2022 年 3 月

# 植德<国际数据合规热点速递>

（自 2022 年 3 月 1 日至 2022 年 3 月 31 日）

—植德律师事务所—

北京|上海|深圳|珠海
Beijing|Shanghai|Shenzhen|Zhuhai
www.meritsandtree.com

# 目录

## 一、美国篇

### 1. 美国参议院通过《加强美国网络安全法案》

美国参议院批准了新的网络安全立法，将强制关键基础设施组织在 72 小时内向网络安全和基础设施安全局(CISA)报告网络攻击，在 24 小时内 CISA 报告勒索软件付款。
《加强美国网络安全法案》在 2 月 8 日由参议员罗伯·波特曼和参议院国土安全和政府事务委员会主席加里·彼得斯提出后，于本周二获得一致通过。
该法案结合了《网络事件通报法案》、《2021 年联邦信息安全现代化法案》和《联邦安全云改进和就业法案》的部分内容，所有法案都是由彼得斯和波特曼撰写的，并在陷入困境之前提前退出委员会。
这份长达 200 页的法案包括几项旨在使联邦政府的网络安全态势现代化的措施，彼得斯和波特曼都表示，鉴于美国对上周有关俄罗斯与乌克兰所表明的立场，该立法是“迫切需要的”。
美国将面临来自俄罗斯越来越多的网络和勒索软件攻击，联邦政府必须迅速协调其对任何潜在攻击的反应。

【来源：腾讯网】

### 2. 美国参议员公布《禁止国税局生物识别法》草案

参议员 RickScott 提出了禁止国税局生物识别法案，该法案将禁止美国国税局(IRS)要求纳税人提交生物特征数据，例如“自拍”式面部扫描以登录账户、获取退款和报税。虽然美国国税局现在声称它不会进一步推行这一计划，但美国人民不能忽视这种对隐私的严重侵犯引发的对每个美国纳税人的分类数据的收集和安全性的担忧——尤其是在此前美国国税局的数据泄露事件泄露了美国纳税人的机密个人数据。

【来源：RickScott】

### 3. COVID-19 疫苗应用程序可能损害用户隐私

当今通常用作安全通行证和旅行护照的测试数字疫苗接种应用程序中约有三分之二表现出可能危及用户隐私的行为。数字护照应用程序存储个人 COVID-19 疫苗

接种状态、全名、身份证号、出生日期和其他个人身份信息(PII)的证明，这些信息以二维码编码或直接显示在应用程序中。然后，用户可以在需要进入病毒传播高风险区域、旅行所需区域等时出示此二维码或疫苗接种证明。Symantec 的团队研究了 40 个数字疫苗护照应用程序和 10 个验证（扫描仪）应用程序，发现其中 27 个存在以下隐私和安全风险。Symantec 报告中强调的第一类问题是，其中许多工具生成的二维码没有加密，而只是编码。编码是一个术语，用于表示将数据（在这种情况下为健康数据）转换为易于扫描和处理的数字格式。另一方面，加密使用加密算法将数据转换为不可读的形式。在这种情况下，只有经过授权的实体才拥有解密数据和读取数据的密钥。通过依赖编码而不是加密，任何在检查站使用 QR 扫描仪应用程序的人都可以解码扫描的数据并推断出敏感的个人详细信息。
Symantec 团队发现的另一个普遍问题涉及从云存储服务按需传输健康数据，在 38%的情况下不需要 HTTPS 连接，从而使用户容易受到中间人攻击.第三个问题涉及 Android 上的外部存储访问权限，这是一个有风险的批准，因为它允许应用程序无条件地访问设备的本地文件。这是 40 个应用程序中的 17 个或总数的 43%的问题。其他安全风险包括硬编码的云服务凭证和 SSLCA 验证的缺失，再次将用户的敏感数据置于风险之中。

【来源：Bleeping Computer】

**4. 美国 SEC 发布新规征求意见：上市公司信息安全事件应在 4 天内披露**

北京时间 3 月 10 日早间消息，美国证券交易委员会（SEC）投票公布一项新规定，加强上市公司发生数据泄露事件时的披露机制，包括披露方式，以及需要在多快时间内披露等。
根据 SEC 提议中的措施，公司必须在当前的报告文件，包括 8-K 表格中详细说明何时遇到了风险，以及采取了什么策略来应对和管理风险。
调整后的规则还要求公司对于信息安全风险对公司财务状况的可能影响进行分析。目前，这些调整正在征求公众意见。SEC 表示，这将帮助投资者更高效地评估信息安全风险，并为此做好准备。

