2022 年 9 月

植德〈国际数据合规热点速递〉

（自 2022 年 9 月 1 日至 2022 年 9 月 30 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

1. 拒绝投票，佩洛西反对拟议的《美国数据隐私和保护法》

近日，美国众议院能源和商业委员会通过了修订版的《美国数据隐私和保护法》（American Data Privacy and Protection Act，ADPPA），该法案即将进入全众议院院投票阶段。其前景要取决于众议院议长南希·佩洛西（Nancy Pelosi）——她将决定何时或是否将在众议院审议全面的隐私法案。经过数周的支持和反对投票的敦促，佩洛西在国会重启之前发表了一份声明，称她不会对当前版本的 ADPPA 进行投票。佩洛西的立场影响了 ADPPA 的立法进程，而这又取决于投票前，就《美国数据隐私和保护法》可以达成什么样的协议。虽然佩洛西的选择并不意味着该法案的最终终结，但它可能被证明是“今年总体上通过该法律的可能性的现实终结”。。

【来源：IAPP】

2. 美驻华使领馆过度采集中方雇员信息，数据或供给美国情报部门

近日，曾在美驻华使领馆工作的人士表示，美方涉嫌以“背调”为由强迫中方雇员提交个人、家庭甚至邻居的信息。据透露，其中除了几乎所有的亲属信息外，竟然还要提供一位邻居的信息，而且是必填项。赵平说，曾有美国使领馆的同事向他的邻居要电话，遭到邻居质疑：“美国人是不是不信任你们中国员工啊？”除了常规调查，有时驻美使领馆安全官还会直接与中方雇员进行安全审查谈话。态度趾高气扬，问话咄咄逼人，令人厌烦。更令人不安的隐患在于，这些被收集的个人信息的流向并不在他们自己掌控之中。中方雇员信息或被“分享”给美情报机构。。

【来源：网易】

3. 美国国税局泄露 12 万纳税人个人信息，含姓名、联系方式和财务信息等

9 月 2 日，美国国税局承认日前在其官网上泄露了一份涉及约 12 万纳税人的机密信息。美国国税局称，机密信息涉及的数据来自企业纳税申报表——990-T 表，泄露的信息包括纳税人姓名、联系方式和拥有个人退休账户群体相关收入的财务信息，但不包括社会安全号码、完整的个人收入信息、详细的财务账户数据或其

它可能影响纳税人信用的敏感数据。目前，美国国税局表示泄露纳税人机密信息是无意之举，发现这一错误后已从网站上删除相关内容，后续将联系所有受影响的纳税人。

【来源：海外网】

4. XX 内部计算机网络遭受黑客攻击

9 月 15 日，XX（某打车软件）获悉内部计算机网络遭到黑客攻击，并在调查期间关闭了多个工程和内部通信系统。据报道，被指控的黑客向网络安全研究人员和《纽约时报》发送了电子邮件、云存储和代码存储库的图像。据与黑客通信的 Yuga Labs 安全工程师 Sam Curry 说称，该黑客是通过向 XX 员工发送短信并伪装成公司技术高层而获得访问权限的。

【来源：iapp】

5. XXX 因违反伊利诺伊州《生物识别信息隐私法》面临集体诉讼

9 月 1 日，美国伊利诺伊州居民 James Luthe 向当地法院提起诉讼，指控 XXX（某美国零售巨头之一）通过摄像头、视频监控系统和 ClearView AI 提供的“面部识别数据库”，非法收集、存储和使用生物识别数据，而未按照伊利诺伊州《生物识别信息隐私法》（BIPA）的要求获得伊利诺伊州公民的同意。该诉讼可能将被裁定为集体诉讼。BIPA 规定，私人实体不得收集个人的生物识别标识符，除非其首先通知个人其标识符正在被收集，为什么以及收集多长时间，并收到该个人的“书面同意” 作为回应。BIPA 还规定，除其他要求外，私营实体不得出售、租赁、交易或以其他方式从个人的生物识别标识符中获利。

