全球数据安全观察

总第 141 期 2023 年第 22 期

(2023.07.24-2023.08.06)

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
1、 关于调整《网络关键设备和网络安全专用产品目录》的公告.....1
2、 民航局发布《关于落实数字中国建设总体部署 加快推动智慧民航建设发展的指导意见》.....1
3、 粤港澳大湾区数据跨境流动合作备忘录签署.....2
4、 金融监管总局：加强第三方合作中网络和数据安全管理.....2
5、 北京市政府印发《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》.....3
7、 《深圳市数据产权登记管理暂行办法》发布.....4
8、 《数据安全技术能力评估要求》等 3 项团体标准立项.4
技术、产品与市场.....6
1、IBM 报告：2023 年数据泄露平均成本高达 445 万美元，51%企业计划增加安全投资.....6
2、2023 年隐私计算行业观察.....7
3、麻省理工推出 PAC 隐私新技术，可在确保隐私的前提下降低数据噪声.....8
4、研究：每万名企业用户每月会遭遇约 183 起敏感数据被发布到 ChatGPT 的事件.....8

5、研究：95%的组织无法在遭网络攻击后 24 小时内恢复数据.....9
业界观点.....10
1、 组建国家数据局：持续优化数据行政管理机构职责体系.....10
2、 《欧美数据隐私框架》落地及对我国跨境流动治理的启示.....11
3、解读:《个人信息保护合规审计管理办法(征求意见稿)》.....14
4、 解读：《中国人民银行业务领域数据安全管理办法（征求意见稿）》.....16
5、 梁昊光：融合数字技术提升数据安全治理能力.....20
数据安全事件.....24
1、违反《数据安全法》！重庆市网信办对属地一公司罚款 10 万元.....24
2、美国蒙特克莱尔镇遭到勒索攻击同意交 45 万美元赎金.....24
3、美国 SAIS 数据库配置错误泄露 572 GB 学生和教师的信息.....25
4、美政府供应商 169GB 健康数据遭俄黑客曝光，千万美国用户受影响.....26
5、北约遭黑客组织袭击，敏感数据泄漏.....26

6、因配置错误，法国汉堡王网站敏感数据遭泄露.....27
7、美国政府承包商 Serco 披露 MOVEit 攻击后数据泄露.....28
8、百行征信因违规处理信用信息被央行处罚.....29
9、科罗拉多州高等教育部警告大规模数据泄露.....29
10、华宝证券因信息系统安全问题收到证监会警示函.....30
11、加拿大不列颠哥伦比亚省医护人员信息遭泄露.....30
12、夏威夷社区学院向勒索软件团伙支付赎金以防止数据泄露.....31

政策形势

1、关于调整《网络关键设备和网络安全专用产品目录》的公告

7月3日，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门更新了《网络关键设备和网络安全专用产品目录》，《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017年第1号）中的网络关键设备和网络安全专用产品目录同步废止。

https://wap.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_9080a8689c58416eaf56f88649c242d3.html

2、民航局发布《关于落实数字中国建设总体部署 加快推动智慧民航建设发展的指导意见》

近日，中国民用航空局发布《关于落实数字中国建设总体部署 加快推动智慧民航建设发展的指导意见》，指导行业全面推动数字化转型、智能化应用、智慧化融合，在“筑牢民航数字安全屏障”部分，意见提出要增强数据安全保障能力：建立数据分类分级保护基础制度，按照“谁管业务，谁管业务数据，谁管数据安全”的原则，完善数据安全工作体系，健

全数据目录管理、监测预警、全生命周期管理等机制，加强数据安全应急处置。

https://www.gov.cn/zhengce/zhengceku/202307/content_6889672.htm

3、粤港澳大湾区数据跨境流动合作备忘录签署

6月29日，国家互联网信息办公室与香港特区政府创新科技及工业局签署《关于促进粤港澳大湾区数据跨境流动的合作备忘录》，在国家数据跨境安全管理制度框架下，建立粤港澳大湾区数据跨境流动安全规则，促进粤港澳大湾区数据跨境安全有序流动，推动粤港澳大湾区高质量发展。

https://www.cnbayarea.org.cn/news/focus/content/post_1076032.html

4、金融监管总局：加强第三方合作中网络和数据安全管理

日前国家金融监督管理总局向各地方银保监局、银行、保险、理财公司等机构下发了《关于加强第三方合作中网络和数据安全管理的通知》。国家金融监督管理总局要求，银行保险机构应强化“服务外包、责任不外包”的主体意识，切实承担数据安全主体责任，统筹管理科技风险，压实外包服务商安全责任，提升整体防控水平。

