Risks Associated with Innovation: The Case of Artificial Intelligence

Dr DJEFEDIE Stéphane Contard

Research teacher Higher School of Economic and Commercial Sciences University of Douala Laboratory of Architectural Finance and Management of Organizations (FARGO) Cameroon

DOI: https://dx.doi.org/10.47772/IJRISS.2025.910000496

Received: 02 November 2025; Accepted: 08 November 2025; Published: 17 November 2025

ABSTRACT

The digital transition is fostering the rapid rise of artificial intelligence, which, in turn, is further driving digitalization, leading to a profound and lasting transformation of society. The growing adoption of artificial intelligence in organizational activities as well as in various aspects of daily life raises the issue of potential associated dangers. This text highlights the emergence of artificial intelligence and examines various risks arising from progressive and disruptive innovations on the social fabric. It also encourages reflection on the expected benefits as well as the precautions to be considered in the context of this technological change.

Resume

La transition numérique favorise l'essor rapide de l'intelligence artificielle, qui, à son tour, accélère la digitalisation et entraîne une transformation profonde et durable de la société. L'adoption croissante de l'intelligence artificielle dans les activités organisationnelles ainsi que dans divers aspects de la vie quotidienne soulève la question des dangers potentiels qui y sont associés. Ce texte met en lumière l'émergence de l'intelligence artificielle et examine les différents risques liés aux innovations progressives et disruptives pour le tissu social. Il invite également à réfléchir aux bénéfices attendus ainsi qu'aux précautions à prendre dans le contexte de cette mutation technologique.

Keywords-Artificial Intelligence, Risks, Innovation, Political Economy, Management.

MOTS-CLES: Intelligence artificielle, Risques, Innovation, Économie politique, Management

INTRODUCTION

About seventy years ago, the debate surrounding artificial intelligence (AI) focused primarily on a technical question: "Can a machine think?" [TUR 09]. Today, this question seems to be decided in favor of AI, whose use is becoming widespread, facilitated by the rise of natural language processing algorithms. Until recently, its use was mainly attributed to large firms such as Amazon's logistics centers. Now, thousands of small organizations are implementing solutions such as automated tracking or activity reports, for example to detect food consumption in prohibited areas of the workplace [OCO 22]. Artificial intelligence also maintains close connections with other branches of the economy. Its progress makes it possible to integrate intelligent microprocessors into a wide variety of equipment: from vehicles to industrial equipment, including household appliances. This development creates an increased need for computing power to manage and analyze the massive volumes of data from these connected devices [HIL 22].

Technological innovation is a key driver of economic and social transformation in contemporary societies. Among the most significant technologies of the 21st century, artificial intelligence (AI) stands out for its ability to automate complex processes, improve business performance, and generate new services and products. However, this advancement is accompanied by multidimensional risks and uncertainties: job losses, algorithmic bias, lack of regulation, technological dependence, and even ethical and societal threats. The central question of this article is therefore the following: how do the risks associated with the adoption of artificial intelligence manifest themselves, and how can organizations anticipate and manage them in a context of rapid innovation? This question is all the more relevant given that AI is often adopted without a systematic analysis of its collateral effects.

Much research examines how AI can mitigate or anticipate risks [MA21; XU 22; YW 21], notably through improved forecasting capabilities [KY 21] or through detection mechanisms to limit fraud and financial crimes [HG 21; QLG 21; SAM 21]. It has also considerably optimized financial risk management, whether market or credit risks, thanks to the automation of data collection, the construction of predictive models, resilience testing, or the evaluation of the performance of systems such as credit scoring [JON 21; KAS 21]. Artificial intelligence tools are also proving valuable in spotting potential risk signals [ARS 21]. Artificial intelligence can also be used to assess risks and ensure effective monitoring in complex logistics networks, as well as in the prevention of money laundering [CSK 21; GGB 20]. Collaboration between humans and intelligent systems—in other words, between human and automated intelligence—tends to produce better outcomes [BHH 21; ZRM 21]. As with any major innovation, the introduction of emerging technologies generates societal concerns. Fear of what is new or poorly understood is well documented. Some nations display a higher cultural tolerance for uncertainty than others [HOF 80; HH 01], and the innovation process remains inherently unpredictable [UZU 20]. Despite this, the potential for social disruption is a universal issue.

Although general opinion tends to consider that artificial intelligence helps reduce a certain number of risks, it can also generate new forms of fragility, which is the focus of our reflection. Several categories of threats associated with the use of AI have been highlighted [CUL 21]. Eric Schmidt, former president of Google, highlights crucial issues such as algorithmic distortions, inequalities, usage drifts, international conflicts, as well as current technical limitations [MUR 21]. A relevant case is the unintentional implementation of racial or socio-economic biases in applications based on artificial intelligence. Furthermore, AI systems rely heavily on the massive exploitation of data, which they process using advanced computing technologies. This data can serve purposes of general interest, commercial or societal. For example, some companies are using artificial intelligence programs to examine their databases to identify consumer habits, brand interactions, and customer profiles. Some of this information is private, which justifies growing concerns about data privacy. To strike a balance between privacy and business objectives, the European Union's General Data Protection Regulation (GDPR) [GDPR 18] stipulates that personal data must be "collected for a specific, explicit, and legitimate purpose and must not be further used in a way that is incompatible with those purposes." It also requires that this data be "processed lawfully, fairly, and in a transparent manner for the data subject" (Article 5, [GDPR 18]). This same article also sets out strict rules regarding the limitation of the amount of data collected and the duration of its retention.

The overall objective of this article is to analyze the risks inherent in integrating AI into organizations, while identifying possible management and regulatory levers. The specific objectives are: - Identify the types of risks (economic, legal, ethical, social) associated with AI. - Evaluate current governance models for technological innovations. - Propose strategies to mitigate these risks.

