

数字经济时代数据要素的法益识别与刑法保护 ——从公共秩序到财产安全、市场秩序

郭旨龙^{*}

内容提要：我国刑法在十几年前就开始设立公共秩序犯罪来保护数据的机密性，但这主要是回应信息经济中社会成员对于数据内容的关切。在当下的数字经济中，数据不再仅仅是直接提供给人类的信息，来支撑起供应链协同和大规模定制，而主要是以大数据的形式给云计算和人工智能提供生产要素性的原始数据。个人数据、企业数据和公共数据都进入了这个价值链，也都面临着威胁。数据的财产、经济性质日益凸显，社会成员愈发重视数据资源持有权、数据加工使用权、数据产品经营权等数据产权本身的保护。对于数字经济中对数据资源持有权、数据加工使用权的侵犯，应当根据具体情形认定为盗窃、毁坏财产或破坏生产经营的行为。鉴于盗窃行为排除占有的固有形象，对盗取数据的行为最好有特别立法以示区别和公平。在出现成熟市场之后，数据的财产性质必然嵌入到整个经济活动中，涉及竞争利益和市场秩序。侵犯数据产品经营权更多是严重扰乱数字经济市场秩序的行为，而非侵犯知识产权的行为。

关键词：原始数据 衍生数据 公共秩序 数据财产 数据竞争

数据已成为经济增长、创造就业和社会进步的重要资源。《中华人民共和国民法典》第127条规定了对于数据和网络虚拟财产的保护，法律有规定的，依照其规定。民法和刑法学界对网络虚拟财产的研究都由来已久。对比之下，民法学界对数据财产的研究虽然较为新近，但也蔚然成风；^{〔1〕}而刑法学界对数据财产的研究却仍处于方兴未艾状态。^{〔2〕}2022年《中共中央 国务院关于

^{*} 郭旨龙，中国政法大学刑事司法学院教授、中国政法大学证据科学教育部重点实验室特约研究员。

本文为国家社会科学基金青年项目“数据竞争不法行为入罪边界的刑法解释研究”（23CFX065）的阶段性成果。

〔1〕 参见梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016年第9期；林涸民：《个人数据交易的双重法律构造》，载《法学研究》2022年第5期；朱晓峰：《论个人数据权益侵害的损害赔偿》，载《甘肃社会科学》2024年第4期。

〔2〕 参见刘双阳、李川：《衍生数据的财产属性及其刑法保护路径》，载《学术论坛》2020年第3期；高艳东、李诗涵：《数字时代财产犯罪中财物的扩张解释：以数据服务为例》，载《吉林大学社会科学学报》2020年第5期。

构建数据基础制度更好发挥数据要素作用的意见》提出推进公共数据、企业数据、个人数据分类分级确权授权使用，构建数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制以及维护前述权益的保护制度。此外，该文件还进一步提出了数据产权、流通交易、收益分配和安全治理四个方面共计 20 条具体发展的意见。^{〔3〕} 根据数据财产权化的基本思路，北京、上海、广州、深圳四大城市都成立了数据交易所，数据产品十分丰富。这就直接对刑法在产权运行机制的全流程保障数据权益提出了要求。刑法研究应当思考在数据产权运行的各个环节是否介入法益的保护、如何进行保护。

一、数据的传统秩序性质及其多元化趋势

（一）数据的公共秩序法益性质

《中华人民共和国刑法》（以下简称《刑法》）在 1997 年修订时增设第 286 条破坏计算机信息系统罪第 2 款，开始保护计算机信息系统内的数据不受非法增加、修改、删除，此时主要为了维护计算机信息系统的正常运行和使用，侧重的是数据的技术性质能够服务于系统的正常运行。^{〔4〕} 2009 年《刑法》修正时增加了非法获取计算机信息系统数据罪，开始保护计算机信息系统内的所有数据不被非法获取，此时保护的法益开始溢出计算机信息系统本身的正常运行。例如，在犯罪人非法获取被害人苹果手机 ID 密码并对手机和 ID 解除绑定之后，被害人无法再使用该 ID 数据操作苹果手机，^{〔5〕} 此时可以认为苹果手机这个计算机信息系统的正常运行受到了侵害。然而，在更多仅仅是侵害数据的机密性的案例中，行为人并未妨碍权利人对数据的继续使用，也就没有妨碍计算机信息系统的正常运行，但非法获取数据仍然是一种扰乱公共秩序的犯罪。那么，公共秩序是如何在计算机信息系统的正常运行本身没有被直接损害的情况下被扰乱的呢？

这就涉及公共秩序应当如何理解的问题。公共秩序法益的理解历来是一个难点。我国学者一般将其解释为生活的稳定与安宁。^{〔6〕} 然而，从这种抽象的定义中我们仍然难以理解非法获取计算机信息系统数据的行为如何扰乱了生活的稳定与安宁。公共秩序利益保护的关键要素可以恰当地归类为三种日常生活平稳的条件：生活便利、生活舒适、生活安宁。这些生活条件是指人们为顺利进行广义上的生活而使用生活场所和生活设施的一般条件，即能够参加有关的生

〔3〕 2021 年底通过的《上海市数据条例》第 12 条第 2 款规定：“本市依法保护自然人、法人和非法人组织在使用、加工等数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益。”第 13—15 条分别规定了合法、正当收集数据的权利，对合法取得的数据依法使用、加工的权利，依法开展数据交易活动的权利；第 49 条鼓励通过实质性加工和创新性劳动形成数据产品和服务。《深圳经济特区数据条例》第 58 条规定：“市场主体对合法处理数据形成的数据产品和服务，可以依法自主使用，取得收益，进行处分。”

〔4〕 “张竣杰等非法控制计算机信息系统案”（最高人民法院第 145 号指导案例）指出，通过植入木马程序的方式，非法获取网站服务器的控制权限，进而将添加了赌博关键字并设置自动跳转功能的静态网页，上传至目标服务器，提高赌博网站广告被搜索引擎命中几率，但未造成系统功能实质性破坏或者不能正常运行，也未对该信息系统内有价值的数据进行增加、删改的，不应当认定为破坏计算机信息系统罪。

〔5〕 参见广东省中山市中级人民法院（2017）粤 20 刑终字第 258 号刑事判决书。

〔6〕 参见张明楷：《刑法学》（第 6 版，下），法律出版社 2021 年版，第 881 页。

活，活动方便、舒适，不受干扰。公共秩序利益的第一要素是生活便利，即生活条件有用，使用起来容易、合适；另一个因素是舒适，即人们由令人愉快的生活条件产生的愉悦感，对获取、使用的生活条件的满意程度；再一个要素是保持和享受外在和内在的平静。^{〔7〕} 非法获取计算机信息系统罪的增设一开始主要是为了打击窃取他人账号、密码等信息的行为。^{〔8〕} 此时的系统内数据是指对线下已有信息的电子化呈现，或者对线下已有事实、概念的电子化描述。^{〔9〕} 这种非法获取侵犯了权利人不欲该数据为他人所知的机密状态的信息安全设定。权利人只想自己知悉和利用该数据，在选定的计算机信息系统上进行操作，开展日常活动。然而，他人非法获取该数据，意味着权利人必须在事先、事后进行预防和处理，其利用该数据进行计算机操作的日常活动也必然偏离既定轨道，此时可以认定为生活的便利、舒适乃至安宁都受到了影响。考虑到计算机在社会中的特殊地位，对整个社会的重要性，以及满足人们对存储在计算机上的信息受到保护安全感的需要——那些使用和依赖计算机的人，如果担心其他人可能未经授权访问他们的信息，可能会无法充分利用计算机——这意味着对信息进行特殊保护，而信息存储在计算机中。^{〔10〕}

可见，虽然计算机信息系统在技术上可以按照原有的方式进行数据处理，但因为数据处理是人们有目的的活动，在系统内的数据的保密性被侵害的情况下，人们利用计算机处理数据、进行日常活动的行为也必然发生变化。在 2009 年左右，政府机关、科研院所、企业单位以及部分专业人士开始日常性地利用计算机工作和生活，计算机内的数据机密性凸显。在这些原始数据服务于工作、生产、营业和生活的场景中，所谓的数据利益以日常生活秩序为利益核心。例如，“统方是指医院对医生用药信息量的统计，卫生部严禁为商业目的进行统方”^{〔11〕}。可见，医院的统方数据是出于非商业目的，即日常医疗活动的顺利开展而收集、存储和传输的。此时统方数据的机密性涉及的就是医院的正常活动秩序。

（二）数据的法益性质多元化趋势

1997 年《刑法》修订时设置了非法侵入计算机信息系统罪和破坏计算机信息系统罪。此时非法侵入的计算机信息系统限于少量的国家事务、国防建设、尖端科技领域的系统，以预防其内的数据受到侵害。而破坏计算机信息系统罪的第 2 款保护的是普通计算机信息系统内存储、处理、传输的数据不受删除、修改、干扰的侵害。作为扰乱公共秩序罪一节中的具体罪名，它们的立法目的都在于维护特定系统或者普通系统所连接的工作、生产秩序，即相关的工作、生产得以稳定、有效地进行。2009 年《中华人民共和国刑法修正案（七）》增设了非法获取计算机信息

〔7〕 See Zhilong Guo, *Public Order as a Protectable Interest*, 41 Legal Studies 410, 416 (2021).

