法商研究 Studies in Law and Business
Vol. 38 No. 2(2021)

个人信息保护的“同意”困境及其出路

吕 炳 斌*

摘 要:作为个人信息保护的核心规范之一,告知同意规则已以“入典”的方式在《中华人民共和国民法典》中得以确立。然而,该规则的实施面临困境,其中既有结构性问题,也有认知问题,更有内在悖论。这也意味着该困境难以彻底解决,只能采取缓解之策。已有的几种解决思路均存在难以克服的问题,并不理想。有必要在法典体系的视野下,基于解释论的立场求得“同意”困境的化解之道。个人信息保护的同意规则旨在保障自然人的信息自主和信息自决,此规范的评价基础是尊重人格尊严和自由发展。依据不同类型的处理行为是否触及人格尊严和自由发展这一核心利益,区分适用明示同意与默示同意,既具有正当性和可行性,可提供更佳的行为指引和裁判指引,又可为化解困境打开通道。

关键词:个人信息保护 告知同意 行为区分说 民法典 解释论

一、问题的提出

大数据时代,个人信息的保护和利用已成为一个突出的问题。《中华人民共和国民法典》(以下简称《民法典》)先行以“入典”的方式确立了个人信息保护的若干核心规范。其中,告知同意规则无疑是最为基础和重要的法律规范。对《民法典》个人信息保护规范的解释论研究,首当其冲的是明晰告知同意的规范内涵。所谓个人信息保护的告知同意规则,一般称之为告知同意原则[①]或知情同意原则,[②]也有少数学者称其为规则。[③] 可见,在术语表达上存在分歧。基于《民法典》第1035条第1款已将该原则具体化,将告知同意作为通常情况下处理个人信息应当满足的

* 南京大学法学院教授、博士生导师

① 参见张新宝:《个人信息收集:告知同意原则适用的限制》,《比较法研究》2019年第6期;万方:《隐私政策中的告知同意原则及其异化》,《法律科学》2019年第2期。

② 参见姚佳:《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》,《暨南学报》(哲学社会科学版)2020年第2期;郑佳宁:《知情同意原则在信息采集中的适用与规则构建》,《东方法学》2020年第2期。

③ 参见高富平:《个人信息使用的合法性基础——数据上利益分析视角》,《比较法研究》2019年第2期;陆青:《个人信息保护中“同意”规则的规范构造》,《武汉大学学报》(哲学社会科学版)2019年第5期。

“条件”,[①]故学理上的抽象原则已转变为立法中的具体规则。本文据此将其称为规则。至于“告知同意”和“知情同意”的用语分歧,两者的英语词源均为“informed consent”,指的是告知后的同意。从其英语词源和我国立法表达来看,有将“告知后”或“被告知”推定为“知情”之意。在原理上,民事活动中的各当事人一般应自行收集必要信息;当在特定情形下需要保障一方知情利益时,民法往往通过对另一方施加告知、说明义务来实现。原因在于,知情与否属于当事人主观事项,难以知悉;与其纠缠于一方的知情与否,不如对另一方施加相对客观的告知义务,以提高规则的可行性。由此可见,一方的告知与另一方的知情在法律构造上是一种对应关系,法律往往通过施加告知义务来保障对方的知情,个人信息保护规则亦不例外。根据立法上的表达,笔者更倾向于使用“告知同意”的术语。此外,在告知同意机制之下,告知是同意的内在规范要求,[②]故亦可将告知同意规则简称为同意规则。

个人信息处理通常应获得信息主体的同意,看似不证自明,然而,从国内外的实践来看,同意规则在实施上面临困境,甚至会形同虚设,进而致使以此为基础构架的个人信息保护制度被架空。我国学界也已认识到这一困境,展开了一些研究。但纵观现有的文献发现,对该困境及其成因的分析尚不透彻;并且,拘于之前的研究背景,大多数的研究是从立法或制度构建的角度提出建议。甚至,其中不乏如下观点:“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”,[③]“同意不应是个人信息处理的正当性基础”。[④] 然而,我国立法逆水行舟,在《民法典》中明确规定了个人信息处理的告知同意要求,正在制订的《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》)中也将进一步确立这种要求。此时,针对这一立法上日益稳固的规则再言放弃,已不合时宜,理性的选择应当是研究如何缓解乃至化解同意规则的实施困境。这也是目前亟待解决的一个问题。

《个人信息保护法》尚在制定之中,草案还存在修改完善的空间,但一个基调是与《民法典》相关规定进行衔接和保持一致。因此,本文最终提出的解决方案将依据已经生效的《民法典》相关规则进行解释。面对个人信息保护的“同意”困境,既然《民法典》已将相应规则纳入其中,就有必要在《民法典》的体系之下,基于同意规则的评价基础和规范意旨,在解释论上得出既具有正当性和可行性,又有助于化解困境的同意规则的适用基准。

---

① 《中华人民共和国民法典》第 1035 条第 1 款规定:“处理个人信息的,应当遵循合法、正当、必要原则,不得过度处理,并符合下列条件:(1)征得该自然人或者其监护人同意,但是法律、行政法规另有规定的除外;(2)公开处理信息的规则;(3)明示处理信息的目的、方式和范围;(4)不违反法律、行政法规的规定和双方的约定”。该条第 2 款规定:“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等”。本文也将在广义上使用“个人信息的处理”这一立法术语。

② 这也是比较法上的通行观点。我国台湾地区所谓的“个人资料保护法”第 7 条就将一般情况下的“同意”定义为“当事人经采集者告知本法所定告知事项后,所为允许之意思表示”。《欧盟通用数据保护条例》第 4 条第 11 款也将被告知作为同意的内在要素。需要指出的是,2020 年 10 月公布的《中华人民共和国个人信息保护法(草案)》第 14 条规定:“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”。此条规定的同意以个人的“充分知情”为前提是法律无法保障的,会造成判断上的困难,应参照比较法上的经验予以修正。

③ 范为:《大数据时代个人信息保护的路径重构》,《环球法律评论》2016 年第 5 期。

④ 任龙龙:《论同意不是个人信息处理的正当性基础》,《政治与法律》2016 年第 1 期。

二、同意规则的实施困境

在告知同意机制之下,同意是一种告知后的同意。这一要求在形式上较易满足。在实践中,信息处理者通常会通过隐私政策、个人信息保护政策等文件履行告知义务,[①]并给个人点击同意的机会。然而,个人的同意却未必建立在知情的基础上。毕竟,一方的告知并不等于对方的知情,在网络空间尤为如此。个人信息保护的“同意”困境的形成,具有较复杂的原因,既有告知同意中的结构性问题,也有信息主体的认知问题。[②]

