全球数据安全观察

总第 105 期 2022 年第 33 期

（2022.09.05-2022.09.11）

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、三部门发布《互联网弹窗信息推送服务管理规定》

近日，国家互联网信息办公室、工业和信息化部、国家市场监督管理总局联合发布《互联网弹窗信息推送服务管理规定》，自 2022 年 9 月 30 日起施行。

《规定》旨在加强对弹窗信息推送服务的规范管理，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进互联网信息服务健康有序发展。

http://www.gov.cn/xinwen/2022-09/09/content_5709181.htm

2、《网信部门行政执法程序规定（征求意见稿）》发布

为了规范和保障网信部门依法履行职责，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，国家互联网信息办公室对《互联网信息内容管理行政执法程序规定》进行修订，明确提出：设区的市级以下网信部门依职权管辖本行政区域内的网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。

https://mp.weixin.qq.com/s/_uHfbtYm_2_mFcNPBJvVaA

3、福建省工业和信息化厅、福建省财政厅发布《关于推进工业数字化转型九条措施》

为进一步贯彻落实工业和信息化部《“十四五”信息化和工业化深度融合发展规划》和省委、省政府关于深化新一代信息技术与制造业融合发展工作部署，加快推动工业企业数字化转型，福建省工业和信息化厅、福建省财政厅提出《关于推进工业数字化转型的九条措施》。

《措施》提出加强数据安全保障。支持工业企业开展工业互联网网络安全分类分级和工业领域数据安全管理，举办工业互联网安全大赛，培育壮大网络安全产业。每年遴选一批工业领域数据安全标杆企业和数据安全优秀服务商，每家给予最高 50 万元奖励。

https://gxt.fujian.gov.cn/zwgk/zfxxgk/fdzdgknr/gfxwj/202209/t20220901_5985934.htm

4、湖南大数据交易所文化大数据交易中心上线

9 月 7 日，湖南大数据交易所“文化大数据交易中心”正式上线。该交易中心是湖南大数据交易所下设的文化数据资产流通全链路机构，将打通从数据归集、加工、交易到应用的产业生态闭环，为湖南和长沙产业数字化、数字产业化提供重要支撑。

https://fzyj.hunan.gov.cn/hnszf/hnyw/zwdt/202209/t20220908_28683204.html

5、《智能网联汽车数据合规指引（2022）》发布

2022 年 9 月 2 日，在以“智能社会与协同治理”为主题的 2022 世界人工智能大会智能社会论坛上，同济大学、上海人工智能实验室联合发布了《智能网联汽车数据合规指引（2022）》。该《指引》是依托国家智能社会治理实验综合基地（上海杨浦）、上海市人工智能社会治理协同创新中心，面向无人驾驶应用场景的区校合作、政产学研联动的研究成果。《指引》采取“数据类型-数据处理行为-数据安全管理制度”的逻辑框架，将智能网联汽车数据区分为个人数据、重要数据、国家核心数据、地理信息数据等，并逐一归纳和梳理数据合规内容。

https://mp.weixin.qq.com/s/leiWvvLiesdWSXg9IVUxyA

6、《数据安全和个人信息保护社会责任指南》（征求意见稿）发布

为落实《数据安全法》《个人信息保护法》等法律法规中所提出关于数据安全和个人信息保护社会责任的要求，放大数据处理和个人信息使用的社会价值，由中国网络安全产业

联盟归口，CCIA 数据安全委员会组织委员单位编制了联盟技术文件《数据安全和个人信息保护社会责任指南》(征求意见稿)。

该文件为组织理解数据安全和个人信息保护社会责任和实施相关活动提供指南，旨在帮助组织在遵守法律法规和基本道德规范的基础上实现更高的组织社会价值，最大限度地致力于可持续发展。

https://www.secrss.com/articles/46706

技术、产品与市场

1、Gartner 发布 2022 云 Web 应用程序和 API 保护魔力象限

8 月 30 日，知名咨询机构 Gartner 发布 2022 云 Web 应用程序和 API 保护魔力象限。当前，云 Web 应用程序和 API 保护市场迅速增长。