https://www.secrss.com/articles/56038

5、 北京市政府印发《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》

近日，中共北京市委北京市人民政府印发《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》。作为北京版“数据二十条”，该意见提出要发展数据安全服务业，支持企业开发数据安全评估、资产保护、数据脱敏、存储加密、隐私计算、检测认证、监测预警、应急处置等产品和服务；并从加强数据分类分级保护、完善数据安全技术体系、支持第三方几口开展数据安全和合规性的评估和审查、建立实施数据安全管理认证制度等方面明确强化数据安全和治理的路径。

http://jxj.beijing.gov.cn/zwgk/zcwj/bjszc/202307/t20230707_3157870.html

6、北京发布首个自动驾驶示范区数据分类分级管理细则

6 月 30 日，北京市高级别自动驾驶示范区工作办公室正式发布《北京市智能网联汽车政策先行区数据分类分级管理细则（试行）》，在国家数据分类分级保护制度下，深入结合示范区车路云一体化数据管理实践经验与企业安全发展诉

求，通过引导明确数据分类策略，定量数据定级方法并提供实操样本案例，有效推动形成依法规范、协同建设、共享红利的示范区数据安全发展模式。

http://kfqgw.beijing.gov.cn/zwgkkfq/yzttkfq/202307/t20230701_3152556.html

7、《深圳市数据产权登记管理暂行办法》发布

7 月 4 日，深圳市发展和改革委员会发布《深圳市数据产权登记管理暂行办法》，对登记申请人及登记主体、登记机构、登记行为等提出规范要求，并规定登记机构应当建立保护数据传输、存储和使用安全的基础设施，加强防攻击、防泄漏、防窃取的监测、预警、控制和应急处置能力建设，制定数据安全事件应急预案，对重要系统和数据库进行容灾备份，定期开展数据安全等级保护测试和渗透测试，关键设备应采用自主可控的产品和服务。

http://fgw.sz.gov.cn/zwgk/zcjzcjd/zc/content/post_10692431.html

8、《数据安全技术能力评估要求》等 3 项团体标准立项

7 月 4 日，中国互联网协会发布《数据安全技术能力评估要求》等 3 项团体标准立项的公告，《数据安全技术能力评

估要求》将规定应具备数据安全能力的企事业单位、政府部门等组织的数据安全技术能力要求，适用于第三方机构展开数据安全技术能力评估，为企业数据安全技术能力自评估提供参考和指导。

https://www.isc.org.cn/article/17166616918355968.html

技术、产品与市场

1、IBM 报告：2023 年数据泄露平均成本高达 445 万美元，51%企业计划增加安全投资

7 月 24 日，IBM 发布了《2023 年数据泄露成本报告》。该报告调查了在 2022 年 3 月至 2023 年 3 月期间受到数据泄露影响的 553 家组织，报告中提到，2023 年全球数据泄露的平均成本达到 445 万美元，创下历史新高。

该报告所研究的数据泄露事件发生在 16 个国家和地区，涉及 17 个不同行业。整个报告中探讨了数据泄露的根本原因以及短期和长期后果，还探讨了能够使公司减少数据泄露损失的要素和技术。关键发现点如下:

445 万美元-数据泄露的平均总成本: 这比 2022 年的 435 万美元增加了 2.3%。从长期来看，平均成本比 2020 年报告中的 386 万美元增加了 15.3%。

53.3%-医疗保健领域数据泄露成本的增加：自 2020 年以来，受到高度监管的医疗保健行业的数据泄露成本上升了 53.3%。**医疗保健行业连续第 13 年报告了成本最高的数据泄露事件，平均成本为 1093 万美元。**

82%-涉及存储在云环境中的数据的比例: 2023 年，云环境经常成为网络攻击者的攻击目标。攻击者通常可以访问多

个环境，**其中 39%的漏洞涉及多个环境，造成的损失高达 475 万美元。**

https://www.secrss.com/articles/57128

2、2023 年隐私计算行业观察

7 月 26 日，中国信通院云计算与大数据研究所副主任闫树正式发布了**“2023 隐私计算行业观察“，**从政策、市场、技术等角度总结了隐私计算现状，并针对当前发展挑战与热点现象带来思考和观察。

观点一：市场需求快速增长，产业处于稳步上升阶段。

观点二：开源提供新动能，持续助力生态繁荣。

观点三：产品能力稳步提升，已具备大规模应用基础。

观点四：AIGC 带来数据流通新模式。

观点五：大模型带来隐私计算发展新机遇。

观点六：尝试技术手段度量“匿名化程度”推进合规性验证。

观点七：通过隐私工程完善企业隐私保护合规要求。

观点八：多技术融合助力突破应用瓶颈。

观点九：公共数据授权运营为隐私计算提供新场景。

观点十：通过互联互通助推构建广泛生态圈。

https://www.secrss.com/articles/57428

3、麻省理工推出 PAC 隐私新技术，可在确保隐私的前提下降低数据噪声

近日，麻省理工的研究人员开发出了一种新的隐私度量方法，称为“Probably Approximately Correct Privacy”，简称“PAC 隐私”，可在保护敏感数据的同时保持机器学习模型性能。PAC 隐私使用一种新的隐私指标，帮助用户自动确定添加最小噪声量，避免对手恢复敏感数据。与其他隐私方法相比，PAC 隐私所需噪声更少。该技术可以在机器学习模型应用中实现隐私保护与数据准确性的双赢。

