场景完整性理论在儿童数据保护监管中的应用
——以英国《适龄准则》和美国COPPA为例

高　奇　刘庆帅
(对外经济贸易大学 法学院,北京 100029 ;中国人民大学 社会学理论与方法研究中心,北京 100872)

【摘要】儿童数据保护的传统路径试图以单一要素对场景的多义性进行阐释,导致理论与实践的不自洽。场景完整性理论以一种个性化体系为儿童数据保护提供了完善思路,信息主体、信息类型和传播原则构成的要素框架,与儿童数据保护中的数字年龄、监护人同意和透明度等规则高度契合。各国重新审视现有法律框架,并以场景为导向进行细化,以英国《适龄准则》和美国COPPA最为典型,通过数据风险评估,以个性化评估取代单一年龄划分的方式,以差异化同意完善严格的监护人同意,在简洁易懂的基础上追求多层次的透明度规则。借鉴域外经验,我国儿童数据保护也要符合在特定场景中的公正。

【关键词】儿童数据　场景完整性　个人信息保护
DOI:10.16034/j.cnki.10-1318/c.2021.04.016

在数字化浪潮中,儿童网络用户规模日益庞大,对于儿童进行专门性的数据保护日益成为一项全球性议题。从隐私理论的演进历程来看,以海伦·尼森鲍姆(Helen Nissenbaum)的场景完整性理论(Contextual Integrity Theory)为代表的观点,逐渐抛弃以单一要素作为隐私的完整定义,转向了一种基于场景的个性化规范框架,并在域外立法上有所反映[1]。2019年,美国《儿童在线隐私保护法》(Children's Online Privacy Protection Act,以下简称COPPA)启动第二次修订。2020年,英国信息专员办公室(ICO)发布《网络服务适龄设计实践守则》(Age Appropriate Design: a Code of Practice for online Services,以下简称《适龄守则》),作为全球首部专门针对儿童网络服务进行适龄设计的规范标准,将于2021年9月生效[2]。上述立法动态与理论前沿相契合,为儿童数据保护带来了新的评价视角。

鉴于此,本文将从儿童的特殊性出发,探讨大数据时代保护儿童数据的现实必要性,以海伦·尼森鲍姆的"场景完整性"理论为视角,对儿童数据保护的海外监管理论趋势和最新立法进行评析,以期为我国儿童数据保护规范提供借鉴。

收稿日期:2021-05-18
作者简介:高　奇,对外经济贸易大学法学院博士研究生,主要研究国际经济法、网络法;
刘庆帅,中国人民大学社会学理论与方法研究中心博士研究生,主要研究青少年社会工作与社会政策。
基金项目:本文系国家社科基金青年项目"移动互联时代立法公众参与的类型特征、形成机制和应对策略研究"(课题编号:17CFX058)的阶段性研究成果。

一、场景完整性理论的内涵与路径构建

基于对英国《适龄准则》和美国COPPA的观察可以发现，各国政府均已重新审视传统数据保护规则，试图在知情同意的基础上建立适应儿童特征的、与网络化逻辑组态的数据保护规则体系。场景完整性理论能够有效地阐释其规则的内在逻辑，在此理解基础上建构的规则正成为一种可行的治理路径。

（一）场景完整性理论的内涵

“场景”一词基于海伦·尼森鲍姆的“场景完整性”理论，影响用户对于隐私敏感程度或接受程度的因素被称为“场景”（context）。个人信息的传播与利用无法摆脱信息主体以及政治、经济、文化等具体场景因素的影响，保护个人信息就是保护该信息传播的完整性不受破坏，确保信息合理流动[3]。该理论认为，在收集个人数据时，对于数据和隐私权的保护，应转向一种以场景为导向的动态的、多元的体系，数据收集以及后期的传播利用不应超出原定场景设想。该理论界定了：场景的意义，何谓个人信息的合理使用，何谓不合理使用等，这些在不同场合不尽相同，需要根据具体场景进行具体考虑。儿童作为特殊数据主体，本身就是场景的体现。