(一)告知同意中的结构性问题

1.信息过载及其规模效应

在告知同意机制之下,信息处理者若有所隐瞒,将面临不利后果。然而,企业出于逐利动机,[③]往往通过信息混杂、行文冗长等方式隐藏重要信息,使个人不易发现。告知文件似乎并不是为了促进个人知情而拟定并提供的。具言之,于企业而言,其履行告知的“目的仅在于规避法律风险”,[④]为其信息处理行为寻求最大的合法化可能;而法律设定的、个人期待的目的在于通过告知促进个人信息保护。在对告知的动机和目的的理解上,不同主体之间可谓存在着一个根本性的背离。上述告知动机和目的上的背离,导致出现信息过载问题。告知文件的篇幅普遍较长,且用语专业晦涩,提供的信息趋于饱和,甚至严重过载。并且,信息过载还存在规模效应。一个人面对的是需要收集个人信息的成千上万的网站平台、手机应用以及线下商家,有些网站、应用和商家还经常修改、调整相关政策。因此,个人面对的是数百份乃至更多的可能随时修改的文件。信息过载会使接受者不知所措,导致接受者随意浏览、挑选信息甚至放弃阅读,这干扰了告知同意背后的基本机制的实现。[⑤] 以上信息过载的负面效应也可得到实证数据的支撑。国外有研究成果表明,如果信息主体要阅读提供给他们的所有隐私政策,那么每年需平均付出 244 个小时;如果只是粗略阅读,那么每年需平均付出 154 个小时。[⑥] 这意味着在信息网络社会,每人将平均每天花费 40 分钟阅读和理解各种网站、手机应用等服务的隐私政策。上述时间还只是阅读的时间,如果计入准确理解所需的时间、专业知识和精力,那么这一“知情”的成本更为高昂。在

① 在传统上,信息处理者一般通过“隐私政策”履行告知义务。2020 年 10 月 1 日实施的国家市场监督管理总局、国家标准化管理委员会《信息安全技术 个人信息安全规范》(GB/T 35273—2020)第 5.5 节要求个人信息控制者制定“个人信息保护政策”。在该推荐性标准实施后,“个人信息保护政策”也可成为专门的告知文件。

② See Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review, 1888-1893 (2013).

③ 由于在现实中最为典型和重要的信息处理者是信息网络服务商和数据企业,因此本文主要以这些企业的信息处理行为为探讨对象。

④ 参见张新宝:《个人信息收集:告知同意原则适用的限制》,《比较法研究》2019 年第 6 期。

⑤ See Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 University of Pennsylvania Law Review, 658-665 (2011).

⑥ See Aleecia M. McDonald, Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: A Journal of Law and Policy for the Information Society, 563 (2008).

我国,据统计报道,在2020年第一季度,网民人均安装63款手机应用程序。[①] 这些手机应用程序的隐私政策文件普遍较长。例如,百度的隐私政策包括总则和10个分则,其总则就有10 467字;分则是按照产品服务分类规定的,每个分则也有上万字。[②] 若粗略地以每份隐私政策一万字计算,则网民每年需要阅读63万字的隐私政策文件。由于隐私政策复杂,阅读和理解的成本高昂,加之潜在风险的遥远,因此信息主体对其置之不理便是自然而然的事情。这也符合个人行为的成本和效益的考量。

2.数据聚合效应及难以预测的未来风险

个人信息遭遇泄露和滥用的风险是潜在的,在大数据技术背景下尤为如此。一个人在不同时间提供的单条个人信息可能并不敏感,从而不会感到存在风险或威胁,但在数据聚合技术下,不敏感的个人信息互相叠加,互为线索,可能分析得出敏感的信息。这种处于未知领域的风险,个人实在难以预测和把握。人们对未来福利或风险的决策选择的难度明显高于对当下福利或风险的抉择,这一因素加剧了个人信息保护的"同意"困境。面对潜在的风险,个人也会抱有侥幸心理,丧失提防之心。如今,承载着个人信息的数据泄露事件不断出现,但作为信息主体的个人对此却无能为力。与其为这种风险所烦扰,不如选择忽视这种并不迫切的潜在风险,可能是大多数人的心态。与未知风险相比,同意处理个人信息的利益却近在眼前,如获得某种特定的信息网络服务。因此,个人的选择往往会受短期获益的影响。同意规则要求自然人在个人信息被收集时就评估信息处理的潜在风险,这其实存在一个结构性缺陷。个人信息的利用期限较长,甚至没有时间限制。从短期来看,个人或许是受益的,但风险往往潜伏在未来。概言之,同意时的成本效益考量依赖于对未知风险的判断,是同意机制中的一个结构性缺陷。

3.选择空间的缺乏

即使个人仔细阅读了隐私政策,但在作出个人信息利用的许可决定时往往缺乏选择的空间,只有一种全有或全无的选择状态。数据已成为信息网络时代最重要的资源之一,很多信息网络服务的商业模式依赖于个人信息的收集和数据的开发利用。个人在就信息处理作出是否同意的决定时,通常伴随着对相应的信息网络服务的需求。网络服务商利用了这种无法放弃的需求。虽然在法律的要求下,告知是网络服务商必须履行的义务,但用户也很难作出同意之外的选择,除非放弃使用该服务。于是,个人往往会即刻点击同意,而不会先研究隐私政策。对于没有选择余地的个人用户来说,研究也几乎不能改变选择的结果。

(二)信息主体的认知问题

1.理性人假设与现实不符

一项法律原则或规则的假定前提至关重要,事关这一原则或规则得以存在的理论支撑。告知同意规则中存在一个假定前提,即自然人是一个理性人,会阅读并理解所有的隐私政策声明,并仔细权衡利益得失,最终作出一个自觉的、理性的选择。然而,这一假定前提在很大程度上与现实并不相符。2018年,中国消费者协会和北京市消费者协会分别进行了手机应用程序个人信息保护的实证调研。中国消费者协会的问卷调查显示,认真阅读手机应用权限和用户协议或隐

① 参见远洋:《2020年第一季度中国网民人均安装63款App》,https://www.ithome.com/0/486/083.htm,2020-05-19。

② 参见《百度隐私政策总则》,http://privacy.baidu.com/detail?id=288,2020-05-06。

私政策的受访者仅占26.7%。[①] 北京市消费者协会的调查报告则得出更低的比例,“只有6.15%的人在安装或使用手机应用程序之前会经常看授权须知”。[②] 由此可见,人并非具有无限的关注力和完全的理性。相反,人的行为会受到有限理性的约束,并会采取试探等带有风险性的决策策略,还可能受到习惯的影响,在同意决策上采取近似策略。正视这一点,意味着需要放弃对告知同意规则实施效果的完美追求,而采取更为现实的态度。

