重构大型互联网平台个人信息处理行为的规制模式

江虎岭
（山东师范大学法学院，济南　250300）

摘　要：[**目的 / 意义**] 在数据价值日益凸显的信息时代，高频次、大规模的信息处理行为加剧了大型互联网平台与信息主体的地位失衡，导致对个人信息处理的混乱和无序。而我国《个人信息保护法》对个人信息处理行为的规制实施效果并不理想，有必要重构对大型互联网平台个人信息处理行为的规制模式。[**方法 / 过程**] 细化个人信息处理的各个阶段，融入场景因素激活“告知同意”条款，完善个人信息保护机构的制度设计，发挥多主体的规制效用，保证救济渠道的多元、畅通，全程推进风险防控。[**结果 / 结论**] 通过对个人信息处理规制模式的重构，有效平衡大型互联网平台、信息主体和国家监管部门的地位与能力，保障信息主体的个人信息安全。

关键词：大型互联网平台　个人信息处理权　个人信息权益　场景理论
分类号：D9
DOI：10.31193/SSAP.J.ISSN.2096-6695.2023.02.06

1　问题的提出

根据《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》）之规定，个人信息的存储、使用、加工、传输、提供、公开、删除等均为个人信息处理行为。而基于信息主体的同意享有此个人信息处理权的个人信息处理者（以下简称“处理者”），以信息处理目的为标准，大抵可以分为两类：一是为实现公共管理目的而处理个人信息的公权力机关；二是以谋利等私益为目的而处理个人信息的市场主体，用户数量巨大、业务类型复杂的大型互联网平台即在此列[1]。在信息价值的驱动下，大型互联网平台以超乎想象的收集速度和处理频次，掌握了庞大的信息量，并在信息处理活动中予以分析运用。然而随着个人信息处理广度和深度的不断增加，大型互联网平台对处理界限的把握显得尤为重要，否则极易演变为“信息利维坦”[2]，侵害个人信息权益。

2022 年 7 月 21 日，关于滴滴全球股份有限公司（以下简称“滴滴公司”）网络安全审查相关的行政处罚决定引发社会公众的高度关注。作为拥有 3.77 亿活跃用户[3]的网约车行业“巨

[作者简介] 江虎岭（ORCID：0009-0009-7542-6691），女，硕士研究生，研究方向为宪法学与行政法学，Email：jhl54550@163.com。

头”，滴滴公司竟在信息主体不知情的情况下违法处理个人信息高达 647.09 亿条。而滴滴公司对个人信息权益的侵害并非短时间酿成的。在近十年的时间里，其能够对个人信息权益造成如此大规模的持续侵害与国家监管部门的履职疏忽也存在些许关系。从官方公布的数据可以发现，国家监管部门只在 2021~2022 年对滴滴公司进行了较为密集的网络安全审查，在此之前只有为数不多的针对特定问题的约谈。

“滴滴公司案”虽然仅为众多案件中的普通一例，但是它所反映的问题却是大型互联网平台在个人信息保护领域的“通病”，具体包括信息处理告知义务的缺失、信息处理监管体系存在漏洞以及信息处理风险防控不够全面等。这些问题使得强势的大型互联网平台对信息主体“步步紧逼”，加剧了二者之间的权利义务失衡，并导致两者地位呈现出严重不对等的状态。为防范个人信息侵害风险，对大型互联网平台信息处理权的规制已是大势所趋。《个人信息保护法》的出台回应了这一现实需求，其中大多条文均围绕对处理者的行为规制与监管展开，尤其在第五十八条对大型互联网平台义务的强调，试图均衡信息主体与大型互联网平台之间的地位差异。然而，《个人信息保护法》的原则性规定要得到切实有效的落实仍需依赖具体路径的填补，本文认为应当从四个方面予以具体化：首先，坚持“告知同意”之首要原则，辅之以场景设置，实现效用加成；其次，规范个人信息保护机构的制度设计，形成大型互联网平台的自我监管；再次，发挥多主体对信息处理行为的监督，消解风险隐患；最后，完善多元救济渠道，充分保障信息主体的合法权益。

