论数据安全的客体

范明志

（中国政法大学数据法治研究院　北京　100088）

内容提要：数据安全与网络安全以及个人信息保护等法律制度相互关联，数据与信息、安全与保护等法律概念相互杂糅，导致数据安全客体范围不清晰。从数据的价值实现、数据安全的独立性、数据安全保护机制及数据利用方式等四个维度，可以辨析出数据安全客体应当是：动态开发利用中的数据、电子记录方式的数据、“风险—控制”社会安全管理意义上的数据、适用算法处理的集合性数据。在有关数据安全的立法、执法和司法活动中，应清晰辨别数据安全的客体，才能将数据安全制度落到实处，促进数字经济健康发展。

关键词：数据安全　客体　算法　数字经济

随着数字中国建设的开展，数据安全的重要性愈发显现。在数据安全、网络安全、个人信息保护等法律制度相互杂糅的背景下，再加上国内外对数据、信息等概念缺乏一致性规范等因素，数据安全的客体范围到底为何，至今还没有形成明晰的共识，这在一定程度上对数据立法、执法和司法实践形成了障碍。法律关系客体的不确定性自始存在，并随着民事关系的扩展日益突显。[①]虽然我国《网络安全法》《数据安全法》《个人信息保护法》已出台，一些实施性的法律规范如《数据出境安全评估办法》《网络数据安全管理条例（征求意见稿）》等对于数据安全做出了较为细致的规定，但是数据安全客体的界定问题仍没有得以完全解决，导致一些重要数据

作者简介：范明志（1970—），男，汉族，山东曹县人，中国政法大学数据法治研究院教授、博士生导师。

本文为2021年度国家社会科学基金重大项目“互联网平台的社会影响及其治理路径研究”（项目批准号：21&ZD195）的阶段性研究成果。

① 梅夏英：《民法权利客体制度的体系价值及当代反思》，载《法学家》2016年第6期。

安全制度如数据分类分级制度难以有效实施。[②] 本文拟从数据的价值实现、数据安全的独立性、数据安全保护机制以及数据的利用方式等四个维度来分析、辨别数据安全客体，以期助益于构建更加完善的数据安全制度。为便于论述，本文对于法律关系客体的概念采取通说，[③]将数据安全客体界定为数据安全法律关系所指向的对象。

一、数据的价值实现对数据安全客体的范围限制

尽管数据被称为信息时代的“石油”，已经被列为继土地、劳动力、资本、技术之后的第五大生产要素，[④]但这是对数据重要性的一种总体性评价，并不意味着所有的数据都是数据安全的客体，也不意味着数据安全成为数据治理的最高标准。数据的价值决定了数据安全本身是一种利益平衡的制度设计，也决定了数据安全客体的界定不是以静态的“数据”概念为标准。

任何一种生产要素，只有在社会生产活动中被利用才能发挥促进社会进步、创造更多生产成果的作用。数据存在的唯一价值就在于利用，数据技术的目的就在于利用数据。在此基础上，数据安全的价值取向也必然不单纯是数据的安全，更重要的是数据开发利用和产业发展。这一思想已经被我国《数据安全法》确认。让数据躺在安全箱中“睡觉”虽然可以实现数据的安全，但是这种安全对于数据的价值实现是没有意义的，几乎等同于数据的“死亡”。在安全的相对性上，数据安全与网络安全具有一定的相似之处：二者都是相对的而不是绝对的。应立足基本国情保安全，避免不计成本追求绝对安全，那样不仅会背上沉重负担，甚至可能顾此失彼。[⑤]

实践中，数据安全与数据利用的关系仍然存在着“理还乱”的现象：一方面，强调数据安全而忽视了数据利用。数据的开发利用实质上就是数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。如果数据仅仅处于存储状态，那么其安全威胁要比在动态处理的过程中要小的多，但同时数据的价值也难以得到充分发挥。事实上，往往是在数据的使用、加工、传输、提供、公开的处理活动中，数据的有效保护和合法利用的状态受到破坏。另一方面，强调数据利用的目的而忽略了数据安全。数据的价值在于利用，要消除“数据孤岛”，实现数据联通。但实际上，数据安全对于数据的开发利用有时会起到一定的阻碍作用，数据的开发利用必然加大数据安全的风险。这种“各说各话”的现象必然导致数据安全与数据利用之间的紧张关系。可见，清晰的数据安全制度，是促进数据开发利用和产业发展的重要前提。

从理论上讲，数据开发利用和产业发展与数据安全之间的相互促进关系是可能实现的。这种关系是一种应然意义上的关系，或者说是一种目标意义上的关系。这种相互促进关系的实现不可能是一种自发的商业化过程，需要以法律制度上的明确安排为前提，因为数据安全既

---

② 陈兵、郭光坤：《数据分类分级制度的定位与定则——以〈数据安全法〉为中心的展开》，载《中国特色社会主义研究》2022 年第 3 期。

③ 多数学者认为法律关系客体即权利义务所指向的对象。参见谢晖、陈金钊：《法理学》，高等教育出版社 2005 年版，第 248 页；魏振瀛：《民法》，北京大学出版社、高等教育出版社 2013 年版，第 121 页。

④ 参见《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》第六部分。

⑤ 中共中央党史和文献研究院编：《习近平关于网络强国论述摘编》，中央文献出版社 2021 年版，第 92 页。

涉及到公共利益、又关系到个体权利，数据开发利用更是一种复杂的经济利益活动，这些均应当落入法律调整的范围之中。就数据安全而言，虽然相关法律制度对于“数据”的含义进行了界定，但是，至于哪些数据能够适格地成为数据安全客体，并不存在一条明朗的界线。如果笼统的将所有数据都作为安全管理的对象，不仅将极大增加安全管理的成本，而且也将使数据开发利用陷入困扰甚至停滞。

