全球数据安全观察

总第 109 期 2022 年第 37 期

(2022.10.10-2022.10.16)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、国务院点赞杭州试点推行的首席数据官制度

近日，国务院推进政府职能转变和“放管服”改革协调小组办公室下发政府职能转变和“放管服”改革简报(第240期)，点赞杭州试点推行的首席数据官制度。

简报指出，浙江省杭州市认真贯彻落实党中央、国务院关于深化“放管服”改革的决策部署，积极适应数字化改革需要，试点推行首席数据官制度，在全市115家市直部门、市属国有企业设立首席数据官、数字专员，为数字政府建设整体推进提供了重要人才保障。

https://mp.weixin.qq.com/s/F4WNL-K48QEwxLakH109Yg

2、《上海市制造业数字化转型实施方案》印发

为推进《推进上海经济数字化转型 赋能高质量发展行动方案(2021-2023年)》以及积极应对新冠疫情带来的新挑战、新机遇，上海市于10月8日印发了《上海市制造业数字化转型实施方案》。

其中，在“完善安全制度体系建设”部分强调围绕工业互联网安全监督检查、风险评估、数据保护、应急处置等方面建立安全管理制度和工作机制，推进工业互联网企业网络安

全分类分级管理制度建设，支持专业机构、企业积极参与工业互联网设备、网络、平台、数据等重点领域安全标准的研究制定，指导督促工业互联网企业提升网络安全防护水平，制定本市重点联网工业企业清单和重要数据保护目录。

http://dt.sheitc.sh.gov.cn/szzc/2129.jhtml

3、民航局《关于民航大数据建设发展的指导意见》

10 月 9 日，为深入贯彻落实党中央、国务院关于数字中国建设的重大决策部署，加快推进智慧民航建设，加强民航大数据建设发展顶层设计，民航局组织印发了 《关于民航大数据建设发展的指导意见》。

《意见》明确要求按照“谁管业务、谁管业务数据、谁管数据安全”的原则，业务主管部门落实对业务数据的管理协调职责，系统推进行业大数据战略实施、标准制定、数据资源共享、大数据开发应用等工作。并在数据安全体系建设要求部分强调要强化安全管理责任和提升安全保障能力。

http://www.gov.cn/zhengce/zhengceku/2022-10/14/content_5718281.htm

4、欧盟和日本拟将“跨境数据流动规则”纳入经济伙伴关系协定

10 月 7 日，欧盟和日本已同意通过就将数据流规则纳入我们的经济伙伴关系协议（EPA）进行谈判，将这种关系提升到一个新的水平，正式讨论将于 2022 年 10 月 24 日在布鲁塞尔开始。

欧盟指出其目标是通过禁止不合理的数据本地化要求来确保跨境数据流动，同时保持欧盟在个人和非个人数据保护和网络安全领域的监管自主权。

https://policy.trade.ec.europa.eu/news/eu-and-japan-start-negotiations-include-rules-cross-border-data-flows-their-economic-partnership-2022-10-07_en

5、尼日利亚《2022 年数据保护法》草案发布

近日，尼日利亚发布了《2022 年数据保护法案》草案，概述了个人数据保护的法律框架。该法案将建立尼日利亚数据保护委员会来监管个人数据处理，并概述了处理个人信息的原则--包括进行数据保护影响评估和任命数据保护官员--违规通知和跨境数据传输限制，以及包括调查和民事救济措施在内的执法能力。

https://mp.weixin.qq.com/s/P12vobca3UsN7gDDeschLA

技术、产品与市场

1、谷歌正式推出“密钥登录”，逐步取代传统密码登录

10 月 12 日消息，谷歌宣布在 Android 和 Chrome 中正式推行密钥登录 “PassKey”，以逐步替代长期使用的密码登录 “PassWord”。

推出的密钥登录可以认为是 “生物密码” 和 “授权登录” 的结合。用户可以在 Android 手机上创建一个基于公钥加密的密钥凭据，创建密钥的时候需要对本人进行生物特征识别，比如 “指纹” 或者 “面部识别” 等。

