

# 数据开放与隐私保护的平衡研究

吕本富 卢超男

(中国科学院大学经济与管理学院, 北京 100190)

**摘要:**[目的/意义]数字经济时代,数据开放成为必然趋势,而数据安全和隐私保护问题是数据开放过程中不可避免的,探讨如何实现数据开放与隐私保护之间的平衡具有重要意义。[方法/过程]本文认为解决数据开放与隐私保护平衡问题的核心是明确数据的产权归属和规范数据开放流程。本文首先从经济学的效率和公平角度出发,以平台企业与用户之间的数据产权划分问题为例,采用成本效益分析法剖析数据产权问题,随后从数据主体层面讨论了如何规范数据开放流程。[结果/结论]提出了数据产权界定应该遵循效率与公平的平衡原则,分离产权中的所有权、使用权、收益权;为实现数据开放过程的规范化,应该积极完善法律法规及相关政策,实现数据分级分类管理,鼓励发展第三方数据安全服务产业。

**关键词:**数据开放 隐私保护 数据治理 数据产权

**分类号:**F49; F273.1; D913

**DOI:** 10.31193/SSAP.J.ISSN.2096-6695.2020.03.02

## 0 引言

近年来,大数据技术、人工智能、物联网、区块链等信息技术不断取得突破,数字经济成为经济高质量发展的重要抓手,而数据作为发展数字经济的底层支撑,其重要性日益凸显。2020年4月,中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》,将数据作为与土地、劳动力、资本、技术并列的生产要素,提出要“加快培育数据要素市场”“促进要素自主有序流动”。数据要素兼具价值和使用价值双重属性,对价值创造和生产力发展具有重大影响,而最大程度的挖掘和释放数据价值的根本在于数据开放,促进数据自由安全的流动,避免成为一滩“死水”,正如凯文·凯利在《必然》中所阐述的“数据并非用来收藏和存储,它们需要的是流动,与其他数据相连接,数据处于流动状态,才能发挥出更为强大的作用”<sup>[1]</sup>。

**[作者简介]**吕本富,男,博士生导师,教授,博士,研究方向为网络经济和网络空间战略、管理智慧等,Email: lubf@ucas.ac.cn; 卢超男(ORCID: 0000-0001-6846-394X),女,博士研究生,研究方向为平台经济,Email: luchaonan17@mails.ucas.ac.cn。

平台经济背景下,数据开放一直是业界和学界所共同期待的。通常认为,数据开放可以有效减少市场摩擦,促进交易,提升市场效率,降低搜索匹配成本,用户在享受个性化服务的同时,也可以享受基于他人开放数据的溢出效应(从别人披露的信息中获益,比如评论排名)<sup>[2]</sup>。但是,由于数据同时具有一定的私密性和潜在经济价值,数据安全和隐私保护成为了数据开放过程中不可避免的问题。人们在网络上的一言一行都会留有痕迹,各大互联网平台可能比你自已还了解自己,淘宝了解我们的购物习惯,腾讯熟悉我们的社会关系网络,百度、谷歌等知道我们的检索习惯,滴滴记录我们的出行规律……即使是被认为无害的数据,一旦被大量收集和不当使用,也会造成隐私泄露,引发一系列问题,不仅影响个体用户的正常生活,也对企业的数字资产造成侵害,破坏行业竞争。例如,近年来国内的电商平台、门户网站、互联网金融平台频繁爆出非法收集窃取用户数据、大数据杀熟、数据泄露、个人信息明码标价、公开买卖等。

美国学者 Charles Fried 认为没有隐私权,人就失去了成其为人的重要要素<sup>[3]</sup>。Goldfarb 和 Tucker 通过不愿在线营销研究调查中披露收入来衡量用户的隐私偏好,数据显示随着时间的流逝,用户对隐私的关注日益增加<sup>[4]</sup>。然而对数据要素的过度保护会抑制数据红利的充分释放,如何实现数据开放与隐私保护的平衡,是数字经济时代公共监管所必须面对的巨大挑战。现今全世界普遍采用的是基于严格的“告知—许可—例外”的隐私保护模式,其效果并不是很好。

