Advances in Social Sciences 社会科学前沿, 2024, 13(6), 338-344
Published Online June 2024 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2024.136505

Hans汉斯

数字经济背景下新型犯罪问题的刑法保障

何逸宁，裴兆斌

大连海洋大学海洋法律与人文学院，辽宁 大连

收稿日期：2024年4月24日；录用日期：2024年6月18日；发布日期：2024年6月27日

摘　要

数字经济是随着经济社会不断发展而产生的新经济形态，为人类社会发展提供便利的同时，也催生了一些不同以往的新型犯罪，而这种新型犯罪则由于其出现时间短、发展速度快、治理难度大等特点，对数字经济的发展形成了较大的冲击，产生了一些传统刑法难以应对的困境，对社会管理秩序和现行法律体系形成了冲击，阻碍了数字经济的高质量发展，因此，在数字中国建设整体布局规划和“十四五”数字经济发展规划出台的背景下，如何紧扣数字经济的发展逻辑，运用刑法手段对数字经济背景下产生的新型犯罪问题进行应对，是数字经济的法治保障研究的重要课题，具有重要且深远的研究价值和意义，本文针对数字经济发展过程中产生的三类新型犯罪问题进行了剖析并提出了相应解决对策，用以解决刑法该如何回应数字经济背景下新型犯罪带来的冲击这一关键问题。

关键词

数字经济，新型犯罪，数据，人工智能，虚拟财产

Criminal Law Protection for New Criminal Issues under the Background of Digital Economy

Yining He, Zhaobin Pei

School of Ocean Law and Humanities, Dalian Ocean University, Dalian Liaoning

Received: Apr. 24th, 2024; accepted: Jun. 18th, 2024; published: Jun. 27th, 2024

Abstract

The digital economy is a new economic form that has emerged with the continuous development of the economy and society. While providing convenience for the development of human society, it

文章引用: 何逸宁, 裴兆斌. 数字经济背景下新型犯罪问题的刑法保障[J]. 社会科学前沿, 2024, 13(6): 338-344.
DOI: 10.12677/ass.2024.136505

has also given rise to some new types of crimes that are different from the past. However, due to its short appearance time, fast development speed, and difficult governance, this new type of crime has had a significant impact on the development of the digital economy. It has created some difficulties that traditional criminal law cannot cope with, which have impacted the social management order and current legal system, and hindered the high-quality development of the digital economy. Therefore, in the context of the overall layout plan for the construction of Digital China and the release of the "14th Five Year Plan" for the development of the digital economy, how to closely follow the development logic of the digital economy and use criminal law methods to respond to the new types of crimes that arise in the context of the digital economy, This is an important topic in the research on the legal protection of the digital economy, which has important and far-reaching research value and significance. This article analyzes the three types of new criminal problems that arise in the development of the digital economy and proposes corresponding solutions to address the key issue of how criminal law should respond to the impact of new crimes in the context of the digital economy.

Keywords

Digital Economy New Type of Crime, Data, AI, Virtual Property

1. 引言

随着互联网、云计算、大数据等数字科技的迅猛发展，人类社会已经向数字经济时代大踏步地迈进，数字经济是实现经济社会高质量发展的新动能，2020 年，我国数字经济总量跃居世界第二，成为引领全球数字经济创新的重要策源地。党的十八大以来，习近平总书记始终高度重视数字经济的发展，多次针对数字中国建设作出重要指示，在党的二十大报告中，习近平总书记再次针对数字中国建设作出新部署、提出新要求，“十四五”数字经济发展规划当中更是明确提出，要进一步完善与数字经济发展相适应的法律法规体系，同时，随着数字经济的不断发展，对数字经济安全产生威胁的新型犯罪也层出不穷，对传统的刑法规制造成了全新的风险和挑战，对数字经济的发展速度和发展质量都造成了较大的影响，因此，在数字经济飞速发展的社会背景之下，如何运用法治手段应对威胁数字经济安全的新型犯罪问题，是充分发挥刑法社会保护功能的重要路径，也是提升我国数字经济的法治保障能力的重要课题。

