

大数据时代的隐私侵犯与伦理困境

——以 Facebook 数据泄露事件为例

郑继冬

河北工程大学 河北邯郸 056038

摘要: 本文深入剖析了 Facebook 数据泄露事件,探讨了该事件在技术、法律及伦理层面上的多重影响。通过分析事件的背景、经过、影响,本文揭示了大数据时代下个人隐私保护的脆弱性以及企业数据伦理责任的缺失。同时,结合工程伦理原则,本文讨论了如何在技术进步的同时,确保个人隐私的安全与尊重,为未来的数据治理提供启示。

关键词: 大数据技术; 隐私侵犯; 工程伦理; Facebook 数据泄露; 数据治理

引言

随着信息技术的飞速发展,大数据已成为推动社会进步和经济增长的重要力量。然而,大数据的广泛应用也带来了前所未有的隐私保护挑战。Facebook 作为全球最大的社交媒体平台之一,其数据泄露事件不仅暴露了用户隐私安全的巨大漏洞,也引发了公众对数据伦理和企业社会责任的深刻反思。本文旨在通过对 Facebook 数据泄露事件的详细分析,探讨大数据时代下的隐私保护伦理问题,为构建更加安全、负责任的数据环境提供借鉴。

一、案例背景

(一) 公司概况

Facebook 成立于 2004 年,总部位于美国加州门洛帕克,是全球最大的社交媒体平台之一,拥有超过 20 亿的活跃用户。Facebook 通过提供社交网络服务,收集并处理大量用户数据,用于广告推送、内容推荐等商业活动。

(二) 事件概述

2018 年 3 月,英国《卫报》和美国《纽约时报》联合报道,Facebook 允许 52 家科技公司访问其用户的个人数据,这些数据包括用户的私人消息、好友列表等敏感信息,且这些访问行为并未获得用户的明确同意。这一消息迅速引发全球关注,被称为“Facebook 数据泄露门”。随后,Facebook 面临多起诉讼和监管调查,其股价也因此大幅下跌。

二、案例正文

(一) 事件经过

据报道,Facebook 与这些科技公司签订了“白名单”协议,允许它们在用户不知情的情况下访问其数据。这些公司利用这些数据优化自己的产品,甚至进行政治宣

传和 market 分析。Facebook 的这一行为严重违反了用户隐私保护的基本原则,引发了公众的强烈不满和质疑。

该事件起源于 Facebook 的一个第三方应用开发者 Aleksandr Kogan,他开发了一款名为“this is your digital life”的 Facebook 应用,该应用通过用户授权收集了包括用户个人信息、朋友列表、点赞内容等在内的大量数据。然而,Kogan 并未遵守与 Facebook 的协议,而是将这些数据非法提供给了政治咨询机构剑桥分析公司(Cambridge Analytica),后者利用这些数据分析了用户的政治倾向、性格特征等,并可能用于了政治竞选广告的精准投放。与剑桥大学学者合作获取数据的 Christopher Wylie 告诉《观察者报》:“我们利用 Facebook 收集了数百上千万用户的个人资料,并建立起一个分析模型,从而利用这些现有的用户信息,精确的瞄准他们‘心魔’,来获得他们内心的真实需求(达到左右其观点的目的)。而这也是剑桥分析这个公司建立的意义所在。”

下图为 Christopher Wylie 接受采访时的照片,据 Christopher Wylie 所说,剑桥分析在脸书上的部分应用是被特殊允许的,用来收集用户数据包括用软件和加入软件的用户,而且还会穿入用户整个朋友圈网络,比如状态更新、点赞有时候还有私人信息,公司只需要接触几十万用户,就能扩展到整个社交网络。由此可见,在大数据时代下,网络用户以及毫无隐私可言。

在剑桥分析被爆滥用用户数据事件之后的 4 天里,Facebook 相关高层管理人员并没有对此事件做出任何回应,直到周二,Facebook 发表声明称:“CEO 扎克伯格和 COO 雪莉·桑德伯格以及他们的团队认识到这次事件的严重性,并且正在夜以继日地工作,以便获取所有的事实真相,并采取相应的措施。”在接受《The Daily Beast》

Facebook数据泄露事件概述表格

序号	事件时间	泄露数据量	泄露内容	影响范围	应对措施
1	2018年	5000万	用户数据	北美用户	封禁违规账号，进行全面审计
2	2019年	4.19亿	电话号码	全球用户	禁用电话号码搜索功能
3	2019年12月	2.67亿	姓名、电话号码	美国用户	未明确提及，但加强了安全措施

