2022 年 10 月

植德〈国际数据合规热点速递〉

（自 2022 年 10 月 1 日至 2022 年 10 月 31 日）

—植德律师事务所—

北京|上海|深圳|武汉|珠海|海口

Beijing|Shanghai|Shenzhen|Wuhan|Zhuhai|Haikou

www.meritsandtree.com

目录

一、美国篇 4

1. 美英两国政府间《为打击严重犯罪而访问电子数据的协议》生效 4

2. 美国加利福尼亚州州长签署两项新法案以保护堕胎隐私数据 4

3. 美国总统拜登签署行政命令实施《跨大西洋数据隐私框架》 4

4. 前 Uber 首席安全官因向黑客支付赎金被认定犯妨碍司法罪 5

5. 亚利桑那州总检察长与谷歌就欺诈用户获取位置数据达成 8500 万美元的和解5

6. LifeBridge Health 同意以 950 万美元就 2018 年数据泄露事件的集体诉讼达成和解 5

7. 美国白宫发布关于加强国家网络安全的简报 6

8. 伊利诺伊州北部联邦地区法院判决伯灵顿北方圣太菲铁路运输公司违反生物识别隐私法并需赔偿 2.28 亿美元 6

9. 瑞典隐私保护局对 Vklass 展开数据泄露事件调查 7

10. 美国得州总检察长起诉 Google 违法收集、使用生物识别信息 7

二、欧洲篇 7

11. 欧盟理事会正式通过《数字服务法》 7

12. 英国信息专员办公室发布《关于使用实时电话进行直接营销的指南》 8

13. 欧盟和日本拟协商将跨境数据流规则纳入经济伙伴关系协定 8

14. 欧洲议会批准关于跨欧盟边界共享信息的规则草案 8

15. 欧盟数据保护委员会通过程序方面的“愿望清单”和欧盟数据保护印章 9

16. 英国信息专员办公室发布《雇员监控指南草案》 9

17. 爱尔兰数据保护委员会发布有关 Meta 2021 年数据泄露事件的调查决定草案 9

18. 英国信息专员办公室因滥用客户个人信息对目录零售商 Easylife 处以 148 万英镑罚款 10

19. 欧盟委员会推出了欧盟首个获批的欧盟通用数据保护条例认证系统--Europrivacy 10

20. 英国 ICO 对建筑公司侵犯员工隐私的行为处以 440 万英镑罚款 10

21. 法国国家信息自由委员会对人脸识别数据库公司 ClearView AI 处 2000 万欧元罚款 11

三、其他篇 11

22. 澳大利亚采取行动加强银行和电信部门之间的信息共享 11

23. 世界经济与合作组织发布《数据跨境流动：评估关键政策和举措》报告 12

24. 尼日利亚发布《2022 年数据保护法案草案》 12

26. 巴西数据保护局发布《Cookies 和个人数据保护指南》 13

一、美国篇

1. 美英两国政府间《为打击严重犯罪而访问电子数据的协议》生效

10 月 3 日，美国司法部宣布美英两国政府间《为打击严重犯罪而访问电子数据的协议》生效。

该协议将允许服务提供商所持有的与预防、侦查、调查或起诉严重犯罪相关的信息和证据比以往任何时候都更快地被访问，使得执法机构更有效地获取将罪犯绳之以法所需的证据。两国将根据对方国家发出的合格的、合法的电子数据命令共享数据，而不必担心触犯对跨境披露的限制。

【来源：美国司法部】

2. 美国加利福尼亚州州长签署两项新法案以保护堕胎隐私数据

10 月 3 日消息，美国加利福尼亚州州长 Gavin Newsom 近日签署两项新法案，使其成为法律，将对个人堕胎数据保护产生影响。

两项法案分别为 AB 1242 号法案和 AB 2091 号法案。AB1242 号法案将通过阻止州外执法人员为推动反堕胎案件而对加利福尼亚公司执行搜查令等规定来保护堕胎数据隐私。AB 2091 号法案则禁止医疗服务提供者“为回应来自州外的传票或要求而发布有关寻求堕胎护理的个人的医疗信息”。

