doi:10.13582/j.cnki.1672-7835.2024.01.015

未成年人网络保护与“数字检察”的衔接问题及对策

雷小政,闫姝月
(北京师范大学 刑事法律科学研究院暨未成年人检察研究中心,北京 100875)

摘　要:在贯彻《未成年人网络保护条例》时,适度、合理使用个人信息是规范算法推送、提升网络素养、防治网络沉迷等的基础性命题。当前,未成年人个人信息在网络上遭遇泄露或者被不当使用的问题较为严峻,成为整个未成年人网络保护体系的“短板”。鉴于许多互联网平台具有市场主体和监管角色的双重身份、未成年人网络合规制度体系尚不健全等因素,为促进网络保护与司法保护衔接,有必要以“数字检察”为支撑点增强保护力度,提升制度刚性。建议依据互联网平台等级建立“数据备案审查”或“检察进驻监管”机制,健全未成年人数据互联互通机制;在完善刑事追诉、公益诉讼的同时,细化强制性亲职教育。

关键词:未成年人网络保护;个人信息;数字检察;互联网平台
中图分类号:D915.3　　**文献标志码**:A　　**文章编号**:1672-7835(2024)01-0117-11

进入数字时代,党中央、国务院高度重视未成年人网络保护的相关工作。2023 年 10 月 24 日,国务院公布的《未成年人网络保护条例》(以下简称《条例》)为未成年人在数字空间中的发展权益与网络安全提供了更为坚实的法律依据和全局性的顶层设计。作为我国第一部专门性的未成年人网络保护综合立法,此次公布的《条例》共 7 章 60 条,涵盖了未成年人网络素养促进、网络信息内容规范、个人信息网络保护、网络沉迷防治等重点内容。这一立法的重要背景是,我国未成年人触网情况呈现低龄化、普遍化的趋势,但是,未成年人个人信息在网络上遭遇泄露或者被不当使用的问题日益严峻,严重制约着整个未成年人网络保护体系的功能实现。2022 年 11 月 30 日,共青团中央维护青少年权益部、中国互联网络信息中心和中国青少年新媒体协会联合发布的《2021 年全国未成年人互联网使用情况研究报告》(以下简称《2021 年报告》)显示,我国未成年(6—18 周岁)网民规模已达 1.91 亿人。其中,有 25.5%的未成年网民“在半年内遭遇过网络安全事件”;遭遇“网上诈骗”与“个人信息泄露”的人员比例均有所上升①。与此同时,许多涉及收集、存储、使用未成年人信息的互联网平台也被推上“风口浪尖”。未成年人个人信息的泄露或被不当使用的问题之所以层出不穷、屡禁不止,背后有着深刻的社会治理问题、家庭教育问题、网络法治问题等因素。作为立法层面的回应,《条例》在《个人信息保护法》《未成年人保护法》等基础上,专章规定了未成年人个人信息网络保护的具体规则,明确了网络服务提供者、个人信息处理者、监护人等的主体责任。这些立法举措能否有效解决上述现实问题呢?

毫不夸张地说,一旦松懈对未成年人个人信息的保护,甚至缺失,整个未成年人网络保护体系将沦为“一纸空文”。2021 年《中共中央关于加强新时代检察机关法律监督工作的意见》为检察机

收稿日期:2023-11-20
基金项目:国家社会科学基金一般项目(19BFX077)
作者简介:雷小政(1980—),男,湖南郴州人,博士,研究员,博士生导师,主要从事诉讼法学、少年司法研究。

①各地相继涌现多起泄露、不当使用未成年人个人信息且情节极其恶劣的刑事案件。例如,在 2020 年“肖某、邓某出售未成年人信息民事公益诉讼案”中,肖某、邓某通过自建“五六七发卡”互联网平台,广泛收集未成年人个人信息并非法出售,数量高达 95 万余条。参见杭州互联网法院(2021)浙 0192 民初 9214 号。

关加强对未成年人权益保护,尤其是个人信息网络保护等重点领域的法律监督提供了重要指引①。最高人民检察院在2021年《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》中进一步强调了对未成年人个人信息实施特殊保护原则。除了依法追究泄露、不当使用未成年人个人信息犯罪外,针对一些监管部门、互联网平台等疏于保护问题,要求各级检察机关积极发挥法律监督职能,通过检察建议、公益诉讼等方式加强个案监督和诉源治理②。也就是说,针对各互联网平台中以数字化为存在形态的未成年人个人信息,从被动走向主动,从办案走向治理,以"数字检察"为驱动,以"数据共享"为特色的强制保护机制,逐渐成为新时代检察机关法律监督工作的新趋势、新潮流③。需要密切注意的是,在检察机关"唤醒各类数据",打通"数据壁垒",助力未成年人个人信息网络保护的同时,如何尊重各类互联网平台,尤其是《条例》规定的"未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者"(以下简称重要互联网平台)的经营自主权,保障其商业秘密不受任意侵犯,如何在监督的过程中保障未成年人个人信息的安全性,避免出现再次泄露、不当使用的风险,都应做出积极回应。积极回应这些争论,找到数字赋能与数字安全之间的平衡点,对全面、准确、依法贯彻《条例》和提升整个未成年人网络保护质效、水平而言,具有极其重要的理论与现实意义。

一　数字时代未成年人个人信息立法的理论基础

根据主体性理论,个人信息属于个人自主的范畴。一般而言,个人对其信息的处理享有知情权、决定权。根据联合国1948年发布的《世界人权宣言》第12条,个人信息保护主要体现为"对个人私生活、家庭、住宅和通信的尊重"和"个人事务的自决(自由)原则"。探讨未成年人个人信息在立法层面的特殊性时,存在两个普遍认可的前置性命题:一是在电子化技术广泛应用以前,除隐私之外的个人信息一般被置于公共领域自由流通。随着数字时代的到来,个人信息泄露、被不当使用的恶性案件频发,日益凸显个人信息保护的必要性。二是在成人化语境和相关司法体制中,受"儿童私有财产论"的影响,作为父母的隶属品,较少提及未成年人对其个人信息的处理权,更遑论个人自主或自决。随着少年司法体系的发展,尤其是"国家亲权说"等理论的普及,未成年人对其个人信息的独立权利开始受到重视④。

