[公开]360NELab-DST-0-047-20210621

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 47 期 2021 年第 23 期

（2021.06.14-2021.06.20）

大数据协同安全技术国家工程实验室

目录

政策形势

1、欧盟跨境数据传输新规：评估政府数据请求效力成企业最大难点

近日，欧盟委员会发布新版欧盟承认标准合同条款（SCCs）。有专家表示，新版 SCCs 的规定对于涉及欧盟的数据跨境流动活动呈利好趋势，但也对数据进口方提出新的挑战，尤其是针对数据进口方当局请求提供数据时，如何有效评估政府请求的法律效力甚至对本国主管监督机构的数据访问要求提出质疑，必将成为企业在开展相关数据跨境活动时最头痛的实操难点。

https://mp.weixin.qq.com/s/vvMlNUayw1UqjGFZL5bPIQ

2、四部门开展摄像头偷窥等黑产集中治理

为切实保护公民个人隐私安全，中央网信办、工业和信息化部、公安部、市场监管总局决定，自 2021 年 5 月至 8 月，在全国范围组织开展摄像头偷窥黑产集中治理，打击不法分子利用黑客技术破解并控制家用及公共场所摄像头，将智能手机、运动手环等改装成偷拍设备，出售破解软件，传授偷拍技术，供客户“偷窥”隐私画面并借此牟利等严重侵害公民个人隐私的行为。

https://mp.weixin.qq.com/s/iMJBTD-Ujxjg6wPzpAyV1w

3、工信部规范“618”短信营销：“默认”用户同意就擅自发送属违法侵权

随着“618”年中商业营销活动临近，部分电商平台违规发送营销短信扰民问题开始呈现上升态势。近日，工业和信息化部召开行政指导会，警示电商平台企业规范营销短信发送行为，未充分核实注册用户意愿，“默认”用户同意，擅自发送“618”商业营销短信的，属违法行为。阿里巴巴、京东、拼多多等主要电商平台企业，以及相关基础电信企业和短信息服务企业参会。

https://mp.weixin.qq.com/s/XQI859091DhyEm_w6-ftmA

4、工信部：《关于加强车联网卡实名登记管理的通知（征求意见稿）》

近期，为贯彻落实《中华人民共和国网络安全法》《中华人民共和国反恐怖主义法》等相关法律法规要求，加强车联网卡实名登记管理，工业和信息化部起草了《关于加强车联网卡实名登记管理的通知（征求意见稿）》，并向社会公开征求意见。

https://mp.weixin.qq.com/s/p7dEZgEqm6VduoOywdIxaw

5、非法获取员工及客户敏感信息，法国宜家被罚 100 万欧元

据媒体报道，近日，全球最大的家具零售商宜家因法国分公司非法监视员工和客户被罚 100 万欧元。据悉，因内部知情者举报，法国宜家被曝在 2009 年至 2012 年之间、通过掌握警方内部数据库、雇私家侦探等方式，非法获取公司雇员以及宜家客户的个人资料和敏感信息，其中特别收集了工会活动人士和与宜家发生纠纷的客户信息。随后法国检方对宜家展开调查，最终法国宜家解雇了涉案的 4 名高管，并对内部政策做出修改。

https://mp.weixin.qq.com/s/Ts2tWF12cRbI9j9hCgtUwg

业界观点

1、中国信通院发布《移动互联网数据安全蓝皮报告（2021年）》

近期，中国信通院发布了《移动互联网数据安全蓝皮报告（2021年）》。报告全面梳理移动互联网数据安全发展现状与趋势，深入探讨移动应用在数据安全全周期面临的问题和挑战，并从数据安全管理要求，技术防范能力等多方面进行梳理，以期为移动互联网行业企业提供支撑和帮助。

从国家宏观政策角度来看，围绕数据安全保障能力建设，“十三五”规划中明确提出了要强化信息安全保障，加快数据资源安全保护布局。如建立大数据管理制度、实行数据分类分级管理，加强数据资源在采集、存储、应用和开放等各环节的安全保护，加强公共数据资源和个人数据保护等。中共中央关于“十四五”规划和二〇三五年远景目标建议明确提出建设网络强国、数字中国，发展数字经济，建立数据安全保护基础制度和标准规范，保障国家数据安全。

从行业微观应用角度来看，我国数字经济获得了新的发展空间，并深刻融入到了国民经济的各个领域。如，直播带货、在线游戏、在线教育和在线办公等新业态迅速成长，数字经济显示了拉动内需、扩大消费的强大带动效应，促进了

我国经济的复苏与增长。在数字经济蓬勃发展的过程中，数据安全是关键所在。除了数据本身的安全，对数据的合法合规使用也是数据安全的重要组成部分。滥用数据或进行数据垄断，不合法合规地使用数据，将大大削弱数字经济的发展活力与动力。

https://mp.weixin.qq.com/s/k6w-Tn1lS9ECgkurJPUovg

2、[调查]未来十年勒索软件攻击所致损失将超 2650 亿美元

勒索软件如今已成为最具破坏性也十分流行的一类恶意软件。如果勒索软件登陆脆弱系统，系统上的文件通常会被加密，用户被锁在系统之外，只有支付了赎金（一般以加密货币支付）才能获得解密密钥。

