数据价值演变下的个人信息保护：反思与重构

方　禹

摘　要：数据认识的问题对个人信息保护制度的构建十分关键。通过模型构建的方式，以数据价值如何释放为切入点，构建三个层次数据的理论模型。利用框架模型，分析发现不同类型数据所可能产生的价值、存在的问题与规范期望之间的冲突点。对比认知期望和规范期望，解释实践中出现的有关个人信息保护问题的认识偏差。阐述不同层次数据的特点，以及实践中不同层次数据的交叉性，提出解决认识偏差的思路。以三层数据的理论模型为视角，分析个人信息保护的思路、个人信息的界定、个人信息保护的具体制度等所可能存在的障碍，提炼得出初步结论。

关键词：个人信息保护；大数据；数据治理；单一数据

［中图分类号］D912.8　　［文献识别码］A　　［文章编号］2096-6180（2020）06-0095-16

引言

在社会信息化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。[1] 个人信息保护立法受到广泛关注，各方利益诉求十分强烈和迫切。2020 年 7 月 3 日，全国人大常委会审议了《中华人民共和国数据安全法（草案）》，规定了数据分类、安全保障义务等内容。2020 年 10 月 14 日，全国人大常委会审议了《中华人民共和国个人信息保护法（草案）》，回应了监管机构、权益设置、主体义务、法律责任等个人信息保护立法的主要元素，同时也在“单独同意”、审计等方面作出了制度创新。然而，草案能否承受各方高度关注之重，仍有待进一步观察。实际上，数据、个人数据、信息、个人信息、大数据等概念的交织，使得本身极具复杂性的个人信息保护和数据安全问题，在学界、产业界和普通民众的聚光灯之下，面临更广泛、更深刻的法益协调和平衡工作。如何认识数据并形成有效的规制思路，需要框定视角并通过模型建构的方式，来分析具体存在的利益博弈和真实矛盾，以准确把握通过立法所需要真正调整的法律关系。

［作者简介］方禹，中国信息通信研究院互联网法律研究中心主任。

〔1〕 参见全国人大法工委：《关于〈中华人民共和国个人信息保护法（草案）〉的说明》，https://www.thepaper.cn/newsDetail_forward_9665985，最后访问时间：2020 年 10 月 21 日。

一、数据价值视角下的数据类型划分

（一）数据治理

研究数据治理首先要搞清楚“数据”和“治理”这两个概念，其研究成果十分丰富，基本能够形成一致的认识。对于数据，梅夏英对数据和信息进行了深入的对比，从而使人们对数据有了一个清晰的认识。[2] 对于治理，一般是相对于管理而言，最明显的区别体现在参与方的数量和参与的程度上。治理过程中，参与主体更为广泛，主体能动性发挥的空间也更广。治理概念的提出，源于行政监管能力与被监管对象的力量对比发生了逆转，单一的行政力量不足以应对强大的被监管对象。根据“全球治理委员会”的定义：治理是个人和制度、公共和私营部门管理其共同事务的各种方法的综合。它是一个持续的过程，其中，冲突或多元利益能够相互调适并能采取合作行动，它既包括正式的制度安排也包括非正式的制度安排。[3] 治理与管理最明显的区别就是参与主体的数量和程度的差异。管理过程当中，以监管为中心，实施监管活动，被监管方处于被动地位。治理过程当中，仍然以监管为中心，但是参与主体不仅包括被监管方，还进一步延伸到行业和个体，多元主体参与治理活动，发挥各自的作用。管理活动适合比较简单、清晰的社会关系调整，以威权式、命令式手段可以达到预期效果。治理活动适合复杂、动态的社会关系调整，仅仅依靠威权式、命令式手段可能达不到预期效果，复杂的社会关系牵涉多方利益，这种利益交织在同一场景下可能此消彼长，调整这类社会关系以利益平衡为目标，而非只追求单一、纯粹的利益。同时，这类社会关系在不同场景之间异化性较强，不宜实施机械、单一的管理要求。治理活动中，选择或者创设有效的法律制度，是实现治理目标的关键。

人们对“数据”和“治理”的认识和理解基本趋于一致，有关争论实际上是对于如何治理的具体规则和具体制度选择层面的认识存在差异，而反诸“数据”和“治理”概念本身来寻求解决方案。数据治理问题的解决，需要进一步通过外部环境的适配，来探寻数据治理规则建立的应然性要求。数据治理的问题包括三个方面：数据价值、数据安全和用户保护。数据价值表现为多个维度，包括经济价值和非经济价值，也包括短期价值和长期价值，还包括局部价值和全局价值。数据价值的释放是数据治理的最终目的，价值释放的过程中所带来的数据安全问题，是立法和行政监管应予以解决的。在确保数据安全的前提下，应该尽量多地释放数据价值。广义上的数据安全包括个人信息保护[4] 问题，但是个人信息保护加入了用户权利的考量因素。对数据价值和数据安全进行成本收益分析时，若增加用户保护的考量，则会影响分析结果。

---

〔2〕 梅夏英：《数据的法律属性及其民法定位》，《中国社会科学》2016 年第 9 期，第 164－183、209 页。

〔3〕 *See* Commission on Global Governance，*Our Global Neighborhood*，http://www.gdrc.org/u-gov/global-neighbourhood/（last visited Apr. 27，2020）.

