

数据的二元划分与体系保护

冯德淦

(南京大学法学院, 江苏南京, 210093)

摘要: 数据可以进行二元划分, 分别是代码符号层面的数据和语义信息层面的数据。代码符号层面的数据虽然客观存在, 与法律上的物有一定相似, 但是由于其缺乏竞争性, 同时权利轮廓也不明晰, 因而无法构造出“数据文件所有权”, 应当借助保护性规范对其进行保护, 具体又体现为保护数据的完整性和数据不被窃取。语义信息层面的数据, 在私法领域主要体现为对个人信息的保护, 构造个人信息绝对权对其进行保护的途径并不可行, 由于公法对个人信息保护的成熟性, 应当借此以保护性规范来保护。两个层面的数据都蕴含着财产利益, 最恰当的方式是利用合同制度实现保护。两个层面的数据均具有一定的公共属性, 私法对其保护时应当作出一些限制。

关键词: 数据保护; 代码符号; 语义信息; 个人信息; 保护性规范

中图分类号: D913

文献标识码: A

开放科学(资源服务)标识码(OSID)

文章编号: 1672-3104(2020)05-0070-12



一、问题的提出

21世纪是互联网和大数据的时代, 伴随着网络信息技术的不断发展, 数据每天被不停地产生、加工、存储、整合和使用。为了应对大数据时代的数据保护问题, 我国于2017年通过的《民法总则》第127条在一定程度上为数据的保护划定了轮廓。虽然该条并未对保护路径予以具体化, 但是却原则性地表明我国在私法领域需要对数据进行保护^①。从客观上讲, 我们已经看到数据对民事主体的意义, 其不仅体现在人身利益, 还关涉财产利益。至于如何对数据进行保护, 是通过赋予一项具体的权利, 还是借助保护性规范, 则是民法需要回应的问题。

自《民法总则》颁布实施以来, 私法领域开始对数据的保护予以关注, 其讨论主要集中在两个方面: 一个是数据到底指向什么, 为什么需要

予以保护; 另一个则是有无赋予数据权的必要性。这些讨论在我国数据领域形成了不同的观点, 对数据的定位以及保护路径作出了有益的探索。但是仍然存在两个问题: 一是在客体单一范畴下进行争论, 易导致体系性思维的缺失; 二是缺乏对其他相关制度的参照, 只是孤立地研究数据的保护。笔者将在探讨数据本质的基础上, 体系性地分析数据保护的必要性、可能路径, 以及相关必要的限制, 以求能对二元化的数据保护体系的构建有所裨益。

二、数据的二元化区分

(一) 数据的涵义

在当代信息化社会, 从价值的角度来看, 数据无疑对个体和社会都具有积极的意义。如果将数据定性为保护的客体, 那么必须对数据的内涵进行深入研究, 才能理清我们究竟要对数据保护

收稿日期: 2019-04-09; 修回日期: 2020-04-01

基金项目: 国家社会科学基金青年项目“风险社会视阈下人工智能产品责任研究”(18CFX046); 教育部国家建设高水平大学公派研究生项目(201806190060)

作者简介: 冯德淦, 江苏淮安人, 南京大学法学院民商法学博士研究生, 主研究方向: 民法学, 联系邮箱: deganfeng1990@163.com

到什么程度。对数据的讨论，必然涉及大数据。究竟什么是大数据？较为接受的观点是，大数据指那些规模宏大而且复杂，以至于很难用现有数据库管理工具或数据处理应用技术来处理的数据集。因而，大数据最起码有几个特点，即规模大、高速性以及多样性^[1]。大数据是诸多数据的集合。在大数据时代，特定主体的数据保护显得尤为重要，因为这些数据在我们看来是客观存在的。通常情况下，我们在讨论数据之时，所指向的是那些存储在服务器或者硬盘的符号和代码。然而，我们在讨论个人数据之时，往往不受客观存在的限制，具体地指代那些与个人有关的抽象信息，会不自觉地和个人信息，以及具有特定意蕴的某些内容结合在一起。由此来看，在该层含义上，数据又特指那些符号所承载的具体含义。为了有效地与智力成果相区分，还有一种更加狭窄的理解，认为数据仅仅是那些非智力创造层面的东西，由机器自主生成的特定的代码符号。因此，代码符号和语义信息最起码在逻辑上是可以区别对待的，它们之间有时存在必然联系，有时需要区分对待，有时又可以完全独立。

回归数据存在的具体情形。我们一般会在三个层面上观察数据，分别是数据载体、代码符号和语义信息^[2]。首先，从数据的载体来看，最容易理解的就是硬盘，或者由网络运营商所管理的服务器。这些载体是数据存在的具体技术设备，为数据的保存提供技术支撑。虽然我们未必总能知道这些存储设备的具体形状，但是无论是我们自己控制，还是被网络运营商控制，我们都确信，必然存在一个具体的有形设备，来作为数据的载体。需要注意的是，数据载体的权利归属和数据的归属未必总是属于同一人，尤其在网络数据激增的情形下，数据载体往往属于服务商，用户仅仅具有使用相关存储空间的权利。其次，从代码符号来看，数据可以定义为被机器可读的代码符号。从这个层面来说，数据往往被当做存在于存储设备上的代码符号。该种理解实际上表明数据本身并不直接指向信息，而需要通过编译的过程才可以转化为人们理解的内容。欧盟委员会选择了这样一种方式来理解数据，它明确表示“与这一范围无关，重要的是构建如下的(权利)框架，

以便只保护符号层面的信息，而不保护语义层面的信息”^[3]。最后，从数据所承载的语义信息来看，其是代码、符号，甚至是文字所揭示的可供人们理解的内容。有许多学者是从该层面理解数据的，并且强调数据和信息是不能割裂开来讨论的，认为数据之所以具有经济利益，正是因为其背后所承载的信息^[4]。

