全球数据安全观察

总第 77 期 2022 年第 05 期

（2022.02.07-2022.02.13）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、银保监会发布 2022 年 2 号文：加强数据安全和隐私保护

近日，中国银保监会办公厅印发《关于银行业保险业数字化转型的指导意见》（银保监办发〔2022〕2 号）。《指导意见》共七个部分，三十条，包括总体要求、战略规划与组织流程建设、业务经营管理数字化、数据能力建设、科技能力建设、风险防范、组织保障和监督管理等。

《指导意见》指出，加强**数据安全和隐私保护**。完善数据安全管理体系，建立**数据分级分类管理制度**，明确保护策略，落实技术和管理措施。强化对数据的安全访问控制，建立**数据全生命周期的安全闭环管理机制**。加强第三方数据合作安全评估，交由第三方处理数据的，应依据"最小、必要"原则进行脱敏处理（国家法律法规及行业主管部门、监管部门另有规定的除外）。关注外部数据源合规风险，明确数据权属关系，加强数据安全技术保护。加强对外发布信息安全管理。

https://mp.weixin.qq.com/s/OctOzxveZ66v8l8jPw7vLw

2、国家发改委牵头发布《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》

近期，国家发展改革委牵头，会同商务部、广东省、深圳市等研究制定《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》，《意见》重点提及放宽数据要素交易和跨境数据业务等相关领域市场准入，涵盖数据要素交易、数据资源产权、公共数据开放、数据安全等内容。

《意见》具体包括：一、在严控质量、具备可行业务模式前提下，审慎研究设立数据要素交易场所；二、鼓励深圳开展地方性政策研究探索，建立数据资源产权、交易流通、跨境传输、信息权益和**数据安全保护**等基础制度和技术标准；三、鼓励深圳市探索立法，明确处理者义务或主体参与权利，依法处理个人信息，保护数据处理者合法利益；四、加快推动公共数据开放，编制公共数据共享目录；五、开展数据跨境传输（出境）安全管理试点，建立**数据安全保护能力评估认证**等数据安全管理机制。六、利用区块链、量子信息等先进技术实现数据可交易、流向可追溯、安全有保障，探索建立数据要素交易领域相关标准体系；七、探索建设离岸数据交易平台。

https://mp.weixin.qq.com/s/MTPpSuMXKCsp7RafYLnnmg

3、工信部发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》二次征求意见

2 月 10 日，工业和信息化部再次发布《工业和信息化领域数据安全管理办法（试行）》，根据此前《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）收到的公开意见，工业和信息化部进行了修改完善，再次面向社会征求意见。相较于 2021 年 9 月 30 日发布的《征求意见稿》，此次《公开征求意见稿》共计八章四十一条，主要做了如下调整：目的依据中添加了《个人信息保护法》和《国家安全法》。适用数据范围扩大至工业数据、电信数据和无线电数据。对一般数据、重要数据和核心数据的定义做了调整，对备案申请时间等具体数字做出明确规定。补充了主体责任，在数据全生命周期管理方面，围绕数据出境和数据跨主体处理进行了条款补充。

https://mp.weixin.qq.com/s/k4wWhO147p6QCN7B1wFlgQ

4、上海市发布全市首份《企业数据合规指引》

近日，上海市首份《企业数据合规指引》（下称《指引》）正式出台。据悉，《指引》由上海市杨浦区检察院联合市信息服务业行业协会、市数据合规与安全产业发展专家工作组、区工商业联合会制定发布。

《指引》主要对企业的数据合规管理架构与风险识别处理规范作出了规定，包括**数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障**等内容，督促企业对数据进行合规管理，有效惩治预防数据违法犯罪。此外，还特别对数据刑事风险进行了提示。

https://mp.weixin.qq.com/s/fNuD9hgqPZHC_FYkEn0cKQ

5、浙江省发布《浙江省公共数据条例》

1 月 21 日，浙江省十三届人大六次会议审议通过《浙江省公共数据条例》，将于 3 月 1 日起正式施行。《条例》是全国首部以公共数据为主题的地方性法规，也是保障浙江省数字化改革的基础性法规。

