Deep Science Publishing
https://doi.org/10.70593/978-93-49910-26-3_12

DeepScience
Open Access Books

Chapter 12: Establishing secure, ethical, and sustainable artificial intelligence frameworks in retail and manufacturing infrastructure

12.1. Introduction

Artificial Intelligence (AI) is rapidly emerging as a technology that will allow businesses to better engage with their customers and supply chain operations. AI-enabled technologies—machine learning, computer vision, robotics, deep learning, neural networks, natural language processing—will enable companies to gain a competitive edge in creating new products and services, along with competitive advantages in cost and time efficiencies. While AI is enabling transformation in every industry, its advances in the areas of big data, cloud computing, and storage will significantly enhance the capabilities of the retail and manufacturing sectors, as they manage highly complex infrastructures focused on consumers. While there are numerous opportunities AI implementations can unlock for the retail and manufacturing sectors, the latent risks remain, particularly those pertaining to customer privacy, discrimination, and workforce disruption. In this new predictive era, the interplay of technology, ethics, and values has emerged as a critical pathway to sustainable AI implementations (Binns, 2018; Jobin et al., 2019; Mittelstadt, 2019).

AI is projected to give rise to improvements across various retail and manufacturing infrastructure segments. For the retail sector, visual search and image recognition enhancements will improve the customer experience across search and visual merchandising, resulting in higher engagement, an increased number of transactions, and ultimately, revenue growth. In supply chain operations, manufacturing and inventory oversight will be enabled through AI technological capabilities that digitally enhance the existing workforce. This will allow supply chain operations to function in a more nimble and efficient manner, delivering quicker response times to shifting market demand. In the eCommerce area, simplified operations and services will be delivered through chatbot applications that facilitate virtual shopping services for customers. In set pricing and promotions, systems will be able to set optimized prices based on demand-sensing

analytics pulled from the market. AI-enabled promotions will sense demand elasticity and set optimized offers to yield desired results (Strubell et al., 2019; Raji et al., 2020).

12.1.1. Significance of Artificial Intelligence in Retail and Manufacturing

Artificial Intelligence (AI), a broad field of study, is driven by the notion to equip computers and machines with the ability to perform a variety of intricate tasks along with the capacity to independently learn from experience and multiple rounds of human interaction to considerably reduce the need for explicit pre-programming as well as with the capability of continuous improvement. Businesses involved in retail and manufacturing are focusing more and more on the potential impact of AI on various issues such as enhancing customer experience, improving operational efficiency and enhancing productivity and profitability through automation of mundane tasks as well as employing intelligent processes for areas like supply chain management, inventory tracking, forecasting and replenishment, data management, manufacturing process modeling, design and development, quality auditing, marketing, sales, post-sales support and other customer services.

Fig 12 . 1 : AI applications in Retail and Manufacturing

Despite being a comparatively recent invention, AI-enabled and AI-driven systems are actively being used for diverse purposes in everyday life. AI technologies and tools such as natural language processing, speech recognition, visual recognition, deep learning and machine learning, chatbots, intelligent agents, drones and autonomous vehicles, and AI-powered robotics have enabled hardware and software systems to perform tasks ranging from planning travel, translating languages, and playing chess, to identifying disjointed objects in images, guiding automation in warehouses, factories, and groceries, and even

performing complex surgeries. Giants from the technology domain are in a fierce race to better their offerings of services and systems that are embedded with various AI systems and technologies. In retail and manufacturing, targeted integrations of AI in various activities have had a considerable impact on productivity, efficiency, security, and customer experience.

12.2. The Importance of AI in Retail and Manufacturing

AI offers new opportunities for traditional manufacturing and retail sectors. Integrating AI systems provides smarter and safer ways in developing, manufacturing, and distributing products. Service provisions by both technology-enabled solutions and customer-contact employees will be enhanced. Over the years, AI has had a major impact on the transformation of retail and manufacturing sectors. Numerous operations and applications have made use of tools, processes, and systems enabled with AI technologies.

The use of AI and AI-based products and solutions transforms the needs of retail and manufacturing businesses for the enhancement and sustainability of their current operations, products, and processes. These transformations accelerate performance of these classic sectors which represent the backbone of many economies today. These AI-based transformation propositions and investments involve clear and understanding responses from process owners, strategic planners, and financial analyzers on the abilities, sustainability, and acceptability of the enabling technology in day-to-day provision of services by both humans and machines.

