人民数据 PEOPLE DATA

大数据风控与权益保护研究报告

RESEARCH REPORT

ON BIG DATA RISK CONTROL AND RIGHTS PROTECTION

人民数据（国家大数据灾备中心）

中国经济体制改革研究会互联网与新经济专业委员会

2020年6月

目 录

习近平总书记在中共中央政治局就实施国家大数据战略第二次集体学习时强调，要推进数据资源整合和开放共享，保障数据安全。2020 年新型冠状病毒疫情的爆发，加速“大数据”时代的到来。数字科技技术在疫情精准防控、推动复产复工及经济社会秩序全面恢复方面，提供了强大支撑。与此同时，数据安全与个人信息保护成为社会热点议题。为此，人民网人民数据与中国经济体制改革研究会互联网与新经济专业委员会合作，共同撰写了《大数据风控与权益保护保护研究报告》，助力大数据更好服务我国经济社会发展和人民生活改善。

报告包括 4 部分内容：一是梳理抗疫期间大数据的应用情况；二是跟踪有关数据治理方面的法律法规建设最新动态；三是研究点评涉及大数据权益保护的 10 大典型案例；四是基于技术进步和公共利益保持平衡的考虑，探索提出大数据风控与权益保护的 12 条原则。

一、新冠疫情加速“大数据”时代到来

当前，5G、移动互联网、人工智能、区块链、云计算、大数据、物联网等新兴数字科技发展方兴未艾，应用场景日趋丰富，相关产业高速发展。2020 年，新型冠状病毒疫情爆发，危急关头，各地政府通过电信大数据、位置大数据、电力大数据，助力疫情溯源、精准防控和指导复工复产，各行各业借助互联网大数据迅速实现分布式办公、服务场景转换。可以说，“智慧城市”建设谈了这么多年，在这次疫情防控中才第一次得到了广泛深入的应用。

习近平总书记在 2 月 14 日中央全面深化改革委员会第 12 次会议上强调，要鼓励运用大数据、人工智能、云计算等数字技术，在疫情监测、分

析、病毒溯源、防控就治、资源调配等方面更好发挥支撑作用。此前，总书记提出：运用大数据提升国家治理现代化水平。善于获取数据、分析数据、运用数据，是领导干部基本功。

（一）大数据助力政府精准防控

今年春天以来，各地政府积极运用大数据支撑疫情防控、物资调配、居民生活保障、复工复产复学等工作，大数据成为公共卫生预警响应机制的重要引擎。

比如地方政府运用“健康码”网络系统，把个人健康、出行情况和高风险地区信息结合起来，并根据发展动态实时更新，实现个体和城市的数据化，实现“精准抗疫”。多地政府综合卫健、公安、交通等各部门数据及以及电信运营商、航空、铁路、互联网消费等企业的数据，通过将人员迁徙变动情况与往年数据对比等手段，精准预判地区人员流动数量、来源地、空间分布、从业情况等，研判疫情发展趋势和对经济社会影响，为有效做好疫情防控提供依据。

如上海“一网通办”移动端“随申办”推出的“随申码·健康”服务，通过汇聚卫健、公安、交通等各部门的数据建模、分析评估，计算出疫情期间的个人红色、黄色、绿色三种风险状态，为本地区人员防疫健康状况实现精准管理。广东“粤省事”上线疫情防控服务专区，并上线“粤康码”、个人健康申报等疫情防控服务。“粤康码”与全国一体化政务服务平台“防疫健康信息码”数据互通，实现各地区来粤人员健康数据实时互认。

此外，通过大数据，多地政务服务平台提供疫情信息服务、发热门诊查询、防控知识、重要公告等信息发布，实时发布疫情可视化图表与疫情

的发展态势，从而有效帮助大家了解周边的疫情态势，提高群众防控意识。

今年 2 月，“国家政务服务平台”微信小程序上线“新型肺炎疫情防控专题”，专题提供包括实时动态、提供预防、确诊患者同行人员自查、就医指引、定点医院导航等 60 余项服务。市民不但可以第一时间了解疫情防控信息，也可以查看日常预防知识，以及当前地区的医疗救治定点医院及发热门诊信息。

工信部官员在媒体通气会上表示，通过电信大数据，可以统计分析全国特别是武汉和湖北等重点地区的人员动态流动情况，分析预测确诊、疑似患者及密切接触人员等重点人群的动态流动情况，支撑疫情防控部署，还可以实时采集、汇总和处理电信相关数据，及时提供各类数据分析结果，为疫情防控提供精细化数据支持。

（二）大数据助力复工复产与经济社会复苏

复工复产与经济社会全面恢复领域，政府各部门积极利用大数据，优化网上服务，推动政务服务事项“不见面审批”“线上办理”，让政务服务不因疫情而停摆，也最大限度地减少了申请者外出和聚集，进而避免审批事项办理过程中因聚集而带来的感染风险。

比如，疫情期间，“国家政务服务平台”陆续推出“小微企业和个体工商户服务”、“复工复产”、“就业服务”等服务专题，将各部门、各地区相关的办事服务在国家平台上分类汇集，提升政务服务效率与质量，助力复工复产。江苏政务服务网及江苏政务服务 APP 先后推出“小微企业和个体工商户复工复产服务”“苏政 50 条”专栏，汇聚政策信息、发布办事指南、接受咨询投诉、嵌入部分事项办理入口，推动惠企政策全面落地，

为复工复产“加油提速”。

另一方面，通过大数据支持和推动受疫情影响的各类企业复工复产，帮助企业共渡难关。多地政府通过分析和应用企业税收大数据，破解产业链供需对接不畅、企业资金短缺、上下游产销脱节等难题，比如把企业纳税信用作为企业融资贷款依据，同时从宏观层面分析追踪经济运行态势，精准辅助政府决策。

