**马化腾**

作序

力荐

**腾讯云**

**腾讯研究院**

Tencent

Research Institute

**汤道生**

*数字经济* ***路-油-车*** *系列丛书*

**四in**

**数接沿理：** **数据政策发展与趋势**

丛 书 主 编 ◎ 司 晓 杨 乐 王融◎ 著

**危子工常出版话**

中国工信出版集团

htip:www.phel.com.en

**6 URLC ELEGTSCKCS NGR**





**腾讯研究院**

Tencent

**Research Institute**

腾讯云

**数字经济路-油-车系列丛书**

**Tim**

**=E**

**一** **个**

**数据治理：** **数据政策发展与趋势**

丛书主编◎司 晓 杨 乐

王 融 ◎ 著

**電子工常出版社**

**Publishing House of Electronics Industry**

北京·BEIJING

**内容简介**

数据作为与土地、劳动力、资本、技术并列的数字经济时代涌现的新型生产要素，是驱 动数字经济发展的“助燃剂”,对价值创造和生产力发展有着广泛影响。本书由长期从事数 据政策研究的资深专家王融女士撰写，她结合数据技术、业务、产业的一线发展情况和研究 积累，搭建了数据要素公共政策的完整框架：提出了数据权属问题的含义及其特征、个人数 据的隐私性与经济性二元性及近年来司法实践对企业数据财产利益的探索与确认；介绍了世 界各国数据保护的做法，特别深入分析比较了欧盟GDPR与美国加州 CCPA 两大体系的发展 趋势；探讨了面部识别、区块链、隐私计算等新兴技术领域带来的影响、挑战和机遇；勾勒了 全球数据跨境流动的政策景况；介绍了我国个人信息保护立法与实践的总体特征，以及我国 数据治理方面的努力与成效，特别是对抗击新冠疫情期间数据采集、使用、保护与责权处置 等进行了深入剖析和解读。本书视点高、视野广，知识广博、见解深刻，内容精道、力透纸背， 是数据要素方面货真价实的优秀专著。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

**图书在版编目** **(CIP)** **数据**

数据要素：数据治理：数据政策发展与趋势/王融著.一北京：电子工业出版社，2020.11 (数字经济路-油-车系列丛书/司晓，杨乐主编)

ISBN 978-7-121-39486-7

I.① 数…Ⅱ.①王…Ⅱ.①信息经济一经济发展一研究一中国IV.①F492.3

中国版本图书馆 CIP 数据核字(2020)第163058号

责任编辑： 祁玉芹

印 刷： 中国电影出版社印刷厂

装 订： 中国电影出版社印刷厂

出版发行： 电子工业出版社

北京市海淀区万寿路173信箱 邮编：100036

开 本： 710×1000 1/16 印张：16.5 字数：240千字

版 次 ：2020年11月第1版

印 次： 2020年11月第1次印刷

定 价： 58.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社 发行部联系，联系及邮购电话： (010)88254888,88258888。

质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式： qiyuqin@phei.com.cn。

III



予



**新基建是路，数据是油，产业互联网是车**

**马化腾**

突如其来的新冠疫情，给经济社会发展带来了巨大冲击。在抗疫中，数 字经济展现出强大的发展韧性，在保障人们生活学习、支撑复工复产、提振 经济等方面发挥了重要作用。国家统计局数据显示，2020年一季度我国信息

传输、软件和信息技术服务业增加值同比增长13.28。

近期国家积极布局新基建、数据要素培育，以“上云用数赋智”等举措 助力数字经济新业态新模式发展，给数字经济注入了强劲的发展势能，推动 迈向一个以新基建为战略基石、以数据为关键要素、以产业互联网为高级阶

段的高质量发展新阶段。

**新基建是数字经济发展的战略基石**

以 5G、 人工智能、数据中心等为代表的信息基础设施，作为新基建的重 要组成部分，是数字经济发展的战略基石。与传统基础设施一样，新基建是 关乎国计民生的重大战略工程，同时服务于生产和生活两端，需要做长远规

划和顶层设计。与传统基础设施不同，新基建受物理空间限制较小，可以跨

区域、跨时段高效配置，对抗突发事件的弹性和韧性更强。更重要的是，新

原文题目：《推动上“云”用“数” 建设产业互联网》,发表于《人民日报》(2020年5月7日)。

**IV**

基建所在的领域都是基于云计算、大数据等数字技术形成的朝阳产业集群， 正处在快速发展期，虽然短期内无法像传统基建投资那样迅速形成固定资产 拉动经济增长，但长期发展潜力巨大，是我国转变经济发展方式、实现高质

量发展的重要着力点。

新基建与传统基建的关系是互补相融，而不是互斥对立的。实际上，随 着数字技术日益成熟、应用场景日渐增多，铁路、公路、机场等传统基础设 施越来越智能化和自动化，与数字技术的结合也越来越紧密。未来，新基建 与传统基建必然会深度融合，界限逐渐模糊，共同服务于经济的长远健康发展，

持续提升人民生活水平。

**数据是数字经济发展的关键要素**

生产要素的形态随着经济发展不断变迁。早在300多年前，被马克思称 为“政治经济学之父”的威廉·配第t1) 就提出“劳动是财富之父，土地是财 富之母”的著名论断。工业革命之后，资本、知识、技术和管理相继成为新

的生产要素和财富之源。

随着数字技术和人类生产生活交汇融合，全球数据呈现爆发增长、海量 集聚的特点，数据日益成为重要战略资源和新生产要素。习近平总书记指出： “要构建以数据为关键要素的数字经济。”党的十九届四中全会(21首次提出 将数据作为生产要素参与分配。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》(3),将数据作为与土地、劳动力、资本、

技术并列的生产要素，要求“加快培育数据要素市场”。

[1]威廉 · 配第(William Petty,1623—1687年),英国古典政治经济学创始人、统计学创始人，

其最著名的经济学著作为《赋税论》(1662年)。

[2]中国共产党第十九届中央委员会第四次全体会议于2019年10月28日至31日在北京举行。 [3]发布日期为2020年3月30日。

V

序

数据要素涉及数据生产、采集、存储、加工、分析、服务等多个环节， 是驱动数字经济发展的“助燃剂”,对价值创造和生产力发展有广泛影响。 中央将数据作为一种新型生产要素，有利于充分发挥数据对其他要素效率的 倍增作用，意义十分重大。我们要秉持开发利用和安全保护并举的基本原则， 充分释放数据红利，不断弥合数字鸿沟，推动数字经济发展迈向产业互联网

的新阶段。

**产业互联网是数字经济发展的高级阶段**

当前，数字经济发展的重心正在从消费互联网向产业互联网转移。产业 互联网以企业为主要用户，以提升效率和优化配置为核心主题，是数字经济 发展的高级阶段。2018年9月30日，我们提出“扎根消费互联网，拥抱产 业互联网”的新战略，引发了产业互联网的热潮。新冠疫情防控期间，远程 办公、在线教育、健康码和智慧零售等典型产业互联网新业态新模式发展迅猛， 数字技术在新冠疫情防控、复工复产和增强国民经济韧性方面发挥了重要作

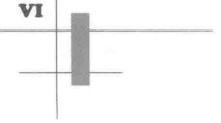
用，产业互联网的发展按下了快进键。

2020年4月7日，国家发展改革委、中央网信办联合印发《关于推进“上 云用数赋智”行动培育新经济发展实施方案》,明确提出了“构建多层联动 的产业互联网平台”的工作推进思路，努力推动数字化转型伙伴行动。加快 制订实施产业互联网国家战略，用数字技术助力各行各业和公共服务机构实 现数字化转型升级，越来越成为我国经济高质量发展和国家治理能力现代化 的重要途径。在此背景下，腾讯更加坚定要成为各行各业的“数字化助手”, 启动了“数字方舟”计划，助力“农、工、商、教、医、旅”六大领域的数

字化转型。

产业互联网的快速发展在网络、算力、算法和安全等方面都提出了更高

要求，迫切需要进一步加快以5G、数据中心、人工智能、物联网等为核心内



容的新型基础设施建设。因此，新基建是“数字土壤”,是数字经济发展的 战略基石，将为产业互联网发展提供基础保障和必要条件。另一方面，产业 互联网是新基建的市场先锋，是新基建的需求来源，将对新基建起到自上而 下的反哺作用。准确研判产业互联网的发展态势，有助于廓清新基建的主攻 方向，避免盲目投入。而数据作为关键生产要素，它的感知、采集、传输、 存储、计算、分析和应用实际上贯穿了新基建和产业互联网融合发展的每一

个环节。

综合起来，新基建、数据要素和产业互联网紧密相连、互相促进。有专 家将三者关系类比成“路—油—车”。新基建是通往全面数字社会的“高速 公路”,数据是驱动数字经济发展的新“石油”,产业互联网则是高效运行 的“智能汽车”。当然，这只是一个大致的类比，实际上三者关系远比“路—油— 车”复杂得多，比如产业互联网的IaaS (基础设施即服务)(4)等底层业务 形态实际上也兼具了“路”的功能。只要“路—油—车”三者协同发展，我 们一定能够构建出一个包括线上线下企业、政府部门、科研院所、公益机构 和广大用户在内，充满韧性的数字生态共同体。腾讯在其中将秉承“科技向善” 理念，专注做好连接和工具，立足成为各行各业的数字化助手，与合作伙伴 共建新生态，助力新基建、数据要素和产业互联网的深度融合。各方相互依

存、相互促进，共同繁荣数字经济生态，就可以合力推动经济发展动力变革、

效率变革、质量变革，提升国家数字竞争力。

[4]IaaS(Infrastructure as a Service, 基础设施即服务)是指把IT 基础设施作为一种服

务提供给公众服务模式。

**VII**



**前** **言**



**数字社会的信任基石——基于数据的信任关系**

信任在社会财富创造和经济增长中扮演着重要角色，在网络连接的数字 社会中更是如此。腾讯研究院文章——《经济增长的信任基础》,结合区块 链技术的应用与发展，探讨了塑造社会信任的正式制度(法律、监管、司法) 与非正式机制(社会风俗、伦理、技术)之间的相互关系。文章提出：科技

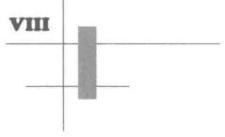
应当与其他信任机制相互结合，用科技增强传统信任，才能走向更广阔的天地。

本文将在此基础上继续讨论数字社会最重要的信任话题之一——隐私 保护，该领域不仅再次验证了上述观点，而且呈现了更为紧密的互动关系 隐私权迈向个人信息保护，是制度在回应信息技术带来的信任新风险，但 制度不可避免地具有滞后性。为减少规制惯性带来的负面效应，制度应保 持适度弹性，以使制度与技术进行更包容的双向互动，彼此调整完善。在人 工智能新兴技术领域中，我们也欣喜地看到了这种良性互动，以联邦学习 (Federated Learning)为代表的AI 技术方向，在保障隐私和数据安全

的前提下，为进一步挖掘数据价值、创造社会福祉带来了新的解决方案。

**一、制度对技术的回应：隐私权向个人信息保护扩展**

回顾过去一百多年，在面对科技对个人安宁、自主性可能造成威胁时，



制度均做出了积极的回应，并据此搭建监管框架，试图重建信任基石。

1890年，快速发展的“八卦新闻”及摄影技术应用对个人生活带来了侵扰， 美国学者由此提出了现代隐私权利理论1), “个人独处的安宁”逐步被司法

实践认可并成为法律原则。

到二十世纪六七十年代，计算机大规模应用普及，防御性的、事后救济 性的“隐私权”难以解决个人信息非法收集和利用问题，私法领域的“隐私权”

逐步发展为公法领域的个人信息保护制度，即在未发生隐私侵害后果之前，

就明确个人信息处理的方式，包括知情同意、最小化、目的特定、保障安全

与可问责等。欧、美等发达国家和地区率先完成了个人信息保护立法。

进入二十一世纪，在应对云计算、大数据、物联网等带来的个人信息保 护挑战中，欧盟扮演了领导者角色。欧盟《通用数据保护条例》 (GDPR) 细 致规定了数据处理的合法性基础，并通过高额的违规处罚，促进了各行各业 在数据保护方面的关注与投入，在全球范围内形成了立法示范效应，更是明

确了数据保护前所未有的重要性。

**二、制度的天然缺陷：滞后与规制惯性**

如同其他领域的法律制度一样，隐私与个人信息保护的立法过程就是“回

应—滞后一再回应一再滞后”的循环递进过程。

首先，个人信息保护制度的基石——“个人信息”的定义一直处于被挑 战状态。大数据的出现模糊了个人信息与非个人信息的边界。大量数据更易

被关联和聚合，大大增强了将非个人信息转化为个人信息的能力。如果法律

[1]Samuel D.Warren 6 Louis D.Brandeis.The Right to Privacy,4HARV.L.REV.193 (1890).It defines the right to privacy as the“right to be let alone,”in areaction to the development of journalism and gossip columns。

**IX**

**前言**

固守传统，适用于严格界定的“直接可识别身份的信息”,那么在大数据环 境下，数据利用的安全风险又如何被规制?如果扩张个人信息的边界，那么 又将扩张到何种程度，而不至于超出法律体系运行本身可负担的合理边界? 这是实务中围绕 Cookie 记录、搜索记录、动静态IP 地址、设备ID 是否属 于个人信息等不断进行争议的根源。随着物联网、智慧城市，包括产业互联 网的加速部署，将带来更多类似的争议。网络上的信息日夜不分地紧密结合 在一起，汇合成支撑社会运转的巨大信息流。在此情形下，将某一主体所提 出的原信息从信息束的整体中独立拆分、收回(撤回)、取消或删除的难度 日益加大，甚至在某种程度上，在原信息主体完全未知的情况下，它会自动

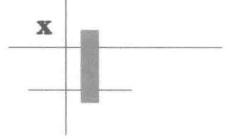
地在网络世界中互相进行联系、融合和更新l2)。

其次，个人信息保护基本原则难以应对新型信息实践。各国现行的个人 数据保护原则主要基于1980年经济合作与发展组织(OECD) 制定的《隐 私保护及个人数据跨境流通指南》,而该《指南》形成的背景主要是针对 六七十年代政府和大公司使用计算机收集和处理个人数据的，因此确立了目 的特定、知情同意、最小化等原则。但在当前以数据驱动的经济发展中，以 上原则的适用性已经显得力不从心。过去，数据的收集往往事前就可明确目的； 当前，数据价值和创新依赖于后续的挖掘利用。过去，数据收集通过单个采 集完成，知情同意机制尚可运转；当前，数据收集大多通过机器被动同步完成， 围绕知情同意有效性的质疑不断增多。过去，政策监管框架聚焦于如何减少 用户所面临的风险；当前，政策更多地聚焦于如何在保护与促进创新、经济 增长之间保持平衡。个人信息的使用与否不再取决于个人与社会整体的交往、 融入意愿，而是一种在多数情况下无须进行选择的生活方式、交往方式，这

体现了社会运转方式的全局性、整体化变革3]。

[2][3]民法典工作项目组.与民法典同行.大数据时代下个人信息保护的立法模式变革，

2018-03-07。



再次，区块链技术对现有个人信息保护实践带来了根本性的挑战。如果 说移动互联网、云计算、大数据是对个人信息保护机制如何落地执行的挑战， 那么 GDPR 尚可在体系内部进行修补。然而，区块链的出现及应用，对个人 信息保护规制范式带来了根本性冲击。区块链创建了一种全新的信任机制， 可以通过共识算法、去中心化分布式存储使参与者达成共识。这与个人信息 保护机制建构的中心化规范范式不相适应(4)。传统个人信息保护制度体系重 点指向的是现实世界里中心化的数据控制者，如政府机构、银行、医院及各 类互联网中心化平台。而在去中心化的区块链逻辑中，让分散在全球各节点(背 后是个人或机构)的参与者遵循统一的数据保护框架，对任何一家监管机构 都充满了挑战。更进一步，在区块链防止篡改的信任逻辑中，也很难支持数 据保护制度中的更正权、删除权甚至被遗忘权等权利诉求；单点记入、全网

同步功能也与 GDPR 中的数据最小化原则格格不入。

尽管区块链与数据保护法律原则在底层逻辑上存在冲突，但不可否认的 是，区块链的功能目标与数据保护制度目标是兼容的。区块链有利于提升人

们对个人数据的控制权，更好地保护用户隐私。

总之，当现有制度在尝试解决技术带来的问题时，往往会陷入规制的路 径依赖，如在个人信息保护机制中，继续加强知情同意，继续加强个体权利， 然而这些应对对于实际问题的解决似乎效果有限。正如欧盟的 GDPR在2016 年甫一问世，制度规范就已走向固化。相比之下，新技术却仍在以惊人的速 度高歌猛进。在区块链之外，无人驾驶、面部识别、可穿戴设备、智能家居、 医疗监测器械、行为生物数据、无人机等一个又一个技术应用，不断地丰富 数据驱动的新领域。对于这些新技术，是严格套用GDPR 予以规范，还是适

度平衡隐私保护与创新发展，是政策制定者无法回避的现实问题。

[4]Michèle Finck.Blockchains and Data Protection in the European Union,Max Planck Institute for Innovation and Competition Research Paper No.18-01。

**XI**

**前言**

综上所述，现有的个人信息保护制度带有一定的缺陷。如果从区块链技 术等新兴技术的发端开始就将其完全套用在规制范围内，甚至视之为违法技 术，那么无疑会扼杀实现数据保护目标和技术发展的一种可能。反之，更多

地采取宽容的态度，让制度与技术彼此适应和完善，就会在互动中取得双赢。

欧盟理事会在 GDPR 实施一周年的评估报告中写道： “我们应该看到技术在 某些领域的应用也可能拥有巨大的优势，并有可能加强欧洲公民的隐私保护。”

例如，基于区块链的“零知识证明技术”能够实现使用尽可能少的个人信息，

同时验证某一特定主体的身份15);差异隐私技术能够实现数据集中而带来的 价值，但同时保持特定自然人身份不被识别t6]。法律的适用应当为技术发展 留有“一定空间”,而不是对技术完全规训。这也许是欧盟数据保护委员会 (EDPB) 迟迟未就区块链出台合规指南的重要原因之一。

**三、制度也塑造和促进了隐私安全技术的发展**

以欧盟GDPR 为代表的个人数据保护制度促进了合规与隐私文化的发展， 并推动业界用技术来解决隐私、安全问题。近年来，这个话题在学术界和行 业实践中都经历了爆炸性增长，包括多方安全计算(Secure Multi-Part y Computation,MPC)、 同态加密(Homomorphic Encryption)、差分 隐私(Differential Privacy)等安全技术加速从理论走向实践，相关

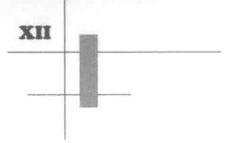
应用实践在金融、医疗、政务等领域渐次展开。

[5]零知识证明技术指的是，特定主体能够在尽可能少向验证者提供甚至不提供任何有用的信息的情 况下，使验证者相信某个论断是正确的。AHN Gail-Joon,“Zero-knowledge proofs of retrievability",Science(Information Sciences),Vol.10(8),2011,pp.1608-1617。

[6]差异隐私技术指的是，从统计数据库查询时，最大化数据查询的准确性，同时最大限度地减少识 别其记录的机会，这种机制的核心是给查询的结果增加一定的噪点。Mannhardt,Felix,

"Privacy-Preserving Process Mining",Business &information systems engineering,Vol.61(5),2019,pp.595-614。

[7]中国信息通信研究院云计算与大数据研究所.多方安全计算技术与应用研究报告，2019年12月。



基于大数据的机器学习既推动了AI 蓬勃发展，又让AI 在隐私安全 这个方向上形成了新的分支——面向隐私保护的机器学习(Privacy- Preserving Machine Learning),其中又以联邦学习最具代表性。联 邦学习正在广泛的跨学科领域获得吸引力：从机器学习到优化、信息理论和 统计，再到密码学、公平性和隐私[8]。

**(一)隐私安全计算的新兴领域——联邦学习**

尽管“数据是人工智能时代的石油”已经被作为广泛共识，然而现实中 出于数据安全的担忧和隐私合规要求，各个机构主体掌握的数据是分散而碎 片化的，数据往往难以在规模化基础上实现价值利用。在这种背景下，联邦 学习作为一种行之有效的解决方案越来越引发人们的关注。联邦学习可以使 得各方在不披露原始数据的情况下达到共建模型的目的，即在不违反数据隐 私保护法规的前提下，连接数据孤岛，通过算法实现数据价值利用。联邦的 含义是指各个数据的拥有体之间是平等的，因此，联邦学习不仅着眼于隐私

保护，而且致力于解决数据权属带来的数据利用激励问题。

“联邦学习”的核心包括两个过程，分别是模型训练和模型推理(9)。在 模型训练阶段，模型信息可以在各方之间交换，但数据不能交换。因此各方 的数据安全及基于权属的数据权益都可以得到保障；而在模型推理阶段，训

练好的联邦学习模型可以置于系统的各个参与方，供多方共享。

联邦学习的“布道者” 杨强教授用“羊吃草”的例子对此进行了解释： 在机器学习领域，模型效果的提升依赖于数据训练，所以机器学习模型就像

[8]Peter Kairouz and H.Brendan McMahan conceived,coordinated,and edited this work.Correspondence to kairouz@google.com and mcmahan@google.com.

Advances and Open Problems in Federated Learning。

[9]杨强，刘洋，等.联邦学习.北京：电子工业出版社，2020,pp.4。

**XII**

**前言**

一只小羊，而数据是草。在传统方法中，要建立机器学习模型，需要到各个 草场(数据供应商)收购数据。但现实是，隐私和数据安全保护的要求使得 获取数据成为障碍，草不能直接运出本地，这也就是我们常见的“数据孤岛”

困境。

在此情况下，联邦学习提供了新的思路：让羊群在各地移动，而草不出 本地。也就是机器学习模型以分布式的方式构建，而不需要数据在本地区域 之外移动。这种“数据不动，模型动”的优势是，对于每只羊的所有者而言， 并不知道羊吃到肚子里的草到底是什么样，在隐私得到保护和数据安全的前 提下，实现了机器学习模型的不断完善。除隐私保护和数据安全这一动机外，

联邦学习的另一个发展动力来自最大化利用云系统下的终端设备的计算能力。

**(二)联邦学习——在保护用户隐私的前提下，让数据价值惠及个人**

2019年，谷歌在Google I/0大会上展示了G-Board 应用，在ToC (或表为2C, 消费者场景)中应用联邦学习技术，在保护隐私的前提下，实 现了更新迭代手机输入法预测模型(10)。以往，由于手机本地输入包含大量的 用户隐私信息，因此无法将这些信息上传用于预测用户输入的智能输入法的 模型训练。而通过联邦学习，每部安卓手机都可以在本地训练模型，随后将 模型参数上传汇总，从而帮助更快地提升输入法的准确性。自2017年以来， 苹果一直在利用差分隐私技术来发现最受欢迎的 emoji 表情及Safari 中的

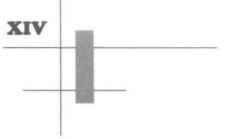
媒体播放项，并将其与联邦学习相结合，这两种技术都有助于改进苹果Siri

智能助理响应的准确性。

在 ToC场景之外，联邦学习在 B2B(企业到企业场景)中也大有可为。

越是受到数据隐私和孤岛效应困扰的领域，越是联邦学习落地的最佳场景。

[10]<https://www.businessinsider.com/google-io-live-blog-all-announcement> coverage-updates-2019-5。



典型领域包括医疗、金融、教育、智慧城市等，在这些领域，联邦学习可以 让数据价值真正惠及个人。[11]例如，在医疗领域，英国国王学院组建“人工 智能中心”,在英国国民医疗系统NHS 的4家信托机构之间进行联合学习部署， 使得这些超大型学习模型训练得以应用；英伟达医疗和 MELLODDY 制药集团 合作，在欧洲10家不同的制药公司之间提供了联合学习系统；腾讯天衍实验 室联合微众银行研发的医疗联邦学习，在脑卒中预测的应用上，准确率在相 关数据集中高达80%。通过应用联邦学习技术，医疗领域的数据福祉正在被 探索与开发。借助于人工智能的数据分析可以挽救生命，而且不必以牺牲个

体的隐私为代价。

在金融领域，平安科技公司正在研发、建立全球首个面向金融行业的联 邦学习平台“蜂巢”。 “蜂巢”能够应用于多方信息的安全协作计算，满足 银行和金融机构的风险评估、反洗钱、监管等多场景应用需求；微众银行通 过多维度联邦数据建模，将风控模型的效果提升了约12%,相关企业机构有 效节约了信贷审核成本，整体成本预计下降5%～10%,并因数据样本量的

提升和丰富，风控能力进一步增强。

**四、技术与制度，如何形成互动式进步?**

如何形成技术与制度之间的互动增强?隐私与个人信息保护领域似乎正 在形成一种参考模型：制度对技术发展需要具有包容性，同时，技术本身在

价值目标上也应与制度保持一致。

制度的包容性被证明很重要。人工智能、区块链等新技术都受到了 GDPR 的影响，但这并不意味着与制度互不兼容。在2018年5月GDPR生效之际，

[11]王健宗.数据隐私保护新曙光——联邦学习的机遇、挑战与未来.联数，第1卷，第8期，

**XV**

**前言**

曾有学者认为：因为GDPR 要求算法解释输出原理，这意味着所有的深度学 习都将会处于违法状态。对此，我们认为： GDPR 确实对技术发展带来了重大 影响，但我们无须将这种影响过分夸大，实际上欧盟“第29条工作组”已经 发布相关指南，明确数据控制者并不必然要解释复杂的算法。在大部分情形下， 只需面向用户，用尽可能简明的方法和语言告知背后的基本逻辑即可。可见， 即使在“最严格的欧盟”,对包括区块链、面部识别等人工智能应用，也未

予以一刀切式的否定性评价。

另一面，技术也需要与制度坚守同样的价值目标。正如联邦学习技术展 现的那样：在保障数据安全与隐私的前提下，实现数据共享，促进多源(元)

数据的碰撞、融合，最大限度地释放数据价值12。

以联邦学习为代表的隐私安全技术与GDPR 等数据保护制度所坚守的价 值目标是一致的，后者甚至推动了前者的发展。联邦学习需要满足数据保护

制度要求，其完整的合规性框架至少应包括如下两个方面。

(1)数据处理目的的合法性。正如即使是合法的手段也不应当应用于非 法的目的一样，联邦学习的应用场景本身应是正当性的，例如医疗领域的疾 病分析与诊断、金融领域的信贷风险评估等。特别是在医疗领域，数据汇聚 分析对于人类福祉更有着极大的价值。在 ToC 的其他应用场景中，如果联邦 学习方案最终面向用户提供个性化服务，那么也应向用户呈现相关的逻辑，

以保障用户的知情权。

(2)处理过程的合法性。其中包括模型(算法)隐私，以确保恶意行为 者无法对训练数据进行反向工程；输入隐私，确保参与各方输入的算法参数 不会被其他方观察到；输出隐私，保证除应用最终结果的用户外，其他各方

都看不到算法的最终输出。例如，在 ToC 场景中，苹果应用差分隐私和联邦

[12]梅宏.在《联邦学习》中的推荐语.北京：电子工业出版社，2020,pp.4。

**XVI**



学习技术来对众多用户的个人数据进行了优化分析，并最终应用于与用户有 关的个性化服务，整个过程中个体用户的数据不会被其他方观察到，但最终 每位用户都享受到了数据汇聚分析后的便利和效率提升。在通过数据实现“我

为人人，人人为我”的价值创造过程中，不以牺牲个人隐私为代价。

当然，没有任何技术是没有缺陷的，联邦学习同样需要在实践中不断完善，

并推进隐私保护各技术领域的进步，只要其始终与制度价值目标保持一致。

**五、结语**

在迈向数字社会的转型过程中，我们比任何时刻都更加渴望信任。过去 一百年的信息技术进步与制度回应的实践，让我们更加清晰地看到：构建数 字社会的信任基石，需要在正式与非正式的信任机制之间形成凝聚互动，而 不是仅仅依靠其中的一种。单一强调伦理，无法避免“杀熟”现象；完全依 赖法规监管，便要承受“抑制创新”发展的结果；而技术万能论更是早已破灭。 数字社会的信任构建，需要学术(理论和工程)、商业实践、社会治理拧麻

花般的协作共建。

美国政府在2014年关于大数据的第一份白皮书——《抓住机遇、坚守 价值》中指出：大数据分析所拥有的潜力，将逐步侵蚀长久以来在公民权利 保护方面形成的价值基石，但大数据本身也蕴藏着解决信任、隐私、公民权 利保护等方面的潜力。如果运用得当，大数据将成为推动社会进步的历史性 助推器。因此，公民与数据的关系应当扩展，而不是压缩，以便抓住这一历 史性的机遇和潜能。我们应拥抱大数据，同时最大限度地保护人们在隐私、

公平、自觉方面的价值基础。



水

序 /

**前** **言** /VIl

**第** **一** **篇** **数据的权属与竞争** /001

第1章 数据产权：无处安放的数据权属 [002](#bookmark1)

第2章 关于大数据交易的核心法律问题——数据所有权探讨 005

一、关于数据所有权的两种观点 [005](#bookmark2)

二、讨论数据所有权的前提是承认数据具有财产属性 008

三、对数据所有权界定的一种思路 [010](#bookmark3)

四 、结语 [015](#bookmark4)

第3章 隐私与竞争：数字经济秩序的平衡之道 [017](#bookmark5)

第4章 个人信息保护与市场竞争的互动关系 [023](#bookmark6)

**——从前者的视角观察**

一、引言 [023](#bookmark7)

二、 隐私与市场的关系 [025](#bookmark8)

三、个人信息保护法律制度对市场竞争的影响 [027](#bookmark9)

四 、个人信息保护制度扩张对市场竞争的影响 [034](#bookmark10)

五、数据可携权等制度面临的质疑与挑战 [044](#bookmark11)

六、结语 [051](#bookmark12)

**第二篇** **世界各国数据保护做法** [**053**](#bookmark13)

第5章全球视野下的个人数据保护立法与实践 [054](#bookmark14)

一、个人数据保护法的全球普及 [054](#bookmark15)

二、GDPR 从文字走向落地，正负面影响并存 [055](#bookmark16)

三、美国加利福尼亚州出台CCPA, 与欧盟保持立法差异 057

四、国内多部法律并行推进数据保护规则 [058](#bookmark17)

五、个人数据跨境流动机制曲折发展 [060](#bookmark18)

六、跨域执法数据协作新的探索与冲击 [061](#bookmark19)

**第6章** **欧盟《通用数据保护条例》详解** [064](#bookmark20)

一 、极大地扩展了《条例》的适用范围 [064](#bookmark21)

二、统一的《条例》规则之下仍有一些例外 [066](#bookmark22)

三、一站式监管 [067](#bookmark23)

四、处理数据须有合法理由 [067](#bookmark24)

五、坚实强大的数据主体权利 [069](#bookmark25)

六、严格问责：数据控制者 [071](#bookmark26)

七、数据保护官 [072](#bookmark27)

八、安全保障措施 [074](#bookmark28)

九、对数据画像活动的特别规制 [078](#bookmark29)

十、监管权力、处罚与司法救济 [080](#bookmark30)

**第7章** **欧盟《通用数据保护条例》:十个误解与争议** [082](#bookmark31)

一、引言 [082](#bookmark32)

二、 相关问题的讨论与分析 [083](#bookmark33)

三、 结语 [103](#bookmark34)

第 8 章 美国联邦与地方隐私立法的互补 [104](#bookmark35)

第9章 美欧隐私保护立法会走向趋同么? [106](#bookmark36)

一、CCPA 对适用范围做了合理排除 [107](#bookmark37)

二 、CCPA 仍然保持了美欧个人数据保护法的最大差异， 112

延续了opt-out 模式

三、 结语 116

**第10章** **我国个人信息保护刑事立法进展及企业风险防范** 118

一、加速推进个人信息保护刑事立法 [118](#bookmark38)

二、我国个人信息刑事保护的主要特点 [120](#bookmark39)

三、我国个人信息刑事保护制度要点 [122](#bookmark40)

四、企业的刑事风险防范策略 [132](#bookmark41)

五 、结语 [138](#bookmark42)

**第11章** **《民法典人格权编》的影响与改变** [140](#bookmark43)

一、引言 [140](#bookmark44)

二 、把握“个人信息”特殊属性，合理处理与“隐私权” 141

的关系

三、个人信息定义回归“识别说”标准 [142](#bookmark45)

四、民事立法亮点， 《人格权编》的免责事由 [143](#bookmark46)

五、借鉴国际立法经验，延续个人信息处理基本规则 144

六、填补“民事保护”板块，构建更加完善的个人信息 145

保护法律体系

七、全面的制度建设，仍留待《个人信息保护法》 146 八、结语 147

|  |  |
| --- | --- |
| **第三篇** **特殊领域的数据保护政策** | **/149** |
| 第12章 面部识别技术隐私与数据保护政策趋势 | 150 |

第13章 区块链的隐私和政策保护趋势 [153](#bookmark47)

第14章 儿童个人信息保护——美好的权利如何脚踏实地 157

一、引言：儿童个人信息保护，难点在哪里? [157](#bookmark48)

二、儿童个人信息保护，从哪里借鉴经验? [159](#bookmark49)

三、儿童个人信息保护的核心制度设计 [161](#bookmark50)

四、儿童个人信息保护，仍有许多细节性的实务问题 165

五、结语：儿童个人信息保护，仍应在生活场景中探寻 168

方案

**第四篇** **数据共享与数据流动** **/171**

第15章 Facebook 数据事件的深度拷问 [175](#bookmark51)

**第16章** **欧盟数据共享政策探索** [180](#bookmark52)

**第17章** **数据跨境流动政策认知与建议** [185](#bookmark53)

一、关于讨论前提的两点澄清 [186](#bookmark54)

二、美欧数字跨境政策发展概况及差异 [188](#bookmark55)

三、数据跨境政策面临的共性问题及对中国的参考建议 193

四、复杂的数据流动政策对跨境业务的影响 [198](#bookmark56)

五、数据跨境流动合规建议 [200](#bookmark57)

**第五篇** **数据治理与政务数据规则** **/205**

第 1 8 章 数据治理——精细科学的政策平衡 [206](#bookmark58)

一、2018年，数据治理的灰色之年? [206](#bookmark59)

二、欧盟 GDPR, 灰暗中的希望? [207](#bookmark60)

三、 美欧隐私政策在走向融合趋同吗? [210](#bookmark61)

四、数据治理，期待更为精细和科学化的政策平衡 212

**第19章** **“隐私”与“公共健康”的决策平衡** 215

**——疫情下各国个人信息保护的10个共识、差异与挑战**

一、背景 [215](#bookmark62)

二、规则、做法与讨论 [217](#bookmark63)

三、 大型科技公司积极参与抗击疫情，但承诺谨慎处理 225

用户数据

**第20章** **“健康码”折射政务服务数据规则** 231

一、解决“个人信息保护”问题，需厘清各方的角色 232

与责任

二、“健康码”本质上是政务服务，政府扮演数据控制 233

者角色

三、区分“控制者”和“处理者”,将为数据处理活动 234

提供更明确的法律指引

四、“健康码”政务项目中的政府和企业的责任与边界 235

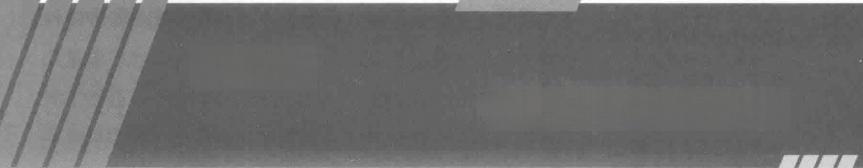
五、我国现有个人信息保护法律体系与上述规范框架 237

尚存差距

**后记**

/239

/HIH !!!!||!!



**第一篇**

**数据的权属与竞争**

自 3Q 大战以来，互联网市场围绕数据的竞争日益白 热化，特别是近两年，从“新浪诉脉脉”、“菜鸟顺丰之争” 到“大众点评诉百度地图”,几乎每个纠纷都同时引发了 对数据权属、竞争与隐私保护等问题的关切。当这些问题 重叠交汇时，我们如何厘清数据权属边界，并妥善协调竞

争与隐私问题?

**002**

**数据要素**

数据治理：数据政策发展与趋势

本章内容根据作者 2016年11 月 4 日 在 “数据产业与新治理 论坛”上的演讲整理 而成。作者分享了主 题为“无处安放的数 据权属”的演讲。其 中说道：如果衍生数 据应用了独创性的加 工方法，那么具有知 识产权保护的可能 性；对于加工方法并 没有独创性，但企业 投入了成本、资源获 得的衍生数据，虽并 不以知识产权形态存 在，但企业的正当合 法利益也具有法律保 护价值。



**第1章**

**数据产权：无处安放的数据权属**

**摘要：**数字经济的特点是多向的、动态的，数据权利 设计不能只体现为初始数据单边的财产权分配，更应当同

时反映动态结构和目的。

在讨论数据权属问题时，首先需要明确数据权属是什 么、数据是什么。2016年6月公开征求意见的《民法通则》X 草

案)提出了数据信息作为知识产权客体，引发了许多争议。

尽管我们在很多场合混用数据和信息两个概念，但细 究起来，二者仍然存在差异。数据是对事物的描述与记录。 同时，我们当下使用的“数据”概念更多的是在网络信息 技术快速发展背景下提出来的，强调以电子方式存在的数 据能够被电子方式读取、传输和处理。而信息代表了一种

普遍意义的表达，强调了通过数据表达背后的实质内容。

抛开产权界定与边界这一问题，数据权属问题实际关 切的是，数据作为什么权利的客体。而由于数据本身是一 个底层概念，其具有多种划分的标准和类型，需要结合不

同数据类型再展开讨论。

从个人数据保护法律视角出发，个人数据尽管其边界

**003**

**第一篇** **数据的权属与竞争**

仍有极大争议，但究其本身来说是一个非常明确的法律概

念。与个人相关的，且能够识别个人身份的信息，这是大

部分法律所采纳的定义，它们是个人信息相关权利利益所

保护的对象；而在政府数据开放的讨论语境下，政府数据

也是一种重要权利的客体，即公民对数据的知情权、访问

权和使用权的客体，其定义是指政府履行公共职责，在公

共税收支持之下展开公务活动所收集处理的数据。对比个

人数据和政府数据的法律定义，可以发现其出发点有异曲

同工之处。个人数据、政府数据的界定都包含了身份标准，

分别与个人、政府身份紧密关联，且均因特定身份的主体

的行为而产生。

与个人数据和政府数据相比，商业数据的法律界定最

模糊。个人数据与政府数据都有相对明晰的法律规范体系，

严格地说，商业数据并不是一个法律概念。所以业界所关

心的数据权属问题，更多是围绕商业数据的困惑。

说到商业数据，现有法律体系能够部分实现对财产权

利的确权。例如，如果数据具有独创性，是智慧成果，那

么很大程度上可以通过知识产权实现财产的权益界定与保

护。数据是有商业秘密属性的，也可以通过现有的商业秘

密规则予以保护，解决部分权属问题。

还有一部分是容易被忽略的。在商业实践中，通过合

法、合规的方式实现数据开发及在此基础上的数据权属安

排。例如，我国并没有明确的数据权属规定，但这并未影

响各地在政府部门的推动下，建立数据交易平台。尤其是

美国发展多年的数据经纪行业，通过合同协议在具体业务

**004**

**数据治理：数据政**

场景中明确数据权益，包括对原生数据、衍生数据的权益

做出细致安排，这恰恰是市场对数据权属的有效实践。

所以在这样的背景之下，《民法通则》(草案)征求 意见稿对于数据的规定引发争议就不足为奇了。将数据信 息两个相近的概念叠加混用，在并未考虑到不同类型的数 据特点的情形下，统一纳入知识产权的保护客体，漏洞便

显现出来了。

考虑到数据生态的复杂性和数据权利的多样性，赋予 企业专属、排他的数据权利并不可行，与现有的法律体系 也难以形成协调与自洽的连接，特别是与个人数据、政府 数据相关的场景下，矛盾更加突出。对于由个人数据构成 的商业数据，这在移动互联网发展阶段尤为明显。对于这 一部分的数据，可以结合匿名化技术的发展，对数据权属 做出更细致的安排。在欧盟，虽然其实施严格的个人数据 保护制度，但也很早就对匿名化数据予以了认可，企业可 以自由处分这些数据。当然，达到匿名化标准，使得企业

能够享受匿名化带来的法律适用豁免，还有许多工作要做。

**005**

**第一篇** **数据的权属与竞争**



**第2章**

**关于大数据交易的核心法律问题**

—— **数据所有权探讨**

**摘要：**清晰的产权归属是交易的前提与基础。然而， 当前关于数据的产权归属问题还远未达成共识，特别是在 去除个人身份属性的数据交易中，到底是数据主体(产生 数据的个人)还是记录数据的企业拥有数据的所有权，各 方莫衷一是。笔者提出的思路是：原始/底层的个人数据， 所有权归用户本人；而在原始数据基础上，经过充分匿名

化获得的数据集，企业享有限制性的所有权。

**一、关于数据所有权的两种观点**

在风起云涌的大数据时代，数据的收集、分析与利用 逐渐构成企业运营的核心。除自身提供服务获得的数据外， 企业对数据的需求进一步向外围扩展，以买卖、共享为特 征的数据交易成为引人注目的商业现象。2015年4月15日， 贵阳大数据交易所挂牌成立，成为我国首个专门提供数据 交易的服务平台。7月22日，武汉也成立了东湖大数据交

易中心。

本篇文章发表于2015

年，正是各地如火如

茶地兴建大数据交易

平台之际。彼时，“大

数据”是被各方追随

热捧的概念，但人们

对大数据价值利用的

认识并不深入，大数

据交易平台成为“聚

光灯下的焦点”,迫

切需要解决“数据交

易”的合法性问题。

然而，从今天的视野

来看，数据价值利用

有多种方式、方法，

并不以传统的“交易”

(或买卖)为核心。

因此，不论是理论还

是从实践，本篇文章

仅仅是一个探讨的开

端，其中的观点还远

未成熟。围绕数据权

属的讨论，应当随着

技术、应用、市场的

发展变迁而不断深入。

数据交易的前提是清晰的产权归属。如果产权存在瑕

**006**

**数据要素**

数据治理：数据政策发展与趋势

疵，那么意味着交易存在法律风险。贵州数据交易所确立了9项交易原则， 其中之一即是“数据买卖双方要保证数据所有权、合法、可信、不被滥用”。 虽然在一个多月的时间里，贵阳交易所已经完成了11笔数据交易，然而可以

看到，各方对于数据的所有权问题目前并没有形成统一的看法。

大数据的数据源十分广泛，包括用户数据，也包括不具有身份属性的其

他数据，如天气、矿产资源数据等。本文不泛泛讨论各类数据的产权问题，

而只对其中最具有争议性质的，即原始数据是用户个人数据的情形下，数据

交易中的产权问题予以分析。

有人主张，应当对用户数据设立“财产权利”,强调个人对数据享有的 优先财产权利，并以此对企业的数据利用、交易行为予以制约。认为数据交 易产生的数据商品化现象将给个人隐私带来极大的伤害，并产生难以预计的 信息安全问题，大范围失控的数据交易也将为违法活动提供温床。因此提出 对数据这一新型生产资料，在法律上另设一财产类别，或可称之为“数据财产”, 与现有法律认可的无形财产分开。这一新型财产权利的设立应当重新定位价 值顺序，权利的出发点是人而非物，数据主体(即产生数据的本人)应拥有 优先的权利。无独有偶，在围绕我国“Coo kie 第一案”的讨论中，有学 者也认为，要彻底解决未来数字经济的难题，法律有必要承认用户个人对数

据的财产权利，进而对互联网公司的行为加以约束l2)。

另一种观点则代表产业界立场，认为数据控制者(即确定收集目的，面 向用户个人收集和使用信息的主体)对数据拥有绝对的所有权。2015年7月

23日，阿里巴巴旗下的云计算公司阿里云发起数据保护倡议。这份公开倡议

[1]利求同，大数据卖的就是隐私，

<http://www.thepaper.cn/newsDetail>\_forward\_ 1353973\_ 1。

[2]胡凌.朱烨案界定网络隐私.财新周刊，2015年06月24日，

<http://weekly.caixin.com/2015-06-19/100820889.html>。

**007**

**第一篇** **数据的权属与竞争**

书明确：运行在云计算平台上的开发者、公司、政府、社

会机构的数据，所有权绝对属于客户；云计算平台不得将

这些数据移作他用。

这份倡议主要着眼于解决云计算服务提供者(云平台)

与云计算服务使用者(云客户)的关系，倡议提出云平台

不得将客户的数据移作他用。从处理云平台与云客户的关

系出发，该原则无疑是值得肯定的。正如在现实生活中，

租户的财产，房东无权处分一样，云平台当然不得侵害云

客户的数据。但值得注意的是，在强调云平台不得侵害客

户数据的同时，这份倡议中也触及了所谓的“云客户”与

其提供的数据之间的关系，提出云客户对其数据享有绝对

所有权。然而，在云计算环境下，“云客户”不等于“个

人用户”。云客户包括开发者、公司、政府、社会机构及

普通个人用户。在排除普通个人用户的情形下，按照倡议

的绝对所有权观点，意味着开发者、公司、政府对于其在

提供服务或履行职责的过程中获得的用户个人数据享有绝

对的所有权，并因此可以自由地使用、分享、交换、转移、

删除。相应地，作为产生这些数据的用户本人，则不能对

企业、政府、开发者的数据处分活动主张任何权利。

显然，上述两种观点有着不同的价值取向，前者以用

户个人为优先项，通过用户行使个人数据财产权，间接地

对企业数据交易活动起到限制作用；后者则从产业的立场

出发，希望明确企业对于数据的完全的、绝对的所有权，

为企业的数据处理活动松绑，最大限度地减少来自外界的

干预。

**008**

**数据要素**

数据治理：数据政策发展与趋势

[3]王利明，杨立新， 王轶，等.民法学(第 四版).北京：法律 出版社，2015。

二 、讨论数据所有权的前提是承认数据具有

财产属性

尽管上述两种观点在结论上分道扬镳，但二者有一个 共同的认知起点，即承认数据的财产属性(或者说基于数

据可以产生财产权益),这正是讨论数据所有权的前提。

依据《元照英美法词典》的解释，所有权是指一个人 享有的对某物 (Thing) 独占性的支配权，是对物的占有、 使用和以出租、出借、设定担保、转让、赠予、交换等方 式予以处分等权利的集合，也是法律承认权利人对作为权 利客体的物(包括有形财产与无形财产)所享有的最充分、

最完整、最广泛的权利。

尽管我国《物权法》中的“物”仅指有体物，包括动 产和不动产，但我国法律不排除权利可以作为物权的客体， 例如知识产权中的财产权利等13]。也就是说，作为最重要 和基本的物权——所有权，可以以财产权利作为客体。因 此，如果承认在数据之上具有财产权利，那么便有了讨论 数据所有权的法律基础。而无论是市场实践还是法学理论， 我们看到，个人数据具有财产属性已经成为不可逆转的历

史潮流。

从市场实践看，个人数据的商品化充分说明了其具有 财产性质。这种财产性质不仅体现为个人数据具有使用价 值，更体现在其转让价值得到了市场的认可。2014年4月， 荷兰学生肖恩·巴克尔斯建立一个拍卖网站来专门出售自

己的个人信息，信息内容包括他的住址、医疗记录、个人

**009**

**第一篇** **数据的权属与竞争**

日程安排、电子邮件内容和所有社交网络上交流的信息，

其中网上交流信息包括他的在线聊天记录、消费偏好和浏

览器历史记录。拍卖网站吸引了超过40个买家前来竞拍，

最终肖恩·巴克尔斯以350欧元的价格出售了自己的个人

信息。此外，基于个人数据的财产价值，当前甚至出现了

一种新的商业模式，即用户可以按一定的价格将个人信息

出售给服务商，之后服务商寻找广告主或者其他数据需求

方将用户数据变现。

若我们继续深究下去，就会发现很多向用户免费提供

的互联网商业模式实际上都建立在以个人数据为对价的基

础上，只不过相较于出售个人数据获得直接对价这种显性

的价值体现方式，互联网商业模式中个人数据的财产价值

体现是隐形化的。以搜索引擎广告联盟商业模式为例，联

盟网站获得广告费的基础是联盟能够利用用户的搜索历史

Cookie 记录，向用户投放个性化的广告。因此，尽管用

户免费使用了搜索引擎，但实际上是用户的搜索记录等行

为数据反哺了搜索业务，是搜索业务得以存续和发展的价

值源泉。

而从法律的视角来看，现代人格权的发展已具备为数

据商品化提供法律支撑的理论基础。个人数据是个人数据

保护法保护的对象，个人数据权利的来源是人格权。传统上，

人格权区分于财产权，人格不能像财产一样进行利用和交

易。然而在市场经济与现代商业的推动之下，人格权不仅

具有精神利益，而且也具有财产利益的观点，在法学理论

层面已得到普遍认可。最典型的即肖像权。明星、公众人

**OI0**

**数据要素**

**数据治理：数据政策发展与趋势**

[4]王利明.论人格 权商品化，法律科学 (西北政法大学学报), 2013(4):54-61。

[5]王利明.人格权 法研究(第二版).北 京：中国人民大学出 版社，2012。

物通过合同方式转让个人的肖像使用权，并从中获得财产 收益，已成为司空见惯的商业现象[4]。对此我国现行立法 也已提供了法律支撑。《民法通则》第100条规定，公民 享有肖像权，未经本人同意，不得以营利为目的使用公民

的肖像。本款规定从反向确认了肖像权具有财产权益15]。

在这一点上，个人信息权与肖像权并无本质的不同。 二者之间的主要差别仅在于：虽然每个人都享有基于本人 肖像的财产权益，但这种财产权益的实现还有待于市场的 认可。换言之，并不是每个人都有机会主张自己肖像权的 财产权益，仅有明星、公众人物等少数群体有机会予以主 张；但从个人信息来说，不论是明星还是普通百姓，市场 均认可其个人数据的商业价值。理论上，每个人都能有行

使其对个人数据财产权益的可能。

因此，承认个人数据的财权权益已具备相应的法理基 础，只是在规则层面还需要在具体的法律制度中进一步明 确个人数据权中的财产利益，并对数据商品化利用设立相

应的法律规则。

**三、对数据所有权界定的一种思路**

在明确了数据具有财产利益后，接下来需要回答的问

题是，在大数据背景下，这种财产权益的所有者是谁?

