

全球数据安全观察

总第 70 期 2021 年第 46 期
(2021.12.06-2021.12.12)

目录

政策形势	1
1、工信部下架豆瓣、唱吧等 106 个 App	1
2、重庆：《重庆市数字经济“十四五”发展规划》印发	1
3、郑州：《郑州市数据中心产业发展规划（2021~2025 年） （征求意见稿）》发布，投资规模超 1800 亿	2
4、广州市海珠区数据经纪人试点工作方案	2
5、北京数字经济标杆城市建设场景发布	3
业界观点	4
1、App 超范围收集个人信息“七类”隐蔽问题需紧盯不放 ...	4
2、国内外隐私计算标准现状	4
3、今年美国有大约 4000 万人的个人健康信息在泄露事件 中被曝光.....	6
4、新型智慧城市数据安全研究与思考	7
5、鼓励依法合理有效利用数据，为数据安全提供基础性法律 保障	8
安全事件	9
1、未经许可收集人脸信息，英国一公司面临 1700 万英镑罚 款.....	9
2、荷兰税务局违反 GDPR，被罚 275 万欧元	9
3、法国交通巨头 57,000 名员工个人信息和源代码泄露 ...	10
4、美国食品进口商亚特兰大承认勒索软件攻击	10
5、南澳大利亚州 8 万名政府雇员信息恐被泄露	11
6、沃尔沃承认数据泄露，部分研发数据被盗	11

政策形势

1、工信部下架豆瓣、唱吧等 106 个 App

2021 年 12 月 9 日，工信部在《关于下架侵害用户权益 App 名单的通报》中指出，今年以来，工信部持续推进 App 侵害用户权益专项整治行动，加大常态化检查力度，先后三次组织对用户反映强烈的重点问题开展“回头看”。在被工信部信息通信管理局通报存在“超范围收集个人信息”等问题一个多月后，豆瓣等 APP 因未及时整改被下架处理。

<https://mp.weixin.qq.com/s/NzBEvOPmM0iSYvuZKnDKiA>

2、重庆：《重庆市数字经济“十四五”发展规划》印发

为加快打造“智造重镇”、建设“智慧名城”，不断激发我市数字经济创新发展活力，再创数字经济发展新优势，重庆市人民政府印发重庆市数字经济“十四五”发展规划（2021-2025 年）。规划指出，到 2022 年，集聚“100+500+5000”（100 家创新能力强、发展后劲足、带动效应显著的数字经济龙头企业，500 家前沿领域高成长创新企业，5000 家“专精特新”中小微企业和创新团队）数字经济领域市场主体，打造千亿级数字经济核心产业集群，创建 10 个国家数字经济应用示范高地，高水平建成国家数字经济创新发展试验

区。到 2025 年，大数据智能化走在全国前列，全市数字经济总量超过 1 万亿元，建成国内领先、具有全球影响力的数字经济创新发展高地，数字经济成为支撑我市“智造重镇”“智慧名城”建设的主力军。

<https://mp.weixin.qq.com/s/E1Mmvr7RZrdkghL4WtbOog>

3、郑州：《郑州市数据中心产业发展规划（2021~2025 年）（征求意见稿）》发布，投资规模超 1800 亿

12 月 6 日，郑州市发改委网站发布《郑州市数据中心产业发展规划（2021~2025 年）（征求意见稿）》公开征求意见的公告。《公告》显示，到 2025 年，郑州市打造为具有全国影响力的数据中心产业基地，建成全国一体化算力网络国家枢纽节点核心城市。互联网数据中心直接投资及带动投资规模超过 1800 亿元，互联网数据中心业务收入及关联产业年均收入超过 850 亿元。

<http://www.21jingji.com/article/20211206/herald/1dbc2a5496b01cd11d5c8e408acdfa98.html>

4、广州市海珠区数据经纪人试点工作方案

广州市海珠区推出《广州市海珠区数据经纪人试点工作方案》（以下简称《试点方案》），率先开展数据经纪制度

探索，为向全国数据要素市场建设提供“试验田”。

《试点方案》坚持以供给侧结构性改革为主线，以市场化配置为导向，以培育数据经纪人为抓手，促进数据可信有序流通和市场化利用，加速数据与经济活动融合。要求建立试点监管制度，在资格认定、分类分级管理、风险防控机制、数据安全与隐私保护、日常监管、从业人员管理及数据管理能力等方面，探索建立健全数据经纪人监管制度体系。

https://mp.weixin.qq.com/s/Y7Q_-gnnEI6kpTHbSuoSsg

5、北京数字经济标杆城市建设场景发布

12月7日，在京港洽谈会2021数字经济赋能产业发展专题活动上，北京市经信局发布了北京数字经济标杆城市建设的两大场景：高级别自动驾驶示范区和大数据交易所。

相关负责人表示，经过5到10年的持续努力，北京将成为引领全球数字经济发展的六个高地，即城市数字智能转型示范高地、国际数据要素配置枢纽高地、新兴数字产业孵化引领高地、全球数字技术创新策源高地、数字治理中国方案服务高地、数字经济对外合作开放高地。

