数据战“疫”如何纳入法治轨道

张继红 彭诚信

- 从疫情初期到疫情攻坚阶段，人口流动数据追踪、确诊和疑似患者信息、人员健康数据的动态监测以及病毒疫苗的研发等方面都有数据共享助力“战疫”的身影。
- 为了在最大限度发挥数据使用效能的同时保护个人隐私，疫情数据共享活动应始终秉承法治理念，遵循合法原则、目的限制原则、最少够用原则及安全原则这四项基本原则。
- 政府各部门之间、企业与政府部门之间的数据共享都应在法治轨道内运行，遵循合法原则，以保护个人隐私为基本底线。明确共享数据的使用目的和主体机构，合理确定共享范围，遵守目的限制和最少够用原则，避免过度共享。

近日，在中央全面依法治国委员会第三次会议上习近平总书记强调，“疫情防控越是到最吃劲的时候，越要坚持依法防控，在法治轨道上统筹推进各项防控工作，保障疫情防控工作顺利开展”。习总书记的重要讲话，深刻指出了法治思维和法治理念应贯穿疫情防控工作的全过程，疫情数据共享也不例外。

数据共享助力疫情防控

新冠疫情爆发后，从中央到地方迅速建立了垂直管理的疫情联防联控体系。不论是疫情初期人口流动数据的追踪、疑似和确诊患者的确定，还是疫情攻坚阶段人员健康数据的动态监测以及病毒疫苗的研发，都有数据共享助力“战疫”的身影。

第一，人口流动数据共享实现联防联控。

因疫情具有传染性强、涉及地区广等特点，如何做好重点疫区流出人口的防控工作、避免二次传染，对于我国其他省份及地区是否能够实现早预防、早发现、早控制都极为关键。

目前随着各地加快复产复工，人口跨区流动加大了防疫难度。如果仅仅通过个人自觉申报相关信息，恐怕会错过最佳防控时机。虽然瞒报行为重则入刑、轻则施以行政处罚，但毕竟属于事后惩戒措施。此时，人口流动数据共享是支撑疫情态势研判、防控部署的重要基础，是联防联控、精准施策的主要依托，意义重大。

以飞机和高铁为例。当购票人输入身份证号码并确认一致时，包括铁路运输部门及航空公司将来自武汉等重点疫区的乘客信息共享给目的地交通运输管理部门。交通运输管理部门再将上述信息共享给本地政府疫情防控部门、公安部门以及其他相关机构，实现信息一次采集、多次使用。在飞机或高铁等交通工具尚未到达目的地前，就可根据乘客信息进行重点布控，及时启动相应的隔离措施，实现精准防控。

第二，确诊和疑似患者信息共享，实现重点易感人群防控。

在防控过程中一旦发现确诊或疑似病例，各地政府都会统一发布通告（公布患者特定时间段的行踪轨迹），寻找密切接触者。这里的行踪轨迹信息，即是根据电信运营商通过患者手机号码调取的活动数据。

2019年我国移动电话用户的普及率已经达到114.4部/百人，电信企业的大数据分析可以检测疫情发生以来该手机用户是否来自或曾经到过疫情重点地区。电信企业的用户行为轨迹数据与交通运输企业的票务数据共享给工信、交通运输、公安等部门，形成公路、铁路、民航、通讯、医疗等疫情相关各方多源数据监测、交换、汇聚等信息联动，再按照特定时间、特定地点作为检索条件，筛选出该时间段及地点的密切接触者，并将密切接触者信息共享给当地疫情防控部门，可以提前进行医学隔离观察，开展重点易感人群的疫情防控。

运用数据互通和共享技术，有利于排查疑似感染者，独立建档跟踪管理，提前部署医学隔离观察。跨部门、跨企业的数据共享，可以实现对疑似病毒携带者进行准确追踪，利用多维度数据拼接技术实现精准“画像”，将疑似携带者的行踪轨迹、活动场所、交通工具等信息有效整合，并通过大数据技术掌握病源流向及可能的蔓延区域。

第三，地方政务数据共享助力复产复工。

各地方政府依托近些年来建立的政务数据共享机制，实现了疫情数据共享的快速联动，为复产复工提供技术支持。以上海为例，出台《上海市公共数据和一网通办管理办法》《上海市公共数据开放暂行办法》等规章，成立上海市大数据中心牵头负责对全市公共数据进行汇集共享，形成人口、地理空间、信用信息、电子证照、宏观经济等若干基础数据库和主题数据库，为公共数据共享奠定了制度基础，有利于消除“数据孤岛”现象，实现数据管理的联动配合。

不久前，上海市在全市范围内推广“随申码”，以恢复社会生产生活秩序。“随申码”就是依托上海市大数据中心公共平台汇集的数据资源，根据健康状况、来源地、曾经与病例接触程度等情况，经过分析评估后，测算风险状态，以实现上海市民健康状况的动态管理。从2月24日起，上海市所有线下政务服务大厅都推出“随申码”服务，办理业务的人员需要出示“随申码”，显示绿色的方可进入大厅办理业务。同时，为了节约线下检测成本及时间、方便复产复工，长三角地区实现了共享互认健康码。

