全球数据安全观察

总第 78 期 2022 年第 06 期

（2022.02.14-2022.02.20）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、习近平总书记：加强数字经济等重要领域立法，完善反制“长臂管辖”等法律法规

习近平总书记2021年12月6日在十九届中央政治局第三十五次集体学习时的讲话中提出，要加强国家安全、科技创新、公共卫生、生物安全、生态文明、防范风险等重要领域立法，加快数字经济、互联网金融、人工智能、大数据、云计算等领域立法步伐，努力健全国家治理急需、满足人民日益增长的美好生活需要必备的法律制度。总书记指出，要坚持统筹推进国内法治和涉外法治，按照急用先行原则，加强涉外领域立法，进一步完善反制裁、反干涉、反制“长臂管辖”法律法规，推动我国法域外适用的法律体系建设。

https://mp.weixin.qq.com/s/Zu9NCtQ1PWIzd4yLGnZG4g

2、交通运输部等八部门修订发布《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》

2月15日，据中国交通新闻网消息，交通运输部、工业和信息化部、公安部、人力资源和社会保障部、中国人民银行、国家税务总局、国家市场监督管理总局、国家网信办八部门联合修订发布《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》（简称《通知》），

增加了事前联合监管要求，完善了全链条联合监管事项，细化了全链条联合监管流程。

《通知》要求地方有关部门优化服务流程，严把行业准入关，督促网约车平台公司不得接入未取得相应出租汽车许可的驾驶员和车辆。完善了全链条联合监管事项，将未取得网约车经营许可擅自从事经营活动，网约车平台公司向未取得相应出租汽车许可的驾驶员和车辆派单及未按规定向网约车监管信息交互平台传输有关数据信息，存在低价倾销、欺诈、对个人在交易条件上实行不合理差别待遇，危害网络安全、数据安全、侵害用户个人信息权益，非法经营资金支付结算，侵害网约车驾驶员劳动保障权益，不依法纳税，危害公众利益、扰乱社会秩序、影响社会安全稳定等八方面违法违规行为纳入联合监管工作事项。

https://mp.weixin.qq.com/s/cJKGNZG6sL4gnnDZvelmpA

3、《网络安全审查办法》正式实施 企业赴国外上市融资应守住国家安全底线

2 月 15 日，国家互联网信息办公室、国家发展和改革委员会等十三部门联合发布的《网络安全审查办法》（以下简称《办法》）正式实施。《办法》对上市审查申报的要求、时机和主体都做了明确要求。《办法》第七条提出，掌握超

过100万用户个人信息的网络平台运营者赴国外上市必须申报审查。中国网络安全审查技术与认证中心设立网络安全审查咨询窗口，开始接收网络平台运营者赴国外上市的审查申报。

https://mp.weixin.qq.com/s/pNRaXF0ceEBqBmeaUd9gfA

4、欧洲数据保护委员会宣布启动首次联合执法行动

2月15日，欧洲数据保护委员会（European Data Protection Board，以下简称“EDPB”）在官网宣布启动首次联合执法行动，在接下来的几个月时间里将协调欧洲经济区的22个国家监管机构（包括EDPB）对公共部门使用云服务的情况展开调查。监管机构将探讨公共机构在使用基于云的服务时在GDPR合规上面临的挑战，包括获取云服务时实施的流程和保障措施、与国际传输相关的挑战等。

https://mp.weixin.qq.com/s/vNJxfLf52a4EK46xNFJ2AA

5、美国国土安全部成立网络安全审查委员会

2月3日，美国国土安全部（DHS）宣布成立网络安全审查委员会（Cyber Safety Review Board，CSRB）。网络安全审查委员会的职责是向总统和国土安全部主任提供咨询建议，以提升美国国家网络安全。委员会没有监管权力，也不是执

法机构，其目的是总结分享经验教训，促进美国国家网络安全的进步。CSRB 的任务是审查和评估重大网络安全事件，以便政府、行业和安全社区能够更好地保护国家网络和基础设施。

https://mp.weixin.qq.com/s/7qV7jdPaqdQJBtUaHtVzDw

6、美国发布《儿童在线安全法案》草案

近日，美国议员提出《儿童在线安全法案》(Kids Online Safety Act)，该法案为 16 岁及以下的未成年人提供了更强的在线保护。立法者表示，该法案将“为未成年人提供保护他们信息的选项”，并要求设置“选择退出算法推荐”。该提案要求对算法、产品特征和定向广告系统进行年度评估。布莱克本说，该法案“通过设置必要的安全护栏”解决了潜在的危害，这将“提高透明度，让父母更加安心。”

https://mp.weixin.qq.com/s/XpDz3MiFg04TePxO7wbfOg

技术、产品与市场

1、谷歌宣布推出 Android 隐私沙盒，计划年内发布开发者预览版

2 月 16 日消息，谷歌宣布推出 Android 隐私沙盒，旨在引入更新、更具私密性的广告解决方案，以限制与第三方机构共享用户信息，但却不损害广告主短期利益。据介绍，谷歌计划在年内随测试版一起发布隐私沙盒开发者预览版。