不同的场景决定了不同的信息流动规范和评价要素。影响场景完整性的因素包括三个方面：信息主体（actor）、信息类型（information type）和传播原则（transmission principle）①。其中，信息主体是指信息传播中的行为主体，包括信息的发送者、传播者、接收者、使用者等，不同主体在不同的场景下被赋予不同的角色，享有不同的权利和义务。信息类型是指信息的属性、特质与划分。敏感信息的界定需要置于场景之中，并不存在一种普适性、一般性的划分标准。传播原则是指信息在不同场景流动过程中的约束性规范，常见原则包括控制性原则、当事人同意、禁止信息向公众领域扩散等。

该理论认为，信息流动需要遵守特定场景下的流动规范，如果这些规范中的某一环节被违反，便破坏了场景完整性，会产生隐私风险。风险产生后，需要分析用户对于风险或者损害的接受程度，降低损害或风险直至用户可接受的程度，这在欧盟《通用数据保护条例》（GDPR）中被称为数据保护影响评估（DPIA）。场景不同，风险不同，《适龄守则》将隐私风险界定为：“任何重大潜在的物质的、身体的、心理的和社会层面的伤害”。由此可见，违反场景要素导致的风险的含义十分宽泛。

在上述原则上，判断数据保护是否符合当事人预期、是否合理方面需要考察以下方面：一是确认数据从谁流向谁；二是界定数据的类型；三是数据传播的约束性规范。主体、类型和传播原则这三项影响因素，虽然基于传播学理论提出，却与法律关系的主体、客体、内容不谋而合，二者具有高度一致性。信息主体即法律关系主体是法律关系的参加者，信息类型则是权利和义务所指向的对象，是法律关系的客体。传播原则是主体在一定条件下所享有的权利和承担的义务，是法律关系的内容。因此，借由“场景完整性”理论讨论数据的法律保护，既符合法律关系的三要素，也与传播学理论相契合，内在逻辑具备一致性。当实然的信息传播情形与应然的传播要素不一致时，就突破了保护隐私的预期设想，也就破坏了场景的完整性。从这个角度去衡量数据保护法律关系的主体、客体和内容，许多问题便迎刃而解。

---

① 关于场景理论的具体模型，参见 Barth A , Datta A , Mitchell J C , et al. Privacy and Contextual Integrity: Framework and Applications. IEEE, 2006.

（二）英美改革法案中以“场景”为导向的路径构建

场景的理念并非一蹴而就。在2015年美国《消费者隐私权法》（草案）中，“尊重场景”（Respect for Context）作为单独的章节出现，被赋予了法律意义，信息控制和透明度都要求依据具体场景进行[4]。2018年，GDPR也将场景作为一种导向，搭建起了场景完整性规则。如第22条“数据控制者义务”规定，机构应设定在职场、个人或家庭目的下利用，并根据其个人信息处理行为的性质、范围、场景、目的而承担相应责任。

《适龄守则》中凸显以场景为核心的构架，对处理儿童信息的规定进行细化、澄清。“适龄化”一词的理论根源便基于“场景”。该标准从欧盟与英国的数据保护法规入手，介绍了网络服务提供者和监护人在其中扮演的角色，重点规定了15条儿童适龄的网络服务设计标准，意图在于为儿童在线隐私与安全提供指引。其中规定，“ICO必须考虑儿童在不同的年龄阶段有不同的需求这一事实”“尊重儿童不断提高的做出选择的能力”。其中涉及场景化的规定包括：（1）机构在进行数据活动处理之前，应在早期进行数据保护影响评估，具体包括“向儿童和父母咨询、评估必要原则和比例原则、确定降低风险的措施”。（2）适龄应用。机构采用基于风险的进路来识别用户的年龄，在数据处理中专门针对儿童的权利和自由建立相应水平的保护举措。（3）透明度要求。针对不同年龄段的儿童，应提供多重选择。（4）家长控制。若服务提供家长控制的功能，则应提供与儿童年龄相适宜的提示信息等。《适龄守则》通过上述场景化规定，为儿童数据保护建立了以场景为基础、以数据评估为手段，通过区分细化不同的数字年龄、监护人职责、透明度要求进行风险控制的儿童数据保护体系，摆脱了以成年人和未成年人二元划分的儿童数据保护构架。