在未来数字化社会的发展进程中，数据将成为社会生产、管理活动的基本要素和存在方式。数据安全应当以更加精准的方式发挥作用，数字经济必然是一种更加开放的经济形态，数据的共享与合理使用将成为越来越普遍的现象。如果数据安全的界限不清晰、不合理，数字经济的开放程度将大打折扣。从当前国际层面来看，虽然主权国家普遍意识到全球数据安全治理以及合作的重要性和紧迫性，但却依旧不断颁布单边限制数据流动的法规，日益呈现出“新数字孤立主义”的倾向。[⑥] 数据安全的动态在很大程度上表现为进行安全管理的数据范围的增减，因此，建立一种相对稳定的数据安全客体范围，是保证数字经济发展的基础条件。当前，元宇宙经济形态已经开始破冰，元宇宙本身就是数据的集合，数据将成为关键生产要素，[⑦]对于数据安全的要求和对于数据利用的要求都将提上更高的层次；更不消说在未来数智化社会[⑧]中，整个社会与自然界都实现数字化存在，数据成为人类的生存状态，如何建立数据安全与数据利用的良性互动关系，将成为数据制度的关键性内容。

鉴于数据具有体量巨大、时效性强、价值密度低疏等特点，其安全制度应当是一种与数据利用技术密切相关的一种机制。数据安全价值的判断，仅凭数据自身的行业、性质、体量等表层因素是不够的，必须结合国家政治、经济、文化乃至社会成员利益等相关因素进行综合判断，建立一种以危害安全为标准的判断机制。判断数据安全价值的依据是数据的相关性，如果抛开数据的具体开发利用，去空想数据的安全价值，往往会落入数据所记载信息内容的安全价值判断的窠臼之中，从而偏离了数据安全的制度领域。

因此，从数据的价值实现而言，数据安全制度的客体应当是开发利用意义上的数据。没有开发利用价值的数据、被禁止开发利用的数据，虽然也符合数据的概念，但是在法律关系上，不应属于数据安全的范畴，应当适用其他法律规范。比如开展涉及国家秘密的数据处理活动，应当适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。[⑨] 数据安全法律制度应当展示出清晰的“数据客体区分体系”，即如何区分不同数据的安全价值，如何在合理监管中分别将他们归入自由流通、规制流通、禁止流通的渠道，在价值实现中保证数据安全，从而实现数据安全与数据利用的良性互动。而基于“相关性”的数据开发利用，注定了数据安全价值的判断

---

⑥ 阙天如：《全球数据安全治理的趋势与困境》，载《中国社会科学学报》2022 年 10 月 13 日。

⑦ 参见叶毓睿等：《元宇宙十大技术》，中译出版社 2022 年版，第 283 页。

⑧ 数智化社会所展开的是一种超大规模、超复杂的经济社会关系全新形态，数智化逻辑是人机互融、虚实同构、算法主导。参见齐延平：《数智化社会的法律调控》，载《中国法学》2022 年第 1 期。

⑨ 参见《中华人民共和国数据安全法》第 53 条。

不是一个简单制定标准的问题。

二、基于数据独立价值的数据安全客体指向

数据安全的客体当然是数据,数据是指任何以电子或者其他方式对信息的记录。[10] 从字面来看,这是一个清晰的表述。但是数据与信息为同一事物的形式与内容,在对信息保护已经形成了较为成熟法律体系的背景下,是否还有必要另行制定一套数据安全的法律制度?换言之,数据安全的独立价值何在?从更具体的对象来看,如何区分个人数据与个人信息,并分别将他们与不同的法律制度相对应?因此有必要对数据安全的独立性进行分析,从而辨析出数据安全的客体指向。

(一)数据安全应当独立于信息安全

相对于信息安全,数据安全的独立性取决于数据的独立价值。从概念上看,信息是人类对世界的认知,是一种属人的认识现象。[11] 信息描述的是其内容,因此它是一个实体性概念,也是一个偏重于个体表述的概念。那么,信息安全当然应当限定于那些具有保护价值的具体信息,比如个人隐私、商业秘密、国家秘密等。但是信息作为一种认识必须依靠一定的载体和形式才能存在,德国法学家 Herbert Zech 认为信息包括三个层面的内容:承载结构层面的信息、符号代码层面的信息和实质语义层面的信息。[12] 其中符号代码层面的信息指的就是作为信息记录的数据。除了电子数据,手势、语言、文字、图片、密码、印刷术等都可以作为信息的记录方式,因而也属于数据的范畴。因此对于数据与信息的关系可以描述为:数据是以特定符号代码(当今尤指电子数据)对信息的记录方式,与信息分别是同一认识现象的记载形式(载体)与内容(意义)。因此有学者指出,在互联网世界中,任何对于信息或数据的保护最终都具有保护实质信息内容和数据形式完整的双重任务,两者不能完全割裂开来。[13]

二者之间内容与形式的关系并不妨碍其各自的独立性。有学者指出,将信息和传输信息的载体混为一谈是一种典型的混同,信息的载体本身并不是信息,只有从载体中理解和辨识出来的意义才是信息。[14] 那么,数据安全问题应当是关于“数据形式”的问题,而不是关于“信息内容”的问题。照此看来,如何处理数据与信息的关系,就成为辨别数据安全客体的一个重要前提:如果将数据与信息看作同一事物,那么数据安全就等同于信息安全,数据安全与信息安全的立法应当呈现出“一体化”的立法体例,将信息纳入数据安全的客体将是必然选择,当然也可以反过来说,将数据安全作为信息安全的组成部分;如果将数据与信息分别看作独立的“形式”与“内容”,那么数据安全就应当仅指向数据这种信息记录方式意义的安全,信息内容意义上的安全则属于其他法律规范的内容。数据安全与信息安全的立法必然呈现出“二元化”的立法体

---

⑩ 《中华人民共和国数据安全法》第 3 条第 1 款。

⑪ 参见肖峰:《信息技术哲学》,华南理工大学出版社 2016 年版,第 32 页。

⑫ See: Herbert Zech, Information as Property, Journal of Intellectual Property, Information Technology and Electronic Commerce, 2015, pp. 194 – 197.

