北源律师事务所
BEIYUAN LAW FIRM

数据合规资讯（10 月）

（截至 2022 年 10 月 31 日）

数据合规资讯 2022 年 10 月

导读

一、国内数据合规资讯

（一）最新法规

1. 民航局印发《关于民航大数据建设发展的指导意见》
2. 全国信安标委发布关于征求国家标准《信息安全技术 智能手机预装应用程序基本安全要求》（征求意见稿）意见的通知
3. 14 项网络安全国家标准获批发布
4. 工业互联网平台首批国家标准正式实施发布
5. 工业互联网总体网络架构国家标准正式发布
6. 工信部印发《网络产品安全漏洞收集平台备案管理办法》
7. 国家邮政局发布关于《寄递用户个人信息安全管理规定》草案公开征求意见的通知

（二）热点案例

1. 药店因录入购买“四类药”者个人信息被告，法院判决驳回原告诉讼请求
2. 芜湖市繁昌区审理全区首例侵犯公民个人信息刑事附带民事公益诉讼案
3. 广东高院发布个人信息保护典型案例

（三）监管执法

1. 网信办公布“清朗·打击网络谣言和虚假信息”专项行动曝光第二批网络谣言溯源及处置典型案例

2. 市场监管总局组织开展网络交易突发事件应急演练
3. 工信部发布关于 APP 侵害用户权益整治“回头看”发现问题的通报（2022 年第 6 批，总第 26 批）
4. 上海某科技公司因违反数据安全法被处罚
5. 深圳证监局通报其辖区内某券商 OA 系统遭受攻击
6. 福建省网信办开通数据出境安全评估申报通道
7. 河北省网信办发布关于“简动”等 43 款 App 违法违规收集使用个人信息情况的通报
8. 四川省通信管理局发布关于川渝两地侵害用户权益 APP 名单的通报（第四期）
9. 陕西省通信管理局发布关于侵害用户权益行为 APP 的通报
10. 山东省、海南省网信办开通数据出境安全评估申报通道
11. 北京市通信管理局发布关于 20 款问题 APP 的通报
12. 2022 年世界互联网大会乌镇峰会将于 11 月 9 日至 11 日举行

二、国际数据合规资讯

（一）立法活动

1. 欧盟《数字市场法案》全文公布
2. 英国 ICO 发布《雇员监控指南》（草案）
3. OECD《跨境数据流动报告》发布
4. EDPB 批准 Europrivacy 作为欧盟数据保护印章
5. 欧盟理事会针对《人工智能法案》即将达成统一意见
6. 澳大利亚拟立法加大对反复或重复侵犯个人隐私行为的处罚力度

7. 欧盟《数字服务法案》全文公布

（二）监管动态

1. Uber 前首席安全官被判妨碍 FTC 调查
2. 荷兰法院判决美国软件开发公司向其拒绝开启网络摄像头的前员工支付 7.5 万欧元
3. 美国得克萨斯州起诉谷歌：未完全征得用户同意收集生物识别信息
4. ICO 对建筑公司侵犯员工隐私的行为处以 440 万英镑罚款

（三）安全快讯

1. LofyGang 使用 100 多个恶意 NPM 包毒害开源软件
2. 泄露约 30 万用户信息，丰田公开道歉
3. 美国安全公司推出“不要追踪儿童”工具，旨在保护儿童隐私
4. 澳大利亚零售巨头 220 万用户数据被黑客窃取并在线出售
5. 澳大利亚医疗保险公司 390 万用户信息全部泄露

正文

一、国内数据合规资讯

（一）最新法规

1. 民航局印发《关于民航大数据建设发展的指导意见》

2022 年 10 月 9 日，民航局正式印发《关于民航大数据建设发展的指导意见》，旨在加快推进智慧民航建设，加强民航大数据建设发展顶层设计。该意见明确了民航大数据建设发展的总体框架（即“三个导向，六个方向，六个靶向”）、主要任务和保障措施。

