Dispute Settlement 争议解决, 2025, 11(1), 257-266
Published Online January 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.111034

Hans汉斯

论大数据背景下未成年人信息保护的法律完善

祖凌云

青岛大学法学院，山东 青岛

收稿日期：2024年12月19日；录用日期：2025年1月18日；发布日期：2025年1月26日

摘　要

随着我国互联网技术的不断提高和经济的不断发展，我国早已进入到互联网大数据时代，未成年人也逐步成为主要参与者，然而大数据在带给未成年人便利的同时，也增加了未成年信息侵权案件发生的风险。就我国目前的未成年人信息保护而言，我国法律上主要存在着未成年人年龄划分机制不合理、监护人同意制度不完善、网络运营商规避规定、赔偿标准较低等问题。我国应该借鉴美国《儿童在线隐私保护法》、欧盟《通用数据保护条例》等有参考价值的制度，将我国未成年人划分为14周岁、14~16周岁、16~18周岁三个年龄阶段；立法上完善监护人同意制度在知情同意等规则上的不足；加大网络运营商的义务和责任；引入惩罚性赔偿机制，通过对未成年人信息保护的问题进行分析并提出相应对策，完善我国未成年人信息保护的路径。

关键词

未成年人，个人信息，法律保护

On the Legal Improvement of Minors' Information Protection under the Background of Big Data

Lingyun Zu

Law School, Qingdao University, Qingdao Shandong

Received: Dec. 19th, 2024; accepted: Jan. 18th, 2025; published: Jan. 26th, 2025

Abstract

With the continuous improvement of China's Internet technology and the continuous development of the economy, China has already entered the Internet big data era, and minors have gradually become the main participants. However, big data brings convenience to minors, but also increases the risk of minors' information infringement cases. As far as the information protection of minors in China is

文章引用: 祖凌云. 论大数据背景下未成年人信息保护的法律完善[J]. 争议解决, 2025, 11(1): 257-266.
DOI: 10.12677/ds.2025.111034

concerned, China's laws are mainly characterized by such problems as unreasonable system of age division of minors, imperfect system of guardian consent, evasion network of regulations by network operators, low compensation standards and other issues. China should learn from the United States "Children's Online Privacy Protection Act", the European Union "General Data Protection Regulations" and other valuable reference systems and divide minors in China into three age stages: 14, 14~16 and 16~18; legislate to improve the insufficiency of the guardian's consent system in terms of the rules of informed consent and other rules; increase the obligations and responsibilities of network operators; and introduce punitive compensation mechanism, through analyzing the problems of the protection of minors' information and proposing corresponding countermeasures to improve the path for the protection of minors' information in China.

Keywords

Minors, Personal Information, Legal Protection

1. 引言

随着信息时代的不断发展，人们越来越多地从面对面的现实交流向数字化传送转变，这使得人们在接受譬如微信支付、通信便捷等数字化生活方式带来方便的同时，也不得不面临着信息泄露等不同方式侵权的风险。而未成年人作为社会群体中的大部分，其本身辨识能力弱、潜在利益大、接触网络逐渐低龄化等特点，使得其更易在复杂的大数据时代受到伤害，因此在大数据时代急需解决未成年人信息保护的问题。而我国关于未成年人信息保护的法律存在诸多不足，本文将结合我国相关规定与国外具有借鉴意义的相关制度对未成年人个人信息保护制度进行完善。

2. 未成年人个人信息保护的概述

未成年人信息和成年人不同，因为未成年人易受伤害的特殊性，与其利益相关的所有信息都会成为侵权的对象，某些在成年人看来无足轻重的信息有可能发生未成年人信息侵权案件，所以未成年人所受到保护的信息的范围应该在成年人的基础上进行扩大，并有针对性地进行分类。

2.1. 未成年人个人信息的界定

我国《个人信息保护法》第 4 条[1]和第 28 条[2]、《民法典》第 1034 条[3]都对个人信息进行了界定。由这些规定可以看出，我国个人信息公认的特征是可识别性，但分类上存在不同。我国个人信息保护法将个人信息分为敏感个人信息和非敏感个人信息，而我国民法典将个人信息分为私密信息和非私密信息，两个划分之间存在较大的不同。在性质上，敏感信息侧重的是受到侵害的风险，即是否涉及个人尊严和

[1]《中华人民共和国个人信息保护法》第 4 条：个人信息是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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

