

大数据时代知情同意规则的困境与出路

李禹希

天津大学法学院, 天津

收稿日期: 2022年12月1日; 录用日期: 2022年12月13日; 发布日期: 2023年1月10日

摘要

知情同意规则是个人信息处理者收集个人信息的合法性基础, 是个人信息保护的“帝王条款”。但是在大数据时代, 海量的数据处理加大了有效获取同意的难度, 使得知情同意规则的有效性备受质疑。对此, 我们不能否认知情同意规则的必要性, 而应该从知情同意规则所确立的“告知-知情-同意”三个环节上寻求破解困境的出路, 增强知情同意规则的有效性。

关键词

知情同意规则, 个人信息保护, 大数据时代

Difficulties and Solutions of Informed Consent Rules in the Age of Big Data

Yuxi Li

Law School, Tianjin University, Tianjin

Received: Dec. 1st, 2022; accepted: Dec. 13th, 2022; published: Jan. 10th, 2023

Abstract

Informed consent rule is the legal basis for personal information processors to collect personal information, and is the “imperial clause” for personal information protection. However, in the age of big data, massive data processing has increased the difficulty of obtaining consent effectively, making the effectiveness of informed consent rules questioned. In this regard, we can not deny the necessity of the informed consent rule, but should seek a way to solve the dilemma from the three links of “inform informed consent” established by the informed consent rule, and enhance the effectiveness of the informed consent rule.

Keywords

Informed Consent Rules, Personal Information Protection, Big Data Era

Copyright © 2023 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



1. 问题的提出

《民法典》第 1035 条第 1 款第 1 款¹确立了收集个人信息的知情同意条款,成为保护个人信息的“帝王条款”。《个人信息保护法》第 29 条²对敏感个人信息则规定了单独同意及特殊情形下的单独书面同意,进一步对《民法典》的知情同意进行了完善。关于知情同意,有的学者称之为知情同意原则,有的学者称之为知情同意规则。鉴于《民法典》第 1035 条第 1 款第 1 款已经将知情同意具体化、规则化,并将知情同意作为信息处理者处理个人信息应当满足的条件之一,笔者更赞同知情同意应该是规则,而不是原则,因此本文称之为知情同意规则。知情同意规则是个人信息处理中最基本的规则,也是处理者收集个人信息的合法性基础。知情同意规则的设计初衷是将个人信息的知情权和同意权赋予信息主体本身,而信息处理者则负有向信息主体告知之义务,信息处理者处理个人信息的法理依据来自于用户授权,从而最大限度地保证信息主体的信息自决权。[1]知情同意规则的完成意味着信息处理者处理个人信息之前需要经历三个环节:(一)信息处理者告知用户;(二)用户收到即知情;(三)用户同意。这三个环节看似环环相扣、无缝衔接,可以构建起保护个人信息的严密闭环。[2]但是在实践中,这三个环节往往在形式上完美满足,但是实际效果上却难以令人满意,尤其在大数据时代,随着个人信息的爆发式增长,海量的数据处理加大了有效获取同意的难度,使得知情同意规则的有效性备受质疑。

2. 知情同意规则遭遇大数据时代

2008 年 9 月,《自然》杂志第一次正式提出“大数据”的概念,大数据这一“概念”由此滥觞。2012 年 2 月 12 日,《纽约时报》一篇专栏文章称“大数据时代”已经来临,标志着人类进入了大数据时代,因此 2012 年也被人们称为大数据时代元年。有学者将 1945 年人类进入信息时代之后到 2012 年人类进入大数据时代之前的这半个多世纪的时间段称之为“小数据时代”或者“前信息时代”。[3]

与“小数据时代”相比,“大数据时代”需要收集和处理的的数据规模非常巨大,数据收集和处理的远远超过了之前传统数据库获取和处理数据的能力,对数据的开发利用成为经济发展和社会进步的主要推动力。在“小数据”时代,由于收集的数据数量比较有限,个人信息处理者可以与信息主体就其中关键信息进行面对面的交流,信息主体可以基于个人信息处理者的充分告知下而作出有效的同意,知情同意规则在此基础上发挥了极其重要的作用。

知情同意机制发挥作用的前提是建立在用户充分知情的基础上。但是进入大数据时代,数据处理的规模之大、种类之多、处理之频繁和复杂远超以往,使得个人信息处理者告知和收集用户同意的成本和难度大大增加。此外,在大数据时代,公权力机关、企业等个人信息处理者依靠大数据处理技术,可以

