2020数字医疗

疫情防控新技术安全应用分析报告

2020·02

CAICT 中国信通院

CHMIA 中国卫生信息与健康医疗大数据学会 Chinese Medical Information and big data Association

联合出品

中国信息通信研究院安全研究所
卫生信息安全与新技术应用专业委员会
数据保护官（DPO）社群

版权声明

前　言

2020 年伊始，新冠肺炎疫情在武汉暴发，十几天时间内迅速蔓延至全国。面对突如其来的重大疫情，全国人民在党中央和国务院的坚强领导下，众志成城，抗击疫情。在此期间，众多企事业单位积极参与到疫情防控的工作中，综合应用人工智能、大数据、云计算、区块链等新技术，更加实时、准确、全面地为疫情防控提供强有力的决策支撑，在疫情防控工作中发挥了不可或缺的重要作用。

中国信息通信研究院安全研究所在有关部门的指导下，联合中国卫生信息与健康医疗大数据学会卫生信息安全与新技术应用专业委员会和数据保护官（DPO）社群，聚焦 ICT 新技术在新冠肺炎联防联控工作中的安全应用，分析了中国电信、中国移动、中国联通等基础电信运营企业以及平安、腾讯、旷视等科技公司支撑疫情防控工作的典型案例，研究了人工智能、大数据、云计算、区块链等新技术在提升疫情防控效率、构建态势感知能力、支撑防控资源调度和促进工作信息公开等方面的安全应用，总结了 ICT 新技术在重大公共卫生事件预测、防控、诊疗、恢复等环节工作中的安全应用思路。同时，报告重点探讨和研究了数字医疗健康领域 ICT 新技术应用的网络与信息安全问题，以疫情防控为背景，从个人隐私保护、网络和信息安全防护等方面进行分析，研究了国内外相关疫情防控的大数据应用与信息保护的法律法规与参考标准，阐述了新技术应用安全的重要性。基于以上的分析和研究成果，总结形成本报告，供行业主管部门、疾控部门、医疗机构以及相关企事业单位参考使用。限于研究时间和编者

能力，部分报告内容难免存在纰漏，不足之处恳请业界同仁批评指正。

数字医疗在不断向前发展，ICT 的产业融合与安全保障是发展必不可少的长效机制。面对严峻的疫情形势，信息通信业上下齐心，充分发挥技术手段与平台优势，强化新技术的安全应用，助力打赢防控疫情攻坚战。

目 录

一、新技术在数字医疗领域应用现状

（一）新技术在数字医疗领域应用的政策背景

新一代信息技术是国务院确定的七个战略性新兴产业之一，是国家重点扶持的产业对象。近年来，党中央、国务院高度重视，就人工智能、大数据、云计算、区块链等领域发展，作出一系列战略部署，有力地推动了我国新一代信息技术产业发展。

在我国“十三五”规划纲要中，明确提出要实施网络强国战略，加快建设“数字中国”，推动物联网、云计算和人工智能等技术向各行业全面融合渗透，构建万物互联、融合创新、智能协同、安全可控的新一代信息技术产业体系。数字医疗领域是新一代信息技术融合渗透的重点领域，中共中央、国务院发布一系列政策法规推动新技术在数字医疗领域的应用融合。

2018 年 8 月，国务院办公厅印发《关于促进“互联网+医疗健康”发展的意见》，指出要加强区域医疗卫生信息资源整合，探索运用人群流动、气候变化等大数据技术分析手段，预测疾病流行趋势，加强对传染病等疾病的智能监测，提高重大疾病防控和突发公共卫生事件应对能力。支持研发医疗健康相关的人工智能技术、医用机器人、大型医疗设备、应急救援医疗设备、生物三维打印技术和可穿戴设备等。

2018 年 9 月，国家卫生健康委员会发布《国家健康医疗大数据标准、安全和服务管理办法（试行）》，在健康医疗大数据标准管理、安全管理、应用规范、监督检查等方面给出具体的指引，进一步推动健康医疗大数据的应用和发展。

2019 年 10 月，在中共中央政治局第十八次集体学习会议上，习近平总书记讲话指出，要探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务。

从以上系列政策法规和指导意见中可以看到，党中央和国务院高度重视新一代信息技术的发展和应用，尤其鼓励新技术与数字医疗领域的深度融合应用。以人工智能、大数据、区块链为代表的新技术，在解决医疗资源分配不均、提升医疗服务效率、防控公共卫生事件等方面具有巨大的应用前景。

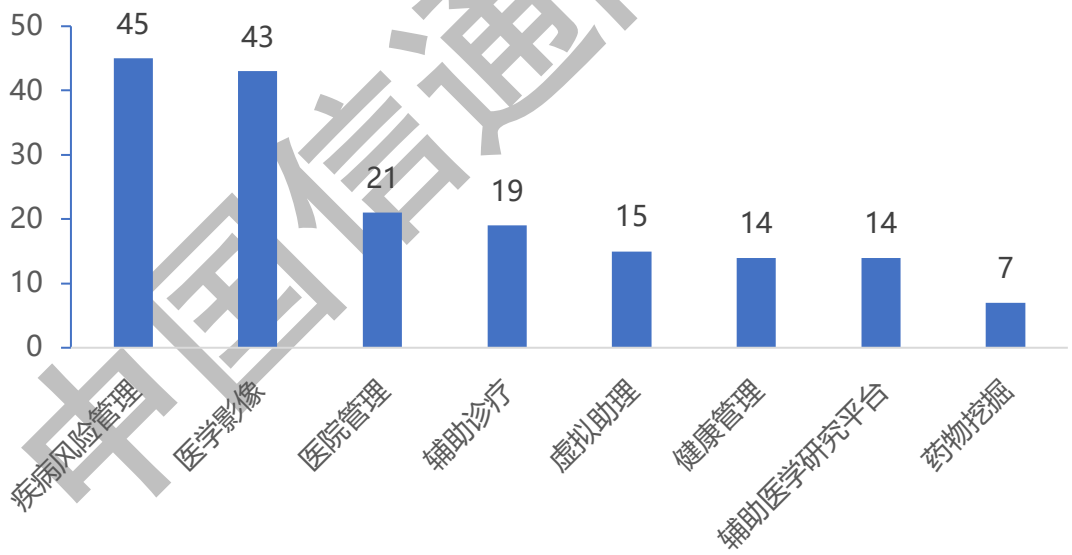
（二）新技术在数字医疗领域应用的现状分析

1. 人工智能+医疗前景广阔

随着机器学习及深度学习的成熟和广泛应用，人工智能技术给各行业都带来了越发深入的变化，逐步成为行业发展的基础设施。数字医疗是此轮人工智能热潮中最为火热的应用领域，也是目前人工智能技术最具前景的市场。据 IDC 统计数据，到 2025 年人工智能应用市场总值将达到 1270 亿美元，其中数字医疗将占市场规模的五分之一。

人工智能技术在数字医疗领域应用归纳起来主要集中在以下八个方面：一是疾病风险管理与预测，包括基因测序与检测服务，预测癌症、白血病等重大疾病；二是医学影像，主要运用计算机视觉技术解决病灶识别与标注、靶区自动勾画与自适应放疗、影像三维重建等需求；三是医院管理，如病例结构化、分级诊疗、DRGs（诊断相关

分类）智能系统、医院管理决策支持系统等；四是辅助诊疗，主要指除医学影像外的辅助诊疗，包括医疗大数据辅助诊疗、医疗机器人（主要指诊断与治疗环节的机器人）等；五是虚拟助理，即医疗领域的虚拟助理，基于医疗知识系统，通过 NLP（自然语言处理）和智能语音技术等与用户进行交互，为用户提供医疗咨询、自诊、导诊等服务；六是健康管理，主要包含营养学、身体健康管理、精神健康管理三个场景，基于用户数据为用户提供个性化健康保健服务；七是辅助医学研究，利用人工智能技术辅助生物医学相关研究者进行医学研究；八是药物挖掘与研究，利用人工智能的算法和技术，可以降低药物研发成本，缩短新药研发时间。目前各类应用场景的企业数量统计如图 1 所示。



