■ 专　论　　文章编号:1001-2397(2023)01-0034-15

隐私政策的多维解读:告知同意性质的反思与制度重构

丁晓东

(中国人民大学 法学院,北京　100872)

摘　要:基于隐私政策的告知同意是个人信息保护的核心制度,但对其性质应当进行反思,对其制度应进行重构。告知同意在不同国家和地区具有合同、声明、基本权利合规等多重特征,在我国也应被视为多维制度工具。仅从意思自治角度看,告知同意面临信息过载、决策过频等难题,即使进行制度改进,也无法实现个体的充分知情和明确同意。但隐私政策的阅读对象不仅是即时交互场景下的个人,也包括企业内部人员、市场评级者、执法司法者和非交互场景下的个体。隐私政策可能充当信息处理者的合规章程、市场声誉信息机制的媒介、司法诉讼与行政执法的依据、赢取个体信任与进行隐私教育的工具。应解绑告知与同意,适度放松同意要求,但应强化对隐私政策的告知要求。隐私政策对外可以采取不同提醒方式与分层架构,对内应成为内嵌到不同部门与产品的合规指引,在形式上采取基于风险的模块化披露。

关键词:隐私政策;告知同意;个人信息;意思自治;公私法融合

中图分类号:DF529　　**文献标志码**:A
DOI:10.3969/j.issn.1001-2397.2023.01.03　**开放科学(资源服务)标识码(OSID)**:

一、问题的提出

告知同意是个人信息保护的核心制度。《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)将告知同意作为信息处理者处理个人信息的“一般规定”,其中第 13-18 条详细规定了告知同意制度,其他条款在不同场景对如何适用这一制度进行了规定。[①]稍早之前出台的《中华人民

收稿日期:2022-08-07

基金项目:最高人民法院 2022 年度司法研究重大课题“算法技术的法律规制研究”(ZGFYZDKT202211-01)阶段性成果

作者简介:丁晓东(1982),浙江淳安人,中国人民大学法学院教授、博士生导师,未来法治研究院副院长。

① 其他条款的规定包括委托处理个人信息(第 21 条);转移个人信息(第 22 条);向其他处理者提供个人信息(第 23 条);公开个人信息(第 25 条);公共场所收集个人信息(第 26 条);处理公开个人信息(第 27 条);处理敏感个人信息(第 29 条);处理未成年人个人信息(第 31 条);向境外提供个人信息(第 39 条)。

共和国民法典》(以下简称《民法典》)也将征得“自然人或者其监护人同意”作为处理个人信息的首要条件。[①]在域外,隐私政策与告知同意也扮演了重要角色。美国在20世纪60-70年代引入了公平信息实践制度,在若干立法领域要求收集个人信息必须向个人进行告知;到了20世纪90年代,随着互联网的兴起,企业纷纷采取隐私政策,逐渐成为通行做法。欧盟等其他地区虽然与美国市场化的模式不同,但在隐私政策与告知同意方面,也将其作为立法与规制的核心。[②]

基于隐私政策的告知同意的重要性毋庸置疑,但在基本原理与实践效果方面,却一直存在争议和批评。就其原理来说,告知同意在法律上应当如何定性,告知同意是一种格式合同吗?当信息处理者在其网站或交互界面上设置隐私政策,用户点击同意或继续使用,这一行为是否构成一种民事行为上的意思表示;相应地,当企业或个人违反隐私政策中的内容,这是否构成了传统合同上的违约;或者,告知同意是否是一种免责声明;或者,当信息处理者获得个人同意后,就构成侵权法上的违法阻却事由;又或者,基于隐私政策的告知同意是一种信息处理者的合规行为?[③]

在实施效果方面,基于隐私政策的告知同意也面临众多问题。例如,《个人信息保护法》中的告知同意、单独同意与书面同意的合规应作何种要求;对用户进行告知,是否可以将隐私政策放置在网站的某个链接中,还是需要使用单独弹窗形式;企业获取用户同意,应当采取选择加入(opt-in)还是选择退出(opt-out)模式?此外,有学者指出,告知同意面临“流于形式”的风险[④],个人信息主体常常没有时间、精力和兴趣阅读隐私政策,企业所获取的同意也常常不是用户的真实意愿。在告知同意制度饱受批评的背景下,如何改进和完善这一制度亟需明确。

为了分析上述问题,本文对告知同意制度的性质进行分析。本文认为,基于隐私政策的告知同意具有合规工具、声明与合同等多重特征,应采取公私法融合的多维视角对其进行分析,避免单一视角。在制度实施效果上,告知同意难以在即时交互界面实现对用户的有效告知,用户也面临无效选择与选择疲劳的困境,仅从意思表示的视角难以厘清这一制度。隐私政策的读者对象并不仅限于即时交互界面的个体,还包括企业内部人员、社会主体与市场专业人员、执法机构等主体。采取公私法融合的多维视角,可以发现告知同意可以作为企业内部合规的工具、市场声誉机制的信息媒介、司法执法的依据、信任沟通与隐私教育的工具。为重新激活告知同意制度,应解绑告知与同意,适度放松同意要求,强化告知要求。隐私政策应当依据场景,采取不同提醒模式与分层告知框架,隐私政策应内嵌到企业内部与产品合规中,并依据风险点而进行模块化设计。

二、告知同意性质的反思

反思告知同意制度的法律性质,有助于深化对告知同意制度的认识。借助比较法视野,可以发现,

① 《中华人民共和国民法典》第1035条。

② 王利明、丁晓东:《论〈个人信息保护法〉的特色、亮点与适用》,载《法学家》2021年第6期,第1-16页;Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 Minnesota Law Review 1733 (2021).

③ 高富平:《同意≠授权——个人信息处理的核心问题辨析》,载《探索与争鸣》2021年第4期,第87-94页;程啸:《论个人信息处理中的个人同意》,载《环球法律评论》2021年第6期,第40-55页。

④ 周汉华:《个人信息保护的法律定位》,载《法商研究》2022年第3期,第55页;Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 Pace Law Review 307 (2020).