〔4〕 本文不区分个人数据和个人信息，根据行文方便，混合使用。

（二）技术变迁背景下的数据价值体现

数据能产生什么价值？这是分析问题的前提，只有明晰了数据价值的具体所在以及与之伴随而出现了何种问题，才能帮助厘清所需要采取的制度设计。数据的价值主要包括经济价值和非经济价值。经济价值是能产生经济效益的价值，包括直接经济价值和间接经济价值。从当前数据应用情况来看，能够产生直接经济价值少，而间接经济价值体现的则比较明显，比如利用数据所实现的精准营销、市场分析等。非经济价值主要体现于数据所具备的情报功能、预测功能，即通过数据来反映或者推断某种事实。涂子沛认为，数据产生利润的方式目前只有两种：广告和信用。[5]《数字经济与数字治理白皮书（2017）》中指出数字经济可以实现五个方面的红利：（1）重构商业模式；（2）提升劳动生产率；（3）促进产业升级；（4）推动万众创业；（5）创造就业能力。[6] 张新宝认为，个人信息商业价值的发掘与商业运作尤其是营销模式的改变有重大关联。[7] 程实认为，数字经济可以通过不同渠道降低经济活动成本，也在不同层面影响着经济主体和对应福利，数字经济可以降低五个方面的成本：（1）降低搜寻成本；（2）降低复制成本；（3）降低交通成本；（4）降低追踪成本；（5）降低验证成本。[8] Paul B.C.van Erp 等认为基于交通数据的分析，能够对交通状况进行预测 [9]，体现的就是一种预测价值。张芳认为大数据能够在电商活动中产生精准营销价值。[10] 张启贤认为，大数据在金融领域应用，可以提高银行业管理效率及降低银行违约风险，可以促进证券行业信息化程度的提升，可以提升保险业对相关新型产品和保险产品的风险评估，还可以通过数据监控有效防止互联网、金融、企业和相关领域出现诈骗、洗钱等风险问题的发生 [11]，这体现的是情报价值。刘姝认为，通过大数据发挥数据库的价值，基于用户的需求和习惯实现精准投放 [12]，这体现的是营销价值。Wilson J 等认为，数据的价值不仅是经济价值，也有非经济的价值，其通过医疗大数据应用归纳出提升公民生活水平的公共价值。[13] 数据的价值体现了多元认知，如经济价值、营销价值、情报价值、预测价值等。无论是何种价值，其所关注的是基于数据所形成的事实——已知的事实和未来的事实。这种事实的形成，取决于数据应用的技术能力。针

〔5〕 涂子沛：《数文明》，中信出版集团 2018 年版，第 36 页。

〔6〕 中国行政体制改革研究会、中国信息通信研究院互联网法律研究中心、国家信息中心、华为技术有限公司、腾讯研究院联合研究课题组：《数字经济与数字治理白皮书（2017）》，第 9－13 页。

〔7〕 张新宝：《从隐私到个人信息利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期，第 38－59 页。

〔8〕 程实：《数据要素的经济价值》，http://finance.sina.com.cn/zl/bank/2020－04－20/zl-iirczymi7294364.shtml，最后访问时间：2020 年 4 月 27 日。

〔9〕Paul B.C.van Erp Victor L.Knoop Serge P. Hoogendoorn, *On the Value of Relative Flow Data*，113 TRANSPORTATION RESEARCH PART C: EMERGING TECHNOLOGIES 74，74－90（2020）.

〔10〕 张芳：《大数据精准营销在电商领域的应用与价值略述》，《中国市场》2020 年第 12 期，第 159－160 页。

〔11〕 张启贤：《基于互联网金融的大数据应用模式及价值探析》，《网络安全技术与应用》2020 年第 4 期，第 149－150 页。

〔12〕 刘姝：《运用大数据思维盘活“小数据”价值——浅析皮书数据库的大数据应用尝试》，《出版广角》2020 年第 6 期，第 41－43 页。

〔13〕Wilson J，Herron D，Nachev P，McNally N，Williams B，Rees G，*The Value of Data: Applying a Public Value Model to the English National Health Service*，JOURNAL OF MEDICAL INTERNET RESEARCH（2020）.

对同样的数据样本，不同的技术能力所形成的事实也不相同。有必要认识不同的数据技术能力所对应的风险和收益，进而通过成本分析的方法得出一些结论。

（三）三种层面的数据类型划分

根据技术发展和应用程度，可以将数据分为单一数据层面的数据、统计层面的数据和大数据层面的数据。本文简称为单一数据、统计数据和大数据。[14] 三种层面数据的变化体现了数据价值的演变，从个体到群体，从量变到质变。理解三种层面数据的内涵，是后文论述的基础。

单一数据即个体（包括人和物）所产生的数据，其数据类型单一，比如某个自然人的姓名、身份证号码等，或者某个机器设备、零部件的型号、状态信息等。由于信息化技术水平不够，无法实现单一数据的汇集，使得数据处于分散、碎片化的状态。比如，在智慧交通兴起和发展以前，各个路口的红绿灯数据是单一的，分散且碎片化的，不能形成数据汇集。单一数据的价值极低，甚至没有价值。自然人所产生的单一个人信息几乎没有什么价值，只有规模化的个人信息集合才能产生相应的价值。但是对单一数据的滥用会产生个人信息权益受损的问题，我们大多数有关个人信息保护的讨论中，所针对的其实是单一数据。比如徐玉玉案件中，由于徐玉玉相关个人信息的泄露，造成了其财产、人身的伤害，而这种危害后果是基于徐玉玉本人的单一数据所发生的。个人信息保护相关法律规定所规范的个人数据也基本是围绕单一数据所设计的。更为直观地理解单一数据，还可以以人肉搜索为例。人肉搜索针对的是单一数据，通过分散于网络的、有关某个具体自然人碎片信息的大规模收集和整理，从而具体化拼凑出该自然人的身份信息。人肉搜索过程中，虽然也有大量信息被收集，但是从属性上看，所有的信息明确指向单个自然人，所以也应该被视为单一数据。从法益上来看，对单一数据的不当处理，可能会引发侵犯隐私权的风险，但未必会引发个人信息保护的问题。此外，数据跨境执法实际上也是单一数据层面的问题，比如美国联邦调查局（FBI）要求调取微软存储于爱尔兰服务器中数据的案件，对国家安全、数据安全层面造成负面影响。

统计数据是单一数据的汇集，比如身份证号码的列表等，典型表现形式就是数据库，其特点是同一类型或者简单多种类型的数据集合。虽然数据量可以非常大，但是数据种类相对单一、固定，只能挖掘出统计事实。通过统计数据能够得出统计结论，比如总量、均值等。零售商可以基于同期销售情况的统计数据，来进行进货量的决策。这种数据应用依赖于信息化手段，但尚未达到大数据的技术水平。比如，前述智慧交通的例子中，利用技术手段汇集城市各个路口的红绿灯数据，再加以分析，得出有关拥堵的交通信息，就是统计数据的应用。利用手机信令数据分析城市人口的时空分布[15]，也是一种统计数据的应用，但这些都不是大数据应用。因为这种分析还是基于同种类型的数据（手机信令）的汇集，即便数据量足够大，也只是统计数据的层面。大数据的核心不在于数据量级之大，而是能够对多类型、多维度的数据进行分析，反过来说分析基础也

