

# 全球数据安全观察

总第 74 期 2022 年第 02 期

(2022.01.03-2022.01.09)

# 目录

<b>政策形势</b> .....	<b>1</b>
1、国务院办公厅印发《要素市场化配置综合改革试点总体方案》 .....	1
2、《2022 年度天津市公共数据资源开放计划清单》发布：释放公共数据价值，助力数字经济发展 .....	2
3、《国家大数据（贵州）综合试验区“十四五”建设规划》发布 .....	2
4、河南省人大通过《河南省数字经济促进条例》 .....	3
5、中国人民银行印发《金融科技发展规划(2022-2025 年)》 .....	4
<b>技术、产品与市场</b> .....	<b>5</b>
1、2022 年全球 IT 行业 10 大预测：网络安全、数字优先成为核心驱动力 .....	5
2、2022 中国数据安全十大发展趋势预测 .....	5
3、2022 年，哪些安全技术创新值得期待？ .....	6
4、《全球数据合规与隐私科技发展报告》发布：国内首提“隐私科技”概念 .....	7
5、海南省公共数据资源开发利用试点成果发布，数据产品超市上线 .....	8
6、2021 年商用密码发展呈现新变化 .....	9

**业界观点..... 10**

- 1、人民网评：进一步保障网络安全和数据安全 ..... 10
- 2、解读：《网络安全审查办法》与时俱进，修订后补充数据安全与海外上市管理 ..... 11
- 3、国标《重要数据识别指南》起草发生重大修改 ..... 11
- 4、王春晖：营造良好数字生态的三大法治基石 ..... 12
- 5、《互联网信息服务算法推荐管理规定》构建算法安全治理体系 ..... 13

**数据安全事件 ..... 14**

- 1、美国连锁酒店 McMenamins 披露遭勒索攻击，发生数据泄露 ..... 14
- 2、因违反欧盟隐私规定，谷歌脸书或被罚超 15 亿元 ..... 14
- 3、SlimPay 因泄露 1200 万银行数据被罚 18 万欧元 ..... 15
- 4、Broward Health 遭遇数据泄露，影响了 130 万人 ..... 16
- 5、美国无线运营商 UScellular 批露了数据泄露事件 ..... 16
- 6、新加坡百货公司奥奇（OG）数据库被入侵，会员资料外泄 ..... 17
- 7、印度医学会的推特账号被泄露 ..... 17
- 8、“掩盖”数据泄露，前 Uber 首席安全官被指控 ..... 18
- 9、黑客使用视频播放器从 100 个网站窃取信用卡 ..... 18
- 10、恶意软件 ZLoader 利用微软的数字签名验证窃取敏感信息 ..... 19

# 政策形势

## 1、国务院办公厅印发《要素市场化配置综合改革试点总体方案》

近日，国务院办公厅印发《要素市场化配置综合改革试点总体方案》，推动要素市场化配置改革向纵深发展。《方案》提出了八个方面试点任务，包括：进一步提高土地要素配置效率，推动劳动力要素合理畅通有序流动，推动资本要素服务实体经济发展，大力促进技术要素向现实生产力转化，探索建立数据要素流通规则，加强资源环境市场制度建设，健全要素市场治理，进一步发挥要素协同配置效应。

《方案》在“探索建立数据要素流通规则”方面中提出了四项任务：**一、完善公共数据开放共享机制。**建立健全高效的公共数据共享协调机制。**二、建立健全数据流通交易规则。**探索“原始数据不出域、数据可用不可见”的交易范式。**三、拓展规范化数据开发利用场景。**发挥领军企业和行业组织作用，推动人工智能、区块链、车联网、物联网等领域数据采集标准化。**四、加强数据安全保护。**强化网络安全等级保护要求。

<https://mp.weixin.qq.com/s/cOFrOPVKkdA4TFW-V-jr3A>

## 2、《2022 年度天津市公共数据资源开放计划清单》发布： 释放公共数据价值，助力数字经济发展

近日，为深入贯彻落实习近平总书记关于建设网络强国、数字中国的重要论述，整合多维、多源公共数据资源，推进行业数据价值挖掘，释放公共数据价值，助力数字经济发展，激发社会创新活力，培育数字经济新产业、新业态、新模式。天津市委网信办、天津市大数据管理中心联合发布《2022 年度天津市公共数据资源开放计划清单》（以下简称《开放计划清单》）。

