武漢大學學報(哲学社会科学版)
WUHAN UNIVERSITY JOURNAL (Philosophy & Social Science)
第72卷第5期 2019年9月
Vol. 72 No. 5 Sept. 2019 119~129
DOI:10.14086/j.cnki.wujss.2019.05.012

个人信息保护中“同意”规则的规范构造

陆 青

摘 要 权利人同意是个人信息处理的正当性基础之一,同意既可能构成合同等交易行为的给付内容,也可以是单纯表达对他人商业利用不法性的排除。两者分别体现了权利人对其个人信息的积极和消极控制。同意在法律性质上属于意思表示,因此对同意规则的规范构造可以从意思表示的方法(包括明示、默示,原则上不包括沉默)和实质要求(包括意思自治、知情同意和弱者保护)加以展开。主张任何信息在收集、使用上都必须得到用户(明示)同意,或者相反,主张一般信息都可以通过默许同意的方式取得用户授权,都是不可取的。同意的例外规则需要再整合,特别是根据个人信息主体要求签订和履行合同所必需的信息无须适用同意规则。

关键词 个人信息权;数据保护;同意规则;意思表示;大数据时代;新兴权利
中图分类号 D913 **文献标识码** A **文章编号** 1672-7320(2019)05-0119-11
基金项目 浙江大学“人工智能与法学”专项资助项目(18DFX009)

随着大数据时代的到来,个人信息的保护问题引起了人们普遍关注。对此,《民法总则》第110条规定:自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的,应当依法取得并确保信息安全,不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息,但对何为“依法取得”和“非法”并未作直接规定。而在此之前出台的一系列规范,如全国人大常委会2012年通过的《关于加强网络信息保护的决定》第2条,2013年修正的《消费者权益保护法》第29条、工信部2013年通过的《电信和互联网用户个人信息保护规定》(以下简称《个人信息保护规定》)第9条,2014年最高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》(以下简称《网络侵权司法解释》)第12条,2016年全国人大常委会通过的《网络安全法》第41、42条,均提及在收集、使用或利用个人信息时原则上须经个人(用户)同意。2013年工信部实施的首个个人信息保护国家标准《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》(以下简称《指南》),2017年国家标准化管理委员会颁布的《信息安全技术个人信息安全规范》(以下简称《规范》)则对同意规则有丰富细致的表述。但必须说明的是,不同公私法规范下的同意规则并不完全一致。比如,《网络安全法》第42条第1款明确提到未经被收集人同意,不得向他人提供个人信息,除非是经过处理无法识别特定个人且不能复原的。《网络侵权司法解释》第12条提到网络用户或者网络服务提供者利用网络公开个人隐私和其他个人信息,造成他人损害的原则上应当承担侵权责任。在免责规定中,仅第1项和第3项中提到须经“书面同意”,而第2、4、5、6项均未提及公开个人信息须经个人同意或书面同意。

一、问题的提出

综合比照前述法律文件,存在以下问题值得深入研究。第一,前述各条文所称“同意”究竟属于何种法律性质,其与收集、使用个人信息的“双方的约定”是否存在本质差别。第二,在同意的具体规范要求上,同意的形式和内容均有何种限制要求。比如,收集、使用个人信息是否均须征得个人/消费者/用户的知情并同意,同意是否或者何种情况下必须以明示、书面方式作出;“收集、使用个人信息”是否也涵盖“向他人提供”“公开”个人信息等情况。第三,同意规则是否应有例外,如有,包括哪些情形。

前述问题涉及对个人信息保护中同意规则的规范构造,理论争议颇多。近年来,更有学者从同意基础的理论根基不牢固、同意缺乏必要性和真实性、同意基础不符合经济考量、例外规则的大量存在削弱了同意基础的效力等角度对同意作为个人信息处理正当性基础提出了深度质疑[1](P128-132)。不过,在笔者看来,设置同意规则的根本目的在于保护个人对其信息的自决权益,以最大程度地捍卫个人尊严和行动自由。能不能行使自己的权利和是否享有该权利是两回事。对于个人信息的控制能力,我们不能简单地理解为数据主体在事实层面的实际控制力。这种控制力,恰恰体现在法律对数据主体所赋予的权利以及配套的保护和救济措施之上。从存在大量同意规则的例外这一点上,并不能当然地得出同意不能作为合法性基础的结论,毋宁是提醒我们要关注个人信息保护和数据促进利用,私人权利和公共利益之间的冲突和平衡问题,从而建构更为弹性合理的规范机制。更何况,考虑到我国现行法上的制度安排,如何科学建构同意规则的规范体系显然是更为现实和迫切的话题。无独有偶,在 2018 年 5 月生效的欧盟《一般数据保护条例》(以下简称《条例》)中,同样以用户同意作为首要的合法性基础来建构个人数据保护的一般规则[2](P47-49)。

基于此,笔者将结合同意的法律性质、规范要求和例外制度设计三方面,结合比较法经验,审视本国法上“同意规则”的规范构造。须补充说明的是,从个人信息权益保护的角度,本文旨在从私法层面对同意的法律性质的探讨出发去勾勒同意规则的规范内容,但分析的内容并不局限于私法性质的规范层面,目的在于最大限度地对现行法上的多元规范,甚至包括相关国家标准进行梳理、评价。