[2]《中华人民共和国个人信息保护法》第 28 条：敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

[3]《中华人民共和国民法典》1034 条：个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

生命财产安全；而私密信息侧重的是非公知性，即对隐私权的保护。在保护方面，根据民法典，我国学理上有观点将对私密信息的保护模式称为“二进阶递进适用模式”，优先适用于隐私权的规定[1]；根据《个人信息保护法》，我国对敏感信息的保护适用的是其第 28 条到第 32 条的具体规定。

我国并没有关于敏感信息和私密信息的具体划分标准，而对该问题的相关讨论，有些学者提出的观点笔者比较认同：私密信息和敏感信息应属于交叉关系，即可以把个人信息划分为私密敏感信息、敏感非私密信息、私密非敏感信息和非私密非敏感信息四大类。并且应该根据具体情况具体划分，比如不同身份的同一种信息的归类不同，对于明星等特殊身份的人而言电话号码的泄露不会危害到生命财产安全，但会侵犯到隐私，属于私密非敏感信息，而对于已经公开在互联网上的同意被他人知晓的电话号码属于非私密非敏感信息，所以个人信息的分类要结合具体情况具体分析[2]。

我国个人信息的特征为可识别性，即可以确认该自然人的身份，未成年人个人信息作为个人信息的一种，其首先要满足的便是可识别性，即包括未成年人的姓名、出生日期、身份证件号码等一切可以识别未成年人身份的信息。

而未成年人作为一种特殊主体，其所牵涉的信息不应该仅局限在可识别的信息，还应该包括其在日常生活中与其利益紧密相关的全部信息。在学校，未成年人以各种形式留存的活动记录、关于个人成长信息的成绩单或者所上交的带有个人主观色彩的周记作文等，对于其他成年主体而言并不是应该保护的范围，但基于未成年主体的特殊性，都应纳入到未成年人个人信息保护范围内。在家庭生活中，未成年人所写的日记、所收到的信件等也属于未成年人个人信息。也就是说，应对未成年人的个人信息作广义理解，不仅包括可识别未成年人身份的个人信息，也包括与其利益相关信息。且按照个人信息的分类也将未成年人个人信息在不同情况下分为四大类：私密敏感信息，如未成年人的行踪轨迹、IP 地址等信息，一旦泄露既侵犯了未成年人的隐私权，又会对其生命财产安全造成危害；敏感非私密信息，如未成年人已经自愿或者监护人公开的未成年人的活动记录等信息，虽然属于敏感信息，但已经不具有非公知性；私密非敏感信息，如未成年人在学校或者 APP 上所填写的个人或者监护人的电话号码或邮箱等信息，其泄露不会危害到个人尊严和生命财产安全，但会侵犯到未成年人或其家人的隐私；非私密非敏感信息，如未成年人已经记录并且容易检索到的姓名、年龄等信息，具有公知性并且不会危害到个人尊严和生命财产安全。对于某种信息具体属于哪一类，应结合具体情况具体分析。对于未成年人的私密敏感信息，应对其进行最高强度的保护，适用民法典和个人信息保护法中根据实际情况更有利于保护私密敏感信息的规则。

2.2. 大数据背景下未成年人个人信息保护的必要性

首先，目前未成年人个人信息侵权问题越来越多。据《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，未成年人互联网普及率持续提升，2021 年我国未成年人互联网普及率达 96.8%，较 2020 年提升 1.9 个百分点。未成年网民表示“自己曾在过去半年内遭遇过网络安全事件”的比例为 25.5%，其中遭遇网上诈骗、个人信息泄露的比例略有升高，个人信息未经允许在网上被公开的比例为 6.1%。由此数据可以看出，未成年人遭受网络问题越来越多，大数据背景下的未成年人的信息保护迫在眉睫。

其次，未成年人是无民事行为能力人或者限制行为能力人，他们不能独立完成绝大多数的民事法律行为，需要由其监护人代为行使部分或全部，且我国关于个人信息保护的规定是以成年人为中心建立的，往往会忽视未成年人特殊的需求，比如在侵权行为发生后未成年人更难证明侵权行为的发生以及侵权行为和危害结果之间的因果关系等。

再次，互联网作为包括未成年人在内的绝大部分人活动的场所，其包含的大数据良莠不齐，带给用

户方便的同时，也不可避免地会对用户造成侵害，而未成年人作为正在发展中的不成熟的个体，其本身心智尚未健全、辨识能力弱、潜在利益大、接触网络逐渐低龄化等特点，使得其极易受到网络环境的干扰，更易在复杂的大数据时代受到伤害，在大数据背景下其安全更应受到足够重视。

