“开盒”风波又起 数据泄露何时休

► 本报记者 李洋

近日，某大厂就“高管女儿‘开盒’”事件发布声明。声明着重强调，“开盒”信息来自于海外的社工库——一个通过非法手段收集个人隐私信息的数据库。

“开盒”一词也称“人肉开盒”，为网络黑话，是指通过非法手段搜集他人隐私信息，包括但不限于姓名、电话、身份证号码、家庭住址、工作地点、银行流水、上网、开房记录、名下财产等敏感信息，并将这些信息公开在网络上，引发网民对被“开盒”者进行网暴。

数据时代，个人信息难免会在网络空间留下痕迹，由此带来信息泄露风险。近年来，“一言不合就‘开盒’”的现象在青年社交群体中并不鲜见，这里甚至不乏未成年人的身影。针对“开盒”造成的严重后果，应该从哪些方面采取措施加以遏制？

AI制图：晁毓山

黑色产业链浮出水面

作为网络暴力违法犯罪行为的一种，“开盒”背后暗藏着一条巨大的隐私贩卖黑色产业链。

“‘人肉开盒’已拥有完整的产业链，分工明确、利益环环相扣，严重侵犯了公民的个人信息安全和合法权益。”康德智库专家、上海市光明律师事务所合伙人陆艳对记者分析说，首先，在产业上游，黑客通过拖库、撞库等手段攻击网站和系统，窃取大量用户数据；同时，部分行业“内鬼”如银行职员、电信员工等，利用职务之便将掌握的用户隐私信息非法出售，为黑产业提供源头数据。其次，在产业中游，社工库运营者将分散的数据进行整合、分析和归档，形成庞大的个人信息数据库，并通过加密聊天软件如Telegram等隐蔽渠道，向有需求者提供付费查询服务，价格因信息类型和敏感程度不同而有所差异，例如，户籍信息查询价格约为50元，而实时定位信息则高达2000元左右。最后，在产业下游，不法分子利用获取的个人信息，实施网络暴力、诈骗或商业间谍活动，从而实现“数据—流量—资金”的非法闭环，从中获取巨额利益。

“人肉开盒”触犯法律法规会获什么罪名？北京市京师律师事务所律师卢鼎亮对记者说，“人肉开盒”可能会涉及侵犯公民个人信息罪、非法获取计算机信息系统数据罪等；如果“开盒”后还有对受害者进行侮辱、诽谤、威胁等行为，可能构成侮辱罪、诽谤罪、寻衅滋事罪等；搭建社工库并售卖信息的行为，涉嫌触犯侵犯公民个人信息罪；黑客攻击网站获取数据的行为涉及破坏计算机信息系统罪、非法侵入计算机信息系统罪等。

如何追溯跨国犯罪链条

上述事件中提到的“社工库”，其全称是“社会工程学数据库”，是犯罪人通过攻击网站、欺诈用户等手段获取大量个人隐私数据再整合分析、集中归档形成的数据库。

搜索某海外社工库不难发现，网页中充斥着各种明码标价的查询服务，不同查询类型价格不同，用户可以搜到开房信息、微信记录、家庭成员、工作单位、居住地址等各种隐私信息。

如何追溯海外社工库跨国犯罪链条？陆艳表示，当境外主体侵犯境内法人或自然人信息且行为涉嫌犯罪时，依据我国刑法保护性原则，我国法律同样具有管辖权。当前，境外信息泄露问题猖獗，在此情形下，公民若发现此类侵权行为，可向公安机关报案。公安机关在受理后能够借助国际司法协助等多种途径展开调查。然而，由于我国警察在境外并不具备执法权，调查工作主要依赖司法协助推进，这使得公民权益保护在实际操作过程中面临诸多困难。

“追溯跨国犯罪链条，应当加强国际执法合作，各国警方和相关机构共享情报信息，追踪犯罪嫌疑人的网络活动轨迹、资金流向等。利用技术手段，加强技术反制措施，以切断犯罪链条的传播途径。同时，加强对跨境网络服务提供商的监管和合作，共同打击跨国网络犯罪。”卢鼎亮表示。

数据泄露呈现新特征

当下，数据泄露呈现一些新特征。

一是攻击方式更加隐蔽和复杂。攻击者通过修改数据，使AI模型产生错误的预测。例如，在图像识别任务中，攻击者可以在图像中添加微小的扰动，使模型将其识别为其他类别。攻击者利用模型输出推断训练数据的信息。例如，在医疗诊断任务中，攻击者可以利用模型输出的预测结果，推断患者的疾病信息或个人信息。攻击者通过分析模型的输出或更新前后的模型差异，推断出训练数据中是否存在特定样本。

