未成年人个人信息保护:理论澄清与规则重塑

安　琪
(云南民族大学 法学院,昆明 650504)

【摘要】从概念界定而言,未成年人个人信息的范围应体现出对象的特殊性,未成年人权益保障与网络产品和服务提供者的商业利用目的、未成年人信息自决权的多元立法价值也需得到进一步澄清。尽管我国已经初步建构了未成年人个人信息保护的立法规则,但实践表明,当下非授权的恶意收集、使用未成年人个人信息的行为较为普遍,作为安全保障重要途径的监护人"告知—同意"模式面临失范风险,且针对网络产品和服务提供者的监督机制尚未发挥长期的影响力,权利救济路径也因法益保护的错位而产生阻碍。未来应当将"最有利于未成年人"原则予以细化落实,并以年龄为界分点构建未成年人信息的分层授权机制。此外,应针对未成年人不同的个人信息类型设置强度不同的监管规则,畅通被侵犯主体的权利救济路径,以实现多层次、精细化保障未成年人个人信息安全的目的。

【关键词】未成年人　个人信息　信息安全　保护路径
DOI:10.16034/j.cnki.10-1318/c.2023.02.010

在数字时代的背景下,网络在未成年人的学习及生活中扮演着不可或缺的重要角色。中国互联网络信息中心发布的《2021年全国未成年人互联网使用情况研究报告》显示,2021年我国未成年网民达到1.91亿人,小学生互联网普及率达95.0%,触网低龄化趋势愈加明显[1]。随着互联网在未成年人群体中的普及,如何保护未成年人个人信息安全引发公众的强烈关注。《中华人民共和国未成年人保护法》《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》)、《儿童个人信息网络保护规定》等法律法规对这一问题作出了积极回应,彰显了我国保障未成年人个人信息的决心。但鉴于现有的立法多为原则性规定,难以有效回应实践中频发的恶意收集、利用未成年人个人信息等行为,与保障未成年人权益的整体目标相抵牾。本文拟就未成年人个人信息相关的理论问题展开论证,在厘清如何平衡未成年人个人信息保护领域涉及的多元价值的前提下,探讨我国当下未成年人个人信息保护面临的风险挑战,继而提出立法完善思路及具体程序构建内容,以期就教于同仁。

一、未成年人个人信息保护的理论澄清

作为本文的研究对象,未成年人个人信息的概念内涵及权属外延是展开论证的基础。笔

收稿日期:2023-01-18
作者简介:安　琪,云南民族大学法学院讲师,硕士生导师,主要研究讼诉法与司法制度。

者认为，该界定需要在我国未成年人权利保障的整体语境下完成。

（一）未成年人个人信息的界定：对“可识别性”的反思

有关个人信息的概念，我国采用的是国际上通行的“识别说”，即“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。”①在现有立法统一采用“识别说”的前提下，《个人信息保护法》以及《未成年人网络保护条例（征求意见稿）》将14周岁作为划分未成年人与成年人个人信息的标准，将不满14周岁的未成年人个人信息界定为敏感信息，适用严格的程序规范。

但上述立法概念可能难以回应日益增长的保障未成年人个人信息的需求，特别是伴随着网络技术及大数据手段的发展，未成年人个人信息的界定范围受到冲击。一些本不具有指向性的信息经过数据的整合再加工，便可“转化”为具识别性的个人信息。这一特征在社会关系相对简单、信息较为集中的未成年人群体中尤为显著，即便有对未成年人姓名、肖像的匿名化处理，也可以通过信息主体所在区域、年龄、性别等公开信息拼凑出未成年信息主体的身份，继而引发网络霸凌、网络侵权等侵害未成年人人身权、财产权的行为，也会令网络产品和服务提供者刻意规避法律规范，挖掘出匿名化的未成年人数据背后具有商业价值的信息。故从立法层面上亟需反思目前界定未成年人个人信息范围的合理性，在“最有利于未成年人”原则的指引下，对未成年人个人信息实现最大程度的保障。

