Dispute Settlement 争议解决, 2026, 12(2), 119-125
Published Online February 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.122050

Hans汉斯

数字经济背景下企业数据安全的刑法保护

朱怡铭

华东交通大学人文社会科学学院，江西 南昌

收稿日期：2026年1月6日；录用日期：2026年1月29日；发布日期：2026年2月11日

摘　要

随着经济的发展，以往的经济模式也发生了相对应的变化。从传统的实体信息逐步转化为虚拟数据等，因此建立符合我国国情的企业数据保护符合中国法治现代化的内涵和精神。数字经济新模式的出现，为信息储存、传播、保护提供了便利，但是现有的刑法规制对于企业高商业价值和高应用价值的衍生数据保护仍然存在不足。主要体现在对于“数据”的解释模糊不清和“数据”保护的范围界限，侵犯企业数据的危害行为认定以及所触犯的罪名适用把握，判决较为混乱难以统一等。刑法作为最后的权利保障法，存在其谦抑性质，具有兜底的功能。因此针对上述问题，有必要就现有的刑法进行完善来填补企业数据保护的不足。根据企业数据的商业价值和应用价值来建立分级保护制度，同时为了最大程度地保证市场经济的活力，防止企业之间利用数据保护制度相互打击，可最大程度地发挥刑法的谦抑性，防止以保护为名而恣意扩张刑法的适用范围。在这过程中，应充分发挥实质认定的出罪功能。

关键词

法治现代化，企业数据，刑法保护，分级制度

Criminal Law Protection of Enterprise Data Security in the Context of Digital Economy

Yiming Zhu

School of Humanities and Social Sciences, East China Jiaotong University, Nanchang Jiangxi

Received: January 6, 2026; accepted: January 29, 2026; published: February 11, 2026

Abstract

With the development of the economy, the previous economic model has also undergone corresponding changes. From traditional physical information to virtual data and so on, therefore, establishing an enterprise data protection system that suits China’s national conditions is in line with the connotation and spirit of China’s modernization of the rule of law. The emergence of new digital

文章引用: 朱怡铭. 数字经济背景下企业数据安全的刑法保护[J]. 争议解决, 2026, 12(2): 119-125.
DOI: 10.12677/ds.2026.122050

economy models has provided convenience for information storage, dissemination, and protection. However, the existing criminal law regulations still have deficiencies in protecting the high commercial and application value derivative data of enterprises, mainly reflected in the ambiguous interpretation of "data", the unclear boundaries of the scope of "data" protection, the determination of harmful acts that infringe upon enterprise data, and the application of the charges involved, with judgments being rather chaotic and difficult to unify. As the ultimate law for safeguarding rights, criminal law has its modest nature and serves as a fallback. Therefore, in response to the above problems, it is necessary to improve the existing criminal law to fill the gaps in enterprise data protection. A hierarchical protection system should be established based on the commercial and application value of enterprise data. At the same time, to ensure the vitality of the market economy to the greatest extent and prevent enterprises from using the data protection system to attack each other, the modesty of criminal law should be fully utilized to prevent the arbitrary expansion of the application scope of criminal law under the guise of protection. During this process, the exculpatory function of substantive determination should be fully exerted.

Keywords

Modernization of Rule of Law, Enterprise Data, Criminal Law Protection, Grading System