12.2.1. Significance of AI Innovations in Retail and Manufacturing

Academic research has employed the term artificial intelligence (AI) for multiple decades in diverse fields of study. However, only recently have we witnessed the diversification of research in the subfields of AI, ranging from robotic process automation to deep learning. These innovations have combined with machine learning to help create computer systems that enable new solutions to cybersecurity, finance, health care, manufacturing, retail, supply chain, and technology infrastructures for predictive diagnostics and analytics, among many others. Before 2018, there had been only two foundational academic studies on AI - the first one acknowledged the vitality of AI to the development and innovation of every industry sector; while the second argued the need for better financial data reporting of the impact of AI investments and innovation across sectors. Thanks to new broad, open access data occurring since the 2018-2019 periods, new analyses have emerged linking AI deployment and R&D expenditures with productivity growth. The accelerated growth of investments in AI for

knowledge-based tasks seen since 2018 by early adopters motivated a study of investment allocation for AI by the rest of those industries and companies playing catch-up.

In addition, a growing list of AI start-ups, mostly focused on the creation and generation of novel solutions to specific business problems by use of large pre-trained deep learning models in natural language understanding, language processing and computer vision capabilities, using both text and visual modalities. The advent of disruptive AI driven technologies helping to improve business decision-making have further underscored the urgency to develop new, innovative business strategies by company boards and top management across business sectors. Various AI-enabled technologies have already become fully deployed in decision support tasks in marketing and business development across retailing and services. These technologies include recommender engines powered by collaborative filtering based on implicit data, sorting through massive amounts of data simultaneously, coding messages persuasive enough to effectively sell a product, and generating effective dialog for chatbots and virtual assistants to answer customer questions and close business opportunities.

12.3. Current State of AI Technologies

While innovators in both retail and manufacturing sectors have long exploited the unique characteristics of AI, there are few clear winners in the race for differentiation today. Most industry players are still learning to integrate AI into their own operations, as product cycles shorten and demand cycles and styles become increasingly volatile. Enterprises have taken different steps and are at different stages in the journey. There are AI technologies that apply AI for established use cases, such as demand forecasting and inventory management. There are experiential AI technologies, which push the boundaries of customer experience and employee interface. But still, it has not reached the tipping point of standardization. Technologies and technology applications are evolving and maturing at varied cadence across the value chain. The integration of AI technologies is enabling companies at various points in the retail and manufacturing value chain. AI algorithms designed to mimic or improve relatively simple decision-making acts performed before by as many as a billion human workers are increasingly able to solve problems involving estimating parameters for statistical models or other mathematical operations on data that are at the type of tasks performed before by human workers in roles located primarily in developed economies. These tools are finding their market. It is also becoming commonplace for companies in retail and manufacturing sectors to focus their near-term implementation activities on these operational workloads, as the return on investment from the automation of processes that takes decisions based on structured data, or selecting values from an available set of options,

have gotten companies in other service sectors returns on investment greater than that of other investments in enterprise technology.

12.3.1. Overview of AI Applications

The use of artificial intelligence in industries is not novel. Experts have written on the subject for many years now, and expert activities like predictions and marketing have taken precedence. The emerging areas, which are often termed machine learning, deal with the more specific use of algorithms to learn from the data, and have been shown to be more widely useful across nearly all industries because they take less expert effort than constructing rules-of-thumb for every application. As a result, application companies across retail and manufacturing are working hard to produce platforms that address specific needs that can be met with such algorithms. Specific services are available for many functions that are typical of businesses, such as system monitoring to guarantee that they function properly, cybersecurity services to safeguard the networks, and virtual assistants to enhance human activity. More complex routines are also being packaged. For example, intelligent offerings help in analyzing and understanding a variety of consumer images and initiate actions such as price changes if an anomaly is detected. Other integrated offerings help in predicting desired stocking levels and initiating actions for supply chain optimization such as selecting suppliers based on deliveries. Solutions in computer vision leverage advancements at the image level and apply them in diverse areas such as automating source inspections and datacenter monitoring that require gesture recognition. Cleverly designed social sentiment engines assist in the prediction of company health and evaluating the impact of decisions such as new product introductions or promotions. Natural-language-based document analyzers help in assigning intents to emails and categorizing business documents, replacing the rules-based engines that have been standard for this work.