《条例》聚焦破解部门间信息孤岛、提升数据质量、赋能基层、保障安全等共性难题，推动浙江打造全球数字变革高地。《条例》明确了公共数据范围、平台建设规范、收集归集规则，推动公共数据有序开放，规定开放属性确定机制、明确开放范围和重点、分类开放，并明确受限开放条件和要求，助力省域治理高效协同激活数据要素市场。

https://mp.weixin.qq.com/s/8UfzFrRFWsDN6Rxsq6w1rA

6、广东省发布《广东省公共数据安全管理办法（征求意见稿）》

2 月 7 日，广东省政务服务数据管理局发布《广东省公共数据安全管理办法（征求意见稿）》，公开征求意见。该管理办法旨在加强广东省数字政府公共数据安全管理，规范公共数据处理活动，促进数据资源有序开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。该《征求意见稿》包含总则、基础制度体系、全生命周期数据安全管理、数据安全支撑保障、监督与法律责任、附则共六章。

https://mp.weixin.qq.com/s/JKpu6cXMyrPxJU2rPHXwCg

技术、产品与市场

1、Gartner 报告：2022 年法律、合规和隐私领导者的首要任务

近日，Gartner 发布《2022 年法律、合规和隐私领导者的首要任务》，通过对**高级律师、法律运营，合规和隐私高管**面临的常见挑战进行民意调查，了解法律和合规领导者在 2022 年重点关注方向和首要任务。

根据 2022 年 Gartner 法律与合规高管优先事项调查，法律、合规和隐私领导者在 2022 年需要解决的五大挑战依次为：**被日常需求限制的战略效益；第三方风险管理的复杂性超越了治理和技术的实施速度；合规计划没有跟上利益相关者的期望（例如 ESG、DEI）；隐私政策和程序没有与不断变化的隐私法规保持同步；跟踪监管变化的工具杂乱无章且效率低下。**

https://mp.weixin.qq.com/s/A0yGkYgCdOJhuiPNOgd6Hw

2、国内首个！隐私计算类金融应用产品纳入国推认证

2 月 9 日，市场监管总局联合人民银行发布《金融科技产品认证目录（第二批）》，**多方安全计算金融应用产品被重磅纳入**，引起行业热议！这是隐私计算领域首个被纳入国推认证的产品类型。

根据认证规则，多方安全计算金融应用产品认证依据被指定为 2020 年中国人民银行正式发布的《多方安全计算金融应用技术规范》(JR/T0196-2020)金融行业标准、2021 年中国支付清算协会发布的《多方安全计算金融应用评估规范》(T/PCAC0009-2021)标准。此外，认证规则规定了金融科技产品认证的基本认证模式为：**型式试验+获证后监督。**

https://mp.weixin.qq.com/s/PI3-eLGSLEX35RObDIFTsw

3、2021 年 80%的关键基础设施遭受勒索软件攻击

Claroty 最新发布的《2021 年全球工控安全台式报告》显示，2021 年 80%的关键基础设施组织遭受了勒索软件攻击，同样比例的组织报告称其安全预算自 2020 年以来有所增加。

报告还发现，不断加速的数字化转型和熟练网络安全人员的短缺，是导致对关键基础设施的多次高调攻击的主要原因。数字化转型、远程工作和安全人才短缺持续存在：自新冠疫情大流行以来，数字化转型继续加速，73%的组织计划继续以某种身份进行远程/混合工作。近 90%的受访者希望招聘更多的 OT 安全人员，但 54%的受访者表示很难找到合格的人才。

https://mp.weixin.qq.com/s/0_djVGZdmYi89Y-zadaMew

4、《数据安全风险分析及应对策略研究（2022 年）》发布

近日，中国信息通信研究院与奇安信联合撰写的**《数据安全风险分析及应对策略研究（2022 年）》**正式发布。报告从理论与实践层面对当前企业面临的内外部数据安全风险进行分析与研究，完成了以下几方面的探索：**一是梳理了当前数据安全面临的突出问题；二是提出了数据安全体系建设的行动思路和关键举措；三是提出了数据安全建设发展建议。**

报告认为，当前数据安全面临的几个突出问题：**一是 APP 对用户信息的过度采集；二是账号弱口令的使用普遍；三是数据权限分配、使用的不透明；四是 API 接口面临严重攻击威胁；五是数据安全的持续状态难以保持。**