https://mp.weixin.qq.com/s/TD5R8aaNYEV9QseL2lQH4A

4、研究：每万名企业用户每月会遭遇约 183 起敏感数据被发布到 ChatGPT 的事件

据 Netskope 称，对于每 10,000 名企业用户，企业组织每月会遇到大约 183 起敏感数据发布到 ChatGPT 的事件。

源代码在暴露的敏感数据中所占比例最大。Netskope 发现，发布到 ChatGPT 的源代码比任何其他类型的敏感数据都多，每月每 10,000 个用户就有 158 起事件。ChatGPT 中共享的其他敏感数据包括受监管的数据（财务和医疗数据、个人身份信息）以及不包括源代码的知识产权，以及最令人担忧的嵌入源代码中的密码和密钥。

根据全球数百万企业用户的数据，研究人员发现生成式人工智能应用程序的使用量正在快速增长，在过去两个月中增长了 22.5%，增加了用户暴露敏感数据的机会。

https://www.helpnetsecurity.com/2023/07/28/chatgpt-exposure/?web_view=true

5、研究：95%的组织无法在遭网络攻击后 24 小时内恢复数据

虽然大家都承认勒索软件攻击是当前所面临的最大网络安全威胁之一，但根据一份最新的调查研究显示，大多数组织仍然缺乏强大的网络弹性战略或数据安全能力去应对此类威胁，并保持业务的连续性。

根据海外安全企业 BigID 发布的研究内容显示，在今年的调查中，有 67%的受访者对其所在组织能够在一场网络攻击事件中恢复数据和关键业务连续性没有完全的信心，而在去年，表达出类似担忧的受访者所占比例还只是 40%。由此可见，更多的企业、组织对自身恢复能力缺乏信心，而且普遍是在具备一定备份能力的条件下。

在这份研究的相关调查中，当假设发生网络攻击，95%的受访者表示需要超过 24 小时的时间来恢复数据和业务流程，71%的受访者表示需要超过 4 天，41%的受访者表示需

要超过一周，结果是让人触目惊心的。而在勒索软件攻击中，每一分钟都很重要。企业数据无法访问、业务中断的时间越长，其面临的风险也会越大，甚至可能导致对其下游企业用户乃至终端个人用户都会产生巨大影响。

https://mp.weixin.qq.com/s/mo1HCo_HB6EkJdezVJJHcA

业界观点

1、组建国家数据局：持续优化数据行政管理机构职责体系

党的十八大以来，部分地方政府已先行探索成立数据行政管理机构，深入比较分析国家数据局与省级数据局机构设置和职责配置对应关系，对于理解和把握数据行政管理机构职能重塑具有重要意义。

（一）统筹数据资源整合共享和开发利用

职责范围聚焦在数字经济和数据资源整合共享和开发利用方面。组建国家数据局是在保持数据行政管理职责总体稳定前提下，遵循适度调整、稳中求进原则，在数字经济和数据资源整合共享和开发利用方面优化数据管理机构和职责体系的一次重要尝试。

机构属性为部委管理的国家局。

职责履行的重点是加强宏观管理。

（二）统筹推进我国数字经济规划和建设

省级数据局机构设置和职能配置形成了数据综合治理型、数字政府建设引领型、数字经济发展驱动型三种主要模式。

在机构设置上，国家数据局的机构规格彰显了通过数字经济驱动发展的改革目标。

在职能配置上，省级大数据局和国家数据局主要职责基本对应，而且职责整合集中程度较高。

（三）持续优化数据行政管理机构职责体系

持续优化数据行政管理机构职能体系，既要立足当下结合实际合理设置地方数据管理机构，又要着眼于全面建设社会主义现代化国家，注重解决数字中国建设事关长远的体制机制问题，为推进国家治理体系和治理能力现代化、构筑国家发展新优势创造有利条件。

持续优化数据行政管理机构职能运行机制。

更好统筹发展和安全，提高数据管理法治化水平。

在地方试点基础上探索数据行政管理大部门体制。

http://www.cbdio.com/BigData/2023-08/04/content_6174524.htm

2、《欧美数据隐私框架》落地及对我国跨境流动治理的启示

2023 年 7 月 10 日，欧盟委员会宣布《欧美数据隐私框

架》(EU-US Data Privacy Framework)（以下简称“数据隐私框架”）已通过充分性认证，标志着欧美间个人数据合法流动的第三次尝试正式落地。当然，欧美间的数据流动自此能否一帆风顺，还要看美方的措施能否通过欧盟法院司法审查。