Gartner 预测，到 2024 年，70%实施多云战略的企业将青睐云 Web 应用程序和 API 保护平台（WAAP）服务，而不是 WAAP 设备和 IaaS 原生 WAAP。到 2026 年，40%的企业将根据 API 保护和 Web 应用程序安全功能选择 WAAP 供应商，与 2022 年不足 15%的比例相比有所上升。

Web 应用程序和 API 保护平台（WAAPs）主要保护面向公众的网络应用程序和 API，可以缓解大部分运行时攻击，尤其是开放网络应用安全项目（OWASP）的网络应用程序威胁、自动化威胁和对 API 的专门攻击。

https://www.gartner.com/doc/reprints?id=1-2B148MS9&ct=220906&st=sb

2、2022 年密码学的全球新兴趋势

经济时代，组织依靠公钥基础设施 (PKI)和加密技术在其企业 IT 基础设施和互联产品解决方案中建立所需的数字

信任。致力于为汽车、金融、医疗保健和零售等垂直领域提供自动化数字安全管理的 Keyfactor 发布的一份产业报告指出，**2022 年密码学的新兴趋势包括：PKI 的治理兴起、后量子密码学（PQC）研究更为活跃、eIDAS 得到扩展、供应链安全的需求凸显、数字机器身份成为制造业的未来、加密敏捷成为主流。**上述六大趋势的预测有助于分析和研判对公司业务的影响和加密需求的变化。

量子计算对经典的非对称加密算法构成了重大威胁。为了应对这一威胁,各国持续关注并推进对后量子加密(PQC)算法的研究开发。在此方面，美国 NIST 一直在进行为期多年的公开竞赛，以评估各种 PQC 算法，并选择确定将被认可为 PQC 标准的算法。NIST 举办了为期五年的竞赛，旨在为未来的 PQC 标准选择候选算法。这意味着从 2022 年开始，相关的标准草案将陆续出台，最终标准预计将于 2024 年出台。IETF 和 NIST 的官方标准制定发布，将标志着 PQC 时代的到来。新的标准将为针对广泛的政府和工业部门的解决方案所应涵盖的内容提供合理预期。

https://www.secrss.com/articles/46620

3、核心目标：落地！美国防部将发布新版零信任战略，定义百余项具体能力

美国国防部负责网络安全的副 CIO David McKeown 表示，五角大楼即将发布新的零信任战略。与以往框架不同，新战略将概述国防部实现**“针对性”零信任**所需要的几十种能力要求。

McKeown 在比灵顿网络安全峰会上表示，这项战略预计将在本月内发布。文件提出了“经过明确定义、用于实现针对性零信任的 90 项能力要求。还定义了检查条款，以及实现特定能力时需要的条件。这 90 项能力将成为国防部达成针对性零信任的基石。”

他补充称，该战略还定义了另外 62 项能力，一旦达成将助力五角大楼实现“更先进的零信任”，足以支撑国家安全系统或者其他“极为重要的”系统。

https://www.secrss.com/articles/46722

4、《城市大脑标准体系建设指南（2022 版）》发布

2022 年 9 月 3 日，城市大脑建设高峰论坛期间，《城市大脑标准体系建设指南（2022 版）》（简称《指南》）正式发布。在 23 家地方主管部门的指导和支持下，全国信标委智慧城市标准工作组组织中国电子技术标准化研究院、上海数字

产业发展有限公司、山东浪潮新基建科技有限公司等 45 家产学研用单位共同编制形成。

《指南》明确了城市大脑标准体系建设总体要求，构建了城市大脑标准体系总体框架，从城市大脑总体标准、基础设施标准、数据标准、关键支撑能力标准、应用服务标准、建设管理标准和安全保障标准等七大方面提出了具体建设内容，并围绕机制建设、标准研制、标准实施、国际合作等方面提出了具体组织实施路径。