〔8〕 参见高铭喧：《中华人民共和国刑法的孕育诞生与发展完善》，北京大学出版社 2012 年版，第 513 页。例如非法查看平台内招标项目的投标情况、报价单等。参见江苏省南通市崇州区人民法院（2020）苏 0602 刑初字第 306 号刑事判决书。

〔9〕 根据欧洲理事会 2003 年《关于网络犯罪的公约》第 1 章对有关术语的定义，“计算机数据”是指“在计算机信息系统中存储、处理或传输的任何事实、信息或概念的表达形式，包括能确保计算机执行某项功能的程序”。例如非法获取的软件源代码。参见浙江省杭州市中级人民法院（2017）浙 01 刑终字第 512 号刑事判决书。

〔10〕 See The Law Commission, *Computer Misuse*, Working Paper No. 110, 1988, paras. 6.7–6.8.

〔11〕 浙江省青田县人民法院（2014）丽青刑初字第 415 号刑事判决书。

系统数据罪，进一步保护了普通计算机信息系统内数据的保密性和可用性，其目的仍然是为了更好地保护普通用户工作、生产和生活的稳定与顺利进行。这些刑法罪名保护的数据都要求是计算机信息系统内存储、处理或者传输的数据，即服务于计算机信息系统的正常运行，进而服务于人们工作、生产、生活的稳定与顺利进行，这才保护了经由计算机信息系统的操作而产生的公共秩序新内容。

然而，随着数据介入和承载了越来越多、越来越复杂的利益生成和分配过程，侵犯数据行为的定性也产生了变化的需要。《最高人民法院、最高人民检察院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》（以下简称《关于办理危害计算机信息系统安全刑事案件的解释》）将非法获取支付结算、证券交易、期货交易等网络金融服务领域的身份认证信息 10 组以上的，以及其他领域的身份认证信息 500 组以上的行为认定为构成非法获取计算机信息系统数据罪。认定身份认证信息为系统数据在当时没有问题，而且有很大的必要性，因为身份认证信息，如用户名、密码、动态口令和证书等数据，是与系统安全相关的数据中最为重要的数据类型，是网络安全的第一道防线。^{〔12〕}但前提要求是，该身份认证信息是计算机信息系统所存储、处理、传输的数据，而不能是置放于某个数据存储设备、没有与某个计算机系统相连接的数据。换言之，不是所有与系统安全相关的数据都是系统数据，只有系统内存储、处理和传输的那一批数据才是系统数据。

在越来越多的普通公民开始使用计算机后，数据的个人信息性质也逐渐凸显。2009 年的《刑法》修正增加了侵犯公民个人信息的罪名，打击的是国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人的行为。众多的单位匹配了社会的信息化，个人接受这些服务或管理的过程中产生和“交出”了诸多个人信息。在计算机信息系统内，可被认定为个人信息的数据不仅为单位日常工作的开展所必要，也为公民个人身份的确认和个人活动的识别所必要，成为公民个人日常活动开展的要素。如果被非法获取，不仅影响单位日常工作的正常开展，也会威胁公民的财产、人身等合法权益。但不管是为单位生产、工作所需的系统内数据，还是个人利用个人信息开展活动所需的数据，侧重的都是信息安全。

在今天看来，这些身份认证信息无疑是典型的公民个人信息，相关行为可以甚至应当认定为侵犯公民个人信息罪。然而，在 2011 年《关于办理危害计算机信息系统安全刑事案件的解释》出台时，公民个人信息的保护仍然限于 2009 年《刑法》修正增设条款所保护的国家机关或者金融、电信、交通、教育、医疗等单位在履行职责或者提供服务过程中获得的公民个人信息。此时，虽然网络金融服务领域的身份认证信息可以认定为金融单位在提供服务过程中获得的公民个人信息，非法获取的构成侵犯公民个人信息犯罪，但其他领域的身份认证信息，能否认定为此处规定的“单位”在提供服务中获得的个人信息，存在疑问。是故，用非法获取计算机信息系统数

〔12〕 参见喻海松：《〈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〉的理解与适用》，载《人民司法·应用》2011 年第 19 期。

据罪来保护所有身份认证信息的安全，更具周延性。然而，2015 年《刑法》修正将“单位在履行职责或者提供服务过程中获得”的限制删去，包括了所有场景下产生的个人信息，此时将所有的身分认证信息都认定为公民个人信息犯罪的对象，不存在任何问题。认定为个人信息更具周延性，因为个人信息数据不要求存储在某个系统内。此时，非法获取身份认证信息的行为一般会同时构成两罪。

那到底是认定为扰乱秩序的非非法获取计算机信息系统数据罪，还是认定为侵犯公民人身权利的侵犯公民个人信息罪呢？常规思路是从一重罪论处，这似乎是一种以刑制罪的思路，其合理性在于满足了重罪重罚的罪刑相当原则。然而，罪刑相当原则的完整表述是对犯罪分子所判处的刑罚（可做广义解释，包括罪名标签带来的谴责和烙印）应当与其所犯的罪行和承担的刑事责任相适应。适用重罪之刑满足了与承担的刑事责任相适应的需求，却忽视了与所犯的罪行相适应的需求。行为人同时触犯扰乱秩序的非非法获取计算机信息系统数据罪，与侵犯公民人身权利的侵犯公民个人信息罪，如果只考虑刑罚轻重，而没有考虑到罪行特质，可能忽视了与所犯的罪行相适应的需求。在两罪法定刑幅度相同的情况下，根据罪行特质予以裁判的需求更加凸显出来。是故，在刑法全面保护各种场景下产生的个人信息之后，身份认证信息等系统内的数据，只要具有个人信息的特殊属性，就更应作为个人信息来为刑法所保护。若行为人明知系统内的数据为个人数据，其目的主要是获取之后作为个人数据来使用，而非作为系统内的数据来使用，以扰乱信息系统相关的工作、生产、生活秩序，则此类情形应当认定为侵犯公民个人信息罪，以突出对公民个人信息的保护，而非突出非法获取计算机信息系统数据罪，避免使之成为信息时代的口袋罪。此时重要的是利用承载了个人信息的数据来获得进一步进行财产操作的权限，而非通过系统内的数据来获得其传达的一些信息。

同理，在系统内的数据具有财产性质时，也应当考虑用财产犯罪的相关罪名予以制裁，而非用计算机犯罪的罪名去保护财产相关的利益，否则就是放任计算机犯罪成为信息时代的口袋罪。以下将论及，在数据成为数字经济的基础要素之后，数据的财产化、经济化成为一个不可避免的法益增生方向，需要刑法的体系化应对。

二、数字经济中数据要素的功能演化与犯罪威胁

理清数据在数字经济中的功能性作用的演化，才能更好地理解数字经济中数据面临的犯罪威胁。由此，我们能够更好地呈现出数据涉及多重法益的原因，以及此种法益变迁性及法益特征可能带来的对刑事司法工作特别是数据犯罪定罪的挑战。

（一）数字经济中数据要素的功能演化

我们很容易直接将数字经济和延续数百年的工业经济进行对比，这就会导致数据在数字经济中的功能仍然被理解为一种信息和知识，即提供给我们人类经济体的内容。但一二十年前信息经济中的数据就已经具备这种功能。在信息经济中，代表性的通用技术是数字通信系统，经济要素中的信息开始体现价值，信息技术产业和被信息技术化的各行业的核心商业主体仍然是大企业，

其依赖数据直接传递给人类的信息来支撑起供应链协同和大规模定制。^{〔13〕}此时的数据在传统的互联网化和信息化的经济活动中的应用主要体现为，在以企业家自我为中心的小生态圈中，人们期待数据直接向其提供内容以获得更好的智力或行动力。行为人主观上往往已经有了获取某种特定类型的信息的既定目的。我国刑法在十几年前就开始以公共秩序犯罪来保护数据的机密性，这主要回应的是信息经济中社会成员对于数据内容的关切。非法获取、传输一般数据的行为主要是非法侵害了一般数据中蕴含的具有实质内容的信息。^{〔14〕}