二、“同意”的法律性质

在我国法上,鲜有学者对个人信息使用中的“同意”的法律性质作出专门讨论。而在相关规范表述上,“同意”和“约定”时而分列,时而合并。比如,在《消费者权益保护法》第 29 条第 1 款中,第一句提到“经营者收集、使用消费者个人信息,应当……并经消费者同意”,第二句提到“经营者收集、使用消费者个人信息……不得违反法律、法规的规定或双方的约定收集、使用信息”,似乎有意将同意收集、使用和按照双方的约定收集、使用信息区别开来(类似的表述方式也可见《网络安全法》第 41 条第 1 款和第 2 款)。而最高人民法院《网络侵权司法解释》第 12 条中则使用“经自然人书面同意且在约定范围内公开”的表述(虽然未采用更易理解为合同性质的“双方的约定”的表述)。那么,同意行为与“约定”是否有规范差异,其是否属于一个相对独立的法律行为? 需要说明的是,明确同意的法律性质,不仅关涉同意能力上的要求和未成年人保护,还与该种同意可否撤销、撤回等问题密切相关。

对此解释上的困惑,笔者认为,首先需要对现行民法上“同意”一词的规范表达进行体系性的梳理。具体来说,民法上关于“同意”一词存在多种用法,具体包括法定代理人同意、担任监护人所需机关同意、合同权利变动时须经对方当事人同意、对合同中承诺的界定、物权处分上的同意、军婚离婚的同意、以营利为目的使用肖像的同意、医疗行为中患者与近亲属的知情同意、公开病例资料和隐私的同意等。不同的同意规则,针对的内容各不相同,有的涉及身份关系,有的涉及财产关系,有的处在合同关系之中,有的则并无合同关系,因此必须结合同意规范的具体情境判断其法律性质。而最后三项同意规则与本文讨论主题关系最为密切,须作进一步说明。针对以营利为目的使用肖像的同意在《民法通则》第 100 条中

有所体现，该条间接肯定了在经得同意下人格权商业化利用的可能。对于这种商业化利用，有学者认为，其并非在人格权之外创设一项独立的权利，而是基于人格权可能包含的财产利益，将包含于权利客体当中的使用价值，通过让位使用等方式转化为具有流通性财产利益，进而为权利人现实享有[3]（P11）。尽管该条并未明确这种商业化利用的方式（有偿无偿，订立或不订立合同），但可以肯定的是，法律对人格权商业化利用可能性的确认，主要集中在促进人格权权能由消极向积极扩张上，即从消极对抗外来侵扰转向对人格要素的积极利用。这就意味着，肖像权人对他人商业利用的同意，并不仅仅限制于对自身权利的消极保护，还包括通过合同授权许可使用其肖像中所承载的财产性要素。因此，此处的同意既可能构成合同等交易行为的内容，也可以是单纯表达对他人商业利用不法性的排除，分别体现了权利人积极和消极的控制。针对医疗行为中的知情同意在《侵权责任法》第 55 条中有所体现。该条并未笼统地规定所有的诊疗活动都需要经过患者同意，而是区分了两种不同的类型：就病情和医疗措施，医务人员仅有告知义务，而需要实施手术、特殊检查、特殊治疗的，医务人员不仅需要告知，还必须得到患者或近亲属的书面同意。该条中的“同意”，显然并不涉及人格要素的积极利用，而是在消极控制层面排除了医务人员行为的不法性。学理上将这里的“同意”作为侵权法上的免责事由归入“受害人同意”的范畴，在构成要件上包括必须有明确具体的内容，受害人须具有同意能力，同意必须真实自愿，加害人必须尽到充分的告知说明义务，不得违反法律的强制性、禁止性规定以及公共秩序、善良风俗。在同意能力的要求上，学者明确指出，此种“同意能力不同于行为能力。在法律行为制度中，为了维护交易安全而要求从事法律行为的当事人必须具备行为能力。但是，受害人的同意是其对自己权利的处分，因此不能完全适用民法中关于行为能力的规定。德国民法通说认为，受害人的同意能力不能以有行为能力作为判断标准，应依据个别案件中受害人的识别能力作为标准。……一些重大手术如器官切除手术，则无行为能力人或限制行为能力人没有同意能力，必须经过法定代理人的允许”[4]（P304）。此处对当事人同意能力的要求并无绝对的年龄限制，而是根据所涉医疗行为对身体的介入程度来具体判断当事人对行为后果的识别能力；关于公开病例资料和隐私的“同意”，在《侵权责任法》第 62 条有所体现。从内容上，该条仅限于规范相关个人信息的公开问题。此处的同意在本质上涉及主体对其个人人格要素的消极控制，即允许个人自由地决定如何处理自己的身体及相关信息，进而以同意来排除他人相关处理行为的不法性。

前述分析可以为我们研究个人信息保护上的同意性质提供一些规范思路：第一，个人信息既存在消极防御的问题，也存在积极利用的问题。相应的，此种同意也必须结合具体语境判断其性质：在排除他人使用、公开个人信息的不法性层面，权利人同意无须具备行为能力；而在积极授权他人商业利用个人信息时，同意可能成为相关合同给付内容的一部分，因此当事人须具备相应的行为能力。如此理解，也符合《消费者权益保护法》和《网络安全法》将同意和“双方的约定”分别规定的文义结构。第二，从前述关于医疗行为同意问题的讨论可知，若干预身体的行为，除涉及重大手术须经法定代理人同意外，原则上无须具备行为能力。那么，举重以明轻，在涉及与人身关系紧密程度往往更弱的个人信息问题上，消极同意的作出同样无须具备行为能力，而只须考察其是否具备相应的意思能力。第三，在存在医疗合同关系的场合，前述《侵权责任法》第 62 条规定：病历资料和其他隐私信息的公开，必须经过患者同意。这意味着，即使当事人之间存在合同关系，对个人信息处理上的同意依然具有独立的规范意义。换句话说，除非明确约定或者基于相关的附随义务，否则存在合同关系本身并不当然地意味着在对当事人个人信息处理的同意。