此次推出的隐私沙盒建立在 Android 已有的网页端基础之上，为改善 Android 隐私提供了一条清晰的路径，同时又不会影响用户对免费内容和服务的访问。据介绍，开发者已可以在 Android 开发者网站查看隐私沙盒的初始设计方案并且分享反馈。谷歌计划在年内，随测试版一起发布开发者预览版。

https://www.secrss.com/articles/39308

2、2022 年中国隐私计算市场分析：隐私计算价值循环正式启动

隐私计算产业诞生于技术的成熟和市场的需求，爆发于数据监管与扶持政策的出台。其意义在于在保护信息安全的前提下，实现全方位数据流通，作为底层技术助力大数据体系建设，进而促进经济发展。

政策驱动下产品研发、项目验证测试和实际落地均在加速，隐私计算市场发展火热，但是处于探索期。具体体现于技术性能仍需提升，实际应用效果转化仍然有待验证，同时产业发展受限于数据源质量和权属等问题。

三大隐私计算技术的结合运用、隐私计算技术于区块链、人工智能技术的融合应用、隐私计算平台间的互联互通已经成为行业共识，但是技术的成熟仍然需要时间，需要在实际应用中逐个突破。

隐私计算目前主要落地于金融、政务和医疗三大领域，但是隐私计算在工业、制造业等实体经济的运用对经济发展作用更大，这将是隐私计算产业重点挖掘的领域。隐私计算作为大数据治理体系的底座，将会协同产业链上下游，共同致力于国家经济发展。

https://mp.weixin.qq.com/s/nU_18iHhz1W_rWnsMm8ASw

3、Gartner：IAM 技术发展六大趋势

由于数字业务依赖 IAM 赋能的数字信任，安全和身份管理成为企业业务生态系统的重要基础。日前，Gartner 列出了 IAM 技术发展的六大趋势，企业可以参考其完善已部署的 IAM，以更好地满足不断变化的需求。

（1）更智能化的访问控制

（2）更好的用户体验

（3）将设备身份统一纳管

（4）实施 API 安全控制

（5）适配多云环境

（6）更完善的 IGA（身份治理和管理）功能

https://mp.weixin.qq.com/s/3gS_JECat4DYhT461z0ubg

4、澳大利亚智库发布《大数据与国家安全》报告

近日，澳大利亚洛伊国际政策研究所（Lowy Institute）发布《大数据与国家安全：澳大利亚决策者指南》，报告指出，大数据推动经济社会创新发展，同时也在加剧国家安全威胁。当前正值维护地区安全的关键时刻，澳大利亚需要了解和应对大数据相关威胁，并且利用大数据等新兴技术以获取战略优势。

大数据作为一种新兴前沿技术，其影响国家安全的三个特征为：数据丰度、数字连接、技术无处不在，这三个特征持续快速进步，对国家安全构成新的威胁。利用大数据等技术在个人和国家层面上实施影响和干预，具有挑战民主原则和体制的潜在力量。除非在可能的情况下降级风险，否则将导致问题扩散失去控制。对澳大利亚来说，当务之急是缓解与大数据相关的国家安全威胁，确保技术的发展和创新能够

反映国家的价值观和文化，并管理大数据和新兴数字技术，以改善社会质量。

https://www.secrss.com/articles/39136

5、2021 年与勒索软件相关的数据泄漏几乎翻了一番

根据安全公司 CrowdStrike 周二发布的 2022 年全球威胁报告，2021 年与勒索软件相关的数据泄露和交互式入侵显着增加。

导致数据泄露的勒索软件攻击数量从 2020 年的 1,474 次增加到 2021 年的 2,686 次，增长了 82%。2021 年受数据泄露影响最大的行业是工业和工程、制造和技术。