以此来看，我们对数据的理解最起码在两个层面进行。一种认为数据仅仅指代码符号。这是从一个十分宽泛的角度来理解数据，那些被生成、收集或者说被存储的代码符号均是数据，不管其是否与自然人相关，还是由机器生成，也不管其是否已经被破译，或者说被人们所理解。另一种则认为数据不应当与语义割裂开来。数据应当与信息结合在一起理解，单纯的不含信息的数据，仅仅是二进制代码的比特形式，对于收集使用的人们而言并无任何价值。上述对数据一元化的理解，都注意到了数据的某个方面的特征，却忽略了数据本身的二元性特质。存储设备是代码符号的载体，而代码符号则是具体信息的载体，如果所有的代码符号都可以直接转化为语义信息，那么确实没有必要在法律层面严格区分代码符号和语义信息。我们应当看到，虽然大部分代码符号可以直接被解读为语义信息，或者说仅仅机械化的解读就可以转化为语义信息，但是也存在一些数据并不能被直接转化为信息，却不能否定其价值。最为典型的的就是机动车驾驶的参数、天文测量的数值以及人类身体的指标等。这些数据并不能直接转化为信息，而需要通过人们的再加工，或者大数据的重新统合，才能产生具体化的信息。

既然无论是代码符号，还是语义信息，都对主体具有一定的价值，那么法律就需要对其归属和保护进行确认。如果我们仅仅将数据保护看作是对信息的保护，无疑会忽视对那些难以直接被认定为信息的代码符号的保护。如果我们单单认为数据就是代码符号，而不与其背后所揭示的或者可能揭示的信息联系在一起，又难以回答为什么需要保护数据。就此而言，代码符号和语义信息确实有很强的联系，但是两者之间又有不同的含义。这就相当于，一本写着汉字的书籍，有形

的载体是纸张,而代码符号则是纸张上的文字,语义信息则是懂汉语的读者的认知。如果主体精通汉语,代码符号和语义信息会直接产生联系,那么大家不会那么严格区分代码符号和语义信息。但是对一个不懂汉语的外国人而言,纸张仍然是有形的载体,纸张上的文字则仍然是代码符号,当然这并不能否定代码符号的潜在价值。可见,从对主体的价值角度来考量,数据的内涵确实可以分为代码符号和语义信息,两者对主体均有特定的价值。

(二) 代码符号和语义信息的二分

不可否认,任何一项权利都有可能兼具财产利益和人格利益,但是有可能主要表现为其中一种利益,民法将其归为特定的利益范畴。数据的二元化区分,恰恰也建构在财产利益和人格利益二分上^②。如上文所述,代码符号虽然部分可以直接转化为语义信息,但是终究需要予以转化,再加上有些代码符号不能直接转化为语义信息,需要借助其他技术手段,因此我们认为代码符号本身并不向我们展示任何语义信息。代码符号在民事主体的掌控范围内,蕴藏着主体对其的支配价值和交换价值,无疑是可以用来进行估价的,或者说它本身就是一项无形财产。语义信息则主要向人们展示内容,在实践中较为常见的是个人信息,包括个人隐私、消费记录等。从对民事主体的价值来看,其植根于人格权,是民事主体对于自己所创造信息的控制,以及对涉及自身信息的保有。虽然在特定的语境之下,个人信息也具有一定的财产价值,但是其仍然是一种抽象性的存在,往往只是借助于合同来实现交换价值,难以直接向不特定的主体展现其价值所在。我国《民法总则》也对两者予以区分,其中第127条规定:“法律对数据、网络虚拟财产的保护有规定的,依照其规定。”将数据与网络虚拟财产放置在一起,网络虚拟财产已经清楚地表明是保护财产利益,那么数据在该条中所强调的也应当是其蕴含的财产利益^[5]。与之相对应,《民法总则》对个人信息的保护也予以了规定,其中第111条前段强调,自然人的个人信息受法律保护,后段则进一步表明了个人信息的专有性。理论上认为,该条主要是为了维护自然人的信息自主权,

是保障人格利益的条款。

我国《物权法》第2条规定:“本法所称物,包括不动产和动产。法律规定权利作为物权客体的,依照其规定。”代码符号层面的数据实际上与传统的有体物并无本质差异,都是客观存在的,并且能够被人们感知或揭示。其与传统有体物最大的区别在于,一般情况下有体物可以被他人从外部感知,并且具有确定的形状,诸如动产和不动产都有这种特点。而代码符号层面的数据,本身也是客观存在的,能够被人们通过相关载体予以感知,却无法予以触摸或者具体地被认识。在某些特征上,代码符号层面的数据似乎与电、能量类似,然而更加抽象,在某些方面偏离了传统物的范畴。不可否认的是,其确实存在于某些载体之上,并且为特定的主体所拥有。语义信息层面的数据,则与代码符号是相对分离的,是代码符号所指向的内容。语义信息本身并不是客观存在的物,具有一定的抽象性,也不寄存于任何有形载体之上,仅仅是借助于代码符号来揭示内容,一旦为他人所知悉,某种意义上就脱离了代码符号而单独存在。该种知悉本身并没有对代码符号造成损害,也没有阻隔信息主体对信息的知悉和使用,但是却违背了信息主体的意愿,或者说侵犯了信息主体的信息自主权。从上述分析来看,代码符号层面的数据很接近民法上传统的物,而个人信息层面的数据则偏向体现为人格权。

就逻辑关系而言,两者实际上是不同层面的客体。从对两者的保护来看,主要存在如下几种情形:在有的案件中仅仅是代码符号受到侵害,最为典型的是侵权主体并没有关注信息内容,只是删除了存储设备中的代码数据;在有的案件中仅仅是语义层面的信息受到侵害,最为典型的是侵入他人的电脑,窥探他人个人信息,但是没有复制、删除或破坏任何代码符号;在有的案件中代码符号和语义信息都受到了侵害,最为典型的是侵权主体侵入他人存储设备进行删改和传播。就具体的立法文件而言,对上述两个层面的数据都有保护,同时在语词上也没有太大的区分。如2000年的《欧盟基本权利宪章》第8条强调对个人数据的保护,该种个人数据指向的是个人信

息。再比如 2018 年 5 月 25 日通过的《欧盟通用数据保护条例》(GDPR)，也主要是为了更好地保护个人信息。我国理论界和实务界一直在呼唤，但仍然未制定的“个人信息保护法”某种意义上也是针对个人信息的。可见，大部分数据保护法是为了保护个人信息不受侵害。到目前为止，只有在刑法中，特别是以《德国刑法典》第 303a 条为代表，确立了针对代码符号层面数据保护的规定^[3]。从我国《民法总则》对个人信息和数据区分立法的路径来看，我国立法者似乎也是有意区分代码符号层面的数据与语义信息层面的数据而对它们分别进行保护。此种区分符合事物的客观规律。