《开放计划清单》主要对标先进省市，结合重点行业、特色领域和区域特点，汇总包括信用、交通、医疗、就业、社保、教育、环境、气象、企业登记监管等民生保障服务相关领域的**政务数据向社会开放**。《开放计划清单》包括市级、区级两个部分。其中，市级部分收集了 47 个市级部门共 943 个开放计划目录；区级部分收集了 16 个区共 1104 个开放计划目录。

[https://mp.weixin.qq.com/s/bUOe\\_KmTEAPR0a8DzTx29A](https://mp.weixin.qq.com/s/bUOe_KmTEAPR0a8DzTx29A)

## 3、《国家大数据（贵州）综合试验区“十四五”建设规划》 发布

2022 年 1 月 6 日，贵州省政府新闻办组织召开的新闻发

发布会上发布了，“十四五”期间，国家大数据（贵州）综合试验区有 8 个方面试验任务。

8 个方面实验任务具体包括：迭代更新数字经济融合创新、数字政府治理创新、数字社会服务创新、数据要素市场培育、新型数字基础设施等五项任务；继承深化大数据制度创新大数据交流合作等两项任务；大数据安全保障试验任务。

<https://mp.weixin.qq.com/s/NZBOeBDMbFqz4C9N1Xu-rg>

#### 4、河南省人大通过《河南省数字经济促进条例》

河南省第十三届人大常委会第二十九次会议表决通过《河南省数字经济促进条例》，将于 2022 年 3 月 1 日起施行。《条例》从数字基础设施建设、数据资源开发利用、数字产业化发展、产业数字化转型、数字化治理和服务、数字经济促进措施、数字经济安全保障和法律责任等方面对数字经济的促进作出了规定。

条例指出，省人民政府及工业和信息化、发展改革、科技等有关部门应当统筹电子信息制造业发展，做好重大项目推进、产业链上下游对接配套、龙头骨干企业培育，打造电子信息制造优势产业集群。县级以上人民政府应当鼓励企业开放数字化应用场景，宣传数字经济文化，推广先进经验、成功模式。

<https://mp.weixin.qq.com/s/e4bqeUdKPUVLVBGAWA7T7w>

## 5、中国人民银行印发《金融科技发展规划(2022-2025年)》

近日，中国人民银行印发《金融科技发展规划(2022-2025年)》，《规划》依据《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》制定，提出新时期金融科技发展指导意见，明确金融数字化转型的总体思路、发展目标、重点任务和实施保障。

《规划》提出八个方面的重点任务。一是强化金融科技治理。二是全面加强数据能力建设。三是建设绿色高可用数据中心。四是深化数字技术金融应用。五是健全安全高效的金融科技创新体系。六是深化金融服务智慧再造。七是加快监管科技的全方位应用。八是扎实做好金融科技人才培养。

<https://mp.weixin.qq.com/s/wksVcFm8Mewl1NRyv52hXg>

# 技术、产品与市场

## 1、2022 年全球 IT 行业 10 大预测：网络安全、数字优先成为核心驱动力

IDC 预计，到 2022 年，全球一半以上的经济将基于数字化或受数字化影响，因为大多数产品和服务都将采用数字化交付模式，或者需要数字化增强才能保持竞争力。为了在数字化优先的世界中赢得竞争，组织需要优先投资于数字化工具，以增强物理空间和资产。因此，到 2024 年，一半以上的 ICT 投资将与数字化转型挂钩。

<https://www.secrss.com/articles/37899>

## 2、2022 中国数据安全十大发展趋势预测

根据过去一年对全球网络安全市场的研究与理解，明朝万达结合中国网络安全产业的发展特色与发展阶段，展望未来的中国网络安全产业，对中国网络安全市场做出以下十大预测：

（1）覆盖数据资产全生命周期的数据安全管控平台将成为未来可持续发展的必要条件；

（2）AI 伪造数据引发的多种安全问题，其应对方案将提上日程；



(3) 个保法实施推动后个人信息权属整体解决方案的诞生与衍进;