美国投资咨询机构 Cybersecurity Ventures 预测，鉴于勒索软件以几秒钟一次的速度攻击企业和消费者，到 2031 年，此类网络犯罪攻击可导致全世界损失 2650 亿美元。 这家网络安全机构还估测，今年勒索软件将给我们带来约 200 亿美元的损失，比 2015 年跳涨 57 倍。

https://mp.weixin.qq.com/s/RDYx-Xr5A5x0lMvoLv1LPA

3、赛迪专家刘权：个人信息保护困局亟需打破

数字经济时代，随着个人信息价值的凸显，个人信息收

集乱象突出，个人信息泄露事件频发，个人信息滥用程度严重，我国个人信息安全面临着严峻的挑战。监管执法部门已通过开展一系列联合专项行动，严厉打击侵害公民个人信息的违法违规行为。然而，当前个人信息安全逐步呈现出“问题频出-监管打击-安全平稳期-问题再次复现”的往复循环的态势，黑客攻击、内鬼窃取、APP 过度索权等均成为了个人信息保护的难题。国家层面，需加快个人信息保护立法和监管；企业层面，规范个人信息安全管理；个人层面，提升个人信息保护意识。

https://mp.weixin.qq.com/s/FyiliXctVDam-FspqbsPSg

4、企业数据泄露的法律治理困境与规范适用

目前，企业数据泄露的治理在法律层面存在多重困境：其一，企业数据泄露的责任界定不清晰。其二，各国关于企业数据泄露的法律体系不同，对企业数据泄露的界定标准、责任承担及域外适用等规定不统一。其三，泄露企业数据的违法成本、犯罪成本较低，远远低于企业的防范成本，对相关责任主体的威慑不足。其四，企业通过诉讼或者仲裁的方式处理企业数据泄露事件的周期较长，不利于及时止损。

大数据时代，面对严峻的数据泄露问题，我国应当尽快形成完善的数据泄露防治体系，明确相关主体的责任边界，

对掌握海量数据的企业提出更高的管理、维护、监控和处置要求，对数据企业的主管部门提出更高的监管和执法要求。有效预防和治理数据泄露事件，促进国家数字经济健康发展。

https://mp.weixin.qq.com/s/ltoe7eIRpW7Bqklf3-Tsgg

5、生产要素视角下的数据安全分析

在数据作为生产要素的背景下，可以把新形势下的数据安全划分为**五个核心场景**：（1）数据的采集安全。（2）数据在存储载体上的安全。（3）数据在业务过程中使用和流转的安全。（4）企业将来自自身各个业务系统甚至合作伙伴的大量数据打通汇集之后，可以依据这些数据本身作为业务，在大数据平台以及相关的终端上，展开数据分析、挖掘和建模活动。（5）对个人主体数据进行归一化的处理。

围绕着以上的场景，数据安全新的技术方向有以下几种：（1）数据自动化识别和分类分级技术；（2）数据主体归集和授权映射技术；（3）基于数据可用的数据匿名化技术；（4）融合和计算衍生数据血缘关系图谱；（5）数据使用流转关系映射；（6）数据关联资产识别与数据风险模型。

https://mp.weixin.qq.com/s/v291X3n44UtsIRibcOFYKw

安全事件

1、淘宝 11 亿条用户数据泄露，两男子用爬虫技术非法获利 34 万

2021 年 6 月 16 日报道，商丘市睢阳区人民法院 6 月 3 日在裁判文书网公开的刑事判决书显示，两名犯罪分子在淘宝爬取并盗走大量数据。经过检方核实，被盗取的淘宝用户数据近 12 亿条。法院裁定，这家公司一名员工收集超过 10 亿条淘宝用户资讯，虽然是用以为客户提供服务，但该员工及其雇主判处三年以上监禁，并处以总计 45 万元人民币的罚款。

https://www.solidot.org/story?sid=68048

2、网络安全公司 Cognyte 泄漏 50 亿条数据

2021 年 6 月 16 日报道，一名安全研究人员近日在网上发现了一个由网络安全分析公司 Cognyte 运营的不安全数据库，该数据库采集了从一系列在线数据泄漏事件中收集的约 50 亿条记录，并且无需身份验证即可访问。存储的数据是 Cognyte 网络情报服务的一部分，用于提醒客户注意第三方数据泄漏。

https://mp.weixin.qq.com/s/jb8r1544zBO-Xary4PB7jg

3、游戏界巨头 EA 源代码被盗窃，黑客以 2800 万美元出售数据

2021 年 6 月 15 日，据外媒报道，游戏巨头艺电(Electronic Arts)遭到黑客攻击，攻击者从该公司窃取 750 GB 的数据，并完全访问了 FIFA21 配对服务器、FIFA 22 API 密钥和一些微软 Xbox 和索尼的软件开发工具包。目前，攻击者正以 2800 万美元的价格出售这批数据和访问权限。

https://www.freebuf.com/news/277401.html

4、超过 10 亿份 CVS 健康档案在网上曝光

2021 年 6 月 17 日，WebsitePlanet 与研究人员 Jeremiah Fowler 发现了一个不安全的数据库，其中包含超过 10 亿条记录。该数据库属于美国医疗保健和制药巨头 CVS Health，该数据库已在网上曝光。每个人都可以访问该数据库，无需任何类型的身份验证。

https://securityaffairs.co/wordpress/119081/data-breach/cvs-health-data-leak.html

5、奥迪、大众客户数据在黑客论坛上出售

2021 年 6 月 17 日，一位在数据泄露期间被盗的知名数据卖家将奥迪和大众的数据放在一个流行的黑客论坛上出

售。数据泄露涉及奥迪、大众以及美国和加拿大的一些授权经销商的 330 万客户。

https://www.bleepingcomputer.com/news/security/audi-volkswagen-customer-data-being-sold-on-a-hacking-forum/