创建完毕后，这个密钥凭据可用于解锁所有在线帐户 —— 既可以解锁 Android 手机上的帐户，也可以解锁附近所有设备的帐户。这个 FIDO 密匙登录功能由微软 / 苹果 / 谷歌联合出品，属于行业标准。因此它是跨平台的，包括 Windows、macOS 和 iOS 以及 ChromeOS。

https://hackernews.cc/archives/41912

2、研究表明指尖的热量可用于破解密码

近日，苏格兰的网络安全专家已经开发了一个系统，利用热成像和人工智能（AI）来即时破解密码（通过 CTV 新闻）。该系统被称为 ThermoSecure，通过分析一个人在电脑

键盘或移动设备上输入密码时指尖留下的热量痕迹来工作。由于热感应图像上较亮的区域显示最近被触摸过的区域，这使得猜测所用字母、数字和符号的顺序成为可能。

格拉斯哥大学副教授穆罕默德-卡米斯博士和他的团队使用机器学习和 1500 张最近使用过的键盘的热图像来训练一个人工智能模型，以读取热特征并研究可能的密码组合。

该研究发现，较长的密码更安全，因为 ThermoSecure 在 20 秒内破解了 67%的 16 个字符的密码。该系统对较短的密码效果更好，对于 12、8 和 6 个字符的密码，其成功率分别提高到 82%、93%和 100%。

用户的打字风格也很重要，因为在键盘上停留时间较长的”猎取式”键盘用户比打字速度快的”触摸式”键盘用户产生的热信号更持久。在该研究的测试中，ThermoSecure 猜出第一组密码的成功率为 92%，而后者的成功率只有 80%。

https://hackernews.cc/archives/41873

3、IAPP《2022 年隐私技术供应商报告》：两大类别入选 364 家厂商

近日，IAPP 发布了第六次年度“隐私技术供应商报告”。之前的报告中逐年审查了隐私技术市场的增长和趋势。本次报告中 IAPP 列出了 364 家隐私技术厂商。

在过去六年中，隐私技术已成长为一个关键行业，为不断发展的全球监管体系提供隐私保护解决方案，使得我们所有人都更加重视隐私保护。值得注意的是，虽然隐私技术行业呈指数级爆炸式增长，但它正处于根本性巨变的边缘，时刻面临着业务整合的契机和针对特定客户解决方案的专业化。对于目前市场上存在的隐私技术产品，IAPP 将其主要分为“隐私项目管理”和“企业隐私管理”两部分。

https://mp.weixin.qq.com/s/7Q8jLXjuMxWumeGnqyAidw

4、八种让人“意想不到”的数据泄露方式

（1）镜片反射泄露视频文本：Zoom 和 Microsoft Teams 等视频会议平台已成为远程/混合工作模式的主要手段。然而新的研究发现，戴眼镜的视频参会者可能会因为眼镜镜片反射而意外泄露信息。

（2）职业资讯触发钓鱼攻击：攻击者会在 LinkedIn 等专业社交网站上搜索新职位，在数据中介网站上查找员工的电话号码，然后发送网络钓鱼信息。

（3）社交媒体泄密：社交应用软件意外泄露数据是切实存在的一大威胁。

（4）错误使用数据库：对数据摄取脚本而言，IP 地址或 URL 的简单拼写错误会导致使用错误的数据库。

（5）证书透明度日志泄露敏感数据：利用此类日志证书中的各种详细信息，来追踪公司并详细列出有效的用户名或电子邮件地址，甚至攻击安全控制措施较少的应用系统，以便接管系统和横向移动。

（6）看似无害的 USB 设备：恶意设计的硬件（设备上预装恶意软件）、蠕虫感染以及硬件供应链感染。

（7）报废设备泄露隐私数据：旧的办公室打印机在丢弃回收时，没有事先擦除 Wi-Fi 密码等隐私数据。

（8）电子邮件泄密：员工出于疏忽发送的非恶意电子邮件经常也会导致数据泄露，例如员工的社会安全号码（SSN）等。

https://mp.weixin.qq.com/s/F3Odx9X7MU_ArV6vWwGKwg

5、上海数据交易所正式上架中国移动 136 个数据产品

近日，在上海数据交易所一站通金融数据交易板块下，中国移动上海公司完成“中移梧桐风控”系列 136 个数据产品挂牌，推进实现上海数交所金融板块银行领域数据全品类覆盖。

