



学生个人信息成为黑灰产交易筹码

记者实测注册校园交友软件后骚扰电话频繁

□ 本报记者 韩丹东 文丽娟

近期,四川、山西等地公安机关接连破获非法倒卖学生个人信息大案:校园“内鬼”违规导出数据,运维人员监守自盗,中介层层加价转卖,非法倒卖学生个人信息的黑灰产业链条浮出水面。

与此同时,《法治日报》记者对多款校园交友软件开展实名注册实测,采用专属姓氏溯源方式排查泄露源头,注册后很快便接到众多信贷、兼职类骚扰来电。

学生个人信息究竟如何从校园、平台、机构流出,又怎样在黑灰产业链条中被层层倒卖?记者对此展开了采访。

骚扰电话接踵而至

多名受访学生表示,他们日常会高频使用多款校园墙、校园社交、学生专属交友软件,这类平台主打校园交友、同城互助、校园树洞等功能,深受学生群体青睐。为测试平台信息安全程度,记者对多款热门校园交友软件进行实名注册体验;在注册不同软件时,记者特意预留了区分度不同的专属姓氏信息,以此排查信息泄露渠道,排除其他干扰因素。

注册完成后短短几天时间,记者的手机便频繁接到陌生人的来电骚扰,类型高度集中,主要分为两类:

一类是信贷贷款推销电话,来电人员话术统一,反复询问是否有资金需求,主动推销各类贷款业务,声称“征信不好,没有信用记录,也可以办理贷款”,另一类是兼职招募骚扰电话,对方频繁推送各类陌生兼职岗位,不间断询问是否需要兼职工作。

多名来自不同高校的大学生同样遭遇过个人信息泄露带来的困扰。

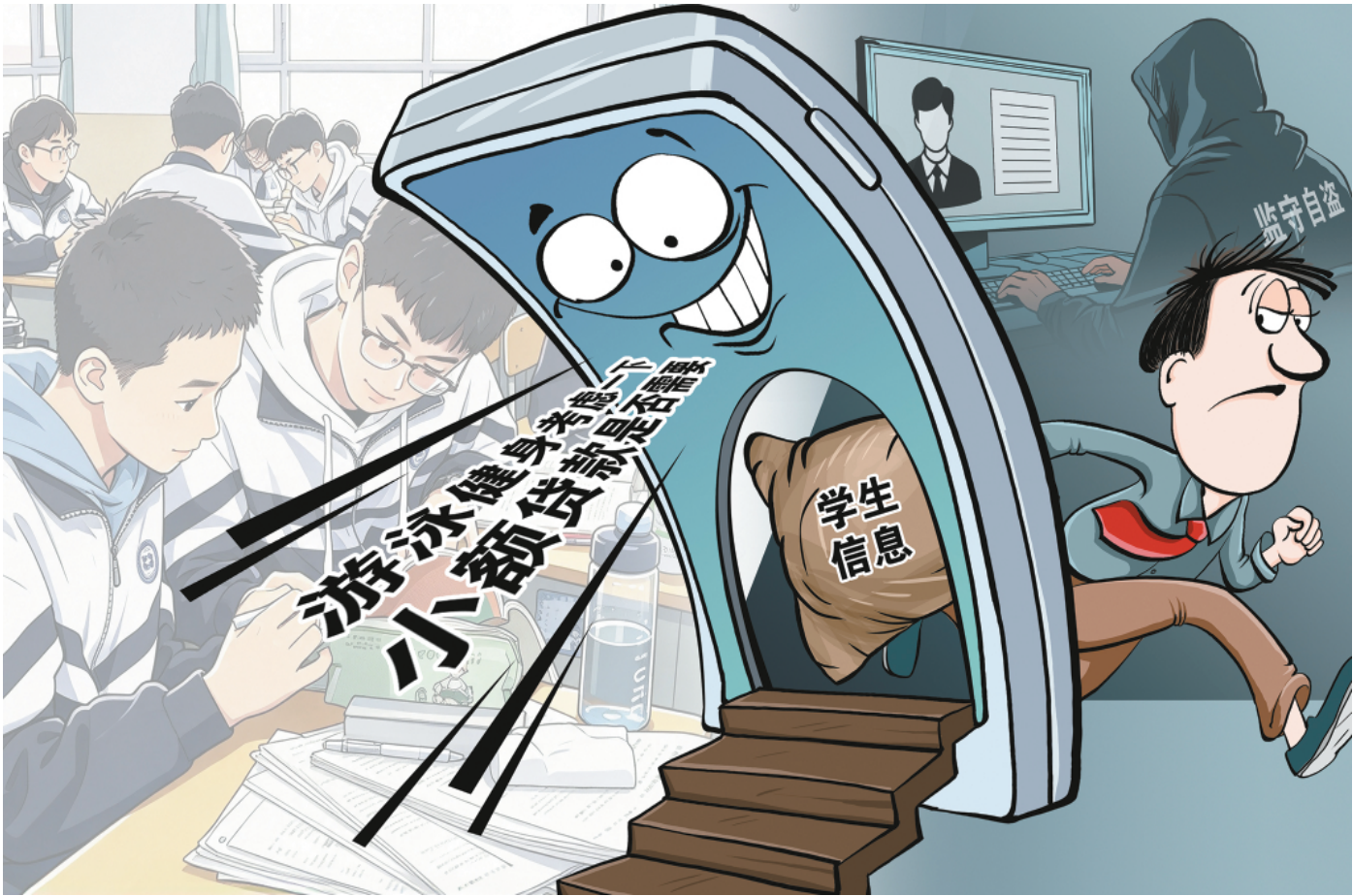
北京某高校新闻与传播专业的蒋同学在某平台为领取考研备考资料填写了自己的手机号码,提交表单后,骚扰电话数量明显增多,某平台工作人员反复向她推销考研培训班。她联系客服要求停止致电但并未起效,直到她明确告知将发起投诉,骚扰来电才最终停止。