《数据隐私框架》应欧盟所要求的“基本等同”和“比例”原则，对之前的欧美数据跨境机制进行了修改，同时根据施雷姆斯二号案判决中的诉求做出了重大调整，设立独立法庭审查美国情报机构数据收集工作。

新《信号情报行政令》建立的机制并未完全解决施雷姆斯二号案所提出的关切：DPRC 仍属于美国行政系统内部的自我纠正机制，而非完全独立的法院；并且申诉人无法直接面对 DPRC，而必须通过隶属于美国政府的特别律师表达意见。因此，该机制能否满足欧盟法院所确定的“可通过诉讼保护权利”标准尚难判断。

不过，欧盟 GDPR 事实上也并不适用于欧盟各国的情报活动。欧盟另行订立的《刑事个人数据保护指令》以及欧洲人权法院根据《欧洲人权公约》所做出的判决是规范欧盟各国情报活动的法律规则。虽然法院的判决禁止了对个人数据的大规模监控行为，但也认为如果基于国家安全及对抗严重犯罪的目的属于特例，可以保留。法院对于欧盟内部的情报活动主要通过“比例”原则进行限制，要求国家安全必须受到

了真实、紧迫且可预见的威胁情况下才可以进行相关活动。而政府在调取或收集这些数据之后，对数据进行的读取或利用等行为都必须严格符合当初调取或收集时的目的，并要有法院或独立行政机关复核。因此，如果针对《数据隐私框架》的施雷姆斯三号案将来真的发生，美国或许可以通过比较欧盟自己的立法与《数据隐私框架》中对于情报活动的限制以及救济措施有效性的方式来应对欧盟法院的司法审查。美国司法部长指定欧盟为符合条件国家时所附的备忘录中已经明确指出，欧盟各国在大规模情报收集活动中所需要遵循的要求已经与美国《信号情报行政令》赋予欧盟公民的保护相去不远。

随着我国《数据出境安全评估办法》、《个人信息出境标准合同办法》、《个人信息保护认证实施规则》等法规和标准的不断出台，中国的数据出境安全管理制度架构已基本成型。同时，现有的制度设计也为我国通过缔结或者参加国际条约或协定的方式作为个人信息出境的路径预留了空间。而欧美之间二十多年来在数据跨境流动领域的博弈，是一次对欧盟的立法原则在实践中检验的有益探索，也为我国未来有可能通过缔结或者参加国际条约或协定开辟个人信息出境新路径提供了非常有价值的借鉴。

https://www.secrss.com/articles/56847

3、解读:《个人信息保护合规审计管理办法(征求意见稿)》

8 月 3 日，中央网信办就《个人信息保护合规审计管理办法》(简称《办法》)及配套的《个人信息保护合规审计参考要点》(简称《要点》)公开征求意见。本文拟从个人信息保护合规审计的效用、触发条件、审计基准这三方面，谈一谈对我国个人信息保护合规审计工作的理解和认识。

一、个人信息保护合规审计的效用

开展个人信息保护合规审计的目的，是在于明确以下事项：一是个人信息处理者是否实施了管理个人信息处理活动的相关政策和程序；二是这些政策和程序是否符合个人信息保护相关的法律法规的要求；三是个人信息处理活动是否真实地遵照这些政策和程序来展开，以及存在哪些差距；四是提出对这些政策和程序的具体内容、执行等方面的改进建议。

二、个人信息保护合规审计的触发条件

对于“自行开展审计”，《办法》规定“处理超过 100 万人个人信息的个人信息处理者，应当每年至少开展一次个人信息保护合规审计；其他个人信息处理者应当每二年至少开展一次个人信息保护合规审计”。

对于“部门委托审计”，《办法》规定的触发条件是“履行个人信息保护职责的部门在履行职责中，发现个人信息处理

活动存在较大风险或者发生个人信息安全事件的”。从笔者的经验来说，可能导致监管部门认为存在较大风险的因素，包括以下事项:

根据向监管部门提出的投诉，个人信息处理者对此的回复，以及个人信息处理者的合规“历史”;

个人信息处理者自我报告的违规行为（例如对个人信息安全事件的报告或通知），以及该处理者提出的补救行动;

与个人信息处理者的日常沟通中，如果展现出个人信息处理者对个人信息保护合规控制的缺乏，以及对个人信息保护立法的薄弱理解;

新闻报道，如披露个人信息处理者在处理个人信息方面存在重大缺陷的新闻报告，以及来自其他监管机构的信息;

个人信息处理者发布的各种声明（如社会责任报告）或披露的各种信息，特别是这些信息凸显了其在个人信息处理中存在的问题;

上线新技术新应用时，触发公众舆论或没有采取相应额外的个人信息保护措施;