进一步需要说明的是，传统民法上区分以意思表示为核心要素的法律行为和作为意的表达的准法律行为。既然在消极防御层面，信息主体的同意并不构成法律行为，因此不乏学者将此种同意行为界定为准法律行为的性质，强调权利人的同意并非直接实现其所欲实现的特定法律效果。同意虽然必须依靠当事人意愿的表达，但其之所以能产生排除他人行为不法性的效果，乃是基于法律的直接规定。由此也

可以解释,为何信息主体表达同意时无须具备行为能力[5](P144)。不过,这种观点显然值得商榷。一则意思表示虽然是法律行为的核心要素,却并不意味着意思表示的作出必须具备法定的行为能力。事实上,具备何种意思能力取决于具体情境下当事人所作意思表示的能力要求,也即行为人实践自身的自由意志,并承担相应的法律后果的能力要求。这种意思能力,在合同交易上体现为行为能力的要求,在缔结婚姻的行为上体现为结婚能力的要求。然而,在个人信息处理上,表达同意的能力要求必须结合具体的信息处理情境,比如个人信息使用、收集、公开的具体内容、对权利人可能造成的影响等多种要素加以综合判断。二则无论是在积极利用还是消极防御层面,信息主体同意他人处理其个人信息,旨在践行个人的行动自由和信息自决,实现的正是其所欲实现的法律效果。倘若认为相关法律效力并非直接来自当事人的同意,而是来自法律规定,则事实上削弱了同意作为意思表示可能具有的规范表达空间。三则将同意界定为意思表示,这在比较法上也能得到印证。比如《欧洲一般数据保护条例》中,就将同意界定为是"数据主体通过声明或明确肯定方式,依照其意愿自愿作出的具体的、知情的及明确的意思表示,意味着数据主体同意其个人数据被处理"[2](P228)。

个人信息处理上的同意作为意思表示,本不合适划定统一的能力要求,但基于未成年人保护的特别考虑,欧洲法上的《条例》专门规定"关于直接向儿童提供信息社会服务的,对 16 周岁以上儿童的个人数据的处理为合法。儿童未满 16 周岁时,处理在征得监护人同意或授权的范畴内合法。成员国可以通过法律对上述年龄进行调整,但不得低于 13 周岁"并规定"第 1 款不应影响成员国的一般合同法律,如与儿童有关的合同要件或效力"[2](P232)。我国法上,也有学者认为未成年人的理解能力判断标准如果不明确,不利于保护未成年人的合法权益,故建议采《规范》第 5.5(c)的规定,以 14 周岁为界决定其同意能力;收集不满 14 周岁的未成年人的个人信息,应征得其监护人的明示同意。从更好地保护未成年人信息自决权益的角度,未来立法的确有必要作明确规范。

进一步需要讨论的是,对个人信息处理的同意是否可以随时撤回或撤销。在欧洲法上,《条例》第 7 条第 3 款规定,"数据主体有权随时撤回其同意。同意的撤回不应影响在撤回前基于同意作出的数据处理的合法性。在作出同意前,数据主体应被告知上述权利。撤回同意应与作出同意同样容易"[2](P232);第 21 条规定,"1. 数据主体有权在特定情况下随时反对依据本条例第 6 条第 1 款(e)项或(f)项规定对其个人数据进行的处理,包括根据这些条款进行的数据画像。除非控制者能够证明其合法利益高于数据主体的利益、权利和自由,或者法定请求权的确立、行使和抗辩有更强有力的法律依据。2. 若为直接营销目的处理个人数据的,数据主体有权随时反对因为该商业目的处理其个人数据,包括与直接营销有关的数据画像。……"[2](P241-242)之所以允许数据主体原则上可以随时撤回或撤销其同意,或行使反对权,目的在于维护数据主体的个人信息自决权,避免个人尊严和行动自由受到之前同意表示的拘束,进而妨碍其人格的自由塑造。在我国法上,也有学者在探讨人格权的商业化问题时,从人格自治的角度出发,指出"虽然人格权商业化是主要基于自愿选择的结果,但是,随着主客观环境的变迁,这种许可有可能会演变成对权利人人格发展的限制。在这种情形下赋予权利人撤回许可的权利,也是为了维护许可人的人格自治利益的需要。为了保障合同相对人的交易安全,必须对撤销权行使的条件加以明确。并且因行使撤销权对无过错一方造成损害的,应由权利人承担相应的赔偿责任"[3](P15)。对此,笔者认为,同样需要延续此前关于同意性质的讨论,区分侵权和合同两种不同语境加以分析。若对个人信息的同意并不直接涉及合同交易领域,而仅消极表达对他人行为违法性的排除,此种"受害人的同意无须向行为人送达,但是在他人的加害行为实施之前,该同意可以随时撤回"[4](P302)。个人信息权利主体的同意与其尊严和行为自由紧密相关,属于个人信息自决的具体体现。除非涉及公共利益等特殊情形,原则上可以随时撤销或撤回(具体是撤销还是撤回取决于是否已经发生效力);而在合同领域,若同意他人处理个人信息是交易内容的组成部分,尤其是仅与个人信息的财产价值相关而并不直接影响当事人