（二）未成年人个人信息保护的立法价值再厘清

《个人信息保护法》中对立法目的表述为“为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用”。可见立法者试图寻求保护个人信息与发掘个人信息价值之间的平衡关系，以促进信息产业的发展。但由于未成年人不具备完全的个人信息自决权，甄别、筛选有害信息的能力也有待提升，需要国家、社会、家庭的及时干预和介入。因而，合理利用未成年人个人信息的立法目的要让位于更高位阶的未成年人个人信息安全的保障，立法者应在“最有利于未成年人原则”的指引下，实现对网络产品和服务提供者行为的有效规制，相较于利用个人信息的商业价值，应将保护未成年人个人信息权益作为首要考虑的价值。

此外，还需要关注如何平衡保障未成年人信息安全的需求与可能让渡的未成年人隐私权。在“国家亲权”理论下，国家已成为超越家庭单位之上的责任主体，以保障未成年人利益的最大化[2]。该理论也在《未成年人网络保护条例（征求意见稿）》中得以体现②，但这一缺少外部监督的追踪保护机制，可能带来对未成年人隐私权保障的冲击，造成网络服务提供者擅自单方扩大访问未成年人信息范围的后果，在立法中并不乏见类似的可能侵犯未成年人隐私信息的内容。需要明确的是，应在强调尊重和保护未成年人的隐私权的基础上，严格控制网络安全保障措施的适应范围，避免出现任意适用干预措施对未成年人隐私权带来消极影响。

二、未成年人个人信息保护的实践应用困境

如上文所述，未成年人个人信息具有特殊属性，即更模糊的“可识别性”边界与显著的国家干预性。我国立法构建了未成年人个人信息保障的框架，设置了从收集到利用未成年人个人信息环节的诸多规则，以实现从事先预防到事后救济的全过程保障。但上述法律保护框架在

①《中华人民共和国民法典》《中华人民共和国网络安全法》以及《个人信息保护法》中均有个人信息的立法界定内容，考虑到特别法及新法的特征，本文采用《个人信息保护法》第四条的立法表述。

②《未成年人网络保护条例（征求意见稿）》第四十三条规定：“网络服务提供者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示，并采取停止传输等必要保护措施，防止信息扩散。”

实践中却面临失范风险，具体如下。

（一）未成年人个人信息保护的规则失范

首先，现有立法对未成年人个人信息的界定主要以年龄为区分标准，会令立法保护对象范围面临窄化的风险。立法通过将不满14周岁未成年人的信息界定为敏感信息，辅之监护人同意规则实现保护目的，而对于处理已满14周岁的未成年人个人信息的行为，《未成年人网络保护条例（征求意见稿）》中则重申了《个人信息保护法》中确立的“合法、正当、必要和诚信原则”，其他处理信息范围等内容也基本比照成年人个人信息的“最小授权原则”，难以体现未成年人信息安全保护的特殊要求。对于已满14周岁的未成年人而言，尽管其在信息识别的能力和风险防范意识上有所提升，但与成年人个人信息自决权依然有差异，可能因个人信息被滥用而带来较大网络安全隐患。若一刀切地将14周岁作为个人信息保护的分界点，则会导致对已满14周岁未成年人信息特殊保护目的的落空。

其次，除了上述敏感信息使用规则外，具有巨大商业利用价值的自动化决策行为未被立法者纳入规制的范畴①。诚如上文所述，在未成年人保护领域，网络服务提供者利用个人信息的价值应让位于我国保障未成年人信息安全的价值。但由于立法未禁止针对未成年人的自动化决策行为，导致网络产品和服务提供者在利益最大化的驱动下，诸多针对个人信息展开的分析行为缺乏对主体的明确告知及授权，在理应客观、全面获取、吸收信息的未成年人群体中，在其毫不知情的情况下，网络产品和服务提供者通过隐蔽性的收集信息，分析其偏好，继而“投其所好”地选择性推送信息，使未成年人困于“信息茧房”却浑然不知，无疑不利于其合理使用网络资源。