除上述立法外，早在1998年，美国便出台了《儿童在线隐私保护法》，为13岁以下的未成年人数据保护提供了指导说明和监管规则，2003年该法案第一次修订生效。2019年美国联邦贸易委员会启动了对该法的第二次修订，并公开征求意见，以确保该法能够满足活跃的市场技术变化。根据公开获取的资料，建议中提到的主要完善内容包括：调整年龄限制，采取灵活的年龄设置；增加透明度审查，机构需采取更加开放、便于外部审查的算法设计；注意教育技术带来的发展变化，学校可以代为父母做出授权等[5]。以上修改均可纳入场景的概念进行解释。

综上所述，场景完整性理论转变了传统儿童数据保护中二元论的固化思维，认识到信息从一个主体流向另外一个主体时诸多要素均对儿童的隐私期待产生影响。在未来，基于场景理论的儿童数据保护监管构造，将为儿童隐私保护提供一个更加有效的理论支撑。

二、儿童作为特殊数据保护主体的原因及困境

（一）儿童成为特殊数据保护主体的原因

1. 主体特殊性与数据持久性的二律背反

根据隐私控制理论，隐私是个人享有的决定自己何时、以何种方式以及在何种程度上披露自身信息不受干扰的权利[6]。《儿童权利公约》第16条规定，儿童的隐私、家庭、住宅或通信不受任意或非法干涉，其荣誉和名誉不受非法攻击。无论是从理论还是从公约层面，在数字化时代与网络环境下，对于个人信息的控制权由成年人享有，儿童也应当享有。但是，由于自身认知能力的欠缺，儿童普遍具有上网意愿强烈、上网方式熟悉、安全意识缺乏的特征，极易陷入“以隐私换便利”的错误认知中。儿童的监护人也可能对儿童信息保护造成负面影响，例如，许多父母在社交平台经常“晒娃”，就泄露了儿童的面部信息。儿童自身及其监护人对网络如何影响儿童的人格声誉以及未来发展尚未产生深刻认识。

网络中的信息数据所具有的持久性的特点，将对儿童的未来发展造成潜在危险。如联合国

儿童基金会研究中心伦理顾问Gabrielle Berman所说:“从儿童身上收集的网络数据可能在未来不确定的时刻,被网络服务提供者用不确定的算法用于不确定的客服端,以创建儿童所不知道的数字身份”[7]。面对儿童不经理性思考而存留下来的网络数据,如果无法有效删除,则容易导致未成年人的数字身份失控。

2. 行业自律缺失的治理黑洞

互联网企业对于自身的约束能够在保障儿童隐私、打击侵权行为上发挥直接而重要的作用。遗憾的是,互联网产业创新重于规范,漠视数据安全,追求便利与利益,仅依靠自身规范,监管效果十分有限。以抖音为例,下载并注册抖音账号时,并未出现单独的未成年人用户协议,未成年人相关条款隐藏在《用户服务协议》中。注册抖音账号时,仅需手机号码与验证码,没有年龄提醒以及单独的未成年人用户服务协议或隐私政策,注册之后弹出可自行设置的青少年模式,但该模式存在程序化倾向,用户点击“好的”之后即可直接使用该程序。通过推定监护人同意的模式,未成年人使用抖音服务不存在任何障碍,这实际上剥夺了监护人的拒绝权。在程序上虽然满足了告知与授权的两个步骤,但监护人难以获得实际的监护权。

3. 损害结果多元的弥散风险

网络服务提供者收集到的数据,一方面可以供自身使用,另一方面可以转移或者出售给其他网络服务提供者。随着物联网技术的发展,智能产品层出不穷,损害不仅局限于财产安全,甚至可能通过跟踪、监视行为威胁人身安全。2018年5月,IOS平台青少年手机监控应用程序TeenSafe服务器发生泄漏,由于Apple.ID以及邮箱地址和密码没有加密设置,因此,黑客访问其服务器后直接访问儿童个人数据[8]。2020年,知名儿童游戏Animal Jam的制作公司WildWorks同样发生了数据泄露事件,4600万条记录泄露,内容包括用户名、密码、性别、出生年份等[9]。

比数据泄露损害更为严重的是数据滥用。国际计算机研究所2018年的研究报告显示,活跃在市场上的过半Android应用,涉嫌违反了COPPA[10]。大量儿童隐私数据已经在暗网(dark web)上被非法贩卖。犯罪分子可以将不同的儿童数据信息进行拼凑,通过创建数字合成身份(synthetic identities)进行诈骗、申请贷款或办理信用卡等活动。在我国,利用网络收集个人信息,然后出售、牟利,日益形成了一条隐秘且完整的产业链,利用职务便利非法获取、买卖儿童个人信息获刑的公开报道屡见不鲜[11]。