⑬ 梅夏英:《信息和数据概念区分的法律意义》,载《比较法研究》2020 年第 6 期。

⑭ 参见肖峰:《信息的哲学研究》,中国社会科学出版社 2018 年版,第 5 页。

例，避免二者在法律规范中可能产生的交叉重合就应当成为相关立法中的重要原则。如果不能清晰地将上述两种立法体例区分开来，那么必将在法律规范上带来混乱，也必然对执法、司法活动造成障碍。

从我国《数据安全法》的立法目的来看，我国数据安全采取的是数据与信息分立的二元化立法体制。从该法第1条可以看出，我国《数据安全法》所规定的数据安全，只是数据作为信息记录方式的安全，并不包括信息内容安全本身。因此要界定数据安全的独立性，必须搞清楚数据独立于信息的具体法律意义。

数据是否具有独立于信息的法律意义，需要从数据的种类进行分析。根据《数据安全法》对于数据的定义，数据可以分为两种：电子方式记录的数据（以下简称“电子数据”）和其他方式记录的数据（以下简称“传统数据”，包括语言、文字、图画、密码、印刷等方式的数据）。从传统数据来看，比如手写文字、书面印刷等，数据与信息往往是一体呈现的，不存在专门的数据处理技术，信息处理与数据处理难以区分，单独保护数据的需求难以显现出来。这也解释了为什么以前只有对信息保护的法律规范，传统数据不具有独立于信息的法律意义。那么，电子数据是否具有独立于信息的法律意义呢？在电子数据发展初期，电子数据乃当代计算机和互联网技术领域出现的新事物，它的独立法律意义及其规则形式尚无成规可循，故一定程度上被忽略了。[15] 也许就是这个原因，欧盟的《通用数据保护条例》才没有对数据与信息进行严格的区分。但是，随着数据处理技术的逐渐成熟，数据具备了不同于信息的处理方式与价值，我国分别出台了《数据安全法》和《个人信息保护法》。那么电子数据所具有的独立于信息的法律意义何在呢？这里先要区分具体信息的电子数据与集合信息的电子数据两个概念。

具体信息的电子数据与集合信息的电子数据具有不同的法律意义：对于具体信息的电子数据而言，二者仍然是形式与内容的关系，完全可以通过对于内容的保护达到保护形式的效果，或者使单独保护数据形式变得没有必要；对于集合信息的电子数据而言，虽然也是对于信息的记录，但是，达到一定规模的数据集合的价值并不是具体信息价值简单相加，“大数据”概念表达了数据的集合性，只有当数据规模达到一定程度，其功能方可得以充分发挥。大数据之所以有价值，乃是因为通过对大量数据（包含海量信息内容）的分析和加工，可以得出进一步的信息内容（例如广告精准投放、个人画像如征信）。[16] 有学者认为《数据安全法》规定的是信息与数据一体化的“广义数据”，从总体上保护和规制所有“有信息价值”的数据及其相关行为。[17] 实际上，《数据安全法》规定的数据概念虽然没有排除具体信息的电子数据，但是该法的主要任务并不是从技术上规范数据对信息的记录方式，而是为了“规范数据处理活动，保障数据安全，促进数据开发利用”——显然这是在集合数据意义上的目的规范。具体信息的电子数据与集合信息的电子数据的法律意义差异，是数据技术高度发展的产物：计算机技术的快速进步使数

---

⑮ 梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》2020年第6期。

⑯ 纪海龙：《数据的私法定位与保护》，载《法学评论》2018年第6期。

⑰ 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》，载《法学》2022年第7期。

据逐渐成为处理信息的主要技术手段，由于信息数量持续激增，只有使用电子数据方式才能够完成对信息的储存、加工、传输、利用等处理活动。在数据技术处理信息的过程当中，电子数据的独立价值得以彰显，也使数据安全也具有了独立的意义，甚至延伸出长臂管辖与域外效力的法律问题。[18] 集合信息的电子数据不仅超越了信息集合本身（不通过数据处理方法）的价值，也超越了具体信息的电子数据的功能与价值。

从上述关于数据与信息的关系可以看出，数据安全独立于信息安全的要点在于：数据安全强调的是数据的整体性、保护的法益在于数据处理上的价值；信息安全强调的则是内容安全的个体性、保护的法益在于信息内容上的价值。尽管数据与信息在概念上存在形式与内容的关系，数据安全必然涉及到信息安全，但是只有集合意义上的电子数据才能成为数据安全的客体。

（二）在数据安全意义上，个人数据应当区别于个人信息

虽然我国立法中不曾出现“个人数据”的表述，但是在我国一些法学研究中也经常出现将“个人数据”与“个人信息”混同使用的情况，[19]明确或者无意识地断定两者之间并无差别。欧盟《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）将个人数据表述为“任何已识别或可识别的自然人（数据主体）相关的信息”，[20]并且在序言第 26 条规定该条例不适用于匿名化处理的信息。这与我国《个人信息保护法》关于个人信息的定义基本一致，[21]可以说，GDPR 对于个人信息与个人数据没有做严格的区分。但是，对于数据安全而言，个人数据与个人信息不是可以等同的概念。个人数据就是与具体个人挂钩的数据，是直接涉及具体某个人的知识的记录或数值。[22] 换言之，个人数据是关于个人信息的数据，是对个人信息进行数字化处理意义上的一种数据，个人数据安全是指数据处理上的安全；个人数据处理并不是指处理数据中的个人信息内容，而仅是对信息记录方式上的处理，比如将个人数据进行存储或者算法处理。个人数据的处理确实可能涉及到个人信息，比如违法数据处理行为可能导致个人信息的泄露，但这不影响个人数据与个人信息的区分。在此角度上，个人数据属于数据安全的客体，而具体的个人信息却不应当被归入数据安全客体的范围。

