Universal Library of Engineering Technology Research Article

ISSN: 3064-996X | Volume 2, Issue 3

Open Access | PP: 105-110

DOI: https://doi.org/10.70315/uloap.ulete.2025.0203019

AI-Powered CRM Systems and the Ethics of Data Use: Personalization Vs. Privacy

Sergei Berezin

Student at Midwestern Career College in the Associate of Applied Science in Information Technology Program.
Founder and Inventor of CRM-System for Restaurants with AI Integration, Chicago, USA.

Abstract

This paper will discuss some of the ethical dilemmas that arise from using artificial intelligence in CRM systems, with a particular emphasis on striking an appropriate balance between service personalization and data privacy protection. This study identifies the major risks, regulatory requirements, and technical solutions necessary to ensure the ethical application of AI in customer relationship management. With business increasingly based on information, 81% of Americans say there is a lack of clarity in information usage by companies; 68% are human-factor-related data breaches—the need for codes of conduct usage rises. The uniqueness of this study lies in its comprehensive examination of the technical, regulatory, and organizational dimensions involved in the Salesforce and Facebook cases. The methodological base includes a systematic review of 21 sources, comparative technology analysis, and standard compliance assessment. It has been discovered that AI algorithms based on historical data can be biased, for instance, in lending and targeting advertisements; therefore, these models need audits and corrections. Major findings underscore the need for a multi-layered approach to balancing personalization and privacy. This paper will serve data scientists, CRM developers, digital lawyers, and regulators who deal with AI ethics.

Keywords: *Artificial Intelligence, CRM Systems, Data Privacy, GDPR, Algorithmic Bias, AI Transparency, Differential Privacy, Data Ethics, Data Minimization.*

INTRODUCTION

Artificial Intelligence plays a significant role in the rapidly evolving software of today's world, specifically in Customer Relationship Management systems, where data has become a crucial element in business success [1]. Through AI integration, companies achieve high levels of service personalization, customer behavior analysis, and optimized interaction processes, increasing efficiency and profits. But with such development, the ethics concerning personal data protection and privacy have also risen significantly; thus, this issue is receiving increased attention from both researchers and practitioners. The primary reason for the growing interest in ethics in AI applications within CRM systems is the handling of vast volumes of personal information. The company gathers and studies details about customer' likes, dislikes, and interaction history, which heightens the risk to their privacy. The situation worsens because customers themselves are unsure exactly what data is collected and how it is used; therefore, trust in organizations is eroded. More than four in five Americans (81%) believe that there is a lack of transparency in how companies use the personal information they collect from consumers [2]. Another area of interest is the opacity of AI algorithms. Developers cannot easily interpret decisions based on machine learning, let alone clients; thus, an accountability problem arises [3]. Opaqueness further increases bias risks, as biased-data-trained algorithms may discriminate against specific consumer groups.

MATERIALS AND METHODOLOGY

The paper undertakes a review of relevant literature on the ethics of data use, personalization, and privacy in AI-driven CRM systems from 21 sources: academic articles, industry reports, company cases, and regulatory documents. The theoretical basis for this work stems from two articles that primarily focus on integrating AI into CRM. Unanah and Mbanugo [1] reported improved marketing effectiveness in pharmaceuticals due to predictive analytics, while Yoo et al. [12] demonstrated that personalized AI-CRM can create a competitive advantage, provided it maintains algorithmic transparency. The ethical and legal aspects are revealed through GDPR [8], DPIA practices [11, 13], and studies showing discrimination by algorithms [9, 20]. For instance, AI models in lending increased racial disparities [9].

Citation: Sergei Berezin, "AI-Powered CRM Systems and the Ethics of Data Use: Personalization Vs. Privacy", Universal Library of Engineering Technology, 2025; 2(3): 105-110. DOI: https://doi.org/10.70315/uloap.ulete.2025.0203019.

This study was methodologically synthesized.