美国有时将告知同意视为传统合同,但更多情况下将其视为类似产品说明书的企业声明;而欧盟整体将其视为公法基本权利的合规要求,但也具有一定的消费者合同的特征。《个人信息保护法》采取和欧盟类似的保护型的立法进路①,但和欧盟与美国都有所不同。无论是我国还是欧美,隐私政策都呈现公私法融合特征,是一种多维法律制度工具。

(一)美国:作为合同与声明

基于隐私政策的告知同意制度起源于美国。20 世纪 80-90 年代,互联网企业开始走出实验室,进入商业领域,随着互联网企业开始广泛收集个人信息,其对个人隐私的威胁引起了社会的关注。为了消除社会的担忧,同时,为了避免政府对互联网企业采取严厉的规制措施,互联网企业开始在其网站上设置隐私政策说明,在自由放任与政府规制之间寻求一条"自我规制"的中间道路。到 21 世纪初,几乎美国所有的互联网企业都自愿设置了隐私政策。②

在多数案件中,美国法院将告知同意视为没有传统合同约束力的声明(statement)。③例如,在 2005 年的一场集体诉讼中,西北航空公司在其隐私政策中规定,其收集的个人信息只用于特定目的,但实际上西北航空公司却与一家联邦机构共享大量消费者数据,用于研究航空安全。法院在该案件中否定了告知同意的合同性质。④在少数的案件中,法院将告知同意作为传统合同看待。例如,在 2005 年针对捷蓝航空(In re-JetBlue Airways Corp. Privacy Litigation)和针对美联合航(In-re American Airlines Inc. Privacy Litigation)的诉讼中⑤,法院认为,被告违反隐私政策的信息处理可以被视为合同违约。当然,只有在点击协议(clickwrap)或引起用户反复注意的浏览协议(browsewrap)中,美国法院才有可能将其视为合同。根据美国法院的主流看法,用户在这类协议中有机会浏览隐私政策,因此,可以将其视为合同。⑥而在浏览协议中,法院一般倾向于否定其合同性质⑦;只有浏览协议采取弹窗模式,显著提醒用户,法院才可能将其视为合同。⑧

(二)欧盟:作为基本权利的合规措施

欧盟采取个人信息基本权利保护的路径,将个人信息被保护权视为一种宪法基本权利。《欧盟基本权利宪章》第 8 条第 1 款规定:"每个人都有权保护与其有关的个人数据。"《一般数据保护条例》第 1 条第 2 款也规定:"本条例保护自然人的基本权利和自由,特别是其个人数据被保护的权利。"在这一背景下,欧盟整体上将设置隐私政策与获得告知同意视为公法基本权利的合规措施,但也在一定程度

① 张守文:《信息权保护的信息法路径》,载《东方法学》2022 年第 4 期,第 50-62 页;龙卫球:《〈个人信息保护法〉的基本法定位与保护功能——基于新法体系形成及其展开的分析》,载《现代法学》2021 年第 5 期,第 84-104 页。

② Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 Penn State International Law Review 587, 594 (2007).

③ 最新的实证研究,参见 Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 Yale Journal on Regulation 45-115 (2019). 更早之前,Oren Bar-Gill 教授的研究得出了相反结论,参见 Oren Bar-Gill et al., *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 The University of Chicago Law Review 7 (2017).

④ In re Nw. Airlines Privacy Litig., 2004 WL 1278459, at *5 (D. Minn. June 6, 2004); In re Nw. Airlines Privacy Litig., 2004 WL 1278459 (D. Minn. June 6, 2004).

⑤ 379 F. Supp. 2d 299 (E.D.N.Y. 2005); 370 F. Supp. 2d 552, 554 (N.D. Tex. 2005).

⑥ Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, Oxford: Oxford University Press, 2d ed., 2007, p. 242.

⑦ Stephen Y. Chow, *A Snapshot of Online Contracting Two Decades After ProCD v. Zeidenberg*, 73 Business Lawyer 267 (2017).

⑧ Cullinane v. Uber Techs., Inc., 893 F.3d. 53, 62 (1st Cir. 2018); Meyer v. Uber Techs., Inc., 868 F.3d 66, 75 (2d Cir. 2017).

上具有消费者合同的性质。

首先,欧盟法下的隐私政策并非传统合同或声明。如果说美国法上的隐私政策可以被视为市场中可以自由设计的合同或声明,具有自我规制的特征,那么欧盟法则排除了其市场化特征。在欧盟法上,信息处理者没有美国企业那样广泛自由设置隐私政策的权利,其隐私政策所规定的内容、告知的方式都必须符合法定合规要求。正如施瓦茨(Paul Schwartz)所指出,欧盟法的基本假设是,处理个人信息将对公民的人格尊严产生威胁,威胁"法秩序",因此,对个人数据保护在整体上采取了"信息不可让渡性"(information inalienability)的制度框架,将其视为一种不可交易与不可自由设定的人权。①

其次,欧盟法下的告知同意也并非侵权法上的免责事由或违法阻却事由。免责事由将告知同意视为过失相抵、受害人故意、第三人过错、自甘风险、正当防卫、紧急避险的行为,但告知同意仅仅是信息处理者合规的一环。信息处理者即使获得用户的明确同意,也可能因为违反"目的限制""数据最小化"等诸多原则而被认定违法。②正如库纳(Christopher Kuner)教授所言:企业总是痴迷于将告知同意视作为获取个人信息"提供充分法律依据的机制,但忽略了处理的法律依据",欧盟法所规定的数据处理的合法性基础"不是一项具体行动,而是一项重要原则,在公司合规计划的所有阶段都应牢记"。③

再次,欧盟在隐私政策的司法与执法问题上也采取了合规进路。当信息处理者的隐私政策不够清晰明确,或者其信息处理行为与其隐私政策存在不一致,其救济一般通过行政执法进行救济。个体也可以参与这一过程,可以向独立数据监管机构或法院提起申诉或诉讼,但这种申诉或诉讼都是依据基本权利的合规要求而提起,并非依据信息处理者违反合同而提起。④在信息处理者对个人造成损害的侵权诉讼中,《一般数据保护条例》也以违法性作为前置条件,即只有信息处理者违规的前提下,个体才能进行侵权之诉。⑤

最后,欧盟的隐私政策也具有一定的消费者合同特征。一方面,虽然欧盟坚持个人信息保护的基本权利特征,并且引入了"目的限定""数据最小化"等原则,但《一般数据保护条例》等法律仍然给予了个人与信息处理者一定的平等协商空间。例如,当信息处理者希望获取更多个人信息,以便为个人提供更多服务,此时信息处理者仍然可以在基础服务所需的个人信息之外,通过告知同意而获取更多个人信息。只不过,信息处理者不能通过"捆绑""搭售"等方式拒绝为个人提供基础服务,也不能拒绝个人的撤回权等其他权利。另一方面,欧盟也在很多地方借鉴了消费者保护法的规则,例如,《一般数据保护条例》"重述"第42条直接引用了《1993年关于消费者合同中不公平条款的理事会指令》,指出任何未经单独协商的合同条款,如果"导致合同双方的权利和义务发生重大不平衡,损害消费者利益",都是不公平的。⑥

---

① Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 Berkeley Technology Law Journal 1269 (2005)

② 张新宝:《个人信息收集:告知同意原则适用的限制》,载《比较法研究》2019年第6期,第1-20页;刘权:《论个人信息处理的合法、正当、必要原则》,载《法学家》2021年第5期,第1-15页;武腾:《最小必要原则在平台处理个人信息实践中的适用》,载《法学研究》2021年第6期,第71-89页。

③ Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, Oxford University Press, 2007, p. 242.

④ Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 The Georgetown Law Journal 115, 138-146 (2017).