三、作为符号层面数据的保护

(一) 符号层面数据保护的必要性

在现代社会，人们每天接触的事物纷繁复杂，单凭个体的能力无法将所有的信息完好记忆，我们需要借助于纸质或者电子设备进行存储。除此之外，许多呈现给我们的视频、音频，以及相关文本，自然人凭借个人能力来记忆存储存在巨大的困难，同样需要借助电子设备进行保存。正如上文所述，虽然代码符号需要借助某种物理载体进行存储，但是代码符号与传统物权法上的物仍然存在区别，因而在保护的必要性上也可能存在差异。在计算机硬盘或者网络运营商的存储设备中，代码符号往往是以二进制比特的形式，借助电磁方式存在，单纯依靠人类肉眼并不能识别，这与传统的电、气、热具有相似性。不过，代码符号层面的数据与传统的电、气、热仍然存在差异，主要表现在电、气、热具有经济学上的竞争性特征，并不能被多个主体无害他人地同时使用，代码符号层面的数据却可以被不同的主体同时享有，在使用上并不会相互影响。最为典型的例子就是对一些视频、音频的复制，该种复制不仅成本低，而且可以无限被复制^[2]。即便如此，考虑到符号层面的数据对于民事主体具有重大意义，其本身对于生产生活以及社会加工具有重要价值，法律不能忽视对该层面的数据利益的保护，但是在保护的方式上应当考虑其特

殊性。

符号层面数据保护的内容主要体现在两个方面：一方面是对数据完整性的保护，另一方面则是保护数据不被窃取。学术界就侵害数据完整性的保护并无太大争论，因为一旦破坏了数据完整性，原来的数据享有人就不能再对数据进行使用。这就相当于对其“特殊财产”实施了加害行为，数据主体的相关利益也就受到侵害，侵权法当然需要对此予以保护。而就数据的窃取而言，则会存在一定争论。由于代码符号层面的数据并不具有传统物权法上物所具有的竞争性，其他民事主体即使对其实施了复制行为，只要不是删除行为，原则上并不会侵害数据原享有者的利益，仅扩大了数据使用主体的范围。从这个角度来看，窃取行为似乎并没有给数据主体造成损害。值得注意的是，虽然代码符号层面的数据没有达到知识产权保护的程度，但是其本身渗入了行为人的智力和体力劳动，或者说是由行为人特定行为而生产的，我们应当保护其独占使用的权利，避免让他人未付出任何对价就可以使用^[3]。因而，代码符号层面的数据虽然不具有经济上的竞争性，但是出于对特定主体智力成果的保护，我们应当赋予特定主体独占使用的地位，他人在未得到允许之时，不能对其进行使用。

(二) 保护的可能性路径之检讨

对代码符号层面数据的保护，比较法上有三种方式：借助载体的所有权进行保护，创设特定的数据权利进行保护，通过保护性规范进行保护。首先，借助载体的所有权来保护。这是许多国家采纳的模式。德国判例法针对破坏数据完整性和独占性的行为，主要是以数据载体为出发点，而不是针对数据本身创设权利来单独保护^⑧。按照这种观点，代码符号一般都要存储在载体上，任何窃取和破坏行为都是通过对载体所有权的侵害来完成的。这是通过迂回的方法，在不对传统侵权法保护客体进行突破的前提下，完成了对代码符号层面数据完整性和独占性使用的保护。其次，创设特定数据权利进行保护。该途径无论是在比较法上还是在我国都非常有市场。德国学者对于创设权利一直秉持特别谨慎的态度，有学者认为代码符号层面的数据与传统的物在

形式上虽然存在差异,但是本质上仍然具有物的某些特征,可以赋予该层面数据以权利,直接纳入侵权法中保护,无需采取迂回路径进行救济^④。最后,采取保护性规范进行保护。伴随着数据保护的发展,人们已经认识到数据和载体并不是一回事,然而将数据直接上升为一项独立的权利则存在法教义学上的困难。尤其是以德国侵权法为代表的权利、利益区分保护模式,在权利的轮廓还未明晰之前,原则上不会直接赋予一项新兴的利益以权利地位来进行保护,往往采取单独设定保护性规范的模式来保护^⑥。

上述三种方式,存在较大问题的是第一种方式。早期在云存储还没有得到运用之时,作为代码符号的数据一般会存储在固态硬盘或者其他实体存储设备中,相关存储设备往往与数据属于同一主体所有。此时,如果加害人破坏了数据的完整性,或者说窃取了数据,都可以认为侵害了所有人的数据载体所有权,因而可以借助载体的所有权进行扩张保护。随着科学技术的不断发展,尤其是网络云存储技术的发展,网络用户一般会将数据存储于云端,此时虽然存在有形的存储器,但是云存储器主体和具体的网络用户并非为同一主体。网络用户的数据被侵害或者被窃取时,他们对存储器并不享有所有权,因而无法通过诉诸数据载体的所有权来保护自己在代码符号层面的数据利益。

第二种方式和第三种方式在我国不乏支持者。如针对权利的保护模式,我国有学者认为,应当对代码符号层面的数据赋予“数据文件所有权”,并且强调此处的“所有权”并非传统物权法意义上的所有权。虽然数据并非有体物,但是它与有体物在权利的内容和规范意义上具有极大的相似性,因而可以赋予其“数据文件所有权”^[2]。再如针对保护性规范的保护方式,我国有学者认为,并非所有的利益保护都需要上升到与生命权、健康权和所有权这些绝对权的高度,数据利益的保护也还不能上升到法定财产权保护的高度。持该观点的学者还认为,采取绝对权保护的模 式可能面临如下困境:数据利益竞争性的缺失、权利主体确定的困难和立法成本过高的障碍。为了缓解上述权利保护的困境,学者主张

