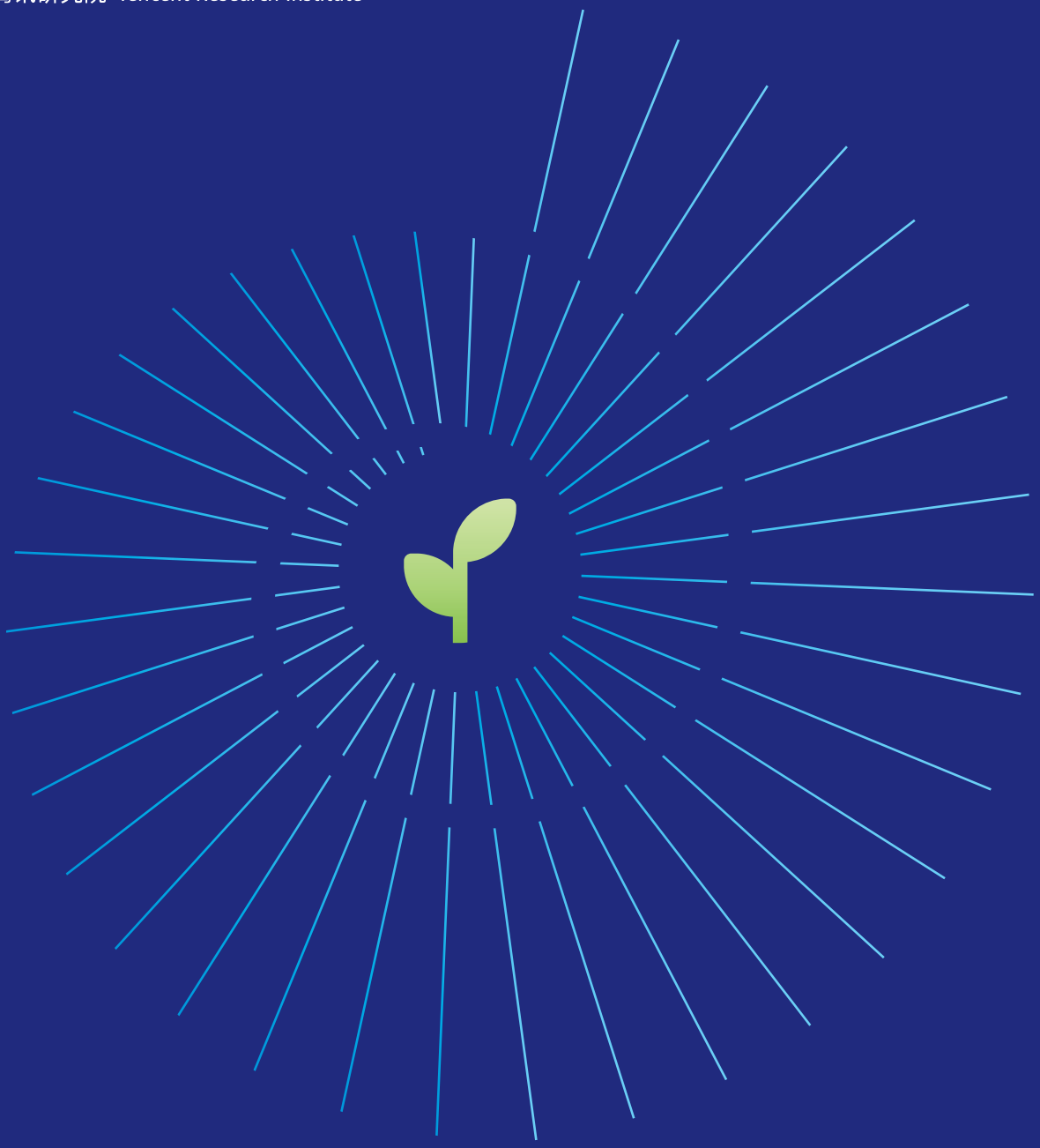
腾讯研究院

规则的激荡与新生

2020 年数据治理年度报告

腾讯研究院 Tencent Research Institute



引言

2020 年新冠疫情爆发，数字化转型按下快进键，社会运转加速构筑于数据之上。“健康码”等数字化疫情防控手段让“数据治理”不再是一个抽象议题，全民参与其中，切身体会“数据治理”体系作为数字社会基础性规范的重要性。

所谓数据治理体系，是指为实现数字社会可持续发展，围绕数据如何收集利用而搭建的公共政策框架体系。其核心是各方主体（包括政府部门、企业、消费者及社群机构等）关于数据收集与使用达成的基本共识、立场与规则方案。

为推进“数据治理”公共政策讨论，腾讯研究院从 2018 年起连续三年推出数据治理年度报告，搭建数据治理体系框架，识别关键政策议题，总结国际经验与差异，为数据治理的科学化、精细化发展提供研究基础。

2018 年，我们发布了业内第一部数据治理年度报告——《迷雾中的新航向》，全面展现了“数据治理”的全貌与重点，变革与走向。对数据主权、跨境数据流动、个人数据保护、数据权属、数据共享等从宏观到微观的重点政策议题展开深度分析。

2019 年，区别于 2018 年首期报告的综合性，回应年度重要关切：数据主权——国际执法协作领域的数据跨境获取问题，形成专题报告：《云深处的数据规则——CLOUD 法案与它的蝴蝶效应》。至此，数据治理已经走向了最为复杂的核心领域。

2020 年，数据治理规则继续在激荡中碰撞，各方主体的诉求表达更加清晰：个人视角下的以隐私保护为核心的数字权利规则诉求；产业视角下的数据创新与竞争规则诉求；国家视角下的数字经济竞争力和数据安全诉求；国际视角下的数据主权协调诉求。这四个视角彼此紧密联系、互动影响，共同推进数据治理向纵深发展。

2020 年“数据治理”年度报告——《规则的激荡与新生》，沿用目前业界形成共识的研究框架，从个人、产业、政府、国际四个视角，对八个核心议题：疫情下的数据治理、全球数据保护立法与监管、政务数据管理、人脸识别应用、隐私安全计算、数字广告行业、数据跨境流动、跨境执法数据调取，深度呈现在激荡和碰撞中逐步浮现的数据治理新规则。

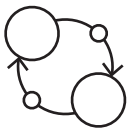
目录

2020 数据治理议题全景

2020 年，数据治理领域展现了更多的具体行动方案。在百年未有之大变局下，为抓住历史性发展机遇，各方主动提出规则方案，数据治理从混沌走向秩序重建。在规则的激荡与碰撞中，中国以开放心态，积极参与全球治理，对重大国际问题提出中国方案，并以其包容性为数字治理提供了新的选项。人类社会共同迈向数字时代，需携手共建彼此认同的数据规则，构建个人、企业、国家之间的信任基石，共享数字经济发展利益与社会福祉。

1 疫情下的数据治理——

“隐私保护”与“公共健康”的平衡



应对新冠肺炎疫情，各国就个人信息处理形成了诸多共识，但也存在明显差异。以“健康码”与“蓝牙追踪”为代表的“中心化”与“去中心化”两种数据处理方案，为疫情防控提供了科技助力。方案虽有不同，但其核心关切仍在于厘清公共卫生部门和私营部门的角色，二者应遵循相应的数据保护框架，实现个人隐私保护与公共健康管理之间的平衡。

2 全球数据保护立法与监管——

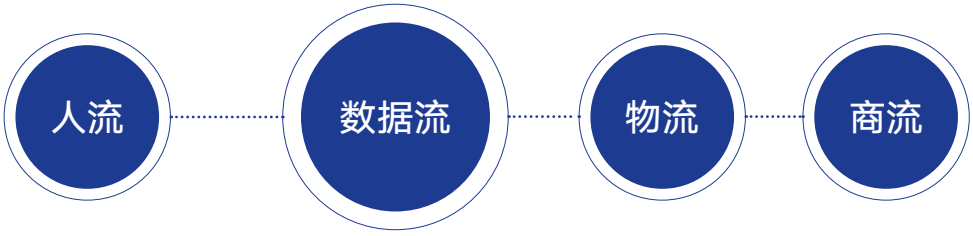
立法持续铺开，监管执法趋严

2020 年，作为数字时代的永恒话题，个人数据保护立法与执法继续在世界范围内铺开。新兴市场国家的数据保护立法接连生效，早期已出台法律的国家也陆续开启立法修订工作。我国《民法典》《个人信息保护法（草案）》的出台更为清晰地勾勒了个人数据保护的中国方案。在监管执法方面，欧盟数据保护执法的案件数量、罚款总额持续增长，我国则通过多种监管执法手段来推进数据保护。

3 政务数据管理——

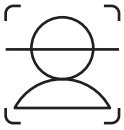
助力社会治理现代化，规范利用提上议事日程

以“健康码”的应用为代表，政务数据管理在疫情防控中发挥着重要的功能。依托数据资源汇聚分析、数字技术支撑和产品思维驱动，传统科层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，实现了社会治理现代化的一次跃升。



4 人脸识别——

未知与担忧并存



在疫情防控的背景下，人脸识别更广泛地应用在公共场所。对公众而言，人脸识别技术存在着大量未知，人们对于人脸识别的信息收集、运作机制、应用场景等缺乏足够的了解，因而表现出警惕和恐惧的心态，人脸识别面临着来自各方的质疑。在欧洲，虽然《人工智能白皮书》最终放弃一刀切禁止人脸识别，但如何规制人脸识别应用已无疑成为核心议题；美国部分州陆续通过立法对执法部门的人脸识别技术应用作出规范；在中国，人脸识别也成为了公众热议的话题，但尚未形成成熟的讨论框架。

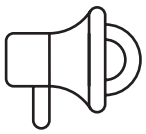
5 隐私安全计算——

开启数据价值创造新篇章

2020 年，“数据生产要素”深入人心。但“保护个人隐私”与“尊重他方数据权益”成为横亘在数据价值创造面前的两座大山，这一现实挑战促使业界尝试通过技术方案解决隐私安全和数据共享激励问题。以多方安全计算 (Secure Multi-Party Computation)、同态加密 (Homomorphic Encryption)、差分隐私 (Differential Privacy)、联邦学习 (Federated Learning) 为代表的隐私安全计算技术群落正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，2020 年被业界称为“隐私计算元年”。

6 数字广告行业——

“隐私保护”背后的商业模式之争

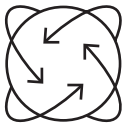


2020 年，数字广告行业酝酿着一场巨变。6 月，Apple 公司宣布了 iOS 14 一项新的隐私规则，App 开发者在对用户进行广告跟踪时需要事先取得用户的明确同意。此项新规的执行将可能导致数字广告行业收入的大幅降低。

Apple 新规引发了来自开发者的广泛质疑，Facebook 对此公开表达反对意见，由此展开了互联网不同商业模式的质疑与对峙——以 Facebook 为代表的 App 开发者通过免费服务获取流量，通过广告业务变现来覆盖运营成本并获取收入，即广告 + 免费服务模式；而 Apple 则通过对体系内 App 收费服务的抽成获得收入，因此鼓励 APP 采取收费模式。因此，这一规则调整的背后，除了消费者隐私保护缘由外，实质是两种不同数字商业模式之争。据 2021 年 1 月有关报道，Facebook 或将考虑就 iOS14 隐私新规及 App Store 有关规则对 Apple 提起反垄断诉讼。

7 数据跨境流动——

规则的“破”与“立”



2020 年，外部环境剧烈变化，围绕数据跨境流动议题的调整与探索更加深入。在海外，欧盟法院继“安全港”之后再度废除“隐私盾”，欧美跨大西洋数据传输需要新的协调。英国脱欧进程推进，其与欧洲大陆间的数据流动再添变数；在国内，《个人信息保护法（草案）》对个人数据跨境流动的未来制度方向有了更清晰的定位，各自贸港、自贸区陆续发布方案，均提出要创新跨境数据流动管理机制。《区域全面经济伙伴关系协定》的签订也将为我国在东亚地区的数据跨境流动注入新的活力。在数字全球化的主旋律下，跨境数据流动机制呈现更多探索与创新。

8 跨境执法数据调取——

全球治理呈现多样性

2018 年 2 月，美国通过了《澄清域外合法使用数据法案》，法案确立的跨境电子取证新模式对国际数据治理规则体系产生了长期而巨大的影响。2020 年，各国政府就该法案的谈判与对数据跨境执法机制的探索仍在争议中继续，英国和澳大利亚正在积极加入，欧盟对此展开谨慎评估。2020 年 9 月，我国提出《全球数据安全倡议》，在国际舞台上逐步形成更为清晰的立场表达——秉持多边主义，兼顾安全发展，坚守公平正义。

2020 数据治理时间轴

国际

1月

《加州消费者隐私权法案》

1月1日，《加州消费者隐私权法案》（California Consumer Privacy Act of 2018，简称 CCPA）正式生效[1]。加州隐私保护立法进程并未就此停止，同年11月3日，加州通过了《加州隐私权法案》（California Privacy Right Act，简称 CPRA），对 CCPA 进行了新的增补和改进，将于2023年1月1日生效[2]。

2月

《塑造欧洲数字未来》

2月19日，欧盟委员会发布《塑造欧洲数字未来》，明确将以“科技为人”“公平且自由竞争的数字经济”“公开、民主且可持续的社会”作为欧洲数字未来的发展方向[3]。同日，欧盟也发布了具体行动文件：《欧洲数据战略》和《人工智能白皮书》[4]。在最终版本的《人工智能白皮书》中，欧盟委员会改变了其在草案[5]中表明的“3到5年内禁止公共领域使用人脸识别技术”态度，将是否禁止人脸识别应用问题交由成员国自行决定。

3月

欧盟《关于 COVID-19 大流行下数据保护权的联合声明》

3月30日，第108号公约委员会主席与欧盟数据保护委员会委员共同发布《关于COVID-19大流行下数据保护权的联合声明》[6]，申明抗击新冠疫情中的数据保护共识与要求。继该声明之后，欧盟数据保护委员会也发布了多份涉及新冠肺炎疫情下数据处理问题的文件指南[7]。

4月

澳大利亚《电信立法修正案（草案）》

4月17日，澳大利亚参议院法案审议委员会对澳大利亚政府3月提交的《电信法修正案（草案）》进行了审议，该修正案旨在修订1979年制定的《电信（监听和访问）法》[8]。若修正案通过，澳大利亚将允许相关协议国的执法机关、国家安全机构直接访问位于澳大利亚境内的数据以进行执法活动，此举也为澳大利亚加入美国2018年3月出台的《澄清域外合法使用数据法案》（简称 CLOUD 法案）相关协议铺路[9]。此前，英国已于2019年10月与美国就《CLOUD 法案》达成协议[10]。

5月

苹果谷歌联手抗疫，蓝牙匿名追踪患者功能上线

5月20日，Apple公司在其iOS13.5系统更新中首次加入了“曝光通知”（Exposure Notification）功能[11]，此举是Apple与Google于4月10日宣布合作开发联系人追踪技术以抗击新冠肺炎疫情后的具体推进。此外，两公司将联手在iOS和Android系统中发布应用程序编程接口（API），并在确保隐私保护、透明度、个体同意的前提下，构建基于蓝牙的联系人跟踪机制以开展疫情信息交互[12]。

6月

欧盟《数据保护作为增强公民赋权和欧盟实现数字化转型的基础——GDPR实施两周年》报告

6月24日，欧盟委员会发布了题为《数据保护作为增强公民赋权和欧盟实现数字化转型的基础——GDPR实施两周年》的报告[13]。这是自2018年5月GDPR实施以来欧盟的首份评估报告。报告显示，GDPR增强了对个人的赋权，但同时也存在着投诉门槛过低、监管机构不堪重负、中小企业的特殊豁免难以落实等问题[14]。

7月

欧盟法院宣布“隐私盾”（Privacy Shield）无效

7月16日，欧盟法院作出判决，宣布欧盟与美国间的“隐私盾”（Privacy Shield）数据传输协议无效，大量企业无法再依靠“隐私盾”协议实现合法的数据跨境传输[15]。欧盟法院在该判决中指出：美国国内法对公权力访问数据的限制不能满足欧盟法的要求，不符合比例性和严格必要等原则[16]。

8月

通过监管沙盒方式，探索儿童个人信息保护机制

8月19日，英国信息委员办公室（Information Commissioner's Office，ICO）宣布将以“儿童个人信息保护”与“涉及公共利益的数据共享”为主题，重新开放其作为免费服务的监管沙盒，以此为实施和完善《儿童适龄设计准则》提供经验支持，并支持企业和组织通过使用个人数据的方式开发、创新产品和服务[17]。2019年9月至2020年9月，英国ICO已进行了隐私保护监管沙盒的首期尝试，期间探索了生物识别、预防犯罪、卫生部门技术创新等领域的数据治理问题[18]。

9月

Apple 推迟第三方广告跟踪限制要求

9 月 3 日，Apple 公司称，为给予开发者一定的过渡期间，今年 6 月提出的对第三方广告跟踪的限制要求，将推迟至 2021 年初开始实行[19]。此前，苹果公司要求："在新版 iOS14 系统中，所有 App 在进行用户信息跟踪之前都必须先征得用户许可。"[20] Apple 公司就用户信息追踪方面强化的隐私政策，引起了 Google、Facebook 等数字广告行业从业者的不满[21]，数字广告行业的商业模式将面临挑战。

10月

Apple 隐私政策变更引发反垄断申诉

10 月 22 日，针对 Apple 公司隐私政策中对第三方广告的严苛要求，法国互动广告局（The Interactive Advertising Bureau France）、法国移动营销协会（Mobile Marketing Association France）等机构向法国竞争管理局（Autorité de la concurrence）提起反垄断申诉，并请求竞争管理局发布临时禁令，以阻止申诉审查过程中 Apple 公司新的隐私政策对数字广告行业产生损害[22]，此举为首次以反垄断为由对在线隐私措施提起的法律审查[23]。

11月

《区域全面经济伙伴关系协定》（RCEP）正式签署

11 月 15 日，《区域全面经济伙伴关系协定》（Regional Comprehensive Economic Partnership，简称"RCEP"）在东亚合作领导人系列会议期间正式签署[24]。RCEP 中对成员国间数字贸易与跨境数据传输作出的规定，为促进东亚区域内数据跨境流动提供了新的国际协议框架，也反映了我国在构建国际区域一体化格局方面的努力。

12月

欧盟《数字服务法》与《数字市场法》草案

12 月 15 日，欧盟委员会公布了《数字服务法》与《数字市场法》两部立法草案[25]。《数字服务法》是对《2000 年欧盟电子商务指令》的全面升级，确立了更为严苛的平台责任规则；《数字市场法案》则是欧盟数字领域的反垄断法。两部立法都直指美国大型互联网平台，严苛义务与法律责任均为其量身定制，体现了欧盟对美国互联网企业的焦虑与防御心态。立法目前处于草案阶段，后续仍有漫长立法程序，欧盟能否通过规则布局，重新赢得数字发展机遇仍有待检验。

2020 数据治理时间轴

国内

1月

《人脸识别线下支付行业自律公约（试行）》

1月21日，中国支付清算协会发布《人脸识别线下支付行业自律公约（试行）》。《公约》从安全管理、终端管理、风险管理、用户权益保护等方面作出了规范，明确人脸信息的采集要坚持“用户授权、最小够用”的原则，对原始人脸信息采取加密存储，与用户个人隐私进行安全隔离[26]。

2月

《关于做好个人信息保护利用大数据支撑联防联控工作的通知》

2月9日，中央网络安全和信息化委员会办公室发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，要求收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，为疫情防控、疾病防治所收集的个人信息不得用于其他用途[27]。

3月

《个人信息安全规范》（2020版）

3月6日，国家市场监督管理总局、国家标准化管理委员会发布国家标准《个人信息安全规范》（2020版）[28]，该标准将代替2017版规范。作为国内个人信息保护重要的“软法规则”，新版标准结合2017版规范实施以来出现的可操作性问题，以及App专项治理工作组的工作重点进行了修订补充。

4月

《关于构建更加完善的要素市场配置体制机制的意见》

4月9日，中共中央、国务院印发《关于构建更加完善的要素市场配置体制机制的意见》[29]。《意见》将数据作为与土地、劳动力、资本、技术并列的要素之一，提出要加快培育数据要素市场，具体包含推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护三个方面[30]。

5月

《中华人民共和国民法典》颁布

5月28日，《中华人民共和国民法典》[31]颁布，《人格权编》独立成编，确认了自然人的隐私权与个人信息保护，延续了《网络安全法》以来我国关于个人信息保护的法律原则，并结合实践，规定了基于正当理由处理个人信息的民事责任免责。

6月

地方积极开展数据规范立法工作

我国各地方积极开展数据规范立法工作，侧重点包括公共数据、数据交易、个人信息保护等。

6月17日，浙江省政府发布《浙江省公共数据开放与安全管理暂行办法》，是全国首部省域公共数据开放办法，于2020年8月1日正式施行[32]。

7月15日，深圳市司法局发布《深圳经济特区数据条例（征求意见稿）》，旨在规范数据活动，促进数据资源共享开放和全面深度开发利用[33]。

7月30日，天津市互联网信息办公室发布《天津市数据交易管理暂行办法（征求意见稿）》，强调涉及国家安全、公共安全和个人隐私的数据不得交易[34]。

7月

《中华人民共和国数据安全法（草案）》

7月3日，《中华人民共和国数据安全法（草案）》在中国人大网发布并公开征求意见。《数据安全法（草案）》内容主要包括：确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据安全与发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施[35]。

8月

《全面深化服务贸易创新发展试点总体方案》

8月12日，商务部发布《全面深化服务贸易创新发展试点总体方案》，指出要顺应新形势下数字经济的发展趋势，在数字贸易领域，推动数字营商环境便利化，探索完善数字贸易的监管模式，在试点地区开展数据跨境传输安全管理试点[36]。

9月

《全球数据安全倡议》

9月8日，国务委员兼外长王毅在“抓住数字机遇，共谋合作发展”国际研讨会高级别会议上发表题为《坚守多边主义 倡导公平正义 携手合作共赢》的主旨讲话，提出《全球数据安全倡议》，表示全球数字治理应遵循秉持多边主义、兼顾安全发展、坚守公平正义三原则[37]。

10月

《个人信息保护法（草案）》

10月21日，《个人信息保护法（草案）》[38]在中国人大网发布并公开征求社会公众意见。《草案》旨在保护个人信息权益，规范个人信息处理活动，保障个人信息依法有序自由流动，促进个人信息合理利用[39]。

11月

《SDK安全指引》

SDK监管是2020年个人信息保护领域的监管重点之一。11月27日，全国信息安全标准化技术委员会发布《网络安全标准实践指南——移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》[40]，强调SDK不得留存设备唯一标识符。

12月

“人脸识别第一案”

12月29日，杭州中院公开审理郭兵与杭州野生动物世界有限公司服务合同纠纷二审案件。该案被称为国内“人脸识别第一案”。一审判决后当事双方均提起上诉，郭兵主张野生动物世界收集和使用其个人生物识别信息过程中存在欺诈行为，应当删除郭兵所涉全部个人信息；野生动物世界则主张收集郭兵个人生物识别信息并无不当，无需对相关信息进行删除。该案将择日宣判[41]。

1.《Attorney General Becerra Issues Advisory Outlining New Data Privacy Rights for California Consumers》，https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-advisory-outlining-new-data-privacy-rights.

