信息定义为“能够连结(link)到特定个人或设备的信息”,相较于欧盟指令及《数据保护通用条例》中抽象的“识别性”(identifiable),《消费者隐私权利法案(草案)》进一步指出了个人信息“关联性”(linkable)的特征,且将范围拓展到“设备”(device)的规定,体现了基于大数据时代个人信息范围扩展的考量,是难能可贵的进步。[36] 随后列举构成个人信息的具体类型,如姓名、邮箱地址、电话号码、身份证号、指纹等,并指明能够以合理方式连结到前述类型的信息均属个人信息,颇为值得称道。其规定构成对欧盟数据保护指令及《数据

〔36〕 关于个人信息的“连结性”,笔者曾以专文详细阐述,参见范为:《论巨量信息时代个人资料之定义与去识别化》,发表于“2014 第十八届全国科技法律研讨会”,国立交通大学科技法律研究所等主办,新竹(2014)。

保护通用条例》中“直接识别”与“间接识别”划分方式的改进,其列举的具体类型为通常意义上能够直接辨识个人的信息类型,最后指出能够与其“关联”或“绑定”的信息均属个人信息,很好地抓住了个人信息辨识个人的方式与实质,同时有助于缓解抽象界定带来法律适用不确定性的困境,实为对传统定义的飞跃。然而需要指出的是,同《数据保护通用条例》类似,美国《消费者隐私权利法案(草案)》的定义未能充分强调个人信息高度依赖于场景并唯能在具体场景中加以判断的特征,因而同样存在路径性局限。

此外,美国《消费者隐私权利法案(草案)》也规定了大量的排除条款,如将合法公开可得的信息、经去识别化处理的信息、雇员信息、网络安全信息等排除出个人信息的范围。同时在适用主体方面,较欧盟数据保护指令做出更多例外性规定,如将一年中处理 10000 名以下用户非敏感信息且只进行内部利用的机构排除出适用主体范围,以及排除单纯将信息用于信息安全维护的情形等。另外,定义场景的条款中也排除了将信息用于反欺诈、严重暴力犯罪侦查、安全维护、维护机构权力及财产、商业记录留存等状况。[37] 上述排除规定体现了场景理念与隐私风险导向,留出了相当的灵活空间,有利于促进个人信息合理利用,其出发点值得提倡,然其例外规定也过于宽泛,也使得信息滥用行为有机可乘,例如,对于排外条款中的“公开信息”与“雇员信息”,若经第三方收集用于其他目的或场景之中,乃至比对挖掘产生新的敏感信息,无可否认会为当事人带来不可预期的隐私风险。因此,该草案中关于排除适用的具体规定虽体现出对隐私风险的考量,[38] 然而未充分顾及到具体场景中隐私风险的差异,不能为用户隐私提供充分保障,同时增加了机构在合规方面的复杂性。

(二)目的限定与信息最小化原则

在数据普遍流转与后续利用的现代商业模式中,个人信息的利用目的往往难以在收集之初所预期,传统目的限定原则的适用遭遇严重困境。目的限定原则要求个人信息的收集需具备特定的目的,后续利用及传播不得违背此目的。[39] 欧盟《数据保护通用条例》中基本沿用了传统指令对于目的限定原则的规定,[40] 然而已有场景和风险要素的初步导向,如前言第(50)条指出,判断个人信息后续处理是否符合原始目的,“应评估后续目的与原始目的之符合性,尤其应考虑到与原始目的的关联、信息收集的原始场景(尤其是用

---

〔37〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec.4(a)(2)(A), sec.4(a)(2)(C), sec.4(b)(1)(D), sec.4(b)(2)(A), sec.4(n).

〔38〕 See, e.g., *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec.4(b)(2)(A).

〔39〕 See e.g., European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC (1995), art.6(1)(b); See also See Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), at 14.

〔40〕 See The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 – 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, art.5(1)(b).

户的合理预期)、个人信息的性质、后续处理行为可能引发的后果、信息的安全保障等等要素”。

美国《消费者隐私权利法案(草案)》中相关规定主要体现在“尊重场景”与“收集与利用限制”两条。如前所述,该草案以场景理念取代了传统目的限定原则,以“相应场景中合理”的标准[41]作为个人信息处理的合法性授权,以促进信息的合理利用。场景中合理标准的引入是该草案最大的亮点,其大幅扩展了个人信息处理的合法事由,有助于减轻机构合规负担,促进个人信息的流通及创新利用,同时更加侧重用户在具体场景中的隐私期待,是平衡信息价值开发及用户隐私保护的极佳路径。虽传统框架中对于“目的”的解释也日趋宽松,[42]然而二者的差别在于,场景理念从用户的接受度出发,强调合理性标准是个人信息处理符合用户的合理隐私期待,降低隐私风险,而并非僵化审视与原始目的的“符合性”,就此意义而言,场景理念是对目的限定原则的超越与升华。然而与此同时应当指出,该草案虽然详细列举了场景构成要素,但对于“合理”性判断标准并加以明确规定,也未加以方向性引导。如前所述,场景由多元因素构成且各因素影响力不同,需要综合考量及评估,因而是否具备合理性的判断十分复杂。虽然可以期待在后续施行细则中加以明确,但仍然会造成法律适用方面极大的不确定性,此亦为该草案受到诟病的主要原因。正如联邦交易委员会委员柏瑞尔(Julie Brill)所言,该草案过分依赖于业界后续制定施行细则,影响了本身规制力的发挥。[43] 与此同时,该草案规定只有“不具合理性”的前提下才应进行风险评估,然而是否具备合理性的判断多元复杂,同样是“程度性”而非“是非性”的判断,并且是风险评估的结果而非前提。场景标准的设立体现了个案分析精神,但关于合理性的判断方式本身却陷入二分法局限。是否具备合理性的判断同风险评估具有内在一致性,风险评估应贯穿个人信息生命周期的全程,不应将二者割裂开来。总之,是否具备合理性的判断方式缺乏明确性,以及同隐私风险评估流程的割裂,是草案的重大局限。