另一所高校金融学专业的研一新生张同学每隔半个月左右就会接到一通骚扰电话,他曾浏览过健身相关内容,此后健身房推销电话接踵而至。“有可能是平台采集了我的浏览行为数据,将健身需求标签连同联系方式一并给到商家。”张同学说,“现在不少小程序、App都需要手机号码授权,很难确认到底是哪一次操作造成的信息泄露。”

近期正在求职的某高校大四学生刘同学每隔二三天就会接到一通骚扰电话,部分来电者甚至能够精准报出他的姓名、学校、年龄。信息泄露的线索指向一次线下面试:他在现场如实填写纸质个人信息登记表,面试结束之后,大量打着“包就业”旗号的技能培训推销电话持续了半个月。

信息泄露的现象并不止于大学校园。不少中小学生家长同样因为孩子的个人信息外泄,频繁遭到中介骚扰。

来自湖南的一名学生家长向记者回忆,孩子就读高二期间,自己被频繁接到陌生来电,对方以“保障入学名额”为噱头,劝说家长预交相关



费用。

来自浙江的一名家长说,他的孩子上小学四年级,经常接到各类营销小升初培训的短信和骚扰电话。他将来电话号码拉黑,可源源不断的虚拟号码,真实手机号依旧打入。

案件揭开信息黑市

学生个人信息泄露并非个案,记者梳理公开报道发现,近年来多起特大侵犯公民个人信息案件被破获,其共同特征是:泄露源头往往是机构内部人员利用职务便利“监守自盗”。

例如,公安部网安局2026年8月发布的打击侵犯公民个人信息犯罪典型案例显示,山西太原公安网安部门从教培“精准推销”电话入手,破获王某杰等人侵犯公民个人信息案。经查,王某杰在教培机构任职期间,为完成招生指标,与多名教培机构工作人员非法交换和出售学生数据,又向多家眼科医院和学校的工作人员购买大量学生个人信息,形成“内鬼窃取、行业倒卖、精准推销”的犯罪产业链。王某杰等人非法获取公民个人信息50余万条,涉案金额30余万元,12名犯罪嫌疑人已被依法提起公诉。

学生个人信息为何成为黑灰产的“香饽饽”?互联网法治研究院(杭州)特邀研究员张继红分析,学生个人信息完整度高且商业价值大,通常涵盖姓名、性别、身份证号码、户籍、学籍,就读学校和班级,监护人联系方式、家庭住址等多维度内容,数据完整性与准确度远优于普通用户信息,能够精准匹配各类营销需求。