据中国移动上海公司相关负责人介绍，该系列数据产品涵盖基础信息核验、定制模型分、客户关系修复和支付卫士四大类别，本次挂牌的 136 个数据产品包括**基础信息核验类**

和**模型评分**两类。基础信息核验产品从通讯数据出发，生成对于风险有区分度的多维度标签数据，如三要素验证、通话时长、欠费停机次数等；模型评分产品基于中国移动自有数据沉淀通用模型，可应用信贷风控场景，识别团伙、博彩、洗钱、流量造假等行为。

https://mp.weixin.qq.com/s/Qn2EaWHx2YzMeGoJKT6yBQ

业界观点

1、360 周鸿祎：下一片蓝海，是产业数字化

中国前面 20 年是互联网的上半场，是腾讯、阿里、百度、360 等公司用数字化的方式解决了老百姓消费互联网生活方式的数字化，因为巨大的人口红利，所以有很多场景的创新，有很多应用体验的创新，改变了中国互联网。

但下半场，未来 20 年周鸿祎认为主角应该是各级政府、各种传统企业，特别是制造企业，中国的传统产业今天如何用云计算、大数据、人工智能、物联网、数字化安全，把业务再造一遍，就意味着每个行业都值得重做一遍（这就是蓝海）。

360 现在也在转型，周鸿祎称之为“上山下海，扶助中小微”。“上山”就是登科技高峰，为国家解决一些“卡脖子”问题。“下海”就是下数字化蓝海，因为整个中国数字化战略里，最大的机会就是产业数字化。

https://mp.weixin.qq.com/s/PcSxvGOw73d9avd4GA-Dhg

2、周道许：加强金融数据安全治理，助推金融业隐私保护生态构建

10 月 10 日，由上海华瑞银行与中国人民大学国际货币

研究所、金融科技研究所联合主办的“ 华瑞金融科技系列沙龙”第 3 期线上研讨会成功举办。 IMI 学术委员、清华大学金融科技研究院金融安全研究中心主任周道许参与研讨。

他认为，要找到数据“安全”与“运用”之间的平衡点，需要重视三个方面:

一、数据确权和隐私保护是金融数据安全的关键，两者相辅相成。

二、金融数据的跨境流动需求将会不断增加，有两个方面的问题需要解决。一是需要进一步细化金融数据跨境流动的相关法律法规建设工作；二是金融数据跨境流动安全面临双重监管，需要对相关监管流程进行梳理。

三、要进一步细化金融数据安全管理分类分级、加强金融数据全生命周期安全的监管。

https://www.sohu.com/a/592474976_674079

3、何晶晶：高校数据安全需做好全生命周期数据合规管理

“数据安全不代表数据合规了，这其实是两个维度的事情。”在 9 月 27 日举办的武汉高校信息化建设与网络安全研讨会上，中国社会科学院国际法研究所副研究员何晶晶强调。

在她看来，数据安全建设是确保网络不被攻击、数据不被泄露，而数据合规是需要满足法律法规要求。整体来说，

数据合规治理需要“合规”与“安全”并重。

何晶晶指出，高校的数据不仅体量大，而且敏感性较高。首先，高校有着大量学生、教职工的个人信息，包括身份证、家庭住址等，这些数据都是整理归纳得非常好的。另外，高校还有着大量的实验数据和宝贵的科研成果，涉及到一些重要论文、研究项目等等。

何晶晶从个人信息保护的角度出发，指出数据全生命周期各阶段应达到的安全要求，并针对高校当前的数据安全现状，建议可以从以下三方面入手，提高高校对数据合规的重视程度：

首先，**建立并完善高校数据合规监管体系**。教育系统应制定各项数据合规标准规范体系，进行等级保护测评及风险评估，持续开展数据合规性检查和指导工作，构建数据合规及监管管理体系；

其次，**建立全流程的高校数据安全运营体系**。通过测绘高校在互联网中数据资产的分布，建设覆盖全方位的数据安全态势感知体系，构筑全天候的威胁攻击防御堡垒，并组建数据安全应急中心，全面提升高校的数据安全防护能力；