2　大型互联网平台现有规制模式之弊病

《个人信息保护法》通过对个人信息处理规则、处理者义务以及监管部门职责的规定，为规制大型互联网平台的信息处理行为提供了基本模式。然而，随着个人信息处理程度的深入及技术的精进，现有规制模式之弊病日渐凸显，条款失灵、监管无力、风险防控体系的缺失为大型互联网平台所利用，其规避法律、肆意处理个人信息的行为，对个人信息保护造成极大的威胁。

2.1　流于形式的“告知同意”条款

“告知同意”是处理个人信息的前提。根据《个人信息保护法》第十三条、第十四条的规定，处理个人信息应该取得信息主体的同意，并且是信息主体在充分知情的前提下自愿、明确做出的。“告知同意”因此被视为个人信息权益保障的首要机制[4]。然而，面对强势的大型互联网平台，信息主体知情同意的权益似乎已经被束之高阁，徒留一副“空架子”。根据国家统计局公开数据，2021 年我国互联网上网人数为 10.32 亿人，其中仅手机上网的人数便高达 10.29 亿人[5]。如此大规模的网民数量得益于各类大型互联网平台的发展，甚至将“平台用户”与“网民”进行同义置换亦无不可。而个人要想成为平台用户，首先要进行注册，向平台提供自己的基本信息，这俨然已成为信息主体“刻在骨子里”的习惯，自愿与否似乎已经不在考虑之列；其次，信息主体必须勾选隐私协议方可进入平台并正常使用。就隐私协议本身而言，一方面，作为当下“告知同意”最普遍的表现形式[6]，其内容主要涉及隐私范畴、信息处理方式、法律责任等，这虽然是个人信息权益保护的关键，但由于其文字冗长且晦涩难懂，事实上鲜有信息主体会耐心读完，不阅读而直接勾选是大部分人的习惯性选择。另一方面，即便用户仔细阅读，对于其中不合理或

不符合用户预期的内容也无法与平台协商并修改，依然只有“同意”或不使用两个选择。由此可见，信息主体并没有选择的自由，只能向大型互联网平台“屈服”，从而形成大型互联网平台对信息主体的“隐形强迫”。而隐私协议本身，正如荷兰学者苏珊·蓝道指出的那样，似乎并不是为人们使用（信息平台）而设计的，其目的在于穷尽所有意外情况以防范其发生[7]，从而成为大型互联网平台规避法律责任的一种方式。

此外，在信息主体“同意”之后，诸多不为人知的信息追踪也在悄然发生。如前所述，“滴滴出行”作为一款出行类软件，其对个人信息的处理显然已经超出了软件运行所必须，辐射范围之广甚至触及用户极为隐秘的身份信息，而这一切均是超出“告知同意”之外、为信息主体所不知的。“习惯性被迫”和隐秘的信息追踪愈演愈烈，其背后所隐藏的正是大型互联网平台与信息主体之间的地位失衡。此处虽然以滴滴公司为例，但以收集和处理个人信息为商业活动之前提，已经是信息时代各个领域大型互联网平台的普遍做法。

事实表明，“告知同意”虽然是个人信息处理的法定前提，但实际上并不能保障信息主体在信息处理活动中的主动地位。因此，要达成保护个人信息权益与发挥信息流通价值之间的平衡，亟待对“告知同意”条款进行柔韧化[1]改造。

2.2 监管无力的个人信息保护机构

个人信息保护机构，顾名思义，是对个人信息处理行为进行监管与规制以保护个人信息权益的机构。根据《个人信息保护法》之规定，此类机构可以分为两种：一是隶属于处理者的个人信息保护机构（以下简称“处理者内部机构”）；二是国家设置的履行个人信息保护职责的监管部门（以下简称“国家监管部门”）。

在《个人信息保护法》中，对处理者内部机构的规定只有第五十二条，“达到国家网信部门规定的信息处理数量标准的处理者应当指定个人信息保护负责人，负责对信息处理活动及所采取的保护措施进行监督”。此外，第五十八条强调大型互联网平台有义务成立主要由外部成员组成的独立机构，以建立健全个人信息保护合规制度体系。然而，在实践中，由于数量标准与规模不确定、监督职责不明确等问题，其实施效力如何颇值得怀疑。一方面，由于《个人信息保护法》没有规定明确的数量与业务类型复杂标准，国家网信部门规定的标准也往往不为信息主体所知晓，大型互联网平台因此可以轻易逃避监管；另一方面，由于监督职责不明确，大型互联网平台要么不设立个人信息保护负责人，要么以“无专职人员”“无专门机构”“无具体职责”的“三无”机构敷衍了事，其对个人信息处理权的内部规制根本无从谈起。