来源：*http://www.caac.gov.cn/XXGK/XXGK/ZCFB/202210/t20221013_215627.html*

2. 全国信安标委发布关于征求国家标准《信息安全技术 智能手机预装应用程序基本安全要求》（征求意见稿）意见的通知

2022 年 10 月 9 日，全国信安标委发布发布《信息安全技术 智能手机预装应用程序基本安全要求》（征求意见稿）并向社会公开征求意见，截止时间为 2022 年 12 月 9 日。征求意见稿中规定，除直接支撑操作系统运行或实现智能手机基本功能所必须的基本功能应用程序外，其他预装程序均应可卸载。基本功能应用程序包括系统设置、文件管理、多媒体摄录、接打电话、收发短信、通讯录、浏览器、应用商店等。

来源：*https://mp.weixin.qq.com/s/BflQk2x2ifXyr80KqJpitA?scene=25#wechat_redirect*

3. 14 项网络安全国家标准获批发布

2022 年 10 月 19 日，根据 2022 年 10 月 14 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2022 年第 13 号），全国信息安全标准化技术委员会归口的 14 项国家标准正式发布。此次获批发布的国家标准涵盖了生物识别、汽车数据处理、即时通信服务、快递物流服务、网上购物服务、网络支付服务、网络音视频服务以及网络预约汽车服务领域，进一步明确了对具体领域的信息安全技术要求，有助于进一步提高各领域的数据安全保障水平。

来源：*https://mp.weixin.qq.com/s/f7LvDe4wrGfsnuD0wfDfNQ*

4. 工业互联网平台首批国家标准正式实施发布

近日，国家市场监督管理总局（国家标准化管理委员会）发布 2022 年第 13 号中华人民共和国国家标准公告，批准 GB/T 41870-2022《工业互联网平台 企业应用水平与绩效评价》和 GB/T 23031.1-2022《工业互联网平台 应用实施指南 第 1 部分：总则》2 项国家标准正式发布，这是我国工业互联网平台领域发布的首批国家标准，对我国工业互联网平台标准化建设具有重要意义。

来源：*https://mp.weixin.qq.com/s/N9CkPwlQJ9zv3ieIsNtXVQ*

5. 工业互联网总体网络架构国家标准正式发布

近日，国家标准化管理委员会发布 2022 年第 13 号中华人民共和国国家标准公告，批准发布国家标准 GB/T 42021-2022《工业互联网 总体网络架构》，这是

全国工业互联网网络领域发布的首个国家标准，标志着全国工业互联网体系建设迈出了坚实的一步。

《工业互联网 总体网络架构》国家标准围绕工业互联网网络规划、设计、建设和升级改造，规范了工业互联网工厂内、工厂外网络架构的目标架构和功能要求，提出了工业互联网网络实施框架和安全要求，有助于加快构建高质量的工业互联网网络基础设施，有助于引导全行业全产业的数字化、网络化、智能化水平提升，对于加速产业数字化转型具有重要意义。

来源：https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2022/art_396adac1d4294aaa9a94c344c7f9c867.html

6. 工信部印发《网络产品安全漏洞收集平台备案管理办法》

为规范网络产品安全漏洞收集平台备案管理，工业和信息化部近日印发《网络产品安全漏洞收集平台备案管理办法》。《办法》所称网络产品安全漏洞收集平台，是指相关组织或者个人设立的收集非自身网络产品安全漏洞的公共互联网平台，仅用于修补自身网络产品、网络和系统安全漏洞用途的除外。《办法》规定，漏洞收集平台备案通过工业和信息化部网络安全威胁和漏洞信息共享平台开展，采用网上备案方式进行。拟设立漏洞收集平台的组织或个人，应当通过工业和信息化部网络安全威胁和漏洞信息共享平台如实填报网络产品安全漏洞收集平台备案登记信息。该办法自 2023 年 1 月 1 日起施行。