**OII**

**第一篇** **数据的权属与竞争**

**(一)基于不同场景的所有权界定**

本文在一开始就介绍了两种较为对立的观点： 一种观点认为个人对数据 拥有优先的财产权利，另一种观点则认为企业对数据拥有绝对的所有权。笔 者认为，上述两种观点都有偏颇之处，均体现出了“一刀切”的特点。考虑 到当前对大数据的认识尚处于初级阶段，几乎难以提出“放之四海而皆准” 的统一规则。科学的做法是，区分不同的场景予以判断和分析。具体到大数

据交易的数据所有权问题，笔者认为，目前应至少区分以下两大类场景。

第一类场景是，以个人数据为交易对象的场景。首先需明确的是，依据 现有法律规定，我国禁止公民个人信息的出售行为。2012年《全国人大常委 会关于加强网络信息保护的决定》规定： “任何组织和个人不得窃取或者以 其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个 人电子信息。”已经颁布的《中华人民共和国刑法修正案(九)》也继续重 申了出售个人信息罪。但从未来看，个人信息的交易合法化也并非完全没有 可能。个人信息本质上是私权的处分对象，只要处分不对公共利益构成损害， 则是个人的自由。换言之，只要经个人知情并同意，理论上个人信息就可以 用来出售。正如上文中介绍的那样，市场上已经出现了出售个人信息的商业 模式。况且，人们对个人信息乃至隐私的观念也在演变之中，比如“00后” 与“80后”在隐私观念上已经有了显著的变化，更年轻的一代更加积极主动 地拥抱网络，将自己的生活状态甚至心情感悟等日常生活的点点滴滴都公布 于网络，并从中获得分享乐趣[6]。因此，在法律上并不能完全排除个人将其

信息出卖而获益的正当性。

在此类场景下，笔者认为个人数据的所有权人就是数据主体本人。所

有权人(Owner) 是指对物(Thing) 或者财产 (Property) 享有所有权

[6]Tene O,Polonetsky J.A theory of creepy:technology,privacy and shi**ftSmg** social norms.Yale Journal of Law 6 Technology,16 Yale J.L.6 Tech,

59,2013。

**012**

**数据治理：数据政**

(Ownership) 的人，即对物或财产享有占有、使用、收

益、转让或处分等权利的人。

第二类场景是，在个人数据基础上，对数据做出匿名 化处理(或称去身份化处理)后进行的交易。在此类场景 主要讨论匿名化数据的所有权问题，而这正是当前大数据

交易中最急迫的问题。

笔者的观点是，对于在用户数据基础上对数据做出匿 名化处理的数据集(以下简称匿名化数据集),企业(即 数据控制者)对该匿名化数据集享有有限定的所有权。对

这一观点，可以分以下两层进行解释。

第一，企业对匿名化数据集享有所有权。从法律层面 看，企业对用户数据的匿名化处理切断了用户对匿名数据 的法律联系。理由是，用户对数据主张权利的来源是个人 信息保护相关法律。个人信息保护法适用的对象是个人数 据，在数据去身份化后，该数据已经排除在个人信息保护 法范围之外。而这也是国内大数据交易合法性最基础的逻 辑。贵州数据交易强调： “交易所交易的不是底层数据， 而是清洗、分析、建模之后的数据结果。”但这里需要指 出的是， “数据清洗”不等于“数据匿名”。数据清洗是 从大数据分析与利用的角度出发，通过加工整理，将不规 则的数据转变为规则的数据，去除无用元素，从无序转变 为有序，从而为数据分析打下基础；而数据匿名化强调的 则是去除数据中的用户身份数据，消除数据的身份可识别

性，是从保护用户隐私的角度而开展的工作。如上分析，

**013**

**第一篇** **数据的权属与竞争**

数据清洗并不必然实现数据的匿名化，在涉及所有权问题时，必须强调只有

经过充分匿名化的数据，企业才对其享有所有权。

一定程度上承认企业对于匿名化数据集享有所有权，除因为匿名化切断 了个人与数据的法律联系外，还考虑到了三个因素： 一是企业对于数据的记录、 存储投入了巨大的技术、网络、人力、管理成本。如果没有企业的记录行为， 数据不可能被留存与记载，更无从谈起商业价值(7。因此，在法律上，应当 对企业的投入与成本做出平衡考虑。二是，从推动技术与业务发展的角度而言， 大数据是推动未来社会经济发展的重要动力。在法律上赋予企业对匿名化数 据集的所有权，有利于明确数据的产权边界，保障企业的财产权利，增加数 据交易的法律稳定性与可预期性，为企业利用数据创造财富提供积累机制。 三是，赋予企业对于匿名化数据的所有权，有利于规范数据交易市场，遏制

数据的非法黑市交易，让数据在有序可控的规则之下充分流动[8I。

第二，必须强调企业对匿名化数据集享有的所有权是有限制的。尽管所 有权是物权体系中对物及财产的最完整的权利，但不否认所有权包括两种类 型，即完整的所有权和有限定的所有权。完整的所有权可以对物及财产行使 占用、使用、处分、收益等权能。所有权人在理论上拥有无限的支配权，只 受一般法律限制，例如相邻权或不妨害他人的约束。作为受限制的所有权，

在对物及财产权利进行使用或者处分时要受到一定的限制。

**(二)企业对匿名化数据集享有有限制的所有权**

对企业关于匿名化数据集的所有权做出一定限制，出于以下三个方面的

考虑。

[7]陈小江.数据权利初探.<http://legal.people.com.cn/n/2015/0711/c188502-27287962>.

html。

[8]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(3):38-59。

**014**

数据治理：数据政

其一，从权利的优先顺序考虑。企业匿名化数据的基础是用户的原始数据。 从价值溯源来看，原始数据是价值的源泉。原始数据包含了用户的身份数据， 该身份数据兼有财产利益和人格利益，且人格利益是核心。而匿名化数据主 要体现为财产利益。在民法诸权利体系中，人格权优先于财产权，特别是财

产权来源于人格权时，应当以人格权为优先，受到人格权的限制。

其二，从个人信息保护法的原则考虑。个人信息保护法规定了目的限制 原则与必要原则。这两个原则对于数据的匿名化及后续利用将起到限制性作 用。目的限制原则要求企业使用用户个人信息的目的应当与收集用户个人信 息时告知用户的目的保持一致，如果超出了当初收集时确立的目的，则应当

告知用户，并经得用户的同意。

其三，从当前匿名化技术及大数据发展趋势来看，数据的匿名化是一个 较为相对的概念。在可获得的数据源越来越丰富、数据算法越来越强大的背 景下，已经被匿名化的数据集存在重新恢复身份数据的可能性。因此，即使 匿名化后的数据不再适用个人数据保护法，但从维护隐私与信息安全的大原 则出发，企业应当对数据集的匿名化以及匿名化后的后续利用的隐私与信息 安全风险进行评估。如果该风险较高，那么企业在行使所有权时应当有一定 的限制19)。例如，缩小交易对象范围或对交易对象做出约束，以确保其下游 用户对数据的使用不会对用户造成歧视与不公，以及网络与信息安全受到危

害的情况。

从当前国际上针对大数据交易规则的讨论来看，也印证了上述的判断。 对于企业开展数据交易进行一定的限制主要来自对用户隐私及信息安全风险

的担忧，限制性措施的核心是使企业的数据交易活动能够实现一定的透明度。

[9]Information Commissioner's Office.Anonymisation:managing data

protection risk code of practice.<https://ico.org.uk/for-organisations/> guide-to-data-protection/anonymisation/,2012。

**015**

**第一篇** **数据的权属与竞争**

例如，美国联邦贸易委员会(FTC)2014 年针对数据经纪行业发布了报告《数 据经纪行业，呼唤透明与问责》,表达了FTC对数据交易缺乏透明性的关切， 并建议国会应当专门针对数据经纪行业立法，通过立法要求开展数据交易活

动的企业对用户提供透明度，具体体现在以下几点10]。

·向用户公示其获得(包括购买、共享)数据的渠道、数据的类型，并

为用户提供退出机制。

·要求数据交易方除披露原始数据类型外，还应当披露企业基于原始数

据，利用大数据分析对消费者特征标签化的处理活动。

·对于健康医疗等敏感信息的交易活动，尤其需要提升透明性，用户必

须充分知情并明确表示同意。

从国内实践而看，目前更多地强调了企业对匿名化数据拥有所有权，而 对企业行使所有权的必要限制缺乏关注，更没有提出对数据交易透明性的要 求。贵阳数据交易所成立一个多月便完成了11笔数据交易，除第一笔交易披 露了交易双方主体外，其他各笔交易的主体、交易的数据类型、数据渠道公 众均一无所知。从交易所网站显示的信息来看，交易所可交易的数据类型多 达30种，其中包括医疗、教育、电信等高敏感性的数据领域。数据交易存在

的隐私与信息安全风险堪忧。

**四、结语**

在大数据时代，人与数据的关系应当扩展而非压缩，只有如此才能把握

[10]Federal Trade Commission.Data Brokers -A Call for Transparency and Accountability.<http://www.docin.com/p-861802697.html>,May 2014。

**0I6**

数据治理：数据政

历史性机遇，推动经济发展与社会进步]。解决数据产权问题， 一方面要着 眼于明确产权归属，为数据交易的顺利开展提供稳定的法律基础；另一方面， 仍要关切数据交易带来的隐私与信息安全风险，对数据交易活动做出相关限

制性要求，尤其是提出透明性方面的要求。

[11]Executive Office of the President.Big Data:Seizing Opportunities, Preserving Values.<http://www.docin.com/p-816632946.html>,May 2014。

**017**

**第一篇数据的权属与竞争**

**第** **3** **章**

**隐私与竞争：数字经济秩序的平衡之道**

**摘要：**数据的二元属性(个人数据所关联的隐私性与

作为生产资料的“经济性”)也许在互联网商业模式兴起

之时就存在，为什么直到当下，隐私与竞争问题的交汇才

会如此突出?也许回顾在线商业的发展历程会给出问题的

线索。在移动互联网的推动下，用户数据的隐私属性越来

越强。在门户互联网时代，网络信息大多具有公开属性，

如新闻、电商、BBS 论坛信息大多是公开的，信息自身具

有被传播的需求，并且搜索引擎的及时出现很好地打通了

数据的流动，互联网体现出了明显的去中心化特征。

步入移动互联网时代后，移动互联网随时随地收集着

高度个人化的数据，如照片、通信、邮件、活动轨迹等。

物联网的加速部署，让个人数据的排放更加无处不在(国

外最早提出data exaust 概念，意指在数字化时代，数

据是人类活动行为的伴生物),网络世界对个人的数据勾

画甚至比物理世界本身更加精细。用户对数据的安全性有

了更高的期待，隐私保护的关注度也水涨船高。

此外，在平台经济模式下，平台数据的流动性大大降

低，同时，数据成为平台竞争力的重要方面。 一个有意思

的现象是，过去这十年，既是移动互联网兴起的十年，又

**0I8****数据治理：数据政**

是互联网平台经济模式崛起的十年。

一方面，数据自身的隐私属性决定了用户仅限于与特 定企业分享特定数据， 一般情形下，并不会出现跨平台的 数据流动，因此与桌面互联网时代相比，移动互联网有更 突出的数据孤岛现象；另一方面，移动互联网生态下的平

台经济模式越来越成熟。

苹果、安卓形成底层操作系统，但在上层应用部分， 平台模式让新的市场进入者有机会进入每个细分领域。例 如，在苹果iOs 系统中，苹果提供iMessage 即时通信 服务，但也容纳其他同类通信服务；谷歌的安卓操作系统， 更是打造了充分开源、开放的竞争生态。在社交、娱乐、 出行、支付、内容等各个领域，新的市场进入者通过搭建 平台对接供给，吸引并留住用户，最终沉淀数据，并继续

通过对数据的分析挖掘来增强平台自身的竞争力。

从移动互联网演进到人工智能时代，数据的二元性将 更加突出。数据越来越具有私密性，深入用户的各个生活 场景，所覆盖的广度和挖掘的深度将不断增加；同时，没 有哪类技术比人工智能更加依赖于数据的“喂养”。各平 台对数据的争夺也越来越激烈，这解释了为什么短期内的

大量纠纷都围绕此而展开。

关于隐私：在数据经济的商业模式中，要做到法律合 规，在形式上保障用户的知情权和选择权，这并不难。但

要真正地，切实地保护用户隐私，我们还应该做些什么?

**019**

**第一篇** **数据的权属与竞争**

关于竞争：围绕数据的争夺，市场公平竞争的边界在

哪里?竞争法的传统规则在数字经济时代下，应当有怎样

的更新，才能既实现数据价值的最大化，又有利于鼓励市

场投资?

分析数字市场竞争纠纷，隐私与竞争法律机制无法相

互替代，而应各司其职，协调互补。

从隐私机制出发，尽管当前互联网的商业实践面向用

户实现隐私权利的解决方案仍有种种缺陷，冗长的隐私政

策和乏力的“知情一同意”机制不断引致“隐私已死”悲

观论，但无论是从用户期待来看还是从市场供给来看，抑

或是从政策环境来看，隐私机制依然重要并持续发挥作用。

实际上，以欧盟为代表，仍在致力于完善用户个人数据保

护法律机制；在国内，有关个人数据保护的立法、监管、

司法也均在不断加强。因此，对于涉及用户个人信息相关

的数字市场纠纷，隐私及个人信息保护机制仍应当是发挥

作用的主要法律机制之一。

当然，隐私与竞争机制的互补性就在于，单靠其中的

一种机制无法解决全部问题。例如，企业履行充分的告知

同意义务，主要解决隐私问题，但数据获取中的隐私合法

性并不代表竞争上的正当性，否则，类似于“3Q 大战”中

假借用户之名的不正当竞争行为就不会通过司法诉讼程序

得以纠正。

并且，从隐私视角来看，对所涉纠纷的数据属性、获

取数据的方式和手段的分析，也可以为竞争问题的判断考

**020**

**数据治理：数据政**

虑提供一定的参考。例如，如果纠纷中的信息属于A 平台 用户的个人信息，甚至是敏感信息，那么B 平台在未经用 户同意的情况下获取此类信息则涉嫌侵犯了用户的隐私利 益，同时也对A 平台履行对用户个人信息安全保障义务造 成妨害，在未与A平台协商一致的前提下通过技术手段截 取数据，可以在一定程度上作为竞争行为的不正当因素予

以考虑。

另一方面，从竞争机制出发，数字市场的竞争自由和 创新自由必须以不侵犯他人的合法权益为边界，以是否有 利于建立平等公平的竞争秩序为判断标准。这对于我国来 说尤其有现实意义。我国的互联网市场竞争正是从“蛮荒 的丛林法则”一路走来，通过不断的司法诉讼来明确竞争 的规则边界的。这些竞争规则在数据竞争阶段依然有重要

意义。

例如，在“3B 大战”中确立的“非公益必要不干预” 原则明确：网络服务提供者干扰他人互联网产品或服务的 运行，必须限于保护网络用户等社会公共利益的需要，并 且应当确保干扰手段的必要性和合理性。以数据截取为目

的干扰行为同样应当受到此类规则的约束。

特别是，结合移动互联网生态的上下游特征，包括操 作系统、手机应用商店、安全软件等上游经营者，更应在 数据获取中保持克制，不得利用其技术权限上的优势，对

下游经营者实施非实现其功能所必需的数据截取行为。

如果通过不正当的方式肆意侵略其他平台(特别是下

**021**

**第一篇数据的权属与竞争**

游经营者)的数据，用户隐私期待无法得到保障，新的市

场进入者也将始终无法建立其自有的核心数据竞争力，数

字经济生态终将丧失活力之源。而归根结底，在失去竞争

的市场，个人的隐私保护也只是一场空想。在过去的十年，

苹果iOs 系统和谷歌 Android 系统的生态繁荣无不证明

了这一点。

总之，隐私与竞争二者彼此交汇，并作为移动互联

网时代最重要的秩序体系，相互支撑起数字经济的活力

与繁荣。

**结语**

保持数字经济的持续活力，隐私保护与竞争规则缺一

不可。从“3Q大战”到近期的“新浪诉脉脉” “顺丰与菜

鸟纠纷”,都展示了隐私与竞争复杂交织的一面，但同时

也让我们有机会深入理解“隐私”与“竞争”政策相互依

存的本质关系，二者无法相互替代，而应各司其职，协调

互补。

在“新浪诉脉脉”等类似的案例中，我们已看到司法

实践对于此类问题的有益探索， “三重授权原则”的提出

兼顾了隐私与竞争，明确了平台间基于用户数据的商业利

用应当各自通过用户授权，妥善解决隐私保护问题。同时，

平台间的数据利用合作也应当通过商业协商合作实现，反

对以干扰、侵入系统等不正当手段截取其他平台数据。正

如“大众点评诉百度”案的二审判决明确的那样： “如果

**022**

**数据治理：数据政**

不加节制地允许市场主体任意地使用或利用他人通过巨大 投入所获取的信息，将不利于鼓励商业投入、产业创新和 诚实经营，最终损害健康的竞争机制。”而在无序的市场

竞争中，用户隐私保护也终将落空。

**023**

**第一篇数据的权属与竞争**



**第** **4** **章**

**个人信息保护与市场竞争的互动关系**

——**从前者的视角观察**

**摘要：**本文从个人信息保护法的视角，探讨了个人信

息保护与市场竞争的互动关系，并以个人信息保护法中的

“知情一同意”原则、欧盟数据可携权等为例，进一步解

构了个人信息保护机制的不同模式对市场效率与竞争的影

响，以及个人信息保护法与竞争法的竞合与冲突。

**一、引言**

一个多世纪前的工业时代，隐私保护学说和竞争法制 度几乎同时诞生[121。人类历史上也首次通过法律制度来 保护喧嚣市场中个人的安宁与自由，免受外界过分滋扰； 同时保护经营者的竞争自由，建立公平、正当、有序的市 场秩序。长久以来，隐私保护法与竞争法区隔明显，二者 在调整行为、执法机构、救济机制等方面泾渭分明。例如， 房东在租户的屋子里安装了窃听装置，毫无疑问人们将围

绕隐私问题而探讨，与竞争法无关。

但是， 一百多年后的今天，信息通信技术所带来的数 字化洪流将人类社会推入了以数据为生产资料的新时代，

隐私与竞争问题变得不再那么容易区隔，而是密切交织在

[12]如果聚焦于美

国法律史， 一个有意

思的发现是，美国隐

私法原理和竞争实体

法诞生于同 一 年。

1890年，美国人萨姆

尔·D·沃伦(Samule

D.Warre n) 和路易

斯·D 布兰代斯(Louis

D.Brandeis) 在《哈

佛法学评论》(第四期)

上发表的《论隐私权》

一文是有关隐私权的

第一篇法学专论。自

此以后，法律实务和

法律学说都对隐私权

问题展开了孜孜不倦

的探索。而与此同时，

美国的第一部竞争成

文法《谢尔曼法》也

于1890年颁布。

**024**

**数据要素**

**数据治理：数据政策发展与趋势**

[13]“3Q 大战”指自 2010年9月开始的网 络安全企业奇虎360 与腾讯之间的一系列 纠纷，争议包括隐私、 竞争等话题，纠纷诉 讼至2014年最高院 判决告终。北京奇虎 科技有限公司诉腾讯 科技(深圳)有限公 司、深圳市腾讯计算 机系统有限公司滥用 市场支配地位纠纷案，

(2013)民三终字第 4号。

[14]北京淘友天下技 术有限公司等与北京 微梦创科网络技术有 限公司不正当竞争纠 纷上诉案，(2016)京 73民终588号。

[15]“顺丰菜鸟之争” 是指2017年6月发生 的快递企业顺丰与阿 里菜鸟网络之间的争 议，同样包含隐私、

竞争话题，该纠纷以 国家监管部门的介入 而告一段落。

[16]大众点评诉百度 不正当竞争案(2016) 沪73民终242号民事 判决书。

[17]本书中的“隐私” 概念涵盖了隐私权学 说的隐私利益保护，

以及以隐私权为基础 的个人信息保护，为 行文简洁，统一表达 为“隐私”。

一起。同一个市场活动，可能会同时引发隐私与竞争问题 关切。特别是在国内互联网市场，自“3Q大战”[13 以来， 数据竞争日益白热化，从“新浪诉脉脉”[14]“菜鸟顺丰之 争”(15)到“大众点评诉百度地图”案(16),其共同的特点是： 每个争议都同时触发了数据权属竞争与用户隐私保护两大 讨论焦点。隐私与竞争问题彼此交织，呈现复杂的市场面 貌。但究其原因，更多地与数字经济的生产资料——数据

本身的二元性相关。

其一是数据所带有的用户权利属性。个人依据隐私与 个人信息保护法，享有隐私保护利益以及个人数据利益(7)。 数字经济中的数据资料十分广泛，包括不具有个人身份属 性的其他数据，如天气、矿产资源、工业数据等。但不可 否认，我们正在经历的移动互联网时代所累积的数据矿藏 中最有价值的部分多集中于个人数据。当然，也有人质疑， 由于网络世界的无孔不入，用户基于数据的隐私权利早已 不复存在。但事实恰恰相反，隐私保护权利不论是在学说 上还是在法律实践上，都有着长足的发展。人们普遍认为： “隐私”并不是信息分享的对立面，而是对信息分享的控制。 用户与特定的经营者分享个人信息，并不影响用户就该部 分信息对经营者主张“合理的隐私期待利益”,欧盟更是 强化了用户的个人数据保护权利，各国网络安全法关于网 络服务提供者的安全保障义务，也很大程度上构建在保护

用户隐私权及个人信息合法利益的基础之上。

其二是数据本身的竞争价值属性。数字经济，不止于 经济活动本身的数字化。离开数据的支撑，产品和服务提

供将难以为继；更为关键的是，竞争方式的数据化，导致



**第一篇** **数据的权属与竞争**

**025**

某些商业活动离开数据的哺育后，产品和服务无法得以优化，从而无法形成 核心竞争力。以搜索引擎业务为例，谷歌公司2016年处理的搜索请求超过2 万亿次，平均每秒超过6万次以上(18),也正是基于巨大、丰沛的数据资源， 谷歌公司的核心算法得以不断优化，仅2014年核心算法就改进了890次之多。 算法和数据之间的良性互动，使得谷歌公司始终在搜索结果的相关性、快速性、

及时性上保持了领先竞争力。

对于隐私与竞争问题的交汇，如何协调适用隐私法和竞争法，有着不同 的观点。有观点认为，对数字市场竞争问题的考虑不仅应当关注价格因素， 而且应纳入隐私等非价格因素；但也有反对者认为，仍应区分竞争与隐私问 题的不同性质，将隐私问题交由隐私法和相应的执法机构去解决(19)。但事 实上，尽管同一类行为同时触发了隐私与竞争关切，但隐私法与竞争法的制 度目标、调解方式仍有明显区别，关键在于不论是隐私问题的调查分析，还 是竞争问题的调查分析，都不应再满足于片面的一元元素的分析，而要考虑 到其他方面。换言之，个人信息保护法与竞争法要彼此关注和呼应原本属于

对方领域的问题。

**二** **、隐私与市场的关系**

**(一)隐私保护与市场效率并不完全是对立关系**

对于隐私保护和市场效率，普遍存在着二者对立的误解，认为隐私保护

降低了信息流动的效率，对创新发展有阻碍作用。法律经济学者理查德·波

[18]Danny Sullivan.Google now handles at least 2 trillion searches per

year,available at <https://searchengineland.com/google-now-handles-2>- 999-trillion-searches-per-year-250247,last visited on Dec.23\*2018。

[19]Maurice E.Stucke and Allen P.Gruenes,Big Data and Competition Policy,

**2016,pp.259-260。**

 **026** 数据治理：数据政

斯纳 (Richard Posner) 认为，隐私并不如人们所感知那样，它并不是多

数人所相信的社会价值。

隐私机制在降低信息流动效率的同时，存在隐私与市场和谐关系的另一 面，即隐私保护机制可帮助市场更有效、更稳定地运行。隐私让个人区别于 他人，成为独立的个体，这是人类繁荣的驱动力。同时，个人无法在真空中 获得自我实现，他或她需要进入社会，了解到他人的信息，而市场在其中发 挥了重要的角色。如果隐私缺失，那么一些社会活动、机制以及人类所认同 的价值观念将遭到侵蚀。事实上，隐私一直是市场机制有效运行的不可或缺 的一部分。已有社会试验表明，在工作场景中，如果雇主使用全面的监控系统，

那么实际上雇员的工作效率最低(201

**(二)隐私是市场竞争中一个重要的维度**

隐私与竞争是市场得以持续活力发展的两大基石。二者背后的价值根基 都折射了人类对自治和自由的追求。隐私保护关涉个人自由与安宁，而竞争 法则保障经营者的经营自由秩序。充满竞争活力的市场，也将为用户提供有

效的隐私保护供给。

以美国市场为例，尽管谷歌、Facebook 等巨头企业已经覆盖了搜索、 社交的主流市场，但基于用户隐私保护功能的业务创新依然活跃。在搜索市 场，以“不追踪用户”为竞争卖点的 DuckDuckGo 明确表明不会记录用户 的搜索行为，默认不利用存储在用户本地终端上的Cookie 数据(以下简称

Cookie)。2016 年 DuckDuckGo 搜索总量超100亿次(21),在全球市场的

[20]Ryan Calo,Privacy and Markets.A love Story,Legal Studies Research Paper.No.2015-26,University of Washington School of Law。

[21]Dodgvaci/10P-on-- cheg!aved at on

Feb.23\*,2018。



**第一篇** **数据的权属与竞争**

热度翻倍，成为全球第5大搜索引擎网站[2]。2017年第一季度，主打“阅 后即焚功能”的快照(Snapchat) 社交软件日活跃用户已达1.6亿，每日 视频点播量和 Facebook 的相当[2]。可见，隐私保护仍然作为人类最基本 的需求而存在，而一个有效竞争的市场能够面向此类需求提供服务，并展开 竞争。而对于苹果、Facebook 、 谷歌这些大型互联网公司而言，也始终将 隐私保护作为其核心理念。以苹果为例，该公司表示，隐私保护一直是其产 品的核心卖点之一。从最初的设计阶段开始，隐私保护的理念就已植根于产 品与服务之中。在2016年协助 FBI 调查案件的事件中，苹果与美国政府公

开叫板，指责政府不应要求其在产品中增加后门(24)。

**027**

**三** **、个人信息保护法律制度对市场竞争的影响**

竞争法划定了数字经济中市场主体的经营行为边界，而由于个人信息保 护法律制度直接设立了数字经济中最重要的个人数据的收集、流转与处理规 则，从某种程度上来说，个人信息保护法律制度本身对数字市场竞争会带来

影响。

**(** **一** **)opt-in** **与** **opt-out** **模式对市场效率的影响**

“知情-同意”原则是个人信息保护的基本原则与核心内容，但这一原

则在欧盟与美国的立法中有着不同的具体体现。在欧盟的个人信息保护立法

**[22]**Alexa.The top **500** sites on the web,available at https://www.alexa.

com/topsites/category/Computers/Internet/Searching/Search\_Engines,last visited on Feb.23\*,2018。

**[23**]Snapchat -Statistics 6 Facts,available at <https://www.statista.com/> topics/2882/snapchat/,last visited on Feb.23,2018。

**[24**]Apple -Customer Letter,available at <https://www.apple.com/customer>- letter/,last visited on Feb 5",2018。

**028**

**数据治理：数据政**

中， “知情一同意”更多地表现为明示同意，或者表达为 opt-in (选择参与)模式，即在收集个人数据之前，应 当事前得到数据主体的本人的明确同意，否则即为违法。 而在美国的立法中则相反，更多地表现为默认同意，也就 是opt-out (选择退出)模式，即在数据收集的过程中， 默认用户同意数据处理活动，用户如若不同意收集及处理

活动，可以通过退出的方式来实现拒绝权。

opt-in 与 opt-out 两种模式更早出现在反垃圾邮 件制度中。opt-out 模式的立法是建立在假定邮件接收者 同意的基础上，直到邮件接收者行使拒绝权。这两种模式 有着明显的优劣点。在邮件场景中，opt-out 模式减轻了 企业的合规负担，有助于商业邮件的快速传播，但它把成 本转移给了消费者，为了退订E-mail, 用户必须打开并 回复；相反， opt-in 模式虽然有利于消费者举证企业违 法发送邮件，但它同时大大限制了互联网上的商业活动，

减少了合同机会。

opt-in 与opt-out 两种模式的优劣点，对于个人信 息的收集、处理效率也产生同样的影响。按照欧盟数据处 理的合法性原则要求，在商业场景中处理个人数据，大部 分情况下应当得到数据主体的同意，数据主体有权阻止有 关自己的数据的处理。在数据处理者将数据主体的数据出 于商业营销目的披露给第三方之前，应当通知数据主体对 象，后者有权拒绝此类披露。数据主体本人对于有关个人 数据的收集、处理活动依法享有较强的控制力。在欧盟个

人数据保护立法改革之后，《通用数据保护条例》General

**029**

**第一篇** **数据的权属与竞争**

Data Protection Regulation,GDPR) 更是增强了

这种同意机制，要求同意必须是具体的、清晰的，是用户

在充分知情的前提下自由做出的。若数据控制者希望获得

的同意的事项区别于此前已取得同意的事项范围，则需要

向用户做出单独并且明确的说明；若将同意数据处理作为

签订合同的前提条件，而这种数据处理事实上超出了提供

服务所必需的范围，则将违反有关“同意应当是自由做出”

的限制性规定。

在这种“同意”的高标准下，虽然 GDPR条例并没有 明确禁止“推定同意”模式(敏感数据处理、数据画像活 动例外),但在实践中通过推定方式获得用户同意将很难 被认为是有效合法的。也就是说，当前实践中普遍存在的 通过冗长晦涩的隐私政策来获取用户同意，或者让用户在 签订业务协议时通过“打钩”方式做出一揽子授权的方式 将可能失去合法性。业界普遍认为，GDPR条例关于有效

合法同意的严格规定，使得用户的同意不会像现在这样被

轻易获得(25)。更重要的是，GDPR条例赋予了数据主体可 以随时撤回同意的权利。数据控制者应当明确告知用户现

有的该权利，并为用户方便地行使该权利提供便利。

与欧盟相比，美国则在更多情形下选择认可“默认同 意”。在美国个人信息保护相关法律法规中，鲜有对同意 做出类似于欧盟的严格解释。要实现合法的数据处理活动， 并不必然需要个人的明确同意，更多的场景是只要为个人 提供退出渠道即可，这就在企业的数据处理活动中留下了

巨大的合法性空间。

[ 2 5 ] 王 融 . 欧 盟 数

据保护通用条例详

解.大数据，2016年

第4期。

**030**

**数据治理：数据政**

美国的《合理使用信息原则》(Fair Information Practice Principle,FIPP) 是美国在消费者隐私保护与个人信息保护监管中所应 用的重要原则。该原则源于美国健康、教育和福利部1973年的专题报告《公 民记录、计算机和权利》,这份报告是1974年《隐私法》的核心，在美国多 个州的数据保护规则中得以体现。这一原则在美国隐私监管的重要机构—— 美国联邦贸易委员会的执法活动中也发挥着指引作用(26)。FIPP 提出的合理 使用个人信息原则包括：透明性、个人参与、明确用途、数据最小化、使用

限制、数据质量和完整性、安全性、可追责与审计。

与欧盟相比，美国的隐私保护原则不再特别强调个人的权利，特别是个 人对于数据处理活动的控制力(集中体现为知情-同意是数据处理活动的合 法性要素),而仅仅是弱化为透明性和个人的参与。这些原则更多从对企业 的最低责任出发来规定，例如企业应当明确用途、提供安全保障等。在多数 情形下，能够为用户提供退出机制，则满足了主要的合规要求。即使是在通 信行业最为严格的隐私法规文件——2016年美国联邦通信委员会(FCC) 通 过的《宽带网络服务提供商隐私指导草案》中，美国监管机构依旧遵循了美 国法中常见的“告知一同意” (Notice and Consent) 框架，并细分出

了以下三个类别：

(1)默认同意。适用于提供宽带网络服务所必须用到的消费者数据，以

及向用户推销类似于用户已经购买的宽带网络服务时所需要的消费者数据，

还包括满足“符合消费者预期的其他目的”时需要用到的数据。 《宽带网络 服务提供商隐私指导草案》认为，在用户与网络服务提供商之间达成关系时，

已经默认网络服务提供商使用上述数据，因此不再需要用户额外的同意。

(2)选择退出(opt-out) 。 宽带服务提供商在提供服务时能收集到

[26]Daniel J.Solove and Woodrow Hartzog,“The FTC and the New Common Law of Privacy”,Columbia Law Review Vol 114,p.583。

**031**

**第一篇** **数据的权属与竞争**

一系列用户数据，当宽带服务提供商向用户推销“与通信相关的服务时”, 或向其下属机构共享用户数据以向用户推销“与通信相关的服务时”,《宽 带网络服务提供商隐私指导草案》允许在宽带服务提供商组织内部共享和使

用用户数据，除非用户明确选择退出这样的信息共享。

(3)选择参与(opt-in) 。 上述两类情形之外的其他任何(包括与第三方) 使用、共享用户数据的行为原则上都是禁止的，除非用户明确表示选择参与。 尽管这一草案已明确了默认同意和选择退出机制，但对于宽带服务商对部分 数据的利用行为，草案尝试引入了明示同意机制，遭到了强烈反对，最终被

否决127]。

对于opt-in 、opt- out 模式的不同运用，是欧美个人信息保护立法体 现出严格与宽松区别的重要原因之一。同时，也对于将个人数据作为重要生 产资料的数字经济市场效率产生了直接的影响。在移动互联网、云计算、物 联网技术应用下，无处不在的智能终端、传感器，实现时时刻刻的数据收集 与计算。在这种业务模式中，事前一一取得用户的明确同意，对于数据处理

效率、业务模式都带来不可忽视的影响和效率损失。

**(二)禁止跟踪机制对数据获取的影响**

除 opt-in 、opt-out 外，在个人信息保护政策中发展出的自律性准

则——禁止跟踪(do not track)机制也同样对数据获取效率产生影响。

要理解禁止跟踪机制，首先需要理解存储在用户本地终端上的cookie 数据(以下简称 Cookie) 。Cookie 是指网站为了辨别用户身份而存储在

[27]Michael Kan,“Congress dismantles Internet privacy rules,allowing

ISPs to sell your web history",available at <https://www.pcworld.com/> article/ **3185880**/privacy/us-house-votes-to-undo-broadband-privacy-rules. html,last visited on Feb.23",2018。

**032**

数据治理：数据政

用户本地终端上的数据(通常经过加密)。网站利用Cookie 数据， 一方面 得以为用户提供个性化服务，另一方面对这些数据信息进行集合化分析，完 善网站经营策略，同时，网站可以根据这些浏览记录来掌握用户的浏览习惯， 以便更好地投放广告和提供服务。以 Cookie 为基础的用户数据分析是互联

网商业模式的主要特点。

Cookie 通 常 以 user@domain 格 式 命 名 ，user 是本地用户名， domain 是所访问的网站的域名(28),大多数的第三方监测工具和网站分析 工具都会采用第三方 Cookie 。 所谓第一方和第三方的说法，是用来确定 Cookie 的归属的，这个归属是指Cookie 中记录的域 (domain) 。 第一方 和第三方的主要区别是，Cookie 中的域名是否和被访问网站的域一样，是 就是第一方，否就是第三方。在1993年Cookie 技术诞生时，Cookie 具有 专属性原则(即A网站存放在Cookie 的用户信息， B网站是无权访问的), 但随着互联网广告产业的发展，网站除了嵌入自身的 Cookie, 还可以在网 页中嵌入第三方的 Cookie, 这就使得网站可以跨站使用其他网站Cookie

中的个人信息，从而产生了隐私泄露风险。

2010年12月，美国联邦贸易委员会发布的隐私问题报告中要求设计一 个禁止跟踪系统让用户能控制自己在网络上的隐私信息120)。随后，微软公司 宣布其下一款浏览器(Internet Explorer 9.0) 将会提供一个阻止第三

方追踪的黑名单，用以保护用户的隐私不被追踪。

当用户提出禁止跟踪请求时，具有禁止跟踪功能的浏览器在http 数据

传输中添加一个头信息(headers), 这个头信息向商业网站的服务器表明

[28]第三方 Cookie 与搜索引擎+网站广告原理，载于<http://www.mamicode.com/info>- detail-377965.html,2018 年2月23日最后访问。

**[29**]Federal Trade Commission(FTC):Staff Issues Privacy Report,Offers Framework for Consumers,Businesses,and Policymakers,Federal Trade Commission,Retrieved 2 May 2012。

**033**

**第一篇** **数据的权属与竞争**

用户不希望被追踪，这样，遵守该规则的网站就不会追踪用户的个人信息来 用于更精准的在线广告(30)。值得注意的是，禁止跟踪功能是一种自律机制， 它完全依赖于网站服务端是否自律，也就是说广告商可以忽略这个机制。有 些公司同意不再将用户数据用于保险、医疗等行业，但是依然有可能会用在 市场研究和产品开发中。因此，美国对于第三方 Cookie 隐私问题的解决方

案——禁止跟踪机制，并不是强制的法律规定，而是行业达成的自律承诺。

禁止跟踪在这一标准中区分了第一方和第三方，如果用户仍然使用的是 第一方平台的应用或者网页，那么该平台可以继续跟踪用户，但第三方则不能。 从保护用户隐私的角度来说，这是对于第三方Cookie 的合理规制，因为用 户在访问特定网站时，该网站留存和分析自己的 Cookie 数据是为了向用户 提供更好的服务，符合用户的合理隐私期待。但对于用户访问网站之外的其 他第三方获取其Cookie 数据，并用于广告营销分析，则超出了用户的合理

期待边界。

但从数据获取的视角出发，该标准实际上对第一方、第三方获取用户数 据做出了区别对待，第一方可以按默认方式获取用户行为数据，而第三方则 默认不能获取，除非用户主动关闭禁止跟踪机制。因此，如同opt-in 与 opt-out 模式影响了数据获取的效率一样，作为重要的隐私保护机制，禁止

跟踪机制实际也影响了不同市场主体获取数据的效率。

**(三)欧美个人信息保护政策对互联网产业的影响**

欧盟和美国个人信息保护政策有着较大的区别，其中对待opt-in、

opt-out 的不同立场以及关于 Cookie 的禁止跟踪机制的态度是这种区别的

典型代表。

[30]维基百科：请勿追踪 . 载<https://zh.wikipedia.org/wiki/8E88AFSB78E5%8B8BFSE>

88BF8BDSE8SB8&AA,2018 年2月2 3 日 最 后 访 问 。

**034****数据治理：数据政**

欧盟在最早制定个人数据保护立法时就崇尚对个人信 息自决权的保护，在个人权利的保护与互联网发展创新这 一对矛盾中，欧盟立法更倾向于对个人权利的保护，且该 指导思想一直延续至今。美国对于互联网的管理一直崇尚 的是保护创新，倡导行业自律，不通过严格的法律来限制 企业行为，因此美国个人信息保护在个人权利保护与发展 创新之间选择了后者。美国的做法在促进企业发展与创新 方面确实起到了积极作用，目前全球市值排名靠前的互联 网企业大部分都来自美国，而在欧洲却缺少这种大型的互 联网企业。当然，欧盟关于个人信息保护的严格立法在某

种程度上也是对美国互联网巨头企业的一种制衡。

**四** **、个人信息保护制度扩张对市场竞争的影响**

除 opt-in 、opt-out 、 禁止跟踪等个人信息保护机 制会对市场效率带来直接影响外，近年来随着欧盟对个人 信息保护法的持续改革， 一些新的保护机制与制度也会对

市场竞争带来影响，其中尤以数据可携权制度为代表。

针对成员国个人数据保护碎片化问题，以及云计算、 大数据带来的法律适用挑战，欧盟2012年启动了对《1995 年数据保护指令》的制度改革，在经过长达四年的立法进 程后，欧盟于2016年4月通过的GDPR条例于2018年5 月25日正式生效。GDPR条例继续坚守保护公民基本权利 的传统做法，全面提升个人数据保护力度，相比于1995年

版的指令， GDPR条例对数据主体的权利规定更细致入微，

**035**

**第一篇** **数据的权属与竞争**

为个人有效行使权利提供了坚实的法律保障。其中不仅包

括传统的个人信息保护法律中的个人权利，如知情权、访

问权、反对权等，还全面引入了新型的权利类型，其中最

典型的是数据可携权(第20条)的规定。

**(一)欧盟数据可携权的相关规定**

欧盟委员会在首次提出的 GDPR 条例草稿的第一个版

本中，就出现了数据可携权。此后，在2014年3月的欧

洲议会讨论版本中，可携权与数据获取权合并在一起。

2016年4月，在GDPR条例的最终版本中，数据可携权再

次被单独列为一个条款，并在其适用范围方面留出了许多

开放空间。

GDPR条例对于数据可携权的规定主要集中在第20条，

具体如下。

1. 当存在如下情形时，数据主体有权获得其提供给数

据控制者的相关个人数据，且其获得的个人数据应当是结

构化的、普遍可使用的和机器可读的，数据主体有权无障

碍地将此类数据从其提供给的控制者那里传输给另一个控

制者：

(a) 处理是建立在第6-1-a 点或9-2-a 点所规定的

同意，或者6-1条所规定的合同的基础上的。

(b) 处理是通过自动化方式确定的。

2. 在行使第1段所规定的携带权时，如果技术可行，

**036**

数据治理：数据政

数据主体应当有权将个人数据直接从一个控制者传输到另一个控制者。

3. 行使第1段所规定的权利，不能影响第17条的规定。对于控制者为 了公共利益，或者为了行使其被授权的官方权威而进行的必要处理，这种权

利不适用。

4. 第1段所规定的权利不能对他人的权利或自由产生负面影响。

尽管 GDPR 条例明确引入了数据可携权，但也考虑了数据主体权利与其 他正当权利之间的平衡，仅仅第20条难以完全解释数据可携权可能包含的丰 富含义，以及在具体实践如何执行。因此，作为欧盟个人数据保护立法解释 的权威机构，欧盟“第29条工作组”于2016年12月通过了《个人数据可携

权指南》,并于2017年4月对其进行了修订[31]。

《个人数据可携权指南》明确指出，数据可携权源于数据主体对于个人 数据的可访问权，但与可访问权存在许多差别。这项权利的核心目的是，赋 予数据主体对于个人数据更强的控制力。同时，考虑到这项权利赋予了数据 主体从数据控制者处直接获得并转移数据的权利，因此这项权利也将对数据 市场竞争带来直接的影响，用户切换服务提供商的门槛更低，减少了被数据“锁 定”服务的可能，进一步促进了数据的流动，并增强了企业(作为数据控制者)

之间的竞争。另一方面，对于用户而言，由于增强了个人对数据的控制力，

将有利于数据的汇聚，用户可以将使用不同服务产生的数据共同传输到第三 方，实现新的数据利用。例如，在健康领域，用户可以更加方便地对个人不

同的医疗数据、健身数据进行汇聚和利用。

《个人数据可携权指南》澄清了此项权利适用的基本前提，即要考虑数

[31]Article 29 Data Protection Working Party:Guidelines on the right to data portability,Adopted on December 13,2016,last revised and adopted on April 5,2017,16/EN WP 242 rev.01。

**037**

**第一篇** **数据的权属与竞争**

据处理活动的合法性要素，包括经过了数据主体的同意，

或者是为了履行合同而必需。明确这项权利仅仅适用于数

据主体提供 (provided) 给数据控制者的数据，但《个

人数据可携权指南》也提出， “提供”并不仅仅限于数据

控制者在明知、积极的状态下获得的数据(例如数据主体

通过在线电子表格的方式提供的数据),也包括因数据主

体的活动而产生的数据。

从 GDPR条例对数据可携权的表述看，该权利并不限

定在转移数据的场景。作为“数据访问权”的升级版，该

权利首先满足用户获得自身数据的需求，至于在获得该数

据后用户是否再转移，则取决于用户的选择。因此《个人

数据可携权指南》中举了两个具体的场景的例子： 一是用

户在使用在线音乐播放服务时，可以获得关于个人最近播

放的音乐清单数据；二是在使用电子邮箱服务时，获得邮

箱联系人信息。实践中，其实已经有这样的自发的商业形

态，例如 Google TakeOut, 用户可以按多种开放的数

据格式获取 Google+ 上的相关个人数据。

在用户选择直接转移的场景下，即从一个服务商传输

到另外一个服务商时，GDPR条例要求服务商应当“无障碍”

(without hindrance) 地进行传输。因此 GDPR条例

的背景及引言部分在解释数据可携权时，也鼓励数据控制

者形成更加具有兼容性的数据系统，以更有效地帮助用户

实现该权利。当然，使用“鼓励”这一措辞本身也意味着

发展兼容性或者互操作性的数据、系统格式，而这并不是

数据控制者的法定义务。

**038**

数据治理：数据政

**(二)数据可携权的适用问题**

1.数据可携权在哪些情形下适用?

根据 GDPR 条例第20条，数据可携权适用于自动化的数据处理活动， 并且该处理活动获得了数据主体的同意，或者该处理活动是为了履行与数据 主体签订的合同。因此，对于用户同意或者履行合同之外的数据处理活动， GDPR 条例并没有建立一般意义上的数据可携权。例如，金融机构依据欧盟《反 洗钱法》等行业专门立法的要求开展的防范和识别洗钱的特定数据处理活动， 并不适用于数据可携权。又如，在雇员数据领域，由于雇员的数据收集及处 理活动往往是在就职场景中发生的，而在这一场景中，考虑到用户的同意往 往并不是“自由”做出的，同时一些人力资源数据处理系统的合法基础是建 立在合法利益的基础之上的，或者是为了满足劳动法的基本合规要求，因此

对于雇员领域的数据可携权的适用，也需要个案式地分析判断。

2. 数据可携权适用于哪些数据?