1. 引言

随着科技生产力的发展，数字经济作为新兴的经济形态登上了历史的舞台，扮演着举足轻重的角色。所谓的数字经济是指直接或间接利用数据来引导资源发挥作用、推动生产力发展的经济形态，随着我国工业化发展，在科技领域也有了重要突破，在技术层面其主要包括大数据、云计算、物联网、区块链、人工智能、5G 通信等各种新兴技术。数字经济不仅带来了经济领域的新产业和新业态，也渗透到了人们社会生活的各个领域。在提高生产、生活效率的同时，也带来了新的社会风险。企业作为推动中国现代化的生力军，具有重要地位。目前我国企业创新和专利申请在世界均处于领先地位。大疆、华为、比亚迪等公司有数量庞杂的商业秘密。如何保障如此海量企业数据的安全，成为了一个急需解决的难题。企业的健康安全发展，离不开数据保护治理体系的构建。而刑事规制是社会治理体系的一个重要组成部分，也是整体社会治理体系发挥效能的后盾和保障。因此，企业数据安全领域的保护离不开刑法的参与。21年底，国务院印发《"十四五"数字经济发展规划》的通知，对于我国数字经济的发展做出了具体的工作部署和战略安排，今年七月国务院常委会再次就数字经济做出了加速推进数字产业化、产业数字化的决定。我国的立法在新兴领域存在着"刑法先行"的现象，例如 2009 年《刑法修正案(七)》新增保护个人信息的罪名，在行政立法和民事立法之前将公民个人信息纳入保护范围[1]。在此背景下，现有的"侵犯商业秘密罪"或"非法获取计算机信息系统数据罪"无法涵盖特定的企业数据保护，所谓的商业秘密是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息。而企业数据是企业在经营活动中产生、收集和储存的所有信息。简单而言商业秘密只有在符合法律规定的条件下才受到保护，企业数据的范围要更加宽泛。而"非法获取计算机信息系统数据罪"其保护的客体是国家计算机信息系统的管理秩序和信息安全，其本质保护的是计算机信息系统秩序而并非企业数据。因此适用上述罪名对侵害企业数据的行为进行规制，违反了罪刑法定原则以及法益保护原则。鉴于此，有必要全面正确认识企业数据保护的重要意义，清醒认识我国企业数据刑法保护面临的困境，构建符合我国国情的企业数据

刑法保护制度

2. 企业数据及数据安全概述

(一) 企业数据概述

1、企业数据的定义

传统的企业数据从泛指来说包括公司经营范围、企业名称、法人代表、联系方式、企业规模、经营范围等。此类信息均可从天眼查等软件上查询到，均属于公开状态，此类信息属于一般企业数据并没有保护的价值和意义。传统值得保护的企业数据范围一般是指商业性企业数据，其是指由公司开发或者创新，所有权属于公司并且受到法律保护的专利或者商业秘密，同时对外提供数据服务。而数字经济背景下的企业数据定义出现了变化。《数据安全法》第三条将数据的概念界定为“任何以电子或者其他方式对信息的记录。”企业数据则是将个人信息或者政务数据收集后进行处理进而类型化的数据集合。”[2]同时该法也规定了范围主要是对个人和组织。“企业数据”作为“数据”的衍生定义，同样适用该规定。因此可以理解为，企业数据是指企业收集个人信息和组织数据并处理通过电子或其他方式进行储存以及利用的数据。同时在数字经济时代背景下，企业数据的类型和模式也出现了新的变化，企业的架构变化推动着企业内部不断衍生出众多的数据类型，这些基本的数据类型共同构成了企业数据。

