ARTIFICIAL INTELLIGENCE, RISKS AND INSURANCE

Some thoughts for executives and directors

April 2025

DiotSiaci

The media frenzy around artificial intelligence (AI) is in actuality quite recent. It took off with the launch of ChatGPT at the end of 2022 and the inception of generative AI. Before that, the term AI had surfaced amid a stream of advances in IT that have driven ever more processing power, speed of execution, and increased data available for processing thanks to the exponential development of the internet over the past 25 years.

But generative AI was immediately perceived as transformative on three counts:

- Because it is trained to understand natural language, it can be used by people with no knowledge of computer languages or programming and so the potential user base is much larger.
- By reproducing processing results in an equally natural form but also in code, text, image, video, paintings or even music, the prospects for potential applications are endless.
- After assisted intelligence and then augmented intelligence, generative AI offers greater autonomy because once deployed, it is constantly enriching itself based on its own results and any new data it has access to.

It is believed that generative AI will have a major impact on the operation of companies in all dimensions: commercial, administrative, production and research. Some business leaders are looking at a complete reorganisation of their operations around the functionalities enabled by AI[1]. Others[2] are giving orders to freeze all recruitment of staff for tasks that AI can perform.

Like any major development, AI offers companies as many opportunities for development and optimisation of resources as it does for creating new risks or exacerbating existing risks. Faced with such inescapable changes, the implications and scope of which have yet to be defined, boards of directors, whose role is to define the company's strategy and determine how it is organised, must support their management teams in this existential reflection.

Understandably, executives and directors are starting to ask questions about the personal risks they could incur by initiating or delaying the initiation of changes, about what preventive measures they can adopt for themselves and the company, and about the effectiveness of the insurance cover provided for these new risks.

Based on our experience as a risk manager for companies and financial institutions, we seek to provide some answers by distinguishing between:

- the risks incurred by executives and corporate officers (executive corporate officers); and
- the risks incurred by the company.

1. The Economist weekly edition. 22/4/2023 - The generation game

2. Bloomberg.com 01/05/2023 – IBM to pause hiring for back-office jobs that AI could kill

Risks incurred by executive corporate officers

The main sources of risk

In civil matters, any natural or legal person who believes they have suffered damage as a result of actions by a company executive can hold the latter legally liable and seek compensation. Shareholders, partners, creditors, customers, suppliers, employees and any other stakeholders in the life of a company can take action against its executive corporate officers. But it is important to be aware of the difference between the act of taking legal proceedings and their chance of success. Claimants, other than partners and creditors whom we will consider in a moment, must be able to establish that the executive committed a fault outside of their corporate functions, i.e. a serious and intentional fault, in order for a case personally directed against them to be admissible, failing which the case will somehow be redirected against the company itself, for which the executive is merely the representative.

Shareholders or partners, on the other hand, in the event of a loss of value of their investment, and creditors, in the event of an increase in their liabilities, have legal mechanisms at their disposal to take action against the executive personally if they believe the latter has committed a fault.

In addition to civil action that can be brought by shareholders against a solvent company and by or on behalf of creditors in the event of judicial liquidation, cases can also be taken up by an administrative authority such as, in France, the AMF, the CNIL or the competition authority. And, furthermore, it will soon be possible to make a case for failure to comply with EU regulations governing artificial intelligence, which can result in administrative sanctions or fines.

Grounds for action

Based on certain grievances raised in cases of personal liability against executives, we set out below some examples of the types of professional misconduct that could arise in relation to artificial intelligence and form the basis of a claim for compensation:

- Recourse against executives following action against a company for damage suffered by a third party (disclosure of confidential data, infringement of the intellectual property of others) or damage suffered by the company itself (dissemination of sensitive data belonging to the company, fraud to the detriment of the company facilitated by artificial intelligence technology, heavy administrative penalty imposed on the company for failure to comply with regulations governing AI). Executive corporate officers could be found liable for failing to put in place tools that are preventive (formalised governance, staff training, supervision of practices, human verification of AI production) or protective (amendment of the company's insurance policies to cover risks arising from AI).
- Disproportionate investments in AI technology compared to the company's resources and the results actually achieved.
- Excessive dependence on AI technologies where, following an incident originating within or outside the company, the latter has to deal with complete or partial interruption of its production or services.