GDPR 条例第20条对所适用的数据仅仅做了两个限定： 一是与本人相关 的个人数据，二是数据主体提供 (Provide) 给数据控制者的个人数据。因 此，匿名化的数据并不适用于数据可携权，但根据GDPR 条例对匿名化数据 (Anonymous Data)和假名数据(Pseudonymous Data)的区分，以及

对假名数据仍然属于个人数据的判断，假名数据仍然适用于数据可携权(32)。

在实践中往往会出现这样一种情形，即数据控制者掌握的数据往往同时 关涉几方数据主体，如电话记录不仅包括呼叫方信息，而且包括呼入方信息。 对此，“第29条工作组”的解释是，尽管同一份数据关涉多个数据主体，但

对于单个数据主体来说，这一份数据仍属于其个人数据，因此，其有权行使

[32]EU:General Data Protection Requlation Recital 26。

**039**

**第一篇** **数据的权属与竞争**

数据可携权。只是对于数据接收方而言，对于所接收到的

数据主体本人以外的其他第三方个人的数据，不可开展对

第三方权利及自由有所损害的数据处理活动。

“提供”给数据控制者的数据包括两类： (1)数据

控制者明知或者积极获取的数据，例如通过电子表格方式

由用户提交的数据，这在账户类信息中非常明显；(2)“提

供”也包括数据控制者在提供服务的过程中，通过自动记

录，“观察”(Observe) 得来的个人数据，比如搜索关

键词记录、流量数据、位置数据等。但“提供给”数据控

制者的数据并不包括：数据控制者根据用户提交的数据，

以及其观测而获得的数据，通过算法加工而产生的分析数

据，推测数据。例如，控制者为用户建立的用户画像数据、

信用评价数据等，这些数据的产生离不开控制者的智力和

资金投入，控制者对此类衍生数据也享有合法权益，不能

完全交由用户行使转移权利。

3. 对数据可携权适用的限定

GDPR 条例对适用于数据可携权的情形做出了必要的

限定，第20条第4款要求：数据可携权的适用不能对他人

的权利和自由产生负面影响。实践中，对他人的权利和自

由可能产生负面影响的例子更多地存在于数据可携权涉及

的数据中，不仅包括请求行使该权利的数据主体，而且可

能包括其他个人数据。典型的例子就是前面所提到的通讯

录、通话记录、邮件往来记录等信息。这些信息属于请求

行使数据可携权的用户，但同时也关联到与其有交互的其

他用户。

**040**

**数据治理：数据政**

在这种情形下，由于并没有机制使得其他用户了解这 种数据转移，对其他个人的权利产生负面影响的可能性会 很大。比如，对于通过数据可携权接收到数据的新的数据 控制者而言，其可以面向其他用户开展市场营销服务，甚 至是在未经其允许的情况下直接向其提供服务，从而侵犯

了不知情的第三方个人的基本权益。

为了避免这种情形的发生， “第29条工作组”给 出了一条非常艰难的解决路径。首先，涉及此类情形的 数据转移，获得数据的“新的”数据控制者所开展的数 据处理活动应当仍能保证数据主体的唯一控制 (Sole Control) 。 也就是说，这种数据转移只能服务于数据主 体的个人或者家庭活动。例如，个人可以将邮件通讯录上 传至云盘，用于个人的信息留存、备份目的。第三方云盘 仅能提供此类存储服务，而不能超出“唯一控制”目的提 供其他服务。获得数据的新的“数据控制者”不应当基于 其商业目的，利用数据主体提供的其他第三方的个人数据 开展商业活动，例如通过获得的新数据，丰富第三方的个 人数据画像，或者创建第三方的个人数据档案。其次，为 了防止对第三方个人产生危害，《个人数据可携权指南》 鼓励数据控制者能够对用户数据进行剔除，以保证尽可能

最少地涉及其他第三方数据。

考虑到这些数据已经通过数据可携转移到了新的数据 控制者手里，做到上述要求无非是要求商业主体能够“洁 身自律”地不去触碰新数据，这无异于一种幻想。大多数

数据保护规则会增加数据市场上新的竞争主体的进入门

**04I**

**第一篇数据的权属与竞争**

槛，因为它会限制对个人数据的收集和使用。但是数据可携权为市场参与者 带来了便利，它使收集个人数据变得更加便利，进而便利市场进入。数据可 携权刺激竞争，对数据再使用有着积极的作用；但它也给市场参与者增加了 合规负担，并且对于包含其他第三人情形的数据可携转移，对不知情第三方 的权益保护的作用是积极的还是消极的，目前的GDPR条例及“第29条工作组”

的《个人数据可携权指南》似乎都没有给出明确的答案。

GDPR条例中对于数据可携权的适用排除了对于他人的权利或自由产生负 面影响的场景。而在实践中，可能相关的他人合法权利还包括商业秘密、知 识产权(特别是软件版权)。但是，对这些权利的考虑并不必然可以拒绝用 户提出适用数据可携权的全部要求，在特定情形下，可以将涉及他人合法权 利的信息剔除之后提供给用户。在实践中，这种剔除工作本身也带来了挑战。 许多企业持有的数据资产没有达到受知识产权保护的资格，这些数据不会产 生知识产权冲突。但特殊的数据库权利区分可能会困难，因为数据库上存在 多种权利，独立于系统的附加保护层更不容易剥离。商业秘密也是如此，虽 然信息是由用户提供的，但是并不排除它构成更广泛的商业秘密权的基础[33]。 而对于用户而言，其不能通过适用数据可携权对他人合法的知识产权权利予

以侵害。

**(三)数据可携权项下的法定义务**

为了协助用户实现数据可携权，数据控制者负有相对应的法定义务。如 在数据主体的请求下，以特定格式提供或者传输相关个人数据。为进一步澄 清法定义务的内容，《个人数据可携权指南》将数据控制者分为响应数据可 携权请求的数据控制者(Data Exporter)以及在此请求下接收相关数据

[33]Inge Graef,Martin Husovec,Nadezhda Purtova,“Data Portability and Data Control Lessons for an Emerging Concept in EU Law”,TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES,No.22/2017。

**042**

**数据要素**

**数据治理：数据政策发展与趋势**

的数据控制者 (Data Importer) 两类，以明确其法定

义务的边界。

首先，对于响应数据可携权请求的数据控制者 (Data Exporter) 来说，其只面向数据主体本人，并不负有检 查数据接收者是否符合个人数据保护法各项要求的义务。 因为从数据流转来看，该数据接收者并不是由数据控制者 挑选的，而是由数据主体本人决定的。因此，数据控制者 需要采取配套措施，以证明其向第三方传输的数据是经数 据主体本人请求的。另外，数据可携权并不影响数据留存。 数据控制者并不能以在将来有可能要为数据主体提供数据 可携服务为由，超出数据处理目的的合理期限留存数据。 这也意味着，对于数据控制者已经删除而不再保留的数据，

用户也无法主张数据可携权。

在实践中，数据可携的请求可能事实上是由数据处理 者操作的，在数据控制者与数据处理者之间的合作协议中 需要明确相关事宜。GDPR条例第28条规定的“数据处理 者”中明确说明“数据处理者应当采取合适技术与组织措 施，其处理方式符合本条例要求，并且保障数据主体权利”, 对于联合的数据控制者，则应在协议中明确在处理数据可

携权请求时二者的责任分工。

其次，对于数据接收方而言，应当确保其通过数据可 携方式接收的数据与其数据处理活动是相关的，通过传输 获得的数据不能超过其数据处理目的。超过必要范围的数 据，数据接收方不得保存或处理。例如，在用户在电子邮

件服务中，行使数据可携权，将其邮件传输到一个安全的

**043**

**第一篇** **数据的权属与竞争**

电子档案存储平台中，以实现用户“唯一控制”的备份存

储目的。数据接收方并不需要去获取用户在上一个电子邮

件服务中所有的电子邮件通信者的联系信息。

考虑到数据接收方也是GDPR条例所规范的数据控制

者，因此在其通过数据可携权方式获取数据时，也应当符

合GDPR条例第14条的相关规范，即“当个人数据并不从

数据主体本人处收集时，数据控制者应当提供的信息”的

要求，向数据主体提供包括数据处理目的等相关必要信息。

当然，数据接收方并不负有法定义务必须接受来自数据主

体的个人数据。

再次，数据可携权并不影响用户行使其他数据权利类

型。当用户发起数据可携权需求时，并不必然要求原数据

控制者删除其个人数据。只要原数据控制者仍掌握和处理

用户数据，用户就仍然可以向其主张行使各项数据权利。

如果用户认为其数据可携权未被充分满足，那么也可以通

过主张其他权利，如数据访问权，来向数据控制者提出质

疑。GDPR条例中规定的数据可携权可能会与欧盟成员国

的国内立法，或者其他行业领域的专门立法中规定的类似

权利有重合现象。如果用户依据其他行业的专门立法来请

求数据转移，那么适用专门法，而不适用GDPR条例。例

如，根据《欧盟支付服务指令》,用户可以将个人的银行

账户信息转移给第三方的账户信息服务提供者。而当用户

适用GDPR 条例而主张数据可携权时，其他专门立法并不

必然凌驾于GDPR条例之上，这需要具体案例具体评估，

以避免其他立法规定不合理地影响到 GDPR条例的适用。

**数据要素**

**数据治理：数据政策发展与趋势**

**五** **、数据可携权等制度面临的质疑与挑战**

数据可携权在欧盟2012年数据保护制度改革建议稿中 一经提出，就受到了众多质疑。这一新创设的权利能够为 用户提供便利，减少用户转换服务提供者的成本，从而能 够更有效地促进业务竞争。但是深入研究会发现，有关锁 定用户的成本以及用户转换服务时所遇到的阻碍问题完全

可以通过竞争法来解决。

竞争法历经百年发展历史，已经形成了较为严密和 成熟的基础理论，它不仅考虑到了用户的锁定成本，而且 考虑到了锁定还会带来一定的消费者福利，甚至一定的转 换成本可以鼓励对新技术业务的投资，从长期来看是具有 效率的。竞争法的适用是以企业在市场上具有显著市场地 位，并滥用该地位损害正当的市场竞争为前提的，其规则 适用具有复杂而严密的程序要求和违法构成要件。而根据 GDPR条例规定，数据可携权作为用户的基本权利，可以

被要求适用于任何一个机构，包括新兴企业在内。

美国学者皮特斯·怀尔(Peter Swire) 与扬尼·拉 各斯(Yianni Lagos) 在“为什么数据可携权可能会降 低消费者福利?”一文中，对2013年的GDPR条例(草稿) 中关于数据可携权的规定曾进行了全面的批判，认为数据 可携权与竞争法机理背道而驰，动态效率和创新减少，并

且会对数据安全等带来威胁。

**(一)数据可携权的规定可能与竞争法背道而驰**

数据可携权的观点是很有吸引力的，消费者也喜欢可

**045**

**第一篇** **数据的权属与竞争**

以将数据轻松转移到新的服务商的便利性，但是，数据可

携权的条款与美国的反垄断法，甚至与欧盟竞争法并不吻

合。竞争法中经营者滥用市场支配地位行为的前提是其被

认定(或推定)具有市场支配地位。欧盟委员会认为，市

场份额低于40%的公司较难具有市场支配地位；美国的反

垄断法对市场力量的要求也很高，除高的市场份额外，经

营者必须具备影响准入门槛的能力才可能被证明具有强的

市场力量。但是，欧盟数据保护草案中规定的数据可携权

适用于任何通过自动化方式处理数据的公司，包括初创公

司，并不考虑该经营者是否具有比较强的市场力量，这就

与竞争法的规定相背离。

竞争执法机构很难对没有市场力量的中小企业( SMEs)

采取执法行动，因此规范中小企业的数据可携权有三大可

质疑之处： 一是中小企业很少有市场力量；二是中小企

业的合规负担相对于收益来说可能更重；三是条例草案

中还就数据转移模式进行了特别规定，提出了Export-

Import Module(EIM) 的数据转出转入模式，这一命

令远远超出了先前的关于互操作性的法律规则。如果小型

软件公司从一开始就被要求编写EIM 程序以遵守数据可携

权，那么创新就可能会受到影响。

观察数字经济的商业模式，“锁定”在很多场景下是

一种理性的竞争选择，服务商会有动机避免用户随意切换。

例如，尽管谷歌、Facebook 面向用户提供其数据副本，

但往往会对用户直接将个人数据转移到其他平台有所限

制。Faceboo k 阻止谷歌浏览器 Chrome 直接将用户朋友

046

**数据治理：数据政策**

关系导出，即使用户可以通过手动方式整理其个人社交网 络档案信息，将个人照片、音视频下载整理。Facebook 的服务协议中也明确禁止用户通过自动化方式收集用户信

*[34]Facebook 用户*

协议安全条款：未经 允许，您不得通过自 动化方式(如收获机 器人、机器人、蜘蛛、 scraper) 收集用户 信息内容。

息内容(34),

在考察实现消费者福利目标的最佳方式时，美国和欧 盟竞争法有“理性地适用”规则，而不是拘于条例草案关 于数据可携权的简单规定。对于数据的格式，条例草案条 款要求数据以“结构化的” “通用的”模式提供。尽管结 构化的数据格式可以实现更简单的数据传输，但关键问题 是，没有明确的工具可以确定哪些格式被认为是结构化的。 一旦数据执法机构负责确定哪些格式是结构化的，它还需 要确定该格式是否被普遍使用。结构化格式不一定是常用 的，因为许多标准并未被广泛采用。实践中，由数据执法

机构来衡量消费者实际使用的数据格式的难度很大。

**(二)数据可携权可能会减少动态效率和创新**

数据可携权可能对动态效率和消费者福利产生重大

影响。

首先，数据可携权创造了一个不正当的激励。条例草 案规定：数据可携权仅适用于“以电子和常用结构化格式” 处理数据的公司。根据条例草案的字面意思，公司如果决 定不使用电子和结构化格式，就可以避免承担数据可携义 务，包括提供具有EIM模式的数据格式。具有讽刺意味的 是，这种旨在提高互操作性的措施可能导致企业减少使用

促进互操作性的标准格式。随着使用非结构化格式的增加，

**047**

**第一篇** **数据的权属与竞争**

数据可携权可能会加剧当前的“数据锁定”问题，而这正

好与期望的结果相反。

其次，实现消费者福利的主要考虑因素是如何为创新

创造激励。数据可携权和互操作性的支持者通常认为更大

的互操作性会导致更多的创新。但是，进入市场的成本降

低后，在数据的互操作性方面也会减少创新。解决第一方

和第二方之间的创新问题是一项复杂的任务。这种复杂性

的问题须基于特定的市场特点而非一刀切的数据可携权规

则。而过去的商业实践表明，科技行业的动态竞争才会产

生更多创新。

科技市场的基本特征是一个玩家领先，然后成为

市场领导者，往往拥有很大的市场份额。经济学家对

这一现象提出了三个术语：先发优势(First-mover

Advantage)、 网络效应(Network Effects)和倾覆

效应(Tipping Effect)。业务创新的进入是昂贵而具

有风险的，如果规则明显降低到了进入市场的盈利水平，

那么可以预期新业务中的创新将会减少。

竞争法鼓励创造动态效率的技术创新，但数据可携权

的规则在市场竞争激烈的情况下，往往会减少创新。基于

欧盟法规定的数据可携权制度，公司可能会因为预期收益

较低而决定不进行风险投资，消费者可能会因此享受不到

创新福利。

**(三)数据可携权可能会带来数据安全风险**

数据可携权最为突出的问题是，对用户本人身份的验

**048****数据治理：数据政**

证问题，如果他人假借用户之名行使数据可携权，将带来 严重的数据安全问题。GDPR条例在总结过去制度经验的 基础上，做出了不对用户身份进行验证的规定，其中第11 条是关于不需要识别的处理，具体为： (1)如果控制者 处理个人数据的目的不需要或不再需要控制者对数据主体 进行识别，那么控制者就不再具有为了遵循本条例而维持、 获取或处理额外信息以识别数据主体的责任。(2)对于 第1段所规定的情形，如果控制者能够证明其不适合识别 数据主体，如有可能，数据控制者应当告知数据主体。在 此类情形下，除非数据主体为了行使第15至20条所规定 的权利，需要提供额外信息而使得对其识别变得可能，第 15至20条将不应适用。也就是说，如果数据处理并不需 要识别用户身份，那么数据控制者并不要求获取更多的信 息去验证用户身份，这实际上是出于保护用户身份安全的 角度而设计的条款。相应地，在用户并不主张数据权利的 情形下，包括主张(访问权、更正权、删除权、被遗忘权、 可携权)等权利，数据控制者没有义务去为这些权利的实

现提供辅助。

当然， GDPR 条例第12条规定了在没有身份信息的场 景下，用户主张行使权利的情形。第12条(2)规定：控 制者应当对数据主体行使第15至22条的权利而提供帮助。 对于第11条(2)所规定的情形，当数据主体请求其行使 第15至22条的权利，控制者不应拒绝，除非控制者能够 证明其并不适宜识别数据主体。换言之，如果由用户发起

数据权利主张，那么应由用户提供相应的额外信息，以帮

**049**

**第一篇数据的权属与竞争**

助数据控制者验证其身份，为后续实现权利提供基本的必

要条件。需要澄清的是，验证身份并不必然代表验证用户

的真实身份，而是需要验证主张数据权利的用户和服务中

的数据主体的身份一致。因此， 《个人数据可携权指南》

要求数据控制者不得因为验证的需要，而要求数据主体提

供超过必要范围的个人信息用于验证。实践中，用户可通

过用户名、密码访问到个人数据，此类信息并没有披露出

用户的真实身份，但同样满足了身份验证目的。考虑到数

据可携权可能带来的数据转移后果，对数据主体本人的权

益影响会更大，因此如何去确定身份验证标准仍需要深入

探讨。

更为重要的是，在欧盟现有的数据保护基本权利框架

内，数据可携权这一新创制的权利与个人现有的数据安全

权利紧密相关。因此，定义数据可携权应充分认识到数据

安全权利的风险。欧盟法并没有关注到数据安全权利，数

据可携权将带来安全风险，无障碍获取数据更是增加了额

外的风险。如果将其应用于敏感信息领域，由于互联网上

缺乏有效的认证机制，那么更容易导致数据可携权在线服

务面临安全挑战。

**(四)数据可携权能否促进互操作性的实现**

GDPR 条例第20条规定：数据主体有权无障碍地将

个人数据从其提供给的控制者那里传输给另一个控制者。

在实践中，可能以下方式会构成“障碍”:(1)收费，

或者是收取不合理费用；(2)数据格式缺乏互操作性；

**050**

**数据治理：数据政**

(3)没有数据访问入口； (4)过分延迟； (5)在获取完 整数据时过分复杂；(6)对可访问数据库增加复杂度等。 GDPR 条例第20条(2)进一步规定：如果技术可行，数 据主体应当有权将个人数据直接从一个控制者传输到另一 个控制者。需澄清的是，本款并不意味着要求数据控制者 发展出与其他数据控制者相互可操作的数据处理系统，只 是在客观上已经具备这种技术传输条件时，不得拒绝用户 直接转移数据的请求。从方便数据传输的角度， GDPR条 例第20条(1)实际上已经提出了具体的要求，包括结构化、 可普遍使用、机器可读，这三点实际上可以视为“可互操作”

的最基本要求。

上述规定的核心是解决数据的再利用问题，即用最小 的成本在实现用户转移数据的同时，也无缝实现对数据的 再利用。以“机器可读”为例，传输的数据不仅包括数据 内容本身，而且需要包括相关元数据，以协助其他数据系 统识别、提取相关数据。 《个人数据可携权指南》指出， 数据控制者在考虑以何种数据格式提供数据时，应当考虑 数据主体再利用该数据的场景，以有利于实现用户的数据 再利用目的。当然，这直接带来的问题是，对数据控制者 提出如此之高的要求，是否已经超出了数据保护法的边 界?不仅担负保护用户数据的责任，而且需要考虑到数据 的后续利用，甚至进一步要为第三方对数据的后续利用扫 清障碍，提供尽可能多的信息，这是否已经违背了市场竞

争中最基本的原理?

对于计算机开放性的支持者而言，互操作性是一个理

**051**

**第一篇数据的权属与竞争**

想的目标。1991年欧盟发布的《计算机程序指令》允许第二方对第一方程序 进行观察研究，复制必要的信息，以实现与第一方产品的互操作性。但到目前， 并没有法律规定要求第一方提供EIM 模式来帮助第二方实现互操作性。不可 否认的是，互操作性具有十分强的吸引力。但与此同时，市场趋势也表明消 费者喜欢对互操作性有所限制的系统，典型地如苹果系统。实际上这些限制 有助于保护安全和隐私，降低应用程序获取不必要的个人数据所带来的风险。 这些消费者偏好的例子表明，通过确定数据可携权，对所有在线服务提供商

提出互操作性要求缺乏客观评判的尺度。

**六、结语**

本文系统讨论了隐私保护与市场竞争之间的关系，并从个人信息保护法 的视角出发，探讨了个人信息保护制度对市场竞争的影响，特别以“知情- 同意”这一核心的个人信息保护机制的不同模式来探讨其对效率、市场竞争

的影响。

随着个人信息保护制度的发展，其中尤以欧盟GDPR条例为代表，个人 信息保护制度与竞争法律制度产生了越来越密切的互动关系。GDPR条例中提 出的数据可携权，是个人信息保护制度的一次极大扩张。欧盟竞争事务委员 阿尔穆尼亚 (Almunia) 指出“数据可携权已经直达了竞争政策的核心”(35) 这直接产生了个人数据保护法与竞争法的竞合问题。竞争执法机构是否可以

以数据控制者违反数据可携权的要求，开展竞争法执法?

[35]Commissioner Almunia,“Competition and Personal Data Protection”,

speech given at the Privacy Platform event:Competition and Privacy in Markets of Data in Brussels on November26,2012,available at http://

europa.eu/rapid/press-release\_SPEECH-12-860\_en.htm.,last visited on Feb.24th,2018。

**052****数据治理：数据政**

GDPR条例对数据可携权只有一个条文规范，尽管欧 盟数据保护机构——欧盟“第29条工作组”专门对争议极 大的数据可携权发布了《个人数据可携权指南》,但仍未 解决数据可携权带来的问题，而且《个人数据可携权指南》 的相关说明还反映出欧盟立法者对数据可携权的考虑并不 成熟，其初衷是为了增强用户对个人数据的控制权，但显 然并没有对可能带来的竞争、安全问题开出良方。这些问 题包括但不限于：在个人数据涉及其他第三人时，如何在 适用数据可携权规定的同时，避免对不知情第三人合法权 利的损害?面向所有数据控制者都适用的数据可携权，如 何解决中小企业的合规负担问题?数据可携权如何在保护 用户合法权益的同时，为市场创新提供适当激励?作为个 人信息保护执法机构是否有足够的能力解决数据可携权带 来的市场竞争扭曲问题?由此可知，关于大数据应用中个 人信息保护法与竞争法关系问题的研究仅仅是一个开始，

理论研究与实践探索还任重而道远。

IHHH!!!!!!!!!!!!!!!



**第二篇**

**世界各国数据保护做法**

2018年，是个人数据保护立法与实践具有里程碑式成

就的一年，这一年，欧盟GDPR 生效，美国加州CCPA出台，

并继续带动全球个人信息保护立法步伐。与此同时，随着

云计算的快速发展，数据跨境流动，跨域执法数据协作机

制成为一个新的议题。

**054**

数据治理：数据政



**第5章**

**全球视野下的个人数据保护立法与实践**

**摘要：**2018年是国际个人数据保护立法多有成就的一 年，从“新兴国家”的越南、印度、巴西，到“发达国家” 的澳大利亚、加拿大、日本和韩国，都多有动作。欧盟的 GDPR和美国加州的CCPA 更是具有标志性的事件。我国也

非常关注个人信息保护与数据治理的综合性问题。

**一** **、个人数据保护法的全球普及**

截至2018年，全球近120个国家和独立的司法管辖区 已采用全面的数据保护或隐私法律来保护个人数据，另有

近40个国家和司法管辖区有待批准此类法案或倡议。

新兴国家表现出对个人数据保护立法的极大热情。 2018年6月12日，越南《网络安全法》通过，对个人信 息保护做出了规定。2018年，印度发布《2018个人数据保 护法(草案)》。2018年8月14日，巴西批准了《通用

数据保护法》,该法将于2020年初生效。

发达国家补充和完善既有法律。2018年2月22日， 澳大利亚隐私法修正案《数据泄露通知计划》(NDB) 正

式实施。2018年11月1日，加拿大《个人信息保护和电



子文件法案》 (PIPEDA)

据泄露通知报告要求。

**055**

**第二篇** **世界各国数据保护做法**

修正案生效，增加了强制性数

GDPR 生效，开启欧盟成员国新一轮立法。尽管 GDPR

与其前身1995年的《数据保护指令》不同，它直接适用于

所有成员国，但每个成员国仍然需要更新本国的数据保护

法，以使其与GDPR 保持一致，并且，根据 GDPR 中预留

给各成员国的立法空间来补充国内法。据统计，在GDPR中，

包括儿童年龄标准、敏感数据的保护规则等50个领域可以

由成员国来继续做出规定，这也使得所谓的GDPR“一站式”

立法在欧盟仍然有碎片化的风险。

二 、GDPR 从文字走向落地，正负面

影响并存

GDPR本身还是一个处于探索塑造期的新生儿，需要

大量条款和细则予以澄清。截至目前，欧盟数据保护机

构——EDP B已发布共20项、约15万字的“指南”以回

应各方关切。指南涉及的内容极其广泛，包括数据保护官、

数据保护影响评估、识别主导监管机构、行政处罚、充分

保护认定、BCR 基本原则等。

欧盟各成员也陆续颁布GDPR指南。2018年2月，德

国联邦和州独立数据保护机构会议(DSK) 分别发布了数

据控制者、数据处理者的处理记录模板，以及GDPR第30

条处理记录指南。2018年9月下旬，法国数据保护监管机

构“国家信息与自由委员会” (CNIL) 发布了关于区块链

的 GDPR 合规指南。

**056**

**数据治理：数据政**

欧盟各成员国监管机构 DPA开始执法活动。体现 GDPR 严格性的重要因素之一是其巨额的罚金，但从目前 已有案例观察，GDPR的执法力度总体呈现轻缓色彩，这 说明监管执法仍处于过渡阶段。GDPR生效后，欧盟各成 员国的监管机构所收到的违规投诉和数据泄露报告的数量 均显著增加，但各国因违反GDPR 而导致的罚金数额总体 不大。对于具体处罚，大多成员国 DPA对第一次违规行为 只给出警告、建议和纠正措施。德国数据保护当局更是明 确表示，处罚应当“责罚相符合”,德国数据保护当局没

有意愿加入GDPR最高罚款的“案例竞争”。

围绕 GDPR的争议纠纷也涌入司法系统。全球首例关 于GDPR的法院裁决凸显出GDPR与实践的冲突。2018年 5月29日，互联网名称与数字地址分配机构 ICANN 向德 国波恩法院申请临时禁令，请求法院禁止德国域名注册商 EPAG 在分配域名时放弃收集域名申请者的技术联络和行 政联络的数据，但法院驳回了申请。 一般而言，技术联络 和行政联络数据是确认域名注册主体真实身份的关键，对 于预防和调查网络犯罪、知识产权维权都具有重要意义， 如果因GDPR合规要求而拒绝收集此类数据，对互联网世

界的身份管理带来了新的难题。

除了法律实施层面，外部观察者就GDPR对数字经济 的影响展开研究。从正面看，GDPR 显著促进了机构对于 数据保护的投入。据估计，《财富》世界500强公司在对 合规投入约78亿美元。但与此同时，也有许多中小企业因

担心过高的法律风险，宣布停止向欧洲地区服务。



**第二篇** **世界各国数据保护做法**

2018年11月，美国权威经济学组织——国家经济研

究局 (NBER) 发布报告《GDPR对科技创业投资的短期影

响》。该报告以翔实的数据，严谨的计量经济学模型，对

GDPR给欧洲科技行业带来的负面影响进行了分析。表明

在 GDPR推行后，欧盟国家企业的融资总额、融资交易笔

数以及每笔融资交易金额均大幅减少，GDPR使新企业每

周减损90万美元投资，使成熟企业平均每周减损710万美

元投资，其对于新业务发展的负面影响是显著的。

**057**

三 、美国加利福尼亚州出台 CCPA,

与欧盟保持立法差异

2018年6月28日，美国加利福尼亚州公布《2018年

加州消费者隐私法案》(CCPA) 。 本法案对企业提出了更

多通知、披露义务，并针对数据泄露规定了法定损害赔偿

金，是目前美国州层面最严格的隐私立法，也被视为最具

有GDPR 色彩的美国隐私立法。这不禁引人联想：加利福

尼亚州立法是否代表了美欧隐私立法走向融合趋同?

形式上，CCPA与 GDPR有相似之处，但仍然有三方

面的根本性差异，突显了美国法的实用主义哲学，重视权

利保护与技术创新之间的平衡。

第 一，CCPA的适用做出了合理排除。其一，在守规

则的实体上， CCPA做了三类排除： (1)仅提供数据服

务的企业 (Processor),(2) 非营利机构， ( 3 ) 没

有达到适用门槛的中小企业。而在 GDPR下，所有任何规

 **058** **数据治理：数据政**

模的实体都受约束，遵守相同的高标准合规要求，这也解 释了为什么 GDPR 生效后对中小企业带来市场竞争的扭曲 效应。其二，在规制的数据处理活动上， CCPA重点规制 数据的收集、买卖和共享三种活动，而 GDPR笼统地包含

了所有数据处理活动。其三，在排除适用的数据活动上，

CCPA非常务实地排除了“集合信息”“去识别化数据”, 以及联邦法已经覆盖的医疗、征信、驾驶、金融、政府公 开数据等；而GDPR 仅排除了匿名数据，根据欧盟对匿名 数据的严格解释标准，GDPR 对于匿名数据的排除适用门

槛极高。

第二， CCPA仍然保持了美国隐私法的基本特色，仍 然以“选择一退出” ( opt-out) 为主要机制。

第三，围绕着同意机制，CCPA比 GDPR有更多的弹

性空间。

**四** **、国内多部法律并行推进数据保护规则**

自2016年《网络安全法》首次在法律层面构建了个人 信息保护较为完整的法律制度闭环后，我国法律层级的数 据保护制度建设步入加速期，其中既包括网络法，又包括

传统法，并兼有公法与私法视角。

2018年8月，《电子商务法》历时五年终获通过，其在《网 络安全法》基础上，对个人信息保护规则做了进一步细化。 例如要求经营者对于用户查询、更正、删除用户信息及用

户注销的方式和程序进行明示，且不得设置不合理的条件



**第二篇** **世界各国数据保护做法**

**059**

使上述权益无法实现等。而在实践中，作为电商应用的高

频场景，大部分电商平台自身也支持用户查询、修改包括

名称和收货地址在内的个人信息，对个人订单也可轻松实

现删除等操作。但对于“删除” “注销”功能如何与数据

留存等安全性义务相衔接，还需做探讨。

2018年9月6日，作为《民法典》首编——《人格权编(草

案)》面向全社会公开征求意见。本编内容包括隐私权和

个人信息保护，从民法视角提供保护机制。但从公布的条

文看，其将民事主体的姓名、名称、肖像、隐私、个人信

息的并列提法，似乎显露了在民法理论层尚未厘清隐私与

个人信息之间的交叉重叠关系。此外，该编对《网络安全法》

中的个人信息保护条款多有复制，这引出了作为私法的《人

格权编》与公法的《网络安全法》的相互关系问题。

2018年9月10日，全国人大公布十三届全国人大常

委会立法规划，其中《个人信息保护法》《数据安全法》

一并列入第一类项目立法项目，集中代表了我国公法体系

对于数据安全问题的关注。但结合《人格权编》带来的私

法与公法规则的关系问题，我们又将面对《个人信息保护

法》与《数据安全法》两套公法规则体系的协调与统筹问题。

不同性质法律规范的重叠交叉揭示了我们正处于一个

微妙的历史变化期——从“个人信息保护”向“数据治理”

转变，“数据治理”正在以更宏大的议事命题显现，形成

了围绕数据资产的隐私保护、创新竞争、安全性主权等更

复杂化、更多维的公共政策讨论场。

**060**

**数据要素**

数据治理：数据政策发展与趋势

**五、个人数据跨境流动机制曲折发展**

2018年，欧美分别主导的个人数据跨境流动机制在曲

折中取得实质性进展。

GDPR 对欧盟数据跨境流动政策限制有所松缓。

第一，GDPR明确禁止了原“95数据保护指令”下， 部分成员国针对跨境数据流动增加事前备案或者许可要求 的做法，规定只要符合了跨境数据流动的条件，则成员国 不得再予以限制。第二， GDPR赋予“95数据保护指令” 中的有约束力公司规则(BCR) 正式的法律地位。第三， GDPR增加了成员国数据监管机构可以指定标准合同条款 的渠道。第四，除了对国家做充分性认定外，还可以对一 国内的特定地区、行业领域以及国际组织的保护水平做出 评估判断。第五， GDPR引入了签章、行为准则认证等跨

境流动机制，为后续与APEC CBPRs衔接提供了可能空间。

在此背景下，日本、韩国积极争取进入欧盟“白名单”。 2018年9月，欧盟正式启动对日本的充分性认定程序。11 月15日，韩国国民议会提交了《个人信息保护法》“修订”, 新的“修订”将使韩国个人信息保护执法系统获得独立地

位，这将有望为韩国期待已久的欧盟充分性认定铺平道路。

除 了GDPR外，欧盟面向全球推行的——《有关个人 数据自动化处理之个人保护公约》(“第108号公约”) 在2018年5月18日完成了版本迭代，继续推动欧盟之外 国家向欧盟数据保护标准靠拢，并继而实现欧盟的数据跨

境流动理想框架。

**061**

**第二篇** **世界各国数据保护做法**

当然，在 GDPR严格的个人权利保护机制下，欧盟放

宽对个人数据跨境流动政策的过程并不是一帆风顺的。

继“安全港”协议被欧盟法院推翻后，在2017年Max

Schrems 起诉 Facebook 一案中，标准合同条款机制的

合法性也遭到挑战。目前，关于该机制合法性的最终结果

正在等待欧盟最高法院的裁决。

而在大西洋另一端，美国主导下的“亚太隐私数据跨

境体系” (APEC CBPRs) 也在沉寂期后迎来实质性进展。

2018年3月，新加坡加入CBPRs 体系。11月，澳大利亚

和中国台湾地区申请加入并获得APEC批准。截至年底，

在APEC 21个经济体中，已有8个经济体加入CBPRs 体系。

**六、跨域执法数据协作新的探索与冲击**

2018年3月23日，美国总统特朗普签署了长达2000

多页的政府预算支出法案。作为预算法案最后一部分的

“澄清合法使用海外数据法案” (clarify Lawful

Overseas Use of Data Act, CLOUD) 被连同一并

签署，随即生效。

CLOUD法案解决的是刑事领域的证据跨境调取问题。

在内容上分为美国调取域外证据规则和外国调取美国所控

制的数据规则。在流程上规定了美国与其认可国家之间的

证据调取程序，以及通信服务提供者的抗辩程序，其中，

被美国认定为合格的外国政府，与美国政府将建立起更为

便捷的跨境数据调取路径。

**062**

数据治理：数据政

但这并不能一蹴而就地解决数据跨境调取问题，只是 为其提供了一个框架。不论是对适格外国政府的认定标准， 还是对行政协议订立的要求，都带有原则性特征。该法案

在实践中发挥作用，还要对其进一步解释和细化。

该法案的意义在于，尝试推动美国现有的数据安全 和司法协助法律能够适应当前以云计算为代表的数字技术 的发展，改革现有的冗长司法协助机制MLAT, 为执法协 作中的数据跨境获取设定新的实质性和程序性保护规则， 同时为美国企业减少来自海外本地化要求提供一种制度动 机。但与此同时，该法案导致了对行政权力过度扩大危害

隐私等基本人权的担忧。

在美国提出CLOUD 法案之后，欧盟迅速做出反 应。2018年4月17日，欧盟提出了《电子证据条例》 (e-Evidence Regulation, 简称《条例》)草案， 该草案于12月7日获得欧洲司法部长批准，而欧洲议会计 划在2019年5月底换届之前完成对《条例》的表决。《条

例》包括以下内容。

《欧洲数据生成令》(European Production Orders): 允许一个成员国的国家机关直接从服务提供 商处获取电子证据(例如应用程序中的电子邮件、文本或 消息，以及识别犯罪者的信息),该服务提供商在另一成 员国的法定代表人有义务在10天内做出答复，并在紧急情 况下于6小时内做出答复(现有欧洲调查令的回复期间最

长为120天，法律援助的处理周期则为10个月);

《欧洲数据保全令》 (European Preservation

**063**

**第二篇** **世界各国数据保护做法**

Orders): 允许一个成员国的国家机关要求另一成员国

的通信服务提供者或其法律代表保留特定数据，以便随后

通过司法协助、欧洲调查令或欧洲电子证据调取令提取这

一数据。

简言之，欧盟《电子证据条例》允许执法官员更快地

从其他国家获得电子证据，虽然目前该条例因为隐私争议

而尚未获得绝对支持。

对于这一问题，我国仍然坚持传统的跨境司法协助方

式。2018年10月26日，我国《国际刑事司法协助法》发

布实施，规定了我国和国外之间相互提出调查取证请求的

程序性和实质性规则，但其仍旧是围绕传统的司法协助方

式，并没有突破性进展。

而从跨域执法数据协作问题本质来看，其更适合在国

际平台上进行讨论。2018年4月，联合国公布《跨境提取

电子证据实践指南》,可以看出，联合国对直接跨境调取

电子证据总体持谨慎态度，既没有完全复制CLOUD法案的

框架，也没有完全抱定旧有规则，而是在充分尊重国家主

权的情况下对个别情况下的直接取证进行了试探性规定。

总之，跨域执法数据协作机制中出现最大的突破是，

在特定情形下，允许外国执法机关直接向位于某国国内的

通信服务提供者调取数据。这种新机制对传统形式的通过

司法协助请求，依赖被请求国机关调取数据的方式形成了

冲击，而深藏在其背后的是对国家主权是否延伸至网络空

间的判断。尽管从目前各方发布的规范来说还都是框架性

规范，但已揭开了数据跨境执法协作改革的序幕。

**064**

**数据治理：数据政**



**第6章**

**欧盟《通用数据保护条例》详解**

**摘要：** 欧盟《通用数据保护条例》于2018年5月25日正式生效。为踏 上数字时代新秩序的起跑线，全球企业都在积极准备合规工作。本文全面梳 理其带来的重大变化，既为企业提供参考，又为我国政府考虑大数据背景下

的数据保护规则提供新视角。

2012年，欧盟启动对1995年《数据保护指令》(1)的修订工作。在历

经四年多的立法协商之后，欧盟《通用数据保护条例》 (Gen eral Data

Protection Regulation, 简称《条例》)2正式通过，并于2018年5

月25日全面实施。以下详细介绍《条例》带来的十方面的主要变化。

**一** **、极大地扩展了《条例》的适用范围**

法律的适用范围，从过去的“属地”向“属人”扩展。1995年《数据保

[1]Directive 95/46/EC of the European Parliament and of the Council

of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2]REGULATION(EU)2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

data,and repealing Directive 95/46/EC(General Data Protection

Regulation) (Text with EEA relevance)THE EUROPEAN,4.5.2016 L 119/1 Official Journal of the European Union。

**065**

**第二篇** **世界各国数据保护做法**

护指令》的适用范围取决于属地因素，要么机构的成立地

在欧盟，要么利用欧盟境内的设备进行了个人数据的处理

活动(仅传输通道除外),才会落入规制范围。《条例》

不仅考虑了“属地”因素，还增加了“属人”因素，具体

如下。

1. 对于成立地在欧盟的机构来说，《条例》的适用范

围并未发生大的变化，但强调了无论数据处理的活动是否

发生在欧盟境内，都统一遵循《条例》(第3.1条)。例如，

一家在德国成立的公司，若通过位于中国境内的云来处理

数据，则同样适用《条例》。

2. 对于成立地在欧盟以外的机构，适用属人因素。

只要其在提供产品或者服务的过程中(不论是否收费)处

理了欧盟境内个体的个人数据，将同样适用于《条例》。

此类情形还包括对欧盟境内个人活动的监控行为(第3.2

条)。根据《条例》说明部分的解释，监控行为包括利用

Cookie 等互联网工具对个人网络活动的跟踪分析活动。

也就是说，任何网站甚至APP 只要能够被欧盟境内的

个人所访问和使用，产品或服务使用的语言是英语或者特

定的欧盟成员国语言、产品标识的价格为欧元，都可以被

理解为该产品、服务的目标用户包括欧盟境内用户，从而

需要适用《条例》。这也是缘何《条例》在全球引起极大

震动的核心原因之一。不论是银行、保险、航空等传统行业，

还是电子商务、社交网络等新兴领域，只要涉及向欧盟境

内个人提供服务并处理个人数据，都将落入《条例》适用

范围，除非放弃欧盟5亿人口的发达市场!

**066**

**数据要素**

**数据治理：数据政策发展与趋势**

**二** **、统一的《条例》规则之下仍有一些例外**

此次立法的主旨之一是，结束1995年《数据保护指令》以来欧盟成员国 之间的数据保护法律制度差异问题，《条例》的统一规定将直接适用于欧盟 成员国。但值得注意的是，《条例》仍然各成员国预留了一定自主空间，举

例如下。

1. 《条例》对于儿童个人数据做出了特殊保护规定，但允许成员国对于

儿童的年龄标准在13～16岁之间做出调整(第8.1条)。

2. 在处罚方面，《条例》规定了实施行政罚款的一般性条件，但同时也 授权成员国可以规定其他处罚类型，这些处罚可以适用于违反了《条例》但

并不符合行政罚款条件的违法行为(第84条)。

3. 数据保护官( Data Protection Officer,DPO) 的设立。除了条 例规定必须设立 DPO 的情形， 《条例》还授权成员国可以扩展必须设立 DPO

的其他情形(第37.4条)。

4. 成员国可以在未来针对基因、生物识别及健康数据的保护做进一步规

定(第9 .4条)。

5. 成员国可以依据《条例》的基本原则，针对雇佣领域的数据保护，做

出进一步的规定(第88条)。

除以上列举之外，此类授权成员国可做出进一步具体规定的条款在《条 例》中还有很多。因此，尽管统一的《条例》为企业大大降低了合规的复杂性，

但仍需注意到统一之外的差异性3]。

[3]GT alert,EU General Data Protection Regulation:What Impact for Businesses Established Outside the EU,April 2016。

**067**

**第二篇** **世界各国数据保护做法**

**三、** **一** **站式监管**

对于向欧盟不同国家提供业务的企业或者在不同国家

都有设立地的企业来说，《条例》会极大减轻合规成本。

企业不再需要与多个不同成员国的数据监管机构打交道。

根据新的一站式监管机制( One Stop Shop), 企业主

成立地所在国家的监管机构将作为主导监管机构 (Lead

Supervisory Authority), 对企业的所有数据活动

负有监管权力，监管效力辐射至全欧境内。

当然，为保证监管的协调统一性，《条例》为此精

心设计了一套复杂的咨询机制。主导监管机构的监管决定

要最大程度上反映其他成员国监管机构的意见。若不能

达成一致意见，则交由欧盟数据保护委员会 (European

Data Protection Board,EDPB) 处理(第56、60、

61条等)。

**四** **、处理数据须有合法理由**

处理个人数据必须要有合法理由，包括：数据主体的

同意，为了履行合同需要，履行法定义务的需要，以及数

据控制者的合法利益等。以下对“同意”及数据控制者的

合法利益及敏感数据的处理等重点条款做进一步的解释。

1. 关于同意。《条例》对于同意的有效标准严格很多。

同意必须是具体的、清晰的，是用户在充分知情的前提下

自由做出的。若数据控制者希望获得的同意的事项区别于

**068**数据治理：数据政

此前已取得同意的事项范围，则需要向用户做出单独明确的说明；如果将同 意数据处理作为签订合同的前提条件，而这种数据处理事实上超出了提供服

务所必需，则将违反有关“同意应当是自由做出”的规定(第7条)。

在这种高标准下，虽然《条例》并没有明确禁止“推定同意”模式(敏 感数据处理、数据画像活动例外),但在实践中通过推定方式获得用户同意 将很难被认为是有效合法的。也就是说，当前实践中普遍存在的通过冗长晦 涩的隐私政策来获取用户同意，或者让用户在签订业务协议时通过“打钩” 方式做出一揽子授权的方式将失去合法性。业界普遍认为，《条例》关于有

效合法同意的严格规定，使得用户的同意不会像现在这样被轻易获得[4]。

更重要的是，《条例》赋予了数据主体可以随时撤回同意的权利。数据 控制者应当明确告知用户现有该权利，并为用户方便地行使该权利提供便利

(第7 . 3条)。

在处理儿童个人数据时，必须获得其父母或者其他监护人的同意，并且 该举证责任在于数据控制者，数据控制者必须能够证明其从监护人那里获得

了同意(第8条)。

2. 关于数据控制者的合法利益。1995年《数据保持指令》和《条例》都 规定了除获得同意以外的其他数据处理的合法理由，其中包括符合数据控制 者的合法利益。 一般认为，数据控制者出于营销目的使用个人数据符合其合 法利益，但与此同时，《条例》赋予了数据主体对于营销活动的绝对反对权。 换言之，数据控制者可以以营销为目使用用户个人数据，但用户随时可以提

出反对，数据控制者必须立即停止使用。除此之外，将数据控制者的合法利

[4]Hogan Lovells.Future-proofing privacy,A guide to preparing for the EU Data Protection Regulation,[2015-06-15]

<http://www.hoganlovells.com/en/publications/futureproofing-privacy-a>- guide-to-preparing-for-the-eu-data-protection-regulation。

**069**

**第二篇** **世界各国数据保护做法**

益作为数据处理的合法理由的情形在实践中非常有限。数

据控制者必须能够证明，其合法的利益显著高于数据主体

的个人权利和自由(第6条)。

3.关于敏感数据的处理。敏感的个人数据包括：能够

揭示个人的种族、政治倾向、宗教和哲学信仰、商业团体

资格及关于个人健康或者性生活的数据，在敏感数据类型

中， 《条例》还明确加入了基因数据和生物数据，这类数

据的处理能够唯一地识别出特定个人(第9条)。

敏感个人数据的特殊性在于，作为一般法则，禁止处

理敏感数据，除非特定的例外条件能够满足。这些例外条

件包括：数据主体的同意，或者数据主体已经将上述信息

公开；为了建立、履行或者保护合法的诉求必须处理上述

敏感信息；为了公共利益的需要，或者与公共利益相关的

归档、科学、历史或者统计目的之用。但总体的原则是，

这些对于敏感数据处理的例外情况的解释将会非常狭窄。

**五、坚实强大的数据主体权利**

相比于1995年《数据保护指令》,《条例》对数据主

体的权利规定得细致入微，为个人有效行使权利提供了坚

实的法律保障。

1.知情权。 《条例》规定，数据控制者必须以清楚、

简单、明了的方式向个人说明其个人数据是如何被收集处

理的。可以想见的是，当前企业普遍应用的隐私政策必须

**070**

**数据要素**

**数据治理：数据政策发展与趋势**

进行大幅改革，才能满足合规要求。条例规定了应当告知

用户的信息内容包括(第12条、条13条):

·数据控制者的身份和联系方式，数据控制者指定的 代表信息；数据保护官 (DPO) 的相关信息；数据

的接收者或者数据接收者的类型。

·数据处理的目的和合法基础。如果合法基础是基于 用户的同意，那么应当告知用户享有撤回同意的权 利，并且该撤回不得影响先前的数据处理中用户的

合法利益。该信息应当以单独、显著的方式显示。

·若涉及自动化的数据处理，包括数据画像活动，则

需要提供基本的算法逻辑，以及针对个人的运算结果。

·个人数据的保留周期，以及采取该周期的理由。

·依据法律，数据主体享有的权利，投诉权以及相关

的监管机构。

·若数据传输到第三国，则需要告知用户该第三国是 否通过欧盟的充分性决定，若没有通过，则需要告

知数据控制者采取了何种保障措施。

·若数据不是径直从数据主体处直接收集而来的，则

需要告知其数据的来源和类型。

2.访问权。数据控制者应当为用户实现该权利提供相 应的流程，若该请求是以电子形式提出的，则也应当以电

子形式将数据提供给个人。控制者不能基于提供该服务而

**071**

**第二篇** **世界各国数据保护做法**

收费，除非数据主体的请求明显过量，超过负担(第15条)。

3.反对权。对于两种情形，数据主体享有绝对的拒绝

权：始终有权随时拒绝数据控制者基于其合法利益处理个

人数据；始终有权拒绝基于个人数据的市场营销行为。条

例还引入了限制处理的权利。例如，当数据主体提出投诉

时(如针对数据的准确性),数据主体并不要求删除该数据，

但可以限制数据控制者不再对该数据继续处理(第21条)。

除以上权利之外， 《条例》还全面引入了新型的权利

类型，其中最引人注目的是数据可携权(第20条)、被遗

忘权(第17条)。

总体来看，《条例》对于数据主体权利的补充完善， 不仅极大地增强了数据主体对于个人数据的控制能力，而 且对企业如何保障实现数据主体的权利提出了具体的要 求，对企业的制度建设、措施配置、业务流程乃至 IT 系

统设计产生直接影响。

**六** **、严格问责：数据控制者**

《条例》大大简化了企业日常的合规负担，特别是废 除了目前各成员国关于数据处理及境外转移的许可或者备 案程序。但是取而代之的是，要求企业在内部建立全面的 问责机制，以实现《条例》的真正落地15]。特别是，《条例》 旨在对个人数据处理中的个人权利和自由提供充分的尊重

和保障，因此，对于数据控制者和处理者的约束规范十分

[5]需要说明的是，

尽管1995年《数据保

护指令》中提出了数

据控制者、数据处理

者两个主体概念，但

绝大部分法律要求只

是面向数据控制者提

出的。 《条例》继承

了这两个主体概念，

但是将数据处理者也

直接纳入了规范的范

畴。另外，按照《条例》,

数据控制者是指单独

或联合其他方决定了

数据处理目的和方法

的主体，包括自然人、

法人、公共机构等。

数据处理者是指代表

数据控制者进行数据

处理的主体，包括自

然人、法人、公共机

构或其他实体(第4.7

条、第4.8条)。

**072**

**数据要素**

数据治理：数据政策发展与趋势

严格。欧盟数据保护机构“第29条工作组”已经将制定相关细则列为工作优

先项[6]。

**七、数据保护官**

对于设立地在欧盟的机构来说，以下是必须设立 (Data

Prote-

ction Officer,DPO)的法定情形：

·政府部门及公共机构作为数据控制者的。

·机构核心业务涉及以下大规模活动的：日常的以及系统性的监控数据

主体；处理特殊类型的个人数据，或者数据处理活动与刑事定罪相关。

DPO必须具备数据保护的专业知识和技能，有能力且能独立地履行职责。

DPO 的联系方式必须予以公布，且向监管机构报备。集团公司可以指定一位

DPO, 但前提是 DPO 能够方便地接入公司其他运营地处理相关事务(第37条)。

对适用于《条例》但设立地在国外的机构而言，其必须在欧盟境内指定 一个代表(机构)17),以作为该机构与数据保护监管机构之间的联系点(第 27条)。

文档化管理(Documentation) 。 做到一举一动都有据可查。数据控 制者必须全面记载其数据处理活动，包括数据处理的目的、数据的类型、数

据接收者的类别，以及转移至第三国的数据接收者的名称或类型，数据保存

[6]EU,ARTICLE 29 DATA PROTECTION WORKING PARTY,Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR),Adopted on 2 February 2016。

http://ec.europa.eu/justice/data-protection/article-29/documentation/

opinion-recommendation/files/2016/wp236\_en,pdf。

[7]代表可以是机构，也可以是个人，但应当具有处理个人数据保护事宜的专业能力。

**073**

**第二篇** **世界各国数据保护做法**

的时间，采取的安全保障措施等，保留有与数据处理者的

合同附件。250名雇员以下的中小企业可以豁免该要求，

但是如果核心业务涉及大规模的处理个人数据或者处理敏

感数据以及涉及违法定罪数据处理的则不能例外。文档化

管理不仅是企业内部的管理措施，而且是数据保护监管机

构履行职责的重要抓手(第30条)。

数据保护影响评估(Da ta Protection Impact

Assessments,DPIA) 。 对于高风险的数据处理活动，

要事先进行数据保护影响评估。《条例》并没有对高风险

进行界定，但以下情形应当事前评估：对个人特征的系统

性评价，该评价会对数据主体产生法律上的影响；对大量

敏感数据的处理；以及对公共领域大规模的系统性监控(第

35条)。

事先协商 (Prior Consultation)。如果数据保

护影响评估的结果显示是高风险，且数据控制者没有有效

的降低风险的措施，那么数据控制者应当就数据处理活动

向相关的数据保护监管机构进行事先协商。监管机构应当

在收到协商申请的特定期限内提出处理意见，并可以采取

纠正措施。除此之外，成员国在制定涉及数据保护的立法

时，也应当事前征求数据保护监管机构的意见(第36条)。

数据泄露报告 (Data Breach Notification,

DBN) 。《 条例》将数据泄露定义为导致偶然的或者非法

的数据破坏、损失、改变、非授权的披露等(第4条)。

一旦发生数据泄露事故，数据控制者就需要及时通知监管

机构，如果可行，应不超过72小时，除非该泄露不可能会

**074**

**数据要素**

**数据治理：数据政策发展与趋势**

造成对个人权利和自由的破坏风险，若未在72小时内报告 监管机构，则后续报告应当说明迟延报告的理由。对于数 据处理者而言，其应当在意识到泄露事故及风险后及时报

告数据控制者(第33条)。

数据泄露报告中至少应当包含以下内容：关于数据泄 露事故的描述、涉及的数据主体总量、类型以及数据记录 的总量；企业 DPO的姓名和联系方式，泄露可能造成的结 果，企业已经采取的止损措施。数据控制者应当将所有的 数据泄露事故予以文档化，以便监管机构能够检查其合规

工作(第33条)。

如果数据控制者采取了适当的保护措施，特别是采 取的措施能够使得数据难以被一般人所理解(例如加密措 施),或者并不会对数据主体产生实际的威胁或损失，那 么数据控制者可以不必履行数据泄露报告义务，但这些证 明责任都在数据控制者。当然，数据监管机构可以否决数 据控制者做出的风险判断，强制要求其履行泄露通知义务