⑤ 《一般数据保护条例》第82条规定:"任何因为违反本条例而受到物质或非物质性伤害的人都有权从控制者或数据者那里获得对损害的赔偿。"

⑥ Jane K. Winn & Mark Webber, *The Impact of EU Unfair Contract Terms Law on U. S. Business-to-Consumer Internet Merchants*, 62 Business Lawyer 209, 217 (2006)

(三)我国告知同意制度的性质

结合比较法与我国法律,可以发现告知同意制度的性质应做多维解读。一方面,《个人信息保护法》与欧盟《一般数据保护条例》具有较高的相似性,都将个人信息被保护权视为一种基本权利①,并将告知同意制度视为处理个人信息的合法性基础之一。这就意味着我国现行立法下的告知同意也具备合规要求的属性,而非传统合同或格式合同。②事实上,《个人信息保护法》在立法过程中曾经试图用合同中的意思表示来进行规定。一审稿第 14 条曾经规定:"处理个人信息的同意,应当由个人在充分知情的前提下,自愿、明确作出意思表示",但二审稿很快就删除了"意思表示"。这表明,我国的立法者也清晰地觉察到了告知同意制度与传统合同自治之间的区别,将告知同意制度视为具有保护型特征的法律制度。

另一方面,我国的文化背景与立法细节也与欧盟存在若干区别,《个人信息保护法》虽然也将个人信息被保护权视为一种基本权利,但并未像欧盟那样高度抽象化,反而在整体上比较关注消费者权利保护。③在《个人信息保护法》的实施机制层面,我国的制度反而和美国具有若干相似性,例如,二者都未设立独立监管机构,而是采取了多部门监管与救济体制。④ 在理论和制度优化层面,应将告知同意视为一种兼具消费者合同、声明、基本权利合规的多维制度。

三、告知同意的实施困境

在实践中,告知同意面临多方面的困境,学术界更是从多个不同角度对告知同意进行了批评,指出这一制度可能走向形式主义。同时,一些试图强化告知同意的做法不仅无法有效回应这些困境和批评,反而可能加剧某些问题。告知同意面临的困境,与前一部分提到的分析有密切关系。如果仅以合同的视角看待隐私政策与告知同意,这一制度将很难取得积极效果。

(一)告知的困境

就告知而言,隐私政策常常无法有效告知用户。信息隐私法的研究从各个角度指出,用户面对冗长、专业、枯燥的隐私政策,很少用户会在各种交互界面阅读隐私政策,阅读此类政策需要大量时间和专业知识。有国外学者推算,如果要通读网络隐私政策,一个人平均每年需要大约 244 个小时。⑤这还是在十年前,随着社会生活的全面数字化,各类物联网、智能家居收集个人信息的场景无处不在,隐私政策的复杂性、专业性更甚于以往。⑥而没有专业性知识,阅读隐私政策就可能像普通人阅读微积分,看上去每个字都认识,但实际上却很难理解或进入语境。例如,绝大部分普通用户都不了解动态 IP 与

① 王锡锌:《个人信息国家保护义务及展开》,载《中国法学》2021 年第 1 期,第 145-166 页;彭錞:《宪法视角下的个人信息保护:性质厘清、强度设定与机制协调》,载《法治现代化研究》2022 年第 4 期,第 50-64 页。

② 韩旭至:《个人信息保护中告知同意的困境与出路——兼论〈个人信息保护法(草案)〉相关条款》,载《经贸法律评论》2021 年第 1 期,第 47-59 页。

③ 张守文:《消费者信息权的法律拓展与综合保护》,载《法学》2021 年第 12 期,第 149-161 页。

④ 丁晓东:《〈个人信息保护法〉的比较法重思:中国道路与解释原理》,载《华东政法大学学报》2022 年第 2 期,第 73-86 页。

⑤ Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 Journal on Telecommunications and High Technology Law 273, 274 (2012).

⑥ 智能算法的问题又大大加剧了这一问题,万方:《算法告知义务在知情权体系中的适用》,载《政法论坛》2021 年第 6 期,第 84-95 页。

静态 IP 的区别,也很难理解 SDK(Software Development kit,软件开发工具包)处理个人信息的运行原理。在专业背景知识不充分的情形下,个体就很难理解或容易误解各类隐私政策中的内容。①

此外,用户很少会对隐私政策提起兴趣。在过去的十几年里,信息隐私研究最热门的研究主题之一即是"隐私悖论"(privacy paradox):人们虽然口头上对个人信息保护无比重视,但实际上却并不太关心隐私政策,很容易就"用隐私换便利",而且是换取极小的便利。②行为主义研究阵营中的法学家、经济学家和心理学家指出,造成这一现象的原因在于侵害个人信息的风险常常不确定,而且是非即时性的。对于这样一种风险,个人不太可能有兴趣对其进行阅读和了解。

事实上,现代社会中的产品说明与信息披露早已面临很多困境,个人信息保护中的告知同意只是又增添了另一例证。本·沙哈(Omri Ben-Shahar)教授曾经在经典论文《强制披露的失败》中描述过这一现象,现代社会中的个人每天都会遇到海量的信息提示:从使用剃须刀的产品说明,到收发快递的邮政说明,到吃饭时餐厅食物过敏提示。在信息过载(information overload)的背景下,消费者拒绝阅读隐私政策或产品说明,其实是一种理性选择。正如本·沙哈教授所言,"一次披露可以处理,但海量披露会压垮人,人们不可能关注比洪水更多的披露。"③

(二)同意的困境

就用户同意而言,首先,在个人没有充分知情的前提下,个人同意可能变成了一种没有理性的情绪表达,无法反映个人的真实想法与意志。理查德(Neil M. Richards)和哈特佐格(Woodrow Hartzog)两位教授曾将这类同意概括为"非知情的同意"(unwitting consent)。两位学者指出,由于个体不理解法律协议、不理解技术背景或不理解后果风险,个体在很多情形下所作出的同意只是一个空壳,远非"知情和自愿同意的黄金标准"(gold standard of knowing and voluntary consent)。④

其次,个体同意可能具有被诱导性或胁迫性。其中原因可能有多种,例如,市场可能被一两家头部平台所垄断,用户没有太多选项;或者即使用户有比较多的选项,但面对用户黏性和路径依赖,个体也可能很难说不。此外,企业常常有很多的技巧和"套路"让用户同意,例如,企业通过巧妙的交互界面设计,常常诱导用户同意其隐私政策。近年来,此类现象已经引起了越来越多的关注。例如,哈里·布里格努尔(Harry Brignull)将此类套路称为"暗黑模式"(dark patterns)⑤;一系列信息信义义务的研究认为企业可以对用户进行操控(manipulation)。⑥这些研究的共同发现是,个体的同意常常是被支配或操控下的非真实意思表示。

---

① Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 The Journal of Consumer Affairs 100, 100(2007). 对隐私悖论的批判,Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 George Washington Law Review 1 (2021),索洛夫教授的批判并不影响本文的论证,因为其批判也同样承认用户很难在短时间内有效获取信息。Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Reivew 1880, 1883 (2013).

② Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Washington University Law Review 1461, 1463 (2019);申琦、邱艺:《打开隐私悖论背后的认知黑箱》,载《西南政法大学学报》2021 年第 5 期,第 84-95 页。

③ Omri Ben-Shahar & Carl Schneider, *The Failure of Mandated Disclosure*, 159 University of Pennsylvania Law Review 647 (2011).

④ Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Washington University Law Review 1461, 1463 (2019).

⑤ Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 Journal of Legal Analysis 43, 44 (2021).

⑥ Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 Harvard Law Review Forum 11, 11 (2020); Tal Zarsky, *Privacy and Manipulation in the Digital Age*, 20 Theoretical Inquiries in Law 157 (2019); 冯健鹏:《个人信息保护制度中告知同意原则的法理阐释与规范建构》,载《法治研究》2022 年第 3 期,第 31-42 页。

最后,个体的同意也常常被绑定,无法作出具有“颗粒度”(granularity)的同意。信息处理者处理个人信息,有时是为了实现基础服务功能,有的是为了提供额外的增值服务或进行数据的进一步利用,还有的则可能对用户产生危害。面对信息处理者的多重目的,用户常常很难对所有目的进行“颗粒化”的分析,并分别一一作出同意或拒绝。更多的情况是,用户常常同意为了实现各种不同目的的信息处理,导致同意机制的异化。伯特·贾普·库普斯(Bert-Jaap Koops)教授将这类异化称为“功能蠕变”(function creep),认为同意机制常常导致个人信息被用于个人并不真正认同的初始目的,违反“目的限定”原则。①

(三)强化告知同意的困境

应当看到,现行的不少法律、指南与意见都看到了告知同意的困境,并对其进行了针对化的改进。例如针对告知,《个人信息保护法》第 17 条明确要求,个人信息处理者在处理个人信息前,应当以“显著方式、清晰易懂的语言真实、准确、完整地”向个人告知,《一般数据保护条例》同样规定控制者“应当以一种简洁、透明、易懂和容易获取的形式,以清晰和平白的语言来提供”。但如果仅从个体认知出发,则此类告知仍难以解决上述无兴趣、无时间、无专业、信息过载等难题。例如,当法律要求信息处理者采取“警示”的方式进行告知,但一旦“警示”过多,个人就会对此类警示疲劳;当法律要求信息处理者采取清晰平白语言,隐私政策就会更加冗长;当法律要求隐私政策简洁,告知就会不全面、不清楚。无论如何,要求信息处理者在一个交互界面对微型不确定的专业风险问题进行充分告知,无异于是一个不可能完成的任务。②

同意的困境同样难以解决。《一般数据保护条例》对于同意功能的弱化非常关注,并进行了针对性的规定。例如,其第 4 条第 11 款明确规定了同意的四个要素:自由作出(freely given)、具体(specific)、知情(informed)、通过声明或明确行动明确表明数据主体的意愿(Unambiguous indication of wishes),并且在“重述”和 EDPB(European Data Protection Board,欧洲数据保护委员会)关于同意的指南中对这四项要求作出了进一步规定。但这些要求无法解决个体无意进行太多决断这一根本性困境。在个人信息保护中,个体的同意并不像买卖大额商品或从事高危活动,一个理性个体不可能对此类微型权益进行深思熟虑的权衡。当法律作出强制规定,要求信息处理获得个人同意必须获得更高级别同意,此类强制规定只会增加用户负担。例如,当企业对所有个人信息收集均采取弹窗形式,或者要求用户采取“选择加入(opt-in)”而非“选择退出(opt-out)”的方式进行同意,那么,此类做法只会降低用户体验,而非激发真实同意。③

四、隐私政策的另类用途

从个体控制出发,告知同意面临困境,效果有限。但转换视角,从信息处理者自我规制、市场声誉

① Bert-Jaap Koops, *The Concept of Function Creep*, 13 Law, Innovation and Technology 29 (2021).

② 这一问题在传统格式合同中就存在,参见 Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 The Journal of Legal Studies 1, 22 (2014).

③ 对于“选择加入”与“选择退出”的利弊分析,参见 Hans Degryse & Jan Bouckaert, *Opt in Versus Opt Out: A Free-Entry Analysis of Privacy Policies*, https://ssrn.com/abstract=939511(Last visited on June 20, 2022).

机制、法律有效实施、沟通教育工具等角度出发,却可以发现作为告知同意载体的隐私政策的若干"意外"作用,隐私政策除了为用户个体提供告知,还可以发挥其他作用。

(一)自我规制的章程

从消费者或用户的角度看,隐私政策艰深晦涩且无足轻重,但从专业人员的角度看,隐私政策却是理解企业处理个人信息的重要参照,帮助信息处理者建立良性的合规流程与制度。① 在没有隐私政策之前,企业内部可能各自为政,没有专业人士专门从事个人信息保护工作,也没有人了解个人信息处理的整体图景、形成处理个人信息的统一流程。但通过隐私政策的人员设置、前期调研、条款拟定、协调沟通,此类情形却可以大为改善。在这个意义上,隐私政策可以成为信息处理者自我规制的章程。

如今,各国法律都将企业自我规制作为个人信息保护的重要一环。例如,《个人信息保护法》第51条规定,企业应当"制定内部管理制度和操作规程"等措施,第52条规定,符合要求的信息处理者"应当指定个人信息保护负责人,负责对个人信息处理活动以及采取的保护措施等进行监督";《一般数据保护条例》也规定了企业内部合规建设、数据保护官(Data Protection Office, DPO)等制度。②这些制度与隐私政策的功能密切相连,离开了隐私政策,企业内部将很难建立统一的个人信息保护政策,所谓企业的自我规制也无法展开。③

(二)声誉机制的媒介

隐私政策还可以成为声誉机制的重要媒介,建构个人信息保护的市场机制。单就个体而言,个人信息保护由于其专业性与信息高度不对称性,无法形成普通商品的信誉市场,甚至可能导致劣币驱逐良币的"柠檬市场",造成企业处理个人信息的机会主义行为倾向。④但市场中存在大量的中介机构,这些机构可以通过对隐私政策的理解、评级与认证,为信息处理者的信息处理提供打分机制,促成声誉机制的形成。

事实上,在隐私政策的发展历程中,此类机构就扮演了重要角色。例如,成立于1998年的在线隐私联盟(Online Priracy Alliance,OPA),这一机构由80多家全球化公司组成,将"领导和支持自律倡议,为在线隐私创造一个信任的环境"作为其使命。该机构不仅自己发布在线隐私通知指南、自我规制执法框架,而且要求其所有成员都使用并公布其自身的隐私政策。通过对其成员隐私政策的监督,该机构在早期个人信息的行业保护方面发挥了重要作用,促进了市场声誉机制的有效发挥。⑤

声誉机制与社会监督制度也在各国法律中被广泛应用。例如,《个人信息保护法》第58条要求大型平台建立"个人信息保护合规制度体系,成立主要由外部成员组成的独立机构对个人信息保护情况进行监督"。《一般数据保护条例》第40-41条规定了"行为准则"(codes of conduct),对代表信息处理者的行业协会制定更加细化的规则进行了规定,第42条对"建立数据保护认证机制、数据保护印章和

① 高秦伟:《个人信息保护中的企业隐私政策及政府规制》,载《法商研究》2019年第2期,第19页。

② 个人信息保护制度中的企业自我规制,参见 Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation Self-Regulation, or Co-Regulation?*, 34 Seattle University Law Review 439, 458 - 459 (2011).

