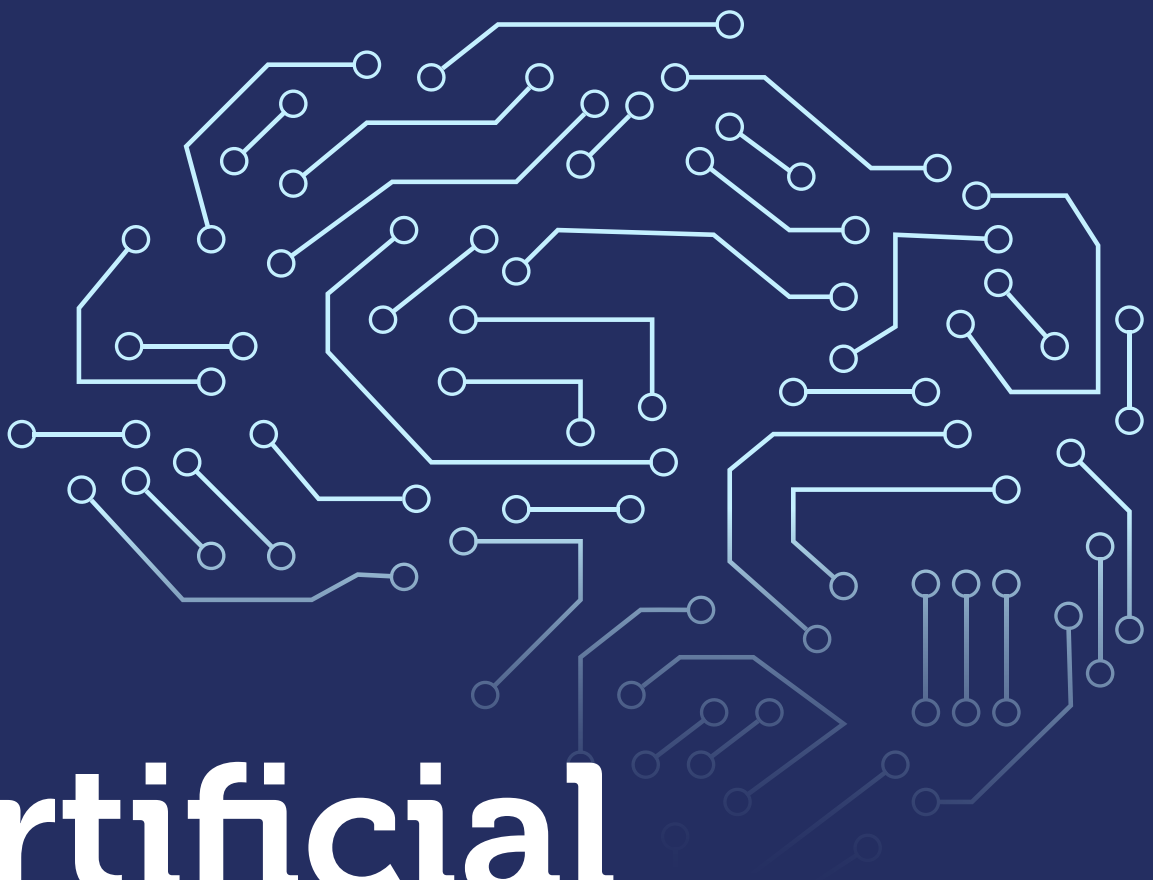


Artificial Intelligence and Work

Advocating for a technological social dialogue

FO Cadres

Introduction

In recent years, debates have been increasingly centred around the transformations taking place in our society under the influence of Artificial Intelligence (AI). Yet, there's a growing disparity between the widespread use of digital technologies and our limited understanding of them.

In the workplace, most employees are kept at arm's length from the emerging issues and the goals pursued by AI deployment, often insufficiently informed by companies, which may also be hesitant to disclose their true intentions. However, both employers and employees are gradually recognizing the significance of these technologies' deployment in the workplace.

AI, what are talking about?

Initiated in the 1940s-1950s, with significant growth in the 1970s-1980s thanks to computerization, Artificial Intelligence (AI) is a field of computer science that focuses on creating systems capable of performing tasks that normally require human intelligence. AI is a logical and automated process typically based on an algorithm and able to perform well-defined tasks. Among the numerous definitions of AI, the «historical» definition adopted at the Dartmouth Conference in 1956 states: «(...) All aspects of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.» AI aims to develop systems that can learn, plan, perceive, understand natural language, and interact autonomously with their environment. This definition emphasizes the goal of partially reproducing human cognitive abilities in computer systems.

To clarify the subject of AI, the European Parliament adopts a definition of the term «artificial intelligence system» - also adopted in this work - which is «a machine-based system designed to operate with varying degrees of autonomy and that can, for explicit or implicit goals, generate outcomes such as predictions, recommendations, or decisions that influence physical or virtual environments.» AI encompasses a variety of technologies, ranging from machine learning systems based on statistical algorithms to symbolic reasoning systems based on formal logic. The general definition of AI thus encompasses a wide range of techniques and approaches aimed at imitating or reproducing human intelligence in computer systems that, beyond their operational purposes, are profoundly reshaping our daily lives.

AI, a central tool in the workplace

Digital tools and other AI systems occupy a central place in businesses and administrations and have become an inseparable instrument of work overtime. This centrality became evident during the COVID-19 lockdown period. Beyond the immaterial nature of work, it is the continuous deployment of digital tools in our professional lives (computers, software, connected devices, applications...) that reinforces this observation. Some employees were able to access their work tools from home (telecommuting)

while adapting their activities, and others found themselves in reduced activity or partial unemployment. At the same time, some workers, previously invisible, have seen the importance of their profession being recognized. Although digital tools have become central in the daily lives of workers, discussions within the company rarely focus on this point. This observation is even more damaging considering that deployed AI systems are not mere tools, but rather complex socio-technical devices whose development is often far removed from the expectations of the workers who depend on them. It is undeniable that the transformation of the collective work environment in this new era will have lasting consequences on management, work control, surveillance, the reliability of collaborative platforms and online communication, as well as on the boundary between professional and personal spheres, requiring sustained attention to safeguard personal privacy.

Observers suggest a profound change in workplace culture. However, we must ask ourselves whether this mutation represents an ethically defensible future. Indeed, mass automation, the development, and deployment of Artificial Intelligence Systems (AIS) are not inevitable. They must be the result of collective negotiations and power dynamics that engage employers, workers, and their trade unions, as well as companies and public authorities.