应当以刑法规范和网络安全规范作为保护性规范,构建违反保护性规范的侵权保护方式,这样既能达到对数据利益的保护,同时也避免了泛权利化^[5]。

客观地说,在云存储时代,第一种方式借助于载体来保护符号层面的数据,由于载体所有人和数据利益享有者二分,确实已经不能适用数据利益保护的发展,因而我国法律应当予以摒弃。就第二种方式和第三种方式而言,一种采取创设权利的方式来保护,另一种借助保护性规范来保护,尽管在整合进路上存在差异,但是二者在具体问题的处理上具有相似性。到底哪一条路径更加适合我国,则需要结合现有条文规范具体考察。我国《侵权责任法》第2条规定,侵权法救济的客体不仅包括权利,相关利益同样也在侵权法的保护范围之中,因而,从立法文义层面来看,我国侵权法并没有采纳严格区分权利和利益的保护模式。从侵权法的规定来看,我国完全可以赋予一项数据权来对符号层面的数据利益进行保护。针对符号层面的数据利益,我国确实有学者主张赋予一项特殊的所有权,而不是单纯地构建数据权。既然涉及所有权构建,不能忽视我国《物权法》的相关规定,根据其第2条规定,物权的客体严格限定为动产和不动产,如果要对物权的客体予以拓宽,则需要借助于其他法律规定。因此,在缺少法律规定的情况下,我们没有办法直接构造出所谓的“数据文件所有权”。或者说,即便构造出一项权利,权利的归属和定位可能会引发长久的争论。首先,随着科学技术的发展,数据通常涉及多个数据主体,例如在医患关系中就是这种情况。其次,个人数据也可能与其他人的数据权利相冲突,例如消费者在使用汽车制造商固有的数据自动驾驶产生新的数据,谁是“数据生产者”?最后,当复制数据之时,会出现另一种形式的多重权利。无论复制是否合法,它都会对归属问题产生影响,谁是复制数据项的所有者?如果此时还涉及民法中的加工,那么数据归属于复制者还是原所有权人?^[7]这些问题没有彻底解决,就贸然赋予数据所有权反而会带来其他问题,确实需要谨慎处理。当然,像有些学者所论证的那样,创造一项新的所有权,主

要是利于数据交易。这是站不住脚的。因为即便没有新的所有权，现代民法中的交易模式同样可以为数据的财产交易提供一定保障^⑤。

与权利保护路径的困境相反，数据的保护性规范在我国一直存在于实证法中。针对多个主体的问题，由于保护性规范将个人数据定性为一项利益，主体上并不具有排他性，多个主体可以就个人数据享有不同层面的利益，相互协作共同实现彼此的目的。从保护性规范的具体归属来看，大致可以分为两种，分别是刑法规范和网络安全法规范。就刑法规范而言，我国与许多国家一致，针对网络数据的保护设置了特别条文，其中《刑法》第 286 条分 3 款分别对“破坏计算机信息系统功能”“破坏计算机信息系统中存储、处理或者传输的数据和应用程序”“故意制作、传播计算机病毒等破坏性程序从而影响计算机系统正常运行”等三种不法行为进行了规制。在具体操作上，我们可以借鉴《德国刑法典》第 303a 条在民事领域的适用方法，纳入侵权法的保护范围。不过遗憾的是，与《德国刑法典》第 303a 条一样，出于刑法保护主观条件的严格性，我国《刑法》第 286 条就主观要件被限定为故意。这在一定程度上压缩了民事领域对数据的保护范围，因而需要进一步借助其他条文规范。而网络安全法规范，可以对刑法规范做补充，我国于 2016 年制定的《网络安全法》并没有将主观要件严格限定为故意，其第 10 条和第 21 条针对建设、运营网络或者通过网络提供服务的人进行了确定，阐明了其在提供网络服务之时的义务。同时，该法第 27 条还对网络使用者的义务进行了确定，虽然仅规定“不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据”，但是在解释论上可以对侵入他人网络、干扰他人网络正常功能做扩张性解释，将破坏数据的完整性也纳入其中进行保护。因而，在我国侵权法中通过借助保护性规范，将破坏数据完整性和窃取数据的行为纳入规制范围内，可以达到对代码符号层面的数据妥善保护的目。

（三）符号层面数据保护的限制

符号层面数据保护在一定程度上与知识产权保护相类似，对该层面的数据利益的保护应当

设定例外和限制规定。例外和限制主要体现在为了产品的安全改进、有利于公共利益和为了科学研究等。这对于公共部门职能发挥和技术进步都有积极的意义。

第一种情况是为了产品的安全改进而限制数据利益。消费者购买了产品，在使用产品过程中所产生的数据应当属于消费者所有，如果生产者需要使用这些数据来履行监管市场上产品的义务，此时对消费者数据利益的限制就具有正当性。需要谨慎的是，该种限制仅在为了产品的安全保障而使用该数据时才有意义，如果是为了提高产品的性能，与安全性无关，而对消费者数据权益进行限制，就没有合理性可言。关于一般性的提高产品性能的使用数据，并不是为改进产品的安全保障，这应当是一个开放性竞争的问题。市场上所有同类产品的生产者都应该被同等对待，他们都可以基于对价取得用户的使用数据，使用者也可以基于对价的考量，将数据出售给可以充分利用数据的人^[3]。

第二种情况是为了公共利益而限制数据利益。比较容易理解的是，政府的某些部门为了特定的公共利益而使用个人数据，特别是那些用于统计的和公共目的的数据，诸如统计资料、城市规划、环境保护和民用基础设施建设等，在这些方面有必要对数据权益做一定的限制^[3]。较为复杂的情形是，在不特定的第三方需要使用数据之时，到底有无限制数据的必要^⑥。不特定的第三方主体需要使用数据与为了公共利益使用数据存在一定差别，不特定的第三方需要数据有时仅表明数据具有很强的价值性，并不能表明这种需求是基于公共利益而产生。实践中，我们一方面要保护不特定第三人使用数据的权利，另一方面还要保护数据主体的经济利益。为了达到上述目的，我们应当借鉴《著作权法》上的合理使用制度，在第三方和数据利益享有人之间寻找平衡，通过对价制度来构建数据使用许可制度。

第三种情况是为了科学研究而限制数据利益。正如我国《著作权法》的限制一样，为了科学研究，可以限制数据享有者对数据的独占利益。需要深入研究的是，科学研究对数据所采取的限制，是否仅被限定在非营利性科学研究中，