2.知觉定式和边际递减效应

告知同意机制高度依赖于自然人的认知。在心理学上,影响形成正确认知的因素包括背景知识、行为人的预期和知觉定式。[③] 在知觉定式的影响下,人们对经常出现的事物会降低敏感度,通俗地讲,就是会产生“熟视无睹”的反应。不同的信息处理者征求类似内容的同意,也会引发心理学上的边际递减效应。也许个人对第一次或前几次的“同意”比较谨慎,越是往后,这种谨慎程度就会日益降低。甚至,过度的同意请求、超负荷的信息告知可能引发个人的抵触心理,但在不存在选择空间的情况下,为了使用信息网络服务,又不得不选择同意。边际递减效应实际上也是受习惯影响的。有学者对80人进行分组实验,结果表明:针对拖放、滑动、多选框选择或者只是简单的点击同意等不同的同意方式,网络用户在初期的反应会有所差别,其中左右或上下拖放的方式最容易引起用户的注意,但在习惯的影响之下,随着告知同意次数的增多,不同组别的用户对不同的同意方式所付出的时间都会减少,并在最后趋于相同。[④] 这也印证了我们通常所说的“习以为常”这种行为习惯。

3.疲于应对与堪忧的同意质量

信息过载、同意过频、风险难以预测以及各种认知问题综合在一起,导致自然人管理个人信息的难度越来越大,甚至处于失控状态。有实证研究成果表明,随着网络用户对个人信息的管理难度日益增大,加之数据泄露事件层出不穷,用户对个人信息保护会产生一种徒劳和厌倦之感;并且,比起保护个人信息的关注和需求,这种徒劳和厌倦之感会在更大程度上影响人们的行为。[⑤] 在疲于应对的状态下,人们在作出决定时一般会付出更少的精力。甚至,即使网站或应用软件提供修改隐私和个人信息保护默认设置的机会,很多用户也不会再花心思去修改,因为个人已经陷入疲倦的状态。个人在疲倦状态下作出的同意决定的质量甚为堪忧,离法律设想的理性、自觉的知情同意相去甚远。在同意规则的实施中,应当将个人从疲于应对的状态中解放出来。

(三)告知同意的内在悖论

除了上述结构性问题和认知问题之外,告知同意还存在内在悖论。这也是导致告知同意机

① 参见中国消费者协会:《App个人信息泄露情况调查报告》,https://www.sohu.com/a/251503286_100017648,2020-04-11。

② 杨滨:《北京市消协发布手机APP个人信息安全调查报告》,《北京晚报》2018年3月7日。

③ 参见[美]菲利普·津巴多、[美]罗伯特·约翰逊、[美]薇薇安·麦卡恩:《津巴多普通心理学》,钱静、黄珏苹译,北京联合出版公司2017版,第115页。

④ See Farzaneh Karegar, John Sören Pettersson, Simone Fischer-Huübner, The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention, 23(1) ACM Transactions on Privacy and Security, 5:1-5:35 (2020).

⑤ See Hanbyul Choi, Jonghwa Park, Yoonhyuk Jung, The Role of Privacy Fatigue in Online Privacy Behavior, 81 Computers in Human Behavior, 42-51 (2018).

制实施困境的重要原因。(1)隐私政策、个人信息保护政策在“充分告知”和“简单易懂”之间存在一个根本性的悖论。[①] 充分告知会导致内容冗长,致使个人不愿投入时间去阅读和理解;简单易懂的告知可促进个人的阅读,但往往难以传递复杂的内容,难以促进和保障个人的知情。(2)在同意与否的选择之间也同样存在一个悖论。在现实中普遍采取接受或不接受的二选一模式。在此之外增加选项,似乎可扩大个人的选择空间,但也将带来新的问题。选项的多样化会增加复杂性,相应地会带来更大的混乱风险,[②]未必总是有利于个人。(3)告知同意规则的实施在强度上也存在悖论。根据法治的基本理念,法律规则应当严格实施。然而,一律以最严格的态势适用同意规则,其结果将适得其反,未必有利于强化对个人信息权益的保护。具言之,信息网络服务商会发出更多的同意请求,对用户造成更多的干扰;信息网络服务商也会告知更多的乃至超负荷的信息,使用户难以有效阅读和理解。然而,用户却缺乏有效的选择空间,仍不得不以同意个人信息的采集和利用为条件接受服务,进而会导致用户对信息网络服务商发出的同意请求更不敏感,在绝大多数场合直接点击同意,同意规则的实效将更加糟糕。[③] 可见,同意的强度并非越强越好。这也意味着在实践中不宜一味追求严格的同意要求。总之,告知同意机制存在内在悖论,其实施中难免遭遇困境。并且,内在悖论的存在,也意味着这一困境无法得到彻底解决,只能试图缓解。

(四)小结

告知同意规则旨在改变个人信息的处理者与提供者之间的信息不对称状态,致力于保护个人信息权益,有其存在的必要性和正当性。然而,告知同意机制具有内在缺陷,其实施将面临困境,很可能流于形式。规则形同虚设,会使法律的整体实效大打折扣。法律不能被有效实施或实效不佳,也会影响人们对法治的信任和期待。如果以最严格的要求实施告知同意规则,那么又会加剧个人面临的告知过度、信息过载、同意过频、疲于应对等问题,难以使该规则担当起个人信息保护的基础性规则的重任。那么,如何化解告知同意规则的实施困境?在立法明确纳入这一规则的背景下,放弃和废除这一规则的观点已不可取,解决问题的方案应当是改善法律规则的实施,从而促进其有效性的发挥。

三、现有解决思路的不足

(一)抽象的场景导向理念

面对同意规则在实践中的僵化,探寻弹性合理的适用方法和判断标准,在个人信息保护和利用之间构建一个动态的利益平衡空间获得了学者的推崇。[④] 有论者在比较法研究的基础上,建议引入场景导向的理念,对个人信息的处理行为进行风险评估,依据风险的高低程度适用不同的

① See Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review, 1885 (2013).

② See Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review, 1885 (2013).

③ See Bart W. Schermer, Bart Custers, Simone van der Hof, The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection, 16 Ethics and Information Technology, 171-182(2014).

