

计算机信息系统作为财产的 私法保护

张浩然*

内容提要：数字经济催生各种新型财产形态而要求完善财产权制度，理论上多通过逐一界定客体属性构造财产权模型，非物质财产形态的多样化与动态性使传统制度模式面临困境。不同于传统工业经济，数字经济的市场交易形式由商品交换转变为平台提供服务，企业将各种生产要素纳入平台组织整合开展竞争，财产保护需求由控制单一生产资料转变为控制要素活动系统，可整体性地确认计算机信息系统的财产权益而实现对各类财产要素的保护。按照“有体—无体”的财产二分框架，计算机信息系统的物理硬件可受物权法保护，代码内容的保护则主要依靠知识产权法上的技术措施制度，无法及于非版权内容，制度扩张的前提取决于计算机信息系统之上能否成立私人财产权。回归物权法视角，计算机信息系统物理层、应用层、网络层整体作为“物”成为财产权客体，所有人和占有人有权排除他人非法访问、破坏和控制计算机信息系统，限制访问系统可排除破坏技术措施的非非法侵入行为，公开访问系统则对一般公众访问负有容忍义务。在此产权框架下，权利人可通过技术措施自主进行计算机系统资源的配置、利用、收益和处分，实现平台自治与法律保护的激励相容。

关键词：计算机信息系统 财产权 知识产权 数据产权 技术措施

大陆法系一直将独立的“物”作为基本单元进行理解并以其建构财产权制度，坚持一物一权主义，每一独立财产之上有对应的财产权，每有新财产形态产生即需建立新财产权制度。随着科技的进步，财产形态经历了由物质财产到知识财产再到数字财产的转变，新型财产形态层出不穷，传统财产权构建模式的局限性愈发凸显。18世纪之前，社会经济形态以物质资料为基础，财产权被抽象为对物的支配，财产权制度相对稳定。以第一次工业革命为转折，作品、发明等知识财产的出现打破了物质财产的一元结构，知识财产类比于有体物被作为“无体物”保护，知识客体具有传播性、共享性特点而难以进行排他性控制，只能围绕其商业化

* 中国社会科学院法学研究所助理研究员。

本文系国家社科基金青年项目“数据保护的知识产权治理理论与实施机制研究”（23CFX025）的阶段性成果。

利用方式建构排他性权能组成“权利束”，这使得知识产权制度难以像有体财产权制度一样提炼出高度抽象化的客体类型、权能，而只能随着知识客体及其利用形式的发展不断调整。进入数字经济时代，非物质财产的范畴由人类主观创造的知识拓展到客观信息的数字化形式，知识客体之外如网络虚拟财产（包括网络账号、游戏装备、虚拟货币等）、数据乃至算力等新型财产范畴不断出现，加剧了由物权、知识产权为主体构成之财产权体系的调整张力。理论上多以“主体—权利—客体”的传统模式界定各类新型客体，构造财产权制度。然而，在新型财产保护中将客体作为权利内容和边界划定的依据面临两方面困难：一是由于非物质财产具有无形性、非竞争性、非排他性等特点，难以清晰地划定和对外彰显权利范围；二是随着技术发展不断有新客体形式产生，法定财产权面临不断被新技术突破的窘境。

本文无意对各制度模型的妥适性作逐一分析，而旨在基于数字经济社会组织形式变化提出另一种被忽视的制度选项，即各类要素赖以存在的载体——计算机信息系统（简称计算机系统）之上构造财产权制度，从而间接实现对其内部要素的财产保护功能。因为在数字经济环境下，社会交易形式已由大规模商品交换转变为以平台为中心的服务提供，市场竞争成为企业组织资源构造平台、提供服务的过程，平台对内不再需要通过高度标准化的财产权制度促进市场交易，对外可通过技术手段“私人定制”产权保护，财产保护需求从控制具体的生产资料扩展至控制要素活动的整体系统。计算机系统作为数字经济秩序建构的基本单元，在德国法、美国法上均被纳入财产权保护范围，成为各类新型财产利益保护的重要制度工具。我国刑法未明确将各类网络财产利益界定为财物、财产，但学说上存在财产犯罪、计算机系统犯罪等多种保护路径。在国内私法研究中，关于计算机系统的财产权制度研究却基本处于空白状态，少数学者关注到各类新型财产与其载体之间的关联性，提出了架构财产权、代码空间权、网络平台专有权等制度方案，〔1〕围绕权利客体、权益属性及制度构造存在较大分歧。基于此，本文将具体阐述这种财产保护模式转变的理论依据和现实基础，检讨现有私法体系对计算机系统保护的不足，从而探索其专门财产权制度构造，以期各类新型财产保护提供一般性制度方案。

一、计算机系统产权保护的正当性

（一）从要素产权到系统产权：数字经济财产保护的制度需求变迁

经济活动的基本任务在于解决人们需求的相互依赖性与供给的极端分散性之间的矛盾，作为第二性的财产权制度应当服务于第一性的社会资源配置现实加以构造。工业经济是以商品生产为社会供给载体、以市场交易为资源组织方式而形成的社会组织形式，价格机制是市场主体间信息传递和资源配置的主要方式，通常单一商品对消费者的效用相互独立，通过有效市场竞争可以确定产品均衡价格和最优产出。财产权制度主要为维护市场竞争的价格机制而存在，立法在各要素之上逐一界定财产权（下称“要素产权”），可实现两方面功能：一方面可解决财产交易利用中的外部性问题，避免市场失灵；另一方面，在大规模市场交易中，高度标准化的

〔1〕 参见胡凌：《数字经济中的两种财产权——从要素到架构》，《中外法学》2021年第6期，第1581页以下；吴伟光：《构建网络经济中的民事新权利：代码空间权》，《政治与法律》2018年第4期，第111页以下；吴伟光：《通过网络平台专有权实现对企业数据权益的保护》，《政治与法律》2023年第11期，第39页以下。

财产权制度可以降低交易成本、促进交易。数字经济出现后,面对各类新型财产要素,既有理论多主张构造新型财产权,默认前提是要素财产权的确立可以进一步优化市场的资源配置功能。然而,市场机制及财产权制度的功能发挥是有边界的,这种边界在数字经济时代已发生了显著变化。

在传统经济学理论中,资源配置存在组织与市场的二分,由于市场交易估价、谈判、缔约与执行都伴随着成本,面对不确定性或复杂性时人具有有限理性,尤其在信息不充分、不对称情况下交易双方的机会主义行为将导致交易难以完成,价格机制难以发挥作用。^{〔2〕}市场力所不及之处,产业组织(主要是企业)作为一种专门收集、整理和出售信息的机制对市场价格发挥补充作用。^{〔3〕}市场参与者通过一系列长期契约组合形成企业,以内部专业化分工减少有限理性,内化风险收益消除不确定性和机会主义,从而有效地决定资源流向,弥补市场在资源配置中的不完备性,^{〔4〕}在企业内部科层制中不存在分割创设独立财产权的需求。

数字经济时代,这种企业市场的二分法叙事逐渐被打破,社会资源配置主要方式由大规模市场交易转变为以网络平台为中心的资源整合和服务提供,竞争价格机制的适用空间被压缩,平台作为新型产业组织的资源配置功能大幅扩张。与传统工业经济中商品效用相互独立不同,数字经济具有典型的网络效应,各信息产品或服务对消费者的效用函数往往相互依存,系统环境、用户数量等是其内部财产要素价值的重要影响因素。在此情形下,单一商品效用具有极大的不确定性,导致有限理性、不确定性、信息阻滞等市场不完备情形逐渐普遍化,单纯通过财产权和价格机制难以实现平台资源的有效整合。平台作为一种新的生产组织形式起到了传统企业弥补市场不完备性的功能,通过一系列合同协调和风险决策,将各种商品、服务、劳动、知识等组合在一起形成新的整体性供给,将市场交易信息不充分、不对称风险及收益内部化,市场竞争基础单元由单一商品转变为网络平台。^{〔5〕}在资源配置过程中,市场机制中各类要素的财产权归属于分散化的市场主体,通过大规模交易和竞争机制配置资源;在组织内部,企业对内部生产资料拥有完整的财产权,以科层指令直接配置资源;相对于前两者,平台内部形成了一种独特的产权结构和资源配置方式。

具体而言,平台组织者打造平台内部空间、基础设施,以网络账户形式将平台空间出租给使用者,用户在网络账户内部不断生产内容,平台藉此识别用户身份并记录积累数据。在产权分配上,平台并非依靠完全的所有权收回投资,而是与用户之间形成了一种结构性分置关系:对于信息内容层面的生产资料,用户拥有有限产权,可对其生成内容占有、利用、处分,同时平台通过格式条款保留对相关内容的免费使用权;在数据代码层面,少数底层数据对于用户而言通常不具有直接价值,平台通过用户协议获得对底层数据的占有和使用权,通过挖掘聚合后的数据提供公共服务、配置资源。^{〔6〕}这种产权分置结构赋予了平台直接调配内部资源的能力,

〔2〕 参见[美]奥礼弗·E.威廉姆森:《市场与层级制:分析与反托拉斯含义》,蔡晓月、孟俭译,上海财经大学出版社2011年版,第24页以下。

〔3〕 参见[美]阿曼·A.阿尔钦、[美]哈罗德·德姆塞茨:《生产、信息费用与经济组织》,载[美]罗纳德·H.科斯等:《财产权利与制度变迁:产权学派与新制度学派译文集》,刘守英等译,格致出版社、上海三联书店、上海人民出版社2014年版,第61页以下。

