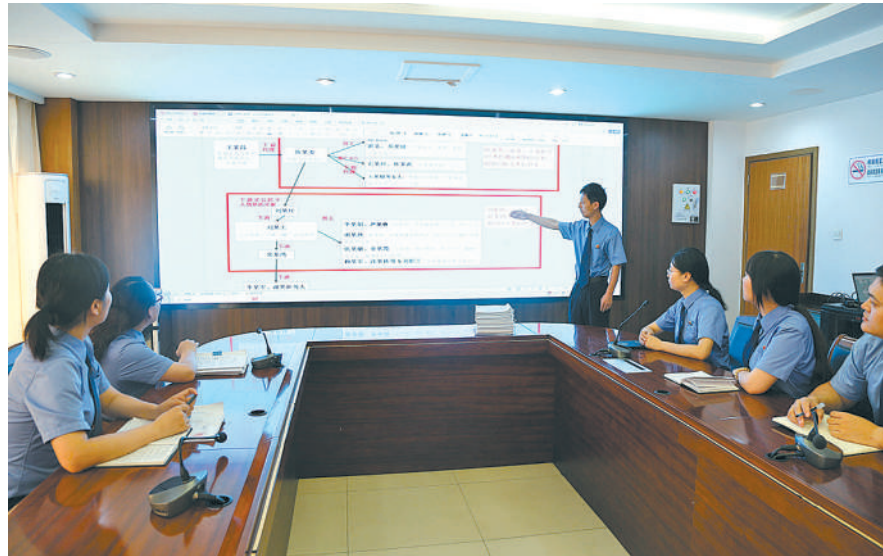


书城老板搭建淫秽书城网站,通过在网站内投放保健品免费领取广告的方式非法收集公民个人信息并进行售卖——

# 书城背后暗藏黑色产业链

## 刑案速写

□本报记者 卢志坚  
通讯员 孙鑫鑫 邱友诗



2022年9月20日,灌南县检察院检察官对书城网站传播淫秽物品、非法收集公民个人信息等上下游、关联性的犯罪行为进行分析研判。

书城老板搭建淫秽书城网站,在公众号内设置链接,通过站内投放保健品免费领取广告非法收集公民个人信息并交易。司法机关顺藤摸瓜,一条通过投放保健品免费领取广告方式非法获取、倒卖公民个人信息的产业链逐渐浮出水面。

经江苏省灌南县检察院提起公诉,4月23日,法院以传播淫秽物品牟利罪、侵犯公民个人信息罪判处主犯陈某委有期徒刑八年五个月,并处罚金175万元;分别判处其余12名同案犯有期徒刑二年至五年,各并处罚金。5月28日,由该案牵出的刘某士等8人侵犯公民个人信息案一审也有了结果:主犯刘某士被判处有期徒刑五年,并处罚金800万元;其余7人分别被判处有期徒刑一年六个月至四年六个月,各并处罚金。

两案的部分被告人不服,提出上诉。近日,连云港市中级人民法院二审均裁定驳回上诉,维持原判。

### 搭建书城“自立门户”

2021年3月,灌南县公安局接群众报警,称某微信公众号可链接到一个存有大量黄色小说的书城网站。经立案侦查,灌南县公安局发现书城负责人陈某某等涉嫌传播淫秽物品牟利罪,并先后抓获陈某某等13人。

2020年6月,长期经营网络小说生意的陈某某,听闻王某昌(因犯传播淫秽物品牟利罪、侵犯公民个人信息罪已被判处有期徒刑九年)经营的书城比较赚钱,便想学习其经营方法。经打听得知,王某昌搭建了一个含有淫秽书籍的书城网站,通过利用公众号链接网站、微信群推广、诱导用户充值阅读牟利,并利用网站投放保健品免费领取广告通过点击量牟利的方式,非法收集公民个人信息进行交易,还将书城网站“租借”给下级代理作为公众号链接使用,从中按1:9抽成。看到王某昌的书城利润可观,陈某某开始做王某昌的书城代理。

陈某某在经营中发现,只要有一个书城网站和一个微信公众号,就完全可以自己经营,于是决定“自立门户”。2020

年10月,他依托自己的文化传媒有限公司,雇用陈某某、陈某某等人,先后搭建“钉钉文学”“派派文学”书城网站,并招募游某、邓某琼为技术、客服,运营上述书城网站,联系石某州、杜某瀚等流量中介推广微信公众号。陈某某还发展了王某超等6人作为下级代理,将搭建好的书城网站“租借”给他们作为公众号链接使用。据公安机关侦查,2021年1月至4月,书城网站充值总金额高达310余万元。