〔14〕 大数据应为一项技术，为方便行文，本文作为数据形式的一种来表述。

〔15〕 海晓东、刘云舒、赵鹏军、张辉：《基于手机信令数据的特大城市人口时空分布及其社会经济属性估测——以北京市为例》，《北京大学学报（自然科学版）》2020 年第 4 期，第 518－530 页。

必须基于多类型、多维度的数据。统计数据能够进行因果分析，而大数据技术能够发现数据与数据之间的相关性。如果能够通过信令数据、就业数据、交通数据等进行分析，得出未来房价或是生育率等走向趋势，就比较符合大数据的要义——通过寻找海量数据之间的相关性来获得预测结果。统计数据附加了人类劳动，其价值大于单一数据，最主要的体现是情报价值。利用统计数据，一般可以作预测分析，但是直接经济价值的释放并不明显。所以，单一数据与统计数据之间的冲突并不明显。统计数据仅仅增加了单一数据的数量累计，而没有发生质变的效果。从法感情的角度说，用户倾向于认为统计数据放大了风险。而统计数据也确实明显体现出侵犯用户权利的现象，比如骚扰电话、垃圾短信、电信诈骗等都是基于统计数据而得以实现的。

大数据是最容易被误解的。其本质上是一种技术手段，而不是一种数据，特点是通过海量数据，结合算法等技术手段，得出相关结论。大数据对数据资源的要求非常高，一般认为包括 5 个 V，即数据量大（volume）、速度快（velocity）、类型多（variety）、价值（value）、真实性（veracity）。大数据的“大”是指海量数据，既包括数据量大，也包括数据类型的丰富。大数据要分析与某事物相关的所有数据，而不是依靠分析少量的数据样本。[16] 大数据要求的是混杂性，而非精确性[17]，有观点指出，即使数据再不良，理论上也可以通过算力来弥补。[18] 利用因果关系获取事实与利用相关关系获取事实，是大数据与统计数据最关键的区别。西医诊断以数据的因果性为基础，通过对应的检查数据来确定病因和诊疗方案，比如血液白细胞上升，就意味着存在炎症。而中医则不局限于因果性，通过“望闻问切”四诊法寻求的是数据的混杂性、多样性，进而依据多种数据进行综合判断，而这种判断不是以因果性为基础的，而是以相关性为基础的，是阴阳平衡，而不是单一的“药到病除”。中医诊治很难通过临床医学进行验证，因为相关关系的验证通过因果分析很难奏效。通过大数据分析得出的结果能够远超过统计数据的简单分析，因此利用大数据能够大幅度增加数据价值的释放，传统数据所具备的经济价值在大数据运用中释放得更为充分，甚至往往能超过预期，间接经济价值效果更加明显。大数据对海量数据、类型丰富的需求使得数据交易市场基础得以充实，也能激发直接经济价值的产生。周涛认为，进入大数据 3.0 版本后，将产生数据运营商和数据客（dacker），个人、团队和企业可以在已有数据的基础上进行数据分析、加工和挖掘，数据市场进而产生。[19] 大数据能够释放的间接经济价值在商业营销方面十分明显，利用大数据进行的个性化推荐能够提高效率、降低成本。大数据同样放大了传统的安全问题，跨境数据流动的安全问题就是在大数据的语境下产生的。大数据对隐私保护的挑战非常严峻，从而衍生出个人信息保护问题。一般而言，大数据应用于宏观层面，但是微观层面同样存在大数据的应用，或者大数据原理的技术方式。比如，用户画像就是一种微观环境中的大数据。用户画像所得出的

〔16〕［英］维克托·迈尔－舍恩伯格、肯尼思·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 29 页。

〔17〕［英］维克托·迈尔－舍恩伯格、肯尼思·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 46－61 页。

〔18〕 周俊：《数据价值化探讨》，《电信技术》2019 年第 12 期，第 94、98 页。

〔19〕 周涛：《大数据 1.0 版本，2.0 版本和 3.0 版本 颠覆性变化下的商业革命》，《人民论坛》2013 年第 15 期，第 24－25 页。

结论与用户的个人数据之间未必形成因果关系，大多数情况下是相关关系。收集用户的个人数据越多，所能形成的用户画像就越准确。这些个人数据之间的相关关系的发现，是人类智力所不能达到的，通过算法的分析，找到相关关系，从而给出匹配结果，可以看作是一种大数据技术的应用。

（四）基于三层数据划分所认识的偏差

数据治理以大数据为背景，但大数据技术并未充分普及，成熟度也不够。很多研究和讨论是在统计数据的基础上展开的，从而很难得出准确的结论。杭州互联网法院在“微信数据权益”案中认为，平台数据“可以分为两种数据形态：一是数据资源整体，二是单一数据个体。网络平台方对于数据资源整体与单一数据个体所享有的是不同的数据权益”。区分单一数据、统计数据和大数据后，可以简单地用成本收益的方法进行分析，对比数据价值的释放和数据安全问题的产生，能够粗略归纳出一些结论。单一数据的成本远大于收益（价值小而风险大），因此对单一数据的规制力度较强。统计数据的成本与收益大致相当（价值明显而风险也明显），因此对统计数据的规制力度适中。大数据的成本远小于收益（价值非常明显而风险并不具化），因此对大数据的规制还不明确，或者说执行并不到位。比如说，跨境数据流动问题的产生，应该是大数据层面的担忧。由于大数据可以通过海量数据分析得出有价值的情报，所以各种类型的数据出境后一旦被大数据分析，可能对国家安全形成负面影响，因此需要对整体跨境数据流动进行一致性的限制。相反，如果是基于统计数据的担忧，只需要对特定领域、特定类型的数据作出跨境限制。我们有关数据安全问题的讨论，如果针对的是大数据，那么究竟有何种现实的威胁，还缺少具象化的论证，也缺少具体数据和案例的佐证。大多数担心的安全问题是基于想象而产生的。比如，大数据层面的跨境数据流动，能够产生什么样的风险，并没有现实的、具体的案例予以佐证。“棱镜门”事件的曝光，一度引发国际层面对数据安全问题的担忧。“棱镜门”事件所涉及的数据其实是在统计数据的层面——通信数据的集合，以及单一数据层面——对特定对象通话内容的直接侦听。很多国家对于跨境数据管理针对的是个人数据，比如欧盟《通用数据保护条例》（GDPR）的规定，防止的是个人数据的外流，其目的是保护个人基本权利。如果出于大数据层面的担忧，应该禁止或者限制所有类型数据的出境，以避免多类型、大数量的数据外流后，被大数据技术分析出不利于国家安全的情报。[20]