的人格发展,应当对当事人撤回或撤销同意加以限制,对作为合同相对人的数据处理者,应赋予主张损害赔偿的权利。但具体的交易领域,如涉及赠与合同任意撤销权、委托合同和承揽合同中的任意解除权以及消费者领域针对弱势主体信息不对称的反悔权等规则是否可以扩大或类推适用,应结合具体合同关系再作判断。

三、“同意”的规范要求

前文提到“同意”在法律性质上属于意思表示。因此,从“同意”的形式和实质来看,都应符合意思表示相关的规范要求。

(一)“同意”的形式要求

《关于加强网络信息保护的决定》《个人信息保护规定》等均未就同意的方法作出规定,而《网络侵权司法解释》第 12 条第 1 款第(一)(三)项中提到:网络用户或者网络服务提供者利用网络公开个人隐私和其他个人信息须经自然人的书面同意,否则网络用户或者网络服务提供者应承担相应的侵权责任。但此项规定是否可以类推到网络服务之外的领域以及公开之外其他利用个人信息的场合,依然有待商榷。

值得关注的是,在国家标准层面,《指南》第 5.2.3 条中明确规定:处理个人信息前要征得个人信息主体的同意,包括默许同意或明示同意。收集个人一般信息时,可认为个人信息主体默许同意,如果个人信息主体明确反对,要停止收集或删除个人信息;收集个人敏感信息时,要得到个人信息主体的明示同意。根据《指南》的该规定,个人敏感信息是指一旦遭到泄露或修改,会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。个人一般信息是指除个人敏感信息以外的个人信息。默许同意是指在个人信息主体无明确反对的情况下,认为个人信息主体同意;明示同意是指个人信息主体明确授权同意,并保留证据。2017 年国家标准化管理委员会颁布的《规范》丰富了个人敏感信息的内容,同时对同意的方法进行了改造。其规定,对于一般的个人信息收集仅在特殊情况下要求明示同意;而针对敏感信息必须得到明示同意。明示同意是指个人信息主体通过书面声明或主动做出肯定性动作,对其个人信息进行特定处理做出明确授权的行为。同时,肯定性动作包括个人信息主体主动作出声明(电子或纸质形式)、主动勾选、主动点击“同意”“注册”“发送”“拨打”等。

前述《规范》对一般信息和敏感信息的区分,对明示同意的界定方式(包括对“肯定性动作”的表述),似乎受到欧洲法的影响。不过,与中国法不同,欧盟的《条例》在“鉴于条款”第 32 项提到,同意可以通过书面陈述(包括电子形式)或者口头声明。同意方式可以包括在浏览网页时在方框里打钩,对信息社会服务进行技术设置或者其他陈述或行为以清楚表示接受对其个人数据的处理。因此,沉默、默认勾选的对话框或者不作为不构成同意。可见,同意必须以积极、主动的方式作出。而针对特殊类型的个人数据处理、包括数据画像在内的自动化决策、向第三国或国际组织传输个人数据(第 49 条)三种特定情形,《条例》还提出了“明确同意”的要求。“明确同意”并不意味着一定需要有书面和签字盖章的声明,甚至可以是口头的声明,但必须针对数据处理有特定、清楚的表示,且这种表示是建立在对特定场合下个人信息保护上存在的风险有充分了解的基础之上的。与欧盟的《条例》对比后可以发现,在我国法上,《规范》中的“明示同意”似乎在规范要求上恰恰处在欧洲法的“同意”和“明确同意”之间。《规范》所提到的“明示同意”仅针对敏感信息和特殊情况下的一般信息收集,而其规范内容包括了以肯定性动作的方式表示同意,似乎对于其他场合个人信息的收集不需要“书面声明或主动做出肯定性动作”。

对此,笔者认为,既然同意的法律性质是意思表示,那么在现行法层面,就应从意思表示的规范出发探讨同意作出的方式。对此,《民法总则》第 140 条规定: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。按相关释义

书,所谓明示的意思表示,是指行为人以作为的方式使得相对人能够直接了解到意思表示的内容,包括表意人采用口头、书面方式直接向相对人作出的意思表示;默示方式作出的意思表示,是指行为人虽没有以语言或文字等明示方式作出意思表示,但以行为的方式作出了意思表示。也就是说可以通过行为推定出其作出一定的意思表示;沉默是一种既无语言表示也无行为表示的纯粹的缄默,是一种完全的、纯粹的不作为[6](P434-435)。结合该条规定,笔者得出如下意见。

第一,既然同意是意思表示,个人信息保护中明示同意、默示同意甚至以沉默方式的同意也应遵循相同的规范界定,尤其是沉默仅在法律规定、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。"默许同意"的表达,容易混淆默示和沉默的规范差异,应当慎用。

第二,如果能够确定意思表示的内容,明示和默示本身地位相同,而明示的方式包括书面和口头形式。在网络领域,个人信息的公开是否应按前述司法解释,一定要自然人采取书面形式表示同意,笔者持保留意见。但对于敏感信息,现行法仅在国家标准层面提出特别的保护要求,显然并不足够。未来立法可以考虑借鉴欧洲法,在明示同意的基础上,针对敏感信息提出更高的规范要求(即采"明确同意"标准)。

第三,沉默在现行法上本就是意思表示例外的表达方式,因此,个人信息保护中的同意原则上也不能以沉默的方式作出。在网络语境下强化个人信息保护的角度,有必要借鉴欧洲法的规定,明确在网络服务领域沉默(不作为)以及默示勾选的对话框不能构成同意。

