

全球数据安全观察

总第 61 期 2021 年第 37 期

(2021.10.04-2021.10.10)

目录

政策形势	1
1、工信部：《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》发布	1
2、上海市《上海市数据条例（草案）（征求意见稿）》出台	1
3、《新一代人工智能伦理规范》发布	2
4、信安标委《数据分类分级指引（征求意见稿）》出台 ...	3
5、上海市地方标准《数据去标识化共享指南》自 10 月 1 日起实施	3
业界观点	4
1、政企合作共筑数字安全与发展规则的重要性和迫切性凸显 4	
2、新时代下数据安全风险评估工作	4
3、11 省份已出台“数据条例”，加强数据监管刻不容缓	5
4、从《数据安全法》视角探讨重要数据保护	6
5、调查：超 90% 的恶意软件隐藏在加密流量	6
安全事件	8
1、Facebook 全球瘫痪 6 小时，引发美欧监管机关强烈关注	8
2、跨国工程巨头伟尔集团（Weir Group）遭受勒索软件攻击	8
3、美国媒体集团考克斯媒体集团(CMG)受到勒索软件攻击	9
4、BrewDog 泄露了超 20 万名股东和客户的数据	9
5、亚马逊旗下直播平台 Twitch 遭入侵：大量源代码和财务细节泄露	10

政策形势

1、工信部：《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》发布

2021年9月30日，工业和信息化部发布了《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》。定位为工业和信息化领域数据安全顶层管理设计，一是全面对接《数据安全法》要求。在工业和信息化领域对国家数据安全管理制度进行细化，明确开展数据分类分级保护、重要数据管理等工作的具体要求，为行业数据安全监管提供制度保障。二是构建工业和信息化领域数据安全监管体系。明确工业和信息化部、地方工业和信息化主管部门、地方通信管理局等管理部门的职责范围，建立权责一致的工作机制。三是明确数据保护要求。根据工业、电信行业实际情况，明确了数据全生命周期安全保护要求，指导行业企业健全数据安全管理和技术保护措施，履行保护义务。

<https://mp.weixin.qq.com/s/AUP1nTRmGaqZuOTO2uYMKg>

2、上海市《上海市数据条例（草案）（征求意见稿）》出台

2021年9月30日，上海市人大常委会办公厅出台了《上海市数据条例（草案）（征求意见稿）》。该条例为了保护

自然人、法人和非法人组织与数据有关的权益，规范数据处理活动，促进数据依法有序自由流动，保障数据安全，加快数据要素市场培育和数字经济发展，根据《中华人民共和国民法典》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律、行政法规，结合上海市实际制定。

<https://mp.weixin.qq.com/s/s3E3lxUMtNy6YI7j2ekA0A>

3、《新一代人工智能伦理规范》发布

《新一代人工智能伦理规范》旨在将伦理道德融入人工智能全生命周期，为从事人工智能相关活动的自然人、法人和其他相关机构等提供伦理指引。

《伦理规范》经过专题调研、集中起草、意见征询等环节，充分考虑当前社会各界有关隐私、偏见、歧视、公平等伦理关切，包括总则、特定活动伦理规范和组织实施等内容。

《伦理规范》提出了增进人类福祉、促进公平公正、保护隐私安全、确保可控可信、强化责任担当、提升伦理素养等 6 项基本伦理要求。同时，提出人工智能管理、研发、供应、使用等特定活动的 18 项具体伦理要求。

<https://mp.weixin.qq.com/s/PKKkpykQhD2uuNoBdz0w7A>

4、信安标委《数据分类分级指引（征求意见稿）》出台

2021年9月30日，全国信息安全标准化技术委员会出台了《网络安全标准实践指南——数据分类分级指引（征求意见稿）》。该实践指南依据法律法规和政策标准要求，从国家数据安全管理视角对数据分类分级进行了研究，给出了数据分类分级的原则。