《个人信息保护法》第六十条规定，国家监管部门主要有三：一是国家网信部门；二是依照《个人信息保护法》和有关法律、行政法规的规定，负有个人信息保护和监督管理职责的国务院有关部门；三是负有个人信息保护和监督管理职责的县级以上地方人民政府有关部门。在第六十一条中规定国家监管部门的职责为“接受并处理相关投诉与举报，调查并处理违法个人信息处理活动”等。可以看出，上述监管职责只停留在原则化规范的层面。且不说国家监管部门是否具有对大型互联网平台构成外部制约的现实能力，在实践中，由于个人信息处理行为极为密集、复杂，拥有内部便利的个人信息保护负责人之职责发挥尚且欠佳，更何谈国家监管部门的外部规制。

2.3 缺失的过程化风险防控

大型互联网平台的信息处理活动因个人信息价值的凸显而日渐普泛化，不同处理阶段对个人信息的需求也各不相同。要防范大型互联网平台的信息侵害风险，需要兼顾各个信息处理阶段，实现全过程的风险防控。《个人信息保护法》中虽然有对风险防控的类似提及，如第五十五条规定的事前个人信息保护影响评估、第六十四条规定的国家监管部门发现风险时的具体职责履行、第六十六条规定对违法处理者的责任追究等，这些规定表面上似乎涵盖了对个人信息处理的各个阶段，但是均未形成对过程化风险防控系统且具体的规定。然而，若强行将泛泛提及的“事前评估”、“发现风险并采取措施”和“违法追究”的规定解释为过程化风险防控的表现，恐怕难谓周延[8]。这从“滴滴公司案”中便可见得，虽然事发之初，《个人信息保护法》并未出台，但是《中华人民共和国网络安全法》第四章与第五章中亦不缺乏对网络信息安全与风险防控的法律规定。由于法律规范的抽象性和国家监管部门对过程化监管的疏忽，在“滴滴出行”被正式纳入网络安全审查范围时，其对民众日常生活的“浸润”和对个人信息侵害早已达成相当规模，而无论最终审查和处理结果如何都无异于亡羊补牢。因此，要抵御大型互联网平台“技术霸权”可能造成的信息侵害风险，基于《个人信息保护法》之规定，构建过程化风险防控体系不失为一个良策。

3 大型互联网平台规制模式之重构

要重构大型互联网平台信息处理的规制模式应当基于《个人信息保护法》的规定，对现有规制举措加以细化、完善，以保障对大型互联网平台的规制有法可依。而过程化风险防控则需依赖多主体的各自履职和协同推进，在个人信息的实质性处理阶段，形成大型互联网平台、国家监管部门、信息主体甚至社会公众共同参与的多元治理结构[9]，避免对信息处理行为的规制出现漏洞。

3.1 场景因素激活“告知同意”条款

为保障信息主体在信息处理活动中的主动地位，使“告知同意”回复其预设效力以对个人信息处理权有所规制，有必要借助场景因素对“告知同意”条款进行改造。

场景因素被认为是为僵化的信息处理规制进行动态调整的理论设计，最早起源于海伦·尼森鲍姆的“场景理论”[10]，强调对个人信息处理活动的规制应当以场景为导向，不同的场景存在特有的信息适当性与流动管理规范，并基于此形成一套由信息类型、参与主体以及信息传输原则组成的规范框架。其中信息传输原则作为具体场景中信息流动的主要约束规范[11]，针对不同场景中个人信息保护的不同程度做出回应，意图改变对个人信息处理行为的刻板规制[12]。在这种灵活适用的背景下，为防止处理者对个人信息的滥用，必须以严格的标准对个人信息处理行为合理与否进行判断，此时，“合理预期”标准便应运而生。根据尼森鲍姆的观点，特定场景的信息规范内含于政策、法律与习惯之中，因此该场景下的信息处理类型、参与者、行为的程度、风险等早已在信息主体普遍接受的基础上形成合理预期。“合理预期”标准的出现使得“告知同意”被暂时搁置，在持续的信息处理过程中，信息主体相信处理者会在既定范围内行为，只要信息处理行为尚未超出上述范围，那么处理者无需征得同意便可自行处理个人信息。换言之，场景理论通过信息规范框定了特定场景中的风险范围，一旦突破框架的限定则意味着信息主体合理预期的