2.《Proposition 24 - the California Privacy Rights Act of 2020》，https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.

3.《Communication: Shaping Europe's digital future》，https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

4.《Communication: A European strategy for data》，https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066;《White Paper on Artificial Intelligence: a European approach to excellence and trust》，https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

5.《Structure for the White Paper on artificial intelligence – a European approach》，https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf.

6.《Joint statement on the right to data protection in the context of the covid-19 pandemic》，https://rm.coe.int/covid19-joint-statement/16809e09f4.

7. 例如，《Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak》，https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_en;《Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak》，https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementreopeningbordersanddataprotection_en.pdf.

8.《Standing Committee for the Scrutiny of Bills（Scrutiny Digest 8 of 2020）》，https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2020/PDF/d08.pdf?la=en&hash=D8280024D217522C8BAF6B9BB524D20B5B988317.

9.《Bill to usher in new era of international crime cooperation》，https://minister.homeaffairs.gov.au/peterdutton/Pages/international-crime-cooperation.aspx#:~:text=The%20Telecommunications%20Legislation%20Amendment%20(International,subject%20to%20an%20international%20agreement.

10.《U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online》，https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

11.《Framework：Exposure Notification - Implement a COVID-19 exposure notification system that protects user privacy》，https://developer.apple.com/documentation/exposurenotification.

12.《Apple and Google partner on COVID-19 contact tracing technology》，https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

13.《Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation》，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

14. 王融，朱军彪：《GDPR 2 周年，来自欧盟内部的反思与启示》，载微信公众号“腾讯研究院”，https://mp.weixin.qq.com/s/Iw1J0lYQOa5Kl8fszvqkgw.

15.《The CJEU judgment in the Schrems II case，https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

16. 判决原文见：http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227.

17.《Children's privacy and data sharing in focus as regulatory sandbox re-opens》，https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/children-s-privacy-and-data-sharing-in-focus-as-regulatory-sandbox-re-opens/.

18.《A six month review of the Sandbox by Ian Hulme，Director of Regulatory Assurance at the ICO》，https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/combining-privacy-and-innovation-ico-sandbox-six-months-on/.

19.《Details for app privacy questions now available》，https://developer.apple.com/news/?id=hx9s63c5.

20.《Apple 通过 iOS 14 重塑 iPhone 体验》，https://www.apple.com.cn/newsroom/2020/06/apple-reimagines-the-iphone-experience-with-ios-14/.

21. Greg Bensinger:《Goliath vs. Goliath - Facebook and Apple's fighting over data privacy rights doesn't help consumers much，until it does》，https://www.nytimes.com/2020/12/19/opinion/facebook-apple-privacy.html.

22.《French associations representing the online advertising ecosystem file complaint against Apple》，http://www.sri-france.org/2020/10/28/french-associations-representing-the-online-advertising-ecosystem-file-complaint-against-apple/.

23.《Apple Faces Antitrust Complaint in France Over Privacy Changes in iPhones》，https://www.wsj.com/articles/apple-faces-antitrust-complaint-in-france-over-privacy-changes-in-iphones-11603893625#:~:text=Advertising%20companies%20and%20publishers%20have,to%20roll%20out%20are%20anticompetitive.&text=The%20case%20is%20one%20of,privacy%20measures%20on%20antitrust%20grounds.

24.《区域全面经济伙伴关系协定》（RCEP）领导人联合声明》，https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/t1832614.shtml.

25.《The Digital Markets Act: ensuring fair and open digital markets》，https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

26.《中国支付清算协会关于印发＜人脸识别线下支付行业自律公约（试行）＞的通知》，https://www.scpca.org.cn/Public/upload/file/20200326/1585194073124353.pdf.

27.《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm.

28.《GB/T 35273-2020＜信息安全技术 个人信息安全规范＞正式发布》，http://pip.tc260.org.cn/jbxt/privacy/detail/20200307123754442334.

29.《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》，http://www.gov.cn/gongbao/content/2020/content_5503537.htm.

30.《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》，http://www.gov.cn/gongbao/content/2020/content_5503537.htm.

31.《中华人民共和国民法典》（2020 年 5 月 28 日第十三届全国人民代表大会第三次会议通过），http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml.

32.《浙江省公共数据开放与安全管理暂行办法》，https://www.zj.gov.cn/art/2020/6/17/art_1229017137_557682.html.

33.《深圳市司法局关于公开征求＜深圳经济特区数据条例（征求意见稿）＞意见的通告》，http://sf.sz.gov.cn/hdjlpt/yjzj/answer/5748.

34.《天津市互联网信息办公室关于对＜天津市数据交易管理暂行办法（征求意见稿）＞公开征求意见的通知》，http://credit.tjhbq.gov.cn/detail.do?contentId=2641e0e3413c4260937f2444750377db&channelId=fe5c6171fc734662baede0a82ef6154e.

35.《数据安全法草案：落实数据安全保护责任规定支持促进措施》，http://www.npc.gov.cn/npc/c30834/202006/97f149839ff04c428224f6344ead7e38.shtml.

36.《商务部关于印发全面深化服务贸易创新发展试点总体方案的通知》，http://www.gov.cn/zhengce/zhengceku/2020-08/14/content_5534759.htm.

37.《中方提出＜全球数据安全倡议＞》，https://www.fmprc.gov.cn/web/wjbzhd/t1812947.shtml.

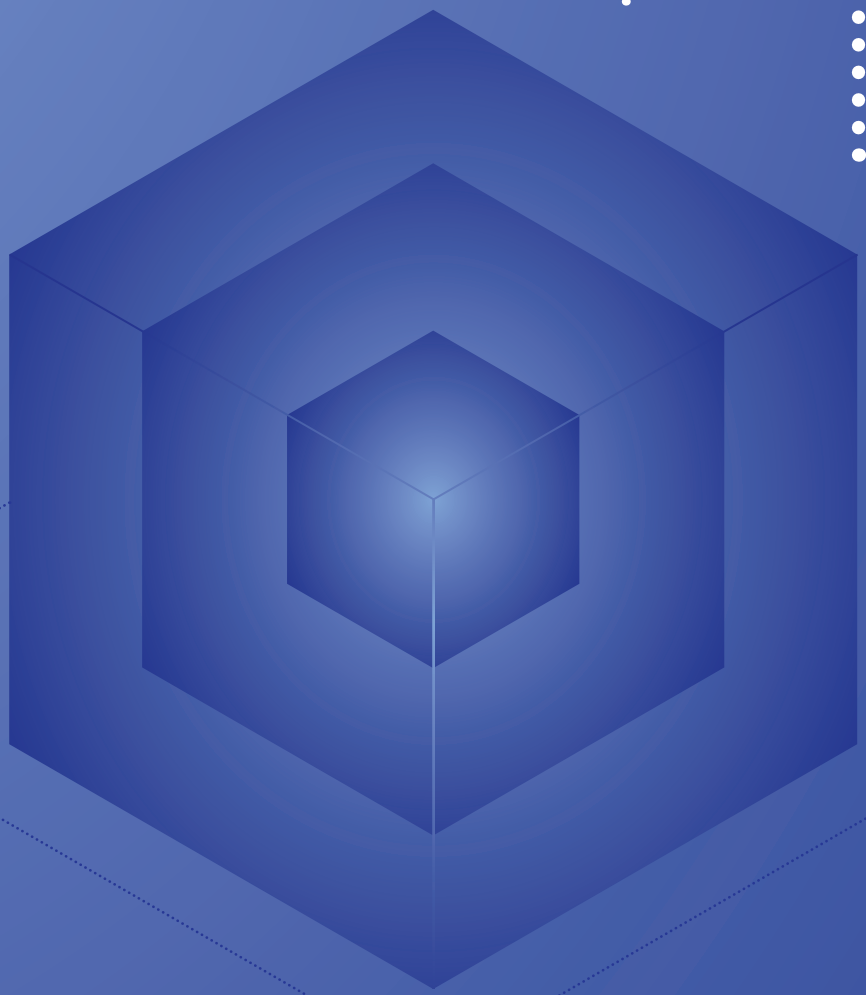
38.《个人信息保护法草案等多部法律草案公开征求意见》，http://www.npc.gov.cn/npc/c30834/202010/9f67b926535948719c2a0b0220dce9ed.shtml.

39.《个人信息保护法草案首次亮相》，http://www.npc.gov.cn/npc/c30834/202010/569490b5b76a49c292e64c416da8c994.shtml.

40.《关于发布＜网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引＞的通知》，https://www.tc260.org.cn/front/postDetail.html?id=20201126161240.

41.《“中国人脸识别第一案”二审开庭 将择日宣判》，http://www.chinanews.com/sh/2020/12-29/9374298.shtml.

2020 年
数据治理专题分析



疫情下的数据治理——
“隐私保护”与“公共健康”的平衡

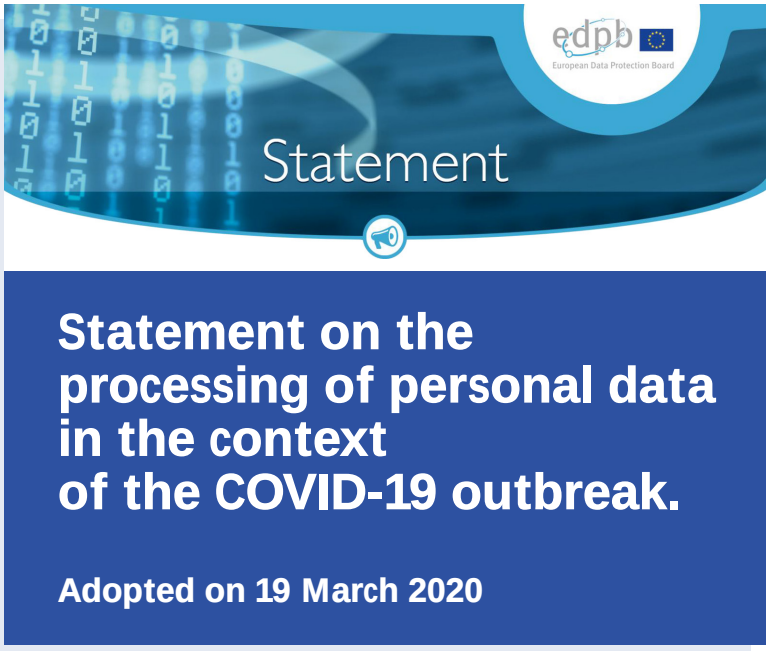
1

前言

2020 年，新型冠状病毒（COVID-19）的全球性爆发对各国医疗卫生体系乃至公共安全带来持续挑战。借助对个人信息的收集和处理，能够有效助力疫情的防控，但随之而来的隐私泄露、数据安全等问题也成为挥之不去的担忧。

本专题梳理分析了 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 大类共识、尚存的差异以及面临的共同挑战。随着疫情进入常态化，各国也尝试通过不同的技术支持方案来控制疫情，其中又以我国的“健康码”和 Google 与 Apple 推出的“蓝牙跟踪”引起的关注最多。两者分别依循“中心化”与“去中心化”两种不同技术思路，但共同的目标是实现更加优化的公共健康管理，以最小的隐私泄露和数据安全风险，帮助人们重新回归正常生活。

01 疫情下各国数字治理的共识、差异与挑战



（1）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，相关法律规范并不会成为影响疫情防控的制度阻碍。欧盟数据保护委员会在 2020 年 3 月 20 日发布的《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，例如欧盟《通用数据保护条例》(General Data Protection Regulation，简称 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。"[42]

（2）法律基本原则仍应得到遵循

在强调应对公共卫生事件优先的同时，欧盟各国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。例如西班牙数据保护局的报告特别指出，即使在紧急卫生情况下，个人数据的处理也必须继续依照目的限制、准确性等 GDPR 和国内法确立的原则[43]。

（3）对雇主收集信息范围存在分歧

疫情期间，雇主是除了特定的公权力机关、卫生部门之外最主要的疫情信息节点。然而，各国目前在基本共识之外，就具体规

42. 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.

43. See agencia espanola proteccion datos (AEPD), 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/documento/2020-0017-en.pdf.

则仍存在分歧。例如，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（Commission nationale de l'informatique et des libertés，简称 CNIL）在其 2020 年 9 月 23 日发布的指南中便对雇主提出了严格要求，其认为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等均不被允许[44]。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。例如，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（但不能要求详细的旅行行程）[45]。

（4）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，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 CNIL 指出，卫生部门可以收集健康数据，并有资格采取适合于具体情况的措施[46]。此外，也有很多国家试图通过紧急状态下的立法打通跨部门信息共享。美国卫生与公共服务部（U.S. Department of Health and Human Services，简称 HHS）2020 年 3 月发布公告：在全国范围的公共卫生紧急状态期间，将在特定情形下豁免基于《健康保险流通与责任法案》（Health Insurance Portability and Accountability Act，简称 HIPAA）隐私规则的制裁和处罚[47]。

（5）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，但具体措施的激进程度有所不同。亚洲国家如韩国政府机构利用智能手机定位数据和信用卡购买记录[48]，新加坡于 2020 年 3 月 20 日推出名为 TraceTogether 的应用程序[49]，这些措施大部分具有很强的隐私侵入性。相较来说，欧盟国家在位置信息的处理与使用上更为谨慎。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》中提出建议，公共机构应首先寻求以匿名方式处理位置数据[50]。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[51]。

44. See Commission nationale de l'informatique et des libertés, Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs, September 23 2020, available at: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles (last visited on January 07 2021).

45. See UK Information Commissioner ' s Office, Data protection and coronavirus - what you need to know, https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/ (last visited on January 07 2021).

46. See Commission nationale de l'informatique et des libertés, Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs, September 23 2020, available at: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles (last visited on January 07 2021).

47. See U.S. Department of Health and Human Services (2020), COVID-19 & 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.

48. See As Coronavirus Surveillance Escalates, Personal Privacy Plummets , available at: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html (last visited on January 07 2021).

49. 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 January 07 2021).

50. 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.

51. See Facebook: Italian Ministry seeks to leverage big data with help from Facebook and telcos, March 17 2020, available at: https://privacyinternational.org/examples/3421/facebook-italian-ministry-seeks-leverage-big-data-help-facebook-and-telcos (last visited on January 07 2021).

（6）随着疫情升级，更具争议性的人脸识别、无人机投入应用

除了位置信息应用，人脸识别、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。在人工智能技术加大政府防疫措施的执行力度、提升公共卫生系统抗疫负载能力的同时，也应将该类技术的应用限制在必要范围内。

（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

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与医疗物资生产，例如特斯拉宣布切换部分汽车生产线生产呼吸机。Google、Apple 等科技企业也就冠状病毒的预防控制展开合作，但这些公司对用户数据仍然持十分谨慎的态度，一般采取匿名化或聚合数据来提供趋势分析。

（8）教育、医疗等在线服务常态化带来的隐私挑战

疫情之下，远程在线教育成为教学常态，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隐私保护的担忧。美国教育部下属的学生隐私政策办公室（Student Privacy Policy Office，简称 SPPO）便于 2020 年 3 月 20 日发布了疫情期间针对学生网上教育的指导[52]；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。世界隐私论坛也呼吁提供远程医疗服务的科技公司应对病人医疗数据保持克制，保障其安全性。

（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

数字科技的规模化应用在有效抑制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都存在巨大差异，尤其是以韩国、新加坡、中国为代表的亚洲东方国家和西方国家间的差异较为明显。有观点认为：这种差异往往根植于不同地域、文化和认知传统。亚洲国家其隐私观念的内核仍然是东方式的集体主义，而欧洲国家深厚的隐私文化传统早已被立法者融入 GDPR 等隐私保护规范当中。

（10）激进的“隐私争议性”管理措施如何退出？

在抗疫进程中，法国、西班牙等 60 多个国家曾宣布进入或继续保持战争状态或者紧急状态。在这一状态下，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人民的权利[53]。在承认这些措施必要性的前提下，仍应当坚持最小化和必要原则，并防止数据被利用于其他目的。当危机结束之后，各国将如何从这些激进的管理措施中退出？有学者从我国实际出发提出，一旦疫情缓解或结束，健康码就必须脱离强制性和约束性，相关数据的处理将不再必要，根据存储期限最小原则，均应删除或匿名化[54]。

52. See Student Privacy Policy Office, FERPA & Coronavirus Disease 2019 (COVID-19) Frequently Asked Questions (FAQs), available at: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf (last visited on January 07 2021).

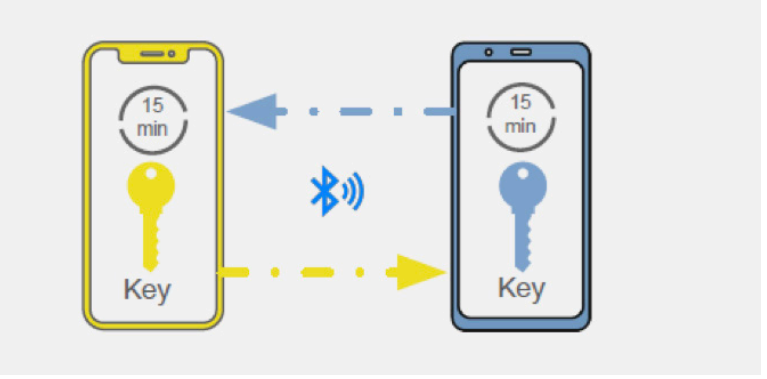
53. See Cas Mudde, Coronavirus outbreak 'Wartime' coronavirus powers could hurt our democracy – without keeping us safe, March 24 2020, https://www.theguardian.com/commentisfree/2020/mar/24/wartime-coronavirus-powers-state-of-emergency (last visited on January 07 2021).

