E-Commerce Letters 电子商务评论, 2024, 13(2), 910-917
Published Online May 2024 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2024.132107

Hans汉斯

基于联邦学习的精准广告营销合规分析

谷　语

浙江理工大学法政学院、史量才新闻与传播学院，浙江　杭州

收稿日期：2024年1月29日；录用日期：2024年2月19日；发布日期：2024年5月9日

摘　要

互联网精准广告营销成为广告市场的主要营销模式，在数据与技术的加持下，精准广告营销给用户和广告主带来了更好的广告体验。精准广告营销作为互联网广告时代发展的必然产物，通过预设用户画像和标签，依靠算法模型进行匹配，在提升广告投放精准度的同时，对用户的数据隐私也带来了不可忽视的风险。国内外针对该问题发布了一系列法律法规，使得用户拥有对其个人数据的掌控权，面对愈发严格的监管，兼顾安全与效率成为广告产业的必然选择。针对这一问题，联邦学习提出新的解决方案，联邦学习可在兼顾用户体验与广告精准度的同时，保护用户的数据隐私与个人信息安全。本文通过论证联邦学习对相关法律规则的供给，对联邦学习精准广告营销场景进行合规性分析，同时提出针对该场景下的监管重点，联邦学习不是完美的解决方案，仍然存在合规挑战。

关键词

精准广告，联邦学习，自动化决策，隐私安全

Compliance Analysis of Precision Advertising Marketing Based on Federated Learning

Yu Gu

Shi Liangcai School of Journalism and Communication, School of Law and Politics of Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: Jan. 29th, 2024; accepted: Feb. 19th, 2024; published: May 9th, 2024

Abstract

Internet precision advertising marketing has become the main marketing model of the advertising market. With the support of data and technology, precision advertising marketing has brought

文章引用: 谷语. 基于联邦学习的精准广告营销合规分析[J]. 电子商务评论, 2024, 13(2): 910-917.
DOI: 10.12677/ecl.2024.132107

better advertising experience to users and advertisers. As an inevitable product of the development of the Internet advertising era, precision advertising marketing, by presetting user profiles and labels, relies on algorithm models to match, while improving the accuracy of advertising, it also brings risks to users' data privacy that cannot be ignored. A series of laws and regulations have been issued both domestically and internationally to address this issue, enabling users to have control over their personal data. Faced with increasingly strict regulations, balancing safety and efficiency has become an inevitable choice for the advertising industry. In response to this issue, federated learning proposes a new solution that can protect user data privacy and personal information security while balancing user experience and advertising accuracy. This article demonstrates the supply of relevant legal rules by federated learning, conducts compliance analysis on federated learning precision advertising marketing scenarios, and proposes that federated learning is not a perfect solution for regulatory priorities in this scenario, and there are still compliance challenges.

Keywords

Precision Advertising, Federated Learning, Automated Decision-Making, Privacy and Security

1. 引言

2021 年国家统计局发布的《数字经济及其核心产业统计分类》[1] 中，将数字广告产业列为数字经济及其核心产业。互联网数字广告的营销模式已经发生转变，精准广告营销成为广告主更为青睐的低成本高收益营销模式。然而随着行业的迅猛发展，也迎来了更为严格的监管。《个人信息保护法》《互联网信息服务算法推荐管理规定》[2] 等法律法规对广告行业提出了严格要求。在严格的监管下，国内国外都展开了企图通过技术达到法律要求，联邦学习目前已经在众多互联网大厂中投入使用，以数据“可用不可见”的方式保护用户行为数据。本文对联邦学习在精准广告营销中的合规性进行探讨，提出针对合规科技的监管模式，助力精准广告营销合规。

2. 精准广告营销模式

2.1. 精准广告营销的概念

随着智能手机与社交媒体的快速发展，数字广告已经实现由以门户网站和搜索引擎为发布渠道的互联网广告，转变为以电商平台和短视频、社交媒体等为发布渠道的社交媒体广告。精准广告又称定向广告、个性化广告，是借助信息数字技术，通过收集和分析用户个人数据对其需求和偏好进行预测，并据此投放具有针对性营销内容的行为[1]。精准广告营销是广告行业中最为主流的营销模式，精准广告中的行为广告已经成为广告主和广告商重点关注的发展方向。在行为广告中，广告商会根据用户在网络上的行为，如浏览网页、APP、搜索内容、网络发言等行为，通过算法分析用户可能感兴趣的内容，然后向