12.3.2. Challenges Facing AI Integration

While data-driven systems are now evolving with impressive capabilities, widespread adoption and practical impact of AI techniques face many significant challenges. For example, up to 80% of an AI project budget and time is spent on data preparation. This is in part due to the fact that much data generated in retail and manufacturing lack the structure that is needed for efficient AI processing. Creating, cleaning, labeling, and maintaining high quality data is extremely costly, especially when AI-enabled systems are productized and need continuous data quality support. Consequently the cost-benefit analysis might be unbalanced against the integration of an AI system. Out of box techniques of basic neural nets are not guaranteed to bring the maximum payoff. To

leverage the current cutting-edge techniques to achieve a significant increase over the baseline behavior of legacy systems, large investments on custom solutions and high performance computing are usually required. External help from specialized players is often needed to try to achieve the desired impact, but the availability of local, quality talent is an additional bottleneck. The development and operational deployments of AI products have their own unique challenges that do not apply to traditional software. The lifecycle of model training, validation, monitoring, and updating is very different, yet integrated into other development processes like those used for decision support, pricing, or planning software. Without investment in specialized tools that facilitate a model lifecycle, the speed and efficiency improvements that AI products could bring may not be fully realized.

12.4. Ethical Considerations in AI Deployment

Deploying AI systems in manufacturing and retail is a formidable challenge; developing an ethical framework will ease the negotiation challenges. Among the ethics frameworks available, the framework provides an effective start point. Using this framework makes some aspects of responsibility clearer, and other perspectives more difficult to frame clearly. However, this ethical framework is complicated and often contradictory due to the nature of AI combined with business intentions and agency relationships. AI is a tool, and possessor companies are responsible for handling it benevolently.

To satisfy its innate ethical and community responsibilities, businesses must also consider any stakeholder consequences duratively, not as a momentary performance in accord with Spending=Profits. Good people tend to predict good long-term interaction outcomes, and they want to hire other good people with a similar focus. The primary short-term focus should be a practical definition of fairness that fits the well-understood realities of the specific manufacturing task and its environment, lasting not just a day or a year, but for as long as possible. Then there must be an accurate monitoring feed from the actual task, as well as sufficient logic to apply the fairness correction before the bias has caused a large enough decrease in performance to negate the positive effect of implementation.

Furthermore, business integration efforts should strive to ensure that the clear ethical governance distributed across the various production and HR considerations for all involved organizations embraces possible goals, the possible guidelines for achieving those goals, the range of anticipated consequences of following any of those guidelines, and the overall overriding guidelines governing the final decision-making procedures for rollout project choices. Careful communications and easy monitoring and correction can help ensure that concrete best practice implementations satisfy the promised goodwill implementations that satisfy not just business but also community aims.

12.4.1. Bias and Fairness in Algorithms

Problems of bias and fairness have long bothered humans, often being at the core of their politics and conflict, deeply scrutinized by many philosophers. Thus, the question arises if bias and fairness of human decision-making process can be fully objectivized, such that an automated decision-making process with algorithm implementation would benefit from it. We explore in this section some aspects of bias and fairness in the context of AI adoption in the retail and manufacturing industries, providing arguments for and against what seems to be an objectivization of human behavior and decision-making process.

Through the diffusion of AI systems and the implementation of algorithmic decision-making across the domains of retail and manufacturing, bias may not only emerge in the AI or algorithm itself at play but also in the training data or model data as well as the human being that adopts it. Some of these biases can be summarized as follows: (1) data bias – faulty, imbalanced, or insufficient training data can lead to algorithms that are biased in their decisions; (2) algorithm bias – biased algorithms may be a result of implicit assumptions, incorrect approximations, or specific design choices made by developers; (3) user bias – algorithm users can influence algorithmic output and adopt biased algorithms in the decision-making process. Bias informs the fairness of algorithms and plays a role in their scope of application. A retail or manufacturing setting is fair for algorithmic decision-making if any moral discrepancies or injustices do not exist in the supported and automated process, and that there are no differences between real and applied decision-making conditioned on sensitive values.

The development of fair algorithms thus requires more and more transparent decision-making models and interactive support that allow users to comprehend the workings of the algorithm applied and its specific application domain, as well as the included decisions taken by the algorithm in certain situations. Only then this helps to scrutinize algorithmic decision-making and to fight bias on all dimensions.

