人民日报海外版

2025年7月7日 星期一

责编：霍旻含 邮箱：huominhan@163.com

『融』观中国

严惩“开盒”，给隐私“上锁”

——“守护清朗网络空间”系列报道④

本报记者 **霍旻含**

今年3月，一则“13岁未成年人开盒孕妇”事件引发热议，把“开盒”一词推上风口浪尖。

何为“开盒”？即不法分子通过非法手段，搜集并公开他人姓名、身份证号、住址、联系方式等敏感信息，目的多为煽动网络暴力、诽谤攻击或谋取利益。

5月底，中央网信办印发通知，要求强化“开盒”问题整治工作。“开盒”屡禁不止，根源在哪？网友该如何给个人隐私数据“上锁”？记者进行了采访。

扫描二维码
看“融”观中国主页

“开盒”网暴，为何“防不胜防”？

一天醒来，手机被无数条恐吓电话和私信“轰炸”，家住北京的插画师小蔡意识到：自己被“开盒”了。

“这些信息来自不同的账号，大多是新注册的，IP地址都一样，拉黑一个，又来了10个。”小蔡说，“我几年前发布的动态也被翻出来，在一个我不知道的群里被辱骂造谣，然后又截图发给我；对方甚至晒出我家地址，威胁绑架。”

而这一切的发生，不过是因为小蔡曾在群聊里为另一位被这名“开盒者”攻击过的网友抱不平。弄清原委后，小蔡报了警。经过警方介入，对方终于消停。

回想起与“开盒者”对抗的这段经历，小蔡心有余悸：“我完全不认识他，和他也没有过任何利益纠纷。他‘开盒’我，仅仅因为我在群里说他做得不对。这件事很恐怖，给我身体和心理上都带来很大伤害。”

提到“开盒”，不少人会想起“人肉搜索”。二者有哪些关联和不同？

曾处理过不少相关案件，成都铁路运输中级法院互联网审判庭副庭长、四级高级法官何定洁告诉记者：“一定程度上说，‘开盒’是过去‘人肉搜索’的技术升级版。”

具体而言，传统人肉搜索主要依赖网友“众筹”，即通过公开讨论、信息交换等方式获取他人隐私；而“开盒”更加组织化、产业化，通常由专门的“开盒者”或违法及游走在法律边缘的“黑灰产”提供服务，信息获取更加精准高效。

因此，“开盒”比“人肉搜索”更加广泛和隐蔽。

“由于个人信息买卖交易的黑灰产业链条已经成形，现在来看，‘开盒’并不是一个门槛和成本很高的行为。”中国社会科学院大学法学院副教授、互联网法治研究中心主任刘晓春解释，“大多数情况下，由于开盒者匿名发布信息，责任主体往往难以直接查实，增加了追责难度。”

在已曝光的案例中，许多被“开盒”的个人隐私数据来自境外“社工库”，即不法分子收集泄露的个人信息后搭建的数据库。最多花费几百元，就能“买”到一个人的户籍地址、婚史记录、身份证正反面、名下房产、银行卡流水等全套信息。

这些被交易的信息是如何泄露的？

有报告显示，2023年，全网监测并分析验证有效的数据泄露事件超过19500起，涉及金融、物流、航旅、电商、汽车等20余个行业。今年的315晚会也曝光，一些所谓“获客软件”能从社交记录、购物订单中窃取他人信息，然后打包出售。

尤其近年来，人工智能等新技术推动各类智能设备普及，给个人信息保护带来更多考验。

“一方面，智能设备在使用过程中持续采集使用者的语音、影像等敏感数据信息，若安全防护不足，易被黑客攻击窃取；另一方面，不同设备间的数据互通共享机制如果缺乏规范，也容易导致信息跨平台无序流转，从而形成更加隐蔽的个人信息泄露链条。”何定洁告诉记者。