〔4〕 参见曹正汉:《寻求对企业性质的完整解释:市场分工的不完备性与企业的功能》,《经济研究》1997年第7期,第76页以下。

〔5〕 参见前引〔1〕,胡凌文,第1589页。

〔6〕 参见胡凌:《数字架构与法律:互联网的控制与生产机制》,北京大学出版社2024年版,第99页以下。

在科层指令和价格机制之外催生了一种新的资源配置方式——数据机制。^{〔7〕}基于线上数据种类和数量的积累、算法和智能技术的成熟，平台在买卖双方、产业链两侧及整个生态系统提供数据采集和分析服务。完善的数据采集、处理、使用及评价反馈机制使数据能够正确显示各类市场要素的稀缺程度和消费者偏好，平台可通过代码和算法构造用户的行为规则和参数，直接调配平台及其产业链中的经济资源进行定向推送和匹配交易。

这种资源配置秩序的形成并非来自国家权力自上而下的建构，而是平台基于逐利动机私人构造的结果。除少数物质财产可通过既有物权制度保护外，多数数字化生产资料处于权属尚未界定的状态。与物理世界的运行规则由自然生成不同，网络平台的运行规则均是人为设定的，平台内部架构和代码设计可以决定数据访问的权限、范围，即使法律尚未认定特定生产要素是否构成财产并进行财产确权，平台也可通过系统架构、代码措施、算法设计等技术措施构建起平台内部的产权保护和生产分配秩序。通过与用户订立大量的格式条款协议，平台获得了这种私人分配秩序合法性的概括确认，从而完成了资源配置私人秩序的建构。然而，依靠技术措施和用户协议仅能维持平台资源分配秩序的基本运行，却难以阻止恶意侵入。在立法尚未对各类新型财产要素确权保护的前提下，诸如数据爬取、盗取游戏装备、外挂软件等数字资产盗用行为不断发生，导致平台内部资源配置失序。因此，由国家强制力保障的法定财产权制度仍不可或缺。但新型财产权制度构造需面对的已不再是传统生产组织中的市场失灵问题，而是在平台成为新的资源配置组织形式的前提下，如何保障整个平台系统内要素利用和配置架构即系统产权不受破坏，从而避免组织失灵的问题。

（二）系统产权保护的正当性解析

随着平台成为网络空间各类财产利益的载体，企业将各类商品、服务、劳动、知识进行整合构造平台。按照劳动财产理论，“只要他使任何东西脱离了自然存在的状态，并加入了自己的劳动，即附加了他自己的东西”，即具有作为财产保护的正当性。^{〔8〕}更重要的是，较之具体要素产权模式，将系统作为财产确权对象更具法政策优势。具体而言：

1. 要素产权难以周延概括和保护平台内部生产资料

传统财产权构造遵循“主体—权利—客体”模式，通过界定生产要素客体来划定支配权范围。传统经济条件下，市场交易的主要形式是商品交换，划定各种不同商品之上的财产权可促进要素流通、保障市场秩序运行。在互联网环境下，尤其随着5G网络、云技术等逐渐普及，信息产品交易不再依靠商品交换，如软件、游戏、影音等都以流媒体服务形态出现，互联网近乎非竞争性、低成本且不受时间和物理距离限制的访问形式，使内容提供者可在其平台内集中提供信息产品，用户不再实际占有任何可控虚拟财产，必须通过固定账户访问平台才能使用，市场交易由有形商品交换转变为网络访问服务，消费者购买到的是平台资源的访问权限及获得服务的资格。在服务范式之下，财产权客体难以准确界定并且不断变化，数据等要素仅是平台要求保护的生产资料之一，诸如虚拟物品、流量、注意力、推送排名、网络账号、算力等资料形式难以被准确界定，并随着平台架构拓展和经营模式改变而不断变化。但这一系列商品服务形式都以平台系统为载体，实践中存在的外挂软件、广告屏蔽、恶意跳转、网络爬虫等互

〔7〕 参见刘诚、夏杰长：《线上市场、数字平台与资源配置效率：价格机制与数据机制的作用》，《中国工业经济》2023年第7期，第89页以下。

〔8〕 [英] 约翰·洛克：《政府论》下，丰俊功、张玉梅译，北京大学出版社2014年版，第36页。

联网财产权益纠纷的主要类型，直接指向的生产要素看似互不相关，本质上都指向平台空间内部资源访问和控制权限的争夺，将整个系统作为财产权益配置的直接对象，可实现对平台内部生产资料更加全面的调整和保护。

2. 要素产权难以优化资源配置效率

在大规模市场交易条件下，财产权制度的标准化构造可以降低交易成本从而促进交易。在数字经济条件下，企业将处于高度流动状态的各类生产要素从市场抽离纳入平台，依靠数据机制进行高度个性化的资源调配，大规模同质化交易和市场竞争已非常态，依靠标准化财产权制度促进交易的必要性不再明显。同时，这种以系统架构为依托的数据机制相对于竞争价格机制更具效率而具有保护正当性。在传统市场经济视角下，个体需求偏好很大程度上被忽视，高度抽象化的厂家组织或者消费者通过规模化交易产生的价格信号开展行动、调节供需关系。^{〔9〕}在平台经济中，用户不再是抽象的消费者而是具有具体特征的人，平台通过收集海量信息和智能化处理，体现各类市场要素的稀缺程度并精准匹配消费者偏好，相对于传统市场机制实现了更大范围和更有效率的资源协调。然而，要素财产赋权本质上是通过纠正外部性问题来发挥市场配置资源的功能，无法实现对这种平台内部资源分配秩序的保护。对平台活动系统的产权保护体现为对平台内要素价值和分配秩序合法性的确认，可以保障平台通过数据机制实现更有效的资源配置。

3. 系统产权可更有效地保护平台内部要素

平台内部不再以市场而是以数据机制为主配置资源。在商品交换范式下，信息产品一旦公开交易便意味着失去控制，故只能依靠法定财产权保护其市场独占利益来解决外部性问题。数字时代的社会交易由商品交换转变为平台提供服务，财产要素流动主要依靠计算机之间的数据资源交换，企业可通过代码设定用户行为规则，实现对要素流动的私力控制。故有学者提出“代码即法律”，甚至代码是比法律更加有效的产权保护工具。^{〔10〕}以当前广泛讨论的数据确权问题为例，立法尚未进行专门的财产权构造，企业已开始借助代码技术保护数据产权并建立起基本的数据利用和交易秩序。故在进行要素财产赋权之外，另一种思路是承认和保护平台系统内的代码架构，间接实现对平台内要素产权的保护。在数据保护的讨论中，代表性理论为财产权模式，围绕数据生成、加工、利用各环节提出了不同赋权模型，尽管制度细节上存在不同，基本观点均是根据数据生成贡献将数据财产权初始配置给生产者，赋予其对数据控制、使用、处分的权利。^{〔11〕}相较而言，系统产权保护同样可实现数据控制、使用、处分的保护功能，其优势在于可以有效解决数据财产权构造中的三方面难题：

首先，数据财产权理论面临客体界定难题。财产权构建的前提是权利客体和边界可被有效界定。在“小数据”时代，数据可按照预定的关系模型收集存储并作为静态数据库存在，故可成为财产权客体而被纳入知识产权保护范围。“大数据”相对于“小数据”的显著变化在于，新一代技术架构可在短时间内对大体量、低价值密度的数据进行分析，大体量、多样性、快速变化、低价值密度之“4V”特点的大数据集成为新的生产要素，其在内容上从静态、

〔9〕 参见周雪光：《组织社会学十讲》，社会科学文献出版社2003年版，第31页，第60页。

〔10〕 参见〔美〕劳伦斯·莱斯格：《代码2.0：网络空间中的法律》，李旭、沈伟伟译，清华大学出版社2009年版，第191页。

〔11〕 参见王利明：《数据何以确权》，《法学研究》2023年第4期，第68页以下；张新宝：《论作为新型财产权的数据财产权》，《中国社会科学》2023年第4期，第144页以下。

离线数据向动态、在线数据转变，具有较高的时效性。在此背景下，在线实时数据交易已成为数据开放共享的主要形式，平台通过调用开放应用程序接口（Open API）允许第三方持续实时访问其平台数据资源，^{〔12〕}所交易的并非特定化的数据集合，而是当下不断变化以及未来可能产生的数据或持续访问数据的服务。按照传统财产权的逻辑，权利客体在具有独立性和特定性的前提下，才能对外彰显其支配范围并排除他人干涉，而大数据集合本质上是零散堆积的代码符号，具有动态性，对公众来说难以识别其客体内容边界，直接进行财产确权将存在限制网络空间行为自由的风险。相对而言，数据因其所在平台或载体而可被识别和公示，平台代码措施主动划定了要求保护的边界，为行为人了解无形、动态的数据集合的边界提供了媒介，更加具有保护的确定性。现有司法实践中，法院通常并非通过原被告数据是否相同或相似判断是否侵权，而是通过被告是否未经许可侵入原告平台判断是否构成侵权。^{〔13〕}将平台系统作为产权保护对象，可以更加有效地破解要素财产权路径下客体不确定的缺陷。