2. 数字经济带来的新型犯罪挑战

当前，我国的社会呈现出较为明显的数字化转型特征，大数据、人工智能等新技术层出不穷的同时，也带来了社会生产生活方式的全面革新，2021 年《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》即“十四五”规划发布，清晰设定了未来数字经济发展的基本原则和目标，数字经济已经成为国家经济高质量发展的新动能，数字经济规模处于快速扩张期，不过，随之而来的则是威胁数字经济安全的新型犯罪案件层出不穷，数字经济的发展在带来大量机遇的同时，也为安全风险防控带来了全新的挑战。

2.1. 网络数据安全风险

随着数字经济的飞速发展，互联网的运用也渗透到了经济社会生活的方方面面，无论是学习、工作

还是生活和娱乐，几乎都离不开互联网的运用。与此同时，网络数据也呈现爆炸性的增长趋势，数据是数字经济时代的关键生产要素，没有数据的收集、筛选、运用，就没有数字经济的效益产出[1]，在利益的驱使下，针对网络数据安全的犯罪也随之出现，如数据存储服务器非法入侵、个人信息贩卖等违法行为，严重侵害了国家数据管理秩序、个人隐私权等法益，而由于网络数据的泄露和传播导致的电信网络诈骗等下游犯罪更是会严重侵害公民财产权益，而我国针对网络数据安全领域的新型犯罪尚未形成体系化的刑法规制，网络数据安全风险的防控水平亟待提高。

2.2. 人工智能安全风险

数年前的 AlphaGo、不断发展的自动驾驶和近年来异军突起的 ChatGPT 等新技术，无一不体现着在数字经济的发展过程中的时代风口——人工智能，人工智能产业不断发展和升级，带来了无数的便利和便捷，但与此同时，也带来了巨大的未知性和不确定性，这种未知的背后则隐藏着巨大的安全隐患，自动驾驶技术造成的生命财产安全风险、利用 AI 机器人实施犯罪行为、机器人脱离操控实行的犯罪行为等具有严重社会危害性的行为刑法该如何进行规制，虽然目前人工智能技术仍处在发展提升期，但人工智能具备的超强学习和升级能力，其背后的风险和隐患也会随之更新升级，从长远来看，如何规制人工智能安全风险也是刑法所面临的重大问题。

2.3. 网络虚拟财产安全风险

由于数字经济的快速发展，网络世界当中的虚拟事物正在逐步参与到人们的现实生活中，加之网络交易的扩大化，类似于游戏账号、游戏装备、游戏点数等具备一定的价值，也需要持有人付出一定的金钱、时间、精力，同时也可以在互联网上进行交易，因此，逐渐形成了网络虚拟财产。而随着网络虚拟产业的发展壮大，网络虚拟财产的体量也不断增加，由于网络虚拟财产的持有者可以通过交易和流通获得实际的经济利益，犯罪分子便也对此虎视眈眈，产生了包括盗窃游戏账号、装备进行交易等类型的侵害公民网络虚拟财产的新型犯罪，为我国数字经济和虚拟产业的发展带来了新的挑战。

3. 传统刑事治理面临的困境

近年来，为了适应数字经济给刑法所带来的冲击和挑战，我国已经通过刑法修正案、司法解释、规范性文件等进行了回应，自 2015 年《刑法修正案(九)》的颁行代表着我国针对网络犯罪的刑事立法在数量及严密程度上均达到巅峰[2]，通过对第 253 条、第 287 条、291 条等条款的修改，回应了社会关切；《刑法修正案(十一)》也将通过新型犯罪手段实施的网络化侵害写入其中；截至目前，我国涉网络犯罪司法解释及规范性文件共有 14 部，其中，司法解释有 7 部，其他规范性文件有 7 部[3]。这些无一不体现着立法者对于新型犯罪所侵害法益的关注，尽管对于新型犯罪问题，我国已经初步形成刑法规范规制、司法解释填补、指导案例引领的“三位一体”新格局[4]，但面对层出不穷的新型犯罪风险，传统刑事治理仍然面临一定程度的困境。