数据来源：前瞻产业研究院、博裕金融懂医行数据库

图 1 我国人工智能+医疗各大场景公司数量

2. 健康医疗大数据初见利好

随着“健康中国 2030”规划的不断推进，健康医疗大数据作为国

家基础性战略资源的重要地位不断凸现。党中央、国务院、各级地方政府不断出台鼓励健康医疗大数据建设发展的政策文件，健康医疗大数据发展已进入初步利好阶段。2019 年 7 月，国家卫生健康委员会批复支持宁夏回族自治区建设“互联网+医疗健康”示范省（区），同时提到将在宁夏开展健康医疗大数据中心及产业园建设国家试点。这意味着宁夏将成为继福建、江苏、山东、安徽、贵州之后第六个国家健康医疗大数据中心与产业园建设国家试点。其中，江苏为东部区域中心，贵州为西部区域中心、福建为南方区域中心、山东为北方区域中心、安徽为中部区域中心，宁夏则是示范省区，我国国家健康医疗大数据区域中心建设已相继推开。

健康医疗大数据在数字医疗领域应用场景主要包括辅助决策、健康/慢病管理、医疗智能化管理、基因数据、传染性疾病预测防控等。根据数据的不同来源，可将健康医疗大数据划分为院内数据、院外数据和基因数据。

院内数据主要指医疗机构采集和存储的健康医疗数据，包括患者基本信息、诊疗信息等。院内数据在质量和规模上最具竞争力，目前各省市三级医疗机构多存有高质量的诊疗数据，且已经具备一定规模。然而这类数据的应用将依赖政策指导，且面临严峻的隐私安全问题。

院外数据主要指由智能硬件或在线医疗企业采集的健康医疗数据，如个人体征信息、问诊信息等，该类数据增长迅猛，但维度多且缺乏整合，质量参差不齐。

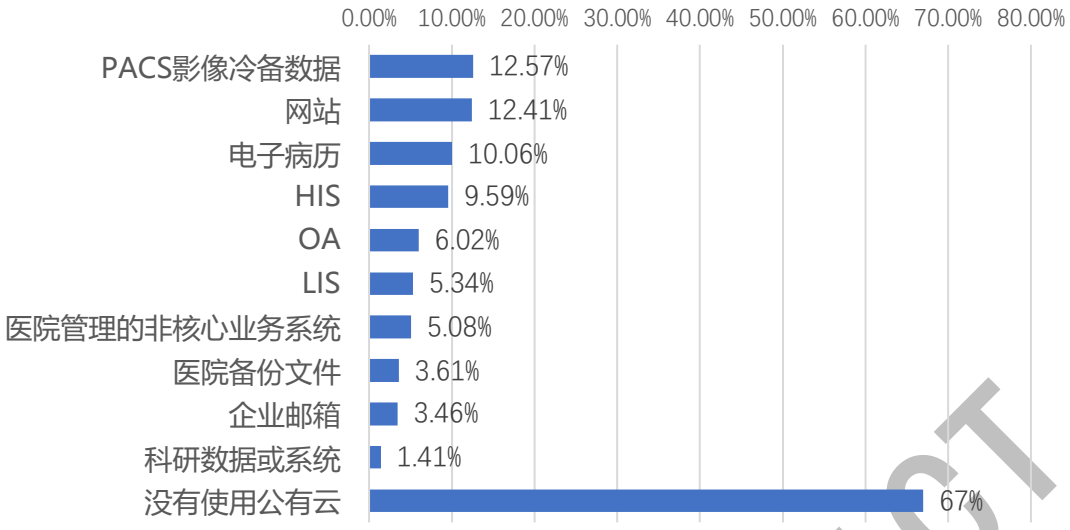
基因数据多由技术型企业自建数据库自行采集，或者通过与实验

室合作的方式获取，目前已具备一定规模和质量，但尚未形成规模化服务，数据所属的企业主要集中在北上广深等一线城市。

虽然当前健康医疗大数据规模及应用快速发展，但数据安全始终是健康医疗大数据无法规避的问题，如何在保障数据安全的前提下开展数据交换、处理和分析，将是今后健康医疗大数据发展需要重点关注和解决的问题。

3. 医院服务云化稳步提升

据 CHIMA 发布的《2018-2019 年度中国医院信息化调查报告》（以下简称：调查报告）统计，有 33%的医院使用了公有云，其中公有云应用在 PACS（医疗影像存储与传输系统）影像冷备数据的领域占比最高，为 12.57%；其次为应用在网站领域，占比为 12.41%。具体数据如图 2 所示。与此同时，调查报告显示采用服务器虚拟化技术医院占比全部调研医院的 63.71%，三级医院及三级以下医院使用服务器虚拟化技术占比分别为 79.18%、46.47%。虚拟化技术是云计算的基础，可以看到大部分医院已经使用云计算及相关技术，但为了保障医疗数据安全，大部分医院尤其是三级医院云化的方向是自建私有云为主，公有云为辅。



数据来源：《2018-2019 年度中国医院信息化调查报告》

图 2 医院使用公有云领域整体分析

4. 区块链医疗应用方兴未艾

区块链技术是一种集成创新技术，由于其去中介、防丢失、防篡改和易追溯的技术特点，在解决医疗数据安全问题、提升数据交换效率、追踪溯源医药产品等方面具有巨大应用潜力。目前区块链技术已在医联体数据互联互通、药品溯源、医保系统核保、电子病历处方流转等部分场景试点实施。

2017 年 8 月，阿里健康将区块链技术应用于常州市医联体底层技术架构体系中，实现当地部分医疗机构之间安全、可控数据互联互通，解决医疗机构的“信息孤岛”和数据安全问题。2018 年 7 月，顺丰对外发布了“顺丰医药供应链‘方案+’”和“顺丰医院‘方案+’”解决方案，在医药物流领域研发并落地了区块链医药溯源、无人机医药运输等特殊服务。