(二)儿童数据保护传统规则下的困境

传统规则下,对于儿童的数据保护是基于知情和同意构架的[12]。机构在收集儿童数据之前,需要告知儿童或者监护人对于数据的处理情况。一般的表现形式是发布用户协议或隐私声明,由儿童自身或监护人同意作为对个人数据收集和利用的合法授权。然而,在这种知情同意以及监护人控制的传统框架下,能否对儿童产生实质保护存在疑问。

1. 儿童的数据保护需要通过衡量成熟度来决定赋予儿童何种自我决策的权利

《儿童权利公约》第12条规定,“缔约国应确保有主见能力的儿童有权对影响到其本人的一切事项自由发表自己的意见,对儿童的意见应按照其年龄和成熟程度给予适当的看待。”对儿童成熟程度进行划分的标准分为两种:一种是较为常见的年龄标准,采取这种方式,能够得出是或否的明显结论,执行起来更为容易。但儿童还受外在环境、自身条件等差异的影响,一刀切会忽视儿童的个性化发展程度。另外一种方式是在理想状态下,依据每个儿童的成熟度以及相应的网络环境进行个性化评估。以个体为单位的个性化评估虽然理想,但在当前技术和成本条件下并不现实[13]。

2. 在成熟度划分基础上对权利和义务的设定更为重要

一方面,儿童随着自身成长,依赖成年人并被照顾的需求不断降低,国家以及监护人的干

预理应降低；另一方面，儿童包括言论自由和表达自由在内的自我决策的权利应当被相应赋予，这种关系被一些学者称为赋权和保护（Empowerment vs protection）[14]，二者存在紧张关系。在区分不同成熟程度的前提下，如何赋予儿童相应权利，又避免过度保护，成为一大问题。

3. 知情同意机制为儿童用户及其监护人带来沉重负担

个人信息流转的复杂性与隐私声明的简单易懂之间产生了矛盾。个人信息在存储后以何种方式得到利用和存储往往难以预料，机构为了合规要求，需列出冗长复杂、晦涩难懂的隐私说明，给用户带来了沉重的理解负担。有研究表明，如果用户将一年中所使用的网络服务用户协议声明全部阅读完毕，需要花费244小时[15]。正如学者Susan Landau所言，隐私声明远非为人类使用而设计[16]。因此，现实中大多数用户，无论是成年人还是儿童，均直接点击同意，忽视隐私协议内容，被迫接受同意，告知和同意沦为形式。

事实上，在互联网时代，儿童数据的特殊性保护问题尚未得到解决。而随着大数据时代的到来、物联网技术的发展，监护人知情同意的传统保护方式已经无法为儿童提供切实有效的保护手段，需要扩展新的理论与方法。

三、场景完整性理论阐释下的儿童数据保护新理念

基于前述英美改革法案中以场景为导向的路径构建，笔者从信息主体、信息类型以及传播原则出发，对英国《适龄守则》和美国COPPA涉及场景完整性的亮点进行逐一阐释。

（一）信息主体的场景化：细分数字年龄

1. 细分数字年龄的必要性

如上文所述，对儿童成熟度进行划分的方法有两种，一种是年龄，一种是个性化评估。基于年龄进行划分是目前的主流规定，达到年龄界限的儿童视为具有能力处理个人数据，未达到年龄界限的儿童需要父母给予同意或者拒绝。至于年龄的确定标准，各国法律中并没有作出解释，“一刀切”的模式显得过于随意，也缺乏实证数据支持。以美国为例，为何选取13岁作为标准，一种观点认为，英语数字中对于child（儿童）的界定是12周岁，超过13周岁的不再是child，而是teenager（青少年）。还有一种观点认为，这与美国电影分级制度一致，其中PG13为特别辅导级，建议13岁以上儿童观看，而NC.17级是属于17岁以下禁止观看的影片[17]。