③ William McGeveran, *Friending the Privacy Regulators*, 58 Arizona Law Review 959 (2016).

④ Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 Journal of Corporation Law 143, 144-145 (2020); 潘静:《个人信息的声誉保护机制》,载《现代法学》2021年第2期,第155-170页。

⑤ Privacy Alliance, Online Privacy Alliance, http://www.privacyalliance.org/resources. 这一机构现在已经不再活跃,但诸如TRUSTe和ePrivacyseal等类似机构已经更为成熟。

标记,以证明控制者和处理者的处理”合规的认证(Certification)制度进行了规定。这些兼具合规与声誉机制的制度如要发挥作用,都离不开隐私政策这一工具。

(三)法律实施的依据

隐私政策还可能成为个人信息申诉、司法与执法的重要依据。如果说隐私政策在企业自我规制与市场声誉中扮演的是“软法”治理的角色,那么,当相关组织与机构提起申诉、诉讼或进行执法时,隐私政策就可能变成“硬法”治理的一部分。

一方面,个体、社会组织可能依据隐私政策提起申诉或诉讼。为了调动社会各主体参与个人信息治理,各国都在不同程度上赋予了个体与社会组织的申诉权或诉讼权,以发挥此类主体被比喻为“私人总检察长”的作用。[①]例如,《个人信息保护法》第 50 条第 2 款和第 69 条分别赋予了个体的个人信息权利之诉与侵犯个人信息权利导致的侵权之诉,第 70 条规定了“人民检察院、法律规定的消费者组织和由国家网信部门确定的组织”可以提起公益诉讼。[②]《一般数据保护条例》也认可了个人申诉与司法诉讼权,并且在其第 80 条中首次引入了代表性诉讼[③],规定“数据主体有权委托非营利机构、实体或协会代表其行使”申诉和司法救济的权利。美国新近影响巨大的《数据隐私保护法案》(American Data Privacy and Protection Act,ADPPA)也规定,个体可以向监管机构提起申诉,如果监管机构或总检察长对于个人投诉不采取行动,个体还可以直接提起诉讼。[④]在此类诉讼中,隐私政策往往在其中扮演关键性角色,个体与社会组织往往依据隐私政策对信息处理者展开调查和提起诉讼。[⑤]

另一方面,监管机构、检察机构的执法活动也高度依赖隐私政策。当执法机构根据个人举报或相关线索进行个人信息执法,其切入口往往是隐私政策。[⑥]例如,美国联邦贸易委员会在过去几十年里承担了信息隐私的重要执法功能,其在“Facebook 与剑桥分析公司丑闻”等重大案件中,就是从调查企业的隐私政策开始,一步步调查企业的信息处理是否具有欺诈与不公平现象。[⑦]在欧盟的若干重要案件中,隐私政策也常常是监管机构的执法线索与监管对象。例如,2019 年,法国国家信息自由委员会(The Commission Nationale Intormatique & Libertés,CNIL)对谷歌处以 5000 万欧元的罚款,其理由就是谷歌的隐私政策不够清晰。[⑧]

(四)沟通教育的工具

对普通用户而言,隐私政策中的告知内容还可能具有沟通教育功能,为用户提供个人信息保护的相关知识与联系方式等信息,强化用户的个人信息保护意识。

一方面,隐私政策可能成为一种沟通工具。在用户打开或登录网站、下载或安装相关软件时,个体很可能没有心思详细浏览隐私政策;用户可能更想尽快浏览网站、完成相应工作。但在平时,也有用户

---

① Danielle Keats Citron & Daniel J. Solove, *Privacy Harm*, 102 Boston University Law Review 793, 810-833 (2022).

② 相关制度建构,参见余凌云、郑志行:《个人信息保护行政公益诉讼的规范建构》,载《人民检察》2022 年第 5 期,第 31-36 页;蒋红珍:《个人信息保护的行政公益诉讼》,载《上海交通大学学报(哲学社会科学版)》2022 年第 5 期,第 28-38 页。

③ Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 Florida Law Review 365, 426-428 (2019).

④ American Data Privacy and Protection Act, TITLE IV, Sec. 403.

⑤ 最为有名代表性诉讼当属奥地利公民马克西米利安·施雷姆斯(Maximillian Schrems)所为,他提起了包括推翻美欧数据传输的安全港协议、隐私盾协议的相关案件,对欧盟乃至全球个人数据保护都产生了重要影响。

⑥ Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia Law Review 583, 585-686 (2014).

⑦ Facebook, Inc., F.T.C. No. 1823109 (July 24, 2019).

⑧ The Sanctions Issued by the CNIL, https://www.cnil.fr/en/sanctions-issued-cnil (Last visited on June 20, 2022).

可能想更多地了解隐私政策与信息处理实践。此时,用户就可能抱着学习钻研的态度理解隐私政策,隐私政策就能发挥其告知功能,承担与用户进行沟通交流的桥梁。而且,隐私政策不仅包括了个人信息处理的相关做法,还包含联系性信息、执法性信息等各类信息,这有利于个体建立对信息处理者的信任。例如,我国《个人信息保护法》规定隐私政策中的告知应当包括"个人信息处理者的名称或者姓名和联系方式""个人行使本法规定权利的方式和程序"以及"个人行使本法规定权利的方式和程序"等事项。《一般数据保护条例》,美国联邦层面与各州的立法也作出了类似的规定。这些告知事项等于为个体提供了一本维权工具书。

另一方面,隐私政策可能增强用户的个人信息保护意识,从而间接促进个人信息保护。近年来,大量研究指出,个人信息保护面临"大规模微型侵权"的难题,仅仅依靠个体救济,难以对各类大型信息处理者进行有效制约。[①]而集体监管以及公权力支持的私法救济要发挥作用,就需要公民提高隐私意识,通过个体维权、公共舆论监督等方式促进个人信息保护制度的落地。目前,各国已经通过相关制度进行推动,例如,《个人信息保护法》第 11 条规定国家"加强个人信息保护宣传教育",《一般数据保护条例》第 57 条规定了监管机构应当"提高公众意识"。除了这些规定,隐私政策的合理呈现也扮演关键性角色,可以让用户在日常生活中意识到个人信息保护的重要性。当然,此类呈现应当是适度的、合理的,如果基于隐私政策的告知非常频繁,甚至严重降低用户体验,那么此类呈现就可能造成用户的麻木心态,甚至形成逆反心理。[②]