(一)数字时代未成年人个人信息的特殊性

在当前各国立法体系中,对成年人个人信息、未成年人个人信息的本质界定,尤其是立法定义,基本上是同一的,并且主要围绕"大隐私权"范畴抑或"独立的新型权利"展开。例如,在美国,个人信息权长期以来被认为属于"大隐私权"范畴。自20世纪70年代以来,美国法院通过司法判例建立了"信息性隐私权",形成与"自治性隐私权""物理性隐私权"并列的三分法局面⑤。与之形成鲜明对比的是,在欧盟的一些公约和瑞典、德国、法国等国家的个人信息保护法中,普遍将"个人信息受保护权"确定为独立于隐私权的一项新型权利,强调建构专门的个人信息保护法体系。

在数字时代,为何要对未成年人个人信息实施特殊保护,以及为何各国普遍通过专门立法对其中的权利义务关系进行规制?一个关键性的历史背景是,第二次世界大战后,随着科学技术的发展,大多数西方国家为了方便对社会的管控和治理,纷纷依托公共机构建立有关公民个人信息的巨型数据库,并用于登记人口基本信息。从商业应用和利益等角度,新兴的互联网科技公司陆续大规模收集并处理其用户的个人信息,且使用的动机和能力远远超过传统公共机构。在互联网平台中,未成年人个人信息与成年人一样,主要表现为以数字化存在形态的个人数据。每个人都已成为由个人信息和个人数据这些"数字细胞"组合

①2023年10月27日,最高人民检察院负责人在"国务院政策例行吹风会"上介绍,近3年来,检察机关立案涉未成年人网络权益和个人信息公益诉讼案件就达到了524件。

②贾宇:《论数字检察》,《中国法学》2023年第1期。

③2023年2月2日,针对场所违规接纳未成年人、校车安全、信息网络安全、事实无人抚养儿童、强制报告、校园安全等重点领域,最高人民检察院发布了一系列大数据赋能未成年人检察监督典型案例,强调通过数据碰撞主动发现批量监督、类案监督线索。

④王贞会,蔡沐铃:《美国治理网络性侵害未成年人犯罪的联邦立法及对我国的启示》,《中国青年社会科学》2022年第5期。

⑤Whalen v. Roe, 429 U.S. 589(1977).

而成的“数字人”①。一般认为，未成年人信息一旦泄露或被不当使用，容易造成比成年人更为严峻的不良后果和影响。归纳学术界的理论研究观点，大致有三种学说：（1）身心健康说。在少年司法领域，不少学者主张，未成年人面对不法侵害的道德防御能力天然处于弱势状态②，与成年人有所不同的是，未成年人身心发育尚未成熟、心理防线较为脆弱、压力承受能力有限，即使是面对因个人信息引发的相同侵害行为，容易给其身心健康造成更为严重、深远的侵害。（2）家庭损失说。由于父母或其他监护人授权使用手机、网络等因素，未成年人的个人信息往往与其父母或其他监护人的各种信息有所关联。当未成年人的信息被泄露或不当使用时，很有可能给整个家庭带来财产、人身安全等风险。一些不法分子往往利用未成年人的信息对其父母或其他监护人进行诈骗、勒索等。（3）次生伤害说。因不法分子在线上索取、推送、买卖未成年人信息，导致“隔空猥亵”、线下强制猥亵、强奸等性侵未成年人案件频发，对社会公共道德建设带来极其不利的冲击和影响③。

（二）“倾斜式”立法中的特殊保护逻辑

基于“保护个人信息权益”和“促进个人信息合理利用”立法目的之间的平衡，学术界对个人信息保护的立法模式，长期以来存在着“分类保护模式”与“单独立法模式”等理论分歧。在“分类保护模式”中，一般根据泄露或不当使用的危害程度和后果，将个人信息区分为非敏感信息（一般信息）和敏感信息进行保护④。在“单独立法模式”中，多数主张需要对高敏感的个人信息通过单行立法的方式予以保护⑤。随着数字时代的到来，加上未成年人个人信息的特殊性，将其视为需要特殊对待的信息种类或者界定为高敏感信息进行“倾斜式”立法日渐成为一普遍趋势。许多国家和地区在未成年人信息自主权的年龄限制、监护人同意制度、互联网平台监管等方面纷纷出台了一系列专门法案或改革措施⑥。其中，2016 年欧洲联盟《一般数据保护条例》被称为“史上最严个人数据保护法”。其第 8 条明确规定了互联网平台的一项核心义务：“处理 16 岁以下的儿童的个人数据，必须获得该儿童父母或监护人的同意或授权。各成员国可对上述年龄进行调整，但是不得低于 13 岁。”

在我国，从《民法典》到《个人信息保护法》《未成年人保护法》《条例》等法律法规的立法脉络来看，对未成年人个人信息进行“倾斜式”立法，并进行特殊保护是十分清晰和明确的。在《民法典》和《个人信息保护法》的基础上，《未成年人保护法》第 4 条明确规定：“处理涉及未成年人事项，应当保护未成年人隐私权和个人信息。”在对未成年人信息进行特殊保护时，上述法律法规融合了前述“分类保护模式”和“单独立法模式”的制度设想，并在未成年人个人信息网络保护上呈现以下两个显著特点：一是以 14 周岁为年龄划线再次区别保护的等级。与《刑法》第 237 条中强制猥亵罪中被害人年龄划线一致，《个人信息保护法》第 28 条采取“最低年龄划线”的方式，将不满 14 周岁未成年人的个人信息界定为“敏感个人信息”，并在第 31 条将监护人同意作为个人信息处理者处理信息的一般原则，以实现特殊保护。二是以最有利于未成年人原则进行统筹，并确立实施性原则和相关义务体系。即使对 14 周岁以上的未成年人个人信息，也并非放任不管，而是要求贯彻和坚持最有利于未成年人的原则予以严格保护。《未成年人保护法》第 72 条对此规定了信息处理者应当遵循合法、正当和必要的原则。除了上述“倾斜式”立法外，各地监管部门、互联网平台根据年龄区间积极探索了许多对未成年人信息的各类保护路径，如“监护人同意”条款、“青少年模式”版块等⑦。

二　检察机关进行专门法律监督的归因分析

值得思考的是，上述立法规定是否与现行网络管理机制、企业合规治理水平、监护保护能力和认

①雷小政：《大数据为未检工作注入新动能》，《法治日报》2023 年 2 月 9 日。

②玛格丽特·K·罗森海姆，富兰克林·E·齐姆林，戴维·S·坦嫩豪斯，等：《少年司法的一个世纪》，高维俭译，商务印书馆出版 2008 年版，第 16 页。

③朱光星：《网络隔空猥亵儿童的定罪研究——以保护儿童为分析视角》，《中国政法大学学报》2022 年第 4 期。

④张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期。

⑤周汉华：《中华人民共和国个人信息保护法（专家建议稿）及立法研究报告》，法律出版社 2006 年版，第 79 页。

⑥Daniel J. Solove. “Privacy Self—management and the Consent Dilemma”, *Harvard Law Review*, 2013(7):1889-1893.

