Open Journal of Legal Science 法学, 2023, 11(6), 5695-5700
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.116813

Hans汉斯

数据犯罪困境及治理进路探索

张　迪

道里区人民法院，黑龙江　哈尔滨

收稿日期：2023年8月22日；录用日期：2023年8月30日；发布日期：2023年11月20日

摘　要

数据时代飞速发展，数据犯罪随之而来，鉴于立法的滞后性，我国现行刑法并没有对数据安全进行全流程保护的规定。本文旨在探索研究数据犯罪在刑事立法的完善问题，以设置一套相对统一的数据犯罪的定罪量刑标准，以更精准的在司法实践中区分罪与非罪、此罪与彼罪。本文将采用理论分析法、比较研究法的研究方法围绕数据犯罪在司法实践中遇到的困境，从立法和司法两个层面分析，并提出完善数据犯罪治理的相关对策，试图推动数据犯罪刑事立法的发展。

关键词

数据安全，数据犯罪，计算机

Data Crime Dilemma and Governance Approach Exploration

Di Zhang

Daoli District People's Court, Harbin Heilongjiang

Received: Aug. 22nd, 2023; accepted: Aug. 30th, 2023; published: Nov. 20th, 2023

Abstract

With the rapid development of the data era and the consequent data crime, in view of the hysteresis of legislation, China's current criminal law does not provide for the protection of data security in the whole process. This paper aims to explore and study the improvement of data crime in criminal legislation, so as to set up a relatively unified set of conviction and sentencing standards for data crime, so as to more accurately distinguish between crime and non-crime, this crime and that crime in judicial practice. This paper will adopt the research methods of theoretical analysis and comparative research to focus on the difficulties encountered by data crimes in judicial practice,

文章引用: 张迪. 数据犯罪困境及治理进路探索[J]. 法学, 2023, 11(6): 5695-5700.
DOI: 10.12677/ojls.2023.116813

analyze from two levels of legislation and justice, and propose relevant countermeasures to improve data crime governance, in an attempt to promote the development of criminal legislation on data crimes.

Keywords

Data Security, Data Crime, Computer

1. 数据犯罪概述

1.1. 数据概念之明晰

数据是逻辑推理、分析的基础，是原始事实和信息的数字化集合。数据安全法将数据定义为“任何以电子或者其他方式对信息的记录”。即依托计算机及网络信息系统以及相关存储介质传输、存储、处理的电磁数据，此定义属于广义的“数据”概念。在广义概念的基础上，数据安全法从宏观的视角确立了我国数据安全立法的基本框架，对于数据安全领域的制度安排、配套措施、标准制定等方面进行统筹性、系统性、体系性地规定，为数据安全领域的发展提供重要助力。

在刑事法领域，犯罪对象直接指向数据的罪名为非法获取计算机信息系统数据罪，非法获取计算机信息系统数据罪中的“数据”，应当解释为身份认证信息，但伴随计算机技术不断深入发展，“数据”的概念也应随之发展。因此在司法实践中，对“数据”概念的解释，不再局限于身份认证信息，应结合具体案件的情形做扩大解释，以实现数字经济转型背景下对数据权益的充分保护。对数据的扩大解释，并不违反罪刑法定原则，因为若仍拘泥于传统的“数据”范围，无法适应数据时代的发展，则无法实现对数据法益全面保障的目的。

1.2. 数据犯罪的内涵界定

数据犯罪是具有鲜明时代特征的新型概念。针对数据是否做扩大解释，数据犯罪呈现出不同的定义模式，狭义的数据犯罪是指具体的罪名，即以数据为犯罪对象的计算机罪名，主要是指规定在我国《刑法》中的具体罪名。狭义的数据犯罪概念，能够准确描述数据犯罪的本来面貌，避免与其他罪名产生适用分歧。广义的数据犯罪是以数据为犯罪对象、以数据为犯罪载体、以数据为犯罪工具的与数据相关的犯罪。此时，数据犯罪作为庞大的犯罪集合体而呈现，包含以数据形态呈现的个人信息、知识产权等诸多法益内容[1]。数据犯罪的罪名界定需要高度依赖于实际的法益侵害类型。司法实务中，针对数据的不同解释，数据犯罪主要包括以下四类：一是计算机类犯罪，针对作为数据、信息载体的计算机信息系统的犯罪；二是财产类犯罪，将数据解释为虚拟财产、电子货币等数据财产权利；三是人身犯罪，将数据解释为公民个人信息罪；四是知识产权犯罪，将数据解释为著作权、商业秘密等。刑法中其他诸多罪名的法益亦能呈现出虚拟化、数据化的表现样态，同样能够被数据犯罪所涵盖，但其余罪名尚未呈现出体系性、系统性的数据犯罪特征，而是散见于刑法分则罪名之中，侵害对象表现为国家秘密、公司、企业重要信息、信用卡信息等特定领域的数据犯罪[2]。