目前区块链技术在数字医疗领域应用仍处于探索阶段，其应用形态和价值有待进一步挖掘。

二、新冠肺炎疫情防控中新技术的应用研究

（一）新冠肺炎疫情防控形势严峻

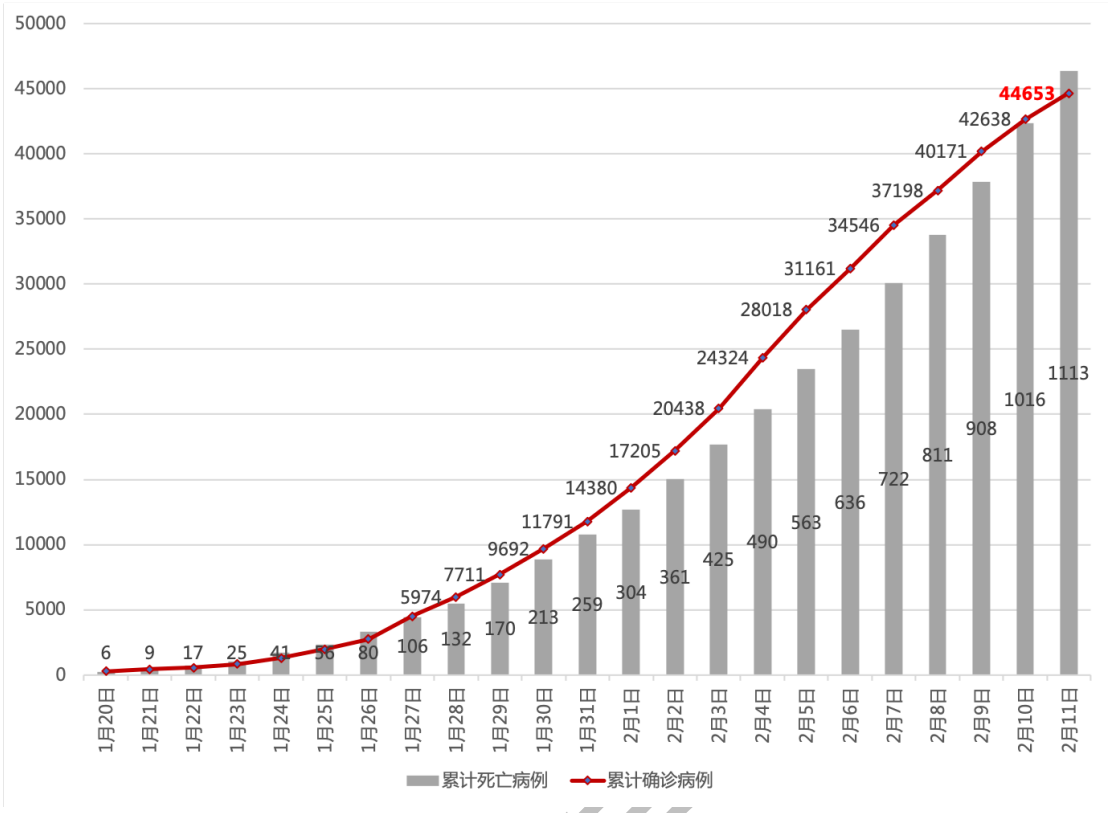
2019 年 12 月 29 日，湖北省和武汉市卫生部门接到当地一家医院报告聚集性不明原因肺炎病例，4 名患者均为华南海鲜批发市场从业人员。12 月 30 日,湖北省和武汉市卫生部门启动调查和病例搜索工作。12 月 31 日,国家卫生健康委和中国疾控中心介入调查应对工作，同日，武汉市政府向社会发布疾病暴发信息。

2020 年 1 月 1 日，基于初步调查结果，关闭华南海鲜批发市场。1 月 3 日，武汉市在全市启动不明原因病毒性肺炎监测、病例调查、华南海鲜市场环境及动物调查和标本采集工作，当日向世界卫生组织、周边国家和地区通报了相关信息。1 月 8 日，确认新型冠状病毒为此次暴发的病原。1 月 10 日，中国疾控中心与世界卫生组织和各国分享了病毒的全基因序列。1 月 10 日后，中国疾控中心等机构和企业开发并测试了 PCR 检测试剂盒，用于对武汉疑似病例的检测、诊断。1 月 15 日，国家卫生健康委印发新型冠状病毒肺炎诊疗、防控方案，规范病例监测、报告、诊疗、管理、密切接触者管理、实验室检测。1 月 20 日，国务院同意将新型冠状病毒肺炎纳入传染病法和卫生检疫法管理，并启动全国范围应急防控工作。1 月 21 日，中国疾控中心发布 PCR 试剂的探针和引物序列。1 月 23 日，湖北武汉及其他地市开始不同程度地停运城市公共交通。

2020 年 1 月 25 日，党中央成立应对疫情工作领导小组，在中央政治局常务委员会领导下开展新型冠状病毒肺炎疫情防控工作，全面

升级防控响应级别。2 月 8 日，国务院联防联控机制发布会上，新闻发言人现场发布关于新冠病毒感染的肺炎暂命名的通知：新型冠状病毒感染的肺炎统一称谓为“新型冠状病毒肺炎”，简称“新冠肺炎”，英文名为“Novel Coronavirus Pneumonia”，简称为“NCP”。

此次新冠肺炎疫情发展极为迅猛，据国家卫生健康委员会公布的数据，截至 2 月 11 日 24 时，全国 31 个省（自治区、直辖市）和新疆生产建设兵团累计报告确诊病例 44,653 例，累计治愈出院 4,740 例，现有确诊病例 38,800 例（其中重症病例 8,204 例），累计死亡病 1,113 例，现有疑似病例 16,067 例。累计追踪到密切接触者 451,462 人，尚在医学观察的密切接触者 185,037 人，从 1 月 20 日至 2 月 11 日新冠肺炎疫情累计确诊病例和死亡病例情况如图 3 所示。由于疫情暴发在春节假期前夕，春运期间全国范围大量的人口流动加剧了疫情的蔓延。在这场疫情防控战役中，各行各业纷纷建言献策，各类新应用层出不穷，新技术在疫情防控中的价值逐渐显现。



数据来源：国家卫生健康委员会官方网站（数据截至 2020 年 2 月 11 日 24 时）

图 3 新冠肺炎疫情发展趋势

（二）新技术在疫情防控中的典型应用案例分析

基于主流媒体新闻数据分析和典型企业应用案例研究，报告团队总结和整理了人工智能、大数据、云计算、区块链等新技术在新冠肺炎疫情防控工作中的典型应用模式和应用案例，具体分析呈现如下。

1. 人工智能提升疫情防控工作效率

新冠肺炎疫情发展迅猛，借助春运的人口流动蔓延至全国，各地都面临着巨大的疫情防控压力，迫切需要提升疫情防控工作效率。一方面，需要高效研究和试验新型冠状病毒，找到病毒的防治之法；另一方面，各地大量流动人口登记排查耗费巨大人力，亟需提升效率。而效率提升正是人工智能算法的强项，也是人工智能技术的在疫情防控工作中应用的核心点。

（1）人工智能技术加速冠状病毒研究

引起武汉肺炎的新型冠状病毒与“非典”病毒、艾滋病毒、埃博拉病毒、流感病毒一样，都属于 RNA 病毒，其单链结构导致病毒更容易变异、不易开发疫苗。RNA 序列有丰富的空间结构，这些结构能决定 RNA 的功能，进而帮助设计分子药物和分子检测仪。冠状病毒的基因组长达 3 万个碱基，最快的经典算法测序也需要等待很长时间。人工智能的算法优势在此体现，各家人工智能厂商纷纷开放算法来提升效率。2020 年 1 月 30 日，百度研究院向各基因检测机构、防疫中心及全世界科学研究中心免费开放线性时间算法 LinearFold，该算法可将新型冠状病毒的全基因组二级结构预测从 55 分钟缩短至 27 秒，提速 120 倍，节省了两个数量级的等待时间。2020 年 2 月 1 日，浙江省疾控中心上线自动化的全基因组检测分析平台，基于阿里达摩院研发的 AI 算法，原来需要耗费数小时的疑似病例基因分析将缩短至半小时，并能精准检测出病毒的变异情况。

（2）人工智能技术助力社区疫情防控

随着新冠肺炎疫情发展，基层社区居民排查、快速摸清人员健康状况和流动情况，成为防控新冠肺炎疫情的重要措施。习近平总书记指示“全面落实联防联控措施，构筑群防群治的严密防线”，为我们同舟共济做好疫情防控工作、群策群力打赢疫情防控阻击战指明了方向和路径。然而，社区住户密集、人员流动大等问题，让人员较少的基层医疗卫生机构、居委会等组织难以快速完成居民排查，而且人工排查仍存在交叉感染风险。此时，基于自然语言理解、智能语音交互