其次，数据财产权理论面临权利主体确定难题。赋权观点的基本出发点在于劳动财产理论，按照“谁投入、谁贡献、谁收益”的朴素正义观，将财产权归于其生产者，根据数据生成过程的不同，既包括组织生产的网络平台，也包括各个生产环节的参与者（如智能设备的使用者）。^{〔14〕}然而，一方面，数据生成涉及包括用户、设备运营商、平台等在内的多方合作网络，不同商业模式下界定数据生产者存在操作困境和不确定性。另一方面，这种按劳分配的朴素逻辑并不符合平台经济运行规律，因为在考虑交易成本的前提下，产权分配并非基于生产贡献，而应授予对要素价值影响最大的一方，其在经济利益激励下将会主动组织生产并实现物尽其用而避免租值耗散。^{〔15〕}平台经济下，内部各生产要素价值并不具有完全的独立性，网络属性是其首要特征。由于这种网络外部性的存在，市场无法自主配置资源，平台通过网络架构和协议安排将一系列生产要素组合成为新的商品或服务向社会提供，在价值分配中按照数据信息内容的分层形成了用户与平台产权的结构性的分置。其中，数据集合与整个平台网络的价值密切相关，成为平台直接调配资源、实现不确定的网络外部性价值的基础，故有必要保护平台对数据的产权。在此基础框架下，平台会根据数据对不同主体的效用作出进一步的安排，多数情况下普通用户不存在数据使用需求而一般由平台留存使用，企业用户根据其数据使用需求则会提出分别留存使用的要求，各自享有数据利益，即市场主体自治会选择出对数据价值影响最大的一方作出产权安排并实现自我保护。如果按照生产者标准“一刀切”地在多生产环节上进行多重权利配置，反而会导致多方主体在权利行使过程中的协调困难，尤其授予某一方用户对其数据的绝对财产权将造成平台结构的瓦解。^{〔16〕}更为合理的方式是，在初始产权分配时确认平台对其构造系统的概括产权，承认平台企业有权组织生产和分配，自行调节内部要素产权归属，从而推动实现平台公共性价值的最大化。^{〔17〕}

再次，数据财产权面临权利保护有效性难题。数字技术的出现对无体财产权保护提出了根

〔12〕 参见周汉华：《数据确权的误区》，《法学研究》2023年第2期，第6页。

〔13〕 参见前引〔1〕，吴伟光《通过网络平台专有权实现对企业数据权益的保护》文，第47页。

〔14〕 参见刘文杰：《数据产权的法律表达》，《法学研究》2023年第3期，第42页。

〔15〕 参见〔以〕约拉姆·巴泽尔：《产权的经济分析》，费方域等译，格致出版社、上海三联书店、上海人民出版社2017年版，第88页。

〔16〕 参见胡凌：《互联网“非法兴起”2.0——以数据财产权为例》，《地方立法研究》2021年第3期，第31页以下。

〔17〕 参见前引〔1〕，胡凌文，第1589页。

本性挑战,著作权领域即为著例。互联网出现之后,作品可以完美复制并不受时间、地域限制地在全球范围内传播,权利人难以实时发现、监控传播行为,导致法定权利难以得到有效保护。〔18〕数据财产权面临同样的问题,在平台技术措施未得到承认和保护的前提下,侵权者可以相对低的成本进入他人网络空间、获取数据,数据一旦脱离了控制便可无限复制,难以识别内容、不断动态变化的数据集合在他人网络后台的分析利用更是无法被监控,权利人将难以发现侵权行为、确定侵权行为人、制止侵权行为和获得权利救济。从著作权保护经验来看,代码在数字时代已成为相较法律更有效的武器,〔19〕权利人通过代码措施建立作品传播的“可信系统”将著作权保护前置化,立法可通过保护代码措施间接实现著作权保护的目标。数据产权保护同样可循此逻辑,在企业可通过代码措施对数据建立初步保护的前提下,确认和保护系统产权,以事前方式减少未经允许不当获取数据的行为,使产权保护更具有效性。

此外需要澄清的是,系统产权并非对要素产权的完全替代,在厘清二者作用边界的前提下,可形成多种保护机制的有效协同。如前所述,系统产权保护的意義之一在于,对于平台内部流动、客体无法精确界定的新型要素(如游戏道具、网络账户、数据API等),保护系统产权相对于要素产权可更好地发挥产权保护和资源配置功能,而跨平台资源流动则超出了系统产权的作用空间,要素产权保护仍不可或缺,二者可发挥互补功能而非相互排斥。仍以数据问题为例,除通过开放API进行在线实时交易,另一种数据交易的主要形式为离线数据包交易。类似于树木从林地上分离,数据从系统中分离形成数据产品后即完成了客体特定化,与传统数据库无异而可成为财产权客体。笔者认为,可参照传统数据库保护赋予投资者排除他人对数据集提取和再利用的权利。〔20〕这与系统产权保护并不冲突,因为系统产权在于对平台内数据持有、加工、利用状态的确认和保护,排除他人的不当侵害行为,不具有要素之上利益的排他性归属效能,不排斥嗣后在离线加工的数据产品之上进行确权。同时,要素财产权的实施依靠系统产权保护才能实现。如前所述,非物质财产权利保护在网络环境下面临困难,离线数据交易最大的阻碍在于数据一旦交易便可无限复制、隐蔽利用以及黑市交易,即使赋予数据财产权也难以及时发现侵权行为并有效主张权利。实践中对此相对有效的解决方式是在数据可信空间内的托管交易,即数据供应方将数据提供给平台,数据买方只能在数据平台提供的特定环境和条件下交易数据。〔21〕类似于著作权可信系统,数据可信空间的运行要求对系统产权提供保护,防止他人破坏其内部网络安全、数据控制措施,间接实现保护内部数据产权的功能。

因此,适应数字经济社会组织形态的变化,有必要对财产确权的基本单元作出调整,首先对各类要素赖以存在的系统提供产权保护,确认和保护平台内部要素的产权结构和分配秩序,在此基础上补充性地进行必要的要素财产权构造。

(三) 系统产权保护的客体识别

将整个平台系统作为新的财产客体的前提在于清楚界定其内涵和外延,这也是当前理论构

〔18〕 参见[美]威廉·W.费舍尔:《说话算数:技术、法律以及娱乐的未来》,李旭译,上海三联书店2013年版,第7页以下。

〔19〕 参见前引〔10〕,莱斯格书,第191页。

〔20〕 参见张浩然:《由传统数据库保护反思新型“数据财产权”》,《法学杂志》2022年第6期,第152页以下。

〔21〕 目前我国已有部分数据交易所(如贵阳大数据交易所)通过构建可信数据空间保障数据交易,在可信空间内进行全过程数据密文计算后最终交付计算结果,实现数据“可用不可见”“可控可计量”。国家层面将此作为数据交易的基础性架构加以推广,2024年国家数据局印发《可信数据空间发展行动计划(2024-2028年)》(国数资源〔2024〕119号),提出到2028年再构建100个以上可信数据空间,对数据流通利用全过程动态管控。

造面临的主要挑战。现有私法体系并未将之作为财产保护的直接对象，理论上以及相关领域立法存在两种界定方式。有学者倾向于将这种平台系统界定为一种类似物理空间的虚拟空间。所谓空间，是指一个容纳和承载事物或活动的环境，作为人与人之间互动、交流和协作的场所。对空间的认知已成为人类认识客观世界的重要过程与途径。在互联网构造中，人们受现实观念影响，比照物理空间关系构造网络世界，通过赛博技术将现实世界的对象以数据形式映射并存储到计算机环境中，将虚拟环境作为现实世界互动的发展延伸。因此，空间概念成为理解互联网运作和治理的重要工具，计算机之间通过互联网连接而形成的互动场域被称为“网络空间”，即以计算机软硬件、网络设备为载体构建的一种人造电磁空间，用以支撑人们在该空间中开展各类信息通信的相关活动。^[22]私法上有观点以此为基础，主张将通过代码或技术措施区隔出来的私人化网络空间作为财产授权的基本单元，并称之为“代码空间”“架构空间”“平台空间”。^[23]

在既有立法中与之相关的是，刑法和行政法上采用“计算机系统”概念作为界定互联网上承载的各种法益的基本单元。在20世纪90年代互联网发展成熟后，计算机系统即被公法纳入调整范围并对其内涵外延进行了界定。1997年刑法规定计算机系统犯罪后，2011年《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》（法释〔2011〕19号）将计算机系统正式定义为“具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等”。欧美立法以及相关国际条约和技术标准也采用了类似定义，从构成和功能两方面进行了界定。构成上，计算机系统不等于单纯的硬件，而是以下不同层面硬件、软件、网络的结合：物理层，包括计算机、服务器、存储设备等；应用层，包括操作系统、应用程序、数据库等支持硬件运行和数据处理的内容；网络层，包括局域网、广域网、虚拟专用网络等用于连接各个计算机终端的协议和链路。^[24]功能上，软硬件结合应实现自动数据处理功能，技术上至少具备信息输入输出、存储处理和控制反馈功能，才构成最小单元的信息系统。^[25]通过构成和功能相结合的界定方式，计算机系统概念具有较强的包容性，普通网站、在线游戏、微信等社交平台皆可被涵盖在内。这种包容性并非意味着可随意界定系统范围，计算机系统作为一种客观实在而存在，同一系统要求所有者有能力对其系统内所有领域进行控制变更，所有元素受统一管理控制。系统边界可通过物理边界结合逻辑边界的方式确定，由系统互连列表加以记录和体现。^[26]

两个概念从不同角度对互联网的基础单元进行了界定，二者紧密关联但侧重不同。计算机系统是互联网在技术实然构造层面的基本单元；网络空间则依赖于计算机系统呈现，其并非真实存在，而是理解互联网资源配置方式、构造人们行为互动模式的重要工具，更强调其作为互动场所的社会性特征和人的关系性要素，主要涉及网络空间治理中的用户行为、内容监管、数

[22] 参见方滨兴等：《网络空间主权研究》，《中国工程科学》2016年第6期，第1页以下。

[23] 参见前引〔1〕，胡凌文；前引〔1〕，吴伟光两文。

[24] 参见〔美〕赞姆斯·F.库罗斯、〔美〕基思·W.罗斯：《计算机网络：自顶向下方法》，陈鸣译，机械工业出版社2021年版，第34页以下。

[25] 参见张羽：《浅析信息系统边界的法律认定——从刑法保护的视角》，《保密科学技术》2023年第12期，第52页。

[26] See Marianne Swanson, Joan Hash & Pauline Bowen, *Guide for Developing Security Plans for Information Technology Systems*, NIST Special Publication 800-18 Revision 1, p. 9; Brian Sizemore, *Determining System Boundaries for Federal IT Systems*, <https://www.giac.org/paper/gsec/2882/determining-system-boundaries-federal-systems/104860>, last visited on 2025-05-02.