④ 参见陆青:《个人信息保护中“同意”规则的规范构造》,《武汉大学学报》(哲学社会科学版)2019 年第 5 期。

同意要求;甚至,在风险属于可预期范围、信息处理行为合理时,豁免同意要求。[①] 也有论者在吸收场景理念和风险理念的基础上,提出建立在场景和规则遵循情况之上的“情景合理测试”,具体考虑因素包括环境、时空、行为等场景要素以及风险控制能力等规则遵循情况。[②] 然而,纳入场景、风险等因素的考量,并不能提供明确的判断标准。即使在此学说提倡者的进一步论述中,合理、可预期、风险高低等的判断仍具有高度的不确定性,难以为个人信息利用关系中的各方提供明确的行为指引。在基于场景和风险导向理念的多因素判断法背后,隐含着动态体系论的方法论基础。该方法论导致的规则弹性化,为部分学者所推崇,并被赋予过高的期待,但一不小心,就会滑入自由法学的泥潭,造成过大的自由裁量空间,进而致使法律规则的实施存在恣意和不确定性,影响法的安定性。[③] 为克服这一弊端,动态体系论要求要素的限定性,具体包括“要素是哪些要确定”以及“要素的数量要有确定性”。[④]然而,场景和风险导向理念出于对法律效果的弹性化追求,并不能提出明确限定的要素,更不用说赋予这些要素不同的权重,从而提供理性的、可反驳的法律论辩平台和法律解释空间。场景和风险导向理念存在的恣意和不确定性只会加剧个人信息保护和利用中的乱象。

(二)不易界定的敏感信息与一般信息

另一种思路是区分敏感信息与一般信息,施加不同的同意要求,从而改善规则的实施。这其实是一种着眼于客体的场景化区分对待的思路。2013 年 2 月 1 日实施的国家质量监督检验检疫总局、中国国家标准化管理委员会《信息安全技术 公共及商用服务信息系统个人信息保护指南》(GB/Z 28828—2012)第 5.2.3 节即采用了这种两分法。《个人信息保护法(草案)》的立法也延用这种思路,在草案中专设一节规定敏感信息的处理规则,其中提高了对处理敏感信息的同意要求。[⑤] 然而,这种界分法存在不确定性,极大地影响了这种思路的可行性。首先,敏感信息的概念难免存在模糊性。《个人信息保护法(草案)》第 29 条规定“敏感个人信息是一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息”,并进行了举例说明,包括宗教信仰、民族、种族、个人行踪等信息。该定义试图将敏感信息与隐私中的私密信息相区别,但仍然存在“可能导致”“严重危害”等不确定因素,而这会影响对敏感信息的认定。其次,敏感信息的本质和关键在于信息的敏感性,而个人对信息的敏感度会受到文化传统、教育背景、生活经历和法治环境等外部因素的影响。不同的个人、不同的群体对敏感信息的认知会存在差异,很难得出一个完全一致的确定性结果。例如,有学者就中美大学生对敏感信息的感知进行实证调研,发现中国大学生的平均敏感度高于美国大学生,但美国大学生在电子邮件内容等事项上

① 参见范为:《大数据时代个人信息保护的路径重构》,《环球法律评论》2016 年第 5 期;田野:《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》,《法制与社会发展》2018 年第 6 期。

② 参见蔡星月:《数据主体的“弱同意”及其规范结构》,《比较法研究》2019 年第 4 期。

③ 参见解亘、班天可:《被误解和被高估的动态体系论》,《法学研究》2017 年第 2 期。

④ 参见解亘、班天可:《被误解和被高估的动态体系论》,《法学研究》2017 年第 2 期。

⑤ 《中华人民共和国个人信息保护法(草案)》第 30 条规定:“基于个人同意处理敏感个人信息的,个人信息处理者应当取得个人的单独同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的,从其规定。”书面同意的内涵比较清晰,而单独同意似乎是与一揽子同意相对而言的,但在法律上仍可有明示或默示的不同方式,这一概念的含义仍需进一步界定。此外,过于强调单独同意并无益于解决前文指出的告知过度、同意过频等问题。

的敏感度则明显高于中国大学生。[①] 最后,敏感信息的认定,也难免纳入对情景和风险等因素的考量。由于敏感信息的判断依赖于敏感度的认定,存在不确定性,因此以封闭式列举的方式对敏感信息加以明示列举存在弊端,对其弥补的措施是辅之以个人信息处理的情景和目的等因素的综合考量。[②] 这就增加了敏感信息的判断难度,并会导致不确定性。以最常见的上网储存在用户本地终端上的数据为例。网站收集储存在用户本地终端上的数据既可能是信息网络服务的必要(为提高用户体验),也可能是为了绘制个人数字画像,进而进行自动化分析和决策。对于前者而言,此时处理的信息并不敏感,而在后一场合,储存在用户本地终端上的数据就变成了敏感信息。可见,同样的信息在不同的情境下的敏感度存在区别。综上所述,基于敏感信息与一般信息的区别差异化适用同意要求,首先会面临敏感信息与一般信息的认定困难,而这会严重影响同意规则的适用。笔者赞同对敏感信息提供特殊保护,但一般信息与敏感信息的区分对待在解决个人信息保护的"同意"困境方面作用有限。

(三)并不可靠的"匿名化"

除上述两种方案之外,还有一种方案是鼓励匿名化处理个人信息。这种方案也聚焦于作为客体的个人信息。长期以来,国内外个人信息保护立法均将匿名化当作灵丹妙药,《民法典》第 1038 条也将"经过加工无法识别特定个人且不能复原的"作为个人信息保护的例外。匿名化似乎为个人信息保护找到了出路。有学者就认为个人信息的匿名化处理可产生豁免知情同意的效果。[③] 这似乎也可以缓解"同意"困境。然而,这种观点是建立在匿名化技术足够可靠的假设之上,但这一假设可能与现实不符。(1)匿名化技术和重新识别技术好比一对处于对抗游戏中的竞争技术,从目前来看,重新识别技术更胜一筹。有学者甚至认为它"占据了永久的优势"。[④] 在计算机科学中,不断有人基于各种目的研究"去匿名化"算法。[⑤] 即使经过匿名化处理,在数据中剩余的琐碎信息也可能和外部的辅助信息相结合,用来解锁身份。实证研究亦表明,在匿名数据中重新识别出个人并不困难。[⑥] 法律鼓励匿名,但信息技术的发展已可使得个人信息在"可识别"与"不可识别"的双重维度中摇摆动荡。[⑦] (2)在大数据技术背景下,彻底的匿名化更不可能,因为大数据分析可以使残缺的个人信息互相关联和重新组合,再度识别出个人。随着大数据的聚集和外部信息的丰富,解锁匿名数据中的模糊身份的概率也会相应递增。早在 20 余年前,科研人员就已经认识到匿名化在理论上的局限性,并放弃了强大的匿名化假设。[⑧] 在大数据时代,匿

① 参见王敏:《价值趋同与文化存异:中美"千禧一代"大学生对敏感数据的感知对比》,《新闻与传播评论》2018 年第 5 期。

② 参见胡文涛:《我国个人敏感信息界定之构想》,《中国法学》2018 年第 5 期。

③ 参见林洹民:《个人信息保护中知情同意原则的困境与出路》,《北京航空航天大学学报》(社会科学版)2018 年第 5 期。

④ See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCAL Law Review, 1752 (2010).