【来源：Health IT Security】

3. 美国总统拜登签署行政命令实施《跨大西洋数据隐私框架》

10 月 7 日，美国总统拜登签署《关于加强美国信号情报活动保障措施的行政命令》，以实施今年 3 月宣布的《跨大西洋数据隐私框架》下的承诺。

《跨大西洋数据隐私框架》是美欧之间就数据跨境流通的第三次尝试，该框架采用了新的美国情报收集隐私保护措施。此前的《安全港协议》、《隐私盾协议》均以欧盟法院认定无效告终。

《行政命令》要求对美国国家安全机构访问和使用欧盟和美国个人数据采取新的法律保障措施。其加强了当前美国情报收集对公民隐私自由的保障，并为个人数据被美国情报机构非法收集的公民创建了一套独立的、具有约束力的多层补救机制。

【来源：新浪财经】

4. 前 Uber 首席安全官因向黑客支付赎金被认定犯妨碍司法罪

10 月 6 日消息，美国联邦法院陪审团认定前 Uber 首席安全官 Joseph Sullivan 在美国联邦贸易委员会调查该打车软件 2016 年数据泄露事件期间，因未能向当局报告该事件及向黑客支付赎金而被认定犯有妨碍司法罪。

作为美国第一起针对公司高管因外部人员入侵而提起的重大刑事案件，一旦联邦法院正式宣判，**该案将成为美国首次对数据泄露事件的首席执行官责任作出裁决的标志**。目前，宣判日期尚未确定。

【来源：iapp】

5. 亚利桑那州总检察长与谷歌就欺诈用户获取位置数据达成 8500 万美元的和解

10 月 5 日消息，亚利桑那州总检察长 Mark Brnovich 宣布与谷歌就欺诈用户获取位置数据案达成 8500 万美元的和解。

亚利桑那州总检察长办公室于 2018 年开始调查该案，经调查发现，谷歌在用户禁用跟踪设置的情况下，仍收集和使用智能手机的位置数据。最终，双方就该欺诈用户获取位置数据行为达成和解，**和解的大部分资金将归入州政府的普通基金。**

【来源：iapp】

6. LifeBridge Health 同意以 950 万美元就 2018 年数据泄露事件的集体诉讼达成和解

10 月 6 日消息，LifeBridge Health 已同意以 950 万美元就 2018 年数据泄露事件的集体诉讼达成和解。

案中，LifeBridge Health 因感染恶意软件，使未经授权的个人可以访问托管其电子医疗记录、病人登记和计费系统的服务器。经调查，LifeBridge Health 确认 582,174

名患者的信息有可能被泄露，暴露的信息包括姓名、出生日期、地址、诊断、处方药物、临床和治疗信息、保险细节以及数量有限的社会安全号码。

根据和解条款，**LifeBridge Health 公司同意设立一个 80 万美元的基金来支付集体成员的索赔，并将投资 790 万美元用于额外的安全措施，以防止进一步的数据泄露，包括数据加密、网络监控、安全意识培训、资产跟踪和多因素认证。和解总额中剩余的 77.5 万美元将用于支付法律费用。**

【来源：HIPPA JOURNAL】

7. 美国白宫发布关于加强国家网络安全的简报

当地时间 2022 年 10 月 11 日，美国白宫发布了一份关于加强国家网络安全的简报（以下简称“简报”）。该简报列举了美国政府为改善关键基础设施、确保全国电动汽车充电站等新基础设施的网络安全而采取的几项措施。简报中还列明了美国政府为**打击勒索软件攻击而采取的一系列措施**，例如阻止犯罪分子转移非法资金等。值得注意的是，简报中提及了**为物联网设备开发标签的计划**。上述标签将用于展现物联网设备的网络安全情况，帮助消费者判断哪些物联网设备符合最高的网络安全标准，已经开始在常见的高风险技术，如路由器和家用摄像头上使用。

【来源：美国白宫官网】

8. 伊利诺伊州北部联邦地区法院判决伯灵顿北方圣太菲铁路运输公司违反生物识别隐私法并需赔偿 2.28 亿美元

伊利诺伊州北部联邦地区法院（位于芝加哥）判决伯灵顿北方圣太菲铁路运输公司（下简称“BNSF”）违反伊利诺伊州生物识别隐私法（下简称“BIPA”），需向提起集体诉讼的卡车司机支付 2.28 亿美元赔偿。BIPA 规定，收集生物识别信息必须经过书面同意，而 BNSF 公司在使用指纹系统来管理司机进出取货时，未经司机书面同意就收集了后者的指纹信息。陪审团据此认定 BNSF 违反 BIPA 达 45,600 次，以每次最高 5000 美元的额度最终对 BNSF 判处 2.28 亿美元赔偿款。据悉，伊利诺伊州**目前是美国唯一拥有该项生物识别隐私规定的州**，许多立法者曾尝试推翻该项法律，但至今仍未成功。