¹ 《民法典》第 1035 条第 1 款第 1 项: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:(一)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 《个人信息保护法》第 29 条:处理敏感个人信息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。

轻易取得对信息主体的优势地位，由此个人信息处理者和信息主体之间形成了一种极端不对称的信息鸿沟。这种极端不对称的信息鸿沟可能会使个人信息处理者为了追求利润或者效益最大化而忽视知情同意规则的要求。[4]因此以上种种不利原因使得知情同意规则的实行举步维艰，面临诸多困境。

3. 知情同意规则在大数据时代面临的困境

3.1. 用户知情同意的难度较大

在知情同意机制之下，企业一方面要履行告知义务来规避法律风险，一方面又要最大限度地维护企业自身的利益，尽最大努力获取用户同意。也就是说，企业履行告知义务的目的只有两个：规避法律风险和获取用户授权，至于用户是否真正知情和真心同意，企业并不关心。因此，企业一方面会通过制定严密的隐私和个人信息保护政策来从法律形式上履行告知义务，另一方面则通过将政策文件做的冗长难懂、隐藏重要信息等形式来最大限度地获取用户同意。一旦进入实际的隐私政策，访问者很快就会遇到大量的法律术语(如“个人行踪轨迹信息”、“自动化决策”和“匿名化”等等)和技术术语(如“cookie技术”、“网络信标”和“间谍软件/广告软件”等等)。[5]这些无疑都加大了用户知情同意的难度。

3.2. 用户知情同意的能力欠缺

知情同意规则能够发挥立法者预期效果的前提是个人信息主体都是具有知情同意能力的理性人。作为具有知情同意能力的理性人就必须具备一定的法律专业知识和隐私保护意识。但是在现实生活中，大多数用户的法律专业知识缺乏，隐私意识和个人信息保护意识并不强烈。根据美国的一项研究表明，一般上网的人花在一个链接的网页上的时间不超过一分钟，所以很少有人会花时间滚动到首页底部的隐私政策链接，点击显示的小字体链接。[6]此外，由于隐私政策的专业化程度较高，当代隐私政策的语言适合那些至少上过三年大学的人。面对冗长难懂的隐私政策、个人信息保护政策，用户要么因缺少隐私保护意识而不愿意花费太多的时间和精力去仔细阅读，要么阅读之后因缺乏法律知识，难以发现其中与自身利益密切相关的重要信息，导致知情同意规则的实际效果与设计初衷严重背离。

3.3. 用户拒绝的成本太高

在知情同意机制之下，在信息处理者履行告知义务且用户知情之后，用户依然难以做出拒绝的选项。如果信息处理者是公权力机关，用户几乎无法拒绝公权力机关的收集要求。如疫情防控期间，政府收集处于本行政区域公民的个人行踪轨迹信息，用户如果瞒报或者拒绝政府的收集要求，则会面临着行政处罚甚至触犯刑法的风险。如果信息处理者是企业，用户拒绝即意味着无法享受企业提供的服务。如高德地图收集用户的个人行踪轨迹信息来提供导航服务，如果用户不同意高德地图的隐私和个人信息保护政策，用户就无法使用其导航服务。因此，在目前的知情同意机制之下，用户拒绝成本之高让用户不假思索地勾选同意选项几乎成为用户麻木的常规操作。在这种情况下，用户对信息处理者的隐私政策几乎一无所知，知情同意机制实际上变成了一种表面上的、形式上的同意。

3.4. 信息的聚合效应

抛开上述知情同意规则本身面临的困境，即使知情同意规则被很好地执行和遵守，也不能完全保证个人信息可以被很好的保护。以个人行踪轨迹信息为例，在大数据时代，一个人在某一时间某一地点产生某一条个人行踪轨迹信息可能既不属于私密个人信息，也不属于敏感个人信息，对自然人的人身财产权益也不存在风险或者威胁。但是在大数据时代，信息处理者收集了用户大量的个人行踪轨迹信息，通过大数据算法技术分析和人工智能画像，依旧可以推测出信息主体的很多重要敏感的个人敏感信息或习惯，勾勒出信息主体大概的个人形象。这种由信息的聚合效应带来的风险是知情同意规则所难以解决的。[7]

3.5. 知情同意对大数据合理利用的阻碍

在大数据时代，数据取得了和土地、资金、劳动力等生产要素同等的地位，大数据的开发和利用对国计民生的作用难以估量。在这种情况下，过于严格的知情同意规则同时加大了信息处理者处理信息和信息主体获取服务的成本，一定程度上阻碍了大数据的合理利用。在知情同意机制之下，用户没有同意，企业就不能随意处理用户的个人信息，否则就要承担企业违规的风险。企业为了达到合规的目的，必须设计严密的隐私政策并收集用户同意。但是大数据时代的数据处理具有高频率、自动化、专业化、场景化等特点，如果每一次数据处理都要求信息处理者收集用户同意，就会大大降低数据利用的效率，对某些以大数据利用为基础的企业来说，更是一种沉重的负担。