还是说可以扩展适用于带有商业目的的使用。从对数据享有者利益保护的角度来看,我们对这种扩充应当持谨慎态度。对数据利益限制的不断扩充会导致数据利益保护的机制失效,因为每一项对数据的使用,都有可能被看作是对数据的分析研究活动,这种扩充实际上消解了数据享有者的利益。所以说,如果是带有商业性质的抽象科学研究,原则上研究者不能直接使用他人的数据,而需要付出对价予以协商。

另外,在哪些情况下可以引入法定许可制度。就比较法上有益的探讨而言,主要集中在社会教育和个人学习等方面。德国就有学者认为,为了防止数据的使用受到阻碍,可以设想对某些数据分析实行法定许可制度。这种法定许可制度,可以对那些在公共福利方面不那么突出的,而又有使用数据的必要情形,起到补充作用。在我国《著作权法》和《专利法》中都有类似的规定,可以帮助我们在数据享有者和数据需求者之间寻找平衡,既保障了享有人的数据利益,同时也给有使用需求的人提供了获得数据的途径^⑦。

四、作为信息层面数据的保护

(一) 信息层面数据保护的必要性

信息层面数据的保护,即对个人信息的保护。该种数据信息的保护起源于对人格尊严和人格自由的重视。由于历史传统等原因,早期欧美国家认为,对自然人个人信息的保护,目的是为了保护隐私权等基本人权,关系到人的尊严和人格的自由发展^[4]。在很长一段时间内,美国是借助隐私权对个人信息进行保护的,只有在加害人公开披露了自然人不愿意公布的令人难堪的私密信息之时,受害人才能受到侵权法的保护。我国有学者持同样的观点^⑧。隐私权的客体范围有严格限定,并非所有的个人信息都可以被认定为隐私。此外,隐私权的保护内容一般局限为私生活安宁、个人私密不被公开、个人私生活自主决定等。个人信息的保护则更加强调自主决定和支配。从结论上看,两者确实存在交叉,但是现有隐私权的理论无法构建对个人信息的全面保护。正是出于上述考量,德国法采取了不同的做法。

德国学者认为个人信息的保护应当从一般人格权出发,定性为个人信息自主权。个人信息自主权和隐私权属于并列概念,都是从司法裁判中逐步发展出来的^⑨。虽然美国法和德国法的定位存在差异,但是基本思想都是借助侵权法来对个人数据进行保护。随着社会的不断发展,有学者开始认为,应当摒弃传统的隐私权和人格权保护路径,不应当仅借助侵权法保护个人数据,还应当将个人数据认定为财产权,通过财产规则来保护^[8]。持上述观点的学者认为,通过责任法来保护个人数据,实际上是让侵权人先获得数据信息,然后再基于侵权法对受害人进行赔偿。通过侵权法保护个人数据,很难通过意思自治实现个人数据的财产价值。而将个人信息直接认定为一项财产,信息主体和使用人的价格协商程序前置,通过双方之间的协商进行个人数据交易,更有利于实现个人数据的财产价值^[9]。持个人数据财产属性观点的学者实际上并不否认个人数据的人格属性,他们只是想强调个人数据不仅具有人格属性,还具有很强的财产属性,并且想以财产属性作为核心内容构造个人数据保护屏障。

需要注意的是,信息层面的数据与网络虚拟财产存在一定差异,法律在信息层面所保护的个人信息,不能简单将之定位为民事主体的经济利益。信息层面的个人信息虽然具有财产价值,但是其本身并不是我国《物权法》上所规定的物,甚至不像代码符号那样能够被间接感知,它的客观价值具有不确定性。从这个角度来看,信息层面个人信息人格利益的保护,相较于财产利益的保护具有更加深远的意义,财产利益往往也蕴含在人格利益之中。此外,个人信息的财产利益并非一定通过财产权模式来实现,还可以借助其他方式实现。我国学者也认为,信息层面的个人信息实际上反映的是民事主体对于个人数据的自主决定的利益^[10]。学者们进一步认为,该种利益主要表现在三个层面:一是有知悉自己的个人数据被他人收集、被他人使用和用于何种事项之上,有同意被他人使用的权利;二是知悉自己个人数据被转让,有同意和拒绝转让的权利;三是有权查询自己的个人数据,并且对缺漏和遗失的个人数据有权要求更改^[4]。

信息层面的个人数据实际上体现了个人在社会生活中的自主利益。如果一国法律不对该种利益予以保护，无论在公共生活领域还是在私人生活领域，个人自主决定的空间将会被消解。法律将无法为个人针对他人非法收集、使用以及转让数据的行为，构建保护屏障，此时民事主体的人格利益和财产利益将会受到双重侵害。为了避免上述窘境，对个人数据进行专有保护一直是德国等欧洲国家个人数据保护法的出发点。个人数据信息不被视为公共财产，相反，数据主体可以决定是否、由谁、以何种目的、何时以及在多大程度上处理这些数据^[11]。德国联邦宪法法院在著名的“人口普查案”中认为，所有的个人信息都应该受到保护，个人对自己的数据拥有决定的权利。因此，至少在人们接受个人信息自主利益的前提下，对个人数据进行保护的结论是没有问题的。我国宪法虽然没有直接阐明对个人数据信息进行保护，但是对私人生活领域以及通信自由等予以确认保护，足以体现对个人数据信息的保护意图。从保护民事主体人格尊严和人格自由的角度出发，我们有必要保护信息层面的个人数据。从具体的保护范围来看，信息层面个人数据保护与隐私保护有一定的类似，但是又有超越隐私权的趋势，其保护的不仅是隐私权所限定的客体，对于一切涉及个人的数据信息均应当予以保护。这也是公法和私法对自然人的最基本保障。

（二）保护的可能性路径之检讨

对信息层面数据的保护，现有理论通过三种方式进行：第一种方式是确立一项个人信息权，且认为该项权利是一项绝对权，以此来全面保护个人信息；第二种方式是认为应当确立一项个人信息权，但是该项权利并非绝对权，仅是一项防御性权利；第三种方式则认为个人信息的保护，不应当创设个人信息权，仅应当通过保护性规范进行。