据治理等非技术因素。^[27]从界定财产权保护对象的角度,这种空间概念并不能阐明其内部生产资料构成,依靠人们对物理空间的认知也难以清晰地界定其边界所在,而计算机系统概念则更加清晰地界定了其内部构成和外部边界。基于此,以下将以计算机系统为对象,探寻其在私法上的财产属性及保护制度构造。

二、计算机系统产权保护的私法局限与完善路径

计算机系统已成为数字经济市场竞争的基本单元,现有私法体系内部尚缺乏对其财产属性的清晰定位和保护,有必要首先对现有制度和理论进行全面检讨,进而探索计算机系统私法保护的路径选择及制度构造。

(一) 计算机系统私法保护现状与理论探索

计算机系统在我国最早是受公法保护,1994年《计算机信息系统安全保护条例》及2005年治安管理处罚法规定了计算机系统安全的行政保护;1997年刑法增加了非法侵入计算机信息系统罪和破坏计算机信息系统罪,建立了计算机系统的刑事保护框架。通常而言,公法与私法之间存在后置法与前置法的关系,民事主体之间的财产关系首先由私法调整,严重侵害民事权益的行为才由公法规制且以私法知识为前提。^[28]但是,对计算机系统之上的财产权益,现有私法体系缺乏直接界定,有少数侵入破坏计算机系统的刑事附带民事案件涉及民事救济,但法院仅概括判决损害赔偿而未具体阐明其民事权益属性。^[29]

究其原因,既有私法财产体系以物质与非物质财产的二分框架展开,而计算机系统是一个物质与非物质内容相结合的特殊系统,难以整体地获得保护,只能区分物理层、网络层、应用层的物质财产和非物质财产进行分层保护。在物理层,计算机、服务器等硬件资产可以获得物权法保护,但仅延及硬件的物理功能和价值,应用层的操作系统、应用软件、数据库以及网络层的网络协议等代码内容(以下统称为“代码内容”)皆难以获得物权法保护。数字经济中各类财产要素以及分配秩序主要通过代码内容加以构造,这主要依靠知识产权法和反不正当竞争法进行调整。作为主要的非物质财产权制度,知识产权客体为作品、发明、商标等有价值信息,计算机系统代码构造并非其直接调整对象,由于历史的偶然性,著作权法为代码内容提供了部分保护。如前所述,互联网出现后著作权保护面临极大挑战,企业自发地采取技术措施维护作品传播秩序,《世界知识产权组织版权条约》(WCT)和《世界知识产权组织表演和录音

[27] 参见陈宗章:《网络空间:概念、特征及其空间归属》,《重庆邮电大学学报(社会科学版)》2019年第2期,第63页。

[28] 参见陈兴良:《民法对刑法的影响与刑法对民法的回应》,《法商研究》2021年第2期,第27页。

[29] 截至2025年2月12日,在北大法宝数据库中以破坏计算机信息系统罪和非法侵入计算机信息系统罪案由进行检索,共得判决书1210份,涉及刑事附带民事案件15件,法院均未对计算机信息系统涉及的民事权益属性进行分析。主要包括三类情形:1.部分案件法院认为民事救济的前提是被告侵入、破坏行为造成计算机系统内部财产的直接损失(如数据灭失、服务器更换等),网站嗣后恢复正常运行的,法院认为不存在损失而驳回诉讼请求。参见北京市大兴区人民法院(2015)大刑初字第1597号刑事附带民事判决书;北京市海淀区人民法院(2016)京0108刑初1084号刑事附带民事判决书;北京市海淀区人民法院(2018)京0108刑初651号刑事附带民事判决书。2.部分案件法院判决被告赔偿损失,但未说明赔偿依据。参见四川省射洪县人民法院(2013)射洪刑初字第226号刑事附带民事判决书。3.部分案件法院以侵权法一般条款(原侵权责任法第6条、民法典第1165条)为依据判决被告赔偿损失,但未说明侵害权益性质。参见辽宁省沈阳市和平区人民法院(2017)辽0102刑初380号刑事附带民事判决书;辽宁省阜新市新邱区人民法院(2020)辽0903刑初20号刑事附带民事判决书。

制品条约》(WPPT)选择为技术措施提供法律保护,我国著作权法也禁止规避和破坏技术措施的行为,在流媒体时代这主要体现为对计算机系统代码架构的保护。然而,由于技术措施法律保护的原因及属性模糊不清,其止步于作品内容保护,未一般性地适用于其他财产保护。作为法益保护法,反不正当竞争法可规制侵入计算机系统侵害他人财产权益的行为,此类案件大多通过反不正当竞争一般条款或“互联网专条”作为兜底条款调整。然而,反不正当竞争司法实践仍然沿着要素产权保护的思路,保护对象为各要素之上的财产利益:首先判断经营者对数据、视频等是否享有值得保护的合法权益,进而判断竞争者行为是否损害了该权益,最后判断行为的正当性。按此思路,计算机系统的独立财产地位并未得到考量,违法侵入、破坏技术措施仅作为判断行为正当性的参考因素,类似计算机系统侵入行为因涉及财产要素、损害结果不同而成立侵权与否也有所不同,对经营者在计算机系统内部自主构建的财产秩序未形成独立、稳定、可预期的保护框架。

按这种分层框架,有学者提出构建对计算机系统代码内容的专门保护,主要有两种路径:一是从传统物权法出发,将计算机系统代码内容理解为一种“空间”,类相比于房屋等有体财产,建立一种类似物权的财产权,即前述架构财产权、代码空间权、网络平台专有权模型;^[30]二是从知识产权法出发,将技术措施保护扩张至非作品内容,为计算机系统代码内容提供一般性保护。^[31]鉴于知识产权法上的技术措施制度已对计算机系统提供了一定保护,且为既有私法体系内最主要的保护制度,从维护立法体系一贯性出发,本文首先以技术措施制度为研究对象,分析其法律保护的理论基础,探索打破体系隔阂扩展技术措施保护的可行性。

(二) 计算机系统代码保护的理论检讨

著作权法对技术措施的保护包括版权保护措施和接触控制措施。前者基于著作权保护衍生而来,保护正当性及适用范围几乎不存在争议,后者用于防止未经许可阅读、欣赏等“接触”作品的行为,这超出了传统著作权的控制范畴,本质上是权利人在计算机系统内部采取的私力措施。后者的法律属性及适用范围存在很大争议,主要有两种观点:一是将之纳入知识产权框架,认为保护接触控制措施属于一项新著作财产权,应限于作品内容而无法适用于其他领域;另一种观点认为保护接触控制措施与著作权不存在直接关联,系基于对财产私力保护的正当利益,可将其保护范围由作品内容一般性地扩张至其他领域。探索这种制度可能性,需首先厘清接触控制措施保护的理论基础。

1. 知识产权理论

技术措施保护由WCT、WPPT规定,各成员国也多将之规定于著作权法,我国有学者即根据规范定位解释其制度正当性,认为其是一种未被阐明的著作财产权即“接触权”。^[32]主要理由在于,数字时代作品利用形式由获取作品复制件转变为直接体验作品内容,著作权应由控制复制扩大到控制接触,技术措施保护赋予了作者控制作品数字化访问的权利。^[33]然而,著作权法并未将之规定为一项著作财产权。著作财产权因作者作出了具有独创性的表达而自动

[30] 参见前引〔1〕,胡凌文;前引〔1〕,吴伟光两文。

[31] 参见王迁:《论规制视频广告屏蔽行为的正当性——与“接触控制措施”的版权法保护相类比》,《华东政法大学学报》2020年第3期,第59页以下。

[32] 参见熊琦:《论“接触权”——著作财产权类型化的不足与克服》,《法律科学》2008年第5期,第88页以下。

[33] See Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U. S. Copyright Law*, 50 *Journal of the Copyright Society of the USA* 113 (2002).