4. 知情同意规则困境的破解之道

4.1. 规范告知的形式

研究表明，用户希望被告知，告知他们是谁正在收集他们的个人信息、正在收集他们什么样的个人信息、如何收集他们的个人信息以及打算用这些个人信息做什么。在知情同意机制之下，知情是同意的的前提，而信息处理者告知是用户知情的前提。因此个人信息处理者在处理个人信息之前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知与个人信息处理直接相关的各项事项。美国联邦贸易委员会(FTC)在其制定的《公平信息实践原则》中提出了五个主要原则，首要原则就是“注意原则”，即企业有义务提醒消费者注意与其密切相关的隐私条款，且消费者不能在没有通知的情况下就其消费行为做出知情的决定。^[8]我国《民法典》第 1035 条第一款将信息处理者履行告知义务的必要条件规定为“公开处理信息的规则”和“明示处理信息的目的、方式和范围”，以此作为衡量企业是否履行告知义务的重要标准之一。但是“信息处理者告知”并不等于“用户知情”。现实生活中，企业的隐私政策为满足合规要求通常都会有这两项内容，但是企业往往将其隐藏在冗长的文字海洋中，用户根本没有耐心也没有能力去看出隐私政策中的重要内容。企业应当向用户提供清晰的、容易理解的隐私政策，并将重点内容进行标注，从而方便用户综合各方面情况做出是否同意的决定。以导航软件收集用户的个人行踪轨迹信息为例，这种收集对企业为用户提供服务是必要的，但是企业应该在其隐私政策中详细说明并且用不同颜色的文字将收集和处理个人行踪轨迹信息的规则、目的、方式和范围以及其他与用户人身财产权益有重大利害关系的内容进行重点标注。

4.2. 规范同意的强度

在民法体系之中，同意是一种意思表示，意思表示是民事主体设立、变更、终止民事法律关系的核心要素。《民法典》第 140 条³规定了明示和默示两种意思表示形式，其中默示又分为作为的默示和不作为的默示，并且规定不作为的默示即沉默“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，才可以视为意思表示”。与之相对应，民法中的同意也具有了三种强度：明示同意、作为的默示同意和不作为的默示同意。在个人信息处理领域，明示同意和作为的默示同意可以看做知情同意机制之下的同意无须质疑，但是沉默是否也可以在个人信息处理领域成为一种同意，学者们争论不一。有学者提出，可以通过相关立法规定在某些特定的情形下，沉默也可以视为个人信息处理中的同意。但是这种观点可能并不符合中国个人信息处理领域的实际情况。^[8]目前来看，没有必要也不应该通过立法将个人信息处理领域的沉默视为同意的意思表示，处理个人信息往往也不涉及到当事人的约定，而企业与

³《民法典》第 140 条：行为人可以明示或者默示作出意思表示。沉默只有在有法律规定、当事人约定或者符合当事人之间的交易习惯时，才可以视为意思表示。

用户之间的隐私政策的同意(即使这种同意是经常性的)也不能视为民事活动中的交易习惯。此外,个人信息处理不同于普通的民事法律行为,个人信息处理会涉及到民事主体重大的人身财产权益。如果将个人信息处理领域中当事人的沉默在特定情况下也视为知情同意机制的同意,可能会严重损害信息主体的信息自决权,使知情同意机制完全沦为企业获取用户个人信息的程序性手段。知情同意机制之下的同意应当只包括明示同意和作为的默示同意,不包括沉默即不作为的默示同意。因此个人信息处理者不能将用户沉默视为同意,处理用户个人信息必须取得用户的明示同意或作为的默示同意。《个人信息保护法》第29条还对敏感个人信息提出了单独同意规则,提高了对敏感个人信息的同意要求。一般个人信息往往是通过隐私政策进行一揽子授权就可以处理,而敏感个人信息则必须取得单独同意才可以处理。这在实践中主要表现为两种情形:(一)同时处理一般个人信息和敏感个人信息。如互联网企业同时收集用户的姓名、年龄、职业、个人行踪轨迹信息,在这种情况下,对于姓名、年龄、职业等一般个人信息可以通过一揽子授权获得同意即可进行处理,但是对于个人行踪轨迹信息这种敏感个人信息则必须另外进行单独授权同意才可以处理。(二)同时处理多种敏感个人信息。如互联网企业同时收集用户的生物识别信息、医疗健康信息、行踪轨迹信息等多种敏感个人信息,则对于每一项敏感个人信息都必须取得用户的单独授权同意才可以进行处理。