(二)"同意"的实质要求

对于个人信息保护上的同意的实质要求,现行法并无直接阐释,而仅在原则层面强调"收集、使用个人信息,应当遵循合法、正当、必要的原则"(如《消费者权益保护法》第 29 条)。笔者认为,在实质要求上存在不同的规范进路。

1. 基于意思自治的规范要求。根据传统民法,意思表示不仅须满足表示能力上的要求,还必须真实、自由。《合同法》强调自愿原则,《民法总则》在民事法律行为一章,就虚假表示、重大误解、欺诈、胁迫、显失公平的法律行为撤销和违反强制性规定与违背公序良俗、恶意串通的法律行为无效作了专门规定,目的在于保障当事人的意思自治。实际上,不仅法律行为本身不能有瑕疵,作为法律行为要素的意思表示同样不能有瑕疵。如果存在各种瑕疵,即使并未构成法律行为,相关意思表示也可适用或准用相关规范加以撤销。具体到个人信息保护领域,就不真实自由的同意意思表示,也应有前述规范的适用空间。

在判断同意的表达是否真实自由的问题上,比较法上可以提供一些经验。在欧洲法上,《条例》在对同意的定义中明确将"自由作出"作为第一实质要素。《条例》第 7 条中规定:当评估同意是否是自愿作出时,应尽最大限度地考虑合同的履行包括服务的提供是否以基于不必要的同意个人数据处理为条件。"鉴于条款"第 43 项中进一步说明:"为确保同意是自愿作出的,在特定情形下,数据主体与控制者之间是不平等的,特别是当控制者是公权力一方且基于特定情形下予以考虑的所有条件认为同意不可能是自愿作出的,该同意并不能成为该特定情形个人数据处理的有效法律依据。如果不允许对不同的个人数据处理操作分别作出同意,尽管这对于个别案例来说是恰当的,或者尽管同意并不是合同履行的必要条件,若包括服务条款的合同履行是以同意为基础的,则同意被推定为并非自愿作出的。"[2](P197)因此,当事人的地位是否平等,不提供信息是否会对数据主体带来实质上的不利益,同意是否是合同履行的条件甚至是对待给付的内容,这些都会影响对同意自愿性的判断。

欧洲法对"自愿作出"的规范逻辑,重在强调"尽最大限度地考虑合同的履行包括服务的提供是否以基于不必要的同意个人数据处理为条件"。而在我国法上,"同意"和"必要"是个人信息收集合法性的两个必要条件。《个人信息保护规定》第 9 条第 3 款提到不仅需要个人同意,而且电信业务经营者、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;《网络安全法》第 41 条要求网络

运营者不得收集与其提供的服务无关的个人信息。不过,在欧洲法上,如果对个人信息的处理是履行合同包括提供相关服务所必需的,除非涉及敏感信息,一般不需要用户再表示同意,盖此时处理个人信息的合法性基础在于合同本身。中国法上不分场景地一味要求“必要 + 同意”,存在过于严苛的问题,反而影响了同意规则的有效实现。事实上,在网络服务合同领域,除个人信息的提供直接构成合同给付义务的组成部分外,基于《合同法》第 60 条第 2 款的诚信原则下的附随义务,或者基于《合同法》第 42 条推演出的“先合同义务”,同样可以推演出个人提供履行受领所必要个人信息的义务。在这些场合,即使网络服务商采用的是“使用即同意”的条款,同样无须再就相关信息的收集征得用户的明确授权同意。

因此,在网络服务合同关系中,判断同意是否自由作出的问题,就可能转化为如何去解释提供相关的个人信息是否属于“合同履行之必要”。对此,在立法没有具体明确的情况下,单纯依靠诚信原则、合同目的解释等传统民法方法去判断显然有些捉襟见肘。有学者认为应该重新审视传统的个人信息保护架构,对信息最小化原则或必要性原则进行重新诠释,即主张一种场景和风险导向的新架构:“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。”[7](P109)这显然是一种值得推崇的更为弹性、情境化的判断思路。

2. 基于知情同意的规范要求。严格来说知情是同意的内在规范要求。同意的前提是信息控制者的充分告知,只有充分了解同意所针对的内容,权利人才能做出有效的同意。现行法上,就信息处理者的告知义务范围,主要包括:(1)收集、使用信息的目的、方式和范围(《个人信息保护规定》第 9 条第 2 款;《消费者权益保护法》第 29 条第 1 句;《网络安全法》第 41 条);(2)公开收集、使用规则(《消费者权益保护法》第 29 条第 2 句;《网络安全法》第 41 条);(3)查询、更正信息的渠道(《个人信息保护规定》第 9 条第 2 款);(4)拒绝提供信息的后果等事项(《个人信息保护规定》第 9 条第 2 款)。

同样在知情同意的规范要求上,欧洲法的要求显然更为详细。欧盟“个人数据保护工作组”认为,充分告知与个人数据处理相关的信息,是数据主体实施同意的本质要求,否则所谓个人控制实为形同虚设。而要取得一项有效的同意,数据控制者最低程度必须告知以下信息:(1)控制者的身份;(2)每项需要征得同意的数据操作的目的;(3)何种类型的数据会被收集或使用;(4)存在撤回同意的权利;(5)根据《条例》第 22 条第 2 款(c)项,使用的数据将会用于对数据主体具有重要影响的自动化决策;(6)由于缺乏充分性决定,或缺少根据《条例》第 46 条的适当保障,数据传输可能带来的风险[8](P16)。《条例》第 7 条第 2 款要求:如果数据主体通过书面声明的方式作出同意,且书面声明涉及其他事项,则要求数据主体表示同意的请求应以易于理解、易于获得且与其他事项显著区别的形式以清楚平实的语言呈现。“鉴于条款”第 32 条提到:若需要以电子形式请求数据主体作出同意的,则此等请求必须清楚、简明,且不会对所使用的服务造成不必要的干扰。与欧洲法相比,中国法上在告知的内容范围上相对狭窄,就信息控制者的身份、存在撤回同意的权利、是否会用于自动化决策、数据传输可能存在的个人信息保护上的风险等均未有所要求;在告知的方式上,并未强调必须以清楚平实的语言呈现。无论是告知内容还是告知方式,均有进一步通过立法加以完善的空间。

