数字经济背景下非法获取计算机信息系统数据罪的法益重构

葛崇皓

山东科技大学文法学院　山东青岛

【摘要】数字经济浪潮催生数据要素独立价值，传统刑法保护模式陷入规制困境。为了构建适配数字经济发展的法益保护体系，文章分析了现行罪名以系统功能破坏为入罪标准导致的规制盲区、罪名竞合混乱及量刑失衡等司法难题，探索了传统法益理论在应对数据非物质性、主体复合性、侵害隐蔽性时的解释危机，研究了德国技术中立规范、美国数据控制权理论、欧盟信息自决权模式的域外智慧。研究表明，应当突破系统载体中心范式，确立数据独立法益地位，构建机密性、完整性、可用性三维框架，建立价值量化、控制权破坏、危害范围的综合判断标准，形成罪名分层、刑罚梯度、规范衔接的体系化保护机制。

【关键词】数字经济；非法获取计算机信息系统；数据罪；法益重构

【收稿日期】2025 年 11 月 19 日　【出刊日期】2025 年 12 月 3 日　【DOI】10.12208/j.ssr.20250484

Reconstruction of the legal interests of the crime of Illegally obtaining data from computer information systems in the context of the digital economy

Chonghao Ge

School of Literature and Law, Shandong University of Science and Technology, Qingdao, Shandong

【**Abstract**】The digital economy wave has given rise to the independent value of data elements, and the traditional criminal law protection model has fallen into a regulatory predicament. In order to build a legal interest protection system that is compatible with the development of the digital economy, this article analyzes the judicial problems such as regulatory blind spots, chaotic competition of criminal charges and unbalanced sentencing caused by the current criminal charges taking the destruction of system functions as the criterion for criminalization, and explores the interpretive crisis of traditional legal interest theories in dealing with the immaterial nature of data, the complexity of subjects and the concealment of infringement. The extraterritorial wisdom of the German technology neutrality norm, the American data control rights theory, and the EU information self-determination rights model was studied. Research shows that it is necessary to break through the system carrier-centered paradigm, establish the independent legal interest status of data, construct a three-dimensional framework of confidentiality, integrity and availability, establish a comprehensive judgment standard for value quantification, control rights violation and the scope of harm, and form a systematic protection mechanism featuring hierarchical charges, gradient penalties and normative connection.

【**Keywords**】Digital economy; Illegally obtaining computer information systems; Data crime; Reconstruction of legal interests

引言：数据要素已在国家战略层面获得新型生产要素的地位定位，数据权益的财产属性在司法实践中不断显现，但刑法第 285 条第 2 款仍将计算机信息系统安全作为核心法益，传统保护模式难以回应数据要素市场化配置的现实需求，由此引发的入罪标准模糊、罪名适用混乱等司法困境日益突出，法益重构成为破解理论与实践张力的关键路径。

1 非法获取计算机信息系统数据罪传统法益保护的现实困境

司法实践中以"破坏计算机信息系统功能"作为入罪标准，导致大量未破坏系统完整性但严重侵害数据权益的行为被排除在刑法规制范围之外，爬虫技术获取电商平台用户消费数据、绕过技术保护措施提取企业核心算法参数等行为因系统运行正常而难以定罪，

传统法益保护模式无法涵摄数据要素流通中的新型侵权样态；罪名适用层面呈现明显的竞合混乱状态，获取个人征信数据既可能触犯侵犯公民个人信息罪亦可能构成本罪，获取企业客户名单既涉及商业秘密保护又涉及计算机数据保护，司法机关在个案中往往依据数据载体而非数据价值属性进行罪名选择，法律适用标准缺乏统一性[1]；此外，量刑困境更为突出，现行司法解释将"数据量"作为核心量刑要素，获取百万条低价值日志数据的量刑可能重于获取千条高价值商业数据。

2 非法获取计算机信息系统数据罪法益重构的正当性基础

2.1 数字经济时代数据要素价值的根本性转变

数字经济时代数据要素价值经历了从边缘到中心的本质跃迁，传统模式中数据仅作为业务记录工具依附于物理资产，而当前数据已转化为独立生产要素参与价值创造，其可复制性带来边际成本递减，单一数据集能够在多场景反复使用却不损耗原值，由此打破了传统要素的稀缺性约束。数据在流通聚合中产生倍增效应，不同维度数据融合生成超越原有价值总和的新型资产，促使企业估值将数据纳入核心资产[2]。