五、告知同意制度的重构

从上文分析出发,可以对告知同意进行重构。告知同意一旦重新设计,就既能避免告知同意在个体层面的困境,改善其作用;同时,这一制度也能保留甚至强化其多种功能。

(一)告知与同意的适度解绑

首先,告知与同意应当进行适度解绑。[③]从个体意思自治的角度出发,告知与同意往往被视为一个问题的两面:同意必须先进行告知,告知最终是为了获得同意。[④]但从上文的分析出发,会发现二者并不一定需要深度捆绑:告知的对象在有的情况下可能对个体发生作用,但在更多的情形下,其对个体产生的作用有限[⑤], 而对信息处理者内部人员、市场与社会主体、法律实施者,其告知反而有效。既然如此,同意就不应成为隐私政策的唯一或最重要目标,而告知也不应以个体作为唯一对象。

---

① 丁晓东:《从个体救济到公共治理:论侵害个人信息的司法应对》,载《国家检察官学院学报》2022 年第 5 期,第 103-120 页;Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 Boston College Law Review 1893 (2019).

② 吕炳斌:《个人信息保护的"同意"困境及其出路》,载《法商研究》2021 年第 2 期,第 87-101 页;马新彦、张传才:《知情同意规则的现实困境与对策检视》,载《上海政法学院学报(法治论丛)》2021 年第 5 期,第 100 页。

③ 近年来有部分文献注意到这一点,参见于海防:《个人信息处理同意的性质与有效条件》,载《法学》2022 年第 8 期,第 99-112 页;Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 Journal of Information Policy (2019).

④ 这一问题的背后是学界已经讨论很多的个人信息自决权的困境,参见杨芳:《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》,载《比较法研究》2015 年第 6 期,第 22-33 页。

⑤ 王琳琳:《个人信息处理"同意"行为解析及规则完善》,载《南京社会科学》2022 年第 2 期,第 80-91 页。

在同意要求方面,应适度放松其形式要求,避免同意要求的不断“升级加码”。[①]同意可以有多种不同设置。例如,法律可以将同意等同于明示同意,即要求用户明确进行点击;法律也可以将很多行为视为默示同意,例如,将用户浏览或知晓用户协议的情况下继续使用视为同意。法律还可以进一步强化同意,例如,要求信息处理者设置默认不同意的对话框,只有用户明确打钩和选择加入(opt-in),此时才将用户行为视为同意;或者法律可以要求信息处理者对不同类型的个人信息收集进行分别同意,要求用户在对话框进行多种选择。在个人信息保护面临挑战的情形下,人们很容易想到强化同意的解决方案。但正如本文分析,在个体无兴趣、无时间、无专业、信息过载的背景下,对同意作过高要求,会让同意流于形式,带来上文所列举的种种弊端。[②]

当然,避免同意的升级加码并不意味着取消同意,或者在所有的情形下都应当放松同意的形式要求。当个体所需要同意的信息处理属于较为重要的事项,并且普通个体对于此类事项具有充分认知时,此时同意不但必要,而且还需要通过各种形式对同意的形式作出严格要求。例如,当电脑或手机调取摄像头,或者当网站获取账户、密码等个人信息,此时信息处理者应当获得个体的明确同意。此类明确同意不但有利于个人信息的自我保护,而且有助于信息处理者获取个人信任,促进和谐信息关系的建立。[③]

从各国法律看,美国在同意方面要求较低。一方面,美国很多领域并不要求个人同意,但包括美国联邦贸易委员会在内的很多机构都出台了隐私政策指南,企业也基本都建立了隐私政策告知。另一方面,就要求同意的情形,美国在大部分情况下都采取了选择退出(opt-out)要求,即隐私政策的默认选项是企业可以处理个人信息。[④]例如,《加州消费者隐私法》赋予了个体拒绝企业出售其个人信息的权利,但个体要行使这一权利,应该通过选择退出的方式拒绝。[⑤] 只有在涉及敏感信息或特定情况,美国法才以选择加入(opt-in)的方式来获取同意。

相比美国,欧盟在同意方面的要求较高。《一般数据保护条例》的重述第 32 条认为:“明确的肯定性行为”包括“通过书面声明(包括通过电子手段)或口头声明”,但“沉默、预先勾选的方框”不构成同意,而且“当处理有多个目的时,应给予所有目的的同意”。EDPB 在其 2020 年发布的《关于〈一般数据保护条例〉同意的指南》中认识到了这一点,指出“同意请求不应不必要干扰(unnecessarily disruptive)”相关服务,但仍然认为,如果以“较少侵犯或干扰的方式”(a less infringing or disturbing modus)会引起“模糊性”,则仍会“中断使用体验”。[⑥]欧盟的这一立场使得其网站的同意设置变得复杂而繁琐,对于保护用户与消费者的良好体验并不友好。

---

① 林洹民:《个人信息保护中知情同意原则的困境与出路》,载《北京航空航天大学学报》(社会科学版)》2018 年第 3 期,第 13-21 页;翟相娟:《个人信息保护立法中“同意规则”之检视》,载《科技与法律》2019 年第 3 期,第 58-65 页。

② 这一设计也更符合个人信息保护的基础法理,个人信息被保护权具有工具性特征,并非绝对性权利,参见张新宝:《论个人信息权益的构造》,载《中外法学》2021 年第 5 期,第 1144-1166 页。

③ 近年来,中外文学者都开始注重信任在个人信息保护中的作用,参见 Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 Harvard Law Review Forum 34, 35 (2020);姚佳:《知情同意原则抑或信赖授权原则——兼论数字时代的信用重建》,载《暨南学报(哲学社会科学版)》2020 年第 2 期,第 48-55 页。

④ 这一做法也招致了不少学者的批判,Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 Minnesota Law Review 1219, 1241 (2002).

⑤ California Civil Code, section 1798.115.

⑥ EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, para 82.