而在真正的数字经济中，虽然数据的作用是给数字经济提供数字化的知识和信息，但作为关键生产要素，其作用越来越不限于给人们直接提供内容性的信息和知识，更多是以大数据的形式给云计算和人工智能提供生产要素性的原始数据。此时的数字经济，通过移动互联网生产和收集的海量消费者数据，以及物联网生产和收集的大数据，以平台的云计算和人工智能支撑面向消费者的直接服务，或者支撑各种小前端面向消费者的服务。此时，原始数据以大数据的形式出现，为云计算和人工智能技术的计算运行提供原材料，来加速有意义的信息和知识的产出及其变革。由此我们可以理解，数据在数字经济中的主要作用，不是给人们直接提供信息内容，而是给机器智能（和数据分析师等新型从业人员）提供生产要素，这是一个专业的生产活动。更好的数据分析有助于更好的决策、产品和服务的创新，有利于对未来事件的预测。行为人主观上往往可能没有获取某种特定类型的信息的既定目的。由此，我们能更好地把握数字经济中的数据功能及其犯罪威胁。

（二）数字经济中类型化数据的功能表现及其犯罪威胁

1. 数字经济中个人数据的功能表现及其犯罪威胁

个人数据即体现和承载个人信息的数据，是能够单独识别特定自然人身份或者体现特定自然人活动情况的数据，或能够结合其他数据合理地识别身份条件或体现活动情况的数据。^{〔15〕}前者主要是指手机号码、身份证号、电子邮箱、金融账号等，往往可以直接用于数字经济中的广告推送，后者是指消费记录、收入记录、用电记录、网络用户行为痕迹数据、地理位置信息、健康数据等，结合其他数据可以合理识别自然人，可以用于数字经济中的有针对性的推销活动。因此，随着计算机化数据和先进贸易的发展，我们的日常生活与互联网相连，基于电子消息和网络站点的交流，电子购物和数字交往是新的主流趋势，组织、建立在虚拟空间之上的一切都是数字化的，数据盗窃对个人来说仍然是一个巨大的危险。^{〔16〕}早期侵害个人数据主要是为了实施诈骗、网络暴力等违法犯罪活动。例如2009年中国商业联合会相关部门收到诸多电视购物企业申诉，称其掌握的个人电话号码等数据被他人盗用，直接用于欺骗消费者购买产品甚至销售假冒伪劣产品。^{〔17〕}

〔13〕 参见汤潇：《数字经济：影响未来的新技术、新模式、新产业》，中国工信出版集团、人民邮电出版社2019年版，第9页。

〔14〕 参见刘宪权：《数据犯罪刑法规制完善研究》，载《中国刑事法杂志》2022年第5期。

〔15〕 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018年第3期。

〔16〕 See Aarushi Chopra, *Criminal Threat of Cyber Data Theft: An Analysis under the Indian Criminal Law*, 18 *Supremo Amicus* 23, 25 (2020).

〔17〕 参见郁棠：《电视购物企业数据被盗用情况严重》，载《中国商贸》2009年第9期。

然而，随着数字经济的蓬勃发展，个人数据的价值及其面临的犯罪威胁发生了变化。就数字经济而言，个人数据是数字经济大数据的主要来源，因为个人是数字经济活动的主体，掌握相关的个人数据才能促进数字经济的发展。收集的种种个人信息是最粗糙、最原始的非结构化数据，只有逐步清洗、处理成结构化的数据，才能够运用到数字经济活动中。个人信息的个人自决模式，强调激励数据权利人自主决定“共享或转让”其合法持有的数据，这和承认数据财产性的赋权模式在理念上具有相通之处。个人日常操作留下的单次数据，可获得的信息量和价值都是非常有限的，但个体日常网络轨迹的数据量累积到一定数据量级时，可以推出该个体几乎所有的重要信息。^{〔18〕}此时单个人的数据也成为数字经济活动中非常重要的数据来源。现实中偶有数据主体将成年累月积攒的个人数据打包出售的案例。^{〔19〕}“个人应被国家赋予访问、获取、整合、利用和出售与个人直接相关或个人参与创造的数据的权利，即形成数据交易市场。”^{〔20〕}此时，若全面的个人数据被非法获取，将对个体的经济生活和财产权益产生重大威胁。群体的个人数据的收集与分析更是如此，更能推导出该社群乃至国族的整体特征和发展趋势等重要经济信息。

2. 数字经济中企业数据的功能表现及其犯罪威胁

企业数据，是指在企业生产、经营、服务等活动中产生、收集的数据。^{〔21〕}它既包括收集的个人信息，也包括脱敏后无法以合理的技术手段或社会成本还原为个人信息的个人信息，还包括完全与个人信息无关的数据。第一类企业数据兼具个人数据的属性，因此企业的数据权利要受到个人的信息权利的制约。例如淘宝公司依其与网络用户的约定收集、使用网络用户信息，即浏览、搜索、收藏、加购、交易等网上行为痕迹信息，通过特定算法深度分析过滤、提炼整合出“生意参谋”数据产品。^{〔22〕}此时的企业对收集的具有个人信息属性的数据，只具有在合法控制数据资源基础上的有限的加工使用权，包括进行筛选、分类、排列、加密、标注、转换、汇聚、分析、统计、关联、挖掘或聚合等加工活动的权利，还包括进行（个性化）展示、用户画像、自动化决策、定向推送、信息合成和第三方应用管理等使用活动的权利。^{〔23〕}对此可设置有限财产权，主要赋予数据控制者对抗他人不当获取与利用行为的权利。例如行为人恶意部署程序，采集并保存运营商服务器中的用户登录 cookie 数据等信息，用于后续社交、购物用户的恶意添加好友。^{〔24〕}但企业对投入创造性劳动之后获得的、与个人信息不直接对应的衍生数据享有独立的财产权益或竞争性利益，^{〔25〕}包括独立的数据资源持有权和进一步的加工使用权，以及相应的数据

〔18〕 参见田刚：《大数据安全视角下计算机数据刑法保护之反思》，载《重庆邮电大学学报（社会科学版）》2015年第3期。

〔19〕 参见屈一平：《揭秘大数据买卖在中国》，载《小康》2014年第14期。

〔20〕 谢楚鹏、温孚江：《大数据背景下个人数据权与数据的商品化》，载《电子商务》2015年第10期，第32页。一次完整的个人数据交易同时包含表意人的承诺与个人的同意。参见林涓民：《个人数据交易的双重法律构造》，载《法学研究》2022年第5期。

〔21〕 参见龙卫球：《再论企业数据保护的财产权化路径》，载《东方法学》2018年第3期。

〔22〕 参见浙江省杭州市中级人民法院（2018）浙01民终字第7312号民事判决书。

〔23〕 参见邓辉：《数据“三权分置”的新路径》，载《中国社会科学报》2022年9月28日，第4版。

〔24〕 参见浙江省绍兴市越城区人民法院（2019）浙0602刑初字第636号刑事判决书。

〔25〕 参见顾全：《数字经济案件分类体系及裁判规则研究》，载《中国应用法学》2022年第5期。

产品经营权。数据产品也可能面临侵害，例如犯罪人招揽、组织、帮助他人获取数据产品“生意参谋”中的数据内容。

第二类企业数据原则上不涉及个人信息权利的制约。用匿名化等脱敏技术处理后，数据的人性在规范上被消除，企业作为数据控制者有持有、使用、进一步加工和处分的权利。第三类企业数据主要是指生产设备维护、货物管理系统、物联网等方面与自然人个体并无直接联系的数据，这些数据与自然环境、物品、设备直接相关，在数字经济中可用于提高产品质量、服务效率。^{〔26〕} 以上两类数据的价值往往不在于其直接呈现的信息，而在于累积之后可以成为数字经济再生产的重要要素。学者认为，数据是数字经济运行中比石油更为重要的资源，是从政府到本地公司顺利运行的关键。没有数据，进步就会停止。绝大多数的企业使用数据为他们的商业机会提供动力，把数据作为形成一个商业战略不可或缺的组成部分。然而，电子结构中的任何信息/报告都比纸质文件更容易被盗，因为它们便于携带，易于复制。不仅如此，它可能被偷走的数量也令人恐惧。^{〔27〕}

3. 数字经济中公共数据的功能表现及其犯罪威胁

公共数据，是指公共主体在提供公共服务时产生、收集的数据，或者水务、电力、燃气、通信、公共交通、民航、铁路等公用事业运营企业在提供公共服务时产生、收集的依法应当公开的数据。^{〔28〕} 前者包括气象、地震、民政、公安、经济等党政、事业单位在提供公共服务时产生的数据，是对天气等事件、状态或群体活动的记录。这些高价值数据集涉及的主题领域可以有地理空间、地球观测和环境、气象、统计、公司所有权以及人群流动性。后者包括供电公司收集的用电量，移动通信公司收集的位置信息、通话信息，公交公司收集的公交车定位数据，医院收集的健康数据等脱敏数据。这样的数据可以被重新使用，并支持或改进不同的产品或服务。允许公共数据被轻松地重新用于其他目的，包括商业目的，可以刺激经济增长并帮助应对社会挑战。它们是中小企业和创业公司创造新产品、提供新服务的宝贵资源。

以上数据若涉及国家安全，依照《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国保守国家秘密法》等规范不得公开，若涉及商业秘密，依照知识产权法律规范由商业主体决定是否公开。公共数据与国家秘密、商业秘密以及财产的界限是个问题。^{〔29〕} 学者认为，数据是否被视为财产在很大程度上取决于具体法规的措辞。例如，在试图指控维基解密创始人朱利安·阿桑奇公布被泄露的政府文件时，美国检察官显然在考虑以“贩运赃物”的罪

〔26〕 工信部2020年公布的《工业数据分类分级指南（试行）》第2条规定：“本指南所指工业数据是工业领域产品和服务全生命周期产生和应用的数据，包括但不限于工业企业在研发设计、生产制造、经营管理、运维服务等环节中生成和使用的数据，以及工业互联网平台企业（以下简称平台企业）在设备接入、平台运行、工业APP应用等过程中生成和使用的数据。”

〔27〕 See Aarushi Chopra, *Criminal Threat of Cyber Data Theft: An Analysis under the Indian Criminal Law*, 18 *Supremo Amicus* 23, 23–24 (2020).