- Comparative analysis of technologies — comparison of approaches to data management, eg, RBAC [16] vs blockchain [15] and their impact on privacy. Gartner data on the transition to "small and wide data" showed that data localization reduces leak risks but also limits personalization [17].
- A systematic review of regulatory requirements — GDPR [8], DPIA [13], and ICO [13] recommendations revealed the need for "ethical design" of systems, as in the Salesforce case, where transparency principles are built into product architecture.
- Data control cases and surveys — the AU10TIX study [2] showed that 81% of Americans trust not companies in matters of data control. A Cisco report [6] confirmed that trust in AI is directly linked to privacy awareness.

RESULTS AND DISCUSSION

Data privacy is a vital component in ensuring protection against unauthorized access, use, or disclosure of customers' personal information. This is particularly critical within CRM systems, where large information troves are analyzed by AI to make personalized offers. Major risks associated with it include data breaches due to cyberattacks, technical malfunctions, or even simple human error. Research [4] found that human errors were responsible for 68% of data breaches in 2024; therefore, internal risks can also be inadvertently increased by AI agents. For example, an AI agent might disclose sensitive project information simply because it has not been properly configured to exclude project updates from all its communications [5]. Once positioned rapidly and trickery employed to elicit sensitive information, vulnerabilities can then be exploited by attackers. Another risk is the misuse of data by companies, which applies customer data for unintended purposes without explicit consent. The Report [6] sheds light on how, now, most consumers, 53%, are aware of privacy laws. Uninformed consumers feel much less confident in protecting their data (81% vs 44%). In total, 63% of consumers believe that AI can be useful in improving their lives, and strong privacy laws make 59% feel comfortable sharing information in AI applications. However, it is noted that 30% of Generative AI users are entering personal or sensitive information into these tools, despite 84% expressing concern about publicly available data entered by them into Generative AI.

Another major facet of technology ethics in CRM systems is AI algorithm transparency, as it directly influences customers' understanding of the logic behind the decisions made and, consequently, their trust in it. By transparency, we mean that customers and businesses can understand how and on what data someone else is making recommendations using AI. Most, if not all, machine learning algorithms, particularly deep learning ones, work as what you would call black boxes, so much so that even experts find it quite hard to explain the decisions they make. This poses a significant problem for customer trust, as they may not appreciate why certain services or products are being pitched to them.

As long as there is clarity about what brands do with the data, consumers want the digital ads of the brands to portray them as familiar and trustworthy. In the study [7], it was found that 87% of consumers believe it is important to buy from brands or retailers that understand the "real me".

Such opaqueness compounds concerns about privacy, as a misapprehension about data processing raises suspicions among customers about potential misuse. The evolution of explainable AI methodologies is poised to be a significant stride towards overcoming these issues, making algorithms more interpretable and bolstering customer trust in CRM systems alike, thereby meeting mandates at international levels, such as GDPR [8].

Potential biases in artificial intelligence algorithms make discrimination based on algorithmic bias very possible within CRM systems. These algorithms learn from historical data, which embodies all those social or historical inequalities. If, for example, the data indicated higher churn rates in certain demographic groups, these groups might be unfairly labeled by the algorithm, resulting in less favorable terms being offered or their exclusion from targeted campaigns. It has been found that algorithms used in financial services can discriminate based on race [9], even when race is not an explicit consideration, but rather through correlations with parameters such as location or income. In CRM systems, such biases can lead to unethical treatment of customers and conflict with both ethical principles and consumer protection laws. Their mitigation demands algorithm audits, representative data usage, and debiasing techniques, along with objectivity in decisions. There is a risk of discrimination, but the role of artificial intelligence in CRM systems also raises other ethical concerns, including user autonomy, informed consent, and accountability for decisions made by algorithms. The user should have control over the data and be capable of making decisions based on information about its use, which is frequently not the case due to insufficient provision for transparent information and management tools. Informed consent implies that the customer knows explicitly all the purposes and ways of data processing and gives explicit consent; however, this is hampered by complex and unclear privacy policies. Survey [10] indicates that only 9% of adults say they always read a company's privacy policy before agreeing to its terms, and another 13% say it does so often. Further, it has been reported that 38% of Americans say they do this sometimes. There is a portion of the population that outright refuses to read these policies at all; more than one-third of adults, 36%, say they have never read a privacy policy before agreeing to it, underscoring the need for simplification of customer communication. The survey data has been depicted in Figure 1.