第四，医疗数据共享，助力疫苗、药物研发和科研攻关。

通过医疗数据的汇集共享、深度分析，可以使研究人员和临床医生访问不同类型的数据集，分析和研究传染病的分子基础，特别是为传染病和药物反应的病因提供解释，不仅能够帮助临床医生为患者制定更有针对性的早期治疗策略，提高诊断的准确性，还能加速病毒研究和疫苗实验，缩短治疗传染性疾病疫苗和新药的研发时间，大大降低疾病防控的研发成本。

目前疫情正在日本、韩国、意大利、美国、澳大利亚多个国家和地区蔓延，我国卫生部门第一时间将病毒基因组共享给国际数据库，以帮助其他国家迅速采取防控行动。应该说，与世界卫生组织及其他疫情高发国家在疫苗研发、病毒检测、药物研制、病毒溯源等方面展开交流合作，共享医疗数据特别是病毒基因组数据，将有利于聚合全球最先进的医疗资源和研究力量以遏制和攻克新型冠状病毒。

数据共享所应遵循的基本原则

疫情数据共享及相关信息的公开缓解了普通民众的恐慌心理，但亦存在确诊及疑似患者的个人隐私信息被不当泄露、疫情数据使用目的被不当改变等问题。为了在最大限度发挥数据使用效能的同时保护个人隐私，疫情数据共享活动应始终秉承法治理念，遵循以下四项基本原则。

（一）合法原则

疫情数据牵涉诸多政府相关部门、医疗机构、科研机构、企业以及个人，数据收集、共享、存储、利用、传输的各个环节，都应当秉持合法原则，在法治框架下有序进行。同时，亦要加强对个人数据保护力度，严厉打击侵犯、泄露、不当获取和不当利用数据的行为。具体而言，在数据采集阶段，相关机构应告知信息主体基本信息及采集目的，以确保其知情权得以保障；在数据利用及共享阶段，要明示使用目的、方式和范围，并取得被收集者同意。对于此次新冠病毒构成公共卫生事件，属于被收集者同意的法定例外情形，这也符合公共利益优先保护的基本原则。即便如此，在疫情特殊时期，也要树立有原则、有条件的数据共享意识，确保共享行为的合法合规。

关于疫情数据共享制度，我国《突发事件应对法》《传染病防治法》《国境卫生检疫法》《突发公共卫生事件应急条例》《国家突发公共卫生事件应急预案》都做了框架性规定。但对于跨地区、跨部门的数据共享都是原则性规定而缺乏应有的细化，这也带来了具体适用上的模糊性，需要依据目的限制以及最少够用原则加以明晰。

（二）目的限制原则

目的限制原则，即指数据收集和之后的处理必须与特定目的直接相关，并按照该目的进行后续数据处理，不得收集与拟定目的不相关的个人数据，不得超越、偏离之前的特定目的。目的性考量，是评判个人数据共享是否合法、正当的关键因素。

2月9日，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》，再次强调此次疫情联防联控工作中需关注个人信息保护，其中第3条明确指出，“为疫情防控、疾病防治收集的个人信息，不得用于其他用途”。欧盟于2013年通过的《关于严重跨境健康威胁的决定》建立针对严重健康威胁的早期预警和响应系统，针对存在健康威胁、感染危险或已经感染的人可以采取接触追踪措施。在符合接触追踪措施目的时，允许主管部门收集并在成员国之间共享必要的个人数据。这里就是目的限制原则的具体体现。

（三）最少够用原则

该原则也可以称为“最低介入原则”，要求数据控制者所收集处理的个人数据应限定在特定目的所需的最小范围内，以对数据主体造成最小影响为标准去处理数据，避免失“度”问题。但在实务操作中，所谓“度”并没有一个非常精确的衡量标准，需要结合个案及场景具体分析。

抗疫之初，在确诊患者密切接触者的排查工作中，有些地方政府为寻找密切接触者而无限度曝光武汉返乡人员的个人信息，甚至是悬赏追查来自武汉及其他重点地区的人员信息。上述做法虽然出于防疫的正当目的，但手段明显逾越必要限度，已构成对个人隐私权的侵害。为实现重点人群的排查目的之需，疑似及确诊患者的行踪轨迹信息，如何时何地乘坐何种交通工具、何时何地在哪一商场购物、何时何地居住在哪一小区单元楼等信息足以帮助公众判断其自身是否与确诊患者密切接触。但确诊患者的其他个人信息，如姓名全称、身份证号码、电话号码、具体门牌号码等就并非排查的必要信息，应做相应的保留或脱敏化处理。否则，可能构成违法。

