个人信息匿名化图像技术及标准化研究

行业报告

一、研究背景及概述

随着信息技术的快速发展，个人信息的收集、处理和使用变得日益频繁，个人信息泄露和滥用的风险也随之增加。个人信息匿名化技术作为一种有效的隐私保护手段，其核心目标是在保护个人信息主体隐私的同时，促进数据的合理利用和流通。在互联网广告、医疗健康、金融服务等领域，匿名化技术的应用对于平衡个人隐私保护和数据利用需求具有重要意义。

近年来，为应对汽车数据安全事件和风险，国内外高度重视数据安全工作，出台了系列的政策和标准法规。《通用数据保护条例》（GDPR）于 2018 年 5 月 25 日在所有欧盟成员国生效，此条例给个人信息数据安全与隐私权设立了严格的保护标准。在国内，随着《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》的先后落地，汽车领域数据安全方面的监管政策文件密集出台。目前，相关学者已经就个人信息隐私保护方法和人脸图像匿名化的方法的研究取得了若干成果。在此背景下，为应对数据安全风险、落实数据合规，许多汽车企业已着手数据安全建设。我国汽车、交通、信息等行业的骨干企业、科研院所及高校等也在积极

开展智能网联汽车重要数据与个人信息保护的相关工作，加快推进智能网联汽车数据安全政策法规落地，对智能网联汽车数据安全要求及对应测试要求标准需求强烈。数据在传输过程中需要进行匿名化处理，以确保信息不被泄露。因此，汽车数据匿名化检测平台对于落实数据安全和个人信息保护相关法规要求具有重要作用，有利于数据资源的开发利用和开放共享，有助于推动自动驾驶技术的产品研发和服务创新，能够进一步促进智能网联汽车产业高质量发展。

二、研究内容

（一）国际标准和法规

欧盟通用数据保护条例（GDPR）为个人数据的保护设定了高标准，要求在处理个人数据时必须遵循数据最小化、目的限制、数据主体的权利等原则。GDPR 还定义了匿名化的概念，即数据在处理后不应再与特定个人相关联。美国健康保险便携性和责任法案（HIPAA）规定了医疗保健信息的隐私和安全标准，包括去标识化的要求，以保护患者的隐私。加利福尼亚消费者隐私法案（CCPA）为加州居民提供了更多的隐私权保护，包括对个人信息的访问、删除和拒绝出售的权利。ISO/IEC29100 系列标准提供了个人信息保护的指导，包括匿名化和去标识化的技术方法。

（二）国内标准和法规

《个人信息保护法》规定了个人信息的处理规则，强调了数据主体的知情权和选择权，并对个人信息的匿名化处理提出了要求。《网络安全法》规定了网络运营者收集和使用

个人信息的基本原则，包括数据的匿名化处理。《信息安全技术 个人信息安全规范》（GB/T 35273）规定了个人信息处理活动应遵循的原则和安全要求，包括匿名化和去标识化的定义和技术方法。

《个人信息去标识化指南》提供了个人信息去标识化的具体指导，包括直接标识符和间接标识符的处理。《个人信息去标识化效果分级评估规范》列举了去标识化的数据处理手段，如抑制、泛化、分解、干扰、压缩等，并将个人信息去标识化分为接受需评估内容、进行定性评估、进行定量评估三个阶段。

全国信息安全标准化技术委员会（SAC/TC260）在汽车数据安全相关的基础标准方面，已发布 GB/T 35273—2020《信息安全技术 个人信息安全规范》、GB/T 37964—2019《信息安全技术 个人信息去标识化指南》、GB/T 38628-2020《信息安全技术 汽车电子系统网络安全指南》等多项国家标准，在研国家标准包括《信息安全技术 汽车数据的安全处理要求（报批稿）》《信息安全技术 网络数据处理安全 要求（报批稿）》《信息安全技术 网络预约汽车服务数据 安全要求（报批稿）》等。信安标委还发布了《汽车采集数据处理安全指南》《汽车电子网络安全标准化白皮书》等系列标准化工作成果。