按照三层数据进行分析，可以为如今数据治理中出现的一些困境找到逻辑基础。数据治理问题的一些难点实际上是应对不同层面的数据所产生的。正确认识和理解这些困境，才能准确地发现问题，作出科学合理的制度安排。

个人信息保护问题的争议之所以产生，是因为诸多个人信息保护制度构建，是以单一数据为对象的，避免的是单一数据的负外部性。这也是为什么以欧盟为代表的个人数据保护法规，都是

〔20〕实际上，采取强硬的数据本地化政策也未必能应对大数据威胁。有关大数据分析可以在当地进行，再将结论传输境外，而不需要传输数据本身。

以个人基本权利的保护为基础的。这在很大程度上是为了规避单一数据负外部性的数据安全问题。然而，个人数据的价值释放是以统计数据、大数据为基础的，特别是大数据。比如，前述用户画像的例子，微观层面对个人数据的价值挖掘是基于大数据技术所实现的。大数据的特点是对数据类型、数量的高度需求，数据越多、越丰富，越能释放价值。这一点与个人信息保护的最小化原则、必要原则等相冲突。从技术特点来看，统计数据、大数据并不关注具体自然人的身份信息——虽然大数据技术能够比较容易地确定自然人身份，但这并非运用大数据技术的目的，也并非商业模式之基础。这一点又与个人信息保护以能够识别自然人身份的信息为调整范围有冲突。个人信息保护中，数据价值和数据安全所规范的数据并非同一层次的数据，因此而产生的矛盾很难调和。在这一点上认识不清，就很难形成共识和定论。

数据流通之所以难以形成规模，也是同样的原因。数据流通应当以大数据为基础，而目前大数据技术的应用和普及尚不成熟。除了超大型互联网平台，企业与企业之间的数据需求主要还是统计数据层面的。统计数据的类型化很强，需要确定类型数据的量化集合。买卖双方存在博弈，需要满足双重偶然性，才能形成交易。统计数据的技术不能发现相关性，数据需求基于因果关系而产生，因此数据需求类型非常固定，价值体现十分具化。有价值的数据卖方不想卖，无价值的数据买方不想买，这种价值仅仅体现于简单的情报价值，或者能够直接服务于买方的业务模式，因此数据交易只能发生在同业竞争者之间，而双方由于竞争关系的存在，往往缺乏交易动能。现在对数据交易的促进主要是在“需求量”上求解，而忽视了“需求”本身并不存在——认为问题是交易量不够，进而忽视了交易需求本身是否存在。对于大数据而言，情况就大为不同，因为大数据的需求是各种类型的海量数据，数据类型化的需求并不强烈。数据交易的基础能够广泛达成。举一个简单的废品回收利用的例子，可以更形象地说明这个问题。利用不同的技术手段，对废品回收利用的市场需求会发生较大的变化。假定某企业需要回收盛装可乐的易拉罐，如果技术水平较低，需要回收的是形状相同、材质相同、容量相同的易拉罐，进而清洗处理后再次利用。这时企业回收所需要的易拉罐类型非常固定，必须符合双重偶然性，交易才能发生。如果技术水平提高，企业通过熔化重塑的技术可以制造新的易拉罐，那么企业回收需求就仅限于材质，比如必须是铁器或者铝器等，但是对于形状、容量等就没有要求了。这时交易的双重偶然性大大提升，交易市场形成的可能性变得很高。假如能够成熟地运用 3D 打印技术，那么材质的限制也可以打破，企业回收任意材质的废品，都可以通过 3D 打印制成易拉罐，那么连双重偶然性的交易基础都不再需要。交易的可能性几乎普遍存在，交易双方很容易达成一致，从而能够广泛地形成交易。通过这个案例的假设，可以分析数据流通的实际障碍，并非绝对地是由于数据权属不清所造成的。如果大数据技术得不到充分普及，数据交易就难以形成市场规模。正如同 3D 打印技术不够成熟和普及，在一定程度上限制了废品回收的市场规模。

公共数据资源开放的重要性受到各方关注，也从另一角度佐证了我们正面临的是统计数据的问题，而非大数据的问题。正是因为受目前的技术水平限制，导致数据需求停留在统计数据层面，

数据本身的价值就尤为重要（能够建立因果关系）。不难理解，统计数据中最具价值的数据由政府部门、公共机构等所掌握。根据前述分析，这类数据的交易基础、流通基础广泛存在，相关行业、相关领域对这类数据的需求十分明确，很容易通过主管部门的划分找到对应的数据资源。然而，如果大数据技术足够成熟，数据分析能力持续提高，对数据资源的特定化、类型化的要求降低，可能同时也会使得公共数据资源开放的需求相应下降。

二、多层面数据交织中的个人信息保护制度偏差

（一）小引

个人信息保护问题复杂且具有争议，个人信息保护既可以通过民法予以保护，也可以通过行政法予以保护，还可以通过刑法予以保护。高富平认为，基于不同的保护目的，可能构建出不同的法律制度。〔21〕实践中，不同背景、不同主体、不同场景〔22〕的变化，都会出现个人信息理解的偏差，影响个人信息保护规则的实施效果，甚至发生个人信息保护规则失灵的后果。比如，“知情同意”规则在人工智能中应用于无人驾驶领域，就导致有效同意难以实现。

这些差异化实际上就是不同层面数据的交织，在个人信息保护问题中的体现。目前，主流观点对于个人信息的定义，其实属于单一数据层面。如果说个人信息保护制度的目标就是保障用户权利，那么现在的制度设计无可厚非。但是，无论国内还是国外，都十分强调安全与发展的平衡。个人信息保护领域同样如此，GDPR 虽然强调对个人数据进行基本权利的保护，但是在其前言中还是认识到技术发展、经济发展的重要性。如果以平衡安全和发展为目标，对个人数据保护的单一数据层面和个人数据价值释放的统计数据或大数据层面，就存在强不兼容性。制度设计应该以此为前提而展开，才有可能形成较为科学、合理的制度安排。