【来源：documentcloud】

6. 谷歌就 2018 年位置数据诉讼“原则上”达成和解

9 月 13 日消息，谷歌和智能手机用户达成了一项“原则上的协议”，以解决一项长达四年的联邦集体诉讼，该诉讼指控谷歌在用户选择不进行跟踪时跟踪他们的位置。该诉讼最初是由圣地亚哥居民拿破仑·帕塔西尔于 2018 年提起的，指控谷歌在“位置历史记录”设置被关闭的情况下仍旧收集位置数据，除非人们关闭一个单独的设置——“网络和应用程序活动”。目前，和解方案尚未最终敲定。

谷歌和消费者的法律顾问表示，他们计划“共同努力敲定一份长期和解协议”，并于 10 月 12 日发布另一份报告。

【来源：mediapost】

7. 西北工业大学遭网络攻击，源头系美国国家安全局

9 月 5 日，国家计算机病毒应急处理中心发布《西北工业大学遭美国 NSA 网络攻击事件调查报告》（之一）。2022 年 6 月 22 日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布《警情通报》，证实在西北工业大学的信息网络中发现了多款源于境外的木马样本，西安警方已对此正式立案调查。国家计算机病毒应急处理中心和 360 公司联合组成技术团队，全程参与了此案的技术分析工作。本次调查发现，在近年里，美国 NSA 下属 TAO 对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备（网络服务器、上网终端、网络交换机、电话交换机、路由器、防火墙等），窃取了超过 140GB 的高价值数据。TAO 利用其网络攻击武器平台、“零日漏洞”（0day）及其控制的网络设备等，持续扩大网络攻击和范围。经技术分析与溯源，技术团队现已澄清 TAO 攻击活动中使用的网络攻击基础设施、专用武器装备及技战术,还原了攻击过程和被窃取的文件,掌握了美国NSA及其下属TAO对中国信息网络实施网络攻击和数据窃密的相关证据，涉及在美国国内对中国直接发起网络攻击的人员 13 名，以及 NSA 通过掩护公司为构建网络攻击环境而与美国电信运营商签订的合同 60 余份，电子文件 170 余份。

9 月 13 日，国家计算机病毒应急处理中心发布《美国 NSA 网络武器“饮茶”分析报告》，报告显示，在西北工业大学的网络服务器设备上发现了美国国家安全局（NSA）专用的网络武器“饮茶”（NSA 命名为“suctionchar”），“饮茶”编码复杂，高度模块化，支持多线程，适配操作系统环境广泛，包括 FreeBSD、Sun Solaris 系统以及 Debian、RedHat、Centos、Ubuntu 等多种 Linux 发行版，反映出开发者先进的软件工程化能力。“饮茶”还具有较好的开放性，可以与其他网络武器有效进行集成和联动，其采用加密和校验等方式加强了自身安全性和隐蔽性，并且其通过灵活的配置功能，不仅可以提取登录用户名密码等信息，理论上也可以提取所有攻击者想获取的信息，是功能先进，隐蔽性强的强大网络武器工具。在此次针对西北工业大学的攻击中，美国 NSA 下属特定入侵行动办公室（TAO）使用“饮茶”作为嗅探窃密工具，将其植入西北工业大学内部网络服务器，窃取了 SSH、TELNET、FTP、SCP 等远程管理和远程文件传输服务的登录密码，从而获得内网中其他服务器的访问权限，实现内网横向移动，并向其他高价值服务器投送其他嗅探窃密类、持久化控制类和隐蔽消痕类网络武器，造成大规模、持续性敏感数据失窃。随着调查的逐步深入，技术团队还在西北工业大学之外的其他机构网络中发现了“饮茶”的攻击痕迹，很可能是 TAO 利用“饮茶”对

中国发动了大规模的网络攻击活动。

【来源：国家计算机病毒应急处理中心】

8. 16 家金融公司被处 18 亿美元罚款，违反记录保存规则

美国监管机构当地时间 27 日对 XX 银行集团、XX 银行等 16 家华尔街金融公司处以总计 18 亿美元（约合人民币 129 亿元）的罚款，原因是这些公司员工使用个人电子设备和手机应用程序商谈业务，却没有保存相关通信记录。众多华尔街银行多年来难以杜绝员工在上班期间使用个人电子设备，通常是完全禁止员工把个人设备带入交易大厅。**新冠疫情暴发后，员工居家办公导致这一问题加剧。美国商品期货交易委员会一名委员则表示，员工使用个人设备是为了逃避监管，有时甚至是在高管指示下进行。那些高管明知违规，却想隐藏商业沟通内容。**