【来源：新浪科技】

**5. 拜登就数字资产发布行政命令，涉及隐私和安全保障**

这份行政命令是美国“有史以来第一个解决风险和利用数字资产及其基础技术的潜在利益的整体政府方法”。拜登还指示财政部和其他联邦机构研究加密货币对金融稳定和国家安全的影响。

该命令制定了涵盖六个关键优先事项：消费者和投资者保护，金融稳定，非法融资，美国在全球金融体系和经济竞争力方面的领导地位，金融包容性，负责任的创新。
其中包括鼓励监管机构确保充分监督并防范数字资产带来的任何系统性金融风险；指示美国商务部与政府合作建立关于数字资产技术的框架；优先考虑隐私安全、打击非法利用，并减少负面气候影响；紧迫着手研发央行数字货币。
这份行政命令本身并没有引入新的法规，也没有向监管机构提供政府关于他们应该采用哪些法规的立场，该命令要求联邦贸易委员会、SEC 和 CFTC 等联邦机构一起协调对加密行业的监督，依据各个部门的任务复杂程度不同，白宫将给予 60~210 天不等的时间完成研究并形成相关报告，其中财政部需要“制作关于货币和支付系统未来的报告”。
路透 3 月 7 日援引消息人士称，拜登的命令设定了 180 天的期限，要求在此期间内提交一系列关于“货币的未来”和加密货币将在不断变化的环境中发挥的作用的报告。

【来源：经济形势报告网】

**6. 美国怀俄明州：制定《遗传学数据隐私法案》**

州长马克·戈登（Mark Gordon）于 2022 年 3 月 8 日签署了怀俄明州遗传数据隐私法案，该法案于 2022 年 7 月 1 日生效。
《遗传数据隐私法》要求任何从个人收集遗传数据的企业：(1)在收集之前向消费者提供有关遗传数据收集、使用和披露的透明信息，以及(2)在收集之前获得个人的明确同意遗传数据。该法案还包括严格禁止如何披露和保留遗传数据。该法律不适用于根据 HIPAA 收集受保护健康信息的涵盖实体或商业伙伴。
法律赋予消费者在数据不再被使用或出于收集目的需要时要求删除数据的法定权利。它还为消费者提供了向任何违反该法案的人寻求损害赔偿的私人诉讼权。

【来源：the National Law Review】

**7. 美国某公司遭遇集体诉讼：还没判决就同意赔偿用户 1480 万美元**

3 月 24 日消息，据 9To5Mac 报道，一起集体诉讼已在庭外和解，XX 公司同意向特定时间段内进行付费订阅的美国居民支付总计 1480 万美元（约 9442.4 万元人民币）。用户起诉 XX 公司称，该公司将用户数据存储在了非 XX 公司的服务器上，违反了服务条款和条件。而 XX 公司否认存在不当行为，但已同意支付这笔款项，以避免进行法院审判。和解协议包括在 2015 年 9 月 16 日至 2016 年 1 月 31 日期间支付订阅费用的所有美国用户，用户无需任何操作，邮箱将会收到通知，账户

将自动获得赔偿。数百万用户获得的赔偿会按照当初订阅的等级进行分配，比如订阅 1TB 的用户获得的钱会明显比订阅 50GB 的要多。

【来源：IT 之家】

## 二、欧盟、英国、亚洲篇

### 8. 英国信息专员办公室发布保护隐私的治理方法章节草案，征求意见咨询将于 9 月 16 日结束

近日，英国信息专员办公室（The Information Commissioner's Office，ICO）发布关于隐私保护治理方法的章节草案并公开征求意见，征求意见将于 2022 年 9 月 16 日结束。在草案第一章“匿名化简介”中，ICO 概述了在数据保护法背景下应用匿名化的法律、政策和治理问题。第二章“可识别性”侧重于如何在可识别性的背景下评估匿名化。ICO 探索了一系列可识别性、数据共享场景以及管理重新识别风险的指南。这些关键原则阐述了 ICO 对有效匿名化的看法。在第三章“假名化”中，ICO 解释了假名化和匿名化之间的主要区别。第四章“问责制和治理”解释了企业在匿名个人数据时应采取的治理方法，例如使用 DPIA 来识别和降低风险，ICO 提示称，技术需要和法律保持同步发展，以确保匿名化技术持续符合法律规定。