（二）个人信息再界定

个人信息保护最底层的逻辑不自洽就是对个人信息定义的理解。目前，个人信息的定义主要有两种方式：（1）识别论；（2）关联论。无论采取何种方式，个人信息的定义都有过宽之嫌。笔者此前已撰文阐述。通过单一数据、统计数据和大数据的理解框架，我们可以进一步发现个人信息定义的问题所在。立法中对个人信息的定义针对的是单一数据，这是基于用户保护的角度。而数据价值的释放是以统计数据为基础，甚至是以大数据为基础的。从统计数据、大数据的视角看个人信息保护问题，对个人信息定义的理解，会发生很大的变化。前述人肉搜索的例子中，有关自然人的数据是分散、碎片化的，通过整合而具备了识别自然人身份的效果，这是通过统计数据层面实现的。前述用户画像的例子中，有关自然人的数据是“海量”的、丰富的，通过算法（大数据技术）形成了用户画像。这些数据如果分别置于单一数据层面，都是不能识别自然人身份的。

〔21〕 高富平：《论个人信息保护的目的——以个人信息保护法益区分为核心》，《法商研究》2019 年第 1 期，第 93－104 页。

〔22〕 Helen Nissenbaum，*Respecting Context to Protect Privacy: Why Meaning Matters*，24 SCIENCE AND ENGINEERING ETHICS 831，831－852（2018）.

放置于统计数据层面，问题就会产生，比如“步态识别”技术，就可以通过步态分析来达到身份识别的目的。[23] 按照通行个人信息定义的理解，步态也应当作为个人信息的类型予以保护。放置于大数据层面，问题更为突出，个人信息的定义强调的是因果关系，而大数据并不以因果关系为前提，通过相关关系就能分析出结果，比如微观层面的大数据——用户画像。那么个人信息的范围还将变得更宽，甚至是无穷大。程啸认为，个人信息保护的范围越来越广，甚至在许多情况下，连界定哪些信息属于个人信息都存在困难。[24] 我们可能还无法想象未来通过何种数据能够识别自然人身份。由此可以发现，问题的症结在于，我们所期待保护的是单一数据层面，以此对个人信息进行界定，同时也制约了统计数据，特别是大数据的形成，用户保护和数据价值相冲突，且难以调和。

个人信息保护的出发点是单一数据层面，防止个人身份被不当识别。但是，统计数据、大数据层面并不一定要识别自然人身份，甚至有些信息并不能识别自然人身份。比如，新冠疫情期间这一问题就十分突出。应对迅速蔓延的疫情，只有及时、准确掌握疫情相关人员信息，才能迅速采取针对性的措施，避免疫情的进一步扩散。对此，有必要采取技术手段，确定密切接触人员的范围。确定的目的是能够将密切接触的信息通知到个人，并进一步采取相关措施。这一技术手段并非要识别自然人身份，而是建立联系渠道。有可能通过技术机制取得的仅仅是某个人的手机号码，而并未获取这个人的身份。当然，如果说手机号码不是个人信息，可能不符合大众认识。更进一步来举个例子，为了确认密切接触人群，安卓系统（Android）和苹果系统（IOS）所开发的蓝牙追踪技术，也引发了个人信息保护的担忧。从法律层面看，假设用户 A 被确诊，通过该蓝牙技术可以追踪到用户 B、C、D 等，通过用户 A 从用户 B、C、D 处所收集的信息是否属于个人信息？需要用户 B、C、D 的同意吗？当用户 A 被确诊时，他所掌握的与用户 B、C、D 的接触信息就会被上传到疫情防控机构，此时是否构成了一项个人信息转移行为，这种转移是否需要取得用户 B、C、D 的同意？如果答案都是肯定的，这种机制能否覆盖平时的情况？例如当我们使用有些 App 时，需要上传手机通讯录，此时 App 所征求的是手机所有人的同意。但是，通讯录中的联系人信息并不属于手机所有人，而是对应联系人的个人信息。这实质上是一项个人信息转移的活动。实践中，我们并没有征求对应联系人的同意，也很难操作。德国 WhatsAPP 案中 [25]，用户 E 注册使用 WhatsAPP 时，必须同意接受其用户协议，向 WhatsAPP 提供其手机通讯录中联系人的信息。但用户 E 未从联系人处得到同意。法院裁判用户 E 的母亲（因 E 是未成年人，由其监护人承担义务）有义务取得孩子手机通讯录中所有联系人的书面同意。如果在疫情防控过程中，适用德国 WhatsAPP 案的思路，数据防疫的作用将大为减弱，甚至是不可实现。而在平时，如果通讯录的读取需要逐一取得联系人的同意，也不具有强操作性。这对如何确定个人信息保护的客体，以及如何进行个人信息保护提供了讨论的空间。

〔23〕 王亮、胡卫明、谭铁牛：《基于步态的身份识别》，《计算机学报》2003 年第 3 期，第 353－360 页。

〔24〕 程啸：《民法典编纂视野下的个人信息保护》，《中国法学》2019 年第 4 期，第 26－43 页。

〔25〕 周学峰、李平：《网络平台治理与法律责任》，中国法制出版社 2018 年版，第 135 页。

（三）个人信息保护之目的

个人信息保护的目的不是构建积极的控制权，而是避免消极后果。从近年来各国个人信息保护立法情况来看，强化用户对其个人信息的控制权比较普遍。实际上，用户基于知情同意而让渡出数据后，其控制能力就几乎不复存在。数据控制者、数据处理者通过统计数据、大数据来对个人数据进行使用，完全脱离了单一数据层面。这时，市场实践出现“原子化”，用户监控一个企业是否遵守法律规定十分困难，甚至是不可能的。〔26〕一味强化用户的控制权很有可能陷入制度的空想，赋予用户并不实际的权利。基于统计数据、大数据层面的技术应用，使得数据成为数字经济的关键生产要素。数据的收集和使用成为必然，也是数字经济社会人类的理性选择。用户一旦让渡出数据，就很难再对该数据形成有效控制，通过法律规定强制性对用户进行广泛赋权，很大程度上会抑制数据价值的释放，甚至完全扼杀部分产业模式。〔27〕将个人信息保护的目标定位于保障用户权益无可厚非，但是这种权益需要辩证地理解。数据共享、数据流通和大数据应用，给生产生活带来的便利性是能够被普遍感知的。统计数据和大数据都是由单一数据所组成的，其运作机理发生了质的改变。强用户赋权能够大幅度提升用户隐私、安宁等方面的权益，但是对于用户享受数字经济时代红利却有负面的效果。用户也在便利性和隐私性之间权衡，有些用户出于对隐私的担心，主动放弃了使用某些互联网工具或者功能。这也反映了基于单一数据的隐私诉求与基于统计数据、大数据的价值诉求的冲突。在理解统计数据、大数据的基础之上，个人信息保护目标的实现就应当以“用户实际上无法有效控制其让渡的数据”为前提，重点解决用户让渡数据以后可能遭受的不利后果。如冯果、薛亦飒提出“数据信托”的思路，将数据主体和数据控制者之间视为数据信托的法律关系，数据主体是委托人和受益人，数据控制者是受托人，承担信托责任。数据主体与数据控制者之间以信任为基础形成信托关系。〔28〕由此，保护个人信息的法律制度，需要解决信任的问题，而不只是赋权的问题。