54. 参见许可：《健康码的法律之维》，载《探索与争鸣》2020 年第 9 期，第 136 页。

02 “蓝牙跟踪”与“健康码”——两种不同的疫情防控技术方案

为抗击疫情，Apple 和 Google 在 2020 年 5 月联合开发了蓝牙接触者追踪工具。在嵌入全球两大主导的智能手机操作系统后，该工具可触达全球 30 亿智能手机用户，规模之大，无出右者[55]。国内媒体的解读也往往将其与国内的“健康码”相联系，并类比为全球最大的健康码项目。然而，深度比较后会发现，二者在基本理念、运作原理、覆盖范围、推进方式、效果考察等方面存在较大差异。

Google 与 Apple 的蓝牙接触者追踪项目虽然也依赖各国公共卫生管理部门的参与，但仍然是一个强调“分散化”的、自下而上的技术方案，这与我国的“健康码”，以及韩国、新加坡、英国等以政府为主导、以“中心化”为主要特征的技术管理措施有着显著不同。对此，我们无法作出孰优孰劣的简单判断，但对二者的深入比较，将有助于彼此借鉴启发。一套良好的疫情管理技术体系既可以包含中心化部分，也可以吸收分散化方式，共同的目标是实现更加优化的公共健康管理，以最小的隐私泄露和数据安全风险，帮助人们重新回归正常生活。

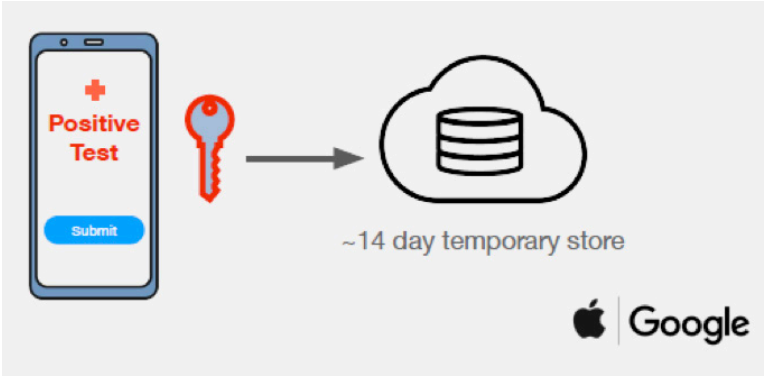


（1）谷歌苹果蓝牙接触者追踪工具基本原理

在用户主动选择打开该工具的情形下，智能手机会自动生成本地追踪密钥（Tracing Key）、临时追踪密钥（Temporary Tracing Key）、滚动接近标识符（Rolling Proximity Identifier）等层层加密、相互嵌套的密钥。这些密钥存储在用户的智能手机中，并且实时更新（当日追踪密钥每 24 小时更新，滚动接近标识符每 15 分钟更新）。

55. See Apple and Google partner on COVID-19 contact tracing technology, 10 April 2020, available at: https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/.

当两个用户处于蓝牙信号可连接的距离之内（如 9 米之内），智能手机会自动交换并存储滚动接近标识符。如果有人确诊感染新冠肺炎并通知公共卫生机构，仅限公共卫生机构访问的中央服务器会生成该患者的确诊密钥，此后，卫生机构应用程序会向过去 14 天与确诊者交换过滚动接近标识符的所有人（即与确诊者有过接触历史的人）发送确诊密钥。如果本地匹配成功，用户会收到通知，告知其曾经与感染者接触 [56]。



（2）“蓝牙跟踪”VS“健康码”

不需要建立中心化的用户数据库，并在用户本地进行匹配计算

两家公司鼓励各国卫生服务部门构建以分散方式运行的接触者追踪应用程序，政府并不需要建立用户个人信息的中心化数据库 [57]。除仅有卫生部门能够访问的中央系统维护最小数据（确诊密钥信息）之外，技术运行所涉及到的其他用户数据（包括蓝牙接触信息和元数据）都以加密方式存储在用户手机本地，与确诊信息的匹配计算也将在手机上而不是中央服务器集中进行 [58]。但各国在落地实施过程中曾对此产生分歧。

我国推行的“健康码”，以及在韩国等国家实施的疫情管理技术措施则代表了一种中心化的数据管理思路。强有力的政府部门在其中发挥核心角色，统领汇合各方数据。例如我国一体化政务服务平台“防疫健康码”，集中了卫生健康、工信、交通运输、海关、移民管理、民航、铁路方面的数据，数据类型广泛、规模庞大 [59]。与此相似，韩国政府机构根据 2015 年 Mers 传染病爆发后的立法授权，汇集了智能手机定位数据和信用卡记录等各类数据，

56. See Privacy-safe contact tracing using Bluetooth Low Energy, 10 April 2020, available at: https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf.

57. See Alex Hern, NHS in standoff with Apple and Google over coronavirus tracing, 16 April 2020, available at: https://www.theguardian.com/technology/2020/apr/16/nhs-in-standoff-with-apple-and-google-over-coronavirus-tracing.

58. See Contact Tracing Bluetooth Specification, available at: https://blog.google/documents/58/Contact_Tracing_-_Bluetooth_Specification_v1.1_RYGZbKW.pdf.

59. 国家政务服务平台：http://gjzwfw.www.gov.cn/index.html。

追踪冠状病毒患者轨迹，并建立病毒传播链[60]。英国国民医疗服务系统（National Health Service，NHS）也建立了专门统一的数据平台，数据管理以一种中心化的方式运行[61]。

强调用户自愿选择加入，受参与用户人数等因素影响，蓝牙接触者追踪工具的有效性还有待论证

蓝牙跟踪项目的参与需要经过用户的自主同意。对个人用户而言，这意味着在隐私和健康之间做出自我选择，用户也可能会出于社会责任感而加入该项目。有 80% 的受访者表示，如果该项目足够透明，会选择加入[62]。但是，我们也可以看到在新加坡，类似的 Trace Together 蓝牙追踪应用，只有六分之一人口下载使用[63]。根据斯坦福大学接触者跟踪项目 Covid-Watch 的研究人员分析，只有大约 50%至 70%的人口使用安装接触者追踪工具，数字追踪才能发挥效果。

60. https://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus.

61. https://www.gov.uk/government/speeches/data-sharing-during-this-public-health-emergency.

62. See Coronavirus: NHS contact tracing app to target 80% of smartphone users, https://www.bbc.com/news/technology-52294896.

63. See About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong, available at: https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for.

（3）蓝牙追踪项目的借鉴与启示：

不断反思和改进信息收集范围和处理模式

收集基于蓝牙的接触信息而非收集个人的实时位置信息，是在个人隐私保护和实现疫情预警功能二者之间寻找平衡的一种尝试，这种另辟蹊径的做法的效果还有待检视，但其对隐私和数据安全的谨慎心态仍然值得借鉴。这一模式以用户为中心，在实现对用户做出疫情预警这一目标的同时，也将更好地保护用户数据。而我国也在不断反思并对“健康码”的应用进行规范化。2020 年 4 月 29 日，国家市场监督管理局发布了《个人健康信息码》系列国家标准，以实现个人健康信息码的码制统一、展现方式统一、数据内容统一，统筹兼顾个人信息保护和信息共享利用[64]。

紧密协调自动化技术与人工措施

蓝牙接触者追踪虽然可以依赖技术手段实现大部分自动化的数据处理，但整个系统的有效性以及安全性仍然离不开机构或人工措施。在最早将蓝牙技术用于感染者追踪的新加坡，编写 Trace Together 应用程序的技术专家也认同，数字接触追踪技术不可能完全取代传统的人工流行病学追踪[65]。

疫情技术体系可同时包含“中心化”与“去中心”两种路径

中心化和非中心化的技术路径，并不是非此即彼的关系，二者可以相互借鉴经验，并共同构成疫情防控的技术措施体系。在很多国家的疫情防控实践中，既可以看到中心化模式的技术措施，也可以看到去中心化的技术手段。不论是“中心化”还是“去中心化”，其根本仍在于厘清公共卫生部门和私营部门的角色，遵循相应的数据保护框架，实现个人隐私保护与公共健康管理之间的平衡。

64.《市场监管总局（标准委）发布＜个人健康信息码＞系列国家标准》，载国家市场监督管理总局网：http://www.samr.gov.cn/xw/zj/202005/t20200501_314959.html。

65. See Sidney Fussell and Will Knight, The Apple-Google Contact Tracing Plan Won't Stop Covid Alone, 14 April 2020, available at: https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone/.

结语

疫情将数据的收集与处理推向前所未有的深度，开启了一场“数字社会治理”的大型试验。各国政府在具体做法上虽仍有差异分歧，但也逐步形成了基本共识——数据应当在社会治理中发挥重要作用，同时遵循基本法律原则，保护个人隐私与数据安全。

全球数据保护立法与监管——
立法持续铺开、监管执法趋严

前言

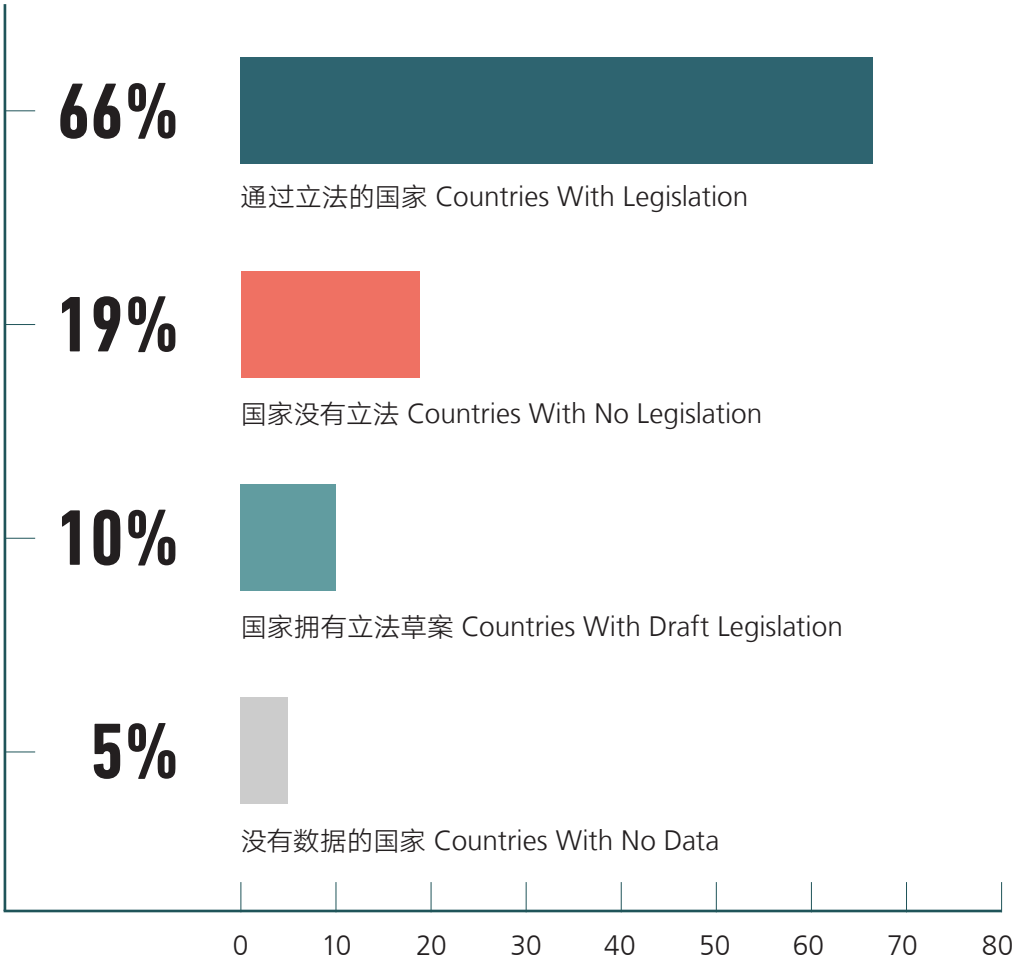
2020 年，作为数字时代的永恒话题，个人数据保护立法与执法继续在全球铺开，早期已出台立法的国家陆续开启了立法修订工作。《民法典》《个人信息保护法（草案）》的出台更为清晰地勾勒了我国个人信息保护的制度特点。而在监管执法方面，欧盟 GDPR 执法案件量、罚款总额仍持续增长，我国则通过多种监管执法手段来推进数据保护。

2

01

数据保护立法：全球铺开、细分深化

Data Protection and Privacy Legislation Worldwide



（1）发展中国家与发达国家体现出不同的立法阶段性特点

2020 年，数据保护立法继续在全球铺开，但在不同国家呈现出不同的阶段性特点。目前，已有 128 个国家在数据和隐私保护方面正式通过了相关立法，约占全球国家总数的 66%，另有约 10% 的国家已公布了相关立法草案并在审议过程中[66]。从 2015 年到 2020 年，全球范围内已具备数据和隐私保护立法的国家数共上升了 11%[67]。

66. See Data Protection and Privacy Legislation Worldwide, available at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited on January 11, 2021).

67. See Data and privacy unprotected in one third of countries, despite progress, available at https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress (last visited on January 11, 2021).

发展中国家立法陆续生效

为应对计算机大规模处理个人数据带来的挑战，美欧在 70 年代迅速通过立法方式将隐私权扩展至个人信息保护，相比而言，发展中国家整体起步较晚，当前正在迎头赶上。虽然受疫情冲击，部分国家推迟了相关立法，但最终大都陆续生效。例如：

泰国

2020 年 5 月 27 日，泰国 2019 年制定的《个人数据保护法》（The Personal Data Protection Act，简称 PDPA）中一些重要条款（如有关个人数据保护的数据当事人权利、投诉、民事责任以及处罚等）生效；

南非

2020 年 7 月 1 日，南非 2013 年制定的《个人信息保护法》（Protection of Personal Information Act，简称 POPIA）历经波折也终于生效；

巴西

2020 年 9 月 18 日，巴西 2018 年制定的《巴西一般数据保护条例》（Lei Geral de Proteção de Dados Pessoais，简称 LGPD）生效；

印度

2020 年 11 月 19 日，印度法律、司法、电子及信息技术部部长 Ravi Shankar Prasad 表示，印度很快将完成其个人数据保护法立法；

中国

2020 年 5 月 28 日，《民法典》正式通过并将于 2021 年 1 月 1 日生效。2020 年 10 月 21 日，《个人信息保护法（草案）》公开征求意见。

发达国家
推进法律修订工作

几乎所有（96%）的欧洲国家已制定了数据与隐私保护立法。因此，与发展中国家在制度方面刚刚起步不同，发达国家目前已陆续进入到法律修订阶段。欧盟实际上在 2018 年已经完成了对早期 1995 年数据保护指令的修订改革，以全面适应大数据、人工智能时代的数据保护新要求。

韩国

2020 年 1 月 9 日，韩国通过了其“数据三法”（《个人信息保护法》、《信用信息法》、《信息通信网法》）的修正案[68]，且在 2020 年 2 月 4 日又对《个人信息保护法》进行了相关修订[69]，主要将之前较零散的个人信息保护相关条款统一整合至《个人信息保护法》中，并完善了监管机制、增加了多种处理个人信息的法律基础，以激活韩国数字产业。2021 年 1 月 6 日，韩国个人信息保护委员会再次公布新的《个人信息保护法修正案（草案）》[70]，以进一步增强个人信息权利保护、监管机构的独立性等；

日本

2020 年 6 月 5 日，日本国会通过《个人信息保护法修正案》，该修正案将在两年内生效，但具体生效时间仍未确定；

新西兰

2020 年 6 月 30 日，新西兰通过了《隐私法 2020》（Privacy Act 2020），并于 2020 年 12 月 1 日生效，新法在“侵犯隐私行为的通报”、“企业机构向境外的跨境信息披露”、“隐私执法权”等方面对原有的隐私法进行了修订[71]；

68.《국회 본회의, 데이터 3 법 · 연금 3 법 · 청년기본법 등 201 건 의결》，载韩国国会网，http://www.naon.go.kr/content/html/2020/01/09/0ae208d6-7462-4761-bdbf-d1d6c6a4cfd5.html。

69. 2020 年 2 月 4 日的修正案，https://www.pipc.go.kr/np/default/page.do?mCode=D010010000。

70. 2021 年 1 月 6 日的修正案（草案），https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK。

71. See https://www.privacy.org.nz/assets/Privacy-Act-2020-Information-Sheets/Privacy-Act-2020-information-sheets-full-set.pdf.

新加坡

2020 年 11 月 2 日，为适应新的数字经济需求，新加坡议会通过了法律修正案，以修改其 2012 年颁布的《个人信息保护法》；

加拿大

2020 年 11 月 17 日，加拿大创新、科学与工业部提交《数字宪章实施法案》(Digital Charter Implementation Act，简称 DCIA) 的 C-11 法案至国会审议，该法案将废除此前《个人信息保护和电子文档法》(The Personal Information Protection and Electronic Documents Act，简称 PIPEA) 的部分内容，以新的制度来规制基于商业目的的个人信息收集、使用、披露等行为。而作为该法案的核心，其将颁布《消费者隐私保护法》(Consumer Privacy Protection Act，简称 CPPA) 和《个人信息和数据保护法庭法》(Personal Information and Data Protection Tribunal Act)。其中，《个人信息和数据保护法庭法》将新设一个专门法庭，以审理涉及数据保护执法令的上诉案件，同时也将建立与新的 CPPA 相适应的行政处罚体系。

美国

美国以各州为主，在消费者保护、人脸识别领域持续推动、加强隐私与数据保护。2020 年 7 月，美国缅因州《保护在线消费者信息隐私法》(An Act To Protect the Privacy of Online Customer Information) 生效，该州为继加州、内华达州之后对消费者隐私保护进行专门立法的第三个州。2020 年 9 月，华盛顿州参议员 Senator Carlyle 公布了《华盛顿隐私法 2021》草案，以公开征求意见。此外，纽约州、密西西比州、伊利诺伊州、德克萨斯州的隐私法案也正在立法进程中。

就疫情中大量使用的人脸识别技术，美国各州也纷纷作出回应。2020 年 3 月 12 日，华盛顿市通过了专门涉及人脸识别的法案 (编号 SB 6280 – 2019-2020)，其规定使用人脸识别需要通过训练和偏见测试 (Training and Bias Testing) 并要求政府披露使用人脸识别的情况。2020 年 5 月以来，美国加利福尼亚州旧金山市与奥克兰市、威斯康辛州麦迪逊市、俄勒冈州波特兰市、佛特蒙州等纷纷出台了城市执法部门的“人脸识别禁令”。

（2）我国个人信息保护的完整法律框架逐渐清晰

2020 年 5 月 28 日，《民法典》正式通过并于 2021 年 1 月 1 日生效，其中“人格权编”明确了我国“个人信息”的定义及其与“隐私权”的关系，以及处理个人信息的基本规则、免责事由等内容。在我国已有对个人信息的刑事、行政保护后，《民法典》人格权编填补了我国个人保护体系中的“民事保护”板块，将有助于我国构建全方位的公民个人信息保护体系[72]。

《人格权编》的立法过程也是定分止争的过程。长期以来，学界对“隐私权”和“个人信息保护”之间的关系充满争议。《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“隐私权”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。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。

72. 参见《< 民法典人格权编 > 问世——“健康变色码”能停止异化吗?》，载微信公众号“腾讯研究院”：https://mp.weixin.qq.com/s/yJtEqqLnsuQOAk517Tlzxg。

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 111 条确立了自然人对个人信息享有民事权利——个人信息权的结论。《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”，显然也是采纳了后者意见。

“个人信息”与“隐私”确有差异。与“隐私”更多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，形成相对独立的公法体系，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。正如欧盟 GDPR 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。

此次《人格权编》吸收了司法实践的有益总结，并结合《网络安全法》等相关行政法规范，提出了个人信息处理民事责任的免责事由，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），这些规定有效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，同时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与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。

继《民法典》之后，2020 年 10 月 21 日，《个人信息保护法（草案）》公布，《草案》对个人信息保护的原则和规则进行了更加细化的规定，涵盖了不同种类个人信息的处理、数据跨境流动、个人在数据处理过程中享有的权利种类、国家机关的个人信息保护职责等。作为首部完整系统的个人信息保护法律，《草案》体现了对个人信息保护法律中国方案的积极探寻，为数字经济产业的健康发展带来充分利好；有利于通过法律制度保障数字产业，帮助数字产业建立消费者信任；有利于在复杂的数据处理生态中创建权责明确的数据保护秩序；有利于与国际规则接轨，提升国家与企业形象，助力企业“走出去”。

此外，个人信息保护相关的行政法规、规范性文件、行业标准、地方立法等也相继出台或更新。

2020.1.20 全国信息安全标准化技术委员会发布《信息安全技术 个人信息告知同意指南（征求意见稿）》；

2020.3.6 发布《信息安全技术 个人信息安全规范》修订版本，为个人信息保护提供实践指引；

2020.11.19 发布《信息安全技术 个人信息安全影响评估指南》，该标准将于 2021 年 6 月 1 日正式实施。

02
数据保护监管与执法：执法趋严，多管齐下

欧美：
行政执法处罚为主的规制模式

总体来看，以欧盟 GDPR 与美国 CCPA 为代表的欧美数据保护执法，均不约而同地选择了“以效率为先、行政执法处罚为主”的规制模式[73]。从相关数据[74]来看，2020 年欧盟 GDPR 的执法案件与罚款数额均有了大幅提高：相比 2019 年的 144 件，2020 年 GDPR 的罚款案件增加至 318 件，罚款总额也从 2019 年的约八千七百万元增长至 2020 年的约一亿七千万元，迄今为止单个案件罚款额度最高 10 个案件中也有 6 起是在 2020 年做出。GDPR 的处罚对象除了企业以外，还包括政府部门，例如 2020 年 8 月爱沙尼亚数据保护执法机关对警察无正当理由调取当事人健康信息的情况处以罚款[75]。

在美国，不论是联邦层面的个人信息保护主要执法机构联邦贸易委员会（Fedearal Trade Commission，FTC），还是州层面——以加州 CCPA 为例，所授权的检察长，均采取的是行政处罚机制。英文中表述为 civil penalty，直译是“民事罚金”，但实质为行政处罚。特别从加州而看，CCPA 对私人诉讼在实体和程序上有严格的限制，将私人诉权限缩在较小的范围之内。

73. 王融、黄致韬：《迈向行政规制的个人信息保护：GDPR 与 CCPA 处罚制度比较》，载微信公众号“腾讯研究院”：https://mp.weixin.qq.com/s/87qPnJ7OK2KZpmoRSZbYxg。

74. 数据来源：https://www.enforcementtracker.com/?insights。

75. See Uudishimupäring tõi väärteotrahvi, available at https://www.aki.ee/et/uudised/uudishimuparing-toi-vaarteotrahvi (last visited on January 11, 2021).