(4) 基于元数据管理与敏感数据发现的数据安全分类分级产品将更加成熟;

(5) 以数据安全评估为抓手, 构建数据安全组织体系、制度体系、技术体系、运营体系等为核心的数据安全治理服务将成为数据安全重点工程;

(6) 对数据资产自动化检测工具的需求将越发迫切;

(7) 数据安全将不再聚焦单个产品, 呈现能力化和服务化的趋势;

(8) AI 技术被广泛应用在数据安全治理体系建设中;

(9) 基于大数据的用户异常行为感知技术(UEBA)趋于场景化应用;

(10) 智能语义分析(NLP)技术成为敏感数据精准发现的重要手段。

<https://mp.weixin.qq.com/s/19DQrxPRGd6gg-2tRghMA>

### 3、2022 年, 哪些安全技术创新值得期待?

随着安全初创企业和传统安全厂商不断竞争带来的技术革新, 以解决现有和新涌现的安全问题, 2022 年仍将是行业值得期待的一年。许多令人兴奋的技术都围绕着人工智能

( AI )、数据共享和数字生态系统而展开，它们是安全数字化转型的核心。

- 隐私增强计算 ( PEC ) 的兴起
- 更强大的 API 安全能力
- 人工智能强化学习技术
- 孪生神经网络 ( SNN ) 的安全应用
- 万物身份 ( All Things Identity ) 时代开启
- 更优化的云工作负载安全性

<https://www.darkreading.com/dr-tech/6-security-tech-innovations-we-re-excited-to-see-in-2022>

#### 4、《全球数据合规与隐私科技发展报告》发布：国内首提“隐私科技”概念

“师夷长技以制夷”，应对数字化时代下的隐私保护痛点，也需要采取数字化的方式。因此市场上涌现了许多隐私保护技术及相应的解决方案，企业也开始关注“隐私科技”的话题并逐步付诸于实践。

隐私科技是指用于支撑隐私保护与合规的日常运营流程，且嵌入到 IT 架构和业务场景中的一系列技术解决方案，在保证个人信息全生命周期的增强保护和个人信息处理活动规范化的基础上，实现保护个人信息权益，提升数据流通、

共享与开放，促进个人信息合理开发利用的目的。

隐私科技实施程度最高的前三类解决方案是细粒度访问权限控制，数据去标识化、匿名化工具和个人信息主体同意授权管理。然而需求最迫切的前三类为数据自动化发现、分级分类与标识，数据流动监控和数据去标识化、匿名化技术。

<https://mp.weixin.qq.com/s/HERjvBWbiA9V3mHP4fNl8Q>

## 5、海南省公共数据资源开发利用试点成果发布，数据产品超市上线

海南作为全国 8 个公共数据资源开发利用试点省之一，经过一年半的探索实践，通过搭建数据产品超市，创新公共数据资源开发利用新模式，促进数据共享流通与融合利用。

据悉，数据产品超市基于多方安全技术和联邦计算的技术架构，实现了会员注册与认证、产品上架与审核、需求发布、数据开发、监管审核、运营监控等功能，为各级政府和各类企业提供善政、兴业、便民、利商的数据产品，有效促进公共数据资源的利用与大数据产业的发展，推进数据要素流通，服务海南自贸港建设。

省大数据管理局长董学耕表示，建设数据产品超市，要构建好总体框架，构建公共数据产品开发利用“1+3+N”模

式，即构建 1 套海南省数据产品开发利用体系，强化数据产品交易服务能力、数据产品开发支撑能力、平台管理能力，生成 N 个数据产品。

<https://mp.weixin.qq.com/s/BIhF-qLKv-AvM7w74CHvzQ>

## 6、2021 年商用密码发展呈现新变化

2021 年以来，密码领域也呈现出新的发展特征：一是商用密码管理要求正向各领域持续深度融入。二是新技术新业态中的密码应用需求日益增强。三是密码人才培养和队伍建设工作机制进一步完善。四是各地方加快推动区域密码产业发展步伐。五是商用密码产学研用各方生态交流持续活跃。