2. 数据犯罪面临的问题

2.1. 立法层面

法律具有滞后性，应对社会的发展变化，法律难以及时予以调整，数据犯罪亦是如此。在立法层面，本文从数据安全法益和数据保护模式两个方面论述刑事立法的滞后性。

2.1.1. 数据法益

我国现行刑法中，以“数据”作为犯罪对象的罪名主要为非法获取计算机信息系统数据罪、破坏计算机信息系统罪等计算机罪名，以及与计算机无关的危险作业罪、妨害药品管理罪等涉及数据的罪名，这些与计算机无关的数据犯罪，在犯罪行为方式上表现为涉及篡改或者伪造生产安全数据、药品申请注册数据等，其侵害的法益表现为生产安全数据、药品申请注册数据等[3]。也就是说当前数据时代飞速发展，刑法语境下的数据，并不仅仅停留在过去单纯的身份认证信息、计算机的简单数据犯罪的层面。数据犯罪也在顺应时代的发展，数据开始逐渐涉及到生产安全数据、药品管理数据等多重领域，其保护的法益层面也从过去的财产法益扩张至人身法益、知识产权法益，甚至是公共安全法益、国家安全法益。虽然数据法益的保护形式，在很多情形下可以被包含在人身财产法益中，即数据法益与人身、财产法益发生竞合，但由于当前数据欠缺刑事立法的独立性，对于无法被包含其中的情形，成为了我国数据犯罪的治理难题。当前规定在我国《刑法》中涉及数据犯罪的罪名，主要是以保护计算机系统安全而展开的相关罪名，其立法的初衷与当时计算机兴起的时代背景相呼应，因此其对数据安全的保护作用是有限的。正如有学者认为，法益所具有的抽象性、概括性特征，并不代表在客观上否定其被独立保护的必要性，数据法益亦是如此[4]。因此，我国刑事立法中应加入对数据安全法益的保护，以应对当前大数据背景下，衍生出的各种数据犯罪行为，让裁判者有法可依。

2.1.2. 数据保护模式滞后

鉴于立法的滞后性特征，我国刑法针对数据安全的保护还停留在预防犯罪的保守模式，当前大数据持续发展，数据显现出经济、社会、政治等多重价值，关系到个人利益、企业利益、甚至是国家、社会安全的稳定。伴随数据不断的更新，数据犯罪的行为手段也随之多样化。因此，针对数据犯罪停留在过去被动性防治的模式，已无法适应时代的发展需求。

现有刑法涉及的数据安全保护，无法覆盖数据生命周期的始终，无法对数据安全起到有效的保护作用。《信息技术安全数据安全能力成熟度模型》将数据生命周期划分为数据采集、数据传输、数据存储、数据处理、数据交换以及数据销毁六个阶段，与六个维度的数据安全要求一一对应。同时，我国《数据安全法》将“数据处理”作广义理解，明确规定数据处理包含数据的收集、存储、使用(即狭义的数据处理)、加工、传输、提供、公开等。两者均大致覆盖了数据全生命周期链条中的各个环节。实践中针对数据实行的犯罪行为方式不仅表现为对计算机信息系统中存储、处理、传输数据的非法获取、删除、修改、增加，还体现在数据监听、数据伪造、数据投毒、数据勒索、数据滥用、过度挖掘等一系列行为。但我国刑法所体现的侧重点主要在于非法获取和破坏(删除、增加、修改)两种行为类型，这不仅无法满足对网络数据犯罪行为规制的现实司法实践需求，而且与国家制定的标准以及《数据安全法》的内容相悖。

2.2. 司法层面

鉴于立法对于司法实践的指导作用，刑事立法的缺失直接导致司法适用混乱，本文从涉及数据犯罪的罪名之间界限不清及数据犯罪法律属性混淆两个方面论述数据犯罪在司法适用中遇到的问题。