采访时，Facebook表示：“发生这样的事件，整个公司都感到十分愤怒，我们有一种被蒙骗的感觉，我们一直致力于大力保护用户信息的政策，同时我们也会采取一切必要措施，来确保用户信息的安全。”

（二）影响分析

1. 用户信任危机

Facebook数据泄露事件严重损害了用户对其的信任度。许多用户开始质疑Facebook的数据保护能力，并考虑减少或停止使用其服务，甚至删除账户。这种信任危机不仅影响了Facebook的用户基础，也对其商业模式和未来发展构成了威胁。

2. 法律风险

Facebook因数据泄露事件面临来自全球多个国家和地区的法律诉讼和监管调查。这些法律纠纷不仅可能导致巨额罚款，还可能影响其在全球市场的声誉和竞争力。此外，随着数据保护法规的不断完善，Facebook未来在数据保护和共享方面将面临更加严格的监管要求。Facebook和FTC，就剑桥分析事件达成的和解协议，被联邦法院正式批准，在正式生效的协议里，Facebook认罚50亿美元，还将在安全隐私方面做出相应的整改。这50亿美元的罚款，相当于其2019全年营收的7%，盈利的27%，大约为一个月的营收。

3. 品牌形象受损

作为行业巨头，Facebook的数据泄露事件对整个互联网行业产生了负面影响。公众开始更加关注数据安全和隐私保护问题，对互联网企业的信任度普遍下降。这种趋势加剧了市场竞争的激烈程度，也促使其他企业加强数据保护措施以挽回用户信任。

三、工程伦理分析

（一）违反的伦理原则

1. 尊重隐私原则

Facebook未经用户明确同意，擅自允许第三方访问用户数据，严重侵犯了用户的隐私权。这一行为违反了工程伦理中的尊重隐私原则，即工程师在设计和实施技术系统时应尊重和保护用户的隐私权益。

2. 诚实与透明原则

企业应对其产品和服务的运作方式保持诚实，不能误导用户。Facebook对外宣称其平台保护用户隐私，但

在数据共享和使用上存在重大缺陷，未能如实向用户说明其数据可能被第三方获取和使用的风险。

3. 责任原则

作为数据收集和处理的主体，Facebook有责任保护用户数据的安全和隐私。然而，在数据泄露事件中，Facebook未能履行这一责任，导致用户数据被滥用和泄露。这一行为违反了工程伦理中的责任原则，即工程师应对其技术行为的后果负责并承担相应的责任。

4. 公正原则

Facebook的“白名单”协议存在明显的不公平性。只有少数科技公司能够享受这一特权，而大多数用户则无法得知自己的数据被如何处理和利用。这种不公平性加剧了信息不平等和社会分化现象，违反了工程伦理中的公正原则。

（二）违反的技术规范

1. 数据保护法规

GDPR（通用数据保护条例）：作为一项严格的数据保护法律，GDPR要求公司在处理用户数据时必须获得用户的明确同意，并确保数据的安全性。Facebook在数据处理过程中的疏忽，导致其违反了这一法规。

2. 信息安全标准

ISO/IEC 27001：这一标准提供了信息安全管理框架，要求企业采取适当的措施保护用户数据的机密性、完整性和可用性。Facebook在用户数据的保护措施上显著不足，未能有效实施信息安全管理。

3. 用户协议与隐私政策

Facebook的用户协议和隐私政策未能清晰地阐述数据使用的具体情况，导致用户在同意条款时缺乏对数据使用方式的真实了解。

（三）总结

Facebook用户数据泄露事件揭示了社交媒体平台在数据隐私和伦理责任方面的重大缺陷。此事件不仅违反了多个伦理原则，还触犯了相关的技术规范和法律法规。为了重建用户信任，企业需要在数据保护和用户隐私保护上采取更为严谨和透明的措施，确保用户的知情权和选择权，积极承担社会责任。这一事件也提醒我们，数据科学的从业者在技术创新的同时，必须时刻关注伦理问题，确保技术的发展造福社会。同时，Facebook的数

据泄露事件暴露出当前数据治理体系的不足,包括数据访问权限控制、数据加密保护、数据共享协议等方面的技术标准和规范亟待加强。为了防范类似事件的再次发生,需要不断完善和更新数据保护技术规范以适应技术发展的需求。^[7]

