全球数据安全观察

总第 92 期 2022 年第 20 期

（2022.06.06-2022.06.12）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、两部门发布数据安全领域认证实施规则

6 月 9 日，据国家网信办官网消息，国家市场监管总局、国家网信办发布《关于开展数据安全管理认证工作的公告》（下称“公告”）。

公告显示，国家市场监管总局、国家网信办决定开展数据安全管理认证工作，鼓励网络运营者通过认证方式**规范网络数据处理活动，加强网络数据安全保护**。从事数据安全管理认证活动的认证机构应当依法设立，并按照《数据安全管理认证实施规则》（下称“《实施规则》”）实施认证。

《实施规则》以 GB/T 41479《信息安全技术 网络数据处理安全要求》及相关标准规范为认证依据，规定了对网络运营者开展**网络数据收集、存储、使用、加工、传输、提供、公开**等处理活动进行认证的基本原则和要求。此外，《实施规则》明确，认证模式为“技术验证+现场审核+获证后监督“。认证证书有效期为 3 年。证书到期需延续使用的，认证委托人应当在有效期届满前 6 个月内提出认证委托。

https://mp.weixin.qq.com/s/BTXIatcNMqjv0STspU2qBQ

2、上海发布《新型数据中心“算力浦江”行动计划（2022-2024 年）》

近日，上海市通信管理局在官微“上海通信圈”发布了《新型数据中心“算力浦江”行动计划（2022-2024 年）》（以下简称“《行动计划》”），表示将通过构建高性能算力为主的多元算力服务生态体系，依托上海新型互联网交换中心平台交换架构的独特性，探索打造全国首个算力交易集中平台，助力上海打造国际数字经济标杆城市。

《行动计划》中明确指出，到 2024 年，上海市数据中心总算力规模将超过 15EFLOPS，高性能算力占比达到 35%，人均可用智能算力超过 220GFLOPS/人，上海枢纽节点内数据中心端到端单向网络时延小于 15 毫秒。

《行动计划》将持续统筹优化建设布局作为重点任务之一。一方面，将加快建设新型数据中心集群，应建尽建，数据中心单体机柜功率不低于 6kw;另一方面，布局边缘中心，在五大新城、重点产业聚集区规划布局 3 个以上数据中心;同时，探索布局国际数据中心，满足合规跨境数据存算需求。

https://mp.weixin.qq.com/s/Hkzt2bKYeugzaVYo4Yx1GA

3、《四川省数据条例（草案）》提请一审，探索建立公共数据授权运营机制

6 月 7 日，备受关注的《四川省数据条例(草案)》(以下简称“条例草案”)提请四川省十三届人大常委会第三十五次会议首次审议。

结合四川省数据管理现状和需求，条例草案强化了地方政府及其有关部门数据管理的主体责任，确保各司其职、各负其责、共同发力，从体制机制上营造促进数字化发展的良好条件。同时提出，**建立以公共数据为主的数据资源体系，明确全省建立公共数据资源体系，实行统一目录管理；制定完善数据相关标准，规范数据收集和汇聚方式，确保数据依法产生并有效汇聚整合**。如何促进数据要素有序流通？条例草案提出，建立公共数据共享、开放机制，推动公共数据在各地区、各部门间共享和依法对社会开放，探索建立公共数据授权运营机制，满足政府、产业、社会数据需求；统筹规划数据要素市场，完善数据交易规则，发展数据资产评估、交易中介服务等市场运营体系；落实国家战略要求，在公共数据共享、标准互认、政务协同等领域与重庆市开展合作，推动区域数据协同发展。

聚焦数据资源高效开发利用，条例草案明确全省统筹规划基础设施布局，构建高效协同、智能融合的基础设施支撑

体系；围绕资金、人才、科研、生产要素等方面制定保障措施，明确对数据领域新业态实行包容审慎监管，培育数字核心产业集群；加强数字技术发展运用，推动数字经济与实体经济融合，加快数字产业化和产业数字化协同发展，提升公共服务和社会治理效能，全面推进数字四川建设。