〔28〕 参见齐英程：《作为公物的公共数据资源之使用规则构建》，载《行政法学研究》2021年第5期。

〔29〕 企业数据依据其性质和功能可财产权化的程度最高，但是公共数据、个人数据则受到相当的限制。严格说来，公共数据受到公共功能重大约束，出于公共管理的特性，具有极强的国家安全、公共安全、个人隐私安全、企业商业秘密安全等相关性，在融入经济化过程中需要特别克制和慎重，个人数据则与纳入人格权益的个人信息保护紧密相关也应受到相应限制。参见龙卫球：《法治建设为构建数据基础制度保驾护航》，载《中国网信》2022年第9期。

名起诉，但此案到底是盗窃，还是复制，存在争议。^{〔30〕}对于无法作为开放数据提供的某些公共部门数据，我们应当有促进其重新使用的机制。但是，“作为数据资产，公共数据资源汇聚后面临机密性保护的问题……作为数据要素，公共数据资源面临完整性和可用性等安全挑战，数据被恶意篡改、非法使用和过度开发等问题亟需关注”^{〔31〕}。依法应当公开的数据，一般不存在他人非法获取的问题，但仍然存在他人非法删除或毁坏的问题；而企业在提供公共服务时产生、收集的数据，则可能存在他人非法获取的问题。

综上所述，个人数据、企业数据和公共数据涉及数字经济中数据的整个价值链生成和危险源介入的环节。原始的个人数据、企业数据和公共数据在被收集后，进入数据清洗（匿名化）和降噪、检测异常值、消除异常等数据预处理阶段，再进入数据集成和形成学习模型的数据处理阶段，最后形成知识模型以进行预测或处理。从收集原始数据的阶段开始，就存在非法获取权利人合法持有的数据的风险；在数据预处理和数据处理阶段，还存在着以干扰数据质量等手段破坏数据加工、使用的问题；学习模型是一种大数据处理工具，可能符合软件著作权的要求，受到相应的侵犯威胁，而最后形成的知识模型是一种数据产品，可能被非法使用，经营活动也可能受到干扰。这些新型犯罪威胁呼唤着相关刑法保护的转型。

三、数字经济中数据要素的财产、经济秩序法益性质

在当下的数字经济中，社会成员愈发重视数据资源持有权、数据加工使用权、数据产品经营权等数据产权本身的保护。这些重要的趋势可以统称为数据的财产、经济属性日益凸显。

（一）数据要素的财产属性凸显

随着公民个人接入互联网的普及、公民网络活动轨迹（包括搜索记录和下载记录）的广泛收集，大数据时代来临。手机上网的移动互联网时代彻底引爆了大数据时代。连接到物联网（IoT）的物体如智能家电，和连接到互联网的工厂机器人，也意味着数据的主体来源、时空范围都得到了极大的拓展；而大数据分析技术的日益成熟，更是使得数据挖掘、清洗和衍生活动不断更新。此时侧重保护的是数据本身的安全。这些数据在类型上不同于早期的系统内数据，不是指对线下已有信息的电子化呈现，或者对线下已有事实、概念的电子化描述，供使用计算机的人们直接获取内容性的信息，而纯粹是新技术时代为适应新的经济形态而爆发的数据类型，主要供应云计算和人工智能的运行。“特别是在大数据时代，数据的独立价值和权利属性已经越来越得到广泛重视。”^{〔32〕}网络服务提供商不再是收集服务本身必要的信息，而是开发和利用诸如 cookies

〔30〕 See Jonathan Clough, *Data Theft? Cybercrime and the Increasing Criminalization of Access to Data*, 22 Criminal Law Forum 145, 151 (2011).

〔31〕 陈发强等：《公共数据资源开发利用网络安全保障模型研究》，载《2022 年西湖论剑·网络安全大会——数字城市安全治理理论论文集》，第 14 页。

〔32〕 李玉萍主编：《网络司法典型案例（刑事卷·2019）》，人民法院出版社 2020 年版，第 38 页。然而，司法者却仍然依赖非法获取计算机信息系统数据罪这一扰乱公共秩序罪的罪名来保护数字经济时代数据的独立价值。参见北京市海淀区人民法院（2017）京 0108 刑初字第 2384 号刑事判决书。这将在本文第三部分予以批判分析。

的技术，尽量地收集用户在接受服务时所伴随的数据。此时，收集的数据不一定为日常生产、经营、服务等活动的顺利开展所必需，不再有明显的公共秩序关联。特意收集的数据（有明确的加工、衍生意图），以及为日常活动的顺利开展必须收集的数据，如果有加工和衍生的数据，都是以财产性质为利益核心。可见，此时的收集者看重的是数据资源持有权，这种权利在合法处理数据的基础上产生。^{〔33〕}

挖掘的过程就是使用的过程，衍生的数据就是劳动产品。从数据收集，到数据清洗（匿名化）、数据预处理（降噪、检测异常值、消除异常），再到数据集成、形成知识模型等数据处理，整个数据挖掘的过程，都是使用原始数据的过程。越来越多的数据处理者从事的是一种专业性的生产性活动，即汇集大量关联的原始数据，通过清洗、提炼、转换、标记和组织等方式将大数据转化为可被机器识别和分析的格式，即通过改进数据的可用性来为机器智能提供生产要素（初级的数据产品）。而为不同主体、不同目的所集成的数据，形成的知识模型，乃至进一步部署和应用知识模型所获得的数据，都是衍生的数据。例如某公司成立项目组，研发出手机 APP“淘车大师”，面向注册用户有偿提供车辆的维修和保养记录查询，且向其他公司接端口以直接查询类似数据和进行数据模型分析。^{〔34〕}可见，数据资源持有权权利人在将原始数据的可用性改进之后，可对初级数据产品进一步加工和使用，也可提供或许可给他人使用，此时处于流通阶段和交易阶段的他人不但获得数据资源的持有权，而且也开始获得数据加工使用权，且对加工出来的高级数据产品进一步享有数据产品经营权。

数据的上述使用过程使得数据成为财产。财产的本质在于使用价值，即对于法律主体的欲望和需求能够进行满足的效用。数据的使用过程就表征了数据对于其使用者的使用价值。对于财产的本质有很多种解释，其中一种解释是人将自己的意志或人格置入某事物，从而产生了财产主张，使之成为他的财产。^{〔35〕}我国也有学者接受这种主客体关系的财产本质解释视角，^{〔36〕}这允许了技术社会变化背景下财产的扩容。这种视角面临的诘难可能是，计算机系统的数据也为系统操作所必要，为何不都认定为财产。人类信息体需要通过特定信息化环境中的社会实践、规范或习俗承认的表达方式将使用意思传播出去，信息为他人所知时，他人才有必要考虑是否加以尊重，法律才有必要考虑是否加以保护和调整。^{〔37〕}人们在使用非个人数据例如灾害情况，以及个人信息例如张三的收入情况，由此在计算机系统内确定张三要获取的救济时，这些个人数据和非

〔33〕 对于“个人性数据资源和企业性数据资源，持有者可以享有数据资源的排他性和竞争性……可以通过司法解释发布数据资源持有权的具体认定要素，以统一数据资源持有权的判定标准”。来小鹏：《用好数据要素，需理解数据资源持有权基本内涵》，载《科技日报》2022年9月5日，第8版。“其一，数据来源者有权持有自己所产生的数据。比如，个人持有本人的消费数据、健康数据，企业持有自己的生产数据、销售数据，政府部门持有政务或社会管理数据等。其二，数据处理者‘依法持有’其他主体的数据。”邓辉：《数据“三权分置”的新路径》，载《中国社会科学报》2022年9月28日，第4版。

〔34〕 该类数据却被行为人非法复制、保存，供他人有偿查询。参见江苏省盐城市中级人民法院（2020）苏09刑终字第205号刑事判决书。

〔35〕 参见〔德〕黑格尔：《法哲学原理》，范扬、张企泰译，商务印书馆1961年版，第50页；Margaret Jane Radin, *Property and Personhood*, 34 Stanford Law Review 957, 959 (1982)。