77.《天津市委网信办开展疫情防控相关 App 违法违规收集使用个人信息专项治理工作》，载中国网信网：http://www.cac.gov.cn/2020-03/13/c_1585639125228327.htm。

78.《国家网信办启动 2020“清朗”专项行动》，载新华网：http://www.xinhuanet.com/politics/2020-05/22/c_1126020214.htm。

79.《2020 年 App 违法违规收集使用个人信息治理工作启动会在京召开》，载中国网信网：http://www.cac.gov.cn/2020-07/25/c_1597240741055830.htm。

我国：
多种监管与救济方式并行

2020 年，我国个人信息保护行政监管与专项整治活动贯穿全年，愈加深入和严厉。

2020.2.10 中央网信办发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，强调要加强疫情期间个人信息保护。此后，各地方对疫情防控下 App 违法违规、公民个人信息保护等问题予以关注。例如，3 月 13 日，天津市委网信办宣布开展疫情防控相关 App 违法违规收集使用个人信息专项治理活动[77]；

2020.5.22 中央网信办宣布将在全国范围内启动为期八个月的 2020“清朗”专项行动，针对网络暴力、侵犯公民个人信息、恶意营销等问题进行治理[78]；

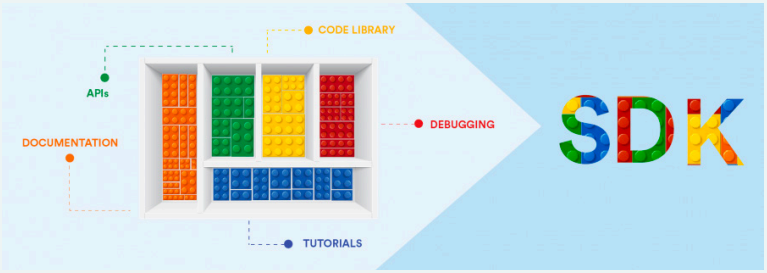
2020.7.25 中央网信办、工业和信息化部、公安部、国家市场监督总局召开会议，在回顾 2019 年执法成果后，宣布再次启动 2020 年的 App 违法违规收集使用个人信息治理工作[79]；

2020.12.21 工业和信息化部发布今年第 7 批《关于侵害用户权益行为的 APP 通报》[80]。此前，工信部已多次组织第三方检测机构对手机应用软件进行检查，并自 5 月 15 日起相继公布多批通报名单，督促存在问题的企业进行整改。

80.《关于侵害用户权益行为的 APP 通报（2020 年第七批）》，载工信部网站：https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2020/art_fb7c796f64304c0d8a5c9c3e45e714f8.html。

SDK 的规范化与监管成为政府工作重点

2020 年 5 月 22 日，App 违法违规收集个人信息治理工作启动会明确：“制定发布 SDK、手机操作系统个人信息安全评估要点”“对用户规模大、问题反应集中的 App、SDK、小程序等进行深度评估”等为眼下治理工作重点之一[81]；2020 年 7 月 22 日，工信部发布公告称将重点整治 SDK 违规处理个人信息等问题[82]；2020 年 11 月 13 日，App 违法违规收集使用个人信息治理工作组发布了《关于 35 款 App 存在个人信息收集使用问题的公告》，多款 App 因存在 SDK 收集个人信息问题而被点名整改[83]；2020 年 11 月 27 日，全国信息安全标准化技术委员会发布了《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》，对 SDK 的常见风险给出了实践指引。



金融领域，陆续披露相关个人信息保护违规行政处罚案例

2020 年 8 月 15 日，上海银保监局披露：交通银行股份有限公司太平洋信用卡中心和招商银行股份有限公司信用卡中心分别被罚 100 万元，其违规案由涉及客户个人信息保护、催收、资信调查等[84]。2020 年 10 月 21 日，人民银行发布公告称，其已就相关分支机构侵害消费者金融信息安全的行为进行立案调查，并分别对农业银行吉林市江北支行、中国银行石嘴山市分行、建设银行德阳分行、建设银行娄底分行、建设银行东营分行、建设银行建德支行及相关责任人予以警告并处以罚款，同时也进行了约谈并责令其立即整改[85]。

81.《2020 年 App 违法违规收集使用个人信息治理工作启动会在京召开》，载中国网信网：http://www.cac.gov.cn/2020-07/25/c_1597240741055830.htm。

82.《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》，载工业和信息化部网站：http://www.gov.cn/zhengce/zhengceku/2020-08/02/content_5531975.htm。

83.《关于 35 款 App 存在个人信息收集使用问题的通告》，载中国网信网：http://www.cac.gov.cn/2020-11/17/c_1607178245870454.htm。

84. 针对招商银行的处罚决定，见《沪银保监银罚决字〔2020〕10 号》，https://www.cbirc.gov.cn/branch/shanghai/view/pages/common/ItemDetail.html?docId=920602&itemId=1000；
针对交通银行的处罚决定，见《沪银保监银罚决字〔2020〕8 号》，https://www.cbirc.gov.cn/branch/shanghai/view/pages/common/ItemDetail.html?docId=920603&itemId=1000。

85.《严肃查处侵害消费者金融信息安全权行为 切实保护金融消费者长远和根本利益》，载中国人民银行官网：http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4113407/index.html，2021 年 1 月 11 日访问。

86.《2020 年公安机关侦办侵犯公民个人信息刑事案件 3100 余起》，载新华网：http://www.xinhuanet.com/2020-12/30/c_1126926723.htm，2021 年 1 月 11 日访问。

87. 参见《全国首例检察机关提起的利用互联网侵害隐私权民事公益诉讼案当庭宣判》，载河北检察院网，http://www.he.jcy.gov.cn/jcxw/jjyw/202012/t20201207_3067553.shtml。

88. 参见《全国首例适用民法典的个人信息保护民事公益诉讼案宣判》，载微信公众号“杭州互联网法院”，https://mp.weixin.qq.com/s/X3rPn4NRIeHFwvQHGO62dw。

刑事方面，全国公安机关推进“净网 2020”专项行动

截至 2020 年 12 月 20 日，全国共侦办侵犯公民个人信息刑事案件 3100 余起。其中涉疫情人员个人信息网泄露案件是公安机关的打击重点，已有 1500 余名违法人员因此受到治安处罚。此外，侵犯未成年人和老年人公民个人信息、暗网侵犯公民个人信息、买卖人脸识别数据等犯罪活动也是今年刑事打击的重要内容[86]。

民事方面，明确引入“个人信息保护”案由，探索公益诉讼

针对以往个人信息保护案件中存在的案由不明、个人取证举证难、赔偿数额低等问题，与之相匹配的诉讼制度正逐步形成：

一方面，最高人民法院在 2020 年 12 月 30 日印发经修改的《民事案件案由规定》，将“个人信息保护”单列为一项案由，由此解决了个人信息保护案件因归类不明而分散在隐私权、姓名权、一般人格权、名誉权等案由下的问题；

另一方面，检察机关也正尝试以民事公益诉讼的方式提升个人信息民事保护。以往的公益诉讼局限于“4+1”的法定范围，即“生态环境和资源保护、食品药品安全、国有财产保护、国有土地出让和英雄烈士保护”。当前，各地检察机关已就“个人信息”的民事公益诉讼机制展开尝试。2020 年 8 月，河北省保定市人民检察院提起首例利用互联网侵害隐私权的民事公益诉讼，该案于 2020 年 12 月经由保定市中级人民法院不公开审理并当庭宣判[87]。2021 年 1 月，杭州互联网法院对首例适用民法典的个人信息保护民事公益诉讼案宣判[88]。

结语

2020 年，数据保护立法继续在全球铺开、深化，继续延续数字社会的立法主流。而从监管与执法活动来看，欧美因数据保护而处以的行政处罚案件数量与罚金规模亦不断增长。而我国通过多种形式推进监管执法，针对不同技术与应用场景下的个人信息提供更加全面的保护。

政务数据管理——
助力社会治理现代化，规范利用提上议事日程

3

前言

2020 年初爆发的新冠疫情，推动政务数据管理向前迈进一大步，依托数据资源汇聚分析、数字技术支撑和产品思维驱动，传统科层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，实现了社会治理现代化的一次跃升。与此同时，各地针对政务数据管理的立法工作也正在积极开展，政务数据管理沿着逐渐规范化的趋势发展。

01 政务数据管理发挥重要功能

（1）“健康码”的应用与发展

“健康码”最早孵化于腾讯、阿里等互联网企业的政务服务基础架构。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。从 2020 年 1 月底广州政务微信小程序“穗康”的推出，到 2 月初深圳成为全国首个疫情期间凭“码”出行的城市，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，国务院发文明确鼓励有条件的地区推广个人健康码等信息平台，并在国家政务服务平台中推出“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”覆盖范围和准确度。3 月 20 日，国家卫健委宣布大力推动各地互认互通工作。

从发端到全面推进，“健康码”深度卷入了各级政府部门、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，关系到过度收集个人信息、用户救济、信息泄露风险等问题能否得到根本性解决。

政府
作为“数据控制者”

政府部门在“健康码”政务服务中处于“数据控制者”角色。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，其决定了“健康码”应用中数据采集的类型、内容、使用方式、用途。而作为“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的基本原则，具体包括：

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。2 月 5 日，习近平主席在中央全面依法治国委员会第三次会议发表重要讲话，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。例如工信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”过程中，正在探索各类透明公开的方式，保障用户知情权。如上海市“随申码”、广东省“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营管理机构制定的用户协议和隐私政策。深圳政府还专门编制了《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，可能会出现健康码并不准确的情况，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要求。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”以上的安保措施，引入了包括加密存储、加密传输、访问控制等安全措施。

企业作为“数据处理者”

作为“数据处理者”的企业主体，除了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，包括：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，擅自转包。

而在国外，政务数据管理在新冠疫情的防控过程中同样发挥着重要的功能。2020 年 3 月，英国政府委托 NHS（National Health Service，英国国家医疗服务体系）England and Improvement 和 NHSX 开发数据平台，该平台将为负责协调行动的国家组织提供安全、可靠和及时的数据以作出明智有效的决定。NHS England and Improvement 将创建统一的数据存储，以将多个数据源导入到一个安全的位置，即后端存储或初始存储，所需数据将来自 NHS 及其合作组织，例如 NHS Digital 的 111 个在线 / 呼叫中心数据和英格兰公共卫生的 Covid-19 测试结果等数据。该平台将提供有关疫情进展的准确事实，并将数据进行整合与统一，以成为支持决策所需的可靠信息来源 [89]。

89. https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

02
政务数据管理中的数据泄露风险

数据泄露问题是政务数据管理过程中面临的挑战之一。根据 PublicTechnology 报告，截至 2020 年 3 月底的 12 个月内，英国中央政府实体向信息专员办公室（ICO）报告了总计 495 起个人数据泄露事件，其中十分之一需要正式调查，至少有 10 起事件需要有关部门采取补救措施。这比上一年报告的数字略有 1.9%的增长。与 2017-2018 财年（欧盟《通用数据保护条例（GDPR）》生效之前的最后一个财年）相比，报告的数据泄露事件数量增加了 290%。在 2020 财年，监管机构还收到了来自地方政府部门的总计 1006 个数据泄露报告的汇总。英国信息专员办公室的一位发言人提到，“针对与教育部学习记录服务处获得的数据相关的一些潜在数据合规问题，英国 ICO 正就此进行调查。”[90]

我国的政务数据管理当前也存在完善改进的空间。在个人信息收集方面，一些政府部门开发的政务服务 App 存在着合规问题。2020 年 11 月 13 日，App 违法违规收集使用个人信息专项治理工作组在官微发布通告称，35 款 App 存在个人信息收集使用问题，此次被点名的不乏由地方政府部门开发的 App，如安徽省数据资源管理局开发的皖事通（V1.7.5）和南京市公安局开发的宁归来（V4.3.0）。此外，也包含一些城市生活服务应用，如鄂汇办（V3.2.5）、爱山东（V2.3.6）、幸福秦皇岛（V2.3.8）等[91]。

在政务数据管理中，数据用途是否正当同样可能成为引发公众质疑的问题。9 月 3 日，江苏省苏州市推出“苏城文明码”，给测试范围内的市民进行文明打分，形成市民文明程度“个性画像”，文明积分等级高的市民将会享受工作、生活、就业、学习、娱乐的优先和便利；同时，“文明码”还可对综合文明指数较低的人员起到警示和惩戒作用。这一举措引发了公众的广泛质疑，因其有将文明功利化的趋势，将市民完全异化为数据测量评估对象并给予工具性评价，在接受行政处罚后还将再次被记录在“文明码”中的机制也引发了人们对“一事二罚”的担忧[92]。

90. https://publictechnology.net/articles/news/excl-whitehall-departments-reported-500-personal-data-breaches-ico-fy20

91. https://www.sohu.com/a/431666056_161795

92. http://paper.people.com.cn/zgcsb/html/2020-09/14/content_2008843.htm

93. https://www.zj.gov.cn/art/2020/6/17/art_1229017137_557682.html.

94. http://www.cq.gov.cn/zwgk/fdzdgknr/lzyj/xzgfxwj/szfbgt_38656/202009/t20200918_7896095.html

95. http://www.gzic.gov.cn/dsjzsk/zcwj/202010/t20201013_64034517.html

96. http://www.hunan.gov.cn/hnszf/xxgk/wjk/fggz/flgzst/202012/t20201203_13974778.html

03 地方积极推进政务数据管理立法

我国各地方也在积极为政务数据管理制定规范。

2020.6.17 浙江省政府发布《浙江省公共数据开放与安全管理暂行办法》，于2020 年 8 月 1 日正式施行。《办法》旨在规范和促进浙江省公共数据开放、利用和安全管理，加快政府数字化转型，推动数字经济、数字社会发展，包含数据开放、数据利用、数据安全、监督管理和法律责任等部分[93]。

2020.9.11 重庆市政府发布《重庆市公共数据开放管理暂行办法》，自发布日开始施行。《办法》旨在促进和规范重庆市公共数据开放和利用，提升政府治理能力和公共服务水平，推动数字经济高质量发展，提出公共数据开放应当遵循“统筹部署、需求导向、充分应用、统一标准、分类管理、安全可控”的原则[94]。

2020.9.25 贵州省人大常委会发布《贵州省政府数据共享开放条例》，2020 年 12 月 1 日起施行。《条例》从政府数据管理、政府数据共享、政府数据开放、监督管理等明确贵州省政府数据共享开放事项[95]。

2020.11.28 湖南省政府发布《湖南省政务信息资源共享管理办法》，将于 2021 年 3 月 1 日起施行，其旨在推动和规范政务信息资源共享，加快“数字政府”建设，促进政务部门业务协同，提高行政效能，提升政府治理能力和服务水平，明确政务信息资源共享应遵循需求导向、无偿使用、统一标准、统筹管理、安全可控、严格保密的原则[96]。

结语

政务数据管理规范正提上议事日程。在新冠疫情防控背景下，有效的数据管理将有助于政府实现高效有序的疫情防控，也能够为政府履行日常职能带来便利。与此同时，政务数据管理也面临着过度收集个人信息、数据泄露等安全风险。为此，各地方正在积极展开政务数据管理有关立法，为政务数据管理与数据共享制定相应规范。

人脸识别——
未知与担忧并存

前言

2020 年，人脸识别继续在安防、金融、娱乐、零售、医疗卫生等多领域加速普及。在疫情推动下，人脸识别更广泛地应用在公共场所。与此同时，对公众而言，由于人脸识别技术存在着大量未知，人们对于人脸识别的信息收集、运作机制、应用场景等缺乏足够的了解，因而表现出警惕和恐惧的心态，人脸识别面临着来自各方的质疑。人脸识别作为一项新兴技术，有着广阔的探索空间与应用前景，因此各国在人脸识别的立法规制上保持着谨慎态度，并未对人脸识别技术进行全面禁止，而是针对特别场景的风险展开规则探索。

4

01 美国：执法部门应用人脸识别引发争议

在美国，人脸识别技术的主要应用主体包括执法部门与私人主体。对于执法部门而言，人们担心执法部门可能会通过人脸识别技术来识别示威者，从而阻碍人们行使公民权利，对民主制度造成危害；对于私人主体，人们主要对私人主体是否会超出约定目的滥用人脸识别技术存在顾虑。围绕着这样的质疑，美国出现了多起涉及人脸识别技术的诉讼纠纷，其中以对 Clearview 公司的质疑最为典型，与此同时，美国各州正逐步对人脸识别技术的使用进行限制。

（1）风口浪尖的 Clearview

Clearview AI 是一家成立于 2017 年的科技公司，在 Clearview 应用中，用户上传一张照片，便可以查看照片中个体在 Facebook、YouTube、Twitter 等社交网络和其他网站上公开的照片，并获取这些照片的链接。到 2020 年，Clearview 的数据库已经包含超过 30 亿张图像 [97]。Clearview 的数据库涵盖的图像数量大，覆盖范围广，具有开放性。

正是由于这样的优势，Clearview 获得了大量用户，特别是执法机构的青睐。根据其 2020 年 2 月泄露的客户名单，Clearview 已被 27 个国家 / 地区的 2200 多个政府机构、执法部门、公司甚至个人所使用，并执行了近 500,000 次搜索 [98]。

97. See Kashmir Hill, The Secretive Company That Might End Privacy as We Know It, February 10 2020, available at: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (last visited on April 3 2020).

98. See Ryan Mac, Caroline Haskins and Logan McDonald, Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA, February 27, 2020, available at: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement (last visited on April 3 2020).