加强数据安全管理和个人信息保护备受关注，条例草案也给予着重关注，**提出建立数据安全责任制，明确政府部门和数据处理者数据安全管理的职责义务；建立分级分类保护、风险防范预警、应急处理机制和安全评估监管等制度，构建完备的安全防护体系，筑牢数据安全底座**，严格落实上位法对个人信息保护的规定。

https://mp.weixin.qq.com/s/yvxkh-2ITIjjRrcKVIowDg

4、《厦门经济特区数据条例（草案征求意见稿）》

6 月 2 日厦门市发布《厦门经济特区数据条例（草案征求意见稿）》，公开征求意见。条例从数据资源、数据要素市场、数据安全、应用与发展、法律责任等方面做出规定，为促进数据作为生产要素在市场中发挥作用、推动数字经济的发展提供法治保障。

其中提到对首席数据官、公共数据资源平台、数据交易和数据平台等内容。首席数据官：在本市政务部门和公共服

务组织探索建立首席数据官制度。首席数据官由单位相关负责人担任，协同管理数据工作与业务工作，提升本单位的数字化管理能力和管理水平。公共数据资源平台：市大数据主管部门设立公共数据资源平台，作为本市公共数据汇聚、共享、开放的统一基础设施。政务部门、公共服务组织不得新建其他跨部门的公共数据共享、开放平台或者系统；已经建成的，应当按照有关规定进行整合。信用数据产品和服务交易板块：本市支持信用数据按照国家和省的有关规定进行市场化开发与运用，探索设立专门的信用数据产品和服务交易板块。数据银行：探索设立数据银行及相关机构，鼓励自然人、法人和非法人组织自愿地将其数据依法提交到数据银行，由数据银行依法进行存储、管理、经营和处理。探索建立数据的知识产权保护制度。

https://mp.weixin.qq.com/s/9jL03_dTOSWksazy49Zy0Q

5、全国首批“数据经纪人”诞生

日前，经广东省政数局批准同意，广州市海珠区率先推出全国首批“数据经纪人”名单。首批入选的3家“数据经纪人”试点企业分别是广东电网能源投资有限公司、广州金控征信服务有限公司、广州唯品会数据科技有限公司。这3家企业分别涉及电力行业、电子商务、金融等领域，均拥有丰富

的社会数据和成熟的运营经验。

据介绍，数据经纪人是在政府的监管下，具备开展数据经纪活动资质的机构。该机构要具备生态协同能力、数据运营能力、技术创新能力、**数据安全能力**和组织保障能力，围绕重点领域开展数据要素市场中介服务，推动数据流通规范化。

数据经纪人主要有三方面的职责：一是受托行权，即数据拥有者可以授权数据经纪人行使权力；二是风险控制，在数据流通交易过程中起到中介担保作用；三是价值挖掘，挖掘数据要素价值，充当数据价值发现者、数据交易组织者、交易公平保障者、交易主体权益维护者等多重角色。

明晰“数据经纪人”概念后，接下来要解决的就是如何选取“数据经纪人”。经海珠区政务服务数据管理局深入研究，海珠区首创了“数据经纪人”分类分级标准：

根据“数据经纪人”自身基础及业务范围可划分为技术赋能型、数据赋能型、受托行权型三个类别；

按照企业数据管理能力成熟度等级、信息安全等级保护等级、企业自有（或实际控制）数据规模等条件，以及相关试点企业数据采集和处理是否符合国家相关安全要求等因素，将“数据经纪人”分为三个等级。

https://mp.weixin.qq.com/s/T-cFzCabDDBfZzNBLaqA-Q

6、“中国+中亚五国”数据安全合作倡议

6月8日，“中国+中亚五国”外长第三次会晤在努尔苏丹举行。会晤通过《“中国+中亚五国”数据安全合作倡议》。摘要如下：

中华人民共和国、哈萨克斯坦共和国、吉尔吉斯共和国、塔吉克斯坦共和国、土库曼斯坦、乌兹别克斯坦共和国（以下简称各方）欢迎国际社会在支持多边主义、兼顾安全发展、坚守公平正义的基础上，为保障数据安全所作出的努力，愿共同应对数据安全风险挑战并在联合国等国际组织框架内开展相关合作。中亚各国支持中方提出的《全球数据安全倡议》。