另外，从概念上看，个人数据具有二重含义，一是集合概念，指的是个人信息类别意义上的数据集合；二是个体概念，是指个人信息的电子记录方式，即使个人信息的形式表达。从当前数据研究的法学角度来讲，一般是从数据集合的角度来研究数据，所谓“大数据”。将个人数据等同于个人信息，除了语言意义外，并无法律上的表达价值。从这个角度来看，个人信息与个人数据仅仅在微观层面是同一事物，当个人信息的数量达到一定的程度，并以电子方式表现出

---

⑱ 刘练军：《个人数据与个人信息之辨析》，载《求索》2022 年第 5 期。

⑲ 参见盛小平、唐筠杰：《我国个人信息权利与欧盟个人数据权利的比较分析：基于〈个人信息保护法〉与 GDPR》，载《图书情报工作》2022 年第 6 期。

⑳ 丁晓东：《个人信息保护原理与实践》，法律出版社 2021 年版，第 51 页。

㉑ 我国《个人信息保护法》第 4 条规定：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

㉒ 刘练军：《个人数据与个人信息之辨析》，载《求索》2022 年第 5 期。

来,那么就进入了集合性的个人数据概念;个人数据仍然是数据的一个种类,不能推导出个人信息属于数据安全客体的结论。

在前述数据与信息相区别的前提下,个人数据与个人信息的混同必然导致一些不必要的困惑:首先,相对于数据这个种概念而言,个人数据是属概念,是数据的一个种类,与其他种类的数据并列,比如环境数据、交通数据等,都具有数据的集合性、算法适用性的特点;但是,个人信息的记录方式未必都表现为电子数据,也可能以其他方式比如文字、图像、符号等传统数据方式存在。将二者等同就会将传统数据(非电子数据)形式的个人信息也纳入到电子数据的安全保护体系。这既不是数据安全法的本意,[23]也会带来法律适用上的混乱。其次,个人信息保护法是基于人格权保护发展而来的权益保护法律体系,如果将个人信息等同于个人数据,个人数据是数据的一种,那么个人信息保护法岂不成了数据安全法的下位法?再次,个人信息保护法的立法目的在于保护个人信息权益,而不是关于个人信息的数据安全。我国《个人信息保护法》没有出现过"数据"一词。如果将个人数据等同于个人信息,那么,对于数据的保护也将成为个人信息保护法的任务,这与个人信息保护法的定位是不相协调的。有学者指出,个人数据权的权利客体是个人数据,它是一种无体物,个人信息权的权利客体是个人信息,它是一种有关个人的知识;这两种权利客体不但各自独立,而且有时候它们之间甚至不存在任何的勾连关系。[24]

在我国日常表达、学术研究甚至立法活动中,有时个人信息被认为数据安全的对象,比如《网络数据安全管理条例(征求意见稿)》,主要原因在于,大多数情形下数据权益与个人信息具有不可分割性。数据的意义离不开数据中所蕴含的个体信息,而信息又总是关系个体隐私和尊严。[25] 欧盟《通用数据保护条例》(GDPR)即通过数据保护形式保护个人信息,体现了数据与个人信息的紧密联系。[26] 我国的数据安全在实践上起源于个人信息的数据保护,随着在消费领域的大规模信息技术应用,我国率先对于消费者个人信息保护的进行法律关注,消费者个人信息的个体性在一定程度上掩盖了个人信息集合作为大数据的属性,并忽略了个人数据处理时的算法介入。

总之,个人信息保护是在人格权基础上发展而来的一个尚未成熟的人身权益法律制度,尚未形成系统的"个人信息权利体系"。而数据则是一个具有广泛性、通用性的信息形式概念,任何对于信息的记录都是数据。因此,从数据安全意义来看,个人数据应当是指一定数量个人数

㉓ 《数据安全法》的立法指导思想体现在其第4条:维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。可以看出,《数据安全法》的调整对象是宏观(至少是集合)意义上的数据,而非具体数据、个别信息。这也是《数据安全法》与《个人信息保护法》、商业秘密保护相关法律法规、《中华人民共和国保守国家秘密法》调整范围的界限。在《数据安全法》的实施性法律规范——《网络数据安全管理条例(征求意见稿)》中,则直接以"网络数据"概念将传统数据排除在数据安全的客体范围之外。

㉔ 刘练军:《个人数据与个人信息之辨析》,载《求索》2022年第5期。

㉕ 贾文山、赵立敏:《数字经济时代的个人数据保护:欧美立法经验与中国方案》,载《首都师范大学学报(社会科学版)》2022年第5期。

㉖ 王利明:《论数据权益:以"权利束"为视角》,载《政治与法律》2022年第7期。

据的集合，而不是具体个人信息意义上的个人数据。

三、基于法律保护机制的数据安全客体定位

对于实践中将数据与信息混同为数据安全客体的现象，还可以通过对各自法律体系运行的对比分析，来反证数据安全客体应当定位于数据形式，而非信息内容。

当然，我们应当承认数据安全与信息保护的法益具有交叉重叠性，这是数据与信息被混同为数据安全客体的重要原因。一方面，数据安全的法益是多重的，既有数据相关者的安全利益，也有数据持有者的利益，还有公共利益。有学者将其表述为“自身安全”“自主可控”和“宏观安全”三个层面。[27] 是故我国《数据安全法》第1条在立法目的上既规定了“保护个人、组织的合法权益”，也规定了“维护国家主权、安全和发展利益”。另一方面，信息保护也涉及到与数据安全相似的法益：信息的“自身安全”“自主可控”和“宏观安全”。《个人信息保护法》既有个人信息私法权益保护，也有个人信息在公共利益上的保护，比如个人信息跨境提供的规则。数据安全与信息保护的法益具有重合性是正常的，因为数据与信息本身具有形式与内容的关系。但是，法益上的重合性并不意味着法律保护机制是一致的，区分数据安全与信息保护的法律机制，可以显示出数据安全客体的具体定位。