〔36〕 参见张天一：《时代变动下的财产犯罪》，元照出版公司2015年版，第76、79、81、101页；易继明：《财产权的三维价值——论财产之于人生的幸福》，载《法学研究》2011年第4期。

〔37〕 参见郭旨龙：《信息理论视角下的数字财产及其刑法保护》，载《法制与社会发展》2023年第4期。

个人数据的确为使用者所需要，这种使用的情况也传递出了使用者的使用意思。

然而，使用价值必须有转化为交换价值的可能性，使用之事物才能被视为法律上的财产。这种可能性意味着使用价值不仅是某个特定的计算机系统使用所需，也为其他人所需。恰恰在这一点上，原始数据并不能理所当然地被认为是为其他数据主体所需，例如张三采集的某种野花开花的数据。原始数据只能必然地被认为是对特定的数据主体的计算机操作所必需，例如对于张三的野花数据进行处理所必需。与之相反，海量、来源广、分布散、价值不清晰的大数据的特意收集，就意味着它们要被加工分析、提炼挖掘出可以用于生产、经营等商业活动的价值相对清晰的数据。这些被特意收集的数据集也完全可能被其他竞争者所需要，此时就必然有产生交换价值的可能性。

显然，数据是可以具有财产性价值的。美国《纽约州刑法典》第 155 条规定了非法持有被盗窃的财产罪，并规定财产是任何金钱、动产、不动产、计算机数据、计算机程序、商品、物质或事物，只要具有价值。如果法院认为窃取电话信用卡号码后，只有在持有该卡的情况下才构成犯罪，那么将卡号记录在自己所有的纸上或者自己的记忆中就不是犯罪。这种观点的非逻辑性在于，被持有的卡的卡号并没有比不被持有的卡的卡号更具有价值，号码本身才是关键的事物，具有内在的价值，因为仅仅持有号码就能使得持有者拨打电话。^{〔38〕}事实上，我国司法也承认了数据可以在赃物犯罪中作为财产。2011 年《关于办理危害计算机信息系统安全刑事案件的解释》第 7 条将计算机系统数据认定为掩饰、隐瞒犯罪所得罪的行为对象。这是因为，数据犯罪已然是一个犯罪产业链，核心在于获取数据后销赃获利，对于中间窝藏数据的人应当认定为掩饰、隐瞒了犯罪所得中的无形物。^{〔39〕}既然被非法获取的数据可以被认定为赃物，数据本身具有财产性质也就不言而喻了。然而，数据的财产性质是在非法获取数据的产业链中显示的。数据的财产性价值通常在于使用该数据于某个具体的情景之中的好处，而非将该数据作为一个抽象的事物的价值。^{〔40〕}前已述及，在数字经济的情景中，特意收集的数据就具有使用之后的好处。虽然现阶段仍然面临确权争议，但我们可以搁置确权争议，根据权利束理论承认数据要素上除了可能存在个人信息利益和社会公共秩序等利益外，还存在数据处理者和经营者的财产利益。由此，我们可以展开数字经济中数据要素财产属性的刑法保护研究。

（二）数据要素财产属性嵌入的经济秩序

对于财产利益的保护可以考虑运用财产犯罪条款，但这并不能完全覆盖对于财产性数据要素的保护需求，我们需要同时注重经济秩序维度下的保护。这是因为，数据资源持有权、数据加工使用权、数据产品经营权等数据产权本质上都是围绕着数据的财产属性而展开的设计框架与运行过程。正是因为数据具有财产属性，数据才得以成为数字经济活动的基础要素。虽然数据的此种数字经济基础要素的性质以其财产性质为基础而展开，但其性质却不限于财产性质。数据资源持有权是一种基础性的财产权，在此基础上可以进行加工使用等生产经营，可以进行加工出来的数

〔38〕 See Orin S. Kerr, *Computer Criminal Law*, 5th Edition, West Academic Publishing, 2022, pp. 146 - 147.

〔39〕 参见喻海松：《网络犯罪二十讲》，法律出版社 2018 年版，第 59 - 61 页。

〔40〕 See Orin S. Kerr, *Computer Criminal Law*, West Academic Publishing, 2022, pp. 149 - 150.

据产品的经营，并可以同时产生和维护市场竞争优势。对财产性质进行了充分的界定，就能进一步确认相关的生产经营利益和竞争利益、市场秩序。只有在早期的简单交易中，财产性质才和经济活动没有紧密联系。在出现成熟市场之后，财产性质必然嵌入到整个经济活动中，涉及竞争利益和市场秩序。所以，刑法规范在数字经济时代也需要在财产刑法规范之外考量经济刑法规范的保护。

刑法对于市场（经济）秩序的构成性，根据法默教授的研究，在于三个层面。^{〔41〕}首先，刑法规定了财产安全（反对盗窃）和合同安全（反对欺诈），这对于个体能够追求自我利益的稳定社会秩序具有基础性的作用。其次，刑法规定了市场的界限，即能够被买卖的对象是什么，能被允许的交易类型有哪些，能缔结交易合同的主体有哪些，由此规定了能够商品化的东西及其能被交易的条件。最后，刑法规定了市场的完整性，确保了市场的公平有效运行。有了刑法在上述三个层面的构成性保障，市场和经济才能在最基本的层面上得以运作和展开。第一个方面的财产安全保护显然是由财产刑法规范来完成。第二个方面的界限确定，主要是由市场秩序中的非法经营规范来完成，这在数据要素市场形成的初期还不是一个急迫的问题。第三个方面的市场完整性是由市场（经济）刑法规范来保障。所以，后续两个部分将分别探讨财产刑法规范和市场（经济）刑法规范如何对数据要素的不同法益性质进行保护。

需要说明的是，我国刑法中广义的市场秩序为第三章的市场经济秩序，包括狭义的市场秩序（第八节）和知识产权秩序（第七节）。狭义的市场秩序也可认为是前七节没有涉及的市场经济秩序的兜底，但其核心内容包括正当竞争的市场秩序。

四、数字经济中数据要素的财产刑法保护体系

以扰乱公共秩序的计算机犯罪来制裁侵害数据安全的行为，此种刑法思路早已有之，迄今仍有影响。^{〔42〕}然而，这种思路在当代需要被反思和限制，以顺应经济文明演进中人们的生活利益形态迭代的趋势。网络用户行为痕迹数据包括浏览记录、下载记录和搜索记录等，这些类型繁多的大数据经过云计算、人工智能分析等信息技术的处理，可以产生极大的经济效用，其财产价值日益凸显。与之相比，这些大数据与系统安全、公共秩序的联系却并不明显。如果说利用 cookies 技术记录的用户痕迹能够帮助用户快速地登录账号，不用再次输入账号、密码，那么删除了记录就妨碍了系统内数据的可用性，妨碍了用户的快速登录，这些记录数据与其生产、工作或生活有效进行的秩序直接相关。然而，非法获取这些记录数据则难以涉及此类秩序（除非是非法获取了上述的身份认证信息、影响其登录）。此时，认定为相关的财产犯罪更能实现公平的标签效应，准确地反映行为人相关行为的罪行特质。再者，前已述及，计算机犯罪只能保护系统内存储、处理、传输的数据安全，如果数据和系统没有直接联系，例如存放于独立的设备中，则不受计算机信息系统安全罪名的保护，此时更加需要反映数据特殊性质的个人信息犯罪、财产犯罪

〔41〕 See Lindsay Farmer, *The "Market" in Criminal Law Theory*, 85 Modern Law Review 435, 454 (2022).

〔42〕 参见张浩然：《数据财产与数据安全法益保护的重叠及协调》，载《法律适用》2022年第9期。

等相关罪名的保护。

以上论述承认了侵犯数据资源持有权和数据加工使用权的行为应当被考虑在财产犯罪的涵摄范围内，但数据的财产性何以具体得到财产刑法的保护？这主要涉及有关行为应被认定为盗窃、毁坏抑或破坏生产经营的问题，以及承认数据财产犯罪的法律政策与刑法技术问题。

（一）数据财产犯罪的行为类型区分

传统财物的物理性意味着不可复制和排他占有，因此传统财物被盗取后，权利人难以再同时占有财物和行使使用、收益或处分的权能。而数据的非物理性意味着可复制性和非竞争性，因此数据被盗取之后，数据资源持有权的权利人仍然可以同时占有自己的一份数据并发掘和利用数据所蕴含的信息和价值。在此意义上，数据的盗取行为和传统财物的盗取行为具有的危害性和危害方式迥异，有必要进行单独的刑法评价。^{〔43〕} 根据《数据安全法》第 3 条，数据是指任何以电子或者其他方式对信息的记录。是故，我们可以参考以非电子方式记录的信息被盗是如何处理的。