最后，由于现有立法规定的粗疏，未明确收集未成年人个人信息的范围和具体方式，导致实践中网络产品和服务提供者较为隐蔽地收集用户信息行为尚未被纳入立法规制的范畴。例如，未成年人在使用网络服务时会通过检索商品、浏览特定内容、购买特定商品等活动暴露自己的行为偏好，网络服务器也会在Cookies文件中储存浏览网页地址、检索内容、停留时间等信息，完成对用户行为的记录[3]，这类带有显著个人特征的未成年人个人信息，可能在商业利益驱动下，被擅自收集和利用。此外，在使用网络产品的过程中，可能存在动态收集非授权信息或向第三方提供未成年人个人信息的行为，而立法并未设置使用过程中未成年人监护人再次强制授权的规定，导致实践中通过注册时的单次授权行为便默认可以适用于之后的所有信息收集行为，有刻意规避立法规则的嫌疑。上述立法空白领域带来了未成年人信息安全的潜在风险。

（二）“告知—同意”框架的应用考察

立法层面通过设置监护人“告知—同意”程序作为实现未成年人信息安全的重要保障途径，但该程序在运行时趋于形式化和非强制性等特征，导致这一本应扮演“守门员”角色的程序在实践中难以发挥应有作用。下文主要以未成年人常用的12个应用程序（以下简称APP）的隐私条款为研究对象②，考察“告知—同意”框架在实践中的应用现状。

1. 未成年人的身份验证形式化

经比对发现，所选取的12个APP中的《隐私政策》均采用了“选择加入”（opt-in）模式（即仅有授权模式下才能对个人信息进行有效的处置行为）以及专门的“未成年人保护”章节，这说明实践中未成年人信息安全保护规则已基本落实。但同时，各APP对未成年人的年龄界分标准

① 《个人信息保护法》第七十三条第二款规定：“自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。”

② 本文根据2022年7月互联网周刊发布的各类别应用排名前10的APP榜单，在其中筛选出未成年人访问频率较高的社交、短视频、娱乐直播、二次元、游戏五个领域，分别选取其中排名前二至前四位的APP共12个作为考察对象，分别为“微博”“微信”“QQ”“小红书”“抖音”“快手”“哔哩哔哩”“快看”“王者荣耀”“和平精英”“虎牙”“斗鱼”。

并不统一，大部分APP采用与立法一致的18周岁为标准，也有采用《个人信息保护法》中的14周岁为标准。而在信息范围的划定上，部分APP呈现出收集未成年人信息的无差别性，即便在其他有明确说明未成年人信息收集规则的APP中，也将收集信息的范围表述为“在法律允许、父母监护人明确同意或保护未成年人所必要”，缺乏对未成年人群体个人信息的特殊保护。

就身份验证的形式来看，依然有部分社交、短视频APP未设置强制验证身份的规则，即便未注册账号也可以通过游客身份浏览视频、观看APP内容。而在强制验证身份的APP中，验证方式主要为手机号码注册或第三方账号授权，未成年人可通过控制监护人手机的方式轻易完成虚假身份验证，且大部分APP允许第三方授权，也会导致未成年人在完成某一APP授权后便可借此躲避身份验证程序。在需要填写生日信息识别未成年人身份的软件中，可以自行修改出生日期，进而“伪装”为成年人继续使用软件。

在所考察的APP中，仅有“和平精英”针对“部分游戏或针对部分用户”启动人脸识别验证身份，但该验证方式并未覆盖全部用户，也会带来未成年人身份识别方面的障碍。未成年人的身份验证不仅在注册时显得颇为形式化，在使用过程中也很难体现出对未成年人身份的核验。在“哔哩哔哩”“斗鱼”的《隐私政策》中也“无奈”地承认了未成年人身份认证的非完备性[①]。可见，当下在未成年人身份验证方式上存在形式化的现象，而一旦无法验证未成年人身份，自然难以启动监护人告知程序。

2. “告知—同意”验证方式的非强制性

尽管所考察的APP均设置了未成年人监护人同意条款，但大部分APP并未说明如何实现对“告知—同意”规则的验证，少数APP以行为默示的方式完成对监护人同意行为的推定，即申请账号、使用功能时便视为已取得同意，体现出验证方式的随意性。而在监护人联系机制方面，收集监护人手机号码、电子邮箱等联系方式也并非强制性要求，在《隐私政策》中仅表述为“可能收集”联系方式验证身份。可见，“告知—同意”规则在实践中易被异化为选择性程序，与立法设置的强制性同意规则相悖。