并且，大数据使信息泄露更容易且迅速。大数据背景下信息侵犯者仅仅只需要一小部分未成年人的信息就可以挖出与其相关的大部分信息，以短视频软件抖音为例，许多分享自己孩子日常的父母在不经意间透露的关于孩子的情况，有可能成为不法分子挖掘未成年人位置、动态的导火索。再加之大数据传播速度之快，第三方在短时间内就可以获得未成年人的信息并进行大范围传播。

最后，未成年人信息泄露在大数据时代的后果极其严重。首先，对还处在发展阶段的未成年人来说，没有成人更为冷静的思考和更为强大的承受能力，信息泄露伴随而来的很可能是伤害性极大的网络暴力，这将给未成年人带来极大的心理压力，很有可能给未成年人带来不可磨灭的创伤，甚至威胁其生命。其次，对未成年人的家庭而言，未成年人的信息被非法买卖，会发生欺诈等侵犯家庭利益的情况，不利于家庭乃至整个社会的稳定发展。

3. 我国法律对未成年人个人信息保护存在的不足

我国关于信息保护的法律制度是以理性的成年人为中心，针对未成年人信息保护的制度方面存在很多不完善的部分。同时，部分网络运营商也利用法律制度的不足去追求自己利益的最大化，逃避法律责任。不足具体存在以下几点：

3.1. 未成年人个人信息保护年龄划分机制不完善

我国关于未成年人个人信息保护年龄的划分在不同的法律规范中都会找到相关规定：《儿童个人信息网络保护规定》中主要保护的是儿童是未满十四周岁的未成年人；《个人信息保护法》中规定对于未满 14 岁的未成年人信息，信息处理者可以在征得同意的情况下，对其进行处理，并应当制订具体的处理规则。《信息安全技术个人信息安全规范》中规定收集年满 14 周岁未成年人的个人信息前，应当取得未成年人本人或其监护人的明确同意；不满 14 周岁的，须经其监护人的明确同意。而我国《民法典》中对个人信息保护没有专门规定年龄，适用总则中关于未成年人即不满十八周岁的规定。

由此可见 14 周岁成为目前零散的法律规范中逐步明确起来的一条年龄线，对 14 周岁以下的未成年人给予更多的保护，而对 14 周岁到 18 周岁的未成年人没有给予明确的法律保护。荷兰学者米尔达·马赛纳特指出在大数据时代儿童信息保护面临着两大困境：赋权与保护；个性化与平均年龄[3]。即未成年人在不同的年龄阶段对权利的渴望程度不同，如果忽视掉不同年龄段未成年人的差异，将无法针对不同年龄段的未成年给予针对性的法律保护，尤其是 14 周岁以上的未成年人在个人信息遭受侵害时无法得到充分的救济。所以目前的我国一刀切的年龄划分机制是不完善的，且这样一刀切的划分方式引起了学界较多讨论：有学者按照英国信息专员办公室(ICO)的适龄设计理念[4]，将未成年人信息保护的年龄划分为 0~6、6~8、8~14、14~18 四个阶段[4]；有学者按照信息自决权将年龄划分为 0~14、14~16、16~18 三个阶段[5]；有学者将年龄划分为 14 周岁以下、14~16 周岁、16~18 周岁，并结合制度设计和具体的应用场景进行个性化区分[6]。

3.2. 监护人同意制度存在不足

我国关于未成年人个人信息保护的监护人同意制度主要包括《儿童个人信息网络保护规定》第 9 条、《个人信息保护法》第 31 条、《民法典》第 1035 条、《信息安全技术个人信息安全规范》5.4.d。从上述法律规范可以看出，我国未成年人监护人同意制度存在的基础是我国的监护关系，也就是监护人对未

[4]《适龄守则》将未成年人分为五个阶段 0~5 岁、6~9 岁、10~12 岁、13~15 岁、16~17 岁。

成年人所负有的监护职责和抚养义务，主要法律依据体现在《宪法》第 49 条、《民法典》第 35 条和《未成年人保护法》第 7 条。我国监护人同意制度目前存在以下几个方面的不足。

首先，知情同意规则的困境。我国法律规范中仅仅规定了告知并同意规则，但是对同意的方式没有作详细的规定，这使得网络运营商可以此为漏洞为自己提供便利，大部分运营商取得同意的方式为提供冗长的用户协议和隐私政策文件，并且仅提供同意和退出两个选择，如果不选择同意就只能退出，大部分监护人会疲于阅读过长的文件而点击同意。即使监护人想要认真阅读，但因为是非专业人士，对于文件中所提到的专业术语和繁杂的步骤无法理解，对一些隐藏在文件中的不利条款也无法查明，长久以来监护人同意制度会成为虚设。