的人工智能技术显现出其威力，该技术能够被应用于社区情况排查和通知回访等场景，避免人员直接接触，同时对比人工拨打电话效率大幅提升。2020 年 1 月 28 日，百度推出针对疫情防控的智能外呼平台，免费向各级政府、卫健委机构、基层社区、疾控中心等相关疫情防控机构开放使用，该平台可提供流动人员排查、本地居民排查/回访、特定人群通知三大场景的外呼服务，日拨打能力可超过 10 万次，极大提升社区疫情防控效率。2 月 5 日，360 金融面向全国各地所有医院、社区、乡村及相关机构免费开放“疫情通”智能机器人服务。“疫情通”基于庞大语义识别语料库，采用深度学习算法结合人机协同模式，以语音形式实现高效沟通，旨在高效探寻、排查疫情信息及智能化统计、分析与处理。平安智慧医疗推出“新型疫情防控服务管理平台”，以智能语音、医学知识图谱、辅助诊疗模型、疫情预测模型等自有核心技术为基础，可帮助一线防控人员，进行一线语音摸排、智能回答区域 12320 卫生热线问题，并对区域内群众的感染风险实现智能分级。讯飞医疗智能语音基于科大讯飞先进的智能语音识别核心技术，通过人工智能语音随访辅助进行重点人群发热筛查和跟进随访，协助进行新冠肺炎疫情的防控和宣教，可提升效率 5 倍以上，减轻基层医务工作者的随访负担，1 月 21 日至 2 月 9 日，该平台已针对新冠肺炎疫情累计服务 1182.1 万人次。

（3）人工智能技术推动测温手段升级

发热是此次新冠肺炎主要症状之一，当前体温检测是机场、火车站、地铁、学校等人流聚集场所防控疫情的主要手段。但是公共场所

人员密集，流动性高，传统额温枪虽然准确但是速度慢，容易引发人群拥堵且会产生一定近距离接触的可能，增加互相聚集形成交叉性传染的风险。此时计算机视觉等人工智能技术就有了较大的应用空间，基于计算机视觉+红外技术的新型测温技术手段，能够以非接触、可靠、高效且无感知的方式进行体温检测，同时能够快速精准定位体温超过阈值人员。2020 年 1 月 25 日，中关村科学城管委员向海淀区科技公司公开征集与“红外测温产品”有关的人工智能技术方案。2 月 2 日百度宣布其研发的多人体温检测技术落地在海淀区清河火车站，自 1 月 28 日上线测试以来，该技术已完成了 1.4 万人的检测，发现 160 人次体温异常，极大提高客运区域多人体温检测效率。2 月 4 日，由旷视科技开发的用于发热及潜在被感染对象识别、筛查与分析的系统“明骥”在牡丹园地铁站和海淀区政府服务大厅正式布设上线，旷视针对人脸口罩佩戴进行了专项优化，无需摘下口罩和排队聚集；其智能疑似高热报警可达 15 人/秒，大流量通道可由一人完成管控，一台机器可以部署十六个通道，基本保证一个地铁口管控，提升了公共空间的安全性和检测效率。

2. 大数据构建疫情防控态势感知

在此次新冠肺炎疫情防控工作中，大数据技术可谓是功不可没。此次武汉疫情正值春节春运时期，全国范围内的春运大迁徙成为病毒快速传播的催化剂，在此期间从武汉回到全国各地的人群多达 500 万，如此庞大的人口流动以及产生的影响在传统手段下几乎是无法监控的。然而在当今数字化的社会生活中，数据已经渗透到我们衣食住行

的方方面面。正因为如此，在疫情发生后，基于海量数据的大数据技术能够迅速发挥其威力，在疫情预测预警、人员流动监控、物资调配分发等方面发挥了重要作用，成为全国范围内的疫情态势感知和预测的重要手段。

据中国互联网络信息中心（CNNIC）发布的第 44 次《中国互联网络发展状况统计报告》显示，截止 2019 年 6 月，我国手机网民规模达到 8.47 亿，网民手机上网的比例达到 99.1%，手机和 App 俨然已成为生活必备品，在疫情时期网民更是依赖于使用手机与外界沟通。用户行踪轨迹最有助于精准锁定“潜在传染源”，以手机及 App 相关的个人信息大数据为出发点，可以有效监测人口流动和分布。

从政府部门到企业，均开始借助大数据技术开展疫情防控工作。2020 年 1 月 27 日，工业和信息化部召开疫情防控大数据专家会商会，研究部署大数据支撑服务疫情防控相关工作。各地通信管理局积极响应，主动与当地新冠肺炎防控指挥部工作机制对接沟通，了解当地疫情防控精准排查工作对大数据的需求，组织当地通信运营企业开展大数据统计分析，为确保从源头防控疫情，当地精准施策提供有力的数据支撑。

基础电信运营企业在有关部门的指导下，基于脱敏后的大数据能力，在保证用户隐私安全的基础上，配合相关部门重点开展对定点医院、发热门诊、人员聚集区等重点区域的人流变化分析，提供疫情防控相关的支撑服务。自 1 月 26 日至今，北京移动持续为北京市委市政府、市发改委、市通管局、市经信局、市卫健委等部门及东城、西

城、海淀、朝阳等 13 个区县提供疫情专项分析服务，对各区街乡进行细分监测，持续输出人口流动及疫情相关监测数据、分析报告，同时协助朝阳区完成“数字战‘疫’”地图的研发及部署。联通大数据参与搭建广东省疫情防控指挥大数据平台，充分利用“数字政府”政务大数据资源，对相关数据进行实时监测和动态分析，加强疫情数据共享和地图服务，支撑疫情防控决策指挥，实现对重点疫区来粤人员“一人一档”精准管理和服务。在福建，中国电信应南平、福州、宁德、漳州等地市人民政府需求，运用大数据分析，梳理细分所在地市相关信息，加强对流动人员的疫情监测，助力福建省各市县疫情精准防控。

1 月 22 日，百度地图迁徙大数据平台上线升级版，截止目前已开放查询 300 多个城市，包含来源地、目的地、迁徙规模指数、迁徙规模趋势图等信息，直观表现春运期间各地人口迁徙情况，为疫情提前布防提供数据基础。1 月 25 日，百度发布新冠肺炎搜索大数据报告，被相关政府机构作为决策参考。2 月 3 日，360 地图发布“地图迁徙大数据”，用户从手机或电脑进入可查看 2020 年 1 月 1 日至今全国除港澳台城市外的迁徙趋势状况。

然而，在应用大数据技术基于个人信息进行疫情防控的同时，也需要注重个人隐私信息的保护，本报告将在后文对此进行重点分析。

3. 云计算支撑疫情防控资源服务

云计算技术已经发展到相对成熟的阶段，在疫情防控的工作中，它更多承担着水电煤一般的基础性资源作用。云计算技术在疫情防控中的应用可以归纳为两大方面，分别是云资源和云服务。

（1）云资源为疫情防控工作提供基础资源

疫情防控是一项复杂和艰巨的工作，从病毒研究和疫苗研制、从新建隔离医院到各地上线疫情防控平台，都需要大量的 IT 资源支撑，而云计算在疫情防控 IT 资源供给方面扮演了极为重要的角色。1 月 26 日，中国电信向“火神山”医院交付云资源，为 HIS（医院信息系统）、PACS 等核心系统部署提供计算与存储能力，实现火神山医院核心业务系统上云。1 月 28 日，中科曙光宣布，将联合业界伙伴共同向相关科研机构免费提供超 100PFlops 算力的强大计算资源，助力对于新冠肺炎防治的科研攻坚。1 月 29 日，阿里云正式宣布：疫情期间，向全球公共科研机构免费开放一切 AI 算力，以加速本次新型肺炎新药和疫苗研发。2 月 1 日，滴滴宣布，免费向国内科研机构、医疗及救助平台等开放用于抗击疫情相关工作的 GPU 云计算资源和技术支持。

（2）云服务为远程学习和工作提供支撑

据《新型冠状病毒肺炎诊疗方案（试行第五版 修正版）》指出，新冠肺炎经飞沫和接触传播是主要的传播途径。为了规避由于人员聚焦带来的潜在病毒传播风险，国务院将春节假期延长，并推迟大专院校、中小学、幼儿园开学，各企事业单位也大量使用远程办公、视频会议等形式开展工作，基于云服务的视频会议、在线教学等需求量暴增，各类云服务厂商也响应号召积极升级功能、提供资源。1 月 27 日，优酷和钉钉发起了“在家上课”计划，为学生提供安心的学习环境和便利的学习工具，疫情期间“在线课堂”功能免费向全国大中小学开放，