首先，数据安全与信息保护的法理基础不同。信息保护是以“知情——同意”为法理基础的个人（主体）权利模式，模式的核心是对信息主体进行赋权；而数据安全是以“风险——控制”为基础的社会管理模式，模式的核心是对数据进行分类分级并在此基础上建立数据安全认证、风险评估和危机应对等安全制度。[28] 相应地，信息保护是一套主要以权利（益）保护为核心的私法体系，而数据安全则主要是以风险管理为核心的公法体系。依据我国《数据安全法》，保护数据安全的方式主要在于“采取必要措施”，此处的措施主要是指技术措施和管理性措施，技术措施属于工具意义上的手段，管理性措施主要是指行政管理手段和刑事手段，比如数据分类分级保护制度、数据安全审查制度，因而主要偏重于公法保护。甚至有学者认为，数据安全属于独立的刑法法益。[29]虽然对于同一法益可以同时设置公法与私法的保护手段，比如对于公民人身权、财产权的保护，但是公法保护与私法保护的方式有很大不同，而且公法应当保持一定的“谦抑性”。一般来讲，只有当其他法律不足以抑止违法行为时，才能适用刑法。[30] 数据的控制和保护主要体现在公法层面上，私法一般很少直接涉及，除非数据本身属于传统私法保护的范畴（比如隐私和知识产权数据）。[31] 学界主流观点认为我国个人信息保护法律体系的概念基础是作为民事权利的个人信息权，据此推导出信息处理者负有不得侵害个人信息的民法义务，民事责任是个人信息保护的基本手段。[32] 因此，相对于个人信息，作为安全法律关系客体的数据具

㉗ 许可：《数据安全法：定位、立场与制度构造》，载《经贸法律评论》2019年第3期。

㉘ 参见翟志勇：《数据安全法的体系定位》，载《苏州大学学报（哲学社会科学版）》2021年第1期。

㉙ 蔡士林：《我国数据安全法益保护：域外经验与立法路径》，载《深圳大学学报（人文社会科学版）》2022年第6期。

㉚ 参见张明楷：《论刑法的谦抑性》，载《法商研究》1995年第4期。

㉛ 梅夏英：《在分享和控制之间——数据保护的私法局限和公共秩序构建》，载《中外法学》2019年第4期。

㉜ 参见王锡锌、彭錞：《个人信息保护法律体系的宪法基础》，载《清华法学》2021年第3期。

有更显著的公共属性。

其次，数据安全与信息保护的法律效果不同。从语意层面来看，“安全”与“保护”存在互为目的与手段的关系，因此很难区分二者在对象、范围和程度上差别。数据与信息并不总是处于形式与内容的一一对应关系，导致数据安全对信息的保护所到达的效果与信息保护对数据安全所达到的效果不是完全一样的。一方面，通过数据安全保护无法彻底实现信息安全。如上文所述，信息具有多种存在方式，数据只是其中一种；数据安全是指电子数据尤其主要是指网络数据的安全。因此，仅靠数据安全手段并不能达到彻底保护信息安全的目的，在电子数据之外具有多种方式可以破坏信息安全，比如语言、文字等。如果将数据安全扩展到所有信息记录方式的安全，则会不当扩大数据安全的范围，也会把一些没有安全价值的数据也纳入到数据安全的客体范围，比如公开信息的数据。另一方面，通过信息保护也未必一定实现数据安全。电子数据作为一种先进的信息存在方式，完全有可能在不侵害个别信息权益的前提下被用来进行数据挖掘，或者对信息权益之外的其他法益产生危害，比如通过对个人数据的处理来危害公共安全。因此，数据与信息作为不同法律关系的客体，其法律保护机制分别指向了不完全相同的法律效果。

最后，数据安全与信息保护的法律渊源不同。从《民法典》来看，数据与个人信息被规定在不同的编别——数据规定在第一编，而对于个人信息的保护则规定在第四编人格权当中，关于个人信息的法律规范具有明显的独立性，说明个人信息与数据不属于同一法律概念范畴。从《数据安全法》与《个人信息保护法》《网络安全法》的关系来看，无论在立法位阶上还是调整对象上，都应当是相互平行、相互独立的法律规范。但三者关于数据安全和信息保护的法律规范存在一定的重复、竞合、冲突的问题：在《网络安全法》中，数据安全和个人信息保护在一定条件下依附于网络安全，属于网络安全的一部分。[33]《网络数据安全管理条例（征求意见稿）》第 3 章“个人信息保护”，明确将个人信息保护作为网络数据安全的重要内容，有些条文[34]明显不能同时契合数据的集合性与个人信息的个体性。从《数据安全法》与信息保护法律规范的关系来看，数据安全法与国家秘密保守法、知识产权法、商业秘密法、个人信息保护法之间形成了相互并列、各行其是的立法体例和法治实践。就数据安全的主要客体之一——“重要数据”来说，其重要性判断依据是数据整体的性质，而不是数据中某一具体信息的重要性。如果以具体信息的重要性来判断数据的重要性，那么就必然脱离了数据处理的范畴，进入了信息处理的领域，则应当适用信息保护的法律规范。我国《数据安全法》第 52 条规定“承担民事责任“ 的法律依据仍然是已有的个人隐私、个人信息、知识产权等信息保护的规范，《数据安全法》并没有塑造新的法律规则。国家秘密是极端重要的信息，有专门的法律规范进行保护，《数据安全法》第 53 条明确排除了自身的适用。因此数据安全与信息保护各自适用不同的法律渊源，《数据安全法》将自己的规范体系限制在对数据的安全保护上，而不介入到具体信息保护的领域，体

