Open Journal of Legal Science 法学, 2024, 12(11), 6458-6463
Published Online November 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.1211917

Hans汉斯

# 数据犯罪分类分级保护研究

**李铭暄**

天津大学法学院，天津

收稿日期：2024年9月30日；录用日期：2024年10月15日；发布日期：2024年11月21日

## 摘　要

**当前随着科技的发展，我国数据犯罪案例不断增多，但同时也出现了诸如罪名适用混乱、刑法在数据分类保护上的重合等问题。为此，需要进一步明确数据安全法益的内涵，对数据安全进行独立保护，以分类分级保护理念为指导，构建数据安全法益类型化保护体系，对危害数据安全法益的行为实现有效规制。**

## 关键词

**数据，数据犯罪，数据安全法益，数据分类分级**

# Research on the Classification and Hierarchical Protection of Data Crimes

**Mingxuan Li**

Law School, Tianjin University, Tianjin

Received: Sep. 30th, 2024; accepted: Oct. 15th, 2024; published: Nov. 21st, 2024

## Abstract

**Currently, with the development of technology, there are increasing cases of data crimes in China, but there are also problems such as confusion in the application of criminal charges and overlapping of criminal law in data classification protection. Therefore, it is necessary to further clarify the connotation of legal interests of data security and protect data security independently, guided by the principle of classified and graded protection, to build a type-specific protection system for legal interests of data security, and effectively regulate behaviors that endanger legal interests of data security.**

## Keywords

**Data, Data Crimes, Legal Interests of Data Security, Classification and Grading of Data**

文章引用: 李铭暄. 数据犯罪分类分级保护研究[J]. 法学, 2024, 12(11): 6458-6463.
DOI: 10.12677/ojls.2024.1211917

## 1. 引言

随着互联网、5G、人工智能等科技的快速发展，数据安全也成为当下讨论的热点话题。围绕数据保护和利用的犯罪风险不断增加，数据犯罪的相关案件呈井喷式发展，犯罪方式和犯罪产业链也不断复杂化，防范数据安全风险也逐渐引起学界的关注。当前数据犯罪的规制存在立法保护重合、司法扩张适用等诸多问题，究其原因是数据安全法益尚不明晰，造成数据犯罪规制混乱，需要进一步明确数据安全法益，同时引入分类分级保护模式，进行系统化的保护和规制。

## 2. 数据安全刑法规制的现实困境

### 2.1. 数据犯罪类型

在威科先行数据库中，以“数据犯罪”为关键词，检索范围为全文，案由选择刑事，共检索出相关裁判文书116份，涉及“破坏社会主义市场经济秩序罪”、“侵犯公民人身权利”、“民主权利罪”、“侵犯财产罪”、“妨害社会管理秩序罪”和“贪污贿赂罪”。其中“侵犯财产罪”和“妨害社会管理秩序罪”占比较大，侵犯财产罪中尤以“盗窃罪”最多，为11份，在“妨害社会管理秩序罪”中“非法获取计算机信息系统数据、非法控制计算机信息系统罪”数量最多，为62份。掩饰、隐瞒犯罪所得、犯罪收益罪次之，有32份，且大多数是为非法获取计算机信息系统数据犯罪所获得的数据进行收购转卖而构成本罪。

分析以上检索出的判决书可以看出，与数据犯罪有关的罪名可以大致分为三类。一是侵入获取型数据犯罪，即突破技术屏障，非法侵入数据库，从而获取大量信息，例如非法获取计算机信息系统数据罪，侵犯公民个人信息罪、侵犯商业秘密罪等。这一类罪名在实践中也较为常见。二是攻击破坏型数据犯罪，表现为对数据进行删除、修改、增加的行为，致使数据发生意外毁损或灭失，损害的是数据的完整性、可用性。攻击者基于报复、泄愤或打压竞争对手等目的，利用黑客技术侵入他人计算机信息系统或植入后门，并对系统数据、存储介质数据进行恶意删除、修改，例如非法侵入计算机信息系统罪等。三是其他关联型数据犯罪，行为人以数据作为犯罪手段或工具，通过数据或互联网进行传统犯罪，即传统罪名新形态，例如通过删除、修改、损毁数据实施传统盗窃、侵占、抢劫等犯罪行为。例如盗窃罪、抢劫罪等侵犯财产类罪名都有可能包含在数据犯罪涉及罪名中来。