可支持百万学生同时在线上课，并覆盖广大农村地区学校。1 月 28 日，飞书宣布在 2020 年 1 月 28 日至 5 月 1 日期间，向所有用户免费提供远程办公支持，包括商业版完整办公套件、不限时长的音视频会议、无限量的在线文档和表格协作、每位用户 100G 云存储服务、7*24 小时咨询服务、远程打卡及审批管理。1 月 28 日，腾讯会议面向全国用户免费升级开放 300 人不限时的会议功能，直至疫情结束，企业微信疫情期间支持 300 人音视频会议。1 月 29 日，钉钉免费开放百人视频会议功能，向 1000 万家企业免费开放全套的“在家办公”系统。

4. 区块链保障疫情信息公开透明

区块链技术具有去中介、防丢失、防篡改和易追溯等技术特点，其在保障疫情信息公开透明、疫情物资追踪溯源等方面可发挥重要作用。新冠肺炎疫情来势迅猛，各地疫情和防控信息纷繁复杂，各类网络谣言也随之而起，如利用区块链技术记录疫情信息，则能够保障信息来源公开透明、可追溯，提升信息公信力。另一方面，在武汉疫情发生后，全国各地人民纷纷献出爱心，为武汉捐款捐物。整个捐献流程长、周期长、涉及方多，不易监控和把握，而区块链技术适合处理此类情况，如实现捐献物资信息上链，则能够保障物资使用公开透明、不可篡改和可追溯。目前从公开信息看到的区块链在疫情防控应用较少，但仍有部分典型应用案例。2 月 5 日，链飞科技推出全国首个区块链疫情监测平台，实时追踪全国各省市新冠肺炎进展情况，对相关疫情数据进行上链登记，实现数据不可篡改、可追溯，并初步建立透明化监督、事件追责的数据链条，保证疫情信息公开透明。

三、疫情防控新技术应用过程中的安全保障

（一）疫情防控与个人隐私信息保护

2020 年 2 月 9 日，中共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》，指出积极利用包括个人信息在内的大数据支撑新冠肺炎疫情联防联控工作的同时，要做好联防联控中的个人信息保护。

1. 疫情防控中需要保护的个人信息类型

个人信息保护，针对的是个体层面的数据。姓名、家庭住址、身份证号、手机号、行踪轨迹等，均属于个人信息。然而，不同类型和性质的信息应具备的信息保护水平也不相同，当公众利益与个人合法权益冲突时，个人信息保护也需要有一定利益权衡。

目前，在国内现行法律中，没有明确的将某些类型的个人信息赋予更高等级的保护。在国家标准 GB/T 35273《信息安全技术 个人信息安全规范》（以下简称：《个人信息安全规范》）中，提出了“个人敏感信息”的概念，以此区别于个人信息，如图 4 所示。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的范围和类型可参见附录 A。

3.2

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：关于个人敏感信息的范围和类型可参见附录 B。

图 4 《个人信息安全规范》中对个人信息相关概念定义

本质上，《个人信息安全规范》中采取的是场景式的定义。有些信息，例如姓名、电话号码，在平日仅仅是个人信息，但是部分武汉人民（及从武汉返乡人员）的这些信息，在当下疫情防控的特殊情形中，应当认为是个人敏感信息。从个人信息控制者角度看，如果这些信息结合其自身的性质（例如疾控机构）、使用这些信息的目的（例如追踪、隔离）、当下社会的普遍情绪（例如恐慌、猜忌）等因素，“一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等”的，就应当将这些信息“升格”为个人敏感信息来保护。

因此，个人敏感信息这个定义是依赖于场景的——即何种信息在何时落入个人敏感信息这个类别，是和场景密切相关的。这种逻辑，实际上与欧盟《通用数据保护条例》General Data Protection Regulation，

简称：GDPR）定义特殊类型个人信息的逻辑是一致的。GDPR 中规定“禁止以下数据处理行为：处理个人数据，揭露出其种族、民族、政治观点、宗教和哲学信仰，或工会成员身份；处理基因数据、生物识别数据，以识别出特定个人；处理与健康相关的数据，或与自然人性取向或性经历有关的数据。”也就是说，GDPR 中的特殊类型个人信息数据，不是单纯的种族、民族、政治观点、宗教和哲学信仰、工会成员身份这几类具体的信息，而是数据控制者能够用来推断出上述信息的有关数据都包含在内。

例如，数据控制者知道一个清真寺的地理位置，同时得知一位个人每周去该地理位置五次之多，可以推断出这位个人大概率信奉穆斯林。此时，地理位置信息就应当被认定为 GDPR 中的特殊类型数据，享有特殊保护。

同样的，与健康相关的信息也是同样逻辑。在当下，武汉市民（及从武汉返乡人员）几乎等同于新型冠状病毒高危人群，其家庭住址、身份证号码等，被各个方面用于隔离、劝勉等目的。此时，其家庭住址、身份证号码等在 GDPR 中就会被当成与健康相关的信息，而“升格”为特殊类型数据。

2. 疫情防控中个人信息使用的合法性基础

在明确疫情防控中哪些个人信息需要保护之后，我们还需要明确有哪些组织和个人能够获取到这些个人信息，以及判断这些组织和个人获取和使用个人信息的合法性。研究团队将可以获取个人信息的主体划分为地方教育部门、公安部门（掌握铁路、航空等实名信息）、

基层工作人员、电信运营商和互联网公司（包括 SDK 类的企业）五类。

这五类主体中，只有基层工作人员需要主动收集这些个人敏感信息，其他主体则是通过改变信息使用目的的方式，将原本（自身或者别的主体）已经掌握的信息，转用于疫情监测、防控和感染源的隔离这个新的目的。

在个人信息保护法理中，无论是收集信息还是改变信息使用目的，均需要有合法性基础。在我国，合法性基础主要是个人的同意，《网络安全法》中并没有给出同意的例外情形，而此种场景下的数据收集和共享行为的合法性基础，可以从《中华人民共和国传染病防治法》和行政法规《突发公共卫生事件应急条例》获得。具体法律条文如下：

（1）《中华人民共和国传染病防治法》（2013 年修订）总则第十二条：

“在中华人民共和国领域内的一切单位和个人，必须接受疾病预防控制机构、医疗机构有关传染病的调查、检验、采集样本、隔离治疗等预防、控制措施，如实提供有关情况。疾病预防控制机构、医疗机构不得泄露涉及个人隐私的有关信息、资料。

卫生行政部门以及其他有关部门、疾病预防控制机构和医疗机构因违法实施行政管理或者预防、控制措施，侵犯单位和个人合法权益的，有关单位和个人可以依法申请行政复议或者提起诉讼。”

总则的这条规定，配合第三章“疫情报告、通报和公布”中第三十二、三十三条要求疾病预防控制机构“应当主动收集、分析、调查、核

实传染病疫情信息”等，以及第四章“疫情控制”中第三十九至四十一条要求医疗机构和疾病预防控制机构采取的措施，可解读为，疾病预防控制机构、医疗机构为了疫情管控，具备改变个人信息使用目的的法定授权。

（2）《突发公共卫生事件应急条例》（2003 年制定）第三章“报告与信息发布”中的第二十一条:

“任何单位和个人对突发事件，不得隐瞒、缓报、谎报或者授意他人隐瞒、缓报、谎报。”

这条规定，配合第二章“预防与应急准备”第十、十一条中国务院和省、自治区、直辖市人民政府制定、实施“突发事件应急预案”，以及“突发事件应急预案”中应包含“（二）突发事件的监测与预警;（三）突发事件信息的收集、分析、报告、通报制度;（四）突发事件应急处理技术和监测机构及其任务”等内容的要求，再配合第四章“应急处理”第四十四条的规定:

“在突发事件中需要接受隔离治疗、医学观察措施的病人、疑似病人和传染病病人密切接触者在卫生行政主管部门或者有关机构采取医学措施时应当予以配合；拒绝配合的，由公安机关依法协助强制执行。”