设定明确年龄界限，对于儿童自身来说也存在一定问题。受生长环境和能力差异的影响，不同年龄的儿童自我参与和决策的能力存在差异，“一刀切”将限制一部分成熟度较高的儿童的参与权，忽略了儿童的个性化发展。另外，儿童年龄的划分没有考虑到隐私风险的差异，例如，儿童开设社交媒体账户，需要父母同意，而使用电子邮件则未必需要获得父母同意[18]。单纯的年龄划分缺乏对场景以及风险的区分。

2. 细分数字年龄的途径

尽管有学者指出，儿童个性化评估将会增加网络服务提供者和监管者的负担，但并不构成阻碍场景化监管的有力理由。例如，在电影和游戏分级中，儿童年龄划分更为详细。在我国《游戏适龄提示草案》中，依据用户的生理特征、认知能力、道德水平等，将其年龄划分为18岁、16岁、12岁、6岁四个阶段，6岁以下儿童需要在家长陪同下才可以接触游戏，6－11岁的儿童不提倡在游戏中过度社交，12－15岁以及16－17岁的青少年，有必要进行针对性关注等[19]。欧洲非政府组织儿童在线安全联盟（eNACSO）也认同以个体为单位的评估在当前技术条件下并不可行，但这不妨碍对儿童年龄进行细分，设立不同的父母同意方式[20]。

因此，在信息主体场景化中，儿童作为特殊保护群体仅是第一层次划分，需在这一基础上

继续进行场景化，对数字年龄进行详细划分。立法者有必要对年龄跨度和相应的心理状态、生理状态、行为特性进行详细的测试。《适龄守则》中，将儿童分为0－5岁学龄前期、6－9岁学龄初期、10－12岁过渡期、13－15岁青少年初期以及16－17岁即将成年期。不同年龄段的儿童被赋予不同的自我决策权，取代了传统单一划分。《适龄守则》同时规定了年龄的验证方式，包括：自我声明，人工智能，第三方年龄验证，账户持有人确认，权威标识符，设置链接跳转至官方身份认证页面，如填写护照信息等方式等①，以上方式均具有借鉴意义。

（二）信息类型的场景化：着重高风险信息

1. 划分信息类型的必要性

目前，儿童使用网络的监护人同意方式可以分为三类：一类以我国国内微信、抖音在内的软件为代表，为推定监护人同意模式。一类是简单的可验证同意方式，如Facebook要求依据信用卡、借记卡或其他需要身份验证的在线支付系统，确认表示“同意”的人为有资格申请信用卡、借记卡的成年人。最后一类是复杂的可验证同意方式，可由家长签署邮寄知情同意书并返回给网络服务提供者。监护人同意尽管存在着不同的验证模式，但由于缺乏场景化的理念，产生了诸多争议。欧盟GDPR第35条对涉及个人信息的数据进行了分类②，区分了高风险信息与低风险信息，对于低风险的数据处理行为，豁免了部分规定，而对可能引发高风险的行为设定了附加义务。儿童数据作为高风险数据被要求进行影响评估，但对于不同的评估结果应如何处理，却未提出明确要求。这导致各种类型的网络服务都需要得到监护人同意，范围十分广泛，易产生疲劳[21]，使得监护流于形式。另一方面，监护人同意不符合比例原则，在有的严格同意方式中，设置了家长提供身份证件的要求，作为一项敏感个人信息，是否有必要在监护人同意中提供身份证件，值得进一步讨论。

美国的法律中并没有将所有的网络行为都纳入监护人同意范畴，而且基于风险不同划分了不同信息类型，规定了不同级别的监护人同意[22]。没有互动或者数据不需要传播共享的行为产生的数据被视为低风险，使用时无须得到监护人同意。如果网络服务提供商仅在内部使用数据，并不向第三方披露和公开时，可以采用较为宽松的监护人同意形式，如向父母发送电子邮件获得回复后，视为获取监护人同意。而对于涉及敏感信息的网络服务，必须要获得最为严格的监护人同意，如涉及儿童面部信息、身份识别号码或者数据需要向第三方提供时，可以采用电话或者视频的方式获得父母的当面授权，或者采用电子方式填写详细的同意书。

基于信息类型的不同，设置差异化的监护人同意方式，在一定程度上解决了同意疲劳的问题。COPPA在新一轮修订中，提出了明确的监护人同意例外，如涉及教育目的的网络服务提供商在处理儿童信息时，学校可以代替父母进行统一的同意表示，而不需要监护人个体作出回应。监护人具有知情权，学校应将儿童数据如何获取、如何使用、如何处理等及时告知监护人，代替监护人对未成年人的信息负责；还需明确界定教育目的的含义，禁止不必要的数字画像、营销和广告服务等。

