[公开]360NELab-DST-0-057-20210830

大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 57 期 2021 年第 33 期

（2021.08.23-2021.08.29）

大数据协同安全技术国家工程实验室

目录

政策形势

1、工信部：将推动建立数据产权制度、完善数据竞争规则

2021 年 8 月 25 日，工信部发布《关于政协第十三届全国委员会第四次会议第 3087 号（政治法律类 131 号）提案答复的涵》，答复涵中表示要推动建立企业数据安全保障能力水平认证评价机制，持续深化数据安全合规评估，引导行业不断提升数据保护水平。

https://www.miit.gov.cn/zwgk/jytafwgk/art/2021/art_63868fe8984d4e5e839b80777cfbe5d0.html

2、国新办举行《关键信息基础设施安全保护条例》国务院政策例行吹风会

8 月 24 日，国务院新闻办举行政策例行吹风会，国家网信办、工业和信息化部等相关负责人介绍《关键信息基础设施安全保护条例》有关情况。国家网信办副主任盛荣华表示，条例出台并不是针对企业境外上市，而是为了保障关键信息基础设施安全，维护网络安全。企业上市必须必须确保国家网络安全、关键信息基础设施安全、个人信息安全等。

http://www.gov.cn/xinwen/2021-08/24/content_5633100.htm

3、商务部：研究建立统一的大数据全流程管理标准推动商贸流通数字化

《商务部关于加强“十四五”时期商务领域标准化建设的指导意见》将于近日发布，提出将在商贸流通数字化方面，**研究建立统一的大数据全流程管理标准**，推动区块链等新技术标准化应用，更好支撑商务高质量发展。

网络安全和信创方面，提出发展国家可信技术创新与应用平台，突破**可信计算、数据安全、网络安全**等信息安全核心技术，开发网络空间主动防御与保障等应用平台。底层通用技术方面，提出加强与行业领军企业对接合作，重点突破**隐私计算**等薄弱环节，建设**隐私计算基础平台**，打通“数道”“链道”，形成多域协同、自主可控、安全隐私的可信智能计算基础环境。

https://mp.weixin.qq.com/s/jtSg0A89oS2FTIQnJGaCZw

4、《北京市“十四五”时期高精尖产业发展规划》发布

网络安全和信创方面，提出发展国家可信技术创新与应用平台，突破可信计算、**数据安全**、网络安全等信息安全核心技术，开发网络空间主动防御与保障等应用平台。

底层通用技术方面，提出加强与行业领军企业对接合作，**重点突破隐私计算等薄弱环节**。建设**隐私计算基础平台**，打

通“数道”“链道”，形成多域协同、自主可控、安全隐私的可信智能计算基础环境。

提出高水平推动数字贸易示范区建设。以**推动数字贸易开放创新发展**为目标，以**实现跨境数据安全有序流动**为着眼点，推进规则探索、创新政策举措、突破制度瓶颈。

https://mp.weixin.qq.com/s/Mx77Z5He1OxX7tQ2IjFh_g

5、美国加州总检察长发布关于全面遵守州健康数据隐私法的指导意见

2021 年 8 月 24 日，加州总检察长 Rob Bonta 宣布，他已向医疗机构和供应商发出公告，提醒他们有义务遵守州和联邦健康数据隐私法。总检察长特别解释道，在之前发生的多起勒索软件攻击加州医疗机构的事件中，医疗机构都没有尽到通知义务。因此，借此公告提醒医疗机构，当超过 500 名加州居民的健康数据被泄露时，医疗机构必须通知加州司法部。

https://mp.weixin.qq.com/s/oo63F2nDOQ_RlVUDPbN3Lg

业界观点

1、个人信息保护法：为数字社会治理与数字经济发展构建基本法

整体来看，个人信息保护法构建了完整的个人信息保护框架。其规定涵盖了个人信息的范围以及个人信息从收集、存储到使用、加工、传输、提供、公开、删除等所有处理过程；明确赋予了个人对其信息控制的相关权利，并确认与个人权利相对应的个人信息处理者的义务及法律责任；对个人信息出境问题、个人信息保护的部门职责、相关法律责任进行了规定。