未成年身份，影响对“开盒”的处理吗？

在社交媒体上检索“开盒”，记者发现：无论是受害者还是施暴者中，都存在着比例惊人的未成年人。

2023年，视频网站哔哩哔哩曾通报一起案例，称有群体在境外平台有组织地煽动用户对站内UP主进行“开盒”，违法者共计40余人，主要活动人员为未成年人。

“未成年人作为网络‘原住民’，往往更加深入地参与各类网络社群，比如‘饭圈’‘二次元’‘游戏圈’等等。”刘晓春告诉记者，“有时这些社群的价值导向容易走偏——只是对某个角色或明星持不同观点，就发生对立引战，‘开盒’成为一种攻击和报复的手段。”

此外，未成年人的法治意识、网络安全意识较薄弱，有时意识不到自身行为的后果，更可能出于宣泄情绪、吸引眼球、炫耀技能等目的参与“开盒”网暴。

“倘若不加以干预整治，会污染整个网络生态，也给未成年人造成深远的负面影响。”刘晓春说。

那么，未成年人身份的特殊性会影响“开盒”的处理与追责吗？

“司法机关通常会综合考虑未成年人的年龄、心理状态、行为动机等因素，采取宽严相济的处理方式，强调教育和引导作用。”何定洁说，但这并不意味着未成年身份就是“挡箭牌”。

对于未成年人的“开盒”行为，倘若构成犯罪，已满16周岁应负刑事责任；若构成违反治安管理处罚法的侮辱、诽谤、威胁人身安全、散布隐私等，已满14周岁即可予以治安处罚。对于不满14周岁的未成年人，应责令其监护人严加管教。造成损害的，监护人要承担民事责任。

朱慧卿作（新华社发）

而当受害者是未成年人时，最高法、最高检、公安部联合发布的《关于依法惩治网络暴力违法犯罪的指导意见》明确指出：对施暴者要“依法从重处罚”。

长期关注这一领域，刘晓春认为，想解决未成年人参与“开盒”问题，需要不同主体协同发力：“学校应开设相关课程、讲座，让孩子们知道‘开盒’是违法的，会侵犯他人合法权益，需要承担法律后果。平台也需要加大管控力度，实施更有效的监测和预警。”

严防“开盒”，如何为信息“上锁”？

非法获取个人信息的门槛一再降低，背后“黑灰产”不断曝光。面对隐蔽性极强的“开盒”威胁，人们不免担忧：如何为自己的个人信息“上锁”？

联合国网络安全与网络犯罪问题高级顾问、北京师范大学法学院博士生导师吴沈括指出：“网络‘开盒’现象蔓延的后果之一，就是对个人信息的正常流转利用产生消极影响，让民众对个人信息相关的产业产生不信任。这需要国家网信部门尽快出手整治。”

目前，国家已采取一系列加强个人隐私信息保护举措。

今年2月，国家网信办依据《中华人民共和国个人信息保护法》《网络数据安全管理条例》《APP违法违规收集使用个人信息行为认定方法》等法律法规，依法集中查处了82款侵害个人信息权益的违法违规APP（含小程序）。5月，中央网信办又通报了15款APP和16款SDK（即软件开发工具包）。

被查处通报的APP涵盖多种类别，包括手机游戏、在线壁纸、医疗健康、教育培训、在线支付、小说影视、在线交友等。

除此之外，今年3月，中央网信办还会同工业和信息化部、公安部、市场监管总局，发布关于开展2025年个人信息保护系列专项行动的公告。

这份公告划出不少监管“重点”：包括智能穿戴产品、智能家居产品、智能学习终端等超范围收集非必要个人信息，公共场所违法违规收集使用人脸识别信息，扫码点餐、出行乘车、扫码充电等线下消费场景强制收集非必要信息等典型情况。