其次，监护人的非理性决策。监护人同意制度存在的依据，是监护人对未成年人利益的保护，是未成年人的利益与监护人的利益之间的一致性。也就是说，监护人同意制度中的监护人是一个总是能作出最有利于未成年人利益的完美监护人，但是这在实践中是不存在的。未成年人是一个不断发展的个体，其在不断发展的过程中对自身权利的渴望是呈递增的，其与监护人同意制度之间总是存在冲突的。对于未成年人而言监护人主要是指父母，少数指除父母外的机构或其它因收养关系等而形成监护的自然人。所以监护人同意制度主要存在两个方面的冲突：一是父母出于爱子心切的保护目的，对大数据产生误会甚至是抵触心理，片面地阻断未成年人与大数据的接触，直接侵犯未成年人的自我决定权；二是除父母之外的其他监护人对未成年人利益的侵犯。若父母尚有可能对未成年人的利益造成不经意的侵害，除父母之外的其它监护人更有可能出于过失甚至故意的心态以未成年人的信息为对象对未成年人的权益造成侵害。

3.3. 网络运营商规避规定

3.3.1. 规避未成年人用户身份

我国相关法律规定保护未成年人的个人信息，尤其是不满十四周岁的未成年人的个人信息，相关网络运营商应该就未成年人的身份认定制定详细的行业规范，并在识别到不是未成年时及时采取排斥未成年人进入，对所获取的未成年人的信息进行删除等补救措施。但我国存在网络运营商规避未成年人身份，故意获取未成年人信息的情况，主要在未成年人的身份验证上。未成年人身份验证的方式法律文件没有详细的规定，所以行业规则规避该方面对未成年人的保护，规定得过于粗糙。目前大部分 APP 验证未成年人身份的方式为输入姓名和身份证件号码，未成年人完全有可能凭借虚假的身份进入互联网世界，而某些 APP 中可能涉及低俗内容或者以容易误触的方式诱使未成年人进入到泄露定位等个人信息的页面。例如凤凰新闻 APP，曾因“持续传播色情低俗信息”等违规行为被国家网信办要求整改，其介绍显示，APP 中会有偶尔/轻微的成人/性暗示题材，偶尔/轻微的色情内容或裸露。另外，作业帮和小猿搜题的 APP 也被爆出存在色情内容。因而，对未成年人的认证过于简化，加大了未成年人的个人信息被泄露的危险。

3.3.2. 在用户协议或隐私政策中设置陷阱

许多 APP 或者其他大数据的使用前都会需要阅读用户协议和隐私政策文件，但冗长的文件和晦涩的文字恰恰会阻碍用户知情权的行使。网络运营商看似尽到了告知的义务，出现纠纷的时候可以将责任推给用户没有仔细阅读。《经济参考报》记者的一项调查发现，一些应用程序在必要时还会修改自己的隐私协议，如果内容被更新，用户并不能第一时间知道。这种应用程序一般都会在用户协议中表示，公司可以随意制定和修改用户协议或者其它规则，而无需通知用户，这导致了“一次同意，次次同意”的现象。更令人不可思议的是，一些 APP 在协议中还表示，他们拥有永久的、完全免费的用户视频、照片、文字等的使用权，而且“有权授权给任何第三方使用”“实际行使时不需要事先征得同意”，并且很多时候，“转

授权”条款没有具体规定，比如如何授权，授权给哪些人，授权的范围如何，都没有一个清晰的界定。可以想象，在这种情况下，会有多么大的风险。

3.4. 受害方不轻易起诉且赔偿标准较低

在未成年人信息受到侵害时，一方面，对未成年人本身而言，作为受害主体的未成年人维权意识较弱，所以在没有发生较严重的后果之前较少比例的未成年人会运用法律手段去维护自己的权益。而在大数据背景下，网络侵权本身就存在隐蔽性，未成年人也很难意识到自己的信息泄露，所以受害方在尚不知自己权益受到侵害时无法起诉，在自己信息泄露尚未造成严重后果时不会起诉。另一方面，对于已经起诉的案件而言，在大数据世界的数据本身是非实物的，其大容量、多样性和快速度等特点使得其涉及的对象复杂、涉及的程序繁杂，对案件的取证极其困难。这也就是为什么受害方不轻易起诉且胜诉率低的原因。