【来源：英国信息专员办公室】

### 9. 英国一律所因数据泄露违反 GDPR 规定，被英国 ICO 处以近 10 万英镑罚款

3 月 10 日，英国 ICO 对总部位于伦敦的 XXX 律师事务所处以 98,000 英镑的行政罚款，原因是其没有妥善保管其客户数据，并发生数据泄露事故，违反了 GDPR 的规定。据称，在 2020 年的一次黑客攻击中，该律师事务所储存的 972,191 个文件被黑客锁定，而其中的 60 个与法院数据包有关的文件还被发布到了暗网。而疏忽点正在于远程办公时律所允许员工在家中访问他们的网络数据库，因此黑客通过渗透到员工的系统从而获取了法律文件数据包。ICO 认为，该所在数据合规方面存在以下问题：第一，律所没有采取最基本的网络安全预防措施；第二，被盗取的法律文件包涉及到了高度敏感性的个人信息；第三，XXX 律所的网络很早之前就存在系统漏洞，但中间长达半年时间并未应用补丁；第四，没有通过政府主导的 CyberEssentials 认证。ICO 表示，一个加重处罚的因素就是 XXX 律所未能达

到 SRA 在其行为准则中规定的各种标准。XXX 律所强调它将很快重新申请 CyberEssentials 认证，并且表示在袭击发生后，他们已经成功实施了广泛的措施来防止此类犯罪事件的再次发生。

【来源：英国信息专员办公室】

**10. 英国政府就新电信安全法规和业务守则提案展开咨询**

3 月 1 日，英国政府就新电信安全法规和业务守则提案进行公开咨询。本次调查的目的是收集有关法规草案和业务守则草案对受影响企业的影响的信息。本次咨询旨在征求英国通信办公室（Ofcom）和公共网络和服务提供商的意见。2021 年《电信（安全）法案》（The Telecommunications (Security) Act 2021）授权英国政府制定安全法规和发布实践准则，用以保护公共电信网络和服务。该提案要求公共电子通信网络和服务提供者承担总体安全责任，并引入新的具体措施，要求其识别和防止安全隐患，减轻安全隐患带来的任何不利影响，其中明确了需要识别和防范供应链中第三方产品或服务提供商带来的潜在威胁。提案还为公共电子通信网络和服务提供者提供了详细的指导方针。

【来源：英国政府网】

**11. 爱尔兰数据保护委员会因一公司数据泄露，对其处以 1700 万欧元罚款**

3 月 15 日，爱尔兰数据保护委员会（The Irish Data Protection Commission，DPC）宣布，由于 X 公司在 2018 年 6 月至 12 月中发生的共 12 起数据泄露事件中违反欧盟《通用数据保护条例》（GDPR），将对其处以 1700 万欧元（约合人民币 1.18 亿元）的罚款。DPC 表示，在多次大规模个人数据泄露中，X 公司因违反《通用数据保护条例》第 5 条和第 24 条，未能证明其为保护欧盟用户的数据安全采取适当的技术和措施，将被罚款 1700 万欧元（约合人民币 1.18 亿元）。由于 X 公司的欧洲总部设在爱尔兰，所以由爱尔兰 DPC 牵头负责欧盟对其的相关执法。

【来源：爱尔兰数据保护委员会】

**12. 英国信息专员办公室对五家电话营销公司处以 40.5 万英镑罚款**

3 月 15 日，英国 ICO 宣布对某五家进行定向电话营销的公司处以 40.5 万英镑罚款，并要求立即停止电话营销行为。根据《隐私和电子通信条例》(Privacy and Electronic

Communications Regulations），若居民已在电话偏好服务中进行了登记，任何人不得向其拨打营销电话，除非其曾告知来电者希望收到此类电话。上述公司特意从第三方购买了患有老年痴呆等健康疾病的老年人和弱势群体的个人信息，有针对性地拨打了 75 万余通营销电话，导致部分受害者遭受了数千英镑损失，严重违反《隐私和电子通信条例》。

【来源：英国信息专员办公室】

**13. 德国巴登-符腾堡州针对 Cookie 和追踪器常见问题发布新指南（德国国家数据保护局发布最新 cookie 指南）**

2022 年 3 月 4 日，德国巴登-符腾堡州（Baden-Württemberg）为网站运营商和智能手机应用程序制造商发布了新指南，一份第三方 Cookie 常见问题解答文档。专员斯斯蒂芬·布林克（StefanBrink）指出 Cookie 和追踪器已将互联网和智能手机变成了受到严密监控的空间。这些监视措施现在可能被认为是正常的，但实质上是对公民权利的侵犯。指南提出，任何使用 Cookie 和其他跟踪技术、收集、处理和出售公民个人数据的人都必须遵守法律要求。通常，跟踪需要用户事先知情和自愿同意，这通常是通过 Cookie 横幅（“Cookie Banner”）获得的。因此，该文档还展示了 Cookie 横幅中发现的常见错误以及以数据保护为重点的整改示例。