The technologies deployed in the world of work are not neutral

The role of unions involves scrutinizing AIS themselves for their potential impacts on freedoms, democracy at large, and social democracy. Not all technologies are created equal when it comes to respecting fundamental freedoms and democratic values. Technological choices are inherently value-laden and shaped by human decisions influenced by economic and social objectives.

Developers and engineers, whether consciously or not, often embed their biases and cultural norms into the design of technologies, thereby affecting their accessibility and functionality. Technologies are a social construct, capable of intentionally or unintentionally reshaping existing social and economic dynamics, leading to exclusions and perpetuating discrimination. This is evident in the ongoing debates surrounding certain computer and algorithmic systems. These realities prompt a critical examination of how technologies are conceptualized, the values they embody, and the individuals and societies responsible for their creation.

Rejecting all technological determinism

The integration of AI in the field of human resources is redefining industry practices, promising more efficient talent management. This shift towards intelligent systems allows for a detailed analysis of candidates' profiles, better assessment of existing skills, and prediction of employees' professional development. However, this digital revolution is not without ethical concerns, especially regarding increased employee surveillance and the security of personal data.

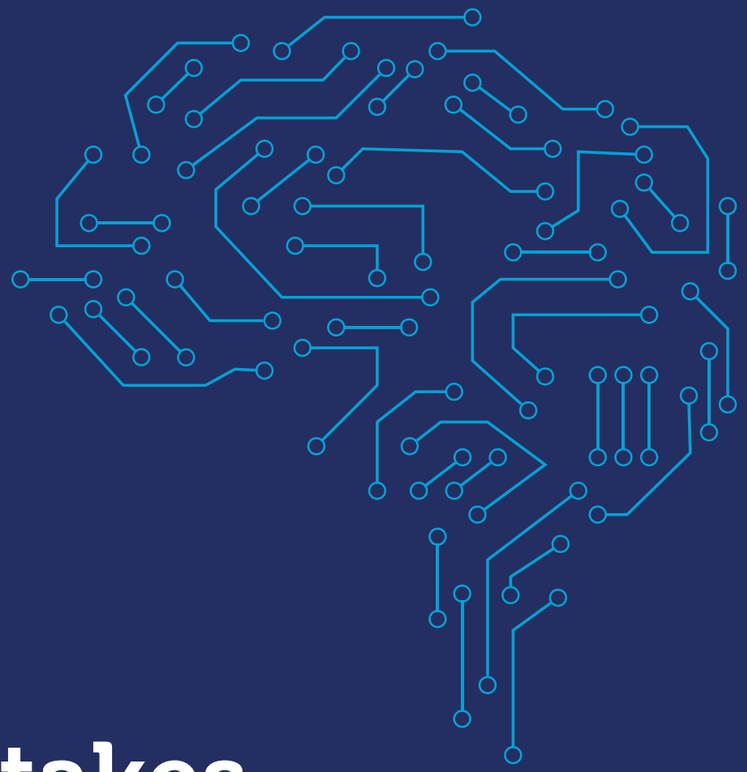
The use of AI, while potentially beneficial for optimizing well-being and job satisfaction, raises privacy issues, as evidenced by the rise in complaints to data protection authorities, particularly since the pandemic-driven surge in remote work. This digital transition therefore calls for increased vigilance and strengthened ethical frameworks to protect employees' rights against potential intrusive surveillance, while also balancing professional and personal life. HR decision-makers are thus faced with a major challenge: integrating AI responsibly to shape the future of work, that is ethically sustainable and respectful of the individual.

Influencing technological choices through union action

The decision to integrate AI technologies must be made collectively. Union action must embrace the 'political' aspect of technologies to exert collective influence on the direction of their deployment, ensuring that progress is tied to social considerations. Objectives such as profitability, economies of scale, surveillance, and profiling should not be the sole focus. It's crucial to move AI systems and their applications beyond the narrow technical perspective and reassess their purposes and impacts on social, economic, and environmental levels.

Furthermore, action must be taken throughout the entire algorithmic chain, from design to usage, employing a combination of technical, organizational, and legal approaches to ensure that AI systems are both ethical and socially responsible, and do not undermine the relevance of labour laws. The desired reorientation of AI, advocated by FO executives and engineers, is achievable through a proactive strategy centred on social dialogue and government intervention. This ensures that technology prioritizes enhancing employee creativity and effort rather than solely maximizing productivity or imposing rigid work methods.

Eric Pérès
General Secretary, Union of executives and engineers- FO



5 stakes

The rise of artificial intelligence is often hailed for its potential to improve businesses and public administrations. However, a more critical analysis reveals significant challenges that these entities struggle to address. The promise of a technological revolution driven by AI clashes with the reality of insufficient preparedness, inequalities in its deployment, and an underestimation of its consequences on human capital.

The enthusiastic landscape that viewed AI as an imminent competitive lever seems to have overlooked the marked disparities among businesses, with some struggling to catch up. The image of the 'augmented' employee masks the complexity of reshaping professional roles and the need for a profound overhaul of skills and organizational structures. Disentangling the sensationalist presentations of new technologies is one thing. Detaching them to appreciate the contributions and potentials of AI in research, industry, or the arts is another. However, this should not lead us to ignore that the emergence of AI systems in our daily lives and in the workplace poses a source of mutations and new challenges that we must address.

Preserving the autonomy of human decision-making in the face of algorithmic systems often perceived as infallible; detecting discriminations inadvertently generated by systems in continuous learning; preserving collective solidarities undermined by the power of digital personalization...The stakes are high, and their implications are already tangible. They question some of the major agreements and balances on which our collective life rests.

Clearly and lucidly reminding of these challenges is the first exercise that the union analysis must undertake to propose, considering fundamental principles, appropriate responses so that technological innovation goes hand in hand with innovation in general and contributes to the construction of a collective vision of our future.