<https://www.secrss.com/articles/37876>

# 业界观点

## 1、人民网评：进一步保障网络安全和数据安全

近日，国家互联网信息办公室等十三部门修订发布《网络安全审查办法》(下称《办法》)，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。

互联网时代，人们在接受网络平台提供的服务时，不仅要在注册环节提供个人信息，而且在使用中还要授权相关 APP 访问各种用户信息的权限。由此带来的结果是，拥有越多用户的网络平台，收集公民个人信息的机会也越多。而相关信息经过大数据分析，可以对用户群体的职业构成、行为偏好、金融消费、出行轨迹等一系列涉及公民隐私的内容进行精准“画像”。信息时代，数据为王，掌握相关数据的敏感性不言自明。确保网络平台规范使用用户信息，确保相关数据的绝对安全，无论对个人，还是对国家，都极为重要。

<https://new.qq.com/omn/20220105/20220105A01UTJ00.html>

## 2、解读：《网络安全审查办法》与时俱进，修订后补充数据安全与海外上市管理

2021年9月1日，《数据安全法》正式施行，明确规定国家建立数据安全审查制度。随后，国家互联网信息办公室联合十二部门修订发布《网络安全审查办法》（以下简称《办法》），自2022年2月15日起施行。

该办法实施仅一年半后便发布修订稿，在审查范围、审查考虑因素方面增加了数据处理活动的内容，并将海外上市带来的风险纳入审查因素，正是为了应对一年以来的形势变化，以强化对网络空间重大风险挑战的防范能力。

[https://mp.weixin.qq.com/s/Tf1binv9vVXmy-kpEY\\_lRw](https://mp.weixin.qq.com/s/Tf1binv9vVXmy-kpEY_lRw)

## 3、国标《重要数据识别指南》起草发生重大修改

近期，起草中的国家标准《重要数据识别指南》发生重大修改。标准的主要改动体现在，取消了对重要数据的“特征”说明，因为这些特征依然不可避免地涉及行业分类，对各地方、各部门制定部门、本行业以及本系统、本领域的重要数据识别细则带来了不必要的约束。为此，标准编制组进一步调研了全球其他国家在网络安全、数据安全领域制定类似标准的情况，并选择了美国制定的《国家安全系统识别指南》作为参照。该指南已运行13年之久，其可操作性已得到

充分证明。目前，《重要数据识别指南》的起草思路与其类似。

[https://mp.weixin.qq.com/s/zb5KCsyNHsWOaun2A\\_A1zg](https://mp.weixin.qq.com/s/zb5KCsyNHsWOaun2A_A1zg)

#### 4、王春晖：营造良好数字生态的三大法治基石

《国家“十四五”规划和 2035 远景目标纲要》特别提到，加强涉及国家利益、商业秘密、个人隐私的数据保护，加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护。

浙江大学教授王春晖表示，《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》是营造良好数字社会生态的三大法治基石。

网络安全的核心是数据安全，在数据对各领域的重要性与日俱增的同时，数据风险与数据安全问题也愈发突显，给人类和社会带来了前所未有的挑战。数据安全与数据治理，不仅关乎数据作为重要生产要素的开发利用，而且与国家主权、国家安全、社会秩序、公共利益、公民隐私等休戚相关。

[https://tech.gmw.cn/2022-01/07/content\\_35430654.htm](https://tech.gmw.cn/2022-01/07/content_35430654.htm)

## 5、《互联网信息服务算法推荐管理规定》构建算法安全治理体系

2021年12月31日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合发布《互联网信息服务算法推荐管理规定》（以下简称《规定》）。

作为互联网信息服务领域贯彻落实《网络安全法》《数据安全法》《个人信息保护法》的重要举措，《规定》聚焦算法推荐服务乱象问题，包括大数据杀熟、诱导沉迷网络、劳动权益保障、偏见歧视未成年人和老年人权益保障。