本文认为,解决数据开放与隐私保护平衡问题的核心是明确数据的产权(所有权、使用权、收益权)和规范数据开放流程。首先,数据交易已经成为近几年来数据开放最常见的方式。目前,国内已经出现了多种数据交易形式,包括由政府指导建立的大数据交易所,如贵阳大数据交易所、东湖大数据交易所等;针对具体行业提供大数据服务的行业性数据交易平台,如中科院和华视互联成立的交通大数据交易平台;专门的数据服务商,比如数据堂,通过对大数据进行采集、挖掘、生产、加工、销售,形成产销一体化的运营。数据交易的本质是将数据作为一种资产在市场上进行流通,而产权明确是任何一个资产交易所必须具备的基础性条件。只有在数据交易之前就明确数据产权归属,才能确定数据流通过程中的权责关系,保证数据安全交易,从源头上减少或规避数据滥用、隐私数据泄露等问题的发生。

其次,在数据产权明晰,权责分配明确之后,需要进一步规范数据开放流程,以确保数据流通过程中的安全。数据开放过程中涉及个人的行为以及互动相关的隐私数据,规范数据开放流程有利于减少数据开放过程中产生的负外部性问题,实现数据开放和隐私保护的平衡。

因此,本文将从明确数据的产权和规范数据开放流程这两个方面展开具体论述。

## 1 数据产权界定

产权(Property Right)指的是“一种通过社会执行而实现的对某种财产的多种用途进行选择的权利”。<sup>[5]</sup>产权不等同于所有权,是一组相对的权利束,包含使用权、处置权、支配权等一组权利,这些权利可能属于同一个主体,也可以分属于不同的主体。合理的产权安排可以起到激励作用,优化资源配置<sup>[6]</sup>。

数据具有很多与实体物品不同的属性:复杂性,由多主体产生,经过多轮处理才能形成有

价值的数 据; 不确定性, 数据的价值很难被标准量化; 可复制性, 数据方便复制, 可以同时存在不同介质中; 特殊的稀缺性, 数据存在无形性, 且理论上可无限复制, 并且复制品与“原物”的价值等同, 数据的稀缺性不同于传统意义的资源稀缺性, 往往体现在获取及控制使用上, 而不是数据本身具有很高的直接价值, 单个数据往往不具有直接的经济价值; 隐私性, 能够识别特定个人身份或特征的数据往往具有隐私性; 时效性, 通常情况下, 如果在一段时间内数据没有被很好的分析使用, 其价值就会随着时间推移而减少。因此, 数据产权的认定比实体产权认定和划分更加复杂, 现有的产权制度, 如物权、所有权、知识产权并不能很好的套用于数据产权问题。数据作为信息载体, 已成为一种战略性资源和重要的生产要素, 其所有权、使用权、收益权等的界定会对数据产权主体既可能包含个人用户、数据收集企业、平台企业, 也可能包含政府机构与数据中介等组织的福利乃至社会福利产生很大的影响。合理的数据产权安排是数据安全有序开放前提, 清晰的权责分配有助于数据在高效率流通的同时又能兼顾公平, 实现净价值最大化。本文将从经济学的效率和公平平衡角度, 采用成本效益分析法剖析数据产权界定问题。

### 1.1 效率角度

诺贝尔奖得主罗纳德·科斯 (Ronald Coase) 提出的科斯定理是分析产权问题的重要工具。科斯定理 (Coase theorem) 指出: 只要财产权是明确的, 并且交易成本为零或者很小, 那么, 无论在开始时将财产权赋予谁, 市场均衡的最终结果都是有效率的, 实现资源配置的帕累托最优<sup>[6]</sup>。科斯定理反映了一个很直观的逻辑, 在交易成本足够小的情况下, 只要产权还没有被配置给使用效率最高的人, 这个人就会不断地抬高出价, 最终结果是相应的产权一定会落到使用效率最高的人手里。但是, 现实社会中, 并不存在交易成本为零的情况。为了要实现效率目标, 初始产权就应该要直接分配给最能有效对其使用的一方。具体到数据产权问题, 由于不同人对数据价值的判定存在主观性, 数据流动过程也涉及大量成本, 因此, 交易成本不可能为零, 把最初的产权分配给数据使用效率最高的一方。问题就转变成了界定谁更能有效的使用好数据, 如何在不同的利益主体之间甄别出那个合适的人, 需要结合具体的情况做具体的分析。