⑤ 参见刘家霖、史舒扬、张悦眉等:《社交网络高效高精度去匿名化算法》,《软件学报》2018 年第 3 期。

⑥ See Arvind Narayanan & Vitaly Shmatikov, Robust De-Anonymization of Large Sparse Datasets, in Bob Werner ed., 2008 IEEE Symposium on Security and Privacy, IEEE Computer Society, 2008, p.111.

⑦ 参见万方:《隐私政策中的告知同意原则及其异化》,《法律科学》2019 年第 2 期。

⑧ See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCAL Law Review, 1716 (2010).

名化的局限性更为凸显。(3)在数据的效用与个人信息的匿名化之间存在着一个根本矛盾。信息越是匿名,数据的效用就越低。因此,数据处理者存在巨大的经济动机使数据信息处于匿名与不匿名的中间模糊地带。任何有用的数据集合都不可能处于完全匿名状态。随着数据实用性的提高,其包含的信息内容就会越多,对隐私和个人信息的保护就会相应降低。正如有的学者指出的那样:“数据既可能是有用的,也可以是完全匿名的,但绝不可能两者兼而有之。”①

由上可见,数据匿名化的作用有被过分夸大之嫌,试图通过匿名化来充分保护个人信息是一个虚幻的承诺,在实践中已被无情地打破。我们应该放弃对匿名化的盲目崇拜,否则匿名化的幻觉将继续掩盖个人信息的安全保护与流通利用之间的权衡问题。数据不可能被彻底匿名化,我们所能追求的是降低重新识别的风险。可能的出路之一是要求信息网络服务商、数据企业在数据交易时,不提供原始数据、基础数据,只提供大数据分析结果。虽然这能够堵住反向识别之路,但也会导致数据的效用大幅降低。可能的出路之二是在法律上施加“禁止反向识别”要求。② 然而,这一要求在执法层面会面临困境。重新识别、反向识别往往是在企业内部进行的,或由个人私下操作,在监控上存在难度。可见,匿名化技术并非解决上述问题的灵丹妙药。着眼于客体的思维难以为解决“同意”困境觅得良策,我们需要超越客体思维,从行为的角度去求得更佳的出路。

四、“同意”困境的解释论出路

(一)告知同意的规范内涵

1.告知的规范内涵和程度要求

根据《民法典》第1035条第1款第2、3项的规定,信息处理者履行告知义务的方式是“公开处理信息的规则”和“明示处理信息的目的、方式和范围”,即采取公示的方式进行告知。如前文提及,法律上有将一方告知推定为对方知情之意。显然,并不是所有的告知都会导致对方的知情。告知应当满足一定的程度要求,以便促进对方知情,从而有助于缓解告知同意机制中的困境。立法规定告知义务旨在解决个人信息处理中的信息不对称的问题,以及维护自然人的个人信息自决权益。为实现这两个目的,告知的程度应当至少满足以下两点:(1)告知应当达到足以令相对人注意的程度,从而有助于解决信息不对称问题;(2)与格式条款的提请注意义务类似,告知还应当给人以该文件载有足以影响当事人权益条款的印象。③ 告知文件也应当将此类条款重点标出,以便引起个人的重点关注,减轻个人的阅读成本。进一步而言,在判断告知是否达到合理程度时,应当采用通常理性人标准,在网络空间即为普通网络用户标准。告知文件应当清晰明白,也应对包括处理行为的潜在风险在内的重点事项进行说明,以便具有通常认识能力的一般人理解。法律上对告知的程度要求只能如此,而无法进一步确保被告知者的充分知情。这在本质上是基于私法自治的原理,被告知者是否愿意充分知悉告知内容是其自由,由其自行选择。法律

① Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCAL Law Review, 1704 (2010).

② 参见张新宝:《我国个人信息保护法立法主要矛盾研讨》,《吉林大学社会科学学报》2018年第5期。

③ 参见崔建远主编:《合同法》,法律出版社2016年第6版,第40页。

上只能确保提供知情的机会,却无法强制性地保障某人知情。事实上,信息也不可能强塞进某人的大脑。当被告知者可以知悉告知文件中载有影响其权益的条款时,也应当付出时间和合理的努力,去阅读和理解这些文件。毕竟,从一方告知到另一方知情之间的间隙,需要告知者和被告知者双方共同努力去消除。

2.同意的规范内涵

根据《民法典》第 1035 条第 1 款第 1 项的规定,除了法律、行政法规另有规定的例外情形,处理自然人个人信息必须满足的条件之一是“征得该自然人或者其监护人同意”。如前文已经明确,这一同意是告知后的同意。此外,在性质上,此处的同意有别于物权处分中的同意,更类似于知识产权许可使用中的同意。从更一般的意义上讲,由于个人信息具有无形性特征,其权利构建在非物质化客体上,因此对个人信息保护规范内涵的理解,在所有权思维与知识产权思维之间更宜借用后者思维。如果在人格权内部寻求类比对象,那么个人信息处理中的同意也类似于肖像权许可使用中的同意。① 肖像权也以可识别性为特征,②与个人信息权益有共同之处。肖像权商业化利用中同意的当然不是肖像权的转让,而是使用许可。同理,个人信息利用中的同意也是一种对使用行为的许可,行为在其中起着关键的作用。

3.同意的不同强度

在《个人信息保护法》专门立法之外,将个人信息保护的核心规则纳入《民法典》,有利于将相关规则置于法典体系之下进行解释。在民法体系之下,同意是一种意思表示,可以由不同的方式作出,这体现着法律对同意的不同强度要求。根据《民法典》第 140 条的规定,包括同意在内的意思表示可以明示或默示作出,但只有在“有法律规定、当事人约定或者符合当事人之间的交易习惯时”,沉默才可视为意思表示。符合交易习惯体现着当事人的信赖,而信赖正是将本人沉默视为意思表示的一个重要的正当性理由。③ 也有学者将信赖原则、诚信原则和交易习惯并列,认为前两项原则在若干例外情形下也可构成沉默的基础,但应当非常谨慎。④ 学界关于能否将沉默视为个人信息处理场合的同意,存在不同的观点。有论者提出拟制同意,即“通过法律将沉默拟制为意思表示”。⑤ 这种拟制同意也被理解为“推定的‘默示同意’”。⑥ 然而,通过法律将沉默拟制为意思表示是对私人自治的一种较强的干预,其目的在于化解法律状态不明的情形,促进交易安全和效率。⑦ 在个人信息处理领域,同意可由明示或默示(行为推断)作出。这既可明确法律状态,也可保障交易安全和效率,暂未见通过法律将沉默拟制为同意的必要性。在该领域,也难谓已经形成交易习惯,沉默作为同意尚不具备典型的通常意义;对方也不能据此产生合理信赖,此处并不存在保护交易安全的需求。此外,个人信息主体保持沉默并不违背诚信原则。无论从何种正当性理由进行判断分析,沉默都不能构成对个人信息处理的同意;否则,当事人什么都没做就被视为同意,会使个人信息的采集和利用回归初始的丛林状态,个人信息保护的立法目的和