信息最小化原则又称必要性原则,要求个人信息收集及后续利用应以实现特定目的

---

〔41〕 美国在 2010 年提出消费者隐私权法案的框架构想时,曾经将“场景”相关的标准阐述为“普遍接受的信息处理实践”,并列举为五种具体的类型,即:提供产品服务,内部运营,反欺诈,履行法定义务及维护公共利益以及第一方产品营销。其收到的社会各方反馈中,部分人士认为此规定过于僵化,会限制商业模式的创新,另一些则认为规定过于宽泛,使机构有机可乘,不利于个人信息的充分保障。美国联邦交易委员会采纳了各方的意见,将“普遍接受的信息处理方式”修改为“同信息互动关系的场景相一致”作为标准,成为《消费者隐私权利法案(草案)》中“在相应场景中合理”的前身。See FTC Report of 2010, F. T. C., Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers-Preliminary FTC Staff Report (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf, F. T. C., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, p. iv.

〔42〕 See generally Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 00569/13/EN, WP 203 (2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

〔43〕 Commissioner Julie Brill, *One Year Later: Privacy and Data Security in a World of Big Data, the Internet of Things, and Global Data Flows, Keynote Address Before the USCIB/BIAC/OECD Conference on "Promoting Inclusive Growth in the Digital Economy"*, F. T. C. Protecting America's Consumers (Mar. 10, 2015), https://www.ftc.gov/system/files/documents/public_statements/629691/150310uscibremarks.pdf.

的最小必要为限,留存不得超过特定目的所必需期限并在目的达成后及时删除。[44] 必要性原则是个人信息保护的"帝王原则",然而海量信息收集、留存与再利用成为常态的大数据时代,其合理性日益受到严重质疑。[45] 美国泰内教授(Omer Tene)甚至指出,信息最小化原则已不再是大数据时代的商业准则。[46] 欧盟《数据保护通用条例》继续沿用传统的信息最小化原则的规定,相较而言,美国《消费者隐私权利法案(草案)》对信息最小化要求的处理体现出积极的态度,规定在个人信息最初收集的目的实现后,机构应删除、销毁信息或对其进行去识别化处理,此规定同欧盟数据保护指令并无二致,[47] 然而在整体以场景贯穿的同时,此款规定却拉回到"原始收集的目的",不失为遗憾之处。此外,在收集及利用的过程中合理地控制隐私风险,将隐私风险降低到相应场景中的最小程度,同样是信息最小化原则在大数据时代的新体现。

此外需指出,美国《消费者隐私权利法案(草案)》中多处体现了对个人信息利用环节的关注,如规定信息用于反欺诈、侦查等情形的排除适用,又如应避免信息用于对用户的差别化待遇等,[48] 体现应对大数据分析引发歧视待遇威胁[49] 的尤为可贵价值的导向;再如规定个人信息用于备份且不在日常获取范围内时,可排除删除规定的适用,[50] 体现出对不同利用目的的区别对待。以利用目的为考量对信息留存加以差别化规定,不失为对信息最小化原则的新解读做出的重要贡献。

(三)用户控制与透明度

传统架构对用户控制与透明度有着严格的法律规定,然在实践中由于缺乏可操作性,用户权利几近架空,[51] 诚如美国施瓦茨(Paul M. Schwartz)教授所言,隐私保障"承诺太多,兑现太少"。[52] 欧盟《数据保护通用条例》与美国《消费者隐私权利法案(草案)》同样

---

〔44〕 Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), pp. 7 - 8; European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC (1995), art. 6 - 7.

〔45〕 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp, p. 5. See also Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 260 (2013).

〔46〕 Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 260 (2013).

〔47〕 European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC (1995), sec. 104(b), art. 6(c).

〔48〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 104(b), sec. 4(n), sec. 103(d).

〔49〕 See, e.g., Neil M. Richards & Jonathan H. King, Three Paradoxes of Big Data, 66 *Stan. L. Rev.* 41 (2013), p. 43.

〔50〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 4(e).

〔51〕 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp, p. 2.

〔52〕 See Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 *Vand. L. Rev.* 1607, 1677 (1999).

高度重视用户对其个人信息的控制权利,却运用了迥异的路径,前者继续强化在实质意义上已经日益失效的知情同意原则,大幅抬高构成有效用户同意的标准,后者则在扭转思路、提升用户权利实质性方面做出了诸多有益尝试。美国《消费者隐私权利法案(草案)》第 4 条(d)款定义"用户控制"为用户享有的对其个人信息处理行为做出决策的能力,包括但不限于做出与撤回同意、更正有误信息、对信息获取的授权及限制,以及其他实现个人偏好的方式。[53] 其规定与欧盟指令无显著差异,[54] 但突出强调了尊重用户"隐私偏好",[55] 体现出以用户为中心的理念,在"用户控制"、"透明度"及"获取与更正"条款中均有对用户控制及用户权利的集中规定。

1. 透明度

透明度是用户行使权利的前提,有助于增进用户安全感及信任,提升用户对信息处理的接受度,实现信息价值的最大开发,因而被泰内教授视为应对大数据时代隐私挑战的核心手段。[56] 美国《消费者隐私权利法案(草案)》将联邦贸易委员会报告中位列第二条的"透明度"提升至首位,其重视程度可见一斑。隐私声明是机构履行告知义务与提升透明度的重要方式,然其在传统机制中日渐沦为机构合规义务的"形式"要件,用户通常既不阅读亦不理解其内涵。[57]

欧盟《数据保护通用条例》虽认识到用户与第三方数据处理者直接联系缺失的困境,并在第 14 条对此做出了针对性规定,然而总体上仍沿袭传统指令的思路,未认识到其所面临的困境。美国《消费者隐私权利法案(草案)》则充分认识到此局限,强化了告知义务的要求,规定了实现透明度的"合理性"标准。虽然在理念上体现了以用户的接受度为核心的考量,然而在可操作性方面仍存在局限。首先,草案并未指明提升告知可操作性及用户理解程度的有效方式,在"尊重场景"条款中,对于"增强性透明度"的要求也只停留于机构应当"设计良好机制"[58] 以帮助用户实现有意义的控制,与合理性判断标准同样缺乏明确性规定。[59] 此外更为重要的是,告知义务的规定并未处理用户与第三方机构直接联系缺失的困境,在个人信息广泛经第三方传播与再利用的环境下,如何实现对用户有意义的告知,事实上,草案仍未走出传统架构,比如第 106 条(a)款规定了用户的获取权,相比

---

〔53〕 *Administration Discussion Draft*: *Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 4(d).