《规定》一方面对所有算法推荐服务提供者的整体要求，例如“建立健全算法机制机理审核、科技伦理审查、用户注册、信息发布审核、数据安全和个人信息保护、反电信网络诈骗、安全评估监测、安全事件应急处置等管理制度和技术措施，制定并公开算法推荐服务相关规则，配备与算法推荐服务规模相适应的专业人员和技术支撑”，另一方面则针对场景提出一系列具体要求。

<https://mp.weixin.qq.com/s/8ilg1RCYsAoV3Xibo52JuA>



# 数据安全事件

## 1、美国连锁酒店 McMenamins 披露遭勒索攻击，发生数据泄露

2022 年 1 月 4 日，美国连锁酒店 McMenamins 披露，其在 12 月 12 日遭遇勒索软件攻击，发生员工数据泄露。据该公司称，攻击者窃取了在 2010 年 7 月 1 日至 2021 年 12 月 12 日期间受雇的个人数据。被盗员工的数据可能包括姓名、地址、电话号码、电子邮件地址、出生日期、种族、民族、性别、残疾状况、医疗记录、绩效和纪律记录、社会安全号码、健康保险计划选择、收入金额和退休供款金额。

<https://securityaffairs.co/wordpress/126293/data-breach/hospitality-chain-mcmenamins-data-breach.html>

## 2、因违反欧盟隐私规定，谷歌脸书或被罚超 15 亿元

2022 年 1 月 6 日报道，因未允许法国用户便捷地拒绝 cookie 跟踪，法国数据监管机构 CNIL 将对谷歌和 Facebook 分别处以 1.5 亿欧元（约合 10.81 亿人民币）和 6000 万欧元（约合 4.32 亿人民币）的罚款。CNIL 表示，通过对 Facebook.com、Google.fr 和 YouTube.com 网站的在线调查发现，虽然两家网站均提供了允许用户“立即接受”cookie 的按

钮，但对于拒绝接受 cookie 的选择却不是同样的容易——用户需要多次点击才能拒绝所有 cookie，而用户只需要点击一次就可以接受 cookie。CNIL 认为，用户可能因为拒绝机制过于复杂而选择放弃，这相当于“变相强制”用户接受 cookie，影响了互联网用户的同意自由，因而违法《法国数据保护法》（the French Data Protection Act）第 82 条规定。

<https://www.secrss.com/articles/38027>

### 3、SlimPay 因泄露 1200 万银行数据被罚 18 万欧元

2022 年 1 月 4 日报道，总部位于巴黎的订阅支付服务公司 SlimPay 被法国 CNIL 监管机构罚款 180,000 欧元，因为它被发现将敏感客户数据保存在可公开访问的服务器上整整五年。目前，SlimPay 已立即采取措施隔离服务器并保护数据，并且在后来的数据泄露通知中，该公司披露了有关安全事件的更多细节，包括受数据泄露影响的人数和个人数据类型。这包括来自 SlimPay 大约 1200 万商户客户的债务人数据，包括他们的邮政、电子和电话联系方式，以及银行识别码 (BIC) 和国际银行帐号 (IBAN) 等银行信息。

[https://www.theregister.com/2022/01/04/slimpay\\_breach\\_fine/?&web\\_view=true](https://www.theregister.com/2022/01/04/slimpay_breach_fine/?&web_view=true)

#### 4、Broward Health 遭遇数据泄露，影响了 130 万人

2022 年 1 月 4 日报道，Broward Health 公共卫生系统披露了一起影响超过 130 万人的大规模数据泄露事件。攻击发生在 2021 年 10 月 15 日，当时威胁行为者破坏了医院的网络并访问了患者数据。这些信息可能包括姓名、出生日期、地址、电话号码、财务或银行账户信息、社会安全号码、保险信息和帐号、包括病史、病情、治疗和诊断在内的医疗信息，病历号码、驾照号码和电子邮件地址。调查确定入侵是通过第三方医疗提供者的办公室发生的，该办公室被允许访问系统以提供医疗保健服务。

<https://securityaffairs.co/wordpress/126285/data-breach/broward-health-data-breach.html>