以上条款可以解析为，人民政府在突发事件应急预案中，可以将除了卫生行政机构、疾病预防控制机构和医疗机构之外的部门、机构、组织、个人纳入，并赋予其信息收集、分析的职权与任务。

综合以上分析可知，《传染病防治法》和《突发公共卫生事件应

急条例》给了人民政府、卫生行政部门、疾病预防控制机构、医疗机构非常强的信息收集、分析的授权。人民政府可以在“突发公共卫生事件应急预案”中将信息收集、分析的权力再次授权给相关部门、机构、组织，这其中就可能包括公安部门、基层一线工作人员。《传染病防治法》和《突发公共卫生事件应急条例》中均要求任何单位和个人均应该配合，这自然包括相关信息的提供。由于《传染病防治法》《突发公共卫生事件应急条例》属于特别法，优于《网络安全法》等一般法律。因此，尽管《网络安全法》中个人信息收集和使用并没有给出同意的例外情形，上述疫情防控中的数据收集和共享行为在法律合法性方面并不存在问题。

3. 国外突发公共卫生事件中的个人信息保护规定

以全球“最严”个人信息保护法著称的欧盟 GDPR 为例，对于像新冠肺炎疫情这样的突发公共卫生事件，除个人同意之外，GDPR 还有另外三个合法性事由可供使用，分别是个人数据处理“为履行数据控制者承担法定义务所必须”、“为保护数据主体重大利益或其他自然人重大利益所必须”和“为执行公共利益之目的任务或数据控制者行使法定职能所必须”。这三个合法性事由，能有力地支撑其疾病预防控制机构、医疗机构，以及相关组织利用个人信息开展疫情防控工作。

当然，在具备合法性的前提下，GDPR 还要求具体的数据处理要遵循以下基本原则包括：合法、公平、透明原则；目的限定原则；数据最少够用原则；准确性原则；存储期限限制原则；完整性和保密性原则；以及权责一致原则。

体现上述思路的一个典型例子是 2013 年欧盟通过的“关于严重的跨境健康威胁的决定”。该“决定”在欧盟范围内建立预警和响应系统（EWRS），并明确针对暴露于健康威胁、存在感染危险或已经感染的人可以采取接触追踪措施。在符合接触追踪的目的时，允许主管部门收集，并在相关成员国之间共享必要的个人信息。而在开展此种数据收集、使用时，“决定”要求数据收集、使用完全遵守欧盟个人信息保护法律框架的规定，也就是符合上述基本原则。EWRS 中关于个人数据交换安全保障措施如表 1 所示。

表 1 EWRS 中个人数据交换安全保障措施的概览

项目	安全保障措施
对在系统中共享的个人数据的有限访问权限	● EWRS 仅可由已获授权的用户访问：国家主管部门（The Competent Authority，由成员国指定的相关权责部门）、欧盟委员会和欧盟疾病防控中心； ● 访问通过安全、个性化的用户账户和密码加以保护； ● EWRS 的信息概览页面已进行显著警示，告知访问用户：通用信息通道不可用于传输追踪接触者所需的个人数据。
选择性通信功能	● 个人数据应当通过 EWRS 中的“选择性信息功能”传输；

项目	安全保障措施
	● 个人数据仅可向接触追踪措施中所涉及的成员国主管部门传输； ● 其他 EWRS 用户、欧盟委员会和欧盟疾病防控中心被自动排除在通过选择性信息通道访问个人数据之外（除非该访问为应对协作行动所必须）。
个人数据的日常更正和处理期限	● EWRS 内置的在线功能，允许更正、删除选择性通信功能中包含的存在不准确、过时、不再必要或违反数据保护法律的个人数据； ● 在选择性信息通道中有特定机制允许所涉的主管部门基于数据主体的请求进行沟通和协作； ● 自发布之日起 12 月内，EWRS 内置的在线功能会自动清除选择性通信功能中所包含的个人数据。
数据控制者的责任划分	● 成员国主管部门和欧盟委员会为数据的共同控制者，欧盟疾病防控中心为数据处理者； ● 作为共同控制者，成员国在告知和数据更正方面承担控制者义务； ● 欧盟委员会在数据最小化存储方面承担数据控制者义务； ● 成员国主管部门负有义务及时通知其他主管部门，如其涉及数据处理违反盟数据保护法律（特别是当所处理的数据并非接触追踪所必需）。

4. 个人信息采集、分析、应用中的保护措施

（1）疫情防控数据采集过程中的个人信息保护

对于返乡、返工人员信息的统计和利用，是疫情联防联控的重要手段之一，需要做好疫情有效防控和个人信息保护之间的平衡。出于传染病防治等公共卫生保障目的，从武汉等疫情严重地区返乡、返工人员应当接受并配合疾病防控有关部门开展的走访调查等工作，同时疾病防控相关部门内部之间也需要共享此类信息。

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，统计相关人员个人信息。这个过程涉及到个人信息的采集、汇总、共享、披露等多个环节，每个环节都应当注意做好个人信息保护工作，以防出现数据泄露、丢失、滥用等情形。

比如，采集过程中，如果各地疾病防控机构、基层街道社区等以纸质填表方式开展的走访调查，则需要严格要求纸质材料不被拍照、复印，进行统一回收，保管妥当。如果以电子方式记录或汇总相关信息，需要责任到人，并保存在特定的终端，并将数据和备份数据加密存储。

在汇总存储环节，尽可能相对集中管理和处理个人信息，采用严密的访问控制、审计、加密等安全措施。

在向疫情防控工作相关方共享、传输相关数据时，应确认对方是有权获取数据的机构或个人，并采取加密传输的措施。

最后，在个人信息使用过程中，需要做到专采专用，严格限制于疾病防控目的，不得挪作他用，并且在疫情防控结束后内按照规定予

以删除。

（2）疫情防控信息披露过程中的个人信息保护

对于疫情报告、通报和公布等对外披露工作，仅公开返乡人员的流动统计数据以及确诊患者的性别、确诊日期、发病症状等非个人敏感信息，即可满足社会一般公众对疫情状况的知情权，而不应公开姓名、年龄、身份证号码、电话号码、家庭住址等。对于确诊或疑似病例所在地区的公众，可公开确诊或疑似病例的大致居住区域，满足此类公众对防控需求的知情权，都不必公开患者具体的个人信息。

如果掌握涉及“密切接触传染源”的重点人群信息，需要与其直接取得联系的，应安排专人负责，保证其联系方式不被扩大传播，相关人员名单应进一步限定知晓范围，予以重点保护。

（3）疫情防控大数据应用过程中的个人信息保护

如前文分析，相较于传统的走访、摸排、登记，将信息技术和大数据分析运用于传染病疫情防控和监测，能够更加及时、准确和高效。当前，全社会广泛采集各类人员信息，用于甄别与武汉相关人员的行踪。广泛采集的背后，势必有着一少部分的管理疏忽、使用不当等现象，甚至在人员信息泄露或非法披露后，相关配合登记工作的人员反而“完全被暴露”在公众视线之下，承受了巨大的心理压力，甚至可能影响其人身安全。而且，对个人信息的保护不力将直接影响到后续信息采集过程中公众、机构对采集方的信任度，而导致效率、精度等下降，让助力疫情防控的效果大打折扣。对保护个人隐私、科学安全使用大数据有以下建议：