- Inaccurate or misleading communication about the expected benefits of deploying AI solutions (increased revenue, improved profitability through cost optimisation, increased efficiency of products or services sold). This phenomenon of misrepresenting AI capabilities has been dubbed "AI washing" in reference to environmental "green washing". The Chairman of the Securities and Exchange Commission has announced a "merciless campaign" against companies and their executives who abuse investors through misleading communication[3]. In mid-March 2025, four lawsuits (following fifteen in 2024) had already been filed in US courts in the form of "securities class actions" for misleading information by a company or its management about the benefits the company could derive from the development or use of AI. These suits came in the wake of a fall in the company's share price, a risk that is all the greater since shares in these types of companies are often considered expensive, with investors attributing a premium to companies likely to benefit from the AI market.

Financial consequences

A claim against the personal liability of an executive can give rise to three types of financial cost:

- Defence costs: Civil, criminal and administrative proceedings can be complex and the defence process is costly, particularly if the executive has to hire "business" experts in addition to lawyers.
- Damages may be awarded by the court or negotiated under a settlement agreement. Making a claim for compensation against executives is sometimes an intimidating tactic to force a settlement agreement with the company or its insurers.
- Financial penalties imposed by an administrative authority or criminal court.

Prevention and protection

Prévention

The mere recognition of a loss (loss of value of securities, increase in liabilities) is not sufficient to obtain compensation. Judges consider economic risk in their assessment of a situation and the possibility that a decision may not produce the expected positive effects. The claimant must therefore establish that a fault has been committed and demonstrate a causal link between the fault and the loss. For their defence, the executives involved must demonstrate that they have behaved responsibly.

Given the aforementioned transformative potential of AI, and bearing in mind that it may be used clandestinely within a company, it is wise to:

- Manage all AI projects as part of a comprehensive, multi-disciplinary and documented approach, led by an ad-hoc team and including one or more directors who can report to the other members of the Board.

3. U.S.Sec - Speeches-Statements 13/2/2024 / Gensler and AI

- Roll out AI projects in small steps, with supervision by experienced employees, in line with the overall approach. Then make adjustments to the overall approach based on the results and observations drawn from decentralised initiatives.
- Supervise the use of AI (authorised applications, communicable data), and start by alerting the teams of the risks that unauthorised use may pose for the company (loss or dissemination of sensitive and valuable data, recourse by third parties).
- More generally, given the novelty of most aspects of AI, it is best to maintain a cautious and measured approach in the deployment of new applications.

Protection

When it comes to the liability of executives, the form precedes and often precludes the substance. If the executives can demonstrate (hence the importance of written communication) that they have made reasonable efforts to limit the occurrence of the risk, it is more difficult for an injured third party to demonstrate fault, even if a loss has been suffered.

Nevertheless, even when they have adhered to such practices, an executive may still find themselves served with a summons. In which case they must raise a defence. This is where directors and officers (D&O) liability insurance is useful. Precautions must be taken concerning the following in particular:

- The scope of exclusions. D&O liability policies have few exclusions, the main one being criminal sanctions, which are uninsurable. Attention should be paid to two other exclusions, which are not systematic but are sometimes introduced by insurers: (i) the exclusion of claims arising from a class action. This restriction distorts the purpose of the cover and must be ruled out; (ii) the exclusion of claims based on “cyber” losses, the scope of which could extend to claims based on loss related to AI.
- The consolidation of new subsidiaries. Cover only applies for faults committed after the acquisition. To avoid the risk of being held liable for previous misconduct, executives must exercise particular vigilance during pre-acquisition due diligence steps and when drafting the contractual documentation (sale agreement and liability guarantee).
- The guaranteed amount. This is the insurer’s maximum commitment. If there is more than one executive involved, this amount is shared, the practice being that each executive obtains their own advice. The amount of the cover should be regularly weighed against the likely cost of defence and the principal amount of any convictions.

Risks incurred by the company

Good control of the risks incurred by a company helps to keep its results stable and ensure continuity of activity, and, if it is effective and documented, constitutes the first safeguard against liability risks to which its executives are personally exposed. This requires careful mapping of risks. What risks does a company incur as a result of active or passive use of AI? Are these risks new or did they already exist, and have they been aggravated? How can you track them, measure their impact and prevent them? Are the insurance policies in place sufficient to cover the financial consequences? Many questions need to be asked.

The answers vary depending on whether the AI models and applications deployed in the company are developed in-house (rarely in full) or purchased and "customised", and depending on the origin of the data they use.

In light of the incipient rise in disputes and incidents, our focus here is to highlight certain risks that are exacerbated by the new wave of generative AI and to provide a few insurance recommendations.

Increased risk of fraud caused by highly realistic AI productions

Artificial intelligence tools are enabling the production of increasingly realistic fake content, causing an increase in the success rate of scams like "CEO fraud". Arup[4], an established British multinational engineering company, was the victim of one such case where one of its employees made a transfer of $25 million in response to instructions from a fake CFO given by video.