2. 划分信息类型的途径

对于儿童数据类型划分最大的困难来源于个人信息与非个人信息、敏感信息与普通信息的二分法局限。个人信息的范围并没有一个抽象概括的精准界定，需要高度依存数据所在的场景。以监护人同意的标准为例，以信息类型为指引，重点针对容易引发高风险的信息进行规制，可以成为一种有效方式。儿童数据如用于构建图像或者对儿童作出不利决定，需要为监护

① 参见：Age appropriate design: a code of practice for online services：3. Age appropriate application.
② 参见 Art. 35 GDPR Data protection impact assessment.

人提供相应的控制机制，网络服务提供商也应根据风险评估等级设计监护人控制机制。当风险级别为低级时，可以考虑采取推定监护人同意模式，甚至豁免监护人的同意；当风险评估等级为中级时，可以采取简易方式获取监护人同意并告知监护人风险；对于高风险信息，则应当进行重点规制，初始披露中以较为复杂的方式获得监护人的控制。除此之外，机构也应当向监护人进行即时披露，增强告知机制，并且主动采取措施降低风险。

对信息类型进行场景化划分，区分中高低风险，必不可少的就是数据保护影响评估（DPIA）。数据保护影响评估作为评估隐私风险的流程与工具，在国际社会上已经获得了普遍认同与实践。欧盟GDPR将风险程度划分为高中低三种级别，机构可结合自身行业自行确定具体划分方式。在《适龄守则》中，也有着明确的数据保护影响评估规定，要求机构根据不同的年龄能力和发展需求进行风险评估，坚持必要原则和比例原则，识别和评估风险，并采取降低风险的措施。作为一种已经成熟的隐私评估工具，与场景化完整性理念一致，在个案中对风险进行评估，既有助于为机构提供明确的指引，也可为机构结合自身行业采取灵活调试的标准留出柔性缓冲的空间。

（三）传播原则的场景化：透明度要求

传播原则是指信息在不同场景流动过程中所具有的约束性规范。让儿童及其监护人理解用户协议和隐私政策的内涵具有特殊的意义。通过增加透明度，有助于增强用户的安全感和信任度，提升机构处理儿童数据的接受度，实现信息价值的最大利用与开发。GDPR第58条也指出，应以儿童易理解的简洁语言向儿童提供信息。但在实践中，由于缺乏场景化理念，如何落实透明度成为棘手问题。例如，在收集14岁以下儿童信息时需要获得监护人同意，此时，用户协议和隐私政策的读者是监护人而非儿童，那么是否有必要针对儿童再设置一份简洁易懂的用户协议呢？简洁易懂是要让儿童易懂，还是让监护人易懂？年龄较小的儿童由于认知能力较差，用户协议和隐私声明中对于数字画像、精准营销、数据处理和使用的规定无论如何简洁易懂，儿童都可能无法充分认知和理解，此时应如何落实透明度规则？在传统机制无法解决上述问题的情况下，简洁易懂的要求已经逐渐沦为一种形式，儿童既不阅读也不理解其内涵。

在场景化理念下应当以场景导向提升信息处理的透明度。《适龄守则》充分认识到此局限，强化了告知义务的要求，规定了实现透明度的“合理性”标准。《适龄守则》规定，向用户提供的隐私条款以及其他公开条款、政策和社区标准，应当风格简洁、语言清晰和适宜儿童阅读理解，特定情形下应及时特别提示。在具体规则上，对于监护人，守则要求机构根据GDPR第13条和14条向家长提供适合阅读的完整信息。对于儿童则区分年龄段：对于0－5岁的学龄前儿童，需向其提供音频视频，告知禁止与允许的行为；对于6－9岁的学龄初期儿童，需向其提供卡通片、音频和视频，简单解释服务中涉及的隐私概念、默认设置、谁可以看到以及如何操作；对于10－12岁过渡期儿童，须向其提供书面或音频和视频，提供简单信息和详细信息选项。当试图改变默认设置时，通过视频音频告知后果；对于13－15岁青少年初期的儿童，需向其提供书面或音频和视频，提供简单信息和详细信息选项。当试图改变默认设置时，通过视频音频告知后果，可提示他们可向父母寻求帮助；而对于16－17岁即将成年的少年，则应向其提供书面或音频和视频，提供简单信息和详细信息选项。当试图改变默认设置后，可提供书面、视频和音频告知其风险与后果，提示可向成年人或其他信息可信来源处查询。