“其次是学校缺乏专业化数据安全保障能

力。学校的核心职能为教育教学,并非专业化的数据处理和管理机构,普遍存在信息安全保障体系缺位问题。部分高校未设置专职个人信息安全管理人员,中小学的信息安全配置更为薄弱;部分学校未常态化投入校园网络运维,数据安全防护等专项经费,缺乏完善的信息存储、权限管理、风险防控机制,导致学生个人信息在存储、传输、运维等过程中存在安全漏洞,极易被非法窃取、泄露和滥用。”张继红说,“此外,学生个人信息泄露具有隐蔽性、滞后性等特点,侵权行为难以被及时发现;普通学生与监护人普遍缺乏溯源、取证的技术能力,无法精准定位信息泄露环节,固定侵权证据。”

《法治日报》律师专家库成员、北京嘉润律师事务所律师高攀告诉记者,学生个人信息贩卖的违法犯罪链条可以分为前、中、后三个环节:在前端,学校、培训机构过度收集学生和家长信息,内部工作人员监守自盗是泄露的重要诱因;在中端,信息被汇总、加工后,在相关平台中传播、售卖;在后端,培训机构、招生中介乃至诈骗团伙利用这些信息进行精准营销或实施电信网络诈骗。

合力构建治理闭环

学生个人信息泄露频发,治理路径何在?受访专家从制度建设、部门协同等多个维度提出建议。

张继红认为,亟须构建全流程闭环治理体系。一是落实备案准入机制,全面推行教育类App备案管理制度,未经备案或备案不通过的

App严禁在校园场景使用,并进一步细化教育场景类“必要个人信息清单”,将学校、平台、运维服务商、教培机构等主体纳入清单规制范围。二是健全常态化合规审计机制,将外包运维等关联服务环节全面纳入合规审计范围。三是强化专项监管抽查与多方共治,严格落实个人信息保护责任入制度,同时联动检察公益诉讼制度,整合学校管理、家长监督等社会力量,构建多元共治格局。

高攀从部门协同角度建议,教育、工信、公安、市场监管等部门在每一个关键节点需形成制度合力。教育部门处于治理链条最前端,应推动学校建立内部数据管理制度,落实教育数据分类分级要求;工信等部门应加强对电话营销环节的管理,对有害信息依法处置,强化对批量外呼号码、被标记的骚扰营销号码的监测与处置;公安机关应坚持全链条打击,不仅要打击倒卖信息的中间商,更要溯源查处泄密的“内鬼”。

在制度长远完善层面,受访专家提到,现有个人信息保护框架仍有优化空间,可进一步优化告知授权机制,针对不同年龄段学生建立差异化保护规则,强化未成年人群体信息权益倾斜保护。

受访专家一致认为,学生个人信息泄露的治理,是一项从源头收集到末端使用的系统工程。并非压实学校、培训机构、互联网平台等主体责任,公安机关全链条打击泄密“内鬼”与倒卖信息的中间商,多部门协同斩断整条黑灰产业链条,才能守护青少年群体的个人信息安全。

漫画/李晓军

□ 本报记者 文丽娟 韩丹东

大学生注册交友App后遭遇骚扰电话,中小学生家长频繁接到培训招生推销,多地接连破获学生个人信息被内部人员倒卖的刑事案件,学生个人信息泄露风险凸显。

多重现象交织之下,学生个人信息保护面临哪些法律难题?遭遇信息泄露后,各方主体应当承担什么责任?受害者有哪些救济渠道?围绕这些问题,《法治日报》记者采访了互联网法治研究院(杭州)特邀研究员张继红,《法治日报》律师专家库成员、北京嘉润律师事务所律师高攀。

贩卖学生信息罪与罚

记者:贩卖学生个人信息,在刑法上如何定性?对出售、提供、购买以及链条上转手倒卖的各环节主体,各自应承担怎样的责任?