【来源：CBS News】

9. 瑞典隐私保护局对 Vklass 展开数据泄露事件调查

当地时间 2022 年 10 月 19 日，瑞典隐私保护局（下简称 IMY）宣布对 Vklass AB 学习平台的数据泄露事件展开调查。IMY 称，目前该机构已接收约 60 起个人数据泄露事故的上报，分析指向的结果是，Vklass 有关学校学生和教师的个人信息被违法下载。此外，根据欧洲《通用数据保护条例》（GDPR）的规定，该事件发生后，公司、当局和其它组织都有义务向 IMY 报告某些个人数据的泄露情况。

【来源：Data Guidance】

10. 美国得州总检察长起诉 Google 违法收集、使用生物识别信息

2022 年 10 月 20 日，美国得克萨斯州总检察长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，违反了该州法律。总检察长帕克斯顿称，谷歌违反了该州一项消费者保护法，该法要求公司在收集用户的生物识别数据之前，必须告知用户并获得同意。根据在得州米德兰县地区法院提交的诉状，**谷歌的生物识别数据收集行为可追溯至 2015 年，该州数百万居民受到影响。**

【来源：个人信息与数据保护实务评论】

二、欧洲篇

11. 欧盟理事会正式通过《数字服务法》

10 月 4 日，欧盟理事会正式通过《数字服务法》（DSA），以确保一个更安全的网络环境。

DSA 建立针对**不同类型中介服务的分层责任框架**，加强数字平台在打击非法内容和虚假信息及其传播方面的责任，并对“非法内容”的概念作了广义界定，有助于构建更加安全的在线环境。

下一步，经欧洲议会主席和欧盟理事会主席签署后，DSA 将在欧盟官方公报上公布，并于生效后 15 个月开始适用于各公司。

【来源：European Council】

12. 英国信息专员办公室发布《关于使用实时电话进行直接营销的指南》

10 月 5 日消息，英国信息专员办公室发布《关于使用实时电话进行直接营销的指南》。

该指南涵盖了营销人员如何遵守《2003 年隐私和电子通信条例》（PECR）的要求和建议的最佳做法。其中，包括概述了什么是直接营销电话，PECR 规定的内容以及企业在使用实时电话时应考虑的因素。

【来源：ICO】

13. 欧盟和日本拟协商将跨境数据流规则纳入经济伙伴关系协定

10 月 7 日，欧盟委员会发布消息称，欧盟和日本将于 2022 年 10 月 24 日正式开始谈判，将有关跨境数据流动的规则纳入其经济伙伴关系协定。

欧盟委员会表示，双方的企业都应该受益，并指出欧盟的目标是“通过禁止不合理的数据本地化要求来确保跨境数据流动，同时保留欧盟在个人和非个人数据保护和网络安全领域的监管自主权。”

【来源：欧盟委员会】

14. 欧洲议会批准关于跨欧盟边界共享信息的规则草案

10 月 10 日，欧洲议会公民自由委员会批准关于跨欧盟边界共享信息的规则草案。

规则草案旨在通过澄清信息交流的程序、规则和时限，促进不同欧盟国家警察和边境官员之间的交流，同时加强欧洲刑警组织的作用。

根据新规则，执法当局应考虑到信息的使用目的，按照与本国当局相同的条件，从其他欧盟国家当局处获得信息。与此同时，**欧洲刑警组织的安全信息交换网络应用程序将成为官方跨境交流的强制性渠道。**

【来源：欧洲议会】

15. 欧盟数据保护委员会通过程序方面的“愿望清单”和欧盟数据保护印章

10 月 12 日，欧盟数据保护委员会通过了一份国家程序法方面的“愿望清单”，希望在欧盟层面实现协调，以促进《通用数据保护条例》的“有力和迅速执行”。

该份“愿望清单”是 EDPB 关于执法合作的维也纳声明中规定的关键行动之一，包括“数据保护机构的调查权力”和 “程序性期限”。目前，该清单已送交欧盟委员会审议。另外，EDPB 还根据 GDPR 第 42（5）条通过了第一个欧盟数据保护印章。