个人信息处理者的规模，包括正在处理的个人信息的数量和性质；以及

其他相关信息，如"内部举报人"的报告、个人信息处理者披露的个人信息保护影响评估报告、个人信息黑灰产中流

传的线索等。

三、个人信息保护合规审计的审计基准

对个人信息处理者制定和实施的个人信息保护相关政策和程序，需要有个“标尺”。《要点》即是承担起这个角色。从要点的内容来看，其构成包括《个人信息保护法》中的具体规定，以及个人信息保护相关的部门规章（例如《要点》中关于数据跨境的内容）。

很显著的一点是，《要点》大量吸收了相关网络安全国家标准的具体规定。例如《个人信息安全规范》（GB/T-35273）、《个人信息安全影响评估实施指南》（GB/T-39335），以及正在制定的相关标准的主要内容。

另外值得注意的一点是，《要点》为参考性质。换句话说，《办法》中规定的审计实施程序、专业机构开展审计所需的权限、对专业机构的要求规范等，是强制性的，但是审计是否完完全全按照《要点》开展，是需要进一步裁量判断的。

https://www.secrss.com/articles/57397

4、解读：《中国人民银行业务领域数据安全管理办法（征求意见稿）》

根据《征求意见稿》第二条第一款的规定，该办法的前提是：（1）数据处理活动开展在境内；（2）需为中国人民银

行业务领域数据相关;（3）法律、行政法规或者中国人民银行没有其他规定。

其中，第一、三项要求都很好理解，值得注意的是所谓的中国人民银行业务领域，其范围在《征求意见稿》并非进行规定。对此，中国人民银行在起草说明中予以明确，“《办法》约束的数据处理活动主要包括：货币政策业务、跨境人民币业务、银行间各类市场交易业务、金融业综合统计业务、支付清算业务、货币管理和数字人民币业务、经理国库业务、征信业务、反洗钱业务等领域的数据处理活动。”因此，仅有前述业务范围内的数据处理活动才属于中国人民银行业务领域数据相关的处理活动。

此外，应当明确的是，《征求意见稿》的规制对象，数据处理者并不包括个人，其在负责中明确指出，数据处理者，是指开展数据处理活动的金融机构和其他机构。

《征求意见稿》定位明确，其准确将自身定义为在中国人民银行业务领域内数据处理活动的一般性、兜底性的法律规范。

1、与现有特定业务领域规范的协调。

2、与国家秘密相关规范的协调。

3、与个人信息保护相关规范的协调。

《征求意见稿》第二章对数据分类分级进行了细化：由

中国人民银行负责组织制定相关行业标准并指导数据处理者开展相关工作，在此基础上，数据处理者应建立业务分类，梳理细化数据资源目录，以此进行数据分类；而在具体的数据分级上，《征求意见稿》要求数据处理者根据精度、规模和对国家安全的影响程度分为一般、重要、核心三级，并在此基础上进一步根据数据敏感性和数据可用性对数据进一步分层级，后续的数据安全保护管理措施以及数据安全保护技术措施，都是在分类分级的基础上进行开展，因而理解此等分类分级制度至关重要。

数据安全保护作为《征求意见稿》的重点内容，占了其中三章的篇幅，主要包括管理措施和技术措施两方面内容，分别从管理层面和技术层面保障相关数据的安全性。其中：

数据出境限制管理措施方面。对于数据出境，《征求意见稿》第二十六条明确要求境内产生和收集的数据原则上存储在境内，如确需向境外提供，应当严格遵守其有关规定事前开展数据出境风险自评估并申报数据出境安全评估。此项规定完全符合《数据安全法》与《数据出境安全评估办法》的要求，但在此基础上，本条的第三款额外要求相关数据处理者应当于每年 1 月底前测算或者估算其上两年累计出境数据规模与范围，并保存测算估算结果和对应的境外接收方联系方式至少三年。可以说，这是中国人民银行根据具体情况对

金融领域的数据处理活动提出了更高的要求。

数据加工安全保护方面。其中重点提及了利用加工数据进行自动化决策的相关规定。该等规定在此前可见于《个人信息保护法》，其第二十四条提出第一款，“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。”对此，《征求意见稿》进行了相似的处理，要求“基于加工生成的数据项面向个人提供自动化决策服务时，应当以适当方式说明加工目的、加工依赖数据基本情况和加工基本逻辑，提升决策的透明度”，并且在技术措施上，要求明确“退出算法自动化决策的替代方案”。

