

数据黑市交易大起底： 专家估计市场规模超1500亿元 “料商”称“一切需求皆可爬”

本报记者 刘琪
见习记者 杨洁

“出全球数据”“无上限收数据”——言狂意妄的数据黑市“料商”，正持续受到监管的严厉打击。

1月19日，国家发展改革委等九部门联合发布《关于推动平台经济规范健康持续发展的若干意见》，明确严厉打击平台企业超范围收集个人信息、超权限调用个人信息等违法行为。从严控非必要采集数据行为，依法依规打击黑市数据交易、大数据杀熟等数据滥用行为。

这是时隔一周政策再次强调打击数据黑市——1月12日正式发布的《“十四五”数字经济发展规划》提出，严厉打击数据黑市交易，营造安全有序的市场环境。

业界专家在接受《证券日报》记者采访时测算，我国数据黑市交易的市场规模已经超过1500亿元。数据在黑市中价值几何、如何流转运作……《证券日报》记者通过多日深入调查，揭开数据黑市产业链的一角。

数据被明码标价售卖

近年来，数据泄露事件时有发生。在监管持续打击下，数据黑市交易行为有所收敛。近期，《证券日报》记者用业内“黑话”诸如“买料（买数据）”“料商（贩卖数据的人）”等在网上搜索发现，相关QQ群、贴吧等的活跃度都有所降低，部分关键词被屏蔽。而此前，该类信息可以在网上检索获得。

然而，数据黑市交易并未真正销声匿迹，而是转入更“隐秘的角落”。记者通过特殊关键词搜索找到了几个相关QQ群，通过多天“蹲点”发现，有“料商”喊出了“出全球数据”“无上限收数据”的口号，甚至有从业者表示，“只要在网页上看到的都可以批量爬”“一切需求皆可爬”。



一系列法律法规出台落地 进一步维护数据安全

2021

- 《中华人民共和国个人信息保护法》
- 《征信业务管理办法》
- 《常见类型移动互联网应用程序必要个人信息范围规定》
- 《中华人民共和国数据安全法》
- 《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
- 《网络数据安全管理条例（征求意见稿）》

例如，一位自称“料商”的网友发消息称，“每天更新一手固话老人资源、股民、医疗、电信网、博彩、信用卡、网贷、医生、教师、海外留学生、海外华侨、宝妈、硕士研究生、医护、保险单、车主、购物等数据。”为试探其数据真实性，记者以买家身份提出测试，但对方十分谨慎地表示“测试的免费”。

记者观察发现，这些QQ群大多打着数据“交流”“学习”的名义，实则做着数据“黑色交易”。例如，不少群里都会发布“出一手精准料，长期合作”“高质量欧盟数据、美国数据，需要联系”等消息。同时，买方也较为活跃，可以经常看到“收无风险邮箱”“无限收信用卡数据”“大量收人脸密正”“谁能采集国际邮箱数据”等消息。

在多数人眼里，数据的经济价值难以明确量化。不过，在数据黑市里，数据却被“明码标价”。比如，在某QQ群里有人发布消息称，“爬外卖App商家数据的捞一个，报价为3分/条，一次性收北京地区全部外卖店铺。”

在记者调查过程中，一位网友小雷（化名）称，自己可精准获得数据资源，并主动添加记者为好友询问是否需要。对于记者“想要北京地区妈妈群体的电话号码数据”的需求，小雷表示，“现成的数据没有，得现爬，0.1元/条，绝对保真。”并发来一张爬数据的网站截图。谈及是否有家庭地址数据，小雷称，“可以有，0.3元/条”，最快两天内可以搞定。

值得注意的是，除了QQ群，境外加密聊天软件也成为数据黑市交易的联络平台。例如，通讯软件Telegram因提供用户匿名、信息端对端加密、聊天信息定时销毁、“阅后即焚”等功

