2025年9月25日 星期四 责任编辑丨何芳芳 版式设计丨李红霞 富阳日报 FUYANG DAILY

从西贝风波看“网络黑社会”

□ 特约评论员 王鋆涛

第十二个国家网络安全宣传周虽已落幕，但“网络安全为人民，网络安全靠人民”这句箴言，仍在公众耳畔回响。近期持续发酵的西贝“预制菜”风波，恰如一面镜子，照出了网络空间的讨论乱象，也让“网络黑社会”的界定与网络讨论的边界问题，成为衍生议题。

9月10日，罗永浩在直播中一句“西贝几乎全是预制菜，还卖得贵”，像一颗石子投入网络湖面，瞬间激起讨论涟漪。消费者关心的是：预制菜的食材从哪来？加工过程是否安全？为何不提前告知？可西贝创始人贾国龙的回应，却跳出了“预制菜透明化”的核心议题，给罗永浩扣上“网络黑社会”的帽子。

罗永浩的吐槽，真的能和“网络黑社会”画等号吗？笔者认为不能。“网络黑社会”从不是个体的随口质疑，而是有组织、有预谋的恶意攻击；不是对行业痛点的揭露，而是为了利益刻意制造混乱。反观西贝风波，即便罗永浩的发声带有个人立场，但其至少戳中了餐饮行业的普遍问题：预制菜信息不透明，消费者知情权被忽视。无数网友跟着讨论“该如何保障预制菜消费权益”，这本身就是正常的公众监督。这种动辄给理性发声者扣恶名的做法，本质上是用“标签暴力”压制讨论，反而比单一的吐槽更接近“网络霸凌”——它堵死了良性沟通的渠道，也让真正的网络黑恶势力，更容易在混乱中隐藏。

值得深思的是，西贝给质疑者贴“黑恶”标签的行为，恰恰暴露出一些主体对“网络黑社会”的认知偏差：似乎只要影响了自身利益，质疑者就是“敌人”，就是“黑势力”。可现实中的网络黑恶势力，从来不是这样的。它们不会针对单一企业的产品问题发声，而是会用“水军”刷屏造谣，用伪造的证据抹黑对手，用“人肉搜索”威胁普通人——就像曾经攻击新东方的密集帖子、伪造万科会议纪要的恶意炒作、定向抹黑同行的舆论攻击，这些有组织的恶行，才是真正的“网络黑社会”。而西贝风波中，消费者对预制菜的追问、对知情权的争取，不过是正常的公民表达，与“黑恶”毫无关联。

随意使用“网络黑社会”标签，不仅会消解了这个概念的严肃性，更可能让公众对“真正的网络黑恶”失去警惕。当大家习惯了“质疑=黑社会”的简单逻辑，反而会忽略那些隐藏在屏幕后的“幽灵”。他们离我们并不遥远：伪造聊天记录诋毁普通网民、用虚假信息撕裂社会共识、刻意煽动群体对立，这些都有它们的痕迹。这些真正的网络黑恶行为，比一句吐槽更具危害性，却可能因为“标签被滥用”，得不到应有的重视。

网络空间需要的不是“标签战”，而是理性的讨论边界；需要警惕的不是对行业痛点的质疑，而是有组织的恶意攻击。这其中，“网络卫士”的作用不可或缺——他们或许是网信、公安部门的执法者，斩断“水军”产业链、打击恶意炒作；或许是坚守理性的博主，用事实厘清讨论边界，避免舆论跑偏。他们的职责从不是维护某家企业的利益，而是守护数字空间的正义，既打击真正的网络黑恶势力，也保护公民正当的发声权利。

个人数据“裸奔” “开盒”狂欢何时休？

□ 裘云珠

当百度副总裁13岁女儿利用“社工库”精准定位孕妇住址，72小时煽动2.3万条网暴信息时，这场由未成年人主导的“开盒”暴行，彻底撕开了数字时代最不堪的隐私伤口。据《2024年数据泄露风险态势报告》显示，当年全年数据泄露事件高达37575起，银行业以6333起位居“泄密冠军”。面对“3000元开盒祖孙三代”的黑色产业链，个人信息保护几成空谈，每个人都可能成为下一张被撕开的“隐私卡片”。