3.1. 网络数据安全风险面临的困境

目前，我国刑法对于网络数据安全的维护主要是通过《刑法》规定的非法侵入计算机信息系统罪、破坏计算机信息系统罪等，虽然从某种程度上来讲，网络数据的存储、传输等步骤都要依赖于计算机信息系统才能实现[5]，计算机犯罪的罪名也一定程度上能够对网络数据安全类犯罪进行覆盖，但是以计算机信息系统为犯罪对象的计算机犯罪，受刑法保护的法益是计算机信息系统安全，而对于侵犯网络数据安全的新型犯罪来说，受到侵害的法益主要是国家的数据管理秩序以及数据所能够产生的数字经济效益，由此可见，计算机犯罪是不同于侵害网络数据安全的新型犯罪的，不能由计算机犯罪的罪名实现全面治

理，而没有关于治理数据犯罪的专门性规定，是当前刑法治理所面临的主要困难之一。

同时，针对网络数据安全的新型犯罪与信息犯罪也存在着混同问题，目前来看《民法典》《数据安全法》《个人信息保护法》等法律虽然对于数据、信息的保护形成了初步的保护体系，但是对于相关的概念和定义并没有实现统一，《民法典》虽然对于“数据”和“信息”的概念和区分都做出了简单的表述，但是并没有进行具体的论述和界定；而在《数据安全法》当中对于数据的定义则是“任何以电子或者其他方式对信息的记录”，从实际运用角度出发，这种定义并不能与信息进行很好的区分；同时在《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》等部分刑事司法解释当中又将数据和信息的概念混同，认为二者之间并没有区别，可以相互替换或代替使用[6]。由此可见，从法律体系的整体角度出发，并没有将数据的概念进行准确的明晰，但正是这种不明晰就会导致侵害网络数据安全的新型犯罪构成要件的认定标准模糊，进而导致对于犯罪的认定上也会产生一定程度的困难。

3.2. 人工智能安全风险面临的困境

人工智能是计算机技术发展至今产生的一种有别于传统计算机技术的新科技，它具备对于人类智能的强大的学习、模仿能力，是一种颠覆性的新技术，如果用于探索未知、弥补人类不足等正向行为，则对社会的发展有益，反之，如果用于实施违法犯罪活动，则会造成前所未有的负面影响。目前，大体上可以将人工智能分为弱人工智能和强人工智能两类，弱人工智能产品可以视为接受人类完全操控的一种新型工具，与传统犯罪的所借助的犯罪工具差别较小，虽然具有人工智能的属性，但是仍然应该被认定为是犯罪分子本人实行犯罪行为的一种延伸，应当由人工智能的操控者全权承担刑事责任，这是毫无疑问的。

而强人工智能则与弱人工智能的规制和治理截然不同，虽然目前强人工智能发展的并不完善，但是随着 ChatGPT 等深度学习人工智能的出现，强人工智能的进一步发展完善也是大势所趋，而强人工智能则很有可能进一步衍生发展产生其自己的意志和行动，如果在这种情况下，使用者对其进行引导性使用，最终导致人工智能凭借自己意志实行犯罪行为，刑法该如何规制？或更甚，在人工智能脱离使用者操控，在设计者、使用者、操控者都无法掌控的情况下独立实施危害行为，刑法又该如何应对？是否应当将强人工智能划分为能够承担刑事责任的主体？我国当前的刑罚体系中的生命刑、自由刑、财产刑、权利刑等刑罚处罚方式主要针对自然人而设立，无法适用于人工智能，那又该如何规制强人工智能犯罪呢？在目前人工智能势如破竹的发展趋势下，传统刑法对强人工智能的规制所面临的困境也在可以合理预见的范围之内，这也是应对人工智能安全风险所亟待解决的困境。