《适龄守则》上述方案有效完善了儿童透明度规则。首先，规则解决了透明度是针对儿童还是监护人这一问题，规定了对于监护人和儿童双重的透明度要求。对于监护人要求提供完整的信息，对于儿童则根据不同年龄段提供符合年龄的简洁易懂的信息。其次，规则试图去保障年龄较小、理解能力较差的儿童的知情权。规则并不要求儿童理解个人信息保护和数据使

用等规则，而是试图以动画的形式简单解释相关行为，这对于儿童的权利意识培养和法律普及有益无害。最后，随着儿童年龄的增大，用户协议和隐私要求不断完善，并逐步与成年人要求相符。设置不同区间的透明度规则虽然会增加网络服务提供商的负担，但有利于儿童利益的提升，无疑可有效覆盖实施成本，具有正外部性。

四、启示

近年来，我国在立法上也认识到了儿童作为特殊数据主体的必要性。2019年《儿童个人信息网络保护规定》出台，成为首个儿童数据保护的专门性立法。2021年生效的《民法典》专章设置了隐私权和个人信息保护。《未成年人保护法》2020年最新修订版将网络保护作为六种保护方式之一进行列明。此外，多项国家标准也对未成年人的数据保护进行了单独规定，已经初步构建起了儿童数据保护体系。从场景完整性的解释路径出发，我国有必要通过隐私理论和法学要素的连接，将儿童数据保护置于场景完整性的框架内进行阐释。

首先，儿童需要依据年龄差异享有不同的权利与义务。依据《未成年人保护法》，网络保护的对象年龄上限设定为18周岁，监护人同意年龄设定为14周岁。而《儿童个人信息网络保护规定》则将保护主体以及监护人的同意年龄均设定为14周岁。《数据安全管理办法》（征求意见稿）第12条规定，收集14周岁以下未成年人个人信息的，应当征得其监护人同意。可见，我国对于儿童数字年龄的划分是14岁和18周岁，存在两个区间，未成年人均可获得特殊的网络保护，14周岁以下需获得监护人同意。相比于《适龄守则》，我国的年龄划分相对单一。《民法典》第19条规定，儿童可以独立实施与其年龄、智力相符合的或者纯获利益的民事行为。那么在网络世界中，与其行为年龄和智力相适应的或者纯获利益的活动，是否可以豁免监护人同意呢？

对于上述问题，我国可以在实证调研的基础上科学划分年龄段。结合我国现有规定，可以将儿童数字年龄划分从2个区间增加至4个区间，即学龄前8周岁、过渡期14周岁、青少年初期16周岁以及18周岁阶段，并可采用自我声明、人工智能、第三方年龄验证、账户持有人确认等方式确认儿童年龄，并在细分数字年龄基础上，确定不同的信息传播规范。

其次，场景完整性理论要求对信息属性、信息特质的界定须在特定场景中进行。《儿童个人信息网络保护规定》第9条规定，网络运营者收集、使用、转移、披露儿童个人信息的，应当征得儿童监护人的同意。《未成年保护法》第12条规定，处理不满14周岁未成年人个人信息的，应当征得未成年人的父母或者其他监护人同意，但法律、行政法规另有规定的除外。前者立法与欧盟GDPR和美国COPPA一致，而后者立法在前者的基础上，增加了“法律、行政法规另有规定的除外”。实践中还是采取了一刀切的监护人同意模式。建议借鉴美国COPPA中的监护人规则，建立基于不同场景下差异化的父母同意方式，进行数据影响安全评估，涉及高风险信息的，如与第三方合作处理儿童数据的，签订协议明确双方处理事项、处理目的、处理范围后，必须获取监护人的明示同意，并可设置较为复杂的同意方式。而对于低风险场景下的信息，可以在规范中明确监护人同意的例外，即明确“法律、行政法规另有规定”的范围包括哪些。比较典型的就是考虑以学校教育为目的收集处理学生信息，可以直接默认同意，无需获得监护人同意。但同时也应在立法中明确教育为目的范围，禁止采取的行为、父母与学校责任的划分等。