〔54〕 European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC (1995), art. 12, 14.

〔55〕 *Administration Discussion Draft*: *Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 4(d).

〔56〕 See, e.g., Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 256 (2013).

〔57〕 Ira S. Rubinstein, *Big Data*: *The End of Privacy or a New Beginning*? NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp, p. 2.

〔58〕 *Administration Discussion Draft*: *Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 103(b)(1).

〔59〕 相较而言,欧盟倡导"层级化"告知(layered notice)的理念,推动"即时性告知"(just-in-time notice)等更为有效的方式,不失为良好尝试。

于欧盟《数据保护通用条例》第 15 条的无差别性规定,美国草案特别强调通过具体评估个人信息处理的隐私风险、对用户的不利影响及信息获取成本等因素,决定用户获取的程度与方式。[60] 此规定虽在表面上限缩了用户的获取权,然在实践中有助提升用户获取信息的效率,朝向获取权的真正落实迈出可贵进步。与此同时其同样存在未指明实现的有效机制、未涉及如何与第三方信息处理者建立有效关联的局限。

2. **用户同意**

欧盟指令为代表的传统机制过度依赖用户同意作为个人信息处理的合法性授权,然而如前所述,用户同意通常无法有效行使,实质上架空了用户的权力。

欧盟《数据通用保护条例》虽然在用户同意的可操作性方面做了积极倡导,大幅强化了构成有效用户同意的标准,然其最大局限在于,并未认识到知情同意机制本身存在严重的局限性,在大数据时代已经日趋失效,因此未能克服用户同意作为传统架构核心的局限性。相较而言,美国《消费者隐私权利法案(草案)》在界定用户同意的法律地位方面做出了关键性革新。相对于欧盟指令及该草案中作为对个人信息处理的核心授权手段,用户同意在草案中退为补充性机制。根据第 103 条(b)款,当个人信息处理行为不合理时,机构需要评估所产生的隐私风险,并采取相应的降低风险手段,包括但不限于提供增强性的披露及用户控制机制,当机构处理行为在相应场景中合理时,无需经过用户同意或满足其他要件而自动获得合法性授权,相比于传统架构过分依赖与架空用户同意[61]的局限,草案大幅减轻了机构及用户的负担,也将关注的重心集中于风险较高的个人信息处理行为,更多关注个人信息如何利用这一实质性问题,而非是否获取了用户的同意,提升了用户控制的实质意义。然而,草案的思路也有显著局限,其规定的在场景中不合理时所应采取降低风险的手段存在突出的路径性问题。首先,用户选择机制的默认设置存在局限。不同于欧盟指令及《数据保护通用条例》中主动、明确同意的要求,[62] 草案中的用户控制[63]更倾向于择出机制(opt-out),第 103 条(b)款规定,个人信息处理行为产生不合理的隐私风险时,机构应为用户提供控制或选择机制,虽未明确规定同意的具体机制,仍可推断为默认用户若不反对即视为对信息继续处理的授权。同意的默认设置至为关键,[64] 择出机制虽有助于减轻机构负担,促进信息的流通与开发,然而在用户同意的行使范围已经由“不合理”的前提被大幅限缩的情况下,用户做出主动同意亦不会为自身及机构带来不合理

〔60〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 106(a)(1).

〔61〕 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning*?, NELLCO Legal Scholarship Repository 2, http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp, p. 2.

〔62〕 See Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 01197/11/EN, WP 187 (July 13, 2011); See also 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 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri = CELEX:32016R0679&from = EN, art. 4 (11).

〔63〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 103(b)(1).

〔64〕 Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 256 (2013).

的负担。草案中择出机制的设置,无疑会影响用户权利的有效行使,使用户面临更大的隐私风险。因此,此处更宜规定用户的“择入”机制。第二,更为重要的是,草案将降低隐私风险的途径主要寄托于强化告知及获取同意,即通过用户控制而非机构采取措施来降低风险,实质是将个人信息处理的风险转嫁给用户。〔65〕 在个人信息处理产生不合理的风险时,机构应主动采取降低风险的措施,或为用户提供降低高风险要素的可操作性机制,而非强迫用户做出“接受”与“不接受”的选择,从而重新陷入“全有全无”的路径困境。

综上所述,对用户同意作为个人信息处理授权的态度差异,构成了欧美立法改革的核心差距。欧盟《数据保护通用条例》进一步提升用户同意的标准,强化用户同意作为合法授权的作用,美国《消费者隐私权利法案(草案)》则融入了场景与风险分析的新理念,以用户接受度及隐私风险为标准审视个人信息处理行为是否得当,是大数据分析盛行的商业模式下极富指引意义的改革方向。然其最主要局限在于,一方面未能针对用户权利难以行使的困境提出可操作的建设性方案,另一方面过分依赖用户的授权或默示同意作为降低风险的手段,草案也由此因未对用户信息提供充分保护而遭到各界诸多质疑。