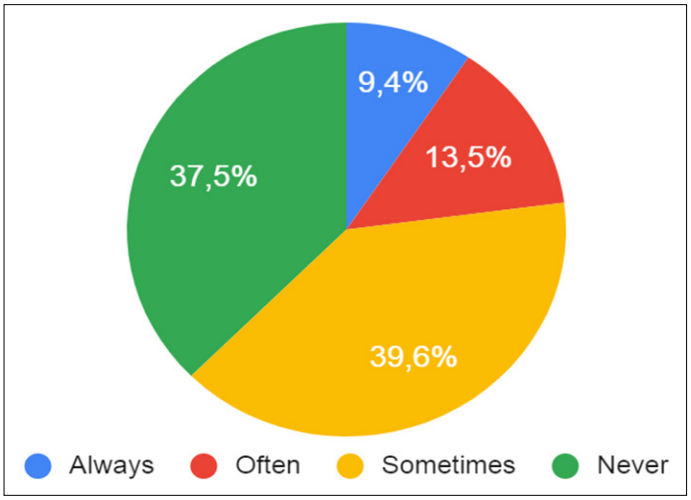

Fig. 1. How often US adults read the company's policy before agreeing with it [10]

Reading privacy policies does not assure complete reading, however. Of those adults who say they have ever agreed to a privacy policy after reading its terms, only a small fraction (22%) reports having read it in full before agreeing to the terms [10]. Most of the time, these readers report that they either skimmed it and did not read it thoroughly (43%) or that they have read only a part of it. Among all U.S. adults, 22% report reading their entire privacy policy, 35% read part of it, and 43% skim it. The survey data appear in Figure 2.

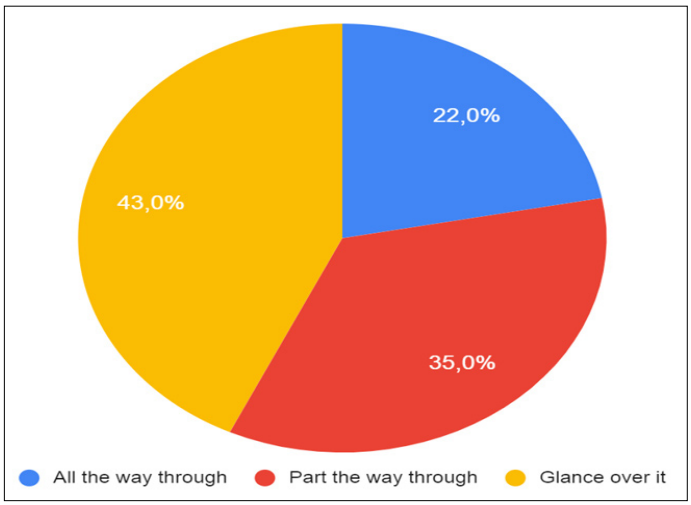

Fig. 2. How closely do US adults read the company's policy before agreeing with it [10]