各方一致认为：信息技术日新月异，数字经济蓬勃发展，深刻改变着人类生产生活方式，对各国经济社会发展、全球治理体系、人类文明进程影响重大。作为数字技术的关键要素，全球数据爆发增长，海量集聚，成为实现创新发展、重塑人们生活的重要力量，事关各国安全与社会经济发展。各方呼吁，各国应秉持发展和安全并重的原则，平衡处理技术进步、经济发展与保护国家安全和社会公共利益的关系。各方重申，各国应致力于维护开放、公正、非歧视性的营商环境，推动实现互利共赢、共同发展。与此同时，各国有责任和权利保护涉及本国国家安全、公共安全、经济安全和社会

稳定的重要数据及个人信息安全。各方强调，应在相互尊重基础上，加强沟通交流，深化对话与合作，共同构建和平、安全、开放、合作、有序的网络空间命运共同体。

https://mp.weixin.qq.com/s/odDz4ElewLe_ngVGTQcRxA

7、美国联邦层面数据隐私法草案面世

近日，美国首个获得两党、两院支持的联邦层面数据隐私法草案——《美国数据隐私和保护法》（草案）（American Data Privacy and Protection Act，ADPPA）面世。除特定情形，草案拟禁止收集生物识别信息、互联网浏览历史、社会安全号码等。

草案主要有四个部分，分别为忠诚义务、消费者权利、企业问责制以及执法部分。具体而言，草案内容包括防止美国人的数据遭到歧视性使用、要求相关实体允许消费者关闭定向广告、为未成年人提供增强的数据保护、要求信息处理者在特定实践方面遵守忠诚义务，同时确保消费者不必为隐私付费等。所谓忠诚义务（duty of loyalty），主要是指信息处理者不得收集、处理、转让超过合理必要的个人信息。在有关“忠诚义务”方面，除了一些草案中规定的特定情形，原则上不得收集、处理或转移社会安全号码、不得将个人的精确地理位置信息转移给第三方、不得收集、处理或转移生

物识别信息、不得转移个人的综合互联网搜索或浏览历史记录、不得从智能手机或可穿戴设备上转移个人的生理活动信息。在消费者权利方面，草案拟规定数据处理需有“透明度”、个人数据所有权和控制权、同意权、未成年人的数据保护、算法公平、数据安全等。关于企业责任，草案拟规定，所有相关企业任命一名或多名隐私官/数据安全官，以负责建立定期审查和更新隐私政策等流程。大数据持有者（large data holder）还需要进行隐私影响评估，权衡数据收集处理与转让对个人隐私的潜在不利影响。所谓大数据持有者为年总收入超过 2.5 亿美元，同时收集、处理、转让超过 500 万个人数据，超过 10 万个人敏感数据。

另外，草案要求美国联邦贸易委员会（FTC）建立一个与消费者保护和竞争相关的新的部门，州检察长或州首席消费者保护官员可以以州的名义提起民事诉讼，同时也赋予个人在法案生效后四年内行使私人诉讼权。

https://mp.weixin.qq.com/s/NvAOAx3A3YiOhYQUmynKRA

技术、产品与市场

1、《2022 数据安全产业洞察报告》发布

数据安全之争，是国家之争、大道之争。数据安全是指通过采取必要措施，保障数据得到有效保护和合法利用，并使数据持续处于安全状态的能力。数据作为新型生产要素，正深刻影响着国家经济社会的发展。数据安全保障能力是国家竞争力的直接体现，数据安全是国家安全的重要方面，也是促进数字经济健康发展、提升国家治理能力的重要议题。

展望“十四五”时期，我国数字经济转向深化发展新阶段，为应对安全新形势、新挑战，数据安全理念内涵、技术产品、产业格局等都将迎来关键变革。在产品和技术创新中，需要产业上中下游通力配合，在模型框架、平台设计、技术实现、服务模式中勇于创新，在数据处理各个环节、各个节点、各类处理者提供完整方案，减少数据安全社会治理短板。我国网络安全与领先国家存在一定差距，但数据安全的差距并没有这么大，所以有望抓住“换道超车”的历史机遇，在数据安全领域追赶乃至超越领先国家。

https://mp.weixin.qq.com/s/U-4dqtaIc77aPspiOg9XXA

2、网络安全人才供需严重失衡，预计 2027 年缺口将扩大到 300 万人

据数据显示，2016 年，我国网络安全市场规模为 336.2 亿元；而 2021 年，市场规模达到 900 多亿元。然而，在这 5 年近 3 倍的高速增长背后，却是网络安全行业人才供需失衡——如今，国内网络安全专业人才累计缺口超 140 万人，首席安全官（CSO）更是整个网络安全行业中的极度稀缺人才。

