数据分级分类制度与数据犯罪的衔接研究

◆苏　杭

（贵州师范大学法学院，贵州 贵阳 550025）

【摘要】我国《刑法》对于数据安全的保障，还停留在静态附属的态度之下，但数据安全法益具有自己的独立性和动态性，现行刑事立法对数据犯罪的界定仍有不足。新建立的数据分级分类制度对数据安全法益识别具有重要的参考价值，可以指导数据犯罪的定罪量刑。因此，应以数据安全法益的确定为前提，以分级分类制度的建立为指引，将数据分级分类的法益识别功能与数据犯罪定罪量刑相衔接，共同完善数据犯罪的刑法保护体系，维护我国的数据安全。

【关键词】数据安全；数据犯罪；数据分级分类；法益识别

2020年，国务院等印发的《关于构建更加完善的要素市场化配置体制机制的意见》，将数据定义为与土地、劳动力、资本、技术并列的第五大生产要素。在此背景下，数据的价值越来越被人所重视，同时，数据爬虫、隐私泄露、去匿名化技术以及非法数据买卖等数据违法甚至犯罪行为也屡见不鲜。为了建立安全的数据环境，我国发布了《个人信息保护法》《数据安全法》《网络安全法》等法律规范，但主要针对个人数据的保护和各自与其他并存的法律规范之间缺乏有效的衔接。在刑事立法层面上，1997年《刑法》首次写入计算机犯罪，《刑法修正案（七）》增设了非法获取计算机信息系统数据、将侵犯个人信息的罪名合并为侵犯公民个人信息罪；2011年两高发布的《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》加大了计算机犯罪的处罚力度；《刑法修正案（九）》修改增加了有关计算机犯罪的条文。经此种种修改，我国对数据犯罪的打击力度逐年加强。但是在实践中，司法机关对数据犯罪这种新型犯罪的裁判尚，存在此罪与彼罪界定不明、类案异判问题。《数据安全法》提出的数据分级分类制度具有法益识别的功能，有助于此罪与彼罪的区分、建立数据犯罪评价标准、完善数据保护法律体系，与数据犯罪定罪量刑相衔接。

一、数据、数据安全及其法益识别

数据在我国法律体系中没有统一的定义。在立法和实践中，信息、数据等称谓在使用时模糊不清，甚至出现混用的情况。纵观立法来看，有关个人信息保护的立法，经历了从隐私—信息—数据的立法模式，在此背景下，可以看出数据有不同于其他概念的独立性，有必要厘清其独特性质。在《数据安全法》中，数据被定义为“任何以电子或者其他方式对信息的记录。”而个人信息在《网络安全法》中被定义为“可特异性识别到个人的信息。”对于信息而言，更多是强调其内容，对于数据则更多的是强调其作为记载内容的载体。因此，对于信息的保护更注重其“保密性”，保护其不被非法窃取和使用；但是对于数据则更看重其安全性，保护其不被非法获取、篡改、删除和使用。

在刑事立法中，对数据安全的保护主要依赖于破坏计算机信息系统、侵犯商业秘密罪等罪名的规定，数据在这些罪名的犯罪客体中属于附属和次要的存在。但是随着数据被确立为一种新型的生产力要素，其流通和交易的频率越来越高，仅仅作为其他罪名的附属客体，不足以满足保护数据安全的需要，数据安全应作为一项独立的法益存在。在一个数据周期中，会出现数据生产者—数据保管者—数据管理者—数据使用者。由于数据具有非竞争性和非排他性的特征，在数据的产生到使用的过程中，数据会逐渐脱离原始权利者的控制，逐渐由其他人来控制数据。因此，对于数据而言，其逐渐由个人控制转向社会控制，并具有社会公共利益的属性。

传统刑法将受到现实侵害或存在现实侵害的危险，作为法益是否需要保护的界定条件。而在现代社会刑法转而开始关注行为人的行为所创造的风险，法益的表述越来越被弱化。《刑法修正案（十一）》新设了独立危险犯，进一步关注到行为人行为所带来的社会危险。对于数据安全法益而言，由于数据具有社会公共利益的集体属性，因而数据安全法益具有一定的模糊性，在风险判断时存在障碍；但即使数据安全法益具有一定的模糊性，但也不能放弃对其相对明确性的界定。显然，鉴于刑法具有谦抑性，并非所有的数据都可以作为刑法需要保护的数据。因此，对数据安全法益的判定要满足两个路径：一是某种数据所承载的法益是否可以上升到刑法所保护的法益；二是此种数据法益侵犯的具体是何种刑法法益，应如何对其进行定罪量刑。数据安全分级分类也就是依据数据的重要性和危险程度，能在很大程度上帮助对于刑法数据安全法益的判定。