可以预计，各地各部门必将以此次疫情为契机，积极部署数字政府及智慧城市建设，推动整个社会治理能力升级，推进社会治理现代化。

此外，5G 基站、工业互联网、大数据中心等“新基建”项目在全国多地加速布局，成为中国后疫情时代经济复苏的重要选择，也将进一步推动大数据产业迅猛发展。

（三）大数据助力企业应对疫情，实现数字化转型

企业领域，疫情加快了企业数字化转型的步伐。越来越多的企业开始“远程办公”“线上经营”，积极运用大数据支持企业复工复产、保障生产生活、实现精准销售，推动经营管理、生产加工、物流售后等核心业务环节数字化转型。

根据腾讯研究院发布的《疫后企业数字化生存调查报告》，企业复工率与数字化程度呈正相关，数字化程度高，则复工率高。企业的数字化程度越高，面对疫情时受到的冲击就越小，复工复产的活力就越强。可以预计，积极利用大数据，实现数据化转型必将成为企业减小疫情影响、实现可持续发展的“必选项”。

（四）大数据时代需发展与管理并重

有学者将此次疫情看作是世界经济发展的风水岭，即 B.C.—Before Corona 和 A.C.—After Corona，疫情之前与疫情之后将会是两个世界。

人民数据和中国经济体制改革研究会互联网与新经济专业委员会在研究中得出结论：新冠疫情防控和恢复经济，是中国大数据应用的一个分水岭和里程碑。疫情后，数据的采集、储存、分析和应用都将进入一个新的阶段，无论是采集范围、应用场景还是使用频率，都会有一个质的飞跃，社会将真正进入“大数据时代”。大数据是企业的核心资产与战略资产，攸关企业经营管理的成败生死。大数据也是政府公共治理的战略资源，直接影响到社会正常运营和应急管理。

中国互联网曾经走过了一条先发展后治理的路径。从 IT（信息技术 Information Technology）到 DT（数据技术 Data Technology）时代，需要发展和治理并重。大数据的广泛应用，关系到个人隐私保护、企业商业安全、国家公共安全，需要对全社会宣导普及数据权益保护意识，政府依法治理，大数据平台依法运营，用户知晓自己的合法权益，大数据所有利益相关方敬畏和恪守大数据应用的法律边界、行业规则和自律规范，消除数据使用的安全隐患。这已经成为正在到来的“大数据时代”一个迫切需要解决的问题。

二、立法机关和社会各界关注大数据的权益保护

（一）全国两会有关大数据权益保护的提案议案发言

据媒体报道，今年全国两会期间，多名代表委员针对数据安全与个人信息保护建言献策。

全国人大代表、第十三届全国人大社会建设委员会副主任委员、中国网络社会组织联合会会长任贤良：防疫期间采取的一些特殊措施，不能没完没了地延续下去。疫情结束后，有关部门应当对收集的个人信息进行封存、销毁。

全国政协委员、百度董事长李彦宏：建议针对疫情采集的个人信息设立退出机制。

全国人大代表、科大讯飞董事长刘庆峰：规范管理数据全生命周期中各环节的安全保障措施，对数据的收集、流转、运营进行规范管理，避免数据泄露、数据资源滥用，对国家利益造成损害。结合各行业数据的敏感程度、数据脱敏与否、数据可用性要求等对大数据资产进行分类分级，采取不同级别的安全防护策略。此外，需要规范大数据运营企业的资质要求。涉及国计民生、国家公共安全、能源、交通等敏感行业的大数据，需要具备国内涉密资质要求的企业才可开展数据采集、汇总分析、存储等大数据运营工作，并严格控制其应用及传播范围。

全国人大代表、广东移动董事长、总经理魏明：加快制定数据安全法已刻不容缓，并提出了确立数据主权、明确数据安全法的管辖范围，对数据经营进行牌照化管理，建立数据采集、加工和利用业务的准入制度，完善数据安全监管体系和数据安全监测预警、应急处置机制，建立责任主体问责制度等一系列建议。

全国人大代表，中国移动通信集团浙江有限公司党委书记、董事长、总经理郑杰：加快制定“数据安全法”。“数据安全法”要细化数据安全与隐私保护规则，保护公民合法权益；明确数据的权利归属，促进数据的确

权、流通、交易和保护；要建立数据合理使用制度，实现个人与数据使用者之间的利益平衡；要建立公共数据开放共享规则，促进公共数据的合理利用；要完整确立中国数据跨境流动制度，应对国际数据竞争。

（二）数据安全保护法律法规

据报道，《个人信息保护法》《数据安全法》已列入全国人大常委会立法工作计划。政府相关管理部门也针对数据安全与个人隐私保护出台了相关规定，采取了一系列措施：

一是涉数据安全行政执法专项治理行动。2019 年，中央网信办等四部门全年开展“App 违法违规收集使用个人信息专项治理”、工信部信管局“信息通信领域 APP 侵害用户权益”、市场监管总局“守护消费”暨打击侵害消费者个人信息违法行为、工信部网安局“电信和互联网行业提升网络数据安全保护能力”等专项执法行动，获评“正当其时”，各大网络平台纷纷表态将严格加强网络保护。

二是涉数据安全刑事惩治力度不断加大。惩治领域，全国公安机关“净网 2019”专项行动工作，对侵犯个人信息数据的违法犯罪行为加大刑事手段打击惩治力度。魔蝎数据、公信宝等诸多公司相继被查，企业高管乃至技术人员被警察带走。

三是数据保护的法律法规建设同步开展。2019 年 10 月，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，规定：任何组织和个人不得利用密码从事危害国家安全、社会公众利益、他人合法权益等违法犯罪活动。任何组织或个人不得窃取他人加密保护的信息，或者非法侵入他人的密码保障系统。

2019 年 5 月，国家网信办发布《数据安全管理办法（征求意见稿）》向社会公开征求意见。征求意见稿明确提出其立法目的为保障个人信息和重要数据安全。规定网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息。征求意见稿规定，网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。网络运营者利用用户数据和算法推送新闻信息、商业广告等（以下简称定向推送），应当以明显方式标明‘定推’字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