Based on this, we pose the following research questions: 1. What are the main risks associated with the use of artificial intelligence? 2. How do these risks vary across sectors? 3. What analytical frameworks can be used to assess and prevent these risks? 4. What recommendations can be made for responsible AI governance? We draw on a multidisciplinary theoretical framework, notably drawing on: - The technological innovation life cycle model (Rogers, 2003) - Technological risk theory (Beck, 1992) - Approaches to algorithmic ethics and AI governance (Floridi, 2018; Jobin et al., 2019) These models allow us to structure our analysis around an analytical model integrating the interactions between innovation, risk perception, regulation, and use. The study adopts a mixed-methods exploratory approach, combining data: - Quantitative, from surveys of technology company managers. - Qualitative, collected through semi-structured interviews with AI experts, lawyers, and CSR managers. - Secondary, analyzing institutional reports (OECD, UNESCO, UN), legal texts, and scientific publications. The conceptual framework articulates the following dimensions: innovation – risk perception – governance – societal impact. The hypotheses tested include: - H1: The more mature an organization is in its use of AI, the more it develops risk management mechanisms. - H2: Highly regulated sectors are better at anticipating ethical risks related to AI. The results show that perceived risks vary greatly depending on the uses of AI. Companies operating in the healthcare, finance, and security sectors express greater sensitivity to ethical and legal issues. The majority of organizations do not yet have clear internal policies governing the use of AI, particularly with regard to algorithm transparency and the processing of sensitive data. The analysis also highlights a disconnect between rapid innovation and regulatory adaptation, exposing companies to risks related to their image, compliance, and user trust. In conclusion, AI-related innovation, while essential, requires rigorous and multifaceted oversight. Risk management must be integrated from the design phase of AI projects, in line with a culture of transparency, ethics, and social responsibility. 1. The creation of internal ethics committees within organizations. 2. Ongoing training of stakeholders on AI issues. 3. The adoption of internationally harmonized regulatory frameworks. 4. The involvement of stakeholders (employees, users, experts) in the governance of AI projects.

Legally compliant processing requires that the data subject has given consent for one or more specific purposes, or that such processing is necessary for the performance of a contract to which the data subject is bound, for compliance with a legal obligation, for the protection of the vital interests of that person or of a third party, for the public interest or for the legitimate interests of the controller (see Article 6, [GDPR 18]). Any failure to comply with these legal obligations may then lead to legal and ethical risks.

LITERATURE REVIEW: Technological progress and uncertainties

A distinction is made between incremental innovation and disruptive innovation [CHR 13]. Innovation is an obligation for organizations wishing to preserve their market position and maintain a competitive advantage. Some sectors of activity are more constrained than others to intensify their innovation efforts.

Most advances are incremental in nature [EBO 84], meaning they involve optimizing an existing technology, process, or service. This allows the company to further differentiate itself from its competitors, which may justify a price increase and, consequently, an improvement in its profitability.

Incremental innovation is part of a continuous process, the duration of which varies depending on the area of activity.

These gradual developments facilitate user adaptation because they respect their learning pace. They constitute a series of adjustments that users must become accustomed to over time. This gradual path to innovation is essential to the sustainability of businesses.

Disruptive innovation results from the accumulation of multiple incremental innovations. It suddenly interrupts the continuous process of incremental improvements. Its adoption by influential users forces the entire sector concerned to follow suit [CRM 13], or risk losing their competitive position.

This type of innovation disrupts the initial implementation schedules planned for incremental innovations, forcing rapid adoption. This acceleration has a direct impact on society, through the consumers of derived products or services. It creates a need for rapid adaptation, excluding those who cannot keep up. This causes economic risks linked to precipitous transformation, as well as social tensions between individuals capable of adapting and those who are left behind. Although it arises from a chain of incremental innovations, disruptive innovation abruptly breaks this cycle, like a shock or a crisis. It produces an effect that anticipates several classic development cycles [WWY 15]. As a result, it offers such a strong strategic advantage that its initiators can freely set their prices.

Incremental innovations require regular changes, whereas disruptive innovations require radical and often rapid changes [CC 11]. Humans assimilate gradual learning more easily because it involves little change in habits.

Conversely, disruptive innovation forces individuals to integrate new knowledge and change their behaviors in a very short period of time, something that would normally have taken much longer. Every technological advance carries potential risks for humans. The substitution of tasks with innovative technologies can lead to the elimination of certain jobs [CRM 13]. Those who fail to keep up with the pace of change may find themselves falling behind those who adapt more easily, thus leading to a social divide. Educational attainment influences the ability to learn quickly, which can accentuate inequalities between social classes and generate societal tensions or imbalances. However, as the Villani report [VIL 18] points out, automation must not exacerbate social and economic disparities. On the contrary, artificial intelligence should serve to mitigate them, provided that thoughtful decisions are made regarding the types of AI to be designed and used.

The introduction of an innovation requires more or less rapid learning and involves a variable degree of new skills to be acquired [MLL 18]. In this adaptation process, disruptive innovation presents an increased and more immediate risk of social division, affecting some individuals more than others. This form of innovation requires policymakers to put in place training and support measures to accompany those who risk being excluded from the benefits generated. A major danger lies in the widening of the income gap between the beneficiaries of the innovation and the others. This situation can cause significant social instability that may lead to popular uprisings.

The growing integration of technological innovations into everyday life increases the risks of social instability [BIR 11]. Indeed, the use of technologies from giants like GAFAM imposes a quasi-obligation of adoption, and those who refuse to comply find themselves excluded. The dominance of GAFAM and BAT has facilitated the work of public administrations in the digitalization of services, to the point that individuals who have not adopted these tools find themselves deprived of access to public services, with no alternatives offered.