### 2.2. 数据犯罪的规制困境

从上述法律检索出的判决书不难发现，数据犯罪在司法实践中存在扩张适用的现象。作为犯罪对象的“数据”范围，既包括与财产犯罪相关联的网络虚拟财产、加密货币等财产性利益，也包括能够识别特定自然人的考生信息、户口信息等个人信息。数据犯罪与传统犯罪在范围上存在交叉，比如通过破解虚拟货币服务商指令代码的方式，另行生成虚拟货币牟利的行为，或者通过撞库收集被害人姓名、身份证号、银行卡号、电话等个人信息的行为，实际上是通过获取数据来侵犯财产权或隐私权，司法实践中却不考虑数据的具体内容而对其作出广义理解，将上述行为评价为数据犯罪，扩张了数据犯罪的适用空间，模糊了数据犯罪与传统犯罪的界限[1]。

而法律规定中也同样存在问题。目前我国《刑法》和司法解释中没有较为明确的关于数据犯罪的概

念界定，只有部分涉及到将数据作为犯罪对象的规定。例如“非法获取计算机信息系统数据”、“破坏计算机信息系统罪”明确规定了“数据”是本罪的对象。此外还有与数据相关的，将数据作为犯罪工具或犯罪表现形式等一系列触犯传统罪名的犯罪。这种立法模式对数据安全的保护不充足，导致司法实践中因法益性质不清而产生罪名适用的偏差。

例如，对于能够识别特定公民身份的个人信息，两高在《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》中规定了“非法获取计算机信息数据罪”中的“数据”包括账号、口令、密码、数字证书等身份认证信息[2]。与此同时，两高发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》则同样将此类信息作为“侵犯公民个人信息罪”中的“公民个人信息”并予以保护。这明显导致刑法在数据分类保护上的重合，也必然会造成司法实践中对数据犯罪的定罪难题。

无论是数据犯罪的扩张适用，还是对不同类型数据保护产生混淆，归根结底在于目前立法者对不同类型数据犯罪所侵害的法益界定不明。法益侵害是犯罪的本质，有必要对数据犯罪的法益予以明确，引入数据法益概念，对数据犯罪进行法益类型化定位与阐释[3]。

## 3. 数据安全法益的重建

### 3.1. 数据安全具有法益独立性

数据安全的概念最早由美国学者提出，欧盟《信息技术安全评估准则》中首次规定了数据安全三要素，即数据的保密性、完整性和可用性。数据必须依据国家法律、规定和标准进行采集、处理和利用。非法获取、利用和泄露数据将会导致个人权益和社会利益受到侵害，其应当受到适当的安全措施保护，防止数据的损失、篡改、泄露和滥用等情形发生。同时，数据主体应当拥有自我决定权，指定数据的使用目的与方式，保障数据主体权利，保护数据涉及个人隐私的信息，防止在未经数据主体同意的情况下被非法收集、使用和传播，从而侵害数据主体的个人隐私权、尊严权。此外，在数据被商业利用时，数据的价值和利益也应当得到合理的保护，尊重数据主体对数据资源的产权保护[4]。

在这之后，世界各国都逐渐开始进行各自的数据安全立法。在此过程中出现了多种立法形式。其中值得一提的是以美国为代表的集中式立法模式，将社会公众对于数据安全的信赖利益作为数据安全保护性立法的基础，围绕此进行数据犯罪各项规范的构建。包括美国《计算机滥用与欺诈法》和德国《一般数据保护条例》等多部法律都对数据安全进行保护立法[5]，欧洲《网络犯罪公约》将数据安全与计算机信息系统安全分开保护[6]。我国在近些年来也进行了许多针对数据安全保护的立法，例如《网络安全法》规定了数据的保密性、完整性及可用性，与国际大多数国家对数据安全的保护模式相接轨[7]。