【来源：EDPB】

16. 英国信息专员办公室发布《雇员监控指南草案》

10 月 12 日，英国信息专员办公室发布《雇员监控指南草案》，开展公众咨询。

该指南旨在根据数据保护立法提供关于监测工人的实用指南，并促进良好的做法。起草指南之前，ICO 已征求了雇主、专业协会、员工利益代表、招聘机构、就业纠纷解决机构、工人、志愿者、员工和就业技术解决方案供应商等相关利益相关者的意见。关于该指南草案的公众咨询将持续到 2023 年 1 月 11 日。

【来源：ICO】

17. 爱尔兰数据保护委员会发布有关 Meta 2021 年数据泄露事件的调查决定草案

10 月 3 日，爱尔兰数据保护委员会发布消息称，已根据《欧盟通用数据保护条例》第 60 条，向欧洲数据保护委员会成员提交了一份关于 Meta Platforms Ireland Limited（MPIL）2021 年 4 月数据泄露事件的调查决定草案。

在涉及全球超过 5.33 亿人和 150 万爱尔兰用户的违规事件发生后，爱尔兰数据保护委员会立即开始调查。该调查涉及 MPIL 是否遵守 GDPR 第 25(1)和 25(2)条规定的义务（“设计和默认的数据保护”）的问题。

【来源：DPC】

18. 英国信息专员办公室因滥用客户个人信息对目录零售商 Easylife 处以 148 万英镑罚款

10 月 6 日，英国信息专员办公室对目录零售商 Easylife 处以 148 万英镑的罚款，原因是该公司**利用 14.54 万名客户的个人信息来预测他们的医疗状况，并在未经他们同意的情况下向他们提供健康相关产品**。同时，该公司还因拨打 1,345,732 个掠夺性直销电话被额外罚款 130,000 英镑。

【来源：ICO】

19. 欧盟委员会推出了欧盟首个获批的欧盟通用数据保护条例认证系统--Europrivacy

欧盟委员会推出了欧盟首个获批的欧盟通用数据保护条例认证系统--Europrivacy。该数据保护印章最近得到了欧洲数据保护委员会的批准，该委员会表示，其目的是"提高（公司和服务）业务的价值和对其服务的信任"。该委员会补充说，Europrivacy "包括许多部门的广泛的数据处理业务"，**除了证明 GDPR 的合规性外，还可以用来评估跨境数据转移的充分性，并选择适格的数据处理者。**

Europrivacy 是第一个证明符合《通用数据保护条例》（GDPR）的认证机制。它标志着在确保尊重欧盟开创性的隐私保护规则方面**取得了飞跃性进展。**

【来源：数据法盟】

20. 英国 ICO 对建筑公司侵犯员工隐私的行为处以 440 万英镑罚款

英国信息委员会办公室(以下简称'ICO') 于 2022 年 10 月 24 日发布了罚款通知，其中对 建筑公司 Interserve Group Limited 处以 440 万英镑的罚款，理由是其违反了一般数据保护条例（以下简称“GDPR”）第 5(1)(f) 条和第 32 条。在 ICO 收到 Interserve 的个人数据泄露通知后，及时进行了调查。

值得注意的是，ICO 发现 Interserve 的以下行为违反了 GDPR 第 5(1)(f) 条：

- 在不受支持的操作系统上处理个人数据，这些操作系统不再是修复已知漏洞的安全更新的主题；
- 未能实施适当的端点保护；

- 未能对员工进行适当和有效的信息培训；
- 未能更新协议；
- 未能对最初攻击的原因进行有效和及时的调查；
- 未能有效管理特权帐户访问。

此外，鉴于上述 Interserve 数据安全措施的缺陷，ICO 还发现 Interserve 未能实施适当的技术和组织措施来确保其处理系统和服务的持续机密性、完整性、可用性、访问和弹性违反 GDPR 第 32(1)(b) 和 (c) 条。此外，ICO 表示，Interserve 未能定期测试、评估和评估技术和组织措施的有效性，以确保违反 GDPR 第 32(1)(d) 条的处理安全。