1. Employment

The rise of AI raises concerns about its impact on employment. Many technological innovations, such as autonomous vehicles and medical assistants, are reshaping the professional landscape. The Council for Employment Guidance indicated in 2017 that 10% of jobs are highly vulnerable to automation and that 50% of them will see their content profoundly transformed within 15 years*. The OECD estimates that 27% of positions are at high risk of automation. Contrary to popular belief, it's not only low-skilled jobs that are affected. Indeed, Goldman Sachs estimates that two-thirds of jobs in the United States will be impacted by AI, while OpenAI, in collaboration with the University of Pennsylvania, predicts that AI could replace 80% of American workers for some of their tasks. Every revolution opens the door to new opportunities. This is the essence of a study by the International Labour Organization (ILO)** that nuances these forecasts, suggesting that AI is more likely to complement jobs by automating certain tasks than to destroy them.

The consequences of this transition depend on our choices: economic policies, current legislation, and the ability to adapt to new professions. Technology is not an inevitable destiny; it is humans who must lead this transition.

2. Health

The introduction of AI presents both advantages and challenges for occupational health. By automating repetitive tasks, it can reduce musculoskeletal disorders and prevent occupational hazards. However, it can also expand the substitutability zone and lead employees to live in anxiety about being 'the next to disappear' or in constant stress due to continuous adaptation. The interaction between humans and machines is not merely a technical collaboration but reflects a cultural and social transformation. If judiciously orchestrated, it has the potential to create a harmonious work environment where technology acts as a lever to enhance human capabilities rather than as a substitute.

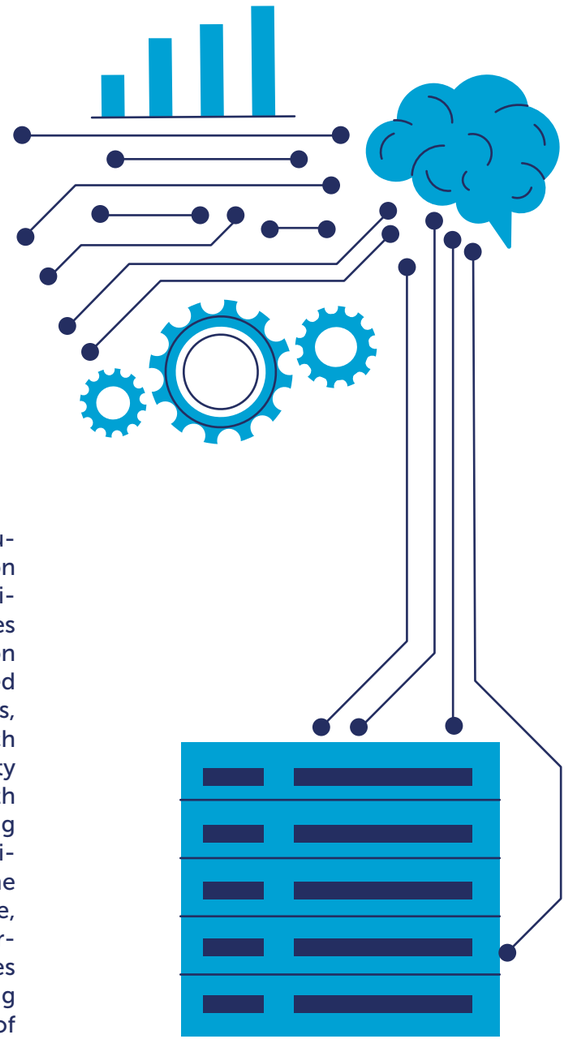
However, the symbiosis between humans and machines also poses major challenges. How can we maintain the engagement, motivation, and well-being of workers when a significant portion of their tasks is automated? How can we ensure that AI, by taking over certain functions, does not lead to dehumanization of the work environment, which can manifest as job devaluation, task, and social relationship impoverishment, or fuel a sense of disempowerment when AI questions the individual's autonomy and legitimacy to make decisions? The complexity of this coexistence urges us to rethink our policies and strategies regarding occupational health in the era of AI.

* COE Report 2017: Automation, digitization, and employment
** OIT - Generative AI and employment: A global analysis of potential effects on the quantity and quality of jobs

DATAFICATION OF THE WORLD SHOULD NOT LEAD TO THE OBJECTIFICATION OF THE INDIVIDUAL

3.

Management



The use of AI raises questions about the evolution of management. The continuous diffusion of algorithmic management, initially established in platform-type companies, challenges the relevance of entrusting the organization and supervision of workers to a system based on a series of calculations. In these contexts, the goal assigned to technology is not so much to free the worker as to increase productivity through a 'customer-centric' approach, with potentially negative consequences on working conditions, despite prevalent rhetoric praising 'liberation through automation'. Some tasks, deemed economically unprofitable, have significant social importance often overlooked. Digitization risks confining employees to purely procedural roles, overshadowing the relational aspects of work with the risk of increasing stress, devaluing the function of work, and intensifying employee control and surveillance. Workers need tools to facilitate their activity, not tools that work in their place or, worse, enslave them. Technology should optimize creativity and personal effort.

4.

Freedom

With the rise of AIS, it's possible to envision three different levels of value creation: ethical, economic, and social. However, the evaluation of AI is often solely based on instrumental economic rationality, which translates into productivity gains and increased efficiency in economic processes. According to Goldman Sachs Research, generative AI could increase global GDP by 7%, equivalent to nearly $7 trillion in additional wealth.

The urgency to rebalance value relations in favour of ethical and social dimensions should not lead us to overlook the issues surrounding the economic value created by AI. Alongside the central issue of anticipating the undeniable impacts of AI on employment, the question of fair redistribution of AI's productivity gains must also be addressed. Just as there is an urgency to adapt our tax system to the economic challenges posed by AI (such as the concentration and transfer of value towards major players in the digital economy), this is essential to seize the economic benefits and support industrial policies that serve innovation and employment, and to fund both public and private investments, especially in the context of the ecological transition.

5.

Value

With the rise of AI systems, we can envision three different levels of value creation: ethical, economic, and social. However, AI is often evaluated solely based on instrumental economic rationality, which manifests as productivity and efficiency gains in economic processes. According to Goldman Sachs Research, generative AI could increase global GDP by 7%, amounting to nearly $7 trillion in additional wealth*.

There is an urgent need to rebalance the value relationships in favour of ethical and social dimensions. However, this should not lead us to overlook the issues surrounding the economic value created by AI. Alongside the central issue of anticipating the undeniable impacts of AI on employment, the question of the fair redistribution of AI's productivity gains also arises. Similarly, there is an urgency to adapt our tax system to the economic challenges posed by AI, such as the concentration and transfer of value towards major players in the digital economy. To capture the economic benefits, support industrial policies that boost innovation and employment, and fund both public and private investments, particularly in the context of ecological transition.