网络安全人才十分稀缺，而每年网络安全相关专业的高校毕业生规模仅两万余人，由此可见，我国网络安全人才供给存在“青黄不接”的情况，人才成长和培养速度显著落后于技术与社会变革的整体速度。现阶段由于行业发展特点，人才队伍呈现底部过大，顶部过小的结构，即从事运营与维护、技术支持、风险评估与测试的人员相对较多，从事战略规划、架构设计的人员相对较少，尤其缺乏既懂业务懂政策、又懂技术懂管理的高端综合型人才。

https://mp.weixin.qq.com/s/ESbe6lnq_yGyJEBuh5N3QA

3、隐私计算重要技术突破，亿级数据密态分析可在 10 分钟内完成

据全球知名知识产权机构 incoPat 动态，蚂蚁集团隐私计算创新技术可信密态计算（Trusted-Environment-based

Cryptographic Computing，简称 TECC）近日再获一项“分布式多方安全计算系统、方法和节点”（公告号 CN113992439B）专利授权。

该技术根据资源消耗和任务可并行拆分程度的不同，可将 TECC 的计算速度提升 10 倍到 100 倍，实现在 1 小时内完成亿级样本密态 GBDT（Gradient Boosting Decision Tree，一种树模型集成算法）建模训练，在 10 分钟内完成亿级数据密态 SQL 分析，可以为顶级数据规模带来非常友好的计算体验，达到了隐私计算现阶段最佳性能效果，也使得 TECC 计算效率接近于数据非加密的明文计算。

TECC 技术的核心突破是，在远程验证的 TPM/TEE 环境中使用高速全密文计算，一方面在性能、可靠性、适用性等方面比传统跨网隐私计算(MPC/联邦学习）有显著提升，另一方面能够有效抵抗困扰 TPM/TEE 的供应链攻击、侧信道攻击、明文数据泄露风险，同时有效抵抗困扰多方安全计算和联邦学习的合谋攻击、恶意敌手攻击与信息熵泄露风险。与其他隐私计算技术相比，TECC 更加适用于对数据安全需求高（如重要数据）、数据规模大（如百万个人信息）、计算逻辑复杂、参与方数量不固定的场景，并支持跨地域数据中心的密态计算需求。

https://mp.weixin.qq.com/s/CMnF-rBdOeZQqgXdgMo9AA

4、企业级开源隐私计算平台—Primihub 正式开源

原语科技自主研发的隐私计算平台 **Primihub** 现已正式在 **GitHub** 平台上开源，Primihub 开源官网：**http://docs.primihub.com/**。Primihub 是由原语科技集结众多技术骨干，联合 Primihub 社区伙伴的支持，从 0 到 1 自主研发打造的隐私计算平台，秉承保护数据在应用过程中的隐私安全，实现“数据可用不可见”。

Primihub 平台融合了 MPC（多方安全计算）、FL（联邦学习）、HE（同态加密）、TEE（可信执行环境）等多种技术路线，提供多安全级别、多性能要求、多场景支持的解决方案，帮助企业用户保护数据隐私的同时，深度连接各个合作方，实现跨数据、跨行业的合作共赢。在提供开源版的同时，原语科技研发了企业版，支持更加丰富的功能。

https://mp.weixin.qq.com/s/Y4-Qhwpwr4wPpPuxodkgXw

5、加拿大公司发布全新数字量子密钥分发技术

6 月 6 日至 9 日，在美国加州旧金山举行的 RSA 大会现场，Quantropi 公司展示了其最新的量子安全加密产品 SEQU SynQK，用于生成和数字分发同步量子密钥。