二、数据安全分级分类制度

数据安全分级分类不仅是《数据安全法》的要求，也将

是构建数据安全保护体系的重要所在。《数据安全法》第二十一条规定我国应建立数据分级分类保护制度，将数据分为一般、重要和核心数据三级。数据分级分类制度的建立是维护数据安全体系的基石，数据的复杂性使得对其的保护不可以“一刀切”的形式进行全方位的保护，必须依照其内容和重要程度进行区分，这也为数据安全法益的界定提供了指引。

（一）数据分类

数据分类是指依据某些数据所承载的内容具有的统一类型来进行同类项合并，主要是确定数据所属的类别。但是，迄今为止，数据分级分类制度仍未完全建立，也无通用分级分类标准。本文以内容为分类方式，说明数据分级分类对刑法数据犯罪的法益识别意义。依据数据的内容，可以分为个人数据、法人及其他组织数据和政府数据。

1.个人数据

个人数据，又称个人信息。《网络安全法》第七十六条对个人信息下了定义，该定义采用了“概括＋列举”的方式规定了个人信息，以“可识别性”作为认定个人信息的标准，包括自然人的姓名、身份证号码等信息。在国外，欧盟《一般数据保护条例（GDPR）》将个人数据界定为“任何已识别或可识别的自然人相关的信息”，同样也将可识别性作为判断标准。即如果凭借该信息可以识别到特定自然人则属于个人信息，反之则不属于个人信息。在国家标准GB/T35273《个人信息安全规范》中，提出了个人敏感信息这个概念。根据该标准，个人敏感信息是指易导致身心受到损害或引发歧视性待遇的个人信息。提出敏感信息是因为该信息所包含的内容易引发巨大的负外部效应，在获取个人敏感信息时，应当适用更严格的程序和规范。在个人敏感信息的交易上也将适用更严格的标准，甚至杜绝敏感信息的交易。

2.法人及其他组织数据

法人及其他组织数据（以下简称组织数据）既包括反映组织本身产生的原始数据，主要包括财务数据、人事数据、采购数据等；还包括企业的客户数据、供应链数据以及行业协会的成员名单和其他机构的年度报告等；也包括通过合同授权、数据采购、自主采集等方式拥有的其他数据集合，比如，行业分析报告、客户画像等。

企业对企业原始数据拥有所有权是毋庸置疑的，对于企业收集、加工处理的其他数据，也应承认企业对其拥有所有权。个人数据在对其进行匿名化处理后，可使其丧失特异识别性，此时该数据不再是个人数据，而信息处理者在付出相应劳动后，其应获得处理信息的所有权。这与作品的改编权是同样的，在获得原作品人同意后，在其作品基础上再进行创作的新作品应该归改编人所有，在原始数据上进行合法处理，也应获得处理信息的控制权。

3.政府数据

政府数据是指行政机构及其授权组织，在履行职责的过程中获取或制作的各类数据，包括税务数据、企业公开信息、法院判决及执行情况、专利申报信息等。因行政机构的公共性，除了依据相关法律规定应当予以保密的数据，有关部门应当向社会大众公开其他数据，减少社会大众搜寻此类数据的成本。还应该注意，虽然政府数据是公共资源，但这并不表示有关部门对该数据丧失所有权，也不表示其他主体可以控制该数据。

（二）数据分级

从刑事立法的角度而言，数据分级是指数据按照其对社会的危害程度分类后进行分级。数据分级对于数据能否上升成为刑法所要保护的法益，具有很重要的作用。按照《数据安全法》等相关规范的规定，数据一般分为一至三级。数据分级分类是一个复杂的过程，对于某个具体的数据而言，在不同的情景中会有不同的定义。如果某些信息结合其自身的性质、使用这些信息的目的、当下社会的普遍情绪等因素，综合判断其符合个人敏感信息的定义。实际上，欧盟《一般数据保护条例（GDPR）》定义特殊类型的个人信息也是同样的逻辑。GDPR并未对特殊类型的个人信息进行列举，而是为其提供了判断标准。丁晓东教授也支持这种观点，他认为“通过在具体场景中确定数据的性质与类型，并根据具体场景中各方的合理预期来确定相关主体的数据权益。”