获得,但所谓“接触权”的产生不仅取决于保护内容是否满足作品构成要件,还取决于权利人是否设定技术措施,未施加技术措施则不存在“接触权”。若非如此,用户未经许可“接触”作品(如看一眼盗版影片)即构成侵权,可能造成动辄侵犯著作权的窘境而带来过高的社会成本。从必要性来看,“接触权”的提出源自作品传播由间接占有到直接体验的转变,因作者无法继续通过出售复制件获利,而认为有必要恢复类似物理时代作品传播的盈利模式,即赋予作者“接触权”来进行“按次计费”。现实却未按预期发展,自由访问的互联网空间发展出了“注意力经济”,作者通过信息网络传播权可界定作品传播的渠道和范围,以内容换取用户注意力而通过广告等方式间接获利,设置“接触权”的必要性不再明显。因此,法律规范的存在方式并不绝对表明法律关系的性质,从制度构造来看,接触控制措施保护与著作财产权逻辑不符,没有必要也不应将技术措施保护局限在著作权法之内。

2. 私力保护理论

私力保护理论认为,虽然破坏接触控制措施不构成对著作权的直接侵害,但作者并非仅依靠著作权获利,还可通过私力措施限制他人对内容的接触,实现信息内容的商业化价值,破坏私力措施的行为因侵犯作者正当利益而构成侵权。^[34]此种正当性论证源自虚拟世界与物理世界的类比。互联网出现前即存在“接触控制”的私力保护形式(如电影放映时通过检票防止未购票者进入),在传播范围由物之四置(如电影院)所限定的情况下,可以通过物权法来保护接触控制措施。互联网出现后,物理控制转变为电磁技术措施,物权法无法再为此种私力措施提供保护,但权利人仍具有采取私力措施保护其创造内容的正当利益,故有必要弥补传统物权法在虚拟世界的不足,为接触控制措施提供法律保护。依此观点,“只要存在这种正当利益——从他人对相关产品或服务的使用中获得报酬,即使在版权法领域之外,用于维护该正当利益的自力保护手段在不违反法律规定的前提下,就应当受到相关法律机制的保护”。^[35]从比较法实践来看,接触控制措施的保护不限于著作权内容,如欧盟1998年《对以有条件获取为基础的服务进行法律保护的98/84/EC号指令》以及日本不正当竞争防止法均规定,受保护技术措施不限于为保护作品而采取的技术措施,一切为保护影像、声音制品而采取的技术措施皆受法律保护。

私力保护理论阐明了代码措施存在的事实状态,却未释明这种法律保护的原因和边界。法律为私力措施提供保护即意味着公众负有避让义务,但并非为正当利益采取的所有私力措施皆可受法律保护。因为信息具有无形性,私力措施必须依附于载体而施加,其是否受法律保护取决于该载体对他人及公共利益的影响。如在自有住宅内举办收费画展而限制进入,该限制不会对他人利益造成显著影响,法律将予以承认并禁止他人擅自进入的行为;若在他人住宅或公共广场内采取限制措施,即使作者对作品内容享有正当利益,此种私力措施也因限制了公众行为自由而难以受到法律保护。^[36]因此,若将接触控制措施类推适用到网络空间提供一般性保护,需进一步厘清这种私力措施受法律保护的条件和边界。

(三) 计算机系统代码保护的财产法基础及待决问题

技术措施的讨论申明了一个长期被忽视的事实,即知识产权与物权制度之间存在无法割裂的功能分担关系。知识产权制度的构造方式是围绕客体利用设置排他性权利,这种排他性权利

[34] 参见王迁:《版权法保护技术措施的正当性》,《法学研究》2011年第4期,第100页以下。

[35] 前引[31],王迁文,第64页。

[36] 参见[日]田村善之:《日本知识产权法》,周超、李雨峰、李希同译,知识产权出版社2011年版,第6页。

设置同时限制了公众利用相同信息，这决定了只有达到一定的创造性高度的内容才能获得保护，并且存在较高的制度成本。较之知识产权保护，私力保护仅限于其私人控制范围，不会对公众造成显著影响，保护客体不限于达到创造性高度而可适用于一切有价值的信息。此外，所有者通过私力控制措施事先排除他人侵害，执法成本更低，保护有效性更高，可以为知识产权保护提供有效补充。既有立法对私力措施的保护可归纳为两种形态：一是借由传统物权实施的私力保护。在知识产权制度出现之前，知识产品即已存在，创作者主要通过私力措施保护产权实现。知识产权制度出现后，无法满足创新性要求的知识产品可通过私力措施保护，知识产权规制成本较高的行为也可交由私力措施调整。盖因物权保护通常限于四至明晰的物理范围而不会造成额外社会负担，在私人财产范围之内权利人可排除他人侵害，而信息内容是否具有创新性价值在所不问。二是专门的商业秘密制度。物权制度可实现一定的信息私力保护功能，特定情形下却无法发挥作用，如就技术方案、客户名单等实际应用的信息，雇员、交易相对人等经授权进入保密场所获悉后，可凭记忆直接应用和无限传播信息而不受控制。现代商业秘密制度通过财产理论、合同理论以及善意义务理论的模块化组合，扩大了私力措施的保护范围，包括两方面：一方面，与普通私力保护措施相同，其限制他人侵入私人秘密领域破解保密措施；另一方面，由于商业秘密客体为区别于公有领域的内容即不为公众所知悉而有价值的信息，私力保护将产生类似于无主物占有的利益归属效果，要求公众在私人领域之外也不得恶意获取、利用、披露受保护信息。从既有保护模式来看，私力措施保护的正当性与载体财产权和信息内容创新价值有关，二者分别决定了不同的法律保护效果：私力措施载体的财产权使公众产生不侵害义务，信息内容创新性使私力措施产生利益上的归属效果。

由此来看，接触控制措施的法律保护系传统物权秩序在数字经济中的延续。传统物理环境下，书店、电影院可通过行使物权控制他人对信息内容的接触。互联网环境下，信息传播物理载体转变为电磁载体，信息控制的侵害形式也由物理侵害扩展为侵入计算机系统、复制删除修改数据等无形方式，传统物权制度因“物必有体”的限制而难以提供保护，导致信息财产保护秩序出现真空，著作权法类比物理世界确立了对技术措施的保护。但在前述电影院等情形，法律保护的原因不仅在于权利人采取了私力措施，更在于其私人财产权。类比此逻辑对接触控制措施提供保护，根本问题在于在计算机系统的代码内容上是否具有类似于传统物权的财产权。在20世纪90年代急于回应新技术挑战的背景下，著作权法采取了特殊规定形式而未充分厘定这一问题。当前计算机系统保护的现实需求与接触控制措施保护需求类似，若类比技术措施制度建立计算机系统代码内容的一般性财产权制度，计算机系统本身的财产属性定位仍是无法回避的大前提，以下将回归传统民法视角对此作具体分析。

三、计算机系统财产权保护的可行性及制度构造

在物理世界，物权与知识产权制度在非物质财产保护中共同发挥作用。在互联网领域，计算机系统替代不动产空间成为经济秩序构造的基本单元，物权制度难以直接适用，导致非物质财产保护秩序出现真空。有必要探索有体财产制度的数字化转型，实现传统财产保护秩序在数字空间的延续。我国法一直忽视物权的非物质财产保护功能及其在数字领域的续造，作为两大法系代表性法域，美国法与德国法均存在将计算机系统纳入传统财产法保护的实践。以下结合相关比较法经验，探讨计算机系统财产权保护的可行性及制度构造。

（一）计算机系统财产权保护的比较法经验

1. 德国法

住宅自古以来就是人类生产生活的核心，在财产保护中具有特殊地位。罗马法时期的家父权及日耳曼法上的家庭领主权，均为住宅安宁利益提供保护，其不仅保护住宅财产权，而且保护对整个住宅空间秩序的支配。^{〔37〕}在德国民法典编纂过程中，由于所有权和占有制度已可实现对住宅空间支配的保护，故就其内部利用未作专门规定。^{〔38〕}但此后司法实践从历史中重新挖掘出了“家宅权”（Hausrecht）概念，经教义学演绎完成了其权利内容的体系化构造，用于网络空间非物质财产的保护。^{〔39〕}

具体而言，尽管德国民法典未将家宅权作为法定物权类型，其却可作为物权利能的集合而存在。根据德国民法典第858条的占有保护及第903条、第1004条的所有权保护，所有人和占有人对其不动产享有家宅权，^{〔40〕}包括两方面权能：一是积极利用权能，权利人可自己或允许他人进入、利用家宅空间，设定空间访问条件、使用目的、行为规则等，维持不动产空间内部秩序而实现预期用途；二是消极防御权能，权利人可排除他人对家宅空间的不法侵害。^{〔41〕}仅从规范基础来看，家宅权的内容似乎已被所有权和占有制度所涵盖，有引入冗余概念之嫌。^{〔42〕}其被广泛适用的根本原因，在于其非物质财产保护功能。德国判例法通过对所有权、占有保护的模块化再整合，赋予了家宅权独立于所有权和占有制度的新内涵，^{〔43〕}主要体现在两方面：一是家宅权不仅保护住宅的物质财产价值，住宅空间内部产生的非物质财产均可基于对不动产的利用受到保护，知识产权客体之外的体育赛事节目、表演、照片、建筑物形象等均在受保护之列；^{〔44〕}二是对非物质财产损害的事后救济，传统物权保护通常限于防止损害物的财产价值或实质妨害所有者使用其财产，却难以实现对非物质财产内容的保护和救济，在家宅权概念下，德国联邦最高法院将对不动产利用产生的成果作为物之孳息加以保护。^{〔45〕}

在物理世界之外，德国法院将家宅权概念类推适用于网络空间，创设了“虚拟家宅权”（virtuelles Hausrecht）。波恩地方法院最早在2000年提出并保护虚拟家宅权。^{〔46〕}慕尼黑第一地区法院则为虚拟家宅权的存在基础作了相对完整的教义学构造；^{〔47〕}网络运营商对存储用户内容的服务器享有所有权，根据德国民法典第903条、第1004条的规定，其可排除任何人对其服务器的利用；如果其服务器是租赁的，其作为占有人可根据德国民法典第858条、第862条排除他人对其占有的妨碍。此后，虚拟家宅权在德国地方司法实践中被广泛认可和适用。^{〔48〕}与家宅权类似，虚拟家宅权包括积极利用和消极防御两方面权能，该权利为平台保护其在网络空间建立的经营秩序提供了支配权基础。然而，德国法院并未达成完全共识，少数法院明确拒

〔37〕 Vgl. Gabriella Piras, Virtuelles Hausrecht?: Kritik am Versuch der Beschränkung der Internetfreiheit, 1. Aufl. 2016, S. 23 ff.