美国曾使用 Clearview 的执法机构包括国土安全部、移民和海关执法局、禁毒署、联邦调查局等。各州警方同样是 Clearview 的客户，在使用其他人脸识别系统搜索不到匹配项时，也会尝试使用 Clearview 开展调查活动，例如，美国移民和海关执法局将人脸识别技术用于调查奴役儿童案件、人口贩运案件等。

与此同时，政府执法机构对 Clearview 的使用引发了人们对隐私安全的警惕。从程序上来看，执法部门在使用 Clearview 的过程中缺乏监管和约束。以芝加哥为例，尽管伊利诺伊州拥有美国较为完善的生物特征识别信息保护法律体系，芝加哥警察局使用人脸识别技术，甚至是与 Clearview AI 合作并不需要市议会的批准，而且没有举办过关于该技术如何使用的公开听证会。

执法部门使用人脸识别技术的目的同样引发了人们的担忧。马萨诸塞州的民主党参议员 Markey 曾表示，Clearview AI 的技术可用于识别和逮捕示威者。在佛罗里达州，迈阿密警方曾利用 Clearview 逮捕了一名抗议者。2020 年 5 月，美国公民自由联盟起诉了 Clearview AI，主张 Clearview AI 违反了《伊利诺伊州生物识别信息隐私法》(BIPA)，在未获得知情或同意的情况下非法收集和存储了伊利诺伊州公民的数据，并将访问权限出售给了执法机构和私人公司。

处在争议中的 Clearview 目前面临着多起诉讼。2020 年 3 月 10 日，佛蒙特州的总检察长 (Vermont Attorney General) 对 Clearview AI 提起诉讼，声称 Clearview AI 违反了佛蒙特州的消费者权益保护法 (Vermont Consumer Protection Act) 和欺诈性数据获取禁制令 (Vermont's Prohibitions on Fraudulent Acquisition of Data)[99]，要求 Clearview 停止收集包含佛蒙特州居民的任何照片，同时删除或销毁已经收集的佛蒙特州居民的照片和面部识别标识符。

在人脸识别技术的目的尚未明确、缺乏法律规制的情形下，公众对 Clearview 安全性的质疑，将 Clearview 推向风口浪尖。

99. https://ago.vermont.gov/wp-content/uploads/2020/03/2020-03-05-Clearview-Letter-ID-227006.pdf

（2）大型科技公司对人脸识别技术持谨慎立场

人脸识别技术在不同皮肤、种族的识别率上存在差异，很可能引发种族歧视和性别偏见的风险。在 2020 年美国爆发“Black matters”运动的背景下，美国各大科技公司纷纷表态对人脸识别应用持谨慎立场，并对人脸识别技术的开发与应用做出了一定限制。

2020 年 6 月，IBM 公司宣布停止提供人脸识别技术的相关服务，因为担心这项技术可能被用来促进种族和性别歧视。IBM 首席执行官 Arvind Krishna 在一份递交到美国国会的公开信中写道：“IBM 坚决反对将任何技术用于大规模监视、种族定性、侵犯基本人权和自由，或任何与我们的价值观、信任和透明原则不符的目的。”[100]

亚马逊宣布正式禁止警方使用该公司的人脸识别软件一年。亚马逊的 Rekognition 也和其他任何人脸识别科技产品一样，能够使用人工智能（AI）来非常迅速地将一张警员用手机拍摄的照片与警方数据库内的数十万张照片进行比对。有研究显示，算法错误识别黑人和其他少数族裔人脸的可能性要大于白人。亚马逊在主张执法部门停用的同时，也呼吁美国立法者对人脸识别技术监管进行立法[101]。

2020 年 2 月，Facebook 向 Clearview AI 发送了停止和终止函，要求其停止为执法目的而使用用户图像来识别其身份。Facebook 发言人称：“抓取人们的信息违反了我们的政策，所以要求 Clearview 停止访问或使用来自 Facebook 的信息。”[102]

微软的人脸识别业务也在作出调整。2020 年 3 月底，微软正在逐渐放弃对人脸识别公司的投资，虽然它仍然通过其 Azure 云计算平台拥有自己的人脸识别技术。此前，微软曾于 2019 年删除了自称为全球最大的公开人脸识别数据库 MS Celeb。微软首席法律官 Brad Smith 曾表示，微软永远不会将人脸识别用于监视目的，出于对该技术可能导致侵犯公民权利和人权的担忧，将拒绝让执法部门接触这项技术[103]。

100. http://stock.10jqka.com.cn/20200610/c620923701.shtml

101. https://www.bbc.com/zhongwen/simp/business-53006438

102. https://baijiahao.baidu.com/s?id=1657968790226814447&wfr=spider&for=pc

103. https://tech.sina.com.cn/it/2020-03-28/doc-iimxxsth2230841.shtml?cre=tianyi&mod=pcpager_fintoutiao&loc=31&r=9&rfunc=100&tj=none&tr=9

（3）各州立法对人脸识别作出限制

基于人脸识别技术的快速发展及其引发的广泛担忧，美国各州开始积极围绕人脸识别展开立法工作。对于执法部门使用人脸识别技术的规制成为了立法中的侧重点。2020 年 10 月 14 日，佛蒙特州立法机关通过了美国全国范围内最严格的禁止执法人员使用面部识别技术的禁令[104]。佛蒙特州的美国公民自由联盟表示，该法律禁止警察未经立法机关同意使用该技术，这是“佛蒙特人隐私权保护的历史性胜利”，也是在该州“加强警察问责制和种族正义的重要一步”[105]。2020 年 12 月 3 日，威斯康星州麦迪逊市通过了一项法令，禁止包括执法部门在内的政府机构使用面部识别技术或从面部监控系统中获得的信息，该法令存在一项豁免，即允许将面部识别技术用于识别和查找人口贩运、儿童性剥削的受害者或失踪儿童，此项豁免旨在维持麦迪逊警察局目前对面部识别技术的有限使用且不再扩大使用[106]。

有的地区还通过了更为严格的人脸识别禁令。2020 年 9 月 4 日，美国俄勒冈州波特兰市禁止政府机构（包括当地警察）以及面向公众的企业（如商店、饭店和酒店）使用面部识别技术。除了停止在城市中使用监视技术外，新规则还阻止了波特兰的“公共场所中的私人实体”使用它，例如杂货店或比萨饼店，但它不会阻止人们在家中使用面部识别技术，例如使用 Apple 的 Face ID 功能以解锁 iPhone[107]。

104. https://www.wcax.com/2020/10/13/vermont-lawmakers-approve-ban-on-facial-recognition-technology/

105. https://iapp.org/news/a/vermont-legislature-passes-facial-recognition-ban/

106. https://iapp.org/news/a/wisconsin-city-bans-facial-recognition-technology/

107. https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html

02
欧盟：《人工智能白皮书》放弃对人脸识别的一刀切禁止

欧盟委员会今年 2 月发布的《人工智能白皮书》中也涉及了当下颇有争议的人脸识别问题。白皮书中针对人脸识别的表述变化反映出欧盟在这一问题上立场的变化。在《人工智能白皮书（草案）》中，欧盟委员会表示正在考虑实施史上最严的人工智能监管措施，将在 3 至 5 年的时间禁止公共或私人机构在公共场所使用人脸识别技术，同时成立相关监督机构，监督技术服务商及其客户对法规的执行情况，在此期间评估这项技术快速发展的影响，并制定风险管理措施以防止其滥用。此前，欧洲议会一份内部备忘录中讨论了人脸识别技术在安全领域的应用，该备忘录被披露后引发了民众强烈抗议，欧洲议会随后坚称没有引入人脸识别技术的计划。2019 年 12 月的《人工智能白皮书（草案）》正是在这一背景下出台[108]。

这一可能的禁令引发了广泛的讨论。业界普遍认为全面禁止人脸识别应用正如切肉刀“一刀切”的做法，而非使用手术刀精确打击来解决潜在问题。随后，在欧盟委员会 2020 年 2 月 19 日正式发布的《人工智能白皮书》中，不再包含全面禁止人脸识别技术的内容，而是规定了对唯一的生物识别信息的原则性规范。《白皮书》认为：基于生物识别信息的 AI 系统对基本权利的影响可能因使用目的、背景和范围不同而存在差别，欧盟数据保护规则原则上禁止以识别自然人为目的处理生物识别数据。根据 GDPR，这种处理只能在特定的条件下基于有限的理由进行，通常是出于重大公共利益的考虑，还应当符合相称性与必要性原则，遵守欧盟与成员国的法律规定，并采取相应的保障措施[109]。

欧盟有关人脸识别的规则仍在讨论过程中。2020 年 9 月 3 日，欧盟委员会 DG Connect 数字化产业部门的技术和系统负责人 Kilian Gross 称，所有的选择都还在考虑之中。

108. https://www.sohu.com/a/376535860_114988

109. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

03
中国：人脸识别成为公众话题，讨论框架仍待明晰

“人脸识别”在国内同样引起公众热议，但争议更多限于在公共场所应用人脸识别作为身份验证手段的合理性。学者在推动公众讨论中发挥了积极作用。其中又以浙江理工大学法政学院郭兵教授提起的“人脸识别第一案”和清华大学劳东燕教授发起的小区、地铁人脸识别讨论为代表。

2019 年 10 月，因为被“强制”要求采用“刷脸”方式入园，动物园年卡办理者郭兵在协商不成的情况下，以服务合同违约为由，将杭州野生动物世界告上法庭。 2020 年 11 月 20 日，杭州市富阳区人民法院作出一审判决，判决野生动物世界赔偿郭兵合同利益损失及交通费共计 1038 元，删除其办理指纹年卡时提交的包括照片在内的面部特征信息。

一审法院未对“人脸识别”作为入园方式的合理性问题展开论证，而是主要援引了《合同法》中的有关规则，认定动物园改变了合同约定的履行方式，客观上增加了郭兵履行合同的负担；对于动物园收集的人脸信息，由于合同当事人在办卡时签订的是采用指纹识别方式入园的服务合同，动物园收集人脸信息超出了《消费者权益保护法》第 29 条所确立的必要原则的要求，因此支持了郭兵主张删除人脸信息的请求。[110] 一审判决后当事双方均提起上诉，郭兵主张野生动物世界收集和使用其个人生物识别信息过程中存在欺诈行为，应当删除郭兵所涉全部个人信息；野生动物世界则主张收集郭兵个人生物识别信息并无不当，无需对相关信息进行删除。

在公共场所中广泛安装人脸识别系统也逐渐引起人们担忧。疫情期间，许多小区安装了人脸识别门禁。甚至在很多地方，原

110. https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=0d5660e6ee794498bbf8ac7d00a8dddb

111. https://mp.weixin.qq.com/s/Rr60t0xiFg6o4bylv3dE-g

112. https://mp.weixin.qq.com/s/Txea80NCr1XUIAb1ei5dZQ

113. http://credit.fzgg.tj.gov.cn/68/34288.html

114.《中国支付清算协会关于印发＜人脸识别线下支付行业自律公约（试行）＞的通知》，https://www.scpca.org.cn/Public/upload/file/20200326/1585194073124353.pdf.

有的指纹、门禁卡设备被取消，人脸识别成为居民出入小区的唯一验证方式。清华大学法学院教授劳东燕对此采取了积极行动，向物业公司和居委会分别寄达法律函，她认为在小区安装人脸识别装置并无必要，而且未经同意收集人脸数据，也违反现行的法律规定[111]。

人脸识别在国内的应用已扩展到令人意外的领域。为了业务上的方便，一些房地产售楼处开始采用人脸识别系统。网络上流传的买房人戴着头盔去售楼处看房的视频，引起舆论热议[112]。在《个人信息保护法（草案）》公开征求意见过程中，如何规范人脸识别成为公众的关切之一。此外，一些地方立法与行业规则也已展开对人脸识别的规范探索。12 月 1 日，天津市人大常委会通过《天津市社会信用条例》[113]，规定市场信用信息提供单位采集自然人信息应当经本人同意并约定用途，不得采集自然人生物识别信息等。1 月 21 日，中国支付清算协会发布《人脸识别线下支付行业自律公约（试行）》，从安全管理、终端管理、风险管理、用户权益保护等方面作出了规范，明确人脸信息的采集要坚持“用户授权、最小够用”，对原始人脸信息采取加密存储，与用户个人隐私进行安全隔离[114]。

结语

围绕人脸识别，未知与担忧并存。在欧洲，即便长期以来坚持对个人隐私保护的高标准，仍然没有“一刀切”地禁止人脸识别，但如何规制人脸识别应用已确定无疑成为核心议题；美国部分州已率先立法对执法部门的人脸识别技术应用作出规范；在中国，人脸识别也成为了公众热议的话题，人们逐渐意识到人脸识别的潜在风险，开始对现实生活中大量出现的人脸识别技术表现出警惕的心态，但整体来看尚未建立起成熟的讨论框架，相关的法律规则仍有待明确。

隐私安全计算——
开启数据价值创造新篇章

5

前言

当前，围绕数据已逐步形成三大共识：一是数据已成为数字经济时代的生产要素，为数字经济发展提供持续不断的新动能；二是数据权属与利益诉求全面觉醒，数据生态中的各方需共享数据利益，形成数据价值创造的持续激励；三是数据中的个人数据，需遵循严格的个人数据保护法规，保障个人隐私。这三大共识也对数据价值创造提出了切实挑战——如何在保护个人隐私、尊重他方数据权益基础上，实现数据价值挖掘？

应对这一挑战，技术领域展开了积极探索。以联邦学习（Federated Learning）、差分隐私（Differential Privacy）、安全多方计算（Secure Multi-Party Computation）为代表的隐私安全技术，尝试在保障隐私和数据安全的前提下，为进一步挖掘数据价值、创造社会福祉带来新的解决方案。

2020 年，隐私安全计算群落取得了长足的进步，业界将其称之为“隐私计算元年”。

01 保护隐私、增强用户信任的“利器”——隐私安全计算

隐私安全计算是指在保护数据本身不对外泄露的前提下能够实现数据分析计算的一类信息技术[115]，是包含人工智能、密码学、数据科学等众多领域的跨学科技术体系，其能实现“数据可用不可见”的效果，目前主要发展出三个技术方向[116]：

（1）为信息处理提供可信的执行环境

以机密计算（Confidential Computing）为代表，其核心思想为通过构建可信的处理环境而形成硬件安全“飞地”，数据仅在该安全区域内进行计算[117]。基于可信执行环境的隐私安全计算，一般将多方数据进行集中的中心化处理，除了硬件提供的安全程度不同之外，和普通的数据计算相比并无本质差别。目前引入可行执行环境较为成熟技术有 ARM 的 TrustZone 和英特尔的 SGX（Software Guard Extensions）。

（2）以分散的方式执行数据处理和分析

以联邦学习为代表，针对数据在不可信环境下的数据协作生产问题，通过不转移数据而转移计算机能力的逻辑解决问题[118]。“联邦学习”包括两个核心过程，分别是模型训练和模型推理[119]。在模型训练阶段，模型信息可以在各方交换，但数据不能交换；而在模型推理阶段，训练好的联邦学习模型可以放置于系统的各参与方，供多方共享。联邦学习最终能够实现“数据不动模型动”的效果，使得对数据的训练分散发生在各参与方中。例如，2017 年，谷歌便已在其 G-Board 上应用联邦学习技术，以实现在隐私保护的前提下，更新迭代手机输入法预测模型[120]。2019 年，英伟达医疗与 MELLODDY 合作，实现了在欧洲 10 家不同制药公司之间提供联合学习系统的效果[121]。

115. 中国信息通信研究院云计算与大数据研究所，CCSA TC601 大数据技术标准推进委员会：《安全多方计算技术与应用研究报告》，第 5 页。

116. See Gartner Identifies the Top Strategic Technology Trends for 2021 , available at https://www.gartner.com/en/newsroom/press-releases/2020-10-19-gartner-identifies-the-top-strategic-technology-trends-for-2021 (last visited on January 8 2021).

117. 中国信息通信研究院云计算与大数据研究所，CCSA TC601 大数据技术标准推进委员会：《安全多方计算技术与应用研究报告》，第 5 页。

118. 普华永道：《数据资产生态白皮书——构建可持续的数字经济新时代》，第 19 页。

119. 杨强，刘洋等著，《联邦学习》，中国工信出版社，2020 年 4 月出版，第 4 页。

120. See Federated Learning: Collaborative Machine Learning without Centralized Training Data，available at https://ai.googleblog.com/2017/04/federated-learning-collaborative.html (last visited on January 12, 2021).

121. See Perfect Harmony: Pharma’s MELLODDY Consortium Joins Forces with NVIDIA to Supercharge AI Drug Discovery , available at https://blogs.nvidia.com/blog/2019/08/08/pharma-melloddy-ai-drug-discovery-consortium/ (last visited on January 08 2021).

（3）处理和计算前进行数据转化

此类技术主要涉及密码学、信息混淆的相应技术，使得计算仅能对经加密的数据进行，意在达到“可证明的安全”，主要包含两类技术：其一，以差分隐私为代表的信息混淆技术；其二，以安全多方计算为技术框架、添加同态加密（Homomorphic Encryption）、零知识证明（Zero-knowledge Proof）、秘密共享（Secret Sharing）等密码学技术工具的技术集合。2017 年，苹果公司已尝试在其 iOS 系统中使用差分隐私技术对用户语言偏好进行分析[122]。

02
2020 年隐私安全计算的长足进展

（1）技术应用加速落地

Gartner 将隐私计算被作为 2021 年主要战略技术趋势之一[123]。而差分隐私技术也被《麻省理工科技评论（MIT Technology Review）》列入 2020 年十大技术突破之一[124]。隐私计算在金融、医疗、政务等各个场景的应用正加速落地。

在金融领域，微众银行 2020 年 4 月发布的《联邦学习白皮书 v2.0》显示，通过其多维度联邦数据建模，风控模型效果约可提升 12%，消费金融类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%[125]；在医疗领域，由翼方健数与厦门卫健委合作的临床辅助决策系统“探路者”，经过两年的试点后，于 2020 年 3 月开始在厦门全市 39 家社区医院全面上线。在不分享患者医疗信息的前提下，该系统通过隐私安全计算技术利用数据并能实现分级诊疗等效果[126]；在政务领域，2020 年美国人口普查的相关数据便采用了差分隐私技术，在对 3.3 亿美国居民人口普查的同时，保证这些数据无法“定位”到个人，从而保护个人隐私[127]。

122.《Differential Privacy Overview》，https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

123. See Gartner Identifies the Top Strategic Technology Trends for 2021 , available at https://www.gartner.com/en/newsroom/press-releases/2020-10-19-gartner-identifies-the-top-strategic-technology-trends-for-2021 (last visited on January 8 2021).

124. See 10 Breakthrough Technologies 2020, available at https://www.technologyreview.com/10-breakthrough-technologies/2020/#differential-privacy (last visited on January 08 2021).

125. 参见《联邦学习白皮书 v2.0》，载 https://aisp-1251170195.cos.ap-hongkong.myqcloud.com/wp-content/uploads/pdf/%E8%81%94%E9%82%A6%E5%AD%A6%E4%B9%A0%E7%99%BD%E7%9A%AE%E4%B9%A6_v2.0.pdf。

126.《翼方健数助力厦门智慧分级诊疗》，载凤凰网：https://finance.ifeng.com/c/80stCf292o9。

127. See Differential Privacy for Census Data Explained，https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx#:~:text=Differential%20privacy%20will%20mean%20that,used%20to%20protect%20small%20populations.

此外，在中国信息通信研究院与中国通信标准化协会大数据技术标准推进委员会于 2020 年 12 月 18 日评选出的 2020 年大数据“星河”隐私计算标杆案例中[128]，中国工商银行软件开发中心基于隐私计算的人脸识别信息保护、腾讯云计算公司开发的通过神盾联邦学习的信贷风控应用、深圳华大生命科学院与深圳华大智造科技股份有限公司为助力新冠疫情防控而开发的病毒基金组隐私计算平台等，均体现了今年隐私计算技术在多领域、多行业的加速应用。

（2）广阔发展前景吸引投资关注

隐私安全计算所具有的巨大发展潜力得到资本青睐。2020 年 2 月，大数据隐私计算平台公司锘崴科技完成数千万元人民币的 A 轮融资；5 月，洞见智慧科技有限公司完成约两千万元的天使融资；7 月，翼方健数公司也宣布完成了数千万美元的 B 轮融资。

国内外，各种隐私计算联盟也在不断组建，隐私安全计算的基础研究如火如荼。

国际层面，Linus 基金会设立的机密计算联盟（Confidential Computing Consortium）在本年会员数量猛增六成，其中不乏 Facebook、AMD、英伟达、埃森哲等企业[129]，而该联盟的创始会员更包括阿里、腾讯、ARM、谷歌、英特尔、微软、百度、华为等世界级企业[130]。该联盟 2020 年也发布了《Confidential Computing Deep Dive v1.0》《Confidential Computing: Hardware-Based Trusted Execution for Applications and Data》等技术报告[131]。

在国内，中国信息通讯研究院于 2020 年 11 月发布了《隐私保护计算技术研究报告》，并在 12 月 18 日牵头成立了公益性产业合作平台“隐私计算联盟”，以搭建政产学研合作交流平台，探索隐私计算基础核心技术，加速行业应用落地。

128.《星河璀璨 |2020 大数据“星河”案例入选公示》，载微信公众号“大数据技术标准推进委员会”，https://mp.weixin.qq.com/s/UYGZ7M-tK1lY2N8YyZdvcA。

129. See Facebook, Accenture, IoTeX, Nvidia and six other companies are joining the Linux Foundation’s Confidential Computing Consortium (CCC), increasing the size of the privacy-focused group by 60 percent, available at https://www.coindesk.com/facebook-iotex-and-r3-among-new-members-of-confidential-computing-consortium (last visited on January 08 2021).