2019 年 8 月，国家互联网信息办公室于发布《儿童个人信息网络保护规定》， 明确任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息，网络运营者收集、使用、转移、披露儿童个人信息的，应征得儿童监护人的同意等。

2019 年 12 月，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合印发《App 违法违规收集使用个人信息行为认定方法》，将共 31 种违法违规收集使用个人信息行为分为未公开收集使用规则、未明示收集使用个人信息的目的方式和范围、未经用户同意收集使用个人信息、违反必要原则收集与其提供的服务无关的个人信息、未经同意向他人提供个人信息、未按法律规定提供删除或更正个人信息功能或未公布投诉

举报方式等六大类。

2020 年 2 月 9 日，中央网信办公开发布《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》，明确为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码等个人信息。

2020 年 6 月 1 日，国家互联网信息办公室、国家发展改革委员会、工业和信息化部、公安部等 12 个部门联合发布的《网络安全审查办法》正式实施，《办法》规定，对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。

三、大数据的应用和权益保护典型案例

（一）墨迹天气 IPO 因数据合规等原因被证监会否决

案例简介：2019 年 10 月 11 日，墨迹科技 IPO 上会被否，证监会发审委明确提出数据合规问题。本案中证监会要求墨迹天气说明“获取用户数据及标签的过程及方法，是否对用户有明示提示，用户授权在法律上是否完备，是否明确告知收集信息的范围及使用用途”，以及说明对数据安全和个人隐私的保护措施与手段。

在致使墨迹天气 IPO 上会失败的四个问题中，收益用户数据赫然在列。

网民的隐私信息和行为习惯是网络安全管理的重要内容。当前中国，互联网发展已经度过了野蛮生长时期，网民在使用网络工具的同时，越来

越关注个人隐私信息的保护。监管部门也在不断加强网民隐私信息的保护和管理，陆续完善相应的法律法规，塑造规范的互联网发展环境。能否积极适应新时代互联网发展规范的要求，摒弃传统发展思维，在保护好用户隐私信息的基础上，探索出新的发展模式，就成为互联网企业必须面对的重大挑战。显然，虽然有众多互联网巨头的掌舵和支持的“墨迹天气”，依然未能交出一份合格的答卷。这也进一步折射出我国整个互联网行业在网民隐私保护方面还存在认识缺陷和风险隐患。

加强数据安全和保护个人隐私已经成为时代的强音，给互联网企业带来挑战的同时，也指明了新的发展方向。一方面，为行业提供了洗牌调整的机会，为规范的企业提供了更大的成长空间；另一方面，任何在此方面打擦边球尤其是投机的行为都会受到惩罚，犯错的机会成本会也来越高。“规范发展才能长远”应成为互联网企业发展成长的重要宗旨。（人民文旅副总裁、人民文旅智库秘书长 谷文杰）

（二）瑞智华胜窃取 30 亿用户信息

2019 年 8 月 5 日《21 世纪经济报道》刊文，被称为“史上最大规模数据泄露案”的犯罪嫌疑人、瑞智华胜 7 名高管，已被浙江省绍兴市越城区检察院提起公诉。作为一家曾在新三板上市的企业，瑞智华胜涉嫌违规非法窃取海量用户信息，用于互联网营销牟利变现。腾讯、百度、京东、今日头条、新浪微博、携程、12306 等 96 个互联网公司的产品数据均有涉及。

瑞智华胜窃取 30 亿用户信息事件一方面表明，对互联网平台个人信息数据开发具有重大商业价值。瑞智华胜的商业模式，最核心的部分是通

过大数据的分析找到特定的广告对象，再通过通过分享、制作有价值、有趣的资讯内容等手段，向特定对象群体推送营销内容，实现营销目的，收取客户服务费用。

另一方面也表明，当前我国数据保护措施存在诸多薄弱环节和风险：非法窃取、滥用个人网络信息可能成为一条黑色产业。个人数据被窃取后，还可能被存储到海外，给整个国家信息安全带来危害。

据媒体报道，瑞智华胜利用技术非法访问用户自媒体账号，实现加好友、加粉操作以及爬取用户订单等信息。之后向第三方公司投放广告盈利。这些 cookie 信息窃取后，还被瑞智华胜存储在境外的服务器上。

瑞智华胜案相关人员已经获刑，但它警示意义发人深省：一是数据开发应该在合法、安全、合规的情况下有序进行；二是互联网平台需进一步构建数据安全保护体系，加强用户信息保护。（中国经济体制改革研究会互联网和新经济专委会副主任 陆琪）

（三）支付宝年度账单

案例简介：2018 年 1 月，支付宝发布年度账单页面中“我同意《芝麻服务协议》”的字号小且默认勾选，涉及用户隐私，引发公众对个人信息安全的担忧。有网民质疑支付宝的诱导行为，呼吁相关部门及互联网企业注重用户隐私保护声音频现。对此，国家网信办迅速约谈了支付宝相关负责人，要求切实采取有效措施，防止类似事件再次发生。支付宝也回应称将加强整改。

在“全民晒单”后随之而来的个人数据隐私问题，成为媒体和大众关注的焦点。当前，大众对于自身隐私问题的关注观念正在转变，也可以说

是觉醒，同时不再是简单的质疑，而是认真的查看了隐私协议，了解如何关闭授权，真正履行用户自身的知情同意的权利。大数据时代下个人信息安全如何保证，也成为所有涉及用户数据的企业值得去思考的问题。

互联网时代，个人数据变得愈发透明，互联网信息的高度共享让公众在享受大数据带来生活便利的同时个人隐私也受到极大的挑战。人们待在数据空间里的时间不断加长，甚至比物理空间还要长，虚拟空间安全风险也更加隐蔽，隐患更加突出。