Quantropi 的 SEQU SynQK 有效地打破了几个世界记录，在 4000 到 15000 公里的距离内以 130 到 190 兆每秒的速度

同时传送至少 5 个量子密钥流(5 个数据流中的每一个都相当于 Google.com 每秒使用的 8 - 12 倍)。

SEQUR 是 Quantropi 的 TrUE 加密解决方案系列中的熵产品，此产品系列提供量子密钥生成和分发功能。目前，该系列产品包括 SEQUR QEaaS、SEQUR NGen 和最新发布的 SEQUR SynQK。

https://mp.weixin.qq.com/s/MtSjaLYGNCl1LIhN3fEBLg

业界观点

1、专家共议加快构建数字经济安全保障体系

日前，中国信息协会信息安全专业委员会、北京天空卫士网络安全技术有限公司联合在京发布《数据防泄露技术指南》，旨在通过构建标准防范体系，助力形成完善的数据防泄露解决方案。来自信息安全产业、数据安全领域的多位专家就提升数据安全管理能力、加快构建数字经济安全保障体系等问题，展开了探讨。

在国家信息中心信息与网安部副主任禄凯看来，保障数据安全不仅涉及公民个人隐私，还涉及企业长远发展和网络安全。“数据资产保护不仅要解决数据泄露风险，还要控制和降低业务风险。通过对数据确权、分类、分级保护，落实数据安全责任制，践行数据安全法和个人信息保护法要求，为实现数字化建设和数字化转型赋能。”

数据防泄露贯穿数据生命周期全过程。“从数据的生成开始，到数据的存储、应用、传输、备份归档到数据的销毁，每个步骤都要有相应的数据防泄露技术作为支撑。”中国信息协会信息安全专业委员会主任叶红认为，数据泄露防护市场需求迫切，应从用户的角度，围绕应用场景和数据处理各环节，明确数据防泄露的策略、技术和方法，这将对数据安全

治理产生很好的促进作用。

“数据分为一般数据、重要数据、核心数据，对数据进行分类分级的前提是识别敏感数据。”中国科学技术大学网络空间安全学院教授左晓栋介绍，当前，数据分类分级制度正逐步建立，全国信息安全标准化技术委员会已立项制定国家标准《重要数据识别指南》。下一步，地方、行业要结合自身特点，基于国家标准制定地方或行业标准、规范，进一步明确重要数据的特征，为数据的分级分类提供支撑。

https://www.scdsjzx.cn/scdsjzx/zuixinzixun/2022/6/13/d674bf29a4664246b95a71acfe5baec6.shtml

2、毛群安：推进卫生健康行业数据安全规范管理

国家卫生健康委规划发展与信息化司司长毛群安在 6 月 9 日“卫生健康数据合规实践与前瞻”研讨会致辞中指出，在我国全民健康信息化发展迅速、国家有关数据安全的法律体系不断完善的背景下，探讨医疗健康数据合规问题，具有重要意义。

毛群安表示，规划司作为承担行业发展规划和信息化顶层设计的部门，在“十四五”期间，将继续坚持需求导向与问题导向，在大力推进健康中国、数字中国两大战略的时代背景下，乘着数字产业升级的大势，精心谋划、科学部署，为

行业发展制定“作战图”。同时，处理好发展与安全之间的关系，织密行业发展的安全网，助推行业的规范、可持续发展。

他进一步提到，规划司正在推进卫生健康行业数据安全管理规范，建立行业数据安全管理配套规章制度和标准规范。委托中国社科院法学所开展“卫生健康行业网络数据安全管理规范研究”的课题研究，希望通过第三方梳理行业痛点与难点，提出有关建议。

https://finance.eastmoney.com/a/202206102408714476.html

3、周汉华：通过“法律+技术”促进卫生健康数据治理现代化

中国法学会网络与信息法学研究会负责人、中国社会科学院法学研究所副所长、“卫生健康行业网络数据安全管理规范研究”课题组组长周汉华在卫生健康数据合规实践与前瞻”研讨会上致辞时提到，“今天我们讨论健康医疗大数据产业的数据安全管理规范以及合规问题，实质上就是讨论如何在健康医疗大数据产业中全面精准科学地实施《网络安全法》《数据安全法》《个人信息保护法》等法律。”周汉华说，该领域仍有许多问题值得关注，包括但不限于以下三方面：

一是数据分类分级问题。健康医疗大数据产业亟**需进一步细化数据分类分级制度**，全面梳理本行业的一般数据、重要数据、核心数据，对不同级别的数据采取不同的保护措施。