<https://mp.weixin.qq.com/s/YvS11unbAh2Ltdcwy9nNlg>

5、上海市地方标准《数据去标识化共享指南》自10月1日起实施

为盘活数据资源，促进数据自由流动，奠定数据要素市场化配置的基础。2021年7月27日，上海市市场监督管理局发布了上海市地方标准《数据去标识化共享指南》（DB31/T 1311-2021），并于10月1日起在全市范围内生效实施。该地标旨在通过“规范共享的数据内容、控制过程的安全有序、约束数据的有限使用”，使数据去标识化共享仍然遵循个人信息保护等的法律法规，以防范数据共享的风险，促进数据合法合规的共享和收集利用，助力本市数字经济高质量发展。

https://mp.weixin.qq.com/s/s4vyHbGxXgOtO4av6_c9UA

业界观点

1、政企合作共筑数字安全与发展规则的重要性和迫切性凸显

2021年9月26至28日，网络法治国际中心执行主任、博导、中国互联网协会研究中心副主任吴沈括提出：第一，有效的政企合作有助于突破数字治理的信任度瓶颈。第二，全面的政企合作有助于突破数字治理的透明度瓶颈。第三，务实的政企合作有助于突破数字治理的激励度瓶颈。助力全球数字安全与发展规则建构的政企合作的共同愿景在于合力建设具备清晰的权益责任分配、鲜明的人文价值底蕴以及合理的内外市场衔接的开放数字生态。

<https://mp.weixin.qq.com/s/xQyU11hHZjPILliyHckabA>

2、新时代下数据安全风险评估工作

在新时代背景下，数据安全风险评估也应具备时代特性。数据安全风险评估的发展一定是以《数据安全法》为根本出发点，以网络安全风险评估的理论框架为准绳，且风险评估的内容和指标将围绕数据为核心对象，以发现数据安全风险为主要目的。

数据安全风险评估核心内容包括：1.数据识别安全评估

2.数据安全法律遵从性评估 3.数据处理安全评估 4.数据环境安全评估 5.重要数据出境安全评估。

目前，数据安全风险评估相关标准体系存在空缺，需尽快建立完善提供依据，数据资产识别和分类分级存在难度，急需行业主管部门及企业自身统筹解决，数据安全风险评估的健康生态尚未建立，需各方协作助力生态建设。

https://mp.weixin.qq.com/s/wk5-exTI7xLZsqO9o_lx9Q

3、11 省份已出台“数据条例”，加强数据监管刻不容缓

加强数据安全保护和监督管理制度建设，各地已经行动起来。据《证券日报》记者梳理，目前，已有山东等 **11 个省份**出台了与数据相关的条例（包括大数据条例、数据条例、数字经济条例，统称为“数据条例”），上海市正在制定数据条例。

当前我国地方数据要素市场尚处于起步阶段，数据交易机制和产品体系有待健全，特别是权属界定不清、要素流转无序、定价机制缺失、安全保护不足等问题成为制约地方数据要素市场发展的主要问题。为更好发挥数据要素价值，推动数据依法有序流动，加强数据监管、明确数据交易的法律规则 and 地位，有利于为各地数据要素市场建设奠定坚实基础。

https://mp.weixin.qq.com/s/yRUhBP_T2UOMQFspjE_R4A

4、从《数据安全法》视角探讨重要数据保护

《数据安全法》规定建立数据分类分级保护制度，数据安全风险评估、报告、信息共享、监测预警机制，数据安全应急处置机制等基本制度外，还针对重要数据规定了重要数据目录制定、数据安全审查和数据出口管制等制度。《数据安全法》的亮点之一就是明确了国家建立数据分类分级保护制度，而数据分类分级保护的核心就是加强对重要数据的保护。

《数据安全法》之所以强调对重要数据进行重点保护，主要原因在于：第一，数据保护有成本，需要集中力量保重要数据。第二，重要数据关系国家安全、社会公共利益，需要重点保护。第三，重要数据不宜都纳入国家秘密进行保护，需要构建对非密重要数据的保护制度。