2.2.1. 涉及数据犯罪的罪名之间界限不清

我国现行刑事立法对与数据犯罪相关的各罪名之间欠缺明确的认定界限，立法的模糊不清直接导致司法适用的混淆。其中主要原因是“数据”并不是我国现行刑事立法所直接保护的法益，而是将数据解释为我国刑法中的“信息”，由于“数据”和“信息”的概念不清，直接导致罪名适用混乱，如我国刑事立法非法获取计算机信息系统数据罪和侵犯公民个人信息罪[5]。我国现行立法中关于数据的保护主要以保护计算机信息系统不受侵犯为主。显然对计算机系统、对“信息”的相关法条不能当然适用于数据犯罪中。我国《网络安全法》对数据虽然已经制定了分类分级制度，但是只有刑法才能认定行为人有罪，才是认定行为是否犯罪的最终根据。

2.2.2. 数据犯罪法律属性混淆

数据犯罪的司法适用在实践中以非法获取计算机系统数据罪为主，这一罪名在适用中，办案人员在犯罪行为属性时极易将其行为手段或工具代替其所侵害的法益，即只要是通过电子计算机实施犯罪的行为则认定为该罪名，从而在导致该罪名在司法实务认定中逐渐显现出兜底的适用趋势。

导致这趋势的原因主要为：其一，数据的具体定性不明。当前数据犯罪所侵害的对象主要以网络虚拟财产为主，其属性在学界颇具争议，当虚拟财产被认定为“物”时，则赋予了数据在法律上的价值属性，非法获取数据的行为，则触犯盗窃罪。当虚拟财产单纯的被认定为其固有的虚拟数据的属性时，非法获取数据的行为，则触犯非法获取计算机罪。但网络虚拟财产在司法解释中被明确规定为系统数据，否定了数据为“物”的价值属性的同时，扩张了了非法获取计算机信息系统数据罪的适用范围，为其成为兜底性罪名打下了基础。二是商业秘密数据化。数据时代的兴起，各行业为了实现高效办公、顺应时代的发展，将办公流程、经营信息从线下搬到了线上。商业秘密也是如此。我国关于商业秘密的保护，主要规定在《反不正当竞争法》中，将商业秘密的属性认定为有价值的信息，鉴于商业秘密的“信息”属性，经常被解释为“数据”，同时，目前我国针对商业秘密及相关知识产权的刑事立法还不完善，司法实践中能够适用的罪名较少，进一步扩张了非法获取计算机信息系统数据罪的适用范围。

3. 完善我国数据犯罪治理的相关对策

3.1. 构建网络数据犯罪的客观归罪标准

建立统一的数据犯罪入罪标准、罪质与罪量标准将有利于完善刑法中数据犯罪的客观归罪要件，同时也将使得目前司法实务中对网络数据犯罪主观归罪的现象有所改变。

3.1.1. 依据数据保护等级确定入罪标准

“数据分类分级保护制度”规定在《数据安全法》第二十一条，明确了在数据遭受侵害过程中，根据对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护的目标，这为防止司法适用“一刀切”或“口袋化”，同时也为确定数据犯罪入罪门槛提供了重要指引。据此，刑事立法也应借鉴于此，通过对数据法益进行等级划分，结合犯罪行为所侵害的法益种类、法益侵害程度设定不同等级的入罪标准。通过设定不同的入罪门槛，刑法可以明确针对侵犯不同级别数据行为的打击力度，以此区分轻重缓急，打击数据犯罪的行为更具有针对性。同时，在刑法确定不同入罪标准的基础上，最高人民法院、最高人民检察院可以联合出台相关司法解释，明晰各入罪标准下的具体情形，为办案人员提供指引，同时也应保留适当裁量空间，以应对司法实践中个案的特殊的复杂情况。

3.1.2. 在数据等级保护的基础上明确量刑标准

在确定了数据犯罪的入罪标准的基础上，应针对具体的罪名设置不同的量刑情节，即针对不同的情

形，确认从轻、从重的量刑情节，可结合对侵害数据法益的种类、程度，对社会危险性等多重因素考量，在同一个罪名项下设定不同的量刑情节，以应对司法实践中的情形。我国现行刑事法律中，对于部分犯罪的认定，主要是通过行为性质判断其是否构成犯罪，通过犯罪行为所取得的经济利益作为量刑的因素考量，对数据犯罪亦是如此。对数据类犯罪的传统入罪标准主要以客观行为性质和数额标准作为该类犯罪的构成要件。数额标准即行为人所实施的行为给犯罪对象所造成的经济损失，或行为人的违法所得。但数据时代迅猛发展，数据犯罪的表现方式也日益多样化，传统的定罪模式已无法顺应时代的发展。当前，认定数据犯罪，应突破传统的犯罪构成要件理论，应更注重行为所侵犯的数据客体，以及其所侵害课题所造成的犯罪结果即社会危害性，并将犯罪数额作为定罪量刑的其中依据之一，而不是决定性因素，进行综合考量。例如，可以通过统计并计算因行为人的行为所引发的浏览、点击、评论、转发数量，以评定行为的社会危害性程度。因此，在具体的司法解释中可以分段设置合理的数值区间，以作为不同的量刑标准。而对于数量特征不明显或者危害结果较为抽象的部分数据类犯罪，则应依据其犯罪情节进行综合考量。