〔38〕 Vgl. Götz Schulze, Das private Hausrecht: Schutzrecht für die Gebrauchsnutzung von Räumen, JZ 2015, S. 382.

〔39〕 Vgl. Philipp Maume, Bestehen und Grenzen des virtuellen Hausrechts, MMR 2007, S. 620 ff.

〔40〕 Vgl. BGH NJW 2006, 1054.

〔41〕 参见前引〔37〕，Piras书，第35页以下。

〔42〕 Vgl. Christian Baldus, Das private Hausrecht: ein Phantom, JZ 2016, S. 449.

〔43〕 参见前引〔38〕，Schulze文，第381页以下。

〔44〕 Vgl. BGH NJW 2006, 377; BGH MMR 2011, 379; BGH GRUR 2011, 323; BGH NJW 2019, 757.

〔45〕 Vgl. BGH GRUR 2011, 323.

〔46〕 Vgl. LG Bonn MMR 2000, 109; OLG Köln MMR 2001, 52.

〔47〕 Vgl. LG München I ZUM-RD 2007, 261.

〔48〕 参见李陶：《体育赛事举办者转播权的私法保护》，《清华法学》2020年第5期，第140页。

绝承认和保护虚拟家宅权。^[49]理论上亦有反对观点认为，虚拟家宅权的创设会限制互联网的自由和开放，并会造成用户与平台的利益失衡。^[50]德国联邦最高法院则对此持模糊态度，尚未明确承认或否认虚拟家宅权。^[51]

2. 美国法

在计算机和互联网出现后，美国法即存在类推适用普通法财产权制度的尝试，曾分别通过适用侵害动产（trespass to chattels）及类比侵入土地（trespass to land）构建对计算机系统的财产权保护。

美国俄亥俄州南区法院最早在1997年“垃圾电子邮件案”中通过侵害动产之诉保护计算机系统。其认为，计算机服务器属于普通法意义上的动产，未经请求大量发送垃圾电子邮件，导致原告计算机系统运行速度变慢，造成对其财产价值的减损而构成侵害动产。^[52]在此后的“eBay案”中，法院继续适用侵害动产之诉并对损害作出了宽泛解释，认为即使他人的访问行为仅占用服务器小部分甚至微乎其微的空间，仍构成对他人财产利用能力的剥夺，^[53]由此赋予了计算机系统所有者排除他人未经允许访问的权利。然而，侵害动产必须以动产价值的实际损害为前提，将计算机服务器作为动产保护，则原告必须证明被告行为对其动产物理价值的减损。此后加利福尼亚州最高法院在“英特尔案”中澄清，单纯的计算机访问并不构成侵害动产，原告必须证明访问行为对计算机系统服务器的物理功能存在干扰或干扰的现实可能性。^[54]随着服务器承载力和网络带宽的发展，用户访问或网络爬虫对服务器物理功能产生的实际损害往往微乎其微且难以证明，实践中也较少适用侵害动产之诉来保护计算机系统。

与侵害动产不同，侵入土地之诉并不要求存在损害的具体事实，只要存在土地侵入行为即成立侵权。为了规制黑客侵入行为，美国联邦类推侵入土地制度制定了《计算机欺诈与滥用法案》保护计算机系统。该法案最早仅作为刑法而存在，保护对象限于涉及联邦政府利益的计算机。随着计算机的普及，1994年修法将保护对象扩大到所有连接互联网的计算机，并规定了禁止他人侵害的民事权利。类比于侵入土地之诉，所有者可禁止他人未经授权或超出授权的计算机访问行为，也可撤回授权而排除他人访问。“未经授权”和“超出授权”的界定决定了计算机系统之上财产权的排他范围，其内涵一直存在争议，早期超出网站政策、合同义务、员工权限、代码措施以及网站通常访问方式的行为皆被视为侵权，^[55]由此也导致对计算机系统的财产权保护存在广泛争议。有观点认为，互联网的特质在于其开放性，该法案赋予了计算机所有者对默认开放网络空间的排他性权利，其财产权边界不清晰且未达成充分共识，导致互联网中多数访问行为都有可能被界定为违法，极大地限制了网络空间的信息传播自由。^[56]近年来，美国法院在“领英案”及“范布伦案”中对计算机系统的保护范围作出了限定，即未经授权或者超出授权访问的前提在于将开放的互联网与私人空间相区隔，要求计算机系统所有

[49] Vgl. OLG Frankfurt/M MMR 2009, 400.

[50] 参见前引 [37], Piras 书, 第 160 页以下。

[51] Vgl. BGH MMR 2020, 391.

[52] See CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S. D. Ohio 1997).

[53] See eBay v. Bidder's Edge, 100 F. Supp. 2d 1058 (N. D. Cal. 2000).

[54] See Intel Corporation v. Hamidi, 71 P. 3d 296 (Cal. 2003).

[55] See Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 Boston University Journal of Science & Technology Law 372 (2018).

[56] See Orin S. Kerr, *Norms of Computer Trespass*, 116 Columbia Law Review 1143 (2016).

者通过技术措施明确限定一个禁止访问的“门”(gate),^[57]越过该“门”则构成非法访问;如果计算机系统并无此“门”,则可自由访问而不存在未经授权或超出授权的问题。^[58]

(二) 我国法上计算机系统财产权的可行制度构造

在非物质财富正在超过物质财富成为社会进步的主导力量的时代背景下,德国法和美国法实践展示了有体财产制度发挥非物质财产保护功能的作用路径。德国虚拟家宅权的权利基础来自服务器等物理硬件的所有权或占有,这与美国法适用侵害动产的基础相同。传统物权保护不能直接延及服务器内部代码内容,德国法通过对物之利用的广义解释,将服务器内部代码内容纳入财产权的保护范围。其优势在于回应了平台对系统产权保护的现实需求,缺陷在于缺乏对其内部非物质财产内容的界定,存在损害的不确定性,类比于住宅空间而依照服务器所在授予绝对支配权,可能对互联网的自由开放造成阻碍,这正是美国法限制适用侵害动产之诉保护计算机系统的原因。与其回避计算机系统中代码内容的定性而藉由服务器外壳对其建立一种模糊概括的支配权,更为精确的方式是,类似美国《计算机欺诈与滥用法案》将计算机系统整体作为独立的对象置于财产法上进行评价,结合社会财产观念和互动方式界定保护范围,实现私人财产利益与公共利益的平衡。但作为大陆法系国家,我国财产权制度与普通法系存在显著不同,计算机系统本身也与不动产空间存在较大差异,难以直接按照侵入土地模式构建计算机系统侵入制度。现结合我国物权法体系和比较法实践,就计算机系统财产保护制度构造如下:

1. 计算机系统整体作为“物”而成为财产权客体

计算机系统由物理层、应用层、网络层构成,由于物权的客体一般限于有体物,理论上通常将之分别评价,即认为物理层的服务器等属于物权客体,诸如计算机软件、数据库等应用层、网络层的非物质财产内容则因缺乏有体性而被排除在外。^[59]然而,界定物之范围的基本原则是遵循功能整体性,依据社会交易观念或经济需要来界定财产确权的基本单元,如果物与物之间的关系是如此地紧密,使其分离会使一个部分遭到破坏、损害或丧失效用,则在此情形,所有的部分均成为该整体物的重要成分。^[60]依此原则,计算机系统指的是具备自动处理功能的系统,只有实际具有输入输出、存储处理和控制反馈的软硬件要素才能成为最小的计算机系统,承担相应功能的软硬件具有不可分性。一方面,计算机系统作为一类特殊的物,其硬件功能的发挥高度依赖软件运行,对软件的操作将实现对硬件功能的侵害,典型如人为破解密码远程锁定他人信息设备的情形;^[61]另一方面,代码内容无法脱离电脑终端、存储设备等载体而独立存在,数据处理功能依赖硬件运行,典型如环境采样设备被破坏而导致监测数据失真情形。^[62]因此,遵循功能整体性原则,计算机系统的物理层、应用层、网络层应作为一个整体进行法律评价。

作为一个整体,计算机系统可满足物的客体要件。民法典未对“物”直接定义,通说认为,物是指存在于人身之外、能够满足人们社会需要、能为人所实际支配或控制的物质客体。^[63]

[57] See *Van Buren v. United States*, 593 U. S. 374 (2021).

[58] See *LinkedIn Corp. v. hiQ Labs, Inc.*, 141 S. Ct. 2752 (2021).