来源：https://mp.weixin.qq.com/s/hlzas3kuff4c1b4qyOv2Eg

7. 国家邮政局发布关于《寄递用户个人信息安全管理规定》草案公开征求意见的通知

2022 年 10 月 25 日，为进一步加强寄递用户个人信息安全管理，保护用户合法权益，促进邮政行业健康发展，国家邮政局起草了《寄递用户个人信息安全管理规定》草案，现向社会公开征求意见，反馈意见截止日期为 2022 年 11 月 23 日。草案中规定了寄递用户个人信息的含义，并对寄递企业提出个人信息保护相关要求。

来源：https://www.spb.gov.cn/gjyzj/c100025/c100029/202210/6cc8f86491ca49c5b70bcfd26f1b723e.shtml

（二）热点案例

1. 药店因录入购买“四类药”者个人信息被告，法院判决驳回原告诉讼请求

原告江某前往被告处购买药品，药店根据市场监督管理局要求对购买感冒发烧、止咳、消炎、抗病毒这四类药品的记录进行网络上传，江某在录入个人信息后因价格昂贵放弃购买。随后江某要求被告处删除其留存的个人信息，而被告方主张，录入信息是因为疫情防控的需要且没有删除渠道。原告遂诉至法院，要求被告方赔偿其经济、名誉损失。

法院认为，处理个人信息应取得个人同意，但是《中华人民共和国个人信息保护法》规定，有以下几种规定情形的，不需取得个人同意：为履行法定职责或者法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需等等。疫情防控期间，为应对突发公共卫生事件，被

告按照法律法规要求，在原告购买涉疫情防控药品时，落实药品实名登记的规定，并无不当，不属于侵权行为。法院判决驳回原告诉讼请求。

来源：*https://mp.weixin.qq.com/s?src=11&timestamp=1667463051&ver=4143&signature=-d*ho5oQwEHsP3Z5vzEWPeICQv5z2mPz5Flx*9BLjy1xv*cI4fATHcVWyMX43cztgqT8hxCwg7tU8w1fWTPpnIEYoIBD4a30YpBilP*xhtaQavKdMCMs46P-DpvgIHXn&new=1*

2. 芜湖市繁昌区审理全区首例侵犯公民个人信息刑事附带民事公益诉讼案

2022 年 10 月 19 日，繁昌区首例侵犯公民个人信息刑事附带民事公益诉讼案在区法院第一法庭公开审理，繁昌区检察院作为公诉机关指控被告人俞某通过 QQ 聊天工具以 300 元的价格向他人购买百度网盘链接，内含大量公民个人信息，俞某陆续在网盘下载公民个人信息共计 360 余万条，并将其中部分小区住户信息、车主信息、淘宝会员名信息等公民个人信息非法出售给他人，从中获利 31240 元，其行为触犯了《中华人民共和国刑法》的规定，应当依法追究其刑事责任。同时，繁昌区检察院作为公益诉讼起诉人，认为其行为对公民个人生活造成滋扰，侵扰他人生活安宁，且公民个人信息存在被他人利用的风险，具有严重社会危害性，违反了《中华人民共和国民法典》中对公民隐私权保护的规定，据此向本院提起附带民事公益诉讼，要求俞某承担赔礼道歉、消除危险等民事侵权责任。

来源：*https://mp.weixin.qq.com/s?src=11&timestamp=1667463085&ver=4143&signature=A-vYwl5HnQy-y4iov5bL6LTJvYgnCuJkKdb6N6qHbqhVGNCSzKxgM2vhEEncpMU*nzEEbdTH010VAKvknGLv5CiMnyF10Tide*N*FNHLZ9iZadoyl4gA-LVeeEln-VcA&new=1*