3. 非法收集信息行为的普遍性

如前文所述，现有立法并未界定收集未成年人个人信息的方式和范围，而这一立法空白导致非法收集未成年人个人信息的行为在实践中较为普遍。部分APP设置了事后删除规则，即“在未事先获得可证实的父母或法定监护人同意的情况下收集了未成年人的个人信息，则会设法尽快删除相关数据”，该规则默示了网络产品和服务提供者在并未得到监护人授权下可以擅自收集未成年人信息的行为，且主要通过事后监督的方式完成对自我非授权行为的纠正，但该自我纠错机制动因不足，可能导致对非法收集信息行为的人为放纵结果。

并且，以上对于监护人“告知—同意”模式的考察建立在监护人明确知晓《隐私政策》、完全理解条款内容的前提下，但实践中不少监护人难以在冗长复杂的《隐私政策》中认识到未成年人信息保护的必要性及网络产品和服务提供者所应承担的义务，随意跳过《隐私政策》的行为可能导致非本意的授权行为，也在一定程度上带来了未成年人个人信息被恶意收集、使用、泄露的风险。

（三）监管措施的应对乏力

我国公权主体监管个人信息处理行为主要采用“行政机关为主、司法机关为辅”的模式。近年来，中央网信办通过积极推进“清朗”等专项行动，短时间内集中解决涉未成年人网络安全

① “哔哩哔哩”和“斗鱼”的《隐私政策》中均规定：“请您理解，除上述已通过实名认证的儿童用户或您主动告知的儿童用户以外，大多数情形下我们无法识别使用我们的产品与/或服务的具体人员信息是否属于儿童个人信息，即我们无法判断收集和处理的设备信息、上网操作记录等不具备明显年龄识别特征的个人信息是否属于儿童个人信息”。

问题的乱象，取得了一定治理效果。但从机制发挥的长效性来看，以此类定期专项行动为主的监督效果可能不彰。针对各网络产品和服务提供者制定的《隐私政策》内容，在完成对其文本审核的前提下，对该信息收集和使用的过程尚未形成动态监管。不少APP非法获取、利用信息的行为，多因为家长的举报而被整改①，体现出一定的滞后性和被动性。

2020年修订的《中华人民共和国未成年人保护法》规定，检察机关可以就侵犯未成年人合法权益的行为提起公益诉讼。2021年全国检察机关未成年人保护公益诉讼立案6633件，其中，办理新类型公益诉讼案件4676件，占比70.5%，涉及向未成年人销售烟酒、网络游戏、电竞酒店、密室剧本杀等新兴业态治理[4]。检察机关借助公益诉讼实现对包括未成年人个人信息在内的司法保障，突出了“能动检察”的理念，但相较于侵犯个人信息行为的普遍性，公益诉讼的启动带有个案意义②，难以形成对行业的整体监督，属于补充型的司法监督模式。

除却公权机关的监督模式外，行业自律也是重要的监督方式，《中华人民共和国网络安全法》（以下简称《网络安全法》）及《未成年人网络保护条例》明确将“加强行业自律”写入其中。中国互联网协会于2002年制定并发布《中国互联网行业自律公约》，在该公约中虽然设置了若干利用公民个人信息的规则，但由于仅为自律义务，并未达到任何实质意义上的监督效果。且该公约公布至今已有二十余年，内容宽泛、缺乏具体规则的条文显然已经难以适应当下互联网环境，仅靠各互联网主体自觉履行行业自律，其效果可想而知。