[1] 国家统计局 2021 年 5 月 14 日第 10 次常务会议通过《数字经济及其核心产业统计分类(2021)》https://www.gov.cn/gongbao/content/2021/content_5625996.htm，2024 年 2 月 23 日访问。

[2] 《个人信息保护法》第二十四条第 2 款规定，通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式；《互联网信息服务算法推荐管理规定》第十条规定，算法推荐服务提供者应当加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则和用户标签管理规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息。

其推送个性化广告。

大型互联网社交媒体平台对精准广告的关注度非常高。Google 认为是“个性化广告是一种强大的宣传利器，对用户来说，它可以提高广告的相关性；对广告客户而言，它可以提高投资回报率”。2021 年 4 月，TikTok 全面对其用户提供个性化的广告推荐服务。Facebook 在 Meta 爱尔兰案的陈述中，直言“个性化广告是构成其服务的核心”。

2.2. 技术原理

2.2.1. 收集用户信息

精准广告模式下，广告商需要先收集用户的行为信息，进而通过算法分析进行用户画像。网站收集用户信息，当前精准广告普遍依赖于 Cookies 技术[2]。Cookies 其实是一个文本文件，当用户浏览某个网页时，服务器会在客户本地终端(包括电脑、智能手机等)的浏览器端相应地存储一个文本文件，该文件通常会以加密的方式，储存包括用户 ID、密码、浏览网页、搜索关键词、停留时间等在内的状态信息[3]。利用 Cookies，用户在下一次登录该网页时无需再次输入账号密码即可访问。

如何利用 Cookie 进行精准广告推送呢？如 Facebook、新浪、百度等平台，其利用 Cookies 在自有网站及其他网站上搜集用户行为数据，在广告交易平台进行算法分析，根据广告主的需求将商品广告针对性的投放在自有或者其他媒体平台。这种集合中小网络媒体资源，通过平台帮助广告主投放广告的形式即为广告联盟[4]。

2.2.2. 用户画像

利用 Cookies 收集用户行为数据后，通过数据处理与数据融合，最终将会形成可以关联到具体用户的用户画像。用户画像即用户信息的标签化，是真实用户的虚拟代表，是建立在一系列数据之上的目标用户模型[5]。无论是电脑端还是移动端，收集用户信息阶段，每个用户都会有唯一的 ID 进行标识，同时会根据这些 ID 在互联网上跟踪用户，以此获取更多的数据。新浪、Facebook 这些广告商会根据这些收集来的数据进行算法分析，即对这些数据进行统计分析得到事实标签，然后对事实标签进行建模分析，得到模型标签，然后进行模型预测，得到预测标签，主要是对未来数据的一种用户行为预测。

收集用户行为信息是进行用户画像的第一步，当用户行为数据收集的越多，数据分析越透彻，所形成的用户画像将越精准。

2.3. 隐私政策

根据上文分析，精准广告营销必然会发生个人数据的收集行为，根据《中国互联网定向广告用户信息保护行业框架标准》(以下称标准)，以互联网定向广告为目的进行的用户信息收集和使用、或向非关联方转移信息时，必须向用户提供是否同意为互联网广告目的收集和使用用户信息的选择和是否同意与非关联方共享该等信息的选择机制。《电子商务法》第十八条也规定了电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项。当用户浏览网站时，若要基于 Cookies 收集用户行为信息，为用户提供个性化广告时，必须经过用户同意。

标准同时规定有关单位应通过隐私政策、标识、即时通知等方式向用户公布收集和使用用户信息的规则。《个人信息保护法》《网络安全法》[3]都规定了个人信息的处理规则必须遵循透明度原则，《个人信息保护法》同时明确规定处理个人信息的应明确告知所处理的个人信息保存期限。廖秉宜、张慧慧、刘定文等基于国内 100 个 APP 隐私政策进行分析，有 78%的 APP 会在 Cookie 定义说明中提及，但仅仅

[3]《网络安全法》第四十一条规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

只是以“我们可能会使用相关技术向您的设备发送一个或多个 Cookie 或匿名标识符”的方式。少数 APP 会明确涉及 Cookies 的存储，其中不足半数涉及 Cookies 的保存期限[5]。