【来源：环球网资讯】

9. 美国政府问责局（GAO）：24 个机构的隐私项目审查及关键发现

近年来，随着新技术的出现和个人信息的广泛利用，个人隐私的保护已成为一个十分重要的问题。联邦机构为各种政府项目收集和处理大量的 PII，因此，他们必须确保他们收集、存储或处理的任何 PII 都不受未经授权的访问、篡改或丢失的保护。GAO 审查联邦机构的隐私项目，**包含了以下内容：(1)机构为确保隐私保护而建立的项目的程度；(2)机构在实施其隐私保护计划时所遭遇的挑战；(3)机构使用隐私影响评估报告的好处和限制；(4)有多少机构拥有专门处理隐私问题的高级官员。**机构和隐私专家发现了隐私影响评估的好处，包括提供公共信息和管理风险。然而，他们也发现了 可能限制评估有效性的因素，如机构并不总能尽早启动隐私影响评估，从而影响项目决策；隐私保护计划不知晓所有带有 PII 的代理系统；隐私保护项目无法让机构工作人员负责开发隐私影响评估。如果没有充分建立隐私保护计划的这些要素，机构就无法保证自己始终如一地实施隐私保护。在实施隐私保护计划时，机构最常面临的挑战如下。更多的信息共享可以帮助机构应对某些挑战。

挑战	报告挑战的机构数量
有足够的资源	21
将隐私要求应用于新技术	20
聘请隐私人员	17
集成隐私和安全控制	16
与其他机构办公室和项目协调	15
确保机构计划正在实施隐私要求	15
留住隐私人员	15
培训隐私专家	14

资料来源：GAO 对机构数据的分析。| GAO-22-105065

【来源：赛博研究院】

10. 华盛顿拟通过《停止算法歧视法案》，立法明确消除算法偏见

9 月 22 日，在美国电子隐私信息中心（Electronic Privacy Information Center，简称“EPIC”）的敦促下，华盛顿特区政府运营和设施委员会（the DC Council Committee）在当天的听证会上讨论了**《停止算法歧视法案》**（Stop Discrimination by Algorithms Act，以下简称“《法案》”），以禁止特定主体在算法决策中使用某些类型的数据，确保消除算法偏见。

首先，《法案》通过明确禁止算法歧视，阐明了民法规则如何在新的数字空间中适用。涉及到生活核心领域（包括教育、就业、住房以及医疗保健和保险等重要服务）的定向广告和自动化决策，都需遵守新立法。

其次，《法案》要求公司事先做好工作确保其算法的公平性，并以“年度偏见审计”的形式向审计长办公室（Office of the Auditor General，简称“OAG”）汇报。

第三，《法案》要求公司披露使用算法的情况，并在做出不利决定（如拒绝抵押贷款、收取更高利率）时向消费者提供更强有力的解释以增强透明度。

【来源：EPIC、CENTER FOR DATA INNOVATION】

11. 网络攻击扰乱酒店供应链！XX 酒店集团加盟商损失惨重

9 月 6 日，XX 酒店集团表示，检测到技术系统中存在未授权活动，导致预订及其他系统出现严重中断。有加盟的酒店业主估算，网络攻击造成的平均损失在 30000 到 75000 美元之间，XX 酒店集团全球约有 6000 家酒店；酒店业主们希望获得赔偿并了解事件细节，为此已向 XX 酒店集团发起集体诉讼。9 月 27 日消息，近期针对 XX 酒店集团的网络攻击影响到了各特许加盟商的业务，导致愤怒的客户、收入损失乃至集体诉讼隐患正持续发酵。

【来源：安全内参】

12. 纽约拟立法全面保护儿童数据隐私 或将强制采取在线安全措施

加州立法机构在 8 月底一致通过了《加州适龄设计规范法案》，该法案要求在线平台考虑儿童用户的最大利益，网站和应用程序限制某些功能，并默认保护儿童身心健康和福祉的隐私和安全设置。纽森州长表示：“我们正在加利福尼亚州采取积极行动，以保护我们孩子的健康和福祉。”