首先，就将个人信息认定为绝对权而言。这是为了对个人信息的人格利益和财产利益进行双层保护，尤其是针对财产利益。将个人信息认定为绝对权，无疑对于构建交易，或者说为双方当事人之间的协商转让提供了方便。其次，就将

个人信息认定为权利，且仅定位为一项防御性权利而言。这种做法是想在个人信息保护和相关信息的流动之间寻找平衡。在我国《民法总则》第六章“民事权利”中，第110条列举规定了自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等绝对权，又在第111条规定了自然人的个人信息受到法律保护，从立法模式的选择上有意将个人信息与其他绝对权分开规定。考虑到立法者是将个人信息保护条款规定在“民事权利”一章中，因此可以认为自然人对个人信息享有个人信息权，不过该种权利并非是绝对权，仅仅是防御性权利。最后，就采取保护性规范的模式而言。虽然我国侵权法并未像德国法那样区分权利和利益分别保护，但是在司法实践中，为了防止侵权法的扩张，还是遵循了上述区分保护的做法。从侵权法保护的路径来看，一般认为只要侵害了绝对权，当然地满足违法性要件，而针对不是绝对权的利益保护，原则上则需要借助背俗侵权和违反保护性规范进行救济。虽然我国将个人信息的保护规定在《民法总则》“民事权利”中，但是它并非传统的绝对权，而需要借助保护性规范来保护。

比较来看，第一条路径与第二、第三条路径有本质区别，前者借助绝对权对个人信息进行保护，后两条路径虽然在具体展开上存在差异，但是都否定了个人信息是绝对权，因而在实施上都需要借助保护性规范展开。第一条路径将信息层面的数据认定为个人信息权。这种观点实际上是赋予信息客体的地位，并且将个人信息权塑造成具有确定边界和排他效力的绝对权^[12]。该种观点在一定程度上反映了我国侵权法不区分权利和利益保护，导致司法实践中权利泛化的倾向。有学者认为，赋予个人信息权，可以鼓励个人不断地披露自己的相关信息，尤其在具有财产属性之时，因为有权利的保护，个人更加愿意披露信息，也提升了数据的价值。这种观点其实并不正确，值得进一步反思。首先，即便不赋予个人信息以权利的外衣，通过合同的方式，也不会降低数据主体的议价能力，数据对主体的价值并不会因为

赋予权利而提升,也不会提升民事主体公开的积极性^[13]。个人信息并不完全符合物权客体的要求,主要表现在其不具备唯一性、特定性和公示性等客体所应当具备的特征。其次,个人信息所蕴藏的财产价值也并非要通过构建绝对权的形式来实现,现有合同法框架下的合同关系完全可以实现个人信息的经济价值,并且解释论上也无任何障碍。最后,个人信息绝对权会导致在个案裁判中权衡个人信息保护和其他价值的利益之时,不自觉地认为权利人拥有较高位阶的利益,除非基于公共利益,否则无法对个人信息进行合理使用。这会引发个人信息垄断的现象,反而不利于社会公共职能的发挥^⑥。

在路径的选择上,我们不仅需要从应然的角度去思考,还应当考虑个人信息的现有规范配置情况。众所周知,个人信息的保护并非肇始于私法领域,而是早期公法为了规制国家和他人侵犯个人信息所衍生出来的规制手段^[7]。就个人信息的保护而言,公法领域无论是宪法、刑法还是一些其他部门法,都为个人信息的保护奠定了基础,同时也确立了一些具体的行为规范。因而借助公法规范来实现私法的行为控制,似乎比贸然创造一个新的且轮廓不那么清晰的权利来得更加可靠。德国学者 Hellgardt 试图在行为控制论基础上,将公法规制理念引入私法,在他看来,规制是法律的功能之一,指的是以超越个案的控制目的,利用法律实现政治上的公共福祉^[14]。在该观点下,规制是一个超越部门法的大概念,各个部门法均具有规制的色彩,同时也可以相互之间进行协作。因而我们应当摒弃在私法中创设个人信息绝对权的做法,而在语词的选择上,是否称其为个人信息权,或者个人信息利益,这在我国泛权利化的语境下并无太大的差异。总之,实证法上对个人信息的保护,还是应当通过保护性规范来实现。可见,第二条路径和第三条路径并无本质区别,而后者将保护方法更好地揭示出来。

虽然我国《侵权责任法》一般条款并没有区分权利和利益保护,但是理论和司法实践中存在按照《德国民法典》第 823 条和第 826 条的一般条款操作的做法^[15]。区分权利和利益保护的方法

实际上是分三个层次构建侵权违法性:第一个层次,如果加害人侵害了绝对权,那么其行为当然具有违法性。第二个层次,如果加害人故意背俗加害他人,由于主观要件补充了客观权利保护的必要性,因此其行为当然也具有违法性。第三个层次,加害人虽然不具备上述两个层次的要件,但是法律规范为了保护特定的利益,单独对相关利益进行了规定。此时,如果加害人侵害了该项利益,不管故意还是过失,其行为也当然具有了违法性。我国《民法总则》第 109 条规定,自然人的人身自由、人格尊严受法律保护,该条为个人信息的保护奠定了基础。同时其第 111 条规定:“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的,应当依法取得并确保信息安全,不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息。”结合《网络安全法》等相关规定,我国实证法上已经构建对个人信息的保护性规范,只要在司法实践中操作得当,就能保护好个人信息。不过从发展的角度来看,保护性规范的设计较为粗糙,未来还有很多工作需要去做。现阶段亟需解决的问题是如何进一步完善我国的保护性规范,以此为信息保护提供良好的保障。需要强调的是,我们没有必要固守公私二分的传统观念,而应当积极促进公私法的协作,以更好地保护个人信息。

(三) 信息层面数据保护的限制

正如上文所阐释的,数据的外延和信息的外延虽然相关,但存在差异。数据包括个人数据和机器生成的数据,信息则不仅存在于数据之上,也可以有其他非代码符号的表现形式。破坏数据的完整性,或者窃取他人数据,未必构成对个人信息的侵害,只有当所窃取数据同时在文义层面表现为个人信息之时,才涉及个人信息被侵害的问题。因此,破坏数据完整性或者窃取数据,并不需要以使用他人数据为条件,而侵害个人信息在表现形式上,往往要求具有在语义层面的使用,更进一步讲是具有商业或利己目的的使用。我国现有学说力求在个人信息主体和使用人之间构建平衡,达到既能保护民事主体的个人信息