Cookies 隐私第一案百度胜诉[4]，法院认为百度公司没有将搜集到的原告网络踪迹信息向第三方或公众展示，故而百度收集到的用户行为信息，通过这些信息在其他网站向特定用户展现广告的行为属于合法行为。但基于海量数据进行用户画像，除了利用 Cookies 等技术进行用户跟踪获得的数据外，展现广告位的网站展示广告的同时，也会使用 Cookies 等技术搜集用户行为数据、广告流量数据等信息，这些信息提供给广告商，将会极大的提升用户画像精准度。在广告业界，对互联网广告效果评价指标主要是“点击率”和“转化率”两个基本指标，其中转化率相当接近于广告的销售效果[6]。然而广告主将转化效果反馈用于用户画像，这种数据提供却涉及《个人信息保护法》中个人信息“提供”问题，需要经过用户的授权同意。量化从广告展示到用户点击再到下单购买的数据转化，精准核算出广告投入总量的效果转化率，可以帮助广告主优化广告传播策略，降低广告预算的无效损耗，提升投资回报率。

此外值得讨论的是隐私政策中的间接收集信息行为。百度的隐私政策中，在用户的明示同意或通过个人信息提供方的明示同意的情况下，百度可以从百度关联公司，合作伙伴及其他受信任的第三方供应商处接收用户的个人信息及其他信息。通过需求方即广告主自有用户数据、广告投放过程中累积的业务数据，以及通过与第三方合作获得的数据组成用户画像的数据来源。在传统的广告投放模式中，需要从第三方数据提供商购买大量的个人数据，帮助决策模型的训练[7]。在《T/CAAAD003-2020 移动互联网广告标识技术规范》中规定在未获得其他参与方(包括用户)同意的情况下，移动互联网广告标识生成方应保障不超出双方的约定对从其他参与方处获取的数据进行存储和使用，或将数据提供给其他第三方，确保其他参与方的合法利益。此类规则规范使得收集用户数据变得更加困难。

3. 联邦学习下的精准广告营销

联邦学习是谷歌最先提出的概念，目的是为了利用用户手机端存储的数据训练模型。联邦学习具体是指依靠机器学习技术，各参与方将本地训练的数据，通过通信机制将参数传到中央服务器，中央服务器收集各方参数进行训练以构建全局模型送回各参与方[8]。

基于联邦学习的精准广告营销在大型广告投放平台有了广泛应用，如字节跳动的 Fedlearner 深度转化投放，华为依托于 TICS 服务搭建的纵向联邦学习平台。在国外，2021 年开始，谷歌公司就率先采用“隐私沙盒”计划来替代传统的 Cookies 技术发布互联网广告，其中一项名叫 Federated Learning of Cohorts (FLoC)的技术会使用机器学习算法来分析用户数据，然后根据个人访问的站点创建人群的集合，避免广告商获得用户的本地数据，从而进行广告发放。Facebook 也提出了 On-device learning 概念，即在设备端机器学习，Meta 大中华区总裁 Jayne Leung 称设备端机器学习，这项技术赋能设备端处理数据，无需将数据发送到远程服务器或云端。可以帮助我们无需了解用户在其他应用程序和网站上采取的具体操作，也可以找到向人们展示相关广告的新方法。

联邦学习分为横向联邦学习、纵向联邦学习和联邦迁移学习三类。横向联邦学习中，各个参与方持有的数据特征相同，但掌握的样本不同；纵向联邦学习则针对相反的情形，即各个参与方持有的数据特征不同，但掌握的样本相同；当大部分参与方所持有的数据，在特征和样本 ID 上的重叠都比较少且数据集分布不平衡时，就会应用迁移学习解决[9]。

3.1. 联邦学习助力精准广告营销

联邦学习可以帮助广告商在精准广告营销模式下，合法合规的注入多方数据，融合数据构建模型，

[4]江苏省南京市中级人民法院(2014)宁民终字第 5028 号。

使数据拥有方的数据在不出本地的情况下，完成数据结果的交换与数据建模。联邦学习模式下各个参与方间只有中间计算结果被交换，并且中间计算结果是加密之后再做传输。

可以利用横向联邦学习增加样本数量，使得媒体可以获得未知用户的兴趣点，进而拉取新用户[10]。广告商需要融合多方数据进行用户画像，用户画像需要基于用户标识符进行用户识别，在横向联邦学习中，就可以基于多方数据中不同的用户的共同兴趣特征，在多方数据的存储端本地进行训练模型，训练好的本地模型发送给中心服务器，中心服务器将汇合模型进行综合训练再发送给各本地服务器，每个训练轮次都会丰富模型，从而增加相同兴趣特征的用户群体，以完成更大用户范围的广告投放任务。