2.2 传统刑法法益理论在数字时代的适用性反思

传统刑法法益理论在数字时代面临物质性框架的解释困境、法益分类体系的定位模糊以及侵害判断标准的失效危机三重适用性挑战。古典法益理论奠基于有体物支配秩序，将法益保护建立在物理实体的占有、使用、收益等权能基础之上，数据作为比特流的非物质存在形态却无法纳入既有的物权保护范畴，其可复制性、非消耗性特征瓦解了传统财产法益的排他性逻辑，导致刑法保护陷入概念工具缺失的窘境。同时，传统个人法益与社会法益的二元划分体系难以准确定位数据法益的归属，个人数据兼具人格属性与财产属性的双重特质，企业数据承载竞争优势却关涉公共利益，法益主体的复合性使得单一归类模式无法涵盖数据权益的多维结构[3]。此外，传统刑法以物理损害、财产减损等可见结果作为法益侵害的判断依据，数据窃取行为却呈现原件留存、痕迹隐蔽的特点，受害者往往难以察觉侵害发生，传统结果犯的构成要件难以捕捉数字犯罪的实质危害。

2.3 域外数据犯罪立法中法益保护模式的借鉴价值

域外数据犯罪立法呈现出法益保护的多维度借鉴价值，主要体现在德国技术中立性规范路径对动态法益的适配、美国数据控制权理论对财产属性的明晰以及欧盟个人信息自决权优先模式对权利主体的强化三个层面[4]。德国刑法第 202a 条确立的数据机密性、完整性、可用性三位一体保护框架，摆脱传统刑法对具体载体的依赖，将法益聚焦于数据本身的存储状态、传输过程与访问控制机制，使得法益内涵随技术演进而自然延展，避免立法频繁修订导致的规范滞后困境。美国《计算机欺诈与滥用法》将未经授权访问界定为对数据控制者排他性支配权的破坏，确认数据作为数字资产的独立价值，将刑法保护嵌入数字经济的产权交易秩序之中，为数据要素市场化配置提供刑事法律保障的正当性依据。欧盟《通用数据保护条例》构建的个人数据主体权利优先体系，将信息自决权从抽象人格权益具象化为可诉性权利束，课以数据处理者明确的刑事合规义务，突破传统刑法将数据犯罪单纯视作财产侵害或秩序破坏的认知局限。

3 数字经济背景下非法获取计算机信息系统数据罪法益重构策略

3.1 法益保护客体的重新界定

法益保护客体的重新界定应当突破传统以信息系统载体为中心的保护范式，转而确立数据本身的独立法益地位，将保护重心从物理设备的安全运行转移至数据资源的完整控制。具体而言，需要摒弃将数据视为系统附属物的陈旧认知，承认数据作为独立权益客体的本体价值，在刑法规范中明确数据的机密性、完整性、可用性构成法益保护的三维核心要素，其中机密性指向数据不被未经授权主体知悉的排他状态，完整性保障数据内容在存储、传输、处理全流程中不被篡改的真实性特征，可用性则维护合法主体对数据资源的持续访问与正常使用能力[5]。界定过程中必须区分个人数据、企业数据、公共数据的不同属性特征，个人数据的法益客体侧重于自然人对其信息的自决控制权，企业数据的保护客体聚焦于经营者因投入成本、技术创新而形成的竞争优势，公共数据的法益内核在于国家机关履行职能所依赖的信息资源安全。界定标准应当结合数据分级分类制度，针对核心数据、重要数据、一般数据设置差异化的法益保护强度，确保刑法介入的精准性与比例性原则，避免保护范围的过度扩张引发刑法谦抑性的违背[6]。

3.2 法益侵害程度的判断标准

法益侵害程度的判断标准应当建立在数据价值量化、控制权破坏深度、潜在危害范围三个维度的综合评估体系之上，摆脱传统以经济损失为单一衡量尺度的局限性思维。数据价值量化维度需要引入数据分级分