以平台企业与用户之间的数据产权划分问题为例, 如果数据由用户个人所有, 那么单个用户的数据量小, 数据维度不多, 数据价值是微不足道的, 并不具备财产属性。但是, 如果平台上的用户在平台上产生的数据都归平台企业所有, 数据规模更大, 数据来源更广, 数据维度更多, 平台企业可以借助大数据分析方法和人工智能等技术来分析预测微观层面的消费者行为, 形成范围经济和规模经济效应<sup>[7]</sup>, 大大提升了数据价值和数据使用效率。但是, 数据产权划分给平台企业也存在一定的成本。一方面, 增加了平台企业侵犯用户隐私的可能性; 另一方面, 平台企业掌握大量用户数据后, 使得“第一类价格歧视”的实施成为了可能, 加剧了人们对数据垄断的忧虑<sup>[8]</sup>。然而, 事实表明, 平台企业拥有数据产权产生的风险其实并没有想象的那么大。Athey、Catalini 和 Tucker 在关于隐私悖论的研究中, 通过实验证明, 即使是对隐私表示出强烈偏好的用户, 也愿意为小额的奖励而放弃个人信息<sup>[9]</sup>。也就是说, 大数据时代, 人们通过隐私信息来换取更多便利的、个性化的服务, 产生社会福利, 净成本并不是很大。数据垄断具有两层意思: 一是指平台对于数据资源的垄断, 但是由于数据的可复制性、非竞争性<sup>[10]</sup>, 平台企业很难实现;

二是指平台企业依靠掌握的数据强化垄断行为,这类问题跟传统的垄断问题并无本质差别,不影响数据产权问题<sup>[5]</sup>。

综上所述可以得出,从效率角度综合比较成本效益,数据产权越向大体量级别的主体(政府、企业)集中,所产生的价值越大,效率也越高,让更能让数据产生价值的一方获得数据的产权是更为可取的。但是,科斯定理本身具有明显的局限性,对于是否达到帕累托最优状态存在很大争议,片面追求资源配置效率可能会导致类似企业过度追求商业利益而剥夺用户福利,进一步降低整体社会福利的问题。

### 1.2 公平角度

经济中的公平强调的是要素投入与要素收入相对称,它是在平等竞争的条件下通过等价交换来实现的。从公平角度出发,主要的衡量标准为相关主体所做的贡献,谁的投入越多,谁的贡献就越大,产权就归谁。具体到贡献的比较,不同主体在不同的立场上得出的结论可能完全不同。从数据生命周期角度分析,从数据的生产到数据收集再到数据使用,各个环节所对应的主体不同。

以个人产生数据、企业收集数据、平台建模分析处理数据过程为例,收集分析可能是同一个平台企业,也可能是不同的主体。原始数据来源于个人用户的行为,表面上个人是原始数据的生产者,但是单个用户的行为本身并不直接形成数据。因此,在无法律规定或合同特别约定的情况下,用户对于其提供给网络运营者的单个用户信息尚无独立的财产权或财产性权益可言。只有将这些行为中蕴含的信息以数据形式收集起来,并进行必要的加工,才会变成有价值的数,而这个过程是需要投入大量的资源和劳动。从成本收益角度,个人用户没有动力也无法承担数据收集、加工的成本,大多由平台企业集中完成。例如,淘宝上的商户并不会专门单独雇人记录每天的营收情况、消费者的访问情况等,而是由淘宝平台利用其技术优势,集中处理,利用规模效应,降低成本。在这种情况下,如果把数据的初始产权界定给个人,那么淘宝平台就失去了做数据收集和分析工作的积极性。

根据公平原则,在数据形成过程中对数据产权的认定上,个体用户和企业均有参与并付出努力,产权单纯划给某个主体都不合理。若是刻意追求公共利益,强调公平,虽然可能在一定程度上保护了数据隐私,但同时也限制了数据价值的挖掘,遏制了企业的创新能力,阻碍了新技术发展。因此,单从公平角度,无法通过直接量化每个主体的贡献来界定数据产权。