《信息安全技术 汽车数据处理安全要求（报批稿）》针对汽车数据在收集、传输等数据处理活动出现的个人信息或重要数据泄露、滥用等安全问题，围绕《若干规定》中车

外个人信息匿名化、车内处理、默认不采集、显著告知等落地中存在的难点问题进行细化，提出可执行的落地方案，可以更好地支撑《若干规定》的实施贯彻。

这些标准和法规共同构成了个人信息和图像匿名化的法律基础，旨在确保个人隐私得到妥善保护，同时允许数据的合理利用。随着技术的发展和隐私保护意识的提高，这些标准和法规也在不断更新和完善中。

（三）标准化的必要性和益处

个人信息匿名化图像技术标准化具有重要的必要性和益处，主要体现在以下几个方面:

保护隐私安全: 随着人工智能和深度学习技术的发展，身份伪造技术日益进步，个人信息泄露和滥用的风险不断增加。通过匿名化图像技术，可以有效保护个人隐私不被非法获取和使用，尤其是在社交媒体平台和公共监控领域。

促进数据合规流通: 在数据驱动的数字经济中，数据共享和交易变得越来越重要。个人信息匿名化技术标准化有助于确保数据在流通和交易过程中符合法律法规要求，降低数据泄露风险，增强数据使用者的信心。

提高数据利用效率: 通过标准化的匿名化技术，可以在保护个人隐私的同时，使数据能够被更广泛地用于统计分析、机器学习训练和科学研究等，提高数据的利用效率和价值。

形成行业共识: 标准化的匿名化技术有助于形成行业共识，统一不同企业和组织在数据处理中的操作规范，降低合规成本，推动行业健康有序发展。

应对司法挑战：由于缺乏统一的匿名化标准，司法实践中对匿名化信息的判断存在差异。标准化的匿名化技术有助于明确司法判断标准，统一裁判尺度，减少法律争议。

促进技术发展与创新：匿名化图像技术的标准化将推动相关技术的发展与创新。例如，基于图像和视频的匿名化方法、视觉可恢复的匿名化方法以及深度学习过程中的隐私保护方法等，都有望在标准化的推动下得到进一步优化和完善。

降低去标识化和匿名化风险：通过标准化的流程和方法，可以更有效地降低去标识化和匿名化过程中的风险，确保数据处理的安全性和有效性。

综上所述，个人信息匿名化图像技术的标准化对于保护个人隐私、促进数据合规流通、提高数据利用效率、形成行业共识、应对司法挑战、促进技术发展与创新以及降低去标识化和匿名化风险等方面都具有重要的意义和价值。

（四）现有标准的评估和比较

个人信息匿名化图像技术的标准评估和比较可以从多个角度进行，包括技术手段、应用场景、安全性、合规性等。以下是对现有标准的评估和比较：技术手段的多样性：现有的匿名化技术包括泛化、压缩、分解、置换以及干扰等方法。例如，k-anonymity 模型要求发布的数据在指定标识符的属性值相同的每一等价类至少包含 K 个记录，以保护个人信息不被识别。应用场景的特定性：匿名化和去标识化技术在不同的应用场景下有不同的安全要求。例如，《个人信息安全规范》对匿名化和去标识化的应用场景、原则及安全要求

进行了具体规定。安全性的层次性：匿名化技术相比去标识化技术具有更高的安全程度，强调处理后的信息不能被复原，以最大程度保护个人隐私和数据安全。合规性的重要性：个人信息匿名化的标准需要符合法律法规的要求。例如，中国的《个人信息保护法》和《网络安全法》对匿名化有明确的规定，而欧盟 GDPR 则提出了匿名信息的合理可能性标准。评估标准的明确性：《个人信息去标识化指南》和《个人信息去标识化效果评估指南》为个人信息去标识化提供了具体的评估框架和量化指标，推动了去标识化技术、流程及配套评估措施朝着定量化的精细方向发展。国际标准的参照性：不同国家和地区对匿名化的定义和要求存在差异。例如，欧盟的 GDPR 和美国的 CCPA 对去标识化和匿名化的处理和定义提供了不同的视角和要求。非结构化数据的挑战性：对于肖像图片和视频这类非结构化数据的匿名化处理，3334 现有标准尚处于发展阶段，需要进一步的研究和实践来制定科学有效的标准。通过这些评估和比较，我们可以看到个人信息匿名化图像技术标准化的必要性，以及现有标准在技术手段、应用场景、安全性、合规性等方面的优势和不足。随着技术的发展和法律的完善，预计未来的匿名化图像技术标准将更加全面、严格和国际化。

本部分内容节选自该课题研究报告，非全部内容，仅供参考了解。