二是数据跨境问题。健康医疗大数据产业涉及大量数据出境场景，如学术交流、国际合作、科研成果发表等，同时我们在研究中发现，目前许多医院的影像检查设备、化验检验设备、病历管理系统等大部分还是由国外企业提供，其中将不可避免涉及到**数据出境问题，需要进一步完善制度**。

三是数据全生命周期安全管理。医疗数据的收集、存储、传输、处理、使用、交换、销毁全生命周期安全管理工作中如何确保医疗数据处理过程中的安全性、保密性、完整性，如何防止医疗数据被窃取、篡改，需要**出台具体的和可具操作性的配套法规与政策**。

http://www.21jingji.com/article/20220610/herald/7824bb6105565d206e6dbeccd17abb53.html

4、何晶晶：卫生健康数据合规需要安全与利用并重

在卫生健康数据安全管理方面，中国社会科学院国际法研究所副研究员何晶晶指出卫生健康行业具有特殊性，在数据全生命周期中，涉及到个人敏感信息的数据可能会在不同的主体机构间流转，如何平衡数据的安全与利用是一个难点。未来可以通过先进的技术手段进一步探索解决方案，高效地实现平衡。

她强调，在卫生健康行业，系统性合规非常重要。“从数

据安全和个人信息保护的角度来说，行业涉及的每个主体与环节都做到合规，才能真正在全链条实现数据合规。”

此外，她建议对卫生健康数据进行分类分级保护，梳理一般数据、重要数据、核心数据，对不同级别的数据采用差异化保护措施，并定期开展安全风险评估。同时做好数据全生命周期安全管理。针对数据跨境场景，坚持数据本地化，保护数据安全和个人隐私。

在个人信息管理方面，打通不同医疗机构之间的信息共享渠道，实现互联互通。利用技术手段强化个人信息处理系统的安全措施，加强入侵防护。针对重要的网络节点，根据上位法的要求进行安全审计。

在监督与保障方面，事件上报机制是系统化流程，当出现数据泄露、损毁等事件时，主体机构应及时向有关主管部门提供相关线索。卫生健康数据安全管理应列入重要的议事日程，从人员、经费、制度上全方位落地。

在卫生健康数据合规文化建设方面，医疗机构应积极开展培训，在日常工作中强化员工数据合规意识，更好地了解隐私数据法律风险及合规处理方法。对于合规能力的评估，建议将医疗机构的评级考核与合规能力挂钩，比如将数据安全治理能力纳入三甲医院考评体系，使医疗机构有更大动力推进数据合规。

http://www.21jingji.com/article/20220610/herald/0577f9e45d316b81935cc678a4d93c8e.html

5、杨涛：数据要素市场建设需系统考量

据日前报道，国家发改委正在牵头制定数据要素基础制度文件。中国社科院金融所研究员杨涛表示，在数字化变革这一历史浪潮中，政府必须做好“善治善管”，才能更稳妥、快速推进数字中国建设。对此，杨涛认为需关注几方面：

一是目标导向，因为数据要素应用与数字化的目标可能是多元的，如服务公共管理、促进经济增长、就业优先、结构优化、可持续发展等，需要厘清目标的优先次序，否则可能出现目标冲突或矛盾，制约数字化实践顺利推进。

二是底线原则，必须明确数字化过程中需避免怎样的“双刃剑”效果，如大型数字平台的垄断、部分公共部门的数据垄断、个人信息被非法收集和滥用等，从而设置好数字化理论与政策的“负面清单”。

三是规则先行，数字化更需要尊重规则，从而稳定市场预期，既要探索和完善相应的法律法规，又要在短期内难以进行法律规制的领域，推动标准化的自律约束，以及数字伦理体系的建设，从而实现创新空间与发展有序的平衡。

四是方法科学，面对大数据杀熟、信息茧房、NFT 与 DeFi

（去中心化金融）等众多数字化新问题，政府自身也要积极拥抱数字化，跳出原有现场与非现场监管的局囿，运用数字化工具来应对数字化风险以及管理难题。

http://news.hexun.com/2022-06-08/206101607.html

数据安全事件

1、被指相册分类功能非法收集使用人脸数据，谷歌付一亿美元和解

2022 年 6 月 9 日报道，近日，美国伊利诺伊州库克县巡回法院宣布，谷歌就此前非法收集和存储伊利诺伊州居民的个人生物特征数据与多位集体诉讼原告达成和解协议，决定向受到影响的居民支付共计一亿美元的和解金，预计最多赔付每人 400 美元。该州居民需在 9 月 24 日前填写表格提出索赔申请。