最后，传播原则中要对透明度有所要求。在我国，监护人同意模式主要是推定同意，《儿童个人信息网络保护规定》中，对于儿童的个人信息保护规则和用户协议，仅要求指定专人负责（参见第8条），相比于征求意见稿，删除了应当简洁易懂的要求（参见《儿童个人信息网络保护规定（征求意见稿）》第5条），这无疑减轻了网络服务提供商的工作量，但是正因如此，推定同意

模式下透明度要求便显得尤为重要。与监护人同意权的落实一样，网络服务提供者需要开发一套简洁易懂的规定，对于简洁易懂的定性，建议借鉴《适龄守则》并结合我国具体实际情况，通过音频、视频、书面等方式告知儿童相应操作。

[参 考 文 献]

[1] 倪蕴帷：《隐私权在美国法中的理论演进与概念重构——基于情境脉络完整性理论的分析及其对中国法的启示》，载《政治与法律》，2019年第10期。

[2] ICO. Age Appropriate Design: a Code of Practice for online Services，https://ico.org.uk/for - organisations/guide - to - data - protection/key - data - protection - themes/age - appropriate - design - a - code - of - practice - for - online - services/

[3] Nissenbaum H . Privacy As Contextual Integrity. Washington Law Review，2004，(1).

[4] 范　为：《数据时代个人信息保护的路径重构》，载《环球法律评论》，2016年第5期。

[5] 华　劼：《论〈儿童个人信息网络保护规定〉之完善——以美欧儿童网络隐私保护立法的比较和借鉴为视角》，载《重庆邮电大学学报(社会科学版)》，2021年第1期。

[6] WESTINA . Privacy and Freedom. New York: Atheneum，1967，p.7.

[7] Berman，G. & Albright，K.，Children and the Data Cycle: Rights and Ethics in a Big Data World，UNICEF Office of Research Working Paper，2017，p.8.

[8] Teen phone - Monitoring App Reportedly Leaks Account Information，https://www.cnet.com/news/teen - phone - monitoring - app - reportedly - leaks - account - information/

[9]《儿童游戏Animal Jam制作公司WildWorks确认发生数据泄漏事件》，https://finance.sina.com.cn/tech/2020 - 11 - 17/doc - iiznezxs2264563.shtml.

[10] Won't Somebody Think of the Children?https://www.petsymposium.org/2018/files/papers/issue3/popets - 2018 - 0021.pdf.

[11]《上海疾病预防控制中心出"内鬼"数十万新生儿信息被售卖》，http://news.youth.cn/jsxw/201705/t20170517_9794846.html.

[12] 宁　园：《个人信息保护中知情同意规则的坚守与修正》，载《江西财经大学学报》，2020年第2期。

[13][22] 付新华：《大数据时代儿童数据法律保护的困境及其应对——兼评欧盟〈一般数据保护条例〉的相关规定》，载《暨南学报(哲学社会科学版)》，2018年第12期。

[14][21] Macenaite M . From Universal towards Child - specific Protection of the Right to Privacy online: Dilemmas in the EU General Data Protection Regulation.，New Media & Society，2017，(5).

[15] 万　方：《隐私政策中的告知同意原则及其异化》，载《法律科学(西北政法大学学报)》，2019年第2期。

[16] Landau S . Control Use of Data to Protect Privacy，Science，2015，(6221).

[17] 孙益武：《儿童个人信息保护是伪命题还是真难题——兼评〈儿童个人信息网络保护规定〉》，载《青少年犯罪问题》，2020年第2期。

[18] ICO. Personal Information Online Code of Practice，2010，https://ico.org.uk/media/for - organisations/documents/1591/personal_information_online_cop.pdf.

[19]《人民网起草〈游戏适龄提示草案〉，将搭建网上提示平台》，http://society.people.com.cn/n1/2019/0626/c1008 - 31197366.html.

[20] eNACSO，Is the UNCRC fit to Purpose in the Digital Era? http://www.enacso.eu/wp - content/up - loads/2015/11/eNACSO_Report_UNCR_IGF_2012.Pdf.

(责任编辑：王俊华)