需要补充说明的是,就信息处理者的告知义务,现行法不同程度地都提到应当明确告知用户收集、使用信息的目的、方式和范围。“明确”一词,旨在强调告知的内容不能模糊宽泛,而必须满足同意作为意思表示的特定性要求。这一点对于个人信息保护显然尤为重要,可以有效地防止“功能潜变”,也即获取信息的原来目的被悄悄地、不知不觉地扩大到包括未获得参与者知情和自愿的同意,进而使个人失去对其数据的控制的现象的产生。所以,如果数据控制者要基于其他新的目的处理数据,除非有其他合法性基础,则必须寻求数据主体进一步的同意,而且不同处理目的之间要求一定的间隔尺度。在这一点上,欧洲法上还进一步要求,数据处理者要就每个特定目的的数据处理告知数据主体相关的信息,以征得后者就每项处理事实的同意,如此确保数据主体能清楚意识到不同选择下会带来的具体影响[8](P11-12)。

我国法上更多是在告知义务的内容上有所规定,而在“明确”之外,对告知义务的实质履行程度并未有更具体的要求,同样有立法完善的空间。

3. 基于弱者保护的规范要求。在网络世界中,作为数据处理者的网络服务商和作为信息主体的自然人之间显然存在着强弱地位的差异。实践中,网络服务商通过采取“使用即同意”的隐私政策或免责声明导致同意原则被实质架空的情况十分普遍。对此,存在着格式条款规制和消费者权益保护两种不同的规范路径。

在格式条款规制方面,《合同法》第 39 条和第 40 条作了专门规定,主要分为三个层次:一是规定了格式条款提供方的合理提请注意义务。根据《合同法司法解释(二)》第九条,如果违反该义务,相关条款可以通过当事人主张撤销的方式不纳入合同内容。二是即使纳入合同,常常须作对提供格式条款一方不利的解释。三是对免除己方责任、加重对方责任、排除对方主要权利的格式条款可以直接认定无效,如此充分保障合同弱势一方的合法权益。不过,《合同法》的相关规定,依然存在解释上的宽泛性弊端,何谓“合理”,是否“免除、加重、排除”相关权利和义务,需要结合具体交易进行判断。而从另一方面讲,格式条款本身存在着便捷交易的核心功能,让网络服务的用户就相关收集信息的内容一一作出同意表示显然也不符合实践需要。因此,如果缺乏对网络服务商明确的告知义务规范和个人信息主体权利的细化规定,只能落实在实质内容层面通过法官、执法部门的事后控制和评价进行格式条款的间接规范。

针对传统民法保护上的不足,有学者提出在数据治理上应引入消费者权益保护机制,“在传统的意思自由为基础的民法模式上增加社会公平价值的考量”[9](P24)。该学者认为,基于个人数据可成为合同对价、互联网服务提供者从用户数据中获利、数据使用协议具有合同属性等事实,数据主体可完成从自然人到消费者的角色嬗变,可以通过设置事前磋商透明化、事中交易诚信化、事后救济有效性等要素建构数据主体的消费者权益保护体系。不过,值得说明的是,消费者之所以被认为是弱势主体,更多是因为其由于信息不对称而造成的弱势地位,因此消费者权益保护法的中心在于明确告知义务、增强消费者的知情权和赋予消费者撤回权、扩大消费者协会权限等救济手段来弥补消费者的弱势地位。此种规范目的与保护个人信息的立场略有不同。后者的规范重心并不局限于确保信息提供和接受上的均衡地位,还包括要最大限度地捍卫个人信息主体的行动自由和信息自决权益。仔细分析该学者的建构思路,可知其在具体规范层面,更多是从美国法的消费者保护经验上提出完善意见,但在现行法层面,令人无法回避的是,《消费者权益保护法》本身专门针对个人信息保护问题在第 29 条进行了具体规定,因此即使将同意规则纳入消费者权益的保障体系进行考察,相关制度的建构也必须建立在对该条的解释层面进行推演。这一点上,该法第 29 条却并未提供比《网络安全法》等其他规范更高和更为细致的要求。

由此我们可以看到,就个人信息保护上的强弱地位问题,尤其是针对“使用即同意”条款的普遍盛行,现有立法,无论是采纳格式条款规制进路,还是强调消费者权益的保护都依然存在进一步立法和司法完善的空间。比如,在立法层面,可以针对网络服务提供者的自定规则建立相应的文本备案审查机制、明确惩罚性赔偿机制在个人信息保护领域的适用空间,以及赋权消费者权益保护组织等多元主体参与数据治理和保护等层面完善现有规定;在司法层面,可借鉴欧洲法就同意的明确性要求,认定网络用户相关的点击、浏览形式并不构成有效的同意,如此来勾勒现有立法在同意规则解释适用上的规范空间。