* Stanford Institute for Human-Centred Artificial Intelligence, Goldman Sachs Research - 2023

10 Principles for Ethically Based AI

Observations highlight the risk associated with overreliance on decisions made by «machines» considered infallible and more «objective» than humans, potentially leading to a lack of accountability. To address these risks, FO-Cadres has identified 10 major principles that lead to 20 operational proposals.

These principles, set against the backdrop of corporate accountability as mandated by the General Data Protection Regulation (GDPR), emphasize the need to implement all appropriate measures from the outset to ensure optimal data protection and minimize data collection while ensuring that this protection is sustained. This commitment is essential to combat the «black box» effect of AI and make algorithmic systems understandable for greater transparency.

Furthermore, these principles advocate for a regulatory approach that goes beyond just the legal framework for data collection. They also question the design of AI systems, and the legitimacy and transparency of the algorithmic processes themselves. This approach highlights the importance of the critical capacity of workers, employee representative bodies, and trade unions to understand, question, and challenge the underlying logics of automated systems that influence, increasingly, the world of business and public administration. In the wake of technological progress, the development of algorithmic systems demands adherence to fundamental principles to establish a framework that balances innovation and human integrity. These principles are not only guides for action but also guardians of our social integrity and even the improved efficiency of AI.

This suggests that any regulation should consider the nature and evolution of the technologies themselves, their role in society, and their interaction with humans. Rather than imposing strict rules, it is advisable to advocate for a framework that promotes a harmonious co-evolution between technology and humans, allowing continuous adaptation of technology to social needs and vice versa.

TECHNOLOGY IS NOT AN INEVITABLE DESTINY; IT IS HUMAN BEINGS WHO MUST LEAD THIS TRANSITION

1. The purpose

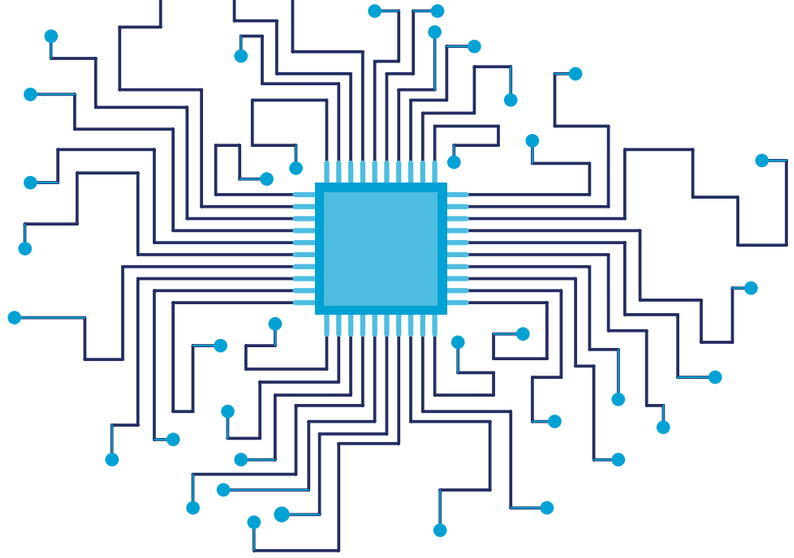
Every deployment of AI must serve a clear purpose that addresses the real needs of society, ensuring to enhance the human condition without compromising our democratic values. Before any deployment of an AI System (SIA), it is fundamental to establish an explicit purpose that respects the rights of employees. Whether AI is used for performance analysis, recruitment, or even fraud detection, it must always respect individual integrity. No data should be collected without solid justification and always ensuring the confidentiality of personal information.

Machine learning algorithms, particularly relevant for HR services, must adhere to these principles even though they generate their own rules from datasets. This characteristic might seem contradictory to the principle of purpose, especially when innovation is seen as an absolute priority. However, even if machine learning aims to uncover unforeseen correlations, its use must be anchored in a defined and legitimate objective, even if that objective is formulated in general terms.

2. The proportionality

Proportionality in law ensures that any measure taken, especially in the digital domain, is adequate, relevant, and limited to what is necessary. This involves a constant evaluation of the benefits and potential disadvantages of each decision, particularly when it comes to large enterprises feeding AI with company data.

While the principle of data minimization specifically refers to the collection, storage, and use of data, emphasizing that only those data which are strictly necessary for a specific purpose should be processed, the principle of proportionality is broader. It encompasses the balance between the means used and the ends pursued. The principle of proportionality remains crucial to ensuring a balance between technological and regulatory imperatives as well as the protection of individual rights and the promotion of responsible innovation.



3.
Loyalty

Fidelity to commitments and loyalty to users must permeate AI, necessitating a design that fairly respects all involved stakeholders, without deceit or bias. The principle of loyalty captures the essence of ethical technology in the context of AI, emphasizing the obligations of algorithm designers over the rights of users.

Originating from the French Data Protection Act of 1978 («Loi Informatique et Libertés»), these principles or mandates dictate that algorithms must be transparent. This transparency is a necessary condition for exercising individuals' rights, such as the right to access, by providing insight into how the algorithm functions without hidden biases or opaque agendas. It also limits the way the algorithm is designed and utilized. Adopting the principle of loyalty entails that companies commit to protecting workers' data, ensuring not only security but also that their use aligns consistently with the defined purposes. The key to successfully implementing this principle lies in a combination of ethical design, transparent communication, and a continual readiness to adjust systems based on feedback and evolving conditions.

4.
Vigilance

The development of AIS and machine learning introduces increasing unpredictability regarding their impacts. Their evolving nature, compounded by the breadth of their applications, makes regulating them complex. In response to these challenges, the principle of vigilance emerges as a methodological answer. It aims to prevent risks and anticipate the unforeseen effects of algorithms.

This principle also seeks to address the excessive trust often placed in AI, which is frequently perceived as infallible, and the abdication of responsibility due to its opacity. More than mere tools, AI is part of extensive algorithmic chains that involve numerous actors, from developers to end-users. This multiplicity can lead to a dilution of accountability.

As a collective duty, vigilance strives to ensure ethics and responsibility throughout this chain, ensuring that this technology is developed and deployed cautiously, with consideration for the public interest, individual rights, and the assessment of impact studies.