<https://news.cnstock.com/industry,rdjj-202112-4793337.htm>

业界观点

1、App 超范围收集个人信息“七类”隐蔽问题需紧盯不放

国家计算机网络应急技术处理协调中心（CNCERT）、中国网络空间安全协会近日发布《App 违法违规收集使用个人信息监测分析报告》。报告显示，我国个人信息保护法律法规体系日趋完善，App 违法违规收集使用个人信息治理取得阶段性成果，强制收集非必要个人信息问题明显减少，超范围收集个人信息行为治理成效初显，但“七类”隐蔽问题仍需紧盯不放。

报告指出，App 超范围收集个人信息的问题目前主要包括七种情形：一是敏感权限声明超出必要范围，二是权限索取超出必要范围，三是收集数据的敏感性超出必要范围，四是收集数据的具体内容超出必要范围，五是收集方式超出必要范围，六是收集频率超出必要范围，七是收集场景超出必要范围。

http://union.china.com.cn/cmdt/txt/2021-12/13/content_41820322.html

2、国内外隐私计算标准现状

目前，国内外针对隐私计算技术概念、技术框架、技术

要求、测试方法等方面已制定了一系列标准。但是比较分散，缺乏顶层设计和规划。ISO/IEC JTC1 SC27 在制定安全多方计算、同态加密等标准；国际电联 ITU-T SG17 已经开始重视隐私计算相关标准的体系化，专门为隐私计算标准预留出标准号段；工信部下属信通院在 CCSA 成立 TC601 大数据技术推进委员会，正在制定大量隐私计算技术与测评标准；北京金融产业联盟成立了数据专委会，开展了金融行业隐私计算标准化工作。

隐私计算相关国内标准

标准组织	标准名称	标准进展
TC260	研究课题《隐私计算技术应用指南》	制定中
	研究课题《多方数据安全交换共享技术要求》	已完结
	研究课题《多方数据融合计算安全指南》	制定中
CCSA	《共享学习系统技术要求》	报批稿
	《隐私保护场景下安全多方计算技术指南》	报批稿
	《基于可信执行环境的安全计算系统技术框架》	征求意见稿
金标委	JR/T 0196-2020《多方安全计算金融应用技术规范》	已发布
CCSA TC601	《隐私计算 多方安全计算产品性能要求和测试方法》《隐私计算 联邦学习产品性能要求和测试方法》等系列标准	已发布
AIIA	《共享学习系统技术要求》	已发布

隐私计算相关国际标准

标准组织	标准名称	标准进展
ISO/IEC SC27	ISO/IEC 4922 《Secure Multi-Party Computation》	Part1: CD 阶段 Part2: WD 阶段
	ISO/IEC 19592-1 《Information technology – Security techniques– Secret sharing》	已发布
	ISO/IEC 18033-6 《Information technology – Security techniques–Part 6: Homomorphic encryption》	已发布
	ISO/IEC 18033-8 《Information technology – Security techniques–Part 8: Fully homomorphic encryption》	刚立项
IEEE-SA	P2830 《Standard for Technical Framework and Requirements of TEE-based Shared Machine Learning》	已发布
	P2842 《Recommended Practice for Secure Multi-Party Computation》	已发布
	P2952 《Standard for Secure Computing Based on Trusted Execution Environment》	制定中
	P3652.1 《Guide for Architectural Framework and Application of Federated Machine Learning》	已发布
ITU-T	F.748.13 《Technical Framework for Shared Machine Learning System》	已发布
	X.1770 《Technical Guidelines for Secure Multi-Party Computation》	已发布
同态加密标准联盟	《Homomorphic Encryption Standard》	已发布

<https://mp.weixin.qq.com/s/5EeZw1OQ28-h-P85tvB14w>

3、今年美国有大约 4000 万人的个人健康信息在泄露事件中被曝光

2021 年 12 月 9 日，美国卫生和公众服务部（HHS）下属部门民权办公室（Office for Civil Rights）报告称，**2021 年** 共计收到 **578 起** 数据泄露事件，要比 2020 年的 599 起要

少。但是数据泄露影响的用户规模明显上升，去年影响了大约 2600 万人，而今年美国大约有 4000 万人的个人健康信息在事件中被曝光。

<https://www.cnbeta.com/articles/tech/1212543.htm>

4、新型智慧城市数据安全研究与思考

“十四五”时期，5G、大数据、人工智能、云计算等信息技术将推动新型智慧城市加速落地。智慧城市平台存储着国家、政府、城市、个人等核心数据资产，其数据安全密切关系到国家和社会的稳定运行。因此，政府亟需构建新型智慧城市一体化数据保障体系，以保证数据在全生命周期得到妥善保护及开发利用。