### 书城背后暗藏“玄机”

因案情复杂,涉案人数较多,2021年4月,灌南县检察院应邀依法介入,引导公安机关对涉案全部书籍进行鉴定、固定并梳理所有电子数据,对照银行流水与微信记录确定涉案金额。

公安机关进一步调查发现,陈某某搭建的两个书城网站不单纯地传播淫秽物品牟利,站内还投放了保健品免费领取广告,一旦有人通过广告链接填写个人信息,这些信息便会被后台程序自动收集。陈某某以每条30元至35元不等的价格将这些公民个人信息销售给刘某环和王某超,刘某环和王某超再加价1元至2元后进行二次售卖。二次销售中最大的买家是刘某士的公司,而刘某士下游最大的买家为史某鸿。

2021年6月9日,灌南县公安局以涉嫌侵犯公民个人信息罪对刘某环、刘某士、史某鸿等13人立案侦查。2022年4月

28日,将陈某某等人涉嫌传播淫秽物品牟利、侵犯公民个人信息案移送灌南县检察院审查起诉。

办案过程中,陈某某的供述让办案检察官感到疑惑:其公司获取的公民个人信息仅含姓名、家庭住址、电话号码3项内容,按照以往办理侵犯公民个人信息案件的经验和用途等上下游查处与打击问题进行分析,进一步明确侦查方向。

### 黑色产业链浮出水面

随着公安机关对案件的不断深挖,一条非法获取、倒卖公民个人信息犯罪链条逐渐清晰。

早在2018年6月,刘某士就带领谢某燕、张某某、李某娟、严某勇、李某霞5人成立厦门某科技有限公司,后期陆续雇用了赖某军、沈某伟等5名职工。该公司主要是设计男性保健品免费领取广告网页,并将含有宣传标语的链接投放到各种网站,诱导他人点击浏览并填写个人信息,然后将这些信息卖给有需求的客户。

办案检察官程伟介绍,刘某士公司获取公民个人信息的渠道有两种:一种是内单,即通过投放保健品免费领取广告自行非法获取公民个人信息;另一种

为外单,当获取的内单供不应求时,就外部购买。自2020年11月起,刘某士公司从陈某某公司非法购买公民个人信息2万余条,然后按产品分类以每条20元至45元的价格出售给保健品销售商家。

“这些信息能够帮助销售商家精准锁定目标客户,让商家实现靶向销售,经过层层倒卖加价,导致一条信息最终以30多元的高价出售。”程伟介绍。

2022年7月15日,公安机关将刘某环、刘某士、史某鸿等13人侵犯公民个人信息案移送灌南县检察院审查起诉。经审查查明,2018年7月至2021年5月,刘某士公司非法倒卖公民个人信息56万余条,公司实际控制人刘某士违法所得910余万元。

公安机关以刘某士公司最大的买家史某鸿为突破口,经深入侦查,下游的保健品销售商家李某军、谢某林等人也浮出水面。他们购买公民个人信息后,安排员工向目标群体电话推销保健品,只要有客户下单就通知厂家发货,并以出厂价3倍的价格销售,从中赚取差价获利。

2024年6月至8月,灌南县公安局以涉嫌侵犯公民个人信息罪陆续将李某军、谢某林等下游犯罪嫌疑人移送审查起诉。目前,该案正在进一步审查中。

至此,这一上下游产业链终于查清:陈某某等人通过搭建淫秽书城网站、投放保健品免费领取广告非法收集公民个人信息并出售,只是这条产业链的源头散户;真正的主力是刘某士等人,其自行获取公民个人信息的同时又从外部购买,既是产业链的源头主力也是“中间商”;史某鸿则扮演倒卖公民个人信息赚取差价的“二手贩子”;销售商李某军、谢某林等人是利用这些公民个人信息实现精准推销的下游犯罪分子。

检察机关审查查明,2020年11月至2021年3月,陈某某搭建的“钉钉文学”“派派文学”书城网站共有991本电子书籍,其中515本是淫秽电子书籍,其利用书城网站非法获取公民个人信息31670条。

2023年3月30日,灌南县检察院以涉嫌传播淫秽物品牟利罪、侵犯公民个人信息罪对陈某某、游某、王某超3人提起公诉;以涉嫌传播淫秽物品牟利罪对李某军、陈某某等10人提起公诉。5月8日,该院以涉嫌侵犯公民个人信息罪对刘某士、刘某环、史某鸿等8人提起公诉,对入职较晚、在该案中作用较小的赖某军、沈某伟等5名职工作出相对不起诉决定。