(第34条)。

依照《条例》规定，强制性的数据泄露报告是没有门 槛的，因此企业应当为此建立周密的制度安排，包括数据 安全管理流程、泄露事故发现、上报预案等，以符合《条例》

的严格要求。

**八、安全保障措施**

《条例》对于安全保障措施 (Security of Pro-

**075**

**第二篇** **世界各国数据保护做法**

cessing) 给予了更具体的规定，特别强调了以下措施：

·对个人数据的匿名化和假名化。

·确保提供持久的机密性、完整性、可用性和系统可

恢复性的能力。

·在物理或者技术事故下及时恢复数据可用性、可访

问性的能力。

·建立定期测试、评估、评价技术和管理措施是否有

效的体系(第32条)。

其中对于个人数据匿名和假名，《条例》明显做了区

分：假名数据是指在缺乏其他信息的前提下(且该信息被

独立存储),不能够被识别指向特定个人的数据。假名数

据仍然属于个人数据，因此适用对于个人数据的安全保障

要求，特别是对于能够将假名数据恢复身份识别属性的额

外信息必须单独安全存储。但相比于普通个人数据，假名

数据在遵循的规范方面要相对宽松。例如，假名化以后，

数据控制者可以将数据用于收集该数据时所确定目的之外

的其他目的：

匿名数据是指已经完全移除了个人可识别信息之后的

数据，该数据不能够再识别出特定个人。匿名数据不再属

于个人数据，不受《条例》规范。

严格问责：数据处理者。对于数据处理者而言，《条例》

带来了重大变化。1995年《数据保护指令》主要适用于数

据控制者。数据处理者主要通过合同的方式承担数据保护

**076**

**数据要素**

数据治理：数据政策发展与趋势

责任。然而新《条例》对于二者在大多数情形下几乎提出

了相同要求。

此外，《条例》还细致规定了数据控制者和数据处理 者之间的合同应当至少包含哪些内容，例如数据处理的目 的、期限、个人数据的类型、数据主体的类别以及双方的

权利和义务。

数据处理者仅能按照数据控制者书面的要求处理数 据，必须确保其员工能够遵守有关保密的要求，并在以下 方面向数控制者提出必要的协助：数据安全、数据泄露、 数据保护影响评估等。如果没有数据控制者的同意，数据 处理者不得二次分包业务；数据控制者可以对分包采取概 括性授权，但如果具体的分包商发生了变化，数据处理者 有义务及时告知数据控制者，后者有权提出反对。数据处 理者对其分包商的数据处理活动负完全责任。在数据处理 服务终止时，数据处理者应当删除或者将数据全部返还给

数据控制者，除非根据法律的要求必须保留这些数据。

数据处理者的违规行为同样适用《条例》规定的严格 处罚，数据监管机构的监管权力也同时及于数据处理者， 包括进入数据控制者的工作场所、发布警告、发布数据处 理禁令等。用户个人也有权直接从数据处理者处主张赔偿。 当然，若是因为数据控制者的错误指令，则数据处理者可

以再行向数据控制者索赔(第28条)。

新规中对数据处理者构建的一系列规范要求，将对云

计算生态体系带来重大影响。按照新规，数据控制者和数

**077**

**第二篇** **世界各国数据保护做法**

据处理者之间的合同在很多情形下需要重新谈判达成。特别是由于《条例》 对于数据处理者大大增加了合规风险，合同中关于安全保障措施、风险管理

以及服务的价格都会受到影响。

完善跨境数据转移机制。关于跨境数据流动的限制是在1995年《数据保 护指令》中提出的，欧盟公民的个人数据仅能转移到与欧盟同等保护水平的 国家。在实践中，部分成员国针对跨境数据流动增加了事前的备案或者许可 要求。《条例》明确禁止了这种“增设许可”的做法，只要符合了《条例》 中跨境数据流动的条件，成员国就不得再予以限制。在此基础上， 《条例》

还进一步完善了数据转移合法机制：

1. 充分性决定 (Ad equate Decision)。相比于1995年《数据保护 指令》,欧盟委员会除对国家可以做出评估外，还可以对其他国家的特定地区、 行业领域以及国际组织的保护水平做出评估判断。这大大增加了“充分性” 这一机制的适用范围。毕竟自1995年《数据保护指令》实施以来，通过充分 性决定的国家还不超过10个18]。《条例》对欧盟委员会做出充分性决定的 程序和标准也进行了进一步详细规范，包括要求至少每隔4年对充分性决定 进行重新审查(第45条)。

2. 有约束力公司规则 (Binding Corporate Rules,BCR)。有约 束公司规则最早由欧盟“第29条工作组”发展而来，初衷是让跨国公司或者 公司集团能够在公司内部进行跨境的数据转移，是欧盟委员会提出的标准化 格式合同的一个替代选择。在1995年《数据保护指令》框架下，大约有2/3 的欧盟成员国认可 BCR。但是取得成员国监管机构对于BCR的认可需要经历 冗长的批准程序(18～24个月不等)。此次《条例》对BCR给予了正式的

法律地位，并详细规定了BCR 获得认可的程序和内容标准(第47条)。

[8]Andorra,2010,Argentina,2003,Canada,2002,Switzerland,2004,Faeroe Islands, 2010,Israel,2011 Isle of Man,2004,Jersey,2008,New Zealand,2013。

**078**

**数据要素**

**数据治理：数据政策发展与趋势**

3. 标准合同条款(Standard Contractual Cla- uses) 。 目前欧委会通过的三个格式合同条款仍然有效。 《条例》增加了成员国数据监管机构可以指定标准合同条

款的渠道，但必须要经过欧委会的认可(第63条)。

4. 经批准的行为准则(Codes of Conduct)。数 据控制者可以组织成立协会并提出遵守《条例》的详细行 为准则。该行为准则可以由成员国监管机构或者欧盟数据 保护委员会批准，并通过有约束力的承诺方式生效。这种 情形主要针对不适用于《条例》但从欧盟接收数据的主体(第

46条)。

5. 经批准的认证机制、印章或者标识(Approved

Certification Mechanism,Seal or Mark)。此类 情形主要适用于公共机构之间的数据转移活动。行为准则 与认证机制是《条例》中引入的新型合规机制，以最大化

发挥第三方监督与市场自律作用。

**九** **、对数据画像活动的特别规制**

根据《条例》界定， “数据画像”(Profilin g) 概 念外延广泛，它指的是： “任何通过自动化方式处理个人 数据的活动，该活动服务于评估个人的特定方面，或者专 门分析及预测个人的特定方面，包括工作表现、经济状况、 位置、健康状况、个人偏好、可信赖度或者行为表现等” (第4.4条)。这一概念被普遍认为能够覆盖目前大多数

利用个人数据的大数据分析活动。例如对个人偏好的分析，



**第二篇** **世界各国数据保护做法**

可涵盖市场中最普遍的大数据分析市场营销活动。

画像活动如果对用户个人产生法律上的影响或者其他重大影响，那么仅 在符合以下条件之一时才是合法的：(1)数据主体明确的同意； ( 2 ) 欧 盟 或者成员国的明确授权；(3)是数据主体和数据控制者之间签订、执行合同 所必需(第22条)。考虑到(2)、(3)仅仅是个别特殊情形，因此，实践 中绝大部分的数据画像的合法基础将建立在用户明确同意的基础之上。而根 据《条例》对于“同意”的高标准要求，业内专家认为，获得用户在数据画 像方面的同意将是难以操作的，这将对大数据背景下的分析营销活动带来极

大的负面影响[9]

**079**

在数据画像活动中，要获得用户合法有效的同意，首先应当向数据主体 全面介绍数据画像处理活动是怎么进行的，收集了用户的哪些数据，算法的 基本原理是什么,评估结果是否会对用户产生法律上的影响。其次，应当明 确告知用户其享有对画像的反对权。此类信息应当明确无误地表达，并足够

引起用户注意的范式，独立于其他信息(第13.2条，第21条)。

此外，基于个人敏感数据的数据画像活动是被禁止的，除非：(1)数据 主体出于一个或者多个特定的目的给予了明确的同意，但是成员国可以通过 立法明确规定即使是在用户同意的情况下，也禁止基于敏感数据的画像活动；

(2)该数据画像活动对于重大的公共利益是必需的(第22条)。

因此，对于依赖于数据画像(包括利用Cookie 等跟踪工具开展行为精

准营销)的企业来说，如何设计一套有效的机制，既能够符合条例有关透明

[9]HUNTONSWILLIANMS.The EU General Data Protection Regulation,a guide for

in-house lawyers,APRIL 2016。

<https://www.huntonprivacyblog.com/2016/04/12/hunton-releases-2016-eu>-

general-data-protection-regulation-guide-for-in-house-lawyers/。

**080**

数据治理：数据政

性和用户同意的要求，又能使得数据分析活动得以继续，

是摆在面前的一道难题。

**十、监管权力、处罚与司法救济**

1.《条例》增强了监管机构的执法权，包括：通知数 据控制者、数据处理者相关违反行为；要求违法者提供相 关信息，或者向监管机构提供访问此类信息的接口；现场 调查、审计；命令修改、删除或销毁个人数据；可以采取

临时性的或限定性的数据处理禁令；科以罚金(第58条)。

2. 《条例》规定了严苛的罚金，分为两档： ( 1 ) 处 以1000万欧元或者上一年度全球营收的28,两者取其高。 针对的违法行为包括：没有实施充分的IT 安全保障措施， 或者没有提供全面的、透明的隐私政策，没有签订书面的 数据处理协议等；(2)处以2000万欧元或者企业上一年 度全球营收的48,两者取其高。此类处罚针对的违法行为 包括：无法说明如何获得了用户的同意，违反数据处理的 一般性原则，侵害数据主体的合法权利，以及拒绝服从监

管机构的执法命令等(第83条)。

3. 司法救济。对于不服监管机构做出的决定或者针对 监管机构的不作为，当事主体可寻求司法救济。其中，数 据主体可以通过司法途径向数据控制者、数据处理者主张 因其违反《条例》而致使数据主体遭受物质上或者非物质 上的损害。若一个以上的数据控制者、处理者涉及侵权，

则共同承担连带责任，除非其能证明其对损害的产生没有

**081**

**第二篇** **世界各国数据保护做法**

责任。 上述司法救济的权利可以由消费者机构代表数据主

体行使(第26条、第80条、第82条)。

**结语**

从1995年《数据保护指令》的34个简单条文扩展到

99条(263页)的详细规范，欧盟数据保护通用《条例》

带来了全面的制度改革，其核心目标是将个人数据保护深

度嵌入组织运营，真正将抽象的保护理论转化为实实在在

的行为实践。对于企业而言，小至隐私政策、业务流程，

大到 IT 系统、战略布局，无一不需要重新审视规划。从

当下着手的准备工作，决定了企业能否有底气在2年之后

站立在数字时代新的起跑线上。

 **082** **数据治理：数据政**



**第7章**

**欧盟《通用数据保护条例》:**

**十个误解与争议**

**摘要：**欧盟《通用数据保护条例》在个人数据保护历 史上具有重要的影响、作用和价值。自然也会产生各种评 论和争议，本章对相关问题的做法、理解或争议进行了详

细说明。

[10]文章对理解

GDPR 提供了一些参 考，但随着大量指南 的发布，其中部分观 点也需要补充及修正。 [11]根据 GDPR 的规 定，第29条工作组也 将由新组建的欧盟数 据保护委员会替代。

[12]部分指南已正式 发布，部分指南仍处 于公众征询意见期。

**一、引言**

欧盟《通用数据保护条例》(General Data Protection Regulation,GDPR) 的重要性毋庸置疑。 作为隐私与数据保护领域20年来最引人瞩目的立法变革，

GDPR 提出了大数据时代个人数据保护的新秩序愿景。

2016年10月，作者曾就 GDPR的主要制度、重要变 化进行了梳理，见旧文《欧盟通用数据保护条例GDPR详 解》10]。GDPR创建了大量的新概念、新原则、新权利 ，

导致产生许多争议和尚待细化的领域。

为澄清相关问题，欧盟数据保护权威机构——第29条 工作组[]发布了一系列的指南|121 以回应各方关切，包

括数据可携权、数据保护官、数据保护影响评估、识别主

**083**

**第二篇** **世界各国数据保护做法**

导监管机构、行政处罚、充分保护认定、BCR基本原则、

数据泄露通知、自动决策和画像、同意、隐私实践透明度等。

这些指南对厘清争议性问题提供了重要参考，但也正说明

GDPR 就像一个新生儿，正处于探索塑造期。

本文聚焦10个最易被误解和最具有争议性的问题，展

现更为全面、客观的视角，以期消除刻板印象和固有偏见，

尽力还原 GDPR的真实面貌。

1.GDPR: 史上最严格的数据保护立法?

2. 用户同意：数据处理的唯一合法基础?

3. 数据控制者的正当利益：还有适用情形吗?

4. 被遗忘权：我随时可以主张删除数据并被世界所

遗忘?

5. 数据可携权：不同的信息服务之间可以无缝迁移?

6. 数据跨境转移：变得更加严格?

7. 云计算：将重建生态体系?

8.人工智能：深度学习即将违法?

9. 区块链：与GDPR 不相兼容?

10. 高昂的处罚不可避免?

**二、相关问题的讨论与分析**

**(** **一** **)GDPR:** **史上最严格的数据保护立法?**

GDPR的严格主要体现在对个人权利的细致保护及对

违法行为的严苛罚金处罚上。但易被忽视的另一面是，

 **084** 数据治理：数据政

GDPR依然完全秉承了1995年《数据保护指令》的二元立 法目标：保护个人权利并促进个人数据的流动。立法的第 一条开宗明义：不能以保护个人数据中的相关自然人为由，

对欧盟内部个人数据的自由流动进行限制或禁止。

尤为值得注意的是，在历时4年的立法商议中， GDPR 的立法者们充分关注到了数据主体享有的并不是绝对权 利，有关数据的权利应当与其他权利及正当利益之间形成 恰当的平衡关系。为此，GDPR 精心设计了大量的但书、 克减条款，对例外情形作出补充，对权利作出适当限制，

对义务、责任予以适当豁免。

需要平衡的其他正当利益及权利包括：(1)公共利益， 例如在医疗健康领域，为实现传染疾病分析与预警目的； (2)科学、历史研究、统计目的；(3)表达自由权与信 息权，为了新闻目的、学术、艺术或文学表达；(4)个人

的其他核心重大利益与权利，例如生命权，健康权； (5)

数据控制者的合法利益等。

围绕上述正当利益与权利， GDPR进行了许多平衡折

中，体现如下。

(1)对每一项数据主体权利，包括数据访问权、被 遗忘权、数据可携权等条款均有限定条件(下文会重点介

绍 ) 。

[13]当然为了避免

豁免的滥用，对豁免 本身也有一些合理的 限制。

(2)对企业义务也考虑了多种情形下的豁免，比如 规模在250人以下的中小企业可以豁免数据活动文档化

记录义务[13]等。

085

**第二篇** **世界各国数据保护做法**

(3)引入了多种变通机制，来调和不同的权利，最 为典型的是在数据跨境转移中构建了多种合规数据转移路

径(14)。

(4)在原则性禁止条款中，均设置了用户同意的例外，

例如对敏感信息的处理。

(5)专设“限制”情形一节，明确权利受到限制的 各种情形，并授权成员国可以继续围绕上述利益通过制定 本国法规的方式，进一步做出例外和克减规定，这实际上

为GDPR未来的落地执行留下了更大的空间15]。

所以总体来看，除严格性外，GDPR 整体体现出的是“平 衡兼顾”。通过制度改革，在用户个人权利和其他正当权 益之间形成更为科学、合理的配置。与此同时，引入诸多 平衡机制的结果是GDPR要远比想象中复杂。正如本文中 所探讨的许多问题一样，实际上就连 GDPR自身也没有给

出明确的答案。

**(二)用户同意：数据处理的唯一合法基础?**

从企业视角出发，往往会得出这样的结论。特别是国 内相关个人信息保护法律文件，也更多地将用户同意作为 数据收集、使用的唯一合法理由。例如，我国的《网络安 全法》第四十一条116)的表述也易被如此理解。然而，这

一情形实际上存在许多误解。

GDPR适用的主体不仅包括企业，而且包括决定和参

与个人数据处理的任何个人、机构，涵盖了政府部门、公

[14]关于数据跨境的

机制，可参见旧文《数

据跨境流动政策认知

与建议》。

[15]见 GDPR 的第三

章“数据主体的权利”

第5节“限制”。

[16]《网络安全法》

第四十一条网络运

营者收集、使用个人

信息，应当遵循合法、

正当、必要的原则，

公开收集、使用规则，

明示收集、使用信息

的目的、方式和范围，

并经被收集者同意。

**086**

**数据治理：数据政**

共机构、司法机构以及其他实体7)。上述个人和实体作 为数据控制者或数据处理者，均需要适用GDPR。因此， 考虑到数据处理的多种可能场景以及与其他正当利益的平 衡，除数据主体的同意之外， GDPR还规定了5类处理个

[17]结合我国网安法 对网络运营者的广泛 界定，第七十六条(三) 网络运营者，是指网 络的所有者、管理者 和网络服务提供者，

实际上同样包含了政 府机构、公共机构和 企业。

人数据的合法基础，具体如下：

(1)为了履行数据主体所参与的合同，或者是在合

同确立前依数据主体的请求而进行的处理。

(2 )数据控制者为了履行法律职责的需要。

(3)为了保护数据主体或另一个自然人的核心利益。

(4)数据控制者为了公共利益或因官方权威要求而

履行某项任务。

(5)对于数据控制者或第三方所追求的正当利益是 必要的，但这种正当利益不得凌驾于需要通过个人数据保 护以实现数据主体的基本权利与自由之上，特别是儿童的

基本权利与自由。

以上5种情形，都可以作为“同意”的其他替代机制， 成为数据处理的合法基础。而从国内来看，对于这一问题， 我国行业标准《个人信息安全规范》也在尝试进行修正，

[18]《信息安全技术 个人信息安全规范》, 2017年12月29日发 布，2018年05月01 日实施。

在同意的例外中，详细罗列了11项情形[。

**(三)数据控制者的正当利益：有适用情形吗?**

作为用户同意的替代机制——“数据控制者的正当利

益”可能是GDPR 中最易被误解的概念。实际上正如本条

**087**

**第二篇** **世界各国数据保护做法**

的限制条件，在很多商业场景中，企业不能够依据自己的 正当利益理由去规避用户同意的需求。但GDPR 将其与用 户同意并列作为数据处理的合法理由，即表明了个人的权 利并不总是优先，而是需要在用户个人权利与数据控制者

的合法利益之间做出平衡。

至少在目前的 GDPR 中，可以适用“数据控制者的正

当利益”的情形包括：

(1)直销场景 (Direct Marketing), 如果企业 已经与用户有实际的交易关系，或者与用户在达成交易的 过程中，那么企业可以适用本条所赋予的正当利益理由， 通过软选择参与(Soft opt-in)方式，即用户默认同

意的方式，向用户发送与其此前交易商品或服务相关的营

销信息，直到用户行使拒绝权为止[19]。

(2)以预防欺诈为目的的数据处理活动(20)

(3)出于保障网络信息安全目的处理个人信息|211。

(4)在集团或者系统内部，出于行政管理需要的数

据披露(22)(排除跨境转移情形)。

(5)向主管部门报告犯罪或者公共安全重大威胁|23]。

[19]详细的适用条

件参见GDPR的姊

妹法规ePrivacy

Regulation, 该法规对

电子营销做出了更为具体

的规定，包括opt-in 的

例外情形。

[20]GDPR RECITAL 47。

[21]GDPR RECITAL 47。

[22]GDPR RECITAL 48。

[23]GDPR RECITAL 50。

考虑到GDPR对于控制者正当利益的界定是开放式的，

因此不排除在实践中还会出现其他正当利益类型也会为执

法机构所认可。

**088****数据治理：数据政**

**(四)被遗忘权：我随时可以主张删除数据并被世界所遗忘?**

“被遗忘权” “数据可携权”是GDPR中最引人注目的两项新型权利， 但同时也引发了巨大的争议。单从名称看，这两项权利给人们带来了多少遐想，

就带来了多少歧义。

GDPR 中的被遗忘权实质上是传统个人数据保护法中“删除权”的升级。 此外，2014年欧洲法院在谷歌西班牙一案中所确立的“被遗忘权”判例(24)

深深影响了正在立法进程中的 GDPR, 并在最终的版本中正式写入129)

GDPR第17条擦除权(“被遗忘权”)共计三款。其中第1款的核心仍 然是传统个人信息保护法中已经确立的删除权：当用户依法撤回同意或者控

制者不再有合法理由继续处理数据等情形时，用户有权要求删除数据。

关于“被遗忘”的精神更多体现在第17条第2款：如果控制者将符合第 1款条件的个人数据进行了公开传播，他应该采取所有合理的方式予以删除(包 括采取可用的技术手段和投入合理的成本),控制者有责任通知处理此数据

的其他数据控制者，删除关于数据主体所主张的个人数据链接、复制件。

也就是说，控制者不仅要删除自己所控制的数据，还要求控制者负责对 其公开传播的数据，要求通知其他第三方停止利用并删除。这是对传统“删 除权”的极大扩张。要知道，在开放的互联网空间，要控制者去确定并通知

所有的第三方几乎是不可能完成的任务。

也正是考虑到“被遗忘权”的强大威力，立法者对其适用做了许多限制，

第17条第3款规定了并不适用“被遗忘权”例外的4种情形。

[24]InfoCuria -Case-law of the Court of Justice,JUDGMENT OF THE COURT (Grand Chamber),13 May 2014(\*),Google Spain SL,Google Inc.VS Agencia Espanola de Proteccion de Datos(AEPD),Mario Costeja González。

[25]当然，GDPR 的被遗忘权(第17条)与欧洲法院判决中提出的“被遗忘权”相比，在权利的内

涵方面仍然有较大区别，可以参考旧文《被遗忘权很美?》,其中对两方面的权利内容做了对比。

**089**

**第二篇** **世界各国数据保护做法**

(1)基于表达自由和信息自由。

(2)基于公共利益和履行法律职责需要。

(3)基于历史、统计和科学研究的目的。

(4)出于提出、实施和保护合法权利的需要等。

简言之，“被遗忘权”虽然与个人权利直接挂钩，但

它与包括言论自由、信息自由流动、公众知情权在内的其

他公共价值追求有着尖锐冲突，即便是在将个人信息保护

作为基本人权的欧盟，也需对其加以限制。

例如，在一个典型的“被遗忘权”案例中， 一名律 师因为报纸网站上刊登了其曾经被指控有伪造罪的相关信 息，将该报纸告上法庭，认为其刊登的信息对其职业生涯 的声誉产生了负面影响，但该律师的主张在法院中并没有 得到支持。法院认为，公众关心的真实信息应当可以被合 法公开，包括在网络上公开。国内也有相关案例，法官同

样以公共利益为由驳回诉讼[26]。

即便做出了诸多限制，“被遗忘权”仍然面临很多质疑。 对于用户提出的“被遗忘权”请求，企业可能首先需要审 查其是否属于立法中规定的例外情形，而“表达自由”“公 共利益”这些抽象的判断标准，无疑会将企业拖入裁判的 泥潭，并由此可能成为一种新形式的“网络审查”。在

GDPR后续实施中，“被遗忘权”仍然有许多问题有待解决。

[26]任某诉百度名誉

权案，也被国内媒体

称为“国内被遗忘权

第一案”,见北京市

第一中级人民法院民

事判决书(2015)一中

民终字第09558号。

 **090** **数据要素**

**数据治理：数据政策发展与趋势**

(五)数据可携权：不同的信息服务之间可以

无缝迁移?

如果说“被遗忘权”容易被普通公众所误解，那么数

据可携权则是更令专业人士易误读的一项权利。

GDPR数据可携权体现在第20条，共有四款。正如“被 遗忘权”是传统删除权的升级，“可携权”可视为传统“访 问权”的增强版，即它首先保证的是用户获得自身数据的 权利。第20条第1款就是这一内容：个人有权获得其提供 给数据控制者的相关个人数据，且其获得的个人数据应当

是结构化的、普遍可使用的和机器可读的。

同时第1款也明确了“可携权”适用的两个限定条件： 一是适用于建立在“用户同意”基础上的数据处理活动； 二是处理是通过自动化方式完成的。结合数据处理活动的 合法基础来看，用户同意仅仅是合法基础之一，因此用户 同意之外的其他数据处理活动并不适用于数据可携权，例 如，为了公共利益，为了预防欺诈的数据处理并不适用可

携权。

“可携”的精神主要体现在第20条第2款：如果技术 可行，数据主体应当有权将个人数据直接从一个控制者传 输到另一个控制者。 “技术可行”的表述，表明 GDPR并 没有将可携权上升到推广强制性的互兼容、互操作技术标

准的程度，而是给市场留下了一定空间。

最后，同样在第3款、第4款对可携权的适用明确了

限制条件，要求不能对他人的权利或自由产生负面影响。

**09I**

**第二篇** **世界各国数据保护做法**

显然，仅第20条一个独立条款难以完全解释“数据可携权”所可能包含 的丰富含义，以及在具体实践如何执行。因此，欧盟“第29条工作组”专门 发布指南[27],以回应数据可携权最具有争议性的问题。因篇幅有限，择取其 中最关键的问题——个人可以通过行使“可携权”,实现在不同服务商之间

的自由切换吗?

如果现实中数据能够简单明了地切分为你的个人数据和我的个人数据， 那么这个问题也许还比较简单，然而在现实的万物互联时代，我们每个人的 个人信息，似乎都与物的信息、机构的信息以及与他人的个人信息黏连在一 起[28]。在转移过程中，如何不对他人权利的造成负面影响，是“可携权”面

临的最大考验。

典型的个人数据可能同时关涉其他第三方个人的数据，如通讯录信息、 电话记录信息、聊天信息、邮件往来信息、转账记录信息等。按照个人数据 的定义，此类数据当然属于个人数据，但数据主体针对此类数据行使“数据 可携权”时，往往可能对其他第三方个人的基本权利带来侵害。因为这些第 三方个人根本没有机会得知自己的数据被他人提交给了新的数据控制者，从 而也没有机会行使自己的权利。这不仅会在不同的服务商切换中带来潜在的

权利侵害风险，而且即使在同一家服务商也存在此类风险。

例如，2010年谷歌公司在启动其社交网络服务Google Buzz 时，不 恰当地利用了其Gmail 用户的关系链数据，在Gmail 用户A 接受Google Buzz 使用邀请时，用户并不清楚其Gmail 的通讯录上的用户都将被自动

拉入Google Buzz,而被拉入的用户也并不知情自己的联系信息已被收

[27]ARTICLE 29 DATA PROTECTION WORKING PARTY:Guidelines on the right to data portability,Adopted on 13 December 2016,As last Revised and

adopted on 5 April 2017,16/EN WP 242 rev.01。

[28]中国社会科学院民法典工作项目组；大数据时代下个人信息保护的立法模式变革，2018年 2018-03-07, 微信公众号“与民法典同行”。

**092**

数据治理：数据政

录并被 Buzz 社区公开，谷歌公司也因此受到 FTC 处罚291。近期爆发的 Facebook 事件中也再次证明，通过好友关系链的数据披露，的确更易对不

知情的第三人造成权利侵害。

在更加重视个人权利保护的欧盟，自然要对此类情况加以限制。GDPR第 20条明确对可携权的行使做出了特别限定，即不能对他人的权利或自由产生

负面影响。“第29条工作组”在指南中进一步做出了详细解释。

对于涉及第三方个人的数据转移，仅仅允许行使“数据可携权”的数据 主体本人对于转移后的数据进行唯一的控制 (Sole Control) , 只能将此 类数据用于个人和家庭事务目的，比如出于个人目的整理通讯录。这切断了

任何第三方利用这些数据的可能性。

接收数据的数据控制者不得基于自己的利益去处理转移后的数据，特别 是禁止对数据中涉及的第三方个人开展商品营销或服务活动，也不得将获得 的数据用于丰富第三方个人的数据画像，或重建其社交圈，即使在数据控制

者本身已经掌握第三方个人数据的情形下也要如此。

为避免对第三人的侵权风险，指南还鼓励数据控制者不论是导出数据的

一方 (Exporter ), 还是接收数据的一方(Importer), 都应当设置相应

的技术工具，帮助数据主体在转移数据时剔除涉及其他第三方个人的数据。

以上规定已清楚地指明，在类似于 Facebook 到 Snapchat 等社交网络 的切换中，并不可能通过用户行使“可携权”来实现一键转换。在很多情形下， 这反而是 GDPR 中所禁止的行为类型，因为它侵害到不知情第三方的基本权

利。例如，用户A将自己的好友信息，包括好友的姓名、手机号码转移到一

[29]US Federal Trade Commission:FTC Gives Final Approval to Settlement

with Google over Buzz Rollout,<https://www.ftc.gov/news-events/press>- releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-

rollout,last visited on Feb 24th,2018。

**093**

**第二篇** **世界各国数据保护做法**

个App 上，在这一场景下转移只能服务于A用户的个人存储、管理目的，接 收数据的App 不得基于自己的经营目的处理用户A的好友信息。直接面向用

户A的好友进行商品营销或服务，都属于明显违反 GDPR 条例的行为。

可携权要关注数据主体本人对数据的控制力(这里集中体现为转移诉求),

但更要保证所涉及的其他第三人的基本权利。

在这种需要兼顾不同方利益的复杂环境下，可携权自身设计是否科学? 是否符合市场实际?这面临许多质疑。其中质疑最大的是“可携权”与竞争 政策之间的关系。 “数据可携权”从表面上看可为用户提供便利，减少用户 转换成本，但是深入研究就会发现，有关锁定用户的成本以及用户转换服务

时所遇到的阻碍问题完全可以通过竞争法来解决。

竞争法历经百年发展历史，已经形成了较为严密和成熟的基础理论，它 不仅考虑到了用户的锁定成本，而且考虑到了锁定也会带来一定的消费者福 利。 一定的转换成本可以鼓励对新技术业务的投资，在长期来看是具有效率 的。竞争法的适用是以企业在市场上具有显著市场地位，并滥用该地位损害 正当的市场竞争为前提的。其规则适用具有复杂而严密的程序前提130]。而根 据GDPR 条例，数据可携权作为用户的基本权利，可以被要求适用于任何一 个机构，包括新兴企业在内。总之，正如“被遗忘权”一样， “数据可携权”

带来的新问题也许也远比想象中的更多。

**(六)数据跨境转移：变得更加严格?**

个人数据的跨境流动制度为欧盟所首创，因此很多人对欧盟这一制度留

下了严格的印象。然而在 GDPR 立法启动时，跨境流动制度中存在的突出问

[30]Peter Swire and Yianni Lagos,WHY THE RIGHT TO DATA PORTABILITY LIKELY

REDUCES CONSUMER WELFARE:ANTITRUST AND PRIVACY CRITIQUE,Maryland Law

Review 2013,72 Md.L.Rev.335。

**094**



数据治理：数据政

题就首先被识别出来。几乎所有的欧盟企业都涉及向欧盟境外传输数据，然 而1995年《数据保护指令》中关于跨境流动的严格规则早已难以适应数据国 际流动|31]。为此， GDPR对跨境数据流动政策进行了大幅优化改革，特别着

力于开辟更多的合法数据跨境方式，提升跨境流动的灵活度。

1. 明确欧盟各成员国不得以许可方式管理跨境数据流动。多年的实践表 明，各成员国对跨境流动采取的许可管理方式并没有实质性地提升个人信息 出境的保护水平，相反，只是徒增了官僚许可管理成本。因此， GDPR重点简 化了数据跨境传输机制，不再采用许可管理方式，只要符合 GDPR中跨境数

据流动的合法条件，成员国就不应当再以国内许可的方式予以限制和干预。

2. 增加了充分性认定的对象类型。除对国家可以做出评估外，还可以对

国内的特定地区、行业领域以及国际组织的保护水平做出评估判断，以增加

能够列入“充分性”决定(Ade quate Decision) 名单的潜在地区。

3. 扩展“标准合同条款” (Standard Clauses Contract, scc) 。 在现有已生效的3个标准合同范本的基础上，增加其他合同范本。 GDPR 增加了成员国数据监管机构可以指定其他标准合同条款的渠道，以便为

企业提供更多的、符合实际需求的跨境转移合同文本选择。

4.将“有约束力公司规则”(BCR) 正式确定为法定有效的数据跨境机制。 BCR 是集团型跨国企业可优先考虑的机制，若集团遵循一套完整的、经个人 数据监管机构认可的数据处理机制，则该集团内部整体成为一个“安全港”, 个人数据可以从集团内的一个成员合法传输给另一个成员。尽管已有部分欧

盟成员国监管机构接受 BCR规范，包括埃森哲、宝马汽车、惠普、摩托罗拉

[31]European Commission -Press release,Commission proposes a comprehen- sive reform of data protection rules to increase users'control of

their data and to cut costs for businesses,25 January 2012。

**095**

**第二篇** **世界各国数据保护做法**

等72家跨国公司获得了BCR认可[32]。但由于1995年的《数据保护指令》

中并未将BCR 纳入，BCR 的法律效力尚不明确，而此次GDPR 解决了这一问题。

5. 发挥行业协会等第三方监督与市场自律作用。GDPR规定数据控制者 可以成立协会并提出所遵守的详细行为准则 (Codes of Conduct)。该准 则经过欧盟数据保护委员会的认证后，可以作为有效的数据跨境管理手段。 此外，经认可的市场认证标志 (Seals and Marks) 也可以作为数据跨境

转移的合法机制，这实际反映了GDPR对美国市场自律治理方式的充分借鉴。

因此，在 GDPR 生效后，企业将会有更为丰富的机制选择，实现更为顺

畅的跨境数据流动。

**(七)云计算：将重建生态体系?**

对云计算而言， GDPR 的确带来了重大变化。在典型的云服务场景中，云 服务商作为数据处理者，而云客户是数据控制者。1995年的《数据保护指令》 主要适用于控制者，处理者通过合同承担数据保护责任。然而GDPR对于控 制者、处理者在大多数情况下提出了相同的要求。例如，承担对数据的安全 保障义务，在管理措施、技术上采取必要措施，包括指定 DPO、在发生数据

泄露事故时及时报告控制者等。

更进一步的是，GDPR对于处理者的专门规定，深入到了处理者(云服务商) 与控制者(云客户)之间的权利义务关系配置，而在过去，这些内容是完全 交由市场自行去解决的。因此有观点认为，GDPR 关于处理者的规范与作为新

生态的云计算格格不入13]。

[32]http://ec.europa.eu/justice/data-protection/international-transfers/

binding-corporate-rules/ber\_cooperation/index\_en.htm。

[33]W.Kuan Hon,GDPR:Killing cloud quickly?Available at <https://iapp.org/> news/a/gdpr-killing-cloud-quickly/。

**096**

**数据治理：数据政**

例如，GDPR要求，如果没有控制者授权，处理者不 应聘用另一个处理者，对于涉及补充或替换其他处理者的 变动，处理者都应当告知控制者，以便使控制者有机会反 对此类变化。对照此要求，目前市场上云服务的集成、转 售业态都将面临业务风险，因为控制者(云客户)随时可

以行使反对权。

要承认 GPDR对云计算生态体系带来的重大影响，但 客观来看，也可以通过合规及业务调整来适应。按照新规， 云服务合同中关于安全保障措施、风险管理以及服务价格

都会受到影响，控制者和处理者需要重新谈判达成。

当然，也仍有许多问题留待后续解决。处理者在云计

算生态里实际体现为不同的类型，典型如 IaaS 、PaaS、

Saas, 它们与服务的客户(控制者)之间的关系，以及数 据处理服务本身都体现出不同的特点，统一适用GDPR一 刀切的规范存在着与实际并不相符合的情况。例如，根据 GDPR规定，处理者只有在收到控制者的书面指示时才可 以处理个人数据，这对于大部分的 IaaS 场景来说几乎是 多余的要求，因为Iaas 更多的是提供基础设施，并不直 接参与客户的数据处理；而在有些服务场景却又是冗赘的， 比如在SaaS 服务中，云服务商需要开展相应的数据分析，

以便不断优化服务体验。

此外， GDPR 要求，如果处理者认为控制者某项指示 违反了数据保护法，其应当立即告知控制者。基于云服务 商与客户之间的服务关系，这种告知机制如何在商业实践 中落地，以及GDPR在多大程度上追究处理者的责任仍有

许多未解事宜。

**097**

**第二篇** **世界各国数据保护做法**

**(八)人工智能：深度学习即将违法?**

《终极算法》的作者，华盛顿大学教授 Pedro Domingos 在2018年 年初称：自5 月 25 日起，欧盟将会要求所有算法解释其输出原理，这意 味着深度学习即将非法。更有文章提出，GDPR 规定了“自动决策可解释权” (The Right to Explanation of Automated Decision): 数据主

体有权要求算法自动决策给出解释，有权在对算法决策不满意时选择退出14]。

然而，尽管承认 GDPR 对数字创新技术与应用带来的重大影响，但我们

也不应夸大这种影响。

首先，GDPR的正式条款中并没有出现所谓的“自动决策可解释权”,只 是在GDPR 背景引言(Recital 71)中阐述了数据主体对于自动化决定不 满意时，可以要求人工干预，并可以表达意见，获取对相关自动化决定的有 关解释。按照欧洲立法惯例，立法的背景引言只是起到帮助理解条款的目的，

自身并不具有法律效力(35)。

其次，GDPR 正式条款中与自动决策相关的条款，共有三个部分，但均 没有提出自动决策可解释的要求。(1)在第22条自动化的个人决策、个人 画像条款中，仅要求数据控制者应当采取适当措施保障数据主体的权利、自 由、正当利益，以及数据主体对控制者进行人工干涉，以便表达其观点和对 决策进行异议的基本权利。(2)在第13条、第14条数据主体的知情权部分，

规定控制者应当为数据主体提供是否存在自动化的决策的信息，以及在存在

[34]Richa Bhatia,Is Deep Learning Going to be Illegal in Europe?Available at <https://analyticsindiamag.com/deep-learning-going-illegal-europe/>。

[35]欧洲法院ECJ 明确指出了立法背景引言不具有法律效力。ECJ has commented directly on the legal status of Recitals,clarifying that:“Whilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule,it cannot in itself constitute such a

rule."Case 215/88 Casa Fleischhandels [1989]ECR-2789,para 31。

**098**

数据治理：数据政

自动化决策的情形下，对于相关逻辑，包括此类处理对于数据主体的预期后 果的有效信息。这一表述也推断不出有算法可解释的要求。(3)同样，在第

15条数据主体的访问权中，也不存在此类要求。

欧盟“第29条工作组”在2017年10月专门就此问题发布了指南(36)明 确澄清：关于自动决策，数据控制者并不必然要解释复杂的算法，对于用户

来说，只需要用尽可能简单的方法告知其背后的基本逻辑或者标准即可。

而最关键的是， GDPR 中规制的自动决策与“深度学习”并不能画等号。 GDPR仅仅规制对于个人产生法律或者重大影响的纯自动化决策，而包括“深 度学习”在内的人工智能显然有广阔的应用领域，不涉及个人数据，不产生

法律影响，也不存在人工干预的人工智能还有很多。

当然，尽管 GDPR中没有明确规定算法的可解释性要求，但算法的透明 和负责任依然是人工智能所面临的重大挑战，算法公开所涉及的商业秘密、 知识产权保护，以及深度学习算法的自身黑箱特点等现实问题，意味着在如 何保证算法的公平、公正、透明性方面还需要深入探讨更加有效的机制，仅

仅依靠所谓的“可解释权”难以走出困境。

**(九)区块链：与** **GDPR** **不相兼容?**

隐私和个人信息保护制度一直不断受到技术创新的冲击与挑战。从1995 年的《数据保护指令》到过去的20多年，是信息通信数字技术发展最快的时期，

因此，GDPR立法中最重要的一个任务就是如何回应数字创新带来的制度难题。

如果说移动互联网、物联网、云计算、大数据对数据保护的具体制度，

包括知情同意机制、安全责任、个人信息边界带来了如何执行的具体问题，

[36]Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679。

**099**

**第二篇** **世界各国数据保护做法**

那么作为互联网诞生以来最具有颠覆性的区块链，对个人信息保护制度的规

则带来了根本性的冲击。

因为区块链是一种全新的数据存储与管理模式，其本质上是一种通过共 识算法，在网络中分布式存储的去中心化数据库。它依靠密码学和数学算法， 无须任何第三方中心的介入就可以使参与者达成共识，以极低的成本解决了 信任与价值的可靠传递难题，对互联网中心化的平台商业模式带来了巨大冲

击，当然也对建立在中心化商业模式之上的数据保护制度带来了冲击。

不论是1995年的《数据保护指令》,还是改革之后的 GDPR, 依然是一 种中心化的规范范式[37]。它的制度体系重点指向的是那些中心化的数据控制 者、数据处理者，如政府机构、银行机构、医院，以及互联网世界中各种各 样的中心化平台。GDPR 建立以来的一系列规范，要求这些中心化的机构去承

担相关的保护义务，从而实现对个人数据的保护目的。

而区块链的数据处理模式是完全相反的去中心化模式，这与GDPR在规

范起点上就无法兼容，并导致了后续的一系列问题。

按照GDPR对个人数据的宽泛定义，以及对匿名化数据的高门槛要求(38), 区块链中以文本格式显示的个人数据，乃至被加密的数据，或者哈希之后与 个人相关的数据，包括公钥、交易数据，在相当大的程度上仍然属于个人数据。 那么参与此类数据处理的、在区块链任何节点上的矿工，都可以被认定为数 据控制者，同时也是数据的处理者(39),从而被要求遵从 GDPR的各项要求。

而对照目前的区块链应用，这几乎是不可能实现的要求，对公共链更是如此。

[37]Michèle Finck,Blockchains and Data Protection in the European Union,Max Planck Institute for Innovation and Competition Research Paper No.18-01。

[38]ARTICLE 29 DATA PROTECTION WORKING PARTY,Opinion 05/2014 on Anonymisa- tion Techniques,Adopted on 10 April 2014,Opinion 05/2014。

[39]Hoganlovells,A guide to blockchain and data protection,September **2017。**

**100**

**数据要素**

数据治理：数据政策发展与趋势

以比特币的区块链为例，截至目前约有11000个节点矿工 分布于全球，不用说数据主体本人，即使对数据保护监管

机构都是很大的挑战。

在数据权利方面，作为数据控制者，也很难按照 GDPR的要求，满足数据主体诉求。更正权、删除权、被 遗忘权等基本权利更是与区块链的核心机理相冲突。区块 链解决去中心化信任的关键功能就在于数据的不可篡改 性。 一旦信息经过验证并添加至区块链之中，就会永久地 存储起来，除非能够同时控制系统中超过51%的节点，否 则在单个节点上对数据库的修改是无效的，而同时控制众

多节点几乎是不可能的。

此外，区块链的单点记入、全网同步功能也与GDPR 中的数据最小化原则格格不入。按照数据最小化原则，数 据控制者应当只是处理满足目的的必要数据，而不得超出 范围。在区块链特别是公有链中，每个节点的数据维护都

会实现自动同步，且并不限制访问。

然而，尽管区块链与GDPR 在底层逻辑上就存在根本 冲突，但不可否认，区块链是实现GDPR立法目标的一种 可能技术路径，特别是在GDPR 作为制度本身仍然存在很 多缺陷的情况下，在现实中仅依靠 GDPR 显然无法实现对 个人信息进行充分保护的美好愿望。而在这一点上，区块

链技术本身可以大有作为。

区块链技术将有利于提升人们对个人数据的控制权，

用户掌握着公钥和唯一的私钥，可以更为自由地选择将个

**IOI**

**第二篇** **世界各国数据保护做法**

人数据在何时披露给何人，相比之下，目前中心化的数据

管理范式，如身份证号、医疗记录则有更多地被非授权披

露的风险。

如果从一开始就保守地将GDPR 用于规范和约束区块

链技术，甚至视区块链为违法技术，那么无疑会扼杀实现

数据保护目标的一条可能技术路径。更多地采取宽容的态

度，并在区块链应用发展过程中将制度与技术进行更双向

的包容互动，彼此调整和完善，将会是一个多赢的结果。

目前已有部分公有链尝试将个人数据单独存储在链下，满

足合规要求。也有越来越多的专家呼吁，GDPR 对于区块

链技术给予恰当的豁免。即使从欧盟的立场出发，这也是

一个值得考虑的选项。

**(十)高昂的处罚不可避免?**

对于GDPR 的严苛印象很大程度上来自高昂的罚金。

这主要源于GDPR对于违法行为在法规中并未设置具体的

罚金等级，而只有最高金额的限制，且仅仅区分为两档，

分别针对不同的违法行为。

(1)处以1000万欧元或者上一年度全部营收的28,

两者取其高；针对：违反隐私保护设计，以及默认隐私保护，

没有实施充分的 IT 安全保障措施、违反数据泄露通知要

求等(第83条第4款)。

(2)处以2000万欧元或者企业上一年度全部营业收

入的48,两者取其高。针对：违反数据处理原则，数据处

**102**

**数据要素**

数据治理：数据政策发展与趋势

理没有合法基础，违反同意要求，侵害数据主体的合法权利等(第83条第5款)。

显然，最高罚金仅仅在最严重的违法行为下适用。监管机构的矫正权力 也并不仅限于罚金，还包括警告、训诫，要求数据控制者或数据处理者改正，

要求对个人数据予以更正或擦除等。

GDPR背景引言中也引入了“轻微侵权”概念，基于对案件具体情况的考虑， 如果违法行为不会对有关数据主体的权利构成重大风险，那么在这种情况下，

可以用训诫取代罚款。

在欧盟“第29条工作组”发布的《行政罚款的适用和设置指南》401中 也明确：监管机构有责任选择最适当的措施，必须考虑所有能够采取的矫正 措施，在具体案件中，采取审慎平衡的方法，处罚措施应当是“有效的、恰当的、

有说服力的”。

此外， GDPR规定了监管机构在评估是否适用罚款条款和罚款金额的标准

时，应当考虑以下因素：

(a) 违法的性质、严重性与持续时间；

(b) 是基于故意还是基于过失；

(c) 控制者或处理者为了减轻数据主体损失而采取的所有行动；

(d) 与监管机构的合作程度；

(e) 监管机构得知违法行为的方式等。

因此，也可以从以上因素着手，在事前形成完善的数据管理制度， 一旦 发生数据事件后与监管机构保持良好密切的沟通，都有助于避免更为严厉的

处罚。

[40]ARTICLE 29 DATA PROTECTION WORKING PARTY,17/EN,WP 253,Guidelines on the application and setting of administrative fines for thepurposes of the Regulation 2016/679,Adopted on 3 October 2017。

**103**

**第二篇世界各国数据保护做法**

最后，考虑到GDPR适用于各类主体，处罚及罚金措

施不仅适用于企业，而且适用于政府机构、公共事业机构

等。为此，GDPR授权成员国可以制定本国的规则，以覆

盖对国内公共机构实施行政处罚的情形。

**三、结语**

GDPR 带来了许多改变。2016年立法文本的正式通过，

并不意味着制度规范都已成熟，相反，秩序建设的进程才

刚刚拉开序幕。特别是本文中所列出的那些充满争议的棘

手问题，面临挑战的不仅是GDPR的适用对象，而且包括

GDPR本身。所以，让我们放松心态，保持开放视角，不

论是对个人数据保护的合规工作，还是对个人数据保护法

律的完善，都是一场需要投入耐心和耐力的马拉松。

**104**

**数据要素**

数据治理：数据政策发展与趋势



**第** **8** **章**

**美国联邦与地方隐私立法的互补**

**摘要：**与美国联邦隐私立法的缓慢进程情形相比，美

国部分州和城市的隐私立法呈现出不同的景象。

虽然在近20年里，美国联邦层级的隐私立法并没有实 质性的推进，但在 Facebook 数据泄露事件后，建立美国 联邦层面的统一隐私立法似乎成了新的共识。然而，考虑 到美国隐私法的传统，联邦统一的立法仍然会与 GDPR有 明显的区别，特别是对于消费者保护实际效果、企业技术 创新发展会有更多的平衡考虑，以促进企业发展、技术创

新之间的平衡。

美国各州都制定了《数据泄露通知法》,在2018年爆 发大规模数据泄露事件的影响下，美国各州进一步完善了 《数据泄露通知法》。很多州立法中引入了向受到数据泄 露影响的个人提供免费信用监测服务的规定。例如，特拉 华州要求公司在特定情况下向受到数据泄露影响的个人提

供一年的免费信用监测服务。

数据泄露制度最早起源于加利福尼亚州2002年的《数 据泄露通知法案》,这一制度有两个主要功能。其一，为

企业保护敏感数据提供动力，因为公开披露的数据安全事

**105**

**第二篇** **世界各国数据保护做法**

件会损害企业声誉并触发昂贵的补救活动。其二，通知数

据泄露的个人，使其能够迅速做出反应，以减少潜在的损

害。但是在数据泄露事件多发的背景下，《数据泄露通知

法》所发挥的实际作用仍有待实践检验。公司对《数据泄

露通知法》的遵守意识和程度并不尽如人意。特别是对于

资源较少的小公司，令其承担证明安全程序合理或在数据

泄露的情况下提供免费的信用监测的义务并不现实。此外，

由于数据泄露规模的扩大和欺诈手段的演化升级，数据泄

露通知制度对于预防减少欺诈的作用已越来越弱。

而在数据泄露通知等传统立法领域之外，部分州将目

光转向了新兴业务领域的数据安全问题。2018年9月28日，

加利福尼亚州通过《信息隐私：连接设备法案》。该法案

旨在管理物联网设备，是美国首部关于“物联网”隐私的

州立法。该法案规定，任何与互联网相连的“智能”设备

的制造商都必须确保该设备具有“合理”的安全功能，“保

护设备和其中包含的任何信息不受未经授权的访问、破坏、

使用、修改或披露”。

除州立法外，为了应对与智慧城市、大数据相关的隐

私问题，城市隐私保护法律法规在美国兴起，成为继联邦

和州隐私立法之后的第三个层次的隐私保护的制度来源，

其主要覆盖对警方使用数据的规制，如西雅图市议会修订

《监视条例》,以避免公共生活中存在普遍和持续的监视。

纽约市也建立了类似法规，并同步探索针对城市使用传感

器技术的指导原则。这些灵活的地方立法成为美国隐私立

法的先行者，为未来联邦层面的隐私立法起到了经验积累

作用。

**106**

**数据要素**

**数据治理：数据政策发展与趋势**



**第9章**

**美欧隐私保护立法会走向趋同么?**

**摘要：**形式上，美国《2018年加州消费者隐私法案》 (简称CCPA) 与欧盟《通用数据保护条例》(简称GDPR) 有相似之处，但究其制度内核，仍然体现着美国与欧盟隐 私制度的烙印差异，美国更加注重消费者保护的实际效果，

以及促进企业发展、技术创新之间的平衡。

自2018年6月美国加利福尼亚州出台《2018年加州 消费者隐私法案》(California Consumer Privacy Act of 2018, 以下简称CCPA) 一年多来，加利福尼亚 州议会、参议院又陆续讨论了十几项CCPA 修正案，并审 议通过了其中六项法案，不断廓清制度规范，推动CCPA

走向“成熟定型”。

不同于以往美国联邦层面的，针对特定行业、特定事 项的隐私法案，CCPA 广泛适用于在加利福尼亚州开展业 务，收集处理加利福尼亚州居民个人信息并符合一定门槛 条件的企业。从全面性来说，这是美国目前最具有典型意 义的州隐私立法。同时，作为科技行业聚集地，加利福尼 亚州的经济体量排名世界第五，CCPA的影响力可与欧盟

的 GDPR 比肩，并且由于二者存在部分相似之处，引起了

**107**

**第二篇** **世界各国数据保护做法**

各方的极大关注：加利福尼亚州立法是否代表着美欧隐私

立法走向融合趋同?