数据使用保护方面。《征求意见稿》明确要求“第三层级数据项原则上不提供导出使用方式，第四层级以上数据项原则上仅提供核验使用方式，确需提供其他使用方式时，应当说明相关必要性，经内部审批并明确对应的风险防范措施后，据此开展。”同时其要求技术上采取加密、数字水印或者脱敏处理等安全保护措施，这无疑极大程度保障了数据使用的安全性。

https://www.01caijing.com/blog/337700.htm

5、梁昊光：融合数字技术提升数据安全治理能力

在数字化进程中，数据安全风险加剧，我们要积极抢占全球数字竞争战略制高点，提升数据安全治理能力以保障数字中国建设。我国积极制定相关法律法规，发布《中华人民共和国网络安全法》《中华人民共和国数据安全法》《网络安全审查办法》等，以积极应对数字化进程加速带来的风险，维护国家网络安全。

（一）深刻把握数据安全治理的重要性及其深远影响

数据安全治理是提升国际竞争力的战略制高点。数据安全治理是全球数字治理的重要组成部分。倘若数据安全出现问题，没有一个国家能独善其身。欧美国家已将数据安全治理纳入政治议题，数据安全相关法律制定也在向精细化方向发展。在全球数字化转型背景下，重视数据安全和提升数据安全治理能力是有效获取数据资源、维护国家安全、提升国际竞争力的关键一步，更是人类迈向数字文明时代的“定海神针”。

数据安全治理是布局数据主权的博弈新场域。当前，国际社会尚未就数据主权治理问题建立相关全球性规则体系，各国已制定的数据安全管辖规则大多都从自身利益出发，容易产生各国规则界限冲突问题。以欧美为代表的数字技术领先国家为抢占数据安全治理国际规则话语权积极推进“数据

立法竞赛”,目的是将与本国利益相符的数据治理导向预先以“软法”的形式向国际社会公布。在布局数字主权的博弈中，各国试图通过构建数据“领土”保障数据安全、强化数据防御韧性，从而主导数字安全治理的话语权。

（二）着力布局数据安全治理战略规划和顶层设计

立足数据保护，增强全球数据安全治理协同性。各主权国家的数据安全治理模式存在差异，在不同程度上阻滞了全球数据安全治理的整合和发展。按照各主权国家对数据安全保护的程度，数据安全治理模式大致可分为宽松型、严格型和折中型。基于全球数据的多样类型与治理的多元诉求，设立权威组织来权衡数据自由流动原则与数据安全原则的合理程度，或将成为未来各国亟待达成的全球数据安全治理规则的通用方式。

融合数字技术与制度管理，建立数据安全保障的创新范式。数据安全面临的风险和挑战错综复杂，必须以科技赋能制度管理。在科技方面，从数字技术入手，系统整合各领域资源以确保数据信息全生命周期的安全性；在制度方面，从行政管理入手，协调各机构，通过健全法规政策和规章制度为数据保护提供法律依据和政策保障。为实现数据在全生命周期的可用性、完整性与机密性的安全保护，要以数据业务属性为出发点，以数据的分级分类为核心，根据数据存放位

置建立以数据为中心的安全架构体系。与此同时，应加强数据安全相关法规政策的制定与执行，使其成为社会治理体系的重要组成部分，构建数据安全管理体系，实施分级管理和等级保护等管理，并结合技术手段，实现基于数据托管与国家监管有机结合的数据安全保障范式。

（三）共谋数据安全治理的高质量发展之道

坚持数据安全流动与发展并重的基本立场。数据安全治理核心在于如何保障数据安全与合法有序流动，我国在参与全球数据安全治理的过程中，应坚守维护国家安全、公共安全以及个人隐私安全的底线，兼顾数据保护和数据流动。结合我国的具体国情和所处的历史发展阶段，确定我国对数据应用发展“开放”与“限制”的程度，在数据利用与维护国家安全之间找到平衡点。

积极开展并促进数据安全领域的国际交流与合作。数字技术深化发展使得各国间的依存程度不断加深，虽然各主权国家在数据治理规则制定中存在分歧和冲突，但积极开展国际合作依旧是当前促进全球数据安全治理的关键因素。加快探索建立相适应的国际治理机制、全球数字规则以及安全治理框架是当务之急。一方面，积极主动参与数据安全治理的多边或双边谈判，在以对等原则、尊重他国数据主权和合理利益诉求的前提下，建立统一的跨境数据流动规则，形成共

同认可的数据保护机制，实现数据有序和安全流动；另一方面，面对各主权国家不断扩大数据安全流通“朋友圈”的形势，积极联合友好国家，促进数据安全流通，依靠与“一带一路”沿线国家和地区、金砖国家、上海合作组织的友好关系，在发展和平衡中提升全球数据安全治理“中国方案”影响力，推动构建全球数据安全治理的新秩序和新格局。