在信息爆炸的时代，高管女儿参与“开盒”并非孤例，个人信息泄露事件依旧层出不穷：《鸣潮》配音演员与玩家互指遭遇“开盒”；杭州周某某等6人为博眼球、非法牟利或取乐，通过境外平台非法收集、买卖并公开800余人的个人信息，浏览量超400万次；家装公司“内鬼”倒卖业主信息、电商平台员工9200万元兜售客户数据……从频繁收到的不明包裹，到精准切入生活的诈骗电话，信息泄露与终端滥用已然形成一条完整的黑色链条。每个人的隐私，都正在看不见的交易市场中被明码标价、悄然流通。

其实，“开盒”之所以猖獗，源于三大症结：技术门槛的断崖式下降、黑色利益链的野蛮生长以及维权困境的现实存在。想让网络信息泄露不再“任性”，破局必须刮骨疗毒。在面对瞬息万变的网络犯罪手段时，法律法规需要保持动态更新，让违法者真正感到“痛”。互联网企业不能只顾收割用户数据红利，却回避数据保护责任。企业则需从源头遏制“内鬼”泄密，绝不能成为违法行为的“帮凶”或“旁观者”。

与此同时，要想刹住“开盒”的恶行，每位网民在享受互联网带来便利的同时，也需主动提升自身的数字素养，在某种程度上阻碍“开盒”恶行。比如不随意授权非必要的隐私权限，定期检查并调整社交媒体的隐私设置，避免在公开平台上过度分享个人信息……这些看似简单的习惯，恰恰是构筑隐私安全的第一道防线，变相提升“开盒”实施门槛。

当云南15岁少年阿英因游戏失利导致父母公司信息遭恶意公开，当孕妇因饭圈争议陷入人肉搜索的漩涡，我们每一个人，都站在数据“裸奔”的悬崖边。这场隐私保卫战没有旁观者——唯有法律真正“长出牙齿”、平台严守底线、企业负起责任，才能遏制“开盒”的野蛮滋生，让数字时代的隐私尊严，不再成为一种奢侈品。毕竟，今天默许“开盒”的泛滥，明天我们每个人就可能成为下一个被精准猎杀的目标。

网络安全周不能“走过场”

□ 李玥珺

9月15日至9月21日的国家网络安全周，本应是提升全民网络安全素养、强化法律认知、紧跟时政热点的关键契机。然而，部分活动却流于形式，让这一重要活动面临“走过场”的质疑，实在令人深思。

宣传形式岂能“困于热闹”。不少地方网络安全周活动看似热闹非凡，实则空洞无物。有的举办大型宣传集市，扫码答题赢小礼品、拍照打卡发朋友圈等互动环节人满为患。参与者大多为小礼品而来，活动结束，网络安全知识便被抛诸脑后。这种形式主义的活动，缺乏对不同群体的精准定位。老年人易遭受网络诈骗，却难在活动中找到针对性讲解；企业员工关注数据安全，活动却未深入实际工作中的操作规范。活动成了主办方的“自嗨”，无法真正走进大众心里。

法律宣贯不能“浮于表面”。网络安全法律是网络空间的“定海神针”，但在网络安全周的法律宣贯中，却存在“浮于表面”的问题。部分活动只是简单宣读条文、播放PPT、发放手册，没有结合实际案例深入剖析。民众对法律的理解停留在文字层面，不知如何运用法律保护自己，也不清楚违法后果。以近期频发的网络个人信息泄露案件为例，犯罪分子通过非法手段获取大量用户信息并进行贩卖。若法律宣贯活动能结合此类案件，详细解读涉及的法律条款、犯罪分子的作案手法以及民众的维权途径，就能让民众深刻认识到法律的重要性。

紧跟热点方能“有的放矢”。网络安全领域日新月异，新威胁、新挑战不断涌现。网络安全周活动应紧跟时政热点，及时回应社会关切。但一些活动却缺乏时效性，仍围绕老生常谈的话题展开，对人工智能安全、区块链安全等热门问题避而不谈。人工智能技术在医疗、金融等领域广泛应用，但也带来了深度伪造、算法歧视等安全隐患。若网络安全周活动能聚焦这些问题，邀请专家深入探讨防范措施，就能引导公众正确认识和使用新技术。

国家网络安全周意义重大，绝不能沦为形式主义的“秀场”。要提升活动实效，各主管部门和基层单位需精心策划，摒弃“为活动而活动”的思维。针对不同群体，设计个性化的宣传内容和方式，如为老年人制作通俗易懂的防诈骗视频，为企业员工开展专业的数据安全培训。在法律宣贯方面，要结合实际案例，让法律条文“活”起来。同时，紧跟时政热点，及时调整活动内容，使活动更具吸引力和针对性。