从我们的观察来看，形式上CCPA与 GDPR有相似之 处，但究其制度内核，仍然体现着美国与欧盟隐私制度的 烙印差异，美国更加注重消费者保护的实际效果，以及促 进企业发展、技术创新之间的平衡。这不仅体现在CCPA 在2018年6月通过时的具体条文内容上[4],并且由于 CCPA的出台过于仓促142),立法者为进一步贴合产业实际， 为条文的后续完善预留了充分时间，并明确在2020年1 月 1 日CCPA正式生效前，加利福尼亚州议会可以继续对 CCPA条文做出修订。因此，从法案2018年通过后一年多 的时间，加利福尼亚州议会通过不断讨论和制定修正案， 推动 CCPA继续走向美国隐私保护法科学务实的一面。本 文将从 CcPA法案的重点条款及后续修订入手，进一步透

视美国隐私立法与欧盟之间的差异性。

**一** **、CCPA 对适用范围做了合理排除**

**(一)在受规制的实体方面，** **CCPA** **做了三类排除**

(1)非营利机构。

(2)提供数据服务的企业(Service Provider, 相

[41]关于CCPA 版本

条款内容与GDPR的差

异性，见王融、余春芳

《迷雾中的新航向——

2018年数据保护政策

年度观察》第一篇中

的分析，2018年12月

29日发表于腾讯研究

院微信公众号。

[42]CCP A 草案于

2017年2月发起，

经历加州议会半年

讨论后搁置。2018

年6月21日由加

州富商Alastair

Mactaggart 支持

的隐私保护组织募集

签名，重新将其作

为一项隐私立法倡议

启动，并与加州议

会达成妥协， 一周后

CCPA审议通过。

当于GDPR 中的Processor), 即接受数据控制者的委托

而提供数据处理服务的企业。此类企业不直接受CCPA规

制，而主要通过与数据控制者之间达成的服务协议来约束。

**108**

**数据治理：数据政**

[43]在考虑企业规模 因素方面， GDPR 仅 规定了在250人以下 的中小企业可以豁免 数据活动文档记录义 务，但本身对该豁免 也做出了很多限制。

(3)没有达到适用门槛的中小企业。这些门槛包括： ①年度总收入达到2500万美元；②每年涉及5万名以上的 加利福尼亚州居民、家庭或相关设备上的个人信息；③出 售加利福尼亚州居民个人信息获利占其年收入的50%或以

上。

作为对比，GDPR并没有区分营利目的、规模大小和 服务性质，从企业到政府部门，从中小企业到跨国公司， 甚至是个人，只要收集处理个人数据，均受规制，遵守相

同的高标准合规要求(43),

**(二)对“个人信息”定义予以合理限定**

2018年6月28日通过的CCPA, 其中对个人信息的定 义受到了GDPR 的影响，即只要与任何已识别或可识别的 自然人(“数据主体”)相关的信息，都可能被视为个人 信息，这将在实践中给受保护的数据范围带来极大的不确 定性。在数字时代，与特定信息主体有关的信息数量庞大，

统一纳入个人信息法律保护范围既不现实又无必要。

正是考虑到这一问题，在 CCPA通过之后，加利福尼

亚州参议院通过的“议会法案874” (Assem bly Bill

No.874) 将个人信息定义修改为： “个人信息”是指直接 或间接地识别、描述，能够合理地(Reaso nably) 相关 联或可合理地连接到 (Linked To) 特定消费者或家庭的 信息。修正法案通过强调“合理性”和“连接触达性”来

进一步限制或缩小CCPA所保护的“个人信息”的范畴。

**109**

**第二篇** **世界各国数据保护做法**

立法者认为，若不对个人信息的定义进行限制，则会

产生意想不到的后果。这将激励或迫使企业去识别那些本

不需要识别的某些数据，从而产生巨大的运营成本，也破

坏了数据安全理念。当然，目前的定义表述似乎也不能完

全解决个人信息定义的范围问题，因为“合理的连接和触

达”仍然包含了许多主观因素，这有待于加利福尼亚州执

法部门在实践中给出进一步的“指南”。

**(三)在受保护的数据类型方面，CCPA** **做了排除**

在适用保护的数据方面， CCPA非常务实地排除了“集

合信息”、 “去身份数据”、政府公开数据、雇员信息、

个人车辆和所有权信息，以及联邦法已经覆盖的医疗、征

信、驾驶员信息、金融数据等。

1.集合信息(Aggregate Information)

“集合信息”是指与消费者群体或类别相关的信息，

其中消费者的个人信息已被移除，这些信息不会与任何消

费者或家庭(包括通过设备)链接或产生合理连接，不再

视为个人信息。

2. 去身份数据 (Deidentified Data)

CCPA规定，对于已经使用了身份信息的企业，其可

以采取技术措施使得信息不能合理识别到特定消费者，这

一过程称为“去身份化”,具体要求包括：

(1)已实施了技术保障措施，禁止重新识别信息所

**II0**

数据治理：数据政

属的消费者。

(2)已实施了明确禁止重新识别信息的业务流程。

(3)已实施业务流程以防止无意中发布已识别的信息。

(4)不尝试重新识别身份信息。

去身份化的信息不再属于个人信息，同样不适用CCPA限制。与 GDPR 在背景部分关于匿名化数据的抽象介绍和相关的高标准解读相比，CCPA沿袭 了美国隐私立法的传统，从技术措施和管理流程着手，使得判断标准更为明

确和易于操作。

3. 政府公开信息(Publicly Available Information)

2018年6月28日通过的CCPA版本中规定： “个人信息”不包含公开可 用信息。“公开可用”是指从联邦、州或地方政府记录中可合法获取到的信息。 同时，立法文本中对“公开可用信息”的排除做了适当限制。若这些数据的

用途与政府记录中公布的数据目的不相符，则信息并非“公开可用”(44)。

但在此后，立法者对上述规定进行了反思修正，并最终删除了对公开可 用信息的限定，即删除了“若这些数据的用途与政府记录中公布的数据的目 的不相符，则信息并非‘公开可用’”。因为这种限定并不合理，企业很难 知晓政府公开数据的目的，即使假设企业可以知晓政府公开数据的目的，在 实践中也并不可能存在企业对此类数据的使用完全与政府目的相同的情况。

删除这一限定后，CCPA不适用于政府公开数据这一结论更加明确了。

4. 联邦立法已经覆盖的信息

**[44]**The California Consumer Privacy Act of 2018.https://leginfo.

legislature.ca.gov/faces/billTextClient.xhtml?bill\_id=201720180AB375。

**II1**

**第二篇** **世界各国数据保护做法**

为了与联邦隐私立法做好协调， CCPA排除了联邦立

法已经覆盖的受保护信息，具体如下145]。

[45]见CCPA 1798.145。

医疗信息。CCPA 不适用于《医疗信息保密法》

(Confidentiality of Medical Information

Act) 和《健康保险流通性与可用性法》(Health

Insurance Portability and Accountability

Act) 管辖的实体所收集的受保护健康信息。

征信信息。受《联邦公平信用报告法》 (Federal

Fair Credit Reporting Act) 规范的征信信息交易

[46]

[46]见 CCPA 1798.145(d)。

金融数据。根据《金融服务法现代化法案》(Gramm-

Leach-Blile y 法案)及实施规则来收集、处理、销售或

披露个人信息。

驾驶员信息(Driver’s Information)。根据

1994年《驾驶员隐私保护法》(Driver's Privacy

Protection Act of 1994) 来收集、处理、出售或披

露的个人信息。

5. 雇员信息

如果对雇员信息 (Employment Information) 与

消费者信息采用同样的保护措施，可能会影响企业对雇员

信息的使用。因此， CCPA通过之后，在劳工组织的推动下，

加利福尼亚州参议院又通过“议会法案25”(Assembly

Bill No.25, 简称AB-25) 将雇员信息排除在了CCPA

**112**



数据治理：数据政

规定的“个人信息”之外(47)。AB-25 规定，在2021年1月1日之前， CCPA 不适用于雇员信息。后续，应当由利益相关者继续协商制定一项更广泛的员

工数据隐私法案，同时可以更加明确加利福尼亚州消费者隐私法案的范畴。

6. 车辆信息和所有权信息

CCPA 规定了消费者对个人信息的各项权利，但是考虑到机动车的特殊性 及其安全需要，“议会法案1146” (Assembly Bill No.1146, 简称 AB- 1146)又做了除外规定：如果企业或服务提供商需要保留维护消费者的个人 信息，以履行根据联邦法律进行的车辆保修或产品召回的条款，则不限制车 辆制造商和经销商共享或保留车辆信息和所有权信息。并且定义车辆信息 (Vehicle Information) 是指车辆信息编号、品牌、型号、年份和里程 表读数，所有权信息 (Ownership Information) 是指车辆登记的一个或

多个所有者的姓名及其联系信息(48)。

二 、CCPA 仍然保持了美欧个人数据保护法的

最大差异，延续了 opt-out 模 式

依据GDPR, 在绝大多数商业化场景下，收集、处理消费者个人数据之前 必须要获得消费者的明确同意，即 opt-in 模式；而在加利福尼亚州消费者 隐私法中，对于16岁以上的消费者的个人信息处理(除出售以外),仍采取 美国隐私法中一以贯之的 opt-out 模式，即除非用户拒绝或退出，公司可以

继续处理用户的个人信息，这体现了美国一直以来在数据保护方面的务实思

[47]AB-25 California Consumer Privacy Act of 2018.https://leginfo.

legislature.ca.gov/faces/billNavClient.xhtml?bill\_id=201920200AB25。

[48]AB-1146 California Consumer Privacy Act of 2018:exemptions:vehicle

information.<http://leginfo.legislature.ca.gov/faces/billHistory>- Client.xhtml?bill id=201920200AB1146。

**113**

**第二篇世界各国数据保护做法**

路。opt- out 模式对消费者而言更为真实有用，同时对新进入市场的企业的

发展阻碍也更小。

而在GDPR 实施一周年的多个评估报告中，都对opt-in 模式的实际效 果提出了质疑。为了履行opt-in 模式，企业和机构向用户发送授权申请， 为获取用户同意的邮件大量涌入用户邮箱，被媒体称为人为制造了最大规模 的“垃圾邮件潮”。在网站页面获取 Cookie 的授权申请，因为合规要求而 冗长复杂，对于用户来说也是负累的，并不因此帮助用户真正做出判断，反 而由于其复杂性而选择略过。在 GDPR 生效6个月后，欧盟消费者对互联网

的信任降至10年来的最低水平(49)。

此外，在知情同意机制方面，相比于严格刚性的 GDPR,CCPA 也体现出 灵活弹性的特征。正如《华盛顿邮报》在欧盟市场所遭遇的困境，《华盛顿 邮报》在无法通过行为广告来补贴业务的情况下，选择直接向用户收费模式， 也面临 GDPR “关于同意是消费者自由、自主选择”的挑战。而对于此问题， 加利福尼亚州隐私法专门留出了弹性空间，其规定：消费者行使了本法规定 的隐私权利，企业不得有歧视对待，但是，如果该价格或差异与消费者所提 供的数据价值直接相关，那么企业还可以向消费者提供不同价格、不同费率、 不同品质的商品或服务。可见加利福尼亚州隐私法仍然承认数据的价值，允

许企业探索可行的商业模式。

除此之外，在个人权利、处罚机制和救济机制等方面，CCPA与GDPR还 存在着很大的不同。这些差异性均体现了美欧隐私立法的根本性分歧。我们

可以通过下面的表9.1 比较，形成一个较为全面的认识。

[49]One year on,GDPR needs a reality check,刊载于ftchinese,http://www. ftchinese.com/story/001083486。

I14

**数据治理：数据政**

表9.1 GDPR 与 CCPA 的异同对比

|  |  |  |  |
| --- | --- | --- | --- |
| 重要区别 | | GDPR | CCPA |
| 1.适用范围 | 1.1受保护的人的范围 | 地理位置标准：位于欧 盟境内的个人 | 居民标准(Resident): 居民标准参见加州  管制法典 |
| 1.2受规制的实体范围 (涉及域外适用问题) | 1.(1)欧盟境内机构； (2)欧盟境外机构  但提供服务或者监控 欧盟境内个人  2.包含Controller&  Processor  3.包含For Profit &None For Profit  4.不做任和规模排除， 从个人到跨国公司 | 1.在加运营的机构  2.仅提供数据服务的机 构(processor),大部 分情形不直受CCPA  管辖  3.仅包含For Profit机构  4.有适用门槛：年收入 在2500万美元或 …… |
| 1.3规制的数据  处理活动 | Processing Data(Process 含义极为广泛) | Collect,Sell,Share Data |
| 1.4排除的数据活动1 | 排除Anonymous Data (AD)的适用(但根据 欧盟对AD的解释，排 除门槛相当高) | 排除Aggregate  Information&De-identified Data(排除范围在现实  中更易操作) |
| 1.5排除的数据活动2 | 无(不排除公开数据) | 医疗、征信、驾驶、金融、 政府数据公开、雇员信  息、车辆信息及所有权 信息 |
| 2.数据分类 | 2.1敏感数据 | 单独列出敏感数据，保 护要求更高 | 无 |
| 2.2儿童数据 | 对于没有意识到是在收 集儿童数据的情形，没 有做出例外规定，这导 致机构的证明责任明显 增加 | 对于企业不实际知晓用 户年龄的情形，做出了 明确排除(延续了美国 CORPA思路和做法) |



**第二篇** **世界各国数据保护做法**

(续表)

**I15**

|  |  |  |  |
| --- | --- | --- | --- |
| 3.保护机制 | 3.1合法基础 | 1.数据处理必须要有合 法的理由(Legal  Basis)  2.大部分情形需要事前  获得同意opt-in模式 | 1.没有列出Legal Basis 2.大部分情形下仍然是 opt-out模式 |
| 4.保护权利 | 4.1知情权 | 应告知涉及数据处理几  乎所有相关信息，包括  机构信息、数据保护官 信息、数据接收方信息、 数据留存信息等 | 主要覆盖所涉及处理的  信息种类，强调是否“出 售”信息 |
| 4.2访问权 | 1.个人可以要求访问被 处理的所有个人数据 2.机构仅能够在证明访 问要求明显过量的情  况下，才能拒绝个人 访问数据的要求 | 1.消费者仅能够访问提 出请求时12个月内被 收集的个人数据  2.机构可以拒绝消费者 12个月之内的第三次 访问请求 |
| 4.3反对权 | 个人可以对任何数据处 理活动进行撤回同意或 者行使反对权 | 消费者仅能针对“出售” 活动行使opt-out模式 |
| 4.4删除权  (欧盟擦除权) | 规定了例外情形：与自 由表达、科学研究、法 定义务冲突情形下不予 支持 | 除了规定了与GDPR一  样的例外情形外，CCPA 还增加：  1.履行与用户的合同 2.识别和修复错误  3.符合消费者期待的内 部使用  4.其他合法使用情形 |
| 4.5可携权 | 1.适用于消费者提供的 所有数据  2.服务于消费者实现机  构到机构的数据转移 | 1.消费者在12个月内被 收集的信息  2.服务于消费者本人获 取数据 |

**I16**

**数据治理：数据政**

(续表)

|  |  |  |  |
| --- | --- | --- | --- |
| 5.执法机制 | 5.1执法主体 | 行政机构：各国DPA可 直接开出罚款 | 司法机构：检察长提出 诉讼后，由法院作出民 事罚金裁决 |
| 5.2罚金幅度 | 高限罚款：全部年度 收入的2%(4%)或者 1000万(2000万)欧元， 两者取其高 | 2500美元/每次违法  7500美元/每次故意违 法 |
| 5.3民事救济 | 个人可以对任何违法行 为提出民事诉讼 | 消费者仅能够针对未加 密个人信息的泄露行为 寻求救济；  在任何法定损害诉讼发 起之前，当事企业应该 与30天的书面改正通知 期，企业在30天内改正 行为，诉讼不再发起(因 企业违法行为而使得消 费者实际遭受经济损失 的诉讼不收此条件约束) |
| 6.总体 | 加州宪法将消费者隐私权作为宪法性权利，这使得加州CCPA与欧盟GDPR  具有了某种相似性，但究其内容，仍体现出欧美法律制度根本性分歧，欧洲 法律体系更倾向于监管扩张，美国法律体系偏克制与务实 | | |

**三、结语**

不同于欧盟从人权项下出发的个人数据保护机制抽象 刚性，美国从消费者权利视角出发的法律机制天然补充了

市场视角，从而更加灵活务实。

CCPA在通过之后的一系列修正案更是表明了美国隐 私法的独特风格，从对opt-out 模式的把握，到一系列 合理的除外规定，再到具体的合规细节澄清(例如企业在

响应消费者需求时，仅需提供电子邮件地址等电子渠道方

117

**第二篇** **世界各国数据保护做法**

式，而不再需要运营维护专门电话)50],都着眼于合理规范数据的商业化利用，

平衡消费者权利和技术创新空间，使其更加符合产业实践且便于实施。

**[50]AB-1564** California Consumer Privacy Act of 2018.http://leginfo.

legislature.ca.gov/faces/billTextClient.xhtml?bill\_id=201920200AB1564。

**II8**

数据治理：数据政



**第10章**

**我国个人信息保护刑事立法**

**进展及企业风险防范**

**摘要：**刑事保护是我国目前在个人信息保护领域应用 最为活跃的法律机制。2017年6月1日， 《网络安全法》 及最新刑事司法解释正式施行，我国个人信息保护刑事立 法适用主体广、入刑门槛低、适用刑罚严厉的特点更为明 确。在此背景下，准确理解立法制度与适用，对企业有效

防范刑事风险至关重要。

**一** **、加速推进个人信息保护刑事立法**

有关公民个人信息保护的刑事规定，主要在《刑法》 第二编分则的第四章“侵犯公民人身权利、民主权利罪”中。 1997年《刑法》中仅规定了侵犯通信自由罪(第252条) 以及私自开拆、隐匿、毁弃邮件、电报罪(第253条)。 随着近几年公民个人信息受到侵害的现象多发，在近年来 的刑事立法活动中，都将个人信息保护作为其中重要的修

法内容。

2009年，《刑法修正案(七)》(以下简称《刑七》)

首次引入了“侵犯个人信息罪”。在《刑法》第253条中

**I19**

**第二篇** **世界各国数据保护做法**

增加了“出售、非法提供公民个人信息罪”和“非法获取

公民个人信息罪”。犯罪主体限定为特殊主体，包括国家

机关、金融、电信、交通、教育、医疗等单位及工作人员。

2015年，《刑法修正案(九)》(以下简称《刑九》)

再次对刑法第253条做了修改完善：(1)扩大犯罪主体范

围。任何单位和个人只要实施违法行为，情节严重的，都

可构成犯罪；(2)量刑增加一档。在原有的“处三年以下

有期徒刑或者拘役，并处或者单处罚金”的基础上，针对

“情节特别严重的”,量刑提升至“三年以上七年以下有

期徒刑，并处罚金”。(3)增加了从重处罚的情形。“将

履行职责或者提供服务过程中获得的个人信息，非法出售、

提供给他人的，适用从重刑。”修改后的罪名统一称为“侵

犯公民个人信息罪”。

2017年5月，最高人民法院和最高人民检察院发布

了《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》(以下简称《解释》)。在个人信息保护刑事

司法近十年实践经验的系统总结之上，《解释》对困扰司

法实践的定罪量刑热点问题做了明确回应。

《刑九》第253条与《解释》是我国针对个人信息侵

害行为独立发展出的刑事规范完整体系，包括了个人信息

罪的罪名罪状、定罪量刑标准、相关法律适用，甚至涉及

诉讼中的举证责任分配问题。这在全球刑事立法及司法领

域也很少见。在该领域，我国已然形成了具有鲜明国情特

色的“中国样本”。

**120**

**数据要素**

**数据治理：数据政策发展与趋势**

[51]周加海，邹涛， 喻海松 . 关于办理侵 犯公民个人信息刑事 案件适用法律若干问 题的解释的理解与适 用，2017年5月。

**二、我国个人信息刑事保护的主要特点**

**(一)刑事司法最活跃**

民事救济、行政监管、刑事打击是个人信息法律保护 体系的三大支柱。我国在民、行、刑三领域的个人信息保 护立法也均有建树。然而在法律适用领域，与民、刑相比， 我国个人信息保护刑事司法实践更为活跃。据统计，自 2009年《刑七》引入侵犯个人信息罪到2016年12月，全 国法院共审结出售、非法提供公民个人信息、非法获取公 民个人信息刑事案件1433起，生效判决人数2112人。特 别是2015年11月《刑九》生效以来，我国对侵犯公民个 人信息犯罪呈高压态势，案件量显著增长，仅一年时间就

审结464件，生效判决人数697人[51]。

刑事追责是我国当前个人信息保护领域应用最广泛、 最深入的法律手段，这与欧洲推崇行政监管、美国倚重民

事救济相比，具有鲜明特色。

**(二)适用主体广**

刑事责任是最严厉的法律责任，只规制严重侵害或 威胁法律的行为，适用也往往更加谨慎。这也是《刑七》 在最初引入相关罪名时，仅把犯罪主体限定为国家机关 及特定行业单位和个人的主要出发点。实际上，从全球范 围来看，在建立有个人信息刑事追惩机制的国家， 一般 也会通过不同方式对“罪名适用范围”加以限制。例如，

美国个人信息保护立法分散在金融、健康、征信以及儿童

**I21**

**第二篇** **世界各国数据保护做法**

隐私等领域，其中仅仅针对个人健康信息违法行为建立了

刑事处罚。美国《健康保险隐私及责任法案》 (Health

Insurance Portability and Accountability

Act,HIPAA) 对犯罪主体限定为医疗机构及工作人员，

并特别强调主观恶意，只有在明知故意或欺诈、虚假陈述

方式获得非法利益的情形下，才会被追究刑事责任。

相比而言，为进一步打击个人信息违法活动，我国《刑

九》在适用主体范围上做了重要突破，“侵害个人信息罪”

不再局限于国家机关、重点行业领域。任何个人、单位都

有可能因非法获取、提供个人信息而被追究刑责。

**(三)入罪门槛低**

“情节严重”是我国将“违法提供、获取个人信息”

行为入罪的核心标准。《解释》从信息数量、违法所得、

信息用途、主观恶性、违法主体五个方面对“情节严重”

做了具象化的描述。从《解释》对五个方面的界定标准看，

我国对侵害个人信息罪的入罪门槛设定较低。以信息数量

为例，对高度敏感的个人信息——“行踪轨迹信息、通信

内容、征信信息、财产信息”非法提供、获取的，数量达

到50条即可入罪；若是将履行职责或者提供服务过程中获

得的此类信息出售或者非法提供给他人的，数量标准减半，

25条即可入罪。

**(四)适用刑罚较严厉**

我国对个人信息罪的适用刑罚包括人身自由刑和罚金

**122**

**数据治理：数据政**

两类。其中，第一档量刑为“处三年以下有期徒刑或者拘役，并处或者单处

罚金”,第二档量刑为“三年以上七年以下有期徒刑，并处罚金”。

从国际比较而言，上述刑罚是较为严厉的。首先，目前仍有部分国家并 没有就个人信息保护设立专门的刑事责任体系，而是仍停留在侵犯公民通信 自由罪、非法入侵信息系统罪阶段。即使是针对个人信息保护，建立有刑事 机制的国家，也通过不同方式对适用做了限定。例如： (1)通过对适用范围 予以限定，如美国的情形，仅针对医疗健康行业；(2)刑罚中仅包括罚金刑， 不包括人身刑，如加拿大、爱尔兰；(3)虽规定了人身刑，但在司法实践中 绝大部分适用罚金刑，如英国、新加坡； (4)人身自由刑设置缓和，不超过 1年或2年，如德国、葡萄牙、荷兰等大部分欧盟成员国的刑法设定，而日

本的最高刑期不超过6个月(52)。

综上，我国的个人信息保护刑事政策是较为严苛的，在此背景下，准确

理解刑事立法制度与适用，对企业有效防范刑事风险至关重要。

**三、我国个人信息刑事保护制度要点**

结合《刑九》《解释》以及最高人民法院和最高人民检察院发布的《侵 犯公民个人信息犯罪典型案例》,理解我国个人信息保护刑事制度可从以下

问题入手。

**(一)哪些个人信息纳入刑法保护?**

第一，《解释》对个人信息的界定做了重要扩展，在“身份识别信息”

基础上，新增了“个人活动情况信息”。从2012年的《全国人大常委会关于

[52]Baker 6 McKenzie,2016 Global Data Protection Enforcement Report -

Enforcement by regulators:penalties,powers and risks,January 2016。

I23

**第二篇** **世界各国数据保护做法**

加强网络信息安全的决定》到2016年的《网络安全法》,

我国立法对个人信息的界定一直限定为身份识别信息。此

次《解释》对个人信息做广义理解，明确“公民个人信息”

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、身份证件号码、通讯联系方式、住址、

账号及密码、财产状况、行踪轨迹等。 “个人活动情况的

信息”明确列入了刑事保护的个人信息范围。

需要明确的是，定义中界定部分与列举部分的关系， 并不是列举信息都必然是个人信息。例如，所列举的“财 产状况、行踪轨迹”只有在能够识别特定人身份或者反映 特定人活动情况时，才属于个人信息。群体的财产状况、

行踪轨迹(如春运热力图)并不属于个人信息。

第二，根据个人信息与人身、财产安全的敏感程度，《解 释》将个人信息区分为三类，并设置了相应的入罪梯度153]。 第一类是高度敏感信息，包括四种信息：行踪轨迹信息、 通信内容、征信信息、财产信息。涉及高度敏感信息的违 法活动，由于定罪门槛最低，因此严格限制在此四类，不 做任何扩展；第二类是敏感信息，包括住宿信息、通信记 录、健康生理信息、交易信息等其他可能影响人身、财产 安全的公民个人信息。与第一类信息相比较，《解释》对 第二类信息的界定仍留有空间，意味着在司法实践中，仍 有可能会出现目前所列举之外的第二类信息类型；第三类 信息是其他个人信息，即上述第二、三类以外的个人信息。 个人信息的类型是定罪量刑的重要依据。信息越敏感，达

到定罪门槛的信息数量越少。

[53]林哲骏 .侵犯

公民个人信息罪定罪

标准研究：以“个人

信息”和“情节严

重”认定标准构建为

视角.尊重司法规律

与刑事法律适用研究

(下):全国法院第

27届学术讨论会获奖

论文集。

**124**

**数据治理：数据政**

第三，新增的“行踪轨迹”仅指个人实际物理位置信息。 《解释》公布后，有观点认为“行踪轨迹”不仅包括实际 物理位置信息，而且可能包括个人在虚拟网络中的活动轨 迹，例如Cookie 中的信息记录。这种理解并不准确。从 立法部门对《解释》的说明看，列入“行踪轨迹”信息类 型的主要目的是，打击利用此类信息的绑架、诈骗等危害 人身安全的犯罪行为，且“行踪轨迹”被列入高度敏感信 息类，有关此类信息的入罪门槛低，因此严格限定为四类， 不做任何扩展解释，用户的网络活动轨迹不属于此类“行 踪轨迹”。当然，网络活动轨迹如与特定人相关联，也可

能被列入其他类的个人信息。

第四，新增加的“财产状况”不仅包括传统银行账户 信息，而且包括互联网金融业务中的账户、财产信息。例如，

第三方支付结算账户、金融服务账户信息及财产信息。

第五， “公民个人信息”保护并不限定于中国公民。 基于平等适用刑法原则，对侵害我国境内外国人、无国籍 人个人信息的案件，以及我国境内行为侵害境外外国人、 无国籍人个人信息的案件，我国都予以刑事保护。这一理 解也符合《网络安全法》的立法精神。《网络安全法》从 一审草案到最终稿也删去了“公民”表述，个人信息并不

以中国公民为限定。

**(二)哪些行为会被追究刑事责任?**

1.“非法提供”和“非法获取”两大类行为

我国刑事立法主要打击个人信息犯罪链条两端的行

**125**

**第二篇** **世界各国数据保护做法**

为，即非法提供和非法获取两大类。而在个人信息保护的

中间环节，如个人数据的留存、更正、删除、加工、分析

等处理行为，更多地留给民事、行政领域立法调整。

2.“违反国家有关规定”是认定“非法”的重要依据

《刑九》并没有列明哪些行为属于非法获取或非法提

供，而是给出了一个笼统的前提——“违反国家有关规定”。

从《刑七)》到《刑九》的重要变化之一是，将“非法”

这一前提从“违反国家规定”扩展为“违反国家有关规定”,

两字之差体现了重大变化。

依照刑法总则第九十六条：本法所称违反国家规定，

是指违反全国人民代表大会及其常务委员会制定的法律和

决定，国务院制定的行政法规、规定的行政措施、发布的

决定和命令。由此刑法中的“国家规定”排除了地方性法规、

地方规章和国务院各部委制定的部门规章。

此次《解释》在《刑九》的基础上，将“国家有关规定”

进一步明确为法律、行政法规和部门规章。部门规章自此

成为个人信息刑事定罪的重要基准之一。而从我国的立法

实践看，有关个人信息保护的规定大量分散在部委规章中，

特别是随着“互联网+”的快速发展，互联网对传统行业、

领域的渗透加速，传统监管部门对信息安全、数据保护的

关注加大，新制定的部门规章中往往会嵌有个人信息保护

条款。例如，2016年交通部等七部委颁发的部门联合规章

《网络预约出租汽车经营服务管理暂行办法》对个人数据

的获取、对外提供制定了更为细致的规定，其中部分规定

**I26**



**数据治理：数据政**

比《网络安全法》更为严格。

**(三)“非法提供”如何认定?**

1.“出售”是“非法提供”的典型行为方式

从《刑七》到《刑九》,“出售”行为都从“非法提供” 行为中单独列出，概因“出售”行为的主观恶意最为明显， 也是现实中“个人信息黑产”的主要形态。但仍需要注意 的是，对于“出售”行为，刑法并没有“一刀切”地禁止， 仍然限定在“违反国家有关规定”的情形下。这与《网络 安全法》一脉相承，也是对《决定》中一刀切禁止“出售

行为”的修正。

[54]北京大兴区人民 检察院《侵犯公民个 人信息犯罪研究》课 题组.侵犯公民个人 信息犯罪的实践应用 探究：从人肉搜索行 为的入罪规制疑难来

考察. 净月学刊，

2015年第2期。

2. “非法发布”行为也属于“非法提供”

“提供”既包括向特定人提供，又包括向不特定人提 供。此次《解释》明确：通过信息网络或者其他途径发布 公民个人信息的，属于“提供公民个人信息”。这在一定 程度上回应了备受争议的“人肉搜索”是否入刑的问题1 , 即违法发布他人的个人信息，情节严重的，可被纳入“非

法提供”情形。

3. 不属于非法提供的情形

合法提供个人信息，主要包括两种情形。

(1)经被收集者同意。《网络安全法》第四十二条 第一款规定：未经被收集者同意，不得向他人提供个人信

息。因此，获得个人同意属于合法提供的情形，且《网络



**第二篇** **世界各国数据保护做法**

**127**

安全法》中并未就同意的形式做出限定。但需要注意的是，

在一些行业特别法中对同意的形式提出了具体要求，如《征

信业管理条例》对于“提供”的规定，部分情形下要求信

息主体的“书面同意”, 《网络预约出租汽车经营服务管

理暂行办法》规定：要求获得信息主体的“明示同意”。

(2)数据经过处理无法识别个人，也无法复原。同

样是《网络安全法》上述条款中的但书规定，对提供匿名

化数据的行为予以了豁免。该条款科学地平衡了安全与发

展二者的关系，为数据合理流动、创新提供了合法路径。

上述两种情形，是我国立法中明确规定的数据提供行

为的合法情形，也是当前企业实务应用最为主要的合法抗

辩理由。当然，除以上合法情形外，从对“非法”的法理

理解出发，对外提供个人信息仍可以有以下合法理由：(1)

为保护信息主体或其他第三方生命、财产的重大利益而需

要提供的； (2)为履行向国家机关、司法机关执法协助义

务而需要提供的。显然，此类情形并非企业日常经营中数

据提供的常见情形。

**(四)“非法获取”如何认定**

1.“窃取”是“非法获取”的典型行为方式

与“出售”行为始终在“非法提供”类行为中单独列

出类似， “窃取”也一直作为“非法获取行为”的典型方

式单列。这强调了获取方式手段自身的非法性，以此类推，

以“欺骗” “抢夺”等非法手段方式获取的当然也属于非

**128**

**数据治理：数据政**

法获取，但这并不意味“非法获取”仅考虑获取手段的非 法性(551)

[55]赵秉志 .公民 个人信息刑法保护问 题研究 .华东政法 大学学报，2014,17 (1):117-127。

2. 无法提供获取信息的正当性，可被认定为“非法

获取”

只要违反国家规定获取个人信息，信息获取者无法主 张其获取信息的正当理由的，无论是以“窃取”等本身非 法的手段来获取，还是以“购买、收受、交换”等其他手 段来获取，都可被认为是“非法获取”。这有利于直接打 击“个人信息黑产”中的买卖交易，但同时也对大数据开 发利用中的商务合作带来了更高的合规风险，特别是通过 第三方渠道获取个人信息的，需要在事前履行更加审慎的

合规义务。

以上两类情形，更多地指向了不同主体之间对于数据 的获取、流转行为，除此之外，此次《解释》对“非法获取”

的含义做了进一步扩展，深入了收集环节。

3.“在提供服务过程中，违反国家有关规定收集个人

信息的，视为“非法获取”

尽管《网络安全法》主要适用于网络运营者，但它是 目前最能完整体现我国个人信息保护制度的主要法律，确

立了个人信息的收集原则及具体要求。参考其第四十一条

规定，以下情形下的收集活动，都可被视为“非法获取”。

(1)未遵循合法、正当、必要原则收集信息。

(2)未公开收集信息的规则，使用目的、方式和范围。

**129**

**第二篇** **世界各国数据保护做法**

(3)未经过被收集者同意。

(4)收集了与所提供服务无关的个人信息。

(5)收集了法律、行政法规禁止收集的信息。

(6)收集了超出约定范围的信息。

可见，我国对“非法获取个人信息”的行为认定已覆

盖到实务中的个人信息收集环节。况且，除《网络安全法》

外，我国仍有相当数量法律、行政法规、部门规章涉及关

于个人信息收集的具体要求， “违法收集个人信息”的刑

事风险点显著增多。

**(五)如何“定罪量刑”**

《解释》第五条规定了“情节严重” “情节特别严重”

两档量刑标准。

1. 符合“情节严重”,适用第一档量刑的情形

① 出售或者提供行踪轨迹信息，被他人用于犯罪的。

② 知道或者应当知道他人利用公民个人信息实施犯

罪，向其出售或者提供的。

③ 非法获取、出售或者提供行踪轨迹信息、通信内

容、征信信息、财产信息50条以上的。

④ 非法获取、出售或者提供住宿信息、通信记录、

健康生理信息、交易信息等其他可能影响人身、财产安全

的公民个人信息500条以上的。

**130**

**数据要素**

**数据治理：数据政策发展与趋势**

⑤ 非法获取、出售或者提供第③项、第④项规定以

外的公民个人信息5000条以上的。

⑥ 数量未达到第③项至第⑤项规定标准，但是按相

应比例合计达到有关数量标准的。

⑦ 违法所得五千元以上的。

⑧ 将在履行职责或者提供服务过程中获得的公民个 人信息出售或者提供给他人，数量或者数额达到第③项至

第7项规定标准一半以上的。

⑨ 曾因侵犯公民个人信息受过刑事处罚或者两年内 受过行政处罚，又非法获取、出售或者提供公民个人信息

的。

⑩ 其他情节严重的情形。

以上10项覆盖了犯罪构成的主体、主观方面、客体、 客观方面的要素，其中第③、④、⑤项，根据信息的敏感 程度，分别设定了50条、500条、5000条的入刑标准。特 殊主体(将履行职责或提供服务过程中获得的个人信息出 售、非法提供给他人的)入刑标准减半。第⑥项查缺补漏，

对同一案件中涉及不同类型的，可按照数量比例累计入刑。

2. 符合“情节特别严重”,适用加重刑的情形

① 造成被害人死亡、重伤、精神失常或者被绑架等

严重后果的。

② 造成重大经济损失或者恶劣社会影响的。

**131**

**第二篇** **世界各国数据保护做法**

③ 数量或者数额达到前款第三项至第八项规定标准

十倍以上的。

④ 其他情节特别严重的情形。

在《解释》出台之前，尽管《刑九》中已经将最高刑 提升至7年，但实务中由于审判人员对个人信息犯罪的危 害性并不确定，大部分法院审结案件做出的是法定刑三年 以下的判决[56]。《解释》对重刑情节予以明确，其中从 信息数量因素看，尽管将重刑门槛定于普通量刑定罪数量 的十倍以上，但由于普通量刑本身的起点低，十倍之后也 仍然不高。如依违法所得标准，违法所得在5万元以上的， 即可构成重刑。因此有学者预测， 《解释》正式实施后，

侵害个人信息犯罪适用重刑可能会出现激增现象。

[56]李玉萍 .侵犯公

民个人信息罪的实践

与思考 . 法律适用，

2016(9):11-16。

3. 为合法经营活动购买、收受公民个人信息定罪量

刑的特殊标准

① 利用非法购买、收受的公民个人信息获利5万元

以上的。

② 曾因侵犯公民个人信息受过刑事处罚或者两年内

受过行政处罚，又非法购买、收受公民个人信息的。

③ 其他情节严重的情形。

特殊适用标准是《解释》为大数据创新活动做出的相

对宽容的处理，即如果企业出于合法经营活动的目的，例

如因广告营销目的，而购买、收受个人信息的，量刑适用

于第一档量刑(3年以下或罚金刑),并不适用从重刑，

**132**

**数据治理：数据政**

且定罪的考虑因素也有所区别，并不再参考信息数量标准， 而主要结合两方面： 一是违法收益(且收益标准也有所提 升，达到5万元以上);二是是否为重复犯罪。当然，适

用“宽容”标准有着严格的限制：

(1)必须为合法经营活动。如广告推销，或者被告

方能够举证证明合法经营活动的其他情形。

(2)只能限定在获取行为，对外提供行为并不适用。

(3)只能限定为普通个人信息，并不包括《解释》

中所列的“高度敏感信息”和“敏感信息”两类。

此类相对宽松的量刑标准反映了立法者在“安全与发 展”之间的平衡。在信息用途上，将合法经营活动区分出来， 此类活动中的非法获取行为并不具有明显的社会危害性，

入刑门槛适度放宽。

**四** **、企业的刑事风险防范策略**

严厉的个人信息保护刑事规范，对打击个人信息违法 犯罪活动将起到更大的威慑作用，也将为企业数据资产构 筑法律安全屏障。但同时，严格的刑事责任，对于企业来说， 尤其是以数据处理为核心业务，或日常运营中处理敏感数 据的企业，如互联网、电信、金融、征信、医疗、教育等 行业领域的经营者，所面临的法律风险不容低估。特别是， 我国“侵害个人信息罪”适用于单位犯罪。单位可作为违

法主体被追究刑事责任，判处罚金，同时，单位直接负责



**第二篇** **世界各国数据保护做法**

**133**



的主管人员和其他直接责任人员也承担相应的刑责。对此，

企业应建立完备的数据管理安全体系，制定系统的风险防

范策略予以应对。

**(一)个人信息分类分级管理**

《解释》出台之前，我国有关个人信息保护的相关立

法中并没有直接体现出对数据的分类思路，仅在2013年的

指导性标准中，提出将个人信息区分为个人敏感信息和个

人一般信息，并推荐适用不同的收集同意标准。

此次《解释》明确将数据自身的敏感程度作为定罪量

刑的直接依据后，在企业实践中实施数据分类分级管理的

必要性将更为突出。实际上，数据分级分类管理已是实务

中的普遍做法，但根据《解释》,企业需要在现有做法的

基础上，对个人信息类别再行细分，同时也需要结合企业

的业务场景，与用户个人利益的相关度、数据自身安全威

胁强弱等维度，系统地梳理数据类别、安全级别，针对不

同级别，实施强弱有别的安全防护。特别是在个人信息获

取、对外提供环节，加大合规投入。

**(二)信息获取，“取之有道”**

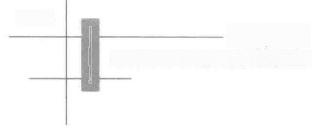
本文并不讨论窃取、骗取等明显具有非法性质的数据

获取行为，而只讨论企业正常经营活动中涉及合规重点的

两类情形。

1.提供服务过程中面向用户，直接收集个人信息的情

形，需保证以下合规要求

**I34**

**数据要素**

数据治理：数据政策发展与趋势

(1)保障用户知情权。公开信息收集规则、收集的 目的、收集的方式和范围，例如通过公告、隐私政策、业

务协议等方式公开法定要求公开的信息。

(2)获得用户的同意。这是决定收集“合法与否” 的关键点。需要结合业务所适用的具体法规、规章，满足 其具体合规要求。如上所述，《征信管理条例》中的“书 面同意”要求，网约车业务规范中的“明示同意”要求等， 通过业务协议等格式条款获取用户同意的，需要满足合同

法中关于格式条款的具体要求。

(3)审查所收集信息与业务提供的相关性，以满足 收集信息的合法、正当、必要原则。其中《网络安全法》 明确禁止收集与所提供服务无关的信息。当然，从《网络 安全法》的表述来看，对收集活动仍然采取的是相对宽松 的标准，即从与业务的相关度来评判，对收集信息的范围

仍留有弹性空间

(4)不得超出用户协议范围收集信息。在用户协议中， 应尽可能明确所收集个人信息的主要类别、类型，以完整

覆盖提供服务所必需的数据，并保障用户的知情同意权。

(5)不得收集法律禁止收集的用户个人信息。如《征 信业管理条例》明确禁止征信机构采集个人的宗教信仰、

基因、指纹、血型、疾病和病史信息。

做到以上合规点，避免落入“违反国家规定收集个人

信息”情形，是防范刑事责任风险的根本。

**135**

**第二篇世界各国数据保护做法**

2.从第三方获取个人信息的合规审查

《解释》将“违反国家规定，购买、收受、交换个人信息”

纳入“非法获取情形”,在实践中主要涉及企业与第三方

合作的场景。目前来看，合规仍有模糊地带。但从企业所

扮演的两种角色出发，可提出如下探讨思路。

(1)企业仅作为服务提供者的角色时，并不负担数

据收集活动是否合法的义务。例如，电信企业为第三方提

供短信息发送服务，从而“收受”第三方提供的电话号码

信息。在此情形下，若短信息服务自身合法，电信企业并

不负有审查第三方获取个人信息是否合法的义务。电信企

业所负的主要义务，是依据与第三方的“服务协议”所承

担的数据安全义务。类似地，云计算服务也属此类情形。

云服务提供者并不负有审查云客户个人信息收集活动是否

合法的义务，而主要依据服务协议承担数据安全责任。

(2)企业从第三方获取数据，是为了实现自身的业

务目的。此类情形是刑法规范的重点，即企业与第三方的

合作，并不仅仅是为第三方提供服务，特别是通过“购买、

交换”方式获得的数据，已带有明显的自身目的。此类情

形下，为保证合规，避免刑事责任风险，建议企业在第三

方收集个人信息的环节，就能够通过第三方向个人披露关

于个人信息收集、交换、对外提供的信息，并征得用户的

同意。

**(三)对外提供，遵循合规高标准**

与“非法获取”相比，“非法提供”的认定更明朗一些。

**136**

**数据治理：数据政**

因为“禁止对外提供”是一般性原则，少数合法提供的情形， 立法已有明确规定。最为主要的合法依据有两方面， 一是 征得了个人的同意，二是进行了数据匿名化。征得个人同 意，并无太多认识分歧。相比而言，匿名化是新近提出的 合规渠道，无论是在学界还是在司法实务界都还存在不同

的看法。

但总体而言，数据匿名化是兼顾隐私保护与数据利用 的有效手段，企业可以采取技术、合同、审计等多种手段， 努力实现数据不再具有身份可识别性，并在此基础上实现

数据的交易流转、加工利用。

需要澄清的是，数据匿名化并不是一个绝对状态，因 为决定数据是否处于匿名状态的两个主要因素——数据算 法和可获得的数据资源始终时刻处于动态变化之中，算法 日益强大，数据资源不断丰富，当前的匿名化并不代表永 久的匿名化，因此在将数据匿名化作为可对外提供的例外 情形时，在具体的司法裁量中也应遵循相对标准，而不是 绝对标准，即在特定的案例中，企业是否采取了相对充分 的匿名化措施，以使得获得数据的第三方采取一般可能的

技术措施，也无法将数据关联到特定个人。

因此，企业是否采取了相对充分的匿名化措施，决定 了其是否可以适用对外提供的例外条款，对比，企业至少

可以从以下方面开展合规检查，预防可能的法律风险。

(1)在对外提供的业务场景中，开展隐私风险评估。

包括评估合作方的数据利用目的、个人隐私的敏感度、合

**137**

**第二篇** **世界各国数据保护做法**

作方所掌握的数据资源、数据分析能力等。

(2)根据隐私风险评估结果，选择有针对性的数据

匿名策略，包括不同的匿名技术方式、加密手段等。

(3)通过合作协议加以限制及明确责任。例如，对

数据的使用场景、目的进行约束；限制关联数据进入特定

的数据场景；对数据访问的技术限制；做出不再试图重新

恢复身份属性的法律承诺；对随机情况下再识别数据做出

破坏处理的约定；对数据的返还、销毁等做出协议安排。

**(四)严格履行网络信息管理义务**

如上所述，我国“侵害公民个人信息罪”仅指向针对

个人信息的非法获取、非法提供这两端行为，并不覆盖其

他环节。但对于电信、互联网企业等“网络服务提供者”

而言，刑法第二百八十六条之一“拒不履行信息网络安全

管理义务罪”也与企业在用户个人信息方面的刑事责任风

险强相关。

《刑九》及《解释》规定：网络服务提供者拒不履

行法律、行政法规规定的信息网络安全管理义务，经监

管部门责令采取改正措施而拒不改正，致使用户的公

民个人信息泄露，造成严重后果的，应当依照刑法第

二百八十六条之一的规定，以拒不履行信息网络安全管

理义务罪定罪处罚。

尽管从本罪的表述来看，已对构成犯罪的情况做了极

大限定，必须同时满足三个前提： “不履行网络信息安全

 **138** **数据治理：数据政**

管理义务” “经监管部门责令改正而拒不改正的” “致使 信息泄露，造成严重后果的”。如此限定，似乎刑事风险

已相对可控。

[57]喻海松 . 网络 犯罪的立法扩张与司 法适用 . 法律适用， 2016(9):2-10。

而事实上，由于目前我国网络信息安全管理法律、法 规分散，在大量的法律、行政法规中均有涉及安全管理义 务的设定，相关监管部门，不仅包括中共中央网络安全和 信息化委员会办公室、公安部、工业和信息化部等日常监 管机构，在特定领域也涉及国安、保密等机构，此外传统 监管部门中国人民银行、国家市场监督管理总局、交通部、 中华人民共和国国家卫生健康委员会也有针对特定行业的 网络信息安全管理要求。尤其关注到“拒不履行信息网络 安全义务罪”中并没有限定监管部门的行政级别，这意味 着除了中央一级的监管部门，省级甚至省以下的监管部门 都可以发出“责令改正”要求157)。本罪的刑事风险显然

并不比想象中的小。

因此，对于企业来说，为有效防范此类情形的刑事责 任风险，应当全面梳理企业所负有的信息网络安全管理义 务，并与监管部门就安全管理工作保持密切沟通，特别是 在个人信息安全防护方面，杜绝因未履行信息安全管理要

求而造成的信息泄露事件。

**五、结语**

业界预测，2017年6月1日《解释》正式实施后，我

国侵犯公民个人信息罪刑事诉讼将出现激增现象。这是该

**139**

**第二篇** **世界各国数据保护做法**

罪名适用范围广、入刑门槛低所带来的结果。同时，由于《解

释》对重刑情形规定十分明确，实践中本罪量刑也将会出

现加重的特点。

除被规范的主体如企业、政府机构及普通个人需要加

强法律意识、遵守法律要求外，对于执法者而言，理解和

适用新规范也会面临新挑战。如上所述，我国个人信息保

护刑事体系是在民事、行政机制尚未及时跟上的背景下，

在刑事领域的先行探索，考虑到社会民众尚未形成对个人

信息保护规则的成熟认知，为避免刑事追责带来过大的冲

击，期待司法实践能够充分利用“初犯免于起诉、处罚”

等缓冲机制。

此外，法律适用中值得进一步思考的问题是，在利用

刑法严厉打击“个人信息黑产”的同时，如何避免对合理

创新活动的误伤。尽管《解释》部分考虑了主观恶意因素，

但并未将其作为定罪核心标准。建议在司法实践中能够加

大对主观恶意成分的考虑，从而区分出更具有社会危害性

的个人信息侵害行为，为市场创新留有空间。

**140**

**数据要素**

数据治理：数据政策发展与趋势



**第11章**

**《民法典人格权编》的影响与改变**

**摘要：** 《民法典人格权编》是我国民法的一大创新， 为隐私权、个人信息的定义、保护和具体实施做出了明确 的规定，填补了《网络安全法》的部分空白，为数据处理 的多场景应用及其正当利益的平衡提供了保障。这一法律 制度的建立对于保护个人权益和支持信息化技术的发展均

具有重大意义。

**一、引言**

《人格权编》独立成编是我国《民法典》的一大创新 和亮点。随着《民法典》的正式颁布，作为其重要的组成

部分的《人格权编》将对社会生活产生积极影响。

近期“杭州健康变色码”事件引发了争议与担忧，将 公民个体异化为数据测量评估对象并给予工具性评价，似 乎成为一场大型社会试验，但我们始终仍需心存对人格尊

严的敬畏，对该类实验的必要性、正当性多打几个问号。

此时《民法典》通过恰如其时，《人格权编》顺应时 代要求，对隐私和个人信息保护予以专章规定。作为基本

民事法律，它将带来哪些影响和改变?