(四)第三方信息处理机构责任

在多元主体的个人信息生态系统中,第三方信息处理者尤其是数据中间商的地位日益凸显,增加了个人信息利用尤其是二次利用的隐私风险,同时由于其缺乏与用户的直接关联,导致用户权利难以有效行使。与此同时,数据处理活动的纷繁复杂性,使得传统架构中的“数据控制者”与“数据处理者”日益难以明确区分。鉴于第三方信息处理机构的突出地位及产生的隐私影响,其责任与义务有待充分明确。欧盟《数据保护通用条例》未能突破传统架构的局限,而是继续强化了“数据控制者”与“数据处理者”的概念及义务划分,但并未就二者的区分给出切实可行的指引。事实上,大数据时代的个人信息生态系统中已不适宜做出此种区分,控制者与处理者的区分徒劳无功,无益于各方主体责任义务的明晰以及个人数据的有效保障,因而无益于解决传统架构的困局。然而值得一提的是,该条例的一大亮点在于,通过引入风险管理的要素,对数据控制者及处理者的义务采取了差分化的规定,对可能引发高风险的处理行为增加了附加性义务,反之风险程度低时豁免部分义务,为个人信息保护的未来实践及监管昭示了难能可贵的方向。相较而言,美国《消费者隐私权利法案(草案)》在此问题上未能提出建设性方案,联邦交易委员会报告曾极力倡导对数据中间商的义务予以专门的立法性规定,〔66〕然而遗憾的是此番发布的草案并未对此做出有效回应,使得多方利益主体的期望落空。回顾草案条文,虽然第 4 条(k)款(1)项将用户与处理信息机构的“直接关联”纳入场景要素加以考量,然而纵观各项规定,其对数据中间商的义务并未加以充分明确,在规定用户权利时,亦未充分考量面临多重关系给用户权利的行使带来的困境,因而在增强用户控制方面未能提出建设性的方案。此

〔65〕 Gabriel Maldoff, *The Risk-Based Approach in the GDPR: Interpretation and Implications*, https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf, p. 8.

〔66〕 F. T. C., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, p. ix, 14.

外值得一提的是,草案中关于机构的安全与隐私维护责任做出细化规定,规定责任原则包含实施内部审计、评估及三方审计等。[67] 笔者认同此规定,并认为需进一步细化,如规定机构应根据自身的规模及状况建立适当的个人信息保护政策、隐私管理体系及标准化操作流程等等。[68]

(五)个人信息的跨境传输

大数据时代,经济全球化及互联网的无国界性使得数据高度互联互通成为必然需求,个人信息的传输利用日益打破国家与地域的限制,与此同时,由于各国个人信息保护立法存在显著差异,不同法域间管辖权分立及冲突加剧,数据本土化立法不断出台,均为机构的数据跨境传输带来严重负担与障碍。保障隐私前提下的数据充分流通是经济发展创新的源泉,消除个人信息跨境传输中的不合理障碍也成为亟待落实的目标。纵观美国《消费者隐私权利法案(草案)》的规定,尽管白宫白皮书曾对跨境传输问题做出重点陈述,[69]倡议增进国际协作,促进搭建国际通用的个人信息保护框架,建立健全国际通用的认证机制,由业界联合制订施行细则,同时加强各国在执法领域的协作,为个人信息跨境传输指明了良好方向,然而草案各项规定中却并未对此迫切需求做出回应。相较而言,欧盟《数据保护通用条例》在个人信息跨境传输方面做出一定改进,在传统的机制的基础上,特别增设了隐私标章(Privacy Seal)、三方认证(certification)机制和认可行为指南(code of conduct)的效力,在法律上认可了企业自律及行业监督的重要意义。

综上,欧美立法通过引入场景与风险要素,均对传统困境做出了一定程度的回应。相较而言,欧盟法改革法案虽然引入了场景与风险的理念要素,然而总体架构上依然承袭了传统理念,未能对传统困境做出有效回应,也未能突破传统架构的困境。美国法的路径在各环节中融入了场景理念的导向,有重要的指引性意义,然其距传统困境的充分解决仍有待进一步完善:个人信息定义方面未充分强调其场景依赖性,目的限定原则方面未明确合理性的判断标准,在用户控制方面未能指明有效可操作的机制,机构责任认定及跨境信息传输方面未加以明确应对。虽然欧美个人信息保护的立法制度与改革路径各异,然而在探索应对传统困境的新思路时,二者却高度趋同地转向了场景与风险导向的理念。事实上,场景与风险导向的思路已成为国际立法的改革的趋势。可以预见,在大数据时代的个人信息保护机制改革与重构中,场景与风险导向的理念势必将发挥日益关键的作用。

四 以基于场景的风险管理重构个人信息保护新路径

鉴于欧美数据保护改革法案中场景与风险理念的优越性及局限,笔者在此基础上初

---

〔67〕 *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, The White House, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, sec. 107.

〔68〕 See generally Russell R. Densmore, Privacy Program Management: Tools for managing Privacy within your organization (2012).

〔69〕 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 – 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, pp. 123 – 126.

步提出建立以基于场景的风险管理为核心的新路径,囿于篇幅,以下仅以传统个人信息保护困境的应对为主线,对场景与风险导向的新路径加以概括说明。

(一)个人信息的定义

个人信息定义的最大困境源自个人信息与非个人信息二分法[70]的路径局限。信息的性质是动态的,无法脱离相应场景做抽象判断,[71]加之联邦交易委员会报告所言,隐私保护的范围已远超出严格定义的"个人信息",一切有关个人或由个人产生的信息均可能造成隐私风险,因此均需要得到相应程度的保护。[72] 实质上,个人信息的范围并不存在一个"预先"的精准界定,个人信息的界定是动态的,并高度依赖于所处的具体场景。[73] 欧盟《数据保护通用条例》并未认识到传统架构的局限,美国《消费者隐私权利法案(草案)》虽在个人信息的连结性定义与除外条款的规定中体现出场景与风险理念,但仍未充分强调个人信息的判断只在具体场景中方有意义,亦未指出应在相应场景中具体评估隐私风险,因此在此意义上,欧美法路径均未跳脱个人信息定义二元化的局限。