3. 广东高院发布个人信息保护典型案例

《个人信息保护法》施行一周年之际，广东省高级人民法院发布一批个人信息保护典型案例，其中包括 2 个刑事、4 个民事案件，涵盖严厉打击侵犯公民个人信息犯罪、防止个人信息“过度收集”、保障行使个人信息查阅复制权、规范网络平台依法使用个人信息等内容，反映了广东法院充分发挥审判职能作用，全面依法保护个人信息权益、规范个人信息处理，维护网络空间良好生态、促进数字经济健康发展的司法实践。

来源：https://mp.weixin.qq.com/s/IO7SPwry3ZABchPuCjQsjA

（三）监管执法

1. 网信办公布“清朗·打击网络谣言和虚假信息”专项行动曝光第二批网络谣言溯源及处置典型案例

中央网信办深入推进“清朗·打击网络谣言和虚假信息”专项行动，截止 2022 年 10 月 5 日，执法机构在重点网站平台共处置网络谣言账号 2800 余个，查处的谣言案例包括疫情防控类、突发事件类及社会民生类谣言。网信办表示将督导网站平台切实履行信息内容管理主体责任，加强日常监测和查证处置。

来源：http://www.cac.gov.cn/2022-10/05/c_1666600385858458.htm

2. 市场监管总局组织开展网络交易突发事件应急演练

2022 年 10 月 10 日，市场监管总局组织开展 2022 年网络交易突发事件应急实战演练。此次演练由总局网监司主办，总局办公厅、新闻宣传司，竞争政策与

大数据中心，北京、上海、浙江等地市场监管部门及阿里、京东、拼多多等平台企业参加演练。

本次演练模拟线上出现违法销售禁限售商品的突发事件，运用数字化手段，通过“实景拍摄+现场模拟”相结合的形式，全过程演练突发事件的事件发生、事件调查、分析研判、III 级应急响应、事件处置、跟踪督导、舆论引导、响应终止等环节。

来源：https://www.samr.gov.cn/xw/zj/202210/t20221013_350719.html

3. 工信部发布关于 APP 侵害用户权益整治“回头看”发现问题的通报（2022 年第 6 批）

工信部持续开展 APP 侵害用户权益专项整治行动。为巩固治理成效，营造共同维护消费者权益的良好环境，工信部于近期开展 APP 侵害用户权益整治“回头看”，组织第三方检测机构对违规推送弹窗信息、APP 过度索取权限等问题进行重点抽测，共发现 38 款 APP（详见附件）存在问题，予以通报。

来源：https://www.miit.gov.cn/jgsj/xgj/gzdt/art/2022/art_62e7b9086fe749ad8538c7efb62d987a.html

4. 上海某科技公司因违反数据安全法被处罚

2022 年 10 月 13 日，上海网信办发现某科技公司在处理政务类数据时违规操作，且未采取相应的技术措施和其他必要措施保障数据安全，导致数据存在泄露

风险。上海网信办依据《中华人民共和国数据安全法》对该公司责令改正，给予警告，并处以人民币五万元罚款的行政处罚。

来源：https://mp.weixin.qq.com/s/gViJnRho08RsyguMQ5x-WA?scene=25#wechat_redirect

5. 深圳证监局通报其辖区内某券商 OA 系统遭受攻击

2022 年 10 月 13 日，深圳证监局公布的最新一期证券期货机构监管通讯显示，辖区某证券公司因网络安全风险管理存在漏洞，导致公司 OA 系统遭受注入攻击影响公司移动端 OA 办公。深圳证监局核查发现，该公司渗透测试及漏洞修复机制不完备，网络安全监控方式和响应机制有待改进，安全防护策略有待加强。同时，该公司信息系统相关人员流动较大，多个重要信息系统运维主岗已离职，多个技术管理环节权限管理不严。深圳证监局表示，辖区各证券期货经营机构应高度重视网络安全保障工作，认真落实网络和信息安全工作责任规划，加强信息技术人员保障，提升网络安全风险防控能力。