最后，**建立全生命周期的高校数据合规管理体系**。从数据的收集、存储、使用、访问、交换、销毁等流程对高校数据进行管理，对流程中的关键环节的操作规范、分类分级管

理、部门职责分工、应急安全检查机制、责任追究等进行全方位管控，重点关注师生个人信息保护。

https://software.it168.com/a2022/1010/6767/000006767558.shtml

4、张小亮：数字经济时代 打造数字安全新高地

数字经济的核心在于信息化，其安全与发展的相互依赖性更加突出。从国家层面，近几年陆续颁布《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》、《网络安全审查办法》、《数据出境安全评估办法》等法律法规，规范了数据经济高速发展背景下的安全要求。可以看出，国家对面向未来的数字安全已经在顶层设计上做了全方位的布局。安全是一项体系化的工作，包含以下几个层面，一是要有顶层上位法律的指引，二是配套标准政策的推广，三是要有产业侧的支撑，四是要将整体的安全能力落地。

随着云计算、大数据等技术的普及和应用场景逐渐成熟，面向行业的应用都部署在云平台上，各类应用生成的数据量正日益快速增长，数据结构和类型越发复杂，这使得控制数据访问权限、防止数据滥用和数据泄露变得更加困难。在数据采集、数据存储、数据传输、数据共享和应用等数据生命

周期的各个环节，都存在着数据泄露风险。从近期爆发的数据安全事件来看，我们既需要让数据产生价值，又要保障数据在全生命周期的安全，这是在数字化应用场景中必须要解决的问题。

针对政企数字化转型面临的安全需求，应该从多个维度去布局，构建科学合理的数字化安全能力体系。政企要形成自己的数据安全治理框架，包括数据安全组织架构建设、数据安全管理体系建设、数据安全技术体系建设及数据安全运营体系建设。从组织架构角度，要明确单位内部的职能架构，定岗定员。从管理体系角度，要从战略、制度、规范及操作文件等层次做好制度规划和建设。从技术体系角度，要围绕数据全生命周期属性，从识别、防护、检测、响应和集中管控等方面开展工具和平台建设。最后，从安全运营角度，制定安全规划，落实安全防护策略，开展安全风险监测与评估，最后进行持续优化和迭代。

https://mp.weixin.qq.com/s/P1u3MQEIvt0ScnNjh_k1eg

5、中国信通院姜春宇："数实融合"，我国大数据产业迈向高质量发展

我国在大数据领域布局早、布局深，**主要分为三个阶段。一是酝酿阶段（2014 年-2015 年）：**2014 年大数据首次写入

政府工作报告， 2015 年国务院发布大数据发展行动纲，明确“数据是国家基础性战略资源”。**二是落地阶段（2016 年-2020 年）：**大数据“十三五”规划发布实施，提出五大发展目标、七大重点任务和八项重点工程，经过五年发展，大数据产业快速向前迈进。**深化阶段（2021 年-至今）：**“十四五”规划全面布局大数据发展，提出五大目标、六大任务和六项行动，产业将步入集成创新、快速发展、深度应用、结构优化新阶段。

对于大数据产业未来发展的方向：**一是数据技术不断推陈出新，创新热点正在从效率优先向安全流通转变。**据不完全统计，目前国内以隐私计算为代表的数据流通类产品已达 120 多款、相关企业超过 100 家，比去年翻了一番，发展势头迅猛。

二是数智化转型进入新阶段，数据应用的系统化、精细化、敏捷化成为关键特征。构建数据驱动的智能化决策能力，是数字化转型的核心。数据应用急需从目前的单点、粗放、低效的传统模式，向系统化、精细化和敏捷化的 DataOps 模式转型，组织架构、业务流程和技术体系也要加速变革。