<https://www.secrss.com/articles/34335>

5、调查：超 90%的恶意软件隐藏在加密流量

分析表明，2021 年第二季度检出的恶意软件中，91.5% 都涉及通过加密 HTTPS 连接投送。上一季度威胁趋势的分析结果表明，攻击者增加了无文件恶意软件的使用，而所有检出恶意软件中近三分之二是零日恶意软件。

企业如果尚未实现控制措施检测藏身于加密网络流量

中的恶意软件，就会面临环境中广泛分布大量恶意工具，自身端点设备可能遭受攻击的风险。WatchGuard Technologies 采用从客户网络收集到的匿名数据分析研究了威胁活动。结果表明，2021 年第二季度检出的恶意软件中，91.5%都涉及通过加密 HTTPS 连接投送。WatchGuard 表示，目前只有 20% 的企业设置有解密和扫描 HTTPS 流量以发现恶意软件的检测机制，意味着其余 80%的企业有可能漏掉九成日常攻击其网络的恶意软件。

<https://www.secrss.com/articles/34973>

安全事件

1、Facebook 全球瘫痪 6 小时，引发美欧监管机关强烈关注

美东时间 10 月 4 日上午 11:45 左右，社交媒体 Facebook，Instagram 以及即时通讯软件 WhatsApp 陷入大规模瘫痪，宕机近 6 个小时，刷新了自 2008 年最长宕机时长。其中包括美国英国在内的数十个国家和地区发生了中断故障，直到 4 日下午开始恢复部分运营。由此，Facebook 股价盘中暴跌 6%，扎克伯格个人财富一日蒸发逾 60 亿美元。

<https://mp.weixin.qq.com/s/TAYOopbqS62clcEBBjJFxQ>

2、跨国工程巨头伟尔集团（Weir Group）遭受勒索软件攻击

2021 年 10 月 9 日报道，近日，苏格兰跨国工程巨头伟尔集团（Weir Group）披露了其 9 月份遭受的勒索软件攻击。该勒索事件导致其发货、制造和工程中断，仅在 9 月份就导致间接费用回收不足和收入延期 5000 万英镑。对于此次勒索事件，伟尔方面表示：“伟尔网络安全系统，对威胁做出了快速反应，并采取了强有力的保护措施——这包括隔离和关闭 IT 系统，特别是隔离和关闭核心企业资源规划（ERP）和工程应用程序。”

<https://mp.weixin.qq.com/s/FPHqeFFBIwy51U7D2b0wqg>

3、美国媒体集团考克斯媒体集团(CMG)受到勒索软件攻击

2021年10月8日,据外媒报道,美国媒体集团 Cox Media Group (CMG) 证实,它在 2021 年 6 月遭到勒索软件攻击,导致电视直播和电台广播流中断。据了解,该公司 800 多名员工的个人信息在这次攻击中被泄露,包括姓名、地址、社会保险号、财务帐号、健康保险信息等。

<https://www.bleepingcomputer.com/news/security/cox-media-group-confirms-ransomware-attack-that-took-down-broadcasts/>

4、BrewDog 泄露了超 20 万名股东和客户的数据

2021年10月8日,据外媒报道,苏格兰著名啤酒厂和酒吧连锁店 BrewDog 已泄露超 20 万名股东和客户的详细信息长达 18 个月,泄露点为该公司的移动 APP,更具体地说,是基于令牌的身份验证系统,这些令牌被硬编码到移动应用程序中,而不是在用户身份验证成功之后再传输。

<https://www.bleepingcomputer.com/news/security/brewdog-exposed-data-for-over-200-000-shareholders-and-customers/>

5、亚马逊旗下直播平台 Twitch 遭入侵：大量源代码和财务细节泄露

2021 年 10 月 6 日报道，Twitch 约 125GB 数据在 4chan 网站上泄露，泄露数据包括几乎所有源代码、大量财务数据、内部安全工具等。Twitch 是亚马逊旗下的视频和游戏服务，现在，其服务的全部源代码，其移动、桌面和客户端应用程序，以及一个未发布的 Steam 商店竞争项目都被泄露了。

<https://www.secrss.com/articles/34909>