4.3. 为用户提供更多的选择

互联网企业的隐私是互联网企业向用户解释如何收集、使用、加工、传输用户提供的个人信息的书面描述和通行做法。但是目前互联网企业的隐私政策几乎都是以一种“全有或全无”形式来完成知情同意机制之下的合规要求。以打车软件收集个人行踪轨迹信息为例,要么完全同意打车软件关于收集用户个人行踪轨迹信息的隐私政策,要么放弃使用打车软件的服务。用户几乎没有第三种选择,只能选择全部同意打车软件的隐私政策。但是不同的用户可能会对愿意提供的个人信息有不同的同意程度,有的用户愿意提供全部的个人信息,有的用户只愿意提供与服务直接相关的那部分个人信息,有的用户只愿意提供部分个人信息来换取部分服务。但是这种“全有或全无”的二选一的隐私政策,几乎没有给用户任何选择的余地。此外,在大数据时代纷繁复杂的个人信息处理事务中试图寻求整齐划一、“全有全无”的知情同意规则也是不合理的。为了应对这种情况,《个人信息保护法》第16条⁴对个人信息处理者因信息主体不同意提供个人信息而拒绝提供服务的做法进行了限制,这是一个良好的开端,互联网企业应该按照《个人信息保护法》第16条的规定对本企业的隐私政策做出相应的调整。企业的隐私政策中应当有征询信息主体同意偏好的特别设计,并提供满足不同需求的同意选项。以交友软件为例,交友软件收集用户的位置信息来为用户推荐附近的人,但是部分用户可能只愿意提供自己的性别、年龄、学历等信息,而不愿意提供位置信息,该部分用户并不在意对方位置的远近,只是通过交友软件认识新的朋友。这种情况下,交友软件应该允许用户不提供位置信息,而依然提供除需要位置信息才能进行的其他服务。

4.4. 允许用户参与

2000年,美国联邦贸易委员会敦促美国国会通过立法,要求公司在采取其他隐私保护措施的同时,“向消费者提供访问网站收集的有关他们的信息的合理途径,包括审查信息、纠正不准确信息或删除信息的合理机会。”^[9]我国《民法典》第1037条⁵也赋予了自然人对其被收集的个人信息的查阅权、复制

⁴《个人信息保护法》第14条:个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由,拒绝提供产品或者服务;处理个人信息属于提供产品或者服务所必需的除外。

⁵《民法典》第1037条:自然人可以依法向信息处理者查阅或者复制其个人信息;发现信息有错误的,有权提出异议并请求及时采取更正等必要措施。自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的,有权请求信息处理者及时删除。

权、异议权、更正权和删除权，这一条与知情同意规则密切连接，是知情同意机制能够发挥其应有作用的重要保障。但是在实践中，《民法典》第 1037 条并没有被很好地贯彻和执行。以个人行踪轨迹信息为例，在用户勾选互联网企业的同意选项之后，用户几乎很难再参与和控制自己的个人行踪轨迹信息。用户不知道自己的个人行踪轨迹信息是否只被用于提供和改善服务、收集者有没有对自己的个人行踪轨迹信息采取必要的安全措施、有没有提供给第三方使用、有没有被其他组织或个人收集或盗取并用于违法犯罪活动等等。企业等个人信息处理者应该允许用户参与其被收集的个人信息的监管过程，充分保证信息主体的查阅权、复制权、异议权、更正权和删除权，以保持个人信息的完整性、准确性和安全性，防止个人信息处理者违法或违约处理用户的个人信息，确保被收集的个人信息在处理在合法和提前约定的范围内。