能，被大量“料商”所采用。

《证券日报》记者通过微信添加了一位“料商”小九（化名），对方十分谨慎，一直使用暗语交流。在得知记者想帮公司买手机号做推广后，小九发了一个“飞机”的表情符号，而该表情指的就是Telegram。随后，记者请国外的朋友下载Telegram与小九交流，但对方警惕性极高，仍一直使用暗语，在发现记者的朋友听不懂暗语后，便不再回复任何信息。

黑市数据从何而来？

黑市交易的数据到底从何而来？记者了解到，目前在网络黑平台流转的数据，来源可以大概归纳为“内鬼”泄露和外部攻击两大类。

所谓的“内鬼”泄露，即部分公司或信息拥有者的内部人员，与不法分子勾结泄露数据，这也是目前数据泄露的主要渠道。原点安全业务拓展总监张乃乾告诉记者，“内鬼作祟”导致的数据信息泄露可以占到85%，这主要涉及内部管理问题。

广州白云法院于2021年4月份公布的一起裁决，就揭露了“内鬼”泄露数据的“升级版”。自2020年6月份起，蒋某、巫某、彭某、王某、刘某在广州市尖峰路某公寓A1115房，由蒋某担任老板，向他人购买某招聘网站的账号，由刘某、王某使用上述账号在该网站发布大量虚假信息收集应聘者的公民个人信息，再由蒋某、巫某、彭某将收集的信息贩卖牟利。蒋某等人非法获取、销售含姓名和电话号码的公民个人信息数量合计42790条。

而外部攻击，则是指黑客攻击或渗透。记者在数据交易QQ群里也注意到，不少人发布“接渗透”的消息。对此，张乃乾表示，所谓“渗透”，是专业的网络安全术语，不法分子通过非法手段将病毒植入系统中，从而窃取数据。

针对黑客攻击的手段，360数科知微实验室安全专家对《证券日报》表示，一般黑客会通过攻击企业的相关后台、数据库等获取数据，这种方式有时也被黑产从业者称为“爬虫”，但并非通常意义上的“爬虫”。此类数据价格不定，单条最高能卖到15元，不过，真假混杂，大部分为虚假或伪造信息。

“当前黑市交易的短信和SDK（软件开发工具包）数据，因信息真实性较高、质量较好，是黑市流转的主流数据，在黑产高质量数据类型中分别占比67%、22%，尤其是短信类数据，在黑市最‘吃香’。”360数科知微实验室安全专家表示，短信类数据的主要泄露源头为各类不合规或管理不规范的代理商平台，泄露途径包括平台被黑客攻击、渗透或内部泄露等。

“黑市”规模估计已超1500亿元

虽然单条数据看似价格便宜，但据《证券日报》记者了解，数据非法交易已经发展出一条成熟的产业链条，在数据获取、加工、贩卖、流通等各环节都拥有详细的团队分工和各类自动化工具，规模较为庞大。

据360数科知微实验室安全专家介绍，在获取环节，产业链中存在不少规模化运作的数据提供公司，主要贩卖DPI、SDK、微信好友等信息，他们拥有自己的官网，有至少5个客户群组、1万个以上账号关注；在贩卖环节，数据贩商会开发专门的后台软件，用于各下游代理商下载相关数据。

正义网于2021年12月份公布的一则消息，就揭露了这条黑色产业链的冰山一角。2019年，田某在通过“暗网”购买了其他黑客非法获取的某科技公司账户数据库后，不断完善该数据库，再通过“暗网”以加密通讯工具联络、比特币结算的方式多次贩卖牟利。据悉，该数据库包含公民个人信息6亿余组。

公安部近期公布的一批2021年侵犯个人信息典型案例，也揭露了不法分子从数据获取到出售获利的全流程。其中一个案例显示，犯罪嫌疑人何某利用与相关单位、企业建设信息系统之机，非法获取医疗、出行、快递等公民个人信息数十亿条，搭建对外提供非法查询服务的数据库，通过“暗网”发布广告招揽客户，出售牟取不法利益。