**14I**

**第二篇** **世界各国数据保护做法**

二、把握“个人信息”特殊属性，合理处理与

“隐私权”的关系

长期以来，学界对“隐私权”和“个人信息保护”之

间的关系有许多争议。《人格权编》吸收了其中的基本共识。

关于“隐私”,《人格权编》吸收了“不愿为他人知晓”“私

密”等关键特征表述，对“隐私”的界定更为科学合理：

“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。”“个人信息中的私密信息，

适用有关隐私权的规定；没有规定的，适用有关个人信息

保护的规定。”这为实践中处理“隐私”和“个人信息”

的关系提供了更为明确的指引。

关于“个人信息保护”,学界主要有“权利说”和“利 益说”两种观点。但从法解释说来看，难以得出《民法总则》 第一百一十一条确立了自然人对个人信息享有民事权利即 个人信息权的结论158]。《人格权编》最终将第六章的标 题从“隐私权与个人信息权”调整为“隐私权与个人信息

保护”,显然也采纳了后者的意见。

“个人信息”与“隐私”确有差异。与“隐私”更 多地归属于私人领域不同， “个人信息”兼具保护和利用 两种属性，需要对个人利益和公共利益加以调和。因此在 近现代立法中，个人信息保护逐步从私权领域的隐私权中 分离出来，形成了相对独立的公法体系159),其立法目标 也旨在于实现个体利益与信息自由流动之间的平衡。欧盟 GDPR的开篇即表明：本条例制定关于处理个人数据中对

自然人进行保护的规则，以及个人数据自由流动的规则。

[58]程啸，民法典

编暴视野下的个人信

息保护. 中国法学，

2019年第04期。

[59]周汉华，个人

信息保护的法律定

位. 法商研究，2020

年第3期。

 **142** 数据治理：数据政

**三、个人信息定义回归“识别说”标准**

“个人信息定义”是个人信息保护法律制度的基石， 如果定义过于泛化，将导致法律难以施行。从2012年的 《全国人大常委会关于加强网络信息安全的决定》到2016 年的《网络安全法》,我国立法对个人信息的界定都坚持 了“识别说”,将个人信息限定为能够识别特定个人的信 息。但在针对个人信息违法行为刑事打击力度不断加强的 背景下，2017年最高人民法院和最高人民检察院发布的《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》对个人信息进行了扩展，除传统的“识别身份信息”外， 还增加了“反映特定个人活动情况的信息”。该定义后来 又影响到了2017年的《个人信息安全标准》,其对个人信

息做了进一步扩展解释。

各国个人数据保护法规对于个人数据的界定，基本上 采纳的是“识别说”。欧盟GDPR中进一步区分为“已识别”

和“可识别”两种类型，但核心仍然围绕“识别身份”。

即使相关信息由特定个人产生，但如果该特定个人的 身份无法识别，那么相关的信息处理并不会对特定自然人 的权益造成侵害或产生侵害的危险，也没有必要对其予以 规范。这与欧盟GDPR将“匿名化信息”排除在个人信息 之外，以及我国的《网络安全法》和《人格权编》将“无 法识别特定个人且不能复原的”排除在非法提供之外的基

本逻辑是自洽的。



**第二篇** **世界各国数据保护做法**

**143**

**四** **、民事立法亮点，** **《人格权编》的免责事由**

我国的《侵权责任法》180首次明确规定了隐私权， 但并不涉及个人信息保护。2014年的《最高人民法院关于 审理利用信息网络侵害人身权益民事纠纷案件适用法律若 干问题的规定》,对于公开个人信息不构成侵权的情形做

了如下规定。

(一)经自然人书面同意且在约定范围内公开。

(二)为促进社会公共利益且在必要范围内。

(三)学校、科研机构等基于公共利益为学术研究或 者统计的目的，经自然人书面同意，且公开的方式不足以

识别特定自然人。

(四)自然人自行在网络上公开的信息或者其他已合

法公开的个人信息。

(五)以合法渠道获取的个人信息。

(六)法律或者行政法规另有规定。

[60]中国《侵权责任

法》于2009年12月

通过，2010年7月1

日实施。2020年5月

28日《民法典》通过，

2021年1月1日起施

行，《侵权责任法》

同时废止。

同时，司法解释对以上免责事由又做了一个总体的除

外规定，即以违反公序良俗的方式公开上述第四项、第五

项的个人信息(自行公开、合法公开、合法获得),或者

公开该信息侵害权利人值得保护的重大利益，权利人寻求

侵权救济的，人民法院应予以支持。典型例子即当年盛行

的“人肉搜索”,尽管“人肉搜索”获取的许多信息是公

开可获得的信息，但其使用方式仍然构成了对特定自然人

**144**

数据治理：数据政

生活安宁的打扰，此种情形下将不再享有民事责任的豁免。

此次《人格权编》吸收了司法实践的经验总结，并结 合《网络安全法》的相关行政法规范，提出了个人信息处 理民事责任免责事由，包括：(1)用户同意； (2)维护 公共利益或本人利益的需要； (3)合法公开信息(但以自 然人明确拒绝或者处理该信息侵害其重大利益的除外)。

这些规定圆满地衔接了民事规范和行政法规范。

“免责事由”一方面恰当地保护了个人利益，另一 方面也兼顾了数字经济发展中对于个人数据的合理使用需 求。数据处理者在获取用户同意后，在与其约定的范围内 处理个人信息，将享有民事责任豁免。对于已经公开的个 人信息，在用户并不明确反对的情形下，数据处理者可以 用于合法正当目的，这将积极鼓励大数据、人工智能的开

发利用，释放以数据为核心生产资料的数字经济发展潜力。

五 、借鉴国际立法经验，延续个人信息

处理基本规则

《人格权编》继续保留了《网络安全法》以来我国关 于个人信息保护的法律原则：合理，正当，必要原则；公 示信息处理规则；个人可提出查阅、异议、删除等请求； 保证数据安全义务，匿名化对外提供的例外规定，数据泄 露通知等规定，并从民事角度再次强调了国家机关及其工 作人员对个人信息的保密义务，这意味着公权机构对个人

信息的侵害也可被纳入民事责任追究。

**145**

**第二篇** **世界各国数据保护做法**

同时，《人格权编》填补了《网络安全法》中关于数

据处理中除“同意”之外的其他合法性基础的空白，用“法

律、行政法规另有规定的除外”作为兜底，为数据处理的

多种可能场景以及与其他正当利益的平衡提供了空间。例

如，数据控制者为了履行法律职责的需要、为了保护数据

主体或另一个自然人的重要利益等。

六、填补“民事保护”板块，构建更加完善

的个人信息保护法律体系

相比欧美从二十世纪六七十年代开始个人信息保护立 法，我国针对个人信息保护的立法起步较晚，早期主要体 现在刑事立法领域。2009年的《刑法修正案(七)》首次 将窃取或以其他方式非法获取公民个人信息、出售或非法 提供公民个人信息且情节严重的行为定为犯罪，将其纳入 刑事打击范围。自此，尽管我国陆续在相关立法中加快了 个人信息保护制度建设，但总体上仍然保留了“刑事立法 先行，倚重刑事手段”的特征。通过刑法积极适用防止侵 犯公民个人信息违法犯罪持续蔓延，是不得已而为之的举 措，刑法只能治标，尚难治本161。再加上我国个人信息 保护刑事立法适用主体广、入刑门槛低、适用刑罚严厉的

特点突出，“刑法先行”的现象亟待克服。

《人格权编》作为民事基本法律，确认了自然人的隐 私权和个人信息保护，结合后续《个人信息保护法》专门 立法，将有助于我国构建起公民个人信息民事、行政、刑

事的全方位保护体系。

[61]喻海松.侵犯

公民个人信息罪的司

法适用态势与争议焦

点探析.法律适用，

2018第7期。

**146**数据治理：数据政

**七、全面的制度建设，仍留待《个人信息保护法》**

《人格权编》借鉴了欧盟 GDPR立法思路，将数据处 理环节的各类行为统一为广义的“处理”行为，包括收集、 使用、加工、传输、提供、公开等具体行为。但《人格权编》 并没有对数据处理者进行定义，这将导致个人信息保护所 指向的义务主体存在模糊性和争议点，留待后续《个人信

息保护法》予以明确。

在数字经济生态中，参与数据处理的机构复杂多样， 如云计算行业中的云服务提供者，提供专业化的数据存储、 传输、访问等计算资源服务；人工智能领域的数据标注服 务，为AI 机器学习提供数据的分类和标注等基础服务； 物联网领域更是包含了从芯片提供商、传感器供应商、无 线模组(含天线)厂商到网络运营商、平台服务商、智能 硬件厂商等种类繁多的服务提供者。在数字化时代，这些

服务样态或多或少地都涉及个人数据处理。

如何对这些形态各异的服务提供者予以法律定性和分 类，并设置相应的法律义务，是近年来个人信息保护立法 的重要议题。从欧盟的GDPR到美国的 CCPA, 大部分立

法采取了二分法。

以 GDPR 为例，将规制主体区分为数据控制者(D ata Controller) 和数据处理者 (Data Processor), 前 者(数据控制者)决定了数据处理的目的和方式，因此是 法律问责的主要对象，其需要保证数据处理的合法性基础，

并直接承担向个人提供查询、修正、删除的义务。因此，

**147**

**第二篇** **世界各国数据保护做法**

在GDPR第二章原则(可问责，获取个体同意)和第三章

数据主体的权利中，义务主体仅指向数据控制者，并不涉

及数据处理者；后者(数据处理者)是接受控制者的委托

而开展数据处理的，因此对于处理者的法律约束主要着眼

于委托关系的正当性，严格按照委托的边界处理数据，保

证数据安全等。

即使其他国家采用的具体表述不同，但实质上都

反映了主体的二分法，如新加坡《个人信息保护法》

中 的 组 织 (Organization ) 和 数 据 中 介(Data

Intermediary) 概念，印度《个人信息保护法(草

案)》中的数据信托者( Data Fiduciary) 和数据处理

者 (Data Processor) 概念，美国CCPA中的经营机构

(Organizatio n) 和仅提供数据服务的机构(Processo r)

都意在区分两种主体在法律适用上的差异性。

**八、结语**

隐私和个人信息保护仅仅是《人格权编》的一小部分，

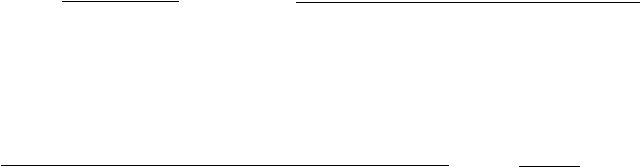
但它从人格利益的高度确认了基本法治原则，将推动形成

尊重人格利益的社会文化，防止类似“健康变色码”异化

的可能出现。但对于全面的个人信息保护制度构造来说，

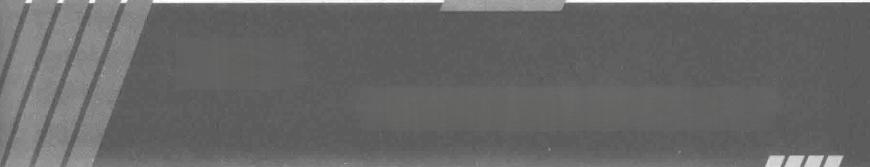
如何结合数字时代的新特点进行更为科学合理的设计，将

留给下一步的《个人信息保护法》。



*/H!!!!!!!!!!!!!!*

/ !!!!||!||!!



**第三篇**

**特殊领域的数据保护政策**

现代社会，新技术的发明和应用带来了技术的进步，

给人们的生活带来了极大的便利，例如面部识别技术在多

种生活场景中的应用，再如区块链由于其去中心化和可信

任机制被社会高度重视并践行。但是这些技术的应用对于

隐私及数据保护的法律与方案，特别是对儿童信息的保护，

是需要引起高度重视的问题。

**150**

**数据要素**

**数据治理：数据政策发展与趋势**



**第12** **章**

**面部识别技术隐私与数据保护政策趋势**

**摘要：**近年来，面部识别技术发展迅猛，在安防、管 理、金融、消费、社交、娱乐等多个领域得到应用。然而， 面部识别技术大规模、多领域的全面应用，带来的不仅是 安全有序的社会环境、高效便捷的服务体验，而且造成了

对隐私保护、数据安全的担忧。

面部识别技术已经产生了一些引人注目的诉讼案件。 2018年12月29日，“谷歌面部识别软件诉讼案”落下帷幕， 法院支持被告谷歌公司的抗辩，以原告不存在实际损害为

由驳回诉讼。在该案中，原告Weiss 是谷歌照片(Google

Photos) 的用户，但另一原告Rivera 不是谷歌公司的

用户，法院判定谷歌公司保存和收集面部模板的行为均未

造成损害，不满足美国宪法第三条(A rticle Ⅲ) 的起

诉原则 (The Standing Doctrine), 即原告没有证

据证明自己遭受了“事实上的伤害”。尽管在诉讼中谷歌 公司并未败诉，但为了避免面部识别技术可能带来的潜在 风险，谷歌公司宣布了包含结合隐私设计原则等在内的人 工智能原则，并提出在解决重要的技术和政策问题之前，

主动推迟提供通用的面部识别软件的API 功能。

**151**

**第三篇** **特殊领域的数据保护政策**

消费者知情同意问题是面部识别技术应用的另一争议

点。2018年4月6日，美国电子隐私信息中心 (EPIC)

等组织向美国联邦贸易委员会 (FTC) 申诉，指控

Facebook 的面部识别功能缺乏有效的隐私保护措施，违

反了FTC 2011年的同意令 (DOCKET NO. C-4365),

该同意令要求 Facebook 在发布超越用户隐私偏好的

更新之前，应获得用户肯定性的明确同意。申诉针对

Facebook 在2018年初生效的功能更新，即在未经人像

主体或上传照片的人同意的情况下，定期扫描用户发布的

照片进行面部匹配和标签。EPIC 强调，这种自动的、欺

骗性的、不必要的个人身份识别破坏了用户的隐私。目前，

此案尚在调查中。

除了消费者知情同意问题，面部识别的数据准确性也

引发了争议。2018年4月，英国《独立报》报道称，数据

显示英国大都会警察使用的面部识别系统在98%的案例中

会出现匹配错误。2018年7月，在美国公民自由联盟(ACLU)

的实验中，亚马逊公司的面部识别软件误判28名美国国会

议员为罪犯，遭到15万人联名抗议。2018年11月29日，

美国七名众议院民主党议员针对面部识别技术的准确性向

亚马逊公司提出问题，指出其给有色人种带来了过重负担，

并可能会扼杀美国人在公共场合行使《第一修正案》权利

的意愿。因为人们可能出于被面部识别的恐惧，而不愿积

极参加抗议活动或宗教活动。

同时，面部识别技术往往与庞大的个人数据库相联系，

因此其带来的更深刻的问题是“公共空间的匿名性悖论”。

**152**

**数据要素**

**数据治理：数据政策发展与趋势**

在公共活动中一张脸的单幅图像可以通过查阅数据库被快 速识别，而如果该数据库与其他数据库相连，那么可能链 接到无尽的个人信息。政府执法部门可以利用该技术持续、 实时、大规模监测民众的言行举止，商家可以利用该技术 记录甚至分享消费者的购物情况及喜好。在公共空间内， 公民原来匿名环境中的安宁与自由以及隐私的基本期待被

彻底颠覆。

暴露在外的面部就像一扇门，而面部识别技术则可能 是打开潘多拉魔盒的万能钥匙，未经主人同意就开门索取

门内个人相关信息的行为，显然存在道德伦理上的问题。

为此，2018年7月，微软公司总裁 Bradford L. Smith 公开发表题为《面部识别技术：公共管制和公司责 任的需要》的文章，建议美国国会展开研究并监督该技术 的使用，科技公司应主动承担道德责任，微软公司会通过 多种途径确保这项技术以人为中心的方式发展。12月6日， Smit h 再次发表文章《面部识别：是采取行动的时候了》, 总结了半年来的相关研究进展，提出该技术面临偏见和歧 视、侵犯隐私和民主自由的风险，分享了微软公司应对面 部识别技术应用问题的六项原则——公平、透明度、问责 制、不歧视、通知和同意、合法监督，并在12月17日发 表的微软报告中具体阐释了这六项原则。我们看到，在明 确的面部识别法律规范之前，科技公司和研究机构已主动

通过自律方式积极提出了建议方案。

**153**

**第三篇** **特殊领域的数据保护政策**



**第13章**

**区块链的隐私和政策保护趋势**

**摘要：** 与面部识别技术更依赖于科技伦理来引导相比，

区块链技术和应用与现有的个人信息保护方式之间仍有较

大落差。

尽管区块链技术将有利于提升人们对个人数据的控制

权，但区块链去中心化的数据处理模式却导致其与传统中

心化范式的 GDPR 难以兼容。

面对区块链应用带来的数据保护合规问题，法国数据

保护监管机构国家信息自由委员会 (CNIL) 在2018年9

月发布了关于区块链技术的 GDPR 指南，做出了首次官方

回应。

第一，对于如何界定区块链中的数据控制者和数据处

理者的问题，CNIL 认为在以下情况下，区块链的参与者

可以作为数据控制者：其一，参与者是自然人并且处理行

为与专业性或商业性活动有关；其二，参与者是在区块链

中登记个人数据的法人。而当一组实体决定对区块链进行

处理操作以达到共同目的时，应由参与者对数据控制者的

职责做出共同决定，即通过创建或指定一个合法人员作为

**154**

**数据要素**

**数据治理：数据政策发展与趋势**

数据控制者。否则，所有参与者将可能被视为联合控制者。

第二，对于如何在区块链上履行最小化原则，以尽可 能减少对数据主体的风险，CNIL 认为，首先应当在事前 仔细评估是否需要使用区块链。如果必须使用区块链，那 么应该优先考虑受许可管理的区块链。其次，在使用区块 链时要仔细选择数据的注册格式。再次，在处理目的合理 且当评估证明剩余风险可以接受时，可以使用没有密钥的 散列 (Hash) 函数存储数据，或者在没有密钥的情况下以

明文形式存储数据。

第三，对于如何确保有效行使GDPR规定的数据权利， CNIL认为，首先，信息权、访问权和可携权在区块链中是 可以实现的。其次，对于在区块链中难以实现的擦除权，可 以采取与风险最小化类似的方法，选择适当的加密方法来存 储数据，从而更接近于实现权利的目的。再次，擦除存储在 区块链之外的数据和能够验证的元素，消除允许访问区块链

上记录的证据，使数据获取变得困难甚至无法检索。

第四，对于区块链的安全性问题， CNIL 认为对于许 可区块链，可以根据参与者利益的潜在分歧或趋同，对最 小数量的矿工进行评估，以确保控制链上不存在超过50% 权力的联盟；应制定技术和组织程序以限制潜在算法失败 对交易安全性的影响；还应记录用于创建交易和开发软件 变更的操作，并制定技术和组织程序，以确保计划权限与 实际应用之间的一致性。如果区块链不是公开的，那么应

特别注意为确保区块链的机密性而采取的措施。

**155**

**第三篇** **特殊领域的数据保护政策**

尽管 CNIL最近发布的指南确实提供了一些允许区块

链在 GDPR下存在的解决方案，但它却为这些解决方案在

实践中如何运作提出了更多问题。

例如，业内专家指出：将一些区块链用户归类为数据

控制者在概念上是有道理的，因为它符合GDPR的原则，

但在实践中这可能很难落实。再者，CNIL 的指导可能适

用于私有区块链服务，但却不适用于公共区块链。私有区

块链服务的所有用户可以同意单一行为准则，而公共区块

链却难以形成行为准则。同时，从技术角度来看， CNIL

指南中的一些建议可能并不完全可行。虽然从本质上讲，

若删除用户访问区块链的私钥，则意味着在私有区块链上

进行了擦除，但是销毁私钥是否等同于擦除在实践中仍是

一个悬而未决的问题。

在区块链的使用应符合GDPR规则的问题上，除 CNIL

的指导外，民间的咨询机构也给出了相关意见。其中比较

有代表性的是咨询机构 Tech GDPR强调的区块链隐私保

护需要遵循“设计隐私”理念。其阐述了这一概念所包含

的七个重要原则，这些原则已被GDPR所确立，因而其已

经成为必选项而不是任选项。这些原则包括：

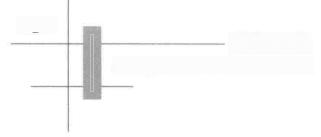
(1)采取事前、预防措施；

(2)将隐私作为默认设置；

(3)将隐私融入设计；

(4)隐私保护和功能性兼顾；

(5)通过端到端的防护实现数据全生命周期的保护；

**156**

**数据要素**

数据治理：数据政策发展与趋势

(6)实践可见性与透明度，保持开放；

(7)尊重用户隐私，以用户为中心。

总体来看，无论是面部识别技术，还是区块链技术， 都体现了现有数据法规难以适用的落差。解决的思路可以 从两端出发： 一是科技行业主动自律，正如谷歌公司、微 软公司积极提出面部识别技术及其他AI 技术的使用原则， 以“科技向善”的理念进行自我约束，明确技术不能突破 的底线；二是立法与监管也需要不断创新，以创造性地提 出解决方案。从区块链数据保护规范来看，如果仅从传统 规制思路出发，那么仅能覆盖一部分区块链应用，而不能

解决全部问题，这将带来规制的市场扭曲现象。

157

**第三篇** **特殊领域的数据保护政策**



**第14章**

**儿童个人信息保护**

——**美好的权利如何脚踏实地**

**摘要：**儿童个人信息保护的关键难点在于，如何识别

儿童、监护关系和监护人的知情同意。如果要求所有的网

络场景，都严格贯彻监护人知情同意原则，则意味着社会

整体要为此付出相应的法律执行成本。

**一** **、引言：儿童个人信息保护，难点在哪里?**

尊重和保障儿童权利是被世界广泛认可的基本通识， 各国个人信息保护法律中也逐步引入了儿童个人信息保 护，并且基于传统的知情同意原则，在涉及儿童个人信息 的场景，考虑到儿童心智不成熟，其很难对个人信息被收 集利用的后果和风险做出理性判断，因此建立了需要征得

其父母(监护人)[1 同意的法律机制。

尽管从儿童权利视角，包括联合国《儿童权利公约》21 在内的官方和民间研究都已开始关注并探讨：儿童对其享 有的隐私、个人信息相关权益处分的独立性，以及基于儿 童动态发展的考虑，是否应当“充分理解、尊重不同类型

儿童在不同阶段的特点与能力”[3],从而质疑法律一刀切

[1]为行文简洁，本

文统一表述为“监护

人”。

[2]1989年《联合国

儿童权利公约》,

https://www.

un.org/chinese/

children/issue/

crc.shtml。

[3]作者陆诗雨。节

选自2019年8月14

日腾讯研究院微信公

众号文章《浅论儿童

数字权利》。

**158**

**数据要素**

**数据治理：数据政策发展与趋势**

的按照儿童年龄划分的信息处分权利差异化的合理性，但 在更为合理的法律机制形成之前，我们仍主要依赖监护人

同意机制来实现儿童的个人信息保护。

正如个人信息保护是个人权利、信息自由流动、公共 利益等诸多正当利益之间的平衡取舍一样，儿童个人信息 保护由于涉及权利主体与权利行使主体相分离的情况，其

在制度落地中注定遇到更多实践问题。

即使是在线下环境中，鉴别儿童及其监护人也需要配 套支持，包括身份证、户口本等资料加以印证。同时，因 为具有面对面接触的条件，这种以识别用户年龄为前提的、 法律上的监护人同意要求，理论上仍可以推行，尽管这意 味着巨大的社会成本付出。例如，我国已推行多年的电话 实名制，虽然在大部分场景下具有在营业厅现场识别的便

利条件，但在推进中仍需克服许多实践难题。

进一步延伸到网络世界时，由于物理位置的隔绝，实 施监护人同意机制更需要相关的技术手段、数据资源予以 协同配合。如果不加区分地要求所有的网络在线服务实施 监护人同意机制，那么将难以避免数据过量收集的问题， 也显著增加了不合理的社会成本。况且，许多线上服务对 于此类数据的收集处理本身就没有必要。例如，对于网络 搜索服务，运营者没有必要去收集、鉴别用户的年龄甚至 监护人的相关信息，并获取监护人同意。用户在使用搜索 服务时，不用说进行年龄验证，即使是账户注册都难以接

受。因此，儿童个人信息保护(特别是网络保护)初心虽好，

**159**

**第三篇** **特殊领域的数据保护政策**

但要将这美好的制度付诸实践，则无法回避一个核心矛盾，即如何实现合理

有效的儿童保护，同时防止过度的和不必要的信息收集。

**二、儿童个人信息保护，从哪里借鉴经验?**

解决问题不是为了产生更多问题。有关儿童个人信息保护的讨论，更多 的并不是纯粹的法律议题，而是符合实践场景的制度探索，经验积累更凸显

其价值。

遗憾的是，到目前为止，作为数据保护引领者的欧盟在这一领域的经 验乏善可陈。美国于1998年制定《儿童在线隐私保护法》(Children’s

Online Privacy Protection,COPPA),同时代欧盟1995年的《数据 保护指令》并未写入儿童个人信息保护，近20年之后，2016年出台的 GDPR 中才明确引入儿童个人数据保护，但也仅有一条主要围绕儿童数据保护的原

则性条款(第8条)14)。

按照欧盟数据保护委员会(Europ ean Data Protection Board, EDPB) 的惯常做法，为了澄清 GDPR中的原则性条款， EDPB会出台更为详 细的“指南”来指导法规落地，截至目前， EDPB已出台了10余个指南来回 应具体的执行问题，包括数据保护官、数据保护影响评估、识别主导监管机

构等，但迟迟未就儿童个人信息保护规定出台更具体的指南。

GDPR将儿童的年龄设定交给了各成员国，可以在13～16周岁之间进行

设定，这就造成了较大差异(比如葡萄牙设定为13岁，西班牙设定为14岁，

[4]EU General Data Protection Regulation,Article 8 Conditions applicable to child's consent in relation to information society services

territorial scope.

**I60**

**数据要素**

数据治理：数据政策发展与趋势

法国设定为15岁，德国设定为16岁)151,更何况儿童个人信息保护在实践

中的确还存在着许多悬而未决的争议。

当然，欧盟立法者在制定 GDPR 时就已注意到，网络世界中数据处理活 动的多样性会对儿童监护人同意原则的实际落地带来极大的复杂性，因此其 在有关儿童个人数据保护的核心条款——第8条中也采取了相当弹性的表述， 为未来的实施预留了制度空间。第8条第3款规定：“数据控制者应当采取 合理努力，结合技术可行性，确保此类情形中对儿童具有父母监护责任的主 体已经授权或同意。”但什么是“合理努力”,什么是“技术可行”,一时

难以给出权威答案。

相反，隐私保护执法一直以务实为显著特征的美国，在全球范围内最早 形成了专门的儿童在线个人信息保护法律——COPPA, 在儿童个人信息保护 领域已积累了20多年的制度建设与执法经验，除了专门立法，作为执法机构 的联邦贸易委员会 (Federal Trade Commission, FTC) 还出台了细则 (COPPA rules)16i、问答清单(COPPA FAQs)(71、六步骤合规计划(A Six-step Compliance Plan for Your Business)[8I 以及推进行业 实际落地的安全港计划 (COPPA Safe Harbor Program)(9), 来指导并 践行儿童信息保护，这对于包括中国、欧盟等在内的、正在探索儿童个人信

息保护具体机制的国家和地区都具有重要的参考价值。

[5]Ingrida Milkaite and Eva Lievens,The GDPR child's age of consentfor data processing across the EU -one year later(July 2019), 由于目前各成

员国仍处于推进GDPR的实施进程中，对于儿童同意的年龄标准仍在动态变化中。 [6]COPPA rules 制定于2000年，并于2013年修订更新。 <https://www.ftc.gov/>

enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-

online-privacy-protection-rule。

[7]<http://www.business.ftc.gov/documents/0493-Complying-with-COPPA>-

Frequently-Asked-Questions.

[8]<https://www.ftc.gov/tips-advice/business-center/guidance/childrens>-

online-privacy-protection-rule-six-step-compliance。

[9]<https://www.ftc.gov/safe-harbor-program>。

**16I**

**第三篇** **特殊领域的数据保护政策**

**三、儿童个人信息保护的核心制度设计**

儿童作为特殊群体，其个人信息要受到严格保护，其

合理性和必要性毋庸置疑。但如上所述，依赖于“监护人

知情同意”的保护机制在实践中将遭遇巨大挑战，包括如

何识别儿童、监护关系和监护人的有效同意。

因此，纵观美国隐私执法机构联邦贸易委员会(FTC)

关于儿童个人信息保护的执行落地及其发布的详细规则，

都始终围绕着“合理必要”这一核心原则，即如何在真正

的社会生活实践中，通过法律制度的设计和具体规范来实

现儿童个人信息的保护目标，同时避免产生过量的负面问

题。为实现这一目标，这些细则围绕以下核心问题展开：

哪些情形需要适用COPPA? 如何认定网络服务运营者对用

户的年龄有“实际认知”?如何取得监护人的同意，包括

监护人识别、有效同意的验证?

**(一)哪些情形适用?**

首先需明确的是， COPPA 并不适用于所有的在线服务。

它规定的“监护人同意”等要求仅指向以下三类情形。

( 1 ) 直 接 面 向 1 3 岁 以 下 儿 童( Directed to

Children Under 13)收集儿童个人信息的网站、在线

服务的运营者(即服务对象专门针对儿童)。

( 2 ) 适 用 于 那 些 虽 面 向 一 般 受 众 (General

Audienc e), 但对收集13岁以下儿童个人信息有实际认

知(Actual Knowledge) 的网站和在线服务运营者。

**162**

数据治理：数据政

(3)面向第(1)类运营者提供广告网络或插件等服务，从而也明知收

集儿童个人信息的第三方服务提供者110)。

FTC 不要求面向一般受众的网站或服务提供者对其用户的年龄进行调 查(11)。因为，如果不对适用范围加以限制，那么会导致大量面向大众服务的 网络运营者在本不需要去收集用户年龄、监护人信息、监护人同意的情况下， 超出业务的需要范围开展此类数据处理活动，增加实际执行难度，也无益于 数据保护，会滋生新的数据安全问题。正如对COPPA的批评意见：验证措施 对隐私带来了更大风险，运营者因此而收集、处理着大量的儿童及其监护人 的敏感信息。因此 FTC也着眼于实际，通过谨慎设计适用范围，避免滋生此

类问题。

**(二)如何判断运营者对用户的年龄有“实际认知”?**

网络服务直接面向儿童(以儿童为目标群体)有着较为客观的参考标准， 例如是否具有以儿童用户为导向的内容、服务等(如儿童动画网站、儿童电 话手表)。相比较，对于面向一般受众的在线服务，其对用户的年龄有“实

际认知”这一适用标准仍有进一步澄清的空间

对此， FTC表示：如果运营者要求并接收用户的个人信息，使其能够判 断用户的年龄，那么运营者即对此有实际认知。例如，运营者在其网站注册 页面要求用户提供其年龄，用户反馈的结果是小于13周岁的，该运营者即具 有 CoPPA定义的实际认知。又如，运营者接到了监护人的明确投诉，也可以

证明运营者对特定用户有实际认知。2019年2月，在 FTC针对抖音国际版

[10]这里需进一步澄清的是，尽管COPPA明确了商业性网站是其规制的对象，但依据联邦法律要求， COPPA同样也适用美国政府部门收集处理儿童个人信息的活动。

[11]<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/> children's-privacy

**I63**

**第三篇** **特殊领域的数据保护政策**

(TikTok,<http://Musical.ly>) 依据COPPA做出的最大一笔罚金案件中， FTC 的主要证据之一是该应用收到了大量来自父母的投诉，表明对其特定的

儿童用户有明确认知[12]。

那么,如果用户在年龄问题上说谎，以便注册一般受众网站或参与运营 者禁止儿童参与的网络服务时，该如何判断运营者的责任?对此，FTC 再次 强调了COPPA并不要求一般受众网站询问访问者的年龄。如果此类运营者选 择以中性方式(比如客观问询用户的出生日期)筛选其用户的年龄，判断是 否属于儿童，那么就取决于用户输入的出生信息，即使用户提供的年龄信息 是不准确的。因此，在一些情况下，这可能意味着儿童能够在违反运营者服 务条款的情况下注册网站或服务，此时运营者并不承担相应责任。除非有其

他证据表明，运营者能够确定用户是13岁以下的儿童。

因此，在实践中，对于一般受众网站，大部分会在隐私政策中明确要求： 如果没有监护人的同意，未成年人不得创建个人账户。用户是未成年人的， 应当请监护人仔细阅读隐私政策，并在征得监护人同意的前提下使用服务。 这在FTC执法实践中被予以认可，也是全球互联网企业普遍采用的做法。例如， Google 、Facebook 、Twitter 的隐私政策和用户协议都包含有此类条款。

**(三)哪些情形有例外?**

FTC 在细则中详尽罗列了不需要获得可识别的监护人同意的例外情形。 例如，为了取得监护人的同意，运营者可能需要收集儿童及其监护人的姓名， 以及监护人的网上联系方式，通过该联系方式向监护人告知其收集儿童个人 信息的目的、方式，以征求其同意。对于这种合理的数据收集， FTC认为运

营者有其合法基础，前提是如果监护人在合理期间内没有做出同意的回复，

[12]<https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically>- inc。

**164**

**数据治理：数据政**

运营者应当及时删除儿童及其监护人的个人数据。

类似的合理例外还有很多。例如，出于保护儿童安全 的目的，出于响应儿童需求的目的(前提是符合一次联系 原则，后续不再主动联系儿童),出于在线服务提供者内 部运营管理的需要对儿童网络识别信息(如IP 地址)的

处理等，都可以豁免监护人同意要求。

同时，为了保证儿童参与网络活动的权利，COPPA还

对“父母同意”原则设计了一些例外：

·即使没有父母同意，也允许儿童通过电子邮件提问。

·当儿童从网上获得时事信息时，可以没有父母的同

意，只要父母被通知并有权取消这些信息。

·当儿童从事联邦贸易委员会认为必要的活动时。

这一制度经验在欧盟的 GDPR中也有所借鉴， GDPR的 背景引言(Recital 38) 也做了类似的排除：在直接向儿

童提供预防或咨询服务时，不必取得儿童监护人的同意。

**(四)在适用** **COPPA 后，应履行哪些合规义务?**

首先，应发布符合COPPA规定的隐私政策。隐私政 策必须清晰且全面描述13岁以下儿童的信息是如何被收集 及处理的。对于直接面向儿童的网络服务，应当在其网站 首页链接隐私政策，如果网站或服务面向的是一般公众， 但是有一个单独部分面向儿童，则应当在该网页的首页链

接隐私政策。

**165**

**第三篇** **特殊领域的数据保护政策**

其次，应告知监护人并获得同意。COPPA要求在收集

儿童信息时应当告知监护人，并获得监护人可识别的同意。

关于什么才是可识别的父母同意，COPPA没有对此进行限

定，仅要求运营者采取合理努力，并结合能够利用的技术

手段，能够合理地推断做出同意的是孩子的父母。这种立

法表述显然也被 GDPR 所参考和效仿。

最后，应保证监护人的其他持续性权利。在获取监护

人的同意并收集处理儿童个人信息后，运营者应当保证监

护人能够继续行使其合法权利，包括访问、删除儿童个人

信息的权利。同时也应当采取合理措施来保证信息安全，

特别是出于安全考虑，如果运营者已删除了相关个人信息，

导致不能支持监护人行使访问权，这本身并不违法。

四 、儿童个人信息保护，仍有许多细节性的

实务问题

关于儿童个人信息的保护不止于法律层面的讨论，

相反，充斥这一议题更多的是实务话题。这也是 FTC 就

COPPA的合规落地发布了大量指南的主要原因，包括面向

运营者的合规指南(其中还包括专门针对中小企业的合规指

南),以及家长、学校的权利指南。另外，FTC还发布了

详尽的问答清单(Q6A), 通过问答清单来回应实践困惑。

由于篇幅所限，我们仅截取问答清单中的典型问题来说明儿

童个人信息保护在实践落地时需要直面及回应的多样疑问。

Q1: 如果孩子们在我的一般受众网站上的注册过程中

**I66**数据治理：数据政

撒谎，我会负责吗?

A:COPPA 并不要求一般受众网站对注册用户进行甄

别，但是一旦知道用户是儿童，就会受到规制。

Q2: 我是否可以阻止13岁以下儿童使用我的一般受

众网站?

A: 可以。如果你选择在一般受众网站或服务中阻止 13岁以下的儿童，你应该设计你的页面，页面设计的方式

不鼓励孩子伪造他们的年龄来访问你的网站或服务。

Q3: 如果我运营一般受众网站，用户可以建立自己的 博客页面和在线论坛，如果儿童用户发布了个人信息，但

是此前并无可显示其年龄的信息，我是否违反了CoPPA?

A: 这种情况COPPA 并不规制。但是，如果你收到了 其他用户的举报，或通过其他方式了解到该用户为儿童，

那么就应启动COPPA 的合规程序。

Q4: 使用信用卡或者政府签发的身份验证信息作为父 母同意的方式，我是否还需要收集其他信息以验证做出同

意的是父母?

A: 不需要。这两种方式足够证明运营者履行了

COPPA义务。

Q5: 我是针对儿童的应用程序的开发者，我是否可以

通过第三方，例如应用商店，来代表我获得父母同意呢?

A: 可以。只要你能确保其符合 COPPA的要求。

**167**

**第三篇** **特殊领域的数据保护政策**

Q6: 如果我的儿童网站上有个“咨询作者”部分，儿

童可以发送电子邮件咨询问题，那么我是否需要提供通知

并征得父母的同意?

A: 如果你只是回答儿童的问题，然后删除儿童的邮

件地址，那么你就符合“一次联系”的例外情形，并不需

要获得父母同意。

Q7: 教育机构可否向网站或者应用收集和披露儿童数

据做出同意?

A: 可以。很多学校与第三方网站运营者签订合同，

为儿童利益提供在线服务。运营者必须向学校做出告知，

并取得学校的同意。

Q8:COPPA 是否禁止成人，例如父母、祖父母、教师

或者教练上传包括儿童照片在内的个人信息?

A:COPP A仅仅适用于从儿童处收集的信息，它不适

用于从成人处收集的含有儿童个人信息的情形。

Q9: 我运营了一个面向儿童的 App 。儿童用户可以上

传照片，并采取各种方式装饰照片，但是 App 不会将包括

照片在内的任何信息从儿童的设备传输到其他地方。这种

情形属于COPPA 界定的信息收集吗?

A: 不属于。因为你的App 所交互的信息存储在用户

的终端上，从未传输，因此这种情况性不属于“收集”个

人信息。

上述问答清单对于指导企业实现合规，推动儿童个人

**I68**

数据治理：数据政

信息保护的实际落地发挥了积极作用。此外，FTC还通过市场化的手段推进 发展 COPPA安全港项目。通过FTC安全港认可的行业组织，可以保证组织 内部的成员符合COPPA的要求，这使得儿童的个人信息保护能够通过行业 自律方式得到广泛实施|13。截至目前， FTC 批准的机构有七家，这些机构 也可以作为第三方向市场上的在线服务企业提供儿童个人信息保护咨询和解

决方案。

**五、结语：儿童个人信息保护，仍应在生活场景中探寻方案**

尊重和保障儿童权利是保护儿童个人信息的本源。映射在当下的数字生 活中，它不应当仅仅是权利宣誓的乌托邦，而应真正走入生活，走入家庭， 走近儿童。它要求我们的制度设计回归实践，实事求是，通过设计真正有效 合理的制度规范来帮助监护人在儿童信息的收集处理中发挥控制力；同时， 这种制度规范的实施成本又不至于太过高昂，与社会生活脱节而沦为束之高

阁的无用条框，甚至带来更多的负面问题。

本文所展示的美国立法与监管机构在这一领域的制度经验，正是在权利 与实践两个维度的务实探索，尽管并不完美，但其探索模式是值得借鉴的， 即应回归到社会生活的场景，特别是当下的数字生活场景，合理分配各方的 义务，实现“社会—平台—家庭—学校—儿童自身”多方一体的保护体系，

并使其真正有效地运转。

儿童个人信息保护是儿童网络保护的组成部分，与最大限度地保护儿童 免受包括网络有害内容、网络沉迷、网络欺凌等负面影响一样，需要在实践

中探寻多种解决方案，且彼此的保护体系应相互衔接。比如，在有害内容预

[13]包括Aristotle International Inc;Children's Advertising Review Unit (CARU);Entertainment Software Rating Board(ESRB),IKeepSafe;

kidSAFE;Privacy Vaults Online,Inc.(d/b/a PRIVO),TRUSTe。



**第三篇** **特殊领域的数据保护政策**

**169**

防方面，从内容过滤软件到应用、设备服务商提供的儿童

模式，都可以成为儿童个人信息保护的有效落地方式；现

有的预防“网络沉迷”制度，包括网络“使用时长”控制，

也远比儿童个人信息保护制度的监护人同意规则干预程度

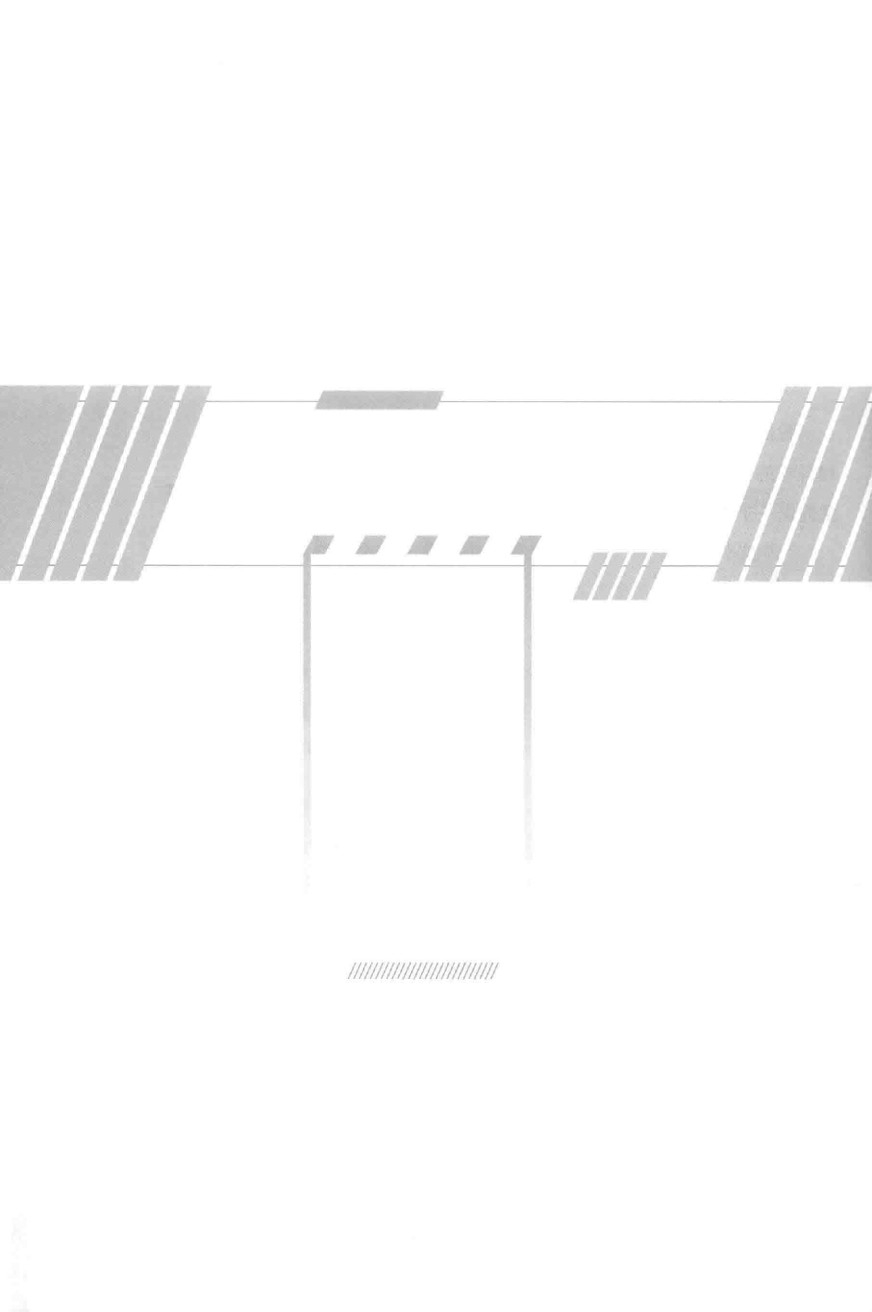
深入，平台向监护人提供的监护便利也更加全面，这些都

应当成为儿童个人信息保护中需要考虑的现实基础。

我们期待，各方共同参与探讨，终究会形成更加务实

和科学的优化方案，实现儿童网络权利保护的初心，为儿

童提供一个更加安全、可靠、健康的数字成长环境。



/



**第四篇**

**数据共享与数据流动**

数据共享最大的风险莫过于数据泄露和数据滥用。美

国和欧盟的政策探索从两端入手，最终仍是在回答同 一 个

核心问题：在促进数据共享、释放数据潜能的同时，如何

最大化地减轻数据泄露和滥用带来的负面作用?美国和欧

盟的探索是可以借鉴的。欧盟提出的明确数据权属、完善

数据共享协议、增强数据共享的安全能力保障，以及美国

以市场生态的视角来看待数据安全问题，即如何为数据安

全提供更持久的市场动机，或许都有启发作用。

**172**

**数据要素**

数据治理：数据政策发展与趋势

**第15章**

**Facebook** **数据事件的深度拷问**

**摘要：** 一向以市场自律主导，主张灵活监管的美国因 “Facebook 丑闻”事件，这两年来几乎都在反思数据泄露 与数据滥用问题，监管机构、产业界、消费者团体、学界

对问题的共同探讨日益深入。

2018年3月，美国《纽约时报》和英国《观察家 报》共同发布了深度报道，曝光曾服务于特朗普竞选团 队的数据分析公司(C ambridge Analytica) 获得了 Facebook 数千万用户的数据，并进行了违规滥用，干预 了包括美国大选在内的多国政治活动，将2016年年末已开

始发酵的“通俄门”事件变成为全球瞩目的焦点事件。

随后，美国国会参众两院各委员会分别或者联合启 动了数十场听证会，深度拷问平台数据治理能力，卷入了

Facebook 、Twitter 、Google 等众多科技公司。

听证会是美国开展事件调查、立法政策讨论最主要和 最正式的方式。过去一段时间以来的听证会，不论是质询 者还是回应者，都在不断加深对相关问题的认识。与其说

是听证会，不如看成是美国目前涉及范围最广、规格最高

**173**

**第四篇** **数据共享与数据流动**

的大型系列政策研讨会，研讨会上的各类观点一定程度上

决定了美国未来的数据监管政策。

我们可以将研讨议题大致分为两类。

议题一 内容监管中的平台责任：涉及选举政治问

题的，监管政策已趋明朗，但泛泛的平台责任议题仍在讨

论中。

在美国，对平台内容进行监管是极其复杂的。美国宪

法第一修正案规定的言论自由原则适用于平台，平台需要

被平等地保障言论自由权，这也是美国国会长期以来一直

没有为平台赋予更多内容管理责任的主要原因。

但是随着时代的发展，要求平台对其上的内容承担责

任的理由也渐渐出现，平台媒体通过信息传播这一重要渠

道获得了社会影响力，这一地位的转变使得平台也要承担

起防止这一力量被滥用进而危害社会的责任。

首先，关于平台被恶意利用、干预选举等政治问题，

平台正积极承担责任，并支持在这一领域建立明确的立法。

实际上，利用网络进行政治宣传在美国早已有之，多年前

奥巴马竞选团队在网络选战中的出色表现就为人所称道，

而特朗普当选超乎预期，并与“通俄门”话题关联，使得

平台在选举中被恶意利用的问题变得紧迫，硅谷科技公司

也意识到了网络上虚假账户、虚假新闻对民主政治的极大

危害，积极支持国会制定《诚实广告法》,加强网络政治

广告的透明性。

**174**

**数据治理：数据政**

而在干预选举问题之外，对于网络上的仇恨言论、儿 童色情等不良内容，尽管立法者也开始讨论对1996 年《通 信内容端正法》(Communications Decency Act) 第230条“避风港”(互联网服务提供者不为第三方内容 承担责任)进行适当的修改，但这种泛泛的平台内容责任 政策还需深入讨论。 一概而论地评价美国加强平台对内容 的监管责任并不准确，相反，出于“言论自由”等美国基 本价值原则，包括 Facebook、Twitter 等大互联网公司 的内容管理措施仍然是十分谨慎的。许多立法者，特别是 原则上反对商业监管的一些人士，希望科技行业证明其能

够自我调节。

议题二 隐私保护和数据安全政策(本文重点关注的

议题):联邦重启隐私立法议题，并得到了科技行业支持。

美国在隐私与数据保护方面的立法长期保持着“碎片 化”特征，即各行业、各领域，以及各州分别针对特定场 景下的消费者隐私保护各自出台法案。这种分散式立法虽

然具有更强的灵活性，但也因过于松散而饱受诟病。

而2018年一系列的听证会表明，关于联邦层面的统一 隐私保护立法再一次成为讨论的焦点。这一次，美国两党、 民众以及主要科技公司似乎已达成了共识：现在的问题不 再是是否需要制定联邦层面的隐私保护法，而是应该制定

一部什么样的联邦隐私保护法。

尽管目前联邦层面的隐私保护立法呼声极高，但因为

美国各州差异巨大，能在联邦层面达成共识的隐私立法不

**175**

**第四篇** **数据共享与数据流动**

会细致翔实，具体的执法细则应根据各州的具体情况进行

规定，制度规范也不会像 GDPR那般严苛。因为即使是最

为激进的CCPA, 相比GDPR也已缓和很多，更加注重消

费者保护的实际效果和促进企业发展、技术创新之间的平

衡。这最显著地体现为以下两点。

第一，受影响的实体范围。在欧盟的 GDPR 下，任何

规模的实体都受GDPR的约束，而 CCPA仅涵盖年收入超

过2500万美元的企业，以及销售大量个人信息的数据经纪

人。

第二，CCPA仍然保持了美欧个人数据保护法的最大

差异。具体而言，在GDPR下，公司收集、处理消费者个

人数据之前必须要获得消费者的同意，即opt-in 模式；

而在CCPA中，对于16岁以上的消费者的个人信息处理，

采取美国一以贯之的 opt-out 模式，即除非用户拒绝或

退出，公司可以继续处理用户的个人信息。

2018年10月10日，在以“消费者数据隐私：审视

欧盟 GDPR 和 CCPA” 为主题的听证会上，欧洲数据保护

委员会主席Andrea Jelinek 和美国CCPA主要发起人

Alastair Mactaggart 应邀展开政策讨论。后者表示：

人们将CCPA 与欧盟的GDPR 进行了比较。虽然存在概念

上的相似之处，但CCPA却有很大的不同。 一个重要的区

别是，CCPA要求用户同意才能进行数据处理。我们担心

此条款可能会伤害新进入市场的企业，因为消费者可能不

太同意新参与者收集和销售他们的信息。那么,下一个

Google 或 Facebo ok 如何成长起来呢?