5.
Transparency

Absolute clarity in algorithmic processes is essential for gaining and maintaining public trust, as well as ensuring an understanding of decisions made by or with the aid of artificial intelligence. An AIS that a person uses or is subjected to must be transparent, which means, the individual should be able to understand its fundamental mechanisms, the motivations of its designers, and those of its users. Additionally, if applicable, individuals should have the right and the practical means to challenge these systems.

While certain technical details may remain confidential, particularly for reasons of intellectual property, the criteria used, and the data collected and processed by the AI must be accessible and explicit. When an algorithm is used for recruitment or performance evaluation, employees must be aware of the nature of the data collected, its purpose, and how it impacts decisions. This transparency is crucial to ensure a balance between innovation and protection.

6.
Law

The use of a strong regulatory framework is necessary to establish «red lines» and, where necessary, block AIS that would contravene democratic principles, social justice, or environmental justice. The French Data Protection Act and the implementation of the GDPR in 2018 fully contribute to this goal. However, relying solely on consent does not adequately address the choice of technology by the individual, especially as it will be ineffective in many cases, for example in a work subordination context. While the use of AI in human resources or by public administrations can pursue legitimate purposes, it should not lead to the systematic automation of tasks, resources, judgments, or spending cuts. In the charters and regulatory tools, the meaning of these activities is often overshadowed by economic rationality.

The development of «fair» technologies that promote individual and collective autonomy, serving social organizations in which people would have control of the tool, could broaden the power of collective action. The goal? To rectify biases, whether they arise from malicious intent or negligence, and to promote a technology that would serve solidarity.

ADAPTING TECHNOLOGY TO SOCIAL NEEDS AND VICE VERSA

7.

Safety

AIS must be designed to be safe, not harming individuals, their property, and their rights. This principle would require algorithm developers to ensure that all necessary precautions are taken to prevent causing physical or moral harm to individuals and communities. This approach also implies using AI only when its net contribution is positive for humanity. This means that in the human-machine relationship, roles must be strictly defined. Technically, this involves designing systems to avoid any nuisance, whether in terms of physical safety or personal data protection. Implementing robust security protocols and compliance with regulations, including GDPR, are essential preventive measures.

Legally, safety demands strict legislation governing the use of AI, with clear guidelines to prevent potential abuses such as excessive surveillance or discriminatory profiling. Establishing international standards for algorithms and requiring their compliance with criteria of fairness and transparency are also essential measures for aligning values.

8.

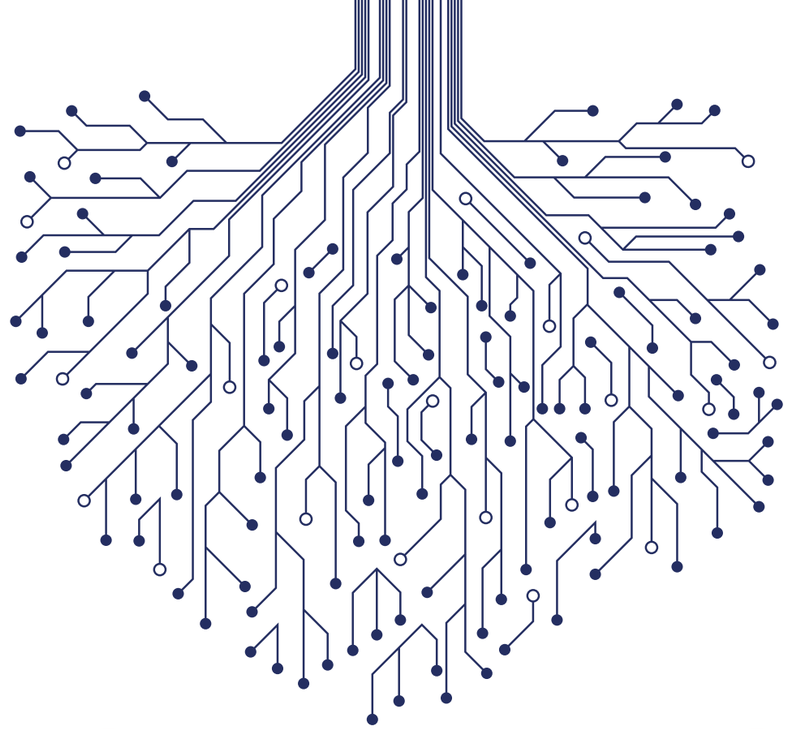
Responsibility

The deployment of any AIS must fully engage the responsibility of the individuals and entities involved in its design, dissemination, and deployment, especially in cases of malfunction or unforeseen adverse consequences.

Technically, this involves establishing rigorous evaluation and monitoring processes, developing transparent and explainable AI systems, and integrating mechanisms that allow them to be deactivated or modified in the event of unexpected or dangerous behaviours. AI accountability should be governed by norms and standards that define requirements in terms of safety, ethics, and compliance.

This necessitates a clarification of the roles and responsibilities of stakeholders throughout the AI lifecycle, from design to implementation and beyond.

FOR A CLARIFICATION OF ROLES AND RESPONSIBILITIES OF STAKEHOLDERS IN THE LIFECYCLE OF AIS



9.

Progress

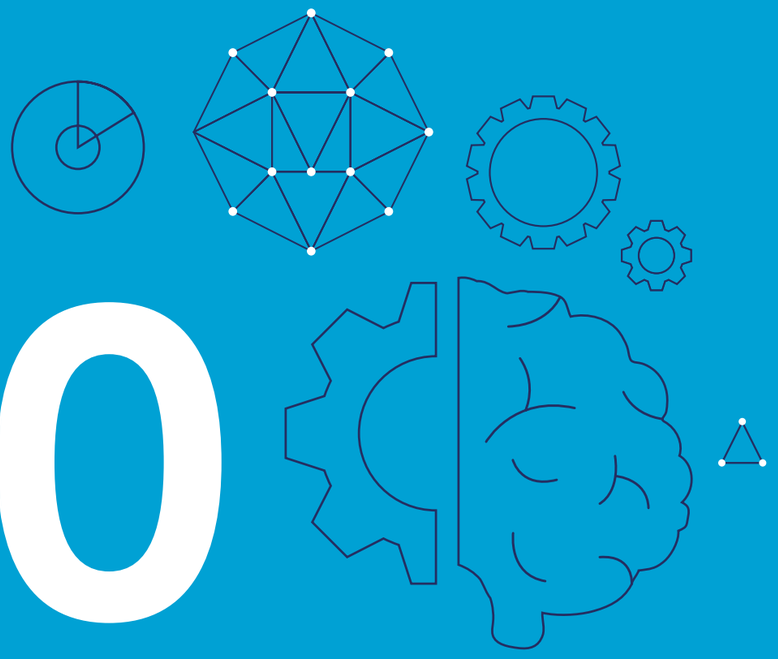
It is important to pursue technological advancements not only for their intrinsic value but also for their contribution to social and human progress. However, these new tools should only be deployed when they improve the living conditions of individuals and communities. Their goal should be to contribute to the organization of professional activities and to enhance their practice.