法案禁止儿童可能访问的在线服务、产品或功能的公司使用其个人信息；收集、销售或保留儿童的地理位置；在默认情况下对儿童进行分析画像；引导或鼓励儿童提供个人信息。另外，还要求隐私信息、服务条款、政策和社区标准透明，具备应对措施来帮助儿童行使其隐私权。

这项法律可能适用于 18 岁以下人群可能使用的诸多数字产品，包括社交网络、游戏平台、联网玩具、语音助手和智能学习工具等。

作为《加州适龄设计规范法案》的一部分，还将成立儿童数据保护工作组，在 2024 年 1 月之前向立法机构提交一份关于实施最佳做法的报告。这项立法的影响还可能超出加州范围，促使许多服务机构在全美引入变革。

【来源：TechWeb】

13. XXX 支付 3500 万美元解决数据安全指控

美国投资银行 XXX 将支付 3500 万美元，以了结美国证券交易委员会对它一家子公司的指控。委员会指这家公司在替换公司硬盘和服务器期间未能保护数百万客户个人数据。报道援引彭博社称，XXX9 月 20 日在没有承认或否认控罪的情况下，同意支付罚款以达成和解。美国证券交易委员会(SEC)指 XXX 不当地处置了数千台设备，其中一些在没有确定所含客户数据已删除的情况下就在网上拍卖。从 2015 年以来的五年内，大约 1500 万客户的资料被泄露。委员会称，该公司违反了"保障和处置规定"。

【来源：中新经纬 APP】

14. 全球最大航空公司发生数据泄露事件

美国航空公司上周末（9 月 16 日）发出客户通知信确认遭遇黑客攻击，声称攻击者获取了数量不明的客户和员工电子邮件账户和敏感个人信息。

美国航空公司的企业传播高级经理 Andrea Koos 告诉 BleepingComputer，该公司员工的账户在一次网络钓鱼活动中遭到入侵，但拒绝透露有多少客户和员工受到影响，而是说这是"非常少数"。

根据通知，美国航空公司在 7 月 5 日发现了这一漏洞，立即保护了受影响的电子邮件账户，并聘请了一家网络安全取证公司来调查安全事件。

【来源：安全内参】

15. 美国国土安全部宣布首个针对各州地区网络安全拨款 10 亿美元的计划

据 E 安全网 9 月 20 日消息，美国国土安全部（DHS）公布了一项专门针对美国各州及地方政府的首个网络安全拨款计划。该计划将在 4 年内向各州及地方政府提供 10 亿美元的资金，其中 1.85 亿美元可用于 2022 财年，以支持各州及地方政府解决其信息系统中的网络风险。网络安全拨款计划是美国网络安全与基础设施安全局（CISA）推进应对网络安全威胁的重要一步，有助于 CISA 与各州及地方建立伙伴关系，以共同应对网络安全挑战。

【来源：全球技术地图】

16. 拜登签署行政令 阐明美国 CFIUS 审查将更关注特定国家安全风险

美国总统拜登日前签署行政命令，要求美国外国投资委员会(CFIUS)加强审查构成国家安全风险的特定领域交易。

对此，束珏婷在当天举行的新闻发布会上指出，美方泛化国家安全概念，不断扩大对外资的审查范围，加严审查条件，设置繁琐审查程序。这不利于正常的投资和贸易往来，不利于促进增长和增加就业，既损害他国，也影响自身。

束珏婷称，美方应纠正滥用安全审查的做法，为企业投资提供公平、稳定、可预期的营商环境。

【来源：中国新闻网】

17. 美方将审计中概股，互联网巨头将首批接受审计底稿检查

市场机构的数据显示，截至 8 月，美国今年 IPO 渠道总募资金额只有 51 亿美元，远低于过去 20 多年约 330 亿美元的同期平均水平。2021 年上半年，共有 37 家中概股在美股 IPO，而 2022 年同期只有 3 家。

根据 PCAOB 的数据，上述四大会计师事务所为 168 家在美国上市的中国大陆公司中的 130 多家提供审计服务，占总数的 78%以上。截至 6 月，总共约有 168 家在美国上市的中国公司接受了 15 家在 PCAOB 注册的香港和内地会计师事务所的审计。这些公司的总市值达到 1.5 万亿美元，如果这些公司连续三年不允许 PCAOB 审查其审计记录，那么根据《外国公司问责法》，它们将被美国交易所除名。