**I76**

数据治理；数据政

2018年12月11日，在美国众议院司法委员会发起

的听证会上，美国最主要的数据监管机构联邦贸易委员会

(FTC) 主席Joseph J.Simons 陈述道：我们在考虑

联邦的统一隐私立法时，必须看到它可能带来的负面结 果 扩展现有平台的市场份额，他们有更多资源投入合 规，从而形成新的竞争优势。欧盟率先推出GDPR, 使得 美国有机会把它视为一次制度试验，看它是否减损了竞争、

带来什么坏处，我们可以在制度设计中找到办法来避免它。

除了美国国会层面发起的隐私立法讨论，担负隐私监 管使命的ETC也陆续发起系列听证会，深度讨论数据政策。 主题涵盖隐私监管(消费者数据的监管),隐私、大数据

和竞争，算法、人工智能和预测分析，数据安全等。

FTC 听证会的重要特征是，参与者的立场及专业背景 的多元化。广泛邀请了监管机构、企业、消费者团体以及 研究机构，参与讨论者的专业既有社会科学背景者，包括 经济学、法学、心理行为学等，又有技术工程专家，包括 计算机科学家、工程师等。这样多元的主体参与，为数据 问题的探讨提供了丰富的多样性，使得会议有机会透视问

题的真实样貌。

1. 经济学家的讨论视角

·数据规制对于数字经济的短期、长期影响。包括以

GDPR为具体案例来讨论其长、短期影响。

·消费者福利的增长与损耗。以在线行为广告为例，

其向消费者反哺了海量的免费内容和免费服务，也

**177**

**第四篇** **数据共享与数据流动**

一定程度上增加了服务供给端的竞争程度。

·数据是如何存储、流动和进化的?技术如何塑造了

数据以及数据的使用?

·比较两种数据使用机制对社会福利的影响。以借贷

市场为例，说明在 opt-in 和 opt-out 两种模式

下的结果：在 opt-out 模式下，有更多的数据被

收集，借贷市场会更加有效地进行匹配，最终借贷

产品的价格更低。

2. 竞争法专家的探讨

·在特定的数据竞争案例中，数据是最终产品还是竞

争的投入要素?

·数据是竞争的武器，还是竞争的目标?

·根据数据的竞争属性，数据是唯一的、广泛获取的

还是易于复制的?

3. 心理行为学探讨

在市场运行中，消费者的隐私偏好作用重要。在市场

调查问卷中，消费者总是反映出更强的隐私保护立场；然

而在具体的市场行为中，消费者的隐私偏好却始终在变化。

短期内，用户更关注分享披露信息、即时获得的效率提升、

便利以及社交满足感，而对长期风险意识不足——披露信

息可能导致丧失安宁、身份信息被窃等安全隐患增加。因此，

消费者教育在数据治理方面也将扮演重要角色。

**178**

数据治理：数据政

这些多元化视角聚焦于一个特定问题时，也会有更多 的碰撞，例如在“数据安全”议题听证会上，讨论围绕以

下问题而展开：

·投资于数据安全的动机是什么?它们是否足够?

·消费者对数据安全的需求是什么?

·消费者需求是否能够有意义地推动数据安全投资?

·我们应该期望消费者参与保护他们自己的信息吗?

·如何才能最好地评估特定公司的数据安全能力，以 及如何将评估传达给有关的利益相关者、高管、董 事会、网络保险公司、信用卡发行机构、消费者和

监管机构?

·针对数据安全，哪些监管和执法方法有效?它们为

什么有效?它们可以改进吗?

这些问题显示了美国在考虑数据政策设计时，始终突 出市场生态视角，希望通过政策设计实现更加完整、有效 的市场自我运行机制，以最大化地实现政策目标。比如在 数据安全问题上，除了法律上要求的合规内容，投资数据 安全的持久动机应当是保护与消费者之间的信任关系，维

护企业商誉，这是市场有序竞争发展的根本。

在听证会，专家们也对美国最早提出的“数据泄露通 知制度”进行了反思。当前由于数据泄露的规模不断扩大

及欺诈手段的不断演化升级，数据泄露通知制度对于预防



**第四篇** **数据共享与数据流动**

减少欺诈的作用正受到更多质疑。而与此同时，数据泄露

刺激了网络与数据安全保险市场的发展，为解决数据安全

问题提供了新的路径。

可见，在数据保护领域，美国仍将与欧盟保持不同风

格的法律特征。通过听证会这一对话平台，美国产业界、

立法者、消费者团体对相关问题展开了深入讨论，以便探

索相关解决方案。近期科技监管政策的走向一定程度上决

定了美国科技行业能否走出危机阴影，从而继续保持美国

科技行业在全球的竞争力。

**179**

 **180** **数据治理：数据政**



**第16章**

**欧盟数据共享政策探索**

**摘要：**一直以严格保护为传统的欧盟同时也在致力于 促进数据共享的政策研究。这或解释了数据治理往往并不

是非此即彼的价值取向，而是科学精巧的政策平衡。

相较于美国，在欧盟，政策关注点投向了另一端—— 数据共享议题。2017年1月，欧盟委员会发布《构建欧盟 数据经济》公报，其预测欧盟数据市场的价值在2020年将 超过1060亿欧元，增长前景可期。公报呼吁构建完善机制， 实现企业间非个人的及机器生成的数据的访问和共享。为 了加深理解，欧盟委员会于2017年7月发布了《欧洲企业 间数据共享指南》,对公司间数据共享和再利用的规模进 行评估，识别阻碍欧洲企业间数据共享和再利用的障碍因 素，并为促进数据共享提出可行建议。2018年4月，经过 产业界、学界、欧盟官方机构的共同合作， 《欧洲数据经 济中的私营部门数据共享指南》报告正式发布(以下简称

《数据共享指南》)。

《数据共享指南》显示，欧洲企业间数据共享的模式 多样，涉及行业范围广泛。不仅仅专属于互联网相关行业，

而且深入工业、农业、能源、物流等传统行业，与新兴行

**I8I**

**第四篇** **数据共享与数据流动**

业一起，以数据的产生与利用作为重要驱动，实现产品、

服务的创新和产业的整体升级。

《数据共享指南》的基础性研究报告中总结了数据共

享的五种不同模式。

(1)数据货币化。数据货币化指通过向其他公司

分享数据而取得额外收入的单边方法，也包括因提供数

据服务而实现数据货币化。例如，荷兰的一家智慧农业

公司Van den Borne Aardappelen 将土壤信息和农

作物数据出售给农药企业和种子企业。又如，西班牙电

信 Telefónica 于2016年创建了一种专门的访问单元

LUCA, 提供来自公司数据的匿名化分析服务，以帮助客户

做出更好的决策；它的许可协议十分全面，在提供客户有

价值的建议的同时，通过对使用权限的严格限制实现对数

据隐私的保护。

(2)数据交易市场。数据供应企业和数据需求企业

通过受信任的中介机构，在其设立或管理的安全在线平台

上交易数据，中介机构对平台上的数据交易收取佣金。例

如，独立的第三方可信数据共享平台 DAWEX 就是一个汇聚

了数据提供者和数据使用者的全球性数据交易平台。

(3)产业数据平台。在特定的产业场景中，部分公

司选择达成战略合作伙伴关系，自愿加入一个封闭、安全

和专属的平台，从数据交换中互惠互利，数据可以在平台

上免费共享，也可以支付对价。这些来自不同公司的数据

集合可以给相关各方带来明显收益，参与此类数据协作平

**182**



**数据治理：数据政**

台的公司可能因此开发出新的产品、服务，或是大幅提高 原有产品、服务的性能与水平。例如，欧洲领先的飞机制 造商空中客车公司(Airbus) 创建了Skywise 平台，为

平台成员提供数据服务以提高生产效率。

(4)数据共享技术服务。与产业数据平台或数据交易 市场不同，技术服务企业的收益并非来自直接的数据分享， 而是通过建立、实施或者维护促进企业间数据共享的技术 方案收取费用。例如， DKE 、API-AGRO 、Nallianand 和 Sensative 建立了他们自己基于网络或基于云服务的 技术方案，来促进数据使用者或商业伙伴间的数据与技术

的分享。

(5)数据开放与数据策略。这些企业实行开放的数 据政策，将数据合法提供给第三方，用于开发新产品和新 服务。采取此策略的公司大多在法律上负有开放数据的义 务，尤其集中在能源领域。例如。法国国家电网运营商 Enedis 已有20多年的数据共享经历。它最初出于法律 义务与第三方分享能源分布和消费数据，目前则将数据共 享作为自身数据转型策略的一部分，其数据已在能源市场、 可再生能源、智能建筑和智能家居等领域被证明是极有价

值的。

同时，报告也指出了阻碍欧洲企业间开展数据共享的

限制性因素。

这些限制性因素来自如下三个方面。

(1)文化组织因素。缺乏对技术解决方案的信任，对

**183**

**第四篇** **数据共享与数据流动**

共享平台的安全性存在怀疑；评估数据资产价值存在困难。

(2)法律监管因素。包括数据权属问题不清、数据

利用合规上的不确定性 (GDPR) 、 数据本地化限制等。

(3)技术运营因素。企业间的数据共享缺乏标准化

模式，不同数据集和信息系统之间缺乏交互操作，缺乏(兼

容)标准。

基于此，报告提出了相关建议。

《数据共享指南》指出，欧洲企业间数据共享在现实

中是大量存在的，在未来还将继续增长，并对促进经济增

长产生积极影响。因此，促进数据共享发展应当是政策制

定者的当务之急：

第一，加快对数据权属的研究，完善非个人数据访问

和流动的法律保障。

第二，推广和促进企业间数据共享许可协议的使用。

第三，提高数据使用的持续审计的技术能力，防止数

据滥用。

对于第一点，欧盟已经通过实质性的政策调整，迈出

了积极一步。2018年10月4日通过的《非个人数据在欧

盟境内自由流动框架条例》在法规层面消除阻碍企业间数

据共享面临的负面因素。 一方面，提出对数据本地化措施

予以最大程度的限制或禁止；另一方面，规定欧盟委员会

应鼓励和促进制定联盟一级的自律行为守则(也称“行为

**I84**

**数据治理：数据政**

守则”),以便在透明度、互通性原则和开放标准的基础上，

助力发展基于数据共享的有竞争力的数据经济。

对于第二点，《数据共享指南》也重申了许可协议在 数据共享中的基础性作用。数据共享通常是在协议的基础 上实现的。双方或多方通过数据使用许可协议就数据共享 的内容、价值及合同上规定的其他方式达成一致。全面的 数据许可协议应该覆盖以下内容：对共享数据本身的描述， 可以访问、使用数据的主体，以何种方式使用，包括数据(分

析)的衍生品权利分配、责任分配等。

最后，为数据共享提供可信、安全的环境， 《数据共 享指南》也从技术视角提供了相关技术解决方案建议。《数 据共享指南》肯定了API 接口作为数据共享方式的优点： 简单快速访问数据，可监控数据的使用，核实违反合同的

行为；迅速处理数据的滥用(终止或暂停数据访问)。

此外，《数据共享指南》还推荐了将算法应用于 数据 (Algorithm to the data) 及隐私保护计算 (Privacy-preserving Computation) 等的技术方 式。这些技术应用将使得数据安全、数据保护及隐私等难 题迎刃而解。其中，算法将确保实现个人数据与隐私保护 的关键因素——尽可能少地转移数据，而隐私保护计算在 确保不泄露输入数据的前提下提取有用信息。因此，数据 计算可以在不同领域(公共或者私人)中同时运行而不必 将数据迁移出公司。这些模型意味着从“分享数据”到“分

享计算”的基本范式转移。

**185**

**第四篇** **数据共享与数据流动**



**第17章**

**数据跨境流动政策认知与建议**

**摘要：**在当前网络空间的治理政策中，没有哪类议题 能够像数据跨境流动一样包含如此复杂的讨论场景：数据 主权、隐私保护、法律适用与管辖乃至国际贸易规则。特 别是在2013年的“斯诺登事件”[口后，随着安全担忧情 绪的蔓延，各国政府引入了形式多样的本地化要求，更增

加了人们对数据跨境流动政策的困惑与误解。

本文通过详细对比美国、欧盟等最具代表性的数据跨 境流动政策，总结它们的共性与差异，以澄清有关该政策 的基本认知，并基于欧盟制度改革中对数据跨境流动政策

的反思，提出相关政策完善建议。

此外，基于中国、美国、欧盟对全球网络空间治理规 则的影响力，本文分析了全球数据跨境流动政策的基本走 向，以及其对数字经济全球化运营可能带来的深度影响，

并面向企业提出相关建议。

对于身处复杂政策框架下的企业来说，不仅需要关注 不同的规制要求，积极寻求多样化合规渠道，更需要从长

远建立全球化与本土化相结合的竞争战略。

[1]斯诺登事件又称

“棱镜门事件”是指，

由美国官方及众多大

型科技公司参与的大

规模国际窃听计划及

行动——棱镜计划，

由于斯诺登的披露和

出走而曝光的轰动事

件。

**186**

数据治理：数据政

**一** **、关于讨论前提的两点澄清**

(一)跨境流动政策与数据本地化措施的关系：

本地化并不意味着绝对禁止数据跨境流动

数据跨境流动政策是指一国(或地区)政府针对数据 通过信息网络跨越边境的传输、处理活动所采取的基本立 场以及配套管理措施的集合。尽管信息网络中数据的传输 边际成本极低，互联网基础协议能够确定网络任意两点之 间传输数据包的最快路径，且不以地理边境为界，但各国 出于隐私、安全等考虑，对从技术上完全可实现的“数据

自由流动”现象从政策层面做了不同程度的干预。

“数据跨境流动政策”这一表述本身是中性的和广义 的，它包含了从开放到保守不同立场倾向的政策类型。它 既可以针对数据流出境外的场景(如欧盟对于个人数据转 移到欧盟以外的管理框架),又可以适用于数据流入境内 的场景(如出于保护公共利益需要，对于儿童色情侵扰、 侵害知识产权等数据，采取措施禁止本国居民通过网络访

问获得)。

相比之下，数据本地化措施从概念本身来说要狭义许 多。数据本地化措施是指出于本国公民隐私保护、国家数 据安全，以及执法便利等目的，要求数据在境内存储、处

理的管理要求集合。

当然，数据本地化措施也可以包含宽严程度不同的类

型，通常包括：

(1)仅要求在当地有数据备份，未对数据跨境流动

**187**

**第四篇** **数据共享与数据流动**

做过多限制。

(2)数据留存在当地，且对跨境提供数据有限制。

(3)要求特定类型的数据留存在境内。

(4)数据留存在境内的自有设施上等。

因此，尽管数据本地化措施正在成为当前全球网络空

间治理的一股潮流，但它仍然仅代表了数据跨境流动政策

的一种方向。而且鉴于“数据本地化”政策的丰富类型，

本地化并不意味着绝对禁止数据的跨境流动，有相当部分

的数据本地化政策仍然给出了很多例外。

(二)数据跨境流动政策适用的数据类型：

主要围绕个人数据

关于数据跨境流动政策的讨论最早始于个人数据保护

法律领域。个人数据保护的国际纲领性文件——1980年经

济合作与发展组织出台的《关于保护隐私和个人数据跨境

流动指南》,内容主要分为“国内适用的基本原则”和“国

际间适用的基本原则”,后者解决的即是个人数据跨境流

动问题。 “斯诺登事件”之后，新一轮的数据跨境流动政

策对数据类型有所扩展。但从各国政策的总体观察来看，

政策对象仍以个人数据为主，在有限的案例中扩展至其他

数据。

国内关于数据跨境流动政策的部分研究文献将政府数

据纳入其中，并基于政府数据类型提出相应的跨境流动管

理策略。此类认知需予以澄清。

**I88**

数据治理：数据政

实际上政府数据中涉及国家秘密乃至安全的部分，在 属性上已经提出了更高的保密性要求，禁止跨境流动本就 是应有之义；不涉及国家秘密的部分，如果具备公开属性， 则应纳入政府数据开放调整范围，也不牵涉跨境数据管理

问题。

归根结底，政府数据无论是否具有秘密属性，都具有 在本地存储的天然特点，绝大部分也不具有跨境流动的商 业化需求。因此，在数据跨境政策讨论中，提出政府数据

类别，对于认知数据跨境流动政策并无特别意义。

综上，本文聚焦于各国针对经贸往来中基于商业目的

的数据跨境流动政策分析。

**二、美欧数字跨境政策发展概况及差异**

数据跨境流动是经济全球化与数字化的伴生物。美国 和欧盟基于各自的政治、经济、法律传统等因素，在不同

的历史背景下，发展出了特色鲜明的数据跨境流动政策。

**(一)美国数据跨境流动政策主要由贸易利益驱动**

美国在克林顿政府时期(即1993—2001年),就已形 成了对数据跨境流动问题的初步策略。美国于1997年发布 的《全球电子商务框架》提出： “只有当个人隐私和信息 自由流动带来的利益取得平衡时，全球信息基础设施才可 能兴旺起来。美国支持为用户提供恰当的隐私保护，以提

升用户使用互联网服务的信心，但各国在公民隐私保护方



**第四篇**

面迥然不同的政策，有可能会形成非关税贸易壁垒。”

对此，美国采取了以下策略：

(1)依据个人隐私保护基本原则会同其主要贸易伙

伴推进符合市场需求的个人隐私政策。

(2)继续与欧盟进行对话讨论以解决数据流动问题。

(3)通过双、多边讨论以及地区性论坛，就跨境流

动问题展开对话。

二十多年来，美国在以上三个方面取得了不同的进展。 首先，尽管与欧盟在个人数据保护路径上存在明显分歧， 2015年欧洲法院甚至废除了美欧执行已逾15年的“欧美 安全港协议”,但不可否认的是，二者之间的政策分歧从 未实质性地影响跨大西洋数据流动。直至2016年“新隐 私盾协议”的达成，也仍旧为欧美实现数据流动提供了积 极机制，目前包括 Google 、Facebook 、Microsoft 等

2500 家美国公司的跨境数据传输仍依赖于该机制。

其次，双边、多边贸易协议已成为美国推进其数据流 动政策的主要渠道。2012年《美韩自由贸易协定》第一次 在贸易协定电子商务章节中规定了跨境数据流动规则。尽 管美国已退出 TPPl21谈判，但由其提出的跨境数据流动规

则已成为不少国际协定电子商务章节的范本。

此外，美国通过亚太经济合作组织 (APEC) 积极推进 《APEC跨境隐私规则体系》 (CBPRs), 该体系倡导数

据治理规则的实用性，对于通过CBPR认证的企业，被认

189

**数据共享与数据流动**

[2]TPP(Trans-

Pacific Partnershin

Agreement), 跨太平

洋伙伴关系协定，由亚

太经济合作组织成员国

中的新西兰、新加坡、

智利和文莱四国发起，

现有十余个国家加入，

中国未加入 TPP。

**190**

**数据治理：数据政**

为满足了隐私保护要求，可以在APEC区域内实现自由的

跨境数据传输。

**(二)欧盟在人权基础下考虑数据跨境流动政策**

与美国将数据跨境政策与贸易政策深度捆绑不同，欧

盟更多地从个人权利保护项下考虑数据流动。

欧盟1995年《关于个人数据处理保护与自由流动指令》 规定：欧盟公民的个人数据只能向那些与欧盟数据保护水 平相同的国家或地区流动。如果数据接收国的法律水平没 有达到欧盟委员会认可的标准，有两种替代方式也可实现 转移： 一种是例外场景，如取得了数据主体的明确同意， 或该转移是为了履行与数据主体之间的协议所必需的；另

一种情形是企业能够证明已采取了充分的保障措施。

此外，欧盟也通过在全球积极推广其个人数据保护制

度，不断扩展可以实现数据自由流动的地区。

1981年，欧洲理事会各成员国签署欧洲《有关个人数 据自动化处理之个人保护公约》(欧洲第108号公约)。 加入该公约，意味着要建立与欧盟相似的个人数据保护立 法，将被视为满足欧盟跨境数据流动“充分性保护”标准 的重要参考。特别是自2010年以来，欧盟加速推进了“公

约”的全球化进程，目前已有46个国家加入了该“公约”。

与美欧相比，中国、巴西等国家更多地从维护网络安 全和数据主权为目的出发，制定跨境数据流动政策。包括

中国、越南、巴西等在内的发展中国家，以及包括澳大利亚、

**I9I**

**第四篇数据共享与数据流动**

加拿大等在内的发达国家，均在不同程度上提出了数据本

地化措施。此类措施对服务贸易全球化可能带来消极影响，

但能在一定程度上保障国家信息安全，特别是可从执法层

面为国家行使司法主权提供依托。

(三)美欧数据跨境流动政策的具体实施机制

有较大差异

美国要在国际上推行宽松的数据跨境流动政策，首先

需要在本国示范。

因此，在美国的一般立法中，难以观察到禁止或者限

制数据跨境流动的明确要求。但在一些特定案例中，美国

也留有了一定的政策回转空间。

例如，美国针对外国投资的安全审查中，可以与外国 投资者签订安全协议，而安全协议可能包括相关的数据本 地化要求。关于数据本地化要求的执行落地，也通常会由 CIFUs(3) 指定的特定政府部门来负责监督执行。

欧盟数据跨境转移政策主要体现在个人数据保护制度

中，相应地，其实施机制也依附于个人数据保护执法体系。

如上所述，欧盟数据控制者实施个人数据跨境流动活 动时，有三种合法方式：(1)数据传输至“充分性认定” 地区；(2)例外场景(包括用户同意或者执行合同需要等); (3)充分保障措施。考虑到“例外情形”可适用场景少， 并不能够为日常化、规模化的数据跨境转移提供稳定的合

法性基础，以下主要介绍“充分性认定”机制和“充分保

[3]CFIUS(The

Committee on For-

eign Investment

in the United

States) , 美国联邦

外资投资委员会，层级

高、权限大，负责审查

对美国有重要影响的外

商投资项目或重大交

易。

**192**



数据治理：数据政

障措施”机制。

“充分性认定”是一个白名单机制。欧盟委员会负责 根据第三国的个人信息保护立法状况、执法能力，以及是 否存在有效的救济机制等因素，做出综合评估。截至目前， 仅有阿根廷、加拿大等不超过20个国家或地区通过了欧盟 委员会的认定。此外，对于美国这一重要的贸易伙伴，欧 盟发展出“安全港框架”,以针对性地解决与美国之间的

数据流动问题。

充分保障措施主要体现为“标准合同文本”(Standar d Clauses Contract,scc)机制和“有约束力的公司规则” (Binding Corporate Rule,BCR)机制。对于前者， 截至目前，欧盟委员会已经形成了三个合同范本，分别适 用于“数据控制者到数据控制者之间的转移” “数据控制 者到数据处理者之间的转移”。此类合同范本通过规定数 据输出方和数据接收方基于合同的数据保护责任，来间接 提供对个人的保护机制；对于后者——“有约束力的公司 规则”则是集团型跨国企业可优先考虑的机制，集团遵循

一套完整的、经个人数据监管机构认可的数据处理机制，

则该集团内部整体成为一个“安全港”,个人数据可以从 集团内的一个成员合法传输给另一个成员。目前，包括埃 森哲、宝马汽车、惠普、摩托罗拉等72家跨国公司获得了

欧盟的 BCR 认可。

由于通过“充分性认定”的国家总是少数，因此充分



**第四篇** **数据共享与数据流动**

**193**

保障措施机制实质上是欧盟各国数据保护机构在跨境数据

流动管理中最为主要的工具。

三、数据跨境政策面临的共性问题及对中国的

参考建议

尽管在政策目标上具有明显差异，但美欧在数据跨境

流动政策中也面临着最为基础的共性问题——如何在全球

化的数字经济中有效达成数据跨境流动监管目标?特别是

在数据跨境流动成为普遍趋势的背景下，对数据跨境活动

的干预愈深，这一问题带来的挑战愈大。

美国凭借其技术、产业优势以及灵活的监管制度优势，

对数据跨境伴生的隐私保护、数据安全问题并无特别担忧，

因此仅建立了“个案式的事后监管”机制，此类机制最大

限度地避免了对数据跨境流动的干预，同时也能有效获得

美国贸易利益和安全利益的双赢。

美国面临的困境是在全球推行数据自由流动时，难以

提出对“数据本地化”进行限制的合理标准，毕竟国际贸

易规则中将安全和公共利益作为基本例外。

而对于中国和欧盟来说，对安全和隐私的担忧却是真

实存在的，因此二者也相应地建立了普适性的数据跨境流

动管理机制。由于中国仍处于制度建设期，尚无法观察其

实践效果，但实施已二十余年的欧盟数据跨境转移管理机

制则较为全面地呈现了其所面临的实际困境。

**194**

**数据治理：数据政**

**(一)欧盟数据跨境流动政策的困境与改良**

欧盟于2012年启动个人数据保护立法改革时，全面 梳理了现有的个人数据保护制度呈现出的种种缺陷。其中 最为突出的问题是，日益增长的全球数据流动与现有监管 制度之间的不适应。几乎所有的欧盟企业都涉及向欧盟境 外传输数据，但如果完全依照1995年《数据保护指令》 所规定的跨境流动管理制度，那么无论是企业还是监管机 构都会难以付诸实践。批评意见认为：欧盟对个人信息的 跨境转移设置严格条件类似于虚幻假象，因为它假想欧盟 的标准能覆盖到除欧盟外的全球各处，但实际情形并非如 此。的确，欧盟跨境数据转移管理的三类方式均已捉襟见 肘。因此，欧盟个人数据保护法规《通用数据保护条例》 (General Data Protection Rules,GDPR) 对跨 境数据流动政策进行了大幅优化改革，特别着力于提升政

策的灵活度。

1.明确禁止各成员国以许可方式管理跨境数据流动。 多年的实践表明，欧盟各成员国对跨境流动采取的许可管 理方式并没有实质性地提升个人信息出境的保护水平，相 反，事前许可制度却带来了官僚主义问题。因此，2016年 的 GDPR重点简化了数据跨境传输机制，明确禁止了许可 管理做法，只要符合GDPR中跨境数据流动的合规条件，

成员国就不得再通过许可方式予以限制。

2. 增加了充分性认定的对象类型。除对国家可以做出 评估外，还可以对一国内的特定地区、行业领域以及国际

组织的保护水平做出评估判断，以进一步扩展通过“充分

**195**

**第四篇** **数据共享与数据流动**

性”决定 (Adequate Decision)覆盖的地区。

3. 扩展“标准合同条款”,除了保留目前已生效的3

个标准合同范文。GDPR 增加了成员国数据监管机构可以

指定其他标准合同条款的渠道，在企业实现合法的数据跨

境转移时，有更多的合法机制可以选择。

4. 发挥行业协会等第三方监督与市场自律作用。

GDPR 规定数据控制者可以成立协会并提出所遵守的详细

行为准则(Codes of Conduct)。该行为准则经由成

员国监管机构或者欧盟数据保护委员认可后，也可以作为

跨境数据流动实践中的合法依据。此外，经认可的市场认

证标志也可以作为数据跨境转移的合法机制。

**(二)欧盟经验对中国的参考意义**

1.中国数据跨境流动政策发展概况

2016年11月出台的《网络安全法》首次以国家法律

形式明确了中国数据跨境流动基本政策。

中国数据跨境流动政策更多的是在“斯诺登事件”后，

基于国家网络安全视角而提出的。但实际上这种政策视角

在2013年前就已显露雏形。

例如，2011年中国人民银行发布的《关于银行业金融

机构做好个人金融信息保护工作的通知》要求个人金融信

息的储存、处理和分析应当在中国境内进行；2013年《征

信业管理条例》规定征信机构对在中国境内采集的信息的

整理、保存和加工，应当在中国境内进行。

**196**



**数据治理：数据政**

此后，出于数据安全目的，本地化要求进一步被写入 网络监管立法，除《网络安全法》外，2014年的《人口健 康信息管理办法(试行)》、2015年的《地图管理条例》、 2016年的《网络出版服务管理规定》、2016年的《网络预 约出租汽车经营服务管理暂行办法》等，都不同程度提出 了数据本地化要求。正在制定中的《个人信息和重要数据 出境安全评估办法》及其配套的标准指南也将全面搭建起

数据出境管理框架。

中国和欧盟均对日益增长的数据跨境流动采取干预措 施，欧盟积累的政策经验与教训对中国而言具有重要参考 价值。特别是与欧盟相比，中国对数据跨境流动活动的干 预似乎更深、更直接，更需要系统考虑如何采取科学有效

的机制，以有效平衡数据流动带来的发展与安全利益。

其一 ， “许可”等事前监管机制已被证明具有固有的 局限性。 一方面，它与全球化数字经济的发展趋势极不适 应。数据的跨境流动并不遵循特定的路径，而通过多种方 式、多种渠道(如E-mail) 提供数据库访问权限，或者 通过内部网络进行交换。传统的许可管理方式与此格格不 入。事前建立一刀切的许可门槛，并不有助于监管目标的

实现，而往往只会增加形式上的行政负担。

当然，在国内此前公布的数据出境文件征求意见稿中， 监管机构已然关注到了这一问题，引入了企业自评估机制，

并体现出将政府评估作为事中、事后监管的思路。

其二，要为“合理有序的数据流动”提供尽可能丰富

的合法渠道。欧盟数据跨境政策的改革方向表明，如果不

**197**

**第四篇数据共享与数据流动**

能提供多样化的有效合法跨境渠道，那么无法向市场传达

政策方向，进而无法在引导企业通过可预期的稳定机制实

现自身的数据跨境需求的同时，实现监管者设定的用户隐

私、数据安全目标。这也是欧盟在对数据跨境流动机制进

行改革时，重点落脚于增加有效渠道的根本原因。

2. 中国可借鉴的有益做法

我国目前初步建立的数据跨境流动政策，如将数据出

境安全评估作为单一合规机制，在现实中恐怕难以适应海

量数据跨境管理需求。建议参考欧盟及其他国家的经验，

设立符合我国国情的多样化合法流动机制。

(1)建立白名单机制。根据个人信息保护状况及对

等措施，将部分国家或地区纳入可自由流动的国家或地区。

考虑到短期内各国无法形成相互协调的数据流动政策

体系，数据跨境流动政策将深度嵌入双、多边的贸易投资

谈判，在国与国之间、区域与区域之间体现出多样性、灵

活性，形成不同的解决方案。

例如，日本、韩国已分别启动与美欧的数据跨境流

动双边谈判，预计日本和韩国将分别与欧洲达成充分性保

护互认协议。同时，由于日本和韩国均已加入美国主导的

APEC 跨境数据流动 CBPRs 机制，日本、韩国与美国的数

据流动也具备顺畅渠道，预计此类区域性的数据流动协议

在未来将成为解决数据流动的主要途径之一。

(2)根据安全评估的主要标准，建立指引性的数据

**198**

**数据要素**

**数据治理：数据政策发展与趋势**

跨境流动协议范本，类似于欧盟标准合同范本，引导企业

在数据出境中通过合同法律机制来管控数据出境风险。

(3)鼓励行业协会及其他自律组织参与安全评估， 作为市场机制补充，在安全评估中发挥作用，从而建立可

落地实施、具有活力的数据管理秩序。

(4)对不同性质的数据采取分类管理方法。不仅区 分个人数据、重要数据，形成对应的跨境流动管理策略， 而且可在进一步的管理实践中根据数据的安全属性进行梯

度性管理。

综上，在信息通信技术与经济全球化深度耦合的背景 下，应当承认数据的跨境流动是绝对的，而对数据流动的 限制是相对的。后者是手段，前者是目标。在数据出境安 全评估指南的制定过程中，有关专家指出：安全评估的实 质是服务于数据出境，是在保障安全的前提下促进数据的

跨境流动。

**四** **、复杂的数据流动政策对跨境业务的影响**

基于中国、美国和欧盟政策之间的巨大鸿沟，在全球 范围内形成协调一致的跨境数据流动政策还很遥远。除了 “数据自由流动”与“数据本地化”之间的冲突，欧盟、 美国、中国数据流动机制的具体差异也决定了在未来一段 时期，涉及数据跨境流动的企业需要面临复杂的政策环境，

这不仅直接关系业务合规，而且对成本负担、技术架构乃

**199**

**第四篇** **数据共享与数据流动**

至战略布局带来深度影响。

首先，包括本地化在内的各类数据跨境流动政策，对

依赖全球数据聚合的业务带来影响。例如，对于金融行业，

跨国银行集团需要建立集中化的数据处理中心；对于跨境

物流行业，集团通过汇聚全球数据来高效调配物流资源。

此类业务的数据集中都将面临挑战。换言之，物联网、云

计算、大数据应用在技术上完全可实现全球数据资源的汇

集，并通过对数据汇集的加工分析，创造出新的经济价值，

而全球割裂的数据跨境流动政策将直接影响此类业务的效

率，甚至影响业务模式本身能否持续开展。

其次，相比于大型企业，中小企业受到的冲击更大。

大型企业往往在数据中心部署方面更具优势，可以利用充

沛的资源和技术方案实现合规要求；而处于发展起步阶段

的中小企业，在跨境业务中部署数据本地化方案将不是一

个轻松的决定，这在一定程度上反映了数据本地化政策带

来的市场竞争效应，其政策门槛削弱了中小企业对跨境业

务的参与度和市场创新能力。

再次，“数据本地化”政策对没有本地化需求的跨境

业务带来负担。尽管在信息通信服务领域，“靠近用户”

会驱动服务商将数据中心建立在本地，提升数据传输速率，

为用户带来更好的服务体验，但不容否认的是，仍有大量

业务场景并不需要考虑这一因素，反而更关切数据本地化

带来的负担成本。例如，面向境外用户提供旅行产品订购

的网站，在初创期可能并不需要考虑在服务本地部署数据

中心；又如， 一些数据容灾备份的安全服务对数据传输响

**200**

**数据要素**

**数据治理：数据政策发展与趋势**

应速度并无特殊需求，也往往并不需要将数据部署在本地。

**五、** **数据跨境流动合规建议**

当前，不仅金融、电信、互联网等跨境服务离不开数 据跨境流动传输支撑，而且制造、医疗健康乃至农业生产

等更多的传统产业也产生了大量的数据跨境流动需求。

例如，飞机制造商波音公司通过其遍布全球的飞机和 航线服务，建立了全面的数据收集系统，用于发现和诊断 问题航班。我国重型机械生产制造企业三一重工通过对装 备运行信息的实时采集，提供远程跨境诊断服务。涉及数 据跨境流动的企业需要建立完善的合规体系，为业务开展

提供法律基础保障。

(一)关注本地数据跨境流动政策的目的及

严苛程度

各国关于数据跨境流动的政策目标决定了其严格程度 和具体要求上的差别。例如，以数据主权和网络安全为驱 动的数据跨境政策，在跨境管理上会趋向于严苛，不仅要 求在本地存储，而且对向境外提供采取了严格限制措施， 涉及的数据范围也更为广泛，会对企业运营带来更深度影 响，需深入业务场景和技术实现方式提出合规方案；而以 保护公民个人信息为目标的政策要求会留有更多的例外空 间和合法转移渠道，且仅涉及个人数据，企业可根据自身

需求选择适合的合规途径。

**201**

**第四篇** **数据共享与数据流动**

**(二)积极寻求多样化的合规渠道**

我国的企业面临两类基本的数据跨境流动合规问题：

一类是从我国收集运营的数据向境外传输、提供的问题；

另一类是开展跨境服务的我国企业在其他海外市场所面临

的当地数据出境政策。

对于第一类问题，我国目前根据《网络安全法》第

三十七条来制定相关配套办法标准，将初步建立较为严格

的数据跨境流动管理制度，企业应根据要求建立完善的出

境数据档案及安全自评估制度，以备相关主管部门实施监

督检查。除了少数例外情况，数据出境的合法路径主要依

赖于企业的安全自评估和主管部门评估。

而越来越多的“出海企业”将面临第二类问题。首先，

在欧盟市场，由于我国的个人信息保护水平与欧盟尚存较

大差距，并不满足欧盟的“充分性”认定标准，欧盟成员

国往往会对传输至我国境内的个人数据活动做出限制。在

此背景下，我国企业要根据欧盟法律要求，积极寻求数据

跨境转移的合法性基础。

在欧盟新的数据保护立法 GDPR于2018年5月生效

之前，中国企业可以利用的合法传输机制尚且相当有限。

例如， “标准合同文本”和“有约束力公司规则”仍很难

为中国企业所利用。相比较而言，作为中国企业的竞争对

手——美国企业(特别是中小企业)则可以利用“美欧隐

私盾”更方便地实现数据合法转移，而日韩企业也有望很

快通过政府与欧盟达成的充分性保护互认协议实现高效的

转移数据。

**202**

**数据要素**

**数据治理：数据政策发展与趋势**

若采取例外情形中的“用户同意”模式，则要满足欧 盟对“同意”的高标准要求，包括向用户充分说明跨境传 输的相关信息，如传输目的国、目的国的个人信息保护水 平以及用户可能面临的风险，并确保用户的同意是在充分 知情的情形下做出的特定授权。因此，此类高标准要求也

决定了“同意”机制多数情况下仅适用于小规模的数据转移。

对于具有一定实力的中国企业，则可以结合业务布局 考虑，选择在欧盟成员国或欧盟认可的“充分保护认定” 国家，如加拿大、阿根廷、新西兰等，建立或选择数据中 心作为“数据港”,以尽可能降低数据跨境传输的成本和 合规风险。此外，在欧盟市场面临的问题也将在其他效仿 欧盟建立跨境流动机制的国家体现，比如非洲等新兴市场

国家，企业需要提前做好合规路径储备。

而在美国及APEC 成员国或地区，由于美国所推行的 APEC隐私框架中的跨境隐私保护规则(CBPRs) 进展缓慢， 我国也未正式加入，我国企业还不能利用该框架中的跨境 数据转移机制。因此在美国、APEC 成员国或地区的数据 跨境转移，我国企业也需更多地考虑数据跨境转移合规问 题，并根据不同国家或地区的跨境转移需求制定不同的合 规方案。其中也可结合各国数据保护水平和国际认可程度， 选择相关国家或地区作为“数据港”,如澳大利亚、新加

坡和我国的香港地区。

**(三)应对数据本地化带来的管辖冲突**

事实上，尽管根据不同国家或地区数据跨境流动政策

**203**

**第四篇** **数据共享与数据流动**

可以选择不同的合规方案，但最终无法回避管辖冲突问题。 互联网是全球性的，然而立法与监管却是基于地域的。长 期以来，互联网的管辖适用问题一直就未得到解决，而当

前复杂的全球数据流动则更进一步加剧了管辖冲突。

例如，各国通过数据本地化立法来解决法律适用和本 地执法问题，但从美国相关案例典型如微软公司诉美国司 法部案(4)中，司法部门认为其无论数据存储在哪里，都 具有其管辖权，使得企业处于进退两难的境地。实际上， 这不仅是大型跨国公司面临的问题，伴随着互联网服务的

全球化趋势， 一些初创企业也将面临此类问题。

针对法律适用和管辖，政府部门和司法机构可以有不 同的主张，包括服务提供商注册所在地(总部所在地)、 数据存储服务器所在地、数据本身所涉及的数据主体所在 地等，多项的法律适用连接点给跨境服务企业带来了更多

的法定义务冲突问题。

当前阶段，司法管辖冲突更多地体现为个案式的。例 如，在涉及诉讼、仲裁等跨境调查中，由于各国法律及监 管要求的不同而造成了直接冲突。随着欧盟具有宽泛适用 范围的《个人数据保护法》于2018年5月的生效，以及更 多数据本地化要求的出现，这种冲突将更加广泛，不再仅

仅限于个案，而是深度影响到业务运营。

[4]指2016年4月微

软公司4月14日向一

家联邦地区法院提起

诉讼，把美国司法部

列为被告，要求修改

关于不得透露政府索

要用户数据行为的法

律。

考虑到国家间的司法协助条约(MLAT) 进展缓慢，

特别如微软公司诉美国司法部案件中所反映出的“政府倾

向”,在国家间烦琐冗长的司法协助程序和直接向服务商

**204**

**数据要素**

**数据治理：数据政策发展与趋势**

发出协助配合要求之间，政府和司法机构更容易选择后者。 这实质上间接鼓励着各国政府更愿意选择数据本地化政 策，数据存储在本地至少有执法便利，在法律适用上本身

也是一个强有力的抗辩。

因此，对于面向全球提供服务的企业而言，在法律适 用冲突中较为安全的选择是，将所服务的不同国家的公民 个人数据存储在不同国家(或该国政策认可的其他地区), 当然这无疑会产生新的巨大成本，且仍会面临复杂的管辖

竞合问题，亟待通过国际层面达成协调机制。

**(四)建立全球化与本土化相结合的竞争战略**

对于全球化的平台企业而言，则需要以“全球化”和“本 土化”相结合的视角破解数据管辖冲突困境。例如，欧盟 没有直接提出数据本地化要求，理论上企业可以选择多种 渠道实现跨境流动。但微软公司却已在尝试更深度的本地 化解决方案。微软公司于2016年底与德国电信合作运营数 据中心，专门向欧盟客户提供服务。根据双方的合作安排， 德国电信的子公司 T-Systems 扮演数据中心“受托人”

角色，负责管理微软公司在德国的数据中心。

正是考虑到在全球政策层面短期内无法提供数据安全 及管辖冲突的协调方案，跨国企业已开始着眼于本地化模 式的调整，包括从技术架构、商业模式等多方面进行改进 优化，通过整合本地化模式，使之既符合当地监管要求，

又形成更为强大的全球竞争力。

*JHHHH!!!!!!!!!!!!!!!!*



**第五篇**

**数据治理与政务数据规则**

数据治理政策的讨论应当是多维框架、多因素互动的。

要用精细化和科学方式设计政策，实现权利保护、产业发

展、国家竞争力提升的多赢。此外，2020年这一场席卷全

球的新冠疫情，也推动着政府数据治理能力驶入快车道。

**206**

**数据要素**

**数据治理：数据政策发展与趋势**



**第18章**

**数据治理——精细科学的政策平衡**

**摘要：**数据的大规模应用，促进了技术发展、社会进 步和文明升级，但数据盗窃、滥用、歧视和数据壁垒等“灰 色阴影”也如影随形，数据治理的重要性被广泛接受，数

据治理的法规及其实施也被放到了前所未有的高度之上。

**一、2018年，数据治理的灰色之年?**

数据泄露、滥用、歧视这些负面事件如同天空中的阴

霾，不断加深着人们对数据治理的悲观情绪。

的确，这一年被数据泄露贯穿始终，规模日益扩大。 从上一年末，美国最大的三家个人征信机构之一 Equifax 数据泄露，到中国最大的多品牌酒店集团——华住集团数 据泄露，再到万豪酒店集团的数据泄露，每次数据泄露的

规模均在亿条以上。

数据泄露之后的滥用问题也在持续升级。Facebook 丑闻中， “剑桥分析”公司涉嫌利用来自 Facebook 的用 户数据影响多国大选，美国国会已连续召开十几场听证会，

深度拷问平台的数据处理规则。

国内媒体爆出的“大数据杀熟”现象，让经济学上的



**第五篇** **数据治理与政务数据规则**

**207**

价格歧视问题被抛向更广泛的公众视野。现实中，平台利

用大数据来攫取消费者剩余是广泛存在的吗?如果是，监

管者和消费者又该如何应对?

除了牵动普通消费者的数据焦虑，国家层面的数据安

全也在面临全新挑战。2018年3月美国Cloud 法 案(cloud

Act ) 出台，美国单边提出了新的跨境数据执法框架，尽

管这是对传统低效的跨国执法合作机制的一种探索改变，

但仍然增加了其他国家(包括中国)数据安全的不确定性。

问题本身让人沮丧，但更令人沮丧的是，我们似乎还

未找到开启答案的钥匙。

**二** **、欧** **盟** **GDPR, 灰** **暗** **中** **的** **希** **望** **?**

2018年5月25日，欧盟 GDPR正式生效，为数据治

理带来新的曙光。欧盟的解决方案坚守保护公民基本权利

的理念，全面提升个人数据保护力度，对几乎所有的数据

处理环节建立了严格规则，以实现对个人的极致保护。

事实上，在2016年4月GDPR正式颁布后的两年过渡

期内， GDPR带给数据治理的积极影响已在不断显现。它

促使企业、政府、医院、学校等任何开展个人数据处理的

机构在数据保护方面给予更多的投入。以2017年的调查为

例， “富时350指数”公司平均为GDPR增加了43万英镑

的支出，“世界500强”企业平均增加了100万美元的支出。

更重要的是， GDPR 推动了全社会更加关注个人数据保护

问题，在过去的两年，我国政府部门、消费者协会针对隐

**208**

**数据要素**

数据治理：数据政策发展与趋势

私政策开展了多次评测活动，引导企业、机构不断提升数据处理活动的透明性。

(一)作为制度新生儿， GDPR 本身也带来了许多争议和尚待细化

的领域

1.宽泛的域外适用范围，不仅对欧盟各成员国的数据保护监管机构带来 执法挑战，同时在学界也引起了公法、国际法学者的质疑。GDPR生效后，许 多中小企业因为担心过高的法律风险，宣布停止针对欧洲地区的服务，而部 分企业则实时调整了商业模式，《华盛顿邮报》索性在欧盟推出了收费版本， 正如其宣传词所说： “请支持伟大的新闻业”。如果《华盛顿邮报》不能通

过用户 Cookie 来实现广告收入，那么用户应当为新闻内容直接付费。

对此，英国读者向英国个人信息保护主管机构ICO(Infor mation Commissioner's Office)提出投诉。按照GDPR所规定的宽泛适用范围， 只要向欧盟境内的个人提供服务，并处理个人数据，就会大概率地落入 GDPR 的管辖范围，由此ICO 对该投诉予以立案调查，但颇为尴尬的是，Ico 仅以 公告的方式提出《华盛顿邮报》的收费模式违反了GDPR关于用户同意有效 性的规定(因为用户没有其他选择),但ICo 对于该事件的调查也只能止步

于此， ICO 现有的执法资源还难以处理类似的域外案件。

除了现实中这些域外管辖带来的难题，在学者的眼中，GDPR宽泛的适用 范围在国际法领域带来了不好的先例。特别是其对于属人管辖的特别延展， 缺乏正当化和合理化的依据，加剧了数字经济背景下国际公法领域的纠纷冲

突。

2.GDPR引入的个人权利也陷入与其他基本权利的紧张冲突中，包括被

遗忘权与知情权、言论自由权的冲突，数据可携权与竞争法的冲突。

3.GDPR数据处理可解释性的要求对人工智能产业，特别是对深度学习、



**第五篇数据治理与政务数据规则**

神经网络学习提出了严峻挑战，使得欧盟包括自动驾驶在

内的AI 产业的发展陷入了困境。

**209**

4. 与区块链技术的倡导的方式完全相反。区块链的

核心本质上是分布式的、去中心化的，而GDPR的制度范

式却承袭了之前欧盟1995提《数据保护指令》中心化的

规范范式(即制度规范都指向核心的数据控制者和数据处

理者)。根据欧盟委员会和法国数据保护机构的观点，新

兴的区块链技术也必须要适用GDPR。因此，在未来 GDPR

和区块链的技术之间，仍将继续存在极大的合规差距。尽

管从技术眼光看，区块链完全可以为数据保护提供一种新

的技术解决方案。

**(二)欧盟** **GDPR** **的负面效应**

随着 GDPR的执行推进，越来越多的现象和实证数据

显示，GDPR实施对于欧盟数字经济竞争力带来了显著的

负面效应，这甚至是欧盟立法者当初在打造GDPR 时未曾

预料到的。

1.GDPR严格的合规要求巩固了大企业的优势地位。

大企业更有实力和资源投入合规工作，而中小企业被迫退

出市场，无形中为大企业收割市场提供了便利。以在线广

告市场为例，GDPR生效后，谷歌公司由于具有更强的合

规力量和产业引导力，其市场份额进一步增加；在云计算

行业，亚马逊公司的AWS、微软公司的 Azure 等领导者

在第一时间内表示可以充分满足GDPR的合规要求，对比

之下，云计算市场的中小玩家却在合规竞争力上难以同步。

 **210** **数据治理：数据政**

2.正式实施半年时的经济数据证实 GDPR 对欧洲科技 创新带来了不利影响。美国知名经济学研究机构 NBER发 布了一份权威研究报告，其采用严谨的计量经济学方法和 真实的欧洲市场活跃度数据，表明在 GDPR生效的半年以 来，其对于欧洲的创新企业的发展负面作用非常明显，尤 其是在中小企业融资的笔数、融资量方面，欧洲的中小企

业陷入了融资的困境。

以上充分显示了GDPR的二维两面性。它在为个人权 利保护带来积极力量的同时，也对技术创新和持续发展产 生了令人无法忽视的负面效应。这表明，对于数据治理， 我们仍需要探索究竟如何设计制度规范，以承载我们更多

的期望目标。

**三、美欧隐私政策在走向融合趋同吗?**

尽管美国43个州和华盛顿特区均制定了数据泄露通 知法案，但从Equifax 到万豪集团，美国一年来从未走 出数据泄露的梦魇。而2019年4月， Facebook 数据泄 露事件也将数据治理问题推向了高潮，美国海内外已经举

办数十场听证会，全方位深度拷问平台数据处理规则。

这过去一年来的听证会，深度卷入了各大科技公司、 消费者代表、隐私保护监管机构、立法者(包括 GDPR 和 CCPA的重要参与者)。通过各方的质询、回应、讨论、激 辩，将数据治理议题推向纵深，美国的数据治理框架也逐

步显现。

**2I1**

**第五篇** **数据治理与政务数据规则**

一方面，以加利福尼亚州为代表的各州对隐私保护

制度进行完善。2018年6月，加利福尼亚州率先推出了

CCPA, 这是美国目前最为严格的隐私法案。

另一方面，在国会众参两院关于制定一部统一的联邦

隐私法的呼声日益高涨，并得到了美国民主党和共和党、

科技行业的一致支持，讨论如何制定一部统一的联邦隐私

法。

面对美国隐私立法的最新变化趋势，我们不禁要问：

以 CCPA 为代表的州立法是否是美欧隐私立法走向融合趋

同的征兆，预示着崇尚市场自由的美国也如欧洲一样开始

侧重对个人权利的保护?