《指南》是我国城市大脑标准化工作的总体性、体系性规划，既可以为当前和未来一段时间内的城市大脑标准体系建设工作提供指导，也可以促进标准在支撑各地城市大脑项目建设、技术创新、产业发展等方面发挥实效。

https://www.secrss.com/articles/46617

5、《数据安全治理自动化技术框架》白皮书正式发布

最近几年，国际上在数据安全方面的自动化和智能化新技术层出不穷，但是这些技术在中国并没有被使用，甚至没有被了解，因为欧美企业不提供这样的技术给中国用户。

数据安全治理自动化（DSAG）通过自动化技术，识别结构化和非结构化数据，从企业内数据资源发现，到对数据进行分类分级，并以数据分类分级对象为核心，用户行为分析

为增强手段，进行数据安全策略的配置和执行，全方位地覆盖数据安全治理周期的每一个环节。DSAG 尽可能使用最大化的合理自动化，令人工干预降至最少，在必要的人工环节使用智能辅助，减少人为错误，更有效率及有效性地提高了数据工作的安全性。

DSAG 的亮点可以概况为“六化一管”，分别是数据分类分级自动化、数据安全处理自动化、行为分析智能化、数据脱敏全面化、API 数据内容分析细粒化、DSAG 编程管理可视化、一把手数据安全管理“一支笔”。

https://mp.weixin.qq.com/s/uVkdT6jglUvPfbJRxNlaiw

业界观点

1、杜跃进：汽车网络攻击事件剧增，智能汽车需要同步考虑安全问题

“当前，全球自动驾驶汽车事故频发，汽车网络攻击事件剧增，国家级的黑客组织和网络犯罪团伙越来越多，只有从汽车智能的实现过程出发，系统地识别安全风险，把握科学的安全原则，才能找到智能汽车安全问题的正确答案。”杜跃进在 2022 中国汽车先锋论坛指出，计算环节都是由软件来实现，如果计算软件被系统入侵，意味着汽车可以被远程控制，软硬件可以被破坏，数据可能被破坏或者删除，甚至被恶意加密。目前已经存在一些风险点，比如 AI 算法被欺骗导致自动驾驶预期功能隐患，AI 数据被污染导致车载智能模型变异等。

对此，给出了保障智能汽车安全的“十大原则”。一是点面结合防范风险；二是运营为王；三是不要迷信理论证明；四是人是薄弱环节；五是建立可信、安全、可控、可对抗、可生存的安全体系；六是全过程落实安全策略；七是高度重视安全建设中的三个关键点加个顶、打好座、要有气，即要有顶层设计，建设安全共性基础平台，通过持续运营和开放创新保持安全体系的生命力；八是以安全大脑为核 心；九是

建立协同网络；十是不断创新。

https://www.freebuf.com/343868.html

2、白硕：通过数据安全流通与增值促进数据要素市场发展

9 月 3 日，2022 世界人工智能大会“数据要素流通技术前沿探索论坛”在上海举行，白硕从技术角度分析了如何打通融合数据要素，实现数据的流通与增值以及元宇宙中如何通过稀缺性技术对虚拟物进行定价以及组合增值。

关于如何实现数据流通，白硕提出了数据要素目录共享。白硕表示，要解决数据要素交易增值问题，就是要把数据要素相互融合、打通，从而形成增值效应。“在数据具体内容隐私保护的情况下，我们可以形成统一的数据要素目录，例如格式、字段、简要说明等，通过目录对数据要素定价。数据要素目录共享后，可以形成要素图谱，数据经过流通组合和多方拼接，进而形成价值高的数据要素。”

此外，白硕还对未来元宇宙世界里，如何实现虚拟物的交易提出了自己的观点。白硕认为，要走向真正的元宇宙，其核心是虚拟物在协议层面的互联互通互操作，虚拟物交易就是其中重要一环。虚拟物本质上就是数据，其交易便是数据交易的一种。虚拟物的产生需要各种区块链、NLP、VR 等技术的结合，虚拟物的技术参数就是数据要素。因此，虚拟物的规格

和特性可以通过要素图谱发布,虚拟物的定价也可以通过稀缺性技术决定,二者有机结合。

https://www.jiemian.com/article/8025930.html

3、杨鹏飞：强化网络和数据安全守住数字政府生命线

9 月 5 日上午,2022 年广东省网络安全宣传周正式启动。在线上开幕式暨网络安全高峰论坛上，杨鹏飞提到广东构建网络和数据安全防护体系重点推动的六项工作,主要包括“发布全国首个省级数字政府网络安全体系总体规划”“建立健全网络安全和数据安全管理制度体系”“持续完善数字政府网络安全和数据安全保障体系”“建立健全个人信息保护机制”“打造粤盾数字政府网络安全品牌”“全国率先发布省级数字政府网络安全指数”等。