落空，从而引发个人信息侵害的恶果。可见，场景理论所强调的风险根源并不在于个人信息及信息处理本身，而在于突破特定信息规范之外而存在的非适当的信息类型与不合理的信息传输[13]。

面对“告知同意”日趋僵化而导致规制无力的被动局面，场景理论借助具体场景中信息规范和合理预期的设置，形成规制信息处理行为的理论框架。但是，有学者认为，场景理论所构建的规范框架是固有而滞后的，在新的技术发展和多维信息流向的冲击下，被框定的信息侵害风险因新因素的介入而与日俱增，规范的陈旧性与发展的创新性之间难免产生落差。虽然尼森鲍姆对此提出了评估之策——利用新信息处理行为的有益性和价值权衡来判断新要素的加入是否必要且合理、旧的规范框架是否值得保留。但实际上，类似的价值判断和合理预期分析向来都是主观大于客观。与其每每在新因素出现之时，耗费较大成本进行信息流通的商业价值、安全价值、基本权益冲突等方面的权衡，不如向信息主体明确告知信息处理中的新变化，在取得同意后，再结合不同场景的既有规范进行权利与义务的减损与增加，更具现实意义。

从表面上看，场景理论与“告知同意”条款的融合似乎使得场景化的信息处理更为繁杂，但实际上“告知同意”的融入减少了监管成本，增强了场景理论的包容性，亦保持了对个人信息处理权的灵活规制。同时，以具体场景的设置对处理者“松绑”，给予处理者更大的缓冲空间，由此削减其因抵触情绪而刻意规避法律、滥用权力之动机。因此，亦可将场景理论的应用视作对个人信息处理权规制的“激励机制”。

在国外，欧盟《通用数据保护条例》（以下简称“GDPR”）和美国《加利福尼亚州消费者隐私法案》（以下简称“CCPA”）都或多或少吸收了场景理论的某些因素，并与“目的限制原则”相结合。目的限制原则是规制个人信息处理行为的基本原则之一，即处理者所进行的信息处理应当以初始处理目的为限。在 GDPR 中，判定两个目的是否相符，需要借助具体场景、信息主体的合理预期等一系列因素，倘若信息处理取得信息主体同意或者是基于公共利益，则无需考虑目的之符合度即可进行进一步处理。[14]CCPA 则更为直接的设置了具体场景，如在企业与另一企业依照双方订立的合同行事时，如果企业出于法律规定的目的做出维护消费者个人信息的行为是合理必要的，则不应再被要求遵守消费者主张删除个人信息的请求。[15]换言之，在该场景下，手段和目的相适用的传统模式直接被合理性标准所取代。只要目的合法、行为合理，即使未征求信息主体同意，处理者的信息处理行为亦存在合法性，并可以对抗信息主体的删除权，由此消费者的相关权利就被减损，而企业的义务性负担顺势减轻。可见，场景理论的引入实现了“合理预期标准”与“目的限制原则”的有机结合，使原本基于限定目的而产生的“告知同意”能够在信息处理中收放自如，增加了信息处理的灵活性。

我国可借鉴这一模式，对信息处理活动进行场景细化和设计，并通过对传统处理目的的合理性解释，实现对“告知同意”条款的重塑，即对“告知同意”依不同场景的侵害风险差异作类型化处理。譬如对游戏软件、视频平台等用户信息侵害风险不大的一般性场景，在遵守“告知同意”条款的同时，只需对信息主体质疑之处进一步说明即可；而对金融服务、商品交易等极具个人信息侵害风险的场景，必须对信息处理的细节进行详细告知，并确保信息主体对处理行为知晓并理解。如此区分“告知同意”场景，既有助于控制处理成本，又在合理性原则的基础上实现了对大型互联网平台信息处理权的“靶向”规制。在后续的信息处理中，只要大型互联网平台的处

理目的与初始目的一致、符合合理预期，则无需再征求信息主体的同意，只需告知即可。需要注意的是，由于信息主体的合理预期远不及目的限制的约束性强，因此，在考虑符合预期的同时，还应当对信息处理的风险予以同步考虑。