【来源：企业数据合规官】

21. 法国国家信息自由委员会对人脸识别数据库公司 ClearView AI 处 2000 万欧元罚款

2022 年 10 月 20 日，法国国家信息自由委员会（CNIL）对美国人脸识别数据库公司 ClearView AI 做出罚款 2000 万欧元的决定，其理由为 ClearView AI 违法收集法国公民个人信息，违反了欧洲《通用数据保护条例》（GDPR）多条法律规定。据 CNIL 调查，ClearView AI 在未经个人同意的情况下从公开网络和社交媒体平台上收集了超过 200 亿张人脸图像，使 ClearView AI 用户能够在上传某人人脸面部信息后获得对应者的其他个人信息。此前，该公司也已经因为同一理由被英国信息专员办公室（ICO）开处过罚款。

对此，CNIL 认定 infogreffe 涉嫌违反 GDPR 第 5(1)(e) 条规定的数据保留要求和第 32 条规定的数据安全义务，遂对其处以罚款。

【来源：法国国家信息自由委员会】

三、其他篇

22. 澳大利亚采取行动加强银行和电信部门之间的信息共享

10 月 6 日，在澳大利亚电信公司 Optus 遭到网络攻击后，澳大利亚政府发布了新

的消费者隐私规则，旨在更好地促进**银行与电信供应商之间的“目标数据共享”**。

根据修订后的规则，电信供应商**将能够与银行共享政府颁发的身份证明文件，以便其能够对受数据泄露影响的客户进行“强化监测”**。该类信息只能用于应对网络安全事件的唯一目的，且银行必须在不再需要时销毁这些信息。

【来源：IAPP】

23. 世界经济与合作组织发布《数据跨境流动：评估关键政策和举措》报告

10 月 12 日，世界经济与合作组织（OECD）发布《数据跨境流动：评估关键政策和举措》报告。

OECD 旨在推动七国集团成员之间的“共同理解和对话”，同时支持“在政策和监管方法方面取得协调和一致的进展，充分利用数据的潜力促进全球经济和社会繁荣”。《数据跨境流动：评估关键政策和举措》报告对跨境数据流动的主要政策和倡议进行了评估，为七国集团成员参与这一政策议程提供信息和支持。具体地，报告涵盖了单边合作、政府间进程、以及技术和组织措施等方面的内容。

【来源：OECD】

24. 尼日利亚发布《2022 年数据保护法案草案》

近日，尼日利亚国家信息技术发展局（NITDA）发布《2022 年数据保护法案草案》（以下简称《法案》）。《法案》分为十三个部分，共计六十七条，概述了处理个人数据的原则与法律依据，列举了数据主体的权利及数据控制者的一些义务，较为系统地规范了**数据违法行为的救济途径与惩罚措施，以及配套的法律程序**。《法案》设专章建立了尼日利亚数据保护委员会，对数据控制者、处理者在尼注册或者具有在尼经常居住地、经营地，数据处理活动发生在尼境内，及定位、监控或者向尼居民销售本国居民个人数据等情况下的个人数据处理活动进行监管。

【来源：尼日利亚国家信息技术发展局】

25. 韩国将设立国家网络安全工作组

2022 年 10 月 17 日，韩国总统室发言人在记者会上发布了关于设立国家网络安全工作组的消息。该工作组将由韩国国防部、国家情报院、大检察厅、警察厅和军事安全支援司令部等部门高层人士参与，并将在国家安保室长的主持下定期召开网

络安全状况检查会议。Kakao 服务器此前的瘫痪事件给本次工作组的成立带来了契机。Kakao 是韩国国家基础通信网，此前由于数据中心发生火灾造成大量服务器损毁瘫痪，给韩国国家安全造成威胁，近日已经基本修复完毕。

【来源：中国新闻网】

26. **巴西数据保护局发布《Cookies 和个人数据保护指南》**

2022 年 10 月 18 日，巴西数据保护局（ANPD）发布了《Cookies 和个人数据保护指南》。该指南旨在澄清与 Cookies 政策和 Cookies 横幅相关的实践操作，它明确了 Cookies 的定义，概括性地给出了对 Cookies 政策和 Cookies 横幅的最佳实践方法，同时也进一步详细说明了巴西《一般个人数据保护法（LGPD）》（2019 年 7 月 8 日第 13.853 号法律修订）的适用与具体义务要求。

【来源：Data Guidance】

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

（执行编辑：深圳办公室 刘时扬）

Merits Tree
植德律师事务所

前 行 之 路 植 德 守 护

www.meritsandtree.com