（四）被侵犯主体救济路径阻塞

依据侵犯未成年人个人信息的行为的性质，可将救济模式划分为民事侵权追责模式和刑事追责模式两种。但实践中，对侵犯未成年人个人信息的行为的追责面临重重障碍。

一方面，尽管理论上被侵犯的未成年人及其法定代理人可以提起民事侵权之诉，但实践中却鲜见仅因为侵犯未成年人信息而提起的侵权之诉。原因在于侵权之诉的成立要件之一为发生损害后果，但多数侵权行为往往较为隐蔽，或尚未构成实质损害后果，例如对因非法扩大收集未成年人个人信息的行为，产生了向未成年人推送不合理内容的后果，单就该行为本身很难说明已构成实际损害的情形，仅能在个人信息涉及私密信息时，适用侵犯隐私权的救济途径，适用范围呈现窄化的弊端。更为常见的是因非法收集、恶意泄露未成年人个人信息并导致的下游损害行为，可以依此提起损害赔偿[5]。但在这些案件中，如何确立侵权行为人也成为实践中的难题，未成年人个人信息的收集、储存、使用过程中可能涉及多个主体，原告需要提出证据证明侵犯个人信息的具体主体，实践中各地法院对原告的上述举证责任采用了有差异化的标准[6]。上述提起民事诉讼的诸多实践障碍，显然不利于未成年人群体维护个人信息利益，也会令侵权救济路径被阻塞。

另一方面，虽然我国刑法设置了“侵犯公民个人信息罪”，但该罪名涉及的个人信息的认定以“可识别性”为标准，意味着上文论述中具有保护必要的未成年人非识别性的信息并未被纳入刑法保护的范畴。此外，我国刑法学界对于该罪名侵犯的法益的讨论，通常认为是个人信息自决权[7]，但从上文对立法价值的理论澄清来看，我国立法并未承认未成年人完全的信息自决权，造成法益保护的错位，未成年人个人信息的特殊保护难以在该罪名中得以体现，导致司法实践中该罪名的适用情况并不理想。

---

① 例如2021年12月，“小红书”APP被曝存在泄露未成年人隐私、留言审核不严的乱象。详见央视网：《晒生活还是隐私？小红书被曝推送未成年人身体隐私》，https://m.gmw.cn/baijia/2021-12/05/1302707274.html

② 例如，在最高人民检察院公布的第三十五批指导性案例——《浙江省杭州市余杭区人民检察院对北京某公司侵犯儿童个人信息权益提起民事公益诉讼、北京市人民检察院督促保护儿童个人信息权益行政公益诉讼案（检例第141号）》中显示了APP运行过程中擅自处理未成年人个人信息所带来的严重后果，但该案系检察机关办理刑事案件中发现了非法处理儿童个人信息的行为，继而启动公益诉讼，带有一定的被动性和偶发性。

三、未成年人个人信息保护的优化路径

基于以上论证，可以看到保护未成年人个人信息安全的立法目的在实践中易受到多方挑战。下文将在未成年人个人信息保护的多元价值平衡关系基础上，提出从立法规范到实践操作的递进式保障机制，以构建我国精细化、更具实践意义的未成年人个人信息保障机制。

（一）立法规范："最有利于未成年人"原则的具化

《未成年人网络保护条例（征求意见稿）》中明确了未成年人网络保护工作应当坚持最有利于未成年人的原则，但从未成年人个人信息面临的风险来看，"最有利于未成年人原则"难以体现在具体的程序设置上。为了保证该原则在实践中的落实，应着重从以下几个方面完善。

1. 明确未成年人个人信息的边界

诚如上文所述，未成年人个人信息概念中的"可识别性"特征被不断挑战，诸如未成年人的网页浏览信息、购物偏好、Cookie信息等非直观识别性信息未被纳入法律保障的视野。但从实践中的风险来看，上述信息依然有巨大的商业价值，甚至会在对上述非识别性个人信息二次处理后产生恶意利用未成年人个人信息的行为，可能引发严重侵害未成年人合法权益的后果。因而，基于立法完善的思路，不宜窄化个人信息的范围，应统一《个人信息保护法》与《网络安全法》中的定义，明确"与其他信息结合识别自然人个人身份的各种信息"为未成年人个人信息的范围；也不应仅以年龄作为区分未成年人与成年人个人信息的唯一标准，赋予司法裁判机关在个案审理时判断个人信息范围的自由裁量权，在个案的讨论时应考虑到使用、加工信息的环境及结果，即便有匿名化的处理，一旦可以经过简单信息整合后便还原识别性，实务部门都应将其认定为个人信息，以扩大未成年人个人信息保障对象的范围。以立法界定为基础，针对不同信息类型适用不同程度的保护力度，从而实现立法的精密化。