该公司的报告强调了与伊朗有关的破坏性行动，威胁行为者使用“Lock-and-leak”策略瞄准了美国、以色列和中东北非地区。CrowdStrike 解释说：“Lock-and-leak 策略操作的特点是犯罪或黑客活动前线使用勒索软件加密目标网络，然后通过参与者控制的角色或实体泄露受害者信息。” “由于他们表面上不作为犯罪或黑客活动实体运作，而是利用专门的泄密网站、社交媒体和聊天平台进行活动，能够扩大数据泄露并对目标国家进行信息操作。”

https://www.securityweek.com/ransomware-related-data-leaks-nearly-doubled-2021-report?&web_view=true

业界观点

1、董月英：从法律视角看元宇宙发展的数据安全问题

元宇宙在 2021 年终于迎来了一个全新的发展阶段，在 2022 年里也将进一步加剧资本竞争、加快技术推进，北京大成（上海）律师事务所权益合伙人董月英从法律实践角度出发，对元宇宙可能涉及的法律问题进行一番梳理，其中对于数据安全与个人信息保护提出了见解。

董月英认为，对于开展数据处理活动的元宇宙公司而言，需依法严格履行《数据安全法》要求的数据安全保护义务，应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应立即采取补救措施。同时，需要及时关注跟进相关数据安全立法，建立健全平台数据合规体系。

董月英表示，元宇宙基于扩展现实技术提供沉浸式体验，这一特质意味着用户的大量个人信息不可避免地将被导入运营平台。运营方在收集、存储、使用、加工、传输、提供、公开、删除用户个人信息时，均需严格遵守法律规定，履行个人信息保护义务，严格遵循具有强制约束力的相关法律法

规，并有必要参酌相关标准、指南，不断完善自身个人信息合规的体系构建。

https://capwhale.com/newsfile/details/20220217/2692cfe96b7740ec9168b85f0a74a4b9.shtml

2、加快数字经济立法的专家观点：安全与发展并举，鼓励地方创新

2 月 16 日出版的第 4 期《求是》杂志，发表了重要文章《坚持走中国特色社会主义法治道路，更好推进中国特色社会主义法治体系建设》。文章指出，要加快重点领域立法。加强国家安全等重要领域立法，加快数字经济等领域立法步伐，努力健全国家治理急需、满足人民日益增长的美好生活需要必备的法律制度。

华东政法大学教授、互联网法治研究院院长高富平表示，数字经济立法，就是要保护有价值的数据生产者的权益，激励他们愿意将数据拿出来与他人分享或交易，实现数据的社会化利用。

高富平认为：“数据安全问题已经突破传统的保密、完整和可用这‘三性’，成为整个社会和国家安全综合体。需要我们分类别地解决这些问题，而不是动辄以安全为由禁止或限制人们对数据资源的利用。”

高富平进一步表示，个人信息保护层面，对应《个人信息保护法》中的个人信息安全防范和保障措施、个人信息泄露的补救措施本质上也是数据安全问题，也应当是数据安全的组成部分。但个人信息权益保护严格来说不是狭义数据安全问题，而是个人信息处理中的权益保护，是防范个人信息滥用问题，是个人信息利用秩序问题，要放在更大范畴内探讨。

https://www.yicai.com/news/101319532.html

3、高艳东：数据主权战争中的反殖民主义

由国家网信办、国家发展改革委等 13 部门修订的《网络安全审查办法》，2 月 15 日起开始施行。其中明确规定，掌握超过 100 万用户个人信息的网络平台运营者，赴国外上市必须申报网络安全审查。不久前，工业和信息化部再次就《工业和信息化领域数据安全管理办法（试行）》公开征求意见。该《办法》扩大了被监管数据的范围，细化了数据分类分级保护制度等，目的是维护我国的数据安全和主权。

浙江省新型重点专业智库浙江数字化发展与治理研究中心研究员高艳东认为，数据不仅影响人们生活，更关乎国家稳定，维护数据主权是大国的共同选择。近年，美国通过技术和规则优势掠夺他国数据资源、影响他国数据主权。我

国应在推动数据合理流动的基础上，谨防成为数据殖民地。

高艳东表示，面对美国的数据霸权，中国要全力捍卫数据主权，反对数据剥削。一方面，中国有能力捍卫数据主权。以 BAT 为代表的中国互联网企业，初步具备和硅谷巨头抗衡的能力，而得益于人口红利和互联网应用的活跃，我国的数据体量不容小视。另一方面，我国应逐渐从战略防守走向主动出击，倡导让各国受益的公平数据理念。通过国际条约等方式，在确保各国主权的前提下，让各国人民能够享受到大数据技术的红利，推动资源共享、互通有无，降低生产成本。