对于已经起诉且胜诉的案件而言，我国在未成年人个人信息保护案件中存在赔偿标准较低的问题。2021 年 3 月 11 日，由浙江省杭州市余杭区人民检察院[5]受理的一起短视频公司侵害儿童隐私民事公益诉讼案，成功结案，此案被称为“未成年人网络保护民事公益诉讼第一案”，但是在此案中，最后的结果是达成调解协议，侵权者仅需要停止侵权行为，完成整改并接受检查，赔礼道歉。2022 年 3 月 18 日，河北省辛集市检察院判决的一起侵犯未成年人个人信息权益案件中涉及的有效信息为 4808 条，每条信息成本几毛钱，而收益远远大于成本，但侵权者仅判处短期拘役和罚金的处罚。由上述两个案件可见，在涉及未成年人信息的案件中，责任承担方式多是停止侵害，赔礼道歉等，赔偿数额较少甚至没有赔偿，即使存在赔偿也仅仅以获益为标准，这对侵权人的惩戒力度不大，难以对其造成震慑，对未成年人的个人信息保护是十分不利的。更何况对未成年人个人信息的侵害主要是利用其潜在价值来获取非法利润，如果惩罚力度不大，不仅未成年人受到的损害没得到弥补，侵权人也会因为获益大于惩罚而再次实施违法行为。

4. 国外相关制度的规定及对我国的启示

国外关于未成年人信息保护的研究早于我国，目前在域外立法中最具有权威性的两部立法是美国《儿童在线隐私保护法案》(简称 COPPA)和欧盟《通用数据保护条例》(简称 GDPR)，其中美国 COPPA 采用可验证的父母同意制度，是对未成年人信息保护的一大贡献，同时也规定了受到保护的未成年人的年龄为 13 周岁并在此基础上进行了改进；欧盟 GDPR 以坚持儿童友好原则为指导，对网络运营商提出了更高要求，其最主要的贡献是引入了被遗忘权，允许数据主体在任何时候删除或者更正有关自己的数据。除此之外 GDPR 作为目前对个人信息规定最详细的法律，其标准要高于 COPPA。下文将对此进行论述。

4.1. 美国未成年人个人信息保护制度

4.1.1. 可验证的父母同意制度方式明确

可验证的父母同意制度是美国 COPPA 最具有贡献性的制度之一，其提出了六种核实家长同意的具体方法：1) 以传真、邮件、电子扫描等形式，将家长所签家长同意书交给操作者；2) 使用信用卡、借记卡或其它网上付款方式，并将此告知家长；3) 家长通过电话表示认可；4) 与员工等职业人士进行视频电话；5) 由政府签发的身份证明文件证实；6) 用面孔辨识技术等来确认等。除了六种验证方式之外，COPPA 还规定了不受六种验证方式限制的情况，比如为了保护服务的完整性而获得的个人信息可以不用父母的同意等。相比于我国的父母同意制度，美国 COPPA 更具体且更具有实施性。虽然美国 COPPA 中规定的较多较详细的验证方式会对网络运营商产生较重的负担，甚至会降低其经济收益，但因为未成年个人信息泄露对未成年人潜在的侵害太大，所以在未成年人利益和网络运营商利益之间进行平衡，应该倾向于

[5]最高人民检察院第三十五批指导性案例，检例第 141 号。

未成年人保护[7]。

4.1.2. 未成年人个人信息保护年龄分段

在 2000 年的时候，美国 COPPA 将 13 周岁作为年龄划分的标准，仅仅保护 13 周岁以下的未成年人，是我国一刀切的划分标准的借鉴。在 2018 年美国国会对美国 COPPA 进行修订，将未成年人信息保护的年龄扩大到了 12~16 岁，在修订审查稿中保护对象的年龄曾被建议提高到 18 岁以下。关于未成年人信息保护年龄的划分总是存在争议：2010 年，美国在对 COPPA 进行修订时，电子隐私信息中心曾经建议国会将年龄要求提高到 18 岁；学界 Lauren A. Matecki 认为，COPPA 中把 13 岁作为受到保护的年龄过低，应该将 17 岁以下的未成年人的信息都纳入保护范围等[8]；于 2020 年生效的美国 2018 年《加利福尼亚州消费者隐私法》针对未成年人的隐私保护采取的是 13 周岁及以下、13~16 周岁、16 周岁及以上三个年龄段。总的来说，美国未成年人信息保护对年龄的划分已经从一刀切的模式向年龄分段迈进，这对我国相关制度的完善有一定的借鉴。