四、结论与启示

(一) 结论

Facebook数据泄露事件是一起典型的大数据时代下的隐私侵犯案例。该事件不仅暴露了Facebook在数据伦理方面的严重缺失也引发了公众对大数据技术应用的广泛关注和深刻反思。通过对此事件的分析我们可以清晰地看到大数据时代下个人隐私保护的脆弱性和挑战以及企业在数据治理方面所面临的困境和责任。^[2]

(二) 启示

Facebook用户数据泄露事件不仅引发了全球对数据隐私的关注,还促使各界对数据伦理进行深入思考。通过对这一事件的分析,可以总结出多个重要启示,为数据科学领域的未来发展提供指导。^[6]

1. 增强用户数据保护意识^[4]

用户教育与意识提升:用户在使用社交媒体和在线服务时,应具备基本的数据隐私意识。企业应开展用户教育,帮助用户理解其数据的使用方式和潜在风险,提升用户的警觉性。

明确知情同意:企业在收集和使用用户数据时,必须确保用户明确理解其同意的内容。这不仅涉及到法律法规,还需在用户协议中清晰展示数据使用的目的和范围。

2. 企业责任与社会责任^[5]

企业应承担更大责任:企业在追求利润的同时,必须对用户数据安全和隐私保护尽到合理责任。确保数据的安全存储、处理和使用是企业的基本责任。

建立透明和信任的关系:企业应该与用户建立透明的关系,定期发布数据使用报告,让用户了解其数据的使用情况和安全措施,增强用户信任。

3. 加强技术规范与合规管理

遵循数据保护法规:企业必须遵循相关的数据保护法规,如GDPR等,确保在处理用户数据时采取必要的法律和技术手段,确保用户数据的安全性和隐私性。

实施信息安全管理标准:采用ISO/IEC 27001等信息安全管理标准,确保企业在数据处理和存储中符合国际最佳实践,降低数据泄露风险。

4. 强化第三方合作的监管

对第三方应用的审查:企业必须对其平台上使用的第三方应用进行严格审查,确保这些应用遵循相同的数

据保护标准,防止数据在未经授权的情况下被滥用。

合同条款的规范:在与第三方合作时,应在合同中明确数据使用的范围和责任,确保第三方在处理用户数据时遵循相应的伦理和法律规范。

5. 伦理审查机制的建立^[1]

设立伦理委员会:企业可以设立伦理委员会,对新技术和新产品进行伦理审查,确保在技术创新时不侵犯用户的隐私权,保护用户利益。

定期评估与反馈:定期对数据使用和保护措施进行评估,并给予用户反馈机会,收集用户意见,及时调整数据管理策略。

6. 技术与伦理的结合^[3]

技术设计时考虑伦理:在数据科学和技术开发过程中,工程师和数据科学家应将伦理考虑融入技术设计中,确保技术的开发和应用符合伦理原则。

使用隐私保护技术:采用数据匿名化、加密等技术手段,在不影响数据分析结果的前提下,保护用户隐私,降低数据泄露的风险。

7. 跨界合作与行业标准

行业合作与信息共享:不同企业应加强合作,共同制定行业标准和最佳实践,提升整个行业的数据保护水平。

政府和行业机构的支持:政府应加强对数据保护的立法和监管,行业机构应提供相应的指导和支持,促进数据安全文化的建立。

参考文献

- [1] 谢思娴, 张建光. 社交网络平台数据治理机制研究——基于Facebook泄密事件的案例分析[J]. 中国信息界, 2018
- [2] 王小侠, 李畅. 从“Facebook”数据泄露事件浅析个人信息权利保护[J]. 长春理工大学学报(社会科学版), 2019
- [3] 刘晓凡. 大数据背景下工程师的伦理责任分析[J]. 电脑知识与技术: 学术交流, 2018
- [4] 肖家明. 控制与告知: 社交媒体环境下用户个人信息资料权的保护——基于Facebook用户信息泄露事件的思考[J]. 硅谷, 2018
- [5] 弓永钦. 从FACEBOOK个人信息泄露事件看平台的隐私保护责任[J]. 北京劳动保障职业学院学报, 2018
- [6] 吴雅婷. 大数据时代社交平台的个人隐私保护——以Facebook泄密事件为例[J]. 硅谷, 2020
- [7] 杨秀梅. 国外数据泄露事件与警示[J]. 保密工作, 2019 (01)