数据黑产不仅有一条自己的完整产业链，还常常作为其他黑产的上游。

“拥有身份信息的数据是黑市买卖的目标，而数据黑市的形成主要是因为个人隐私信息蕴藏着巨大的价值，包括个人的喜好信息、社会关系等。”工信部信息通信经济专家委员会委员、中南财经政法大学数字经济研究院执行院长盘和林在接受《证券日报》记者表示，通过对个人隐私和隐私的解读，既可以实现精准营销，也可以针对用户个体进行更加精准的诈骗。

对于当前数据黑市的规模，观研天下首席研究员方孙维对《证券日报》记者表示，根据统计，2017年我国数据黑市黑产人员规模就已经达到150万人，虽然国内出台了相关政策严厉打击数据黑市，每年都有大量违法人员被抓捕，但由于进入门槛低、收入可观，其规模仍较大，估

1月19日，发改委等九部门联合发布
《关于推动平台经济规范健康持续发展的若干意见》

“依法依规打击黑市数据交易
大数据杀熟等数据滥用行为”

计2021年我国数据黑市黑产人员规模接近200万人，相关产业主要集中在我国西南地区，尤其是缅甸和我国云南交界处。

“随着近年来我国互联网渗透率越来越高，网络流量不断增长，尤其是以智能手机为代表的移动互联网数据流量保持高速增长，2021年我国移动互联网流量已经超过2000亿GB，同比增长30%以上。数据流量的不断增长，也加速了数据黑产的规模扩张，由此估计2021年我国数据黑市交易的市场规模已经超过1500亿元。”方孙维表示。

数据黑市交易为何屡禁不止？

在无锡数字经济研究院执行院长吴琦看来，数据黑市通过“内鬼”、网络技术、黑客等多种渠道完成数据流入、进行不法交易，技术丰富、途径多变，给执法部门的监管带来了巨大困难。

实际上，打击数据黑市交易，两个核心问题就是个人信息保护与数据安全。围绕这两个问题，我国不断完善相关法律法规，最早可追溯到2013年的《征信业管理条例》《电信和互联网用户个人信息保护规定》，此后陆续有《中华人民共和国网络安全法》《中华人民共和国电子商务法》《App违法违规收集使用个人信息行为认定方法》等。

在刚刚过去的2021年，我国相继颁布、施行多项相关法律法规。从年初施行的《民法典》到年底的《中华人民共和国个人信息保护法》，其间还有《征信业务管理办法》《常见类型移动互联网应用程序必要个人信息范围规定》《中华人民共和国数据安全法》《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》等数部法律法规。此外，还有《网络数据安全管理条例（征求意见稿）》。

北京市京师律师事务所律师孟博对《证券日报》记者直言，非法数据交易的犯罪成本低、获益高，是数据黑市交易屡禁不止的一个重要原因。因此，从司法角度而言，要依照《中华人民共和国刑法》相关规定，加大对非法获取、非法提供、非法买卖公民个人信息等犯罪行为的打击力度，提升犯罪分子的犯罪成本，形成有效震慑。

业界：对合法数据需求建立渠道

应该如何有效防范数据泄露？360数科知微实验室安全专家表示，“由于数据流通使用涉及多环节、多合作机构，企业需要有效落实法律相关要求，在注重自身数据安全管理的同时，也要把控好第三方合作和管理，完善数据全链路监控和管理体系，积极与监管机构、公安等部门合作，打击治理数据黑灰产。”

从企业层面来说，上海申伦律师事务所律师夏海龙在接受《证券日报》记者采访时表示，企业可制定更严格的数据管理制度、对涉嫌犯罪的员工及时移送司法、采取更高级别的技术保护措施等，避免数据泄露。