报告指出解决数据安全突出问题，首先要明确体系化建设的行动思路，包括明确数据安全总体战略，建立数据安全管理机构，落实安全策略精准管控，持续保障数据安全运营。并在此基础上，提出了**个人信息保护、特权账号管理、动态授权管控、API 安全防护、全局化数据安全运营**五大关键举措。

https://mp.weixin.qq.com/s/--7wOMXPq3Hn0f7jVn0_eQ

5、网络安全技术发展趋势

2021 年，网络空间安全技术不断更新发展，呈现出创新

活跃的态势。以零信任、人工智能、量子技术和太空技术等为代表的新兴网络安全技术在网络安全领域的发展前景受到世人重点关注。

（1）数字时代下，基于边界构建的传统安全防护正被零信任所取代，零信任逐渐成为数字时代主流的网络安全架构。

（2）人工智能赋能网络攻击催生出更多精准化、智能化、自主化的网络安全威胁。

（3）量子技术为网络空间安全技术的发展注入新动力，后量子密码是缓解量子威胁的重要手段。

（4）“弹性太空”引领太空技术发展方向，具体体现为：分散式、扩散式、多样化部署。

https://mp.weixin.qq.com/s/0RHPknhIXm13iCPcOQUpJA

业界观点

1、解读上海市首份《企业数据合规指引》

春节前夕，上海市首份《企业数据合规指引》（以下简称《指引》）由上海市杨浦区人民检察院联合市信息服务业行业协会、市数据合规与安全产业发展专家工作组、杨浦区工商业联合会制定发布。

《指引》根据《个人信息保护法》、《网络安全法》、《数据安全法》等法律法规制定，旨在引导企业加强数据合规管理，保护个人信息，保障数据安全，规范数据处理活动。

《指引》共有三十八条，按照合规架构与风险识别处理的逻辑划分为六章，从数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障等方面引导企业加强数据合规管理。

https://mp.weixin.qq.com/s/TRLj-yD3kLZ8RpuJRl7K6Q

2、关于《银行业保险业数字化转型的指导意见》的解读

近日，银保监会下发了《银行业保险业数字化转型指导意见》，以全面推进银行保险业数字化转型，推动金融高质量发展，更好地服务实体经济和满足人民群众需要。

《指导意见》明确了银行保险业的数字化转型的工作目标，即“到 2025 年，银行业保险业数字化转型取得明显成

效”，并较为清晰和全面地对金融机构数字化转型工作给出了指引，在明确了数字化转型工作框架的同时，也要求银行保险业机构要高度重视数字化转型工作，保障人力和财务资源投入，未来也会将数字化转型情况纳入银行保险机构信息科技监管评级。

《指导意见》还强调，银行保险机构要加强顶层设计和统筹规划，科学制定数字化转型战略，统筹推进工作，并从健全数据治理体系、增强数据管理能力、加强数据质量控制、提高数据应用能力四个方面要求银行全面提升数据治理与应用能力。

https://mp.weixin.qq.com/s/pn9eFV0kbWTp-3PVlnfiSA

3、《浙江省公共数据条例》解读：破解共性难题 激发要素价值

近日，浙江省十三届人大六次会议审议通过《浙江省公共数据条例》，3 月 1 日起《条例》将正式施行。《条例》里的公共数据，指的是本省国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、供气、公共交通等公共服务运营单位，在依法履行职责或者提供公共服务过程中收集、产生的数据。

作为数字化改革的重大理论和制度成果，《条例》聚焦

破解部门间信息孤岛、提升数据质量、赋能基层、保障安全等共性难题，推动浙江打造全球数字变革高地。

截至 2021 年底，浙江已归集了 838.5 亿余条公共数据，总量在全国居前。在确保数据安全的前提下，管好、用好如此庞大，并且还在不断增长的数据资源，《条例》给出了具有全国引领性的浙江解法。

https://mp.weixin.qq.com/s/PA5HkFJJFMJ9M9rxhEnHaw

4、解读《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》

近日，国家发改委、商务部联合发布《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》（以下简称《意见》），在科技、金融、医疗、教育文化、交通等六大领域推出 24 条放宽市场准入具体措施，深圳再次迎来加快建设中国特色社会主义先行示范区的实施放宽市场准入若干特别措施重磅支持。