自主利益，同时也要兼顾个人信息使用者利益的目的。基于该种出发点，我国现有理论主要有三种限制个人信息主体利益的方式：第一种建议对个人信息进行完全保护，但是可以通过合同方式来实现他人对信息的使用^[12]；第二种认为信息使用的合法性基础不应当仅限于知情同意，应当构建多元的合法性基础^[16]；第三种主张以信息保护和数据开发利益二元化的价值为基础，通过构建“积极确权+行为规范”的方式，在个人信息保护和他人利用数据之间寻求平衡^[17]。

在讨论信息层面数据保护的限制之时，首先需要明确的是，如果个人信息是以代码符号的形式保存的，那么对于代码符号层面数据保护的限制，在这里也应当予以适用。就个人信息特有的限制方式来看，无论是第二种方式，还是第三种方式，都试图在个人信息上构建多元正当性基础，以此来调和信息主体和使用人之间的权利冲突。上述限制思想主要来源于欧美国家，从保护程度来看，欧美国家对个人信息的保护相对起步较早，公法领域对个人信息的保护较为完善，已经有一套完备的保护体系，因此实际上是在寻求一条从保护到适当限制的路径。欧美国家确实可以构建多元合法性体系，将个人信息使用者的特定权利也纳入正当性基础。我国的具体情况恰恰相反。虽然我国在1982年《宪法》中有“公民的人格尊严不受侵犯”“公民住宅不受侵犯”“公民享有通信自由和通信秘密的权利”“国家尊重和保障人权”等相关条款，但是没有明确对个人信息的保护。从宏观角度来看，我国在个人信息方面的保护，主要存在如下问题：一是体系性思维缺失，分散地规定在各个部门法，并且比较陈旧，无法构建个人信息保护的体系；二是条文数量较少，适用范围较为狭窄，并不存在统一的个人信息保护法；三是我国历来有重刑事轻民事的传统，在民事救济上并未构建个人信息主体的损害救济制度；四是条文的可适用性不强，我国公法领域存在许多宣誓性条文，在没有民法理论的支撑下无法转化为可适用的条文^[18]。由此可见，我国还不能将信息的使用提升到与信息主体保护的同等地位。

我国应当将对个人信息享有者的保护放置在对个人信息使用者的保护之前，在模式的选择上应当以第一种方式为基础。虽然个人信息的保护被认为植根于个人信息自主权理论，但是并非所有的个人信息都需要保护，全面保护应当体现在保护程度上而非保护范围上。就现有研究来看，想要通过理论直接勾勒出哪些个人信息需要保护，哪些个人信息不需要保护，几乎是不可能的，恰当的做法是在个案中进行利益衡量。从对个人信息的保护和公共领域的维系来看，如下几种因素需要在确定个人信息保护之时予以考量：信息和主体相关性、公共利益的保护、言论自由的实现、正常交往的实现等。这些因素需要综合考量，从程度和价值上进行衡量，例如某些个人信息和人格的关系较疏远，或者说这些信息是社会交往中必须向公众提供的，那么该种信息并无严格保护的必要^[19]。再比如为了保障公民的言论自由，主体的个人信息利益需要为言论自由利益让步。除此之外，在个案中我们需要通过利益衡量来确定个人信息保护的必要性，以及对特定个人信息限制的可能性。

五、结语

伴随着互联网和大数据时代的到来，数据在生活中扮演着越来越重要的角色。我国学者在分析数据之时，要么将数据定位为代码符号，要么将数据定位为个人信息，缺乏对两者的体系研究。我们应当认识到数据具有二元化特征，一方面可以通过代码符号进行存储，另一方面可以直接表现为个人信息。它们的内容有一定的交叉，但并不存在必然联系。对于代码符号层面数据的保护，我们主要借助其他部门法中的保护性规范，通过侵权法对破坏数据的完整性和窃取数据等行为进行规制，而就该层面财产利益的保护，则借助合同法来完成。对于语义层面数据的保护，在民事领域主要体现为对个人信息的保护，不管称之为个人信息权还是个人信息利益，它们都与绝对权存在差异，因而我们应当借助保护性

规范用侵权法保护,可能涉及的财产利益应当借助合同法保护。符号层面的数据和语义层面的数据都具有一定的公共属性,私法在保护之时应当作出一些限制。

注释:

- ① 早期对数据的保护主要得益于公法的发展。以德国法为背景,从联邦宪法法院的“人口普查裁定”(Volkszählungsurteil)开始,就承认了《德国基本法》第1条第1款和第2条第1款的以一般人格权为基础的个人信息自主权,《欧洲联盟基本权利宪章》第8条也规定保障个人数据的基本权利。CHRISTIAN BERGER. Property rights to personal data?—An exploration of commercial data law, *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3), p.350.
- ② 我国现有研究中,已经有学者主张区分个人信息和数据进行保护,对前者主要赋予人格利益和部分财产利益,而对后者主要构建数据经营权和资产权。参见龙卫球:《数据新型财产权构建及其体系研究》,载《政法论坛》2017年第4期,第63页。
- ③ OLG Karlsruhe NJW 1996, 200; OLG Oldenburg CR 2012, 77; OLG Dresden CR 2013, 196.
- ④ 德国学者认为数据保护已经达到和知识产权保护相同的程度,不应当构造载体权利。HERBERT ZECH. Building a European data economy—The European commission's proposal for a data producer's right, *Zeitschrift für geistiges Eigentum, (ZGE)*2017(3), p.329.
- ⑤ 德国学者认为,为了促进数据资产交易,创造一项新的所有权是没有必要的。没有所有权的模式,通过责任法也能解决救济问题,因此并没有创造新型权利的必要性。GERALD SPINDLER. Data and property rights, *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3), p.405.
- ⑥ 这里的数据不仅限于个人数据,还包括那些机械化生成的数据,或者说机械化与个人无关的数据在这里也是很重要的一个部分。
- ⑦ 我国《著作权法》在第23条、第33条第2款、第40条第3款、第43条第2款、第44条中对著作权的法定许可作了明文规定,其第22条则规定了合理使用。《专利法》某些条文也具有上述特点。
- ⑧ 关于个人信息保护和隐私权的关系问题,可参见张文亮:《个人数据保护立法的要义与进路》,载《江西社会科学》2018年第6期,第172页。
- ⑨ Vgl.BGHZ 13, 334.
- ⑩ BVerfGE 65, 1 (43)- Volkszählung.
- ⑪ 也有学者持相反观点,认为赋予绝对权并不会产生垄断,完全可以类比著作权和专利权等。BENEDIKT BUCHNER. Is there a right to one's own personal data, *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3), p.417.