2、企业数据的分类

在数字经济背景时代下，金融、工业、电信、医疗和汽车等行业均已出台了针对性的数据分类分级指南或技术规范，数据的分类也出现了新的变化。而企业数据的分类目前仍没有具体规定，根据我国 2021 年颁布的《数据安全法》规定了对于数据的分类分级制度，同时根据《GB/T 38667-2020 信息技术－大数据－数据分类指南》的定义，将数据的分类规定为了 5 个等级，是从国家安全和社会公共利益、企业利益等三个方面进行综合评估，其五个等级从低到高分别是低、中、较高、高、极高五个等级。以金融行业为例，金融领域的数据分类分级方法主要体现在《金融数据安全数据安全分级指南》(JR/T0197-2020)和《证券期货业数据分类分级指引》(JR/T0158-2018)中，客户数据、业务数据、经营管理数据三类，客户数据又分为个人客户和单位客户，业务数据则根据不同的业务线再做细分，经营管理数据包括营销服务、运营管理、技术管理、综合管理(员工、财务、行政、机构信息)等。企业数据的分类可以借鉴上述制度的分类，根据企业数据的重要性，以及其出现泄露时候的影响范围及其程度，从刑法的角度可以分为：对于公民个人影响、对于社会的影响、对于国家的影响三个层次。因此可将企业数据分为三类，第一类为一般数据，例如：企业经营范围、法人代表、企业名称等，此类数据一般为公开数据，泄露也不会对公民、社会和国家造成什么影响。第二类为重要数据，主要包括企业的发展规划、财务信息、投融资决策、产购销策略、资源储备、客户信息等。此类数据信息一般来说仅对内部人员知晓和使用，极少数可再特殊情况下进行公开并被公众知悉。泄露时会对公民和社会秩序造成影响或产生损害。但是此类企业数据一般不会直接对国家安全造成危害。第三类为保密数据，主要包括企业的知识产权、技术信息等，此类数据同时有可能属于国家秘密。一般来说仅对特殊人员公开，且只被必须知道得对象访问和使用。泄露时会造成企业社会秩序严重混乱，严重损害国家安全。

(二) 数据安全概述

数据安全的定义

传统的数据主要以纸张、信息等方式保存，其主要损害侵权形式主要是偷拍、复制等。国际上关于企业数据安全的定义为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破化、更改和泄露。其形式大部分都以电子化的方式储存，以数据丢失、外泄和篡改，侵入系统，修改代码等方式损害数据安全。保护企业数据安全的主要意义就是确保只有授

权人员可以访问和使用数据，并在其生命周期内保持数据的准确性、完整性和一致性。作为数据收集者和处理者的企业，是数据赋能的重要主体，其数据权益的刑法保护受到关注[3]。有学者认为，企业的信息专有权是指企业在原信息主体的授权基础上，以及法定授权范围内，通过加工处理原始数据获得的信息享有占有、使用、处分和收益的权利。这种权利被视为新型财产权，属于刑法保护的新型法益[4]。

3. 完善企业数据刑法保护的必要性

(一) 实现法治现代的必然要求

习近平总书记曾指出：“一个现代化国家必然是法治国家。”党的二十大报告提出“以中国式现代化全面推进中华民族伟大复兴”的使命任务和奋斗目标，并强调要“在法治轨道上全面建设社会主义现代化国家”。中国式法治现代化就是中国式现代化的重要组成部分。法治是人类文明进步的标准和重要衡量，在这个历史进程中，需要新的法治观念和法律制度对新的社会关系进行调整，否则将制约甚至阻碍现代化进程。中国式法治现代化具有鲜明的中国特质，是基于中国国情进行的法治创新，以此来适应中国式现代化的发展。完善企业数据的刑法保护制度有利于最大限度地区分企业数据侵权问题中罪与非罪、轻罪与重罪，从而生成逻辑自洽、层次分明、结构合理、刑罚合理符合我国现代化发展国情的刑事立法与司法制度。

(二) 维护科技企业创新法律需求

十八大时我党提出了“实施创新驱动发展战略，建设科技强国”的口号，当前，我国正在面临从科技大国到科技强国的转变。一大批企业科技创新专利喷涌而出华为、比亚迪、大疆、宁德时代等一系列企业均在国际上处于领先地位。数据安全保护也成为了急需解决的难题，企业数据创新发展与因刑法保护不完善导致的数据泄露、传播就会成为难以调和的矛盾，并对企业利益和社会乃至国家利益产生影响。完善企业数据的刑法保护制度，为企业的发展进行保驾护航，能够最大限度地满足我国科技转型时期对于法律的需求。

(三) 保障企业的合法权益

信息爆炸、数据的传播速度对于企业的数据保护提出了新的要求，现有的刑事司法责任体系已经无法兼顾企业数据保护和公共利益的需要。构建完善的企业数据刑事保护政策，打破“电子信息时代，数据泄露传播和保护”的困境，有利于企业健康发展。