《意见》作为支持深圳建设中国社会主义先行示范区的重要基础制度安排，将进一步加快推进深圳综合改革试点，持续推动放宽市场准入，打造更高层次的科技创新机制、更加全面完善的民生服务、更具国际化的金融环境。

https://mp.weixin.qq.com/s/au5lb5aGNfb-vX6z2Bp2GQ

5、委员建议对临床研究数据外流滥用情况全面摸底，国家卫健委回应

临床研究受试者的个人信息数据保护问题近年受到关注，近日，有全国政协委员建议 “国家卫健委、国家药监局会同相关部门对现有和历史临床研究数据外传、外流和滥用的基本情况进行全面深入摸底，为相关领域针对性的立法立规打下更好基础”。

国家卫健委在公布的答复函中介绍，该委拟在部分地区试点实施《医疗卫生机构开展研究者发起的临床研究管理办法（试点稿）》，实施过程中，计划对现有和历史临床研究数据使用的基本情况进行调研摸底，掌握有关情况。

国家卫健委称，将加大临床受试者个人信息数据保护工作力度。根据反馈意见修订完善《涉及人的生命科学和医学研究伦理审查办法（征求意见稿)》，推动文件尽快印发，落实个人信息数据保护在伦理审查和监管层面的要求。积极推进《医疗卫生机构开展研究者发起的临床研究管理办法（试点稿）》的试点实施，加强相关培训，切实做好受试者及研究参与者个人信息的隐私保护工作。

https://www.thepaper.cn/newsDetail_forward_16672028

数据安全事件

1、克罗地亚电话运营商数据泄露影响 20 万名客户

2022 年 2 月 12 日，克罗地亚电话运营商“A1 Hrvatska”披露了一起数据泄露事件，约 10% 的客户（大约 20 万人）的个人信息遭到泄露。威胁者可以访问客户的敏感个人信息，包括姓名、个人身份证号、实际地址和电话号码。威胁者没有访问在线账户，财务信息也没有暴露。目前，电话运营商没有透露有关安全漏洞的详细信息。

https://securityaffairs.co/wordpress/127919/data-breach/a1-hrvatska-data-breach.html

2、英国文化协会曝光了 144,000 份包含学生详细信息的文件

2022 年 2 月 1 日，属于英国文化协会学生的个人信息通过不安全的存储库在线公开，其中包含超过 144,000 个文件（xml、json 和 xls/xlsx）。对文件的分析显示，其中包含英国文化协会学生的个人信息和登录凭据。目前尚不清楚数据在没有保护的情况下在线暴露了多长时间。

https://securityaffairs.co/wordpress/127499/breaking-news/british-council-data-leak.html

3、Maze、Egregor 和 Sekhmet 勒索软件的主解密密钥在线泄露

2022 年 2 月 9 日，据报道，Maze 、Egregor 和 Sekhmet 勒索软件系列的主解密密钥由所谓的恶意软件开发者在 BleepingComputer 论坛上发布。这些密钥由一个名为“Topleak”的用户共享，该用户声称自己是所有三个操作的开发者。Topleak 用户指出，这是一次有计划的泄密，与执法部门最近的逮捕和撤职无关。被指控的勒索软件开发商补充说，勒索软件团伙将永远不会在勒索软件操作中返回，并且曾经制作的工具的源代码已被清除。

https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html

4、财富 500 强服务提供商表示，勒索软件攻击导致超过 50 万个 SSN 泄露

2022 年 2 月 5 日，为数十家财富 500 强公司提供商业服务的组织 Morley Companies 表示去年遭到勒索软件攻击，导致超过 500,000 人的敏感信息泄露。勒索软件攻击始于 8 月 1 日，导致他们的数据“不可用”。 此次攻击影响了“现任员工、前员工和各种客户”的信息。泄露的信息包括姓名、地址、社会安全号码、出生日期、客户识别号码、医疗诊断和

治疗信息以及健康保险信息。

https://www.zdnet.com/article/fortune-500-service-provider-says-ransomware-attack-led-to-leak-of-more-than-500k-ssns-more/