（四）个人信息保护的行业性

个人信息保护的复杂性无庸置疑，行业之间差异性比较大。同样是对数据的收集、使用，生活服务类平台对个人数据的依赖度相对较低，这类平台通过中间服务赚取抽成来构建商业模式，比如外卖平台、打车平台等。但个性推荐类平台对个人数据的依赖度就比较高，这类平台以个性化推荐为基础，通过信息服务来吸引用户，进而以精准营销的方式构建商业模式。如果实施严格的个人信息保护政策，对前类平台的商业模式影响较小，而对后类平台的商业模式可能是颠覆性的打击。总结起来说，线下业务线上化的行业与完全线上化的行业收集、使用个人信息的活动区别度非常明显，未来随着“互联网+”融合程度和数字经济发展程度的深入，数据处理的特点、

〔26〕［德］克里斯托弗·布施：《个性化经济中的算法规制和（不）完美执行》，《环球法律评论》2019 年第 6 期，第 5－19 页。

〔27〕按照对“个人信息”定义的扩张式理解，完全以个性化推荐为基础的商业模式就会受到很大冲击。

〔28〕冯果、薛亦飒：《从“权利规范模式”走向“行为控制模式”的数据信托——数据主体权利保护机制构建的另一种思路》，《法学评论》2020 年第 3 期，第 70－82 页。

模式还有可能进一步区分化，单一、笼统的个人信息保护规则难以适应不同行业的实际需求。

不同行业的数据应用是有差异的，有的是针对单一数据的，必须识别自然人的身份才能维持运营，比如电话营销，对获取特定自然人身份的需求十分明显；有的是针对统计数据的，比如定向广告，只需要获取目标对象的群体性特征就能满足需求；有的是针对大数据的，比如精准营销，需要实现微观层面的有效大数据分析，才能提高精准性。这种区分既是行业的，也是动态的。电话营销、定向广告和精准营销等都属于广告活动，其商业模式是由技术能力所决定的，随着技术水平的提升、更新，业务活动也会从单一数据层面向统计数据、大数据层面转换。差异化的特点需要差异化的应对，为了实现科学性和合理性，需要构建“法律规定+行业准则+行政认可”的治理模式，由立法作出规定，由行业形成共识，由行政部门确认。比如个人信息界定的问题，首先通过立法确定个人信息的内涵和外延，再由行业提出个人信息界定的具体标准，最后经个人信息保护机构确认，从而作为该行业个人信息保护的定义。整个模式是一项法律制度设计，同样需要在立法中予以明确。

2012 年《全国人民代表大会常务委员会关于加强网络信息保护的决定》中规定“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”，确立了对“个人信息”采取“识别说”的定义模式。《电信和互联网用户个人信息保护规定》《网络安全法》《民法典》延续了“识别说”的思路，都将“个人信息”定义为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自然人个人身份的各种信息。2017 年，《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》中增加了“反映特定自然人活动情况”的描述，也基本是在“识别说”的定义框架之下。各类规定在列举个人信息的类型时有所增补，但对个人信息的定性以识别自然人身份为基础的共识已经形成。《中华人民共和国个人信息保护法（草案）》基本坚持了“识别说”的模式，突出强调了“已识别或者可识别”的要件，同时也弱化了对“身份”性的限定，放弃了对具体个人信息类型的列举，并明确匿名化信息不是个人信息，为实践留足了解释和调整的空间。

（五）小结

有关个人信息保护的讨论中，很多都指出了个人信息保护和产业发展之间的平衡问题。但不同层面的数据所触发的机制本质上就有不同，因而无法采取完全相同的平衡策略。目前虽然有很多有益的讨论，但难免陷入问题无解的困境——提出问题，而不能解决问题，或者说不能解决所有的问题而导致了漏洞或空白。制度设计取决于对社会关系机理的准确认知，从而才能选择或者创设适当的法律制度，来调整相应的社会关系，取得应有的效果。个人信息保护争议的根源就是风险产生于单一数据，而收益来自统计数据或者大数据。笔者以为，问题不是不能解决，通过单一数据、统计数据和大数据三个层面的区分，并逐一对个人信息保护所产生的现象进行内在对应分析，找出症结点，再用平衡的思路设计法律制度，就可以初步明确制度设计的方向和具体细节。

三、个人信息保护制度构建

（一）思路之确定

多数个人信息保护立法都是以用户为中心展开的，体现了用户利益优先的思路。前文已有分析，这种保护思路局限于单一数据层面。数据治理所包括的数据价值、数据安全和用户保护三个问题，应该以数据价值为目标，制度设计围绕如何释放数据价值，同时避免数据安全风险，兼顾用户保护。数据价值释放的主体是商事组织，也就是企业。以用户为中心的制度设计潜在地弱化了企业的价值释放作用，不利于数据治理目标的最终实现。我们已经远远超越单一数据的时代，正处于统计数据的阶段，并有很大可能在较短的未来进入深层次的大数据时代。对此，我们的制度考量应该以企业为中心展开，那么何种制度应予建立，就显得十分清晰了。从单一数据的层面来说，用户权益保护更为重要，因此要强化用户赋权，同时制度设计上给用户更多的保护，以扭转其弱势的地位，比如举证责任倒置、公益诉讼的制度设计，由用户来掌握主动权，必要时行使权利即可。从统一数据的层面来说，用户权益保护同样重要，但是单个用户发生权利受损的情况，还是应该转至单一数据层面解决。行政干预的必要性在统计数据层面体现出来，根据统计数据释放价值的特点，规定匿名化、去识别化等管理要求，以平衡统计数据层面的风险与收益。从大数据的层面来说，用户权益或被大幅地稀释，人们或以比特化形式在数字化空间生存，数据风险得以降低，而数据蕴含的巨大价值将被充分释放，制度设计上还需要进行前瞻性研究。