随着数字时代的到来，数据的内涵已变得更加多样和复杂，数据所反映的不再仅仅只是作为媒介储存的信息，其背后承载了更多人与人之间的社会关系，蕴藏着极大的社会经济价值。基于此，对数据安全法益进行独立保护符合司法实践的现状，也是大多数国家立法的共识。法律应当保护数据主体对数据的排他性使用权限，维护数据在社会往来中的安全性和可信赖性，将其作为一种独立的法益来进行保护[8]。

### 3.2. 对数据安全法益进行刑法保护具有合理性

确定一个法益是否是刑法上具体犯罪所保护的法益，需要妥当确定法益是否具有要保护性、特定性、融洽性和可判断性[9]。前文已经提到过数据安全法益内容的特定性，此处仅就其他三个标准进行论述。

首先，数据安全法益需要刑法进行保护。数据异构性、规模性和复杂性决定了数据侵害的层次性，在数字化时代，随着数据采集、传输、存储等多个环节领域的流通使得数据不断被复制和共享，渗透在社会生活的多个领域和各个环节。数据的价值不再局限于数据本身，还承载着个人、组织、社会、国家

多方利益侵害数据可用性的行为，可能影响数据权益者使用以及享有相应利益的自由，某些侵害数据的行为会损害个人的合法财产，例如公民个人所有的虚拟财产；有些还涉及到社会公共利益，群体性数据被窃取、篡改和破坏可能对社会经济的发展造成严重危害；涉及国家秘密的数据还可能涉及国家安全利益的保护。

其次，数据安全法益与数据犯罪的构成要件和不法程度相融洽。数据犯罪具有技术属性，需要以此为依据对“数据”进行范围的界定。同时，数据在不同阶段需要侧重保护的内容不同，例如在数据传输阶段，需要重点保护数据的传输安全及注重保密性，而对于修改数据但并未侵犯数据安全法益的行为则不予刑事处罚。此外，数据安全法益受侵害的严重程度决定了“情节严重”“后果严重”等入罪标准的解释适用。考虑到当前司法现状，可以在目前以违法所得具体数额、被害人的经济损失的标准的基础上，补充以数据性质、数据种类等作为数据安全法益被侵害的不法程度的标准，并逐步将重心转变到后者上，实现以数据安全法益侵害程度来评价数据犯罪的行为后果，做到数据安全法益与不法程度的融洽。

最后，数据安全法益的内容具体清晰，并不与其他法益相混淆。当前司法实践中之所以频繁出现罪名适用的混乱，根本原因在于对具体案件对象的性质判断标准有误。随着大数据时代技术的发展，众多以传统媒介为载体的财产如今往往以数据的形式出现，还有诸如虚拟财产的出现，都引发了许多争议。例如 2013 年两高《关于办理盗窃刑事案件适用法律若干问题的解释》的说明中明确提到，虚拟财产的属性是计算机信息系统数据[10]，使得涉及虚拟财产的案件很多都以非法获取计算机信息系统数据罪定罪处罚，这都导致了该罪的扩张适用。然而数据安全法益从数据本身出发，以数据自身的内容和技术要素作为划定数据安全风险的标准，更好地确定数据安全法益的内容，对不宜评价为危害数据安全法益的行为不认定为数据犯罪显然更有利于解决司法适用混乱的问题。

当前我国数据犯罪的立法规定与司法解释均未能围绕数据安全法益来解释数据犯罪的构成要件，导致数据安全法益的立法批判功能和解释适用功能均未能正常发挥。因此，对数据犯罪的解释适用应着重将数据安全法益纳入数据犯罪的构成要件之中，并对数据进行分类分级，采取等级化保护，对各种数据的法益性质予以识别，通过数据分类分级，认识和把握数据类型、结构，以及由此形成不同层级的数据安全法益侵害风险和保护需求，在此基础上，确定法律保护的重心，并将其作为数据犯罪罪质和罪量的评价依据，为数据犯罪的司法适用提供新的解决思路和依据。