4.2. 欧盟未成年人个人信息保护制度

欧盟 GDPR 是目前规定的最严格的个人信息保护制度，其中对未成年人的个人信息保护中有很多有借鉴意义的专门规定。

4.2.1. 用户协议针对未成年人和监护人明确易懂

GDPR 第 12 条尤其强调，以儿童为对象的资料搜集，应以简洁、透明、易于理解、易于取得的方式，向使用者提供资料，并以清楚、通俗易懂的文字说明。在实践中，网络平台和运营商被要求提供与未成年人理解能力相匹配的用户协议和隐私政策等。在监护人同意制度下，我国未成年人对用户协议的理解并没有得到足够重视，但作为未成年人信息保护的主体，未成年人对用户协议享有和监护人相同的知情同意权，应针对其能力对其保留相关权利。

4.2.2. 最严格的父母同意制度

GDPR 第 8 条提出“父母同意”原则，要求互联网服务提供者在收集、使用和处理 16 岁以下未成年人的互联网信息时，必须征得其家长的同意或授权。这一条款规定对涉及儿童的所有个人信息的收集和处理，必须征得父母的同意，这一最严格的规定引起了很大质疑，这大大限制了网络平台的发展和未成年人的权利，也给家长带来了过重的负担，所以对于我国的借鉴在于避免规定过于严格的父母同意制度。

4.2.3. 遗忘权的规定

欧盟最早对被遗忘权作出规定，许多国家受其影响接连对被遗忘权作出规定。GDPR 第 17 条中明确地包括了与未成年人个人信息有关的情形。在获取未成年人个人信息时，在没有取得其父母同意的情况下，可以要求数据控制者将未成年人的信息删除。也就是说，信息数据主体可以主张删除个人公布的信息，或者要求搜索引擎平台不推送与其有关的信息。由此，对儿童的被遗忘权制度进行了确定。此外，GDPR 还对被遗忘权的例外情形作出了规定，以便在行使言论自由和信息自由权利、存档公共利益等情形下，可以绕过被遗忘权。在我国《儿童个人信息网络保护规定》第 19 条和第 20 条中对被遗忘权已经作了规定，明确赋予了儿童及其监护人更正和删除网络运营者所收集、存储、使用、披露的儿童个人信息的权利。

4.3. 国外制度对我国的启示

4.3.1. 完善相关规定的标准

我国作为社会主义法治国家，应该逐步确定起未成年人信息保护相关法律体系，并结合国外相关制度的发展进行完善：细化未成年信息保护的年龄区间；完善监护人同意制度中的验证方式并重视未成年

人的同意，同时避免监护人同意制度太过严格的极端。

4.3.2. 明确网络运营商的责任和义务

网络运营商在获得利益的同时，应有相匹配的责任和义务，我国并没有作出明确的规定，欧盟 GDPR 在这方面的规定值得我国借鉴。

5. 大数据背景下未成年人信息保护的法律完善措施

为了适应大数据时代的发展和加大对未成年人的保护，美国和欧洲都在逐步调整未成年人信息保护的法律制度，虽然还存在很多争议，但采取的措施都在使得法律更有效地实施[9]。我国在未成年人信息保护的法律方面同样存在不足，急需认识到未成年人信息保护对未成年人成长的重要作用并对法律制度进行有针对性的完善，具体可包括以下几点：

5.1. 完善未成年人年龄划分标准

我国未成年人信息保护的年龄划分标准是一刀切的划分方式，即以 14 周岁为划分标准，这使得 14 到 18 周岁的未成年人的个人信息的保护存在空缺，虽然 14 到 18 周岁的未成年人有一定的辨识能力和思考能力，但是因为他们正处在从未成年人到成年人的过渡阶段，对新鲜事物存在猎奇心理，还是很容易在大数据世界迷失自己，泄露自己的信息，所以 14 到 18 周岁会成为未成年人信息侵权事件频发的重要年龄段。所以应该把未满 18 周岁的未成年人都划为未成年人信息保护的对象，在此基础上再进行细分。应采用三个年龄段，把被广泛认可的心智不成熟的 14 周岁为第一个年龄节点；把我国民法典中能以自己的劳动收入为主要生活来源的心智相对较为成熟的 16 周岁为第二个时间结点；把成年人标志的心智成熟的 18 周岁为第三个时间节点。

首先，针对未满 14 周岁的未成年人，其心智发展不成熟，缺少对是非的认知，应按照我国《个人信息保护法》的规定，将其所有信息划为私密敏感个人信息，对其实行最严格的监护人同意制度，最大程度的限制该年龄阶段未成年人自主决定权的行使，即把把个人信息的处理包括获取、使用等全权授权由监护人管理。