（二）数据泄露通知制度

笔者认为，数据泄露通知制度应该成为数据治理，特别是个人信息保护的核心制度。数字经济时代数据价值释放的基础是统计数据或者大数据。基于前文个人信息保护目标的阐述，用户应该能够享受积极福利，而同时避免消极后果。数据泄露事件对用户的消极后果最为明显。黑客入侵、员工泄密、系统安全漏洞、设备失窃都有可能造成数据泄露。[29] 错误配置的云存储、未受保护的代码存储库、脆弱的开源软件等也可能造成数据泄露。[30] 这些原因既包含了客观因素——系统漏洞或脆弱性等，也包括了主观因素——内部人员的失误或者黑客的入侵等。这些因素不可能完全消除或者杜绝。数据泄露并不能百分百预防。比如，系统漏洞并不可能完全不存在或者得到彻底弥补，而是需要适时更新。但是，漏洞总是先被发现，然后才有补救措施。其中的时间差，有可能会被黑客等利用而窃取数据。内部的违规操作虽然可以通过权限限定、流程管控等予以规制，但是制度总是存在被违反的可能，同样可能由内因导致数据泄露事件。用户让渡数据所期望获得的是数字便利性的对价，让渡行为实际上是基于信任基础。按照前引数据信托的思路，数据

〔29〕 董扬慧、谢友宁：《大数据视野下的数据泄露与安全管理——基于 90 个数据泄露事件的分析》，《情报杂志》2014 年第 11 期，第 154－158 页。

〔30〕 高枫：《2019 年最常见的数据泄露原因》，《计算机与网络》2019 年第 23 期，第 50－51 页。

泄露会在很大程度上破坏信任基础，也会触发信托责任。数据泄露事件会动摇信任基础，但并非双方所期待的。通过数据泄露通知制度，可以一定程度上消除信任基础的减损，也就是抵消负外部性。数据泄露通知制度的处罚条件是发生数据泄露事件，那么用户本身并不具有积极的控制权，而是消极的控制权。因此，对于发生数据泄露事件而不通知的，应当处以较高的处罚。

根据 GDPR 的规定，数据控制者不履行数据泄露通知义务，可处最高 1 000 万欧元或其全球年营业额 2%的罚款。美国没有联邦层面的数据泄露通知法规，但是各州都有数据泄露通知法。部分州规定，个人可以向未履行通知义务造成损害的责任主体提起诉讼赔偿，或者直接依据该州的消费者保护相关法律向泄露方提出损害赔偿。根据各州的规定，有些处罚按照损害人群统计（民事处罚从 500 美金到 50 000 美金不等），有些按照泄露次数统计（泄露一次 2 500 美金），有些则按逾期时间计算（每天最高 1 000 美金）。[31] 法律责任的提升，目的是防止企业刻意逃避通知义务，提高违法门槛，以促进制度的落地执行。同时，在技术手段上也要形成溯源机制，能够在检查中发现瞒报数据泄露的情况。[32] 试想，在完善的数据泄露通知制度之下，理性企业首先要做的是尽可能避免数据泄露的发生，因为一旦发生数据泄露，就不得不履行通知义务，从而对企业声誉造成影响。这就能够形成一种倒逼机制，理性企业就应该根据业务规模匹配相应的技术保障手段和安全保障等级，来最大可能地防止数据泄露的发生。但是，如果没有这种倒逼机制，就需要通过主动性的监督检查来确保企业安全保障义务履行到位，也需要通过法规、标准等形式规定清楚企业应该适配何种技术保障手段和安全保障等级。通过比较研究，可以合理地预见，如果以法规、标准等形式作出规定，企业倾向于满足最低要求即可；而如果通过倒逼机制，企业倾向于最大程度实现安全保障能力。这就是制度设计的妙处所在。

当然，建立数据泄露通知制度，并不排斥监管部门的监督执法活动。实际上，数据泄露通知制度并不增加行政执法成本，反而降低了行政执法成本。数据泄露通知制度的效果在于威慑性，迫使企业在发生数据泄露事件后一定要履行通知义务。这里最需要指出的是，数据泄露通知是一项独立的法律制度，与其他法律制度平行而非互斥。比如，企业对个人数据负有安全保障义务，监管部门可以行使监管职权，对企业的安全保障义务履行情况进行检查或执法。同样，企业履行了数据泄露通知制度，并未消除履行其他要求的义务。企业发生数据泄露事件后，按照要求履行了通知义务，此时泄露通知的法律义务已经得以履行。但是，如果数据泄露是由于企业自身安全保障义务没有履行到位，同样需要承担安全保障义务不到位的法律责任，该责任并不因为数据泄露通知义务的履行而得以免除。数据泄露通知制度和安全保障制度相互独立而非互斥。同时，数据泄露通知还可以成为监管部门发现违法活动的重要线索。根据中兴通讯和数据法盟联合发布的

〔31〕*See The Definitive Guide to U.S. State Data Breach Laws*，https://info.digitalguardian.com/rs/768－OQW－145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf（last visited Apr. 29，2020）.

〔32〕王忠、殷建立：《大数据环境下个人数据隐私泄露溯源机制设计》，《中国流通经济》2014 年第 8 期，第 117－121 页。

《GDPR 执法案例精选白皮书》[33] 梳理的案件情况，很多企业安全保障义务不到位的查处，都是由数据泄露通知所触发的。企业发生数据泄露后，按照 GDPR 的规定履行了通知义务，监管部门随即对其进行检查。发现安全保障义务未履行的，就对其进行处罚。可见，完善的数据泄露通知制度可以提高监管效率，从普遍性监督到触发性监督，从“大海捞针”到精准式执法。就数据泄露通知制度本身而言，执法成本也能降低。数据管理过程中，取证是执法的难点之一，监管部门证明企业违法的技术成本较高，难度也很大。数据泄露是显性的，通知或者没通知都是非常清楚的。是否发生了数据泄露，通过简单的技术手段或者日志查询都可以实现。这在很大程度上能够降低执法成本，同时也缩小了监管范围。