5、6000 多名彪马员工的数据在 12 月 Kronos 勒索软件攻击中被盗

2022 年 2 月 8 日报道，属于 6632 名彪马员工的数据在 2021 年 12 月袭击 Ultimate Kronos Group (UKG) 的一次勒索软件攻击中被盗。攻击者攻击了用于托管多个云应用程序的 Kronos 私有云服务，并在对基础设施加密之前就窃取了数据，可能暴露的数据包括姓名、社会安全号码和其他个人信息。

https://securityaffairs.co/wordpress/127791/cyber-crime/puma-kronos-ransomware-attack.html

6、Conti 勒索软件加密了爱尔兰 HSE80%的 IT 系统

2022 年 2 月 4 日，据报道，美国卫生与公众服务部 (HHS) 发布的威胁简报显示，去年 Conti 勒索软件攻击导致爱尔兰卫生服务机构 HSE 80%的 IT 系统被加密，导致整个爱尔兰的医疗保健服务严重中断，并在大约 700 GB 的数据（包括

受保护的健康信息）从爱尔兰卫生服务机构的网络被盗并发送给攻击者之后，暴露了在攻击前接种 COVID-19 疫苗的数千名爱尔兰人的信息。

https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/

7、渥太华卡车司机抗议活动捐赠网站现安全漏洞：捐赠者数据遭曝光

2022 年 2 月 9 日报道，目前在渥太华抗议加拿大国家疫苗规定的卡车司机使用的捐赠网站已经修复了一个安全漏洞，该漏洞暴露了捐赠者的护照和驾驶执照。

在安全领域工作的一位工作人员发现了一个暴露的亚马逊托管的 S3 储存库，其中包含超过 50GB 的文件--里边有在捐赠过程中收集的护照和驾驶执照。目前还不知道这个储存库到底被暴露了多久，但一位不愿透露姓名的安全研究员留下的一个文本文件显示日期为 2018 年 9 月，并警告称这个储存库“没有正确配置”、可能会产生“危险的安全影响”。

https://www.cnbeta.com/articles/tech/1234625.htm

8、Equifax 信息泄露案落幕：七亿赔款，索赔期限延四年

2022 年 2 月 9 日消息，近日，美国联邦贸易委员会

（Federal Trade Commission，简称 FTC）宣布，信用评分报告公司 Equifax 就 2017 年信息泄露事件与 FTC、消费者金融保护局以及美国 50 个州及地区达成最终和解。Equifax 将客户的索赔截止日期自此前的 2020 年 1 月 22 日延长至 2024 年 1 月 22 日，并免费提供 Experian 四年的信用监控服务。

据报道，2017 年 9 月，作为美国三大信用评分报告公司之一的 Equifax 公布了一起严重的信息泄露事件。黑客于当年 5 月到 7 月间利用网络安全漏洞入侵 Equifax 系统，导致 1.47 亿人信息泄露，其中包括姓名、地址、出生日期、身份证号以及护照、驾照、信用卡信息等，美国、英国、加拿大等多国公民受到影响。

https://www.secrss.com/articles/39075

9、PayBito 加密货币交易所遭受网络攻击，大量数据信息被盗

Security Affairs 网站披露，LockBit 勒索软件团伙声称从 PayBito 加密货币交易所盗取了大量客户数据。

PayBito 由全球区块链和 IT 服务公司 HashCash 运营的加密货币交易所，主要的加密货币包括比特币、以太坊、HCX、莱特币等。目前，部分被盗数据公布在该团伙的 Tor 泄漏网站上。此次网络攻击中，该勒索软件团伙成功窃取一

个数据库，其中包含来自全球约 10 万多名客户的个人数据信息。

除此之外，该团伙还盗取了部分电子邮件数据和密码哈希值，其中一些数据可以轻易被解密。糟糕的是，该团伙还成功窃取了管理员的个人数据，声称如果收不到赎金，将在 2022 年 2 月 21 日公布被盗数据。

https://www.freebuf.com/news/321341.html

10、法国监管机构称谷歌分析存在数据隐私风险

谷歌分析（Google Analytics）是由 Alphabet 旗下谷歌开发的全球使用最广泛的网络分析服务，但目前，这项服务在欧洲面临监管考验。

法国监管机构 CNIL 于 2 月 10 日表示，根据欧盟《通用数据保护条例》（GDPR），在针对一家法国公司网站的调查中发现，这家美国科技巨头在数据传输时没有采取足够的措施保障数据隐私权，有可能导致美国情报机构访问法国网站用户的数据。

https://www.freebuf.com/news/321703.html