130. See Confidential Computing Consortium Establishes Formation with Founding Members and Open Governance Structure – Member Comments, available at https://linuxfoundation.org/en/press-release/confidential-computing-foundation-founding-member-comments/ (last visited on January 08 2021).

131. See White Papers, available at https://confidentialcomputing.io/white-papers/ (last visited on January 08 2021).

（3）技术规范标准体系起步

2020 年，多家机构发布技术标准，以检验、评估隐私计算技术的实际效用与安全性。

2020.7.9 中国信息通信研究院连同多家企业联合发布了《基于多方安全计算的数据流通工具 技术要求与测试方法（修订版）》、《基于可信执行环境的数据计算平台 技术要求与测试方法》、《基于联邦学习的数据流通工具 技术要求与测试方法》[132]；

2020.12.18 针对隐私计算存在的计算过程和结果缺乏可验证性的缺点，中国信息通信研究院联合企业发布了《区块链辅助的隐私计算技术工具 技术要求与测试方法》，将区块链技术对计算的可信证明应用到隐私计算中，进一步完善隐私计算的技术规范体系[133]；

2020.12.30 全国信息安全标准化委员会开始对《信息安全技术 可信执行环境服务规范》征求公众意见。中国人工智能产业发展联盟发布了涉及可信执行环境、安全多方计算的《共享学习系统技术要求》（编号：AIIA/S 02001-2020）。

国际层面，IEEE 于 9 月发布了联邦学习相应标准——《IEEE 3652.1-2020 - IEEE Approved Draft Guide for Architectural Framework and Application of Federated Machine Learning》，隐私安全计算相关标准的探索正全面且系统化地推进中。

132.《最新发布 • 隐私计算系列三项标准正式亮相》，载微信公众号“大数据技术标准推进委员会”：https://mp.weixin.qq.com/s?src=11&timestamp=1607256326&ver=2750&signature=2uyN2SY6M2xwSDFCPmUI*5DMcKMnhjtW*ci*I9U-IPWz204PuHP03*SN5mbVZIvVGVO4Z-3CeTG5gTSO-ZovHUCEszI7-WGML7XBrQsSvepaa2v2yl30f8rleSbzYxiw&new=1。

133.《隐私计算系列再添新标准 • 区块链辅助的隐私计算技术工具标准发布》，载微信公众号“隐私计算联盟”：https://mp.weixin.qq.com/s/cs0WdMOmNvrqC3yodo7hcw。

03

法律制度对隐私计算的审视——隐私安全计算的合规要点

（1）隐私安全计算需保证手段及目的的合法性

通过去标识化、匿名化的方式能够降低识别信息主体的风险，因此，各国个人信息保护法律中也不同程度地豁免相应的合规要求。但目前，针对隐私安全计算技术是否符合法律法规要求的问题，答案并不清晰。以匿名化的方式能享受合规豁免，但需要满足事前、事中、事后持续的隐私风险评估与安保措施，其适用的门槛较高。

隐私安全计算中的联邦学习主要通过避免数据转移来达到数据可用的效果。此时是否仍旧受到用户同意的限制，或者是否能够基于正当利益而进行豁免，也需予以明确；在借助隐私安全技术实现数据处理的安全性后，企业仍应注意处理目的的合法性，保证数据处理目的与服务本身存在合理关联。正如在 TO C 场景中，苹果应用差分隐私对众多用户的个人数据进行了优化分析，并最终应用到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[134]。

134. 参加王融：《再谈数字社会的信任基石—技术与制度，如何形成互动式进步？》，载微信公众号“腾讯研究院”，https://mp.weixin.qq.com/s/cm5CxwXyliOC_aTgXEZU4g。

（2）保证处理过程对用户的透明度

隐私安全计算避免了原始数据的转移或对数据进行加密或混淆而保证安全性，但是其本质上仍旧需要对多方数据进行分析处理，这使得它在某种程度上依然影响着消费者的利益，这是在讨论隐私安全计算合规问题时无法回避的问题[135]。算法的不透明性仍然对个人信息保护法规中所要求的“透明”“目的限定”等原则提出了挑战。对于用户来说，信息处理的黑箱问题更加突出，数据处理者应当尝试明示基本逻辑的方式来解决算法的可解释问题。

（3）责任与安全保障原则

通过隐私安全计算技术处理数据，企业需要保证以下四方面的隐私性：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测到；训练数据隐私，保证在数据训练过程中的安全性与私密性；输出隐私，保证除了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。

135. 参见闫树、袁博：《隐私计算：实现数据价值释放的突破口》，载微信公众号“中国信通院 CAICT”，https://www.secrss.com/articles/23978。

结语

隐私安全计算为释放数据红利带来极大利好。据估计，在2025 年前将有一半的大型企业、组织采用隐私安全计算技术，以在不受信任的环境和多方数据分析中处理数据[136]。国内外各行业均对隐私安全计算均投以极大关注。当然，没有任何技术是没有缺陷的，在对隐私安全计算抱以积极乐观态度的同时，也应当注意到其同样需要在实践中不断完善，真正实现“隐私保护”与“数据共享”的双赢。

136. See Gartner Identifies the Top Strategic Technology Trends for 2021 , available at https://www.gartner.com/en/newsroom/press-releases/2020-10-19-gartner-identifies-the-top-strategic-technology-trends-for-2021 (last visited on January 8 2021).

数字广告行业——
隐私保护背后的商业模式之争

6

前言

2020 年，数字广告行业酝酿着一场巨变。6 月，Apple 公司宣布了一项新的隐私规则，开发者在对用户进行广告跟踪时需要事先取得用户的明确同意。受此新规影响，数字广告行业业务收入将可能大幅降低，引发行业反弹，并由此展开了互联网不同商业模式的质疑与对峙。以数字广告为主要收入来源的 Facebook 指责 Apple 以保护用户隐私为名，采取反竞争的商业行为，强化了操作系统对数据和流量的控制，这对小型 App 开发者造成长期损害。

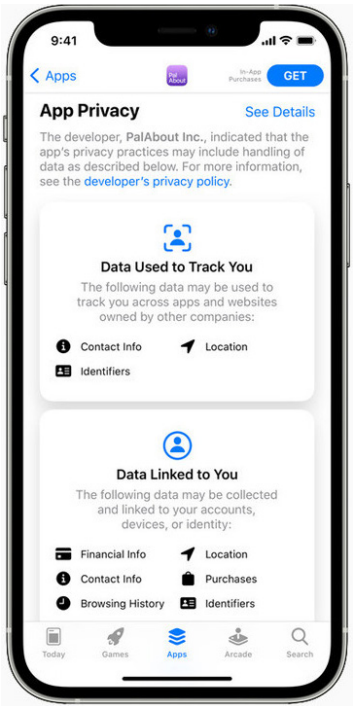
01 Apple 公司隐私新规始末

Privacy

（1）Apple 宣布将推行隐私新规

2020 年 6 月，Apple 公司举行了 2020 线上发布会，宣布将向 iOS 和 macOS 用户推出全新的隐私和安全功能。具体包括以下内容：

第一，在用户同意机制上，Apple 要求开发者在进行跟踪之前需要事先获得用户的同意。在此之前，开发者可以自由跟踪用户设备 ID，除非用户选择退出。这一修改相当于将“默示同意、明示退出”机制更改为“明示同意”机制。



第二，对于 App Store 中的所有 App，均适用隐私披露提示政策。在 App 的运行过程中，将对 App 正在进行的跟踪行为向用户明确提示。每个 App 还应当准确地披露跟踪用户的数据类型，清晰展示相关详情，例如要采集的数据种类、是否会分享以及将与哪些主体分享、数据的用途及可能的结果，从而帮助用户根据这些信息作出决定。

如果 App 未能获得用户同意，那么将不再能获取对应 Apple 设备的 IDFA 码。IDFA 是 iOS 设备广告追踪的标识符，也是 Apple 允许广告商用来了解其手机上的广告行为的唯一标识。

简单来说，Apple 公司计划为用户提供一个隐私选项，让其决定是否分享自己的 IDFA 以实现数据跟踪。Apple 认为，“隐私

是每个人的基本权利，同时也是 Apple 的一项核心价值观。你的设备在生活的方方面面都发挥着重要作用。其中哪些东西可以分享、以及与谁分享，都应该由你来决定”[137]。

（2）以 Facebook 为代表的开发者表达强烈异议

这一新规则将有助于用户控制自己的数据分享，但同时也使广告商跟踪用户变得更加困难。Apple 隐私新规在开发者中引起了强烈的反对声音，开发者担心 Apple 这一调整会使得用户倾向于拒绝启用跟踪功能，而开发者的定向广告业务严重依赖于对用户的跟踪行为。

作为一直以来将广告收入作为主要收入来源的开发者，Facebook 对 Apple 的这项隐私新规表达了强烈的反对意见。Facebook 表示，Apple 公司的这项新规将使得广告跟踪成为一种不太有效的获得收入的方式。

2020 年 8 月 27 日，Facebook 称 Apple 的这项更改将可能会损害小型 App 开发者。新规意味着终止包括用于广告目的而收集用户数据的 Audience Network 工具，而小型公司使用 Facebook 这一工具来投放其目标广告[138]。

137. https://cloud.tencent.com/developer/news/648986

138. https://www.reuters.com/article/us-facebook-advertising-apple/facebook-says-apples-new-privacy-rules-could-hurt-smaller-app-companies-idUSKBN25M2BO

在开发者的反对声音中，Apple 的这项新规出现了转折。2020 年 9 月 4 日，Apple 公司宣布将暂停这一计划的推行。Apple 公司表示，它希望“给开发人员必要的时间进行必要的更改”，这一更改现在将在“明年年初”生效。尽管 Apple 这一新规将暂缓推行，但这项新规引发各项的争议仍在持续。

2020 年 12 月 14 日，Apple“隐私标签”上线，要求 Mac 和 iOS App Store 中的 App 提供其隐私政策的摘要，从而使得用户可以掌握每个 App 收集和访问的数据及其处理方式的详细信息

标签分为三类：

标签将显示 App 收集的位置数据、财务数据和社交联系信息等，以及信息是否链接到服务账号或设备标识符，还将显示 App 将如何共享这些信息。

2020 年 12 月 17 日，Facebook 进一步批评了 Apple 的隐私新规。Facebook 在《纽约时报》、《华尔街日报》和《华盛顿邮报》等报纸投放了整版广告，再次抨击 Apple 利用数据隐私保护措施实行反竞争的商业行为，而 Facebook 正在为各地的小企业与 Apple 抗争。

Facebook 广告和业务产品副总裁 Dan Levy 表示，Apple 的隐私新规将使小型开发者更难从广告中获得收入，这可能会迫使他们尝试开辟其他类型的收入来源，比如付费订阅，而 Apple 将从中抽成 [139]。

139. https://www.axios.com/facebook-war-apple-ad-privacy-cf90d171-9eed-4751-bb9e-fd0ca444f7cb.html

可以说，Facebook 与 Apple 对峙的背后，实际是互联网两种不同商业模式之争。Facebook 所支持的数字广告行业，中小企业可以通过基于行为跟踪的广告投放获得收入，从而获取市场发展机会，并向用户提供免费服务。这在数字媒体行业尤为突出，很多提供免费内容的服务提供者，无法形成用户付费订阅模式，但可以通过加入广告联盟获得收入。这也正是互联网早期起步的核心商业模式；而以隐私为核心卖点的 Apple，则主要以付费订阅模式为主，作为硬件设备、操作系统、App Store 的综合服务提供者，Apple 在其生态体系内，形成了抽佣模式，即凡是在 App Store 上架的 App，必须在销售数字化商品和服务时使用苹果的支付工具，而销售所得的最高 30% 都是归苹果所有的“佣金”。不难理解，Apple 努力推动数字服务的有偿付费模式。在 Facebook 与 Apple 的对抗中，Facebook 也重点指责 Apple 的抽佣问题。2020 年 11 月 17 日，Facebook 表示将帮助热门游戏《要塞之夜》的开发者 Epic Games 起诉 Apple，指控 Apple 从 App Store 购买或下载 App 的内置付费和订阅中抽取高达 30% 的佣金。

Apple 也正在作出妥协。2020 年 11 月 18 日，Apple 宣布将推出“App Store 小型企业计划”，将惠及广大在 App Store 中销售数字商品和服务的开发者，降低付费 App 和 App 内购买的相关佣金。若开发者在上一个日历年的收益在 100 万美元以下，将有资格参加该计划，并享受降至 15% 的佣金费率。但针对销售数字商品和服务收益超过 100 万美元（指开发者扣除佣金后的收入）的 App，App Store 的标准佣金费率仍为 30%。App Store 小型企业计划于 2021 年 1 月 1 日正式启动[140]。

140. https://www.apple.com.cn/newsroom/2020/11/apple-announces-app-store-small-business-program/

最新进展：

2021 年初，Facebook 对于 Apple 公司隐私新规的态度发生转变。1 月 7 日，Facebook 表示：尽管 Facebook 不同意 Apple 的隐私更改计划，但 Facebook 别无选择，只能遵循这些变化，否则 Apple 将有可能将 Facebook 彻底从 App Store 中移除。据 1 月 29 日报道，Facebook 或将考虑对 Apple 提起反垄断诉讼，主要针对 Apple 即将推出的 iOS 14 隐私新规，以及违反隐私新规将在 App Store下架的规定，指控 Apple 滥用其在智能手机市场的权力，强迫应用开发者遵守 Apple 自己开发的手机应用不必遵守的 App Store 规则。

Facebook 表示，跟踪透明功能要求 App 跟踪用户之前需获得用户同意，如果用户选择退出跟踪，将对广告目标定位、优化和衡量广告活动的有效性产生重要影响，广告效果将打折扣。Apple 的这一变化将使它自己受益，但同时损害整个行业，更会损害通过个性化广告实现增长的企业，“我们认为个性化广告和用户隐私可以共存”[141]。

141. https://finance.sina.com.cn/tech/2021-01-07/doc-iiznezxt1025742.shtml

142. https://finance.sina.com.cn/tech/2021-01-07/doc-iiznezxt1025742.shtml

143. https://developer.android.com/about/versions/11/privacy?hl=zh-cn

02 Google 在隐私功能上的积极改变

一直以来，Apple 将隐私保护作为其差异化竞争的重要因素，不断传达出这样的信息：其硬件和服务比竞争对手更安全。由于 iOS 和 Android 生态之间的竞争，Apple 也间接推动了 Google 不断加强 Android 系统的隐私保护[142]。在 2020 年 9 月发布的 Android 11 中，Google 增加了一系列的重大隐私权变更，例如，引入“单次授权”，用户授权 App 访问设备的麦克风、摄像头或位置信息的访问权限仅在授权当时有效；App 在后台访问位置信息时，也将需要执行更审慎的操作来授予权限，App 需首先请求在前台访问位置，再由系统将用户带到“设置”中完成权限授予[143]。

Google 也正在对 Chrome 的隐私功能作出积极改进。2020 年 7 月，Google 逐渐淘汰 Chrome 浏览器中第三方 cookies 的计划取得了新的进展，谷歌宣布将与开发者一起开始测试新的“信任令牌（Trust Token）”方案[144]。

与 Cookie 机制不同，信任令牌在不需要知道用户身份的情况下对用户进行身份验证。信任令牌将无法在整个网站上跟踪用户，但是它们仍可以让网站向广告客户证明实际用户访问了广告或点击了广告。Google 还将对“关于此广告”标签做出调整，新标签将提供经过验证的广告客户名称，用户将可获知哪些公司将自己定位为目标客户，以及 Google 如何收集个人数据。

除此之外，Google 还宣布了 Chrome 浏览器的扩展程序，目前处于 Alpha 模式，称为 Ads Transparency Spotlight，该扩展程序提供“有关在网络上看到的所有广告的详细信息”。用户将能够

144. https://cn.engadget.com/google-tests-ad-trust-tokens-110022198.html

145. https://www.theverge.com/2020/7/31/21349538/google-changes-ads-data-cookies-privacy

查看给定页面上的广告的详细信息，了解为什么广告会显示在页面上，以及页面上存在的其他公司和服务的状态列表，例如“网站分析”或“内容交付网络”[145]。

2020 年 10 月，Google 与开发者和广告技术供应商就“受限广告（Limited Ads）”功能展开了讨论，该功能将使开发者可以简便地向不同意共享其 Cookie 和其他标识符的用户发送非针对性广告。此前，谷歌决定与 IAB（Interactive Advertising Bureau，互动广告局）就欧洲透明和同意框架的更新版本（当前版本为 TCF 2.0）进行整合，这是一个符合欧洲《通用数据保护条例》（GDPR）的可互操作的行业框架，使用户能够对出版商、广告商和供应商如何处理其数据作出同意或拒绝。

TCF 包括 12 个“目的”，用户可以分别就各项目的表示同意或拒绝，例如：“目的 1”-- 在设备上存储和 / 或访问信息 -- 或“目的 4”-- 选择个性化广告。谷歌表示，当目的 1 的同意缺失时，将要求发布受限广告（Limited Ads），也即非针对性广告。开发者可以根据 GDPR 以“数据控制者的合法利益”为理由处理个人数据，“合法利益”基础要求企业进行测试，以确定其收集数据的利益是否超过个人不被收集数据的利益。

对此，行业观察家表示，尽管 Google 尝试对授权同意的场景进行细分，但当用户面对这些选择时，通常不会对同意或不同意分享数据的目的进行区分，他们通常会选择“全部拒绝”或“全部接受”。因此，如果用户决定点击“全部拒绝”按钮，App 开发者将不能以合法利益基础开展数字广告业务。

Google 此项功能也引发了开发者和广告技术供应商的质疑。开发者和广告技术供应商表示，Google 的此项功能将阻止他们从用户中获益。法国在线分类公司 Leboncoin Group 的广告副总裁 Fabien Scolan 表示，对于 Limited Ads，Google 实际上是在让用户决定一个网站能否向他们投放定向广告，“Google 没有权力那么做，这应当是网站自己来决定的事”[146]。

146. https://digiday.com/media/publishers-and-ad-tech-vendors-find-googles-new-limited-ads-feature-to-be-well-limited/

结语

Apple 隐私政策的调整对数字媒体行业一直以来的商业模式提出了挑战。数字媒体行业通常提供免费产品聚集流量，再依靠广告业务变现。其中，个性化的定制广告将能够大幅度提高广告的效益，从而构成了广告变现能力的基础。正如 2018 年扎克伯格在回答参议员关于 Facebook 如何通过免费服务来赚钱的问题时所称，“我们投放广告”。广告业务常年占据 Facebook 90% 以上的收入来源。广告收入也构成了大量公司的主要收入来源。

那么用户对于定制广告的态度如何？在 2018 年欧盟《通用数据保护条例》（GDPR）生效后，一家荷兰公共广播机构开始以清晰的、直接的方式提示所有访问其网站的访问者，“是否选择要与广告商共享数据?”，结果 90%的人选择退出，该机构事实上相当于完全放弃了定制广告收入[147]。