4. 企业数据犯罪问题研究

(一)企业数据犯罪概述

当前，数据安全领域的犯罪行为日益猖獗，亟需进一步完善刑法，以实现对数据安全的全面、系统性保护。数据犯罪与网络犯罪一样，都是特定历史阶段的产物，二者在表现形式上并无本质区别。回顾计算机发展历史，在计算机 1.0 时代，网络犯罪主要表现为以计算机为攻击目标；进入计算机 2.0 时代后，网络犯罪则更多地利用计算机作为作案工具；而到了计算机 3.0 时代，网络犯罪已经演变为互联网空间内的新型犯罪形态。

尽管前两个阶段的网络犯罪本质上仍属于传统犯罪在数字环境下的变异，现行法律框架尚能对其实施有效管控。然而，随着计算机 3.0 时代的到来，网络犯罪呈现出更加复杂多变的特点，成为互联网空间独有的犯罪类型，这使得传统的刑法体系难以应对这些新兴挑战。数据犯罪正是这一背景下产生的一个典型例子。在处理此类案件时，司法机关通常依据被侵害的具体权益来确定适用的罪名。但值得注意的是，数据犯罪所侵犯的利益并非单一，而是包含了多种复杂的权益组合，即所谓的“复合数据利益”。其犯罪客体可能是涉及到企业财产、社会经济秩序、少数可能涉及到国家安全。犯罪客观方面对企业数

据造成侵害所实施的侵权行为主要应该包括采用非法手段对企业数据进行破坏、传播或未经企业允许擅自对数据进行篡改、使用使企业利益遭受损失的行为。少数为采用非法手段获取高新技术、尖端科技等领域的企业数据危害国家安全的行为。此类犯罪具有一定的技术门槛，因此其犯罪主体一般为掌握一定信息技术、具有较高计算机水平同时年满 16 周岁刑事责任能力的自然人，因为企业数据的特殊性，一般涉及到商业发展和运营，因此其侵害主体也可能为其他科技网络公司。在犯罪主观方面，此类犯罪的目的均为使对方信息数据受损或者使对方利益受损，过失犯罪包括疏忽大意的过失和过于自信的过失，而数据侵害行为目的较为明显，具有较强的目的性，因此不存在过失，即此类犯罪主观方面均为故意。

5. 企业数据保护现状

(一) 域外主要国家企业数据保护现状

关于数据保护，传统的发达国家因其特殊的文化土壤和背景，在关于企业数据保护上各有千秋，没有统一的保护政策，立法也参差不齐，大多数国家对于数据的保护仍然集中在对于个人隐私和个人数据的保护里，关于企业数据保护仍然存在比较空白的情况。

美国在企业数据保护主要依靠行业立法、监管和行业自律相结合的方式。虽然没有针对企业信息和隐私保护的专门性法律规范，但美国 50 个州和地区拥有数百项企业数据安全措施。其中，加州的《2018 年加州企业数据法》是非常典型的一个，它对企业信息和主体权利进行了概括性定义，并对企业信息保护作出了具体的要求和限制。而在联邦层面，为了规范境外数据的使用，美国还特别制定了《澄清境外数据合法使用法案》等。

英国的数据保护制度以成文法为立法核心，在欧盟数据保护的法律框架影响下，形成了由英国法典、判例法、民间实践、二级成文法和执法机构组成的数据保护制度体系。比较典型的有《数据保护法》《隐私与电子通信条例》等。为了精细调整和明确 GDPR 原则，英国还在推动《数据保护与数字化信息法案》的审议，以适应新的数据保护需求。

法国的数据保护制度同样在完善中。它遵守欧盟的《通用数据保护条例》，并在此基础上制定了更多法规，如“具有约束力的公司规则”(BCR)，为数据跨境传输提供了解决方案。此外，法国还发布了《信息技术与自由法案》《个人数据保护法》及《数据保护法》等，保障个人数据和重要数据的安全。