In terms of accountability, therefore, companies should be accountable for their algorithm, especially those that have a great impact on the clients. This calls for the development of mechanisms of accountability and transparency in explaining and correcting erroneous or unfair decisions. The General Data Protection Regulation (GDPR) imposes strict requirements on systems powered by artificial intelligence for customer relationship management (AI-CRM), particularly regarding the processing of personal data. Under GDPR, it is lawful, fair, and transparent to process data; therefore, there must be an explicit legal basis for AI-CRM systems to collect and use data, such as the subject's consent, the performance of a contract, or the company's legitimate interest. Besides this major requirement between the consumer and organization, it empowers consumers with rights against organizations over their data; thus, obligations are imposed on AI-CRM developers to abide by these rules [11]. Data minimization under the GDPR may further limit necessary data to that which is essential for achieving any given aim (Henderson, 2019). This compromises the operations of AI-CRM systems to a large extent since they depend on huge data volumes for algorithm training. Where processing poses a high risk to the rights and freedoms of data subjects, the GDPR also mandates a Data Protection Impact Assessment (DPIA); this is generally most applicable to AI-CRM systems because profiling and automated decision-making are inherent risks. Such provisions create very stringent frameworks within which personal data has to be processed, as development information must comply with legality, fairness, and transparency. For example, explicit consent or legitimate interest form the basis upon which lawful systems, per legislation, collect and use data. This requires developers to implement consent management mechanisms and inform users of the purposes and methods of data processing. Additionally, the standards promote data minimization, which limits information collection to only what is necessary for specific purposes. Recent advances in machine learning and deep learning algorithms have positioned generative AI as the "new normal" within businesses, where AI is now a standard term. Consequently, this has trickled down to CRM, resulting in AI-CRM, which stands for AI-enabled CRM systems [12].

Data processing requirements emerging from the GDPR entail the principle of minimization, ensuring data subject rights, and a data protection impact assessment (DPIA) [13]. Principle data minimization will limit information collection; therefore, it may require an architectural redesign of AI-CRM systems to work effectively with smaller datasets. Subject rights impose obligations on developers to provide functionality for managing user information, including the rights of access, rectification, deletion, and portability. This will also require the creation of fronts for submitting requests and implementing automated handling methods, such as providing a copy of the information or removing it on time. Effect checks on data safety are crucial for AI-CRM systems because profiling and auto-choice-making methods can significantly infringe upon the rights and freedoms of individuals. DPIAs should be an easy and adjustable tool used in many fields and efforts. It should not necessarily be complex or time-consuming to carry out a DPIA; however, the degree of rigor involved must be commensurate with the associated privacy risks. This specifically digital product implements the above. "Regency Cakestand 3 Tier" and "White Hanging Heart T-Light Holder" were the most popular items, each attracting over 800 customers [14]. Figure 3 illustrates the top 10 products based on the number of unique customers.

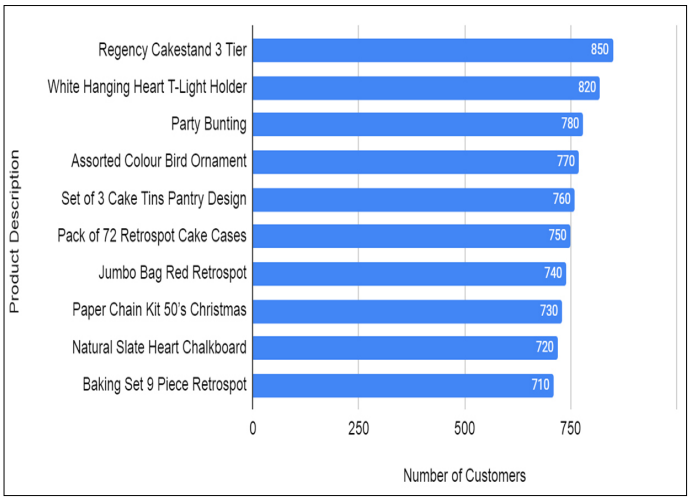

Fig. 3. Top 10 Products by Number of Customers [14]

Data minimization forms the core technical aspect of an artificial intelligence-based customer relationship management system, in that only data critical to achieving the set objectives is collected and processed [15]. This significantly reduces the risks associated with personal data processing, thereby ensuring conformity to international standards. In AI-CRM, data minimization is the selection of meaningful features for machine learning models towards reflecting AI-CRM, capturing non-redundant information, without affecting the quality of personalization.