㉝ 参见翟志勇：《数据安全法的体系定位》，载《苏州大学学报（哲学社会科学版）》2021 年第 1 期。

㉞ 比如，《网络数据安全管理条例（征求意见稿）》第 19 条至第 24 条均是规定“数据处理者处理个人信息”的相关规则。

现了数据与信息的概念区分。此外,从域外立法情况来看,欧美国家并未单独针对数据安全进行立法,而是将数据安全问题一分为二,重要数据的安全依托于网络安全特别是关键信息基础设施安全,个人数据安全融入个人信息保护中。[35] 从而避免了数据安全与个人信息保护之间的交叉重合,保证了法律体系的清晰。我国制定了专门的《网络安全法》,但是并没有将数据安全与网络安全进行明确区分,根据其第 76 条的规定,"网络安全"的概念除包含保障网络稳定可靠的运行状态之外,还包含保障网络数据的完整性、保密性和可用性。[36] 后来我国颁布了《数据安全法》《个人信息保护法》,意味着对于数据安全法益给予了独立、明确的定位,应当可以更加清楚地区分网络安全、数据安全、个人信息保护的不同法律体系。

从以上三个方面可以看出,虽然数据安全与信息保护在法益上有所重合,但是它们分别适用不同的法律保护机制。数据安全的公法定位、效果局限性、独有法律渊源都揭示了数据安全的客体应当属于"风险——控制"社会安全管理意义上的数据,而非权益保护意义上的信息。

四、数据利用方式对数据安全客体的限定

数据安全制度应当契合数据的利用方式。数据只有达到一定的规模效应才具有价值,而没有经过筛选和分析的数据哪怕是海量的也没有价值。[37] 数据最重要的不是数据本身,而是数据分析。哈佛大学盖瑞肯(GaryKing)教授认为,如果没有分析,数据的价值就没法体现。[38] 这种通过大量数据处理信息的方式促生了处理数据的新方式——算法(Algorithm)。算法是旨在解决某一特定问题而设计的指令序列,即在有限时间内将一组输入转化为一组输出的计算过程,或者说算法是基于特定目标的计算模型。[39] 算法的出现,是在人类社会中数据具备独立于信息的法律意义的根本标志,也决定了数据安全与信息保护的不同法律逻辑。随着数据处理技术的迅速发展,算法越来越多地介入到数据处理行为中,尤其是对于人工智能,算法相当于其"大脑",[40]对于数据的处理人工直接操作将越来越少。显然,作为数据处理方法,任何算法的运行皆必须以数据编程的程序化运作为其基本逻辑前提,[41]数据安全也在越来越高的程度上服务于算法处理数据的要求。数据安全的客体也因此应当具备两个特征:一是适应数据安全意义的算法衡量方式;二是具有可适用于算法的数据集合性。

(一)适应数据安全意义算法衡量的方式

如何衡量数据的安全意义?在当前的法律规范体系下,我国对于数据安全的规制模式采取的是重要数据与个人信息保护体系的双轨化,并由此衍生出两种主要确定数据安全意义的

㉟ 参见翟志勇:《数据安全法的体系定位》,载《苏州大学学报(哲学社会科学版)》2021 年第 1 期。

㊱ 张勇:《数据安全法益的参照系与刑法保护模式》,载《河南社会科学》2021 年第 5 期。

㊲ 贾文山、赵立敏:《数字经济时代的个人数据保护:欧美立法经验与中国方案》,载《首都师范大学学报(社会科学版)》2022 年第 5 期。

㊳ 参见钱塘大数据:《哈佛教授:大数据最重要的不是数据本身,而是数据分析》,https://www.iyiou.com/analysis/2017042243761,访问日期:2023 年 1 月 2 日。

㊴ 参见郑婷一、庞亮、靳小龙:《平台经济中的数据与算法安全》,载《大数据》2022 年第 8 期。

㊵ 参见周映锋、朱尚品:《算法的伦理之踵及其消解进路》,载《工业控制计算机》2022 年第 10 期。

㊶ 李振、马金琳:《算法的社会属性及其本质的社会确认》,载《思想理论研究》2022 年第 8 期。

方式:一是数据分类分级保护制度,以确定“重要数据”;二是个人数据的数量标准,以确定需要保护的个人信息数据。这两种方式也划定了需要对数据出境安全评估的基本情形。[42] 无论从一般数据处理的安全意义上,还是从数据出境安全意义上,在算法缺位的情况下,这两种衡量方式均存在实际操作上的困难。