【来源：巴登-符腾堡州数据保护和信息自由专员办公室】

**14. 乌克兰武装部队获准使用 Clearview AI 面部识别技术**

2022 年 3 月 13 日，乌克兰国防部被报道于前日开始免费使用 Clearview AI 的面部识别技术，乌克兰已在此前通过使用该技术发现俄罗斯袭击者、打击错误信息并识别死者。Clearview AI 是一家美国面部识别公司，数据库中共有 100 多亿张图片，其中 20 多亿来自于俄罗斯社交媒体 VKontakte。根据路透社报道，Clearview AI 的首席执行官在俄乌冲突开始后曾致函基辅，表示愿意提供援助，该公司的技术能够帮助乌克兰识别死者身份、确定俄罗斯特工人员、揭穿与战争有关的虚假社交媒体帖子以及让与家人分离的难民团聚。截至发稿，乌克兰当局尚未对路透社的评论请求作出回应。同时有批评者担心该技术一旦识别错误，可能导致平民死亡，并担心“这些技术和数据库被引入战区后很可能脱离控制”。

【来源：路透社】

**15. 法国数据保护机构 CNIL 发布 2022-2024 年战略规划**

近日，法国数据保护机构 CNIL 发布了 2022-2024 年战略计划，专注于以下三个关键主题：鼓励控制和尊重个人权利、将欧盟 GDPR 作为一项值得信赖的资产进行宣传，以及优先针对“高风险隐私问题的监管行动”。CNIL 主席玛丽-洛尔·丹尼斯表示，该计划“应该使 CNIL 能够以灵活的方式与公民、公司、协会和当局一起行动，从而建立一个值得信赖的数字社会。”

【来源：CNIL 官网】

**16. 韩国批准针对大型科技支付系统的法律细则**

据路透社报道，韩国政府近日批准了一项法律细则，禁止占主导地位的应用商店运营商强迫软件开发商使用他们的支付系统。据悉，该法律将于今年 3 月 15 日起实施。韩国放送通信委员会在一份声明中表示，该法律禁止通过不公平地利用移动应用市场运营商的地位，向移动内容提供商强制采用特定支付方式的行为。
但部分大型科技平台的倡导者却反对该法律，他们认为，此举将降低平台确保软件发行商可靠性的能力，使用户面临可能的欺诈或劣质产品，从而对消费者产生负面影响。

【来源：路透社】

**17. 首尔高等法院在 XX 诉讼中裁决中止韩国公平交易委员会命令**

据 KBS World 报道，首尔高等法院近期在 XX 公司对韩国贸易监管机构提起的诉讼中支持了原告，裁决中止了韩国公平交易委员会要求 XX 公司纠正不公平市场行为的命令。由于 XX 公司强迫智能手机制造商仅使用其 Android 移动操作系统，韩国公平交易委员会去年下令采取纠正措施，并对这家全球科技巨头处以罚款。本案的裁决与其他司法管辖区的类似调查结果相呼应，包括欧盟、英国和土耳其。XX 公司随后在今年一月份提起诉讼，要求撤销这一决定，并向首尔高等法院申请了禁令。法院已决定将韩国公平交易委员会的命令暂停至今年 8 月 31 日，称有必要推迟以防止对原告造成不可挽回的损害。但法院同时裁定，对 XX 公司处以的 2249 亿韩元罚款仍然有效。

【来源：KBS World】

## 特此声明

本刊物不代表本所正式法律意见，仅为研究、交流之用。非经北京植德律师事务所同意，本刊内容不应被用于研究、交流之外的其他目的。

如有任何建议、意见或具体问题，欢迎垂询。

## 编写合伙人

**王艺、陈文昊、龙海涛、吴旸、李凯伦**

（执行编辑：深圳办公室　虞晨、余灏、赵乐蓉）

Merits Tree
植德律师事务所

前 行 之 路 植 德 守 护

www.meritsandtree.com

北京：北京市东城区东直门南大街 1 号来福士中心办公楼 5 层、9 层 903-904

上海：上海市长宁区长宁路 1133 号长宁来福士广场 T1 办公楼 18 层 1801

深圳：深圳市南山区粤海街道科苑南路 2666 号中国华润大厦 9 层 905-906

珠海：广东省珠海市香洲区吉大情侣中路 39 号 3 栋 1702 室