① 参见《中华人民共和国民法典》第 1019 条。

② 参见最高人民法院(2015)知行字第 332 号行政裁定书。

③ 参见冉克平:《民法典视野下“本人沉默视为同意”规则的再造》,《当代法学》2019 年第 4 期。

④ 参见杨代雄:《意思表示理论中的沉默与拟制》,《比较法研究》2016 年第 6 期。

⑤ 蔡星月:《数据主体的“弱同意”及其规范结构》,《比较法研究》2019 年第 4 期。

⑥ 参见郑佳宁:《知情同意原则在信息采集中的适用与规则构建》,《东方法学》2020 年第 2 期。

⑦ 参见石一峰:《沉默在民商事交往中的意义——私人自治的多层次平衡》,《法学家》2017 年第 6 期。

规范意旨就会落空。

在排除沉默的方式之后，个人信息利用中的同意仍可有明示和默示两种方式。在“朱烨诉百度隐私权纠纷案”[①]中人民法院就认可了默示同意的合法性，但人民法院的论证思路有待商榷。该案是从百度“通过提供禁用按钮向用户提供选择退出机制”方面去论证用户存在默示同意。从选择退出机制方面理解，用户保持沉默，没有选择退出或表示反对，即被推定为同意。典型的选择退出机制是将不作为的沉默推定为同意。例如，在版权领域，谷歌数字图书馆早期曾试图采取这种策略，要求版权人通知谷歌公司其作品不想被扫描和收录，否则视为同意。[②] 此处的权利人沉默即达到同意许可的效果。然而，在个人信息处理场合，用户并不是什么都没做，并不是真正的沉默。对于典型的上网或使用移动应用程序的行为，与其将用户对个人信息的处理态度理解为沉默，不如认为是用户通过使用网络服务的行为构成默示同意。基于网站和移动应用程序采集个人信息的普遍性，加之以网络服务商已将隐私政策公示告知，从用户使用网络服务的行为可以推断出用户的默示同意。

虽然默示同意中的知情和同意均源于推定，是知情同意的一种弱化版，但是默示同意确有其存在的必要性。个人信息的概念具有扩张性，越来越多的信息类型将成为个人信息，加之在各个领域的信息网络服务不断呈现，收集个人信息的请求也会不断增加。从这个角度看，以默示同意为代表的干扰较少的同意方式具有存在的价值，并将在实践中发挥优势。更为重要的是，默示同意有利于为告知同意的实施提供一定的灵活性。并不是告知同意的强度越高，个人信息保护的力度就越大，“强同意”未必带来“强保护”。此外，也在于告知同意机制具有规制工具的特性，[③]选择合适的告知同意强度，可避免对个人信息收集和利用的规制过度，为大数据产业的发展保留足够的空间。

由于在告知同意中存在难以解决的悖论，因而同意规则的困境是无法彻底解决的。理性的策略是缓解这一困境。明示同意与默示同意的不同强度为解决此问题提供了可能性。接下来的问题是如何区分适用不同的同意强度。

（二）同意强度的区分适用：“行为区分说”之提倡

1.同意规则的评价基础

同意是个人信息自决的集中体现。我国法上的同意规则深受比较法上的个人信息自决权理论的影响。德国联邦宪法法院基于人格尊严和自由发展的理念，从基本权利中推演出个人信息自决权，其社会背景正是数据的自动化处理技术引发的风险和对个人造成的恐惧。[④] 随着信息技术的发展，互联网企业已经超过国家机关，成为个人信息的最大收集者和掌控者，这“促使该权利突破宪法性基本权利的限制，转而具有民事权利的属性”。[⑤] 从个人信息自决权的比较法渊源可见其旨在解决的问题和所维护的价值。近年来，我国加强个人信息保护的呼声高涨，也源于对技术侵入个人领域的担忧。在信息网络和大数据时代，个人信息不当利用的风险给自然人造成

① 参见江苏省南京市中级人民法院（2014）宁民终字第5028号民事判决书。

② See Authors Guild v. Google, Inc., 770 F.Supp.2d 671－673 (2011).

③ 参见高秦伟：《个人信息保护中的企业隐私政策及政府规制》，《法商研究》2019年第2期。

④ Vgl. BVerfGE 65,1 (41 f.).

⑤ 郑观：《个人信息对价化及其基本制度构建》，《中外法学》2019年第2期。

了压力。随着人脸识别技术、拍照扫描技术的发展,线上线下的行为记录都可以数字化,被储存、计算、衡量、分析和评价。人类似乎进入透明人社会。与海量的大数据相比,“大分析”更令人不安,其结果除了用于对个人未来行为的预测之外,还可能产生个人的数字信誉,影响个人的投保、求职、交往等各种行为。① 个人信息保护立法体现了人类对隐私破坏技术、大数据和大分析技术的回应。从个人信息自决的比较法渊源、产生的技术背景中,可见个人信息自决旨在维护人的尊严和自由发展。这也有坚实的理论支撑。在德国学者康德的目的秩序理论中,人是目的本身,而不是手段。② 人作为理性存在的主体,不能作为计算机分析的对象或客体。在德国关于基本权利的教义学中,人的尊严是法秩序的最高原则。③ 在德国民法中,个人信息自决权依托于一般人格权而存在和发展。④ 德国法院在创设一般人格权时也强调人的尊严和人格发展是法律的最高价值。⑤ 不仅是德国,“当今世界各国的法律制度,普遍以‘人的尊严’作为最高的伦理总纲”。⑥我国民法学界的权威学者也认为,人的尊严是法律的最高原则。⑦ 这一理念也体现在《民法典》的个人信息保护规范体系之中。尽管公法学者对将个人信息保护纳入《民法典》人格权编存在一定的异议,⑧但将其纳入人格权编的好处即是确立个人信息属于人格权益,可共享人格权益的价值基础和一般规则。《民法典》总则编第 5 章(民事权利)第 109 条和人格权编第 1 章(一般规定)第 990 条第 2 款均规定了人格权益的一般条款,明确了人格权益保护的价值基础在于人身自由和人格尊严。据此,个人信息保护的基本价值取向也在于维护人格尊严,而不是提高个人信息的经济效益,也不是促进数据产业的发展。维护人的尊严才是立法的目的价值,而对个人信息的利用则只是一种工具价值,工具价值应当服从目的价值。⑨ 进一步而言,人格尊严包括消极和积极两个方面,其范围不限于人格尊严得到他人尊重的消极层面,还包括人格自由发展的积极层面。⑩ 由于人格自由发展可谓人格尊严的外延所在,因此,也可以将个人信息保护的价值基础明确地表达为尊重人格尊严和自由发展。同意规则作为个人信息保护的基础性规范,其价值基础也在此。综上,个人信息保护的同意规则旨在保障自然人的信息自主和信息自决,该规则的评价基础正是尊重人格尊严和自由发展。就自然人而言,其在意并希望得到保护的也是个人信息中的人格利益,而非财产利益。事实上,个人信息附属的财产利益通常需要经过大数据加工处理才