公告还特别提到，要对“通过暗网电报等境外渠道以及境内渠道违规售卖公民个人信息”等违法犯罪行为开展治理。

从根源上消除“开盒”，彻底堵住个人信息泄露的缺口，还有很多工作要做。“相关黑灰产链条经过多年积累，根除起来需要打‘组合拳’。”刘晓春提醒，“不仅国家要完善监管标准、加强执法力度，相关企业也要加强内部组织管理。”

此外，还要做好对公众的教育。吴沈括告诉记者：“‘开盒’发展蔓延，背后有一定社会心理基础——部分人并没有将‘开盒’或‘人肉搜索’当作一种违法行为。”他表示，需要完善法律知识的普及，尤其面向未成年人，做好普法教育与宣传引导。

新媒视点

网络『原住民』需要『守门人』

刘江红 于天歌

近年来，网络上发生了好几起“开盒”风波。所谓“开盒”，可不是“开惊喜盲盒”，而是通过网络信息揭露他人隐私，不仅让受害者“社死”，还对其进行骚扰和恐吓。不同于之前的“人肉搜索”，网络“开盒”背后有一条完整灰色产业链，包括引流获客、技术更新、运营管理等环节。

在已曝光的“开盒者”中，不乏未成年人。作为网络“原住民”和网络文化的重要生产者，他们的动机各异，泄私愤、纯炫技、博眼球，更有甚者从围观看客变成违法帮凶，把“开盒”当成获取群体地位的手段。他们享受着技术赋予的“无所不能”的错觉，却没有明确责任边界，形成了扭曲的价值认同。

我们生活在“大数据时代”，大数据的特点之一在于高度关联。每个人每天在网络空间留下的浏览、下单、评论、点赞等数字轨迹，但凡有不轨之人爬取收集进行关联，就可能拼凑出每个人的爱好、家庭住址、社会关系等隐私信息。“开盒”行为的本质，就是把个人隐私当作商品，把有尊严的人异化为一个个“数据包”展开交易。

在这个过程中，未成年人更容易成为“受害者”和“施暴者”。成为“受害者”，是因为隐私保护意识的缺失，未成年人作为网络“原住民”，更容易在不经意间把个人隐私晒在网上。成为“施暴者”，是因为未成年人法律意识较弱，情绪较不稳定，又具备一定的网络搜索、信息收集能力，容易一言不合就“开盒”。

更有甚者，个别未成年人还将“开盒”作为犯罪牟利的手段。在一起“开盒”案件中，两名未成年人主导的“开盒”团伙竟能形成规模化的犯罪网络。由此看出，“开盒”导致的隐私泄漏、权益侵害，已不是由于单一主体行为失范，而是数据主权缺失及监管滞后带来的系统性隐患。

如今，数字经济带来了巨大的科技创新，也重塑了我们的日常生活和思维方式。每个人不仅是现实世界中有血有肉、有社会关系的人，也成了由各种数据构成的“数字人”。因此，像保护现实生活中的个人隐私一样，必须关注和保护我们在虚拟世界里的那个“数据分身”。尤其是未成年人，更需要社会在其成长过程中为他们保驾护航。

网络“原住民”需要“守门人”，如何当好这个“守门人”？

在短期措施方面，我们需要有针对性地治理对未成年人的“开盒挂人”乱象。密切关注涉未成年人网暴风险，深入排查“校园墙”“留言板”等环节“开盒挂人”问题。阻断传播渠道，督促网站平台深入清理各类违法发布个人信息、诱导网民跟进泄露隐私等信息内容，对存在组织煽动“开盒”、提供“开盒”服务等行为的账号、群组予以关闭或者解散。

从长远看，相关部门需要进一步明确网络“开盒”的法律性质，制定清晰的惩处标准；升级完善个人信息保护措施，严格限制各类平台过度收集和使用用户数据；还需要解决追责中的难题，比如锁定幕后黑手、认定具体行为、评估危害后果等，加强法律惩戒，形成有效震慑。