据此前的外媒报道，美国监管机构已选定阿里巴巴、网易、百度、京东以及百胜中国等作为首批接受审计底稿检查的中概股公司。

根据中美在 8 月底就中概股审计达成的协议，中国证监会将安排在美上市的中国公司及其会计师事务所将其审计底稿和其他数据从内地转移到香港，在 9 月中旬接受美方检查。

根据美国《华尔街日报》16 日的报道，SEC 主席加里·根斯勒披露，美国 PCAOB 的工作人员预计将于 9 月 19 日开始检查在美上市中概股的审计底稿。根斯勒在参议院银行委员会听证会上称，整个过程需要 8 到 10 周，或在 2022 年 12 月初得出检查结果。他还表示，中方监管机构表示会遵守协议规定。

【来源：环球时报】

二、欧洲篇

18. 欧洲拟立法全面禁止人脸识别

欧盟拟禁止在公共场所使用人工智能相机扫描和识别人脸的努力正在获得支持。据 Politico 报道，越来越多的欧盟议会成员支持全面禁止面部识别技术。欧盟议会第三大集团 Renew 与绿党、社会党和民主党签署了一项倡议，支持禁止 "不加区分地实时扫描人群 "的技术。面部识别的反对者声称，这项技术是政府的专制工具，同时容易表现出对有色人种的偏见。民族国家可能反对这项禁令，以便他们的安全机构能够继续使用面部识别。来自 Renew 的支持，与绿党和社会党及民主党团体一起支持一项禁令，表明欧洲政治领导层中越来越多的人赞成对人工智能的限制。。

【来源：politico】

19. 阻止欧洲刑警组织“囤积”个人数据！EDPS 要求驳回两项修正案

欧盟监管机构表示，允许欧洲刑警组织警察保留与犯罪活动无关的个人数据的规则违背了欧洲的数据隐私保护要求，更破坏了监管机构的权力和作用。因此，欧洲数据保护主管（EDPS）已要求欧洲最高法院放弃对 6 月 28 日生效的欧洲刑警组织条例的两项修正案，避免警方囤积这些数据。总而言之，EDPS 在年初告诉警方不要囤积这些记录。几个月后，欧洲立法者通过更新规则授权了这种做法，导致监管机构对修正案提出质疑。为了解决这个问题，该命令要求欧洲警察在收集个人数据后的六个月内检查个人是否与犯罪活动有关。如果这些人没有相关联系，那么执法机构应该删除这些个人信息。

【来源：The register】

20. 澳大利亚运营商 Optus 数据库泄露，约 40%国民信息被盗

据路透社报道，澳大利亚第二大运营商 Optus 一直在与客户联系，告知他们的数据被泄露，至少包括 1000 万客户的个人信息受损，受影响的用户数量相当于该国 2590 万人口的 40%左右。此次数据库泄露的规模使其成为该国历史上最大的网络安全事件之一。据报道，此次涉案信息包括数据库中用户的姓名、出生日期、家庭住址、电话号码、电子邮件地址、驾照号码、护照号码等。

澳洲当局正在调查可能的线索。澳大利亚联邦警察告诉路透社，在“暗网”和其他来源可以购买到 Optus 客户数据和其他“凭证”。Optus 指出，由于执法部门正在调查此事，因此它可以发布的与此数据泄露有关的信息量是有限的。该运营商指出，属于黑客的 IP 地址在欧洲不同国家之间移动。他们建议客户留意他们账户中的任何异常和可疑活动。

【来源：IT 之家】

21. 欧盟《数字市场法》正式签署，将于六个月后实施

2022 年 7 月 18 日，欧盟 27 个成员国一致批准《数字市场法》。该法案旨在规范数字市场秩序，限制数字科技巨头过度垄断和不正当竞争行为。当地时间 9 月 14 日，欧洲议会主席和欧盟理事会事务部长正式签署了该法案。随后欧盟将在其官方刊物上正式发布《数字市场法》并将于 6 个月后实施该法案。。