第一，明确具有收集使用相关个人信息权力的指挥机构、执行机构，并明确相关工作的启动条件和流程规范，按需调取，责任到人。

第二，建立统一集中管理机制，运用去标识化、加密等措施对数据进行预处理，在数据关联分析过程中不指向个人身份，在锁定存在风险的对象后，再进一步进行身份重标识处理。

第三，大数据关联分析结果可主要用于监测疫情态势，涉及触达相关人员需审慎。

第四，采用严密的访问控制、审计、加密等安全措施，防止数据泄露、丢失、未授权的使用。

第五，做好疫情退散后数据处理的方案。

（二）疫情防控与网络和信息安全

在如火如荼的疫情防控期间，除了新型冠状病毒，网络和信息安全问题也需要我们警惕。犯罪分子很可能趁着疫情防控的紧要关头，借助人民群众对于疫情的恐慌心理，开展网络攻击、电信诈骗以及传播网络谣言，影响疫情防控工作的正常进行。因此，网信安全相关部门以及企业和个人都应加强防护，抵御网络和信息安全攻击。

1. 疫情防控期间的网络安全攻击

回顾历史，当重大疫情袭来时，趁火打劫式的网络安全攻击已然屡见不鲜。2014 年 3 月，埃博拉病毒横扫西非，感染万人后向全球扩散，在疫情传播期间，仅 Symantec 一家，数天内四次截获埃博拉病毒主题恶意网络攻击。黑客为达到目的，不惜冒充大型电信服务提供商广发钓鱼邮件，以埃博拉病毒展演诱惑目标，开展钓鱼攻击。2015

年 5 月，源起中东的 MERS 极速扩散，千里之外的韩国一日内即隔离数千人，网络犯罪分子同样借由电子邮件传播恶意软件，Trojan.Swort 木马伪装成一个文件名为“MERS_医院和受感染患者名单.docx.exe”，借 MERS 疫情恐慌洗劫全网。

2020 年 1 月，中国武汉新冠肺炎疫情暴发，黑客团伙借着疫情向我国政府部门、医疗机构发起攻击。

2 月 4 日，360 安全大脑捕获了一例利用新冠肺炎疫情相关题材投递的网络攻击案例，调查后发现是由印度 APT 组织对我国医疗机构发起定向攻击，攻击者精心利用新冠肺炎疫情相关题材做诱饵文档，如“新型冠状病毒感染引起的肺炎的诊断和预防措施”、“武汉旅行信息收集申请表”等，进而通过相关提示诱导受害者执行宏命令，医疗机构、医疗工作领域成为了最大受害者。

在美国，黑客通过将其垃圾邮件伪装成由疾病预防控制中心和病毒专家发布的新型冠状病毒官方警报，告知攻击目标疾病预防控制中心已建立了事件管理平台，以链接的形式诱使他们接受其城市周围新感染病例的更新列表，进而通过钓鱼页面窃取用户凭证，主要攻击目标为个人用户。

在当前疫情防控攻坚战的紧要关头，各级政府、企事业单位和个人更应该提高网络安全意识，加强网络安全防护，规避和防范网络钓鱼邮件、鱼叉攻击和恶意软件，不给网络攻击留下可趁之机。

2. 疫情防控期间的远程办公安全

新冠肺炎疫情防控期间可以说是我国数字化时代最大规模的一

次集体远程办公。对于 IT 互联网企业来说，远程办公并不陌生，但对于大量传统行业的从业人员来说，大规模的远程办公可能带来一系列隐私和数据安全隐患，需要企事业单位管理者和从业人员重点关注。

第一类安全隐患来源于员工的安全意识不足。据 CNBC 关于网络安全风险的研究中，员工的疏忽被证明是最大的威胁。在远程办公环境下，员工脱离了企业的安全边界，从外部互联网环境访问和处理任何能够维持正常工作的账户、文档或数据。多数企业员工对线上办公存在的网络安全风险并不了解，个人电脑、WiFi、邮件、甚至摄像头、U 盘等都可能存在数据泄露风险，且员工无法做到安全事件的及时发现、及时处置。

第二类安全隐患来源于远程办公安全防护手段不到位。特殊时期，大量远程工作人员经常会使用公共 WiFi，例如机场休息室、酒店、咖啡店甚至邻居网络，企业数据安全受攻面成几何级数放大。然而，很多企业原有的安全防护手段不到位，缺乏可靠的安全接入平台，没有 VPN、堡垒机等基础安全手段。一旦开展互联网办公，接入和传输通道均存在较高风险。

第三类安全隐患来源于企业服务暴露面的增加。对于很多企业来说，远程办公意味着部分内部业务系统需要开放互联网访问权限，部分服务开放端口用于远程操作和运维。这些因远程办公而开放出来的系统、服务和端口，一方面可能被黑客嗅探和利用，成为黑客组织、勒索软件、蠕虫病毒攻击的目标；另一方面也可能由于缺乏权限管理及动态回收机制而带来安全隐患。

为了保障远程办公安全有序的开展，研究团队针对性的整理了如下几项关键措施：一是做好员工安全教育，培养员工安全意识，保证员工做好基础的安全防护措施，如保持 Windows 防火墙正常开启、安装系统安全软件、及时修复个人电脑和路由器漏洞、使用高强度密码等；二是完善远程办公必要安全手段，从技术层面增加安全防护，VPN、堡垒机、双因素/多因素认证等技术手段能够增加黑客攻击难度，提升远程办公安全性，针对管理层等高价值目标甚至可以启用硬件密钥或生物认证等；三是重点防护远程办公期间新开放的系统、服务和端口，对于这些系统、服务和端口要充分进行扫描和测试，及时发现和修补漏洞，要建立相应的权限管理和动态回收机制，安全责任落实到具体人员。

3. 疫情防控期间的电信网络诈骗

利用热点事件实施诈骗一直是不法分子的惯用手段，新冠肺炎疫情发生以来，利用疫情相关信息开展电信网络诈骗方式层出不穷，梳理和归纳几类主要的电信诈骗手段如下：

第一类是购物类诈骗。新冠肺炎疫情发生以来，口罩、消毒液、防护服等产品成为紧缺物资，犯罪分子利用大家迫切购买口罩等物资的心理，谎称有货可以代购或者搭建钓鱼网站虚假销售，欺骗用户付款或点击钓鱼链接，以此直接或间接骗取钱财。

第二类是冒充类诈骗。诈骗分子利用人们对于新冠肺炎疫情的恐慌心理，冒充政府部门、疾控部门或者相关药物研究部门推广所谓防治特效药骗取钱财，冒充慈善机构骗取爱心捐助，或者冒充亲属谎称

感染新型冠状病毒，以汇缴住院费等方式骗取钱财。

第三类是退费类诈骗。新冠肺炎疫情发生后，为了减少人员流动、避免人员聚焦，国内、国际部分交通停运，大量火车票、机票、酒店等涉及到退票退费。不法分子利用这一形势，通过虚假电话和虚假信息引导用户点击诈骗网址或提供账户、密码等重要信息，进而盗取用户钱财。

在防范疫情期间的电信网络诈骗方面，需要人民群众提高警惕，在以下三个方面做好防范：一是加强个人信息保护，不轻易填写或提交个人敏感信息；二是认准官方渠道，信息获取、购物交易以及退改签等事项均需要从官方渠道进行；三是提高信息甄别能力，认真核实和辨别陌生电话、虚假信息和虚假邮件，不轻易点击虚假信息和邮件中的链接。

四、新技术在疫情防控中的安全应用思路与工作建议

（一）新技术在疫情防控中的安全应用思路

在新冠肺炎疫情防控过程中，我们看到很多的新技术新应用不断涌现，人工智能、大数据、云计算、区块链等新技术在突发公共卫生事件的预测和防控中发挥了重要的作用。然而，当前涌现的各类应用由政府、企事业单位自主发起，部分功能交叠重复，缺乏系统性的顶层设计。为了进一步梳理清晰新技术在突发公共卫生事件中的应用思路，研究团队从突发公共卫生事件的预测、防控、诊疗和恢复四个生命周期阶段出发，整理了各个阶段中新技术的应用模式，以便为后续防控和研究提供参考，具体如图 5 所示。