高攀:根据《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》有关规定,学生的姓名、身份证号码、家庭住址、联系方式、学籍信息等,只要能够单独或者结合其他信息识别特定自然人身份,就属于刑法所保护的“公民个人信息”。贩卖学生个人信息的行为可能触犯刑法第二百五十三条之一规定的侵犯公民个人信息罪,情节严重的处三年以下有期徒刑或者拘役,并处或者单处罚金;但民事特别严重的处三年以上七年以下有期徒刑,并处罚金。

通过购买、收受、交换等方式获取公民个人信息,即便未再转卖,也属于“以其他方法非法获取公民个人信息”,只要数量或违法所得达到入罪标准,同样构成侵犯公民个人信息罪。

记者:实践中频发机构“内鬼”监守自盗,法律对此有哪些从重处罚规则?单位和个人的责任该如何划分?

高攀:刑法相关规定明确,对于在履行职责、提供服务过程中获取学生个人信息后向外出售、提供的行为,应当从重处罚。配套司法解释进一步降低入罪门槛:“内鬼”作案,认定“情节严重”的数量,数额标准为普通案件的一半。司法实践中要注意避免同一情节重复评价:如果已经凭借减半标准认定构成犯罪,量刑环节就不应再就“内部人员”这一情节再次从重。

在责任划分上,如果倒卖信息是单位集体决策、组织实施,实行双罚制,既要对单位判处罚金,同时追究主管人员、直接责任人的刑事责任;如果是员工个人私下利用职务便利牟利,单位并不知情,则由该员工独立承担刑事责任。但民事侵权层面适用过错推定,单位需要自行证明在数据管理上不存在过错,否则即便系员工个人私自作案,单位仍要承担民事赔偿责任。

自身不知情不能免责

记者:校园交友软件发生信息泄露,平台以“第三方原因泄露、自身不知情”为由能否免责?

张继红:校园交友软件兼具个人信息处理者、网络服务提供者双重身份。作为信息处理者,平台必须落实安全防护,风险处置,事件上报等法定义务;委托第三方处理数据,也要履行监督职责,作为网络服务提供者,对于平台内售卖学生个人信息的私信、帖子,要主动监测处置,及时删除、限制账号,并留存记录上报主管部门。

个人信息保护法确立过错推定原则,处理者不能证明自己没有过错的即承担侵权责任。平台须举证已实际履行等保、加密、权限管理、审计、及时补救、告知和报告等义务,已对委托处理尽监督义务,且泄露与其过错无因果关系,才可减轻或免除相应赔偿责任。若个人信息泄露源于平台违规共享、超期留存或自身管理漏洞、已知风险未处置,平台本身构成直接或未尽保护义务的责任主体。第三方窃取只是损害扩大因素,不能以“第三方原因、自身不知情”为由免责。

记者:部分校园类App“最小必要”原则落地难,原因何在?张继红:按照《常见类型移动互联网应用程序必要个人信息范围规定》,学习教育类App的基本功能服务为“在线辅导、网络课堂等”,必要个人信息限定为注册用户移动电话号码。然而实践中,少数学校在校园类App使用、管理过程中存在强制同意、捆绑授权等违规情形,超范围收集学生画像、人脸识别信息、考勤数据,显示成绩非必要个人信息,明显突破法定收集边界。与此同时,校园场景下个人信息处理的“必要性”认定标准较为模糊,主要依赖个案裁量,尚缺乏统一、规范化的适用标准。

合力斩断黑色产业链

记者:对于被泄露个人信息的学生,合法维权路径有哪些?有哪些可落地的自我保护建议?

高攀:对于已经发现个人信息被泄露的学生,应当及时固定证据,例如保存私信记录、账号名称、发布时间、相关链接等。根据民法典和个人信息保护法相关规定,受害学生可以依法要求信息处理者删除个人信息;对于涉嫌违法处理个人信息的行为,可以向履行个人信息保护职责的部门投诉、举报,涉嫌犯罪的可以向公安机关报案;对于造成损害的,还可以依法提起民事诉讼,主张停止侵害、消除影响以及损害赔偿等法律责任;涉及众多个人权益受到侵害的,还可能符合个人信息保护公益诉讼的条件。

从个人防护角度看,更重要的是降低个人信息泄露后的二次风险。学生个人信息泄露造成的风险往往并不止于泄露本身,还可能进一步演变为电信诈骗,造成财产损失。因此当发现自己的个人信息已经外泄后,应当提高对冒充老师、同学、学校工作人员等电话、信息的警惕,不向陌生人提供验证码、身份证件照片、银行卡号等信息,做到及时止损、避免二次伤害。

记者:面向学生群体,未来个人信息保护制度可以从哪些方面优化?