随着信息安全已上升为国家战略，如何平衡产业发展与个人信息保护也成为企业亟待解决的问题。除了用户自身努力之外，行业与企业作为信息基础设施的运营者，也需在保证正常运转的前提下，加大对数据安全的保护力度，加强对相关数据的安全隔离，运用相关技术，全方位保障用户数据安全，构建逻辑更紧密的防范策略。（人民网舆情数据中心主任数据分析师 侯鑫淼）

（四）旷视科技“课堂行为分析”被指侵犯隐私

案例简介：2019 年 9 月，网络上一张“课堂行为分析”的图片引发网民疑虑和警惕。据媒体报道，南京一高校在部分试点教室安装了人脸识别系统，用于日常考勤和课堂纪律管理。学生是否出勤、是否认真听讲、课堂上是否抬头低头、是否闭眼打瞌睡等行为，均能被智能识别。一些网友认为，它侵犯了学生的隐私权，是一种滥用技术的行为。对此，涉事高校回应称，该系统在校园只是“试点”“规划”，且教室属于公开场所，不存在“侵犯隐私”。教育部科学技术司相关人员在接受媒体采访时表示，校园推广人脸识别技术应谨慎，要加以限制和管理。开发该系统的旷视科

技也发布声明称，该图片只是为技术场景化概念演示。

其实，AI 技术不是不可以用于课堂教学，比如教育机器人辅助教学，以及建设智慧教室，让学生更方便地获得教育资源，参与课堂讨论等都是技术应用的有益尝试。但我们应该清楚的是，学生在全方位监控镜头下的表现和在没有监控下的表现，是完全不同的。这就意味着，人脸识别系统收集的信息存在“失真”的可能，而收集信息的初衷在于更加准确地掌握学生的情况以便更好地因材施教提升教学效果，首先要确保的就是数据的准确性，不准确的信息数据将极大地降低分析结果的可靠性。如此，利用 AI 技术改善教学效果的初衷也就无从谈起。

更为重要的是，并非只要 AI 技术使用得好，就能规避隐私问题。也就是说，即便教室安装人脸识别系统能够提高教学效果也并不一定就代表用户愿意让渡个人隐私权。即便初衷向善，学生个人信息数据被大量获取和存储，同样会引发广大用户对隐私安全的担忧。加之近两年，大数据技术应用引发的个人隐私保护问题日渐增多，这张“课堂行为分析”图片无疑再次刺激了民众对于 AI 技术笼罩下，保护个人隐私倍感无力的神经。

技术本身是中性的，是发挥好的作用还是反作用，关键在于目的和手段。而当下技术应用中不断出现的“侵犯隐私”现象，正是警示我们，随着技术的升级，用户信息安全与数据保护也亟待升级。（人民网新媒体智库助理研究员 朱美娟）

（五）陌陌“ZAO”软件被指过度攫取用户授权

案例简介：2019 年 8 月 30 日，一款名为“ZAO”的人工智能换脸软件在社交媒体成为爆款。网民只需提供一张人脸照片，就可以将选定视频中

的人物面部替换掉，从而生成新的视频片段。ZAO 给网民带来新奇体验的同时，其存在的个人信息安全保护、肖像权、版权等安全隐患，也引发担忧。其中“ZAO”用户协议第 6 条第 1 款规定：“在您上传及/或发布用户内容以前，您同意或者确保实际权利人同意授予 zao 及其关联公司以及 zao 用户全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利，包括但不限于可以对用户内容进行全部或部分的修改与编辑……以及对修改前后的用户内容进行信息网络传播以及著作权人享有的全部著作财产权利及邻接权利。”9 月 3 日，工信部网络安全管理局对 ZAO 运营企业陌陌公司相关负责人进行问询约谈，要求其组织开展自查整改，强化网络数据和用户个人信息安全保护。对此，ZAO 运营团队回应称，将严格按照法律法规和各主管部门的要求，以更加严格的标准，全面加强内容管理、完善各项管理机制，确保用户个人信息安全和数据安全。

虽然“ZAO”很快修改上传了新版用户协议，但公众对“AI 换脸”等技术被滥用的担忧及相关安全隐患的争论远未停止。近年来，人工智能、人脸识别等技术飞速发展，“刷脸”已出现在各种支付和认证环节中，特别是在新冠肺炎疫情期间的身份辨认、体温测量等场景中得到广泛应用。而与新技术带来的便利伴生的是信任危机、数据隐私泄露及侵权等风险。人脸是具有唯一性的生物信息，一旦被复制、盗用，将给用户个人带来难以估量的损失。

大数据时代，当万物互联已成必然趋势，当人工智能深度学习的门槛越来越低，保护数据与信息安全显然不再是只靠用户自身就能防范或解决的简单问题。新技术日新月异，推广和应用过程中如何在隐私、安全、效

用之间找到平衡、划出“红线”，需要各方共同寻求符合发展规律的破解之道。政府的预判与及时规范应走在前面，立法和监管不可少、不能慢，对于非法数据泄露行为要严厉打击，多管齐下保护用户数据安全。生产与运营主体应对新技术新业务进行充分评估，加大技防投入，做好流程监控，加强行业和企业自律，积极采取有效措施堵住漏洞，防患于未然。（人民数据研究院智库中心副主任 李兵兵）

（六）杭州健康“绿码”引发舆论争议

案例简介：今年 5 月，浙江杭州市卫生健康委召开全市卫健系统深化杭州健康码常态化应用工作部署会，提出通过集成电子病历、健康体检、生活方式管理的相关数据，在关联健康指标和健康码颜色的基础上，探索建立个人健康指数排行榜；通过大数据对楼道、社区、企业等健康群体进行评价。此举引发争议，被指“健康码走火入魔了！”6 月，杭州发布《健康码开发运行规范管理办法》，指出杭州健康码是市政府基于实现新冠肺炎疫情防控与恢复生产生活秩序现实需要，也是数字赋能“健康杭州”建设的综合性平台。提出有关部门、单位不得收集与健康码项目提供的服务无关的个人信息，不得违反法律、行政法规规定和双方约定收集、处理、使用个人信息；不得泄露、篡改、毁损收集的个人信息。