【来源：欧盟委员会】

22. 欧盟《人工智能责任指令（提案）》发布

9 月 28 日，欧盟委员会通过了一项关于协调人工智能责任指令中围绕消费者赔偿的规则的提案。拟议的规则将允许消费者对人工智能技术的 "错误行为 "造成的损害提出索赔。委员会表示，索赔的依据可以包括 "侵犯隐私，或由安全问题造成的损害"，同时还指出，"如果有人在涉及人工智能技术的招聘过程中受到歧视"，都可以提出索赔。欧盟委员会首次提出有针对性地协调各国人工智能的责任规则，使人工智能相关损害的受害者更容易获得赔偿。根据《人工智能白皮书》的目标和委员会 2021 年的《人工智能法》提案，为人工智能的卓越和信任制定了一个框架——新规则将确保受害者在受到人工智能产品或服务的伤害时得到同样的保护标准，就像他们在任何其他情况下造成伤害一样。。

【来源：欧盟委员会】

23. 社交巨头 Instagram 被裁定侵犯儿童隐私，罚款 27.8 亿创纪录

当地时间 9 月 5 日，爱尔兰数据隐私监管机构的一位发言人表示，在对社交网络 Instagram 处理儿童数据的情况进行调查后，爱尔兰数据隐私监管机构已同意对其处以创纪录的 4.05 亿欧元（约 27.82 亿元人民币）罚款。该调查于 2020 年开始，重点关注 13 至 17 岁的儿童用户。Instagram 允许这些儿童用户运营商业账户，涉嫌违反欧盟《通用数据保护条例》(GDPR)。爱尔兰监管机构在去年 12 月完成了 Instagram 调查的裁决草案，并在欧盟监管大型跨国公司的“一站式”系统下与其他欧盟监管机构分享。

【来源：IT 之家】

24. 英国信息专员办公室发布《匿名化、假名化及隐私增强技术指南（草案）》

9 月 7 日，英国信息专员办公室（ICO）发布《匿名化、假名化及隐私增强技术指南（草案）》。

隐私增强技术（Privacy-enhancing technologies, PETs）是指通过最小化个人数据使用、最大化数据安全、提升个人自主权来实现基本数据保护原则的技术。草案共分为两部分，分别介绍 PETs 如何有助于数据保护合规和实践中常见的 PETs 类型。草案承认 PETs 有助于实现“通过设计和默认方法的数据保护”，并协助组织遵守数据处理的最小化原则，但也指出 PETs 不是满足数据保护合规义务的“灵丹妙药”，数据处理仍然需要合法、公平和透明。

【来源：ICO】

25. 法国国家信息与自由委员会发布《个人登录令牌或令牌访问》指南

9 月 8 日，法国国家信息与自由委员会（CNIL）发布《个人登录令牌或令牌访问》指南，对数字令牌身份验证的用途进行评估，分析其带来的安全挑战，并提出最佳实践建议。

CNIL 警告，以链接形式制成的访问令牌可能会带来安全风险，因为该令牌可以允许使用者持续访问互联网上的个人数据，如果访问令牌由第三方获取并使用，则可能导致个人数据、用户账户或在线个人空间的完整性或机密性受到损害。同时，如果没有双因素身份验证，单用户远程登录令牌还会导致“额外的安全性风险”。

为此，CNIL 提出以下建议：1）记录令牌创建和使用情况；2）明确令牌的有效期；3）生成不包含个人数据或变量的身份验证链接；4）若令牌允许访问个人数据，则强制实施新的身份验证；5）根据预期目的限制访问次数，例如单次或临时使用；6）在出现可疑密集型请求时，临时或永久删除对所请求资源的访问权限。

【来源：CNIL】

26. 欧盟数据保护委员会就拟议的欧洲警察合作守则发表意见

9 月 12 日，欧盟数据保护委员会（EDPB）发布《关于欧洲警察合作守则的 03/2022 号声明》。

EDPB 表示，它承认警察合作是成员国之间安全的“关键因素”，但“对于所有刑事犯罪，生物特征数据或警察记录的自动搜索不应该是可能的。”此外，EDPB 对拟议的欧洲警察记录索引系统表示担忧，因为它没有充分证明“为什么有必要进行设想的跨境访问警察记录，也没有提供足够的保障措施来实施。”