4.5. 加强执法监管工作

在个人信息被广泛收集和处理的的大数据时代，单纯依靠知情同意机制和个人对信息的自我管理和控制，远远不能达到控制标准。除了通过事先通知取得信息主体同意的知情同意机制之外，还应采取相应的措施来加强个人信息处理过程中的执法监管工作。从比较法的角度来看，世界上主要的监管模式有两种：一种是欧盟的统一监管模式。2018 年 5 月 25 日出台的欧盟《通用数据保护条例》(General Data Protection Regulation, 以下简称 GDPR)明确规定各欧盟成员国建立一个独立的、专门的个人信息保护机构来负责监督 GDPR 的实施。一种是美国的分散监管模式。美国没有指定统一的《个人信息保护法》，也没有建立一个统一的个人信息监管机构，而是由美国联邦贸易委员会(FTC)、美国联邦通信委员会(FCC)、美国消费者金融保护局(CFPB)等机构分别在贸易、通信、金融等各个领域来保护消费者的隐私权益。^[10]而我国的个人信息监管模式则是两者的结合。《个人信息保护法》第 60 条⁶规定，国家网信部门负责统筹协调国务院其他有关部门共同对个人信息的处理和使用进行监管。但是根据《中华人民共和国网络安全法》(以下简称《网络安全法》)的有关规定，设立国家网信办的目的是保障网络安全，维护网络空间主权和国家安全、社会公共利益，国家网信办的工作重点要放在重大国家和社会安全网络事件的监管上，个人信息保护监管并不是其主要工作重点。大数据时代，信息交换量巨大，涉及领域全面多样。分散的监管执法工作效率将明显低于统一的个人信息保护部门，容易在个人信息不受重视的领域出现监管空白，或出现各方推诿拖延的情况，或出现监管重复的问题。随着信息和数据的全球化，个人信息的跨境流动也需要特别的关注和保护。在这种形式之下，设立专门机构负责个人信息保护的执法和监督已成为近年来个人信息保护领域的主要趋势。欧盟的统一监管模式显然对中国有更大的借鉴意义，更符合我国平衡个人信息的流动和利用与个人信息保护的现实需要。因此，为了保持监管机构的独立性和统一性，中国应该设立专门的个人信息保护机构，整合国家网信办和国务院各部门现有监管职能，加强对个人信息保护的执法监管工作。该机构将专门负责保护境内和跨境个人信息，为公民个人提供便捷的一站式维权服务，对个人信息的处理和使用进行严格监督。一旦发现侵害公民个人信息的违法行为，可根据情节轻重，责令违法的个人信息处理者立即改正，并对其进行相应的处罚，从而实现对个人信息的保护的全过程控制和监管。^[11]

5. 结语

在大数据时代，个人信息在政府管理、社会治理、商业利用、疫情防控、犯罪追踪等各方面发挥着越来越重要的作用，个人信息的保护和利用已经成为一个非常重要的问题。知情同意规则作为个人信息

⁶《个人信息保护法》第 60 条：国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

保护的“帝王条款”，在大数据时代面临着诸多困境，主张放弃知情同意规则的说法甚嚣尘上。但是我们必须看到轻易放弃知情同意规则不是一种明智的选择，知情同意规则作为个人信息处理者收集个人信息的合法性基础，在大数据时代依然有其存在的必要性。目前我国《民法典》和《个人信息保护法》对知情同意规则的设计还不够完善。我们应该从知情同意规则所确立的“告知-知情-同意”三个环节上寻求破解困境的出路，对传统的知情同意规则进行重塑，从规范告知的形式、规范同意的强度、为用户提供更多的选择、允许用户参与、加强执法监管等多方面增强知情同意规则的有效性，从而使知情同意规则在大数据时代发挥其应有的功能，更好地构建个人信息保护体系。

参考文献

- [1] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
- [2] 万方. 隐私政策中的告知同意原则及其异化[J]. 法律科学(西北政法大学学报), 2019, 37(2): 61-68.
- [3] 吕炳斌. 个人信息保护的“同意”困境及其出路[J]. 法商研究, 2021, 38(2): 87-101.
- [4] 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[J]. 经贸法律评论, 2021(1): 47-59.
- [5] 程啸. 论个人信息处理中的个人同意[J]. 环球法律评论, 2021, 43(6): 40-55.
- [6] 范海潮, 顾理平. 探寻平衡之道: 隐私保护中知情同意原则的实践困境与修正[J]. 新闻与传播研究, 2021, 28(2): 70-85, 127-128.
- [7] 程啸. 论个人信息处理者的告知义务[J]. 上海政法学院学报(法治论丛), 2021, 36(5): 67-80.
- [8] 李勇. 论消费者个人信息之保护——以告知后同意为中心[J]. 理论月刊, 2014(8): 124-128.
- [9] 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[J]. 法制与社会发展, 2018, 24(6): 111-136.
- [10] 林涸民. 个人信息保护中知情同意原则的困境与出路[J]. 北京航空航天大学学报(社会科学版), 2018, 31(3): 13-21.
- [11] 尹博文. 个人数据交易中知情同意规则的破局与重构[J]. 科技与法律(中英文), 2022(5): 85-94.