英国在 1979 年就有地方法院认定试卷中的信息不能被盗窃。^{〔44〕} 美国也有法院认为，源代码数据可以被物理性地具象，例如写在纸上，但背后的知识财产是无形的，它不能构成被盗的财产。^{〔45〕} 最主要的理由仍然是数据及其承载的信息是非竞争性的，一个数据信息不可能故意地被权利人所不知，然后分割或转让给他人。其次是因为除了个体被授权控制某些信息使用的有限情形，例如知识产权或限制泄密，赋予对数据排他性的所有权会导致不利的社会、经济后果。^{〔46〕} 在社会后果方面，主要是可能限制信息流通和言论自由；而经济后果方面，主要是限制竞争和垄断。至此我们可以看到，主要的反对理由是教义性的，而次要的反对理由是政策性的。

反对将数据信息作为财产保护的核心理由是，数据信息难以被人们实际控制，人们难以有效地确定在特定时间点谁是特定数据信息的所有者。传统的物理性财产能被人们实际控制，所有者有权排除他人的获取或使用，未经同意拿走该财产是盗窃。财产被盗窃是一个零和游戏，即行为人获取财产的同时权利人百分之百失去了财产。数据被盗除了在例外的情况下同时发生获取和排除，例如修改了获取数据的密码，其他时候往往意味着被复制，即行为人和权利人都各自占有一份相同的数据，权利人失去的仅仅是此前享有的对数据的独占，这不是一个零和游戏。在享有独占的情况下，可能通过特殊立法将相关行为设立为一种特别的盗窃。美国俄勒冈州规定，故意获取或使用计算机，意图盗窃财产性信息的，构成犯罪。^{〔47〕} 例如行为人通过损害权利人对密码的排他性占有利益而有效地剥夺了密码的价值，这就构成该法规定的盗窃。^{〔48〕} 问题是，考虑到盗窃行为在数千年以来反映的都是财产必然是有形物的世界现实，财产盗窃必然是零和游戏的形

〔43〕 参见于改之：《从控制到利用：刑法数据治理的模式转换》，载《中国社会科学》2022 年第 7 期。

〔44〕 See *Oxford v. Moss* (1979) 68 Cr. Ap. R. 183.

〔45〕 See *US v. Aleynikov*, 676 F. 3d 71 (2d Cir. 2012).

〔46〕 See Alex. Taylor & Micheál Ó Floinn, *Bitcoin burglaries and the Theft Act 1968*, 3 Criminal Law Review 163, 175 (2021).

〔47〕 See Or. Rev. Stat. Ann. § 164.377 (2) (West 2012).

〔48〕 See *State v. Schwartz*, 21 P. 3d at 1136–1137.

象，刑法是否应当将并非零和游戏的财产剥夺行为认定为盗窃。如果盗窃在现代人观念里的形象仍是如此，如何将此形象与盗窃财产性信息的罪行协调起来？要知道，罪行是沟通和传播关于行为人为人的信息的标签，如果未能足够准确地用罪名和罪状传达行为人的罪行，会导致对行为人在刑事司法系统内未来处境的不适当决定，也会剥夺系统以外多方获取必要信息以评估行为人特性的机会。^{〔49〕}如果盗窃罪直接涵盖盗窃财产性数据的行为，很可能与大众心目中盗窃零和游戏的观念形象大相径庭。

如果是立法特别规定盗窃财产性信息的罪行，那么通过特定的罪状和罪名，可以传达出此类盗窃与传统盗窃的相似性和不同之处。相似性在于，盗窃财产性信息在某种意义上也存在零和游戏，比如盗窃财产性数据使得密码等信息失去了价值，而这些信息唯一的价值目标就是保护权利人排他地控制相关的信息，同时也使得权利人对于数据资源的支配与安全持有发生了有违其意思的变动。在数字经济中，持有大量数据资源的目标也主要在于控制该数据资源的获取和使用范围，以获得自身的竞争优势和发展潜能，或者获得提供或许可他人持有、使用该数据资源的经济利益。不同之处在于，财产性信息的盗窃中权利人仍然可以使用被盗窃的密码等信息。在数字经济中，被盗的数据资源也仍然能为权利人所加工使用。我国台湾地区“刑法”单独增设最后一章“妨碍电脑使用罪”，在第359条规定了未经允许取得、删除、变更他人电磁记录罪，打击“致生损害于公众或他人者”的情形。虽然在立法时没有预想到数据作为财产的情形——预想的主要是妨碍计算机运行的损害情形，至多还包括损害由电磁记录组成的网络虚拟财产的情形——但却在客观上可以涵盖盗取数据财产的损害情形，因为其中的电磁记录（数据）不要求是在计算机系统内，还可以是在相关设备中，这就包括了所有的数据。

所以，我们可以理解英国1979年的牛津诉莫斯案的判决并没有从根本上排除用刑法保护机密信息数据的可能性。英国学者认为，也许正是出于对机密信息时效性过于短暂的担忧，才做出了考前盗窃试卷的相关判决。这并不意味着没有不法行为，而是表明最好把它留给民法而不是刑法来评价，也不宜将与使用机密信息而不是收集机密信息相关的行为认定为犯罪。^{〔50〕}这就涉及财产性数据信息是否应当获得刑法保护以及如何获得保护的 policy 问题了。在数字经济背景下，数据往往是机器智能运算的原材料，数据蕴含价值的可能性是长久存在的，并不存在类似牛津诉莫斯案中该信息对人们而言只在考试期内短暂有效的问题，所以在政策考虑上并非最好留给民法处理。

此外，删除企业数据库中的数据，可以认定为故意毁坏财物，因为数据可以被认定为财物，而删除行为导致数据不可逆转地失去，无法恢复，或恢复存在重大困难，此时是实质性地破坏了权利人的占有，符合故意毁坏财物的构成要件。^{〔51〕}然而，删除数据的行为不一定仅仅构成故意毁坏财物罪，因为具有财产属性的数据可能具有特殊性，例如在功能上主要是服务于特定的生产

〔49〕 See James Chalmers & Fiona Leverick, *Fair Labelling in Criminal Law*, 71 *Modern Law Review* 217, 224 - 239 (2008).

〔50〕 See Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates*, 2nd Edition, Routledge, 2019, p. 142.

〔51〕 电子邮件、照片等数据具有使用价值，可以作为财产加以保护，此类数据的删除或篡改行为可以认定为故意毁坏财物。参见张明楷：《刑法学》（第6版，下），法律出版社2021年版，第1218页。

经营活动，故而删除生产经营必需的企业数据的行为可同时构成破坏生产经营罪，^{〔52〕}即以毁坏财物的手段达到破坏数字经济中企业生产经营活动的目的。例如行为人删除某支付公司代码管理服务器数据，导致公司无法正常从代码管理服务器下载产品源代码，影响了公司正常的生产经营活动。^{〔53〕}破坏生产经营罪能够更为全面地反映整个行为方式和危害，实现较为全面的刑法评价。同时，删除行为不一定能够达到“毁坏”财物的程度，但只要造成数字经济中企业的生产、经营活动难以为继，损失数额较大，就可认定为破坏生产经营罪。

最后，破坏生产经营罪还可以覆盖那些新形式的侵权行为，如拒绝服务攻击，它压制数据，而不是修改或删除数据，再如掺入数据以破坏数据要素质量的行为。这种妨害数据正常使用的破坏行为不仅在公司、企业需要应用该数据进行固有的生产、经营活动时破坏生产经营，而且在特定的大数据公司对数据进行清洗、比对等数字经济时代的新型生产、经营活动时也破坏生产经营。此时，犯罪行为侵犯的是数据的加工使用权，即持有数据的权利人无法按照预期对数据要素进行加工使用，而这种加工使用的活动是数字经济时代的一种重要的数据生产经营活动。

（二）数据财产犯罪的政策与技术问题

在解决了类型区分的问题后，我们仍然面临政策性問題，即我们是否应该将数据非法获取的行为予以犯罪化。利用财产刑法规范去打击，面临的谦抑性问题是，若没有直接损害公共的利益如市场经济秩序，对于直接的财产损害是否不需要刑事处理。计算机犯罪的立法给出的答案是否定的。这涉及数据非法获取行为的泛化，需要刑法的治理。十年前，澳大利亚学者就认为，个人电脑的普及和互联网的出现使人们拥有了前所未有的储存和传输信息的能力。这种通信基础设施现在在商业经营和社会发展中都极为重要，其重要程度在 1970 年代中期是无法想象的。它也为未经授权的信息访问提供了明显的目标，无论访问行为是作为犯罪活动的先导，作为获取竞争对手的商业机密的手段，还是仅仅出于好奇。信息从来没有像现在这样便携、可获取、易受攻击。^{〔54〕}在信息革命和数字经济的浪潮中，数据受到刑法保护的必要性也凸显出来。最近十年，刑法针对数据的财产性质，或者说数据在经济活动中的重要价值，予以特别保护的倾向变得明显。美国学者认为，我们生活在一个财产越来越无形的世界，这种状况很可能会愈发明显。随着财产变得无形，它有一种越来越脱离个人物理性控制的趋势。他人获取我们储存在云端的数据密码使得我们失去了密码的排他性占有所提供的隐私与安全感。^{〔55〕}

根据《模范刑法典》的立法理由，刑法应当打击那些特别打扰社群安全感的有害行为，一是危害特别严重的行为，二是危害小但更可能被那些明显不尊重他人财产所有权的人施加在我们身

〔52〕 参见于改之：《从控制到利用：刑法数据治理的模式转换》，载《中国社会科学》2022 年第 7 期。

〔53〕 参见广东省深圳市南山区人民法院（2018）粤 0305 刑初字第 1923 号刑事判决书。

〔54〕 See Jonathan Clough, *Data Theft? Cybercrime and the Increasing Criminalization of Access to Data*, 22 Criminal Law Forum 145, 146 (2011).