#### 5、美国无线运营商 UScellular 批露了数据泄露事件

2022 年 1 月 4 日，美国最大无线运营商之一 UScellular 披露了一起数据泄露事件。数据泄露发生在 12 月的一次攻击后，据该公司称，未经授权的个人非法访问了它们的计费系统，并获得了包含个人信息的无线客户帐户的访问权限。根据调查，他们认为该事件发生在 2021 年 12 月 13 日至 19 日。客户帐户中的信息包括姓名、地址、PIN 码和移动电话号码以及有关无线服务的信息，包括服务计划、使用情况

和账单。

<https://securityaffairs.co/wordpress/126317/data-breach/uscellular-second-data-breach-2021.html>

## 6、新加坡百货公司奥奇（OG）数据库被入侵，会员资料外泄

2022年1月8日报道，新加坡百货公司奥奇（OG）的会员资料数据库被黑客入侵，受影响的主要是普通和黄金会员，该公司提醒会员警惕钓鱼和冒充邮件等诈骗行动。初步调查结果显示，被盗取的资料包括会员的姓名、住家地址、电邮地址、电话号码、性别、生日，还有经过加密的身份证号码和线上密码等。该公司也为此向会员致歉，已指示管理数据库的服务提供方立即采取管理措施，试图进行补救，以确保数据库的安全。

<https://www.shicheng.news/v/rxmpg>

## 7、印度医学会的推特账号被泄露

2022年1月3日报道，印度医学会官方推特账号 [@IMAIndiaOrg](#)；印度世界事务委员会、[@ICWA\\_NewDelhi](#) 和 Mann Deshi 银行、[@MannDeshiOrg](#) 遭到黑客入侵。目前尚无法确定印度世界事务委员会和 Mann Deshi 银行的帐户泄露事件是黑客攻击的结果还是密码泄露的结果。

<https://www.cnbeta.com/articles/tech/1221691.htm>

## 8、“掩盖”数据泄露，前 Uber 首席安全官被指控

2022 年 1 月 7 日报道，近日，前 Uber 首席安全官加利福尼亚州帕洛阿尔托的 Joseph Sullivan 因涉嫌参与掩盖 2016 年对乘车应用程序的黑客攻击而被增加了额外的指控。该攻击暴露了 5700 万用户和 60 万条司机记录，电汇欺诈已被列入待决指控名单。敏感数据是从第三方云提供商的存储桶下载的，并通过滥用优步工程师无意中发布在代码共享网站上的凭据进行访问。

<https://mp.weixin.qq.com/s/fWWhr9RMY2Z90Tm8KwqYAEg>

## 9、黑客使用视频播放器从 100 个网站窃取信用卡

2022 年 1 月 4 日报道，黑客利用云视频托管服务对百余家房地产网站进行供应链攻击，注入恶意脚本窃取网站表单信息。Unit42 研究人员认为，这些威胁行为者获得了对上游 JavaScript 文件的访问权限，并将其修改为包含恶意撇取脚本。在下一次播放器更新时，视频播放器开始向所有已嵌入播放器的房地产网站提供恶意脚本，从而允许脚本窃取输入到网站表单中的敏感信息。

<https://www.bleepingcomputer.com/news/security/hackers-use-video-player-to-steal-credit-cards-from-over-100-sites/>

## 10、恶意软件 ZLoader 利用微软的数字签名验证窃取敏感信息

2022 年 1 月 5 日报道，据研究人员称，Zloader 恶意软件活动一直在利用微软的数字签名验证来窃取 cookie、密码和敏感信息。

网络安全公司 Venafi 副总裁 Kevin Bocek 表示，这些利用微软数字签名漏洞的违规行为提醒了所有组织，他们需要警惕代码签名攻击。盲目地相信数字签名的安全是不够的，特别是在云计算时代，“我们必须学习快速安全的软件开发管道。相反，组织需要采取措施来不断审查和保护这些非常强大的机器身份。”

<https://www.inforisktoday.com/zloader-malware-exploits-microsoft-signature-verification-a-18242>