出于传染病防治等公共卫生利益，公民应当接受并配合疾病防控有关部门开展的走访调查、如实回答其行踪活动等，同时政府部门及其他数据控制者之间为开展疫情防控也有权通报并共享此类数据。在利用、共享数据过程中，须在疫情管控与个人信息保护之间寻求平衡。

（四）安全原则

目前大量的疫情数据被收集和处理，对于专业机构而言，其数据处理能力和数据安全防护意识相对较强，安全级别也较高。但当前部分机关单位、社区防疫工作人员在数据采集、使用和传递中缺少必要的保护意识和规范的工作流程，大量抽调的防控人员和志愿者在接触和使用个人数据时，缺乏数据安全作业规则和安全培训教育。这里要真正发挥数据效能，必须牢固树立安全理念，建立数据安全防护制度和操作规范体系。对信息系统采集的个人数据，应采取访问控制、加密存储和审计等必要措施，确保其不被泄露、篡改、损坏；在发生或可能发生个人信息泄露、损失、丢失的情况下，应立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

打好数据战“疫”的具体措施

第一，政府各部门之间、企业与政府部门之间的数据共享都应在法治轨道内运行，遵循合法原则，以保护个人隐私为基本底线。

数据共享行为是否合法的判断标准，主要涵盖：数据来源是否合法，特别是在收集个人数据时是否给予其适当的隐私提示，并告知其享有的权利和救济渠道；共享是否超出拟定收集和使用目的；是否在数据主体合理预期的范围内使用数据；共享的主体范围是否必要和适格；对于数据的利用是否对个体或单位造成不公正的负面影响。

同时，一旦发生不当使用和共享时，除了采取纠正措施外，还应采取切实措施落实责任主体，便于数据主体及相关机构启动追责程序，这也是数据主体行使救济赔偿权的具体保障。应当说，明确责任主体、建立追责机制，最能体现法律的震慑作用，彰显法治精神。如前所述，我国从不缺少法律法规及相关行为规范，但只有落实并督促相关人员和组织切实履行其义务，并在违反规定时追究其法律责任，才是真正制度落地的关键。

第二，明确共享数据的使用目的和主体机构，合理确定共享范围，遵守目的限制和最少够用原则，避免过度共享。

政府相关部门、企事业有关单位之间进行数据共享时，应根据不同数据类型的特点合理确定共享的方式和范围，应严格限定因疫情防控目的而收集的个人数据的使用范围，避免与之无关的其他数据应用。同时，充分考虑哪些特定类型数据不宜共享，并结合数据应用的不同场景明确哪些主体可以访问并控制处理数据。

具体而言，在密切接触者排查工作中，交通部门、海关边检部门、社区工作部门以及公安部门是开展数据共享的适格主体，数据共享应明确限定于防疫目的，共享数据主要涵盖：确诊及疑似患者个人基本信息、行踪轨迹信息、亲属关系信息、居住地址信息等。在患者救治以及疫苗医学研发领域，科技部门、卫生健康部门、疾控部门以及科研机构是医疗数据共享的适格主体，共享目的仅限于疾病诊断和科研攻关，可共享的数据包括：确诊患者基本信息、临床检验信息、诊疗观察记录以及其他病理信息等。涉及医疗数据的跨境共享，应明确共享的主体机构；在共享内容方面，建立负面清单制度，即明确划定不得共享的数据范围。

在对外提供疫情数据时，在可行情况下应尽可能提供衍生数据而非原始数据；进行数据公开时，针对具有隐私属性或较强识别性的个人敏感数据，应注意事先采用假名、加密、加盐的哈希函数等技术手段进行去标识化处理。一旦疫情宣告结束，还应及时删除原始数据。

第三，落实安全措施，切实保障数据安全。

疫情数据具有来源多样性等特点，除了来自卫健、交通、公安、工信等政府部门的数据源，还有疾控部门、医疗机构、科研院所等事业单位，以及交通运输、电信、水电气等企业掌握的海量数据源。目前，各地疾病防控机构、基层街道社区等普遍开展走访调查工作，统计、层报相关人员的个人信息，这里应特别注意数据运行环境的安全性，确保采集、存储、共享、传输和披露等各个环节的数据安全工作，以防出现数据泄露、丢失、滥用等情形。

对于掌握并处理个人数据甚至是个人敏感数据的各个机构而言，应当采取相关数据安全保障措施，尤其应健全并完善内部安全机制建设，包括人员管理、内控机制（如数据访问权限管控机制）、稽核制度等组织措施，和物理隔离、去识别化等技术措施等，以避免出现数据意外毁损或不法损害、遗失或非法泄露，未经许可被更改、访问或查阅等风险。

最后，我们也应看到，数据共享只是数据利用和流通的一个环节，是大数据在疫情防控领域的技术应用。倘若要继续发挥其支撑作用，不仅需依赖数据来源的准确性以及传染病防控系统知识的专业性指导，更离不开法治力量的维系、调适及保障。

（张继红系上海政法学院教授；彭诚信系上海交通大学凯原法学院教授、博士生导师）