三是大数据安全规则体系日渐清晰，数据安全合规进入细化实施新阶段。随着《数据安全法》和《个人信息保护法》的颁布实施，数据安全顶层框架和责任体系基本确立。长期

来看，企业需要从组织架构、制度流程、技术工具、人员能力等四个维度出发，构建完善的数据安全治理体系，来满足外部监管要求和内部数据安全需求。

http://www.cww.net.cn/article?id=084BBBF00E874A85B5C5ECB6BFB5918E

数据安全事件

1、上海网信办：某科技公司违反《数据安全法》被行政处罚

近期，上海网信办发现，某科技公司在处理政务类数据时违规操作，且未采取相应的技术措施和其他必要措施保障数据安全，导致数据存在泄露风险。上海网信办依据《中华人民共和国数据安全法》对该公司责令改正，给予警告，并处以人民币五万元罚款的行政处罚。上海网信办相关负责人表示，数据安全关乎人民群众切身利益，关乎国家安全和社会稳定，上海网信办将针对数据安全保护义务履行不力，造成重要数据泄露风险的违法违规行为加强监督检查和执法，进一步营造安全稳定的网络环境。

https://mp.weixin.qq.com/s/kjgOPNDGhH2EFfZ37vzryg

2、Shein 母公司将因数据泄露向纽约州支付 190 万美元

10 月 13 日，据 The Verge 报道，快时尚品牌 Shein 和 Romwe 背后的公司将向纽约州支付 190 万美元，因为数据泄露影响了数百万客户。罚款源于对 Zoetop 公司的指控，即该公司未能保护客户的数据，没有适当地通知客户数据泄露，并试图对泄露的程度保持沉默。

罚款是在司法部长办公室对 2018 年的一次黑客攻击进行调查后作出的，其中信用卡和个人信息，如姓名、电子邮

件和哈希密码被盗。该数据泄露事件影响了 3900 万 Shein 和 700 万 Romwe 账户，包括属于纽约人的 80 多万个账户。

https://www.secrss.com/articles/47894

3、Everest 入侵南非国有电力公司 ESKOM 并勒索 20 万美元

据媒体 10 月 9 日报道，黑客团伙 Everest 入侵了南非国有电力公司 ESKOM。Everest 在 2022 年 3 月发布声明称以 12.5 万美元的价格出售南非电力公司的 root 访问权限，当时该公司否认发生了安全事件。10 月 8 日，研究人员称 ESKOM Hld SOC Ltd 的服务器遇到问题。与此同时，Everest 发布了攻击声明，表示可以访问公司的所有服务器，还提供一个软件包，其中包括带有管理员、root、用于 Linux 和 Windows 服务器的系统管理员密码的服务器等，要求该公司支付 20 万美元。

https://securityaffairs.co/wordpress/136866/cyber-crime/south-africa-eskom-everest-ransomware.html

4、哈佛商业出版社在土耳其的许可公司遭到勒索攻击

媒体 10 月 10 日报道，哈佛商业出版社在土耳其的许可公司遭到了勒索攻击。9 月 16 日，Cybernews 研究人员发现

了 infomag.com.tr 的一个开放的 MongoDB 实例，Infomag 以土耳其语出版《彭博商业周刊》和《哈佛商业评论》。该数据库托管在土耳其，约为 3.9GB，有超过 1950 万条记录，152000 条与客户有关的信息，最早可以追溯到 2017 年。9 月 19 日，Cybernews 重新访问该数据库查看它是否关闭时，得知它遭到了勒索攻击。攻击者勒索 0.01 比特币，并以违反 GDPR 面临巨额罚款为威胁，Infomag 好像并未付赎金。

https://securityaffairs.co/wordpress/136860/cyber-crime/harvard-business-publishing-licensee-hit-by-ransomware.html

5、美国第四大医疗系统 CommonSpirit Health 疑似遭勒索软件攻击

10 月 11 日报道称，拥有逾 140 间医院、被《贝克尔医院评论》（Becker's Hospital Review）杂志评为全美第四大医疗系统的 **CommonSpirit Health** 疑似遭到勒索软件攻击，导致手术延迟、患者护理中断以及在全国范围内重新安排医生预约。

https://www.cnbeta.com/articles/tech/1325679.htm

6、BidenCash 免费发布超过 120 万张信用卡的支付信息

10 月 11 日，据外媒报道，暗网市场 BidenCash 近日公开了超过 120 万信用卡用户细节，这些泄漏的信息包括卡号、过期时间、CVV 号码、卡片持有人名称、银行名称、卡片类型、家庭住址、电子邮件地址、身份证号码和手机号码等等。这些信息足以让网络犯罪分子进行财务欺诈和身份盗窃。