## 社会万象

### 想不劳而获 以“碰瓷”为生

他提前将自己手脚磨破,利用被害人开车拐弯时存在盲区,制造被擦碰的假象,进而要求私了以获得赔偿。近日,由山西省平遥县检察院提起公诉的宋某涉嫌诈骗、敲诈勒索一案,法院经审理后作出一审判决,宋某最终为自己的小聪明付出了沉重代价。

2023年8月3日,平遥县公安局接到群众报警,称遭遇“碰瓷”被讹诈2000元。随后一段时间,又有多位群众报警称遭遇类似情况。综合研判各案情况后,平遥县公安局于2024年5月17日立案,锁定宋某并将其抓获。

经查,为不劳而获,宋某决定利用司机开车时的视觉盲区,以“碰瓷”为生。为提高成功率,他将作案时间选择在晚上,提前在道路拐弯处蹲守,等目标车辆开到拐弯处就制造自己被撞的假象,要求对方赔钱私了。部分被害人以为自己的车真的撞到了宋某,便直接出钱与宋某私了,也有部分被害人认为自己没有碰宋某,但因有急事或害怕宋某纠缠,选择出钱息事宁人。2023年8月至2024年4月,宋某先后在平遥、太原等地作案12起,犯罪金额共计3.85万元。

10月17日,平遥县法院以诈骗罪、敲诈勒索罪判处宋某有期徒刑二年十个月,并处罚金4.5万元,并责令其退赔被害人损失合计3.85万元。(王晓平 鹿瑞波)

### 已婚女子扮单身 假谈恋爱真要钱

婚恋相亲,可能会邂逅一段美妙的爱情,也可能遭遇一个温柔的陷阱。近日,经安徽省凤阳县检察院提起公诉,法院以诈骗罪判处被告人耿某、陈某、曹某有期徒刑三年至一年四个月,各并处罚金3万元至1.4万元。

2019年10月,耿某刑满释放,出狱后认识了江苏省东海县的陈某等人,经商量后他们决定合伙进行婚姻诈骗。2023年4月,耿某听说33岁的凤阳县村民史某一直没有“意中人”,其奶奶邓某很着急,四处为孙子张罗对象。于是,耿某告诉邓某自己在江苏有个远房兄弟,其女儿曹某现年28岁,相貌较俊,至今还没有结婚,可以为其孙子“牵线搭桥”。邓某闻言大喜,催着让一对年轻人尽快见面。

同年4月25日,陈某带着曹某在耿某的陪同下来到邓某家中“相亲”,看着说话轻柔、年轻貌美的曹某,邓某和史某都特别满意。2024年3月6日,在邓家的催促下,双方在东海县“订婚”,为表达诚意,邓家送给女方金首饰、订婚礼等价值2.54万元的物品和现金。

数月后,史某发现曹某系已婚妇女,感觉自己遭遇了骗局,遂报警。经查,耿某、陈某、曹某还采取同样手段,于2022年9月骗取他人钱财3.38万元。

案发后,三名犯罪嫌疑人主动交代了犯罪事实,积极退赔,与被害人达成和解协议,并在值班律师的见证下自愿签署了认罪认罚具结书。6月21日,凤阳县检察院将此案提起公诉。法院经审理认为,检察机关的指控成立,量刑建议适当,予以采纳,依法作出上述判决。(吴长志)

### 开发销售打卡“神器” 不到一年东窗事发

“拥有这款打卡‘神器’,想在哪里打卡就能在哪里打卡,定位修改、打卡照片替换、win模拟统统轻松搞定!”一些不法分子开始在打卡这件事上动起歪脑筋,甚至成立了专门的工作室。5月27日至6月27日,浙江省宁波市海曙区检察院分批对邱某、于某、陈某等9人提起公诉。近日,法院以提供侵入、非法控制计算机信息系统程序、工具罪分别判处9名被告人有期徒刑九个月至三年,均适用缓刑,各并处罚金。

2023年8月,刚大学毕业的小张到宁波找工作,面试几家公司后发现多数公司都需要通过App来考勤打卡,他觉得特别麻烦,在和同学聚餐时聊起此事,同学向他推荐了一个可以实现虚拟定位打卡的网站。小张登录了这个网站,加了网站管理员的微信。

在了解小张的需求后,对方向小张推荐了一款能够实现虚拟定位打卡的软件,但需购买月卡。小张购买了月卡并安装了该软件,经测试发现在家就可以修改定位和照片打卡,从此实现打卡“自由”。但没过多久,小张发现虚拟打卡的行为被公司发现,公司在解雇小张的同时,选择了报警。