3.3. 网络虚拟财产安全风险面临的困境

网络虚拟财产属于随着数字经济不断发展而产生的新兴产物，由于其出现时间晚、发展速度快，导致对于网络虚拟财产的法律规制存在先天性的不足，难以全面应对司法实践当中层出不穷的侵害网络虚拟财产的犯罪案件，我国现有刑事立法当中，并没有对网络虚拟财产做出明确的定义和划分，相关规定较为笼统和粗略，也就导致了我国对于网络虚拟财产的法律地位和保护存在着较大的困境，相似个案之间的处理也存在着一定程度的差异。当前，网络虚拟财产的刑法规制仍然存在一定的空白，导致对网络虚拟财产的侵害活动难以得到有效的控制，从法理上看，主要是由于网络虚拟财产与传统的财产存在较大的区别，对于其是否具有财产属性、是否是刑法所保护的法益这两方面存在较大的争议；在司法实践当中，对于侵害网络虚拟财产的犯罪主要会被认定为盗窃罪、计算机犯罪两类，但是由于对于网络虚拟财产价值的司法认定存在一定程度的空白，导致法律的适用存在较为混乱的情况，对于如何认定其价值，

如何判定侵害行为的严重程度都面临一定程度的困境。

4. 新型犯罪问题的应对措施及建议

4.1. 网络数据安全风险的应对

4.1.1. 调整数据犯罪相关的刑法规范

当前在刑法当中，针对数据的专门保护仅有第 285 条的非法获取计算机信息系统数据罪，但是从犯罪构成要件的角度出发，该罪主要保护的法益是存储于计算机信息系统当中的数据，如果数据储存的媒介不是计算机信息系统，而是其他的数据储存介质，则难以受到妥善的保护。为了对网络数据安全实现妥善的保护，应当针对数据犯罪的对相关条款进行调整和补充，具体可以从以下两个角度出发：

首先，要实现对数据法益的认可，就要明确受到保护的法益之概念和性质，数据法益中的“数据”应当具有不可约为传统社会生产要素的独立属性。数据一方面是传统生产要素的数字化表现，另一方面，只有经过算法处理过后的数据才可能具有独立价值。据此，当数据作为传统生产要素的数字化表现时，数据的价值是附属性的，依赖于传统生产要素价值而产生，因此，此时对数据的侵害本质上是对传统生产要素的侵害。只有对具有独立价值的数据进行侵害时，才存在被数据法益涵盖的必要性。

其次，对数据法益的保护，不能仅仅局限于存储数据，数据是具有流通性的，除了应该着眼于数据存储安全之外，数据流通安全、数据使用安全也都是应当受到刑法保护的重要法益，我们应当以数据流转的全过程为着眼点，构建体系化的数据安全刑法规范。

据此，我们可以参考数据保护体系较为完善的德国刑法，对我国数据犯罪相关的刑法规范进行如下修改：第一，设置“危害数据安全罪”，明确数据法益的刑法地位，第二，将《刑法》第 285 条当中的计算机信息系统这一限制取消，对存储于各种不同介质中的数据进行全面的保护；第三，增设探知、变更、截取数据罪，将从存储到流通的数据流转全过程均纳入刑法规范的保护范围中；第四，增设非法利用数据罪作为兜底，规范由于数据安全遭到侵害导致流出的数据被二次或多次传播利用的行为，缩小泄露数据非法利用的危害范围和程度。

4.1.2. 强化数据的刑事合规

数据作为新型生产要素，为我国的数字经济蓬勃发展带来了生机和活力，各类企业作为数字经济的重要参与者，也是大量数据的拥有者，在维护数据安全上有着不可推卸的社会责任，刑事合规是企业预防刑事风险、构建数字经济安全体系的关键，也是经济社会高质量发展的重要一环。各类企业，特别是具备互联网平台的数字企业应该加强对数据刑事合规体系的建设，以强化企业的数据安全风险防控能力，具体可以从以下三个方面进行：

第一，在我国数据合规仍处于起步期的当前阶段，并没有形成放之四海皆准的数据合规指引体系，缺乏标准化的指引，对此，企业可以积极寻求检察机关的帮助和指引，检察机关作为负有推动数据刑事合规建设职责的主体，有义务引导企业建立健全刑事合规运行机制和体系。对于独立建立刑事数据合规体系确实存在现实困难的中小微企业，可以引入外部专业刑事合规服务机构，协助企业完成数据的刑事合规工作。

第二，建立以政府为主导、检察机关为辅导，依托于大数据管理局等行政机构，成立专门的数据刑事合规机构，对于企业的合规风险、合规漏洞进行监督和风险提示，并对专业刑事合规服务机构进行资格审查，强化数据刑事合规的日常管理工作。