这些泄露的信用卡持卡人主要来自美国，此外还有来自印度、巴西、英国、墨西哥、澳大利亚、西班牙和中国。其中大部分信用卡的有效期到 2023 年，有些甚至到 2026 年。

https://www.cnbeta.com/articles/tech/1325831.htm

7、大疆无人机追踪数据在因未受保护的数据库而泄露

10 月 13 日，据外媒报道，最近，Cybernews 研究团队偶然发现了一个未受保护的数据库，其中包含由 66 种不同 DJI AeroScope 设备创建的超过 9000 万条无人机监控日志条目，其中大多数（53 台）位于美国、一些位于卡塔尔（6 台）以及德国、法国和土耳其。

日志包括无人机的位置、型号和序列号、无人机飞行员的位置以及家乡位置（通常是起飞点）。数据集中不存在个人身份信息 (PII)。总的来说，研究人员在实例中发现了超过

80,000 个唯一的无人机 ID。Cybernews 已向 DJI 和 AWS 通报了数据库泄漏的情况，以便他们尽快解决问题，以降低威胁参与者访问数据集的风险。

https://cybernews.com/privacy/dji-drone-tracking-data-exposed-in-us/

8、澳大利亚警方特工在哥伦比亚数据泄露事件中暴露

10 月 14 日，据外媒报道，在黑客泄露了从哥伦比亚政府窃取的文件后，为澳大利亚联邦警察 (AFP) 工作的秘密特工的身份遭到曝光。

此次泄露来自一个名为 Guacamaya 的黑客组织，其中包括超过 5 TB 的机密数据，包括电子邮件、文件和 AFP 特工用来阻止贩毒集团在澳大利亚开展业务的方法，还包括来自特工的监视报告、电话窃听记录和哥伦比亚官员的工资数据。

https://www.bleepingcomputer.com/news/security/australian-police-secret-agents-exposed-in-colombian-data-leak/?&web_view=true

9、RansomExx 泄露 52GB 巴塞罗那健康中心的数据

10 月 13 日，据外媒报道，勒索软件团伙 RansomExx 表

示，其周二在暗网上发布的一份 52 GB 的文件包含来自提供医疗和社会服务的公共实体 Consorci Sanitari Integral（CSI）的数据。

该组织发布的信息包括了医疗检查结果以及从巴塞罗那医院系统窃取的身份证，该医院系统每年为超过 100 万患者提供服务。CSI 表示，它正在与加泰罗尼亚网络安全局和加泰罗尼亚数据保护局合作，以限制违规的范围。

https://www.bankinfosecurity.com/ransomexx-leaks-52-gb-barcelona-health-centers-data-a-20260?&web_view=true

10、佐治亚州律师协会披露数据泄露事件

10 月 13 日，佐治亚州律师协会表示，其成员的个人信息，社会安全号码，驾驶执照号码和直接存款信息在四月份的网络攻击中泄露。州律师协会由佐治亚州最高法院授权对该州的律师进行道德调查，并制裁那些违反州规则的人。该组织还为该州的律师以及律师名录提供指导和帮助。在一个多星期的时间里，佐治亚州律师协会的官员对一次网络攻击做出了回应，这次攻击破坏了该组织的网络、网站和电子邮件系统。目前该组织表示，它完成了对这一事件的调查，并发现存在信息泄露，包括姓名，地址，出生日期，社会安全号码，驾驶执照号码，直接存款信息和姓名更改信息。这些

信息来自现任和前任雇员以及州律师协会的一些成员，该协会拥有 53000 多名成员。州律师协会正在通过 Transunion 向那些信息泄露的人提供免费的信用监控和身份保护服务，但没有回应澄清服务将提供多长时间的请求。
https://therecord.media/georgia-state-bar-says-ssns-of-members-employees-leaked-in-april-ransomware-attack/

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

http://www.nelab-bdst.org.cn/