Data anonymization is an important privacy protection technique within the AI-CRM approach, involving the removal or masking of identifying features. The associated methodologies, generalization, suppression, and pseudonymization, a mong others, enable analysis and model training while keeping the customer's identity safe as a lower priority. Pseudonymization, in turn, replaces identifiers with time codes; the latter can be reversed if done under a strict regime of security controls. This should always underscore the importance of being accompanied by additional security implementations like differential privacy. Access control is used to manage user rights in an AI-CRM system and to ensure nobody gains unauthorized access to data. Role-based access control (RBAC) distributes permissions according to job functions, thereby limiting employees' actions. Pseudonymization is when identifying information is replaced by time codes so that the identification can be reversed only under a strict regime of security controls. Information is much more secure when encrypted both at rest and in transit; encryption prevents the interception of information [16]. For example, Salesforce utilizes the AES-256 encryption standard for protecting customer data. The strength of access control is in the management of encryption keys and regular updates of policies, which require effort and attention from administrators. XAI techniques, like LIME and SHAP, clearly interpret the contribution of individual features to model predictions. For instance, marketing can use XAI to recommend a specific offer for a customer, building trust and calibrating algorithms. It is forecasted [17] that 70% of organizations will change their concentration from big data to small, broad data; this will provide much more context for analysis and make AI less data hungry.

An analysis of specific cases of AI application in CRM would shed considerable light on the methods of adhering to ethical standards, especially with the delicate balance that must be maintained between personalization and privacy.

Salesforce, a high-quality provider of CRM solutions, demonstrates an excellent approach to utilizing AI ethically. In 2018, Salesforce established the Office for the Ethical and Human Use of Technology, which is responsible for implementing the "Ethics by Design" principle in all its products and services [18]. This office will operate by the Trusted AI Principles, which emphasize responsibility, accountability, transparency, empowerment, and inclusivity. One major activity under this is the Data Review Board, which reviews all AI models to identify any potential biases that may exist within them. For instance, in one of its Marketing Cloud products, called Einstein, the firm discontinued targeting based on demographics and shifted to interest-oriented and behavioral targeting, thereby reducing the likelihood of discrimination. Additionally, Salesforce provides clients with tools to manage sensitive data: in Einstein Discovery, users can identify fields containing controlled information, such as age, race, or gender, which facilitates the effective use of AI [19]. These actions not only ensure GDPR compliance but also establish the firm's reputation as a leading player in fair AI.

Another example that further cements the guilt of CRM in ethical matters is that of Facebook's ad delivery algorithm. Study [20] found that Facebook's algorithm, which automatically determines who to show ads to, discriminated against others by displaying ads to more than two billion users based on their demographic information. For instance, men were more likely to see job ads for tech positions, and women were more likely to see job ads for service positions. This unequal economic opportunity raised concerns about fairness and compliance with anti-discrimination laws. The opacity of the algorithm further compounded the problem, as it made it difficult to spot and rectify bias. In lawsuits and criticism, including a 2022 settlement with the US Department of Justice, Facebook promised to modify its algorithms. Although this case does not involve their AI systems, it highlights the dire need for oversight and auditing once again [21]. This further demonstrates that a lack of transparency and oversight can lead to ethical mishaps, ultimately eroding customer trust. Analyzing these cases reveals best practices for the ethical use of AI in CRM systems. First, biases must be proactively detected and corrected. While Salesforce conducts regular audits through its Data Review Board, in Facebook's case, external researchers identified the bias; therefore, their approach seems more reactive than proactive. Secondly, trust requires transparency. While Salesforce has shown its customers the keys to understanding AIs, algorithms

on Facebook have surprisingly triggered a wide public outcry, mainly due to the opacity. Third, giving customers control over their data, as in Einstein Discovery, increases autonomy and, hence, trust, dovetailing neatly with the GDPR's articulation of data subject rights. Fourth, creating dedicated frameworks, such as the Office of Ethical Use of Technology, ensures regular vigilance towards ethical issues, a more effective approach than the ad-hoc method Facebook employed. Ultimately, continuous learning and adaptation to new research and regulatory requirements are essential for maintaining the high standards of ethics in rapidly evolving technologies. These are the very practices that would enable firms to mitigate risks stemming from privacy and bias while optimizing an appropriate trade-off between personalization and protection in their AI-CRM systems.