Additionally, the principle of purpose must also apply to decisions regarding job cuts. It is necessary to strictly prohibit such manoeuvres unless their utility for the general interest has been demonstrated. In France, several bodies for social dialogue can be mobilized to address issues related to artificial intelligence. They play an essential role in ensuring that the development and implementation of AI systems are conducted with respect for rights, in a fair and responsible manner.

10.

Private life

The rapid growth and increasing sophistication of AIS are making them progressively more intrusive into individuals' privacy. This poses a real risk in businesses where the extensive collection and processing of data, especially personal data, are at the heart of emerging or evolving economic models. In a panoptic world, subject to continuous and «intelligent» machine control, framed by algorithms dictating what to do, how to do it better, and with whom to do it, the risk of employees becoming assistants, servants, or adjuncts to technology is anything but fiction. Algorithmic management is gradually infiltrating every aspect of workers' actions: from recruitment and skills management to surveillance, performance evaluation, and geolocation of employees. Without oversight or information, workers' privacy is threatened: mass surveillance, registration, profiling... Yet, respect for privacy is a cornerstone of social democracy. It must be a fundamental part of the deployment of AI in businesses and public administrations.



20 Fo-Cadres proposals for a socially responsible AI

The debates around AI evoke a shared sentiment where the ambivalence that characterizes technologies blends with the fascination for the computational power of AI systems. This discourse strongly resonates with the experiences of employees and public servants. They are both fascinated by the incredible possibilities offered by using AI and concerned about the risks of its uncontrolled deployment in workplaces. The potential of these technologies is significant enough to trigger fright or too many expectations. While technology can have a magical and fascinating character, it often oppresses employees and public servants when it is at the heart of a deregulated professional universe. Far from yielding to the sirens of neo-Luddism that denounces all technological innovations, it is the call for a critical resurgence in the face of the massive deployment of AI systems in the professional world that must be addressed at the union level. A critical resurgence to question technology considering social needs and to protect workers from all attempts to make them transparent. This resurgence we hope for is operationalized in the following 20 proposals. A modest effort to promote a technological social dialogue capable of combining innovation and protection.

PROMOTING ARTIFICIAL INTELLIGENCE THAT GUARANTEES FUNDAMENTAL RIGHTS

1. Advocating for a right to opacity at work

As businesses claim trade secrets to protect their data and economic privacy, could workers not assert a similar right to opacity in the same spirit? Secrecy, like opacity, requires recognizing these terms as data, a value, and a potential danger. Between absolute opacity, which might suggest concealment or an obstacle to understanding, and total transparency, which reveals and allows knowledge of everything, negotiated secrecy could serve as a balance between these extremes. By opposing workers' opacity to the absolute empire of transparency in the digital age, the power to say no to any form of technological dominion over personal intimacy would be secured. In all cases, while promoting innovation and economic growth, a right to the use of AI at work must be asserted to better protect workers. It is essential to ensure that current regulations are sufficiently adapted to the issues and concerns in the world of work.

2. Systematizing collective prevention and vigilance

Without legal constraints, discussions on implementing criteria that businesses and administrations must meet before deploying any artificial intelligence technology can face difficulties in achieving tangible results. Therefore, it is necessary to positively enshrine in law a principle of prevention for clearly identified risks, which could be referenced in disputes to challenge the deployment of any AI system or demand the conduct of additional impact studies. There is alignment on this issue with the proposed European regulation on AI, where certain AIS are deemed «high risk» (Article 6) and require specific obligations.

MAKING ARTIFICIAL INTELLIGENCE SYSTEMS A SUBJECT OF COLLECTIVE DIALOGUE AND NEGOTIATION

3.

Adopt a principle of responsible caution

When facing potential and unidentified risks at the workplace, it's vital to incorporate a principle of precaution alongside the existing principle of prevention. This proactive approach should aim to enhance knowledge generation and significantly advance the safeguarding of individuals from AI impacts. Rather than obstructing technological progress, this principle should actively engage in it. By fostering a constructive and continuous dialogue on AI usage, it aims to explore innovative solutions while prioritizing worker safety. Additionally, implementing a licensing system that prohibits the development of AIS in certain areas, like HR practices, without prior approval from regulatory authorities could be considered.

4.

Adapting labour laws to the challenges of AI

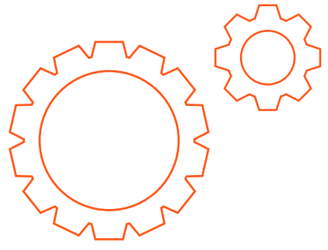
The term «algorithm» is rarely mentioned in the Labour Code, and when it is, the latter relates to articles concerning digital platforms. Although some provisions might be interpreted in the context of AI, including aspects of health, safety, or the consultation-informing processes of workers' representation bodies, the proliferation of AI in the professional sphere necessitates an update or an extension of the Labour Code to specifically address this issue. Potential topics could include algorithmic surveillance and management, the impacts of automated decision-making on employees or public servants, or career management linked to automation. With the advancement of AI, labour law, which has reintegrated the human person within a contractual framework, must now more than ever serve as a tool to protect human dignity at work.

5.

Negotiating Collective Agreements on the Use of AI in the Workplace

In the absence of regulation and negotiated collective control, the use of AI in the workplace can lead to intrusive and abusive surveillance of workers' activities, with risks of systematic exploitation, discrimination, and health and safety issues. This situation demands the involvement of workers and their representatives in decision-making processes that lead to the development and deployment of AI. Social dialogue must be fully integrated so that the use of AI can be discussed and negotiated at all levels of the organization.