网络安全是全社会共同的责任，只有摒弃形式主义，注重活动实效，才能让国家网络安全周真正发挥作用，共筑数字安全长城，让我们的网络空间更加安全、稳定、有序。

让7天的关注延续成365天的守护

□ 李晓池

九月下旬，街角那块“共建网络安全，共享网络文明”的展板被轻轻收进仓库。社区群里的推送消息渐渐淡了，日子又回到了熟悉的节奏。可你有没有想过，安全这事，真能像展板一样“挂了就完事”？

其实，我们常犯一个错：把安全周当成了“七天打卡”，以为收了展板、停了群消息，就万事大吉了。可安全哪有“假期”？就像家里装了灭火器，我们不会只在消防演习那天才看一眼，而是天天记得它在哪、怎么用。安全周的真正价值，是把那七天的警醒，变成往后三百六十五天的下意识动作。

问题出在哪？说白了，知识没落到生活里。安全周里，我们听过“别点陌生链接”，但没人教老人“看链接是不是https开头，有没有官方标志”；听过“刷单都是骗局”，却没人拆解“骗子先给你返小钱，再骗大钱”的套路。知识要是只在台上讲，没进我们的手机、没进我们的家门，遇到真事，照样手足无措。更别提责任模糊了：展板是政府挂的，大家容易觉得“这是他们的事”，自己听了课就算交差。可数字世界里，谁不是当事人？点链接的是我们，输密码的是我们，授权App权限的还是我们。安全不是别人的事，是我们自己防线的重要一环。

怎么让七天的热度，变成全年的温度？得从“听”变成“做”，从“知道”变成“习惯”。

比如，别光在安全周发手册，把防骗技巧“种”进日常。社区电梯口贴张提示：“三看识别陌生链接——看前缀、看标识、看内容”，让居民潜移默化；老年活动室放一台“反诈查询机”，遇到可疑链接，扫一下就能核验；给家长发张清单：“教孩子不把密码告诉同学，不乱扫路边二维码”，简单一句提醒，就能守住家庭的安全防线。当安全知识和生活绑在一起，才能成为实用指南。

再比如，安全周的AI诈骗演示为什么受欢迎？因为大家愿意动手试试。那就把这劲头延续下去：社区每月开一次“安全小课堂”，邻居们一起操作反诈App，边学边练；企业别只在安全周搞模拟钓鱼测试，把它变成员工每月的“常规练习”；学校编个安全情景剧，让孩子演一演“骗子怎么骗人”，比听十遍说教都管用。

那块收进仓库的展板，不是安全的句号，而是逗号。它完成了“唤醒”的任务，接下来，该把安全意识悄悄织进日子里：刷到陌生链接多看一眼，App索要权限多想一想，给父母打电话时多问一句“最近有没有收到奇怪消息”。安全周从不承诺七天解决所有问题，它只是轻轻推了我们一把——让我们在日常里，慢慢学会自己走。

网络安全“集体焦虑”怎么破

□ 许张琨琦

在万物互联的今天，网络安全到底意味着什么？它不仅仅关乎技术层面的防护升级，更与我们每个人的日常行为、法律意识以及整个社会的协同治理密不可分。

如今，网络安全成了一种普遍的“集体焦虑”。大家一方面享受着数字技术带来的便利，乐于在朋友圈、短视频中记录和分享生活；另一方面，却对个人信息泄露、网络诈骗等风险表现出习惯性的忽视和淡忘。这种心态很像我们常面临的“管与不管”的两难——既希望环境有序安全，又不愿被规则束缚；既责怪平台管理不严，自己也嫌安全操作繁琐。真正的网络安全，首先要打破这种“依赖心理”，让每一个人都明白：自己不仅是互联网的受益者，也必须是网络安全的守护者。

为什么法律明明越来越多，执行起来却这么难？从《网络安全法》到《个人信息保护法》，相关法律体系正在不断健全，但现实中却常遭遇执行“软无力”。一些企业打着“优化体验”的旗号回避责任，App过度收集个人信息几乎成了默认行规；很多用户为了方便，无奈让渡隐私，权益受损后却又因为维权成本高而选择沉默。更值得注意的是，部分平台把安全建设视为纯粹成本应付了事，而不是做为发展的基石。法律的生命力在于执行，如果缺乏监管，再好的规定也容易变成一纸空文。