[59] 参见梅夏英:《虚拟财产的范畴界定和民法保护模式》,《华东政法大学学报》2017年第5期,第43页以下。

[60] 参见[德]鲍尔/施蒂尔纳:《德国物权法》上册,张双根译,法律出版社2004年版,第24页。

[61] 参见王琦:《数字私力救济——基于远程控制网联物的权利实现》,《法学研究》2023年第5期,第66页以下。

[62] 参见李某等破坏计算机信息系统案,最高人民法院指导案例104号(2018年)。

[63] 参见最高人民法院民法典贯彻实施工作领导小组主编:《中华人民共和国民法典民法总则编理解与适用》下,人民法院出版社2020年版,第577页。

计算机系统满足前两项要求，争议在于其是否具有可支配性。通常认为，可支配性要求物一般为有形客体，只有具有有形性、能为人感知、可触碰，才具有可支配性。计算机系统应用层的软件、数据以及网络层的各种协议却具有无形性，似乎难以单独满足可支配性要件。然而，这些代码内容无法脱离计算机系统的物理层而存在，结合在一起时便具有了可把握的形式，作为一个整体可符合物的有体性和可支配性要求。对此可借鉴计算机程序的保护思路。德国法上，计算机程序缺乏可被界定的物理特征，诸如硬盘、存储卡等数据载体却属于物而可成为交易对象，存储于载体之上的软件可作为载体的成分而获得物权保护，对软件的修改、删除将构成对载体物理属性的改变。^[64]我国法上，计算机系统整体可作为物权法上的合成物获得物权保护，尽管由不同部分组合而成、各部分相对独立，但功能上相互依赖，通过有线或无线连接构成了一个完整的数据自动处理系统即构成一物，虽拆解后某些部分可成为独立的物，但合成物存续期间，构成其部分的简单物更换或更新，合成物仍保持其同一性。^[65]

2. 计算机系统财产权的权利内容

计算机系统作为物，可依据物权法获得所有权、担保物权等财产权以及占有保护。其中，所有权具有最为全面的支配权能，其内容可概括为所有者不受他人干扰地管理、操作和控制其系统的利益。其具体权能可按照传统物权的占有、使用、收益、处分概念加以描述：占有指权利人对计算机系统的实际控制，包括在计算机系统内组织配置软件、数据、算法等资源，通过代码技术对外实施访问控制、对内规范用户的行为；使用指利用信息系统的功能和资源完成工作任务，其情形高度取决于系统应用场景，包括提供信息内容、提供信息交换服务、进行智能管理运算等；收益指通过计算机系统提供数据或运算服务取得一定经济利益；处分指对计算机信息的全部或部分资源（如存储空间、应用程序、数据资源）等进行转让、出租、销毁等行为。然而，按照传统物权对权利人自用权能的表达，仅能概括地描述计算机系统之上的利益内容，却无法精确地界定计算机系统财产权的排他性范围。因为对有体物而言，财产损害往往以损害权利人的占有、使用、收益、处分为前提，但计算机系统作为一种物质财产和非物质财产的结合，损害往往针对非物质财产内容而具有无形性，不必然影响权利人的占有、使用、收益、处分。因此，需结合计算机系统的利用形式，从排他权角度将侵害行为类型化，从而更加清晰地界定这种财产权的范围。

财产权保护旨在维护权利人对其财产的支配状态，遵循“支配—侵害—排除”的逻辑链条将他人排除在财产支配之外，因此财产损害主要包括占有侵夺、占有妨害和财产物理价值的损毁。计算机系统的损害也可从此三方面划分。从国内及比较法上对计算机系统的刑事保护来看，侵害计算机系统的行为可归纳为两种类型：一是关注所有者对计算机系统的控制支配状态，禁止他人超出授权或未经授权访问计算机的行为，该行为构成对计算机系统占有的妨害；二是对计算机系统功能的损害，包括对数据、应用程序、系统功能的破坏。其中，非法控制计算机系统作为一类相对特殊的破坏行为，会使所有者完全丧失对计算机系统的指令控制，类似物的占有侵夺。因此，对计算机系统财产权的侵害可类型化为以下情形：

（1）非法访问计算机系统

计算机系统尽管依赖服务器等动产而存在，其内部资源却具有类似于不动产的不可移动、不易灭失的特点，在利用方式上无法实现类似于动产的持有，外部用户对计算机系统所有资源

[64] Vgl. Bettina Brückner, in: Münchener Kommentar BGB, 9. Aufl. 2023, BGB § 90 Rn. 25.

[65] 参见张双根：《物的概念若干问题》，《华东政法学院学报》2006年第4期，第106页。

的利用行为（诸如数据获取、存储、处理）皆以访问为前提，对计算机系统的占有妨害以及嗣后损害行为都通过访问实施，非法访问行为的界定很大程度上决定了所有者支配权的范围。从概念本身来看，“访问”来源于数字环境与物理世界的类比，即假设互联网是一个虚拟空间，访问即是用户从一个空间进入另一个空间活动的过程。^{〔66〕}在比较法实践中，非法访问行为也往往参照物理世界的不动产保护加以界定。如德国虚拟家宅权人可决定他人能否访问以及以何种条件访问其网络空间，在不对他人参与社会生活造成重大影响的前提下可自由排除他人访问。^{〔67〕}美国《计算机欺诈与滥用法案》也是参照侵入他人土地排除未经授权、超出授权的访问行为。但从计算机系统的现实运行来看，这种空间进入的可类比性并不存在。计算机系统之间的互动依靠二进制数据的发送接收完成，当用户访问网站时，并非用户进入了计算机系统活动，而是用户计算机向运载该网站的计算机发出访问请求指令，后者经过解析处理指令发回网页数据，用户计算机解析数据并以可视化形式展示给用户，因而形成进入某一网站的视觉观感。在技术层面，访问即用户对目标计算机系统进行指令输入，从而进行通信、存储数据、检索信息或者任何使用计算机资源的行为，本质上是对物的接触和利用。

对一般财产而言，所有权人可以排除他人未经同意对其财产的使用，但计算机系统因其开放性和内部资源的非竞争性而存在一定的特殊性。计算机系统可以通过互联网相互连接，前提在于其相互之间达成了一系列协议，其中超文本传输协议（HTTP）作为最基础的协议，要求其同意彼此的基础性访问请求并进行响应处理，但所有者可以区分不同主体、权限来限制其获取的内容。基于此，互联网自产生之初即存在自由开放的传统，通常连接互联网的计算机默认对所有人开放，允许他人自由访问其内部资源，典型如搜索引擎即以遍历式访问获取存储于不同网站的数据为前提。互联网自由开放的前提在于计算机系统内部资源不同于传统有体物的非竞争性，传统有体物由于物理属性限制，通常只能由有限主体使用，他人使用行为必然意味着所有人利益的减损。计算机系统内部由比特构造，比特没有尺寸、重量限制，可由无限人使用，用户对计算机系统资源的访问通常并不减损所有者及他人的使用，反而使用人越多价值越高，这也推动计算机系统所有者倾向于对外开放其内部资源。正因如此，自由开放成为过去互联网发展的主基调，各大平台早期普遍采取默认开放和普遍免费模式，用户可以自由访问、发布、获取信息，由此吸引用户成为平台内容创造和数据生产的免费劳动力。随着平台内部各类生产要素有效集聚、用户网络基本成型并固化，平台开始尝试通过技术措施限制计算机系统的访问和用户流动。^{〔68〕}但总体而言，当前社会观念以及财产秩序的形成很大程度上仍基于网络默认开放的基本格局，社会公众对网络行为规范远未像在物理空间中访问那样达成清晰的共识，如果按照物权模式允许所有者随意排除他人对计算机系统的访问，将使得互联网领域绝大多数的访问行为都被界定为侵权而导致责任泛滥。同时，这意味着大型平台对其内部用户数据内容的绝对支配，一方面会加剧平台与用户之间关系的不平等，造成过度收集数据、算法歧视、大数据杀熟等剥削行为；另一方面，竞争者（尤其中小企业）也难以获得必要的数字化生产资料开展竞争，会固化现有竞争格局而限制产业迭代升级。

笔者认为，由于计算机系统访问具有无形性且并不直接影响所有者利用，可借鉴传统物权法上对无形侵害的容忍义务来恰当界定访问行为的边界。20世纪初，随着现代工业的发展，

〔66〕 参见戴秋燕：《网络空间访问规范研究》，《荆楚法学》2022年第5期，第40页。

〔67〕 Vgl. BGH NJW 2020, 3382.