A national interprofessional agreement on the use of AI at work appears essential to establish strong guidelines in this area and build effective regulation at the level of professional branches and companies. All bodies involved in social dialogue must be mobilized to address the challenges related to artificial intelligence (AI) in the workplace. Their role is crucial to ensure that the development and implementation of AI contribute to human progress and respect for social democracy.



6.

Encouraging paths of dialogue and collective debate

The Strategic Sector Committees (Comités Stratégiques de Filière - CSF) in France, which bring together key stakeholders from specific industrial sectors (companies, unions, training organizations, etc.) to define development strategies, can play a significant role in addressing the specific challenges posed by Artificial Intelligence (AI). Their role could involve devising specific strategies to integrate AI into their respective sectors, considering the unique characteristics and needs of each one. They would then play a crucial role in supporting the industry to build digital sovereignty and in assisting small and medium-sized enterprises (SMEs) in adopting and using AI that is ethical and respects fundamental rights.

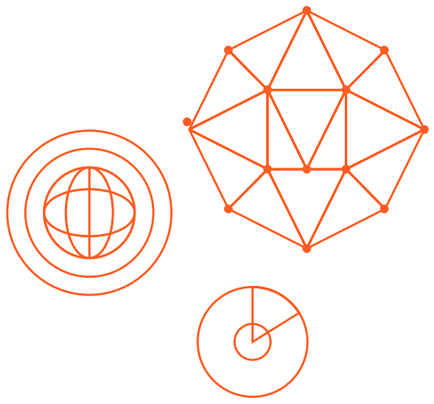
In businesses and administrations, stakeholders are not only employers and employees but also partners, co-producers, and finally, providers of services and solutions. Public debates on technological issues should make room for all these stakeholders for better defence and negotiation of collective freedoms. The composition and role of the Economic, Social, and Environmental Council (CESE) are, from this point of view, a valuable resource that should be leveraged to enrich collective discussions on the challenges of AI in society in general and in the workplace in particular.

7.

Building sector-specific frameworks

To enhance safety and encourage ethical and responsible innovation, the development of certification standards for AI systems, like ISO standards or ABC analyses used in energy performance, should be promoted. These frameworks aim to establish clear objectives that certification seeks to achieve, focusing on standards such as data quality, system security, algorithmic transparency, robustness, resilience of systems, and respect for fundamental rights. They define specific criteria that AIS must meet to be certified. This approach also ensures that, from the design phase, humans remain in control of AI tools.

Creating such frameworks requires initiating collaboration among cognitive sciences, computer science, philosophy, and social sciences. This interdisciplinary approach is crucial to guard against excessive optimism regarding the capabilities of AI compared to human intelligence.



8.

Strengthening the expertise and resources of workers' representative bodies*

In the face of risks that could be generated by the deployment of artificial intelligence, Workers' Representative Bodies (IRP) must be consulted and involved in all phases of the design, development, and deployment of AI systems within the company. They should also be involved in strategic decisions regarding the implementation of AI, including the choice of technologies, suppliers, and data management policies. From this perspective, companies must provide specialized training on artificial intelligence and its implications in the workplace to the members of the Social and Economic Committee (CSE). This training should enable them to understand and adequately assess AI projects and their stakes. Resources should be allocated to allow the CSE to audit AI tools before their deployment in the company and to carry out continuous technological and ethical monitoring of their developments and potential impacts on the organization and working conditions. The jurisprudence of the Pontoise Judicial Court in 2022** established that the introduction of new technology alone justifies the use of expertise by the CSE, without even the need to demonstrate the existence of repercussions on the working conditions of employees.

* Staff representative bodies
** TJ Pontoise,Apr. 15, 2022, n° RG 22/00134, S.A.S. Atos International c/ CSE de la société Atos International)

DEFENDING THE DEVELOPMENT OF INTELLIGENT AND SOCIALLY RESPONSIBLE ARTIFICIAL INTELLIGENCE SYSTEMS

9.

Promoting «Social by Design»

Following the data opening, the challenge now lies in understanding the knowledge and decisions made from this data, with the aim of restoring or enhancing trust in the use of AI tools. We must encourage developers to integrate certification requirements from the early stages of designing AI products and services to naturally incorporate principles of transparency and fairness, as well as the intelligibility of systems and decisions. It also involves promoting an iterative development process that allows for continuous improvements aimed at subsequent certification, particularly within companies. The goal is thus to enable organizations to «open the hood» of the systems they use, turning them into a source for a new social dialogue around issues of solidarity, protection, accessibility, and inclusivity. In addition to ensuring the protection of personal data from the design of an AI tool (Privacy by Design), it is also necessary to safeguard fundamental rights (Social by Design) by encouraging the participation of all stakeholders in this creative process.

10.

Giving effect to the right to intelligibility

Artificial intelligence systems often deliver results without providing the means to understand the logical process they follow. These «black boxes» contribute to the mistrust towards these technologies. Thus, the transparency of algorithms, their employment, uses, and purposes is essential for building trust and encouraging their adoption.

This involves demanding complete information from employers who decide to implement these systems and from their designers. Transparency in how decisions are made is fundamental and must be explainable in clear, understandable language, focusing on basic principles rather than complex technical details.

DEVELOPING COLLECTIVE VIGILANCE SYSTEMS AT THE HEART OF ORGANIZATIONS

11.

Systematic impact studies

Beyond compliance with data protection laws, companies must incorporate as a mandatory phase in the planning and execution of technological projects, from the outset of discussions and before any deployment, a section dedicated to evaluating the social impacts of AI technologies on employment, professions, working conditions, and social relations.

This can be achieved through studies, surveys, interviews, and the formation of discussion groups to assess potential implications. Employee representatives should be involved from the beginning of the process to ensure ongoing monitoring and revision of the collective impacts on workplaces. Following the results, measures taken to prevent and correct biases should be documented in a report made accessible to Workers' Representative Bodies (IRP).

12.