## 4. 数据安全法益类型化保护的体系建构

《数据安全法》明确了数据分类分级保护的模式，对于不同重要程度的数据进行分类分级保护，损害结果更大，重要程度更高的数据保护力度也就更大，反之保护力度相对较小，甚至不受刑法的规制。即便是同一类数据，出于定级要素的不同，也可能受到不同程度的保护，相反，不同种类的数据，如果受到损害相当，也可能会受到同等程度的保护。通过对数据的分类分级，可以避免刑法的扩张适用，对数据安全法益进行更为科学和针对性的保护。

### 4.1. 贯彻数据分类分级保护理念

数据的分类保护指以数据的属性、主体等作为划分的依据，将数据按照不同的类型进行划分及保护。例如根据数据来源的不同，可以将数据划分为个人数据、商业数据和政府数据等等。当前我国与数据犯罪相关的罪名适用混乱就是因为没有对数据进行明确的分类分级，例如侵犯公民个人信息罪与侵犯商业秘密罪是依据数据主体身份的不同设置罪名，但同时三种危害计算机信息系统罪又是依据数据不同阶段进行设置，两种划分标准造成实践中常常出现保护范围上的交叉，也就导致了罪名适用的混乱。

我国《数据安全法》在立法时规定了个人信息、核心数据和重点数据[11]。有关国家核心数据是否属于重要数据，学界目前有众多争议，有学者主张此类数据应当属于重要数据[12]，由于此类数据涉及国家安全等核心利益，其重要程度明显要高于其他重要数据，应当予以更严格的保护，因而笔者赞同对此类数据实行有别于重要数据的更加严格的保护。除此之外，涉及商业秘密、社会公共利益的数据其重要性往往并不逊于部分国家核心数据，因而有理由将此类数据作为重要数据予以保护，即涉及国家安全、社会公共利益等数据都属于重要数据的保护范畴。个人数据则需要注意与个人信息进行区分，除具有可识别性的个人信息之外，其他与个人相关的数据也当然属于个人数据的范畴，而如何进行规制和保护则需要具体分级讨论。

数据分级则是以数据被侵害的程度进行区分，对于法益损害程度较轻、危害不大的无需刑法进行保护，法益损害较高的进行适度保护，而对于损害较重，危害程度较大的进行严格保护。数据的分级保护与分类保护是紧密联系的，即便是同一种类的数据，因为受损害程度不同，受到保护的级别也会不同；反之，不同种类的数据，受到损害的程度不同，也可能会受到同等级别的保护[13]。

## 4.2. 数据安全法益分类分级保护模式的建立

### 4.2.1. 个人数据的类型化保护

个人数据与人格尊严与自由密切相关，体现着公民个人对自身相关信息排他性的自主权，有学者认为这一权利即为个人信息自决权，其所侵害的法益是数据人格法益。即便对具有可识别性的人格要素所衍生出的财产权益进行侵害，也应当认为其是对个人数据法益的侵害。对个人数据的保护应当围绕公民个人对数据的自决权进行区分，将对个人数据的不当采集、不当转移泄露、不当使用等进行分阶段保护。对于敏感个人数据，应当采用更加严格的规制手段，而对于特殊群体，例如涉密人员的重要数据，也应当区分对其与普通公民的数据的保护程度[14]；对于非特殊群体的一般数据，则可以根据实际情况，决定是否应当由刑法进行保护，若未造成严重的危害后果，刑法可以不予保护[15]。

### 4.2.2. 重点数据的类型化保护

不论是涉及市场经济发展的商业数据，还是涉及社会公共利益的公共数据，都涉及到数据的公共属性，对此类数据的损害后果也往往大于对个人数据的危害后果，因而应当采用更为严格的规制措施。同时也需要针对数据的不同特性进行区分，例如对商业数据的保护归根结底是为了促进市场的有序竞争和经济的繁荣，需要重点关注商业数据的财产属性，保证数据的规范流通及合理使用，确保数据控制、数据开发、数据转让、数据许可使用不被过度限制，针对数据自身财产价值的大小进行差异化的保护。对于公共数据，则需要重点保护其背后的公共利益，确保公共数据不被随意窃取、泄露，不被毁坏和滥用。在保护公共数据的安全及有序的同时，保障公共数据的开放共享，确保对公共数据的安全管理。