5 月下旬，杭州设想提出“渐变色健康码”，通过集成公民相关数据，探索建立个人健康指数排行榜，此举被一些网民认为“健康码走火入魔了！”健康码的操作核心在于数据比对，据介绍，当民众自主申报健康码时，后台会自动比对申报人的身份信息和“涉疫情重点人员库”的身份信息，比对申报人的支付宝定位数据和运营商定位数据，比中则赋予红码。

这意味着，搜集信息的维度越丰富，系统所做出的判断便越为精准。

民众对“升级”后的健康码的担忧也源自于此，当个人病历、生活方式等更多维度的信息被收集，一旦被泄露或滥用，对个人带来的风险巨大。健康码作为特殊时期的应急做法，理应具有暂时性、边界性、可恢复性等特征，在防控常态化的后疫情时代，有关部门是否有权收集个人信息、是否会得到民众的明示授权、公开排序是否会引发歧视等疑问是舆论关切的焦点所在。同时，我们看到疫情防控期间已经有被健康码挡在门外的“边缘人”，这里面不仅涉及智能手机的使用、入网知识素养等问题，还涉及到科技实际应用所带来的公平性与选择权的问题，例如当升级后的健康码推行之后，相关资源会向使用健康码的群体倾斜，从而压缩甚至关闭不使用健康码群体的选择空间。

两会期间，不少代表委员就健康码的信息去留问题提出了建议意见，例如有代表建议建立个人信息定期清理机制，对于期限届满的个人信息采取删除数据库、销毁纸质文档的方式予以清除。也有法律专家表示应该彻底销毁，获取个人信息的过程存在法律瑕疵是其一，特殊时期让渡的信息如未能在结束后被销毁会有损公信力是其二。不过也有学者指出，在存在第二波疫情爆发的风险下，彻底删除健康码信息也不现实，应该将信息进行匿名化处理，提高识别难度，加强安全保护级别，并制定规则只能为抗疫、疫苗研发所用。（人民网新媒体智库研究员 曲晓程）

（七）WiFi 万能钥匙“窃取隐私”

案例简介：2018 年 3 月 29 日，央视《经济半小时》栏目对 WiFi 万能钥匙 APP 做了专门的深度报道，揭露了其带来的各种安全隐患。随后，工

信部发布《关于“蹭网”类移动应用程序的通报》，称近日据有关媒体报道，移动应用程序“WiFi 万能钥匙”和“WiFi 钥匙”具有免费向用户提供使用他人 WiFi 网络的功能，涉嫌入侵他人 WiFi 网络和窃取用户个人信息。工信部表示，立即组织网络安全专业机构对上述两款移动应用程序进行技术分析，发现两款移动应用程序具有共享用户所登录 WiFi 网络密码等信息的功能。之后，工业和信息化部网络安全管理局要求上海市、福建省通信管理局开展调查工作，将在核查的基础上，依据《网络安全法》等法律法规进行处理，维护广大网民的合法权益。

近年来，随着计算机科学技术的迅速发展，海量云服务应运而生，大数据的搜集和应用成为当下社会经济发展的重要手段。然而，在大数据环境下，公民的隐私泄露也变得更加容易，由此带来的后果将严重危害公民的财产安全和人身安全。WiFi 密码是以数据形式保存在手机里，即便是加了密的云端，黑客仍可通过一定的技术手段获取。

软件开发者作为网络服务提供平台，应当坚守职业道德，严格执行相关法律规定，切实承担维护公民网络隐私权的责任，采取尽可能的技术手段为平台获取的个人数据加密，不得主动利用平台优势地位非法利用用户的个人信息实施违法犯罪行为。

鉴于此，在完善法律法规的基础上提高网络服务提供者的行业自律意识，建立有效的奖惩机制，注重对个人隐私数据的技术保护，同时也需提高公民的网络隐私权保护意识，为大数据时代公民的网络隐私权保驾护航。（人民数据研究院智库中心主任 王玫）

（八）微博诉饭友未经许可非法抓取、展示微博明星账号数据不正当竞争

案例简介：北京知识产权法院已经判决的微博诉饭友反不正当竞争案（(2019)京 73 民终 2799 号）。法院在认定饭友 APP 经营商复娱公司绕开或破坏微博经营商微梦公司技术保护措施、实施抓取和展示新浪微博数据之行为构成实质性替代和妨碍、破坏新浪微博正常运营的同时，也在判决中提及“用户对涉案数据进行自主安排、授权等因素而免责等可能。”

近年来，因抓取、使用他人数据而引发的网络不正当竞争案例层出不穷，屡见报端。先有新浪微博诉脉脉不正当竞争一案，再有今日头条因涉嫌抓取微博用户数据陷入纠纷，又有新浪微博诉饭友未经许可非法抓取、展示微博明星账号数据等。

目前，流量和数据是互联网公司争夺的最为主要的资源，在此背景下竞争的本质亦是对流量和数据的争夺。互联网的特点是开放，信息的本质是分享，但这并不意味着经营者可以随意抓取他人数据并使用。本案裁判不仅区分了数据链接与抓取行为，也对替代性产品的数据抓取和使用行为的正当性进行了充分论证，同时还表明了司法对不正当竞争行为的规制态度，体现了司法对网络数据保护迫切需求的及时有效回应。（人民网舆情数据中心主任数据分析师 叶德恒）

（九）Facebook 5000 万用户信息遭泄露

案例简介：外媒报道境外社交媒体脸书公司（Facebook）5000 万用户信息被泄露，遭第三方公司“剑桥分析”“窃用”于大数据分析，用于在政治选举中针对目标受众推送广告，从而影响选举结果。更有英美媒体报

道称，这家公司曾经受雇于一些政治竞选团队和推动英国“脱欧”的阵营。

通常互联网平台数据只是关系到用户隐私安全及企业经济利益，而Facebook用户信息泄露刷新了舆论认知：互联网平台用户大数据甚至可以左右选民投票，干涉政治选举。互联网平台数据泄露不仅是经济事件、用户信息保护事件，也可能是影响全球，关乎国家安全与社会稳定的政治事件。