⑦李冉，周进萍：《“青少年模式”：算法变革、功能聚焦与价值失衡》，《传媒观察》2022 年第 11 期。

知水平等契合？上述改革措施是否能落地、生效？根据溯源分析，各地涌现的未成年人信息泄露、不当使用等案例暴露出，许多来自外部环境因素、制度运行因素、履职缺位因素等的掣肘依旧深刻存在。这也是近些年来各地检察机关介入其中进行专门法律监督的动力基础所在。对贯彻《条例》而言，理顺这些深层次的根源并进行归因分析十分必要。概括起来，未成年人个人信息泄露、被不当使用的主要原因可以从以下三个方面加以剖析。

(一)网信部门等有关机关和部门的履职缺位问题突出

根据未成年人的“政府保护”和“网络保护”体系，我国对未成年人个人信息确立了由国家网信部门牵头的“统筹共管”工作机制。具体而言，在未成年人个人信息保护工作中，网信部门负责统筹协调个人信息保护工作和相关监督管理工作，其他有关部门在“职责范围”内落实相应的监管职责。目前，受以下因素的制约，这一工作机制与上述目标仍有不少差距。

1.监管环节未能有效覆盖信息处理全流程

在未成年人个人信息网络保护工作中，网信部门如何发挥统筹协调和指导监督等的功能？从立法授权的角度，主要是依据正当必要、知情同意、目的明确、安全保障、依法利用等原则对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等环节进行全面监管。对未成年人个人信息网络保护而言，理想化的监管情境是，从“收集到删除”进行全流程“穿透式监管”。根据国家计算机病毒应急处理中心针对 2017—2020 年移动应用程序涉及个人信息安全风险的情况统计①，监管部门对涉及个人信息安全风险的执法力度越来越大，也更加严格。但除了少数个案中有对“删除”和“投诉处理”环节的追究和处罚外，网信部门的监管重心基本上偏向“收集”，甚至主要聚焦在这一环节。缺乏对全流程的严管严控，并呈现“头痛医头”的特征，仍然是目前网络管理中亟待解决的一个机制性问题(参见表 1)。

表 1　移动应用程序涉个人信息安全风险情况监测统计(2017—2020 年)

时 间	监管内容	监管环节	涉及个人信息安全风险的应用程序数量/总数(单位:个)
2017 年	存在危险行为代码，窃取用户隐私信息	收集环节	4/12
2018 年	存在危险行为代码，窃取用户隐私信息 私自下载移动应用，窃取用户隐私信息	收集环节	13/42
2019 年	在用户不知情或未授权的情况下，获取用户个人信息，具有隐私窃取属性	收集环节	10/48
2020 年	未向用户明示申请的全部隐私权限	收集环节	21/21
	未说明收集使用个人信息规则	收集环节	
	未提供有效的更正、删除个人信息及注销用户账号功能	删除环节	
	未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内受理并处理	投诉处理环节	

数据来源：国家互联网信息办公室官方网站。2021 年后，相关数据未公开。涉及未成年人个人信息安全风险的典型移动应用程序有“益智推箱子”(版本 V2.3)、“钉子别碰我”(版本 V3.0.0)、“贪玩蓝月”(版本 V 1.0.7.59)、“慧投足球”(版本 V1.0.13)、“生存战争盒子”(版本 V 1.5.0)、“农场模拟器 2018”(版本 V1.8.0)、“星座消消乐”(版本 1.0.0.9)、“秘密花园”(版本 1.1)、“吉祥坊棋牌”(版本 1.17.4)等。

2.统筹、协调、督促和指导的功能发挥不足

目前，对未成年人个人信息负有保护义务的责任主体繁多。在这一领域，明确一牵头的责任主体，发挥实质性的统筹、协调、督促和指导功能就变得异常重要。根据《国务院未成年人保护工作领导小组关于加强未成年人保护工作的意见》的规定，各地未成年人保护工作领导小组要进一步推动未成年人保护工作中的部门协同。遗憾的是，2019 年《儿童个人信息网络保护规定》与 2021 年《个人信息保护法》中对“统筹、协调、督促和指导”的工作机制未做具体化的规定。当前，虽然《条例》第 3 条规定，国家网信部门负责统筹

①自 2014 年起，国家计算机病毒应急处理中心被确定为网信部门的技术支撑单位。其职责之一是定期监测“移动互联网应用程序”的运行是否符合《网络安全法》《个人信息保护法》等相关规定。

协调未成年人网络保护工作，并依据职责做好未成年人网络保护工作，但是处于信息保护“监管前哨”和被赋予特殊“统筹协调”职能的网信部门在行使相关职能上缺乏应有的权力配置和刚性手段，很难直接督促和指导其他机关、部门参与其中。在许多新兴业态中，由于缺乏实质性的统筹和协调，导致在未成年人信息保护上出现“监管空白”的情况。例如，在实践中，一些电竞酒店的未成年人登记住宿率达到 10%—30%，甚至成为未成年人聚众上网、抽烟、喝酒、“吸食笑气”的重要聚集场所，并且因个人信息泄露等诱发了一些网络安全事故和恶性犯罪案件①。问题在于，不少电竞酒店经营者故意规避 2002 年《互联网上网服务营业场所管理条例》中关于未成年人上网的禁止性规定，在网络上向不特定的未成年人推送大量“软广告”，并提供“诱导其沉迷的网络产品和服务”。对网信部门而言，要统筹和协调公安机关、文化旅游部门、市场监督管理部门对这一领域实行协同监管，及时预警和风险管控，除了需要对未成年人身份信息、住宿信息、上网信息等实现数据共享外，还要赋予其对有关机关、部门履职不力的刚性监督管理手段。但是，巧妇难为无米之炊，网信部门无法跨越现有的职权范围，直接代行未成年人保护工作领导小组的职责。