然而除此之外更应指出的是,个人信息的处理是否给用户带来隐私风险的原因并非来自其"是否构成个人信息",而是在具体场景中"被如何使用"以及是否符合用户在相应场景中的合理期待。换言之,信息性质的判断远非"目的",信息处理行为的隐私风险方为衡量机构责任的最终标准。因此,应舍弃探寻个人信息精准定义的路径,转而将关注重心由信息收集阶段转向信息利用阶段,即评估信息在具体场景中的使用引发的隐私风险。当隐私风险较低或在相应场景中合理时,即便信息构成个人信息,机构也仅需承担少部分的义务,有助于减轻机构负担,克服信息性质判断的不确定性,提升个人信息保护水准,同时促进信息的合理利用与充分开发。进一步而言,在场景与风险导向的个人信息保护架构中,应淡化个人信息定义,弱化个人信息与非个人信息在前端收集阶段的区分,将关注重心转向个人信息的使用环节,评估其在不同用途及场景中引发的隐私风险,由此确定机构相应的义务。

(二)目的限定与信息最小化原则

在目的限定与信息最小化问题上,欧盟《数据保护通用条例》沿用传统路径,美国《消

---

〔70〕 Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 258 (2013).

〔71〕 个人信息高度依赖于场景的特征已在国际间日益得到认同。See, e. g., Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 256 (2013). See also Paul M. Schwartz & Daniel J. Solove, Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 *Vand. L. Rev.* 1607, 1677(1999); 另参见刘定基:《个人信息的定义、保护原则与个人信息保护法适用的例外——以监控录像为例(上)》,《月旦法学教室》2012 年第 115 期,第 42 - 54 页。

〔72〕 F. T. C., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, p. 19; See also Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 259(2013); Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA L. Rev.* 1701(2010).

〔73〕 See, e. g., The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 - 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, p. 110.

费者隐私权利法案(草案)》则采用场景中合理的标准取代目的限定原则,在具体场景中评估信息处理行为的合理性,然而如前所述,其最大局限在于仍未能明确合理性的判断标准,同时将合理性判断与风险评估截然分开,为机构在适法性方面带来相当的不确定性及合规负担。建构场景与风险导向的个人信息保护新路径,根本出发点在于明确个人信息处理合理性判断根本上取决于其引发的隐私风险,即所造成的隐私风险是否符合用户的合理隐私期待,或是否对用户造成不合理的负面影响,而判断隐私风险的方式即为隐私风险评估。因此,评估应贯穿个人信息处理各个环节的始终,作为个人信息处理合法性授权,以及机构履行相应义务的前提。因此,为进一步明确合理性的判断标准,应在“合理性”标准基础之上,将其延伸为“风险限定”的导向,即个人信息的处理不能引发高于原有程度的、用户无法预期的风险。风险限定导向体现了场景及风险理念的内涵,并直指个人信息处理合理性的核心判断标准,因而更富指引意义与明确性。

如前所述,隐私风险评估作为评估隐私风险的工具与标准操作流程,已成为国际上普遍认同的理念与最佳实务。根据评估结果,可划分个人信息处理的风险等级,例如采取欧盟《数据保护通用条例》的路径将风险程度划分为高、中、低三级,具体划分风险的方式,机构可结合自身状况与行业最佳实务中加以明确。相比于美国《消费者隐私权利法案(草案)》的模糊规定,以实践中业已成熟的隐私风险评估工具评估信息处理风险性与合理性,有助于为机构的实践提供更加明确可依循的指引,与此同时可结合行业最佳实务等加以灵活调试的标准,同时留出了柔性缓冲的空间。

此外,在对传统架构的重新审视中,信息最小化原则或必要性原则仍不失为核心指导理念,然其在大数据时代海量信息留存与开发的背景下需要作出重新诠释。场景与风险导向的新架构不应再苛求将信息的收集、利用保持在最小必要的范围,而更意味着机构必须将个人信息处理所引发的风险控制在实现特定目的所必须的合理水平,即机构对个人信息进行后续利用时,应将其引发的隐私风险降至实现目的最低水平,个人信息的二次利用不应提升信息原初的隐私风险或给用户带来无法预期的隐私损害。尤其是,当个人信息用于统计分析、提升服务等“无辨识特定个人必要”的用途时,机构应当采取匿名化处理等合理方式,尽量降低对用户带来的隐私风险。与“风险限定”取代“目的限定”类似,在大数据时代,应以“风险最小化”取代“信息最小化”作为机构处理个人信息所应遵循的准则。鉴于现代信息处理商业模式的重心已明显由个人信息的收集环节转向使用环节,信息最小化原则亦应由收集环节的节制转向使用环节的节制。

(三)用户控制与透明度

传统架构中,用户控制与透明度难以操作使得用户权利几近架空,欧美法均未提出切实可行的操作机制,尤其未针对用户与第三方机构联系缺失的困境指明正确方向。诚如学者兰道所言,为实现个人信息的有效保护,应当越过知情同意这一已然失效的中间机制,转而着眼控制个人信息的利用环节,使其更符合用户的隐私偏好与期待。[74]

在大数据时代,落实用户控制,提升信息处理的透明度,首先应以场景导向为核心贯

〔74〕 Susan Landau, Control use of data to protect privacy, 347:6221 *Sci. Issue* 504,504 (2015).