3.2 完善并落实“个人信息保护负责人”制度

在个人信息保护负责人及相关机构的设置方面，2020 年新修订的《信息安全技术——个人信息安全规范》（国家标准 GB/T 35273–2020）（以下简称《规范》）极具参考价值。《规范》11.1（b）项中“应任命个人信息保护负责人和个人信息保护工作机构”的规定，实现了对个人信息保护负责人和个人信息保护工作机构的“捆绑”。关于设立的条件，《规范》11.1（c）项中的规定显然比《个人信息保护法》详细得多，一是主要业务涉及个人信息处理且从业人员规模大于 200 人；二是处理个人信息超过 100 万人的，或者预计在 12 个月内处理个人信息超过 100 万人的；三是处理个人敏感信息超过 10 万人的。[16] 凡是满足上述条件之一，均应当设立个人信息保护负责人和个人信息保护工作机构。虽然该《规范》只是国家鼓励的推荐性标准，不具有强制执行的效力，但是仍然可为《个人信息保护法》中个人信息保护负责人及相关机构的设置提供参考，即以个人信息处理数量、个人信息处理业务种类及从业人员规模等，做出明确、具体、详细的规定，并以上述标准之数量多少、种类繁简、规模大小为区分，决定个人信息保护工作机构“捆绑”出现之必要。

同时，个人信息保护负责人及个人信息保护工作机构之职责可在现有基础上加以扩充。在日常的信息处理中，个人信息保护负责人及相关机构除现有的辅助处理者进行个人信息安全影响评估、防范信息侵害风险等职责外，还可借鉴 GDPR 之规定，增加及时解答大型互联网平台咨询的事项[17]、对个人信息保密等职责[18]。在接受国家监管部门的监督时，增设其及时向国家监管部门报告大型互联网平台的信息处理动向；听取国家监管部门做出的监管建议，并在信息处理活动中提醒并加强对大型互联网平台的监管等职责。

3.3 细化多主体参与的规制过程

首先，对于大型互联网平台及其内部设置的个人信息保护机构而言，在常规的信息处理中，应当将风险监测与评估落实到信息处理的每一个环节，将外部的动态威胁和处理因素变动招致的内生风险及时化解于应对决策之中[19]。而对于未能及时化解的侵害风险应及时采取补救措施，并寻求国家监管部门的协助，依据《个人信息保护法》第五十七条之规定，及时向国家监管部门和信息主体履行风险处理相关事项的通知义务。

其次，对于国家监管部门而言，其在履职过程中应当对风险等级不一的处理事项做区别监管，如对风险等级一般的事项进行建议和行政指导；对风险等级较高的事项定期约谈；对风险等级极高的事项，定期展开细节审查或委托专业机构进行合规审计，亦可要求大型互联网平台定期向其作个人信息处理报告。同时，国家监管部门应遵循高效便民的原则，设置并向社会公布便捷的投诉、举报方式，健全受理、甄别、处置、反馈等机制，及时处理信息主体及社会公众的举报与投诉，并将处理结果与整改建议反馈给个人信息保护负责人，在必要时将处理结果向社会公布。

对于不服从监管、违法处理个人信息、不履行个人信息保护义务的大型互联网平台，国家监管部门则可依据《个人信息保护法》第六十六条之规定，对其做出责令改正、警告、没收违法所得等不同的处理，并责令其暂停所使用的违法处理程序或终止提供服务；对拒不改正的大型互

联网平台及其主要负责的主管人员和其他直接责任人员（以下简称“主要责任人员”）处以罚款。而对违法情节严重的，则由省级以上的国家监管部门处以特定数额的罚款，责令暂停相关业务、停业整顿，吊销相关业务许可或吊销营业执照等，同时，对主要责任人员处以罚款，并可对其做出在一定期限内禁止担任相关职务的限制。

最后，信息主体及社会公众对大型互联网平台的监督作用亦不容小觑，信息主体、社会公众若发现可能或正在发生的侵害风险，应当及时向国家监管部门和个人信息保护负责人反映，及时止损以保障个人信息权益（见图 1）。