12.4.2. Transparency and Accountability

Building accountability into AI tools requires increased regulatory oversight and enforcement, but it also requires companies to be accountable to the communities they impact, schools to teach students about the social implications of AI tools, and for AI creators to take ownership for the long-term effects of their creations. Stakeholders such as labor organizations, civil rights groups, and scholars should partner with companies to raise ethical standards and ensure due diligence in identifying harm, anticipate problems, share knowledge, share assessments of systemic risk, agree on value-based metrics, and prepare remediation plans. Regulation is complicated by the use of models

and AI systems relying on complicated algorithms. Such difficulty can inhibit accountability and mitigate the benefits of AI tool implementation. AI developers, researchers, corporations, and companies should work with local communities to increase availability and develop standardized models and certifications for AI systems. AI corporations should disclose details on how their systems work, with what technology they are powered by, and create impact statements explaining the expected direct and indirect impact on society. Developers of AI systems should also welcome openness through external impact assessments that make contributions to the field of accounting for the social implications of tools in development.

Key actions to ensure accountability mechanisms are used to assess business impact on communities are the creation of "AI Ethics Boards"; third-party review; algorithm guidelines; industry regulations; curriculum guidelines; due diligence; and impact statements. Recommendations from civil rights groups and academics working on AI policy point to the importance of responsible impact statements. Companies should work with guidelines and an external review process to create and share regular algorithm impact reports to create accountability for addressing and modeling expected mitigated outcomes as well as a framework that examines the types of ethical concerns most likely to arise. Using a tool creation impact statement can also promote accountability by increasing awareness of and sensitivity to creators' moral responsibilities, both toward the users of their systems and toward the broader society. These guidelines are important so that new, automated decision-making features provide clear explanations; use reasonable default options; and allow consumer anomaly reporting.

12.5. Security Frameworks for AI Systems

AI-based models, which are gaining quick momentum, are securely deployed using the inferencing hardware security mechanisms. Federated learning protects the sensitive data by keeping it within the device, allowing for a decentralized learning architecture, with multiple devices locally computing model updates, which are then aggregated to form a global model. Recently proposed FL schemes, involving noise and digital gimmick-based methods, achieve secure gradients during participatory learning in a manner aligned with privacy requirements. Small devices can support a more efficient and communication-efficient design for FL through the concept of local model training. It is also seen that concepts from decentralized AI could be used to ensure augmented privacy with federated learning. The decentralized learning architecture allows devices to locally train while assuring robustness to adversarial actions. However, the architecture demands improved communication security due to untrustworthy communications, and heterogeneous AI requires the fast convergence of FL for large model designs.