来源：http://www.csrc.gov.cn/shenzhen/c101531/c5966160/content.shtml

6. 福建省网信办开通数据出境安全评估申报通道

2022 年 10 月 14 日，福建省网信办发布公告，开通数据出境安全评估申报通道。根据《数据出境安全评估办法》和国家互联网信息办公室发布的《数据出境安全评估申报指南（第一版）》要求，注册地为福建的数据处理者向境外提供数据，应当通过福建省委网信办向国家网信办申报数据出境安全评估，申报方式为送达书面申报材料并附带材料电子版。

来源：http://www.fjwx.gov.cn/gs/20221014/2693938.html

7. 河北省网信办发布关于“简动”等 43 款 App 违法违规收集使用个人信息情况的通报

近期，河北省互联网信息办公室组织对运动健身类、房屋租售类等常见类型且公众大量使用的 300 余款 App 收集使用个人信息情况进行了检测，发现“简动”等 43 款 App 存在违法违规收集使用个人信息行为，现将有关情况进行通报。针对检测发现的问题，相关 App 运营者应当于本通报发布之日起 15 个工作日内完成整改，逾期未完成的，将依法依规予以处置。

来源：https://mp.weixin.qq.com/s/8YsDPJF-2a-uW09IT8trNQ?scene=25#wechat_redirect

8. 四川省通信管理局发布关于川渝两地侵害用户权益 APP 名单的通报（第四期）

2022 年 10 月 25 日，四川省和重庆市管局发布公告，四川省和重庆市管局组织第三方检测机构对川渝两地主流应用商店移动互联网应用程序(APP)进行了检查。截止目前，仍有 17 款 APP 未按要求完成整改。通报 APP 应在 11 月 4 日前完成整改落实工作，逾期不整改的，将依法依规进行处置。

来源：https://mp.weixin.qq.com/s/bBxdP95J6pxbiGa9JC4TvQ?scene=25#wechat_redirect

9. 陕西省通信管理局发布关于侵害用户权益行为 APP 的通报

2022 年 10 月 25 日，陕西省通信管理局发布公告，陕西省通信管理局近期组织第三方检测机构对陕西属地 APP 进行检查，截至目前，尚有 3 款 APP 未按照

要求完成整改。通报 APP 所属企业应于 11 月 1 日前完成整改。逾期不整改的，将依法依规处置。

来源：https://mp.weixin.qq.com/s/ixf2Xs-D9dIXF4wngjJNIA?scene=25#wechat_redirect

10. 山东省、海南省网信办开通数据出境安全评估申报通道

2022 年 10 月 26 日，山东省和海南省网信办开通数据出境安全评估申报通道。根据《数据出境安全评估办法》和国家互联网信息办公室发布的《数据出境安全评估申报指南（第一版）》要求，本省向境外提供在境内运营中收集和产生的重要数据和个人信息的组织或个人（以下简称“数据处理者”），应当通过省网信办向国家网信办申报数据出境安全评估，申报方式为送达书面申报材料并附带材料电子版。

来源：https://mp.weixin.qq.com/s?src=11&timestamp=1667207125&ver=4138&signature=B5VYvWbUMsfHSk41Y8KhPFCPq32jlUVwboSxHMXgUJDKb4K6*8S0z*bIRZXRfTnNCm7pn315EmkA2LJlb3cSQH1s3f3xgISo*ZhctkzyecnLPjR9yvbi*6Tf6jBRkhzr&new=1

https://mp.weixin.qq.com/s/uZHQHb6ytfTIcTW3lOoW4g

11. 北京市通信管理局发布关于 20 款问题 APP 的通报

近期北京市通信管理局依据《网络安全法》《数据安全法》《个人信息保护法》《网络产品安全漏洞管理规定》等法律法规，组织开展北京地区 APP 技术检测工作。现北京市通管局就存在侵害用户权益和安全隐患等问题的 20 款 APP 进