目前,《个人信息保护法》对于个人同意的规定仍然较为原则,很多制度仍然有待于实践的进一步探索。《个人信息保护法》第 14 条规定了“自愿、明确作出”,第 23 条规定向第三方提供个人信息应当获取“单独同意”,第 29 条规定处理敏感信息应当获得“单独同意”或“书面同意”。这些规定,一方面对同意作出原则性规定,对特殊情况作强化要求。另一方面,这一立法模式并未对同意的具体要求作出特别明确的规定,为信息处理者在具体实践中建构同意标准留出了一定的空间。我国可以在参考欧美经验的同时,在实践中探索更符合具体场景和用户合理期待的同意机制。①

(二)多样分层的沟通机制

在告知与同意适度分离的思路下,告知不但不能省略,还应进一步强化和完善。由于告知的对象既包括普通个体,也包括企业合规人员、社会主体、司法与执法人员,告知应当采取分层框架,在简洁性、清晰性、具体性等方面作出细致安排,以实现与多主体的有效交流沟通和实质性参与。②

在呈现警示度方面,告知可以采取链接、弹窗、警示等不同程度的呈现形式。底部链接的方式常常为很多网站所采用,以维持页面的简洁。例如,谷歌、百度、必应、搜狗等搜索引擎,这类网站往往在其界面的边角处设置隐私政策的链接,不太容易为用户所注意。相较之下,一般性的弹窗则可以引起用户的关注,而警示性弹窗则可以通过红黄等颜色,更进一步引起用户警觉。不同警示度的告知形式各有优劣。警示度较低的告知往往难以引起用户注意,但也不会影响用户体验;警示度高的告知则刚好相反。为此,法律对于呈现度的要求可以兼顾二者,在具体场景中对相关设置进行判断与优化。例如,对于搜索引擎,大部分情形下搜索引擎所收集的个人信息往往是匿名性或去标识化的搜索信息③,因此,应当可以允许网站设置链接性隐私政策,但其链接名称应当可以在搜索页面中直接找到。

在呈现结构方面,隐私政策可以采取分层结构④,采取各类复杂产品说明书的展开模式。上文指出,隐私政策的简洁性与详细性、专业性与平白性要求各有优劣,为了最大限度发挥优势,避免劣势,可以要求或倡导企业采取双层或多层的隐私政策。在直接和用户交互的界面或第一层链接,隐私政策应简洁平白,为用户提供一目了然的信息目录,避免过于复杂和专业化的表述。第一层链接是信息处理者和普通用户对话的首要窗口,此类设置有利于普通用户获取更多有效信息。但到了第二层或第三层链接,此时的读者可能是企业、社会与执法部门的专业人士,或者对隐私政策抱有更具专业性期待的读者,此时的隐私政策应当展开得更为全面,以兼顾专业性与平白性,为这类读者提供更详细专业的指引。

(三)隐私政策的合规内嵌

如同上文所述,隐私政策不仅写给外部人士看,其对内部合规也具有重要意义。为了发挥隐私政策的这一功能,隐私政策应当成为信息处理者内部的合规指引,内嵌到信息处理的不同部门,成为产品

① 姜野:《由静态到动态:人脸识别信息保护中的“同意”重构》,载《河北法学》2022 年第 8 期,第 126-144 页。

② 冯健鹏:《个人信息保护制度中告知同意原则的法理阐释与规范建构》,载《法治研究》2022 年第 3 期,第 31-42 页。

③ 个人信息的匿名性或去标识化是一个极为复杂的问题,参见丁晓东:《论个人信息概念的不确定性及其法律应对》,载《比较法研究》2022 年第 5 期,第 46-60 页;赵精武:《用户标签的法律性质与治理逻辑》,载《现代法学》2022 年第 6 期,第 102-115 页。

④ 郑佳宁:《知情同意原则在信息采集中的适用与规则构建》,载《东方法学》2020 年第 2 期,第 198-208 页。

设计的一部分。①

隐私政策应当前置和融入信息处理者的内部,在企业内部交流、协调、探讨后确定。正如有学者指出,“起草隐私声明为公司提供了一个盘点和评估内部实践的机会,确保这些实践是最新的、必要的和适当的。它还可以作为一个决策平台,根据与品牌相关的考虑以及法律、政策或市场实践的发展,决定是否继续进行数据实践或部署技术”。②斯怀尔(Peter Swire)教授也曾经进行研究,发现美国格雷姆-里奇-比利雷(Gramm-Leach-Bliley Act,GLBA)法案生效后,许多金融机构第一次在内部进行了广泛的交流,以“了解数据在组织的不同部门之间以及与第三方之间如何共享和不共享”。③在企业内部合规前置方面,应当承认,目前我国在这方面还有较大不足。我国法务人员在企业中的地位相对较低,其协调沟通的能力也相对较弱。未来我国应在这方面加大力度,同时,政府在执法过程中,也应加大对企业内部合规的执法检查。④

隐私政策还应与产品设计结合,成为隐私设计或个人数据保护设计的一部分。⑤隐私设计(privacy by design)的概念为加拿大渥太华信息与隐私委员会前主席安·卡沃基安(Ann Cavoukian)提出。卡沃基安认为,产品设计往往对于个人信息保护具有关键作用,当企业从产品源头对信息收集与处理的方式进行把关,可以比个人更有效地保护隐私,同时实现个人与企业的双赢。⑥隐私设计的概念经过发展,逐渐成为个人信息保护领域的共识。例如,在《一般数据保护条例》采纳了“数据保护设计和默认数据保护”(Data Protection by Design and by Dafault,DPbDD)的原则,第 25 条规定,数据处理者应当通过设计和默认设置来有效实现数据主体的权利和自由。《个人信息保护法》虽然未直接规定隐私设计原则,但也规定了“采取相应的加密、去标识化等安全技术措施”的一些类似规定。⑦在隐私政策的形成与撰写过程中,应将隐私政策视为与前端产品设计密切沟通协调后的产物,而非仅仅是产品成型后的解释说明。⑧

(四)隐私政策的风险与模块化设计

隐私政策还应基于风险,对相关风险点进行模块化设计。例如,针对信息处理者是否进行去标示化操作,其收集的信息是否与第三方共享,企业采取何种措施防止个人信息泄漏和进入黑市,政府执法部门与市场中的第三方机构可以不断发现、调整与列明信息市场中的风险点,引导信息处理者对其进

① 王苑:《中国未成年人网络个人信息保护的立法进路——对“监护人或家长同意”机制的反思》,载《西安交通大学学报(社会科学版)》2019 年第 6 期,第 133-139 页;李芊:《从个人控制到产品规制——论个人信息保护模式的转变》,载《中国应用法学》2021 年第 1 期,第 56-78 页;张继红:《经设计的个人信息保护机制研究》,载《法律科学》2022 年第 3 期,第 31-43 页。

② Paula J. Bruening & Mary J. Culnan, 17 *Through a Glass Darkly: From Privacy Notices to Effective Transparency*, 17 North Carolina Journal of Law and Technology 515, 568 (2016).

③ Peter Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 Minnesota Law Review 1263, 1316 (2002).

④ 对合规问题的公司法分析,参见赵万一:《合规制度的公司法设计及其实现路径》,载《中国法学》2020 年第 2 期,第 69-88 页;李永:《数据合规的模式变革——从权利人“知情同意”到使用者“预测算法”》,载《西南政法大学学报》2022 年第 5 期,第 113-127 页。

⑤ 有学者主张,应以产品责任法的思路保护个人信息,参见 Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 Southern California Law Review 241, 244 (2007); James Grimmelmann, *Privacy as Product Safety*, 19 Widener Law Journal 793, 793-827 (2010).

⑥ Ira Rubinstein, *Regulating Privacy by Design*, 26 Berkeley Technology Law Journal 1409 (2012).