### 1.3 平衡效率与公平

在数据产权界定问题上,仅从效率角度或者仅从公平角度分析都是不合适的。若只考虑效率,将数据产权划分给平台企业,以实现资源配置效率最优,会导致侵犯隐私或数据滥用现象,打击个人产生数据的积极性,阻碍数据的可持续发展;反之,若只考虑公平,可能会使得数据价值开发不足,影响数据利用效率和社会福利。因此,最好的方式是实现效率与公平的平衡,坚持数据开放的主线,在最大限度提高数据利用效率的同时,也注重数据安全和隐私保护,兼顾公平原则,强调公共利益和商业利益相协调。

对此,关于数据产权分配,本文认为关键在于三权分离,即分离产权中的所有权、使用权、收益权。首先,个人是数据生产者,由个人行为产生的原始底层数据所有权归属个人;企业是数

据加工者, 经过平台匿名处理、脱敏建模的数据, 已经确认无法识别特定个人或用于精准用户画像的数据, 数据所有权属于企业。其次, 由平台收集、处理加工后的数据使用权归平台所有。这些数据虽然本质上是个人数据的集合体, 但收集、管理、存储所需成本都由收集一方付出, 因此, 为体现公平, 平台拥有者享有使用权。同时, 为保障个体作为数据生产者的权益, 应该对平台拥有者的使用权作出限制性规定, 比如禁止数据滥用、限制使用时限、用户享有知情权、访问权、使用权、被遗忘权、数据可携带权等处置权。关于收益权, 在整个数据产生、收集、分析、价值实现的过程中, 涉及的各方主体均应享有数据的收益权, 各个主体之间的收益分配可以根据收入产出比通过等价交换实现。值得关注的是, 企业与个体之间的交易, 由于数据体量较大、数据类型繁杂、涉及个体用户较多, 针对每个个体用户的数据定价是十分复杂低效的, 可以借鉴庇古税, 通过设计合理的税收制度, 由政府向使用数据获得收益的企业根据获得收益的多少, 征收一定比例的“数据税”, 再将收取的税收投入数字基础设施建设, 进一步提高数据安全技术, 通过间接转移支付让每个个体都能享受到收益, 进而提高社会整体福利。

## 2 规范数据开放流程

为了实现数据开放与隐私保护的平衡, 在数据产权明晰、权责分配明确之后, 还需要进一步规范含有隐私数据的数据开放使用流程。目前, 国内关于网络信息收集和使用的规则分散于《消费者权益保护法》《电信和互联网用户个人信息保护规定》《人口健康信息管理办法(试行)》《侵害消费者权益行为处罚办法》《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》等法律、法规、部门规章及规范性文件中。虽然, 个人信息保护问题已经引起政府相关部门的重视, 中华人民共和国第十三届全国人民代表大会第三次会议表决通过了《中华人民共和国民法典》, 并将于2021年1月1日起施行, 标志着个人信息保护立法的顶层设计基本完成。此外, 新版的《个人信息安全规范》草案稿已经完成, 于10月1日正式实施, 《数据安全法》也在制定中, 但至今仍未出台统一的标准规范。目前, 国内数据控制主体仍以政府、企业为主, 本文将从政府和互联网平台企业的角度讨论隐私数据规范使用问题。

### 2.1 注重个人信息数据收集的合法性

数据收集可以看作是一种价值交换行为, 比如去银行贷款, 主动提供个人资产信息, 以便获得贷款; 去医院看病, 主动交代个人健康数据, 以便对症下药, 本质上, 其实是一种个性化服务与敏感数据之间的平衡。换句话说, 脱离数据服务谈论敏感数据搜集问题是不切实际的, 收集的信息应该与所提供的服务相关, 具有一定的合法性、必要性。例如, 如果去餐馆吃饭被要求收集收入状况, 是没有任何意义的, 但是如果去买房, 了解收入状况等信息就是必要的。

在我国, 合法性基础主要是个人的同意, 通过点击“同意”按钮或实际使用服务, 用户的数据就可以被合法地搜集。然而, 大多时候用户在点击“同意”时并不明确哪些数据被收集以及数据收集的目的, 用户事实上无法真的基于理性选择——做出决定, 从而使点击“同意”流于形式。绝大部分用户并不在意自己的信息被记录、搜集和分析, 除非会带来人身伤害或经济损失;

