1800万条数据被爬取，检察机关还原事实真相，严惩侵害企业数据安全犯罪，并通过法庭教育让相关行业从业者了解数据领域没有“法外之地”——

合法授权不等于无限授权

通讯员 阮婷

在数字经济蓬勃发展的时代背景下，网络与数据安全已成为护航高质量发展的关键屏障。面对公众不断增长的网络安全防护需求和日益复杂的犯罪手法，检察机关如何以高质效履职有力打击危害计算机信息网络犯罪？

因势而动，顺势而为。近日，上海市静安区检察院办理了一起非法获取计算机信息系统数据案，检察机关充分运用调查核实权，通过自行补充侦查，强化技术证据审查等方式，全面查清犯罪事实，准确适用法律，及时挽回被害单位损失，为网络强国、数字中国建设提供有力法治保障。

从电子数据中拼出犯罪链条

A公司成立于2018年，是一家提供信息网络服务的技术公司，自主研发一款P系统用于整合分析相关数据，并以收费方式提供服务。2023年6月，A公司监测系统突发异常，P系统在48小时内遭高频访问6万余次，约有1000余万条某专业领域相关重要数据被非法下载。A公司系统被迫关停，数据服务业务陷入瘫痪。7月，A公司报案。

经立案侦查，公安机关发现Y公司存在重大作案嫌疑。同年8月25日，该公司负责人杨某主动投案。然而，其到案后拒不供述，辩称“只是用爬虫提高下载速度，账号是合作方给的，不知道数据要付费”。

鉴于该案涉及计算机信息系统犯罪，专业性强，静安区检察院依法介入。面对犯罪嫌疑人的“技术性辩解”，检察官围绕行为人客观上有无使用非法技术手段、主观上对数据权属是否存在明知等关键点，厘清犯罪构成，同时引导公安机关侦查人员及时恢复杨某微信、通话等电子数据，固定、提取后台“查询日志”等，量化被害单位损失。

经初步侦查查明，犯罪嫌疑单位Y公司成立于2019年，犯罪嫌疑人杨某系公司法定代表人。2023年5月，Y公司中标了M公司某规划项目，合同总价为25万元。在开展项目合作期间，M公司向A公司借用P系统临时账号，供Y公司查询上述项目的相关数据。岂料，杨某在使用临时账号期间，发现该系统某些专业领域数据全面、细致，资源蕴含巨大经济价值，竟指示公司员工非法使用爬虫软件抓取、下载大量数据。经鉴定，爬取数据量高达1800余万条。

揭穿“有授权即合法”的辩解

2024年6月3日，案件被移送至静安区检察院审查起诉。检察官在审查电子数据时，发现这样一些异常对话：“感觉要把他们的服务器搞崩了……我们抓取也很温柔了，没有多线程抓……我就担心他们发现我们使用数据量太多。”

更关键的是，检察官在审查Y公司员工孙某与杨某的聊天记录时发现，早在2022年7月，杨某就曾与A公司有过接触，明知A公司系统的商业性质、也明知系统数据属于具有高度市场价值的商业资产。

然而，仅查清杨某主观明知这一事实还远远不够。面对检察官的讯问，杨某一再辩解称，“已由A公司授权”“账号有导出功能”“用爬虫技术只是提速”。

有授权等于合法？A公司提供账号的行为，是否意味着全权授权M公司可以随意查询、下载系统内全部数据？基于合作业务需要，M公司将临时账号交由杨某使用，是否意味着杨某可以随意查询、下载系统内全部数据？一个个问题在检察官心中升起。

“临时账号的权限范围是什么？A公司系统是否设置了反爬措施？合法授权不等于无限授权，查明技术手段是否‘越界’才是证明非法获取的关键。”检察官介绍说。

为此，检察官开展自行补充侦查，通过询问第三方技术公司工作人员、依法询问被害单位业务负责人、调取被害单位提供的书证、充分听取第三方鉴定机构的意见等，查明了关键两点事实：一是权限限制，A公司提供的临时账号明确设限，如对登录时间、查询条数、单次导出数据量等都有要求，但Y公司却在48小时内高频访问，爬取1800余万条数据，远超临时账号的授权范围；二是技术突破，A公司通过密码验证、下载范围、条数速度等对系统数据设置反爬措施，即使是付费用户也仅能获取页面数据，而杨某公司利用爬虫软件绕过防护，直接窃取系统底层原始数据。

检察官指出，杨某看似通过合法渠道实现了账号登录，却在使用账号过程中，以技术手段突破授权边界，利用爬虫软件将导出权限提升覆盖至对全库底层原始数据的获取，该行为严重违背被害单位的授权意志、范围，本质上是超越授权非法获取信息数据。

检察官发表公诉意见。

是否已达“情节严重”的追诉标准

当犯罪手法被层层揭开，检察官又迎来新问题，该案非法获取计算机信息系统数据的犯罪行为，是否已达“情节严重”的追诉标准？

根据最高法、最高检《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第十一条规定，在认定行为是否达“情节严重”标准时，应当考虑非法获取信息数据性质及条数、非法控制计算机台数、违法所得金额及造成经济损失等，要求至少符合上述司法解释规定的情形之一。