1. 数据分类分级保护制度。从理论上讲这是符合逻辑的一种制度设计,但是问题在于这种分类分级制度是否能够落到实处。根据《网络数据安全管理条例(征求意见稿)》,国家建立数据分类分级保护制度,按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度,将数据分为一般数据、重要数据、核心数据,不同级别的数据采取不同的保护措施。国家对个人信息和重要数据进行重点保护,对核心数据实行严格保护。[43] 这样的分类分级制度旨在实现既实现维护数据安全,同时又可以实现数据的充分合理流动、从而促进数字经济的目的。但是,对于可能包含海量信息并且难以被人工处理的数据而言,分类分级制度在实践中至少存在如下两个方面障碍:一是标准过于抽象和僵化。重要数据按照行业划分很难体现其“重要性”,只能从维护国家安全的高度,按照数据的重要程度进行分级。这导致在实践中很难将数据分类分级的标准进行具体化,只能以笼统的“重要程度 + 危害程度”的手段来界定数据分类分级的标准,而且需要适时进行更新。[44] 二是难以发现数据的深层价值。数据的价值并不仅仅表现在数据表面,有的存在于数据的深层联系之中,只有通过算法才能发现其潜在价值,比如通过交通数据来判断国家机关的可能行为。[45] 算法成为数据挖掘的不可缺少的工具,可以分析处理海量数据的算法模型使数据的价值得以放大。而且,随着机器学习(machine learning)能力的精进,大数据在各个领域的表现越发出众。[46] 在没有算法介入的情况下,数据的价值很难被挖掘出来。因此,仅仅以数据本身的性质、行业和数量大小来决定数据的重要程度难以完全符合数据价值认定的内在要求。甚至内容公开的数据集合满足何种条件才能获得法律保护,依然是一个悬而未决的问题。[47]

2. 数据安全的个人信息数量标准。《网络数据安全管理条例(征求意见稿)》与《数据出境安全评估办法》都将“一百万”作为衡量标准的做法,或许在当下还可以作为一种权宜之计,但是从数字经济的长远发展来看,其不足是显而易见的:首先,“一百万人以上个人信息”仅仅是人数的限定,而对信息的性质没有规定任何标准,比如“一百万人以上个人的公开信息”是否属于重要数据? 其次,“处理一百万人以上个人信息的数据处理者向境外提供个人信息”,是对于

㊷ 王春晖:《数据安全出境评估规则与适用——〈数据出境安全评估办法〉解读》,载《南京邮电大学学报(社会科学版)》2022 年第 4 期。

㊸ 参见《网络数据安全管理条例(征求意见稿)》第 5 条。

㊹ 参见王春晖:《我国数据安全法十大亮点解析》,载《中国电信业》2021 年第 9 期。

㊺ 参见《滴滴知道哪个部委加班最多:互联网数据,为何关乎国家安全?》,https://www.163.com/dy/article/GECJ5VDN0511MKLQ.html,访问日期:2023 年 2 月 6 日。

㊻ 参见[英]阿里尔·扎拉奇、[美]莫里斯·E. 斯图克:《算法的陷阱:超级平台、算法垄断与场景欺骗》,余潇译,中信出版集团有限公司 2018 年版,第 23 页。

㊼ 崔国斌:《公开数据集合法律保护的客体要件》,载《知识产权》2022 年第 4 期。

信息处理者在主体条件上的限定，至于该数据处理者向境外提供多少条信息，则在所不问。那么，符合条件的数据处理者向境外提供一条个人信息，哪怕是公开信息，也需要经过国家网信部门组织的数据出境安全评估。这样必然导致一些正常跨境信息处理业务难以开展。从根本上来说，个人数据的安全意义，不仅仅在于涉及人数的多少，还在于信息的类型和内容，但是如果以信息的类型和内容作为评价个人数据安全的标准，则进入信息安全的领域，信息安全大都有专门法律规范，比如个人信息保护法，从而使数据安全法角度的安全评估实际上难以落地。

无论是数据分类分级保护制度，还是个人数据的信息数量标准，存在上述问题的根本原因在于：将数据视为信息的简单集合来进行安全评价，忽略了数据（集合）在所记录具体信息的价值之外所具有的独立安全价值，即与具体信息没有因果关系的安全价值，比如上文提到的气象数据隐含的粮食安全价值、交通数据所隐含的国家安全价值。因此，对于集合意义上的数据而言，数据安全的关键问题是：如何保护数据集合所隐藏的、超出具体信息的安全价值。

数据与信息的差异似乎是解决这个问题的逻辑出发点：数据既是个体概念，也是集合概念，数据的集合概念可以分为数据项、数据集两个更常用的概念。[48] 但是，从信息保护的角度来看，一般是保护特定信息，尤其是对于个人信息的保护，即使对于侵犯多人的信息，也不会按照数据侵权或者数据犯罪对待。比如《最高人民法院、最高人民检察院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》对于侵犯公民个人信息犯罪活动的入罪和量刑，均以侵犯的公民信息的数量为主要参考标准。[49] 法律对于数据的保护，应当注重保护数据隐藏的信息价值，不应当只看数据中的信息数量。即使在对国家安全可能产生严重影响的政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等领域，数据本身也未必直接将其重要性显示出来，算法所呈现的结果与数据表面所呈现的危险系数并不密切相关，从而可能导致数据安全保护过松或者过严的问题。这解释了对于非个人信息的数据，即使不属于国家秘密，也可能需要进行保护的基本逻辑；也回答了为何对于个人数据的安全审查，应当与个人信息保护的安全审查区别对待。

算法越来越成为数据处理的主要方式，仅仅通过对数据所包含的信息内容来评估数据的安全价值，显然难以胜任了。当然算法本身也存在风险因素，算法的设计不当可能导致对于数据安全意义评价的错误。事实上，随着数据安全治理的不断细化，其治理范围不断向算法安全治理迈进并深化。[50] 这恰恰从另一个角度印证了数据安全的相对性，即对于数据风险的控制无法实现绝对化，除非放弃风险背后所隐藏的机会与价值。

㊽ 《网络安全标准实践指南——网络数据分类分级指引》第2.1条规定：网络数据简称数据，是指任何以电子方式对信息的记录。注：数据分类分级的对象通常是数据项、数据集。数据项是数据库表的某一列字段。数据集是由多个数据项组成的集合，如数据库表、数据文件等。

㊾ 参见《最高人民法院、最高人民检察院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》（法释〔2017〕10号）第5条。