早在2016年美国总统大选期间，就有媒体报道特朗普团队基于大数据分析，精准投放广告来说服选民。通过技术手段抓取用户互联网数据，再通过大数据分析用户兴趣特点、行为动态，从而精准投放广告和资讯内容，改变部分选民对总统候选人的看法。每个选民都可以收到一条定制的信息，强调某一特定论点的不同层面。这导致“一千个选民眼中可以有一千个特朗普”。还可以通过大数据营造虚假人气、推送大量政治消息、传播虚假或垃圾政治信息干扰舆论、制造烟雾遮蔽效应混淆公众视听、塑造高度人格化形象的虚拟意见领袖等手段，实现对舆论的干预，进而影响政治进程。

西方利用大数据分析、研判、影响政治活动从一个侧面说明，有了大数据，民意是可以测量和评估的；只要摸准情况，民意也是可以引导与干预的。这为我们规范互联网平台数据运用、加强数据与隐私保护敲响了警钟。（舆情分析师 廖灿亮）

（十）韩国“N号房”事件视频设备泄露隐私

案件简介：2020年4月，据外媒报道，韩国带有“阅后即焚”功能的

社交软件 Telegram 上有一个聊天室，专门以分享色情内容的方式牟利，会员高达 26 万人，收费会员数达 1 万多人（韩国总人口 5200 万）。聊天室的管理员“博士”，通过网络黑客技术窃取年轻女性的资料，包括家庭信息、住址、家庭电话、隐私照片等，威胁女性并在全网直播。韩国媒体披露，至少有 74 名女性，包括 16 名未成年人是“N 号房”事件的受害者。

网络大数据在造福公众的同时，隐私泄露等问题也如影随形。2020 年 4 月，据外媒报道，韩国带有“阅后即焚”功能的社交软件 Telegram 上有一个聊天室，专门以分享色情内容的方式牟利，会员高达 26 万人，收费会员数达 1 万多人（韩国总人口 5200 万）。运营者通过发钓鱼链接、假扮警方、发布有偿兼职等方式窃取女性个人私密资料，包括家庭信息、住址、家庭电话、隐私照片等，随后长期胁迫其提供性剥削照片、视频。至少有 74 名女性，包括 16 名未成年人是“N 号房”事件的受害者。一位韩国记者在“N 号房”卧底期间发现，平均每天潜入约 30 个房间，所有房间单日均有数千名男性参与，在每个房间内，单日上传和分享视频最多可达 1.5 万条。

面对网络泄露隐私，Telegram 等即时通讯软件、匿名化的网络空间以及诱导用户的运营模式，都难辞其咎。2019 年初，这种具有“端对端加密”“阅后即焚”功能的软件（Telegram）成为 Google 商店在韩国下载量增长最快的 APP 之一。除了通讯软件的匿名，“N 号房”的运营模式也鼓励用户参与，因为用户想要继续观看，就必须参与上传，进而参与到线下偷拍乃至性犯罪中。

更为重要的是，“N 号房”的会员高达 26 万人，记者潜入的约 30 个

房间，单日均有数千名男性参与（却只有 2 个人对其进行举报），也说明了无论是软件研发者、“N 号房”运营者，还是广大的男性用户，不仅没有因为“N 号房”泄露年轻女性的隐私、存在性暴力犯罪而进行抵制，反倒集体加入了一场消费隐私、围观针对女性性暴力的狂欢之中，可以说正是这些有意识的消费行为，借助网络共同促成了泄露隐私、性暴力的再生产。

“N 号房”事件表明，网络不是法外之地，无论网络技术怎么发展，都不能沦落为侵犯隐私、侵犯人权、纵容乃至从事犯罪的工具，要通过完善的法律，引导和规范网络健康发展，筑起保障个人安全、促进群体平等的“防火墙”，将网络造福人类的功能最大化。（中国经济体制改革研究会科研部负责人/互联网与新经济专委会副主任 南储鑫）

四、大数据风控与权益保护的 12 条原则

人民数据与中国经济体制改革研究会互联网与新经济专业委员会研究数据安全与个人隐私保护典型案例，提出大数据风控与权益保护的 12 条原则。

（一）合法原则

即对个人数据收集、储存、加工、运输、使用等一系操作时，均要求符合法律法规及行为规范，自觉维护数据主体的合法权益。

我国《数据安全法》与《个人信息保护法》即将立法，目前对于个人数据保护的法规散落在《宪法》《民法典》《刑法》《互联网信息服务管理办法》《儿童个人信息网络保护规定》《关于加强网络信息保护的决定》《App 违法违规收集使用个人信息行为认定方法》等法律法规中。在疫情推动下，

我国将真正进入大数据时代，数据的运用在质和量上都会有一个飞跃，个人数据保护也会面临更多新的难题与挑战。但万变不离其宗，大数据的运用首先必须符合合法原则，这是大数据运用的最根本原则。另外，当前一些互联网企业开展全球业务时，也应注意全球数据安全的法律遵从性。

此次疫情防控，依据传染病防治法、《突发公共卫生事件应急条例》、国家及各地制定的防控预案、应急预案，在相关条款的授权下，各级政府部门及授权机构、平台可以依法收集个人相关数据。此外，为保护公民个人信息安全，国家有关部门出台多项措施，如中央网信办发布《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》、民政部办公厅等四部门联合印发《新冠肺炎疫情社区防控工作信息化建设和应用指引》等，为规范信息收集、保管与使用，防范信息泄露提供了安全保障。随着中国社会对数据治理的高度重视和工作推进，会有更多的大数据方面的法律法规和行政规章出台，需要社会各界特别是商业平台方遵守。（舆情分析师廖灿亮）