（二）个人信息处理者未能依法、充分履行网络保护义务

对未成年人个人信息而言，互联网平台不仅是重要的个人信息处理者，也是加强未成年人网络保护的重要市场主体。国家市场监督管理总局在 2021 年发布的《互联网平台分类分级指南（征求意见稿）》（以下简称《分类分级指南》）中依据用户规模、业务种类以及限制能力将互联网平台分类为超级平台、大型平台、中小平台。虽然《条例》第 20 条特别提及“未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者”，但未进一步依照上述脉络进行分类规制。当前，《个人信息保护法》第 5 章从市场主体和监管角色双重身份出发，对个人信息处理各环节的保护义务和对平台内经营者的监管义务等做出了不同层次的规定，区分一般性义务与附加性义务，构建了一套“层级性、复合型”的保护义务体系。其中，相对普通互联网平台而言，第 52、58 条专门规定了“提供重要互联网平台服务、用户数量巨大、业务类型复杂”的个人信息处理者，即重要互联网平台的两类保护义务：对平台自身保护个人信息情况的合规义务（以下简称为“附加性义务 I”）以及对平台内产品或者服务提供者的监督管理义务（以下简称为“附加性义务Ⅱ”）（参见图 1）。

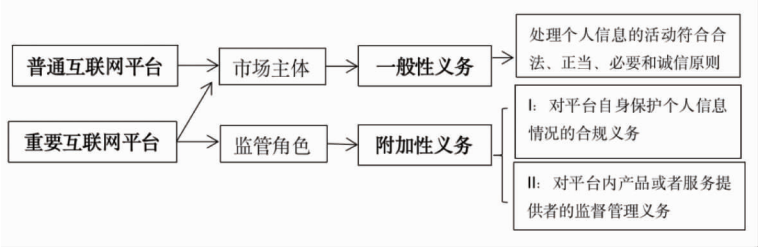

图 1　不同类型平台对应承担的“层级性、复合型”保护义务体系

目前，一些互联网平台未能依法、充分履行上述义务体系，导致未成年人个人信息在网络活动中泄露和被不当使用情形不但没有缓解，反而呈现加剧趋势，突出表现在以下两个方面。

其一，违反一般性义务实施强制性索权等行为。在未成年人个人信息网络保护工作中，对互联网平台而言，首要的一般性义务就是确保其处理个人信息的活动符合合法、正当、必要和诚信原则，并采取措施防止个人信息泄露、篡改、丢失等安全风险的发生。但是，与上述一般性义务背离的是，一些互联网平台凭借规模、数据、技术等优势在用户个人信息方面享有垄断性的支配地位，近乎演化成“数据霸权”，直接规定“不授权就用不了”的强制性索权条款，为其收集个人信息大开“方便之门”。还有一些互联网平台通过模糊化、抽象化的同意条款等“打擦边球”的方式变相索取个人信息使用权。例如，深圳市腾讯计算机系统有限公司发布的“儿童隐私保护声明”（2022 年 9 月 29 日版）规定：“如果监护人不同意相关隐私政策和本声明的内容或不同意提供服务所必要的信息，将可能导致我们的产品和服务无法正常运行，或者无法达到我们拟达到的服务效果。”

①何若愚：《查一查“电竞酒店”》，《检察日报》2022 年 3 月 23 日。

在实践中,多数监护人会基于对互联网平台的信赖而同意这些隐性索权条款。

其二,履行附加性义务时权限边界模糊。根据《个人信息保护法》对重要互联网平台附加性义务的设定,重要互联网平台对平台内产品或者服务提供者具有较为完整的规则制定权、执行权以及准司法救济权①。在履行这一附加性义务时,存在两个突出问题:一是监督管理主体的模糊。《分类分级指南》中的"超级平台""大型平台"是否对应《个人信息保护法》第 52、58 条中重要互联网平台,目前并无明确的法律规定。目前,《条例》也未能厘清其中的冲突和矛盾②。二是相关权限边界的模糊。对重要互联网平台而言,如何在个人信息上监督管理平台内产品或者服务提供者的行为及方式,相关规定较为原则,缺乏对权限范围、正当程序、救济手段等的明确规制③。这可能导致,一些重要互联网平台的监管权限得以盲目扩张,使得平台内一些"普通经营者"对重要互联网平台的策略和行动亦步亦趋,人云亦云。还有一些重要互联网平台侧重商业利益,在监管平台内经营者时流于形式,导致其在未成年人信息收集和使用上处于失控、失管的状态。

(三)未成年人信息保护中的监护缺失、监护不当

因未成年人在认知能力、行为能力上的不足,需要父母或者其他监护人正确履行监护职责,在"第一道关口"保护未成年人个人信息免受侵犯。在一些未成年人个人信息权益受到侵害的实际案例中,主要存在以下两类典型的监护缺失、监护不当情形。

其一,"放纵同意"行为。由于外出务工等现实因素,一些监护人迫于无奈或主动妥协,"放纵"未成年人替代行使"监护人同意"权限。实践中,为便于联络或远程监管,许多监护人将自己实名注册的手机或其他移动设备直接交由留守未成年人使用,使得"手机哄娃""靠网带娃"成为一种监护常态;有的监护人盲目信从"数字包容""数字平等",主动协助未成年人完成人脸识别等监护人验证程序。这导致许多未成年人实际使用监护人账号上网,不仅沉迷于不适宜未成年人使用的一些软件,而且盲目参与直播打赏等网络活动,甚至任意以监护人身份发布自己日常生活的"点点滴滴",加剧了监护人和未成年人信息被泄露或不当使用的风险性。

其二,"网络晒娃"行为。当前,出于信息分享、生活记录等多种目的,许多监护人在微博、微信、抖音、快手、小红书等社交媒体平台"晒娃",未考虑到在网络上发布未成年人照片或视频等可能存在隐私信息安全风险。如有意识地遮蔽关键部位、隐藏与未成年人身份相关的基本信息和可能被商业化运营的数字信息④。这给不法分子通过数据整合分析、描绘"画像"、锁定未成年人身份等实施违法犯罪行为提供了可乘之机。《条例》第 33 条针对未成年人的监护人,不仅赋予了其请求行使查阅、复制、更正、补充、删除未成年人个人信息的权利,而且明确了监护人应当教育引导未成年人增强个人信息保护意识和能力。但需要担忧的是,即使意识到保护个人信息的重要性,许多监护人并不具备对未成年人个人信息的风险防范意识和实际保护能力,也很难从未成年人纷繁复杂的上网活动中甄别、预判潜在的风险来源,更无法对未成年人进行具体的、有实际价值的信息安全引导。