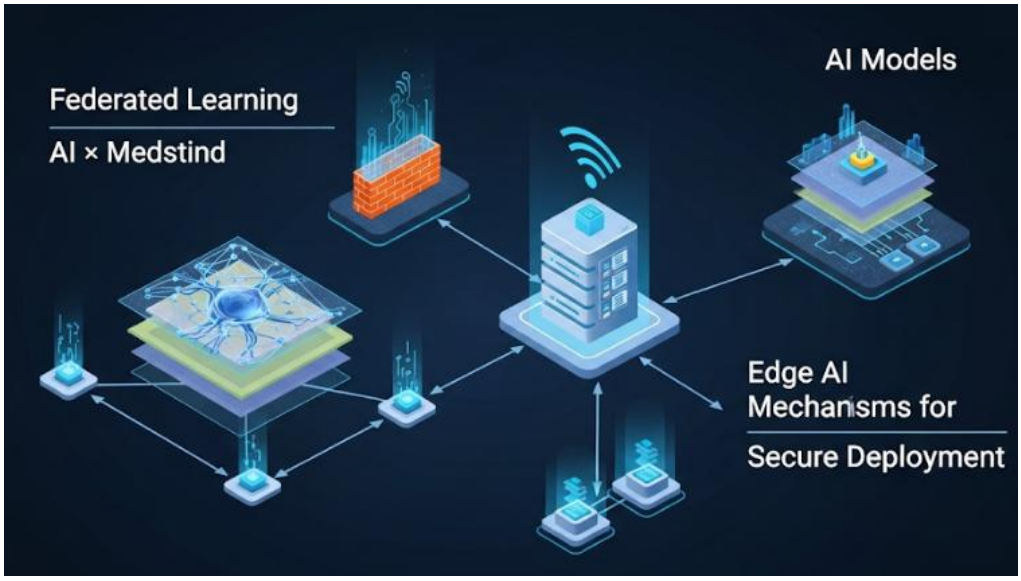

Fig 12 . 2 : AI-based Models and Their Security Mechanism

Edge AI mechanisms for collaborative learning could be designed to flexibly federate locally encrypted models in clearer communication domains rather than random communication settings. The recently proposed domain-aware axis-flipped collaborative learning framework utilizes heterogeneous edge devices to generate and share model updates for the group of intended devices within the same domain. Achieving an efficient and dependable consortium-setup in collaborative distributed edge AI would also augment communication security, reliability, conflict resolution, and trust metrics. The multi-party computation-based protection during AI model updates allows hidden parameters to transferably deploy during real-time edge conditions, avoiding quality degradation during model sharing. Despite these initiatives, many issues within AI security and fast relevance to dynamic edge arrangements and target application areas remain unexamined. These require further research to address, especially with the ongoing threat to data quality issues.

12.5.1. Data Protection and Privacy

This is an ever-present concern, especially in light of numerous data-collection efforts taken by big data companies, stirring widespread panic in the general populace, as they slowly chip away at civilizations' hard-earned privacy. Data is fundamental in training and building AI systems. Shouldn't such data be well secured? Shouldn't it respect every individual's freedom of choice – the ability to say no? Or more practically, availability of reasonable opt-out options and the ability to revoke consent? More so, shouldn't such data be sufficiently obfuscated to protect individuals from any ill-intentioned attacker?

Or perhaps even destroyed should the data be deemed legacy? Policy-makers across the globe have argued about these questions for a long time, leading to rules that outline the laws around transparency while data collection, access to the data collected, control over the data collected, and right to data erasure; also considered the "Right to be Forgotten." Furthermore, such policies expand to not just personal data but also training data for models used for research purposes, known as the Right to Data Portability.

Companies building AI systems must respect such rules to be compliant. Operating in the defined legal framework is good practice and greatly reduces the legal liability in addition to guaranteeing the safety and privacy of individuals involved. Naturally, policy-makers must come out with new individual-driven rules to hold companies accountable, but they can only be expected to be trusted to an extent. Secretive data collection efforts can evade the watchful eyes ahead. It would be naive to assume all policy-makers have been sufficiently educated to understand the complexity around data protection that comes with AI systems. It would be self-destructive to ignore privacy. Failure to address the identified concerns can lead to huge reputational losses: Negative publicity, financial losses, and withdrawal of user consent.

12.5.2. Threat Mitigation Strategies

While AI systems are especially vulnerable to threats, they can also serve as solutions for some cybersecurity and privacy challenges. For example, researchers have developed deep-learning-based solutions for face recognition that can resist impressed or printed-based spoofing attacks. Proposed biometric systems based on deep neural networks have been able to increase liveness-detection accuracy, thereby minimizing user anonymity loss. Additionally, AI-enabled threat detection systems can analyze activity to identify anomalies and automatically adapt security parameters to fend off potential intrusions.

Companies can bolster and secure their operations and protect their infrastructure and data through implementing security benefits of AI and employing traditional cybersecurity methods. Organizations can sift through massive data streams quickly to identify anomalies and proactively mitigate misuse and threats by deploying generative models or other AI models trained specifically to detect risky usage of AI. Such implementations are designed to search systems for flaws and vulnerabilities that are vital for preventing successful hacking attempts. AI can help deflect and absorb threats in practice by rapidly analyzing enormous amounts of IT event data and automatically detecting and remediating events that necessitate a SOC analyst, including identifying and stopping malicious scripts or processes.

Companies can also leverage third-party platforms to alleviate risk factors that are integral to the safe deployment of AI solutions. Platforms that utilize machine learning

can decrease the impact stemming from the shortage of cybersecurity skills at organizations by using natural language processing techniques to allow non-experts to script and automate AI-security protocols. AI-enabled solutions can also mitigate the dangers of employees using AI tools without the explicit approval of security leaders at organizations. For example, actors in the dark Web can offer access to friends to a user's account for a short time, in exchange for a low fee.

12.6. Sustainability in AI Practices

Integration of AI into manufacturing and retail has a significant environmental cost, but it is not accounted in economic figures; true costs however includes costs that take into account economic, ecologic and social aspects. Embedded in this is the question of how to deal with the accountability of the AI company and executives onboard. A starting point for bringing these hidden costs to light is labelling of the digital carbon footprints associated with AI algorithms. By making carbon impact figures a part of deals between companies and AI service providers and between service providers and tech developers, companies can be encouraged to choose low-carbon options when building AI solutions. Moreover, awareness of these costs might create powerful incentives for making servers more energy efficient by using low-carbon energy sources.