高艳东还认为，限制数据出境只是我国为了防范美国数据霸权的阶段性任务，而推动普惠、互利、平等的全球数据观，才是大国的责任。

https://opinion.huanqiu.com/article/46phX2p1G2d

4、企业采用软件对员工网络行为管理引发社会关注

近日，关于某公司安装“行为感知系统”的事件引发对“企业采用软件对员工网络行为管理”这一现象的讨论。

有律师表示，用人单位出于管理目的，在员工知情的情况下，可以有限度地使用该种管理软件，若侵入员工的私人领域，则属于侵权行为。

湖南师范大学人工智能道德决策研究所副教授文贤庆

认为，从科技伦理的角度来说，对员工上班进行全方位的实时监控是不合适的。他表示，“在此类软件已经被广泛使用的现状下，我们只好退而求其次，要求其遵守一些科技伦理的规范，例如告知员工监控的存在、企业使用数据的用途等。”

http://news.cyol.com/gb/articles/2022-02/19/content_j7vaAHwP3.html

5、网友建言：加强顶层设计，多方发力把好数据“安全门”

近日，多位网友在国家发展改革委创新和高技术发展司联合人民网面向社会开展的“我为数据基础制度建言献策”活动中提出建议，希望在数据治理方面形成全国“一盘棋”，进一步完善数据安全保护制度，建立统一的全国各行业基础数据标准和平台系统对接标准体系。

针对于如何将数据“管好用好”，有网友建议：“完善数据基础制度，一定要以全国为出发点，各省区市节点确保数据流通安全有序，加强数据源头保护、杜绝数据泄露和隔绝网络攻击数据基础设施，防范和化解数据终端和数据中心等安全危机，数据保护形成全国‘一盘棋’。”

针对隐私数据的保护，有网友表示：“个人隐私信息在收集前，必须提前告知用户并得到许可，对于恶意收集信息的个人和单位必须严惩严罚。”同时，有网友认为基于数据

的特殊性，数据基础制度在设计上应既体现个人数据的隐私性，也体现基础数据的全民所有性，从而更好地服务社会。还有网友表示：“要充分做好数据系统国产化，数据加密与授权共享等底层技术体系设计与自主可控，做到数据流转的完全可控安全防护。”

http://finance.people.com.cn/n1/2022/0217/c1004-32354046.html

数据安全事件

1、美国一公司暴露了 700 万用户数据

2022 年 2 月 16 日，据报道，Website Planet 网络安全研究人员发现了一个存在安全风险的 Amazon S3 存储桶，其中包含约 700 万人的个人数据信息（姓名、电子邮件、电话号码、地址等）。据悉，存在安全风险的存储桶属于一家美国的营销公司 Beetle Eye，该公司大多数客户是美国人，也有许多客户是加拿大人。研究人员表示， S3 存储桶中包含大概 6000 个文件，总计超过 1 GB 的数据。“该桶”没有正确配置，也不存在任何密码保护和加密来保护其内容，所有互联网用户都可以随意公开访问其中数据。

https://www.freebuf.com/news/321955.html

2、互联网协会数据泄露暴露 8 万会员登录信息

2022 年 2 月 15 日，致力于保持互联网开放和安全的非营利组织互联网协会 (ISOC) 将其 80,000 多名成员的个人数据意外暴露归咎于第三方供应商。这些数据可在未受保护的 Microsoft Azure 云存储库上公开访问，其中包含数百万个 JSON 文件，其中包括全名、电子邮件和邮寄地址以及登录详细信息。

https://www.zdnet.com/article/fortune-500-service-provider-

says-ransomware-attack-led-to-leak-of-more-than-500k-ssns-more/

3、香港海逸酒店遭网络攻击，超过 120 万宾客的个人资料遭泄露

2022 年 2 月 14 日报道，长实集团旗下海逸酒店管理有限公司近日遭受一项网络安全事件的影响，涉及旗下部分酒店的住宿预订资料库，并已识别出约 120 万位人士的资料可能受到影响，调查工作正在进行中。海逸酒店集团表示，在攻击发生后，它立即聘请了第三方法证专家团队调查和控制事件。

https://www.databreachtoday.com/data-leak-at-hong-kongs-harbour-plaza-hotel-affects-12m-a-18517