杨鹏飞还从四个层面阐述完善数字政府网络安全和数据安全保障体系，包括建立数字政府纵深的网络安全技术体系；建立覆盖网络攻击发现、通报、处置、溯源、打击全流程的省市一体化安全运营平台；强化应用安全，政务信息系统从需求设计到上线运行，各个阶段都配以相应的安全措施，系统设计、开发和数据安全保护同步规划、同步实施；针对数据采集、传输、存储、处理、共享、销毁的全生命周期，按照人防、物防、技防“三防”并举，从防护、脱敏、加密和

审计四个维度，开展数据安全保障工作，提升数据安全能力。

此外，从保障机制、人员管理、监督检查等方面加强个人信息保护。定期组织开展针对个人信息保护监督检查，评估政务应用在收集、使用个人信息方面存在的风险，迅速推动整改。

http://www.echinagov.com/news/329244.htm

4、席月民：推进公共数据开放共享的立法进路

近日，中国社会科学院法学研究所经济法室主任对推进公共数据开放共享发表了观点。

席月民提出相较于“政府数据”、“政务数据”，“公共数据”的内涵更丰富，外延也更广，它不但与国家“十四五”规划用语保持一致，有利于建立健全国家公共数据资源体系，而且通过预置公共服务的概念要素，更有利于推动公共数据开放共享及其实际应用创新。

他认为，数字经济立法必须适应信息社会法律变革新趋势。面对当前数字经济和数字法治政府发展中“先地方、后中央”立法进路中的“地方主导”问题，我们需要克服地方立法的固有局限性，积极回应统一建构公共数据开放共享法律制度的现实需求，及时制定统一的《公共数据开放共享条例》。

https://www.ciiabd.org.cn/articles/p9W2LV.html

5、加强数据治理 守护数据安全

日前，工信部相关负责人表示，工信部将加强数据安全工作的系统布局谋划，抓好数据安全监管体系建设，发展好数据安全产业，为国家数据安全保障提供有力支撑。加强数据治理、保护数据安全，为数字经济持续健康发展筑牢安全屏障，是时代发展的客观需要。

如何合理开发利用、保护好数据这个记录公众生活的“密码本”，自然成为题中应有之义。对此，需要整合多方资源，推动企业自律、政府监管与市场调节形成合力，构建系统性、整体性、协同性的数据安全多元共治生态，更好地服务于数字经济发展。

首先，要探索监管与市场服务相结合的安全治理体系。应建立安全可控、弹性包容的数据要素安全治理制度，为数字经济夯实前行道路。应鼓励数据安全产品与服务业发展，提高数字安全投入水平。相关部门与单位应明确强化数字经济安全风险防范的职责，促进数字经济均衡有序发展。

其次，要增强数据安全方面立法的操作性。应进一步细化数据安全立法的相关规定，尽快制定相应的配套实施条例和办法、指南，明确数据分类分级保护、数据安全风险评估、数据安全应急处置机制等方面的条件、标准和程序。创新监

管方式，将数据安全监管与社会信用体系建设联合起来。

再次，要积极推进数据要素市场化配置。加快建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场的进程，促进信息价值发现，保障数据交易的合法性，增强信息流动性，提高获取数据的便利性，推动数据行业健康发展，助力我国抢占全球数字竞争制高点。

最后，在加强数据安全治理的同时，还要努力促进中小企业创新，让全社会共享数字经济发展成果。在信息社会，数据是创新的基础。有关部门应当做好数据区分与数据甄别，要让数据使用者为其行为承担相应的责任，允许鼓励合法合规的数据流通，从而激发数据的创新性再利用，确保个人和国家安全。

http://www.gxorg.com/caijing/cfgs/2022/0903/42193.html

数据安全事件

1、250 万学生贷款记录因违规泄露

据外媒报道，EdFinancial 和俄克拉荷马州学生贷款管理局 (OSLA)已承认，超过 250 万学生用户的个人数据和贷款记录遭泄露，目前正在陆续通知受害者。