CONCLUSION

Artificial intelligence drives deep personalization in CRM, but it also raises the stakes in terms of the trade-off between effective use of data and ensuring privacy. Results of the above analysis pinpoint key threats to confidentiality, algorithmic opacity, and algorithmic bias. Internal actors can cause significant leaks; therefore, all traditional cybersecurity measures must be complemented with AI-specific access control and vulnerability management mechanisms. The legal context, including the GDPR and CCPA, among others, forms a strict framework within which AI-CRM platforms are required to demonstrate legality, fairness, and transparency in data processing. The designers should not only revise the architectures for storing and processing information but also implement DPIA procedures with continuous audits of models, as minimization principles and the realization of data subjects' rights necessitate such actions. The technical solutions for such issues will be delivered through a set of complementary methodologies, including anonymization and pseudonymization, differential privacy, federated learning, and explainable AI tools like LIME SHAP, which can support the improvement of explanations without compromising accuracy.

Salesforce teachings demonstrate that risks of discrimination can be greatly minimized and customer trust can be built if companies take an active approach to ethics by setting up offices dedicated to the cause and having a data review board, and abandoning demographic targeting. This is opposite to the insights that Facebook's delivery ad algorithm provided; it was based on a reactive approach that resulted in unintended discrimination, legal pressure, and even public pressure. The above comparison highlights that timely ethical oversight mechanisms, transparency in recommendation logic, and real data stewardship tools available to users are critical components of Responsible AI-CRM.

The digital use of AI-CRM can be applied ethically only if a multi-strategy approach involving regulatory compliance, technical protections, organizational audit processes, and cultural and ethical principles is integrated.

REFERENCES

1. V. Unanah and J. Mbanugo, "Integration of AI into CRM for Effective U.S. healthcare and pharmaceutical marketing," *World Journal of Advanced Research and Reviews*, vol. 25, no. 2, pp. 609–630, Feb. 2025, doi: https://doi.org/10.30574/wjarr.2025.25.2.0396.
2. AU10TIX, "Americans And Privacy: New Study Finds U.S. Consumers Overwhelmingly Concerned About The Lack Of Control Over Their Personal Information," *PR Newswire*, Apr. 26, 2022. https://www.prnewswire.com/il/news-releases/americans-and-privacy-new-study-finds-us-consumers-overwhelmingly-concerned-about-the-lack-of-control-over-their-personal-information-301532730.html (accessed Mar. 18, 2025).
3. S. Larsson and F. Heintz, "Transparency in artificial intelligence," *Internet Policy Review*, vol. 9, no. 2, May 2020, doi: https://doi.org/10.14763/2020.2.1469.
4. L. Yacono, "9 Internal Data Breach Examples to Learn From," *Cimcor.com*, 2025. https://www.cimcor.com/blog/internal-data-breach-examples (accessed Mar. 12, 2025).
5. "Three Cyber Security Risks Modern Businesses Face with AI Agents," *Metomic*, 2022. https://www.metomic.io/resource-centre/three-cyber-security-risks-modern-businesses-face-with-ai-agents (accessed Mar. 21, 2025).
6. "New Cisco Survey Shows Strong Relationship Between Privacy Awareness and Trust in AI," *Cisco*, 2018. https://investor.cisco.com/news/news-details/2024/New-Cisco-Survey-Shows-Strong-Relationship-Between-Privacy-Awareness-and-Trust-in-AI/default.aspx (accessed Mar. 25, 2025).
7. "See people, not patterns," *Accenture Interactive*, 2019. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/accenture-report-see-people-not-patterns.pdf (accessed Mar. 25, 2025).
8. B. Wolford, "What is GDPR, the EU's new data protection law?" *GDPR*, 2025. https://gdpr.eu/what-is-gdpr/ (accessed Mar. 26, 2025).
9. A. Zewe, "Fighting discrimination in mortgage lending," *MIT News | Massachusetts Institute of Technology*, 2022. https://news.mit.edu/2022/machine-learning-model-discrimination-lending-0330 (accessed Mar. 27, 2025).
10. B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner, "Americans' Attitudes and Experiences with Privacy Policies and Laws," Pew Research Center, Nov. 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ (accessed Mar. 28, 2025).