2. 强化网络产品和服务提供者的保护义务

尽管法律法规中要求了网络产品和服务提供者在收集、使用未成年人个人信息时应遵循的原则及程序，但基于考察发现大部分APP的《隐私政策》中并没有区分未成年人个人信息的特殊范围，即便有所涉及，表述也极为含糊；最核心的监护人"告知—同意"程序极易沦为形式，且通常一经同意就意味着默认后续处理未成年人个人信息的合理性，对未成年人个人信息的保护义务并未达到立法的要求。因而，应采用统一、明确的未成年人个人信息的范围界定方式，并在未成年人身份认证机制以及监护人授权条款方面，适用实质审查方式，严格落实个人信息保护影响评估报告，限制向第三方提供未成年人个人信息的行为，使未成年人个人信息安全保护之目的显著优于商业利用目的。对于网络产品和服务提供者利用算法自动化决策进行内容推送的行为，应设置明确的年龄界限，对于14周岁以下的未成年人，应严格禁止其通过自动化决策的个性内容推送；对于14周岁以上的未成年人，应取得监护人单独明确的授权，赋予未成年人及其监护人是否开启个性化推荐的自主选择权。

3. 实现未成年人信息自决权与保护目的的平衡关系

在现有的"一刀切"立法保护模式下，虽然强化了国家保护及家长监护职能，但却并未体现出对未成年人信息自决权的承认和尊重。上文考察中发现，大多数APP在《隐私政策》的制定中采用18周岁作为需要监护人授权的年龄界分点，且在监护人同意模式下，甚至会共享未成年人个人信息中较为隐私的部分，例如在腾讯发布的《儿童隐私保护声明》中，监护人可以查看包括用户名、密码、头像、昵称、性别、主动发布的内容等，显然忽略了未成年用户个人信息中的隐私属性。未来的立法路径应当部分承认未成年人信息自决权，构建更为精细化的干预手段，根

据未成年人群体各年龄段的特征，分别适用不同程度的监护力度，避免因过度强调保护而可能对未成年人带有隐私性质的信息造成负面影响。

（二）细化年龄分层，构建实质性保护机制

鉴于现有立法着重强调对14周岁未成年人个人信息的保护，导致实践中网络产品和服务提供者将14周岁以上的未成年人信息保护与不满14周岁未成年人群体“一视同仁”，可能带来过度让渡其信息自决权的后果；且与成年人信息保护采用统一保护标准，未体现对未成年人保护的特殊性。在个人信息领域，有必要建构不同年龄段的分层保护机制。

1. 不满14周岁未成年人适用实质性“告知—同意”规则

针对不满14周岁未成年人，宜沿用敏感信息的使用规则，并建立实质性的监护人“告知—同意”机制。在确认未成年人年龄的认证方式上，欧洲数据保护委员会（European Data Protection Board，简称EDPB）认为，可以引入可信赖的第三方验证集约化机制。在我国可借助公安部身份认证系统，或由国家互联网信息办公室建立未成年人信息识别平台，但第三方平台的引入仅为识别未成年人年龄，不作任何数据储存和分析。在“实质同意”的具体实现方式上，可参照美国《儿童在线隐私保护法》（Children's Online Privacy Protection Act，简称COPPA）及欧盟《通用数据保护条例》（General Data Protection Regulation，简称GDPR）中确立的“可证实的父母同意原则”（Verifiable Parental Consent），即通过电话、邮件、传真、信件、信用卡认证、数字识别等验证方式确保已得到父母的授权，在获得授权后还会再次验证身份，以确保授权行为确来自父母[8]。我国司法实践中，在网站或APP将其授权的未成年人个人信息的范围进行充分披露的前提下，可辅助人脸识别、声音验证等方式，完成监护人的授权行为，且在授权过程中，将未成年人个人信息中的敏感信息部分作着重强调。更重要的是，要充分告知监护人的同意撤销权，即在发现有超越授权范围收集未成年人个人信息的行为时，可以随时撤回授权，并要求删除相关个人信息。