2015 年 5 月，谷歌上线“相册分类”功能，该功能可通过识别照片内人物的面部特征，利用算法分析和模型创建判断不同人脸的相似度，将拥有相似人脸的照片归为一组。不过，谷歌并未就其中的信息收集行为向用户进行告知。这一功能引起了用户对生物特征数据安全的担忧。和解协议显示，2016 年 3 月起，伊利诺伊州用户针对相册分类功能对谷歌提起集体诉讼，指控谷歌在未获取用户书面同意的情况下非法收集、存储、使用用户生物特征数据，并认为此举违反了伊利诺伊州于 2008 年颁布的《生物特征信息隐私法》。

https://www.secrss.com/articles/43361

2、百度员工为发泄不满，刻意删改公司数据库被判刑

2022 年 6 月 8 日，根据北京法院审判网公布信息显示，百度一程序员为发泄对上司的不满，将公司数据库删改后被抓，判刑 9 个月。

2020 年八至九月，员工金某因对公司项目安排不满，将数据库的数据部分进行了篡改和删除，导致系统算法无法得出想要的结果，该行为严重影响了其部门工作的正常运转。同时，据公司同事证实，金某在商业质量效能部任职期间，由于对部门领导不满，使用隧道违规从外网接入百度 IDC 并对商业质量效能部 ff.baidu-int.com 平台数据库内表进行清空、篡改、锁定，造成严重后果。

金某的行为一方面导致平台数据不一致或丢失，共计影响了五十多个项目使用平台的快捷操作能力；另一方面，数据库的异常变化也给用户带来了不良体验，对公司形象及经济利益造成了恶劣影响。

https://www.wangan.com/p/7fy7fx344d495ae9

3、FBI 查封了出售数百万被盗 SSN 的臭名昭著的网络黑市

2022 年 6 月 8 日报道，美国执法部门宣布捣毁 SSNDOB，这是一个臭名昭著的网络黑市，用于交易数百万美国人的个人信息——包括社会安全号码即美国人最熟悉的 SSN。这次

行动由联邦调查局、美国国税局（IRS）和司法部（DOJ）在塞浦路斯警方的帮助下进行，查封了托管 SSNDOB 市场的四个域名--ssndob.ws、ssndob.vip、ssndob.club 和 blackjob.biz。

据司法部称，SSNDOB 列出了美国约 2400 万人的个人信息，包括姓名、出生日期、SSN 和信用卡号码，并借此产生了超过 1900 万美元的收入。

https://www.cnbeta.com/articles/tech/1278615.htm

4、美国的在线枪支商店被黑客入侵以窃取信用卡

2022 年 6 月 7 日，两家经营电子商务网站的美国枪支商店 Rainier Arms 和 Numrich Gun Parts 披露了由于其网站上的刷卡机感染导致的数据泄露。

信用卡浏览器是嵌入在网站上或通过看似无害的元素（例如 favicon ）从远程资源中获取的恶意 JavaScript 代码。他们的目的是窃取在订单结账页面上输入的付款信息。

这些撇油器的运营商可以窃取信用卡号、有效期、CVV 代码、客户姓名、电话号码和地址，而这些都是他们进行未经授权的在线购买所需的全部内容。

https://www.bleepingcomputer.com/news/security/online-gun-shops-in-the-us-hacked-to-steal-credit-cards/

5、医疗设备公司 Shields 泄露 200 万美国患者数据

2022 年 6 月 8 日报道，近日，美国医疗设备公司 Shields Health Care Group (Shields)遭遇黑客攻击，泄露了大约 200 万美国人的医疗数据。

Shields 是一家位于马萨诸塞州的医疗服务提供商，专门从事 MRI 和 PET/CT 诊断成像、放射肿瘤学和门诊手术服务。根据公司网站上发布的数据泄露通知，Shield 于 2022 年 3 月 28 日发现遭受网络攻击，对日志文件的检查表明，黑客在 2022 年 3 月 7 日至 2022 年 3 月 21 日期间可以访问 Shields 的系统，从而可能访问包含姓名、社会安全号码、诊断信息等的患者敏感数据。