新型智慧城市的数据安全建设是一个立体多维的复杂工程，应当基于 5G 云网一体的新型数字基础设施，围绕数据安全生命周期，实现从城市物理实体到数字虚拟空间的准确映射，从智能感知、万物互联、安全感知、智能决策、统一管理等多维度，严格遵循“管理与建设并重”思路，围绕数据安全核心技术、数据安全运营、数据安全治理，打造新型智慧城市数据安全建设体系。

<https://www.secrss.com/articles/36868>

5、鼓励依法合理有效利用数据，为数据安全提供基础性法律保障

随着互联网、大数据、人工智能等蓬勃发展，各类数据迅猛增长、海量聚集，对国家治理、社会发展、人民生活都产生了深刻影响。

坚持发展与安全并重。这就要求我们在充分发挥数据资源作为未来基础资源和创新引擎作用、加快发展数字经济的同时，牢牢守住数据安全的底线。

强化个人和组织主体责任。保障数据安全，切实维护个人、组织的合法权益，关键是立足数据安全工作实际，着力解决数据安全领域的突出问题，明确并严格落实包括个人和组织在内的各类数据处理活动主体的安全保护义务与责任。

<https://mp.weixin.qq.com/s/5YnS1mPUgEw7GwoPKIH1Iw>

安全事件

1、未经许可收集人脸信息，英国一公司面临 1700 万英镑罚款

2021 年 12 月 7 日报道，英国信息专员办公室表示，人脸识别技术公司 Clearview AI 可能在大量英国人不知情的情况下收集了他们的图像。该公司为此可能面临 1700 万英镑 (约 2300 万美元) 的罚款。英国信息专员办公室在一份声明中说，Clearview AI 数据库中的图像“可能包括来自英国的大量人员的数据，可能是在人们不知情的情况下，从包括社交媒体平台在内的在线公开信息中收集的。”

<https://mp.weixin.qq.com/s/34rSuMwXqUVrcxKlhA45jg>

2、荷兰税务局违反 GDPR，被罚 275 万欧元

2021 年 12 月 8 日，荷兰数据保护执法机构官网报道，荷兰数据保护局 (DPA) 已对荷兰税务局处以 275 万欧元的罚款。罚款是因为多年来税务局以非法、歧视性和不当的方式处理有关儿童保育福利申请人的 (双重) 国籍的数据。这严重违反了《通用数据保护条例》(GDPR)，即管辖隐私的法律。

<https://mp.weixin.qq.com/s/2dtpo3BCT2m53kjbHtNK-w>

3、法国交通巨头 57,000 名员工个人信息和源代码泄露

2021 年 12 月 8 日，据外媒报道，一家国有法国交通巨头在通过不安全的 HTTP 服务器泄露个人信息后，无意中使近六万名员工面临身份欺诈。

据 vpnMentor 称，该服务器“对任何具有基本 Web 浏览技能的人都开放并可访问”。它包含一个可追溯到 2018 年的 SQL 数据库备份，其中包含超过 300 万条记录，包括了 57,000 名 RATP 员工的详细信息，涵盖高级管理人员和网络安全团队。这些数据包括全名、电子邮件地址、RATP 员工帐户的登录信息和 MD5 哈希密码。

https://www.infosecurity-magazine.com/news/french-transport-giant-exposes/?&web_view=true

4、美国食品进口商亚特兰大承认勒索软件攻击

2021 年 12 月 9 日，据外媒报道，北美食品进口商亚特兰大承认，由于勒索软件攻击，它遭受了涉及员工个人信息的数据泄露。据调查结果显示，与亚特兰大现任和前任雇员以及某些访客有关的某些信息因该事件而被访问和获取。迄今为止，没有迹象表明所涉及的信息被滥用。

https://portswigger.net/daily-swig/us-food-importer-atalanta-admits-ransomware-attack?&web_view=true

5、南澳大利亚州 8 万名政府雇员信息恐被泄露

2021 年 12 月 10 日报道，南澳大利亚政府透露，在上月一家外部薪资软件供应商 Frontier Software 的系统遭到勒索软件攻击后，属于其的 8 万名员工个人敏感信息恐被泄露。

根据该公司对该事件的声明，威胁并未通过其产品转移到客户端系统，数据泄露仅影响特定的分段环境。已泄露的数据包括以下内容：姓名、出生日期、家庭地址、税号、银行账户明细、薪水等。

<https://www.bleepingcomputer.com/news/security/data-breach-impacts-80-000-south-australian-govt-employees/>

6、沃尔沃承认数据泄露，部分研发数据被盗

2021 年 12 月 11 日消息，当地时间 12 月 10 日周五，沃尔沃汽车称已对因遭受到网络攻击而导致公司运营的研发数据被盗一事展开调查。

沃尔沃表示：“迄今为止的调查证实，公司文件存储库之一已被第三方非法访问，在入侵期间公司的有限数量的研发财产被盗。”该公司警告称，此次黑客攻击“可能对公司的运营产生影响”，导致其在斯德哥尔摩的股价下跌 3.5%。

https://mp.weixin.qq.com/s/1Xqmh9_iRtyxXIVIQ_DiZg