The use of deepfakes like this to divert financial assets are first to spring to mind, but companies must be careful to protect all the digital assets that comprise their business value (customers, prices, know-how, research, etc.). Warnings about the risk of misappropriation of tangible and intangible assets should therefore not be limited to employees in financial positions. All employees with access to company systems and data must be vigilant and trained.

In addition to protecting their own assets, they must monitor authenticity when it comes to the use of their identity, or that of their employees, vis-à-vis third parties. BNP Paribas[5] was ordered to compensate a customer who fell victim to a fake bank advisor scam following theft of the bank's telephone numbers. We can identify numerous fraudulent and malicious scenarios made possible by increasingly sophisticated AI and assess how such scams can target critical infrastructures.

4. Financial Times 16/5/2024 / ARUP and Hong Kong deepfake

5. Les Echos 24/10/2024 BNP Paribas and fake bank adviser.

Beware of sleeper agents

With the advent of generative AI, AI ceases to be a mere tool and instead becomes an agent, capable of learning and making decisions independently without human intervention. We must also monitor these systems very carefully to ensure they are fulfilling the function they were designed to carry out.

The European Union's Artificial Intelligence Act stipulates that high-risk applications deployed in specific areas such as critical infrastructures, education, employment and law enforcement must meet particularly strict standards around risk management, data quality, technical documentation and supervision by humans.

More pernicious applications are those which are used by individual companies as decision-making aids and which when used by a large number of players in the same sector can generate herd-like behaviour, the practical effects of which can reduce competition.

Around thirty civil actions were filed in the United States as part of an antitrust enforcement action by the Department of Justice[6], on the basis of an unlawful scheme involving the setting of rental prices. These disputes alleged that property administrators and software publishers coordinated a scheme to inflate rental prices. The software, formatted to achieve the sole objective of maximising rental payments, operated on the basis of the same algorithms and the same data, resulting in the same recommendations being provided.

Numerous other cases[7] involve "hallucinatory" behaviour where applications produce inexplicable results which without human control can result in harmful or even dangerous recommendations that could damage consumer confidence and a company's reputation. Companies, in particular those providing intellectual services, are therefore advised to have documents produced by AI proofread by an expert.

Data protection, the mother of all (legal) battles

Data is at the heart of the AI value chain. Most AI-related disputes concern the collection, processing and use of data. Numerous lawsuits are being filed against AI companies[8]. Almost all developers of AI models (foundation models) are being implicated on grounds that range for instance from the invasion of privacy to the disclosure of confidential information and failure to comply with intellectual property and copyright. In the Cambridge Analytica case (whose slogan was "Data drives all we do"), Facebook was fined $5 billion by the Federal Trade Commission, backed by a court decision (April 2020), and entered into a $725 million settlement agreement to close the class action brought on behalf of Facebook users for allowing third parties access to their private data[9].

6. Justice Department 23/8/2024 RealPage algorithmic pricing schemes

7. New York Times 16/11/2023 Chatbot and hallucination rates

8. ChatGPT eating the world 27/8/2024 Master list of lawsuits

9. Les Echos 23/12/2022 Cambridge Analytica – Facebook

Prevention

Many proceedings are currently pending, with the outcomes being uncertain due to their complexity and lack of precedence. In this evolving legal environment, it is incumbent on companies to control what they can control, in particular:

- The use that their teams make of AI tools by reminding them of the need to protect data that is company-specific and the data entrusted to them. A Business Insider article dated 11 July 2023[10] cited several large groups (including Amazon, Apple, Deutsche Bank, Samsung, Verizon and Wells Fargo) that had decided to prohibit the use of ChatGPT chatbots from their IT systems, pointing to the risk of leaks of confidential data.
- The compliance of the company's practices with the various regulations to which it is subject (AMF, CNIL, EU Act, etc.), as breaches can be heavily sanctioned.
- The dissemination of best practices within the company ("Acceptable Use Policies"), including validation by an experienced manager before transmission outside the company of any production resulting from an AI model.
- Management of their liability by not accepting contractual obligations that could be described as exorbitant and consequently jeopardise the benefit of the insurance policies taken out by the company

Insurance

Once the first safety net, i.e. rules of prudence to prevent risks occurring, is in place, the company's insurance programme offers a second line of defence. The goal is to provide protection from the financial consequences of the risks if they do occur or, for certain policies, if they threaten to occur ("mitigation costs").