### 4.2.3. 核心数据的类型化保护

与国家安全、公共安全、社会秩序等密切相关的核心数据承载着更多的公共属性与公共安全性质，这类数据的安全价值明显高于一般数据和重要数据，需要对全流程各阶段的数据安全及使用进行防护和管控[16]。不同于商业公共数据等注重流通和利用，核心数据优先要保护的是其安全性，需要秉持数据安全管理思路，建立核心数据的安全管理制度。同时，应当在刑法中体现对不同安全等级的数据不同级别的保护力度。对于事关国家安全、受危害程度高的核心数据，应当通过刑法进行严格保护；对于事关国家发展，但需要向民众公布或其他受危害程度不高的数据，则可以采取较低一级的保护措施。同时，也可以针对不同安全等级的数据适用不同的入罪门槛，安全等级较高的核心数据采取较低的入罪门槛，安全等级较低的核心数据采取相对较高的入罪门槛，从而实现对该类数据的类型化保护。

## 5. 结语

当前我国对数据犯罪定性不清，司法实践中出现大量罪名适用混乱的案例，立法上关于数据犯罪的相关罪名适用也陷入误区，刑法对数据犯罪的规制明显不足。根本原因在于数据安全法益定性不明，对数据安全法益分类分级保护意识不够。明确数据安全法益的内涵，对其进行分类分级的类型化保护是维护数据安全，确保更好规制数据犯罪的重要内容。对于个人数据、商业数据及公共数据等重要数据和国家核心数据进行针对性的保护，使危害数据安全法益的行为得到合理的规制，促进数据犯罪刑事治理规范化。

## 参考文献

[1] 韩婧颖. 数据犯罪的司法困境及治理进路[C]//上海市法学会. 《上海法学研究》集刊 2022 年第 17 卷——长三角法治论坛文集. 北京: 北京师范大学刑事法律科学研究院, 2023: 8.

[2] 赵春玉. 大数据时代数据犯罪的法益保护: 技术悖论、功能回归与体系建构[J]. 法律科学(西北政法大学学报), 2023, 41(1): 95-107.

[3] 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.

[4] 苏青. 数据犯罪的规制困境及其对策完善——基于非法获取计算机信息系统数据罪的展开[J]. 法学, 2022, 488(7): 72-83.

[5] 王惠敏. 我国数据犯罪治理的困境与出路[J]. 北方法学, 2023, 17(1): 122-132.

[6] 皮勇. 论欧洲刑事法一体化背景下的德国网络犯罪立法[J]. 中外法学, 2011, 23(5): 1038-1060.

[7] 童德华, 王一冰. 数据犯罪的保护法益新论——“数据内容的保密性和效用性”的证成与展开[J]. 大连理工大学学报(社会科学版), 2023, 44(3): 54-64.

[8] 杨志琼. 我国数据犯罪的司法困境与出路: 以数据安全法益为中心[J]. 环球法律评论, 2019, 41(6): 151-171.

[9] 张明楷. 具体犯罪保护法益的确定标准[J]. 法学, 2023, 505(12): 70-86.

[10] 阎二鹏. “数据安全法益”命题下虚拟财产犯罪的归责路径重构[J]. 政治与法律, 2022(12): 45-59.

[11] 刘双阳. 数据法益的类型化及其刑法保护体系建构[J]. 中国刑事法杂志, 2022(6): 37-52.

[12] 叶涛. 论警务数据安全[J]. 中国人民公安大学学报(社会科学版), 2022, 38(4): 139-147.

[13] 张勇. 数据安全分类分级的刑法保护[J]. 法治研究, 2021, 135(3): 17-27.

[14] 王华伟. 数据刑法保护的比较考察与体系建构[J]. 比较法研究, 2021(5): 135-151.

[15] 于润芝. 非法获取个人数据犯罪的法益分析及处罚限定[J]. 大连理工大学学报(社会科学版), 2023, 44(2): 56-64.

[16] 刘宪权. 数据犯罪刑法规制完善研究[J]. 中国刑事法杂志, 2022, 5(5): 20-35.