二是数据泄露范围更广。由于人工智能技术的全球化应用，数据可能在不同国家和地区之间流动，增加了数据泄露的风险。例如，生成式人工智能的不当使用可能导致跨境数据泄露。AI大模型可以收集用户的语音、手势、表情等多模态数据，这些数据的泄露风险更高。

三是数据泄露的源头更多样。员工在使用生成式AI时可能在无意中输入包含敏感信息的内容，导致企业敏感信息泄露。当AI大模型与第三方应用集成时，可能会绕过应用的安全机制，导致数据泄露。

“这需要采取多种手段来降低信息泄露带来的风险。”萨摩耶云科技集团首席经济学家郑磊建议，在技术手段方面，对敏感数据进行加密处理，同时采用匿名化和去标识化技术，防止从模型结果中反推个人数据；在模型训练时加入噪声，保护训练数据的隐私；结合生物特征识别和其他验证方法，提供更加安全可靠的身份确认手段；利用AI技术快速隔离受影响系统，防止数据泄露进一步扩散。在管理手段方面，扩展数据治理框架，包括人工智能处理数据的指导方针，监控意外的跨境数据传输；合理限制AI系统对数据的访问权限，制定数据备份和恢复计划；定期进行安全审计以检测系统中的安全漏洞，对AI系统的行为和影响进行有效监督。

“尤其是在人工智能时代，数据泄露呈现出规模更大、速度更快、隐蔽性更强、关联性更高及连锁反应更广的特点。”陆艳提醒，为降低信息泄露风险，对个人而言，应谨慎处理敏感信息，如销毁含个人数据的纸质文件，避免在社交平台暴露身份证号码及定位细节，还应优化账户安全，如使用高强度密码、定期修改密码等，警惕网络钓鱼攻击（不点击陌生链接、核实发件人身份）。

“针对网络暴力行为，还需建立长效监管机制，提升执法威慑力。加强公安、网信、通信管理等部门的协同配合。通过多部门协同，合力打击网络暴力行为及背后的黑产链条，重点打击数据贩卖、代‘开盒’等灰色产业，净化网络生态。”陆艳说。

《人脸识别技术应用安全管理办法》6月施行

本报讯（记者 李洋） 近日，国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》（以下简称《办法》），自2025年6月1日起施行。

《办法》规定，应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行个人信息保护义务，承担社会责任，不得危害国家安全、损害公共利益、侵害个人合法权益。

《办法》进一步明确了应用人脸识别技术处理人脸信息的规则。

一是应当具有特定的目的和充分的必要性，采取对个人权益影响最小的方式，并实施严格保护措施。二是应当履行告知义务。三是基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。基于个人同意处理不满14周岁未成年人人脸信息的，应当取得未成年人的父母或者其他监护人的同意。四是除法律、行政法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。除法律、行政法规另有规定外，人脸信息的保存期限不得超过实现处理目的所必需的最短时间。五是应当事前进行个人信息保护影响评估，并对处理情况进行记录。

《办法》还明确了人脸识别技术应用安全规范。

一是实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。国家另有规定的，从其规定。二是应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道实施。三是任何组织和个人不得以办理业务、提升服务质量等为由，误导、欺诈、胁迫个人接受人脸识别技术验证个人身份。四是在公共场所安装人脸识别设备，应当为维护公共安全所必需，依法合理确定人脸信息采集区域，并设置显著提示标识。任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。五是人脸识别技术应用系统应当采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。

国家互联网信息办公室有关负责人表示，《办法》坚持发展与安全并重，妥善处理促进创新和依法治理之间的关系，在保护个人信息权益的同时鼓励人脸识别技术的应用和创新。《办法》第二条规定，“在中华人民共和国境内应用人脸识别技术处理人脸信息的活动，适用本办法。在中华人民共和国境内为从事人脸识别技术研发、算法训练活动应用人脸识别技术处理人脸信息的，不适用本办法的规定。”为开展人脸识别技术的攻关研究和应用创新预留空间，有利于推动相关产业安全健康发展。

《办法》规定，个人信息处理者应当在应用人脸识别技术处理的人脸信息存储数量达到10万人之日起30个工作日内向所在地省级以上网信部门履行备案手续。网信部门会同公安机关和其他履行个人信息保护职责的部门，建立健全信息共享和通报工作机制，协同开展相关工作。