

# 全球数据安全观察

总第 39 期 2021 年第 15 期

# 摘要

## 安全事件.....2

1. 印度股票交易平台 Upstox 超 250 万用户数据被泄露.....3
2. ParkMobile 泄密事件暴露 2100 万用户的车牌数据和手机号码 3
3. 第三方安全漏洞破坏了新加坡求职研究所的相关数据..... 3
4. 风险和合规初创公司 LogicGate 确认数据泄露.....4
5. Celsius Network 披露数据泄露事件..... 4

## 政策形势.....5

1. 交通运输部印发《交通运输政务数据共享管理办法》 ..... 5
2. 数据安全法草案、个人信息保护法草案本月底将迎来二审..... 5
3. 工信部拟加强监管：智能网联车企收集的个人信息和重要数据应在境内存储..... 6
4. 国家医保局印发《关于加强网络安全和数据保护工作的指导意见》 .....6
5. 美国将立法禁止向敌对国家出口公民个人数据.....7

## 业界观点.....8

1. 数据库安全的十个最佳实践..... 8
2. 我国数据安全治理存在的问题挑战..... 8
3. Gartner 发布的技术支持下个人隐私发展阶段的解读..... 9
4. 库克最新演讲全文：重新定义隐私..... 10

# 安全事件

## 1. 印度股票交易平台 Upstox 超 250 万用户数据被泄露

2021 年 4 月 12 日，印度经纪公司 Upstox 数据泄露，泄漏的信息包括姓名、电子邮件地址、生日、银行帐户信息，以及大约 5600 万从公司服务器提取的客户（KYC）文档。

<https://thehackernews.com/2021/04/indian-brokerage-firm-upstox-suffers.html>

## 2. ParkMobile 泄密事件暴露 2100 万用户的车牌数据和手机号码

2021 年 4 月 13 日报道，有人正在网络犯罪论坛上出售北美颇受欢迎的移动停车应用 ParkMobile 的 2100 万客户的账户信息。被盗数据包括客户的电子邮件地址、出生日期、电话号码、车牌号、哈希密码和邮寄地址。

<https://www.cnbeta.com/articles/tech/1114047.htm>

## 3. 第三方安全漏洞破坏了新加坡求职研究所的相关数据

2021 年 4 月 15 日报道，新加坡求职研究所（E2i）表示，由于针对“指定的第三方供应商”的恶意软件破坏，可能已非法访问了 30,000 个人的个人详细信息，包括姓名、身份证号

码、联系信息、学历和工作经历。

[https://mp.weixin.qq.com/s/02OZw0d\\_R0\\_mJ0QaKQyCOQ](https://mp.weixin.qq.com/s/02OZw0d_R0_mJ0QaKQyCOQ)

#### 4. 风险和合规初创公司 LogicGate 确认数据泄露

风险和合规初创公司 LogicGate 在本月初发送给客户的电子邮件中表示，一个未经授权的第三方获得了其 AWS 托管的云存储服务器的凭据，该服务器存储了其旗舰平台 Risk Cloud 的客户备份文件，但 LogicGate 没有透露 AWS 凭据是如何被泄露的。

<https://techcrunch.com/2021/04/13/logicgate-risk-cloud-data-breach/>

#### 5. Celsius Network 披露数据泄露事件

2021 年 4 月 15 日，加密货币奖励平台 Celsius Network 披露了一项安全漏洞，暴露了导致网络钓鱼攻击的客户信息。Celsius 的第三方营销服务器已受到威胁，威胁行为者获得了部分 Celsius 客户列表的访问权限。

<https://www.bleepingcomputer.com/news/security/celsius-email-system-breach-leads-to-phishing-attack-on-customers/>

# 政策形势

## 1. 交通运输部印发《交通运输政务数据共享管理办法》

为规范交通运输政务数据共享，推动交通运输数字政府建设，加快建设交通强国，依据国务院关于政务数据共享管理要求，制定《交通运输政务数据共享管理办法》，用于规范交通运输部及部际、部省相关政务部门因履行职责需要提供和使用政务数据的行为。

<https://mp.weixin.qq.com/s/29HogANxz8gUS7wrPidMEw>

## 2. 数据安全法草案、个人信息保护法草案本月底将迎来二审

2021年4月16日，十三届全国人大常委会第九十一次委员长会议在京举行。会议透露，十三届全国人大常委会第二十八次会议将于4月26日至29日举行，会上将审议多项草案和议案，包括数据安全法草案和个人信息保护法草案。这两份草案分别于去年6月和10月经过初次审议并公开征求意见。截止目前，数据安全法草案共收到651条意见，个人信息保护法草案共收到1245条意见。