Innovation generates additional cost risks for companies during the transition phase from an old technology to a new one [LD 16]. This financial burden is even higher during disruptive innovations. This risk is amplified due to the requirement for rapid adoption, requiring significant investments to adapt infrastructures. This transition, sometimes accelerated by exceptional circumstances such as the health crisis linked to COVID-19, forces organizations to incur expenses to make these changes, thus impacting the economic and social cost of the process. During this phase, some companies may not survive, generating social tensions, particularly in the labor market. The various risks associated with innovation can be mitigated through effective governance within companies and the intervention of public authorities [AC 09].

Case Analysis: The Dangers of Artificial Intelligence

The risks associated with artificial intelligence can be grouped into traditional economic categories, such as market dynamics, competitiveness, or employment, while others are more related to concerns about social disruption.

Market and Political Economy Threats

The market, as is well known, tends to reinforce inequalities by favoring the growth of the most successful companies, leading to the formation of monopolies. The main concern is that tech giants (such as GAFAM in the United States or BAT in China) are establishing themselves as leaders, marginalizing traditional players such as banks and small fintechs [AB 18]. This concentration can be illustrated by examples such as Paypal 's acquisition of Swedish AI company iZettle for $2.2 billion, eliminating a potential competitor. Such strengthening of monopoly power translates into fewer options for consumers and a likely increase in prices. However, given the continued acceleration of technological advances, today's monopolies may no longer exist tomorrow.

These companies, born of technological advances, have seen some of their services transform into essential elements of the economy. For example, email and certain social networks have become indispensable for both individuals and public administrations. The financial value of GAFAM or BAT companies often exceeds the gross domestic product of many countries around the world. This gives them considerable implicit economic power, allowing them to negotiate directly with the governments of major nations regarding their impact on society. The intensive use of these digital platforms by populations also strengthens the influence of these companies on public opinion.

The constant increase in social media platforms' need for digital data storage has become a strategic lever in geopolitical negotiations, raising concerns about the abusive capture of users' personal information in each nation. This phenomenon therefore carries with it the risk of concentration of market power by these companies, as well as possible economic and even political influence.

Beyond these classic economic concerns, sociological worries are also fueled by science fiction writers [FES 19]. One of these concerns the danger posed by authoritarian regimes in an Orwellian state, capable of monitoring not only the behaviors, but also the thoughts and emotions of its inhabitants. Indeed, China has already demonstrated that facial recognition technology can spot a wanted criminal in a crowd of 20,000 people [ZEN 20]. Another possible concern is that companies could exploit all the data to force you to consume according to their choices. A third apprehension is that humans will become subservient to robots or find themselves inferior to them. Today, it is considered that decision-making can be delegated, shared, or integrated into a hybrid system between humans and machines [SBV 19]. Furthermore, the use of surveillance technologies by governments can generate a fear of loss of freedom, diminishing trust in political authorities. This situation could once again lead to risks of social instability, as observed in several countries (Russia, France, etc.).

Management risks: who is responsible?

A more technical concern among market participants concerns the question of ultimate liability in the event of an error. For example, if an artificial intelligence system grants credit inappropriately, causing the bank to fail, who should be held accountable: the human or the machine? Does the manager consider it unfair to be held liable [FRI 19]? Similarly, in the case of an autonomous vehicle involved in a fatal accident, who is at fault: the passenger or the manufacturer?

Recently, several hundred employees overseeing post offices in the UK were wrongly accused of falsifying accounts and embezzling funds due to faulty software. These employees took legal action against their employer, who acknowledged that the computer program contained errors. However, the court did not accept this justification, and management was found liable for these unfounded accusations [OCO 22].

With the development of artificial intelligence, an increasing number of complex activities could be automated. This includes financial management, reviewing assessments, and all operations related to massive data processing. Only final decision-making would remain under human responsibility. This creates a major risk that humans will become dependent on the automation of these functions [RIC 19]. The danger of erroneous strategic decisions based on inaccurate data can be considerable.

The rise in dependence on data and digital technologies is such that human reasoning and discernment now rely on the information provided by these tools [TCY 19]. Thus, individuals put aside their critical thinking and acquired knowledge to rely entirely on technological devices. On the one hand, this creates a significant risk in terms of management, and on the other, the threat that artificial intelligence will become even more efficient. The ability of AI to converge with collected data could allow machines to achieve a level of decision-making comparable to that of humans.

In organizations, artificial intelligence technologies such as genetic algorithms, neural networks, and fuzzy logic are already used for day-to-day management, but their use is expected to extend further to strategy definition [GAV 18]. This raises new concerns: poor strategy development can lead to the failure of the entire structure, while failure to adopt these advanced methods risks placing the company in a weak position against the competition.

National legislation defines and assigns the responsibility of business leaders for validated management decisions and the results obtained, whether financial, economic, environmental, etc. With the growing rise of digital technology linked to the explosion of data management, and consequently the use of AI to process this information, managerial decision-making is becoming more complex [IJS 13]. If the manager relies on innovation to control the volume of data, his assessment of the information to be extracted and the choices to be made are now more exposed to risks.

Operational threats: security and malfeasance

Current literature shows that artificial intelligence can be used to identify and prevent fraud related to bank cards and other financial transactions [SOV 18; BNW 20].

Operational risks arise from biased or unrepresentative data, the choice of algorithmic models, and human decisions influenced by AI interpretations [AH 21]. These vulnerabilities can affect both private companies and public finances [PCE 21]. Furthermore, the increased automation of digital processes makes IT systems more exposed to cyberattacks. It also increases the risk of fraud that is more difficult to detect than that resulting from traditional procedures. For example, NFTs and cryptocurrencies suffer from a lack of regulation, which leads to low trust and an increased risk of embezzlement [MEN 19]. This lack of trust is also evident among patients, who often prefer a diagnosis made by a human professional rather than by an automated system [LDA 22].