类标准作为基础参数，核心数据涉及国家安全、经济命脉、重大公共利益的关键信息资源，其获取行为即便数量较少亦构成严重侵害，重要数据关系企业核心竞争力、个人敏感隐私的信息资产，非法获取行为的侵害程度需结合数据体量、敏感属性进行阶梯式评判，一般数据虽不具备高度敏感性，但大规模批量获取同样形成法益侵害的量变累积效应[7]。潜在危害范围评估需要考察数据流转链条中可能波及的主体数量、权益类型、损害后果，个人生物识别信息、医疗健康记录的泄露可能引发身份盗用、精准诈骗等连锁危害，企业商业秘密、技术方案的获取将导致市场竞争格局失衡、创新激励机制受损，公共服务数据、基础设施运行信息的非法掌握可能威胁社会公共安全，判断时必须将数据的流动性、关联性、衍生性纳入考量范畴，评估非法获取行为在整个数据生态系统中的扩散效应。

3.3 法益保护的刑法体系化配置

法益保护的刑法体系化配置需要构建罪名分层体系、刑罚梯度配置机制、前后法规范衔接网络三位一体的立体防护架构。详而言之，罪名分层体系的构建应当根据数据法益侵害的不同阶段设置递进式犯罪类型，在非法获取计算机信息系统数据罪之外增设非法控制数据罪作为预备行为犯，将破解访问控制措施、植入获取工具、建立非法访问通道等尚未实际窃取数据但已经危及数据控制秩序的预备行为纳入刑法规制范围。刑罚梯度配置机制应当突破现行法定刑偏轻的结构缺陷，针对核心数据、重要数据、一般数据设置差异化的刑罚幅度，对涉及国家秘密、商业秘密、个人敏感信息的非法获取行为配置三年以上十年以下有期徒刑的重刑威慑，对大规模批量获取一般数据但造成严重后果的行为设置三年以下有期徒刑、拘役或管制的中度刑罚，对情节轻微的获取行为保留罚金刑的适用空间，确保罪刑均衡原则在数据犯罪领域的充分实现[8]。此外，前后法规范衔接网络的建立应当强化刑法与《网络安全法》《数据安全法》《个人信息保护法》的协同配合，将行政法规中确立的数据分级分类标准、安全保护义务、合规管理要求转化为刑法判断的前置性规范依据，明确违反行政监管规定构成刑事违法性的转化条件，同时保持刑法的独立评价立场，避免将行政违法等同于刑事犯罪导致的处罚扩张，确保刑法介入的补充性、谦抑性品格在数字经济治理中的坚守。

4 结束语

数字经济加速演进对刑法保护提出持续挑战，法益重构并非一劳永逸的终点而是动态调适的起点，立法者需要保持对技术变革的敏锐洞察力，在数据价值持续膨胀与刑法谦抑性之间寻求平衡点，避免保护不足导致数据要素市场失序，亦防止过度干预抑制数字创新活力。司法机关应当摆脱机械适用法条的惯性思维，在个案裁判中准确识别数据法益的多维属性，将数据分级分类标准转化为具体判断依据，确保刑罚配置真实反映法益侵害程度。

参考文献

[1] 席乐天.网络爬虫型非法获取计算机信息系统数据罪问题研究[D].导师:黑静洁.北方民族大学,2025.

[2] 王怡.非法获取计算机信息系统数据罪司法适用问题研究[D].导师:孙杰.山东政法学院,2024.

[3] 姚瑶.非法获取计算机信息系统数据罪的限缩适用——兼论数据犯罪的法益侵害[J].华东政法大学学报,2024,27(02):94-106.

[4] 何凯.非法获取计算机信息系统数据罪定罪边界研究[D].导师:赵微.宁波大学,2022.

[5] 张剑楠.非法获取计算机信息系统数据罪司法认定问题研究[D].导师:冯剑;罗钢.新疆大学,2022.

[6] 彭雪莲.非法获取计算机信息系统数据罪认定问题研究[D].导师:王晓滨.辽宁大学,2022.

[7] 李紫阳.解释论视域下数据犯罪问题研究[D].导师:张勇.华东政法大学,2021.

[8] 张道伟.利用爬虫技术非法获取数据的刑法规制[D].导师:王安异.中南财经政法大学,2021.