行通报，要求有关 APP 运营企业立即整改，并于 11 月 15 日前提交整改报告。逾期不整改或整改不到位的，将依法依规处置。

来源：https://mp.weixin.qq.com/s/cm8QFZ8NcDWHgh-HgfoJYA

12. 2022 年世界互联网大会乌镇峰会将于 11 月 9 日至 11 日举行

2022 年 10 月 31 日上午，2022 年世界互联网大会乌镇峰会新闻发布会在北京举行，宣布 2022 年世界互联网大会乌镇峰会将于 11 月 9 日至 11 日举行。今年大会主题为“共建网络世界 共创数字未来——携手构建网络空间命运共同体”。本次乌镇峰会是世界互联网大会国际组织成立后的首届年会，采用“线上+线下”相结合的方式举办。

来源：https://mp.weixin.qq.com/s/B2XoyGBLJKVeFM9nu5N5Gw

二、国际数据合规资讯

（一）立法活动

1. 欧盟《数字市场法案》全文公布

2022 年 10 月 12 日，欧盟在其官方公报上发布《数字市场法案》（Digital Market Act）全文，该法案将于当地时间 2022 年 11 月 1 日生效。该法案旨在通过防止大公司滥用其市场力量，并允许让新参与者进入市场以确保欧洲数字市场更高的的竞争程度。该法案为指定的看门人建立了一份任务清单，若不遵守法案规定，则将会有强制执行的制裁机制，包括高达全球营业额 10%的罚款。自认为是“看门

人”的大型互联网企业需要主动向欧盟委员会申报，由欧盟委员会在 45 个工作日内确认企业是否达到“看门人”的标准。

来源：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

2. 英国 ICO 发布《雇员监控指南》（草案）

近期，英国信息专员办公室（ICO）就关于雇主监控员工的指导草案向公众征求意见。该指导草案旨在根据数据保护立法就监测工作人员提供实际指导，并提倡雇主采用良好做法。反馈意见于 2023 年 1 月 11 日截止。

来源：https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-employment-practices/

3. OECD《跨境数据流动报告》发布

2022 年 10 月 12 日，经济合作与发展组织在其官方网站发布了《跨境数据流动报告》。该报告评估了关于跨境数据流的关键政策和举措，为七国集团国家参与这一政策议程提供信息和支持。

来源：https://www.oecd.org/publications/cross-border-data-flows-5031dd97-en.htm

4. EDPB 批准 Europrivacy 作为欧盟数据保护认证计划

欧洲数据保护委员会（EDPB）依照《通用数据保护条例》（GDPR）第 42（5）条批准 Europrivacy 作为欧盟数据保护认证。Europrivacy 是一项通过欧洲研究计划开发的创新方法和认证方案，旨在简化、增强和认证隐私法规的合规性。它涵盖了 GDPR 的要求，可以帮助数据控制者和数据处理者证明它们在所有成员国都符合数据保护的要求。Europrivacy 获批标志着在确保尊重欧盟隐私保护规则方面向前迈出了一大步。

来源：*https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr*

5. 欧盟理事会针对《人工智能法案》即将达成统一意见

欧盟理事会轮值主席国捷克于 10 月 19 日就《人工智能法案》发布了一项新的妥协方案，该方案将成为下月达成协议的基础。《人工智能法案》是一项具有里程碑意义的立法，旨在根据该行业的潜在风险对其进行监管。欧盟理事会电信工作组将于 10 月 25 日讨论新的妥协方案，这将是欧盟的第四个妥协方案。如果没有重大问题出现，欧盟代表们可能会在 11 月中旬之前批准该文本。

来源：*https://www.euractiv.com/section/digital/news/eu-council-nears-common-position-on-ai-act-in-semi-final-text/*

6. 澳大利亚拟立法加大对反复或重复侵犯个人隐私行为的处罚力度

据路透社报道，澳大利亚总检察长称在最近几周袭击数百万澳大利亚用户的网络攻击发生之后，澳大利亚拟向议会提交议案，通过修订隐私法，提高对重复

或严重侵犯隐私行为的处罚力度，加大对遭受重大数据泄露公司的处罚。议案提议把对严重或重复侵犯隐私的最高处罚从目前的 222 万澳元提高到 5000 万澳元，或相关时期营业额的 30%，以较高者为准。