纵向联邦学习模型一是可以融合相同用户的不同兴趣特征，从而丰富用户画像。二是可以解决广告主转化数据的提供问题。首先纵向联邦学习可以融合多方数据拥有者相同用户的不同兴趣特征数据，从而丰富原有用户的特征维度，丰富用户画像完成广告投放。纵向联邦学习可以解决特征不足问题。在此过程中，转化数据无法收集，转化链路存在天然割裂，如流量方的用户特征、广告特征、上下文特征等与广告主方的端内行为数据、后端转化数据、历史兴趣标签、短期行为标签等无法对齐。广告主和广告投放平台在各自环境内部署联邦学习系统，纵向联邦学习可以进行样本粗筛、样本对齐，经过特征选择，启动训练，模型参数配置，并可以进行各项指标的评估，从而完成合作建模问题。

3.2. 联邦学习对隐私保护规则的供给

3.2.1. 必要原则

《个人信息保护法》规定了处理个人信息要遵循必要原则，必要是指处理者处理个人信息不应当超过可以实现处理目的的最低限度，其处理的个人信息应当限于满足处理目的的最小范围之内[10]。

在联邦学习训练过程中，广告主与广告投放平台或广告主与第三方的数据都不会离开其本地，不存在数据的收集与交换，仅需要交换与模型相关的中间数据及其变体，然后由主服务器将中间数据进行安全聚合并反馈给广告主和第三方；广告主和第三方则负责根据聚合后的模型信息进行己方模型的更新，有效保证了广告主和第三方的敏感数据的安全性和隐私性，实现了在融合多个广告主和第三方数据所蕴含的知识的同时保护隐私数据[11]。

其次在联邦学习中，各参与方将处理目地的共同约定为“计算某一特定函数”，后续所有处理活动将围绕寻找该函数与其变量之间的映射关系而展开，并最终完成模型的训练与收敛。围绕该特定函数，联邦训练模型中的数据将限定与该特定函数的计算逻辑范围内，不会用于除该计算目的之外的任何目的，例如在纵向联邦学习场景中，广告主方的转化数据和广告平台方的用户行为数据，运用纵向联邦学习可以将数据融合计算的目的仅限于丰富用户画像。因此利用联邦学习融合广告主与第三方数据可以满足处理个人信息时限与处理目的的最小范围内。

3.2.2. 安全可信原则

《T/CAAAD003-2020 移动互联网广告标识技术规范》规定广告标识生成过程不侵害用户个人信息安全，服务过程无法逆推出任何用户设备信息、个人数据。《广告法》《电子商务法》《中国互联网定向广告用户信息保护行业框架标准》[5]中都规定了收集使用个人信息的要遵循个人信息保护的规定，都应保护被收集、使用用户的个人信息安全。

[5]《广告法》第四十三条任何单位或者个人未经当事人同意或者请求，不得向其住宅、交通工具等发送广告，也不得以电子信息方式向其发送广告。以电子信息方式发送广告的，应当明示发送者的真实身份和联系方式，并向接收者提供拒绝继续接收的方式；《电子商务法》第二十三条电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定；《中国互联网定向广告用户信息保护行业框架标准》第二(四)项规定，第三方和服务提供方以互联网定向广告为目的进行的用户信息收集和使用、或向非关联方转移信息时，应向用户提供关于：(1) 是否同意为互联网广告目的收集和使用用户信息的选择机制；(2) 是否同意与非关联方共享该等信息的选择机制；以及(3) 如何改变或撤回用户同意的机制。该等机制应在第二部分第(三)条规定的隐私声明中明确说明。

用户行为数据在多方传递、处理使用过程中必然存在信息泄露、篡改等严重的安全隐患，利用联邦学习，可在很大程度上避免相关风险。首先在联邦学习中通过差分隐私等技术，在模型的训练过程中添加噪声扰动，使得发布的模型在保持可用性的同时得到保护。可以有效防止数据的泄露、篡改，还可以避免其他非数据拥有方逆推出用户的行为信息等数据，当广告主不愿意向广告投放平台提供转化数据时，就可以基于联邦学习融合转化数据，广告投放平台只会获得训练后的模型或者结果，并不会得到广告主的原始转化数据。