On a more technical level, major security issues are emerging, including the significant risks of hacking related to Big Data, which is concentrated in the hands of a few key players. With the proliferation of transactions on interconnected networks, the threat of cyberattacks is intensifying [VAR 19]. A related risk is the bankruptcy of a major player, which could render many dependent applications unusable.

Data security has become a critical concern, whether it concerns stored customer information or the IT infrastructure of businesses and governments. Personal data breaches regularly make headlines. Furthermore, cyberattacks against government systems have become a veritable "weapon of war" for some countries, as evidenced by the conflict between Russia and Ukraine in 2022. These attacks also frequently target businesses, sometimes with ransom demands to lift the blockage caused by the intrusion.

Another issue concerns " deepfakes ," or synthetic content, which is almost undetectable to the naked eye. Beyond reputational risks and cyber threats, they open up a new avenue for fraud. This issue is particularly critical in the insurance sector. " Deepfakes " can be used to formulate false claims, produce fake appraisal reports, or even simulate the existence and condition of fictitious assets [VEK 21]. Furthermore, consumers express concerns about the protection of their privacy, fearing that their personal data will be accessed or disclosed without consent. This could explain the reluctance to use online chats in banking services [AI 21]. Moreover, customers sometimes perceive these exchanges as generating information asymmetry, since the bank can record the conversation while the customer does not receive a copy.

Table 2.1. Operational risks - Security and fraud

Type of Risk	Risk Level
Non-representative data	AVERAGE
Biases inherent in representative data	Weak
Choice of algorithms	AVERAGE
Human decisions	AVERAGE
Cyberattacks	Pupil
NFT/Cryptocurrency Fraud	AVERAGE
Large amount of data stored with few actors	Pupil

Source: Author

Low Risk => No more risk than in the "old world ";

Medium Risk => Need to address latent implicit risks. Otherwise high risk .

High Risk => Mandatory risk management by stakeholders. Failure to do so may result in negative consequences for businesses and society.

Dangers associated with the collection and processing of data and individual freedoms

The assessment of individual rights remains complex. The Ontario Human Rights Committee [PRO 09] illustrates several challenges in this area. For example, in a high-crime area, how can information be collected while respecting individual privacy rights to determine whether community policing is necessary? Another example is how can data on sexual harassment be gathered when human rights rules and policies are unclear? In these situations, the entity collecting the data should not have a direct interest that could lead to discrimination. A third example concerns the treatment of LGBT people by hotel reception staff. In the event of a complaint, can the establishment require the use of video surveillance for all guests? Can it also collect information on guests' sexual orientation? Would it be necessary to ask each guest about their sexual preferences? The data collected must correspond to the purpose of the collection, which in this case could be to improve the treatment of LGBT people. Regarding transgender people, what happens if the individual identifies as a woman while someone else identifies them as a man?

An example of data analysis might involve identifying the intersections of different characteristics and comparing them with a relevant reference group. For example, if a person is male, young, of Asian descent, and illiterate, should the control group used for comparison be similar in all respects except illiteracy? Even publicly available data can present categorization problems. For example, Statistics Canada uses 12 racial classifications. What happens to a person from two different racial categories? Qualitative data has its own limitations, particularly due to the subjectivity and interpretations of the respondent and the researcher. Similarly, quantitative data may not be appropriate in certain contexts, such as for small samples or non-normal distributions. Therefore, any processing using artificial intelligence tools can also be misleading.

Threat in the employment sector

A labor market vision focuses on the future evolution of work. It analyzes the anticipated proportion of the workforce, as well as the beneficiaries and disadvantaged within it. The substitution of certain functions, or even entire job categories, with technology leads to a possible increase in unemployment. This can also create downward pressure on wages, thus generating a risk of social and political instability.

A recent book found that the most modest jobs would be replaced by automation [BRY 14]. Other research showed that high-skilled positions (in management, professional, and technical occupations) as well as low-skilled service jobs have benefited, while the middle class has suffered losses [DAV 15]. Specialists are therefore the big beneficiaries. For example, Abu Dhabi's sovereign wealth fund, one of the world's largest, is actively recruiting experts, influencers, machine learning specialists, strategists, portfolio managers, risk analysts, as well as professionals from several other specialized fields [ENG 22]. David [DAV 15] pointed out that, even if automation replaces some employees, it also increases their marginal productivity, which tends to boost their income. For example, with the advent of ATMs, teller employees have shifted to more personalized banking services. However, these benefits were expected to be limited as AI progresses toward more creative forms of learning. Recent data from a major consulting firm reinforces these concerns. According to a McKinsey report [MAN 17], nearly half of the tasks performed by employees could be automated, implying that 15% of the global workforce is at risk of losing their jobs, while new positions will require different skills. This automation will put downward pressure on wages in developed countries. Beyond the robotization of repetitive tasks, it is now anticipated that the cognitive functions of managers will also be delegated to machines, leaving humans only those requiring emotional intelligence [HRM 19]. Many banks are reducing their staff in industrialized countries, but it remains unclear whether fintech startups have compensated for this job loss. Physically demanding and often low-skilled occupations are the most likely to be replaced by technology, increasing the risk of a social divide between low- and high-skilled workers. However, rather than talking about job losses, some emphasize the transformation of jobs linked to AI [VIL 18]. Indeed, a job is made up of several tasks: some can be automated, while others are less so. In other words, specific tasks within a job are at risk of being automated. The people most affected are often low-skilled workers, manual workers, as well as some white-collar employees. This also represents an opportunity to develop more human skills, such as creativity, manual dexterity, abstract thinking, and problem-solving skills.

However, all these measures are causing concern and a form of "technophobia" among employees. They fear that the integration of AI into their company will quickly make them redundant [SIN 20]. As a result, they are beginning to consider different career paths [PRE 19]. The risk associated with job automation is also negatively correlated with labor productivity, and more open economies are more exposed to this threat [FNV 21].

Risks linked to other social divisions

Artificial intelligence can both mitigate and increase certain risks, and the majority of banks and FinTechs agree that the impact on organizational risk will be limited, while an increase in societal risks is to be expected [ZAB 21]. Tech giants such as Google, Amazon, Facebook, and ByteDance are often criticized for their lack of ethical consideration in the design of their AI systems, including their use for surveillance purposes and the spread of algorithmic bias, where computer systems consciously or unconsciously reproduce biases derived from biased or corrupted data [MUR 21]. For example, AI can reinforce existing gender stereotypes [ADA 19]. One study showed that Samsung's male and female voice assistant Bixby react differently depending on the gender in the responses provided. Another demonstrated that an algorithm developed by Amazon to analyze job applications tended to penalize those containing the term "woman." Indeed, the algorithm, trained on historical data reflecting predominantly male recruitment, reproduced this bias in the selection of future candidates.

Scams targeting older adults have increased, often committed by their caregivers or family members. To counter this phenomenon, banking institutions are now using artificial intelligence to identify these frauds [CRO 19]. However, integrating new technologies can be more complicated for seniors, increasing their vulnerability to social isolation.

Threat linked to global rivalry: geopolitical issues

The growing dependence of national economies on technology is generating new geopolitical rivalries over control of these innovations. After a period marked by the relocation of production chains, recent years have seen the emergence of government restrictions on the implementation of technologies, perceived as sources of economic advantage and levers of political power. Are we witnessing a return to the era of comparative specialization of states [POR 11]?

Economic rivalry and geopolitical tensions are forcing states to foster technological innovation at home and reduce their external dependence. Several examples from European countries during the COVID-19 pandemic in 2020-2021 concern medicines and electronic components. These sectors have become strategic issues for Western countries vis-à-vis Asia. For example, the United States has encouraged Taiwanese semiconductor companies, such as TSMC, to establish their new factories in the United States. Furthermore, INTEL is considering building a new factory in Europe rather than Asia. In the competition for the development of artificial intelligence, it seems that the country with the largest volume of data will surpass those with the most financial resources. China, with its vast connected population, would thus benefit from an advantage [ZEN 20]. Furthermore, if its population is unaware of its civil rights or willing to sacrifice them to achieve a position of global leadership, China could then design surveillance systems that Western countries would be reluctant to deploy [ZEN 20]. Nevertheless, during the COVID crisis, several other nations have managed to establish tracking systems previously unacceptable to their societies.

Table 2.2. Implicit risk level by type of innovation

Type of innovation		**Type of Risk**				
	Of market and political economy	**Managerial**	**Operational: Security and Fraud**	**Within the market of work**	**Social divisions**	**International competition: geopolitics**
Incremental	Weak	AVERAGE	AVERAGE	Weak	Weak	Weak

Innovation						
Innovation Disruptive	Pupil	Pupil	Pupil	Pupil	Pupil	Pupil

Source: Author

Low Risk => No more risk than in the “old world”;

Medium Risk => Need to address latent implicit risks. Otherwise high risk .

High Risk => Mandatory risk management by stakeholders. Failure to do so may result in negative consequences for businesses and society.

Table 1 summarizes the levels of risk that incremental and disruptive innovation could present.

DISCUSSION

Tolerance for ambiguity is a characteristic of national cultures as described by [HOF 80; HH 01]. Thus, the uncertainty inherent in any transformation is more tolerated in societies where this sensitivity is less marked (such as in Anglo-Saxon countries or in Southeast Asia), unlike in other regions (such as France, Germany, Italy or Spain). The adoption of new developments resulting from innovation is more easily carried out in cultures where intolerance to uncertainty is low. Conversely, in countries where this aversion is stronger, populations tend to show more reluctance towards technological advances, and their integration is more gradual.

It is noted that the majority of companies that have introduced disruptive innovations into society come from Anglo-Saxon or Asian countries. In contrast, companies from other regions focus more on incremental improvements. These disparities can be explained by the economic structures specific to each country [WR 09]. For example, the adoption of financial technologies (Fintech) is much more advanced in Anglo-Saxon and Asian nations than in most European countries. The automation of physical tasks in logistics centers or large retail stores is already normalized in some countries. Conversely, in Europe, this mechanization raises concerns about job losses. This illustrates the differences in the reception of innovation according to national contexts. Innovation is continuous, and its pace is accelerating. Its integration will be more or less easy depending on the country, and the acquisition of new skills will be essential for future generations to be able to adapt to it.

Knowledge acquisition can take several forms: early introduction to technology at school; learning by doing, which allows students to progress more quickly through concrete experiments conducted in the classroom or at high school; and the development of creative thinking, encouraging students to think outside of traditional frameworks to explore original solutions to a problem. This way of thinking is the foundation of "design thinking " and represents the first step in the innovative process. In short, it is becoming essential for societies to transform educational approaches aimed at new generations.

At the same time, public authorities must anticipate future developments and implement training programs in advance to support the retraining of current workers [CU 18]. For example, by training operators specialized in robotic technologies. Some companies are taking the initiative to do this themselves, due to a lack of available qualified personnel. Indeed, carrying out mass layoffs would represent a significant cost and risk aggravating social tensions linked to unemployment.

For example, Renault has decided to convert its Flins site into a factory dedicated to the circular economy in the automotive sector, while ensuring the professional retraining of all its employees. Upskilling workers to adapt to innovations, whether progressive or radical, is becoming a strategic issue for all countries. Furthermore, it is essential to consider how to structure and regulate interactions between humans and technologies. Should regulations be imposed on technology companies when their advances cause job losses? How far should automation be allowed? What legal responsibility should users be assigned in a world where the alternative to technology could disappear? These questions are numerous, as the pace of innovation is accelerating sharply, particularly thanks to the rise in computing capacity and the energy availability that powers them. We are on the cusp of a major technological transformation that requires rigorous management of social implications.

CONCLUSION

What actions should be considered? Many entities may find themselves unable to decide whether data collection is ethical or not, which can lead to the risk of prosecution or legal sanctions. In this context, they may choose to rely on the expertise of specialized organizations: “Sensitive to the issues related to data ethics and their use by artificial intelligence, the Delta organization has established a collaboration with the International Observatory on the Social Impacts of AI (OBVIA), with the aim of building a reference framework intended to provide more precise guidance for its future projects.” [JS 22].

To some extent, artificial intelligence will create new forms of employment, particularly because human intervention is required for data annotation. Platforms such as Mechanical Turk or Hive have developed as digital spaces offering a variety of fragmented tasks, sometimes related to sectors such as catering, but not exclusively. However, once algorithms master labeling autonomously, human intervention could be limited to a supervisory role to detect possible errors. One possible response to this development could be the introduction of reduced working hours (such as a four-day week), combined with the implementation of a guaranteed universal income [ASH 19; AD 21].

The ethical issues surrounding artificial intelligence are reminiscent of those in financial services before the 2008 crisis. In both cases, the complexity of the mechanisms, the lack of transparency of certain algorithms, and insufficient regulations can cause unforeseen and negative impacts. To ensure responsible AI, the process should include design, coding, evaluation, and, above all, auditing [BLA 22]. Philanthropic funding is being mobilized to support research into ethics and explore the positive uses of AI [MUR 21]. However, as the case of Google illustrates, these resources are sometimes allocated only to traditional research profiles. For example, Google fired a Black researcher after she highlighted biases in their AI systems [SHW 21]. Faced with the rapid advances in AI, education and training systems must rethink their approaches to better prepare individuals for new professions. The major problem is the current inability of these structures to adapt their programs to the pace of technological change, creating a growing gap between the skills needed and those available. Thus, beyond the impacts, it is becoming crucial to integrate educational and training dimensions into the development of AI [VIL 18].

According to Gilda Darlas , the major challenge lies in the fact that artificial intelligence tends to amplify the negative aspects of human nature, and that the solution involves a transformation of education from childhood onwards, in order to strengthen shared experiences and empathy between individuals [AD 21]. While playing a protective role for the most vulnerable, educational institutions must also train the most enterprising students to quickly identify and seize opportunities in a constantly changing environment. This involves teaching skills such as resilience, adaptability, and preparation for the professional world. These skills will complement the often-highlighted skills such as creativity, teamwork, analytical thinking, and communication. Of course, these human qualities must be accompanied by a solid foundation in classic financial tools, such as economic data analysis or company valuation, in order to help future professionals understand the recommendations of automated systems and detect their potential errors.

REFERENCES

1. [AB 18] ASHTA A., BIOT-PAQUEROT, G., “FinTech evolution : Strategic value management issues in a fast changing industry”. Strategic Change 27.4 (2018), p. 301-311.
2. [AC 09] ALAKTIF J., CALLENS, S., “La gouvernance, ou la qualité des pouvoirs”. Marche et organisations 2 (2009), p. 15-30.
3. [AD 21] ASHTA A., DARLAS G., “The role of intersubjectivity and shared experience in regulating the dark side of human nature in entrepreneurial finance”. Entreprendre Innover 1 (2021), p. 58-65.
4. [ADA 19] ADAMS, R. “Artificial intelligence has a gender-bias problem-just ask siri”. (2019).

5. [AH 21] ASHTA A., HERRMANN H., “Artificial intelligence and fintech : An overview of opportunities and risks for banking, investments, and microfinance”. Strategic Change 30.3 (2021), p. 211-222.
6. [AI 21] ALT M.-A., IBOLYA, V., “Identifying Relevant Segments of Potential Banking Chatbot Users Based on Technology Adoption Behavior”. Market-Tržište 33.2 (2021), p. 165-183.
7. [ARS 21] ARSIC V.B., “Challenges of Financial Risk Management: AI Applications”. Management: Journal of Sustainable Business and Management Solutions in Emerging Economies 26.3 (2021), p. 27-34.
8. [ASH 19] ASHTA A.. “Work Sharing: A Socioeconomic Perspective”. Journal of Cost Management 33 (nov. 2019), p. 17-21.
9. [BHH 21] BUCKMANN M., HALDANE A., HÜSER A.C., “Comparing minds and machines : implications for financial stability”. Oxford Review of Economic Policy 37.3 (2021), p. 479-508.
10. [BIR 11] BIRTCHNELL T., “Jugaad as systemic risk and disruptive innovation in India”.
11. Contemporary South Asia 19.4 (2011), p. 357-372.
12. [BLA 22] BLACK J., With financial tech and AI ethics expertise — what do I do next? | Financial Times. https://www.ft.com/content/d8c4b5f1-7cef-485d-affd-1ae6b683d86d. (Accessed on 11/09/2022). Fév. 2022.
13. [BNW 20] BERRUTI F., NEL P., WHITEMAN R., An executive primer on artificial general intelligence. McKinsey&Company. 2020.
14. [CC 11] CLAYTON M., CHRISTENSEN C.M., CURTIS L., JOHNSON W., Carmody. disrupting class:
15. how disruptive innovation will change the way the world learns. 2011.
16. [CHR 13] CHRISTENSEN C.M., The innovator’s dilemma: when new technologies cause great firms to fail. Harvard Business Review Press, 2013.
17. [CRM 13] CHRISTENSEN C.M., RAYNOR E., MCDONALD R., Disruptive innovation.
18. Harvard Business Review Brighton, MA, USA, 2013.
19. [CRO 19] CROSMAN P., Can AI help banks thwart elder abuse? | Technology At American Banker. https://www.americanbanker.com/news/can-ai-help-banks-thwart-elder-abuse. (Accessed on 11/09/2022). 2019.
20. [CSK 21] COUCHORO M., SODOKIN K., KORIKO M., “Information and communication technologies, artificial intelligence, and the fight against money laundering in Africa”. Strategic Change 30.3 (2021), p. 281-291.
21. [CU 18] CASADELLA V., UZUNIDIS D., “Innovation Capacities as a Prerequisite for Forming a National Innovation System”. In: Collective Innovation Processes: Principles and Practices 4 (2018), p. 177-199.
22. [CUL 21] CULLEY A., “Identifying and mitigating ‘conduct risk’in algorithmic FICC trading”. Journal of Financial Compliance 4.3 (2021), p. 267-281.
23. [DAV 15] DAVID H., “Why are there still so many jobs ? The history and future of workplace automation”. Journal of economic perspectives 29.3 (2015), p. 3-30.
24. [EBO 84] ETTLIE J., BRIDGES W.P., O’KEEFE R.D., “Organization strategy and structural differences for radical versus incremental innovation”. Management science 30.6 (1984), p. 682-695.
25. [ENG 22] ENGLAND A., Abu Dhabi wealth fund bets on scientific approach using quant experts
26. | Financial Times. https://www.ft.com/content/2c3065b6-7caf-4394-afe5-956ec5d4fe2c. (Accessed on 11/09/2022). 2022.
27. [FES 19] FESNAK M., “Sims, Christopher A. : Tech Anxiety : Artificial Intelligence and Ontological Awakening in Four Science Fiction Novels.” Journal of the Fantastic in the Arts 29.3 (2019), p. 458-462.
28. [FNV 21] FOSTER-MCGREGOR N., NOMALER O., VERSPAGEN B., “Job automation risk, economic structure and trade: a european perspective”. Research Policy 50.7 (2021), p. 104269.
29. [FRI 19] FRIND A., MIL-OSI Banking. https://foreignaffairs.co.nz/2019/10/28/mil-osi-banking-who-monitors-thebots/. (Accessed on 11/09/2022). 2019.
30. [GAV 18] GAVRILOVA T., et al., “Modeling methods for strategy formulation in a turbulent environment”. Strategic Change 27.4 (2018), p. 369-377.
31. [GGB 20] GARCIA-BEDOYA O., GRANADOS O., BURGOS J.C., “AI against money laundering networks : the Colombian case”. Journal of Money Laundering Control 24.1 (2020), p. 49-62.

32. [HG 21] HEDLEY T.P., GIRGENTI R.H., “The forensic professional’s perspective on fraud and fraud detection”. Journal of Financial Compliance 5.1 (2021), p. 85-93.
33. [HH 01] HOFSTEDE G.H., HOFSTEDE G., Culture’s consequences: Comparing values, behaviors, institutions and organizations across nations. Sage, 2001.
34. [HIL 22] HILLE K. Forces driving semiconductor boom are far from over | Financial Times. https://www.ft.com/content/93366bc6-f2e9-492a-a33f-72652820a571. 2022.
35. [HOF 80] HOFSTEDE G., “Culture and Organizations”. International Studies of Management & Organization 10.4 (1980), p. 15-41. DOI : 10.1080/00208825.1980.11656300.
36. eprint : https://doi.org/10.1080/00208825.1980.11656300. URL : https://doi.org/10.1080/00208825.1980.11656300.
37. [HRM 19] HUANG M.H., RUST R., MAKSIMOVIC V., “The feeling economy: Managing in the next generation of artificial intelligence (AI)”. California Management Review 61.4 (2019), p. 43-65. [IJS 13] ISIK O., JONES M.C., SIDOROVA A., “Business intelligence success: The roles of BI capabilities and decision environments”. Information & management 50.1 (2013), p. 13-23.
38. [JON 21] JONES A., Digital credit scoring for affordable housing finance: Syntellect and Reall in urban India.
39. https://practicalactionpublishing.com
(Accessed on 11/09/2022). 2021.
40. [JS 22] JACOB A., SOUISSI S., “L’INTELLIGENCE ARTIFICIELLE DANS L’ADMINISTRATION PUBLIQUE AU QUÉBEC”. Cahiers de recherche sur l’administration publique à l’ère numérique, n° 5, Québec, 2022.
41. [KAS 21] Karina KASZTELNIK. “INNOVATIVE BANK MARKET RISK MEASUREMENT STRATEGIES USING A MODERN MACHINE LEARNING APPROACH: A NOVEL AGLOMERATIVE CLUSTERING MODEL
42. ANALYSIS”. Journal of Business and Accounting (2021), p. 16.
43. [KY 21] KAYIM F., YILMAZ A., “Financial Instrument Forecast with Artificial Intelligence”. EMAJ: Emerging Markets Journal 11.2 (2021), p. 16-24.
44. [LD 16] LEIPZIGER D., DODEV V., et al., “Disruptive technologies and their implications for economic policy: Some preliminary observations”. Institute for International Economic Policy Working Paper Series 13 (2016).
45. [LDA 22] LARKIN C., DRUMMOND OTTEN C., ÁRVAI J., “Paging Dr. JARVIS ! Will people accept advice from artificial intelligence for consequential risk management decisions ?” Journal of Risk Research 25.4 (2022), p. 407422.
46. [MA 21] MILANA C., ASHTA A., “Artificial intelligence techniques in finance and financial markets : a survey of the literature”. Strategic Change 30.3 (2021), p. 189-209.
47. [MAN 17] MANYIKA J., et al., “Jobs lost, jobs gained: Workforce transitions in a time of automation”. McKinsey Global Institute 150 (2017).
48. [MEN 19] MENDOZA-TELLO J.C., et al., “Disruptive innovation of cryptocurrencies in consumer acceptance and trust”. Information Systems and e-Business Management 17.2 (2019), p. 195-222.
49. [MLL 18] MILLAR C., LOCKETT M., LADD T., “Disruption: Technology, innovation and society”. Technological Forecasting and Social Change 129 (2018), p. 254-260.
50. [MUR 21] MURGIA M., Eric Schmidt creates $125mn fund for ‘hard problems’ in AI research
51. | Financial Times. https://www.ft.com/content/68a4ba34-9785-411c-b7f6-3a9ae2f37cd6. (Accessed on 11/09/2022). 2021.
52. [OCO 22] O’CONNOR S., Never mind Big Tech — ‘little tech’ can be dangerous at work too | Financial Times. https:// www. ft. com/ content/ 147bce5d- 511c- 4862 - b820-2d85b736a5f6. (Accessed on 11/09/2022). 2022.
53. [PCE 21] PÁLMAI G., CSERNYÁK S., ERDÉLYI Z., “Authentic and reliable data in the service of national public data asset”. PÉNZÜGYI SZEMLE/PUBLIC FINANCE QUARTERLY 66.Specia (2021), p. 52-67.
54. [POR 11] PORTER M.E., Competitive advantage of nations: creating and sustaining superior performance. Simon et Schuster, 2011.
55. [PRO 09] Processus de collecte de données : six étapes vers la réussite | Wageningen Portals.

56. http://www.gestionorienteeverslimpact.org/resource/processus-de-collecte-de-donn\%C3\%A9es-six-\%C3\%A9tapesvers-la-r\%C3\
57. %A9ussite. (Accessed on 11/09/2022). 2009.
58. [QLG 21] QIU S., LUO Y., GUO H., “Multisource evidence theory-based fraud risk assessment of China’s listed companies”. Journal of Forecasting 40.8 (2021), p. 1524- 1539.
59. [RGP 18] RGPD. “Regulation (EU) 2016/679 of the European Parliament and of the Council”. Regulation (eu) 679 (2018), p. 2016.
60. [RIC 19] RICHARDS G., et al., “Business intelligence effectiveness and corporate performance management : an empirical analysis”. Journal of Computer Information Systems 59.2 (2019), p. 188-196.
61. [SAM 21] SAMMÉ A., “Work smarter, not harder : Artificial intelligence’s critical role in mitigating financial crime risk”. Journal of Financial Compliance 4.4 (2021), p. 344-352.
62. [SBV 19] SHRESTHA Y.R., BEN-MENAHEM S., VON KROGH G., “Organizational decision-making structures in the age of artificial intelligence”. California Management Review 61.4 (2019), p. 66-83.
63. [SHW 21] SHWAB K., AI has a Big Tech problem | Fast Company. https://www.fastcompanyco.za/technology/ai-has-abig-tech-problem-cf3c2a05-54a6-4fd8-850c-6a0690691a24. (Accessed on 11/09/2022). 2021.
64. [SIN 20] SINHA N., et al., “Robotics at workplace: An integrated Twitter analytics–SEM based approach for behavioral intention to accept”. International Journal of Information Management 55 (2020), p. 102210.
65. [SOV 18] SOVIANY C., “The benefits of using artificial intelligence in payment fraud detection: A case study”. Journal of Payments Strategy & Systems 12.2 (2018), p. 102-110.
66. [TCY 19] TAMBE P., CAPPELLI P., YAKUBOVICH V., “Artificial intelligence in human resources management: Challenges and a path forward”. California Management Review 61.4 (2019), p. 15-42.
67. [TUR 09] TURING A.M., “Computing machinery and intelligence”. Parsing the turing test. Springer, 2009, p. 23-65.
68. [UZU 20] UZUNIDIS D., “Introduction générale. De la systémique de l’innovation aux systèmes complexes”. Marché et organisations, 3 (2020), p. 9-15.
69. [VAR 19] VARTANIAN T.P., Regulators’ push for innovation shouldn’t come at expense of prudence | American Banker. https://www.americanbanker.com/opinion/regulators-push-for-innovation-shouldnt-come-at-expense-ofprudence. (Accessed on 11/09/2022). 2019.
70. [VEK 21] VEKIARIDES N., Deepfakes: An insurance industry threat | PropertyCasualty360. https://www.propertycasualty360.com/2021/09/14/deepfakes-an-insurance-industrythreat/?slreturn=20221009141252. (Accessed on 11/09/2022).
71. 2021.
72. [VIL 18] VILLANI C., et al., Donner un sens à l’intelligence artificielle : pour une stratégie nationale et européenne. Conseil national du numérique, 2018.
73. [WR 09] WITT M.A., REDDING G., “Culture, meaning, and institutions: Executive rationale in Germany and Japan”. Journal of International Business Studies 40.5 (2009), p. 859-885.
74. [WWY 15] WAN F., WILLIAMSON P.J., YIN E., “Antecedents and implications of disruptive innovation: Evidence from China”. Technovation 39 (2015), p. 94-104.
75. [XU 22] XU L., et al., “Analysis on risk awareness model and economic growth of finance industry”. Annals of Operations Research (2022), p. 1-23.
76. [YW 21] YANG S., WU H., “The Global Organizational Behavior Analysis for Financial Risk Management Utilizing Artificial Intelligence”. Journal of Global Information Management (JGIM) 30.7 (2021), p. 1-24.
77. [ZAB21] ZHANG B.Z., ASHTA A., BARTON M.E., “Do FinTech and financial incumbents have different experiences and perspectives on the adoption of artificial intelligence ?” Strategic Change 30.3 (2021), p. 223-234.
78. [ZEN 20] ZENG J., “Artificial intelligence and China’s authoritarian governance”. International Affairs 96.6 (2020), p. 1441-1459.
79. [ZRM 21] ZHANG Y., RAMANATHAN L., MAHESWARI M., “A hybrid approach for risk analysis in e-business integrating big data analytics and artificial intelligence”. Annals of Operations Research (2021), p. 1-19.