来源：*https://ministers.ag.gov.au/media-centre/tougher-penalties-serious-data-breaches-22-10-2022#:~:text=When%20Australians%20are%20asked%20to,the%20cost%20of%20doing%20business*

7. 欧盟《数字服务法案》全文公布

2022 年 10 月 27 日，欧盟在其官方公报上发布《数字服务法案》（Digital Services Act）全文，该法案将于当地时间 2022 年 11 月 1 日生效。该法案由欧盟委员会于 2020 年 12 月 15 日连同《数字市场法案》在欧盟议会及欧洲联盟理事会提出，旨在使打击非法内容、透明广告和虚假信息的 2002 年《电子商务指令》现代化，并迫使互联网服务打击错误信息、披露其服务如何放大有争议的内容，并停止根据个人的种族、宗教或性取向来定位在线广告。

来源：*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A277%3ATOC*

（二）监管动态

1. uber 前首席安全官被判妨碍 FTC 调查

旧金山陪审团裁定 Uber 前首席安全官 Joseph Sullivan 妨碍公务刑事指控的罪名成立，起因是他没有向联邦当局报告 2016 年的一次网络入侵。在经过三周的审判之后，美国联邦法院最终作出判决。Sullivan 现在面临妨碍公务罪的五年监禁，以及另一项罪名的最长三年监禁。此案是网络安全高管因决定不披露黑客攻击事件而面临刑事责任的罕见案例。

来源： *https://www.wsj.com/articles/former-uber-security-chief-found-guilty-of-obstructing-ftc-probe-11665004454?mod=Searchresults_pos4&page=2*

2. 荷兰法院判决美国软件开发公司向其拒绝开启网络摄像头的前员工支付 7.5 万欧元

一家美国企业的一名远程雇员因拒绝在工作时打开网络摄像头而被解雇，荷兰法院以非法解雇为由判决公司给该名员工支付 7.5 万欧元，并宣布雇佣合同中的竞业条款和保密条款无效。这名员工入职后被命令参加一个名为"纠正行动计划"的虚拟培训期。他被要求在此期间必须在整个工作日内保持登录状态，打开屏幕共享并启动网络摄像头。该员工称公司每天通过摄像头监控其长达 9 个小时的行为侵犯其隐私，于是拒绝打开摄像头。企业以“拒绝工作”和“不服从命令”解雇该员工。法院援引了《欧洲人权公约》第 8 条，以及欧洲法院的一项裁决，该裁决明确表示企业对员工的监督附加了严格的条件。法院最终裁定企业要求保持摄像机处于激活状态是对原告隐私权的不合理侵犯。

来源： *https://nltimes.nl/2022/10/09/dutch-employee-fired-us-firm-shutting-webcam-awarded-eu7 5000-court*

3. 美国得克萨斯州起诉谷歌：未完全征得用户同意收集生物识别信息

美国得克萨斯州针对谷歌公司提起诉讼，称其在未经许可的情况下收集用户的生物识别数据，违反了得州法律。诉状称谷歌将用户的生物识别数据用于增加公司广告和订阅收入以及提高其人工智能水平等商业目的。该行为违反了该州消费者保护法，该法要求公司在收集用户的生物识别数据之前需向用户告知并获得用户同意。

来源：https://www.wsj.com/articles/texas-sues-google-over-use-of-facial-images-11666276264?mod=Searchresults_pos1&page=1