治理乱象，不仅要关注现象本身的“膝理之患”，更要着眼根本——未成年人的心理健康，从法律普及、道德引导等多方面入手，培养健康向上的用网习惯，涵养积极阳光的上网心态。做到这些，才能从根本上关闭泄露隐私、网络暴力的“盒子”，才能为网络“原住民”打开一片晴空。

（**作者分别为中国传媒大学文化产业管理学院副院长、中国传媒大学文化产业管理学院博士**）

信息链接 ▶▶▶

遭遇“开盒”后，普通人可以怎么做？

● 做好证据保存，为后续维权保留原始材料。

可以截图、录屏保存相关侵权内容，记录发布者和传播者ID、平台、时间、内容等信息，必要时可以委托公证机关进行公证。

● 及时向平台投诉，切断传播链条。

可以依据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》相关规定，要求平台删除侵权、违法内容。

● 向网信办违法和不良信息举报中心（12377）举报或报警处理。还可以向法院提起民事诉讼，主张停止侵害、赔礼道歉、赔偿精神损失，若造成财产损失，如因开盒造成隐私泄露被诈骗，可一并主张赔偿。

日常生活中防止隐私泄露，有哪些做法？

● 向平台、机构提供身份证号、银行卡信息、指纹人脸等敏感信息前，核查其经营资质与相关权限、条款。

● 在使用智能手机时，不点击不明链接、不扫描陌生二维码，不下载来源不明的APP，防止恶意程序窃取通讯录、定位等数据；区分各平台所使用的密码并定期修改。

● 朋友圈、微博等社交平台，避免发布包含身份证号、车牌、门牌号的照片，防止个人信息泄露。

● 从正规渠道，选购正规品牌的智能终端产品。

（**本报记者采访整理**）

银龄触网不迷航，社区筑起“防火墙”

——一位社区工作者的来信

人民日报海外版：

近期贵报刊登的“守护清朗网络空间”系列报道《网上“砖家”谁来管？》，让在社区一线开展工作的我们深有同感。

医疗健康等领域的“伪专业信息”，对老年人来说尤其难以分辨，例如有网络伪专家冒充中医世家传人或三甲医院医生，以“根治糖尿病”“抗癌特效”为噱头，兜售高价“秘方药”。

作为一名社区工作者，也是基层网络清朗行动的观察员，我想结合我们社区组织网络辟谣宣传活动的实践经验，分享社区如何为老年群体编织一张有温度的“谣言防护网”。

首先，必须变“被动辟谣”为“主动防御”。为了构建更完善的谣言防御体系，我所在的社区创新推出了“西楼银发信息员”制度，在3个小区内发展了20余名老年网络志愿者。经过社区培训，这些“银发哨兵”不仅自身具备鉴别能力，更能用方言土语向邻居解读网络套路谣言。例如，71岁的朱姨自编顺口溜，成功化解了社区内30余户老人关于退休高龄老人补助金政策的疑惑。社区同步建立“谣言预警群”，实现了“发现—核实—处置”的2小时响应机制。

其次，社区党委充分发挥党建引领基层治理优势，联合共建单位，定期为社区老年居民开展网络辟谣宣传讲座，讲座内容涉及法律、金融、医疗、教育等领域。共建单位宣讲人通常会采用“以案说法+情景模拟”结合的模式，剖析真实案例，揭示伪专家诈骗套路，现场还原“保健品传销”“投资理财陷阱”“养生伪科学”等高频场景，并提供相应话术帮助老年居民巧妙应对，既强化了大家的防范认知，又提升了实操应对能力，让辟谣宣传真正入脑入心。

守护清朗网络空间，也是守护人与人之间的信任。当我们在社区看到老人们不再为网络谣言疑惑，当老年人的子女欣慰地说“爸妈现在会主动核实链接”，我们更加坚信：只要社会各界携手，定能让银龄一族在数字浪潮中“智享”而不是“迷航”。

天津市河西区桃园街道西楼北里社区党委副书记 **杨哲钧**

2025年7月1日