穿用户控制与透明机制的重构。以场景各构成要素为指引,着重针对引发高隐私风险的因素进行披露,[75]如信息是否用于构建人格图像,或对用户做出不利性决定等等,并为用户提供相应的控制机制。机构可根据具体场景中评估出的隐私风险等级,设计层级化的透明与用户控制机制。例如,风险等级为低时,机构无需主动披露及提供用户控制机制;风险等级为中时,机构可向用户披露高风险因素并提供"择出"的控制机制;尤应注意在风险等级为高时,机构应向用户提供"即时性披露"等增强性告知机制,并为用户提供"择入"的控制手段,主动采取措施降低风险,方能促成用户控制的真正落实。

第二,针对海量信息在用户不知情的状况下收集、用户与第三方信息处理者关联缺失的情况,应强化个人信息处理主体的责任意识,加强第三方信息处理机构与用户的间的联系,第三方机构应当主动向用户披露信息处理状况及提供控制机制。

第三,充分运用隐私架构设计(Privacy by Design),[76]"隐私友好型"的技术架构设计能够延伸用户的控制范围,[77]增加透明及用户控制的可操作性,也是欧盟改革法案中大力倡导的理念。例如机构可以场景构成要素为指引,进行技术架构设计,使用户对高风险要素清晰可见;以"个人信息云"为典型的技术设计方案,有助于用户获取权的落实;"元数据标签"[78]设计能伴随个人信息的整个生命周期,记录信息收集、利用及传输的全过程,使用户有机会详细掌握其信息的利用状况与流程。隐私设计使得信息流转更加透明,调动用户参与信息生命周期的积极性,扭转用户在个人信息生态系统中的弱势地位,同时有助于信息价值的开发,甚至能够衍生出新的商业模式。

鉴于用户对于其信息使用的偏好有所差异,个人信息保护的程度即便经过场景审查与隐私影响评估,也有可能无法兼顾个别用户的需求。因此,增强用户控制与个人信息处理的透明度,使用户能及时获取与控制信息处理状况,有助于对不符合用户期待的处理行为提供及时的调试与救济渠道,也为个人信息的流通与开发提供屏障。

(四)第三方机构责任

数据驱动型商业模式中用户与第三方机构直接关联的缺失,导致对个人信息后续流通使用环节规制不足,用户的知情及控制亦难以有效行使。传统架构中已经难以寻求规制第三方机构责任切实可行的方案。欧美改革法案虽体现出对对此问题的关注,然均未

---

〔75〕 除此之外,有学者亦大力提倡,机构应披露及公开其做出自动化决策所依据的标准,以克服自动化决策带来的人格权损害及歧视化待遇。See Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 271 (2013). See also Neil M. Richards & Jonathan H. King, Three Paradoxes of Big Data, 66 *Stan. L. Rev.* 41,43 (2013).

〔76〕 Ann Cavoukian, 7 foundational principles, https://www.privacybydesign.ca/content/uploads/2009/08/7foundational principles.pdf.

〔77〕 See The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 – 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, p. 106.

〔78〕 See, e.g., Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning*?, NELLCO Legal Scholarship Repository 2, available at http://lsr.nellco.org/cgi/viewcontent.cgi? article = 1359&context = nyu_plltwp, p. 10. See also Carolyn Nguyen et al., A User-Centered Approach to the Data Dilemma: Context, Architecture, and Policy, *in Digital Enlightenment Yearbook 2013: The value of personal data* (M. Hildebrandt et al. eds., 2013).

提供针对性的切实可行之方案。对于第三方信息处理机构监管真空的困境,场景与风险导向的新方案能够在三方面提供思路。

首先,建立“使用者责任”机制。传统机制根植于个人信息直接收集的场景,无法适应大数据时代信息多元流转与后续使用的需求。适应去中心化个人信息生态系统的新架构应将关注重心由个人信息收集转向使用阶段,强化责任原则,建立“谁使用谁负责”的“使用者责任”机制,对于引发一定风险的个人信息处理行为,均统一进行风险评估以确定相应的保障责任,而不论机构是否与用户有直接联系。“使用者责任”机制能无差别地覆盖信息生态系统中的多元主体,无论第一方机构或第三方机构、数据控制者抑或数据处理者皆适用此框架,同时端到端地覆盖个人信息生命周期的各个环节,因而有效应对传统机制对第三方机构监管真空的困境,在个人信息生态系统中更好地规范多元主体的行为,建立大数据时代良好的个人信息保护新秩序。

其次,突出第三方数据处理者的独立法律地位。联邦贸易委员会报告倡议对数据中间商建立针对性立法,明确及突出其责任,同时建议第三方信息处理者提供增强的透明度,如建立专门的网站向用户揭露其身份,并说明信息处理状况及用户权利的行使方式,以此加强自律及与用户的联系。[79] 在个人信息生态系统中,用户隐私的合保障及用户信任的维护要求机构增强自律及责任感。由于面向消费者的第一方信息收集者收集大量用户信息并与用户建立直接的密切关联,报告倡议其承担起信息管理者的责任,[80] 通过与下游流转的第三方处理者明确责任义务,确保用户的隐私的保护维持在同等水平,同时向用户强化对第三方信息处理者身份的披露。

最后,通过技术架构设计强化用户控制。如前所述,良好的技术架构设计能够延伸用户对信息的控制,有助于促进用户偏好在第三方信息处理者处得到同样的尊重。例如“元数据标签”的方案能够将相关的用户偏好及对信息处理的预期绑定于信息生命周期的始终,因而个人信息处理的原始场景在其后续流通与利用中依然能够得以保留。

(五)个人信息跨境传输

随着经济全球化的发展,个人信息的流通日益打破国界限制,[81] 个人信息保护法律政策在区域间的显著差异,造成了机构合规方面的严重负担,严重阻碍个人信息的跨区域传输及价值的开发。联邦交易委员会报告对此亟待解决的问题虽做出了重点强调,然而正式颁布的《消费者隐私权利法案(草案)》讨论稿却并未对此做出回应。在国际上,虽然

〔79〕 F. T. C. , Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www. ftc. gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, p. v.

〔80〕 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 - 142 (2012), http://www. whitehouse. gov/sites/default/files/privacy-final. pdf, p. 105; See also F. T. C. , Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www. ftc. gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

〔81〕 F. T. C. , Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), https://www. ftc. gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, p. 22.