其次，针对已满 14 周岁未满 16 周岁的未成年人，其有一定认知能力和辨识能力，对个人信息能进行一定的保护，但是对一些与个人利益相关的较为私密的信息的自我保护力度不够，所以对其实行较为严格的监护人同意制度，即监护人管理和未成年人自决相结合：在一些与未成年人利益关系较少的个人信息处理时给予未成年人自决权，如在学习软件、生活娱乐软件等在获取昵称、头像等非私密非敏感信息授权时可以由未成年人自己决定；而在涉及未成年人定位地址、肖像照片等涉及私密或敏感的信息时应将权利交给监护人决定。

最后，针对已满 16 周岁未满 18 周岁的未成年人，其心智已接近于成年人，应给予其最大限度的自决权，在涉及非私密非敏感信息、私密非敏感信息和敏感非私密信息的时候由未成年人明示即可获得，但涉及如微信账号授权、银行卡账号密码等私密敏感信息时应得到监护人同意。

5.2. 完善监护人同意制度

首先，可以借鉴美国 COPPA 对监护人可验证的同意制度，针对个性化的场景规定详细且针对性的验证方式。明确列举监护人同意的方式，且具体情况具体分析，对于未成年人信息泄露风险较小的情况下可以向父母短信发送同意书等方式征得同意，而对于未成年人个人信息泄露风险较大的情况下可以通过电话或者视频验证等方式征得同意。比如网络运营商为了更好地提供服务所需要获取的未成年人的姓名、年龄等必要信息时可以通过发送短信等方式进行验证，而在涉及未成年人个人信息泄露风险较大的 IP 地

址或者转让给第三方等情况下应采用视频验证等更为严格的方式验证。

其次，为了避免监护人因为专业知识的欠缺而使得知情权成为虚设，需要设置简单易理解的用户协议和隐私政策。网络运营商应附有一般人理解能力范围内的相关文件，对晦涩的专业术语需要进行必要的解释，并附有联系方式，在监护人无法理解相关内容时可以打电话或者发信息进行咨询，确保监护人在充分理解相关文件内容时作出有利于未成年人个人信息的决定。

最后，为了避免监护人的非理性决策对未成年人自主决定权的侵犯，在识别未成年人身份后，针对于有一定自主决定权的未成年人单独设置符合其年龄的未成年人同意选项，即对有一定自主决定权的未成年人设置未成年人本人和监护人的双层同意制，在监护人保护未成年人的同时，充分尊重未成年人自决权，尽可能地避免监护人非理性决策的不良影响[10]。

5.3. 加大网络运营商的责任和义务

网络运营商的主要义务是用户协议和隐私政策的制定，未成年人个人信息保护政策的遵守以及在个人信息有泄露风险时进行适时的补救等。在域外立法中以明确责任的方式来弥补企业内相关规定的不足的方式值得我国借鉴[2]。我国应在未成年人个人信息保护的专门法律中强调加强未成年人个人信息保护的同时，对网络运营商相关的责任和义务进行较为详细的规定。对其义务进行细化：首先对相关用户协议和隐私政策进行明确的规定，规则简单易懂，授权具体明确；其次对未成年人的身份进行审核，在发现所收集的未成年人的信息不符合规定时，及时自觉或者根据监护人的指定进行通知、更正、删除等补救措施；在未成年人或其监护人行使遗忘权的时候提供便捷的通道，还应该完善证据保存功能，在发现侵犯未成年人信息的行为时，应及时删除相关信息，保存相关证据并及时向有关部门报告，使得未成年人损害最小化的同时，有助于案件的调查。

在规定网络运营商义务的同时，应该规定相对比成年人个人信息侵权更重的责任。未成年人信息保护相对于成年人的不同之处决定了未成年人信息侵权应有更重的责任，使得侵权人对未成年人信息侵权的后果产生畏惧，以便更好地维护特殊主体的权益。我国网络运营商的责任主要规定在《网络安全法》第六章法律责任中，除此之外，在《未成年人保护法》127 条中也有关于具体数额的责任规定，其数额基本在一百万以下。相比而言美国和欧盟的惩罚力度可以说是天价，FTC 在美国保护儿童隐私的案件中开出最大一笔民事罚款为 570 万美元，而美国参议员称这比对于儿童所造成的伤害而言还远远不够[11]。由此可见我国的未成年人个人信息侵权案件的罚款并不算严格，应在此基础上进行适当加重，才能弥补未成年人所受到的伤害并对侵权者起到震慑作用。