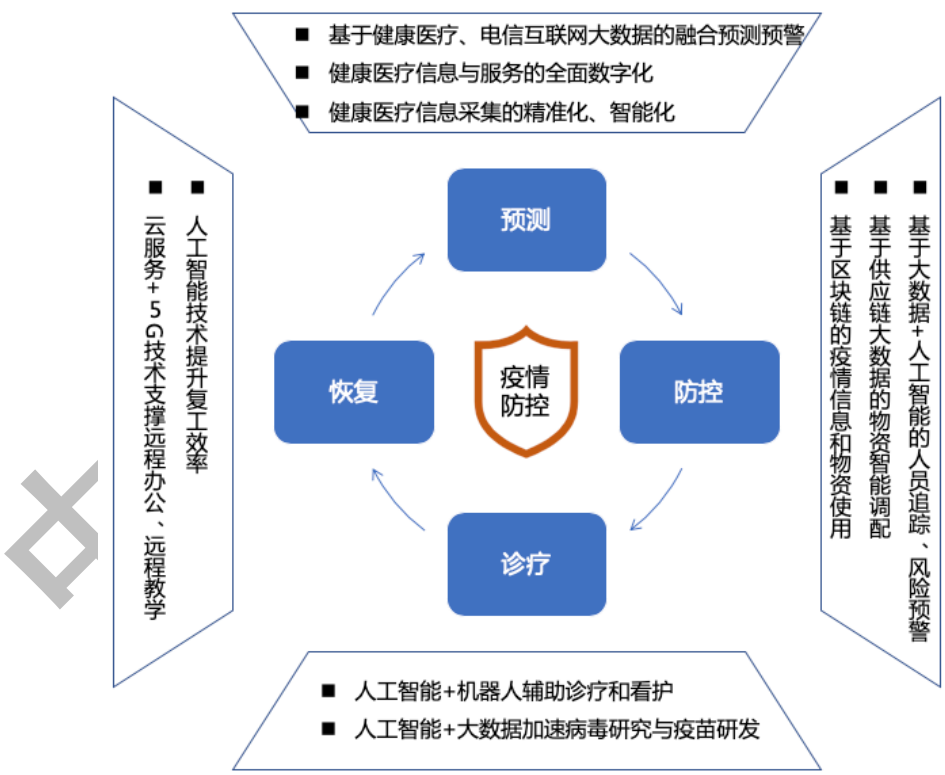


图 5 新技术在疫情防控生命周期中的应用

在公共卫生事件预测方面，大数据技术是最为核心的技术手段。基于健康医疗大数据和电信互联网大数据的融合分析，一定程度上能

够预测和预警某些传染性疾病的暴发趋势。例如通过分析搜索引擎的搜索词数据，结合地域和人群信息，可以获知某地人群正在关注某些疾病或者症状，再结合当地医疗机构的健康医疗数据，就可以相对准确了解到该地域人群的健康状况和发病信息，结合病种相关信息以及大数据模型，可以进一步预测该地是否可能暴发某类传染性疾病，从而可以在一定程度上提前开展疫情防治工作，扼杀疫情于摇篮。不可忽视的是，上述描述的场景需要基于医疗信息和服务的深度数字化和互联互通。与此同时，健康医疗信息的采集也需要更加智能化和精准化，这有赖于传感器以及可穿戴技术在数字医疗领域的大规模推广应用。

在公共卫生事件防控方面，人工智能、大数据、云计算以及区块链均有各自重要的应用场景。人工智能技术与大数据技术结合，基于人员的定位、通信、交易、住宿、交通等数据，一方面可以快速追踪疫情感染人员、潜在被感染人员以及密切接触人员，做到疫情的高效、精准防控；另一方面能够预测预警可能暴发疫情的地区，提前开展疫情防控。基于疫情物资供应链的大数据技术，能够从宏观层面智能地进行物资调配和供给，推动物资供应链的快速运转和物资的合理分配，从而保障疫情重灾区的物资供给。搭建基于区块链技术的疫情信息和物资使用平台，通过区块链去中介、防丢失、防篡改和易追溯的技术特点，保障疫情信息的权威性以及物资的可追溯性。

在公共卫生事件诊治方面，人工智能技术是最主要的技术手段。一方面，可以通过人工智能算法加速病毒研究和疫苗试验，缩短治疗

传染性疾病疫苗和新药的研发时间；另一方面，人工智能技术与机器人技术相结合，可以在一定程度上辅助传染病诊疗和病人看护，如部分机器人可以替代医护人员进行送药等，既能避免医护人员与感染病人的直接接触，也能缓解医护人员人力不足等问题。

在公共卫生事件恢复方面，以云服务为主的信息技术将发挥重要作用。基于云平台的远程办公、视频会议、直播课堂等应用的普及，一方面避免了由于集中办公、集中教学等带来的人员聚焦交叉感染的风险；另一方面支撑大量企事业单位复工复产，降低受疫情影响产生的经济损失。

（二）新技术在疫情防控中的工作建议

1. 相关行业主管部门

政府部门是抗击新冠肺炎疫情的领导者，以人工智能、大数据为代表的新技术在疫情防控中的应用依赖于政府部门的统筹协调和统一部署。如前文分析，在利用大数据开展疫情防控工作中，健康医疗大数据、电信互联网大数据、公共交通大数据等需要国家卫生健康委、工业和信息化部以及公安部等多部门协同合作。因此，首先从顶层设计上国家各部委应加强协同合作机制，建立数据互联互通渠道，完善公共卫生事件应急响应方案，充分发挥大数据等新技术在疫情防控中的优势。其次，国家卫生健康委等行业主管部门应鼓励医疗机构和科研单位加强新技术在疫情防控中的应用研究，推动数字医疗与信息技术融合发展。最后，行业主管部门应把控新技术在疫情防控以及数字医疗中的应用安全，尤其是数据安全，做好数据安全的行业规范和监

督检查。

2. 疾控部门和医疗机构

疾控部门和医疗机构是传染病疫情防控的主力军，新技术在传染病疫情防控工作中的应用和普及，有望提升疾控部门和医疗机构的疫情防控能力，提高疫情防控工作效率，降低受到疫情感染的风险。对于疾控部门和医疗机构，一方面应该鼓励和支持新技术在数字医疗领域尤其是传染病疫情防控工作中的应用，创新思路，勇于接受和尝试新技术，协助新技术在数字医疗各类场景的推广和应用；另一方面，应充分重视新技术应用过程中的网络和数据安全问题，积极做好网络和数据安全防护措施。

3. 企事业单位

企事业单位是疫情防控工作重要的后备力量和生力军，承担着为疫情防控提供弹药和武器的工作。科研机构以及科技类企业往往是新技术的研究者和创新者，应该充分发挥其在新技术领域的技术优势，勇于探索，善于创新，充分挖掘新技术在传染病疫情防控领域的应用空间和应用价值，利用新技术为疫情防控工作提供更为有力的武器。与此同时，企事业单位在应用新技术开展疫情防控过程中，更需要注重技术应用安全和用户个人隐私保护，提高安全意识，建立安全机制，完善防护手段，落实安全责任，保障新技术在疫情防控工作中的安全应用。

4. 普通民众

普通民众是疫情防控工作的中坚力量。在众志成城构筑群防群治

疫情防线的同时，民众也需要提高网络安全风险意识。建议采取以下措施进行防范：一是不轻易打开来历不明的电子邮件及其附件；二是不轻易点击短信或微信中不明来源的链接；三是从正规应用商店或官方网站下载安装应用程序；四是安装杀毒软件并及时更新。欢迎向工业和信息化部网络安全威胁信息共享平台（网址 http://www.cstis.cn，邮箱 cstisaccount@caict.ac.cn）报送涉疫情相关网络威胁信息线索，切实维护网络秩序和公共利益。

中国信息通信研究院安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304911

电子邮箱：guofei@caict.ac.cn, zhangxueyang@caict.ac.cn

传真：010-62300264

网址：www.caict.ac.cn