【来源：EDPB】

27. 挪威数据保护当局发布员工监控工具调查报告

9 月 1 日，挪威数据保护当局（Datatilsynet）发布针对员工监控工具的调查报告《老板看到你了吗？监控员工的数字活动》(Sjefen ser deg? Overvåking og kontroll av arbeidstakeres digitale aktiviteter）。报告主题是监控员工的数字活动，重点研究三大问题：1）数字化工作场所有哪些监控措施和系统；2）专门设计用于监控员工的软件如何运作；3）员工在应对数字监测和控制方面有哪些经验。

报告得出四大结论：**1）一半以上的员工对雇主收集其个人信息没有充分的了解；2）雇主有能力收集员工数字活动中产生的大量信息；3）员工监控软件可能侵犯员工隐私；4）越来越多的员工表示其对网站的访问正受到雇主的监控。**此外，

Datatilsynet 特别关注远程办公场景下的员工监控措施，表示远程办公的推广应用将导致雇主在更大程度上使用数字工具来跟进和协调未在工作场所办公的员工，这将给员工个人隐私保护带来极大挑战。

【来源：datatilsynet】

28. 法国数据保护当局因违反 GDPR 多项义务规定对 infogreffe 处以 25 万欧元罚款

9 月 13 日，法国数据保护当局（CNIL）发布消息称，已对 INFOGREFFE 处以 250,000 欧元的行政罚款，理由是其违反了欧盟《通用数据保护条例》关于个人数据保留期限和安全性的多项义务。

infogreffe.fr 网站规定，会员和订阅者的个人数据（银行详细信息、姓名、邮政和电子邮件地址、电话和移动电话号码、秘密问题及其答案）将保留 36 个月。但 CNIL 发现 25% 的用户的数据被保留超过了确定的保留期限，应用户要求实施的手动匿名化仅涉及极少数账户。CNIL 还发现，在 infogreffe.fr 网站上创建账户时不需要使用强密码，并且由于规模有限，370 万个账户无法输入安全密码。此外，infogreffe 通过电子邮件以明文形式传输用于访问账户的非临时密码，并将用户在密码重置过程中使用的密码、秘密问题及其答案以明文形式保存在其数据库中。

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：CNIL】

29. 澳大利亚在发生大规模数据泄露后将全面修订隐私法

9 月 22 日，澳大利亚第二大电信公司 Optus 称公司遭到网络攻击并发生数据泄露事件，涉及 980 万 Optus 客户，接近澳大利亚人口的 40%，是澳大利亚历史上最大的数据泄露事件之一。

案件发生后，多名澳大利亚政府官员在不同场合强调将加强个人信息保护力度，并推动新一版《隐私法》修订，要求发生数据泄露的公司与银行分享可能受到影响的用户信息从而防止可能的金融诈骗。

多位专家学者在接受南方财经全媒体记者采访时指出，目前很多国家都在尝试通过提高信息的披露比例和披露时效，增强应对各种安全风险的处置能力，但在实施过程中，也需要注意对主体、权限、对象等的限制条件，以及在涉及数据

跨境时潜在的数据主权冲突。

本次澳大利亚政府提出修订《隐私法》的一个重要原因，是 Optus 数据泄露事件造成了一项关键风险，黑客可能会使用被泄露的个人信息，来向银行提交欺诈性申请，或者使用相关信息来欺诈消费者："因此这一项举措可以有效管控相关风险和金融欺诈行为的发生。"

【来源：21 世纪经济报道】

三、其他篇

30. 香港个人资料私隐专员公署就《数据出境安全评估办法》生效发布提醒

香港个人资料私隐专员公署留意到，国家互联网信息办公室发布的《数据出境安全评估办法》（以下简称《办法》）于 9 月 1 日生效。私隐专员公署提醒香港企业，尤其是在内地开展业务的香港企业或机构，例如银行、保险公司和证券公司等，如符合《办法》所订明的情形，可能须按有关规定向国家网信部门申报数据出境安全评估。个人资料私隐专员钟丽玲指出：在《办法》实施前已经开展的数据出境活动，如不符合《办法》的规定，亦须在《办法》实施起计 6 个月内，即 2023 年 2 月 28 日前，完成整改。（来源：香港个人资料私隐专员公署）。