3.2.3. 数据分类分级

《网络安全法》《数据安全法》都提出了数据分级分类保护制度，对数据进行分级分类保护是我过数据保护领域发展的必然趋势，2023 年 8 月央行发布《中国人民银行业务领域数据安全管理办法(征求意见稿)》(下称《办法》)，《办法》中将数据分为一般、重要、核心三级，在此基础上，又将数据按照敏感性分层级，根据数据遭到泄露或者被非法获取、非法利用时，可能对个人、组织合法权益或者公共利益等造成的危害程度，将数据项敏感性从低至高进一步分为一至五共五个层级。2021 年《个人信息去标识化效果分级评估规范》将个人信息标识度分级划分，细化不同分级个人信息的安全措施。

在数据分级分类的必然趋势下，联邦学习可以助力精准广告营销合规。在华为的纵向联邦学习广告场景中，其可信智能计算服务内有一个计算节点，计算节点可以实现数据源注册，并且数据源可以选择是敏感的、非敏感的以及脱敏的设定[2]。此外，在个人信息中可能会包含敏感个人信息，若联合运算的结果中包含敏感个人信息，可以进一步采取差分隐私技术对抗潜在的个人信息攻击行为，防止敏感个人信息泄露。

4. 联邦学习精准广告营销模式监管方向

4.1. 自动化决策与算法透明

在 Cookies 百度隐私第一案中，二审法院的做法证明百度利用 Cookies 等技术收集用户行为数据的行为合规合法。广告主收集的用户行为数据、转化数据提供给广告投放平台用于用户画像。此后，涉及创建提案请求、人工谈判和手动插入订单等传统流程将从数字广告领域消失，广告购买、销售、投放等流程是完全自动化并且交易是实时的，程序化将在未来更加普遍应用[1]。联邦学习属于分布式机器学习技术，《个人信息保护法》中包含了自动化决策的一系列规定，利用自动化决策处理个人信息的，应当保证决策的透明度和结果公平、公正。

利用联邦学习融合多方数据联合建模当属于自动化决策，应当保证决策透明度与结果的公平公正。算法可界定为人类和机器交互的决策，即人类通过代码设置、数据运算与机器自动化判断进行决策的一套机制[12]。联邦学习中，机器学习会不可避免的发生算法歧视现象。算法极易受到程序员所设置的规则影响，从而生成歧视性结果。单次歧视的即时危害虽不易被察觉，却足以在更长时间维度和更长数据链条上产生积累式影响，联邦学习全局模型的不断轮回最容易导致群体歧视泛滥[13]。

4.2. 全行业监管模式

联邦学习属于利用“通过设计保护隐私”的方式保护数据安全。“通过设计保护隐私”被欧盟规定于《通用数据保护条例》中，“通过设计保护隐私”的基本理念是个人信息隐私的未来，不能仅仅通过遵守立法和事后处罚来保证，相反，它意味着从一开始就将隐私保护纳入信息技术系统、网络和业务流程的设计、运营和管理中[14]。域外已经开始了“通过设计保护隐私”的广泛讨论与实践。2018 年 3 月，欧盟数据保护监督局发布了第 5/2018 号意见《关于通过设计保护隐私的初步意见》(Preliminary Opinion on

Privacy by Design)，倡导并支持欧盟及其他成员国探讨通过设计保护隐私以及推广和应用隐私增强技术[15]。早在2010年，欧盟第29条工作组就发布了《关于网络行为广告的2/2010号意见》，其中在提出广告网络供应商的法律义务，广告网络供应商应鼓励并与浏览器制造商开发者合作，在浏览器中实施隐私设计。

2022年10月28日互联网广告标准联合工作组在会议上通过了《互联网广告隐私计算平台技术要求》的送审稿。我国已经广泛开始应用联邦学习等隐私计算技术在互联网广告场景中的实践，通过设计保护隐私是广告领域的必然趋势，但以隐私设计嵌入代码的方式，并不意味着无需再受法律的规制，应采用全行业监管的模式，促进联邦学习精准广告营销场景的法律合规。