参考文献:

- [1] 冯登国,张敏,李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014(1): 246-258.
FENG Dengguo, ZHANG Min, LI Hao. Big data security and privacy protection[J]. *Chinese Journal of Computers*, 2014(1): 246-258.
- [2] 纪海龙. 数据的私法定位与保护[J]. 法学研究, 2018(6): 72-91.
JI Hailong. Private law positioning and protection of data[J]. *Chinese Journal of Law*, 2018(6): 72-91.
- [3] HERBERT ZECH. Building a European data economy—The European commission's proposal for a data producer's right[J]. *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3): 317-330.
- [4] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122.
CHENG Xiao. Personal data rights in the era of big data[J]. *Social Sciences in China*, 2018(3): 102-122.
- [5] 王镭. 电子数据财产利益的侵权法保护——以侵害数据完整性为视角[J]. 法律科学, 2019(1): 38-48.
WANG Lei. The protection of property interests of electronic data in tort law—From the perspective of infringing integrity of data[J]. *Science of Law*, 2019(1): 38-48.
- [6] 于飞. 侵权法中权利与利益的区分方法[J]. 法学研究, 2011(4): 104-119.
YU Fei. The method of distinguishing rights and interests in tort law[J]. *Chinese Journal of Law*, 2011(4): 104-119.
- [7] CHRISTIAN BERGER. Property rights to personal data? —An exploration of commercial data law[J]. *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3): 340-355.
- [8] 张里安,韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛, 2016(3): 119-129.
ZHANG Li'an, HAN Xuzhi. The private law nature of personal information right in the big data era[J]. *Legal Forum*, 2016(3): 119-129.
- [9] 劳伦斯·莱斯格. 代码: 塑造网络空间的法律[M]. 李旭,等译. 北京: 中信出版社, 2004: 197.
LAWRENCE LESSIG. Code: And other laws of cyberspace[M]. Trans. LI Xu, et al. Beijing: CITIC Press, 2004: 197.
- [10] 贺栩栩. 比较法上的个人数据信息自决权[J]. 比较法研究, 2013(2): 61-76.
HE Xuxu. Right to self-determination of personal data in comparative law[J]. *Journal of Comparative Law*,

- 2013(2): 61-76.
- [11] BENEDIKT BUCHNER. Is there a right to one's own personal data?[J]. *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3): 416-419.
- [12] 梅夏英. 数据的法律属性及其民法定位[J]. *中国社会科学*, 2016(9): 164-183.
- MEI Xiaying. The legal properties of data and the position of data in civil law[J]. *Social Sciences in China*, 2016(9): 164-183.
- [13] LOUISA SPECHT. Property rights concerning personal data[J]. *Zeitschrift für geistiges Eigentum (ZGE)*, 2017(3): 411-415.
- [14] ALEXANDER HELLGARDT. *Regulierung und Privatrecht*[M]. Tübingen: Mohr Siebeck, 2016: 50.
- [15] 方新军. 权益区分保护的合理性证明——《侵权责任法》第6条第一款的解释论前提[J]. *清华法学*, 2013(1): 134-156.
- FANG Xinjun. Proof of the rationality of the protection of rights and interests: The interpretative premise of Article 6 (1) of *Law on Tort Liability*[J]. *Tsinghua University Law Journal*, 2013(1): 134-156.
- [16] 高富平. 个人信息使用的合法性基础——数据上利益分析视角[J]. *比较法研究*, 2019(2): 72-85.
- GAO Fuping. The legal basis of processing of personal information: A perspective of interests related to personal information[J]. *Journal of Comparative Law*, 2019(2): 72-85.
- [17] 宋亚辉. 个人信息的私法保护模式研究——《民法总则》第111条的解释论[J]. *比较法研究*, 2019(2): 86-103.
- SONG Yahui. Civil law protection models of personal information: Interpretative theory of article 111 of *China's General Provisions of Civil Law*[J]. *Journal of Comparative Law*, 2019(2): 86-103.
- [18] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. *中国法学*, 2015(3): 38-59.
- ZHANG Xinbao. From privacy to personal information: The theory of interest remeasurement and institutional arrangement[J]. *China Legal Science*, 2015(3): 38-59.
- [19] 杨芳. 个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体[J]. *比较法研究*, 2015(6): 22-33.
- YANG Fang. A historical sketch and critical review of the theory of the right to self——determination of personal information: An analysis on the protection object of personal information protect act[J]. *Journal of Comparative Law*, 2015(6): 22-33.

Binary division and system protection of data

FENG Degan

(School of Law, Nanjing University, Nanjing 210093, China)

Abstract: Data can be divided into two levels: data at the code symbol level and data at the semantic information level. Although the data at the code symbol level exists objectively and is similar to legal objects to some extent, because of its lack of competition and the unclear outline of rights, it is impossible to construct "data file ownership". And the data should be protected by means of protective norms. The protection of the data at the code symbol level is specifically embodied by the fact that the data is integral and that the data is not stolen. The data at the semantic information level is mainly in the protection of personal information in the field of private law. It is not feasible to construct the path of absolute protection of personal information to protect it. Due to the maturity of public law protection of public information, it should be protected by protective norms. Because both levels of data contain property interests, the most appropriate way to protect the data is by exploiting the contract system. On the other hand, as data at both levels have certain public attributes, the private law should also impose some restrictions on its protection.

Key Words: data protection; code symbol; semantic information; personal information; protective norms

[编辑: 苏慧]