〔55〕 See Susan W. Brenner, *Bits, Bytes, and Bicycles Theft and Cyber Theft*, 47 New England Law Review 817, 851-852 (2013).

上的行为。^{〔56〕}英国枢密院在无形配额的盗窃案中也提出，如果一件自由流通物显然是不诚实交易的对象，在权利人被剥夺了它所赋予的利益时，认为它不可能被偷走是很奇怪的。^{〔57〕}相对而言，在牛津诉莫斯案中，没有迹象表明被意图用于特定批次考试中作弊的试卷信息具有任何商业价值。这涉及它是否可以公开交易的问题。如果货币在流通，有些东西就必然在被交易，法律试图通过将这种商品视为财产来打击不诚实获得这种商品的行为，这并非不合理。^{〔58〕}数据要素的大规模交易使得将数据视为财产的合理性显现。2023年财政部发布的《企业数据资源相关会计处理暂行规定》正式将数据资源确认为经济主体的无形资产或存货等资产类别。

第二个政策性问题是，用刑法保护数据的财产性是否真的会阻碍言论和信息自由、促进垄断的发生。我们必须明确，言论和信息自由不是绝对的，著作信息的传播也是如此，必须受到知识产权的限制。对于个人、企业乃至政府合法掌握的数据，就得依照合意的规则进行保护，而非可以任意地去获取和使用，否则将给合法生产、收集和挖掘数据的主体带来巨大的不确定性，打击其积极性，反而有损信息和言论自由的根基。当然，在刑事政策上，应当以“情节严重”限定打击范围，而且基于数字经济时代数据流通和共享的政策理念，应当严格限制未经同意侵犯数据财产权利的认定，对于权利人授权态度不明、授权后又撤回授权、处理已公开数据的情形，应当基于合理使用原则肯定其他数据处理行为的正当性。

同理，我国反垄断法律在本质上反的是滥用垄断地位的行为，而非垄断本身。赋予企业一定的数据财产权并不排斥赋予个体一定的数据财产权。例如个体对其全面的个人数据具有数据可携带权之后，可以参与到数字经济中的数据流通当中，这能在较大程度上消减赋予企业数据财产权带来的垄断问题。通过个人数据交换，新兴产业和商业创新将更容易获得重要的生产资料，从而更公平地与超大型企业竞争，促进市场在资源配置中发挥决定性作用。^{〔59〕}同时，其他数据收集者从数据的原始来源如个人数据主体处直接采集的行为，并未侵犯他人对已经从同一原始数据出处收集、转化和存储的数据享有的权利。

最后是刑法技术性问题，即我们是否应该适用其他的刑法条款，例如财产犯罪条款或市场秩序犯罪条款，而非继续依赖计算机犯罪条款。首先，如果我们只依赖计算机犯罪来解决数据的非法获取等不法行为的定罪量刑问题，那么会面临一些数据的不法获取并不符合计算机犯罪的构成要件的情况。现有的计算机犯罪要求的数据都是计算机信息系统内存储、处理、传输的数据。然而，我们在数字经济活动中的数据并非都是如此。一个U盘、闪存、硬盘、软盘、光盘等外接存储设备中的数据，在该设备连接某个计算机信息系统时，可以认为是该系统正在或将要存储、处理或传输的数据，但在未连接时，就难以做如此的技术性解释。云端存储、传感器存储和传输中的数据也可能面临类似的技术性解释障碍。所以，一个并未对任何计算机信息系统的存储设备中的数据实施非法获取等侵害的行为，并不能构成我国现有的计算机

〔56〕 See Model Penal Code § 250.7 cmt. At 44 (Tentative Draft No. 13, 1961).

〔57〕 See Attorney-General of Hong Kong v. Chan Nai-Keung [1987] 1 WLR 1339, 1342.

〔58〕 See Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates*, 2nd Edition, Routledge, 2019, p. 143.

〔59〕 参见谢楚鹏、温孚江：《大数据背景下个人数据权与数据的商品化》，载《电子商务》2015年第10期；刘权：《平台互联互通的困境与法治回应》，载《中国应用法学》2023年第3期。

犯罪。其次，如果不承认该设备中的数据是财产，就只能依照将该设备本身认定为财产的思路来处理。正如美国法院认为，将雇主的源代码数据通过电子的方式下载然后上传到德国的服务器上，再下载到他自己的计算机上，是通过电子的方式转移代码数据，并没有获得对任何事物的物理性占有。相反，用雇主的纸张产生代码数据的副本，虽然代码数据是无形的，但雇主的纸张却是有形财产，是可以被盗窃的财产。^{〔60〕}但只认定盗窃数据的载体，通过保护载体的价值来保护数据能够实现罪刑相适应吗？至少在我国注重财产价值数额的现阶段，答案显然是“不能”。

五、数字经济中数据要素的经济刑法保护体系

以上探讨主要解决了侵犯数据资源持有权和加工使用权的犯罪定性问题，接下来主要探讨侵犯数据产品经营权的定性问题。学者认为，企业数据的相关收集和分析行为主要目的在于增强其在数字经济市场竞争中的优势，所以相关数据的窃取行为应当被评价为非法获取商业秘密罪而非盗窃罪。^{〔61〕}这涉及收集数据的加工使用权和分析后得到的衍生数据产品经营权的保护。更有观点认为，对于收集的数据进行脱敏、清洗、加工和整合等处理环节之后得到的衍生数据一概属于刑法上的商业秘密。因为数据权利人在数据收集后的分析和衍生过程中会采取适当的保密措施来维护衍生数据的秘密性，且衍生数据具有实用性，因为它们是一种具体的方案或形式，可以直接用于商业实践。^{〔62〕}这涉及衍生数据的产品经营权保护。然而，保密性和实用性的论断不符合衍生数据的商业实际。

（一）数据产品的知识产权保护路径

对于保密性，已经有研究指出，只有权利人对从收集的数据中挖掘得出的数据做了保密化处理，该衍生数据才属于商业秘密。如果权利人未做保密处理，则只是普通型的衍生数据。^{〔63〕}可见，并非所有的衍生数据都当然地满足保密性。例如，医院用药量数据和统方数据，可以经过分析和处理产生新的衍生数据，大众停车位置数据也可以经过分析和挖掘得到新的衍生数据，但这些衍生数据不一定会被采取保密措施，所以它们不一定符合商业秘密的要求。哪怕是用计算机信息系统进行存储，也不一定会设置登录的账号、密码，更何况在用其他不与计算机信息系统连接的设备进行存储时，经常不设置获取其中数据的密码。商业秘密中的保密性具有特定的意义，并非只要采取了保密手段就满足商业秘密中的秘密性。商业秘密的秘密性是指不为社会上其他公众和竞争者所知，以维持其竞争优势。其秘密性是一种特殊的结果状态，而非仅仅是一种手段。例如，淘宝公司根据用户上网痕迹海量数据开发的“生意参谋”数据产品能够为店铺商家提供大数

〔60〕 See US v. Agrawal, 726 F. 3d 235 (2d Cir. 2013), 251-252.