根据其披露的违规信息，造成此次数据泄露的主要元凶是 Nelnet Servicing 公司——一家服务系统和网络门户提供商，为 OSLA 和 EdFinancial 提供相应的服务。

调查结果显示，个人用户信息已经被未经授权的第三方访问，数据泄露已成定局。此次事件中泄露了 250 万学生贷款记录，以及账户持有人的姓名、家庭住址、电子邮件地址、电话号码和社会保险号码，个人财务信息没有泄露。

https://www.secrss.com/articles/46381

2、Instagram 因违反 GDPR 滥用儿童数据被爱尔兰罚款 4 亿美元

2022 年 9 月 6 日报道，Instagram 因违反 GDPR 被爱尔兰数据保护委员会(DPC)罚款 4.02 亿美元。DPC 表示，Instagram 允许 13-17 岁的儿童建立商业账户，这可使这些儿童的信息被公开。并且其用户注册系统中儿童用户的帐户默

认设置为公开，从而公开了此类用户的社交媒体内容，用户必须手动将帐户设置为私人。Instagram 的母公司 Meta 对罚款的计算方式提出异议，称其不符合 GDPR 的文本，导致罚款明显高于其它与 GDPR 相关的罚款，并打算对该指控提出上诉。

https://therecord.media/instagram-appealing-400-million-fine-from-ireland-data-privacy-org-over-gdpr-violations/

3、俄罗斯法院批准对谷歌处以 3.6 亿美元罚款：屡次未删除非法内容

2022 年 9 月 9 日消息，据报道，俄罗斯一法院裁定，支持对谷歌处以 217 亿卢布（约合 3.57 亿美元）的罚款，原因是俄罗斯子公司屡次未按要求删除被俄罗斯视为非法的内容。

据悉，俄罗斯国家通信监管机构“联邦通信、信息技术和大众媒体监督局”（Roskomnadzor）向谷歌发送了 17 条通知，要求谷歌删除一些不准确的信息，但谷歌并未遵守。

由于一再未能删除被俄罗斯视为非法的内容，谷歌早在 2021 年 12 月就被莫斯科一家法院处以 72 亿卢布的罚款。这也是俄罗斯在此类案件中，首次基于营收对一家企业做出罚款。

https://www.ithome.com/0/640/159.htm

4、西北工业大学遭网络攻击，源头系美国国家安全局

9 月 5 日，国家计算机病毒应急处理中心和 360 公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告，调查发现，美国国家安全局下属的“特定入侵行动办公室”多年来对我国国内的网络目标实施了上万次的恶意网络攻击，控制了相关网络设备，疑似窃取了高价值数据。本次调查还发现，在近年里，美国国家安全局下属的“特定入侵行动办公室”对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备，包括：网络服务器、上网终端、网络交换机、电话交换机、路由器、防火墙等，窃取了超过 140GB 的高价值数据。目前，联合专案组已将相关调查结果上报国家有关部门。这次突发案件再次警醒全球，数据安全的威胁必须引起重视，特别是对于高价值数据，在存储和传输过程中都有可能被恶意窃取。

https://mp.weixin.qq.com/s/0ReOzQMM5GS4xXRUPpKCvA

5、乔治亚州的艺术学院被勒索软件攻击致数据泄露

2022 年 9 月 6 日，据外媒报道，萨凡纳艺术与设计学院 (SCAD) 美国乔治亚州著名的艺术学校，有 15,000 多名学生，

该学院遭受了勒索软件攻击，泄露了数百人的敏感信息。

学校的一位发言人表示，一名黑客获得了对 SCAD 信息网络系统的访问权限。SCAD 有理由相信，未经授权的行为者访问的包含某些现任和前任学生和员工个人信息的文件数量有限。

上周末，AvosLocker 勒索软件组织将 SCAD 添加到其泄密站点，让学校有两周的期限支付未公开的赎金。该组织声称窃取了电话号码、电子邮件地址等数据库。专家发现该组织设法获取了至少 69,000 个包含学生信息、人事档案和业务数据的文件。

https://therecord.media/ransomware-attack-on-leading-georgia-art-college-leads-to-data-leak/?web_view=true