Review of policies

The first exercise must be to re-read, or have someone re-read, each insurance policy taken out by the company with a view to examining its applicability in the event that the risks defined in the cover details section were to occur due to an AI application. Various scenarios must be imagined, such as, for example, a fire triggered by the malfunction of thermostats operated by artificial intelligence software, a decision by a company customer taken on the basis of a recommendation issued by an AI tool made available to them and which proves to be harmful, fraud perpetrated against the company.

The main policies to be examined are those taken out to cover:

- Risks of property damage – business interruption, machine breakage and all IT risks;
- Liability risks covered by general civil liability policies, employer liability, product liability, professional third-party liability, and directors and officers (D&O) liability policies;
- Cybersecurity risks.

10. Business Insider 11/07/2023 – Large groups issue restrictions on the use of AI software

This work will reveal:

- If the policies in place apply appropriately, in particular “against all risks with exclusions” policies.
- If grey areas exist that will have to be discussed with the company’s advisers to determine if insurers need to be contacted to have the cover specified, bearing in mind the maxim of French writer Cardinal de Retz that to be unambiguous can be to one’s own detriment (“On ne sort de l’ambiguïté qu’à son détriment”). In some cases, it may be better to make do with implied or “silent” cover.
- If there are gaps in the cover due to exclusions or excessively restrictive wording. Some exclusions are non-negotiable, others are intended to encourage the insured to take out specific cover. For example, exclusions introduced in relation to cyber risk are there to encourage companies to take out specific cover for these risks and enable insurers to carry out underwriting work tailored to these emerging risks.

Cyber liability insurance policies are the most suitable means of covering AI risks that are not included under standard cover. The definitions must be adjusted to take into account terms specific to the AI ecosystem and refer to the regulatory texts with which the company must comply.

Insurers can be expected to increase their information requirements for this extended AI cover (formalised AI governance procedures, list of AI applications, list of service providers used by the company, verification of product liability insurance taken out by service providers, etc.).

Conclusion

As with the term “sustainable agriculture” to describe reconciling profitability in agricultural production with limits on the impact on the environment, it would be prudent at this early stage of the development of AI and given our understanding of its consequences, to start talking about sustainable AI, i.e.:

- Governed as part of an overarching approach led by the company’s management and involving the board of directors.
- Deployed in small steps under the direct supervision of trained employees who in turn report to a multidisciplinary management team responsible for monitoring the positive and negative effects on all levels, in particular legal, social and environmental effects, and where negative effects are concerned responsible for proposing appropriate measures to eliminate or limit those effects.
- With due regard for the interests of all stakeholders, starting with the company’s employees.

Eric REMUS | April 2025

Eric Remus headed up the Financial Insurance department of the SIACI SAINT HONORE Group. He previously founded and managed Assurance & Capital Partners, a brokerage firm specialised in financial risk.

Disclaimer: *This document sets out some reasonable rules and practices for the management of risks incurred by companies and their executive corporate officers. It is of a general nature and is not intended to replace the analysis of the specific risks of a given company or legal advice.*

SIACI SAINT HONORE – DIOT-SIACI GROUP– Insurance and reinsurance brokerage company.

Registered office: Season – 39, rue Mstislav Rostropovitch – 75815 PARIS CEDEX 17 – FRANCE – Tel: +33 (0)1 4420 9999.

A French “Société par actions simplifiée” – Capital: €179.056.753,60– Registered with the Paris Trade and Companies Register under no. 572 059 939– APE 6622 Z – VAT no.: FR 54 572 059 939.

Registered with ORIAS under no. 07 000 771 (www.orias.fr) – Regulated by the French Prudential Supervision Authority (Autorité de Contrôle Prudentiel et de Résolution) – 4 place de Budapest – CS 92459 – 75436 PARIS CEDEX 09 – FRANCE.

Complaints: SIACI SAINT HONORE – Service réclamations – 23, allées de l’Europe – 92587 CLICHY CEDEX – FRANCE.

DIOT – DIOT-SIACI Group – Insurance and reinsurance broker.

Registered office: Season - 39, rue Mstislav Rostropovitch - 75815 PARIS CEDEX 17 - FRANCE – Tel: +33 (0)1 44 79 62 00.

A French Société par actions simplifiée (SAS) – Capital: €1,831,008 – Registered with the Paris Trade and Companies Register under number 582 013 736 – VAT No.: FR 92 582 013 736.

ORIAS No.: 07 009 129 (www.orias.fr) – Regulated by the ACPR - 4 place de Budapest - CS 92459 - 75436 PARIS CEDEX 09 - FRANCE.

Complaints: reclamations@diot.com – www.mediation-assurance.org