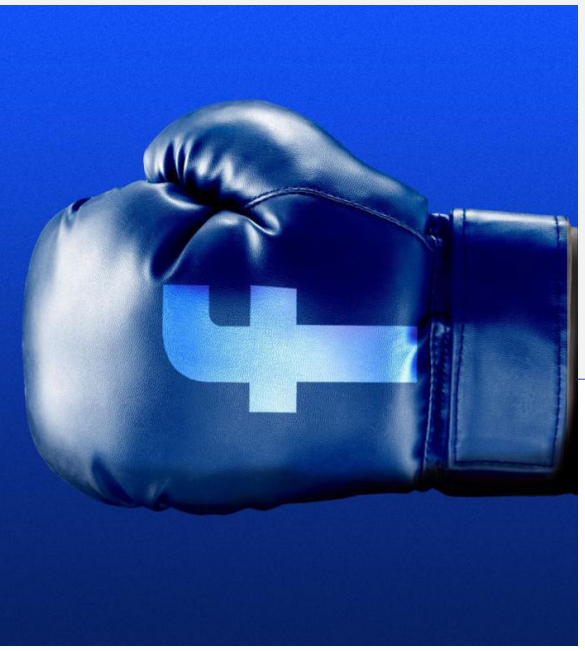
由此看出，用户的选择倾向与数字媒体的商业模式之间的分野是问题产生的根源。对于数字媒体服务提供者而言，用户让渡一部分广告追踪的权利，实质上是作为获得免费服务的对价。而用户通常不会从商业模式存续的角度去考量，或者是出于情感上对广告推送的厌烦，或者是对开发者跨 App 跟踪与精准营销的未知与不安，可以预见到，用户将倾向于做出拒绝广告跟踪的选择。

目前来看，数字媒体行业可能采取的应对与调整主要包括两种路径。

第一种是通过采取技术措施以替代原有的跟踪机制，既能够合乎系统开发者的新规范，又能够继续实现广告业务精准营销，例如 Google 的“受限广告（Limited Ads）”新功能，以及一些综合性媒体，例如 Verizon Media 推出的作为 Cookie 替代方案

147. https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/

148. https://www.mediapost.com/publications/article/358243/verizon-media-unveils-cookieless-id-to-replace-t.html



ConnectID[148]。但这些技术层面的解决方案的效果是否足够理想仍不确定，替代方案下的定制广告精确度可能难以达到原有水平，开发者的广告收入仍面临锐减风险。

第二种路径则是在商业模式上进行整体调整，由原来的以广告收入为基础的免费服务模式转向付费服务模式。当开发者难以从广告中获得足够收入时，将可能会转向付费订阅服务。但这样的商业模式的转变并非适合所有开发者。其中，《纽约时报》是难得取得成功的案例之一。《纽约时报》自 2011 年开始实行付费数字订阅，截止 2020 年 1 月已有超过 500 万订阅用户，减小了其对于广告业务的依赖程度[149]。而对于大量的社交网络服务，付费将为用户的使用增加壁垒，且并不符合产品本身的逻辑，对于这些数字服务提供者来说，保留免费模式的前提下增加适用于附加功能的付费选项是一个可能的选择。但付费订阅模式又可能会引发新的争议，系统开发者通常会从 App 的收费中进行抽成，例如前文提到的游戏开发者 Epic Games 起诉 Apple，指控 Apple 针对从 Apple Store 购买或下载的 App 内置付费和订阅中抽取高达 30% 的佣金。

而从市场竞争的视角来看，目前对行为广告模式的调整，从某种程度上强化了系统开发者，也就是 Apple 和 Google 这样的操作系统服务提供者在数据和流量上的控制地位。在过去，App 的开发者可以基于其收集到的用户信息，参与数字广告业务，并获得广告收入。而在新的机制下，系统开发者在赋予用户更充分的选择权的同时，也减损了 App 开发者获取数据和流量的权利。对广告业务依赖较强的弱势开发者将面临着被挤出的风险，除非接受系统开发者的规则或向其寻求合作，这样的格局实际上为系统开发者构建私域流量生态提供了条件，引发更为深刻的市场竞争质疑。

149. http://m.cankaoxiaoxi.com/culture/culture20200116/2400304.shtml

数据跨境流动——
规则的“破”与“立”

7

前言

2020 年，外部环境剧烈变化，数据跨境流动规则持续深入调整，中国成为规则建设的积极贡献者。在海外，欧盟法院继“安全港”之后再度废除“隐私盾”（Privacy Shield），欧美跨大西洋数据传输需要新的协调。英国脱欧进程推进，英国与欧洲大陆间数据流动再添变数；在国内，《个人信息保护法（草案）》对个人数据跨境流动的未来制度方向有了更清晰的定位，各自贸港、自贸区陆续发布方案，均提出要创新跨境数据流动管理机制。在国内数据跨境相关制度的探索之外，《区域全面经济伙伴关系协定》（Regional Comprehensive Economic Partnership，简称 RCEP）的签订以及其他双多边国际协定的推进，也为我国在不同区域内的数据跨境流动注入新的活力。

01 欧美“隐私盾”被判无效后，跨大西洋数据传输路径需重新构建

（1）“Schrems II”判决否定欧美“隐私盾”效力

2020 年 7 月 6 日，欧盟法院发布“Schrems II”案判决，认定作为欧美间数据传输通道的“隐私盾”协议（EU-U.S. Privacy Shield Framework）无效[150]。该判决认为，美国国内法对公权力访问数据的限制不能满足欧盟法的要求，不符合比例性和严格必要等原则。在美国的监视行为中，欧盟数据主体也缺乏可诉诸的司法补救措施[151]。

这也是欧盟法院继 2015 年判决“安全港”协议（EU-U.S. Safe Harbor Framework）无效后，再一次对欧美间跨境传输机制作出的否定性判决。

150. See The CJEU judgment in the Schrems II case, available at https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

151. 判决原文见：http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227.

（2）“隐私盾”判决后的各方反应：执法跟进与多方表态

爱尔兰数据保护委员会对 Facebook 下达数据跨境传输禁令

2020 年 8 月 28 日，爱尔兰数据保护委员会向 Facebook 下达了初步决定，认为其标准合同条款也不能有效保护数据主体权利，因此限制其将数据传输至美国，以执行欧盟法院“Schrems II”判决，此外还要求 Facebook 在三周内对此进行答复[152]。9 月 11 日，Facebook 向爱尔兰高等法院提起诉讼，称该初步决定将对其数据传输机制产生重大不利影响，且设定的答复期限不符合程序规定。9 月 14 日，爱尔兰高等法院认为 Facebook 可以就此提起司法审查，并暂停了数据保护委员会对 Facebook 在欧美间数据传输的调查[153]。

欧盟、美国官方机构相继发布文件、声明

美国方面

7 月 16 日，美国商务部长 Wilbur Ross 就此发布声明称，尽管美国商务部对欧盟法院的这一判决表示失望，但其仍在研究该判决，以充分理解其实际影响[154]；9 月 28 日，在隐私盾判决之后，美国政府发布了一份白皮书，以帮助企业、机构评估其欧美间数据传输是否满足新的要求。文中提到，美国大多数公司“不会处理美国情报机构要求的数据，并且也没有理由认为它们会这样做”。[155]

欧盟方面

7 月 17 日，欧盟数据保护委员会（European Data Protection Board，简称 EDPB）强调，其将继续发挥建设性作用，确保跨大西洋的个人数据传输，并随时准备向欧盟委员会提供援助和指导，帮助其与美国一起建立一个完全符合欧盟数据保护法的新框架[156]。10 月 29 日，欧盟数据保护监

152. See Ireland to Order Facebook to Stop Sending User Data to U.S., available at https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980#:~:text=A%20European%20Union%20privacy%20regulator,precedent%20for%20other%20tech%20giants (last visited on January 8, 2021)..

153. See Irish High court freezes probe into Facebook's EU-U.S. data flows, available at https://www.reuters.com/article/uk-facebook-privacy/irish-high-court-freezes-probe-into-facebooks-eu-u-s-data-flows-idUKKBN2652FA?edition-redirect=uk (last visited on January 12, 2021).

154. See U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows, available at https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and (last visited on January 8, 2021).

155. See Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision, available at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000kyhX (last visited on January 8, 2021).

156. See Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, available at https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en (last visited on January 8, 2021).

157. See Strategy for EU institutions to comply with “Schrems II” Ruling, available at https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en (last visited on January 8, 2021).

158. See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en (last visited on January 8, 2021).

管局（European Data Protection Supervisor，简称 EDPS）发布了一份战略文件，以帮助欧盟机构遵守欧盟法院的“隐私盾”判决，其中也建议欧盟机构避免将个人数据转移到美国以进行新的数据处理或者需要根据新的变化签订新的合同[157]；11 月 11 日，EDPB 发布了“关于补充措施的建议”[158] 和“关于针对监控措施的欧洲基本保障的建议”[159]，以协助数据控制者和处理者在使用标准合同条款或具有约束力的公司规则方面达到欧盟法院的要求；11 月 12 日，欧盟委员会提出了两部新的标准合同条款（SCC）草案：一部草案用于数据控制者和处理者之间的合同，另一部用于向欧盟境外的数据传输。以上 SCC 草案通过后将取代旧文本，以使其符合《通用数据保护条例》以及欧盟法院“隐私盾”判决的要求[160]；此外，德国及其多个联邦州、捷克、芬兰、法国、爱尔兰等几乎每个欧盟成员国数据保护机构均发表了相应的声明[161]。

而在美国与欧盟发布以上声明、文件期间，美国商务部部长 Wilbur Ross 与欧盟委员会司法专员 Didier Reynders 也于 2020 年 8 月 10 日发表了共同声明，称双方已经就此展开讨论，以评估、增强欧美间的隐私保护框架以符合“Schrems II”判决[162]。

组织、企业发表评论

针对“隐私盾”判决以及其后续的影响，不同企业、组织也发表了评论。2020 年 7 月 16 日，微软首席隐私保护官 Julie Brill 发布文章，向用户承诺微软服务在欧美之间的数据跨境传输安全，在“隐私盾”之外仍可基于 SCC 进行合法的数据传输。此外，也声明微软将继续致力于保护消费者隐私安全，也将继续披露涉及美国政府向微软提出的国家安全令的透明度报告（U.S. National Security Orders Report）[163]。2020 年 12 月 3 日，美国知名科技创新智库“信息技术与创新基金会”（Information Technology and Innovation Foundation，简称 ITIF）发布报告，认为“隐私盾”失效将对所有不同规模的企业产生不合理影响，并将阻碍跨大西洋的贸易与创新[164]。

159. See Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en (last visited on January 8, 2021).

160. See European Data Protection Board - 42nd Plenary session: Presentation of two new sets of SCCs & EDPB adopts statement on ePrivacy Regulation, available at https://edpb.europa.eu/news/news/2020/european-data-protection-board-42nd-plenary-session-presentation-two-new-sets-sccs_de (January 8, 2021).

161. See Reactions to the CJEU's judgment Schrems II, available at https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2020/09/reactions-to-schrems-iiupdated-overviewkoe-final.pdf.

162. See Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross,, August 10 2020, available at https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en#:~:text=Search-,Joint%20Press%20Statement%20from%20European%20Commissioner%20for%20Justice%20Didier%20Reynders,Secretary%20of%20Commerce%20Wilbur%20Ross&text=This%20judgement%20declared%20that%20this,Union%20to%20the%20United%20States (last visited on January 8, 2021).

163. See Assuring Customers About Cross-Border Data Flow, available at https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/ (last visited on January 8, 2021).

164. See 'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation, available at https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic#:~:text=In%20Schrems%20II%2C%20the%20ECJ,to%20those%20in%20the%20EU (last visited on January 8, 2021).

（3）“隐私盾”失效后欧美跨大西洋数据传输并非一片昏暗

尽管欧盟法院宣告了欧美“隐私盾”协议无效，但法院肯定了另外一条数据跨境转移的合规路径——标准合同条款（SCC）的效力，其也进一步指出，数据出口方和接收方都有义务在个案中验证数据接收国是否能够达到欧盟同样标准的保护，当 SCC 的条件不能被遵守时，应立即中止或禁止数据转移或者要求增加额外的保护措施[165]。

脱离开纯粹的法律技术视角，从数字经济发展与数据跨境流动的紧密关系来看，会发现数据跨境流动的前景也并非一片昏暗：促进数据在全球范围内的流动的共识并没有因为欧盟法院废除“安全港”、“隐私盾”而被打破。欧美对于隐私（数据 / 个人信息）应该得到保护这一问题没有分歧，美国和欧盟均认可应对数据提供较高水平的保护。正如 ITIF 在其报告中指出：欧洲和美国的共同点比通常承认的要多，尤其是与中国相比[166]。

双方的争议点在于如何协调国家安全与数据保护之间的关系。欧盟并不反对公权部门出于国家安全访问数据，欧盟法院在 Schrems II 案的判决中指出，第三国当局可出于公共安全、国防和国家安全的目的处理出于商业目的移转的数据，但应有足够的保障机制防止个人权益被过度侵犯。显然，“隐私盾”协议无法提供足够的保障措施。欧美的这一分歧，代表了跨境数据流动的规则协商步入了深水区，自此贸易语境下的数据商业性流动和执法语境下的政府数据获取两个议题之间更加紧密结合[167]。

165. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

166. See ‘Schrems II’: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation, available at https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic#:~:text=In%20Schrems%20II%2C%20the%20ECJ,to%20those%20in%20the%20EU (last visited on January 8, 2021).

167. 王融、朱军彪：《自由贸易试验区扩容，如何创新跨境数据流动制度？》，载微信公众号“腾讯研究院”：https://mp.weixin.qq.com/s/5xGrfSq1ETteiLjGy8XJVg。

02 英国脱欧后与欧洲大陆间数据传输问题仍有待协调

2020.10

自 2020 年 10 月开始，英国政府便持续更新、发布在脱欧过渡期结束后应如何处理数据保护和数据流动的指南[168]。该指南涵盖了在过渡期结束而英国与欧盟未达成相应合意的情况下，相关企业如何确认数据传输标准合同条款以及 GDPR 等法规在 2021 年 1 月 1 日之后的适用范围问题。

2020.12.17

欧洲数据保护委员会（EDPB）通过了《关于英国脱欧过渡期结束的声明》，明确英国脱欧后便不再适用 GDPR 确定的数据自由流动框架，从欧洲经济区向英国的数据传输将被视为“向第三国的个人数据传输”，因此需要评估英国与欧盟之间的其他合法数据传输途径[169]。

2020.12.24

英国与欧盟于 2020 年 12 月 24 日签订的《贸易与合作协议》为脱欧后双方数据传输问题设定了临时宽限期，宽限期内基于商业和执法目的的数据传输仍可继续进行，而该宽限期将有效至欧盟认定英国为“充分性地区”且最长为六个月[170]。

168.《Guidance: Using personal data in your business or other organisationUsing personal data in your business or other organisation》，https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation.

169. See Statement on the end of the Brexit transition period Adopted on 15 December 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_brexit_en.pdf (last visited on January 8, 2021).

170. See Using personaldata in your business or other organization - What action you need to take regarding data protection and data flows with the EU/EEA, https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation.

03
中国：多路径探索数据跨境流动未来图景

立足于发展中国家国情，我国积极探索数据跨境流动的“中国方案”。整体上，我国在重点领域提出了本地化要求，在坚持改革开放不动摇、坚持国内国际双循环的基本方略之下，也在积极为数字经济全球化发展探索相匹配的制度供给，围绕数据跨境流动议题，提供更加多样化的流动机制。对于数据跨境流动机制的探索，我国国内正沿着“自上而下”和“自下而上”两条路径并行展开；而在国际上，以RCEP 的签署为标志，我国区域间数据跨境流动也呈现“增容扩圈”积极态势。

（1）“自上而下”与“自下而上”的双路径探索

“自上而下”探索数据跨境制度

我国在 2016 年《网络安全法》首次明确相关政策立场，提出针对关键基础设施信息的本地化存储及境外传输安全评估要求后，又相继于 2017 年 4 月、2019 年 6 月，分别公布了《个人信息和重要数据出境安全评估办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》，逐步探索数据跨境数据流动管理机制。

2020 年 10 月公布的《个人信息保护法（草案）》第三章也针对个人信息的跨境传输搭建了完整框架。总体上，与国际一般规则相衔接，数据跨境流动机制包括了多元化机制，涵盖了监管部门组织的安全评估、第三方机构认证、数据出境方与接收方的标准合同等。

此外，在金融信息跨境流动方面，2020 年 2 月 13 日，中国人民银行发布了《个人金融信息保护技术规范（JR/T0171-2020）》，相较于《网络安全法》，标准 7.1.3 条 d) 项对个人金融信息数据出境提出了更高的要求：在向境外机构提供个人金融信息时，金融机构除了需要进行安全评估、取得用户同意、符合国家法律规定之外，还需要与境外机构通过签订协议、现场核查等方式明确职责义务。

“自下而上”由各自贸区、自贸港创新管理机制

发展数字贸易，离不开数据跨境流动的支撑。它的重要性不亚于税收、业务开放、数字基础设施建设等优惠政策。今年以来包括海南自贸港、上海自贸区临港片区，以及北京、浙江等多地自贸区方案都无一例外在数据跨境流动制度上着墨许多。目前，中国大陆 31 个省级行政区中已有 21 个被批准建立自由贸易实验区 [171]。2020 年 8 月 12 日，商务部发布《全面深化服务贸易创新发展试点总体方案》，指出要顺应新形势下数字经济的发展趋势，在数字贸易领域，推动数字营商环境便利化，探索完善数字贸易的监管模式，探索数据流动与监管的创新和开放，在试点地区开展数据跨境传输安全管理试点。

相关的试验改革也箭在弦上。例如，《海南自由贸易港法（草案）》已于 2021 年 1 月 4 日公布，相关立法程序正在稳步推行，草案第 42 条明确“建立安全有序便利的数据流动管理制度”、“国家支持海南自由贸易港探索加入区域性国际数据跨境流动制度安排”，第 54 条规定“网络安全等级保护制度”等。此外，各地几乎同步重点发力数字贸易，呈现地方竞争态势，这种自下而上的、从实际产业发展实际需求出发的改革路径，将为数据跨境流动管理创新赋予更多活力和想象空间。

171.《再扩容，新一批自贸区看点多》，载新华网 http://www.xinhuanet.com/fortune/2020-09/29/c_1126555704.htm，2021 年 1 月 8 日访问。

（2）区域数据跨境流动“增扩圈”：RCEP 等双多边协定构建区域数据流动的新法律框架

11 月 15 日，《区域全面经济伙伴关系协定》（RCEP）在东亚合作领导人系列会议期间正式签署[172]。RCEP 中也对个人信息的跨境传输作出了相应安排：如第十二章“电子商务”第十五条“通过电子方式跨境传输信息”规定：基于公共政策、基本安全利益等理由采取的合理限制措施之外，缔约方不得以其他理由限制商业行为中的数据跨境传输；第八章“服务与贸易”附件一“金融服务”第九条也对基于监管、审慎目的的数据本地化存储问题进行了明确。

当下，数据跨境流动规则已经成为双边、多边经贸投资合作框架下的主要议题，我国 RCEP 的签署体现了我国积极尝试与国际通行做法接轨，在经贸、投资以及专题谈判中，主动启动数据跨境流动规则协商。体现了我国对于数据跨境流动政策议题的战略布局，也为我国扩大商业数据“自由流动圈”并构建数字时代的互惠互信合作关系提供了新的模式参考。

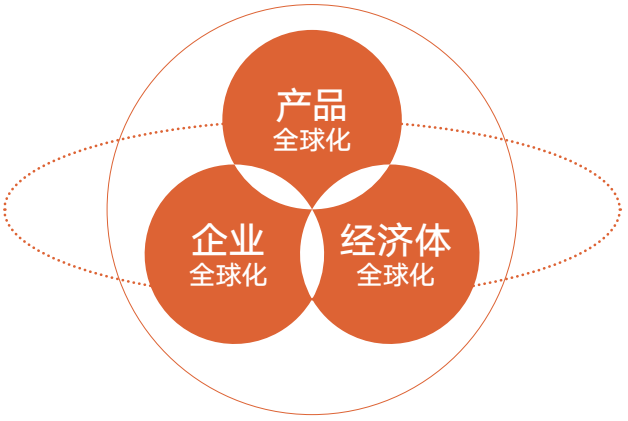
2020 年 12 月 30 日，我国同欧盟如期完成中欧投资协定（EU – China Comprehensive Agreement on Investment，简称 CAI）

172.《区域全面经济伙伴关系协定》（RCEP）领导人联合声明》，https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/t1832614.shtml.