从现行法律法规来看,检察机关对未成年人个人信息网络保护的法律监督,应当是其法定的、应然的职责之一。一方面,面对未成年人个人信息网络保护领域出现的新问题、新要求、新特点,检察机关履行法律监督职责符合我国《宪法》定位和党中央决策部署。在我国,自 1982 年《宪法》颁布以来,检察机关作为"国家法律监督机关"的性质定位始终如一。更为关键的是,2021 年《中共中央关于加强新时代检察机关法律监督工作的意见》不仅对其强化未成年人个人信息保护提出明确要求,而且指明了具体的符合数字化改革的路径。另一方面,我国关于未成年人保护还陆续出台了一系列专门性法律法规,赋予检察

①孔祥稳:《网络平台信息内容规制结构的公法反思》,《环球法律评论》2020 年第 2 期。

②值得期待的是,国家市场监督管理总局、国家标准化管理委员会正在拟制《信息安全技术大型互联网企业个人信息保护监督机构要求》等规范性文件。参见张新宝:《大型互联网平台企业个人信息保护独立监督机构研究》,《东方法学》2022 年第 4 期。

③杨垠红:《大数据使用情境下个人信息的侵权救济》,《福建师范大学学报(哲学社会科学版)》2022 年第 1 期。

④传统的个人基本信息主要包括姓名、性别、民族、政治面貌、出生年月、身份证号码、住址、电话号码等。在对这些基本信息进行收集的基础上,各互联网平台更为关注具有商业价值的以下数字信息,如用户个人的平台账号及密码、消费信息、医疗信息、遗传信息、位置信息、行踪信息、网站访问及浏览信息等。参见刘练军:《个人信息与个人数据辨析》,《求索》2022 年第 5 期。

机关“全流程、全覆盖”的监督职责和较为充分的监督手段，为介入网络保护提供了较大的制度空间。例如，《个人信息保护法》第 70 条设定了专门的公益诉讼条款，明确将个人信息保护纳入检察公益诉讼的法定领域。该条甚至将检察机关放在提起公益诉讼的首位主体，位于“法律规定的消费者组织和由国家网信部门确定的组织”之前，突破了《民事诉讼法》第 58 条将检察机关置于第二顺位主体的规定。这也成为检察机关就一些对个人信息疏于保护的监管部门、互联网平台可以依法提起行政、民事公益诉讼的直接法律依据。此外，最高人民检察院在 2021 年《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》中进一步明确了检察机关对儿童等特殊群体的个人信息进行特殊保护的原则，以及通过检察一体化应对个人信息公益损害网络化①。然而，检察机关对未成年人个人信息网络保护进行专门法律监督能否克服其他主体的现有问题，能否实现预设的法律功能呢？

三　“数字检察”赋能网络保护的运行效果与问题

在贯彻《条例》时，检察机关能否有效应对和解决监管部门、个人信息处理者、网络直播发布者、监护人等不依法履职等问题呢？目前，在各地未成年人保护工作领导小组的统筹协调下，许多检察机关与网信部门、互联网平台等积极对接，通过数据共享、信息互通、打造数字化治理平台等加强对重点环节、关键流程的监督管理，积极对侵犯未成年人个人信息的行为开展法律监督和诉源治理②。本文认为，对其运行效果应当脱离“部门本位主义”的局限，从多个层面进行客观评估。

（一）“数字检察”展现的显著性制度优势

当前，“数字检察”的核心要义在于，统筹数字化技术、数字化思维、数字化认知，培育数字能力和方法，构建检察数字治理机制体系，通过检察大数据中的能动化运用，解决社会治理中的法治“瓶颈”问题，确保公平正义“看得见”且“不迟到”③。以检察机关的“四大检察”职能（刑事检察、民事检察、行政检察、公益诉讼检察）为出发点，“数字检察”被认为可以最大程度地预防未成年人个人信息及个人数据免受篡改、盗用、滥用等侵害，并且提供更为全面、刚性的司法救济手段④。数字赋能法律监督，可以发挥以下两个方面的制度优势。

1.实现监管部门的集约化：从“数据孤岛”到协同监督

相对传统的政府保护、社会保护而言，数字赋能法律监督加强未成年人个人信息网络保护的最大优势是将数据作为新型的生产要素，实现重要互联网平台信息、行政执法信息、司法案件信息等的共享与互通，统合了监督平台，优化了监督流程，实现了多部门间的协同。通过跨部门、跨地区、跨层级之间在未成年人个人信息网络保护上的“互通有无”，可以打破原有各自为政的执法司法局面，打通其中的“数据孤岛”。在贯彻《条例》等法律法规的过程中，检察机关作为国家法律监督机关，相比网信部门而言，更有优势整合民事保护、行政保护、司法保护等多方资源，特别是督促和指导有关机关、部门形成集约化的组织力量，全面嵌入协同监督体系中⑤。例如，浙江省东阳市人民检察院牵头拟定，并与横店影视文化产业集聚区管委会、教育局、公安局、民政局、文广旅体局、市场监督管理局、妇联等八个部门会签实施了《未成年演艺人员权益保障办法》，通过嵌入“885”网络平台，实现了未成年演艺人员身份信息、陪同人员身份、监护人同意状况、住宿地点、参与剧组等的信息备案和数据共享，全面提升了对未成年演艺人员网络

①相关地方规范性文件及代表性实施方案，参见 2022 年陕西省西安市灞桥区人民检察院《检察大数据赋能法律监督实施方案》、2022 年重庆市人民检察院《检察大数据赋能法律监督行动方案》等。