他们也没有能力逐一核实自己的信息如何被使用,也就是说,徒有告知表象,却无告知之实。此外,遇到一些突发情况,例如此次突发疫情,在《通用数据保护条例》(General Data Protection Regulation,简称GDPR)框架下,对于基于疫情监测、防控、隔离等目的,互联网公司、电信运营商基于已掌握的个人信息为相关部门进行传染病防控提供数据支撑,不必拘泥于数据主体的同意要件,可援引第6条(d)“为保护数据主体或其他自然人重大利益”或第6条(e)“公共利益目的执行任务或数据控制者履行所赋予的公共职能所必要”作为数据处理的合法性基础<sup>[11]</sup>。而国内《网络安全法》并没有给出同意的例外情形,国家标准《个人信息安全规范》中关于同意的例外规定也存在欠缺。因此,政府层面应积极推动法律法规相关政策的完善,加速推进《数据安全法》《个人信息保护法》的制定,明确用户数据信息是用户个人资产,保障用户对数据信息使用的知情权、选择权,明确互联网企业保护用户数据信息安全的责任,对违规使用用户敏感数据信息的机构企业,应该给予严厉处罚。

## 2.2 建立数据分级分类制度

首先,厘清个人信息与隐私的定义。最新通过的《民法典》第一千零三十四条规定,“个人信息”是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息,包括姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等<sup>①</sup>。关于隐私的定义,不同文化或者个体对隐私有不同的理解,但是主体思想是一致的,即特定个人(或团体)不愿意暴露的,可用于确认其身份或特征的敏感信息。《民法典》中也清晰地界定了“隐私”是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息<sup>②</sup>,即个人信息中可能也含有不想为他人所知晓的私密信息。根据该定义,隐私数据是在任何情况下都不可以作为开放数据用来交易的。

其次,将个人信息相关数据进行分级管理,如一般数据、敏感数据等。通常情况下,敏感信息如医疗保健数据、金融数据等,应该给予重点保护,不可随意开放流动;而一般数据,在匿名处理之后可以开放交易。但是,对于个人信息数据的分级不是固定不变的,没有统一的标准,应该视场景而定,具体情况具体分析,即何种信息数据在何时落入敏感数据这个类别,是和场景密切相关的。例如在平常,可以将姓名、行程等归为一般个人信息,但是在当下新冠肺炎爆发,出现“武汉毒人”“要求湖北人公开全家信息”“超7000武汉公民信息泄露”事件,多地将湖北人默认为高危人群的情况下,部分湖北籍人民(及从湖北返乡人员)的这些信息数据,可以归为敏感数据予以保护。也就是说,若从数据控制者的角度出发,认为某部分数据“一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等”的,就应当自觉将这些信息数据“升格”为敏感数据予以更高级别的保护。

## 2.3 发展第三方数据安全服务产业

匿名化技术发展成为了现在数据挖掘中隐私保护的最主要的技术手段。GDPR中对于匿名化的定义是指将个人数据移除可识别个人信息部分,并且通过匿名化处理,可以避免数据主体被识别<sup>[11]</sup>。如果将可识别的个人数据通过匿名化技术处理,转变成不可识别的数据再进行数

据开放, 则可以实现数据开放与隐私保护之间的平衡。然而, 由谁来进行数据匿名化处理? 在传统的中心化模式下, 相比于企业, 个人用户处于技术不对等的弱势地位, 即使每次都以匿名身份使用企业提供的各项服务, 也无法避免在各种数据挖掘分析技术下成为一名“透明人”。而企业本身如果自主研发或引进匿名化处理技术, 又将是一笔不小的成本投入, 导致很多企业, 尤其是中小企业缺乏内在激励<sup>[12]</sup>。因此, 可以发展第三方数据安全服务产业, 在数据收集之初就将数据安全相关业务交由专业可信的第三方完成, 从源头切断个人隐私数据相关的风险。