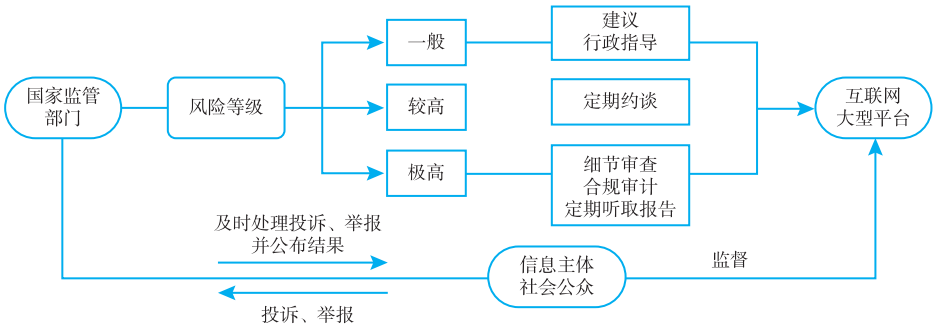

图 1　过程化风险防控中国家监管部门、大型互联网平台、信息主体及社会公众关系图

3.4　保证救济渠道多元、畅通

《个人信息保护法》虽未直接规定信息主体在个人信息权益遭受损害时可对处理者提起诉讼，但是第六十九条对处理者过错责任的规定，即“处理者违法处理个人信息造成损害，不能证明自己无过错的，应当承担损害赔偿责任，并依据个人所遭受的损失或者处理者因此获得的利益确定”，从侧面明确了信息主体可作为规制处理者的诉讼主体出现。因此在风险规制失灵而导致权益损害时，必须保障救济渠道的多元与畅通，使信息主体或法律规定的特定主体可诉诸行政、民事、刑事手段寻求对个人信息权益的救济。

行政救济是对国家监管部门职责履行状况的“选择”救济。当信息主体向国家监管部门就违法违规的信息处理行为进行投诉、举报，试图化解潜在的信息侵害风险时，若国家监管部门不回复或不履行职责最终导致权益损害后果的发生，信息主体即可对国家监管部门提起行政诉讼，由人民法院考量后，依据《中华人民共和国行政诉讼法》第七十八条之规定，判决国家监管部门承担继续履行、采取补救措施或损失赔偿等责任。

在民事救济方面，根据《个人信息保护法》第六十九条和《中华人民共和国民法典》第一千一百一十五条之规定，在对大型互联网平台提起侵权损害赔偿诉讼时，应当依照过错责任原则，由平台承担证明责任，如果其不能证明自己无过错，则应当借助民事领域的“填平原则”，由大型互联网平台承担损害赔偿等侵权责任，弥补已发生或者即将发生的损害后果。

在刑事救济方面，《中华人民共和国刑法》（以下简称《刑法》）第二百五十三条设置了侵犯公民个人信息罪，具体犯罪情节包括违法向他人出售或提供公民个人信息；违法将履行职责或提供服务过程中获取的公民个人信息出售或提供给他人；窃取或者以其他方法非法获取公民个人信息等。若大型互联网平台及其主要责任人员存在上述犯罪情节之一，即存在侵犯公民个人信息的

嫌疑，信息主体则可借助刑事手段捍卫自身的信息权益。

多元救济渠道的完善对化解私益膨胀而导致的信息侵害风险大有助益，其补充了信息处理过程的监管漏洞，无论是对国家监管部门职责的依法履行还是大型互联网平台的合法信息处理均起到一定的震慑作用，由此构建起对个人信息权益的全方位保护。

4 结 语

在信息时代的背景下，大型互联网平台的广泛存在，一方面为社会管理和偏好分析开辟捷径，另一方面也对个人信息权益的保护造成困扰。引入场景理论、完善个人信息保护机构的制度设置以及过程化风险防控确实可对大型互联网平台规制模式的重构有所助益，但仍存在些许问题有待解决。第一，规制场景的设计、风险等级的划分以及各项标准的确定等，均建立在对个人信息处理领域现状的深入剖析基础之上，对《个人信息保护法》的完善将耗费较高立法成本，亟需在立法效率与立法成本之间寻求平衡。第二,《个人信息保护法》的部分条文以普适性规范的形式出现，缺乏可操作性，如何避免规定的杂糅或缺失，并针对不同的处理者，尤其是大型互联网平台的独特之处做出尽可能详细的规定，仍有待进一步研究。总而言之，我国个人信息权益保护任重而道远，唯有构筑起信息主体与处理者地位均衡的基本秩序，方能维护信息时代的个人尊严和社会正义［20］。

【参考文献】

［1］郭春镇 . 数字化时代个人信息的分配正义［J］. 华东政法大学学报，2021，24（3）：55-70.