在安全港协议宣告失效后,欧美新的隐私盾协议已经正式颁布并预期生效,然而欧美间的数据传输仍不容乐观,面临重重困境。由于文化背景与社会习俗的差异,各国公民对待信息处理的态度与接受度有所不同,构成了各国法律难以完全协调融合的根源。世界经济论坛报告通过对影响用户接受度因素的量化调研,更加直观地呈现了用户接受度的显著地域差异。〔82〕

扫清跨境流通的障碍,为个人信息的无障碍流通打开通路,同样应从场景与风险管理的理念入手。场景构成要素即风险评估具体指标的可拆分性与可调节性,决定了其富有灵活性及包容性,通过对具备国际普适性价值的尊重,同时对具有地域差异性的要素(如用户对个人信息使用收益的态度等)的调试,使世界不同地区的个人信息处理行为能够被纳入统一的风险评估体系之中,由此使得国际间通用的个人信息保护架构的构建成为可能。〔83〕

与此同时,为促进区域间个人信息的无障碍传输,应积极推动健全既有的跨境传输机制(如 BCR 等)与国际框架(如《消费者隐私权利法案(草案)》等),加强各国个人信息保护权力机构间的执法协作。此外落实责任原则,着重以"组织机构"为核心明确相应的个人信息保护义务,大力倡导三方认证制度。在此尤为值得指出的是,无论是亚太跨境隐私保护规则(《消费者隐私权利法案(草案)》),还是欧美最新通过的"隐私盾"协议,究其本质而言,皆为在法律上得到认可的第三方认证机制,可以预见,建构在"可信第三方认证"基础上的数据跨境传输势必成为未来发展的主流方向。总而言之,在基于场景的风险导向框架下,通过尊重共同价值与调试差异性因素,能够搭建其协调各国个人信息保护法律制度的桥梁,从而在用户信息保护与数据自由流通间探索出一条双赢路径。

综上所述,以依托场景的风险管理理念构建个人信息保护新思路,对传统框架进行重构,有助于破解传统机制的困境,在大数据时代实现隐私保护与信息开发的双赢。隐私影响评估不仅是欧美法案新增的法定义务,也可作为机构履行保障义务的证明及法律责任界定时的抗辩事由,更是机构用以主动识别及控制风险的极佳工具。运用评估工具,有助于提升信息处理的透明度,减轻机构负担,提升用户的实质控制能力,乃至搭建个人信息在境内外不同主体间高效传输的桥梁。大数据时代,运用基于场景的进行风险管理的新理念,是协调公民权益保护及数据价值开发的极佳路径。

五 对我国个人信息保护立法与实践的建议启示

纵观欧美个人信息保护立法改革,虽《消费者隐私权利法案》尚未形成正式版,《数据

〔82〕 以对地理位置信息的收集为例,我国用户的接受度几乎是西方发达国家的五倍。See The World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf, pp. 6 - 7.

〔83〕 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, J. of Priv. and Confidentiality 2, 95 - 142 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, p. 123.

保护通用条例》也未正式生效,然二者业已在国际间引发广泛关注,对我国构建大数据时代的个人信息保护机制亦具有重要启示意义。

近年来我国政府对公民的个人信息保护日益重视,《刑法》修正案、《消费者权益保护法》修正案及《网络安全法》(草案二次审议稿)中均新增了对个人信息保护的规定,《关于加强网络信息保护的决定》[84]及《电信与互联网用户个人信息保护规定》[85]初步建构了个人信息保护的指导原则,与此同时出台《信息安全技术公共及商用服务系统个人信息保护指南》等指导性国家标准,[86]行业机构也通过推行自律标准等方式不断加强自律。[87]可以看出,当前我国初步构建了个人信息保护体系,然而个人信息滥用问题依然严峻,数据黑产盛行,电信诈骗猖獗,严重影响公民的正常生活和社会秩序,制定统一的《个人信息保护法》的呼声强烈。然而笔者认为,除完善立法体系外,更应冷静思索立法路径本身的局限。特别值得指出的是,我国今年五月颁布的《网络安全法》(草案二次审议稿)[88](以下简称《网络安全法》(草案二审稿))对个人信息保护部分作出了多项规定,然而总体上仍然保留着传统知情同意架构的浓重色彩,恐怕难以实现公民权利保护与大数据产业发展的有效平衡。

如前所述,以欧盟指令为代表的传统架构面临全面困境,不仅在执行方面困难重重,无益于公民隐私的有效保护,更会给企业带来沉重的合规负担,严重阻碍数据价值的开发,制约数据经济的长足发展。在立法路径上面,笔者强烈建议,应充分认识到欧盟数据保护指令及《数据保护通用条例》中知情同意架构为核心的传统路径的局限,将基于场景的风险管理理念贯穿于个人信息保护的立法与执行之中,以适应大数据时代的发展需求。在具体制度建议方面,以下主要以我国《网络安全法》(草案二审稿)为例,结合法律规范相关规定,分析我国个人信息保护立法路径的局限,并提出方向性的建议。

第一,在个人信息定义及法律适用范围方面,草案定义公民个人信息为"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公民个人身份的各种信息,包括但不限于公民的姓名、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",在实务中会造成个人信息界定困难的困境,同时未能强调个人信息的"关联性"特征,更未能点明个人信息高度依赖场景的动态性。在此建议界定个人信息为"能够识别或关联到特定个人的信息",并强调信息在相应场景中的处理行为被用于或可能用于回溯到特定个人之目的,或可能给个人造成差别性待遇及隐私影响,与此同时通过规定"排除事由"或者"适用例外"的场景豁免相关法律义务。此外更为关键的是,应当扭转单纯依赖个人信

〔84〕 全国人大常委会:《关于加强网络信息保护的决定》,http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm。

〔85〕 工业和信息化部:《电信与互联网用户个人信息保护规定》,http://www.gov.cn/gzdt/2013-07/19/content_2451360.htm。

〔86〕 国家标准化委员会:《信息安全技术公共及商用服务系统个人信息保护指南》,http://www.pkulaw.cn/fulltext_form.aspx?gid=221035。