第三，将数据刑事合规写入相关刑事法律规范当中，对于已经实行企业合规，建立了合理健全的刑事合规体系，恰当履行刑事合规职能的企业，在发生刑事合规无法规避的单位犯罪等情况下，实现对涉

案企业的从轻量刑、相对不起诉、适用缓刑或减轻处罚等，用以激励企业积极建设刑事合规体系、履行刑事合规职能。

4.2. 人工智能安全风险的应对

4.2.1. 增设人工智能相关的刑法规范

虽然目前的人工智能犯罪主要以弱人工智能的利用为主，仍然可以认定为犯罪工具的范畴，但是强人工智能被运用于犯罪是可以预见的，而在立法上，应该具备一定程度的前瞻性，因此，推动人工智能相关罪名的增设也是保障数字经济良好发展，维护社会秩序的题中应有之义，具体可以从以下三个角度出发：

第一，参考《刑法》第 286 条拒不履行信息网络安全管理义务罪，设立拒不履行人工智能安全管理义务罪，人工智能服务提供者作为人工智能产业的主要管理者和经营者，应该对于其所提供的人工智能服务承担安全保障义务[7]，采取必要性的措施，以保障其所提供的人工智能服务不被非法利用，避免造成社会危害。

第二，增设人工智能事故罪，人工智能在被设计和使用，特别是在设计使用之初，是完全按照设计者的意图设置运行的，其设计者对于其是否可能发生失控和脱离管理存在一定的预见性，在设计之初就应该对于有可能发生包括摆脱操控等意外事故的情况，可以预见或应当预见，因此，我国应当建立严格的人工智能设计研发责任制度，对于未能良好履行风险防范义务而导致造成人工智能失控或脱离管理等情况，产生社会危害的，应该追究其设计者的刑事责任。

第三，增设滥用人工智能罪，由于人工智能自身的特点，当其被犯罪行为人利用并实施犯罪活动时，有着不同于使用其他工具犯罪的特点，造成的危害可能更严重，因此，将滥用人工智能的行为纳入刑法规范，不仅能够震慑意图使用人工智能实施犯罪行为的人，也能够从源头上对于人工智能的违规违法运用进行预防，以达到遏制滥用人工智能行为，降低人工智能造成社会危害的可能性之目的。

4.2.2. 完善针对人工智能犯罪的刑罚体系

由于当前刑罚体系中的刑罚在设计之初所针对的对象就并非人工智能，因此，直接针对人工智能适用现有刑罚是不合时宜的，我们应该根据人工智能犯罪特别是强人工智能犯罪的特点，有针对性的增设刑罚处罚方式，用以更好的规制强人工智能犯罪。对于增设的处罚方式，可以从以下三个方面出发：

第一，删除数据，将与强人工智能实施犯罪具有因果关系的数据分类、归纳、总结，并将其永久删除，同时设立权限，禁止其再次获取相同或相似类型数据，确保同类犯罪行为不再发生。

第二，修改程序，在导致人工智能犯罪的数据数量占比过大，通过删除数据已经无法降低其危害社会的可能性时，将实施过社会危害行为的人工智能进行重新编程，从根本上修改其运行的框架和底层逻辑，使其无法再度获取可能实施危害行为的数据。

第三，永久销毁，是指将实施了危害行为的具备物理形态的人工智能或人工智能主机、芯片、硬盘进行摧毁和破坏，删除其一切数据和程序后，再从物理上彻底清除和毁损其数据和程序载体。通过删除数据和修改程序无法降低其危害社会的可能性时，使用物理手段，彻底杜绝其实施社会危害行为的可能性。

4.3. 网络虚拟财产安全风险的应对

4.3.1. 明确网络虚拟财产的性质和法律地位

应对网络虚拟财产面临的安全风险、保护网络虚拟财产不受侵害，首先要做到的就是明确网络虚拟财产的性质和法律地位，在现行刑事法律规范当中，并没有对网络虚拟财产作出明确的规定，但是在现