4. ICO 对建筑公司侵犯员工隐私的行为处以 440 万英镑罚款

英国建筑公司 Interserve 的一名员工将网络钓鱼电子邮件转发给另一名员工，该公司未能采取适当的安全措施来防止网络攻击，导致公司 113000 名员工的个人数据被黑客窃取，面临泄漏的风险，其中包括个人信息，例如联系方式、国家保险号码和银行账户详细信息，还包括种族、宗教、任何残疾的详细信息、性取向和健康信息。ICO 调查发现，Interserve 未能跟进对网络攻击活动的初步警报，缺乏员工培训和风险评估，最终使其遭受网络攻击。英国信息专员办公室 (ICO) 因其没有保障其员工的个人信息安全对公司处以 440 万英镑的罚款。

来源：https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/biggest-cyber-risk-is-complacency-not-hackers/

（三）安全快讯

1. LofyGang 使用 100 多个恶意 NPM 包毒害开源软件

LofyGang 使用了 200 多个恶意 NPM 软件包，安装了数千个软件包来窃取信用卡数据、游戏和流媒体账户，然后在地下黑客论坛中公开被盗的证书和赃物。根据 Checkmarx 的一份报告显示，该网络攻击组织自 2020 年以来一直用恶意软件包感染开源供应链。

来源：https://www.darkreading.com/application-security/lofygang-100s-malicious-packages-poison-open-source-software

2. 美国安全公司推出“不要追踪儿童”工具，保护儿童隐私

美国有法律规定，公司不该对儿童进行在线追踪，但该法律并未被严格遵守。根据 Pixalate 最近的一项研究，超过三分之二的最流行的儿童 iPhone 应用程序收集和分享个人信息。美国的一家安全公司 Disconnect 在苹果应用商店推出“不要追踪孩子”(Do Not Track Kids)软件。将软件下载安装在孩子使用的 iPhone 或 iPad 上，该软件就会自动在整个设备商屏蔽追踪器，阻止大量的数据收集。

来源：https://gizmodo.com/do-not-track-kids-privacy-app-childrens-data-1849667220

3. 泄露约 30 万用户信息，丰田公开道歉

丰田汽车公司表示，使用 T-Connect 的近 30 万个客户电子邮件地址和电话号码可能被泄露。 T-Connect 是一种通过网络连接车辆的远程通信服务。受影响的客户为自 2017 年 7 月起使用电邮地址登入该服务网站的个人。

来源：https://finance.yahoo.com/news/toyota-says-information-296-000-073433129.html?gucco

unter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABB9IfqpyU_GffwmA45LYY-oafCu3O0IrbjtUXNclBLFRmSHmn39PupG5bwY_te-8L_RO31z9hjuQKeM9fLu16FdWQ0KQal06QpSC8UIVzL-Ati0PLut7xH7aUJw-vDvdiJQo9kWewnjBtXToCy3hoEAzQ3deZUAqCioSjrmzQ5u

4. 澳大利亚零售巨头 220 万用户数据被黑客窃取并在线出售

Woolworths 的子公司 MyDeal 披露了一起影响 220 万客户的数据泄露事件，黑客还试图在一个黑客论坛上出售被盗的数据。MyDeal 表示，在一名黑客使用受损的用户凭证访问该公司的客户关系管理(CRM)系统，攻击该公司系统。该公司表示，有 220 万客户受到了数据泄露的影响，包括姓名、电子邮件地址、电话号码、送货地址等信息。其中 120 万用户只有电子邮件地址被泄露。MyDeal 已经开始向受影响的客户发送数据泄露通知。

来源：https://www.bleepingcomputer.com/news/security/mydeal-data-breach-impacts-22m-users-stolen-data-for-sale-online/

5. 澳大利亚医疗保险公司 390 万用户信息全部泄露

Medibank 是澳大利亚最大的私人医疗保险提供商之一，为全国约 390 万客户提供服务。近期其宣称遭受了一次勒索软件攻击，攻击者获得了该公司大量的健康索赔数据，包括其子公司和国际学生的个人信息。该公司还表示将继续调查，以确定具体哪些数据在这次攻击中被盗，并将直接通知受影响的客户。

来源：https://thehackernews.com/2022/10/australian-health-insurer-medibank.html