数据分级分类虽然具有一定的复杂性，但其对于指导数据犯罪法益判断的重要作用却是不言而喻的。数据分级分类应遵循先分类再分级的方法，对于其中的一级和二级数据而言，其就不属于刑法数据安全法益所要保护的对象。数据分级分类为数据犯罪定罪量刑提供了参考依据。

三、数据分级分类的法益识别功能与数据犯罪定罪量刑的衔接

数据的种类繁多，刑法一一对其进行同等力度的保护是不现实的。数据作为各种信息的载体，不同的数据对于国家利益、社会公共利益、个人利益的重要性是不统一的。学界一般认为，我国《刑法》中非法获取计算机信息系统数据罪和破坏计算机信息系统罪所保护的法益是一种秩序法益——计算机系统管理秩序，具有一定的抽象性。对抽象法益进行保护在实务中具有一定的难度，计算机信息技术的发展也使得司法工作人员对数据犯罪的把握存在冲突，难免使得其司法适用出现“口袋化”或“虚置化”的趋势，或出现同案不同判的风险。为了减少这一情况的出现，刑法数据犯罪的定罪量刑有必要与《数据安全法》中要求建立的数据安全分级分类制度相衔接。以保护数据安全为核心，发

挥数据安全分级分类制度对于指导数据犯罪定罪量刑的重要作用。

（一）数据犯罪保护法益的确定——明晰罪与非罪的界限

数据犯罪入罪门槛的确定，离不开对数据犯罪所保护法益的明晰。在信息技术飞速发展的时期，刑法应当以更动态、更开放、更独立的态度看待数据安全的存在，例如，在立法上，摒弃将数据安全放置在破坏计算机信息系统罪的附属条文之中，扩大数据的保护范围，除了侵犯公民个人信息罪之外，侵犯其他数据的行为也应一并入罪。在操作上，司法监管可以借助数据分级分类制度对数据进行一般数据和重要数据的区分，出台司法解释对一般数据规定其入罪门槛，而重要数据的入罪门槛在一般数据的基础上有所放低。还可以出台数据犯罪的定罪量刑指导意见，列举某些常见的犯罪情况，明确在分级分类的制度下，不同罪名的定刑标准。当然鉴于数据安全法益的抽象性，在制定指导意见时应留足够的自由裁量空间，方便司法人员针对具体案件做出调整。

（二）数据犯罪量刑的参考——判断刑罚的轻重

我国《刑法》对数据犯罪的常见罪状表述为“情节严重”。具体而言，两高《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》列举了非法获取计算机信息系统数据罪中的“情节严重”情形。所列举的情节标准没有与数据安全法益进行衔接，无法突出刑法对数据安全法益的重视。事实上，数据安全的法益与数据的等级和类别息息相关，对于刑法中非法获取计算机信息系统数据罪的“情节严重”，完全可以与数据安全分级分类制度相衔接，按照数据的类别和等级判断是否属于严重情节。对于如何判断数据犯罪“情节严重”的司法难题，可以依据数据分级分类制度进行判断，但是鉴于数据分级分类制度还不完善，对于数据分级分类不必苛求完全，将数据分级分类作为指导意见确定量刑轻重，避免造成适用法律的僵化。

四、结束语

随着信息技术的发展，数据犯罪形式不断增多。数据安全已经与网络安全、信息安全一起成为国家安全的一部分，但是我国《刑法》对于数据安全的保障还停留在静态附属的态度之下，非法获取计算机信息系统数据罪和破坏计算机信息系统罪只是以数据作为其所保护的法益，但数据安全法益作为一种独特的法益具有其专属的独立性和动态性，需要对其单独进行保护，而数据分级分类制度恰好在数据安全法益的识别上和数据犯罪定罪量刑上有提供指引。现有的刑事立法对数据安全的保护仍有不足，且缺乏与数据分级分类制度的衔接。因此，我国刑事立法应与新出台的《数据安全法》相联系，借助《数据安全法》中确立的数据分级分类制度，对数据犯罪的法益识别和定罪量刑提供判断标准，以完善数据犯罪的刑法体系，维护我国的数据安全。

参考文献：

[1]丁晓东.论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析[J].现代法学,2019,41(03):96-110.

[2]张勇.数据安全分类分级的刑法保护[J].法治研究,2021(03):17-27.

[3]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(07):72-83.

[4]何群,康志雄.我国数据法益的刑法定位及保护路径[J].南京航空航天大学学报(社会科学版),2022,24(03):63-68.

作者简介：

苏杭(1998—),女,侗族,贵州铜仁人,硕士研究生,研究方向:经济法学。