有的司法判例当中，已经有将网络虚拟财产认定为刑法意义上的财物之先例，首先，网络虚拟财产由于其持有者向其投入大量的时间、金钱等，使得网络虚拟财产与现实当中的有形财产相同，具备其自身的价值；其次，网络虚拟财产虽然与有形财物不同，无法在现实当中实际占有，但是网络虚拟财产是由其持有者通过网络进行直接支配的，同时还具备可交易性，与有形财产类似，可以进行交易和转移占有，具备财产的性质。由此可见，网络虚拟财产与刑法意义上的财物具有诸多相同性质，应当承认其财物性质和法律地位，将其纳入刑法保护范围。

同时，认定网络虚拟财产的性质还具备三点优势：第一，够为侵害网络虚拟财产犯罪的司法实践提供支撑，填补司法实践当中将网络虚拟财产认定为财物的瑕疵；第二，能够完善网络虚拟财产领域的民刑衔接，《民法典》当中对虚拟财产的价值和保障已经作出了相关的表述，在刑法中认可其法律地位，更加有利于完善我国法律体系，对网络虚拟财产给予更加充分的保障；第三，对于网络虚拟财产财物性质的认可，有利于司法实践当中用以对该类型的新型犯罪与计算机犯罪之间的区分，使裁判中的定罪量刑更加准确和适当。

4.3.2. 强化网络平台的用户管理

网络平台作为网络虚拟财产的主要承载者，应当严格落实网络平台用户实名制，完善对用户的实名制审核，对未进行实名认证或认证信息有疑问的账户实行限制交易、缩减权限等手段，对于存在疑问的用户交易进行及时的冻结、审核、撤销，依法履行信息网络安全管理义务，最大限度的降低平台用户的网络虚拟财产遭受侵犯的可能性，一旦发生网络虚拟财产侵害案件，也能及时准确的利用其平台实名制信息，协助司法机关准确高效的锁定犯罪嫌疑人，降低司法资源的浪费，最大限度的及时挽回用户的损失。

5. 新型犯罪问题的应对措施及建议

数字经济的高速发展既是风险也是挑战，既带来了全新的经济增长点和新的发展机遇，也同时带来了对传统社会管理秩序的新冲击，为了保障数字经济的高质量发展，实现“十四五”数字经济发展规划，加快建设数字中国，我们必须与时俱进地利用刑法，对危害数字经济发展的新型犯罪进行规制和应对，不断探索数字经济，为我们的社会带来的新挑战之解决路径。随着数字经济的深度和广度不断增强，传统刑法所面临的困境与挑战也会不断增加，因此，我们必须不断的加强探索，将数字经济的法治保障这一课题不断深入研究，对于在数字经济发展中产生的新型犯罪问题，我们必须从刑法学的角度出发，以刑法的根本任务为纲，不断填补法律空白、弥补法律瑕疵，同时数字经济发展的全局角度出发，提出有远见、有前瞻性的有效对策，完善刑事法律规范，推动刑事司法体系的建设。数字经济带来的社会发展和技术革新是空前的，我们必须融会贯通地运用习近平法治思想，建立系统化体系化的法治保障体系，才能够构建起符合时代发展需要的新时代数字中国。

参考文献

[1] 姜涛, 韩辰. 数字经济时代刑法规制网络犯罪的困境与出路[J]. 苏州大学学报(哲学社会科学版), 2023, 44(1): 57-69.

[2] 储陈城. 以利益衡量作为网络领域刑事治理的原则[J]. 法学论坛, 2021, 36(5): 61-72.

[3] 宁利昂. 网络黑灰产业的刑法治理[J]. 青少年犯罪问题, 2022(2): 57-67.

[4] 张昊. 为网络强国数字中国建设提供有力法治保障[N]. 法治日报, 2023-04-19(004).

[5] 钱叶六. 刑法处罚范围适度扩张的合理性及其限制[J]. 警学研究, 2020(5): 46-57.

[6] 刘纯燕. “窃取”网络虚拟财产行为的定性研究[J]. 山西警察学院学报, 2021, 29(4): 13-18.

[7] 单勇. 论互联网平台的犯罪控制义务[J]. 现代法学, 2022, 44(3): 66-81.