㊿ 马海群、张涛：《我国数据与算法安全治理：特征及对策》，https://kns.cnki.net/kcms/detail//11.5181.TP.20221213.2211.014.html，访问日期：2022年12月27日。

（二）具有可适用于算法的集合性

电子数据是信息技术发展到一定阶段的产物，并随着数据的爆发式增长催生了“大数据”等数据集合的概念。算法是用于一定规模数据处理的工具，而非用于直接处理具体信息内容。与此相对应的是，数据安全应当是适应算法的规模数据的安全，而非个体性数据（信息）的安全。《数据安全出境评估办法》将“一定数量”作为个人信息出境评估的条件，说明其（数据安全）理论基础在于总体风险。[51] 尽管《数据安全法》将数据的概念规定为“任何”以电子或者其他方式对信息的记录，但是从实际上看，由于非电子方式的数据安全往往可以由信息保护来完成，因此数据安全应当是指电子数据的安全。尽管目前还不能完全排除人工处理数据的做法，但是算法已经成为处理数据行为的主要工具。从数字社会的发展来看，数据安全与算法安全是伴随始终的命题，数据与算法具有密切联系，数据是算法的重要支撑，应当加强数据与算法安全协同治理。[52] 显然，适应算法处理的数据是集合意义上的数据，而不是具体信息的数据。对于具体信息的数据，已经有相应的制度安排：对于没有保护价值的数据无需法律规范，对于具有保护价值的信息已有相应的法律规范予以保护。比如，个人信息、商业秘密、国家秘密等有重要价值信息的数据处理活动，分别适用个人信息保护法等法律法规。只在数据意义上处理这些有价值的信息，而不问其内容，才属于《数据安全法》的调整对象。

当然，算法并不是数据处理的全部工具。人工对于数据进行直接处理在未来很长一段时间内仍会存在。不管是人工处理数据，还是算法处理数据，都区别于处理具体信息。算法作为数据处理的主要方式和发展方向，只是能够将数据安全客体的规模性彰显出来而已。

五、结论

数据安全客体的确定不仅关系到数据安全制度的实施，也关系到网络安全法、数据安全法、个人信息保护法及相关法规、司法解释之间的条理性。数据安全客体的复杂性决不是一个可以被低估的问题，因为数据本身就意味着需要挖掘、需要算法介入，从而形成一种动态的评估对象，不可能用一种固定标准来划定数据安全客体的具体范围。本文从数据的价值实现、数据安全的独立价值、数据安全保护机制及数据的利用方式等四个方面对于数据安全的客体进行了分析，认为数据安全的客体应当是：动态开发利用中的数据、电子记录信息方式的数据、“风险—控制”安全管理意义上的数据、适用算法处理的集合性数据，从而区别于信息、网络、个人信息等与数据相互关联的其他法律关系客体。

对于数据安全客体在四个维度上的界定，应当在实践中综合运用，单凭某一方面的特征可能仍然难以准确判断。在实践中数据与信息等概念的交叉混同使用可能还会持续相当长的时间。在一些特定场景可能仍然难以区分数据与信息的客体地位，比如数据收集与信息收集，由于都存在数量小、个体性强的特点，用上述四个维度的界定标准未必能够分辨出属于数据安全还是信息保护的规范对象。笔者认为，对于这种特殊情况，一般应当按照信息保护进行处理，

---

[51] 参见丁晓东：《数据跨境流动的法理反思与制度重构》，载《行政法学研究》2023 年第 1 期。

[52] 马海群、张涛：《我国数据与算法安全治理：特征及对策》，https://kns.cnki.net/kcms/detail//11.5181.TP.20221213.2211.014.html，访问日期：2022 年 12 月 28 日。

因为,数据是信息的记录方式,从信息实体内容上进行保护,能够覆盖数据保护的范围与效果,除非有证据证明不涉及信息的具体内容。但无论适用何种规范,均需要避免重复法律适用。这个逻辑可以推演到对于所有非集合性数据的安全法益保护,即通过已有的信息保护规则来保障其“有效保护和合法利用”的状态。这种法律规范的系统性及清晰的相互关系,对于推进网络法治、促进数字经济、建设数字中国的意义是不言而喻的。

随着数据技术的进一步发展,需进一步重视算法适用对于确定数据安全客体的重要性。对数据安全的保护,不应局限于数据本身,还需要进一步考虑到数据对于人工智能的影响。相关法律制度对于数据的规制,也就从数据安全进一步推进到算法安全。[53] 数据安全与算法安全的协调推进,一方面意味着数据安全客体的更具有动态性,另一方面也说明了判断标准的复杂性,过严会危害数据合理流动,过松则不利于数据安全的有效保护。因此,落实《数据安全法》第22条规定的“国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制”,仍然任重而道远。在数字社会发展过程中,数据安全将伴随始终,从开始阶段就对数据安全客体形成清晰的认识,无疑具有重要意义。

On the Object of Data Security

Fan Mingzhi

Abstract: Data security, network security, personal information protection and other legal systems are interrelated, and the concepts of data, information, security and protection and other legal concepts are mixed, resulting in the unclear scope of data security objects. From the four dimensions of data value realization, independence of data security, data security protection mechanism and data utilization, it can be distinguished that data security objects should be: data in dynamic development and utilization, data in electronic records, data in the sense of “risk control” social security management, and collective data processed by applicable algorithms. In the legislative, law enforcement and judicial activities related to data, the object of data security should be clearly identified, so as to implement the data security system and promote the healthy development of the digital economy.

Keywords: data security; object; algorithm; digital economy

(责任编辑:杨志航)

---

[53] 参见杨蓉:《从信息安全、数据安全到算法安全——总体国家安全观视角下的网络法律治理》,载《法学评论》2021年第1期。