The complexity of ethical and sustainable AI practices is further exacerbated by the massive data proprietary aspect of training data. In analogy to the current system of allowing a percentage of a company's profits to be designated as membership dues to charities that assist the designated community of health workers, a loss percentage dedicated to a fund that helps communities that have been exposed to intrusive data collection efforts could be established. The idea would be to create a collective shared by all developers but that supports engendered community at the time of data scrapping and exhaust of paper photos, videos, and other materials uploaded to the digital cloud that were taken unprotected communities subjected to digital pillaging. A percentage from the projects would go into a common pool and be used for that purpose – doing local reparation for data use that couldn't be measured for silos.

12.6.1. Environmental Impact of AI

The carbon footprint of AI systems is significant. From hardware production to data center operation, including AI, ML, and GPU workloads, AI workloads can cause environmental harm, associated energy costs, and high carbon emissions that can prevent reaching net zero goals. It has been estimated that running a single session emits as much carbon as driving a car for 1.5 miles. Further, a model with 175 billion parameters is estimated to use 284.3 gigawatt hours of energy just to train, equivalent to the average

energy footprint of 25,200 American homes in a year. AI training also produces a considerable amount of CO2 emissions; for instance, training a one-shot language model can produce 284 tons of CO2 emissions, estimated to be equal to the lifetime emissions of 46.2 U.S. citizens.

The issue has been getting worse with the increase in AI adoption as a lack of regulation, efforts, and community pressure encourages firms to focus solely on their bottom line and push the environmental impact of AI up the ladder. However, the carbon impact of AI models is increasing faster than the impact of other technology sectors, and thus it is essential to improve the energy and carbon efficiency of these models and their supporting infrastructure to meet that challenge. Burning fossil fuels contributes heavily to global warming. Although in the short term, the environmental impact of AI may increase, AI will contribute to reducing energy-related CO2 emissions by 2.1 billion tons, which is 15% of the world's total energy-related CO2s by 2030. Many companies are now providing sustainable options to contribute towards Net Zero goals, through green AI systems, ecosystem tools, and AI solutions that significantly reduce carbon emissions like training workloads which help accelerate the findings of Net Zero.

12.6.2. Sustainable Resource Management

Establishing a foundation for sustainable resource use becomes instrumental, with ESG scores seen as an all-compassing reporting metric. Digital technology reporting can be mapped back to ESG standards, showing the environmental impact of using and creating new digital technologies, including AI. This section further unpacks this synthesis for perspectives on the relationship of AI and Digital Tech to ESG.

AI tools need to reflect sustainability impacts in what they are reporting on. AI model and data center providers need to have clear direct and indirect emissions targets in place. For on-premise companies, they need to gain competitive advantage or employee loyalty for having a Green Data Center. For cloud companies, decarbonization along with renewables procurement practices need to be at the core of their value propositions. GHG emissions accounting and other aspects of Advanced ESG disclosure need to be at the core of value propositions. For software companies, decoding the climate contribution of software developers and using software better has to be front of mind. The impact of digital and AI on GHG emissions needs to be well understood and codesigned constraints packages put in place to help prevent AI or digital practically occurring GHG emissions. For Advanced ESG modeling companies, integrating advanced AI into the data flow of these sustainability models is likely to be highly attractive to the Formal missions. AI open source tools are also likely to be highly relevant in ensuring future reporting tools are easy to use for fund managers and lawyers.

Digital and AI are critical in enabling Advanced ESG Disclosure and governance. AI can provide the empowerment so actively sought in making product decisions on the basis of values. They are also critical in providing the data models and accounting clarity on the use and control of Digital and AI tools contributing to the GHG Debt.

12.7. Regulatory and Compliance Issues

With the rapid expansion of AI deployment in almost all sectors, multiple advisory and regulatory bodies have started laying down certain regulatory frameworks. Given the global nature of the retail and manufacturing sectors, it is important to know that while local compliance is necessary, it should be aligned to the broad global frameworks. Doing so allows for creating globally applicable systems which can reduce cost of compliance while ensuring that the guidelines and compliance are up to the standards promulgated by the advisory regulatory bodies. The challenges in ensuring compliance will be in covering the regulatory framework laid down by most advisory bodies. There have been many recent comments by authorities from industrialized countries who have laid down the broad ethical guidelines for AI. The following subsections describe the guidelines issued by these bodies. Such standards can be realistically implemented by manufacturers and retailers and may eventually have a trickle down effect onto local regulations.