（三）数据处理登记制度

数据处理登记制度是数据处理者（控制者）将收集、处理个人信息的相关情况报告主管部门的制度。数据治理中，数据处理登记制度应当作为一项基础性制度。从各国立法来看，规定数据控制者和处理者登记制度的不是多数，主要规定于欧盟及其成员国。此外，少数亚洲国家和地区（如韩国和中国香港）和拉丁美洲国家（如秘鲁和哥斯达黎加）也存在登记制度。而美国、加拿大等北美国家、大多数亚洲国家和地区（如日本、新加坡、以色列、印度、中国台湾）、大洋洲国家（澳大利亚和新西兰）目前没有该要求。数据处理登记制度实质上是一个备案的程序，作用是建立双向的联系，实现 DPO（Data Protection Officer，信息保护专员）和 DPA（Data Protection Agency，信息保护机构）之间的信息共享渠道。数据处理登记制度也是一项衔接性的制度，是数据泄露通知制度等其他制度顺利实现的前提。数据泄露事件紧迫性强，要求快速反应，只有 DPO 和 DPA 之间具备常态化的沟通联系机制，才能确保数据泄露通知制度的有效落实。数字经济时代，数据处理将不可避免地普遍化和常态化，数据处理者本身就成为一个数据在数字化生活中存在，十分有必要对其进行基础性、系统性地统计。

（四）跨境数据流动制度

正如前文所分析，跨境数据流动的具体风险尚不可知，至少还没有量化研究的支撑。但是从大数据层面理解，潜在威胁便清晰起来。跨境数据流动监管的目的是降低境外实施大数据分析的可能，因此应该尽量避免大批量、多类型的数据出境，尽可能将数据（并不区分是何种数据）留存在境内，以避免潜在风险。目前，各国对数据流入基本不作限制，关注点主要集中于本国数据流出。各国对跨境数据流动的监管政策，都与本国数字产业发展紧密结合，一般会统筹考虑国家安全、隐私保护、产业能力等多元因素，构建符合本国利益的监管制度。大数据追求数据的混杂性，通过相关关系来预测结果，而不是像统计数据一样通过因果关系来追求精确的结果。因此，如果以大数据为背景进行考量，跨境数据流动就应当以数据本地化存储为基础，例外情形下通过安全评估来确保安全。当然这可能与主流观点相悖，大多数人主张数据自由流动，以促进数字经

〔33〕 中兴通讯数据保护合规部、数据法盟：《GDPR 执法案例精选白皮书》，http://www.199it.com/archives/961140.html，最后访问时间：2020 年 4 月 29 日。

济的发展。薛亚君认为，要求所有数据的存储、管理和处理只能在一个国家进行，会阻碍企业利用云技术的分布式特征所带来的成本和速度的优势〔34〕。然而，这并不能构成跨境数据流动就能带来收益的直接论据。本土化发展起来的互联网企业并不少见，很多企业都是在实现本土规模化之后才寻求海外市场的扩张。要对跨境数据流动进行准确的成本收益分析，还有待进一步的深入论证来思考应当采取何种跨境数据流动的政策。

提及跨境数据流动的管理，数据分级分类制度是得到认可比较多的，廖璇、陈湉认为，数据出境管理要以数据分级管理为基础，对政府数据、军事数据、重要的经济数据、个人信息敏感数据（例如与基因、医疗、银行账户密码相关的数据）等应当禁止流动。〔35〕《中华人民共和国网络安全法》第37条也要求关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。但是，这些数据均是统计数据层面，规制的是因果关系的数据。以大数据视角来看，数据分级分类制度却未必能起到应有的效果。大数据通过混杂数据可以分析相关性，来得出相关结论。如果确实存在安全问题，可能还要进行一般性、普遍性的出境禁止或者限制。

四、数据治理视野下的个人信息保护展望

数据治理与个人信息保护问题在当前阶段交织性非常强。讨论数据治理，很容易异化为个人信息保护问题。限于技术发展水平，现在对数据的认识以及对个人数据的定义方式，导致几乎所有数据都属于个人信息。对数据的担忧往往是对个人信息权利的担忧。随着数据技术的演进和突破，数据治理所依赖的思路和规则都将发生变化。数据可以大致分为三个阶段。第一个阶段主要是人的数据（personal data），这些数据由自然人而产生，同时能够通过感官发现，比如姓名、肖像、身份识别号码等。第二个阶段主要是人机数据（mixed data），这些数据由自然人而产生，但是需要借助机器设备而获取，比如通过具备定位功能的设备而产生的自然人的行踪轨迹，通过智能穿戴设备所读取的心率、血压等。第三个阶段主要是机器数据（machine data），这些数据已经突破我们现在对个人数据的认识。自然人机器化或者机器人拟人化，由此所产生的数据，虽然具备个人数据的特征，但其社会意义已经发生了实质性的变化。法感情的变迁将随着生产生活方式的变化而逐步实现。杨延超假设了一个机器人场景，TOM 利用家庭机器人的管理实现了家居生活高度智能化，便利性极为增强，可见技术成熟后，TOM 对这种智能化、便利化生活的依赖性。〔36〕这种依赖性完全是以数据为基础的，TOM 必须大幅让渡其个人数据。这种让渡在数据 3.0 时代将成为一种必然。正如凯文·凯利在《必然》中提及的，当我们依赖数字而不是文字时，将构建出一个“量化自我”。〔37〕数据 3.0 时代未必很远，思考与之适应的数据治理规则，正当其时。

〔34〕 薛亚君：《数字贸易规则中的数据本地化问题探究》，《对外经贸实务》2019 年第 8 期，第 17－20 页。

〔35〕 廖璇、陈湉：《数据出境安全管理制度研究及启示》，《信息安全与通信保密》2018 年第 12 期，第 17－20 页。

〔36〕 杨延超：《机器人法——构建人类未来新秩序》，法律出版社 2019 年版，第 4、157 页。

〔37〕［美］凯文·凯利：《必然》，中国工信出版社 2016 年版，第 280 页。

Personal Information Protection Under the Evolution of Data Value: Reflection and Reconstruction

FANG Yu

Abstract：This article establishes a theory model of three-level data type according to how the value of data can be released，to find what value can be released and what problem may be arisen within each level of data type. Then this article tries to analyze disputes about personal data protection in practice. Based on the theory model，this article elaborates the features of different types of data，and the interactions among different types of data，and then finds the deviations. From the angle of the theory model of three-level data type，this article further sets forth some obstacles of the legislative idea of personal data protection，the definition of personal data，and the specific legal system of personal data protection，then draws a draft conclusion.

Keywords：Personal Data Protection；Big Data；Data Governance；Single Data

（责任编辑：许可）