2. 14至18周岁未成年人适用监护人共同授权行为

针对14至18周岁的未成年人，应在承认其享有部分信息自决权的基础上，监护人与未成年人共同完成个人信息的授权。对该群体而言，个人信息已经包含了其不愿被人知晓的隐私信息，若其个人信息授权行为一概由其监护人做出，也就意味着监护人依然对未成年人个人信息享有完全的控制权，难以体现对未成年人人格尊严的尊重及保护。在充分告知未成年人及其父母个人信息收集、使用范围的基础上，部分限制监护人授权未成年人个人信息的范围，特别是对于未成年人隐私信息（如账户、密码、私密发布内容）应由未成年人本人完成授权，以实现监护人信息控制权与未成年人信息自决权的动态平衡。同时，该年龄划分标准也并非绝对，可以参照《中华人民共和国民法典》的规定，对于已满16周岁、以自己劳动收入为主要来源的未成年人，视为享有完全的个人信息自决权的主体，可通过上传证明材料的方式，完成个人信息的自我授权。

（三）划分信息类型，实现多层次监管模式

为了避免“一刀切”式的未成年人信息保护模式所带来的风险，可以将未成年人个人信息进行纵向分类，并分别设置相应的程序规范及权利救济路径。

1. 隐私信息适用最严格监管规则

隐私信息，即涉及未成年人隐私权的核心、具有高度私密性的信息，具有显著的人格权利益。我国《个人信息保护法》中以泄露或非法使用后可能带来的危害后果作为界定敏感信息的标准，但涉及未成年人个人信息部分，由于未成年人通常没有收入来源，仅以严重后果反推其信息性质显得不妥，应回归到最核心的隐私权保护领域，将这类信息的保护同未成年人人格尊

严进行衔接，同时将不满14周岁未成年人的信息规定在隐私信息保护的范围，适用最严格的程序规范。具体而言，行政主管部门应设立长效监督机制，积极履行维护未成年人个人信息安全的职责，督促互联网行业尽快形成针对未成年人个人信息保护的行业自律条例，并充分利用大数据展开对网络产品和服务提供者的实时动态监管，积极接受来自社会公众的举报、投诉；在发现有违法收集、利用未成年人隐私信息的行为后，应立即启动监管机制，公布详细的调查处理报告，以实现常态化、精准化行政监督。对司法机关而言，应将“预防为先”的理念植入保障未成年人个人信息安全的领域，在尚未造成严重后果时积极介入，通过提起公益诉讼的方式实现司法监督，并向负有监管职责的行政机关发出检察建议。

2. 事实信息的事先授权与动态监管

事实信息，即信息的内容能够反映出未成年人的个体信息，如联络信息、数字足迹信息、社交信息等，这类信息并不必然具有私密性，具有人格利益和财产利益的二元属性。例如，未成年人在社交APP中的点赞、关注、访问记录等足迹信息，尽管该信息为未成年人在一定范围内主动公开的信息，但在进行处理和分析的过程中，可能做出一些不利于未成年人身心健康发展的自动化决策行为，需要进行明确授权以及后续动态授权，保障网络产品和服务提供者处理信息的行为符合特定目的，且严禁有偏差性地自动化决策。

对于事实信息而言，通常在第一次使用产品完成授权行为后，未成年人及其监护人对事实信息具体如何使用便失去了敏感性，需要由行政部门充分利用大数据技术完成对网络产品和网络服务提供者的行为是否超出授权范围的动态监督。特别是基于事实信息而进行的自动化决策行为，应当进行严格限定，审查其是否对不满14周岁的未成年人进行自动化决策，对已满14周岁的未成年人的自动化决策行为是否得到监护人明确授权，是否符合合法、正当、必要和诚信原则，以营造非偏差性的未成年人网络环境。

3. 衍生信息应纳入法律规范范围

从衍生信息的界定而言，这类信息并非未成年人主动提供，而是通过大数据手段对未成年人个人信息进行深度处理，预测其未来的行动特征、行为趋势等。相较于前两类未成年人主动提供的信息，这类信息属于网络产品和网络服务提供者基于个人信息所作出的预测，带有明显的财产性利益。目前这类信息尚未被纳入法律调整的范围，且从信息产生主体方面，已经摆脱了原信息提供主体，但笔者认为，对这类衍生信息的利用本质上依然是对原个人信息的处理，尽管立法暂未将该类信息纳入调整对象，但从其商业价值属性来说，信息中的预测内容可能直接影响未成年人的行为，且一经泄露或非法使用可能带来严重后果。