6、Vice Society 勒索软件团伙声称攻击了洛杉矶联合大学 LAUSD，并盗窃 500GB 数据

2022 年 9 月 9 日，Vice Society 团伙声称在上周末袭击了美国第二大学区洛杉矶联合大学 (LAUSD)并在使用勒索软件加密之前从受感染的 LAUSD 系统中窃取了 500 GB 数据，但拒绝提供被盗数据的证明。

https://www.bleepingcomputer.com/news/security/vice-society-claims-lausd-ransomware-attack-theft-of-500gb-of-data/

7、葡萄牙武装总参谋部遭网络攻击，数百份北约机密文件泄露

Security Affairs 网站披露，葡萄牙武装部队总参谋部（EMGFA）遭到网络攻击，黑客窃取了大量北约机密文件，直到美国发现几百份文件在暗网上出售并通知葡萄牙相关机构，后者才意识到自身遭受了网络袭击。

从初步调查结果来看，暗网上出售的文件是从 EMGFA、秘密军事（CISMIL）和国防资源总局的系统中流出。此外，调查人员还发现，传输机密文件的安全规则已经遭到了破坏，攻击者能够轻松进入军事通信综合系统（SICOM）并接收和转发机密文件。

https://hackernews.cc/archives/41412

8、DESORDEN 入侵印尼公司 BOGA Group 窃取数十万条记录

据媒体 9 月 2 日报道，黑客团伙攻击了印度尼西亚的一家大型企业 BOGA Group。该公司在印度尼西亚和马来西亚经营着超过 200 家餐厅和奥特莱斯。攻击者声称，为了证明已入侵该公司的服务器，其在下载数据后还在服务器上删除了这些数据。此次攻击窃取了超过 31 GB 的数据和文件，包括 409168 条客户信息（姓名、电话和电子邮件）、16476 条

员工以及财务和公司数据。DESORDEN 还表示，他们预计会对韩国、中国台湾、越南和日本进行更多攻击，并对泰国的数据感兴趣。

https://www.databreaches.net/customer-data-from-hundreds-of-indonesian-and-malaysian-restaurants-hacked-by-desorden/

9、20 万个 North Face 账户在撞库攻击中被黑

2022 年 9 月 7 日，户外服装品牌“The North Face”成为大规模撞库攻击的目标，该攻击导致 thenorthface.com 网站上的 194,905 个账户遭到黑客攻击。可能访问了以下客户信息：全名、购买历史、账单地址、收件地址、电话号码、账户创建日期、性别、XPLR Pass 奖励记录

信用卡数据等支付细节不会存储在网站上，因此攻击者无法访问敏感的财务信息。

https://www.bleepingcomputer.com/news/security/200-000-north-face-accounts-hacked-in-credential-stuffing-attack/

10、20.5 亿条数据泄露？TikTok 否认遭黑客攻击

2022 年 9 月 6 日，据 BleepingComputer 报道，TikTok 近日否认遭黑客入侵及源代码和用户数据被盗，黑客论坛泄露的 20.5 亿条数据与该公司“完全无关”。

上周五，一个名为“AgainstTheWest”的黑客组织在一个黑客论坛发帖声称已经入侵了 TikTok 和微信，并公布了一个 Tiktok 和微信的数据库屏幕截图，声称该数据库是在一个包含 TikTok 和微信用户数据的阿里云实例上访问的。

该黑客组织表示，该服务器在一个 790GB 的庞大数据库中保存了 20.5 亿条记录，其中包含用户数据、平台统计信息、软件代码、cookie、身份验证令牌、服务器信息等。

TikTok 表示，该公司被黑客入侵的说法是错误的，在黑客论坛上共享的源代码不是其平台的一部分，TikTok 的后端源代码从未与微信数据合并。TikTok 还指出，泄露的用户数据不可能是直接抓取其平台造成的，因为它们有足够的安全保护措施来防止自动脚本收集用户信息。

https://mp.weixin.qq.com/s/d-FmZmPGKCSjhKlv998qAQ