At the same time, as countries start enacting the principles laid down above, countries need to be careful to not create an impossible burden on manufacturers especially smaller and local manufacturers, as well local retailers. While digital media is rapidly becoming a critical component of every organization, with more and more of them embracing digital transformation, governing rules and regulations are still hard to formulate. This is amplified by the need to build consumer trust to ensure that data collected during the digitalization phase, which will later be used by AI technologies created as part of the digitalization, is kept confidential and secure. Consumer trust becomes a critical factor for both manufacturers and retailers especially in sectors such as food and fashion.

12.7.1. Global Standards and Guidelines

The AI architecture covers the Generate—Transfer—Act framework, pertaining to the knowledge chain that could be realised through associating components of the peripheral edge, the compute edge, and the cloud. Although highly abstract, it covers the complex topic of an AI global infrastructure, since it could comprise any process, component, middleware, or algorithm that uses any of the elements within the triad. Turning this into an integrated approach for digital twins, design science techniques, AI foundational components, and cross-border intellectual property protection is indeed complex.

Intriguingly, some proposals can be found from national bodies that promise to build on a core of guidelines developed in recent years. However, the focus is different in all cases. For one country, the threat of new technology national champions eclipses the protection of human rights, trust, and accountability; in another, this is shifted towards the perspective of new collusive behaviours; and, in a different region, the risk of contactless AI deployment at the public service, educational and social domains is considered far more catastrophic than lesser problems that could occur within the private sector.

The guidance documents are responses to the challenges implicit in a rapidly growing technology. Therefore, they are all at early state. However, they propose different approaches to the problem, with consequences in the development of the technology itself. For instance, with the issue of general artificial intelligence models, while one region has taken a more cautious (preventive) approach by proposing to categorise this development as Threat to Society, and according to the limited guidance on the topic contained in the many drafts released in 2023, another has proposed a more support-oriented model.

12.7.2. Local Regulations and Compliance

Manufacturing and Retail are the domains used to discuss the topic of AI compliance tools and compliance in general. Countries including Japan, Singapore, China, Qatar among others are creating their own AI regulations with many countries focusing on the practicalities of AI regulation such as safety, compliance and trust. Labelling deals with what rules must be followed and how and why compliance is important. The compliance function is responsible for creating, implementing and monitoring policies and procedures that ensure the company operates within independent regulatory standards and internal policies. Compliance addresses issues of cultural and system control for AI-based systems. This is a coveted domain where the presence of standards and lawyers is crucial. Over the next decade we will see local corporate compliance functions active in the area of AI. Creation of solutions, applications, products and services utilizing AI are among the key pillars for the future. The creation of such solutions quickly and securely both in line with product roadmap and compliance requirements is the desired goal. Balancing between the two goals is challenging. Local regulatory environments do not have a common global approach. For instance the European AI act puts forward a strict set of standards for AI classification, compliance and monitoring. Companies will have to build specialized compliance functions to meet the criteria set out. Other countries are preparing their own AI regulations based on the European AI Act in an effort to be competitive. AI serving autonomous vehicles have the strictest standards both in Europe

and in North America. Practical implementation and existence of compliance tools will help with rapid adoption.