5.4. 引入惩罚性赔偿和公益诉讼制度

我国的损害赔偿可以分为补偿性的赔偿和惩罚性的赔偿，前者侧重于对所受损害的补偿，没有其他作用，以损害为限度；后者侧重于惩罚，目的是为了震慑和惩戒侵权者，其不以损害为限度，并且其数额往往高于损害数额。大多成年人有阅读能力，对于用户协议和隐私政策等有一定的认知，即使其权益受到侵害，大部分成年人也有维护自己合法权益的能力。相比与成年人的冷静和知识面，未成年人社会经验少，心智发展不成熟，侵权者会更倾向于收集未成年人的信息，成本低却获利大，但会给未成年人造成无法估量甚至无法弥补的伤害。所以基于此特殊性，应该在未成年人个人信息保护的相关法律中规定惩罚性的赔偿，参照环境侵权和食品安全侵权的惩罚性赔偿，规定在达到一定程度侵害时受害人或者其监护人可以请求惩罚性赔偿，在弥补未成年人伤害的同时，给侵权者造成一定的震慑[12]。

未成年人个人信息侵权案件近几年发生概率越来越高，并且涉及的利益面广泛，影响较大，符合公共利益的特征，所以将其纳入到公益诉讼中是符合发展的，其也逐渐成为了一种新兴的公益诉讼，其中

比较有代表性的案件是浙江省杭州市余杭区人民检察院诉某知名短视频平台未成年人个人信息保护公益诉讼案，由此可见实践探索是越来越普遍的。但是在实践中，此类公益诉讼存在着取证困难、提出诉讼的适格主体少等不足。所以我们要在法律中规定检察机关和相关监察机关之间的联合，规定具体的取证规则，争取形成完整的证据链；关于未成年人公益诉讼主体的顺位，鉴于检察官在取证方面职权上的优势，可将其置于诉讼权主体的首位。

6. 结论

在互联网大数据时代，未成年人作为主要的参与者，在网络产品和服务中逐渐成为主体，所以在享受其带给未成年人成长、学习和生活便利的同时，还要注意对未成年人个人信息的保护。在此基础上，本文对大数据背景下未成年人个人信息保护方面的现状和问题进行分析，并提出完善未成年人年龄的划分标准、完善监护人同意制度、加大网络运营商的责任和义务、引入惩罚性赔偿和公益诉讼的建议，以增强对未成年人的信息保护力度，为未成年人打造安全的网络空间。

参考文献

[1] 石佳友. 隐私权与个人信息关系的再思考[J]. 上海政法学院学报(法治论丛), 2021, 36(5): 81-98.

[2] 朱晓峰, 黎泓玥. 私密信息与敏感个人信息区分保护论[J]. 经贸法律评论, 2023(1): 21-38.

[3] Macenaite, M. (2017) From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, **19**, 765-779. https://doi.org/10.1177/1461444816686327

[4] 孙跃元. 未成年人个人信息保护中监护人同意规则的检视与完善[J]. 华南师范大学学报(社会科学版), 2023(1): 149-164+208.

[5] 邱饰雪. 民事公益诉讼的新发展——兼论未成年人个人信息保护[J]. 南都学坛, 2023, 43(1): 60-67.

[6] 张继红, 尹菡. 数字时代未成年人个人信息的法律保护[J]. 青少年犯罪问题, 2021(2): 97-106.

[7] Milkaite, I. and Lievens, E. (2019) Children's Rights to Privacy and Data Protection around the World: Challenges in the Digital Realm. *European Journal of Law and Technology*, **10**, 1-24.

[8] Matecki, L.A. (2010) Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era. *Northwestern Journal of Law &Social Policy*, **5**, 369-402.

[9] Bartoli, E. (2009) Children's Data Protection vs Marketing Companies. *International Review of Law, Computers & Technology*, **23**, 35-45. https://doi.org/10.1080/13600860902742612

[10] 徐培颖. 未成年人个人信息保护中监护人同意之完善[J]. 太原城市职业技术学院学报, 2022(5): 180-182.

[11] 单勇. 未成年人数据权利保护与被害预防研究——以美国《儿童在线隐私保护法》为例[J]. 河南社会科学, 2019, 27(11): 49-57.

[12] 蔡一博, 吴涛. 未成年人个人信息保护的困境与制度应对——以"替代决定"的监护人同意机制完善为视角[J]. 中国青年社会科学, 2021, 40(2): 126-133.