谈判，下一步，中欧双方将开展文本审核、翻译等工作，以推动协定最终文本的形成及签署。CAI 对标国际高水平经贸规则，着眼于制度型开放，是一项平衡、高水平、互利共赢的协定，其具体涉及市场准入承诺、公平竞争规则、可持续发展和争端解决四方面内容[173]。从目前公布的部分协定文本来看，CAI 对涉及金融数据转移的贸易自由化的有关原则作出了明确，并对国家可能采取的信息披露要求等进行了限制[174]。

继 RCEP、CAI 之后，我国在双多边合作机制的探索上仍未止步。在 2020 年 11 月 20 日举行的亚太经合组织第二十七次领导人非正式会议上，国家主席习近平表态，中方将积极考虑加入全面与进步跨太平洋伙伴关系协定（Comprehensive and Progressive Agreement for Trans-Pacific Partnership，简称 CPTPP）[175]。我国商务部也在例行新闻发布会上表态：中国对 CPTPP 持积极开放态度，将积极考虑加入[176]。从范围上看，在 RCEP 已涵盖的一些东盟国家及澳大利亚、日本等国外，CPTPP 也包括了加拿大、智利、墨西哥和秘鲁等国；在内容方面，CPTPP 协定是一个全方位严格的贸易协定，在互联网规则和数字经济上设定了高标准，对涉及服务贸易、数字贸易的数据跨境流动与本地化措施等问题也进行了回应。

04 展望：数据跨境流动将何去何从



（1）长期看，数字全球化仍然是未来发展的主流趋势

目前，国内学者对于“数字全球化”发展态势的总体判断是乐观的。针对全球化，江小涓指出：“全球化的三个方面：产品全球化、企业全球化、经济体全球化均体现了较高程度的相互依存性。”[177]；

173. 参见《商务部条法司负责人就如期完成中欧投资协定谈判答记者问》，载商务部网站，http://www.mofcom.gov.cn/article/news/202012/20201203027541.shtml。

174. See CAI Section II Article 3 Paragraph 5, Section III Subsection 2 Article 5 and Section III Subsection 3, EU – China Comprehensive Agreement on Investment (CAI): list of sections, available at https://trade.ec.europa.eu/doclib/press/index.cfm?id=2237 (last visited on January 26, 2021)

175. 参见《商务部召开例行新闻发布会（2020 年 11 月 19 日）》，载商务部网站，http://www.mofcom.gov.cn/xwfbh/20201119.shtml；《商务部召开例行新闻发布会（2021 年 1 月 21 日）》，载商务部网站：http://www.mofcom.gov.cn/xwfbh/20210121.shtml。

176. 参见《商务部条法司负责人就如期完成中欧投资协定谈判答记者问》，载商务部网站，http://www.mofcom.gov.cn/article/news/202012/20201203027541.shtml。

177. 江小涓，清华大学公共管理学院院长，在清华大学 2020 年全球暑期学校 (Tsinghua GSS 2020) 作题为《数字时代的全球化及其治理 (Globalizationand governance in the digitalage)》的演讲，2020 年 7 月 28 日。

178. 李晓东，伏羲智库创始人，在第五届观潮论坛，做题为《逆全球化态势和数字世界共治面临的挑战》演讲，2020 年 8 月 16 号。

围绕数字化，李晓东指出：数字化进程不可逆转。数字世界的大门，再想关是关不上的。在逆全球化短期态势下，所有人依然希望享受到数字网络红利。因此长期来看，发展仍然乐观[178]。特别是今年新冠疫情爆发以来，远程医疗、在线教育、共享平台、协同办公、跨境电商等服务广泛应用，显现了更为强劲的弹性与活力，为全球经济增长注入了新动能，也对数据跨境流动提出了新要求。

（2）实现数字全球化发展，跨境数据流动在其中扮演重要作用

数字服务具有天然的全球化特征，通过信息网络实现全球供给和全球消费。而在供给和消费两端，伴随大量高频的数据跨境流动。高水准数据跨境流动规则的制定，在抢占数字贸易规则决策者身份的过程中起到重要作用[179]，不论是此前的《美国 - 韩国自由贸易协定》、《跨太平洋伙伴关系协定》还是 2020 年 11 月我国签订的《区域全面经济伙伴关系协定》，商业场景下数据跨境流动规则的谈判与制定，对一国数据贸易发展均扮演重要角色。

（3）跨境数据流动机制仍需要更多的探索与创新，以平衡把握因此而带来的安全风险和发展利益

由于各国间的利益和立场存在着巨大差异和冲突，短期来看，要建立单一的全球数据圈并不可行，跨境数据流动机制更多将表现出多样性，而其具体体现在以下几个方面：

国际规则与数据流动圈将更加多样化

不同国家之间，更可能基于不同标准体系、不同互信国家或地区、甚至不同行业或类别，建立相应的“白名单”数据流动圈[180]，因此，各国在双边、多边规则构建方面正在努力探索尝试。当前，欧盟 GDPR 在全球范围的影响力不断增强，各国向欧盟标准积极靠拢。近两年，日本、韩国、印度等均积极申请认证欧盟的“白名单”认证，其中，日本已通过立法改革和双边承诺加入该名单之列。在 GDPR 年度评估中，德国、比利时等成员国都提出应扩大“白名单”的范围，与更多的国家达成充分性决议[181]。

179. 参见中国信息通信研究院：《全球数字经济新图景（2020 年）——大变局下的可持续发展新动能》，http://www.caict.ac.cn/kxyj/qwfb/bps/202010/t20201014_359826.htm。

180. 杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，载“CAICT 互联网法律研究中心”公众号，2019 年 9 月 17 日。

181. Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States,https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf.

数据流动方案将借助多渠道运行

从 1995 年欧盟数据保护指令起，欧盟已开始系统地提出了关于数据跨境流动的规范要求。20 年来的实践积累，让欧盟积累了丰富的经验与教训。其中，最为明确的是：欧盟放弃了事前许可式的跨境管理方式，认为这种方式已难以适应高频化、网络化的数据国际流动。因此，数据流动合规方式的进一步拓展将是大势所趋，如标准合同条款、行业协会等第三方监督与市场自律、行业标准和认证、经认可的市场认证标志等均可能为数据跨境转移提供可能的合法机制。

数据分级分类及相应的流动模式将更为细化

针对数据自身特点，对数据分级分类并进行有针对性的管理，也是被广为认可的机制。从目前来看，综合考虑数据自身性质而对相应的数据匹配适宜管理机制是较为有效的办法，例如：一般性商业数据等非敏感数据可考虑适用自评估，数据出境合同备案等方式管理；金融行业数据，可遵循国际惯例或者行业专业化的跨境流动管理方式，探索相关机制；科研数据，可以作为一类特殊数据，实施特殊管理政策，以促进科学研究；过境数据，即不涉及我国个人、机构的数据，而仅是在我国境内传输、存储、处理，这些数据的流动理应也适用特殊的管理体系。更多的数据分类及分级流动模式的提出与发展，也将在未来实践、细化。

结语

回顾今年全球数据跨境流动的总体态势，“隐私盾”协议失效、英国脱欧等问题均为以欧盟为原点的数据跨境流动规则制造了诸多不确定，但伴随数据跨境流动规则探讨进入深水区，也印证了数字全球化发展依然是未来主旋律。作为数字经济和数字贸易发展的关键支撑政策——跨境数据流动机制期待更多探索与创新，以开放心态，积极参与规则建设，将更有利于把握这一历史机遇。

跨境执法数据调取——
全球治理呈现多样性

8

前言

2018 年 2 月，美国通过了《澄清域外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act)，简称《云法案》(CLOUD Act)。该法案创制了直接向特定服务提供商获取境外电子证据的新模式，对国际数据治理规则带来深刻影响。腾讯研究院 2019 年度报告——《云深处的数据规则》，从云法案的基本原理、具体机制、影响挑战、发展趋势等方面进行了全面分析，指出《云法案》本身只是创立了一种法律机制，但直指各国对网络数据空间中数据主权的核心关切。正如“蝴蝶效应”所描绘的那样，以《云法案》为开端，国际数据治理规则体系将产生长期而巨大的连锁反应[182]。2020 年，各国政府就《云法案》的谈判以及对数据跨境执法机制的探索仍在争议中继续，正如此前预判：跨境数据流动规则的协商已经步入了深水区，贸易语境下的数据商业性流动和执法语境下的政府数据获取两个议题之间已更加紧密地结合在一起。

01 基于《云法案》的政府间谈判在争议中推进

（1）英美已达成政府间协议并于 2020 年生效

2019 年 10 月，英美两国政府于华盛顿签署了基于《云法案》的政府间双边协议。基于此协议，美国与英国相关执法部门在合理授权的前提下，为打击一些严重犯罪（如恐怖主义、对儿童的性侵害、网络犯罪等），可以直接向位于两国的科技公司要求相应的电子证据[183]。就这一政府间协议，英国已于 2020 年 2 月 28 日[184]、美国已于 2020 年 7 月 8 日完成相应的法律程序使其在国内转化生效[185]。

作为《云法案》公布后的首份政府间协议，其规定了一些在《云法案》文本之外的隐私与公民自由保障措施，例如在适用限制、第三国通知、透明度等方面。该协议为英美跨境取证提供了相较于传统司法协助途径而言更为便捷的通道，也为后续澳大利亚、欧盟等与美国签订相关协议提供了可能模板。但对于该机制具体的做法实践、英美两国间的合作效果等仍需留待观察[186]。

（2）澳大利亚修法为《云法案》积极铺路

2020 年 3 月 5 日，澳大利亚政府表示，其已向议会提出《电信立法修正案（草案）》，以修订 1979 年《电信（监听和访问）法》[187]，若该法修订完成，澳大利亚将允许相关协议国的执法机关、国家安全机构直接访问位于其国内的数据以进行执法活动。这是美澳双方自 2019 年 10 月启动就《云法案》相关协议的谈判以来，澳大利亚进行的实质立法进展，其将为澳大利亚后续加入《云法案》跨境数据取证机制铺路[188]。

182. 参见王融、王雅蓉：《2019 数据治理报告——云深处的数据规则》，载微信公众号“腾讯研究院”：https://mp.weixin.qq.com/s/Esku27Tuab8XLQH8-BNiBg。

183. See U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, 03 Oktober 2019, available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists (last visited on January 9, 2021).

184. See The Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020, available at https://www.legislation.gov.uk/uksi/2020/38/made (last visited on January 9, 2021).

185. See Supplementary letter conveyed to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement, available at https://www.justice.gov/dag/page/file/1236281/download (last visited on January 9, 2021).

186. See Apples And Oranges: UK -US Bilateral Data Access Agreement Comes Into Effect, available at https://www.mondaq.com/unitedstates/telecoms-mobile-cable-communications/975500/apples-and-oranges-uk-us-bilateral-data-access-agreement-comes-into-effect (last visited on January 9, 2021).

187. See Bill to usher in new era of international crime cooperation，avaiable at https://minister.homeaffairs.gov.au/peterdutton/Pages/international-crime-cooperation.aspx#:~:text=The%20Telecommunications%20Legislation%20Amendment%20(International,subject%20to%20an%20international%20agreement (last visited on January 9, 2021).

188. See Bill to usher in new era of international crime cooperation，avaiable at https://minister.homeaffairs.gov.au/peterdutton/Pages/international-crime-cooperation.aspx#:~:text=The%20Telecommunications%20Legislation%20Amendment%20(International,subject%20to%20an%20international%20agreement (last visited on January 9, 2021).

（3）欧盟跨境电子证据谈判、立法、国际协作仍无实质进展

欧盟委员会自 2019 年 2 月便向欧盟理事会提议与美国进行关于电子证据跨境获取的谈判，并于同年 6 月获得了授权。欧盟此后在 2019 年 9 月、10 月、12 月与美国进行了三轮正式谈判，主要涉及：数据的种类与定义、可适用的犯罪类型、服务提供商的定义、隐私及程序权利保障等问题 [189]。

欧洲独立智库“欧洲政策研究中心”（Centre for European Policy Studies）在 2020 年 2 月与 10 月相继发布了《电子证据的跨境获取》、《刑事诉讼中的跨境数据调取和数字司法的未来》等报告，解释并重申欧盟在“电子数据跨境执法”上的三个主要战略方向——欧盟内部制定《电子证据条例》、通过《布达佩斯网络犯罪公约》等方式进行国际协商与司法协作、就《云法案》与美国的谈判 [190]，报告中也强调，跨境电子证据的获取应主要服务于打击犯罪而不仅仅是关注高效合作 [191]。

回顾 2020 年，欧盟在以上三个方面均无实质进展 [192]。欧盟法院在“Schrems II”案中认定欧美“隐私盾”协议无效后，欧美之间此前关于国家安全与数据保护之间的分歧更被充分凸显；而从欧盟官方的“电子证据”专题上看 [193]，欧盟《电子证据条例》的立法进程也并无更新；《布达佩斯网络犯罪公约》第二轮议定书草案虽已于 2020 年 11 月 10 日公布征求意见，但由于新冠肺炎疫情的原因，就具体条款的讨论会议也将推迟至 2021 年进行 [194]。

189. See Joint US-EU Statement on Electronic Evidence Sharing Negotiations, available at https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations (last visited on January 9, 2021);See E-Evidence: Start of Negotiations on EU-US Agreement, January 12 2020, available at https://eucrim.eu/news/e-evidence-start-negotiations-eu-us-agreement/ (last visited on January 9, 2021).

190. See Cross-border Access to E-Evidence, available at https://www.ceps.eu/ceps-publications/cross-border-access-to-e-evidence/; See Cross-border data access in criminal proceedings and the future of digital justice, available at https://www.ceps.eu/ceps-publications/cross-border-data-access-in-criminal-proceedings-and-the-future-of-digital-justice/.

191. See Cross-border data access in criminal proceedings and the future of digital justice, available at https://www.ceps.eu/download/publication/?id=30689&pdf=TFR-Cross-Border-Data-Access.pdf.

192. See Video conference of justice ministers, 9 October 2020, available at https://www.consilium.europa.eu/en/meetings/jha/2020/10/09/# (last visited on January 9, 2021).

193. See E-evidence - cross-border access to electronic evidence, available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (last visited on January 9, 2021).

194. See Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime, available at https://www.coe.int/en/web/cybercrime/protocol-consultations (last visited on January 9, 2021).

但整体看，欧盟对于数据主权问题已逐步形成清晰立场，并积极对外输出国际规则。在中美数字竞争中，欧盟面临着技术、产业、人才、投资等方面均落后的窘境。欧盟提出的数据主权，更多是一种“技术 / 数据主权”，其意在增强自身数字化技术基础设施而形成一定防御，同时，通过实施和向国际输出数字监管规则的方式提升自己的数字话语权。

2020.7.2

欧洲议会智库——欧洲议会研究处（European Parliamentary Research Service，简称 EPRS）发布报告《欧洲数据主权》[195]。其认为，欧盟提出的“数据主权”是指欧洲在数字世界中自主行动的能力，并应当从防御性机制以及建立有利于促进数字创新（包括与非欧盟企业的合作）的制度工具两方面来入手。欧盟在未来应当在三个方面加强其数据主权的建设：构建欧洲本地的数据存储处理框架，在数据安全、人工智能和数据安全领域促进可信赖的环境，建立竞争和数字监管规则。

2020.7.30

独立智库——欧盟对外关系委员会（The European Council on Foreign Relations，简称 ECFR）发布了文集《欧洲的数据主权：中美对抗时代——从统治者到超级大国》[196]。文集指出，欧洲的挑战在于缺乏具有全球影响力的重要数字公司以及各成员国在内容监管等问题上存在分歧。欧盟在未来应当一方面积极参与到竞争当中，通过 GDPR 等监管工具的国际影响以鼓励其他国家效仿，另一方面通过数字化支持关键行业、关键技术创新发展。

195. See Digital sovereignty for Europe, available at https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651992 (last visited on January 9, 2021).

196. See Europe’s digital sovereignty: From rulemaker to superpower in the age of US-China rivalry, available at https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/ (last visited on January 9, 2021).

197.《“抓住数字机遇，共谋合作发展”国际研讨会在京举行》，载 http://new.fmprc.gov.cn/web/wjbxw_673019/t1814124.shtml.

02

我国秉持多边主义，倡议达成反映各国意愿、尊重各方利益的全球数据安全规则

2020 年 9 月 8 日，国务委员兼外长王毅在“抓住数字机遇，共谋合作发展”国际研讨会高级别会议上发表题为《坚守多边主义 倡导公平正义 携手合作共赢》的主旨讲话，提出《全球数据安全倡议》[197]。

《全球数据安全倡议》就跨境执法机制、网络空间数据安全问题表明了我国的基本态度：

在供应链和国家网络数据安全问题上，各国“应以事实为依据全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应链开放、安全、稳定”，反对“利用信息技术从事危害他国国家安全和社会公共利益的行为”；

对于跨境数据调取议题，我国倡议“应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据”。而基于打击犯罪等跨境执法调取数据的需求，我国倾向于“通过司法协助渠道或其他相关多双边协议解决”，并且“国家间缔结跨境调取数据双边协议，不得侵犯第三国司法主权和数据安全”。

《倡议》再次声明中国在数据主权和安全议题的基本主张，这些主张契合大多数国家的法律实践和现行的国际规则。当然，除了在国际社会继续推动《倡议》的影响力外，还需要进一步在中国国内立法过程中采取科学的立法技术推进相关措施的落地[198]。可以看到，我国在 2020 年出台的《数据安全法（草案）》、《个人信息保护法（草案）》分别就执法与贸易语境下的数据跨境传输问题确立了制度框架。

198. 刘云：《中美欧数据跨境流动政策比较分析与国际趋势》，载《中国信息安全》2020 年第 11 期。

就跨境执法议题，《数据安全法》（草案）第三十三条明确规定：境外执法机构要求调取存储于中华人民共和国境内的数据的，有关组织、个人应当向有关主管机关报告，获得批准后方可提供。中华人民共和国缔结或者参加的国际条约、协定对外国执法机构调取境内数据有规定的，依照其规定。这表明，除了主管机关批准路径之外，我国与他国缔结的双多边国际条约、协定在未来也是重要的发展方向。

就个人数据的跨境流动，《个人信息保护法》（草案）也建立了基本制度框架：一般情况下，向境外提供个人信息的合规路径包括了多种方式，例如满足安全评估、通过第三方个人信息保护认证、签订合同等；而在涉及关键信息基础设施的跨境信息传输时，则需要更高标准的管理，但草案同样对未来的制度建设留有了空间余地。

针对目前网络法领域，各国法律适用扩张造成的管辖冲突、法律适用冲突问题，为维护我国企业海内外利益、协调国际间法律适用，2021 年 1 月 9 日，商务部出台了《阻断外国法律与措施不当域外适用办法》，以应对他国实施“长臂管辖”的做法。办法确立了信息报告、发布禁令、司法救济等阻断机制，反制国外相关立法中过分延长的管辖权，并为受外国法律制裁限制的中国企业提供救济。

结语

以《云法案》为代表的跨境数据执法调取新机制仍在推进之中。英、澳积极加入，欧盟谨慎评估并寻求自身技术产业发展、积极投身数字规则的国际输出。中国提出《全球数据安全倡议》，在国际舞台上逐步形成更为清晰的立场表达：秉持多边主义，兼顾安全发展，坚守公平正义。2020 年，在“数据主权”议题之下，各方展开具体行动，全球数据治理正呈现出多边性与多样性。

总顾问

司晓 杨健

总策划

杨乐 王融

专家顾问团

张钦坤 黄晓锦 柳雁军 蔡雄山 吴绪亮

叶高芬 张昕 田小军 朱开鑫 彭宏洁 彭云

易镁金 吴鑫 汤捷

主笔

王融

写作支持

戴俊哲 黄楠 闫锦麟

报告设计

苏江鹏

腾讯研究院
Tencent
Research Institute

腾讯研究院是腾讯公司设立的社会科学研究机构，旨在依托腾讯公司多元的产品、丰富的案例和海量的数据，围绕产业发展的焦点问题，通过开放合作的研究平台，汇集各界智慧，共同推动互联网产业健康、有序的发展。

围绕互联网法律、公共政策、互联网经济、大数据等研究方向，与国内外研究机构、智库开展多元化的合作，不断推出面向互联网产业的数据和报告，为学术研究、产业发展和政策制定提供有力的研究支持。

我们坚守开放、包容、前瞻的研究视野，致力于成为现代科技与社会人文交叉汇聚的研究平台。

理解腾讯 / 理解互联网 / 理解当代中国

欢迎扫描二维码关注
腾讯研究院官方公号

腾讯研究院公众号

腾讯研究院视频号