〔87〕 例如,2016 年 7 月,数据中心联盟联合阿里巴巴、京东、360 等八十余家企业共同制定并发布了《数据流通行业自律公约(第二版)》,促进数据流通领域的行业自律。

〔88〕 全国人大常委会:《网络安全法》(草案二次审议稿),http://www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm?from=timeline&isappinstalled=0。

息定义作为法律适用前提的思路,规定但凡造成隐私风险的大规模信息处理行为,均应适用个人信息保护相关规定,即便处理的信息被界定为传统意义上的“非个人信息”或“匿名信息”。

第二,在目的限定原则方面,草案规定“网络运营者收集、使用公民个人信息,应当遵循合法、正当、必要的原则,明示收集、使用信息的目的、方式和范围”,《电信和互联网用户个人信息保护规定》第九条指出“电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的”,依然采取传统架构中严格遵循“目的限定”的思路。建议灵活适用目的限定原则,融入以场景及风险的理念,变“目的限定”为“风险限定”,规定目的的符合性应该具体评估是否带来了超出原始收集时的风险。如果数据的后续处理未超出原来的风险,并且符合用户的合理预期,即使传统意义上“不符合”原始的目的,也可以认定为“合理使用”,无需另行获取用户授权。

第三,在透明度与用户控制方面,草案第四十条规定,“网络运营者收集、使用公民个人信息,应当遵循合法、正当、必要的原则,明示收集、使用信息的目的、方式和范围,并经被收集者同意”。《电信和互联网用户个人信息保护规定》第九条也规定,“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”。这种“一刀切”式的获取用户同意的思路,同样沿袭了以用户同意为主要授权手段的传统路径。在新路径的指引下,我国应积极融入风险评估的导向。具体而言,在提升透明度方面,提升用户控制与透明度的有效性及可操作性,规定机构应重点披露引发高风险的场景构成要素,并为用户提供便于操作的控制手段;在用户控制方面,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风险评估,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,减轻为机构及用户自身带来的负担;在“不合理”或引发的风险程度高时,规定应以显著的方式确保用户知悉引发高风险的要素,并主动采取降低风险的手段,或者取得用户明确、主动的同意作为继续处理的合法授权。

第四,在多元主体责任界定方面。我国现行立法体系中尚未对多元主体责任做出明确界定,数据中间商等主体的法律适用及责任界定尚不清晰。以新理念的角度切入,应淡化传统框架中的“数据控制者”和“数据处理者”的区分,将各方主体统一纳入风险评估的机制。突出第三方主体独立的法律地位,尤其强调个人信息后续处理者和“数据中间商”的责任,规定以“隐私风险”为标准确定各主体的差别化义务。具体而言,可将隐私风险等级分为“高”、“中”、“低”三级,并界定相应等级的保护义务,无论数据处理的主体为何种地位、处于何种数据处理环节,均统一通过评估出的风险等级纳入管理体系。

第五,在数据跨境流动方面,当前我国尚未构建起系统的管理机制,在统一立法层面仅在《网络安全法》(草案二审稿)第 35 条中涉及了数据本地留存的机制。在国际上,除了积极参与“亚太跨境隐私保护规则”等国际框架,以及进行国际执法协作之外,我国应首先建构起体系化的数据跨境流通管理机制,规定数据跨境数据流通应进行基于场景的风险评估,根据风险等级确立相应的管理手段,如风险低时允许自由流通,风险中时进行

流通方面的限制,风险高时原则上禁止跨境流通。从远期来看,以场景理念为主线,隐私风险评估为工具,能够推动国际间个人信息保护与数据传输的通用框架的构建与完善。

此外,在立法技术与监管机制方面,推进个人信息保护全面性立法及施行细则的出台,或可参考美国《消费者隐私权利法案(草案)》的模式建立“安全港机制”,鼓励业界根据立法原则自行拟定可操作的实施细则,并赋予法律强制力及免予直接执行立法条文的豁免权,以协调法律与制度的明确性与灵活性,调动多方主体的积极参与,同时提升法律实施效果。

信任是产业发展的基石,构建公平、信任的产业环境,是数字经济长足发展的基础。在大数据与互联网产业蓬勃发展的背景下,我国在个人信息保护方面能否形成合理、高效的制度设计,关乎公民权益的保护、用户信任的提升和产业的长足发展。当前世界各国均处于个人信息保护法改革与转型的关键时期,在欧美努力摆脱传统框架带来的困境时,我国更应清醒地认识到传统的架构已经走向穷途末路,应积极抓住大数据时代的历史机遇和宝贵契机,积极发展与新技术、新商业模式相适应的个人信息保护架构,避免重走西方国家积重难返的弯路,抓住“弯道超车”的契机,发挥后发优势,力争成为个人信息保护领域的规则制造者与潮流引领者。

[**Abstract**] Big Data analytics promotes new business models while at the same time seriously challenging consumer's privacy. The current data protection framework, built on the "notice-and-consent mechanism", is faced with serious dilemmas mainly in the definition of personal data, meaningful user control, data minimization, third party accountabilities, and cross-border data transfer. Since this mechanism is ineffective in today's world, there's growing trend of finding alternative approaches. Contextual and risk-based approach has gained worldwide recognition and been adopted in the Consumer Privacy Bill of Rights (CPBR) recently released by the US and General Data Protection Regulation (GDPR) approved by the EU. The contextual approach establishes "reasonable in light of context" standard as new authorization for data processing, which reflects the highly contextual nature of privacy and data protection. Risk-based approach requires case-by-case privacy risk analysis and avoids unreasonable privacy risk caused by data processing. But both the EU model and the US model fail to completely solve current dilemmas because of certain drawbacks. On the basis of these two models, a revised contextual and risk-based model is suggested that makes Privacy Risk Assessment an obligation throughout data processing life cycle. Varying data protection obligations according to privacy risk level while relaying on Privacy by Design, this new model aims to offer end-to-end privacy risk control as well as higher transparency and user empowerment.

(责任编辑:姚　佳)