警惕“暗网”卖密

□秉 泽

DOI:10.19407/j.cnki.cn11-2785/d.2020.05.015

据公安部通报，2019年，北京公安机关抓获利用“撞库”等黑客技术窃取境内外电商数据库、并通过“暗网”出售获利的犯罪嫌疑人3名；江苏公安机关抓获在“暗网”上贩卖南京1400余万条居民社保数据的犯罪嫌疑人3名；海南公安机关抓获在“暗网”上贩卖9万余条学生数据的犯罪嫌疑人2名。肆无忌惮出售公民个人信息的“暗网”，再次进入公众视野。

所谓“暗网”，是与“明网”相对的互联网部分。“明网”指的是可以被传统搜索引擎（比如百度）索引到页面的集合，而“暗网”则是隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权等才能登录。“暗网”深不可测，如果说“明网”是露出水面的冰山一角，而“暗网”则是深藏在水面之下的冰山。

“暗网”最大的特点是完全匿名，将你与现实世界里的身份彻底分离。换言之，除非你愿意，否则你在“暗网”上所做的任何事情都不涉及你在现实世界里的身份和生活，就像早期互联网那样，“没有人知道网络另一端是人还是狗”。正是由于“暗网”的这一特点，滋生了大量以网络为勾连工具的各类违法犯罪，比如买卖枪支弹药、毒品、公民个人信息，提供黑客工具、传授黑客技术教程，制作贩卖淫秽物品等。特别是近年来，通过“暗网”售卖公民个人信息日益猖獗。比如，2018年8月，华住集团旗下连锁酒店5亿条用户信息泄露，卖家在“暗网”上以8个比特币的价格打包售卖。

其实，“暗网”也给我国的国家秘密保护带来新挑战。一是“暗网”上攻击中国特色社会主义制度的反动文章非常多，一些理想信念弱化、政治立场不坚定的涉密人员容易被敌对势力洗脑、策反，甚至主动勾连卖密。二是由于“暗网”的服务器地址和数据传输通常是“隐身”的，数据被密码层层保护，主要支付手段比特币也是完全匿名的，可以绕过传统银行业务渠道进行资金往来，这意味着执法部门对“暗网”卖密的监管难度极大。三是“暗网”最早由美国海军研究实验室立项研究，曾经被情报机构用作情报人员秘密传送情报的渠道，后来军方声称退出交给民间非营利组织运营，但实际上是否完全退出不得而知。对此，我们要保持足够的警惕。

“暗网”卖密虽然隐蔽，但却不能成为法外之地和“避罪天堂”，治理“暗网”卖密迫在眉睫。首先，要加快制定个人信息保护法，全面落实《网络安全法》，严控公民个人信息的泄露源头，重拳打击“撞库”、假身份证、黑电话卡、虚假ID、假冒银行账号等网络黑灰产业。其次，要将“暗网”卖密的社会危害性纳入保密宣传教育内容，讲清“暗网”间谍工具的本质，不断提高公民和涉密人员对“暗网”卖密的警觉意识，自觉规范上网行为。最后，要加强政府与企业技术合作，组织展开“暗网”治理技术专项攻关研究，探索阻断、监控“暗网”的新方法，尽快提升适应我国网络空间治理需求的“暗网”管控技术能力，持续通过技术手段追踪和对抗来自“暗网”的威胁，严厉打击“暗网”卖密行为。

责任编辑／李 杰