德国的数据保护法律体系在世界范围内相对来说较为完善，它制定了《刑法典》《联邦数据保护法》等一系列法规，形成了从中央到地方、从一般到专门的全方位数据保护框架。德国还设立了独立的数据保护监管机构，负责监督数据保护法的执行，其处罚措施也较为严厉，结合了行政与刑事手段，有学者认为，数据安全法益具有个人安全、公共安全和国家安全多元性、层次性，需要通过不同的立法参照系进行有差别的法益识别和利益平衡[5]。

(二) 我国企业数据保护现状

1、企业数据犯罪罪名缺失

当前，我国对于企业数据的刑法保护主要是从知识产权角度、个人信息角度、计算机系统角度来进行的规制，如破坏计算机信息系统罪、侵犯公民个人信息罪等。此类犯罪所规制的客体一般来说均为简单客体，而企业数据加害行为一般侵犯的法益涉及到企业利益、社会利益、国家利益等，因此将侵害企业数据的行为确定为上述犯罪，本来就是对上述罪名的扩大解释，但是无论将企业数据犯罪行为解释为何种罪名，均会遗漏其加害行为本身所遗漏的法益，这不符合罪责刑相适应原则，即现有的罪名作为传统工业社会时代的产物无法完全适应信息化时代的发展。

2、企业数据分级保护不完善

根据我国 2021 年颁布的《数据安全法》规定了对于数据的分类分级制度，但是至今效果仍不明显，

因为刑法里并没有建立起适格的刑法保护体系。有学者指出我国数据安全法益包括数据自身安全以及数据利用安全[6]。对于企业数据的保护，主要是通过其他罪名来进行规制的，但是这并不符合企业数据复杂法益的特点。企业数据并不是所有的数据都值得保护的，也并不是所有数据都值得用刑法来进行保护的。例如企业中公开的数据信息就不需要进行保护，但是对于企业数据中有可能涉及到国家秘密、国防建设以及其他信息时，均要进行保护。有学者认为，我国刑法在概念划定与罪名设定两方面均将“计算机信息系统”与“数据”两者予以杂糅的立法模式，使刑法中的“数据”概念不得不依附于“计算机信息系统”，而无法覆盖应当被纳入刑法保护范围的所有数据的外延[7]。根据我国《刑法》规定：“非法侵入计算机信息系统罪的法定刑为三年以下有期徒刑或者拘役；侵犯商业秘密罪情节严重的，处三年以下有期徒刑，并处或者单处罚金，情节特别严重的，处三年以上十年以下有期徒刑，并处罚金;破坏知识产权犯罪的最高法定刑普遍在三年以上十年以下有期徒刑。”而正如前文所言，企业数据与商业秘密以及非法侵入计算机信息系统罪所保护的法益存在或多或少的区别以及差异，适用其进行规制违反罪刑法定。综上，涉及到企业数据的保护，计算机数据化时代的保护明显要低于其他模式。

3、企业数据犯罪缺乏出罪规制

数字经济的时代下，传统的以往的“知情－同意”规则不再适用于企业数据的保护，数据的价值在于使用，如果每个环节都需要经过同意显然违背了效率原则，而对于企业来说，效率是最重要的。同时，企业甚至股东之间也会以侵权为理由借助刑法相互打击，以满足自己的目的。随着经济的高速发展，在网络信息时代，信息高速传播，公民与企业的信息被侵害的可能性越来越大，自我维权意识越来越强，因此刑法一直是属于扩张的状态，这与刑法的谦抑性相违背。为了使企业数据能高效率利用和传播，防止企业之间利用刑法保护相互打击，设置刑法出罪机制就尤为重要。企业数据固然重要，然而不是所有的企业数据都值得用刑法进行保护，刑法应该保持其谦抑性，因此设置合理的出罪途径就尤为重要。但是设立出罪机制时，也要设置较高的出罪门槛，防止在严厉打击侵犯企业产权的背景下，出罪机制被滥用，可以通过企业财产损失，以及成果侵害等角度出发，设置合理的出罪机制，在保证刑法谦抑性的同时，对企业数据进行保护。