四、“同意”的例外规则

关于同意的例外规则,《关于加强网络信息保护的决定》《消费者权益保护法》《网络安全法》均未直接提及。《个人信息保护规定》第 9 条第 4 款规定:法律、行政法规对本条第一款至第四款规定的情形另有规定的,从其规定。其所指第 1 款规定即: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。由此可知,在认可同意为个人信息收集、使用合法性基础的前提下,允许法律、行政法规设有例外规则,自然也包括无须同意的情形。

《网络侵权司法解释》第 2、4、5、6 项，分别涉及为促进公益且作必要公开、自行公开或已合法公开、合法渠道获得、法律、行政法规另有规定等情形下未经个人同意，照样可以公开其个人信息（包括自然人基因信息、病历资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，内容上显然包括敏感信息和一般信息）。在国家标准层面，《规范》的例外规则最为丰富，其第 5.4 条规定：以下情形中，个人信息控制者收集、使用个人信息无需征得个人信息主体的授权同意：a）与国家安全、国防安全直接相关的；b）与公共安全、公共卫生、重大公共利益直接相关的；c）与犯罪侦查、起诉、审判和判决执行等直接相关的；d）出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；e）所收集的个人信息是个人信息主体自行向社会公众公开的；f）从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；g）根据个人信息主体要求签订和履行合同所必需的；h）用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；i）个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的；j）个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；k）法律法规规定的其他情形。《规范》第 8.5 条进一步规定了共享、转让、公开披露个人信息时事先征得授权同意的例外，类型基本相同。前述规则，总体上也反映了基于国家利益、社会利益的需要对个人信息自决的必要控制和限制。但前述规范效力层级、适用范围和要求程度并不相同，依然存在整合之必要。比如，对于为科研目的所使用或公开的个人信息，《网络侵权司法解释》第 3 项（针对信息的公开）和《规范》第 5.4 条（针对信息的使用和收集）均有结果去标识化的要求，但前者同时要求自然人的书面同意，后者却并无此要求。而在共享、转让、公开披露等方面，《规范》第 8.5 条却并未将此种类型列入授权同意的例外。另外，特别需要指出的是，《规范》第 5.4 条第（g）项提到“根据个人信息主体要求签订和履行合同所必需的”，类似欧盟《条例》第 6 条第 1 款第（b）项，此种情况下不需要个人信息主体的授权同意。对此，前文已有讨论，未来立法也有加以明确的必要。

进一步需要说明的是，《规范》第 5.4 条所规定的无需征得个人信息主体授权同意的情况，并未严格区分一般信息和敏感信息。对此，欧洲法上的处理并不完全相同。《条例》原则上禁止数据控制者处理特殊类型的个人信息，但除数据主体明确同意外，第 9 条第 2 款第（b）到（j）项还同时规定了无须同意的其他例外情形，如为数据主体工作、社会保障目的、保护自然人切身利益、必要的机构活动、其他重要利益、被数据主体自行公开、行使司法权、重大公共利益、医疗保健、公共健康、科研历史统计等。须说明的是，即使在这些例外情形下可以处理个人数据，《条例》依然要求相关数据控制者在必要的场合须采取适当、具体的措施来保障数据主体的基本权利和自由。对此，“鉴于条款”第 52-56 条有更进一步的阐释和说明。至于与刑事定罪相关的个人信息，单独规定在《条例》第 10 条，要求此类信息的处理应当仅在公权力的控制下开展，或者被欧盟或成员国法律授权为保护数据主体的权利和自由而提供保护措施的处理情况下开展。任何刑事定罪的综合登记仅可处于官方机构的控制之下[2]（P199，231）。敏感信息与个人隐私、个人行动自由等利益关系密切，因此在与国家利益、社会利益等的协调平衡上，应该有更为丰富的规范层次。在这一点上，中国法有进一步完善的空间。

另外，关于数据的后续处理（二次利用）行为，在中国法上，《规范》区分匿名化（第 3.13 条）和去标识化（第 3.14 条），前者是指通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程；后者是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。《规范》特别注明，个人信息经匿名化处理后所得的信息不属于个人信息，而去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。易言之，对已匿名化的信息，无需再征得个人同意，为不证自明的道理。

对于这一点，欧洲法也有类似的结论。《条例》第 4 条中将匿名化定义为：一种使个人信息在不使

用额外信息的情况下不指向特定数据主题的个人数据处理方式,若该处理方式将个人数据与其他额外信息分别存储,凭技术性和组织性措施无法指向一个可识别或被识别的自然人。《条例》第 11 条规定:如果控制者不需要或者不再需要对其掌控的个人数据的数据主体进行身份识别,则若仅根据本条例的要求和规定,控制者无义务保存、获取或者处理额外的信息来识别数据主体。若在本条第 1 款所述的情况下,控制者应当告知数据主体,说明其并无对数据主体进行识别的职责。在此情况下,排除适用本条例第 15 条至第 20 条(笔者注:《条例》第 15 条至第 20 条,分别涉及数据访问权、更正权、删除权/被遗忘权、限制处理权、个人数据更正、删除或限制处理的告知义务、数据可携带权等),除非数据主体出于行使自身权利需要,而且提供额外身份证明信息。