②相关“数字检察”平台，参见浙江省金华市人民检察院“帮帮我 885”未成年人保护联动平台、浙江省杭州市人民检察院与阿里巴巴集团支付宝安全中心共建的“未成年人保护小程序”、贵州省六盘水市六枝特区检察院“‘遇检未来’智慧未成年人法律监督平台”、浙江省诸暨市人民检察院“星海守望未成年人违法犯罪预防治理平台”、浙江省金华市婺城区人民检察院“未成年人校外安全综合治理平台”、吉林省人民检察院“智慧未检云未成年人综合保护平台”、福建省福州市长乐区“未成年人综合保护智慧数字平台”、江西省九江市濂溪区“濂检小未未检云平台”等。

③张晓东：《数字检察赋能监督促进治理》，《检察日报》2022 年 7 月 21 日。

④2022 年 6 月，全国检察机关数字检察工作会议对以“数字革命”驱动新时代检察工作高质量发展作出了重要部署，要求进一步对具有法律意义的数据信息优化算法模型，以“数字检察”为核心路径完善法律监督的数字化过程。

⑤高志宏：《未成年人公益诉讼受案范围：实践扩张、理论逻辑与制度选择》，《政法论坛》2023 年第 5 期。

保护及司法保护的能力和水平①。

2.以大数据推动溯源治理:从事后救济到"数据站岗"

从最高人民检察院发布的未成年人个人信息被泄露、不当使用的指导性案例来看,多数案例的情形其实由来已久,许多此前被寄予厚望的保护性制度形同虚设或者处于严重滞后的状态②。这些个案有一些共同特点,即通过数字赋能法律监督,整合原本离散、碎片的"留痕"数据和信息,识别研判出社会治理中可能存在的风险因素,通过碰撞、比对聚合的数据以预先锁定风险线索,进行更加精准化的预防和干预。其本质在于,让数据为社会治理"站岗",及早化解风险,避免危害性后果或将其控制在最小范围内。以浙江省诸暨市电竞酒店这一新兴业态数字监督模式为例。目前电竞酒店是网信部门、文旅部门执法中的一个"监管盲区"。诸暨市人民检察院通过碰撞、比对在互联网平台、行政部门中的商业资质、运行信息等,以检察建议、行政公益诉讼听证等方式督促有关机关、部门对电竞酒店的广告推送、住宿登记、上网服务、信息安全等进行严格的监督管理。随后,诸暨市的有关机关、部门为全市11家电竞酒店共480台电脑安装上网登记管理软件。一旦未成年人使用其个人身份住宿、上网将自动触发风险预警系统③。

(二)需要进一步解决的问题

由于检察职能的拓展和对社会治理的融入,"数字检察"为未成年人个人信息保护注入了新动力,同时在客观上也存在一些担忧和争议。在贯彻《条例》时,要使检察机关的法律监督发挥"叠加效应",避免负面效应,需要在个人数据质量、互联网平台经营自主权、个人数据安全等方面进一步解决下列问题。

1.数据共享中"最后一公里"的限制

数字赋能法律监督的一个理想目标是,实现有关机关、部门之间的数据共享。在实际操作上,这就需要打通"最后一公里"的现实瓶颈。由于发展不平衡,许多现有执法司法平台上的未成年人相关信息实际呈现的是一些简单化、静态化的数字,属于定量标尺上的"孤点"④。受制于主管机关的差异和数据标准、证明方法等的不同,许多机关、部门之间储存信息的口径、条件差异明显。因此,期待通过大数据"一键生成""一键通关""一键聚拢"各个重要的、关键的数据要素是不现实的。以数字赋能法律监督为契机,有关机关、部门需要基于各自所处的职责范围、执法阶段、数据特性等进行磋商、协调,合作建立健全分级合理、差序有别、重心互补的数据收集和运用机制。

2.对互联网平台经营自主权的担忧

除了执法司法平台外,互联网平台是储存和处置未成年人个人信息最为关键的"数字工厂"。根据《儿童个人信息网络保护规定》第22条规定,网络运营者应当对网信部门和其他有关部门依法开展的监督检查予以配合。在数字赋能法律监督中,如何界定这一"配合"的内涵和外延呢?基于未成年人个人信息的特殊性,如将"配合"义务仅仅限缩在一些显性的合规行为审查上,是无法实现"穿透式监管"目标的。根据词义的最大射程进行文义解释,各互联网平台可以将其掌握的涉未成年人的全部信息,包括相关的核心技术与商业秘密在内,都应与检察机关、网信部门等共享,供其进行"全流程、全覆盖"监管。但问题是,未成年人个人信息处理流程涉及互联网平台的多个运营环节,对每一"角落"均展开"全面监督"是不现实的。历史上,苏联检察机关依据"一般监督权"深度参与企业内部治理,干预企业经营事项,曾引发较多抗议⑤。当前,对互联网平台经营自主性与未成年人信息特殊保护之间进行平衡,优化我国检察机关的法律监督手段和限度⑥,可以说是决定数字赋能法律监督能够"越走越远"的关键因素。

3.未成年人个人信息可能"二次泄露"

大醇尚有小疵。发挥数字赋能法律监督的功能和效果,必然涉及庞大的,甚至海量的数据收集和数据共享,其面临的风险因素也随之增加。在这一过程中,检察机关和有关机关、部门可以集约化地检索未成年人本身或其参与各种网络活动的基本信息和数字信息。在检察机关和有关机关、

①王迪,闫姝月,倪春霄:《"小演员"权益,检察院来护》,《民生周刊》2022年第16期。

②汤维建:《未成年人公益诉讼彰显检察担当》,《检察日报》2022年3月22日。

③陈东升,何若愚:《以检察之智绘就社会治理好"枫"景》,《法治日报》2022年12月17日。

④罗琳:《信息技术的负效应及其消解对策研究》,《科学技术哲学研究》2020年第4期。

⑤雷小政:《往返流盼:检察机关一般监督权的考证与展望》,《法律科学(西北政法大学学报)》2012年第2期。

⑥王海军:《中国语境下的"检察权"概念考察》,《中国法学》2022年第6期。

部门进行数据抓取和数字监管的同时，可能由于保密措施不当、操作疏忽、“黑客”攻击、滥用职权等因素造成这些信息的“二次泄露”。由于数据共享后的数据数量激增，相比零碎化、个案化的泄露而言，这时的“泄露”可能造成的次生危害会更为严重。毫不夸张地说，避免未成年人个人信息出现“二次泄露”是悬在数字赋能法律监督改革之上的一道“紧箍咒”。