因而，应将该类信息纳入未成年人个人信息的法定分类，在明确授权的前提下，未成年人及其监护人应明确知晓该衍生信息的存在并享有完全的信息控制权。行政监督主体可以参照事实信息，强化网络产品和服务提供者的告知义务、制定进行个人信息保护影响评估义务以及合理使用义务，积极履行对此类衍生信息的动态监管职能。

（四）完善诉讼规则，畅通被侵犯主体救济路径

从上文分析被侵犯主体救济路径现状中不难发现，我国亟须构建更契合保障未成年人合法权益的权利救济程序。未成年人及其监护人在发现个人信息被网络产品或服务提供者擅自使用时，除了向行政机关及时举报外，还可以通过提起诉讼的方式维护未成年人合法权益，在被侵犯用户群体范围较大时，可以向侵权主体提起集体诉讼。对于司法裁判主体而言，不宜混淆隐私权与个人信息的概念，以避免窄化未成年人个人信息权益的保护范围。在侵权行为与损害后果的因果关系证明方面，需要考量被侵犯主体与网络产品和服务提供者在举证能力上的差异性，通过设置特殊举证责任和赔偿连带责任，以降低未成年人维权成本，消除其诉讼障

碍。对于已涉嫌构成刑法“侵犯公民个人信息罪”的行为，可以在未来司法解释中将侵犯主体为未成年人个人信息作为“情节严重”的重要判断标准，检察机关应在起诉环节履行未成年人及其法定代理人有权提起刑事附带民事诉讼的告知义务，并协助其收集证据证实“侵害结果”的发生，以实现对所遭受损失的积极追偿，在必要时可由检察机关代表被侵犯的不特定多数未成年人群体提起刑事附带民事公益诉讼，从司法层面构建更为通畅的救济路径，体现对未成年人个人信息的特殊司法保护。

结语：从实践运行来看，现有立法规定难以有效回应非法收集、利用未成年人个人信息的行为，使立法目的在实践中极易落空。产生上述问题的症结在于现有的制度尚未厘清未成年人个人信息保护的范围等基础性问题，缺乏未成年人权益保障与个人信息商业利用价值以及未成年人部分信息自决权之间的平衡机制。故未来优化路径应当在具化“最有利于未成年人”原则的基础上，设置差异化、精细化规则：一方面，以年龄为基准，设置不同强度等级的保护机制，使现有的信息授权行为更具实质意义和操作性；另一方面，细化未成年人个人信息种类，针对各类型的信息采用阶梯化的行政监督规则，同时完善相关诉讼规则，完善当下权利救济路径，以实现多元立法价值在未成年人个人信息保障领域中的平衡统一。

[参 考 文 献]

[1] 共青团中央维护青少年权益部 中国互联网络信息中心：《2021年全国未成年人互联网使用情况研究报告》，https://news.youth.cn/gn/202211/t20221130_14165457.htm

[2] 郝银钟 盛长富：《未成年人司法的国家亲权悖论与修正》，载《法律适用》，2012年第3期。

[3] 石佳友：《网络环境下的个人信息保护立法》，载《苏州大学学报（哲学社会科学版）》，2012年第6期。

[4] 最高人民检察院：《2021年全国检察机关未成年人保护公益诉讼立案6633件》，https://www.spp.gov.cn/spp/zdgz/202203/t20220307_547781.shtml

[5] 谢鸿飞：《个人信息泄露侵权责任构成中的“损害”——兼论风险社会中损害的观念化》，载《国家检察官学院学报》，2021年第5期。

[6] 程 啸：《侵害个人信息权益的侵权责任》，载《中国法律评论》，2021年第5期。

[7] 刘艳红：《民法编纂背景下侵犯公民个人信息罪的保护法益：信息自决权》，载《浙江工商大学学报》，2019年第6期。

[8] Nancy L . Savitt. A Synposis of the Children’s Online Privacy Protection Act, St. John’s Journal of Legal Commentary, 2002, (3).

（责任编辑：崔 伟）