【来源：CAICT 互联网法律研究中心】

31. G7 隐私监管机构讨论国际数据传输解决方案，推动数据流动立法合作

G7 成员国的隐私监管机构于 9 月 7 日和 8 日在德国联邦数据保护和信息自由专员 Ulrich Kelber 的主持下举行会议，讨论如何让数据在发达国家之间更顺畅地流动。这次会议是作为 2022 年德国 G7 数字部长会议的一部分举行的，讨论在"信任的数据自由流动（DFFT）"背景下的监管和技术发展问题。会议还旨在分享关于"国际数据空间"前景的知识，这代表了一种在国内外组织和部门内部之间共享可信和自愿数据的新兴方法，支持学术界、工业界和公共部门的创新。

【来源：The Wall Street Journal】

32. 俄罗斯《个人数据法》修正案生效

俄罗斯联邦通信、信息技术和大众媒体监督局(“Roskomnadzor”)于 2022 年 9 月 1 日宣布，2022 年 7 月 14 日第 266-FZ 号《个人数据法》修正案正式生效。Roskomnadzor 特别强调，该修正案对 2006 年 7 月 27 日第 152-FZ 号《个人数据法》进行了重大修改。修正案规定，数据处理者必须在 24 小时内将数据泄露及个人数据的跨境转移行为通知 Roskomnadzor，并在 72 小时内向 Roskomnadzor 提供有关数据泄露的内部调查结果并说明原因。此外，Roskomnadzor 规定，关于跨境转移个人数据的通知要求在 2023 年 3 月 1 日才生效。

【来源：Dataguidance】

33. 印度政府将发布新版《个人数据保护法案》与《数字印度法案》

9 月 5 日，印度联邦电子和信息技术部长 Ashwini Vaishnaw 表示，印度政府将发布新版《个人数据保护法案》（updated Personal Data Protection Bill），以及《2000 年印度 IT 法案》（India’s IT Act 2000）的修正案《数字印度法案》（Digital India Act）。

2022 年 8 月 3 日，印度政府宣布撤回 2019 年提出的《个人数据保护法案》，因为印度议会联合委员会 (JCP) 建议对该法案的 99 个部分进行 81 项修订。该法案旨在通过正确定义个人数据、建立数据保护局，以及制定数据使用的政策框架来保障公民隐私，确保在机构和大型科技公司处理个人数据时有一个框架或规则可以遵守。一些隐私倡导者和科技巨头认为，该法案可能会限制其管理敏感信息的方式。此次法案的撤回被印度媒体认为是大型科技公司游说的结果。

【来源：moneycontrol】

34. 印度尼西亚《个人数据保护法案》提交全体会议审议

9 月 7 日，印度尼西亚众议院宣布国防、外交和信息事务委员会与通信和信息部已达成协议，将《个人数据保护法案》（Rancangan Undang-Undang Pelindungan Data Pribadi，以下简称“PDP 法案”）提交全体会议审议，推动其获得批准成为法律。PDP 法案借鉴欧盟 GDPR 相关概念，例如数据控制者、数据处理者、敏感个人数据、数据保护官等。PDP 法案规范所有形式的数据处理，包括采集和收集、处理和分析、存储、更新和更正、展示、宣布、传递、传播、披露、删除或销毁。根据 PDP 法案，个人数据控制者必须在收到更新和更正个人数据的请求后 24 小时

内更新和更正个人数据中的错误和不准确之处，且个人数据控制者有义务将此类请求的结果通知个人数据所有者。

【来源：hukumonline】

35. 韩国个人信息保护委员会因违法个人信息保护法对 Google 和 Meta 罚款共计 1000 亿韩元

9 月 15 日消息，韩国个人信息保护委员会（PIPC）宣布对 Google 和 Meta 处以总计 1000 亿韩元的罚款。PIPC 表示，Google 和 Meta 未经用户同意收集个人信息，并将这些信息用于在线定制广告，构成对个人信息保护法的违反。对此，PIPC 对 Google 处以 692 亿韩元（约 3.47 亿元人民币）罚款，对 Meta 处以 308 亿韩元（约 1.55 亿元人民币）的罚款。Google 和 Meta 对这一决定表示反对，称公司高度重视法律合规以及对用户控制和透明度的承诺。

【来源：iapp】

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 王艺）

Merits Tree
植德律师事务所

前 行 之 路 植 德 守 护

www.meritsandtree.com