⑦ 《个人信息保护法》,第 51 条。

⑧ 对于市场是否可以有效设计产品保护个人信息,有不同观点,但都认同产品设计的重要性。参见 Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Cambridge, Mass: Harvard University Press, 2018, pp. 1-10; Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stanford Law Review 247, p. 247 (2011).

行防范,并在隐私政策中对这些风险点进行模块化的设计。①

采取基于风险的模块化披露,有利于司法诉讼与行政执法。上文提到,隐私政策的一大功能是可以作为社会监督者、行政执法者的依据。为了使这种依据能够有效发挥作用,隐私政策就应当针对个人信息保护中的实际风险进行阐述,形成模块化的清单。一旦形成此类清单,信息处理者就能与监督者、执法者形成有效的风险交流与风险监管,而非对隐私政策中的每个细节都进行无差别的检查。②此外,此类清单一旦模块化,特别是形成机器可读的模块,监督者与执法者就能对隐私政策进行批量化监督,实现监管的智能化与高效化。目前,包括我国在内的世界各国都对隐私政策的合规要求作出了某些规定,或者发布了某些指引,但这些规定或指引的探索仍然较为初步,需要未来进一步围绕风险点进行动态调整与合理设计。

采取基于风险的模块化披露,也有利于个人信息保护市场机制的发挥。如上所述,个人信息保护存在信息不对称的"柠檬市场"难题。为了应对这一难题,学者和专家们提出过不少建议,例如,保罗·欧姆(Paul Ohm)教授主张,应借鉴商标的理念,将互联网企业的隐私政策商标化,供用户直观选择,以此解决隐私政策的信息不对称与市场无序问题。③还有学者主张,隐私政策应模仿食品中的成分标签(label),要求信息处理者按标签进行披露。④本文所提倡的建议与这些建议有一定相似之处,当隐私政策进行基于风险的模块化披露,并辅之以上文提到的个人信息保护认证等机制,隐私政策可以重新激活个人信息保护的市场声誉机制。⑤

六、结语

基于隐私政策的告知同意已经成为个人信息保护法的一般规则⑥,也被视为信息主体不可转让的核心利益。⑦本文从比较法与法律原理出发,对这一制度进行重思,可以发现其性质与制度都应当进行重构。

就性质而言,告知同意制度的性质具有多维特征,在不同国家和地区呈现的面貌不同。在美国,告知同意在采用点击协议的形式下可能被视为合同,但在浏览协议等形式下可能不被认定。但即使被认定为合同,个人也可能因为缺乏损害而无法起诉,隐私政策在更多的情形下具有产品声明的特征,其实施依赖于执法。在欧盟,个人信息保护是公法基本权利在私人领域的辐射,告知同意更接近于基本权利的合规要求。但即使是欧盟,隐私政策也具有一定的消费者合同特征。我国的个人信息保护与欧盟存在整体相似性,但为市场化机制预留了更大空间,告知同意应被视为一种兼具消费者合同、声明、基

① 个人信息保护的风险维度,参见梅夏英:《社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度》,载《环球法律评论》2022 年第 1 期,第 5-20 页。

② 对于个人信息行政罚款的探讨,参见孙莹:《违法处理个人信息高额罚款制度的理解与适用》,载《华东政法大学学报》2022 年第 3 期,第 22-34 页。

③ Paul Ohm, *Branding Privacy*, 97 Minnesota Law Review 907(2013).

④ Corey A Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 The John Marshall Journal of Information Technology & Privacy Law 1, 47 (2008).

⑤ Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 Journal of Legal Studies S13 (2016).

⑥ 衣俊霖:《论个人信息保护中知情同意的边界——以规则与原则的区分为切入点》,载《东方法学》2022 年第 3 期,第 55-71 页。

⑦ 王洪亮:《〈民法典〉与信息社会——以个人信息为例》,载《政法论丛》2020 年第 4 期,第 3 页。

本权利合规的多维制度。①

就实施效果而言,如果仅采取二维视角,将告知同意制度视为合同或意思自治,则这一制度将面临重重困境。信息处理者将无法在即时交互场景下让个人有兴趣、时间和专业能力理解隐私政策,各种改进措施也只会加大信息过载与决策疲劳的困境。但如果拓宽维度,从多维视角看待基于隐私政策的告知同意,就会发现隐私政策的多重功能,隐私政策可以成为企业自我规制的章程、市场声誉机制的媒介、司法诉讼与行政执法的依据、沟通信任与隐私教育的工具。②

基于隐私政策的告知同意制度应进行制度重构。首先,告知与同意应适度解绑,在同意方面适度放松,避免同意要求的不断"升级加码",但在告知方面则应进一步强化与优化。其次,隐私政策在警示度方面可以采取链接、弹窗、警示等不同程度的呈现形式;在结构方面可以采取分层框架,以实现隐私政策与多主体的有效沟通。再次,隐私政策应成为信息处理者内部的合规指引,内嵌到信息处理的不同部门,成为产品设计的一部分。最后,隐私政策应采取基于风险的模块化披露,助推司法诉讼、行政执法与市场声誉机制的有效运行。ML

Multidimensional Interpretation of Privacy Policy: Reflection on the Nature of Notice and Consent Framework and Institutional Reconstruction

DING Xiao-dong

(Law School, Renmin University of China, Beijing 100872, China)

Abstract: Notice and consent framework based on privacy policy is the core system of personal information protection, but its nature and effectiveness should be reconsidered. Notice and consent framework has multiple characteristics in different countries and regions, such as contracts, statements, and compliance with fundamental rights. In China, it should also be regarded as a multi-dimensional institutional tool. From the perspective of individual autonomy, notice and consent framework faces problems such as information overload and too much decision-making. Even if the system is improved, it can not achieve individual full informed consent. However, the reader of privacy policy not only includes individuals in real-time interaction scenarios, but also internal personnel of enterprises, market raters, law enforcement and judicial personnel and individuals in non interaction scenarios. Privacy policy may serve as the compliance charter of information processors, the information media of market reputation mechanism, the implementation basis of judicial proceedings and administrative law enforcement, the tool to win individual trust and privacy education. We should decouple notice from consent, relax the consent requirements moderately, but strengthen the notification requirements of privacy policy. The privacy policy can adopt different reminder methods and hierarchical structures externally, become the compliance guidance embedded in different departments and products, and adopt risk-based modular disclosure in form.

Key words: privacy policy; inform consent; personal information; autonomy of will; integration of public and private law

本文责任编辑:林士平
青年学术编辑:孙 莹

① 作为规制工具的个人信息权益,参见王锡锌:《个人信息权益的三层构造及保护机制》,载《现代法学》2021 年第 5 期,第 105-123 页。

② 作为沟通信任机制的信息披露,参见丁晓东:《基于信任的自动化决策:算法解释权的原理反思与制度重构》,载《中国法学》2022 年第 1 期,第 99-118 页。