Shields 声称没有证据表明任何被盗信息被滥用或通过非法渠道传播。不过，这些数据公开传播可能只是时间问题。通常，此类被盗信息会在网络黑市交易并用于小规模的针对性攻击，然后再转售给参与批量利用的较低级攻击者。

https://www.secrss.com/articles/43273

6、MyEasyDocs 暴露了 30GB 的以色列和印度学生 PII 数据

2022 年 6 月 9 日报道，位于印度的 MyEasyDocs 在线文档验证平台的 Microsoft Azure 服务器暴露了超过 57,000 名

学生的 30.5GB 文件数据。

由 Noam Rotem 领导的 vpnMentor 的 IT 安全研究人员团队发现了一个配置错误的 Microsoft Azure 服务器，该服务器暴露了来自印度和以色列的数万名学生的个人和教育记录，包括：成绩、姓名、专业、电话号码、电子邮件地址、毕业日期、身份证号/学号等。

https://www.hackread.com/myeasydocs-exposed-30gb-israel-india-students-pii-data/

7、土耳其航空运营商飞马航空遭遇数据泄露

2022 年 6 月 9 日据报道，在 AWS 云存储桶未受保护后，土耳其航空公司 Pegasus Airlines 遭受了数据泄露。据报道，属于未知数量客户的电子飞行包信息存储在开放式存储桶中，允许访问敏感信息。土耳其个人数据保护局的声明证实，有人未经授权访问了 Pegasus 持有的某些信息。据监管机构称，泄露的信息包括姓名、姓氏、电话号码、电子邮件地址、职务、过去旅程的航班信息、航班位置以及部分员工的照片和签名图像。根据披露违规行为的安全侦探的说法，在存储桶中发现了近 2300 万个文件，总计约 6.5 TB 的数据。

https://portswigger.net/daily-swig/turkish-flight-operator-

pegasus-airlines-suffers-data-breach

8、匿名者泄露 1TB 俄罗斯顶级律师事务所数据

2022 年 6 月 6 日消息，匿名者勒索团伙（Anonymous）再次袭击俄罗斯，泄露了一家名为 Rustam Kurmaev and Partners (RKP Law) 的俄罗斯顶级律师事务所大约 1TB 的数据。

根据匿名者在网站上发布的公告，泄露的数据包含文件、电子邮件、法庭文件、客户文件、备份文件、客户列表等。该律师事务所与主要银行、媒体、石油和工业公司以及包括美国公司在内的国家利益集团合作。考虑到该公司专门解决房地产、建筑、公司和商业部门的纠纷，数据泄露可能对公司造成毁灭性的影响。

https://www.hackread.com/anonymous-hacktivists-leak-1tb-russia-law-firm-data/

9、Emotet 的新模块可窃取存储在 Chrome 中的信用卡信息

2022 年 6 月 8 日报道，研究人员发现僵尸网络 Emotet 正在使用一个新的模块，来窃取存储在 Chrome 用户配置文件中的信用卡信息。它会收集姓名、信用卡到期年月和卡号等信息，然后会将这些信息发送到 C2 服务器，而不是该信

息窃取模块所使用的服务器。Emotet 于 2014 年开始活跃，在 2021 年初的一次国际执法行动中被拆除。ESET 在上周二透露，自今年年初以来，Emotet 的活动大幅增加，比 T3 2021 增长了 100 倍以上。

https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-credit-cards-from-google-chrome-users/

10、网络安全巨头 Mandiant 疑似遭到 Lockbit 勒索软件入侵

2022 年 6 月 6 日报道，LockBit 勒索软件团伙将网络安全公司 Mandiant 添加到其暗网数据泄露站点的受害者列表，并且声称从该公司窃取了 356841 个文件，不久将在网上泄露这些文件。据外媒报道称被盗文件似乎已包含在名为“mandiantyellowpress.com.7z”的文件中，访问 mandiantyellowpress[.]com 会将用户重定向到显示 ninja 和 flex 图像的站点 ninjaflex[.]com。截至目前，Mandiant 正在调查勒索软件团伙的指控，尚未披露具体细节。

https://securityaffairs.co/wordpress/132011/cyber-crime/lockbit-claims-mandiant-hack.html