6. 企业数据刑法保护对策

(一) 细化增设新的数据类犯罪

笔者认为，对于企业数据有必要专门立法进行保护，因为企业经济在我国经济中占有重要地位，也和民生息息相关。可以从细化数据犯罪的罪名：如设立专门针对数据泄露、数据盗用、数据篡改等行为的罪名，明确各类数据犯罪的具体罪行和处罚标准。企业数据作为种类繁多复杂可以参考我国的妨害药品管理罪，设立妨害企业数据安全罪。同时，在客体上扩大数据保护的法益认定：考虑到数据的多重属性(如商业、个人隐私、公共安全等)，更新法律与技术的适配性就显得尤为重要，随着技术的飞速发展，立法和司法实践也需要加快与新兴技术的适配，尤其是在区块链、加密货币、人工智能等新兴领域对数据安全的影响下，法律框架应更加灵活和前瞻性。在刑法上对数据的保护应更多维度、更加细致，以适应计算机 3.0 时代复杂的数据流动和信息架构。

(二) 建立国际性企业数据保护模式

在当前数据高速传播时期，企业数据泄露、破坏、传播等往往是跨国家、跨区域进行的全球数据流动。因此国际间的法律协作变得至关重要，确保各国法律体系能够联动起来应对复杂的数据犯罪案件。由此，可参考联合国关于反恐的规定。设立独立的企业数据保护办公室，并出台相应的政策，以此来对企业数据进行联合保护。但是在建立跨国合作机制保护的同时，企业数据基于其特殊性，尤其是在我国民企发展迅速的今天，其有可能涉及国家数据主权问题，在数据安全上升为国家安全当下的同时，在建

立“国际性企业数据保护模式”的背景下，仍然需以我国数据安全为主。

(三) 设立完善的企业数据分级保护制度

正如笔者上文所言，建立完善的企业分级保护制度，可以根据其危害性、影响性等综合考量来确定是否需要用刑法进行规制。分级保护中，应该将具体的危害进行数字化，以此来明确其应当接受的刑罚，此处设立可参考我国《最高人民法院最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》，该解释规定利用发送短信、拨打电话、互联网等电信技术手段对不特定多数人实施诈骗，诈骗数额难以查证时，根据其拨打电话的次数，以及发送消息的数量来判断其危害。即当造成的危害无法具体衡量时，可以根据其造成的影响和规模来对其行为进行评价。企业数据因其具有电子信息的特点，其具体的价值更多时候难以直接衡量，此时就可参考上述规定，根据其传播破坏的程度，造成的影响来决定其具体的刑罚，以及是否需要用刑法进行规制。

7. 结语

企业数据的发展进程深刻影响着经济的规划和布局，在当前信息传播爆炸时代，借助互联网进行数据犯罪的比例大幅度上升，作为最后保障法的刑法在大数据时代应进一步完善。设立新的罪名，并且做好分级制度的规定，以此来适应新时代的发展，同时，完善企业数据刑法保护制度，也是中国式法治现代化的必然要求。

参考文献

[1] 田刚. 数据安全刑法保护扩张的合理边界[J]. 法学论坛, 2021, 36(2): 66-75.

[2] 马中磊. 大数据时代企业数据安全刑法保护研究[J]. 浙江万里学院学报, 2023, 36(6): 43-48.

[3] 种政. 数据的刑法保护[D]: [博士学位论文]. 北京: 中国人民公安大学, 2023.

[4] 敬力嘉. 论企业信息权的刑法保护[J]. 北方法学, 2019, 13(5): 73-86.

[5] 张勇. 数据安全法益的参照系与刑法保护模式[J]. 河南社会科学, 2021, 29(5): 42-52.

[6] 杨志琼. 数字经济时代我国数据犯罪刑法规制的挑战与应对[J]. 中国法学, 2023(1): 124-141.

[7] 刘宪权, 石雄. 网络数据犯罪刑法规制体系的构建[J]. 法制研究, 2021(6): 49.