张继红:在立法完善层面,未来可推动同意机制从传统的“概括同意”转为“场景化动态授权”模式,通过构建场景告知规则,将个人同意与具体处理情境和行为绑定,破除单一隐私政策统一适用全部处理场景的弊端。同时,立法需推动个人信息保护从“形式同意”向“实质控制”升级,一方面强化个人信息删除、同意撤回、个性化推送关闭等动态功能的落地实效;另一方面优化授权交互机制,采用分项独立勾选的授权模式,真正落实个人对其自身信息的自主控制权。

针对学生群体,建议采用年龄分段并结合个人信息类型区别设计保护制度:对不满14周岁的未成年人严格保护;对14至18周岁的未成年人,则在最大限度内给予其自主决定权。如果是私密性相对较弱的个人信息,比如注册虚拟账号需要授权收集但不进行披露的信息,如性别、昵称、手机号码等,年龄界限可设定为年满14周岁,从而使该年龄段的未成年人可以正常进行社交及学习活动;对于可能公开未成年肖像、形体及其他信息的视频资料,属于私密性较强的个人信息,则应设定年满18周岁的严格年龄界限,且须经过监护人同意。

此外,现有法律规范及网络运营商的隐私政策中虽有监护人同意条款,但对于征得同意的方式却没有作出具体规定。可以通过电子邮箱等方式向运营商提供父母签署的同意书,或者采取父母电话同意告知、视频通话等方式,使未成年人难以伪造或刻意规避,切实发挥父母同意的监督作用。

专家解读学生个人信息泄露法律边界与维权路径并建议

年龄分段分类区别设计信息保护制度

把党建优势持续转化为司法效能

海口琼山法院以高质量党建推动法院工作高质量发展

□ 本报记者 邢东伟 霍小功

“被执行人邓某已购买船票,即将从海口南港出海。”今年国庆假期首日,海南省海口市琼山区人民法院执行局接到一条线索,被执行人邓某涉案标的33万元,长期四处流动,行踪难以掌握。

机会稍纵即逝,执行局立即启动应急响应,派出党员干警火速赶往海口南港,将邓某成功拦截。在法律的威慑下,双方达成执行和解。这是琼山区法院执行局党支部打造“琼山执行”党建品牌的鲜活实践。

“我们牢牢把握‘抓党建、带队建、促审判’工作主线,以高质量党建引领新时代基层法院工作高质量发展。”琼山区法院党组书记、院长薛蕃超接受《法治日报》记者采访时表示,近年来,该院从理论武装、品牌创建、机制创新、党建共治、先锋引领五个维度持续发力,将党组织的政治优势、组织优势转化为审判质效、为民实效。

党建引领

走进琼山区法院诉讼服务大厅,党员示范岗的标识格外醒目。导诉台前,调解室内,审判庭上,每天都有党员干警忙碌的身影。

据介绍,琼山区法院先后将诉讼服务大厅、审判一线等关键岗位设立党员示范岗36个,由党员示范岗干警带头落实便民立案、信访接待,带头攻坚疑难复杂案件,涉民生重点案件,充分发挥党员干警先锋模范作用。

案多人少,是基层法院长期面临的现实挑战,党员先锋队成为破解办案压力的中坚力量。2025年1月至2026年9月,全院共受理各类案件45万余件,办结392万余件,法官人均办案量

达10004件。

今年8月21日,琼山区法院云龙法庭党支部在海口市秀英区海瑞文化公园组织开展“赓续海瑞正气,坚守司法公为”主题党日轮值活动,切实将廉政教育成果转化为基层司法履职实效。

“近年来,琼山区法院通过机关党委‘搭台’、党支部‘唱戏’的方式,创新推行党支部主题党日轮值机制。”琼山区法院党组成员、政治部主任王飞说,由各支部按月轮流牵头主办全院主题党日活,由机关党委统筹,各支部自主策划开展活动,将巡回审判、廉政教育、志愿服务等融入主题党日,以此激活基层党组织内生动力。