近来的AI换脸诈骗、境外网络攻击等事件频频发生，也折射出技术发展带来的伦理挑战。我们在享受算法推荐带来便利的同时，是否意识到自己的视野可能正变得狭窄？我们在欣然使用人脸识别时，是否想过一旦生物信息丢失，后果有多严重？网络安全不仅是技术对抗，更关乎如何在数字时代保持清醒、保护人的主体性。若失去人文价值的引导，技术越先进，我们可能越感到不安。

构建健康的网络生态，首先要建立贯穿一生的网络安全教育，从中小学课堂到职场培训，把公民责任融入整个学习过程。监管也要更有力度，对滥用数据的行为重罚严惩，让违法者真正付出代价。同样重要的是形成“人人参与、共同治理”的网络安全文化——政府健全法律，企业落实责任，公民提高防范。网络安全不是临时任务，而是一场需要长期投入的全民行动。它的最终目标是让安全意识化作我们数字生活的本能，让法律和规则成为自然而然的行为准则。

只有每个参与者都敬畏规则、承担职责，我们才能在技术日益发展的今天，共同筑牢网络安全的坚固防线。

春江时评

九月短评

真正的网络安全意识提升，不应是“一刀切”的宣传模式，而需更注重“量身定制”。面向老年人，不妨将社区活动室转化为“安全课堂”，通过“模拟接听疑似诈骗电话”的互动形式，帮助他们建立“子女来电后回拨核实”的习惯；针对留守儿童的安全课，可尝试制作动画短片，将“不随便点链接”转化为“远离带小红点的奇怪按钮”这类更具象的提醒。国家网络安全周的意义，在于织密一张“不让任何人掉队的安全网”。当我们的安全科普内容能让老人轻松理解、让孩子清晰记忆，当法律的保护作用能真正延伸到数字世界里的“弱势群体”，这样的网络安全，才更贴近“全民安全”的初衷。

——吴佳（胥口镇人民政府）

网络安全的核心是攻防两端的博弈。传统的网络攻击多以窃取数据、破坏系统为目标，信息爆炸的当下时代，愈来愈频繁出现的AI换脸、网络“开盒”、App违规收集信息、网络谣言捏造等问题，宣告着传统网络攻击手段正迎来一次大跃迁。为应对网络安全质变的威胁，需要更全面的防守策略：政府应以技术对抗技术，研发检测工具并强化平台监管；相关部门需完善法规，依法亮剑并严厉打击黑产；公众要提升自身安全素养，保持理性思维并坚守道德底线。通过构建“技术+法律+人文”三重立体防御体系，共建安全网络空间。

——潘晨钰（富春街道秋丰社区）

AI与网络安全深度融合是必然现状，政府层面需加强对AI技术应用的监管，制定明确的法律法规，规范AI技术的开发流程与使用场景，对利用AI实施网络犯罪的行为依法严厉惩处，形成监管威慑。在全国网络安全标准化技术委员会公布28项网络安全国家标准立项清单中，入选的《网络安全技术人工智能技术涉及未成年人应用安全指南》，就是对构建数据合规、算法安全、内容治理的完整治理技术体系的实践。个人更要主动学习网络安全知识，提升对AI虚假信息的辨别能力，在网络活动中谨慎对待陌生信息，避免泄露个人隐私数据。

——章佳敏（常绿镇人民政府）

今年国家先后出台了《关键信息基础设施安全保护条例》实施细则和《网络安全事件报告管理办法》，进一步完善了我国网络安全制度，健全了高效联动的国家网络安全防御体系。当前，在GDP中数字经济比重突破了45%，在能源、金融、交通等领域，关键信息基础设施高度依赖网络运行，一旦遭到攻击，可能引发系统性风险，危害巨大。这就需要政府、企业、社会协同发力，共同维护网络安全。网络安全的公众意识必须要加强，加大网络安全宣传周的宣传广度，在更大范围内进行宣传。同时要加强行业自律，相关行业组织要推动企业积极承担网络安全责任。

——汪菲（区交通集团）

当前，人工智能、大数据等新技术快速融入社会发展各领域，在为经济社会发展注入强劲动能的同时，也给政务安全、数据治理、个人信息保护等工作带来严峻挑战。网络安全不是孤立静态的，维护网络安全是一项整体、动态、开放的系统工程，一方面依赖管理部门的科学布局与严格监管，另一方面也离不开每一位网民的主动参与。网络空间无边界，但安全防护有底线。只有将全社会的力量拧成一股绳，真正构建起齐抓共管、共建共治的良好格局，才能有效防范化解网络安全风险，汇聚起维护网络安全的强大合力，为数字时代的健康发展保驾护航。

——沈致远（胥口镇人民政府）