孟博表示，电信业务经营者、互联网信息服务提供者等应当严格遵守相关法律法规的规定，切实落实主体责任，对所收集的用户信息严格保密，并建立健全用户信息保护制度。

值得一提的是，多家互联网企业已采取实际行动履行信息保护义务。去年7月6日，阿里巴巴开放平台发布《依法加强消费者订单中敏感信息保护的公告》称，将启动订单处理链路的消费者敏感信息保护方案，对涉及消费者个人敏感信息采取加密、去标识化等安全技术措施；随后在7月9日，京东发布《JD用户订单隐私安全方案》，京东商家开放平台将对订单中的手机号和座机号进行脱敏。

对于普通用户而言，为防范平台侧的数据泄露，360数科知微实验室安全专家建议，需要牢记密码安全三原则：一是密码需要包含字母、数字和符号；二是避免多账号使用同一密码；三是定期更换密码。另外，为防范电信诈骗，下载App和访问网站时要认准官方渠道，不要误点可疑链接和不明来源的二维码。

为进一步杜绝数据的黑市交易，广东格林律师事务所合伙人封芸律师在接受《证券日报》



记者采访时表示，从法律层面来看，首先，要加强个人法律意识。通过立法与普法的方式，树立公民对个人、数据安全等的保护意识。其次，加强对接触、管理电子数据的第三方的监管，App、商家及相关管理部门应当合法合理的取得电子数据，减少不必要个人信息电子数据的采集；同时，第三方有责任和义务管理好采集的电子数据，包括从技术、制度及管理等方面完善数据安全系统。此外，从政府职责来看，要持续加强相关立法、严格执法等。

盘和林则从另一个角度给出了建议，在他看来，打击数据黑市，不仅要加强对非法数据和个人隐私信息获取行为的打击，也要对合法数据需求建立渠道，并强化监管。

安全服务需求快速增长

2021年11月30日，工信部印发的《“十四五”大数据产业发展规划》指出，“十三五”时期我国大数据产业取得了重要突破，但仍然存在一些制约因素。其中包括“安全机制不完善，数据安全产业支撑能力不足，敏感数据泄露、违法跨境数据流动等隐患依然存在”。同时，文件还明确了“十四五”时期六大任务，其中之一是“筑牢数据安全保障防线”。

1月12日正式发布的《“十四五”数字经济发展规划》进一步提出，“建立健全数据安全治理体系，研究完善行业数据安全治理政策”，同时要“进一步强化个人信息保护，规范身份信息、隐私信息、生物特征信息的采集、传输和使用，加强对收集使用个人信息的安

全监管能力”。

有机构预计，我国数据安全市场规模有望在2023年达到97.5亿元。盘和林认为，在此背景下，数据收集、数据处理（涉及清洗、打包、脱敏等）、数据使用（AI和数据分析）以及数据安全公司等，将在未来有更好的发展机遇。

“数据备份、加密、访问控制、密码等基础数据安全产品的需求有望持续提升，相关领域上市公司或将迎来下游需求的快速增长。”方孙维表示。

目前A股市场上已有不少网络安全相关上市公司，包括深信服、安恒信息、奇安信、绿盟科技、启明星辰、美亚柏科、拓尔思等。

《证券日报》记者以投资者身份与美亚柏科投资者业务部门工作人员进行交流，对方表示，公司有专门聚焦数据安全研究的业务，一方面，主要布局央企、国企、政府单位的数据安全，进行数据安全防护；另一方面，将数据安全作为重点完善的方向，着力于将大数据和人工智能技术应用用于为更多行政执法部门开展网络空间社会治理提供产品和服务。

安恒信息近期也在投资者互动平台上表示，数据安全是保障信息技术应用稳定发展的前提和关键，是公司布局的战略方向之一，目前公司通过智能化管理平台，在技术层面实现了风险核查能力、数据梳理能力、数据保护能力以及数据威胁监控预警能力等四大核心能力的建设，在业务层面，实现对数据采集、传输、存储、处理、交换、销毁等全生命周期的管理。

吴琦建议，在数据要素市场建立健全的过程中，数据安全及数据治理公司应当抓住机会，结合政策，探索发展出一条安全可靠的数据交易机制。