尽管从技术上来讲,绝对匿名化是不可能的。通过个人信息匿名化的技术保障来巩固法律保障,鼓励和促进企业在个人信息的利用和保护上齐头并进,显然是走出知情同意原则适用困境的一个重要途径。值得补充的是,欧盟《条例》第 6 条第 4 款和"鉴于条款"第 50 条规定,如果数据处理活动并非为了个人数据被收集时的目的,并且未基于数据主体的同意,亦非基于欧盟和成员国法律所作特定限制,控制者在满足了最初处理的合法性要求后,有责任确认这种后续处理行为的目的是否与最初收集数据的目的相兼容。此时特别需要判断两种目的之间的联系、数据主体和控制者之间的关系,数据的性质、预期对数据主体造成的后果、适当的加密措施等因素[2](P243)。

总体而言,同意原则的例外规定,体现了立法者或相关部门对于作为基本权利的个人数据之外的国家利益、社会利益的考虑,为数据利用的公共政策考量留出了一定的空间。但必须说明的是,尽管不需要征得用户同意,前述例外规则都必须遵循严格的限制条件,以确保个人合法的信息权益不因"公共利益"之名而遭受无端损害。在前述《规范》中,对无需征得个人信息主体授权同意的情况作了相当详细和严格的规定,但不可否认,这些例外规则在规范含义上均存在着一定程度的模糊性。比如,何为"直接相关""重大合法权益"等均很难规范界定,存在自由裁量的广泛空间。这也导致了处理个人数据比较安全的做法依然是尽量取得用户的同意。

五、结论

我国法在个人信息保护上确立了信息主体授权同意的一般规则,但并未在同意的作出方式和实质要求上有更为具体的规范阐释。然而,在一些司法解释和国家标准层面,相关同意规则的设置又亟待进行体系梳理。同意规则在规范上的界定不清,相关规则在过于严苛和过于宽松之间徘徊不定,导致在实践运用层面,尤其是在网络服务中,数据控制者借助"使用即同意"的单方声明、格式条款普遍无视个人信息主体的合法权益,最终反而带来同意规则名存实亡的悖论局面。

不过,在笔者看来,问题的解决并不是去否定同意作为个人信息保护合法性和正当性的基础地位,而是通过重构同意规则的法律构造,通过更为精细、更为清晰的类型化塑造,来更好地平衡和协调个人信息保护和利用上的利益博弈。对此,我们可以通过明确同意作为意思表示的法律性质界定,并借助传统民法关于意思表示作出方式和实质要求上的基本规范内容,结合比较法上的经验,结合个人信息保护领域的特殊语境,在现行法的规范框架下作出体系性的规范构造。如此,在立法论和解释论层面,也许可以为同意规则相关的诸多争议问题,给出一个更为清楚的结论。

还必须说明的是,以意思表示为出发点,回归传统民法的分析框架,目的在于最大限度地保护私益,捍卫个人信息主体在网络世界中的意思自治和行动自由。但同时我们必须看到,个人信息的生成和动态发展,本身必须依托于网络环境。也恰恰是在数据开发利用的过程中,才真正催生了个人信息保护的内在需求。因此,个人信息保护和数据开发利用之间需要有一个动态的利益平衡空间。例外规则的设置,恰恰为这种利益平衡提供了规范依据。这其中,除了社会利益、公共利益等因素的考虑,我们还必须看到个人信息消极防御和积极利用的本质差异。一旦进入交易领域,当事人签订和履行相关合同所必需的

个人信息，就应该成为同意规则的例外。当然，对何为“签订和履行合同所必需”等，实践中必须作严格的解释，以避免例外规则的泛化损害同意规则的基础性地位。

参考文献

[1] 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，(1).
[2] 京东法律研究院. 欧盟数据宪章:《一般数据保护条例》GDPR 评述及实务指引. 北京: 法律出版社，2018.
[3] 姚辉. 关于人格权商业化利用的若干问题. 法学论坛，2011，(6).
[4] 程啸. 侵权责任法. 北京: 法律出版社，2015.
[5] C. Pedrazzi. Voce Consenso Dell’avente Diritto//Editorial Board. *Enciclopedia Del Diritto IX*. Milano: Giuffrè, 1961.
[6] 李适时. 中华人民共和国民法总则释义. 北京：法律出版社，2017.
[7] 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，(5).
[8] Article 29 Working Party. Guidelines on Consent under Regulation. European Commission, 2018-07-06.[2019-03-07]*http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.*
[9] 孙南翔. 论作为消费者的数据主体及其数据保护机制. 政治与法律，2018,(7).

Research on the Normative Construction of “Consent” Rules in Personal Information Protection

Lu Qing (Zhejiang University)

Abstract　The consent of the data subject is one of the legal justifications for the collection and use of personal information, which may not only be seen as fulfillment of contractual obligations, but also exclude the unlawfulness of the commercial use by others, reflecting the positive and negative control of the subject on his personal information. Since the consent has a legal nature as manifestation of will, the normative rules of consent may be based on the rules of manifestation of will, consisting of the form of the manifestation (either explicit or implicit, while silence generally may not be seen as an effective manifestation of will) and the substantive requirements of the will (private autonomy, informed consent and protection of the party in a weak position). A “one-size-fits-all” solution for the collection and use of information seems arguable, whether it requires a prior (explicit) consent of the data subject or an implicit consent suffices for the use of general information. The exceptions to the rules of informed consent need to be reconsidered as it goes beyond the reach of the consent rules when the personal information being collected and used is necessary for the conclusion and performance of the contract.

Key words　right of personal information; data protection; consent rule; manifestation of the will; the era of big data; emerging right

■ **收稿日期**　2018-11-14
■ **作者简介**　陆　青，法学博士，浙江大学光华法学院副教授；浙江 杭州 310005。
■ **责任编辑**　李　媛