https://www.secrss.com/articles/57182

数据安全事件

1、违反《数据安全法》！重庆市网信办对属地一公司罚款 10 万元

近日，重庆市网信办依据《中华人民共和国数据安全法》对属地一科技公司作出责令限期改正，给予行政警告，并处 10 万元罚款的行政处罚。

根据有关部门移交的线索，重庆市网信办对属地一科技公司涉网络数据安全违法行为进行立案调查。经查，该公司因业务开展，收集、存储、处理的网络数据量较大，但未按法律法规要求建立健全全流程网络数据安全管理制度，未组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施，保障网络数据安全等数据安全保护义务，且存在数据库数据泄露的情形。重庆市网信办依据《中华人民共和国数据安全法》第二十七条、第二十九条、第四十五条之规定，对该公司作出责令限期改正，给予行政警告，并处 10 万元罚款的行政处罚。

https://mp.weixin.qq.com/s/OVq7G9S8HKB-kZpXPGJW-w

2、美国蒙特克莱尔镇遭到勒索攻击同意交 45 万美元赎金

据 8 月 1 日报道，美国蒙特克莱尔镇（Montclair）遭到

网络攻击，该镇的保险公司与攻击者协商达成了 45 万美元的和解协议。临时镇长 Hartnett 称，目前攻击已经得到了解决，对该镇业务和运营至关重要的数据也已恢复。但是一些属于个人用户的数据，和涉及为该镇服务并存储过去记录的外部供应商的数据仍有待恢复。这些丢失的数据影响了该镇当局响应《公开公共记录法案》某些要求的能力。

https://www.databreaches.net/cyber-attack-on-montclair-township-led-to-450k-ransom-payment/

3、美国 SAIS 数据库配置错误泄露 572 GB 学生和教师的信息

媒体 7 月 28 日报道称，研究人员发现了一个未受保护的数据库，其中包含与教育机构相关的 682438 条记录。调查发现，数据库属于南方独立学校协会(SAIS)，这是位于美国的一个自愿性地区认证协会。此次泄露的数据共 572.8 GB，时间跨度从 2012 年到 2023 年，包括学生和教师记录、健康信息、社会安全号码、枪击案和封锁通知、学校地图和财务预算等。目前，该数据库已被保护起来。

https://www.hackread.com/data-leak-student-faculty-accreditation-org/

4、美政府供应商 169GB 健康数据遭俄黑客曝光，千万美国用户受影响

8 月 4 日消息，一家美国政府承包商报告称，800 万至 1100 万份健康数据记录被曝光，大规模 MOVEit 数据泄露造成的损失继续上升。

这起违规事件发生在一家名为 Maximus 的公司，该公司是一家管理医疗补助和医疗保险以及许多其他政府项目的承包商。俄罗斯黑客组织 Cl0p 因 MOVEit 数据泄露而受到关注，并一直在通过其暗网站打击各种受害者，现在威胁要泄露约 169GB 的被盗健康数据。

受损的健康数据属于 Maximus 管理的项目的参与者。政府承包商发表声明称，这可能包括敏感的健康信息和社会保障号码，但总损失仍在评估中，修复成本可能超过 1000 万美元。

https://www.secrss.com/articles/57418

5、北约遭黑客组织袭击，敏感数据泄漏

7 月 27 日报道，黑客组织 SiegedSec 近日攻击了北约组织，声称破坏了其 COI 门户，随后泄露了近 1GB 的数据，包括数百份供北约国家和合作伙伴使用的敏感文件。该数据还包含至少 70 名北约官员的全名、电子邮件地址、电话号

码、办公地址和军衔。

SiegedSec 在 Telegram 频道上声称，其对北约的黑客攻击与俄乌战争无关，主要针对的是北约侵犯人权的行为。SiegedSec 还表示，针对北约的最新攻击展示了该组织日益增强的攻击性和攻击知名目标的熟练程度。

尽管北约官员尚未确认数据泄露事件，但据称泄露的文件包含对北约国家和合作伙伴至关重要的信息，引发了人们对潜在安全影响的担忧。

https://www.secrss.com/articles/57142

6、因配置错误，法国汉堡王网站敏感数据遭泄露

8 月 4 日报道，近日，Cybernews 研究团队发现，法国的汉堡王由于网站配置错误而向公众泄露了敏感信息。汉堡王作为美国著名的国际快餐巨头，在全球拥有超过 1.9 万家餐厅，收入 18 亿美元。

这些泄露的信息一旦落入恶意行为者手中，则会成为其对汉堡王连锁店实施网络攻击的工具。由于此次遭遇信息泄露的是求职网站，因此那些在法国汉堡王求职的人可能会受到影响。

事实上这已经不是汉堡王第一次泄露敏感数据了。据报道，早在 2019 年汉堡王就曾因为配置错误，导致法国分店泄

露了购买汉堡王的儿童个人身份信息(PII)。

https://www.freebuf.com/news/373866.html

7、美国政府承包商 Serco 披露 MOVEit 攻击后数据泄露

8 月 3 日，据外媒报道，跨国外包公司 Serco Group 的美洲分公司 Serco Inc 披露了一起数据泄露事件，攻击者从第三方供应商的 MoveIT 托管文件传输 (MFT) 服务器窃取了 10,000 多人的个人信息。