四　构建以“数字检察”为支撑点的立体式保护体系

在社会治理体系改革中，针对其中的“病灶”，既要抓末端、治已病，更要抓前端、治未病。由于国务院行政法规在立法对象上的限制，此次《条例》并未对检察机关介入未成年人个人信息保护的具体程序和法律责任做出全面规定。在贯彻《条例》时，需要以最有利于未成年人原则为指引，全面做好法律法规、司法解释之间的有序衔接、漏洞补充等工作，特别是与“数字检察”工作积极对接，实现从预防到干预，再到诉源治理的立体式保护体系。

（一）监督各互联网平台的强制保护体系建设

涉及未成年人的各互联网平台，应当从收集到使用信息的每个流程均强化对未成年人个人信息的保护义务。为弥补行政履能、行业监管的一些漏洞，可以从以下两方面强化数字赋能法律监督，促进互联网平台在未成年人网络保护中积极履行主体责任。

1.基于年龄区间、应用场景进一步优化未成年人信息强制保护

目前，在国际上，通过统一设定未成年人年龄界限的方式来实现特殊保护的做法受到许多质疑①。考虑到我国的实际情况，基于年龄区间、应用场景进一步健全未成年人信息强制保护机制应当成为各互联网平台合规建设的一个重要版块。除了将 14 周岁作为敏感个人信息的划分界限外，可采用“0—8 周岁”“8—14 周岁”“14—16 周岁”“16—18 周岁”的年龄四分法增设有针对性的保护措施。如对 14 周岁以下的个人信息处理进一步细化适用“监护人”的有效同意标准：针对收集和后续的披露、推广等使用，应当经过“两次同意”，并不得采用象征性、概括性的同意行为；同意的表达方式应当是明示同意，而非默示同意，且不得采用推定同意。对“0—8 周岁”的未成年人个人信息进行披露、推广，需要评估可能引起的负面效应并做好预防性保护措施。对已满 14 周岁的未成年人，公开其肖像、形体及其他基本信息的，需要征求本人的明确意见。对“16—18 周岁”的未成年人，应当依据《民法典》赋予其更为广泛的可独立开展救济的手段和渠道。凡是收集和运用不满 18 周岁未成年人信息的，均应将处理信息的状况详细记录，并供监护人随时查询；同时赋予本人享有“永久删除互联网平台上个人信息”的权利②。

针对具有高风险性应用场景的互联网平台，《条例》高度关注未成年人的身份识别问题，特别是通过第 31 条规定了针对网络直播服务提供者的真实身份信息动态核验机制。在贯彻实施这一规定时，有必要进一步“根治”父母或其他监护人“放纵同意”未成年人上网等规避核验机制的行为③。具体而言，建议在“隐私政策”的授权同意条款中，采取加黑、加粗的形式，专门提示“手机哄娃”“靠网带娃”等对未成年人个人信息及家庭信息的各类风险；在身份认证环节，强制要求跳转对接具备强实名认证能力的互联网平台（如支付宝、微信）或者政府数据库（如公安部公民网络身份识别系统），及时识别和筛选出利用父母或其他监护人身份上网的未成年人。对因未依法履职造成未成年人个人信息受到不法侵害的互联网平台，除了强化一般性的侵权责任损害赔偿外，可以通过立法进一步健全未成年人网络保护领域的专项赔偿基金、救助基金等多元化的责任承担方式。

2.依据平台等级建立“数据备案审查”或“检察进驻监管”机制

本文认为，应当进一步区分互联网平台的等级，尤其是数据规模、技术能力等完善分类监管机制。具体而言，在《信息安全技术大型互联网企业个人信息保护监督机构要求》出台前，可以参

①参见 Schermer B W，Custers B，Van Der Hof . “The Crisis of Consent：How Stronger Legal Protection May Lead to Weaker Consent in Data Protection”，*Ethics & Information Technology*，2014（2）：171-182.

②这一针对未成年人处理自身个人信息权利的立法被形象地称为“橡皮擦法案”。参见 Alessandro Mantelero. “The EU Proposal for a General Data Protection Regulation and the Roots of the‘Right to be Forgotten’”，*Computer Law&Security Review*，2013（3）：230.

③闫姝月：《切实保护触网未成年人权益》，《人民法院报》2023 年 10 月 19 日。

照适用《分类分级指南》中关于互联网平台的划分标准,明确两种监管模式:(1)针对中小平台,可以将"数据备案审查"作为基础设立"未成年人个人信息网络保护备案系统"。除了确立专门的未成年人个人信息处理规则外,还需要定期将未成年人个人信息网络保护情况、投诉举报处理情况、相关数据舆情监测等与检察机关、网信部门等进行对接。(2)针对重要互联网平台,可以根据《个人信息保护法》第58条关于独立监督机构的规定,参照适用检察机关对证券行业的派驻监督模式。具体而言,选派检察官进驻重要互联网平台或设立"检察室",重点监督未成年人个人信息网络保护的合规建设和实施情况。

在数字赋能法律监督的过程中,应当尊重互联网平台等的企业自主经营权及其商业秘密。在实体层面,可以明确法律监督的重心在于保障收集和使用个人信息的合法性、正当性:如收集信息是否具有相应的法律依据,是否经过监护人的实质同意,是否存在隐形或显性强制索权条款,是否对处理流程(收集、存储、使用、加工、传输、提供、公开、删除等)制定了风险控制方案,是否有专门的投诉处理和反馈渠道,是否建设有效的未成年人个人信息网络保护的专项刑事合规体系等。在发生或者可能发生未成年人个人信息被过度收集、不当存储、越界使用、违法转移、违法披露等事件时,相关互联网平台应当立即启动应急预案和采取补救措施,及时开展自纠自查,积极配合检察机关的法律监督。在程序层面完善检察机关行使法律监督权的审批层级和相关流程。各级检察机关对互联网平台发出检察建议或提起公益诉讼的,应当经过检察长的审批同意。对违法处理未成年人个人信息的互联网平台,在符合合规建设有效性标准的情况下,检察机关可以将其纳入合规考察范围,并根据其整改效果作出是否不起诉等轻缓化处理①。

(二)以"未成年人检察数据库"促进数据共享与善用

1.在检察系统自上而下设置"未成年人检察数据库"