要回答这个问题，我们需要首先厘清美欧这两个全球

数据保护政策的体系之间的关系。

长久以来，美欧数据保护政策体现着明显的差异。欧

盟主张统一和严格立法，而美国倾向于分散和宽松立法；

欧盟强调政府部门对个人信息保护的监管权力，而美国则

主张政府的有限干预。这些差别反映了二者对于个人信息

保护政策基础理念的分歧。

当然，在根本分歧之外，美欧之间也有政策的相互借

鉴部分。例如，“数据泄露通知制度”最早发端于美国，

之后被欧盟数据保护法迅速吸收；而在被遗忘权方面，美

国也在一定程度上借鉴了欧盟立法的合理部分，比如在

CCPA中，对儿童这一敏感群体赋予了更为强大的删除权

利。这次加利福尼亚州率先在全美推出了更为严格的数据

**212**

**数据治理：数据政**

保护制度，仍然是美欧政策互动学习的结果，但这并不代

表着美欧数据保护政策走向趋同。

因为即使是最为激进的CCPA,也比GDPR要宽松很多， 也更加注重消费者保护的实际效果和促进企业发展、技术

创新之间的平衡。

而从联邦层面来说，尽管目前统一的联邦隐私立法呼 声极高，但因为美国各州差异巨大，要想在联邦层面达成 共识的隐私立法不会精细或具体，相应的执法细则应根据 各州的具体情况进行规定，不会像GDPR 那般严苛。因此， 在数据保护领域，美国与欧盟仍保持了不同风格的法律特

征，欧盟的GDPR并不是当前数据治理领域的唯一范本。

四 、数据治理，期待更为精细和科学化的

政策平衡

和欧美在数据治理领域的制度探索一样，我国也正面 临同样的制度智慧考验。《民法典》的重要分编——《人 格权编》已正式从底层制度尝试回应隐私和数据保护问题 并会在2021年1月1日起施行，《个人信息保护法》《数

据安全法》也已列入本届人大的立法日程。

对于欧美提供的制度样板，我们难以做出孰优孰劣的 判断。因为任何特定的法律制度都是建立在特定社会历史

背景下的，决定于特定的文化、经济、社会背景。

但任何良好的政策设计必须充分考虑各种因素，数据

213

**第五篇** **数据治理与政务数据规则**

治理政策也不例外。在过去的20年中，我们越来越深刻地

感受到政策讨论背景的历史变化——“个人信息保护”话

题的边界正在不断扩展，正在向内涵更加丰富的“数据治

理”转变。

个人信息作为传统法律保护的客体， 一直处于静态而

稳定的法律关系之中。无论是欧盟视为基本人权还是美国

作为消费者权利保护，权利保护的法律逻辑一直是清晰的。

然而，随着云计算、物联网、人工智能的快速发展，

数据资产在经济、社会活动中的核心和辐射作用愈发凸显。

“数据治理”正在以更宏大的议事命题浮现，形成了围绕

数据资产的隐私保护、创新竞争、安全主权等更复杂化、

更多维的公共政策讨论场。

这些复杂因素代表了从三个视角出发的利益诉求：

第一，从个人视角出发的权利保护诉求。

第二，从产业视角出发的创新、发展、竞争需求。

第三，从国家视角出发的数字经济国际竞争力和数据

主权安全需求。

以上三个视角并不是孤立存在的，而是彼此紧密联系、

互动影响的。这决定了我们当下的数据治理政策也应当采

用多维的思维进路，从个人权利保护、产业发展创新以及

国家数据安全和竞争力方面进行充分考虑和推演，从任何

从单点角度出发考虑的政策必定会带来不合理的结果。例

如，从个人视角出发的GDPR尽管赋予了个人强大的权利，

**214****数据治理：数据政**

但在实践中反而带来了大平台更加巩固市场地位、抑制产 业竞争活力的后果，愈加集中的市场最终会给个人隐私保

护带来更小的选择空间。

特定的数据治理政策会同时带来正、负两方面的效应， 这是大量隐私经济学研究所证明的通识。例如，在雇佣市 场上，如果雇主由于隐私保护管制的原因无法查阅到职位 申请人是否有犯罪前科信息，那么雇主很可能会做出更大 范围的歧视性选择，把对特定人的歧视扩展到对特定群体 的歧视；同理，如果多数消费者都从广告信息中选择退出， 那么实际上会降低产品和服务的竞争度，因为消费者获得 的产品信息更少了；而在依赖于数据共享的科研、医疗领域，

过严的数据保护政策也会带来整体社会福利的明显减损。

如何平衡好数据治理政策的积极和消极影响，并没有 一刀切的解决方案。从美国国会系列听证会对数据政策深 度探讨的外在观察来看，更科学的政策仍然是在充分考虑 数据治理过程中不同因素之间的复杂互动关系。关于未来 的联邦隐私法，我们可以预判它的核心制度和功能仍然主 要依赖于联邦贸易委员会 (FTC), 这在一定程度上决定 了美国未来的联邦隐私法也会更精细地平衡数据治理的不

同要素。

我们呼吁在当前中美数字经济竞争的格局下，数据治 理政策的讨论应当是多维框架、多因素互动的模式，增加 来自产业界、监管界和学界的互动与讨论，用更开放的视 角、更精细化和科学的方式设计更好的政策，更有效地放 大数据保护的正向能力，更小地弱化它带来的负面效果，

实现权利保护、产业发展、国家竞争力提升的多赢结果。

**215**

**第五篇数据治理与政务数据规则**



**第19章**

**“隐私”与“公共健康”的决策平衡**

——**疫情下各国个人信息保护的**

**10个共识、差异与挑战**

**摘要：**新冠疫情给世界带来巨大的灾难，世界各国也

采用了不同的方案防控疫情，恢复秩序。数据的收集、处

理分析在其中发挥了重要作用。各国如何在个人信息保护

与公共利益之间找到平衡?

**一、背景**

新冠疫情在的全球性蔓延，对各国医疗健康体系乃至

公共安全带来了持续挑战。针对个人信息，尤其是个人健

康信息、位置信息的快速收集与分析，能够帮助决策者把

握疫情发展状况，积极采取适当措施。然而，隐私权、个

人信息保护、数据安全等问题也成为挥之不去的担忧。

如何在公共安全与个人信息保护之间找到平衡，考验

着各国政府的决策能力。我们梳理分析了欧盟成员国、韩

国、新加坡、美国、加拿大、阿根廷、澳大利亚等40多个

国家在疫情期间围绕个人信息处理的规则与做法，总结了

10个各国在抗击疫情中针对个人信息保护已有共识、尚存

**216**

**数据治理：数据政**

的差异及面临的挑战。

1. 个人信息保护法律不会妨碍疫情管理措施。

2. 法律基本原则仍应得到遵循。

3. 在许多国家，雇主是除卫生部门之外最主要的疫情

信息节点，对雇主收集信息的规范成为重点。

4. 疫情推动跨部门数据共享。但整体而言，许多欧盟

成员国仍将疫情健康数据限制在公共卫生部门范围内。

5. 相比亚洲，欧盟对位置数据的利用更为谨慎。

6. 随着疫情升级，更具争议性的人脸识别、无人机投

入应用。

7. 大型科技公司积极参与抗击疫情，但承诺谨慎处理

用户数据。

8. 教育、医疗等在线服务规模化、常态化带来隐私

挑战。

9. 疫情下对“隐私”和“公共健康”的决策平衡，更

深层地反映了一国文化和认知传统。

10. 激进的“隐私争议性”管理措施的退出问题。如

果短期内不能退出，那么坚持必要性、最小化原则尤为重要。

**217**

**第五篇** **数据治理与政务数据规则**

**二** **、规则、做法与讨论**

**(一)个人信息保护法律不会妨碍疫情管理措施**

疫情背景下，控制疾病蔓延、保障公共健康毫无疑问成为更优先项。 欧盟数据保护委员会在《新冠病毒爆发期间处理个人数据的正式声明》中开 篇就表明： “数据保护规则(如 GDPR) 并不妨碍针对病毒大流行采取的措 施。与传染病作斗争是所有国家共同的宝贵目标，因此，应以最佳方式予以

支持。” 爱尔兰数据保护专员( Data Protection Commissioner ,

DPC)、 英 国 数 据 专 员 办 公 室 (Information Commissioner’s

Office,ICO) 和西班牙数据保护局 (Agencia Espanola Proteccion Datos,AEPD) 等各国数据保护机构也在各自的指南中提出了相同的观点。

《通用数据保护条例》(GDPR) 第6条、第9条为公权力机关(如公共 健康机构)处理个人数据乃至敏感个人数据提供了正当化的依据，如果数据 处理是为了公共利益 (Art.6.1.e, 如控制流行病及其传播)或者处理对于 保护数据主体或另一个自然人的核心利益是必要的(Art.6.1.d), 那么数

据处理可以不经当事人同意(2|。

[1]See European Data Protection Board(2020),Statement on the processing of personal data in the context of the COVID-19 outbreak,available

at:https://edpb.europa.eu/our-work-tools/our-documents/other/

statement-processing-personal-data-context-covid-19-outbreak\_en。

[2]See agencia espanola proteccion datos(AEPD)(2020),Report from the State Legal Service Deparment(The Spanish DPA)on Processing

Activities Relating to the Obligation for Controllers from Private Companies and Public Administrations to Report on Workers Suffering from Covid-19,available at:<https://www.aepd.es/es/prensa-y>-

comunicacion/notas-de-prensa/la-aepd-publica-un-informe-sobre-los-

tratamientos-de-datos-en。

**2I8**

数据治理：数据政

**(二)法律基本原则仍应得到遵循**

与此同时，欧盟各国的数据保护机构也强调， GDPR 以及其他法律确定的 隐私保护原则仍然需要被遵守。爱尔兰“数据保护专员的疫情指南”明确了 透明性、机密性、数据最小化等合规性要求，该“指南”要求收集数据的组 织必须以简洁、易于理解的语言向个人提供有关其个人数据处理的信息；任 何数据处理都必须以保证安全的方式进行3]。西班牙数据保护局的报告特别 指出，即使是在发生紧急卫生事件情况下，个人数据的处理也必须继续依照 目的限制、准确性等GDPR 和国内立法确立的原则；疫情之下仍然强调个人

信息保护原则与欧盟隐私文化传统的遵守。

**(三)疫情下信息收集与规范问题**

在许多国家，雇主是除卫生部门之外最主要的疫情信息节点，对雇主收

集信息的规范成为个人信息保护的重点。

疫情期间，除特定的公权力机关收集个人信息之外，雇主是最主要的收 集渠道。在欧洲很多国家的社会组织中，社区地位被弱化，因此，雇佣关系 构建了主要的信息网络节点。正因如此，欧盟成员国的法律规制大多关注雇 主与雇员间的个人信息处理。然而，各国目前在基本共识之外，在具体规则

上存在分歧。

在雇主是否可以主动收集雇员个人健康信息的问题上，法国国家信息与 自由委员会(CNIL) 对雇主提出了严格要求。雇主不得系统地、普遍地或通

过个人询问收集雇员及其亲属与新型冠状病毒感染有关的信息。非法处理的

[3]See Ireland Data Protection Commissioner,Data Protection and COVID-19, March 062020,available at:<https://dataprotection.ie/en/news-media/>

blogs/data-protection-and-covid-19。



**第五篇** **数据治理与政务数据规则**

示例包括：强制性地每天测量每个员工和访客的温度，从所有员工那里收集

医疗档案或问卷[4]。

**219**

相比之下，更多国家在这个问题上采取了较为平和、中立的立场。雇主 在遵守相应原则、限制的前提下，出于对工作场所健康、安全的考虑，可以 收集雇员以及访客的个人健康数据。英国数据专员办公室认为，雇主可以要 求雇员或访客告知其是否曾经去过特定国家或是否有感染症状(但不能要求 提供详细的旅行行程)。在不超出所需范围并确保所收集的任何信息都得到

适当保护的前提下，雇主可以收集特定的健康数据15]。

在是否以及在如何公开确诊员工个人信息的问题上，英国“数据专员办 公室”、爱尔兰“数据保护专员办公室”及德国“联邦数据保护与信息自由 专员办公室”都指出，若有员工被确诊或者被判定为疑似病例，出于公共健 康的考虑，雇主应当告知全体员工，以便及时采取防护措施，但在一般情形 下应避免通过公布姓名等方式让其他员工对应到具体的个人。对于非确诊或

疑似病例雇员，雇员在家中隔离不需要说明具体原因。

**(四)疫情推动跨部门数据共享**

及时、准确、充分的信息共享可以有效助力疫情决策与防控。但整体而言， 许多欧盟成员国仍将疫情健康数据限制在公共卫生部门范围内。法国国家信

息与自由委员会指出，卫生部门可以收集健康数据，并有资格采取适合于具

[4]See Commission nationale de l'informatique et des libertes,Coronavirus (Covid-19):les rappels de la CNIL sur la collecte de données

personnelles,March 062020,available at:<https://www.cnil.fr/fr/> coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-

personnelles。

[5]See UK Information Commissioner's Office,Data protection and

coronavirus;what you need to know,<https://ico.org.uk/for>-

organisations/data-protection-and-coronavirus/(last visited on March

302020):

**220**

数据治理：数据政

体情况的措施16)。西班牙数据保护局同样认为，公共卫生部门是受命收集和 管理与病毒传播有关的健康数据的组织，其他个人数据处理者需要遵循公共

卫生部门的指示7)。

很多国家都试图通过紧急状态下的立法打通信息共享通道。2020年，意 大利政府发布的最新法令授权公共卫生部门和民防部门之间数据共享，以管

理紧急情况。

美国卫生与公共服务部(U.S .Department of Health and Human Services,HHS) 于2020年3月发布公告：将在全国范围的公共卫生紧急状

态期间，在特定情形下豁免《健康保险流通与责任法案》隐私规则( Health

Insurance Portability and Accountability Act,HIPAA) 的制 裁和处罚18]。允许医疗服务提供者在公告列举的情况下，无须新冠病毒感染 者授权即可将其健康信息共享给执法机构、护理人员、其他急救人员和公共卫

生部门19]。

[6]See Commission nationale de l'informatique et des libertés,Coronavirus (Covid-19):les rappels de la CNIL sur la collecte de données

personnelles,March 062020,available at:<https://www.cnil.fr/fr/> coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees- personnelles。

[7]See agencia espanola proteccion datos(AEPD)(2020),Report from the State Legal Service Deparment(The Spanish DPA)on Processing

Activities Relating to the Obligation for Controllers from Private Companies and Public Administrations to Report on Workers Suffering from Covid-19,available at:<https://www.aepd.es/es/prensa-y>-

comunicacion/notas-de-prensa/la-aepd-publica-un-informe-sobre-los- tratamientos-de-datos-en。

[8]See U.S.Department of Health and Human Services(2020),COVID-196

HIPAA Bulletin:Limited Waiver of HIPAA Sanctions and Penalties during a Nationwide Public Health Emergency,available at:https://www.hhs.

gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver- bulletin-508.pdf。

[9]See U.S.Department of Health and Human Services,Office for Civil

t9r:le

available at:<https://www.hhs.gov/sites/default/files/covid-19-hipaa>- and-first-responders-508.pdf。



**第五篇** **数据治理与政务数据规则**

221

**(五)相比亚洲，欧盟对利用位置数据识别确诊患者更为谨慎**

尽管面临很多争议，但许多国家已经启动了基于位置信息的追踪，以发 现人员流动和传染源位置，以此来了解病毒状况并抑制病毒传播，但具体措

施的激进程度有所不同。

韩国、新加坡等国家在疫情初期就采取了基于位置信息的管控措施，这 些措施大部分具有很强的“隐私侵入性”。在韩国，政府机构利用智能手机 定位数据和信用卡购买记录，帮助追踪新冠病毒患者最近的活动，并建立病

毒传播链[10]。

韩国政府机构广泛的权力来自近年来对传染病立法的修订()。2015年， 传染病中东呼吸综合征(MERS) 爆发后，韩国的病例数量仅次于沙特阿拉伯， 位居全球第二。政府被批评隐瞒包括患者轨迹在内的相关信息。此后，韩国 修订了《传染病控制和预防法》(Infectious Disease Control and Prevention Act,IDCPA),该法第76 - 2(2)条赋予卫生部长广泛权力， 可以在没有授权的情形下收集已经确诊和潜在患者的个人数据；私人电信公 司和国家警察局应按照公共卫生机构的要求与其共享患者和潜在患者的位置 信息。第6条和第34-2条专门规定公众的“知情权”,要求卫生部长立即向 公众披露传染病患者的移动路径、运输工具和接触历史等信息。因此，当检 测到新病例时，韩国政府会向公众发送警报短信，同时在网站上公布感染者

被收治前的详细行程信息，以提醒访问过该区域的人监视和报告疑似症状[12]。

[10]<https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance>-

tracking-privacy.html。

[11]<https://www.lawfareblog.com/lessons-america-how-south-korean>-

authorities-used-law-fight-coronavirus。

[12]See Nemo Kim,More scary than coronavirus:South Korea's health

alerts expose private lives,March 052020,available at:https:// www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus- south-koreas-health-alerts-expose-private-lives。

**222**

数据治理：数据政

类似地，新加坡也推出了一款称为 TraceToge ther 的应用程序，使 用蓝牙信号探测附近的移动电话，如果一名该应用程序的用户后来检测出新 冠病毒阳性，卫生当局可能会检查该应用程序的数据日志，以找到与他曾经

接触的人[13]。

相比于亚洲国家，欧盟国家在位置信息的处理与使用上非常谨慎，目前 主要集中于地理位置信息的匿名化数据、聚合数据分析。欧盟数据保护委员 会在《新型冠状病毒爆发期间处理个人数据的正式声明》中提出建议，公共 机构应首先寻求以匿名方式处理位置数据，生成有关特定位置移动设备集中 度的报告。如果不可能仅处理匿名数据，那么成员国可以依据《电子隐私指令》 的第15条 (ePrivacy Directive) , 在采取适当保障措施、遵循比例原

则的前提下，采取立法措施对非匿名位置数据进行处理(14。

在此框架下，意大利数家电信公司已经通过其行业协会向意大利政府提 供了匿名用户位置数据集[15]。德国移动运营商德国电信宣布其已将用户的 移动数据匿名共享给联邦政府下属的罗伯特·科赫研究所 (Robert-Koch

Institute), 以统计德国公民在多大程度上遵循政府的抗击疫情政策[16]。

[13]See Saheli Roy Choudhury,Singapore says it will make its contact

tracing tech freely available to developers,available at:https://

www.cnbc.com/2020/03/25/coronavirus-singapore-to-make-contact-tracing- tech-open-source.html(last visited on March **302020)。**

[14]See European Data Protection Board(2020),Statement on the processing of personal data in the context of the COVID-19 outbreak,available

at:https://edpb.europa.eu/our-work-tools/our-documents/other/

statement-processing-personal-data-context-covid-19-outbreak\_en。

**[15]**See Facebook:Italian Ministry seeks to leverage big data with help

from Facebook and telcos,available at:https://privacyinternational. org/examples/3421/facebook-italian-ministry-seeks-leverage-big-data-

help-facebook-and-telcos(last visited on March **302020)。**

[16]See Coronavirus:Deutscher Mobilfunkbetreiber gibt Bewegungsdaten

weiter,available at:<https://frask.de/coronavirus-deutscher>-

mobilfunkbetreiber-gibt-bewegungsdaten-weiter/(last visited on March

**302020)。**

**223**

**第五篇** **数据治理与政务数据规则**

近期，欧盟委员会敦促与德国电信、法国Orange 、 意大利电信、西班牙电信、 沃达丰等欧洲电信运营商共享来自该地区的移动手机匿名元数据，以帮助预

测这种新型冠状病毒的传播[17。

截至目前，对位置信息的利用方式上的差异，典型地反映了不同国家对 待隐私问题上的不同态度。韩国、新加坡针对个体的位置信息的处理，在欧 盟国家来看显然有着“难以逾越的规则和文化障碍”。但随着疫情蔓延，态 势走向严重，欧洲国家也开始探索折中方式。英国政府与牛津大学研究人员 合作开发智能手机跟踪系统应用程序，以提醒与感染者接触的人118]。该应用 程序将与国家卫生服务局(National Health Service) 相关联。同时， 为做好隐私平衡，该应用程序依靠公众自愿分享位置数据，但不会仿照韩国

发布感染者的活动路径。

**(六)随着疫情升级，更具争议性的面部识别、无人机投入应用**

除了位置信息应用，面部识别、无人机、热成像相机等人工智能技术在 疫情之下也被广泛采用。这些技术可以有效减少人与人的接触，及时发现体

温异常、已被感染者，并监督公民减少外出。

在美国，总部位于奥斯汀的雅典娜安全公司(Athena Security) 表 示，其产品安全摄像头可以使用热成像和计算机视觉技术来检测疑似感染的

发烧患者[19]。这些摄像头可以探测到身体12个不同部位的热度，精确度在1℃

[17]See Mark Scott,Laurens Cerulus and Laura Kayali,Commission tells

carriers to hand over mobile data in coronavirus fight,available at: <https://www.politico.eu/article/european-commission-mobile-phone-data>-

thierry-breton-coronavirus-covid19/(last visited on March 302020)。

[18]See Jennifer Valentino-DeVries,Translating a Surveillance Tool into

a Virus Tracker for Democracies,March 1**92020,** available at:https://

www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html。

[19]See Mark Sullivan,Updated:This AI camera detects people who may have

COVID-19,March 19 **2020,** available at:https://www.fastcompany.

com/90479220/this-ai-camera-detects-people-who-may-have-covid-19。

224

**数据要素**

数据治理：数据政策发展与趋势

以内。同时，它使用人工智能模型来放大受试者的肉眼，因为肉眼最能反映 人体的实际温度。与每次只能在近距离工作的体温计不同，雅典娜安全公司 的安全摄像头探测系统更适合扫描机场、超市、医院等人员聚集的场所，其 每小时可以读取1000个温度。该公司的热成像相机已经在美国得克萨斯州奥 斯汀的部分办公场所投入使用，并将于未来几周内部署在一些大型企业和机 场。为缓解隐私担忧，雅典娜公司强调，它的系统不会记录从镜头捕捉到的

面部数据，也不会记录捕捉到的皮肤颜色。

在欧洲，伴随着感染人数和死亡人数的激增，无人机正越来越多地被应

用于政府防疫政策的落实。在法国，警方已经开始使用无人机，以加强公园 等公共场所的锁定与监督。在英国，北安普敦郡的警察正计划扩大无人机队 的规模，并为其配备扬声器，以传播公共信息，提示人们回到室内。在意大利， 为有力地执行限制措施，航空管理局 (ENAC) 授权意大利警方使用无人机监

督市民活动(20)。无人机同样出现在西班牙马德里的街头。

人工智能技术的应用虽然会引发公众对隐私的担忧，但是在新型冠状病 毒死亡率和感染人数持续攀升，公共卫生系统早已超负荷的背景下，为加大 政府防疫措施的执行力度，这些技术应用也被列入应对措施清单。但在另一 方面，为将此类应用限制在必要的范围内，应在事前予以评估，并制定相关

规范，在特定期限内及时删除相关数据。

**三、大型科技公司积极参与抗击疫情，但承诺谨慎处理用户数据**

大型科技公司积极参与疫情抗击，提供资助、开放算力资源乃至直接参

**[20]**See Sharon Braithwaite,Italian police can now use drones to monitor people's movements,aviation authority says,March 242020,available at:<https://edition.cnn.com/world/live-news/coronavirus-outbreak-03>-

24-20-intl-hnk/h\_b5c13ce244635abe5b945f6462b4a374。

**225**

**第五篇** **数据治理与政务数据规则**

与医疗物资生产(特斯拉公司切换部分汽车生产线生产呼

吸机)。据《华尔街日报》报道，美国政府主动寻求与微软、

谷歌、Facebook 等科技企业就新型冠状病毒的预防控制

展开合作。但截至目前，这些公司对用户数据仍然保持十

分谨慎的态度， 一般采取匿名化或聚合数据来提供趋势分

析。

1. 谷歌公司。谷歌母公司Alphabet 旗下的Verily

推出测试网站，美国加利福尼亚州用户可以在该网站上填

入位置等相关信息，随后会被筛选指引到最近的新型冠状

病毒测试地点。针对用户使用谷歌账户登录该服务而产生

的隐私担忧，谷歌公司声明： “用户提供的信息可能与收

集用户标本的卫生保健机构等机构共享。但所有数据都是

单独存储的，与谷歌公司的任何产品和服务都没有关联，

数据也不会用于广告目的。”

2. 苹果公司。苹果公司与美国疾病和预防控制中心

(Centers for Diease Control and Prevention,

CDc)、 白宫冠状病毒工作组(the White House

Coronavirus Task Force) 和联邦紧急事务管理局

(FEMA) 合作推出了一款应用程序(包括网站),用户可

以在上面回答有关症状、密切接触史等问题，应用程序会

根据美国疾控中心的指南基于用户的回答告知其如何密切

监测症状，是否应进行核酸检测或就医等信息。苹果公司

承诺：该应用程序和网站旨在保护所有用户数据的私密性

和安全性，这些工具不需要登录或与用户的Apple ID关

联，并且用户的个人回复不会发送给苹果公司或任何政府

组织。

 **226** **数据要素**

数据治理：数据政策发展与趋势

3.Facebook 公司。Facebook 也考虑匿名化分析数百万用户的 活动，以确定病毒是如何在美国蔓延的，并衡量社交距离措施 (social

distancing) 的有效性。这些结果可能会与政府机构分享，以阻止未来几 周可能出现的紧急情况。此外， Facebook 也为意大利政府提供匿名数据协 助，同时也为哈佛大学公共卫生学院等科研机构提供汇总和匿名化的流动性 数据与人口密度图，以帮助他们建立病毒传播的预测模型。在提供匿名数据时，

科技公司强调不会收集任何有关用户的识别信息，也不是为了长期跟踪用户。

也有一些大型平台在做好隐私保护的前提下，向用户提供疫情相关预警 帮助。优步(Uber) 向消费者发出了额外的隐私通知，称只要发现有乘客或 司机感染新型冠状病毒，优步就会在确定的时间内通知与该车辆有过联系的

司机和消费者。

**(七)教育、医疗等在线服务常态化带来的隐私挑战**

疫情之下，不少国家选择暂时关闭学校，停止面授教学活动，取而代之 的是远程在线教育。线上教育一方面缓解了疫情对学生学业的影响，另一方

面也引发了学生对隐私保护的担忧。

在美国，考虑到数千万学生在学校停课后上网学习， 一些美国参议员正 敦促政府采取措施保护学生个人数据。参议员指出：许多在线教育课程收集 了大量的学生数据，却没有采取足够的隐私或安全措施。教育软件行业普遍 缺乏透明度，在隐私和安全方面的做法也不一致。美国联邦调查局( FBI)

警告称，对学生数据的非法利用可能导致霸凌、追踪、身份盗窃及其他针对

儿童的犯罪l21]。

[21][See pttps://www.washingtonpost.com/education/2020/03/24/senators-urge](Seepttps://www.washingtonpost.com/education/2020/03/24/senators-urge)- trump-administration-protect-student-data-rush-online-schooling/(last

visited on March 302020)。

**227**

**第五篇** **数据治理与政务数据规则**

美国教育部下属的学生隐私政策办公室( Student Privacy Policy office,SPP O) 发布了疫情期间针对学生网上教育的指导12)。其中强 调，学校或教育机构在线上教育过程中处理学生教育记录中的个人身份信 息 (PII) 时，需要严格依照《家庭教育权和隐私权法案》(FERPA) 的

规定。同时，根据隐私技术中心(P rivacy Technical Assistance

Center) 的建议，教育机构应以易读易懂的方式向学生和家长传达其私隐政 策，不应削弱学生在家上网课的隐私保护，不得出售或以其他方式利用学生

数据牟利(23)。

与此同时，远程医疗也因其减少人员接触、避免医院人满为患而被推 荐。为鼓励远程医疗，美国卫生与公共服务部在2020年3月发表声明：将在 疫情期间免除部分远程医疗服务违反《健康保险流通与责任法案》隐私规则 的处罚(24)。这种豁免适用于基于任何理由提供的远程医疗，无论其是否与 新型冠状病毒的诊断和治疗有关。该声明还鼓励医疗服务提供者使用Apple FaceTime 、Facebook Messenger Video Chat 、Google Hangouts Video 、Skype 等主流视频通话应用程序开展远程医疗，而无须担心受到惩处。 对于该举措，世界隐私论坛表示支持，但同时也呼吁提供远程医疗服务的科

技公司对于病人医疗数据保持克制，保障其安全性。

**[22]**See Student Privacy Policy Office(March 2020),FERPA 8 Coronavirus Disease **2019** (COVID-19)Frequently Asked Questions(FAQs),available

at:<https://studentprivacy.ed.gov/sites/default/files/resource>\_

document/file/FERPA820and820Coronavirus%20Frequent1y;20Askedi20

Questions\_0.pdf。

[23]See Student Privacy Policy Office(2014),FERPA and Virtual Learning Related Resources <https://tech.ed.gov/wp-content/uploads/2014/09/>

Student-Privacy-and-Online-Educational-Services-February-2014.pdf。

**[24]**See Department of Health and Human Services,Office for Civil Rights,

Notification of Enforcement Discretion for Telehealth Remote

Communications during the COVID-19 Nationwide Public Health Emergency,

ergenct-a-ts-ic-ial-

telehealth/index.html。

**228**

**数据要素**

**数据治理：数据政策发展与趋势**

在此次疫情推动之下，教育、医疗行业所涉及的未成 年人、医疗等敏感个人数据，将可能迈向大规模的、常态 化的收集处理模式，对该领域的隐私和数据安全带来了全

新挑战。

**(** **八** **)** **“隐私”与“公共健康”的决策平衡**

疫情下对“隐私”和“公共健康”的决策平衡，更深

层地反映了相应国家的文化和认知传统。

数据共享、位置信息追踪、人工智能技术等数字科技 的规模化应用在有效抑制新型冠状病毒快速传播方面发挥 了积极作用。然而，即使是同一种技术应用，各国在接受 程度和推广范围方面也存在巨大差异，韩国、新加坡、中 国为代表的亚洲东方国家和西方国家的差异更为明显。有 观点认为，这种差异往往根植于不同地域、文化体系和认

知传统。

在外在“法律形式”上，韩国、新加坡接近于欧盟， 但其隐私观念的内核仍然是东方式的。韩国、新加坡的《个 人信息保护法》几乎都是以欧盟的GDPR 为模板的，特别 是近年来，韩国积极争取欧盟对其个人信息保护法律制度 的认可。2018年11月，韩国议会提交了个人数据保护法 修订，新的修订将使韩国数据保护执法系统获得独立地位， 有望为韩国期待已久的欧盟白名单充分性认定铺平道路。 但通过疫情可以看到，尽管具备形式上的相似性，但植根

于社会文化的隐私观仍有着巨大的不同。

**229**

**第五篇** **数据治理与政务数据规则**

新加坡、韩国等亚洲国家深受中国儒家文化的熏陶，集体主义是人们思 想观念的一部分。当与公共利益关联更为密切的“健康”和更加注重私人自 由保护的“隐私”两种价值发生冲突的时候，东亚区域的民众人更倾向与将 重心放在公共利益上。普通网民也利用政府网站披露的患者数据，甚至会通

过“人肉搜索”等方式识别和追踪特定个人。

而对于欧洲国家而言，深厚的隐私文化传统早已被立法者融入GDPR 等 隐私保护规范中。面对数字化技术，强大的隐私观念让欧洲人犹豫不前。即 使企业向政府共享的位置信息已经经过匿名化处理，欧洲的官员们仍然对未

来可能出现的大规模监视表示担忧(251

**(九)激进的“隐私争议性”管理措施的退出问题**

截至目前，法国、西班牙等60多个国家已经(或曾经短期地)宣布了战 争状态或者紧急状态。在战争状态或紧急状态下，自由民主秩序被暂时中止， 激进性的管理措施大大扩展了国家的权力并限制了个人的权利126]。不能否 认，这些措施在应对公共健康危机中是必要的。然而与此同时，也需关注危 机结束后，各国将如何从这些激进的管理措施中退出。有学者表达了这样的 担忧——人们越来越依赖数字工具来监测疾病的传播，在健康危机消退之后，

如何防止政府使用这些工具来追踪个人或用于其他目的?(27

[25]See Dave Perera,Matthew Newman,and Hyung-jo Choi,Covid-19 pressures privacy as pandemic spreads globally,March 192020,available at:

<https://mlexmarketinsight.com/insights-center/editors-picks/Data>-

Protection-Privacy-and-Security/cross-jurisdiction/covid-19-pressures- privacy-as-pandemic-spreads-globally。

[26]See Cas Mudde,Coronavirus outbreak 'Wartime'coronavirus powers could hurt our democracy -without keeping us safe,March 242020,https:// www.theguardian.com/commentisfree/2020/mar/24/wartime-coronavirus-

powers-state-of-emergency。

**[27]**See Michael Pisa,COVID-19,Information Problems,and Digital

Surveillance,March 202020,available at:<https://www.cgdev.org/blog/> covid-19-information-problems-and-digital-surveillance。

**230**



**数据要素**

数据治理：数据政策发展与趋势

人类社会已经迈向了史无前例的数字化进程， Statista 统计表明，目 前全球智能手机用户的数量为35亿，这意味接近一半的世界人口拥有智能手 机，且这一数字仍在飞快上涨。如果被允许的话，不仅电信运营商能够精确

跟踪用户，智能手机上基于位置信息的应用也能使跟踪识别发挥到极致。

目前来看，东亚国家或地区对疫情的处理明显好于欧美国家。韩国已经 阶段性地渡过最艰难的时期，新加坡等其他亚洲国家也在很大程度上控制了 疫情，这其中部分得益于早期实施的数字技术应用，但在疫情结束之后也仍 需反思和重新评估相关应用的合理性，在隐私和“公共健康”之间重新确立

平衡点，防止紧急措施的“常态化”。

对此，全球发展中心 (Center of Global Development,CGD) 提出建议：如果社会一致认为在危机时期制定绕过同意的措施是合法的，那 么一旦情况发生变化，就必须有适当的机制来放松这些措施。世界卫生组织 (WHO) 应敦促各国政府制定相应条款，并保证在特定时候自动终止紧急监

视措施[28]。

而在尚未看到全球疫情结束的曙光之前，利用用户数据的疫情管控措施

仍然应当坚持最小化和必要原则，并防止利用于其他目的。

**[28]**See Michael Pisa,COVID-19,Information Problems,and Digital

Surveillance,March 202020,available at:<https://www.cgdev.org/blog/> covid-19-information-problems-and-digital-surveillance。



**第五篇** **数据治理与政务数据规则**

231



**第20章**

**“健康码”折射政务服务数据规则**

**摘要：**疫情中的“健康码”应用可以视为“数字治理”

的一场大型综合试验。依托数据资源汇聚、数字技术支撑

和产品思维驱动，传统基于科层上报制的管理模式演化为

多方参与的、动态精准化的数字治理，通过“数据流”牵

引带动真实世界中“人流”“物流”“商流”的复苏与回归，

实现了国家治理现代化的一次跃升。

“健康码”治理模式在未来可能复用至其他政务管理

议题，这要求我们深度反思“健康码”的经验与不足，为

数字治理的持续化发展塑造良好的规则框架。本文围绕“健

康码”中最具有争议性的话题——个人信息保护，从政务

数据规则视角提出相关建议，提出在《个人信息保护法》

立法中，应将政府部门全面纳入制度体系，为政府部门发

起数字治理提供正面的法律指引，并参考国际通行做法，

区分“数据控制者”和“数据处理者”的角色，建立各司

其职、权责有序的数字治理生态。

**232**

**数据治理：数据政**

一 、解决“个人信息保护”问题，需厘清

各方的角色与责任

[29]2020年2月9日 腾讯正式推出“防疫 健康码”,简称健康码， 后经多次升级，现在 被广泛应用。

[30]2020 年2月7日， 阿里巴巴协助杭州市 政府推出“余杭绿码”, 随后快速升级，于2 月17日在支付宝平台 上运行，并广泛应用。

目前，关于“健康码”个人信息保护问题的讨论多止 步于现象本身，包括过度收集个人信息、信息不准确、如 何保障用户申诉权、存在信息泄露风险等，但忽略了最为 关键性的责任主体问题。要明确这一问题，就需要厘清“健 康码”的性质与各方角色。“健康码”最早孵化于腾讯291

阿里巴巴130)等互联网企业政务服务基础架构。

在疫情发展初期，凭借对用户需求痛点的敏锐把握， 企业快速响应政府需求，在政务服务平台入口开辟疫情相 关功能服务。2020年1月31日，用户通过广州政务微信 小程序“穗康”,可申报登记14天内离返情况及健康状况， 并可预约购买口罩；2月9日，深圳市成为全国首个疫情 期间凭“码”出行的城市；2月11日，杭州实施绿、红、 黄三色动态码管理。精准、高效的数字管理方式，很快在 国家层面得到回应和推进。2月25日，国务院印发《关于 依法科学精准做好新冠肺炎疫情防控工作的通知》,明确 鼓励有条件的地区推广个人“健康码”等信息平台；2月 29日，国家政务服务平台推出“防疫健康信息码”,利用 汇聚的卫生健康、民航、铁路等数据，提升“健康码”的 覆盖范围和准确度。3月20日，国家卫生健康委员会宣布 大力推动各地互认互通工作，目前，全国绝大多数地区的

健康通行码可以实现一码通行。

从发端到全面推进，“健康码”深度融入了政府部门(这

里的政府部门涵盖了国务院、各地地方政府，以及深入社



**第五篇** **数据治理与政务数据规则**

区的街道办事处等各级政府部门)、互联网企业、电信运

营商、事业单位等诸多公、私主体，围绕“健康码”的个

人信息保护职责如何在上述主体之间分配和界定，关系到

相关问题能否得到根本性解决。

**233**



二、“健康码”本质上是政务服务，

政府扮演数据控制者角色

从当前国际主流的个人信息保护法律所采纳的数据控

制者、数据处理者二维规制主体框架入手，可以为“健康

码”有效划定各方责任边界提供参考。政府部门在“健康

码”政务服务中处于“数据控制者”角色(以下简称控制

者)。同其他数字政务项目一样，“健康码”是政府部门

在疫情特殊时期发起的数字化管理项目。政府在“健康码”

中扮演了强有力的角色，是疫情和复工管理的需求方、发

起方、推动方和最终实现方。政府部门决定了“健康码”

应用中数据采集的类型、内容、使用方式和用途。参与“健

康码”应用的企业，为政府部门推进实施“健康码”提供

技术支撑服务，属于“数据处理者”(以下简称处理者)。

科技企业可凭借平台优势为用户提供快捷入口，如微信小

程序、公众号以及各大主流App 均提供了“健康码”入口，

让用户方便地获取“健康码”服务，并通过云计算技术为

数据处理提供高效支撑，例如在“防疫健康信息码”小程

序界面提示：本防疫健康信息码服务由国家政务服务平台

提供……中国电子科技集团提供了相关技术支持。

**234**

**数据治理：数据政**

**三、区分“控制者”和“处理者”** ,

**将为数据处理活动提供更明确的法律指引**

在早期的个人数据保护法律中，并没有控制者和处

理者的明确分野。1995年欧盟《个人数据保护指令》 (Directive 95/46/EC) 主要适用于控制者，处理者通 过合同来承担数据保护责任。然而，随着数据治理生态卷 入更多主体，数据处理越来越专业化和细致化，特别是随 着云计算的发展壮大，作为专门提供数据处理服务的业态， 虽然不能决定数据处理目的，但参与了数据处理，有必要 在法律上明确其独立的法律地位和义务责任。作为1995 年《个人数据保护指令》的立法改革，欧盟在2018年的 《通用数据保护条例》 (General Data Protection Regulation,GDPR) 中正式采用了控制者和处理者的二 分划法。GDPR下的数据控制者是指负责决定个人数据处 理目的与方式的主体，处理者是指受控制者委托而处理个 人数据的主体。GDPR 细致规定了控制者和处理者之间的 数据处理合同应当至少包含哪些内容，包括数据处理的目 的、期限、个人数据的类型以及双方的权利义务。数据处 理者仅能按照数据控制者书面的要求处理数据，必须确保 其员工能够遵守有关保密的要求；在数据安全、数据泄露、

数据保护影响评估等方面为数据控制者提供必要的协助。

**235**

**第五篇** **数据治理与政务数据规则**

四、“健康码”政务项目中的政府

和企业的责任与边界

在清晰厘定“健康码”各方的法律主体地位后，将会

更加明确自身义务和责任，保护公民的个人信息权利，保

障数据安全。

**(一)“健康码”遵循的基本原则**

作为“数据控制者”的政府部门，应当在“健康码”

政务项目中践行数据保护基本原则，包括如下5个方面。

(1)合法正当原则。当前在疫情特殊时期，为保护公

众生命健康，政府部门可依据《传染病防治法》《突发公

共卫生事件应急条例》的相关授权，收集并处理相关信息。

2020年2月5日，习近平总书记在中央全面依法治国委员

会第三次会议发表重要讲话。他强调，要全面提高依法防

控、依法治理能力，为疫情防控工作提供有力的法治保障。

(2)目的明确、必要、最小化原则。政府部门作为

控制者，在确立数据收集范围和使用方式时，应当限制在

疫情相关的必要范围内。例如，工业和信息化部指导下的

行程自主查询短信和“行程码”,不再收集用户的身份证号、

家庭住址等个人信息，实现最小化收集和处理。

(3)透明原则。当前，政府部门在推行“健康码”

的过程中，正在探索各类透明公开的方式，保障用户的知

情权。例如，上海市的“随申码”、广东省的“粤省事”

和贵州省“贵州健康码”在注册时需用户点击同意政府运

**236**

**数据治理：数据政**

营管理机构制定的用户协议和隐私政策；又如，深圳市政 府还专门编制了《操作指引》,向用户告知“健康码”汇

聚分析的数据类型、申诉渠道等。

(4)质量原则。目前大部分“健康码”应用服务都 可以为用户提供查看和更新入口。因疫情动态变化等原因， 可能会出现“健康码”信息不准确的情况，目前大部分地方，

用户可通过12345政务服务热线投诉申诉。

(5)责任和安全保护原则。 “健康码”汇聚了海量 公民个人信息，并且有相当敏感的医疗健康信息、轨迹信 息，这对数据安全提出了更高挑战。目前，各地所推行的“健 康码”应用大部分采取了“信息安全等级保护3级”以上 的安全保障措施，引入了包括加密存储、加密传输、访问

控制等安全措施。

**(二)“数据处理者”的责任义务**

作为“数据处理者”的企业主体，除遵守上述数据保 护基本原则外，还应根据自身的独特角色贯彻以下法律义 务：严格在政府受托范围内处理数据，数据不得用于企业 自身运营目的；承担相应的技术服务时，不得未经政府同

意就擅自转包。

237

**第五篇** **数据治理与政务数据规则**

五 、我国现有个人信息保护法律体系与

上述规范框架尚存差距

(一)政府部门尚未全面纳入个人信息保护

法律体系

首先，在刑事规范方面，我国虽然已将国家机关及其

工作人员纳入适用主体，但囿于刑事规范的狭窄性(主要

针对非法出售、非法提供、非法窃取(获取)等行为),

无法为政府部门处理个人信息提供正面的法律指引。其次，

在近年来出台的《网络安全法》《电子商务法》中引入了

国际通行的个人信息保护法律基本原则，但相关规范条款

着重于对网络运营者、电子商务经营主体适用，并不强调

适用于政府部门。国家标准《信息安全技术——个人信息

安全规范》虽然在适用主体上并不做区分，但其仍然属于

推荐性技术标准，对包括政府在内的各类主体并不具有强

制力。

而对比国际通行做法来看，毫无疑问政府是个人信

息保护法律体系中的重要适用主体。欧盟 GDPR的适用主

体涵盖政府部门、公共机构、司法机构及其他任何实体。

GDPR实施近两年来，政府部门也是个人信息保护的重要

监管对象。2019年9月，保加利亚国家税务局因业务流程

和 IT 系统不能满足合规要求致使公民数据泄露，被欧盟

数据保护机构处以290万欧元的罚款。而在美国，个人信

息保护立法更是发端于对政府机构的规制。美国现代意义

**238**

**数据要素**

**数据治理：数据政策发展与趋势**

上的个人信息保护法——1974年的《隐私法》,适用于联

邦政府部级以上机构收集与处理公民个人信息的活动。

**(二)二元主体有待引入**

我国个人信息保护法律体系中还尚未引入“控制者” 和“处理者”二元主体。如上所述，对“控制者”和“处理者”

法律角色进行区分，有利于数据生态各方主体各司其职，

建立有序的数字治理秩序。目前，对二者角色的区分已 经成为国际通说。欧盟的 GDPR以及受其影响的大多数国 家立法将二者区分出来。印度正在制定中的《2019年个 人信息保护法(草案)》也明确了二者的角色，用Data Fiduciary 和 Data Processor 分别指向控制者和处 理者。在我国目前的个人信息保护法律体系中，还尚未有 这种划分方法，可考虑借鉴引入。在这场前所未有的“疫 情大考”面前， “健康码”无疑是数字治理进入新阶段的 标志性案例。 “健康码”中围绕个人数据保护的相关问题， 通过这场抗疫实践得以显现，应当通过制度规则构建予以 补齐。建议正处于立法进程中的《个人信息保护法》在规 范主体上正式纳入政府部门，并区分控制者和处理者，明

确各方的角色与责任。

239



**后** **记**

2017,我的第一本关于数据的专著《大数据时代：数据保护与流动规则》 出版。彼时， “大数据”概念风头正劲，围绕数据收集、利用、交易等价值 挖掘如火如荼，与此同时，产业界、政府部门对于数据利用规则的了解需求 也呈现井喷的状态。因此专著定位于数据规则中最重要的内容之一——个人 数据保护规则及其法律规则，通过系统梳理各国数据保护监管体制、法律法规， 并结合具体案例的方式，全面介绍了个人数据保护与流动规则，推动数据合

规思维的普及。

三年来，“大数据”依然是数字经济炙手可热的发展领域，并与移动互动网、 云计算、物联网、产业互联网、人工智能的结合越来越紧密，演进到以数据 为关键生产要素的新阶段。同样，围绕数据规则的讨论，也从过去较为单一 的“个人数据保护规则”升维到更为宏大复杂的“数据治理”叙事，涉及数 据权属、数据竞争、数据共享、数据跨境流动、政府数据治理能力、国家数 字竞争力与数据安全等新议题，远远跳脱了个人视角，成为多利益、多因素

交织的新兴公共政策集合域。

正因如此，基于2017年专著基础上的修订，已远远跟不上实践的快速 发展，需要以出版新书的方式，围绕以上提及的数据治理新议题，系统梳理

近年来相关政策议题、发展趋势，并基于对数字经济发展的理解，提出产业

**240**

界的思考、观点与建议。

这本新书恰巧也与腾讯研究院发起的“数字经济‘路—油—车’系列丛书” (含《新基建》《数据要素》《产业互联网》三本书)计划相契合，并最终 作为这套丛书的组成部分得以出版。这本书集合了近年来个人在数据治理领

域的最新思考，并在这次出版中按照完整思路和框架得以呈现。

希望通过这本书能够对读者——不论是对于数字产业一线的同仁(律师、 法务、业务),还是政府部门、学界中关注数据治理政策的官员、学者，了 解数据治理领域公共政策发展与趋势带来帮助，如果能在此基础上，启发和 推动相关政策讨论走向深入。对于个人，更是幸莫大焉。本书中观点不成熟

甚至疏漏之处，也恳请各位专家予以批评指正。

最后，特别感谢我所供职的腾讯研究院———家致力于推动数字经济健 康发展的行业智库机构，基于她搭建的开放、多元、前沿化的研究平台，才 使得我们有机会将技术更迭、产业发展与公共政策研究紧密结合起来，共同 探究背后的趋势与规律。此外，还要感谢在不同阶段协助我开展资料收集整 理工作的实习生，他们分别是余春芳、朱家豪、郭雅菲，闫锦麟，他们参与

了本书部分文章的基础工作，在此一并表示谢意。

王融

2020年小暑，北京中关村

新基建、数据要素和产业互联网紧密相连、互相促进，三者 的紧密关系可类比为“路-油-车”,新基建是通往全面数字社会的 “高速公路”,数据是驱动数字经济发展的新“石油”,产业互 联网则是高效运行的“智能汽车”。

**数据要素**

**数据治理：数据政策发展与趋势**

◆研究了数据要素范畴的“数据权属”“数据保护”及其相关的法律、政策、技术及应用方面的 话题。

◆研究了数据权属问题的含义及其特征、个人数据的二元性(隐私性与经济性)。

◆分析了我国司法实践对企业数据财产利益的探索与确认。

◆分析了世界各国数据保护的做法，研究比较欧盟 GDPR 与美国加州 CCPA 两大体系。

◆分析了人脸识别、区块链、隐私计算等新兴技术领域带来的影响、挑战和机遇。

◆勾勒了全球数据跨境流动的政策景况。

令介绍了我国个人信息保护立法与实践的总体特征，以及我国数据治理方面的努力与成效。

◆介绍了各国抗击新冠疫情期间的数据采集、使用、保护与责权处置。

责任编辑：祁玉芹

封面设计：张祎桐

定价；58.00元