在涉及数据的犯罪中，数据常作为法益侵害对象存在，其表现形式多为存储在电子载体或媒介中，当同一犯罪行为同时侵犯传统法益和数据法益，或者同时侵害不同的数据法益时，应按照刑法中想象竞合的原理处置，即选择其中较重罪名。如果有数个针对数据法益的侵害行为，那么则按照刑法中数罪并罚的原理处置。

3.2. 定罪思路

在涉及数据犯罪的定罪时，统一思路，更有助于在司法实践中有效运用。

3.2.1. 全面评价原则

在司法实践中，涉及数据类犯罪的具体应用，在判断罪与非罪时，应结合数据的获取手段即是否是侵入计算机系统所获取、数据的具体类型、处理方式即是否予以删减或者加工、数据的用途、以及行为所造成的危害后果进行全方位的整体评价。在涉及此罪与彼罪的罪名选择时，行为的人的手段行为、目的行为均应作为行为评价的对象，二者缺一不可。同时应对数据安全产生的危害进行全方位的评价，不能将数据与计算机信息划等号，因为并不是所有侵害数据安全的行为均可以评价为计算机信息系统犯罪。如在盗窃虚拟财物罪中，行为人的手段行为是修改数据，而其目的行为是获取财物，如果将其归类于数据犯罪，就无法全面评价其违法行为，只有将其定位于财产犯罪，才能有效评价其手段行为和目的行为。

3.2.2. 定罪顺序

在定罪顺序上，应首先结合行为人客观行为所指向的行为目的以及其主观意图推断行为所侵犯的法益是否类属于我国现行《刑法》中已经类型化规范的法益，即当数据仅仅作为犯罪的工具或者媒介载体时，不能认定为数据类犯罪。如行为人以数据为工具，以获取财产为目的，其所侵害的仅仅为传统财产法益，应当首先以传统的财产类犯罪定罪量刑，如行为人所实施的行为，客体指向数据，具体举例而言，当数据为个人信息时，构成侵犯公民个人信息罪，此时，具体罪名的认定取决于数据的性质和种类。如果犯罪行为侵犯的数据不能为刑法类型化，其行为属于以数据为对象侵犯数据安全时，则可以以非法获取计算机信息系统数据罪或破坏计算机信息系统进行认定[6]。例如，行为人利用其在 A 公司研发部门的便利，违法公司规定，使用手机、无线路由器等设备突破对方的技术障碍，将其中存储的核心源代码拷贝后带至家中笔记本电脑中保存，同年 6 月在网站上兜售，非法获利数 10 万元。应当认为采用技术手段绕过对方技术障碍，非法获取计算机数据，情节严重的构成非法获取计算机信息系统数据罪。

4. 结语

互联网信息技术日益兴起，数据如同一把双刃剑，其在推动经济发展的同时，多种多样的数据犯罪形式也随之而来，成为司法实践中的难题。因此将数据分类等级保护、数据犯罪的治理等问题纳入刑事立法才能有效的指导司法实践。同时，数据犯罪的预防应与治理并行，从源头上减少数据犯罪，以推动数据时代的健康发展。

参考文献

[1] 冯卫国, 李婷. 论大数据和信息犯罪及刑法规制[J]. 犯罪与改造研究, 2020(10): 14-20.

[2] 顾伟, 孙伟, 陈朝铭. 数字化时代数据犯罪的刑法回应[J]. 上海法学研究, 2022(1): 141-149.

[3] 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.

[4] 李爱君. 数据权利属性与法律特征[J]. 东方法学, 2018(3): 64-74.

[5] 陆旭, 郑丽莉. 以数据为媒介侵犯传统法益行为的刑法规制[J]. 中国检察官, 2020(12): 65-71.

[6] 刘宪权, 石雄. 网络数据犯罪刑法规制体系的构建[J]. 法治研究, 2021(6): 44-55.