4、联邦调查局警告称，俄罗斯民族国家黑客针对美国承包商获取敏感国防信息

2022 年 2 月 17 日，联邦调查局警告说，俄罗斯国家支持的特工正在瞄准美国承包商网络以获取敏感的国防信息，其中一些人获得了至少六个月的持续访问权。

美国网络安全和基础设施安全局 (CISA) 16 日发布的一份声明详细说明了它如何观察到 2020 年 1 月至 2022

年 2 月期间美国已获批准的国防承包商 (CDC) 的“常规目标”。CISA 表示，在两年的时间里，俄罗斯参与者保持对多个 CDC 网络的持续访问，在某些情况下至少持续六个月。FBI、NSA 和 CISA 注意到电子邮件和数据的定期和反复泄露。

https://portswigger.net/daily-swig/russian-nation-state-hackers-targeting-us-contractors-for-sensitive-defense-information-fbi-warns

5、货运服务巨头 Swissport 遭受 BlackCat 勒索软件攻击，造成数据泄露

2022 年 2 月 15 日，据外媒报道，BlackCat 勒索软件组织，又名 ALPHV，声称对最近的 Swissport 的网络攻击事件负责，该攻击导致航班延误和服务中断。

货运和酒店服务巨头 Swissport 公司在 50 个国家的 310 个机场开展业务，并提供货物装卸、维护、清洁和休息室接待服务。

目前，BlackCat 泄露了据称从最近的勒索软件攻击中获得的 TB 级数据。威胁参与者声称他们愿意将整个 1.6 TB 的“数据转储”出售给潜在买家，数据泄露页面包含护照图像、内部业务备忘录以及求职者的详细信息等。

https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/

6、新的 MyloBot 恶意软件变种发送勒索电子邮件，索要 2,732 美元的比特币

2022 年 2 月 15 日报道，已观察到新版本的 MyloBot 恶意软件部署了恶意负载，这些负载被用于发送勒索电子邮件，要求受害者支付 2,732 美元的数字货币。Mylobot 于 2018 年首次被发现，它具有一系列复杂的反调试功能和传播技术，可以将受感染的机器捆绑到僵尸网络中。

https://thehackernews.com/2022/02/new-mylobot-malware-variant-sends.html

7、纽约生育诊所遭勒索软件攻击，导致信息泄露

2022 年 2 月 17 日报道，位于纽约市的一家生育诊所 Extend Fertility 正在通知患者，他们的个人数据可能在最近的网络攻击中被泄露并可能被盗。

专门从事体外受精和冷冻卵子和胚胎的 Extend Fertility 于 2021 年 12 月遭到勒索软件的攻击。该诊所聘请了第三方数字取证专家来确定事件的性质和范围。对这次攻击进行了长达一个月的调查发现，网络犯罪分子可以访问存储受保

护健康信息 (PHI) 和诊所部分患者个人数据的服务器。安全事件中可能泄露的信息包括姓名、性别、家庭住址、电话号码、电子邮件地址和出生日期、病史、诊断和治疗信息、服务日期、实验室测试结果、处方信息、提供者名称、医疗帐号和财务信息。

https://www.infosecurity-magazine.com/news/fertility-clinic-hit-with/?&web_view=true

8、运动品牌美津浓 Mizuno 遭到勒索软件攻击推迟订单

2 月 15 日，据知情人士透露，运动设备和运动服装品牌美津浓(Mizuno)在受到勒索软件攻击后，受到了电话中断和订单延迟的影响。

美津浓是一家日本运动器材和运动服装公司，在亚洲、欧洲和北美拥有超过 3800 名员工。该公司销售各种各样的运动设备，但最著名的是他们的高尔夫球杆，跑步运动鞋和棒球装备。

https://www.bleepingcomputer.com/news/security/sports-brand-mizuno-hit-with-ransomware-attack-delaying-orders/

9、威胁行为者从数十名 OpenSea 用户那里窃取了至少价值 170 万美元的 NFTs

2022 年 2 月 20 日，Security Affairs 网站报道，全球最大的 NFT 交易所 OpenSea 证实，其数十名用户受到网络钓鱼攻击，损失了价值 170 万美元的宝贵 NFTs。OpenSea 联合创始人兼首席执行官 Devin Finzer 证实了网络钓鱼攻击，他还补充说，32 名用户丢失了 NFTs。

https://securityaffairs.co/wordpress/128207/breaking-news/opensea-nft-marketplace-hacked.html

10、国家黑客利用 Zoho 漏洞入侵了红十字会的网络

2 月 16 日，红十字国际委员会表示，上个月披露的针对其服务器的黑客攻击是由国家支持的黑客组织协调的针对性攻击。

在事件期间，攻击者在"重建家庭联系"计划中访问了超过 515000 人的个人信息（姓名，位置和联系信息），该计划帮助因战争，灾难和移民而离散的家庭团聚。

https://www.bleepingcomputer.com/news/security/red-cross-state-hackers-breached-our-network-using-zoho-bug/