（二）最小范围原则

对个人数据的获取与处理应以满足业务所需的最小数据为底线，不得收集其他非必须的个人信息。在国家标准《个人信息安全规范》当中，对最小化原则进行了更为严厉的解释，规定收集的个人信息的类型应与实现产品或服务的业务功能有直接关联，而如果没有这些收集的个人信息，“产品或服务的功能无法实现”。这可以被视为是测试最小化收集的“必要性”，或者说“最小化要求”。

业界人士曾表示对用户数据搜集应遵循“最小原则”，不需要的用户

数据，企业不应该索取，把握好用户数据利用和保护之间的“度”。如何用数据最小化保护个人信息数据安全的最大化是成为企业在实际工作中值得去思考和实践的重要问题。(人民网舆情数据中心主任数据分析师 侯鑫淼)

（三）授权原则

一是授权采集。即平台管理方在获得数据提供方许可的条件下，通过规定方式将数据的使用权授予数据使用方。如果数据主体不同意的，不得对该个人数据进行任何使用或处理。任何超出原有授权范围的，均需再次告知用户。间接获取个人信息时，也必须对个人信息来源的合法性进行认证。

专家指出，大数据时代出现数据拥有权、使用权和控制权的分离，数据经常脱离数据拥有者的控制范围而活跃着，这就对数据需求合规性和用户授权合规性提出新的要求。即使数据需求遵循最小级原则，对数据的提供未超出合理范围，用户授权仍是数据服务的前提。国内外普遍要求，针对未成年人的数据采集，必须先获得监护人的事先授权同意。

二是授权存储。即存储数据前告知并获准同意，告知个人信息主体存储数据的目的和用途，不得强迫、误导个人信息主体同意其收集个人信息。数据存储方要基于“存储前防御、存储中控制、存储后可追溯”的防护理念，在获准存储数据后要采取积极的措施保护数据不受侵害，不被篡改，保护个人的隐私。

随着数据成为重要资产，数据价值不断提升，数据存储的重要性也必将进一步彰显。特别是新冠肺炎疫情加速了许多行业数字化转型，线上业

务的普及带来了数据资料的快速增长。这种新形势下，要坚持数据授权存储原则，一方面要基于个人信息主体知情并同意存储的前提下，保障数据存储安全，防止数据窃取、数据滥用、数据误用。另一方面，正所谓沉睡的数据不会带来很多价值，只有把授权存储的数据，在授权的范围内服务社会治理、公众利益和个人需求，才能激发存储数据资源要素的潜力，推动数据要素市场繁荣发展。（中国经济体制改革研究会科研部负责人/互联网与新经济专委会副主任 南储鑫　人民数据研究院智库中心主任 王玫）

（四）必要原则

所谓必要原则，即要求收集的个人信息类型或打开的可收集个人信息权限与现有业务功能、服务有关，不可收集与所提供服务无关的个人信息。必要原则最早可追溯到上世纪八十年代，早在 1981 年，欧洲理事会就规定个人数据应出于明确、具体及合法的目的而收集；1995 年欧盟进一步对必要原则进行强调，最终成为 2018 年《一般数据保护条例》的六项处理原则之一。

大数据时代，必要原则面临着巨大的挑战，症结在于难以判断“究竟何为必要”，或者“究竟哪些个人信息与服务相关”。鉴于此，如果事前列出与特定服务直接相连的个人信息范围，通过划定清晰范围的方式或将有助于信息收集必要原则的遵循与监管。比如，全国信息安全标准化技术委员会依照这一思路制定了《移动互联网应用基本业务功能必要信息规范（V1.0）》，明确了地图导航、网络约车、即时通讯社交、网络支付等 16 种服务所需的个人信息类型。（人民网新媒体智库助理研究员 朱美娟）

（五）明示原则

所谓明示原则，即采集个人信息数据时必须明示收集的目的、方式和范围，确保公众知情权。此外，采集个人信息数据应有“用户可反馈任何与个人数据隐私相关问题的”渠道。通过该渠道，个人信息数据收集者应按照用户反馈，进行相关要求的处理，如删除、注销账户等。

此次疫情期间，在采集个人相关数据时，授权的互联网 APP、小程序，如“国家政务服务平台”“北京健康宝”等，均会提示收集信息的目的和范围，并经被收集者同意、授权。

值得注意的是，明示一是要在醒目位置；二是内容必须合法，诸如一些 APP 在用户协议中提出用户数据“不可撤销、永久、可转授权和可再许可的权利”等“霸王条款”，且“不同意就不能使用”，将对公众安全带来众多难以预测的风险。（舆情分析师 廖灿亮）

（六）比例原则

公共利益与个人隐私保护之间，需要找到一个相对合理的平衡点。为了公共利益，政府及授权机构依据法律法规的规定，可对个人私人信息进行采集、运用等。但公共利益有时候可能是一个模糊不清的概念。只有为了某个特定的、具体的公共利益牺牲个体权利才具有合法性的可能，而不能漫无边际地以公共利益为由涉足私权领域。

比如疫情防控期间，个人的健康与交通出行数据，对相关部门分析研判、精准防控至关重要。但个人的健康与交通出行数据也往往被认为个人隐私。随着我国疫情防控进入常态化，今后个人信息势必将产生更加多样的大数据应用。因此必须考虑划定公共利益与个人私域的比例。不宜把公

共危机事件中公民暂时让渡个人隐私的权宜之计制度化。在公权力和公民个人、社会之间，需要同舟共济渡难关，也需要保持适度的张力。（舆情分析师 廖灿亮）

（七）封存销毁原则

即对所收集的个人信息设立留存期限，根据采集信息的不同级别划分保存期限，对无留存与研究价值的信息及时清理销毁，对期限届满的个人信息予以封存或消除，降低信息保管成本与泄露风险。

例如，此次疫情期间得益于互联网的助力，运用大数据追踪病毒传播链，实现了疫情的精准防控。但此期间的数据泄露情况也时有发生，例如复工复产之后，不法人员通过个人健康信息拨打电话推销相应商品实行“精准诈骗”。疫情期间的个人信息收集作为应对突发公共卫生事件的特殊举措，在疫情结束之后，可考虑封存、销毁。（人民网新媒体智库研究员 曲晓程）