联邦学习是机器学习技术，如果只是以广告行业的自我监管，工作部门对技术并非术业专攻，很难对精准广告营销中使用的技术进行全面有效的监管。2020年，中国信通院联合多家隐私计算单位共同成立了隐私计算专业组织“隐私计算联盟”，从隐私计算核心技术研究、行业应用落地、标准建设、政策监管研究，技术普及等多个方面构建政产学研合作交流平台。隐私计算联盟由多家隐私计算行业内专业化企业和组织成员组成，专注于隐私计算前沿技术与合规问题，属于行业内的专业人士，应采取法律行业与技术社群相互配合的方式，从法律视角和技术视角共同约束“通过设计保护隐私”的行为，才能实现对其的全面监管。

联邦学习是多种隐私计算技术中的一项安全技术，对于联邦学习在精准广告营销模式中的监管，我国互联网广告监管部门可联同隐私计算联盟针对广告营销场景设立专业化团队，从信息收集、算法监管到广告投放的一系列商业活动进行全流程监管。包括使用差分隐私、同态加密等技术对用户行为信息等数据的匿名化或去标识程度是否符合个人信息保护的相关规定，此外，也应该考虑法律规定与现实的边界，绝对的匿名化是否符合兼顾数据安全与流通的理念，法律规定的理想化或许并不利于现实中的情况，法律相关制度的退让或许更利于个人信息的安全与利用。

5. 结束语

联邦学习并非精准广告营销合规的完美之策，使用联邦学习完成精准捕捉客户不代表其行为不再需要法律的制约，相反，应该建立全行业全流程的监管，广告监管部门与隐私计算联盟等专业组织相互配合，针对隐私计算中的联邦学习这一具体技术在精准广告营销场景中的应用建立全流程的监管，促进精准广告营销合规性的同时，满足用户对其个人信息控制与使用的合理期待，提升社会信任度，促进互联网广告行业的健康发展。

参考文献

[1] 于婷婷, 杨蕴烙. 精准广告中的隐私关注及其影响因素研究[J]. 新闻大学, 2019(9): 101-116.

[2] 廖秉宜, 张慧慧, 刘定文. 精准广告技术中的个人信息保护——基于国内100个APP隐私政策中关于Cookie技术的文本分析[J]. 信息资源管理学报, 2023, 13(1): 103-114.

[3] 朱芸阳. 定向广告中个人信息的法律保护研究——兼评“Cookie 隐私第一案”两审判决[J]. 社会科学, 2016(1): 103-110.

[4] 朱巍. 互联网广告联盟的法律性质研究[J]. 辽宁大学学报(哲学社会科学版), 2017, 45(2): 86-93.

[5] 曾鸿, 吴苏倪. 基于微博的大数据用户画像与精准营销[J]. 现代经济信息, 2016(24): 306-308.

[6] 倪宁, 金韶. 大数据时代的精准广告及其传播策略——基于场域理论视角[J]. 现代传播(中国传媒大学学报), 2014, 36(2): 99-104.

[7] 陈凯, 杨强. 隐私计算[M]. 北京: 电子工业出版社, 2022: 185-186.

[8] 杨瑞仙, 李兴芳, 王栋, 等. 隐私计算的溯源、现状及展望[J]. 情报理论与实践, 2023, 46(7): 158-167.

[9] 刘艺璇, 陈红, 刘宇涵, 等. 联邦学习中的隐私保护技术[J]. 软件学报, 2022, 33(3): 1057-1092.

[10] 陈甦, 谢鸿飞. 民法典评注·人格权编[M]. 北京: 中国法制出版社, 2020: 377.

[11] 梁天恺, 曾碧, 陈光. 联邦学习综述: 概念、技术、应用与挑战[J]. 计算机应用, 2022, 42(12): 3651-3662.

[12] 丁晓东. 论算法的法律规制[J]. 中国社会科学, 2020(12): 138-159, 203.

[13] 唐林垚. 隐私计算的法律规制[J]. 社会科学, 2021(12): 117-125.

[14] 张涛. 个人数据保护中“通过设计保护隐私”的基本原理与制度建构[J]. 华东理工大学学报(社会科学版), 2020, 35(6): 129-144.

[15] European Data Protection Supervisor (2018) Opinion 5/2018: Preliminary Opinion on Privacy by Design. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf