Deep Science Publishing
https://doi.org/10.70593/978-93-49910-19-5_3

Chapter 3: Risk compliance in the era of artificial intelligence: Navigating global regulatory landscapes and financial ethics

3.1. Introduction

Call it "The Quiet Revolution". The march of artificial intelligence (AI) into the world of finance has been deceptively subtle, and vastly more wide-ranging than we may realize. The financial services sector, traditionally not first in line to adopt new technologies, had already begun embracing AI before the pandemic, valuing its many benefits in operational efficiency, targeted product development, data-driven customer service, risk evaluation, and fraud detection. The acceleration of the pandemic opened spaces across the public and private sectors for its utilization. The timing seemed fortuitous; many of the pandemic-era surges of remote work and e-commerce appeared to create both the stimulus and the opportune environment for using AI to reshape workplaces and customer interaction. All that capital investment suddenly flowed into endemic tasks such as insurance processing or approving university loans based exclusively on data; much of this work was also highly subject to risk, especially concerning the ethical use of the demographic data that informed these decisions. AI was a vital partner (Arner, Barberis, & Buckley, 2017; Binns, 2018; Gai, Qiu, & Sun, 2018).

The vast range of AI-enabled applications coalesced as the global industry saw growing demands for enhanced recommendations for investing, investing through robots, radically quickened and eased underwriting, increased speed-to-decision on gaining auto, home, or commercial insurance, and faster assessments of business loan requests. From commercial banks to consumer-oriented FinTechs, deposit, and lending institutions began to plan vast investments in technology and product enhancement.

Longer-term thinking began to account for potential industry employment and support ramifications of this digitization of service. Suddenly, an industry accustomed to massive compliance-related investments was being offered the potential to broaden its investment base and accommodate shorter decision-making timeframes by prudently adopting AI enablement (Zarsky, 2016; Veale & Edwards, 2018).

3.1.1. Overview of AI's Role in Financial Services

Artificial Intelligence (AI) is increasingly becoming a prominent tool deployed across the global financial sector, augmenting a variety of functions. From enhancing the accuracy of consumer credit risk prediction and enabling faster and more efficient customer identification systems to optimizing investment portfolio performance and automating broker-advisor services, the benefits of AI are undeniably vast. Capitalizing on rapidly growing advancements in AI-related technologies such as Big Data, Machine Learning, and Natural Language Processing, financial institutions around the globe are harnessing AI at an accelerated pace.

Fig 3 . 1 : Risk Compliance in the Era of AI

The accelerated engagement of AI within the financial sector, and the consequential benefits it affords, raises several regulatory issues. The public is rightly concerned that the risks inherent in the deployment of AI, such as possible discrimination, systemic and market-wide risks as well as data privacy violations, could undermine its positive contributions. Societal awareness of the bias and transparency problems underlying AI, as well as AI's volatility and propensity toward 'flash crashes,' has heightened following the recent routing of financial system giants. Policymakers have thus initiated efforts to develop a framework suitable for the unique features of AI and its financial risk implications. Increased scrutiny concerning various aspects of AI engagement, from Consumer Protection laws and the implementation of safety and soundness measures to Financial Market Regulation and the framework for international cooperation, is thus taking place.

3.2. Understanding AI and Its Impact on Financial Services

While AI has varied markedly in its definition, it is recognized and agreed upon as consisting of a computation-oriented approach rather than a neuroscience-oriented approach to the question of intelligence. AI integrates the disparate disciplines of computer science, psychology, neuroscience, linguistics, operations research, control theory, and economics, to realize goals with cognitive and intelligent properties - reasoning, relation, perception, learning, and knowledge representation. AI achieves these goals through a conceptual framework consisting of knowledge, efficiency, representation, computational resources, and computation. AI - both in specializations, such as machine learning and deep neural networks, and in breadth and scope - has transformed speed, power, breadth, and user-friendliness to be at the stage to become one of the leaders of the Fourth Industrial Revolution. In finance, AI promises widespread adoption - deriding traditional rules-based programming; revolutionizing trading, investments, insurance, risk management, compliance, and fraud detection; and growing at a powerful rate - both in revenues and contributions to reducing costs that sectors of finance presenting a $3 Trillion Plus industry.

The impact of AI, however, has drawn predictions, warnings, hopes, trepidation, caution, hysteria, and debate. Individuals, organizations, and society have grappled with defining and regulating the predictions, impact, developments, applications, use, and realization of AI in finance. AI also encompasses rigorous, mainstream disciplines of econometrics, data science, machine learning, and computer science and is developing, and applied to prescriptive and descriptive matters of practical concern, research topics, realizing financially focused results, and creating financial knowledge and awareness. Finance, however, in both practice and research, and AI have distinguished elements - finance relates to knowledge, risk, and global markets of diverse and disparate sizes while AI concerns domains with self-confidence and mastery of intelligent and cognitive properties.

3.2.1. The Transformative Influence of AI on Financial Practices

The rapid advancement of artificial intelligence (AI) is perhaps only rivaled by the advent of the internet. Various forms of AI are impacting disparate facets of human experience, with stronger effects felt in developed nations. In recognition of its capability to both increase productivity and negatively impact employment, countries are increasing their investments in AI. Fostered by shifting market conditions due to geopolitical tensions, the COVID pandemic, climate change, and energy shortages, this reorientation marks an increasing convergence of policymaking with national security—in this case, by promoting domestic growth in AI. This trajectory is unlikely to change, especially for technological solutions. It is a matter of time before capabilities emerge not only to address labor scarcity and improve productivity but also to help mitigate climate-related challenges.

How AI is deployed affects its cost-benefit impact—and how related benefits are distributed. As a complement to human effort—optimizing but not attempting to replace human intuition or imagination—AI can yield vast improvements in a range of fields, including healthcare, education, and insurance. Financial services are no different. As a workplace, it has during its visible history undergone several changes in how it implements technology. Each wave of technological innovation has sought to reduce the cost and risk of financial intermediation. AI—along with blockchain, the Internet of Things (IoT), and cloud computing, all essential elements of FinTech—promises to augment this transformative role, alongside a deep wave of consolidation across the global financial intermediary landscape. The resulting emergence of a few large players providing diverse services in different countries, driven by the economics of scale and breadth, signals the inexorable trend toward universal banking powered economically and financially by integration within these growing digital ecosystems.

These players will serve as hosts to, or tie together, multiple platforms offering distinct services. Collaboration rather than disintermediation nationally in diverse ways will characterize the relationship between new entrants and established actors—whether banks, exchanges, or information utilities.

3.3. The Evolution of Risk Compliance in Finance

The financial sector is perhaps the most constrained in the implementation of AI and machine-learning technologies due to the extensive testing, validation, transparency and explanation, and recourse requirements implemented in the risk management framework which has been in an ongoing process of extension, improvement, and adjustment through various reforms, the accounting standard, the Models Aspect of the Act, the regime implemented for insurance companies, and many additional laws and regulations at the national and local level. This section discusses the development and aspects of these various initiatives and consolidates them into six high-level unique values – trustworthiness, oversight, transparency, accountability, explainability, and performance – that any mathematical model must possess to be considered compliant or not.

Risk comes in many different flavors and definitions, and tends to be viewed from the paradigmatic “decision-based” and “states of nature” academic definitions, as the “decision-makers' uncertainty about the ranking of consequences”, or the “unpredictable future deviation from the expected outcome of a decision”, respectively. The financial sector’s unique combination of decision-making uncertainty (this consequence is unknown therefore it should be considered a risk) and states of natural unpredictability (the market return is unpredictable therefore it cannot be modeled) during almost all market realities (decisions can be made but results can only be poured into the market “blind”) except for extreme and transitory highly-liquid “crisis” market events, differentiates the financial sector from other complex strategic sectors, such as warfare and military operations, or the pharmaceutical industry.

3.3.1. The Progression of Risk Management Standards in Financial Sectors

The appearance of financial services regulators transformed financial markets across the world and made their governance and oversight subject to public policies. During the late 17th century, the fire insurance company and the Wagering Act enacted by the English Parliament laid the foundations for securitizing citizens’ productive efforts via monitoring them. Two centuries later, with the 19th-century development of life insurance companies to support workers’ families, and banks whose liabilities were demandable on short notice, the public conversation became concerned about whether the financial market intermediary business model properly served the public interest or was rather a business that operates at the expense of society in the name of profits.

While scandals involving bank and life insurance company failures at the expense of a public good incentivized capitalist states to create central banks, agencies aimed to signal the existence of boundaries for acceptable behavior towards collateralized public interests. The two World Wars and the Great Depression increased the number and power of the state regulatory apparatus complementing market dynamics by trying to minimize the costs of bankruptcies affecting economic activities via cascading models or the deposit or capital requirements a financial institution needs to meet about their clients. Guided by the principles of market self-control presented in the Laissez-Faire axioms, financial institution risk management internal areas matured assuring both decision-makers and other involved stakeholders that refinancing via emitting shares on regulated stock exchanges occurs only when the firm is solvent.

3.4. Global Regulatory Frameworks for AI

With the meteoric surge in the global development of AI technologies, governments and stakeholders recognize the necessity to establish cultural, ethical, and regional priorities for its deployment. Legal and ethical frameworks for risk compliance have generally developed and evolved alongside technology, with codes of ethics established by various global institutions and non-governmental organizations. Now, however, businesses must address violations of new laws regarding specific AI-based use cases and support their compliance with clearly defined internal risk and auditing procedures.

This section examines and compares a sample of current regulatory frameworks through the following two lenses: use case design and objectives. The key regulatory themes and categories that pose potential employer liability and duty are use cases that report on sensitive characteristics; use cases that have a high risk of centralization; objectives that seek enhancement; and use cases and objectives that are exogenous to systems and constituent organizations. We explore the real-world relevance of international themes and categories for regional employers in different parts of the globe.

As a primary actor in global policymaking, the European Union has introduced major regulatory lawmaking moves that many stakeholders expect will influence and inspire compliance efforts and regulatory moves in other areas of the globe. Data-based technology regulation is not new to the EU. The European General Data Protection Regulation became law in May 2018, influencing how European countries, businesses, and institutions develop and comply with privacy laws surrounding data-based technology.

3.4.1. European Union Regulations

The European Union (EU) is taking the lead in developing advantageous AI regulations for the handling of the challenges that come with its rapid adoption. Numerous laws that impact AI have already been enacted; in addition, the proposed AI Act is still in the negotiation phase and represents a milestone development in global AI regulation. In this evolving landscape, compliance in financial services must address legal risks while promoting the safe and responsible use of AI; importantly, financial institutions must also consider the ethical implications of AI in financial services.

The General Data Protection Regulation (GDPR) has worldwide application to companies that collect data on EU data subjects, thus it has a deep impact on AI. Numerous data protection issues arise about AI and its use, such as unlawful data collection, storing, sharing, and usage policies; adoption of new data processing technologies; and protection of data subject rights, among others. AI adoption also implicates Article 22 of the GDPR on automated individual decision-making, as well as the EU's Digital Financial Strategy, which promotes the use of AI, blockchain, and large amounts of data in financial services. GDPR requirements for consent and data protection impact assessments amplify the burden on companies that use AI decision-making processes. The EU is also advancing AI regulations through proposed amendments to financial services directives and regulations and the AI Act, which establishes specific regulatory requirements for AI in banking, insurance, and capital markets. Financial regulators are encouraging the responsible use of AI for the overall benefit of society.

3.4.2. United States Regulations

The United States has historically maintained a laissez-faire approach to the market, placing more reliance on market forces than on ex-ante regulation. This 'no intervention' principle is historically rooted in a belief in the primacy of freedom of expression and also the supernatural efficiency of the markets. The emergence of AI and Digital Technologies, including Social Media, creates strong new market failures or 'regulatory gaps' that may require new ex-ante regulation. These include: the emergence of radical innovations blurring the distinction between personal and public domains regarding surveillance methods exacerbating a dynamic decrease in market competition; controversies surrounding the validity of the copyright free speech distinction when applied to algorithms responsible for the dissemination of speech; and the intervening efficiency of Governments in democracies versus the use of AI and digital technology for surveillance and Social Control by Authoritarian regimes. Even within the limits of a narrower approach to Freedom of Expression and Antitrust, the brewing controversies surrounding Regulatory Gaps indicate an incoming wave of Government Regulation.

Currently, the United States has a patchwork of federal and state laws. In terms of Federal Law, there has been no single focused regulatory action on AI until now. However, many different propositions on AI regulation have been tabled and a plethora of regulations that cover certain aspects of AI have been enacted across various Federal Agencies. Timid steps into AI Regulation have by way of a 2020 Executive Order on Maintaining American Leadership in AI and non-binding Guidelines issued by various agencies. The Federal Trade Commission and the Department of Justice Antitrust Division have recently provided drafts regarding facial recognition technology that could be extended to other AI technologies in the absence of tailored legislation as a first step toward possible regulation.

3.4.3. Asia-Pacific Regulatory Approaches

Regulatory approaches in the Asia-Pacific region are diverse and evolving, with varying policy goals and foundational frameworks. In general, regulation is more challenging compared to other regions, as AI is still broadly defined and policymakers share differing views on the best approaches. Most legislation focuses on narrow applications of AI such as facial recognition technologies, and there is no comprehensive framework at present. The policy is often more responsive in the region, reacting to perceived harms faster than the processes in other areas. Since the region shares core technological competence, these AI governance methodologies are necessary to determine the best approaches to tackle harm. We explore developments from three of the largest economies in the region, namely, South Korea, Japan, and China.

Fig 3 . 2 : Asia-Pacific Regulatory Approaches

The South Korean government has been proactive in exploring how the economy can benefit from generative AI as it has released multiple papers on the subject. Notably, it recently published a strategy and action plan outlining its ambitions for its economy and society. There also exists a parallel draft legislation on the regulation of generative AI, reflecting influences from regulatory initiatives. The National Assembly plans to enact an oversight committee act, amid concerns about data and privacy protection issues relating to the government AI system. The rapid developments in the field have prompted the South Korean Communications Commission to assemble a Generative AI Committee and to simultaneously widen the scope of its AI regulation.

3.5. Ethical Considerations in AI Deployment

AI can be an enormous force for good in the world. But where we can harm, we must take extreme care. The ethical design, deployment, and regulation of AI technologies is one of the most important discussions of our time. Part of the current allure of AI is the ability to offload tasks that are dangerous, repetitive, boring, and time-consuming, which would have known benefits to workers and organizations who utilize AI. While models help with brainstorming, drafting, and research tasks, AI deployment has the potential to upend entire industries, and as such requires the same sort of scrutiny as any major technological upheaval.

Bias and Fairness Early partnerships between tech companies and law enforcement agencies, particularly those that aim to bolster immigration and border security operations, reveal a disturbing and stark contrast to industry-wide pledges to address bias, add greater accountability and transparency to AI systems, and avert the deployment of tech that may replicate or exacerbate inequities. These strategic partnerships have drawn criticism for the potential use of biased predictive algorithms that use arrest history data and other external feature sets that reinforce systemic bias – thus feeding an insatiable need for technological accountability that is more than simply responding to press releases after deployment.

While private sector AI developers may not have any institutional framework mandating fairness and transparency, the associations and partnerships they form, and their support of associations that work towards the creation of AI design frameworks, can be leveraged to encourage private sector companies to create a system where regulation and ethical deployment is in their best interest.

Transparency and Accountability Clone the coder, not the code. Hacker ethos encourages the replication of a coder's innovation. However, for AI, a hedge against nefarious innovation is that coders behind the models must logically limit the levels of access made available through their technologies to avert any illegitimate manipulation. For example, access to pre-existing information and large volumes of collected data enabled prompt engineering to successfully prompt for basic code-writing guidance, by directing the AI model to develop code based on the parameters supplied in the prompt.

3.5.1. Bias and Fairness

AI systems learn from patterns present in the data they are trained on. If those data reflect any prejudices, discrimination preferences, or over-weights or under-weights of various social or ethnic groups, like race, gender, sexual orientation, or others, the risk of bias and unfairness in AI predictions is high, as well as the risk of providing unfair assessments. Thus, whether by design, personal choices, or the impact of social phenomena over a long period, an AI trajectory and predictive path can be influenced by existing risk preference behaviors, creating issues of fairness in the ensuing decisions. The dangers of unfair biases in AI systems can be maintained or amplified, deepening already present issues of discrimination. Unfairness in AI risk models can have leading impacts by design or from predictive bias towards already operating targets and impacted groups, associating risk with their decisions or transactions.

Many factors can influence data collection and labeling, such as historical data collection, algorithm, and model selection, and how predictive modeling is being deployed and used. In particular, there is concern that the application of metrics and models for risk selection applies in a static form for certain groups and population labels and without consideration of statistical balance is being respected. Thereby, mechanisms help in avoiding groups or populations being treated less favorably. From that perspective, identifying and mitigating bias through design, training, and data programming plays a key role in determining the fairness of AI systems. Furthermore, the identified problems regarding bias and fairness risk are seen as being more urgent. In areas such as criminal justice, healthcare provision or credit evaluation offerings, or language modeling or sentiment classification of social media statements, the proposition or deployment of unfair or discriminatory AI produces unethical results.

3.5.2. Transparency and Accountability

To monitor and mitigate risks, companies using AI need to provide sufficient transparency on the role and function of AI systems as well as assurance of robust human oversight to ensure that accountability cannot be avoided. Transparency facilitates independent audits, investigations, and learning, including by affected stakeholders who lack technical expertise, as well as addressing concerns about potential privacy violations in connection with the development and deployment of AI. When AI systems function autonomously, and in high-impact scenarios, and there is a high risk of material violations, harm, and impact on individuals and communities from the use of AI, you would expect the company to be more transparent including sharing proprietary and commercially sensitive information to ensure external accountability. Transparency is particularly difficult for systems that use machine learning at their core, but stakeholders should be informed about what data was used to train and test AI systems, what potential decision-making functions were involved and how, which calculations were made, how the potential consequences of the decision-making were considered and weighed, and what hypothetical scenarios were run to predict the performance of the model going forward; as well as about the resilience of the AI system to errors, in particular if it uses biometrics to identify and classify people for important decisions. Developers can provide this information by writing an explainable model or using post-hoc explainability techniques. For many organizations, especially those that rely on third-party algorithms, implementing these practices might require a significant number of changes to existing systems, procedures, and vendor management processes.

3.6. Risk Assessment Models for AI in Finance

Traditional risk assessment and management policies and regulatory frameworks are obsolete as they do not employ experimental tools or considerations appropriate for emerging technologies. As AI solutions gain prominence in financial services and budgets allocated for developing and deploying AI technologies are shifted at warp speed, assessing AI risks in finance is urgent and of global significance. At the same time, financial services, unlike other industries that are currently the leading early adopters of AI technologies, have distinct differing structural complexities, intensive intercrossing interfaces with the keen propensity of triggering shocks extending for other economies, and the intricacy of transaction summaries occasioning unique implications on assessing AI risk profiles and use case classifications of allocated AI budgets. Ransomware incidents in financial institutions, for example, could have serious consequences as the cross-border ramifications of financial shocks dirtying the interconnectedness with the global economy can be staggering. This chapter discusses preliminary risk assessment models for AI in finance. Both qualitative and quantitative risk assessment models for assessing risks associated with various applied and experimental AI technologies deployed in risk-sensitive, high-stakes decision-making human organizations like those found in finance are discussed as AI risk management framework prototypes. During their push to promote global collaboration and dialogue for AI regulation, both highlighted the necessity of developing risk management tools to validate that developing, deploying, and using AI systems are safe and comply with ethical principles.

3.6.1. Quantitative Risk Assessment

Risk assessment touches all aspects of risk governance, from identification and classification to modeling analysis, and risk reporting. Risk assessment models typically borrow concepts from other disciplines. In most financial institutions, risk assessment is a qualitative exercise; quantitative risk estimators, based on Value-at-Risk and stress testing, are mainly used in the market risk domain. Quantitative risk assessment faces additional challenges in the AI space, in particular, for non-linear models and unsupervised learning. The goal of this chapter is to list the existing risk assessment models and algorithms and to point to some of their flaws and omissions.

Quantitative risk assessment faces several challenges. First, the potential risks are manifold. For classification tasks with labeled data, there are sample size problems to take into account, label noise, class imbalance, uninformative or suspiciously informative features, model complexity, and the fact that classifiers usually do not provide calibrated probabilities. For regression models, the challenges are even more daunting: estimation of risk of miscalibration, prediction intervals and regression quantiles, heavy tails, sparse high-dimensional data, label noise, volatile prediction functions, and uninformative features, modeling of tail dependencies and lack of transferability of tail dependencies to out-of-sample states, predictive sparse high-dimensional multivariate distributions. For clustering and unsupervised learning, there are additional challenges: lack of classifiers, label noise, high dimensionality, and volatility of distance-based measures of distance, dependency, or variable selection. In addition, resources are often scarce.

3.6.2. Qualitative Risk Assessment

Many educational institutions, researchers, and corporations have begun to release AI security risk assessment tools to provide developers and deployers with a way to recognize, understand, and improve security risks within their systems. These tools are far from definitive. They will not solve the problem of poorly specified or compromised goals; nor do they detect all risks. Rather, they serve as supplements—enabling critical thinkers to discover and explicitly acknowledge risks not immediately obvious in a product description or its technical documentation. Moreover, embedding a risk assessment within the standard internal review process, and enabling cross-team dependencies to define the risks they are responsible for mitigating throughout the software lifecycle, will facilitate an organization-wide accountability and cost-sharing model that further cement the focus on user and operator safety and align on priority.

Most commonly discussed RAs focus on deploying AI. Some are general enough to be applicable across many product lines; others focus on narrow areas. RAs can come in document or checklist form; they can be a set of guiding questions, or be fully specified checklists integrated with internal review templates. Tooling for developers can also perform live checklists in document editors during product development. The benefit of a draft is extensibility: A team can report by mailing the draft to the product or applicable review team to encourage their reporting processes or review sessions. That review could require the reviewer(s) to extend the RA with advice for the product team and any developers before documentation, integration, and deployment begin.

3.7. Compliance Challenges in AI Implementation

In several cases, we have seen companies rushing to adopt AI technology and development solutions without fully appreciating or grasping its ethical implications or compliance requirements. This has potentially detrimental consequences for businesses and society at large. The implementation of AI raises many compliance challenges for organizations, from privacy to pro-social risks. As AI reshapes the market for products and labor and adds to the complexity of regulatory compliance, organizations must advance their AI implementation strategies while adhering to regulatory frameworks and company policies. To ensure these strategies fulfill business goals without adverse ethical implications, organizations must enhance their frameworks about data privacy and operational risk.

AI companies need to comply with privacy protection standards, which promote privacy rights, establish consent requirements for data-sharing, offer protection for digital footprints, and establish penalties for violations. One of the most significant requirements is state approval of any algorithm that uses human data to make predictions and recommendations. AI relies on vast amounts of data. An AI tool requires organization-controlled data that is comprehensive and of sufficient size, which is not always available. The current regulatory landscape poses challenges for organizations in implementing AI due to the access restrictions on consumer data that both security and privacy regulations impose. These guidelines can lead to high operational costs since AI algorithms need expensive data cleansing, preparation, and segmentation processes before deployment. Consequently, AI developers cannot use available consumer data to produce an algorithm to test during the implementation stage because it is often not representative of real life, thus leading to bias against people and groups of individuals due to the sensitive nature of the data.

3.7.1. Data Privacy Issues

Of the various compliance risks that AI presents, data privacy issues are perhaps the most severe and controversial. The use of AI requires the ongoing collection and analysis of large datasets containing personal data. Moreover, AI uses and manipulates this data in complex ways that are difficult to understand. While privacy laws have been written to protect individuals from the excessive invasiveness of data processors, AI challenges some of these assumptions by treating the data as inanimate inputs into a largely automated decision-making process. In addition, existing privacy laws were written under the assumption that data collection and use occurs only in the prototypical data controller–data subject transactions, whereas the use of AI by different actors expands the realm of potential data collection and use dramatically, making it impossible for data subjects to understand when they are affected so that their privacy choices and rights can be respected.

The juxtaposition of data subject privacy rights and AI design and application intends ultimately to create friction in both operationalization and pace. Machine learning techniques optimize exposure, leading to models, such as recommender systems, that learn from our collective behavior each moment we spend online rather than on a defined learning set. Achieving targeted ownership of data subjects' capacity to ignore a prompt, ad, or simply another box to click open for future messaging is what the system is built to do, but it often runs counter to the existing rights of individuals. The tension is mirrored elsewhere in the privacy framework with the competition law prohibition against the abuse of consumer market power. The notion of informed explicit consent rests on a significant power imbalance, not unlike that assumed between shareholders and boards of directors in corporate governance. Those who are documented as providing the consent must at the same time be capable of understanding the implications of their actions for data collection and use.

3.7.2. Operational Risks

Challenges for the implementation of AI technologies in business revolve mostly around intellectual property, safety and liability, trustworthiness and cybersecurity, lack of transparency, and ethics. Under operational risks, we include those compliance challenges stemming from the current stage of implementation and the impact of AI technologies in organizations. Operations risks are also referred to as legal and regulatory risks. They arise from the way companies operate which is, in essence, the decisions and enforcement of such decisions made by officers and employees of organizations. Lack of oversight can lead to false answers generated by Chatbots. One of the first amazing results of the combination of transformers architecture and general end-to-end training was shown to make up references to non-existing articles, impersonate famous authors, and demonstrate political bias. However, this fact did not stop other developers and third parties from cutting corners of safety and privacy, providing unsolved, unreliable models; or just abusing these available tools to provoke nasty consequences. Model governance practices are very important in the establishment of AI Risk Management systems for the responsible deployment of these algorithms in organizations. Innovation might seem to drive the responsible and ethical use of these new technologies to the back seat. Organizations want to capture as much of the adoption wave of AI as possible; investors want to see short-term performances. Transparency and ethical values are a long-term investment. Respect for privacy and large-scale adoption of ethical values have an additional impact in financial services where the fines seem to be huge with monetary and reputation consequences associated with violations.

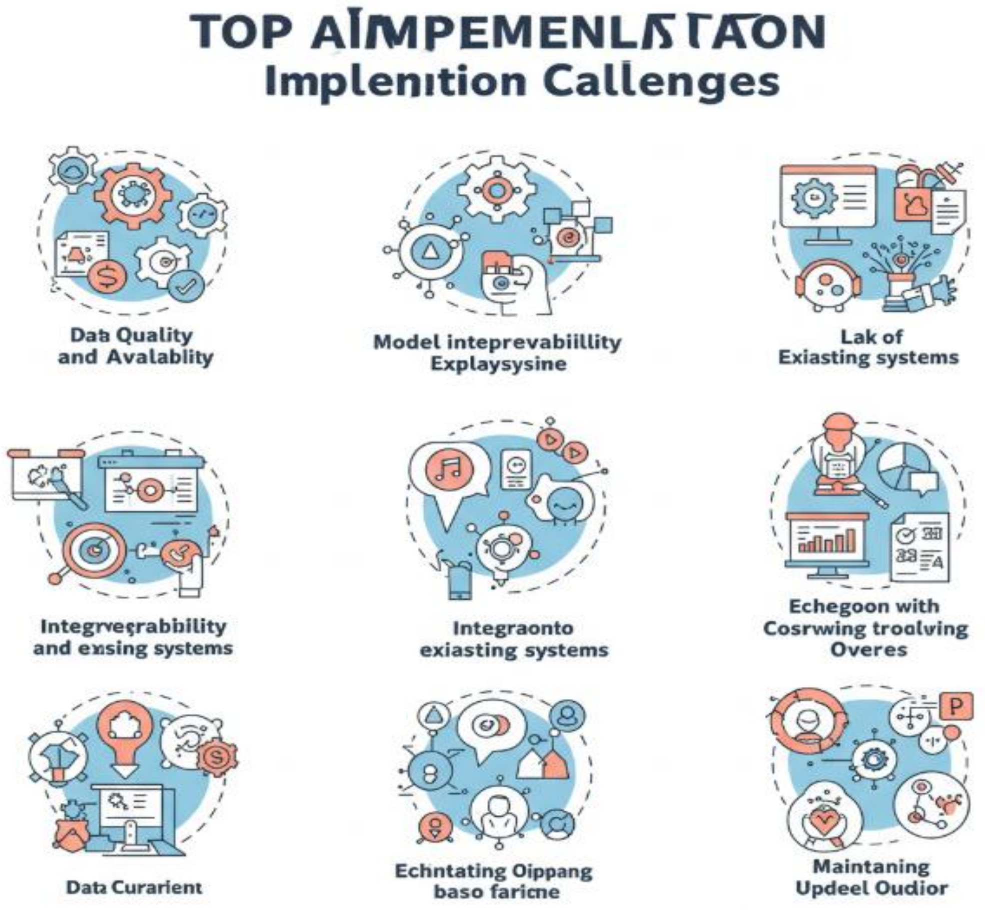
TOP AIMPEMENLATAON
Implenıtion Callenges
Dab Quality and Avalablity
Model inteprevabiillity Explaysysine
Lak of Exiasting systems
Integrvegrabbility and exsing systems
Integraonto exiasting systems
Echegoon with Cosrwing troalving Overes
Data Curarient
Echntating Oippang baso faricne
Maintaning Updeel Oudior

Fig 3 . 3 : Top AI Implementation Challenges

3.8. Conclusion

The ubiquity of AI algorithms in risk management creates tremendous expectations both for transparency and confidentiality. The era of low interest rates for lending is disappearing and financial industries need to re-evaluate their AI risk management. Ethically irresponsible behavior has extensive financial ramifications. A first positive step consists of reflections and perspectives and we built cautiously the case for compliments and confronts. The strategy consisted of reflecting ethically on the use of AI techniques in finance for risk, capital, and portfolio management. Our analysis is rather positive and we concluded with the moral if statement: 'Test and tune them, but do not take them out!'.

An inevitable consequence of our short and positive conclusion is that the unbeatable masters deserve also utmost respect. They may have some to blame for their current situation of relative impotence since they have faulted damagingly - but no treason - during the last financial crisis, by allowing irrational exuberance to reach absurd levels, without intervening in time, by their utmost shareholder equity theory, so to say. But the neuro-human brigade is addressed grafting on traditional artificial intelligence a sort of operational grease or maybe a self-proclaimed dubitable fiduciary role in charge of checking and tuning the outputs determined by the various AI techniques for risk management. Rational exuberance has also to be indeed inserted into the current agenda of the utmost masters. Emphasis should also be put on the now popular investing - undoubtedly blending both profitability and ethical concerns - during the day, the job of AI techniques would be that of janitor - roll up their sleeves and tidy up all the linear and non-linear investment implications coming out from the specific and general behavioral market efficiencies, so guaranteeing a more efficient, less stochastic or, why not, deterministic pricing of all existing financial assets.

3.8.1. Final Thoughts and Future Directions

Considering the increasing sophistication of AI technologies and the methods to manipulate public sentiments and social trust, regulators are called to keep an adequate level of detection without impairing the healthy evolution of technology and adequate support to its adopters. Our study highlights that regulation is currently being implemented in isolated territories, however, with a future perspective of convergence of the corresponding legislations, it is important to prepare a sound legal framework that addresses all the legitimate AI technology uses. In pursuing compliance and implementing a risk-based plan, leading organizations encoded and translated into a set of principles and values their political view of AI technology responsible deployment. Rather than excluding a priori the implementation of AI technology in the financial services industry, they focused on demanding the appropriate audit trails in the AI technology tools they adopted. Not distinguishing firms, from wanted or unwanted uses, the perspective of defining the maximum eligible risks linked with people affected by the systems became the philosophical principle of the responsibility willing AI technology deployment, in which the design must support extreme auditing. From the perspective of knowledge discovery for the advancement of science and the enhancement of the overall individual well-being, the greatest concern relates to systems impacting essential personal rights, for instance, recruitment, police surveillance, insurance attribution, credit scoring, justice conviction prediction, consumer marketing, formative assessment, and classification of health accelerators. There is still an evident conflict between the commercial and societal mandates that institutions must balance. However, the impracticability of adequate public intervention in the private sector, or in other words, the externality effect of certain activities cannot be freshly understood, if not adopting the perspective of the maximization of the social welfare.

References

Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017). Fintech and Regtech: Impact on Regulators and Banks. Journal of Banking Regulation, 19(4), 1–14. https://doi.org/10.1057/s41261-017-0038-3

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

Zarsky, T. Z. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. Science, Technology, & Human Values, 41(1), 118–132. https://doi.org/10.1177/0162243915605575

Gai, K., Qiu, M., & Sun, X. (2018). A Survey on FinTech. Journal of Network and Computer Applications, 103, 262–273. https://doi.org/10.1016/j.jnca.2017.10.011

Veale, M., & Edwards, L. (2018). Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling. Computer Law & Security Review, 34(2), 398–404. https://doi.org/10.1016/j.clsr.2017.12.002