此外,琼山区法院始终把政治建设摆在首位,认真落实“第一议题”,党组理论学习中心组学习等制度,建立常态化、制度化学习体系,将党的创新理论与审判执行、司法便民、队伍建设等紧密结合,夯实司法履职根基。

在党建引领下,琼山区法院各项工作取得显著成效。2025年,该院获评“2023—2024年度全省优秀法院”,司法警察大队荣获最高人民法院“人民法院司法警察工作成绩突出集体”。

品牌赋能

2025年11月,琼山区法院环境资源审判庭走进海口市知识产权保护中心,依法公开开庭审理一起侵害商标权纠纷案件。

庭审结束后,该院“环知红帆”党建品牌小组的两名成员分别与海口市知识产权保护中心工作人员进行知识产权纠纷调解实务专题分享,呈现了一堂沉浸式知识产权法治公开课。

“随着海南自贸港建设深入推进,各类知识产权纠纷与环境资源保护案件日益增多。”

琼山区法院环境资源审判庭庭长国瑞表示,环境资源审判庭利用管辖海口市知识产权和环境资源案件的独特优势,创新打造“环知红帆”党建品牌,设立“环知红帆”党员先锋审判团队,通过党支部建在庭上,品牌融在业务中,实现党建与业务深度融合、双提升。

据了解,琼山区法院坚持“一支部一品牌、一庭室一特色”创建思路,立足各业务庭室职能,围绕生态司法、纠纷化解、家事审判、执行攻坚等重点领域,分类培育、精准打造“环知红帆”“琼山执行”“法护万家”“法耀云门”“审判先锋”“诉服琼琼 红心向融”“红心护民 法润三门”7个特色党建品牌。

2025年9月,琼山区法院党组部署开展2025年度党建品牌阶段性考核评估工作,对各业务庭党支部党建品牌创建中好的经验做法进行总结提炼,以品牌打造助力党建、审判工作质效双提升。

琼山区法院建立党建品牌动态评估考核机制,围绕党建品牌的标识、内涵、经验做法、工作成效等进行考核,防止品牌“空壳化、形式化”。通过以考促干、以评促建,推动各党支部将品牌建设融入日常工作、普法宣传全过程,真正实现党建品牌有载体、业务融合有抓手、工作成效有亮点。

当前,7个特色党建品牌犹如7颗明珠,镶嵌在琼山区法院审判执行工作的各个领域。动态评估考核机制的建立,让每一个党建品牌都成为推动业务发展的“红色引擎”。

多元联动

2026年8月27日,琼山区法院运用“人大代表+法院+综治中心”联动调解机制化解原告上海某农业发展有限公司与被告海南某

供应链管理有限公司合同纠纷一案,入选《海口市营商环境》2026年第31期典型案例。

本案中,原告上海某农业发展有限公司与被告海南某供应链管理有限公司因商业合作产生争议,被告拖欠采购款21万余元长期未支付。法院查明,被告企业存在现实经营困难,并非主观恶意欠付,若简单裁判并强制执行,不利于市场主体健康发展。加之原、被告分属琼琼两地,异地诉讼成本高,双方矛盾对立,信任缺失,传统办案模式很难实现最优解。

为此,琼山区法院联动区人大、区综治中心协同发力,由党员法官、人大代表和调解员组成调解团队,依托在线调解平台开展远程视频调解。经过耐心调解,原被告双方达成分期还款调解协议。

近年来,琼山区法院充分发挥党员法官先锋带头作用,创新建立“人大代表+法院+综治中心”多元联动调解机制,选派政治素质高、调解经验丰富的党员法官常态化下沉琼山区综治中心,主动对接人大代表,借助人大代表公信力强、贴近群众、熟悉民情的优势,合力调处家事邻里、土地纠纷、劳务工资、物业纠纷等基层常见矛盾,将纠纷化解在诉前,化解在基层,有效减轻群众诉累。多元联动调解机制建立以来,受理矛盾纠纷120件,化解81件。

“下一步,我们将持续深化党建业务融合工作体系,深入探索党建工作与审判执行、司法服务、队伍建设全方位深度融合,不断释放党建引领效能,把党建优势持续转化为司法效能,持续增强人民群众司法获得感。”薛蕃超说。