经查,2023年2月至11月,犯罪嫌疑人邱某、于某、陈某指使技术人员开发了一款定制模块,利用服务器防御漏洞接入正版软件使用的服务器,可根据指令生成不符合实际情况的虚假定位,从而达到虚拟打卡的效果。后三人通过网络对外推广该定制模块,并根据月卡、季卡、半年卡、年卡收费30元至150元不等。截至案发,三人通过发展5名下级代理销售上述程序插件非法获利共计32万余元。此外,技术人员黄某也从中获取了非法利益。涉案人员到案后均认罪认罚,并退缴了全部违法所得。(蒋杰 龚鑫 孙琳洁)

# 明明账户有钱却不支付工人工资

□本报记者 刘怡廷  
通讯员 李鑫鑫 严予廷

经湖北省随州市曾都区检察院提起公诉,近日,法院以拒不支付劳动报酬罪判处曾某有期徒刑二年三个月,并处罚金3000元。

2020年5月,曾某承包了一小区的劳务工程项目(包工不包料),并与建筑公司签订劳务合同,工程造价约900万元。此后,曾某按照合同约定组织工人进场施工,工人工资由建筑公司定期打给曾某,曾某再支付给工人。起初,工人都能按时拿到工资,但最后几个月,曾某以未收到工程款为由,只支付了工人部分生活费。

施工一段时间后,建筑公司表示需要修改工程图纸,原定的施工项目有所改动,并出具了施工量的增补单。曾某按照建筑公司要求完成施工后,共收到建筑公司支付的约1001.8万元工程款

(含工人工资)。

“三年了,我们每次找他要工资,他都推脱是建筑公司的问题,让我们直接找建筑公司要钱,但是建筑公司说钱都给曾某了。我们就像皮球一样被踢来踢去。”2023年7月,工人代表刘某到劳动保障监察部门反映情况。

“不是我不给他们工钱,是因为建筑公司没有足额支付工程款。”曾某称,其最终核算的工程款与建筑公司实际支付的1001.8万元有近190万元差额,拖欠工人工资就是因为建筑公司没有支付这190万元。

经核实,曾某共拖欠97名工人约178万元工资。2023年11月,在多次要求曾某支付工资未果的情况下,人社部门将该线索移交公安机关。2024年4月,公安机关侦查结束后,以曾某涉嫌拒不支付劳动报酬罪将该案移送曾都区检察院审查起诉。

“我不认为我有罪,建筑公司给我

打的工程款我全部发给工人了,不是我欠工人工资,而是建筑公司欠我和工人的工资。”面对检察官讯问,曾某辩解道。

“他只付了我们800万元左右的工资。他拖欠我们工资,是因为他和建筑公司在扯皮。”面对前来了解详情的检察官,工人代表刘某、凡某表示。

曾某收到1000余万元,最后支付了工人多少工资?有没有恶意拖欠?

曾某雇用工人,最多的时候一天有500多人,他们一半以上是临时工,流动性很大。曾某多用现金支付工资,在缺乏账本的情况下,工资发放情况很难查证。由于双方都无法出示具体工资流水或收据,根据当时证据,曾某供述和工人证词无法与其他证据相互印证,无法得到确定性结论。由此,曾都区检察院将该案退回公安机关补充侦查,并列继续侦查提纲。

“我们通过查银行流水发现,曾某

于2021年年底就停发工资了,之后两年,他的银行卡有很多大额资金进出账,2022年1月至2024年1月,曾某的一张银行卡就有576万余元流水。有钱但依然不支付工人工资,这就是恶意拖欠了。”办案检察官介绍道。面对巨额流水,曾某辩称那是他做其他工程的钱,跟这个工程没有任何关系。

“工人劳动报酬是受法律保护的,只要你有钱,就应该按时支付工人工资。哪怕你跟建筑公司有纠纷,也不能损害工人的合法权益。”为准确指控犯罪,办案检察官仔细审查曾某的每一笔大额流水,向其展示完整证据链条,并开展释法说理。最终,曾某认罪认罚。

经审查,该院认为,曾某有能力而不支付97名劳动者报酬,数额较大,经有关部门责令支付后仍不支付,涉嫌拒不支付劳动报酬罪。6月,该院对曾某提起公诉。近日,法院经审理,依法作出上述判决。

广告

方正法度 圆融情理

# 探索法治 崭新视野

2025年度《方圆》征订启动

本刊自办发行 您可通过以下两种方式订阅《方圆》杂志

1. 银行汇款  
开户银行: 中国工商银行北京永定路支行  
户名: 方圆杂志社  
账号: 0200 0049 1920 0569 872
2. 扫码订阅