<https://www.secrss.com/articles/30573>

### 3. 工信部拟加强监管: 智能网联车企收集的个人信息和重要数据应在境内存储

工业和信息化部装备工业一司组织编制了《智能网联汽车生产企业及产品准入管理指南（试行）》（征求意见稿）。征求意见稿中指出，智能网联汽车生产企业应依法收集、使用和保护个人信息，实施数据分类分级管理，制定重要数据目录，不得泄露涉及国家安全的敏感信息。在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关规定在境内存储。因业务需要，确需向境外提供的，应向行业主管部门报备。

<https://mp.weixin.qq.com/s/5eF7-fSYeSWtf7i9QvNtw>

### 4. 国家医保局印发《关于加强网络安全和数据保护工作的指导意见》

4月9日，国家医疗保障局印发《关于加强网络安全和数据保护工作的指导意见》，明确部署了加强医疗保障网络安全和数据保护工作的总体要求，从加强网络安全管理、加强数据安全保护和制定保障措施三方面，扎实推进医疗保障信息平台建设及运营维护，防范化解医疗保障系统数据安全风险，促进数据合理开发利用。

[https://mp.weixin.qq.com/s/C6wXMKnog6\\_z2d7l8feOYA](https://mp.weixin.qq.com/s/C6wXMKnog6_z2d7l8feOYA)

## 5. 美国将立法禁止向敌对国家出口公民个人数据

《保护美国人的数据免受外国监视法案》将建立一个跨部门小组对数据进行分类，然后制定一份禁止进口可能威胁国家安全的个人数据的国家名单。本周出台的立法将规定，企业将生活在美国的人产生的数据出口到某些国家是非法行为，因为这些数据可能会对国家安全构成威胁。

<https://www.secrss.com/articles/30578>

# 业界观点

## 1. 数据库安全的十个最佳实践

- (1) 部署物理数据库安全措施;
- (2) 隔离数据库服务器;
- (3) 设置 HTTPS 代理服务器;
- (4) 避免使用默认网络端口;
- (5) 使用实时数据库监测;
- (6) 采用数据库防火墙和 Web 应用防火墙;
- (7) 部署数据加密协议;
- (8) 创建定期数据库备份;
- (9) 保持应用更新;
- (10) 采用强用户身份验证。

<https://www.secrss.com/articles/30420>

## 2. 我国数据安全治理存在的问题挑战

近年来，我国数据治理法治建设不断推进，数据治理职责划分日益明晰，数据治理专项行动取得积极成效，但仍然面临一些问题挑战：（1）个人信息保护力度有待加强。个人信息保护规定和职责较为分散，缺乏实操性、针对性管理规定；个人信息泄露等安全事件频繁发生，严重侵害个人信

息主体的合法权益；新技术应用为个人信息保护带来挑战。

(2) 政府数据开放共享不健全。政府数据存在“数据孤岛”，数据共享不顺畅，数据利用不充分，跨部门、跨系统、跨区域统筹协调难度大。(3) 数据流通交易环境有待改善。数据流通交易规范体系尚未建立，数据交易平台建设不完善，数据壁垒导致数据流通不顺畅。(4) 跨境数据流动治理亟待强化。缺乏统一的、可操作的跨境数据流动规则，关键信息基础设施和重要数据具体认定标准尚未出台，数据跨境安全审核机制亟待确立。

<https://mp.weixin.qq.com/s/3K3pjd6gusIGoPTjImBiMw>

### 3. Gartner 发布的技术支持下个人隐私发展阶段的解读

自新冠疫情蔓延以来，个人隐私信息保护问题正越来越受到关注。世界各国都在不断完善个人隐私信息保护策略及法规，以适应疫情下的种种新变化。风险管理人员也需运用更新的技术手段来应对疫情下关于个人隐私数据保护的新形势。Gartner 将技术支持下个人隐私保护的发展分为三个阶段：建立、维护、发展。

建立阶段概述了隐私管理程序的各项基本功能，对于需要处理个人隐私信息的公司或组织，这些都是必要的工具；维护阶段让组织或公司有一定的时间来维护好自己的隐私

管理程序；发展阶段用一些特别的工具减少隐私风险，包括数据脱敏及标记化、数据生命周期治理等等。

[https://mp.weixin.qq.com/s/B\\_L520JRRiRWcE3A03NlaQ](https://mp.weixin.qq.com/s/B_L520JRRiRWcE3A03NlaQ)

#### 4. 库克最新演讲全文：重新定义隐私

苹果 CEO 蒂姆·库克今天在线上的“计算机、隐私和数据保护会议”（Computers, Privacy, and Data Protection conference）上发表讲话，谴责了 Facebook 等公司的商业模式，并强调了苹果对推进用户隐私的承诺。他们的观点十分明确，技术不需要庞大的个人数据库或通过几十个网站和应用程序拼接在一起，才能取得成功。广告在没有这些技术的情况下存在和发展了几十年。如果一个企业是建立在误导用户、利用数据、根本没有选择的基础上，那么它不值得我们赞美。它应该得到改革。

<https://www.secrss.com/articles/29175>