［2］袁博 . 大数据时代个人信息保护的行政监管立场及其智慧化转型［J］. 西南民族大学学报（人文社会科学版），2022，43（6）：96-107.

［3］中国经济网 . 滴滴出行递交 IPO 招股书［EB/OL］.［2023-5-6］. https://baijiahao.baidu.com/s?id=1702613825200239014&wfr=spider&for=pc.

［4］张涛 . 探寻个人信息保护的风险控制路径之维［J］. 法学，2022（6）：57-71.

［5］国家统计局 . 中华人民共和国 2021 年国民经济和社会发展统计公告［R/OL］.［2022-7-28］. http://www.stats.gov.cn/xxgk/sjfb/zxfb2020/202202/t20220228_1827971.html.

［6］何晓斌 . 个人信息保护中告知同意的开放结构及其公法实现［J］. 行政法学研究，2023（1）：143-153.

［7］Susan Landau. Control use of data to protect privacy［J］. Science, 2015.1.30,Vol 347,Issue 6221:504-506.

［8］彭诚信 . 论个人信息的双重法律属性［J］. 清华法学，2021，15（6）：78-97.

［9］周汉华 . 平行还是交叉 个人信息保护与隐私权的关系［J］. 中外法学，2021，33（5）：1167-1187.

［10］Helen Nissenbaum. Privacy as contextual integrity［J］. Wash. L. Rev., 2004, 79: 119-158.

［11］谷兆阳 . 论“场景理论”不是私密信息判断的合理标准［J］. 科技与法律（中英文），2022，10（4）：83-93，104.

［12］范为 . 大数据时代个人信息保护的路径重构［J］. 环球法律评论，2016，38（5）：92-115.

［13］海伦·尼森鲍姆，王苑 . 何为场景？——隐私场景理论中场景概念之解析［J］. 网络信息法学研究，2021（1）：3-28，236.

［14］General data protection regulation, Whereas(50)［EB/OL］.［2022-6-5］. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

［15］California Consumer Privacy Act of 2018, § 1798.105,(d)［EB/OL］.［2022-6-5］. https://advance.lexis.com.

［16］国家标准化管理委员会 . GB/T 35273-2020. 信息安全技术・个人信息安全规范［S］. 北京：中国标准出版社，2020.

［17］General Data Protection Regulation, Art.38［EB/OL］.［2022-6-5］. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

［18］General Data Protection Regulation, Art.39［EB/OL］.［2022-6-5］. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

［19］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［J］. 环球法律评论，2016，38（4）：20-40.

［20］李旭 . 个人数据法律保护的规范对象：权益基础、行为风险与权力失衡［J］. 人权研究（辑刊），2021，25（2）：382-404，530-531.

Reconstruct the Regulation Mode of Personal Information Processing Behavior of Large Internet Platforms

Jiang Huling

(Law school, Shandong Normal University, Jinan 250300, China)

Abstract: [**Purpose/significance**] In the information age with increasingly prominent data value, high-frequency and large-scale information processing behaviors aggravate the imbalance between large internet platforms and information subjects, leading to the confusion and disorder of personal information processing. However, the regulation effect of personal information processing behavior in the Personal Information Protection Law is not ideal, so it is necessary to reconstruct the regulation mode of personal information processing behavior for large Internet platforms. [**Method/process**] Specifying each stage of personal information processing, integrating scene factors to activate the “informed consent” clause, improving the system design of personal information protection institutions, giving play to the regulatory effect of multiple agents, diversifying and unblocking the relief channels, and promoting risk prevention and control throughout the process. [**Result/conclusion**] Through the reconstruction of the regulation mode of personal information processing, the status and ability of large internet platforms, information subjects and national regulatory authorities are effectively balanced, so as to ensure the personal information security of information subjects.

Keywords: Large internet platforms; Right to handle personal information; Personal information rights; Privacy as contextual integrity

（本文责编：王秀玲）