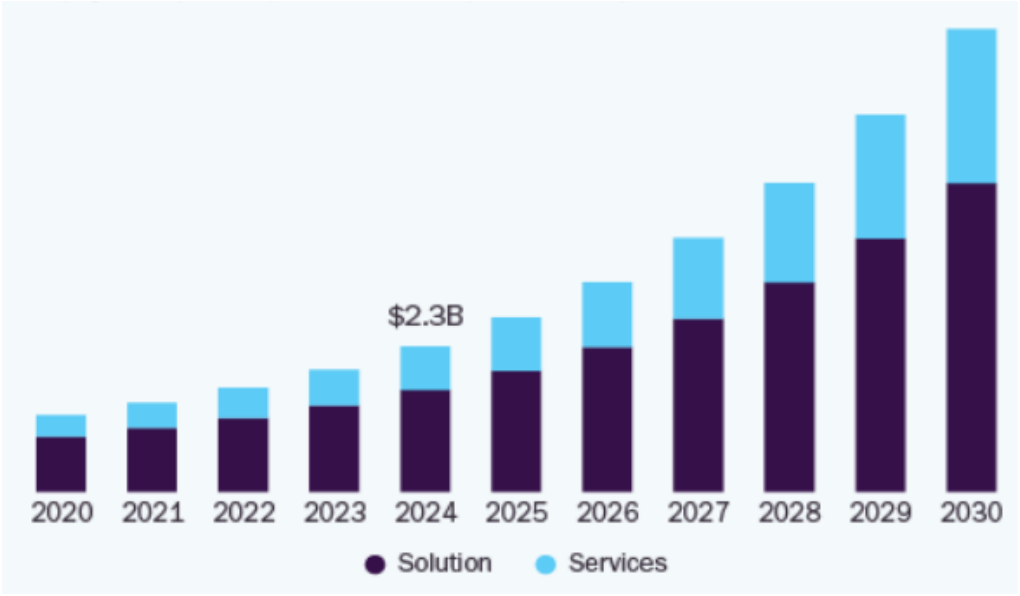

Fig 12 . 3 : AI Trust, Risk And Security Management Market

12.8. Conclusion

In this paper, we explored emerging topics surrounding artificial intelligence (AI) technologies in secured, ethical and sustainable deployments in the retail and manufacturing environments. Within our findings, we've categorized the types of AI technologies that will help reshape the future of retail and manufacturing. This includes the role of ecosystems, Natural Language Processing tools, Machine Learning platforms, Edge AI systems, Vision AI, robotics, and automation solutions, amongst others. Retail and manufacturing organizations must ensure that they create a secure, responsible and ethical approach to the development and deployment of AI tools that augment human labor programs through the deployment of seamless, interconnected services within their work and public environment to maximize productivity from both their human and technological workforce. To this end, partnerships with public, governmental and educational institutions are crucial to secure societal understanding, involvement and acceptance of any future deployments.

It is incumbent upon software makers and hardware creators to create the legal frameworks necessary that prevent these tools from dismantling the very fabric of labor relations, of cooperative collaboration and of human creativity that have made companies in retail and manufacturing the economic engines of every society.

Education, retraining and reskilling programs must be a condition of usage for any organizations deploying AI in retail and manufacturing. Society cannot accept that industry's major shareholders receive disproportionate gains at the expense of the workforce who have dedicated their lives for decades inside these organizations. Companies and society depend on the collective symbiosis between people and organizations. Consciousness on usage, a business model reflecting this reality, an ethical code of conduct and action will be the prosperous road to safely navigate in the decades ahead.

12.8.1. Final Thoughts on the Future of AI in Retail and Manufacturing

A very important NLP revolution has brought natural language understanding into most applications. One of the most conspicuous benefits of AI is the sophistication it allows. Some applications, such as automated customer interaction, already allow the use of AI for customized virtual assistants handling customer queries 24 x 7, while allowing human interventions only when necessary. This has resulted in reduced costs, improved customer interactions, and increased customer satisfaction.

The market is rife with exciting possibilities of augmented human capabilities. A healthcare startup leverages AI for disease preventive services. Its digital health program applies intuitive nudges to help patients prevent diabetes and lean toward a healthier lifestyle. It incorporates AI with IoT, taking continuous glucose monitoring and serving tailored reports to patients. Delivering digital health services through its app boosts accountability, acts as a personalized coach, and dissuades glamorization of unhealthy, sedentary lifestyles. Big multinational companies are looking at the long term and preparing educators and students for wide-scale AI implementation in the workplace and society.

AI promises to deliver incredible efficiencies, higher productivity, improved cost ratios, and revolutionary outcomes for the manufacturing and retail sectors in diverse business areas ranging from supply chain management to customer interactions using virtual assistants, and from asset management to cost savings. Besides core business areas, AI enhances the overall user experience, allowing customers to have fun over the long haul by offering hyper-personalized services.

References

Jobin A., Ienca M., Vayena E. (2019). The Global Landscape of AI Ethics Guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Binns R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, 149–159. https://doi.org/10.1145/3287560.3287598

Raji I.D., Smart A., White R.N., Mitchell M., Gebru T. (2020). Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 33–44. https://doi.org/10.1145/3351095.3372873

Strubell E., Ganesh A., McCallum A. (2019). Energy and Policy Considerations for Deep Learning in NLP. Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, 3645–3650. https://doi.org/10.18653/v1/P19-1355

Mittelstadt B.D. (2019). Principles Alone Cannot Guarantee Ethical AI. Nature Machine Intelligence, 1(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4