〔68〕 参见刘晗：《平台权力的发生学——网络社会的再中心化机制》，《文化纵横》2021年第1期，第31页以下。

财产权侵害由有形侵入扩展为诸如噪声、废气等无形侵害，为了避免绝对的财产权保护对工业发展造成阻碍，德国民法典第 906 条第 1 款专门规定，土地的所有者对来自另一土地的不可量物侵入，在不妨害土地使用或妨害不显著时需予容忍，妨害是否显著应结合“理性的普通人”在具体情形下的合理期待作出判断。^[69] 参照该标准，为平衡公众与所有者之间的利益，如果他人访问行为对计算机系统的使用未造成妨害或妨害并不显著，所有者应负容忍义务，对此应结合计算机系统本身状态以及访问行为的具体情形加以判断。首先，对互联网上公开自由访问的网站及其所依附的计算机系统，以普通用户方式或类似方式访问并不实质影响计算机运行，网站数据资源本质上处于人人皆可浏览的状态，用户访问也未改变这一状态，对此应认为访问行为未造成妨害，所有者负有一定的容忍义务。当然，这并不意味着对自由访问的计算机系统完全不予保护，他人以非正常手段访问，如以大规模或高频率的网络爬虫访问可能造成网络服务器过载或故障风险时，则应构成实质性妨害，经营者仍有权予以排除。其次，所有者可采取措施限制他人对计算机系统的访问，而将之与公众皆可访问的内容相区隔，使计算机系统资源仅由内部或少数人使用，在此情形下所有者可行使其财产权排除未经许可的访问行为。不同于自由访问网站，限制访问网站的内部资源已与人人皆可获得的资源相脱离而具有一定稀缺性，在所有者对计算机系统设置访问限制的前提下，绕过这种限制的访问行为将破坏系统内部数据资源的稀缺性价值而构成对系统使用的妨害。实践中，所有人对计算机系统的访问限制依强度不同包括单方政策声明（如 Robots 协议）、用户协议以及通过技术措施限制等情形。^[70] 前两种情形与公开自由访问网站不存在实质不同，所有者应负容忍义务。所有者的限制措施应以通过技术措施建立对计算机系统的支配力而排除一般用户访问为前提，如通过身份验证、访问授权、虚拟专用网络、加密技术等进行用户权限管理、访问控制，对他人绕过技术限制措施爬取数据等利用计算机资源的行为，权利人可主张排除妨害和损害赔偿。

（2）非法破坏、控制计算机系统

与有体物之上的所有权相同，所有人有权排除他人对计算机系统本身的损害和侵占，即非法破坏和控制计算机系统。破坏计算机系统，依据我国现行刑法第 286 条的规定，指的是对计算机系统功能进行删除、修改、增加、干扰，造成计算机系统不能正常运行的情形。这种“不能正常运行”不能从有体物利用的角度出发，仅理解为计算机系统不能启动或者不能进入操作系统等极端情况。作为软件与硬件的结合，计算机系统的核心价值在于其数据自动化处理功能，这一功能依靠物理层、应用层、网络层结合实现，对三者之一的破坏皆构成破坏计算机系统。在物理层，如对 GPS 设备、环境质量采样设备等数据收集设备进行破坏、干扰造成数据失真；^[71] 在应用层，如通过外挂程序影响软件正常运行，或删除、更改后台数据影响算法推荐结果；^[72] 在网络层，如使用恶意目标代码修改目标网站域名解析服务器，使对特定域名的访问由目标网站转入其他网站的流量劫持情形。^[73] 诸如此类行为皆会影响数据自动处理功能而构成破坏计算机系统的行为，权利人可主张恢复原状请求权和损害赔偿请求权。其中，篡

[69] Vgl. Bettina Brückner, in: Münchener Kommentar BGB, 9. Aufl. 2023, BGB § 906 Rn. 71.

[70] See Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud Abuse Act*, 84 *George Washington Law Review* 1442 (2016).

[71] 参见徐某破坏计算机信息系统案，最高人民法院指导案例 103 号（2018 年）。

[72] 参见李某等破坏计算机信息系统案，最高人民检察院检例第 34 号（2018 年）。

[73] 参见付某、黄某破坏计算机信息系统案，最高人民法院指导案例 102 号（2018 年）。

改系统代码设定和数据内容作为相对特殊的破坏行为，不仅破坏了计算机系统的正常运行，也剥夺了所有人对计算机系统的控制权，使得计算机系统依篡改人指令执行反馈，〔74〕此种情形类似物的占有侵夺，权利人可主张返还原物即排除对其控制权的剥夺并请求损害赔偿。

3. 计算机系统的财产权归属

计算机系统整体作为物可以获得所有权保护，其权利归属可适用所有权一般规则加以判定。通常而言，民事主体会在其所有的计算机硬件之上组织软件、数据资源等形成具有自动化数据处理功能的全新计算机系统，由于计算机系统应用层、协议层内容无法脱离其物理层载体而单独存在，组成计算机系统的硬件的物理范围决定了其基础边界即物理边界。在此情形，通过类似添附的方式，权利人可基于其硬件的所有权实现新的计算机系统所有权的原始取得，其权利范围可通过硬件的物理边界对外彰显。其他民事主体可通过交易继受取得计算机系统的所有权，由于计算机系统硬件和软件的一体性，交易可通过硬件载体支配转移的方式实现。相对特殊的情形是，随着云计算和虚拟化技术的发展，计算机系统边界可以突破其物理硬件限制，通过加密技术、虚拟专用网络等方式访问利用外部服务器上的资源，在数据交换和通信时与使用自身服务器没有实质性区别，故技术层面认为其属于计算机系统的一部分，作为计算机系统外部拓展的逻辑边界。但在法律层面，如果将不同部分界定为同一计算机系统，即存在计算机系统的物理层与应用层相分离、同一物的不同部分分属于不同主体的矛盾，由此导致权利行使的冲突。为了适应有体物时代形成的传统交易观念，建议依据计算机系统的物理边界即物理硬件的所有权来界定权利归属，云服务器上的内容可作为独立计算机系统的一部分，使用者依其事实控制获得占有保护。如在德国虚拟家宅权保护中，在租赁云服务器的情形，尽管使用者并非所有人，其作为占有人可依据德国民法典第 858 条、第 862 条排除他人的占有妨碍。〔75〕类似地，美国法上侵入和破坏计算机系统民事诉讼的原告并不限于计算机系统的所有者，而是包括所有者、控制者在内的受到损害的任何人。〔76〕

我国法上，占有人可依据民法典第 462 条主张对计算机系统的占有保护。占有的成立要求主观上存在占有的意思、客观上对物有事实上的管领力，通常需要以对物的接触建立事实上的控制，却不限于此，依据社会观念认为特定物处于某人的控制支配之下亦可。〔77〕就对世性效果而言，计算机系统的支配和利用并不在于直接物理接触，而在于对内部资源的控制访问，用户通过访问权限、加密技术、虚拟专用网络等技术手段可实现对计算机系统资源的排他性控制时，即成立事实支配而获得占有保护。典型如云服务场景下，用户在云平台上拥有相对独立的空间，可通过账户和密钥实现对该部分的控制，可作为“占有人”受到保护。通过占有保护可实现计算机系统之上复杂利益的精确分配，并避免大型平台对用户利益的完全支配。在对世性法律关系中，无论计算机系统所有者或占有者都有权排除他人的不当侵害；在内部相对关系中，所有人可通过合同与使用者达成精确的利益分配，使用者可以其占有对抗本权，避免用户与平台利益分配的失衡。

〔74〕 典型如利用网络系统漏洞控制计算机 CPU 资源（俗称“抓肉鸡”）挖取虚拟货币的情形。参见浙江省舟山市普陀区人民法院（2019）浙 0903 刑初 114 号刑事判决书。

〔75〕 Vgl. LG München I ZUM-RD 2007, 261.

〔76〕 See Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003).

〔77〕 参见刘智慧：《占有制度原理》，中国人民大学出版社 2007 年版，第 225 页以下。

结 论

面对数字经济中不断出现的各种新型财产形态，理论上多按照传统范式逐一界定客体属性构造财产权制度，以法律之力主导塑造平台内部的财产秩序。基于数字经济社会组织形态革新，本文旨在提供一个新的认知框架，即随着市场竞争形态由商品交换转变为平台提供服务，企业将各种生产要素纳入平台组织整合开展竞争，在平台内部可通过代码限制和合同规则保护各种要素之上的财产利益，财产保护制度需求由单一生产资料控制扩展为系统产权保护。平台的本质是服务于用户互动这一特定业务模式的计算机系统，建议通过整体性地确认计算机系统的财产权实现对其内部一系列财产要素的保护。回归传统物权法视角，计算机系统的物理层、应用层、网络层内容整体可作为“物”获得财产权保护，所有人和占有人可排除他人非法访问、破坏或控制计算机系统。在此产权框架下，所有者可自主采取技术措施在计算机系统内部配置、利用资源并进行收益、处分，实现国家权力与私人自治的激励相容。

Abstract: The digital economy has spurred the emergence of various new forms of property, highlighting the need to improve property law frameworks. Theoretical approaches often attempt to construct models of property rights by defining the attributes of objects. However, the increasing diversity and fluidity of intangible property forms challenge the effectiveness of these models. In contrast to the industrial economy, where market transactions primarily involve the exchange of goods, the digital economy operates through platforms that provide services. Enterprises integrate diverse production factors into the platforms, competing by organizing and coordinating these factors. Consequently, the focus of property protection has shifted from control over individual production factors to control over the entire system, affirming property interests in computer information systems holistically, thereby safeguarding the full range of digital elements embedded within them. Within the tangible-intangible dichotomy, hardware enjoys property law protection, while code content remains partially covered by intellectual property law, mainly via technological protection measures that exclude non-copyright content. The possibility of expansion of legal protection depends on whether property rights can be affirmed in computer information systems. From the property law standpoint, the physical, application, and network layers of a computer information system may jointly constitute a “thing” that serves as the object of property rights. Owners and possessors should be entitled to exclude unauthorized access, interference or control. For restricted-access systems, they have the right to prevent unlawful access by circumvention of technological measures, and for open-access systems, they have the duty to tolerate lawful public access. Under such a framework, right-holders may autonomously allocate, utilize, benefit from, and dispose of resources within computer information systems via technological measures, achieving an incentive-compatible alignment between platform self-governance and legal protection.

Key Words: computer information systems, property rights, intellectual property, data ownership, technological protection measures