11. D. Georgiou and Costas Lambrinoudakis, "DPIA for Cloud-based Health Organizations in the context of GDPR," vol. 22, no. 1, pp. 187–198, Jun. 2023, doi: https://doi.org/10.34190/eccws.22.1.1144.

12. J. W. Yoo, J. Park, and H. Park, "The impact of AI-enabled CRM systems on organizational competitive advantage: A mixed-method approach using BERTopic and PLS-SEM," *Heliyon*, vol. 10, no. 16, p. e36392, Aug. 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e36392.

13. ICO, "What is a DPIA?," *ICO*, May 19, 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/ (accessed Mar. 30, 2025).

14. A. Kandi, "Personalization and Customer Relationship Management in AI-Powered Business Intelligence," *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 11, pp. 704–715, Nov. 2024, doi: https://doi.org/10.22214/ijraset.2024.65159.

15. Dr. Rahul Diliprao Tamhane, Aman Grewal, Ishan Sandhu, Prof. (Dr.) Vivek Rastogi, Arif Mohamed Khan R, and Krishna Bhimaavarapu, "Artificial Intelligence and Blockchain for Enhancing Customer Relationship Management (CRM) Systems: A Review of Emerging Trends and Challenges," *Nanotechnology Perceptions*, pp. 4059–4067, Nov. 2024, doi: https://doi.org/10.62441/nano-ntp.vi.3718.

16. V. R. Male, "Decoding Role-Based Access Control (RBAC)," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 11, no. 1, pp. 2082–2090, Feb. 2025, doi: https://doi.org/10.32628/CSEIT251112211.

17. Gartner, "Gartner Says 70% of Organizations Will Shift Their Focus From Big to Small and Wide Data By 2025," *Gartner*, 2021. https://www.gartner.com/en/newsroom/press-releases/2021-05-19-gartner-says-70-percent-of-organizations-will-shift-their-focus-from-big-to-small-and-wide-data-by-2025 (accessed Apr. 05, 2025).

18. January 10 and 2023 S. S. S. Newsroom, "Why Salesforce Aims to Build Products That Are 'Ethical by Design,'" *Salesforce*, Jan. 10, 2023. https://www.salesforce.com/news/stories/salesforce-technology-ethics/ (accessed Apr. 08, 2025).

19. "Salesforce," *Salesforce*, 2025. https://help.salesforce.com/s/articleView?id=analytics.bi_edd_about.htm&type=5 (accessed Apr. 10, 2025).

20. K. Hao, "Facebook's ad-serving algorithm discriminates by gender and race," *MIT Technology Review*, Apr. 05, 2019. https://www.technologyreview.com/2019/04/05/1175/facebook-algorithm-discriminates-ai-bias/ (accessed Apr. 15, 2025).

21. B. Imana, A. Korolova, and J. Heidemann, "Having your Privacy Cake and Eating it Too: Platform-supported Auditing of Social Media Algorithms for Public Interest," *Proceedings of the ACM on human-computer interaction*, vol. 7, no. CSCW1, pp. 1–33, Jul. 2022, doi: https://doi.org/10.1145/3579610.