规范的第三方数据安全服务产业还可以承担起数据开放安全标准制定、数据安全测评、帮助企业对数据进行分级分类、推进新型数据安全技术(如区块链技术)研发应用等重任, 由此构建数据治理生态, 提高数据开放的安全水平。首先, 人工智能时代充满了不确定性, 当下数据安全治理是充满未知的, 只能摸着石头过河, 不断试错不断调整。在这种情况下, 由政府主导的自上而下的治理模式是不够灵活的; 相反, 鼓励发展数据安全服务产业, 让专业的数据安全组织参与数据安全测评、帮助企业对数据进行分级分类、数据开放安全标准制定, 由实践出发的自下而上管理模式更适合快速变化的时代。其次, 《自然-通讯》杂志发表的一个研究表明, 目前所使用的匿名化技术和数据开放方法可能不足以保护个人隐私或满足数据保护法律法规(如欧盟的《通用数据保护条例》)的要求<sup>[13]</sup>, 因此, 仍需要进一步激发数据安全企业的创新能力, 推进新技术发展。

#### 【注释】

- ①参见《中华人民共和国民法典》第一千零三十四条。
- ②参见《中华人民共和国民法典》第一千零三十二条。

#### 【参考文献】

- [1][美]凯文·凯利著, 周峰, 董理, 金阳译. 必然[M]. 北京: 电子工业出版社, 2016.
- [2]ACQUISTI A, TAYLOR C R, WAGMAN L, et al. The Economics of Privacy [J]. Journal of Economic Literature, 2016, 54(2):442-492.
- [3]FRIED C, Privacy [J]. The Yale Law Journal, 1968, 77(3):475-493.
- [4]GOLDFARB A, TUCKER C E. Shifts in Privacy Concerns [J]. The American Economic Review, 2012, 102(3): 349-353.
- [5]费方域, 闫自信, 陈永伟, 杨汝岱, 丁文联, 黄晓锦. 数字经济时代数据性质、产权和竞争 [J]. 财经问题研究, 2018(02):3-21.
- [6]COASE R. H. The Problem of Social Cost [J]. Journal of Law & Economics, 1960, 3:1-44.
- [7]OECD. Data-Driven Innovation for Growth and Well-Being [R/OL]. (2015) [2020-09-01]. <http://dx.doi.org/10.1787/9789264229358-en>.
- [8]张亮亮, 陈志. 培育数据要素市场需加快健全数据产权制度体系 [J]. 科技中国, 2020(05):15-18.
- [9]ATHEY S, CATALINI C, TUCKER C. The digital privacy paradox: Small money, small costs, small talk [R/OL]. (2017-06) [2020-09-01]. <https://www.gsb.stanford.edu/faculty-research/working-papers/digital-privacy-paradox-small-money-small-costs-small-talk>.

- [ 10 ] JONES C, TONETTI C. Nonrivalry and the Economics of Data [ R/OL ]. (2019-08) [ 2020-09-01 ]. <https://www.gsb.stanford.edu/faculty-research/working-papers/nonrivalry-economics-data>.
- [ 11 ] 京东法律研究院. 欧盟数据宪章 [ M ]. 北京: 法律出版社, 2018.
- [ 12 ] 姚前. 数据隐私保护新思路: 从依赖他方到自主可控 [ J ]. 中国信息安全, 2019(01):104-107.
- [ 13 ] ROCHER L, HENDRICKX J M, DE MONTJOYE Y A. Estimating the success of re-identifications in incomplete datasets using generative models [ J ]. Nature communications, 2019, 10(1): 1-9.

## Research on the Balance between Data Opening and Privacy Protection

LV Benfu LU Chaonan

(School of Economics and Management,  
University of Chinese Academy of Sciences, Beijing 100190, China)

---

**Abstract:** [ **Purpose/significance** ] In the era of digital economy, data opening has become the trend, and data security and privacy protection are inevitable problems in the process of data opening. It is of great significance to discuss the balance between data opening and privacy protection. [ **Method/process** ] Clarifying the property rights of data and standardizing the data opening process are the cores of solving the balance between data opening and privacy protection. This article first analyzes the data property rights issue by using the cost-benefit analysis method from the perspective of economic efficiency and fairness, taking the division of data property rights between platform companies and users as an example. Then it discusses how to standardize the data opening process from the perspective of the data subject. [ **Result/conclusion** ] It is proposed that the distribution of data property rights should follow the balance principle of efficiency and fairness, and the ownerships, use rights and income rights in property rights should be separated; in order to standardize the data opening process, we should actively improve laws, regulations and related policies, implement data classification management and encourage the development of third-party data security service industries.

**Keywords:** Data opening; Privacy protection; Data governance; Data property right

---

( 本文责编: 孔青青 )