首先，个人信息保护法确认了广义的个人信息范围，包括以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，这意味着绝大多数与自然人相关的信息都可以纳入保护范围，体现了个人信息保护法广泛的保护范围。**第二，个人信息保护法提出了处理个人信息需要遵循的原则和要求。第三，个人信息保护法制定了个人信息处理的规则。原则为个人信息的处理活动提供了方向，**规则则让个人信息的具体处理活动有更具体的依据。**第四，个人信息保护法明确了个人信息处理活动过程中的权利和义务。**赋予了个人在个人信息处理活动中的权利，包括查阅复制权、可携

带权、更正补充权、删除权、解释说明权等权利。**第五，个人信息保护法规定了履行个人信息保护职责部门的职责。第六，个人信息保护法规定了相关法律责任。**

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

2、密码技术在《个人信息保护法》中的基石地位和实现

密码对于《网络安全法》和《数据安全法》等所界定的网络数据“属性”保密性、完整性和可用性的保障和实现具有重要作用。密码对个人信息和数据的保密性维护自不待言，通过“特定变换的方法对信息等进行加密保护”，是《密码法》定义的基本表述，属于密码“基因”上的功能要求。密码对完整性的维护，是密码对保密性、可用性保障功能的自然推导，SM3、SHA-3 等哈希算法和 ZUC 的完整性算法都是为此而生。至于可用性，一方面指向信息和数据的普遍可获得性，另一方面，什么人访问什么信息，知情同意、因需知晓又有赖于访问控制，可利用密码的身份鉴别、密钥管理等安全认证机制和功能实现。欧盟的 GDPR 中，也有使用加密技术措施保护个人数据不被未经授权访问的明确规定（第 32 条、第 34 条等）。

https://www.secrss.com/articles/33841

3、数据安全法界定数据安全责任范围

《数据安全法》在 2021 年 6 月 10 日通过，是我国贯彻总体国家安全观，落实统筹安全与发展，将数据安全治理体系建设纳入法治化轨道的重要举措。该法第 4 条规定“维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。”

《数据安全法》既是一部行为法，也是一部监管法，在中华人民共和国境内开展数据处理活动及其安全监管均适用此法。因此《数据安全法》坚持属地主义管辖的同时，也适当发展了属人主义的内容，对境外开展数据处理活动，损害我国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

《数据安全法》扩大了数据的内涵，所称数据是指任何以电子或者其他方式对信息的记录，并重新定义了“数据安全”，让数据安全法律责任不止于数据收集存储环节避免泄露事件的发生，而是从数据处理全流程提出数据安全的保护义务和法律责任。该法所说的数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等，流程上所有主体均负有数据安全保护义务，采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。同时国家建立数据分类分级保护制度，在此基础上区别化确

定各主体的数据安全保护义务与法律责任。

https://www.secrss.com/articles/33815

4、保护数据安全，需解决好数据权属问题

要切实保护好数据安全还需要**从理论上法律上进一步解决数据权属问题**。数据是新的生产要素、生产资料，是基础性资源和战略资源。这个问题不仅关系到数据安全，还关系到国家政治安全、社会公共安全、经济安全、文化安全、企业安全、公民个人隐私和财产安全、数字经济健康有序发展、人类社会的公平正义乃至前途命运。

十三届全国政协委员、社会和法制委员会副主任、中国友谊促进会理事长、公安部原副部长、国家网信办原副主任陈智敏对解决数据权属问题基本原则提出了以下九个方面的看法：党的领导、主体在民、主权在国、政府管理、全民共有、企业开发、共享共用、法律保障、技术支撑。

https://mp.weixin.qq.com/s/0fMLo9_WwQ-FNccThCebCQ

5、联邦学习首次被纳入 Gartner 隐私计算技术成熟度曲线

根据 Gartner 最新发布的“2021 年新兴技术成熟度曲线”（Hype Cycle for EmergingTechnologies, 2021），建立信任、加速增长以及塑造变革将是三大主要趋势，并可推动企业机