检察官指出，Y公司虽与M公司签订了金额为25万元的合作协议，但因数据窃取行为败露，杨某尚未将非法获取的数据用于项目交付，这笔预期收益属于未实现的违法所得，因此现有证据无法认定该案违法所得金额已达“情节严重”的追诉标准，接下来只能从爬取数据行为对A公司造成的经济损失入手。

能否准确认定经济损失，这对下一步开展追赃挽损工作至关重要。为此，检察官围绕公司业务经营模式、收费价格等内容，多次询问被害单位A公司业务负责人、调取相关书证，结合相关司法解释条款内容，深入理解“经济损失”的含义。经进一步审查查明，A公司在发现涉案系统数据遭受爬虫窃取后，被迫第一时间关停系统，停止服务，在此期间损失既定服务费9万余元，而这正是犯罪行为造成的直接经济损失，且该数额已达法律规定的“情节特别严重”标准。

此外，案发后，虽然杨某非法爬取的数据及相关介质已被扣押封存，但从其爬取至案发，数据始终处于不受权利人控制的境地，且根据计算机软件著作权证书、多份服务协议等书证，能够证实A公司被爬取的这上千万条数据的商业价值高达1400余万元。虽然上述商业价值不能直接等同于经济损失，数字领域的价值鉴定也尚无明确的认定标准，但它们如同悬在被害单位头顶的“达摩克利斯之剑”，存在可能泄露的潜在风险，而这一现实的危险亦是刑法评价的内容，应当作为酌定量刑情节予以考量。

据此，检察官认为，Y公司、作为直接负责的主管人员杨某，违反国家规定，超越授权，利用爬虫软件抓取被害单位相关计算机信息系统中存储的数据，情节特别严重，其行为均构成非法获取计算机信息系统数据罪。2025年1月23日，静安区检察院依法对Y公司、杨某提起公诉。

数据领域没有“法外之地”

3月26日，被告单位Y公司、被告人杨某非法获取计算机信息系统数据案在静安区法院公开开庭审理。上海市人大代表王娜、刘忱，人民监督员周琦麟，静安区数据局负责人，以及相关工作人员、行业从业者应邀全程旁听庭审。

为什么选择公开庭审？“数据安全是数字经济的生命线，但不少从业者对技术行为的法律边界认识模糊。”检察官在庭前准备时说，“通过这场庭审，让相关行业从业者充分了解技术创新不能自带‘法律豁免权’，数据领域没有‘法外之地’。”鉴于被告单位、被告人作为数据行业从业单位、从业者却知法犯法，该行为社会危害性较大，检察官特意准备了一堂“行业警示课”。

庭审过程中，公诉人以非法获取计算机信息系统数据罪的构成要件为主线，通过完整的证据链条，全面还原了指控事实。接受公诉人的指控和法庭教育之后，被告人杨某于庭后向法官和检察官均提交了自悔书，承认指控事实，自愿表示认罪认罚，并赔偿被害单位损失共计14万余元。

庭审结束后，静安区数据局工作人员表示：“技术不是违法挡箭牌，合法授权不等于无限权限。对于该案暴露出部分数据行业从业者法治意识淡薄的问题，我们将以案为鉴，通过提升监管能力、强化行业共治、开展普法宣讲等方式加强数据领域安全监管。”

6月3日，静安区法院作出一审判决，以非法获取计算机信息系统数据罪分别判处Y公司罚金5万元；判处杨某有期徒刑三年，缓刑三年，并处罚金3万元。

“5月20日正式施行的民营经济促进法确立了数据作为新型生产要素的法律地位，明确规定国家保障民营企业等各类经济组织依法平等使用数据资源，这既凸显数据对企业创新的核心驱动作用，也对企业数据治理能力提出更高要求。”静安区检察院相关负责人表示，“我们将贯彻落实民营经济促进法关于‘增强数据要素共享性、普惠性、安全性’的要求，立足法律监督职能，聚焦专业化法律监督、智能化技术支撑与多元化协同治理，持续深化网络与数据安全领域工作，着力提升网络空间治理效能，助力企业筑牢数据安全防线，为数字经济稳健发展提供更强法治保障。”

代表点评

一个保护数据安全的典型案例

上海市人大代表 刘忱

近年来数据要素市场快速发展，社会正在步入大数据时代，数据已成为重要的战略性资源和生产力要素，但也暴露出许多问题，该案中被告人非法获取计算机信息系统数据就是一个典型案例。此次庭审中，静安区检察院坚持公正司法，按照法律的规定和程序办事，做到了案件事实清楚、证据确实充分。在数据应用场景日益多元和复杂的情况下，以法律监督的精准履职保护数据安全，具有典型性。此次庭审也能引导大众合理、合法地开发和利用数据，推动行业良性发展。

（来源：检察日报）