① 参见[美]迈克尔·费蒂克、[美]戴维·C·汤普森:《信誉经济:大数据时代的个人信息价值与商业变革》,王臻译,中信出版社 2016 年版,第 5~7 页。

② 参见[德]康德:《实践理性批判》,韩水法译,商务印书馆 2000 年版,第 144 页。

③ 参见张翔:《基本权利的体系思维》,《清华法学》2012 年第 4 期。

④ 参见王利明:《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,《现代法学》2013 年第 4 期。

⑤ 参见[德]卡尔·拉伦茨:《德国民法通论》(上册),王晓晔、邵建东、程建英等译,法律出版社 2013 年版,第 171 页。

⑥ 胡玉鸿:《个人独特性与法律普遍性之调适》,《法学研究》2010 年第 6 期。

⑦ 参见王泽鉴:《民法总则》(增订版),中国政法大学出版社 2001 年版,第 35 页;王利明:《民法的人文关怀》,《中国社会科学》2011 年第 4 期。

⑧ 参见周汉华:《个人信息保护的法律定位》,《法商研究》2020 年第 3 期。

⑨ 参见张新宝:《个人信息收集:告知同意原则适用的限制》,《比较法研究》2019 年第 6 期。

⑩ 参见黄薇主编:《中华人民共和国民法典人格权编解读》,中国法制出版社 2020 年版,第 16 页。

能呈现，难以归个人享有。[①] 在目前的市场环境和技术背景下，个人信息易于被信息网络服务商收集，却难以被信息主体有效控制，自然人人格利益的保护存在不足。同意规则有利于改变其中的市场失灵和失衡状态。同意机制的存在，起码给出了一个停顿的时间，赋予了自然人控制个人信息、维护其中人格利益的机会。

2.基于处理行为的区分适用基准

第一，判断要素的提取。“同意”强度的差异化适用有赖于一种区分的方法，因此需要提取合理可行的判断要素。就方法论而言，法律其实也是一种决策和判断的认知模型，而在现实世界中存在很多变量，“在全面把握这些变量的基础上进行决策是不可能的”。[②] 法律规则尤其是具体的判断方法更需提取关键的、决定性的要素，从而降低人们的认知负担和决策成本。自然人同意的是他人对其个人信息的处理，从而涉及“主体—行为—客体”3 个方面。下文将从这 3 个方面展开，以提取“同意”强度区分适用的判断要素。在主体方面，由于政府处理个人信息大多属于“法律、行政法规另有规定”的情形，因而需要重点讨论的主体是企业。若处理个人信息的主体是提供独占服务的垄断企业，则个人面临的选择机会将会更少，同意常是不得已的选择。从这个角度看，似乎应当将主体作为一个判断要素。然而，就个人信息保护规范旨在维护的人格尊严和自由发展而言，一般企业的数据泄露风险、数据滥用风险同样存在，并且可能更大。由于对垄断企业施加更严格的同意要求，而对一般企业降低标准，并不存在合理性，因此主体并不能成为同意要求区别适用的判断要素。在客体方面，敏感信息与一般信息的区分似乎可以成为一个判断要素，但是如前文已经详细展开，敏感信息与一般信息之间的界分并非总是轻而易举的，敏感信息的认定就会受到个人敏感度的影响，也会受到情景和风险等外部因素的影响。这个变量存在很大的不确定性，极大地影响了告知同意作为行为规范的可预见性，也难以达到降低人们认知负担、提高决策效率的功能性目的。经过上述排除，唯一剩下的要素便是处理个人信息的行为。这恰恰是一个关键的、决定性的要素。每天都有大量的个人信息被收集，并以数字化的形式储存成为数据。这些数据本身往往没有多大的意义，真正的意义在于人们如何处理和对待收集这些数据信息的行为。将个人信息的处理行为作为同意强度区分适用的判断要素，也符合个人信息权益内容和结构的特征。个人信息权益并不能像物权一样建立在对有体物的占有基础上，并不是对客体的圆满状态的保护，而是采取“行为规制权利化”的路径，在特定的利用行为上架构权益保护空间。[③]《民法典》第 1037 条确立的自然人对个人信息的查阅、复制的权利（访问权）以及对错误信息、问题信息的更正权和删除权均是建立在特定行为之上的。同意在本质上也是自决权的体现，但不宜作抽象的理解，而应当理解为对具体的处理行为同意与否的权利。如前文所述，个人信息处理中的同意类似于知识产权许可使用中的同意，针对的都是行为。因此，以处理行为作为同意强度区分适用的判断要素，具有正当性。综上所述，同意强度区分适用的判断要素应当是对个人信息的“处理行为”这一单一要素。相较于多要素的动态体系平衡而言，单一的固定要素具有很大的优势：(1)单一要素可减少裁判者个人偏好影响和自由裁量空间；(2)单一要素相应地增强了规则的可预见性，保障行为主体和社会公众的信赖利益，使规则更好地起到行为规范、裁