构去探索诸如非同质化通证（NFT）、主权云、数据编织、生成式人工智能和组装式网络等新兴技术从而确保竞争优势。同时，联邦学习被首次纳入到科技创新的触发期（Innovation Trigger）中。

https://mp.weixin.qq.com/s/vDI_2wrPfoPWs5RCmGAcaQ

安全事件

1、微软云平台暴露 3800 万条客户数据：因默认配置不当

2021 年 8 月 24 日，据报道，微软低代码开发平台 Power Apps 默认配置不安全，上千款 Web 应用程序错误暴露在开放互联网之上，涉及多个 COVID-19 接触者追踪平台、疫苗接种登记、工作申请门户以及员工数据库的多达 3800 万条记录已经确认暴露。记录中包括大量个人敏感信息，美国航空、福特、多个州政府机构等众多组织受影响。该事件再次表明，流行技术平台中的一项错误设置，很可能引发深远的影响。

https://www.secrss.com/articles/33733

2、一起钓鱼网络攻击泄露了 Revere Health 12000 名患者的医疗信息

2021 年 8 月 26 日，据外媒报道，根据医疗保健公司 Revere Health 上周五发布的新闻稿称，一名医疗保健员工沦为一个网络钓鱼邮件攻击的对象，由此泄露了约 1.2 万名患者的一些医疗记录，其中包括圣乔治的心脏病患者。通过此次泄露获得的信息包括医疗记录号码、出生日期、提供者姓名、程序和保险提供者姓名。据 Freeze 披露称，此次数据攻

击没有泄露信用卡等财务信息。

https://www.cnbeta.com/articles/tech/1171183.htm

3、诺基亚子公司遭 Conti 勒索软件攻击并出现数据泄露

2021 年 8 月 23 日，总部位于美国的诺基亚子公司 SAC Wireless 披露了在勒索软件攻击后发生的数据泄露事件，Conti 运营商能够成功破坏其网络、窃取数据和加密系统。Conti 勒索软件团伙在他们的泄密网站上透露，他们窃取了超过 250 GB 的数据。如果诺基亚子公司不支付他们要求的赎金，勒索软件组织将很快将所有被盗文件泄露到网上。

https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-conti-ransomware-attack/

4、西班牙数据保护局因某公司缺乏安全和隐私保护措施对其罚款 200,000 欧元

西班牙数据保护局（AEPD）于 2021 年 8 月 24 日发布了 PS/00362/2021 号决定，对 Bilbao Vizcaya Argentaria, S.A. 银行处以了 200,000 欧元的罚款。该银行未设置安全和隐私措施的行为违反了 GDPR 第 32 条。该决定特别指出，该银行对于用户个人信息没有采取任何安全措施，只通过在自动应答电话服务中要求客户提供唯一识别数据（DNI）的方式

来确认客户的身份。

https://mp.weixin.qq.com/s/oo63F2nDOQ_RlVUDPbN3Lg

5、未经用户同意收集个人信息，Facebook 等公司被开出 67 亿韩元罚单

2021 年 8 月 25 日，韩国个人信息保护委员会通过了一项决议，对 Facebook、Netflix 和谷歌三家企业共计征收约 67 亿韩元（约合 3714 万元人民币）的罚款，并要求三家公司采取更正措施。韩国个人信息保护委员会介绍称，Facebook 违法项目最多，共达 6 项。2018 年 4 月至 2019 年 9 月，Facebook 未经用户同意，制作并收集人脸识别格式，因而被处以 64.4 亿韩元的罚款。

https://mp.weixin.qq.com/s/WapH-uORJVr_aqpUTpxKlg