当前,要实现未成年人保护方面的大数据互联互通,建立健全"未成年人检察数据库"是最优选择方案。建议在最高人民检察院建立"全国未成年人检察数据库",各省、自治区、直辖市检察机关分别对标建立"数据库"分库。其中,对各互联网平台中涉未成年人个人信息版块,尤其是设立了"未成年人个人信息网络保护备案系统"的,可以要求其自动链入上述数据库系统。未成年人检察部门可以对这些数据的收集和使用开展融合式法律监督。

2.与有关机关、部门的数据共享和协同监督

鉴于许多机关、部门之间储存涉未成年人个人信息的口径、条件差异,在各数字化平台对接的过程中,检察机关应当明确各部门的主体责任、准入要求,督促和监督依法采集、运用和共享涉未成年人个人信息数据。各有关机关、部门需要结合地方执法司法情况,围绕未成年人权益容易受到侵害等风险环节和相关社会治理的漏洞客观、全面采集数据,及时更新并共享相关数据②。具体而言,可以将"未成年人检察数据库"作为基础,实现检察机关与网信部门、民政部门、群团组织等相关专项行动案例库、数据库等的数据共享,建立协同监督机制。如自动对接网信部门"清朗·未成年人网络环境整治"专项行动案例库、共青团中央"未成年人手机上网综合服务平台"、民政部门"困境儿童信息数据库"等。

在推进大数据赋能法律监督的同时,检察机关也要强化对未成年人数据安全并进行监督管理。在数据采集、运用和共享的各个流程,检察机关应当严格贯彻《个人信息保护法》第34条规定,监督有关机关、部门坚持合法、正当、必要和诚信原则,不得超出履行法定职责所必需的范围和限度。特别要注意的是,对电子信息系统中需要封存的未成年人犯罪记录数据,应当严格遵循《刑事诉讼法》规定犯罪记录封存制度和2022年"两高两部"发布的《关于未成年人犯罪记录封存的实施办法》规定,未经法定查询程序,不得进行信息查询、共享及复用。

(三)从严惩治侵犯未成年人个人信息违法犯罪

针对未成年人个人信息保护救济方式总体乏力的问题,在细化数据库的建设与行政监管外,对检察机关法律监督而言,需要重点完善刑事追诉和公益诉讼等救济方式,从严惩治相关违法犯罪。在危及未成年人个人信息安全的行为当中,相当

①参见2022年中华全国工商业联合会、最高人民检察院、司法部、财政部、生态环境部、国务院国有资产监督管理委员会、国家税务总局、国家市场监督管理总局、中国贸促会联合发布的《涉案企业合规建设、评估和审查办法(试行)》第2条规定。

②唐瑞芳:《论公私合作治理模式下个人信息保护机制建构——以规范主义向功能主义转向为视角》,《湖湘论坛》2022年第1期。

一部分属于刑法意义上的“侵犯公民个人信息犯罪”。2017 年最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称《解释》)主要根据个人信息本身的用途和功能,设置“情节严重”和“情节非常严重”的认定门槛,未将未成年人个人信息作为一种特别的信息类型进行单独规定。本文认为,为贯彻特殊保护的理念,在刑事立法中,应该将此类行为直接界定为“情节严重”的情形之一。具体可在《解释》第 5 条增加侵犯未成年人个人信息的专门条款,并在量刑时要求考虑和评估这类犯罪行为对未成年人身心健康的影响程度,以及引发家庭损失、次生伤害的可能性。

面对侵犯未成年人个人信息且涉及公共利益的,检察机关应该充分利用公益诉讼这一保护方式监督制裁相关民事侵权、违法犯罪行为,同时促进行政履职和行业整改。本文建议,要解决“未成年人个人信息受到侵犯”和“涉公共利益”标准的证明难问题,需要进一步结合年龄区间、应用场景等明确对“敏感个人信息”和“不特定人员”的认定细则;同时以数字赋能、数字共享为基础,强化公安机关、网信部门等对检察机关的“互相配合”职责,全面提高检察机关取证能力和水平。

(四)完善监护缺失、监护不当的强制性亲职教育

家庭是人生的第一课堂。父母或者其他监护人是否在网络保护上依法履职是影响《条例》能否“落地生根”的基础性因素。对未成年人个人信息网络保护而言,健康、安全、合理用网的家庭教育指导是实现前端保护、避免风险后移的关键一环。尽管一些互联网平台推出了相关的教育栏目,如腾讯“未成年人家长服务平台”、快手“家庭教育护苗行动大讲堂”等,但是许多父母或其他监护人受制于文化程度、时间精力和认知水平等因素,参与的积极性和实际效果较为有限。当前,有必要针对性地开展预防性家庭教育指导工作,全面提高监护人对未成年人个人信息的风险防范意识和实际保护能力。在贯彻《条例》时,应当实现与《未成年人保护法》《预防未成年人犯罪法》有序衔接,并且依托相关的指导性案例、典型案例,全面推广未成年人个人信息网络保护中针对监护缺失、监护不当情形的强制性亲职教育。针对未能依法履行监护职责,致使未成年人个人信息泄露、不当使用的父母或其他监护人,检察机关应当根据上述法律法规,积极制定并颁布《家庭教育指导令》《督促监护令》等,严格督促其接受相关亲职教育,全面履行家庭教育、家庭保护责任。

Problems and Countermeasures on the Connection Between the Network Protection of Minors and “Digital Prosecution”

LEI Xiaozheng & YAN Shuyue

(Institute of Criminal Law Science/Research Center for Minors' Prosecutorial Work, Beijing Normal University, Beijing100875, China)

Abstract: When implementation of the *Regulations on the Protection of Minors Online*, moderate and reasonable use of personal information is the basic proposition of standardizing algorithm push, improving network literacy, and preventing network addiction. Currently, the problem of minors' personal information leaking or improper use on the network is more serious, which becomes the “short board” of the entire minors' network protection system. In view of the fact that many Internet platforms have the dual identity of market players and regulatory roles, and the network compliance system for minors is not yet perfect, in order to promote the connection between network protection and judicial protection, it is necessary to use “digital prosecution” as a support point to enhance protection and enhance institutional rigidity. It is recommended to establish a “data filing review” or “procuratorial supervision” mechanism based on the level of the Internet platform, and improve the data interconnection mechanism for minors. While improving criminal prosecution and public interest litigation, the compulsory parental education should be refined.

Key words: network protection for minors; personal information; digital prosecution; internet platform

(责任校对　王小飞)