（八）可追溯原则

数据被授权方应该尽到主体责任，在隐私数据的生命周期中确保全流程的跟踪和保护。即数据相关方，如数据控制者，有责任采取具体、实际的措施保护个人数据，确保隐私数据可追溯。

在本次疫情防控中，各级单位都采取了不同程度的限制措施来控制疫情的发展，不仅旅客乘坐飞机火车时要填写健康登记表，而且顾客进入餐馆、商超、银行等场所时也需要仔细写下姓名、电话、住址等个人信息。这些数据控制者应该妥善保管这些信息。一旦出现确诊病例后，可以通过这些信息追踪到与确诊病例同一时间出现在同一场所的其他人，及时对他

们进行排查，尽可能地阻断新冠病毒的二次传播。（人民网舆情数据中心主任数据分析师 叶德恒）

（九）被遗忘原则

随着大数据与人工智能的发展，智能设备、传感器等应用无时无刻记录着人们使用电子设备的行动轨迹，大量的用户痕迹数据被记录，同样面临被随时被泄露的风险。被遗忘原则就是指数据主体应享有个人对数据的控制权，享有对自身不同形式留下的数据痕迹的可删除，取得被遗忘的基本权利。

随着“数据生命周期”与人自身生长周期的变化，数据保存的实际效应也会随着数据本身的准确性和有效性不断递减。因此建议，从国家标准的角度出发，个人信息保存期限应为实现目的所必需的最短时间，即个人信息的保存期限不能超过实现目的所需的最短时间。数据主体在不影响社会评价的基础上理应可通过行使被遗忘权，避免自身相关数据不必要的泄露，增加不必要的风险。

曾经有一个担任公职的年轻人，因同时与多个女朋友关系亲密，被组织上处理，离开原单位后，有关报道仍然挂在网上。尽管他下决心改正并准备结婚，却无法删除相关报道，给他和未婚妻带来烦恼。2008 年瓮安事件中，贵州公安坚持对闹事的中学生进行教育后，不留案底，让他们毕业后顺利融入社会，有的还当了兵。警方能落实未成年人的“被遗忘权”，互联网如何处理这类“被遗忘权”，是一个新的挑战。（人民网舆情数据中心主任数据分析师 侯鑫淼）

（十）整体性安全原则

基于诸多个体授权的数据聚合所形成的整体性数据，不是所有单独个体数据的叠加，而是一种衍生性“公共品”。整体数据产生于平台，但不完全归属于平台，需要算法和分析工具，进行深度加工和各种平台数据的打通分析。整合加工后的数据，反映一个国家经济社会运行和思想文化、意识形态的基本状况，有助于了解国情国力，服务经济社会发展。对整体性数据，需审慎使用，避免因为数据采样、数据标签和数据维度的不完整，数据挖掘工具和指标体系的不健全，产生对国家宏观状况的偏差概括和误读。

(十一)保护开发者原则

大数据时代，数据开发能够带来巨大收益，但也需要开发者投入资本、技术和人力，如何保护合法数据产品成为业主关注焦点。因此，在数据运用过程中，确认数据产品开发者对于合法数据产品享有独立的财产权益，利于保护开发者的合法权益。

2018 年 12 月，淘宝诉美景公司大数据产品不正当竞争案宣判。法院认为，淘宝公司系“生意参谋”零售电商数据产品的开发者和运营者，该数据产品主要为淘宝、天猫商家的网店运营提供数据化参考服务、帮助商家提高经营水平，淘宝公司对该数据产品享有竞争性财产权益。美景公司运营其“咕咕生意参谋众筹”网站，以提供远程登录服务的方式，招揽、组织、帮助他人获取“生意参谋”数据产品中的数据内容，并从中获取利益。法院认为，美景公司未付出劳动创造，将涉案数据产品直接作为获取商业利益的工具，构成不正当竞争，判令美景公司停止侵权并赔偿经济损

失。可以说，该案的判决提供了一个富于启发的个人信息保护思路。（人民网舆情数据中心主任舆情分析师 礼平）

（十二）出境合规原则

2019 年 6 月，国家网信办对外公布了《个人信息和重要数据出境安全评估办法(征求意见稿)》。该文件明确，存在“数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益”等情况，数据不得出境。

大数据是政府公共治理的战略资源，直接影响到国家安全与社会正常运营。因此，在境内收集和产生的个人信息和重要数据应当在境内存储，确保数据安全。对于确实需要出境的其他数据，也要以不会危害国家安全和社会公共利益为前提，且要经过个人信息主体的授权和能保证数据安全。比如当前个人通过互联网跨境购物的信息数据，有专家认为属于个人的主动行为，可视为个人主体同意的数据出境。

随着疫情后“新基建”的推进，产业互联网建设加快，因此，提出大数据出境原则，也是在保护产业数据安全。（舆情分析师 廖灿亮）

五、后记

波士顿动力公司研发的两只机器狗合作开门的视频，曾受到网友热捧，一度登上微博热搜。有专家提出疑问：两只狗合作进入一个房间的确有趣，但如果他们被另一些群体远程操作控制，则恐怕不是一件美妙的事情。

互联网、大数据、人工智能具有改变世界的巨大能量，如果这种能量脱离人类文明的规范，也会带来巨大的伤害。需要警惕在社会治理中对大

数据的过度攫取和应用，也需要制止商家用大数据“杀熟”等不当竞争行为。2020 年中央重视“新基建”，产业互联网建设提速。如果说消费互联网时代，大数据安全侧重保护消费者个人权益；产业互联网时代，涉及能源、交通、金融等社会经济的命脉，一旦数据安全有任何闪失，可能对全社会是一场失序的灾难。因此，此时此刻研究大数据应用的法律边界和利益相关方的权益保护，具有特别重要的意义和紧迫性。

（报告统筹廖灿亮）