〔61〕 参见于改之：《从控制到利用：刑法数据治理的模式转换》，载《中国社会科学》2022年第7期。

〔62〕 参见刘双阳、李川：《衍生数据的财产属性及其刑法保护路径》，载《学术论坛》2020年第3期。

〔63〕 参见张弛：《互联网背景下财产概念的流变及对刑法适用的影响》，上海交通大学2019年博士学位论文，第238-240页。

据分析参考，这种数据产品需要用户订购，在计算机上获得服务。^{〔64〕}可见，淘宝公司对这一衍生数据采取了保密措施，但我们不会认为这是一种商业秘密，因为这是公众只要付费订购就能获取的信息，只具有有限的保密性，也即具有有限的公开性。所以，尽管某一主体通过提供“远程登录已订购涉案数据产品用户电脑”技术服务的方式，招揽、组织、帮助他人获取涉案数据产品中的数据内容以从中牟利，但这并未侵犯淘宝的商业秘密，只是一种未经授权亦未付出新的劳动的不正当竞争行为，有碍数据经济产业的发展。^{〔65〕}

对于实用性，衍生数据并非都是作者提到的预测型、统计型或指数型衍生数据，能够直接用于商业经营活动中。医院用药量数据和统方数据所产生的衍生数据，或者市民停车位置数据所产生的衍生数据，固然可以作为一种数据产品而直接具有商业应用价值，但是，围绕着整理、分析、发掘等整个衍生过程所产生的数据模型则不一定直接具有商业实用性。在衍生过程中发挥关键作用的学习模型，以及学习模型经过反复的机器学习所形成的智能化知识模型，是专属于特定衍生数据挖掘者、包含了其智慧的数据处理工具和程序架构。^{〔66〕}此时，数据模型是一种特殊的数据呈现，更多是一种一般性的知识、经验或智慧，即可能挖掘出实用性衍生数据的数据工具，而非商业活动中实用性的衍生数据本身。作为实用性衍生数据的挖掘工具的学习模型，及其生成的智能化知识模型，可以是一种计算机程序，受到侵犯著作权罪的保护，即禁止未经许可而复制该模型。^{〔67〕}

既然衍生数据不一定都符合商业秘密的保密性和实用性，那么，收集的初始数据更不一定符合商业秘密的保密性和实用性。此时，数据收集者对数据还未开始进一步处理，不管是海量的结构化数据，还是海量的非结构化数据，抑或是海量的动态数据流，往往都比处理后得到的衍生数据价值要低，数据收集者很可能不会费力去做好保密措施。这些收集的初始数据仅仅是人类、机器或自然活动的原始反映和记录，大概率不能直接应用于商业经营活动的实践当中，否则就没有必要进一步处理它们以获取真正具有实用性的衍生数据了。所以，衍生数据不一定能得到侵犯商业秘密罪的保护，收集的初始数据更不可能得到该罪的保护。我们必须寻求其他的刑法保护。

（二）数据产品的市场秩序保护路径

我国早已将特殊数据通过各类秘密相关犯罪予以保护，还通过计算机犯罪保护计算机信息系统中存储、处理、传输的数据，通过公民个人信息犯罪保护具有个人性的数据，但对不涉密、不涉及个人，也不在计算机信息系统内的数据（如存于U盘、硬盘等计算机相关设备中的数据）保护不足。而且，用上述既有罪名进行保护也忽视了数据的财产性质。我国学者认为应当在商业秘密条文之后新增规定，规制数据盗用行为。^{〔68〕}但是，数据不一定涉及知识产权。商业秘密之外的邻接权、数据专有权等知识产权立法保护路径可以实现部分数据的刑法保护，但知识产权路

〔64〕 参见浙江省杭州市中级人民法院（2018）浙01民终字第7312号民事判决书。

〔65〕 参见浙江省杭州市中级人民法院（2018）浙01民终字第7312号民事判决书。

〔66〕 参见张弛：《互联网背景下财产概念的流变及对刑法适用的影响》，上海交通大学2019年博士学位论文，第212页。

〔67〕 参见张弛：《互联网背景下财产概念的流变及对刑法适用的影响》，上海交通大学2019年博士学位论文，第241页。

〔68〕 参见杨翱宇：《美国法信息盗用制度的演进及其对我国数据财产权益保护的启示》，载《政治与法律》2019年第11期。

径仅仅是市场经济秩序保护的一类路径。

在数字经济的视野下，非法获取和使用数据的行为规定在兜底性的扰乱市场秩序罪中更合适。2022 年 11 月，国家市场监督管理总局公布了《中华人民共和国反不正当竞争法（修订草案征求意见稿）》，重点回应了数字经济公平竞争的实践需要，正如修订说明中所言，“随着新经济、新业态、新模式的层出不穷，利用数据、算法、平台规则等实施的新型不正当竞争行为亟待规制”。该征求意见稿明文列举的典型商业数据不正当竞争行为包括：以盗窃、胁迫、欺诈、电子侵入等方式不正当获取其他经营者的商业数据；披露、转让或者使用以不正当手段获取的其他经营者的商业数据。这些行为显然是对新型市场秩序的新型扰乱方式。这就是鉴于僵化、滞后的法定知识产权制度，构建企业事实上合法控制数据的支撑保护制度。^{〔69〕}

概言之，若数据违法行为涉及特定类别的机密信息，可以用诸如计算机数据和系统、商业秘密、内幕交易、知识产权、隐私、国家安全等有关领域的罪名去保护。但数字经济背景下的数据并非都能用这些关注数据机密性的罪名去加以保护。这其中主要的区别就在于，强调信息机密性的诸多罪名，是根据信息的既定特定类型来加以保护的，而数字经济中数据的刑法保护则强调要对数据本身加以保护，不论其承载了何种信息内容。这是一种预防性、综合性的保护。其预防性在于，在没有挖掘出具体的信息种类之前，就加以保护；其综合性在于，可以挖掘出的信息种类不是单一的，而是多种多样的。既然是一种预防性的、综合性的保护，那么兜底式的市场秩序保护显然比专业领域的知识产权保护更契合数字经济视野下的数据保护。对于他人合法控制的原始数据的肆意加工使用，以及对于衍生数据的非法披露、使用或者允许他人使用等行为，是可能严重扰乱数字经济中数据要素市场和产业秩序的犯罪，需要扰乱市场秩序罪的持续、密切关注。

六、结 语

随着互联网和数字技术的普及，数字经济很容易受到包括数据犯罪在内的网络犯罪的影响，我们正坐在一个定时炸弹上，这对任何个人、任何公司和整个数字经济都是有害的。^{〔70〕} 探求数字经济中数据的财产类型及其面临的侵害行为类型，历史性地反思和体系化地应对，是确保数字经济持续发展的关键一环。经济文明演进中人们的生活利益形态迭代，刑法对人们生活利益的识别、保障和实现也应有新的因应理路，以回应和牵引现代经济文明与刑事法治的重要价值。^{〔71〕} 从解释论的立场看，侵犯数据资源持有权和数据加工使用权的行为，可能符合盗窃、毁坏、破坏生产经营的犯罪构造。但鉴于盗窃行为排除占有的固有形象，对盗窃数据行为的单独立法是体现数字经济基础要素公平保护的标签。在解释论上，数据产品经营权的保护难以依赖固有的侵犯商

〔69〕 参见张浩然：《从创设型机制到支撑型机制：数字时代信息财产法律保护的范式转型》，载《武汉大学学报（哲学社会科学版）》2024 年第 1 期。

〔70〕 See Aarushi Chopra, *Criminal Threat of Cyber Data Theft: An Analysis under the Indian Criminal Law*, 18 *Supremo Amicus* 23, 31 (2020).

〔71〕 这在数字技术发展促进的经济文明演进中亦是如此。参见焦艳鹏：《元宇宙生活场景中的利益识别与法律发展》，载《东方法学》2022 年第 5 期。

业秘密罪等知识产权犯罪来进行，而更需要立法论上扰乱市场秩序罪的更新。数据加工使用权的一些保护情形亦是如此。

至于认定财产犯罪或经济犯罪后，对其危害性程度的认定问题，数据交易所等专业机构可以全方位、多维度评估数据产品质量，出具专用质量评估报告，并高效化、智能化评估数据产品价值，出具专有资产评估报告。限于主体和篇幅，此处不能充分展开。但两种情况下基于法益测量的入罪程度和量刑阶梯判断有一个明显的区别。在数据的财产法益情形中，主要依赖数据的财产价值评估，聚焦被害人直接损失。在数据的经济秩序法益情形中，虽然也看被害人的经济损失，但这种损失是由竞争优势的丧失带来的，需要系统性评估数据的市场价值之外的收集成本、加工成本、运营成本、市场的地位、市场的前景、市场的周期等因素，同时可以较为顺畅地通过行为人经由获取竞争优势而获得的不当利益来评估被害人的经济损失。

Abstract: More than a decade ago, China's criminal law began to establish public order crimes to protect the confidentiality of data, but this mainly responded to the concerns of members of society about the content of data in the information economy. In the current digital economy, data is no longer just information directly provided to humans to support supply chain collaboration and mass customization, but mainly in big data to offer cloud computing and artificial intelligence with raw data as production elements. Personal, corporate, and public data are all entering this value chain and are all at risk. The property and economic nature of data are increasingly prominent, and members of society pay more and more attention to the protection of data property rights such as the right to hold data resources, the right to process and use data, and the right to operate data products. Infringement of the right to hold data resources and the right to process and use data in the digital economy shall be identified as theft, destruction of property or destruction of production and operation according to the specific circumstances. Among them, given the inherent image that theft excludes others' possession, it is desirable to have special legislation for data theft to show distinction and fairness. After the emergence of mature markets, the property nature of data is necessarily embedded in the entire economic activity, involving competitive interests and market order. Among them, the infringement of the right to operate data products is more of the behavior that seriously disturbs the market order of the digital economy, rather than the infringement of intellectual property rights.

Key Words: raw data derived data public order data property data competition

(责任编辑：林涸民)