① 参见张新宝：《〈民法总则〉个人信息保护条文研究》，《中外法学》2019 年第 1 期。

② 蒋舸：《作为算法的法律》，《清华法学》2019 年第 1 期。

③ 参见吕炳斌：《个人信息权作为民事权利之证成：以知识产权为参照》，《中国法学》2019 年第 4 期。

判规范的引导作用,有利于实现法的安定性;(3)就成本和效率而言,单一要素可大幅度减少判断成本,提高决策效率,既减轻了司法负担,又可促进交易便利。

第二,处理行为的两大类型。法典化的一大好处是可将具体规则置于法典体系下进行解释。个人信息处理中的同意分为明示同意与默示同意,可依据《民法典》总则编第 140 条关于意思表示的规定解释得出。出于区分适用两种同意方式的目的,对处理行为进行分类,若法律上缺乏明确的规定,则其界分基准可求助于《民法典》总则编第 109 条规定的人格权益保护的价值基础。《民法典》第 109 条具有"对人格权下属各条文的统领作用",[①]可用于人格权具体规则的解释。在现实中个人信息处理行为多种多样,其分类可以从个人信息保护的价值基础上找到基准。这一价值基础既有立法上的依据,又有比较法和理论上的支撑,具有充分的正当性。个人信息保护需要落实到对处理行为的规范之中,对不同的处理行为的法律评价也应基于这一价值基准。据此,个人信息的处理行为可分为两大类型:(1)触及人格尊严和自由发展的个人信息处理行为;(2)与人格尊严和自由发展无涉的个人信息处理行为。这两大类型恰好可对应于同意的两种方式。这两大类型具有开放性,可容纳现实中多种多样、不断发展的个人信息处理行为。当然,这两大类型还略显抽象。为减少判断成本,进一步提供具体化的指引,还可在两大类型之下,根据现实中的个人信息处理情况,归纳出若干通常类型、典型类型作为其下的亚类型或子类型。在原理上,类型是规范与事实之间的中介,在其划分中,规范性因素和经验性因素均将参与其中。[②]以个人信息保护的价值基础为基准进行分类,考虑的是规范性因素;以个人信息处理情况为依据做进一步的类型塑造,考虑的则是经验性因素。在"触及人格尊严和自由发展的个人信息处理行为"这一大类之下,典型的子类型有:公开并向不特定对象出售个人信息或实施类似性质的行为,为了绘制用户画像的信息处理行为,即将人作为"客体"进行分析的处理行为。在"与人格尊严和自由发展无涉的个人信息处理行为"的大类之下,典型的子类型有:为了不针对特定个人的大数据分析而进行的信息处理行为,仅仅为了提供服务或维护系统正常运行而进行的信息处理行为。这些子类型只是目前的典型类型。在未来,随着实践的发展,对典型类型可以进行补充更新,但其划分和归类标准已经确立。如果有新的个人信息处理行为出现,那么首先可以运用类比思维,与上述典型的子类型进行比较,尝试将其归入既有的类型之中。至于类似性的认定,学界存在"构成要件类似说""实质一致说""同一思想基础说""共同意义说"等不同的学说。[③] 在探寻生活事实和典型类型之间的实质一致、思想基础相同或意义相同时,都难免涉及价值判断。此时,个人信息保护的价值基础依然可以发挥作用。其次,如果新的处理行为难以归入典型类型,那么可尝试直接依据前述两大类型的区分基准进行判断。最后,如果新的处理行为在是否触及人格尊严和自由发展的认定上存在难度,那么往往意味着其中的风险处于未知的领域,对此就应持谨慎的态度,可适用较为严格的同意要求。

第三,同意强度的区分适用及其意义。同意规则面临形同虚设、名存实亡的实践危机,但并非无可救药。如前所述,告知以公示的方式进行,其灵活性有限,但同意的实施却存在较大的灵

① 参见最高人民法院民法典贯彻实施工作领导小组主编:《中华人民共和国民法典总则编理解与适用(下)》,人民法院出版社 2020 年版,第 548 页。

② 参见[德]卡尔·拉伦茨:《法学方法论》,陈爱娥译,商务印书馆 2003 年版,第 15~340 页。

③ 参见刘士国:《类型化与民法解释》,《法学研究》2006 年第 6 期。

活空间。这为解决困境打开了通道。要缓解同意规则的实施困境,需要从同意强度的区分适用着手。同意有明示和默示两种方式,个人信息的处理行为也恰好可以分为两大类型。在此划分的基础上,对不涉及人格尊严和自由发展的行为类型适用默示同意可以使同意规则的实施产生灵活性;反之,对涉及人格尊严和自由发展的处理行为类型,坚持适用明示同意可以更好地维护个人权益。这种区分适用方法正契合同意规则的评价基础。当然,法律、行政法规也可以豁免前一类型中一些处理行为的同意要求,但若无明确的豁免,则其仍应适用默示同意的方式。依据不同类型的处理行为是否触及人格尊严和自由发展这一核心利益,区分适用明示同意与默示同意,不仅具有正当性,也具有可行性,并且有助于化解“同意”困境。(1)就个人而言,这一区分适用法在很大程度上可以将个人从同意过频、同意麻木和疲于应对的状态中解放出来,减少个人应付告知同意的时间和精力,同时使个人对可能影响其人格权益的信息处理行为更加敏感和谨慎,集中精力处理此类同意,从而提高同意的质量。(2)就信息处理者而言,互联网和大数据企业等信息处理者可能主张个人信息的敏感度不易把握、且依赖于场景和风险分析,从而难以判断个人信息是否属于敏感信息,但是信息处理者对由其自身主导的个人信息处理行为应有较为清晰的认识,这种行为是否触及自然人的人格尊严和自由发展也应当在其掌控之中。基于处理行为的类型去区别实施不同的同意方式,对其并不存在障碍。(3)就裁判者而言,若个人信息纠纷已经进入司法程序,则意味着被诉的侵害行为已经发生,此时法官只需重点对个人信息处理行为进行客观考察和分析,并可借助类型化思维,将之纳入典型类型,或与典型类型进行类比,较为轻松地判断该行为是否触及自然人的人格尊严和自由发展,从而区分适用明示同意与默示同意。这不仅可行,而且还可大幅度节省裁判成本、提高司法效率。

五、结　论

我们不得不承认,告知同意规则存在内在的困境,但这一规则对于个人信息的保护又是如此重要,以致不能轻言放弃。也正是因为这一规则在个人信息保护规范体系中的基础性地位,我们必须孜孜以求地寻求更佳的出路和方案。将个人信息保护规范置于《民法典》的体系之下进行解释,在明确同意的规范内涵、不同强度和评价基础之上,提出基于处理行为的判断基准,即“行为区分说”:对不涉及人格尊严和自由发展的个人信息处理行为,可适用默示同意;反之,则应适用明示同意。经过本文的论证分析,这种方案具有正当性和可行性。由于在告知同意机制中存在内在悖论,“同意”的困境是难以彻底解决的,而只能缓解。“行为区分说”扎根于个人信息保护规则的解释论,即兼顾了法的安定性和法律体系的融贯性,又允许同意强度存在合理差异,配之以告知义务的合理程度要求,可在很大程度上化解告知同意机制中的结构性问题和认知问题,将个人从疲于应对甚至失控的状态中解放出来,提高同意的质量,从而提升规则实施的效果。在未来,随着实践经验的积累,同意规则的实施困境有望得到进一步化解。

责任编辑　　**何　艳**