Serco 在向缅因州总检察长办公室提交的违规通知中表示，这些信息是从其福利管理提供商 CBIZ 的文件传输平台中泄露的。攻击中泄露的个人信息包括以下信息的任意组合：姓名、美国社会安全号码、出生日期、家庭邮寄地址、Serco 和/或个人电子邮件地址以及当年选定的健康福利。

Serco 目前正在与 CBIZ 合作调查此次违规行为并评估事件的全部范围，重点是确保第三方供应商已实施安全措施以防止未来再度发生此类事件。

https://www.bleepingcomputer.com/news/security/us-govt-contractor-serco-discloses-data-breach-after-moveit-attacks/?&web_view=true

8、百行征信因违规处理信用信息被央行处罚

8 月 4 日，人民银行官网的行政处罚信息再次更新，百行征信因两项违规被罚，同时两名相关责任人一同被罚。

具体来看，百行征信存在以下违法行为：1、违反征信机构管理规定；2、违反信用信息采集、提供、查询及相关管理规定。行政处罚内容：警告，罚款 51.5 万元。

黄某安（时任百行征信有限公司运营部客服中心异议处理员）和汪某飞（时任百行征信有限公司运营部客服中心团队主管）对百行征信违反信用信息采集、提供、查询及相关管理规定行为负有责任，分别被罚 7.1 万。

https://mp.weixin.qq.com/s/mOZftw1__5ola5DNfRuZdQ

9、科罗拉多州高等教育部警告大规模数据泄露

8 月 5 日报道，科罗拉多州高等教育部 (CDHE) 在 6 月份遭受勒索软件攻击后，披露了一起影响学生、往届学生和教师的大规模数据泄露事件。

据调查显示，威胁行为者在 6 月 11 日至 6 月 19 日期间访问了他们的系统。在此期间，威胁行为者从该部门的系统中窃取了 2004 年至 2020 年 13 年的数据。

被盗信息包括全名、社会安全号码、出生日期、地址、地址证明（对账单/账单）、政府身份证复印件，对于某些人

来说，还包括警方报告或有关身份盗窃的投诉。

CDHE 没有透露有多少人受到影响，但由于违规范围从 2004 年到 2020 年，可能涉及大量个人。

https://www.bleepingcomputer.com/news/security/colorado-department-of-higher-education-warns-of-massive-data-breach/

10、华宝证券因信息系统安全问题收到证监会警示函

8 月 2 日报道，近日，上海证监局向华宝证券出具警示函，因华宝证券在 5 月 22 日的网络安全事件中存在变更重要信息系统前未充分评估技术风险、未制定全面的测试方案等问题。

具体来看，上海证监局认为华宝证券存在以下问题：

一是变更重要信息系统前未充分评估技术风险；二是变更重要信息系统前未制定全面的测试方案；三是生产运营过程中未全面记录业务日志和系统日志以确保满足故障分析需要；四是事件调查过程中向上海证监局报送的部分数据不准确不完整。

https://www.freebuf.com/news/373677.html

11、加拿大不列颠哥伦比亚省医护人员信息遭泄露

8 月 2 日，据外媒报道，不列颠哥伦比亚省健康雇主协

会（HEABC）服务器上的三个网站发生数据安全事件，数千名医护人员的个人信息遭到泄露。

黑客在 5 月 9 日至 6 月 10 日期间访问了 HEABC 系统，直到 7 月 13 日，工作人员“发现了潜在的异常情况”后才发现漏洞。

HEABC 总裁目前并无透露有多少员工受到影响，但表示涉及 24 万个电子邮件地址，并与护照信息、驾驶执照、生日和社会保险号码受到影响。

https://bc.ctvnews.ca/b-c-health-care-workers-private-information-subject-to-data-breach-1.6502818?&web_view=true

12、夏威夷社区学院向勒索软件团伙支付赎金以防止数据泄露

7 月 28 日报，美国夏威夷社区学院（UH）承认，它向勒索软件参与者支付了赎金，以防止约 28,000 人的被盗数据泄露。

夏威夷社区学院是一所公立社区学院，拥有超过 50,000 名学生。2023 年 6 月 19 日，NoEscape 勒索软件团伙在其勒索门户网站上列出了 UH，威胁称如果不支付赎金，将在一周内公布 65 GB 的被盗数据。

该学院仔细考虑了所有选择，并决定向网络犯罪分子付费，以保护数千名学生的个人数据。UH 在一份报告中解释道：“在确定被泄露的数据很可能包含大约 28,000 人的个人信息后，夏威夷大学做出了艰难的决定，与威胁行为者进行谈判，以保护敏感信息可能被泄露的个人。”

https://www.bleepingcomputer.com/news/security/hawaii-community-college-pays-ransomware-gang-to-prevent-data-leak/

《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