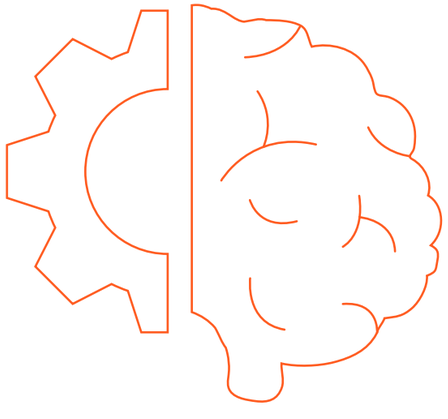
Enabling reversibility of AIS

AI tools need to be regularly adjusted, updated, or modified to adapt to new data or conditions. Reversibility would allow for this flexibility, better managing the risks associated with their use. If a system proves to be faulty, biased, or causes unexpected damage, it should be possible to disable it or revert it to a more stable previous version. In practice, reversibility can be challenging to implement, especially for complex AI systems or those integrated into critical infrastructures. Careful planning, regular testing, and systematic design that allows for flawless disconnection or regression might include features such as an «emergency stop button» or «safety valves,» as well as restoration options, data backups, and secure withdrawal protocols. Additionally, users should have the ability to challenge the use of any tool they consider harmful to their professional or personal lives.

13.

Encouraging experimentation

Trust is built on reciprocity and evolves over time. It cannot be decreed. Therefore, it is essential that the development and deployment of AI systems in the workplace occur «without coercion» and with the utmost transparency. The company must demonstrate that the use of AI tools contributes to wealth growth in a socially responsible manner where employees' fundamental rights are preserved. The regulatory «sandbox,» a symbol of innovation, can contribute to this endeavour. It allows for testing and experimenting with AI tools in a controlled environment, reducing risks and ensuring compliance with legislation, including the GDPR. This approach, which offers flexibility or temporary adaptations of regulatory standards, promotes responsible innovation while being overseen by the CNIL to ensure that employees' fundamental rights are protected regarding the collection, processing, and use of personal data.



14.

Create a supervision committee

As AIS technologies are evolutionary and learning-based, requiring auditing both upstream and downstream, the creation of a supervisory committee would ensure continuous monitoring of the use of AI tools. Comprising employee representatives, the DPO, the CIO, and the CISO, this committee would be tasked with supervising, with the assistance of experts in ethics, social sciences, technology, law, and risk management whenever possible, the use of AI tools and ensuring that they are used responsibly, without risks to employees and without producing negative externalities for the company. This committee would propose appropriate collective vigilance and regulatory measures during periodic reviews. Ethical and social evaluation checklists could be used to ensure that ethical considerations are considered at different stages of the product development cycle. The recommendations and their justifications would be addressed to the executive committee and the employee representative body and made accessible, under appropriate modalities, to the stakeholders of the company for consultation purposes, particularly in case of disputes. In the case of SMEs, the responsibilities of the supervisory committee could be integrated into the regional interprofessional joint committee (CPRI), which serves as a social dialogue platform).

15.

Building binding charters and codes of conduct

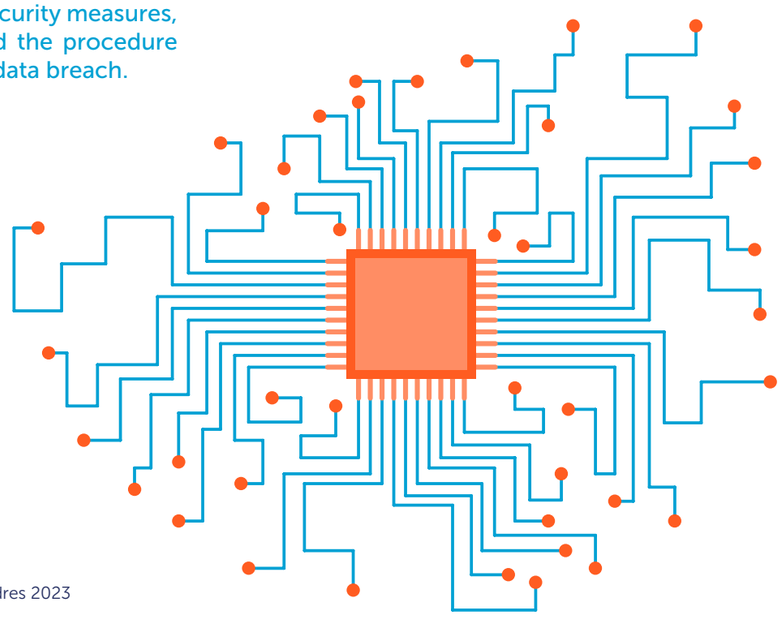
The numerous charters and codes of conduct drafted to influence behaviours in line with rules or values are often voluntary instruments of self-regulation lacking independent oversight and legally binding rules. To effectively regulate the deployment of AI in the workplace, these charters, and codes, certified by the CNIL in accordance with the provisions of Article 40 of the GDPR, must introduce evaluation mechanisms and address technological risks.

This work requires close cooperation with supervisory authorities to benefit from advice capable of developing guidance on data protection and privacy in the workplace. The validity of these regulatory tools should be conditional on the existence of an agreement compliant with the regulations, particularly regarding the duration of data retention, access modalities and security measures, transparency obligations, and the procedure to follow in case of personal data breach.

16.

Create a register of AI tools and their uses

Taking examples from certain cities and local administrations, such as Amsterdam and Helsinki, which have created public registers of algorithms to increase transparency around the use of AI and algorithmic technologies by public authorities, it would be appropriate to make it mandatory to maintain a register documenting all uses of AI deployed within the company. This register, similar to the one provided for in Article 30 of the GDPR for personal data processing, should include information regarding the nature of AI tools, processing activities performed under their auspices, as well as the nature of the data collected, and the purpose pursued by these different systems. Such a register, made known to various stakeholders, would formalize obligations of transparency and loyalty.



STRENGTHENING THE INFORMATIONAL AUTONOMY OF PLAYERS THROUGH TRAINING AND INFORMATION

17.

Building an AI-specific training plan

Human resources professionals, chief information officers (CIOs), and employee representatives should receive joint training to raise awareness about the implications of implementing artificial intelligence within the company. Companies and administrations should establish a specific AI training plan for employees to update their knowledge on recent developments in AI and digital technologies, as well as their social implications. This regular training offering should lead to greater awareness of the social and ethical implications of AI systems.

In this regard, training for engineers is essential to sensitizing them more deeply to the issues related to the tools they design and to clearly inform them about the measures taken to ensure data security and privacy protection in the use of AI.

18.

Contribute to manager training

The deployment of digital tools such as AI can impact interactions between managers and teams. Some software may even interfere with the core managerial function or participate in decision-making itself. Therefore, managers must be able to understand the new forms of expertise required to work effectively with these tools and help their teams to adopt these technologies. Specific training modules on the managerial implications of AI usage should be integrated into the career path of managers. These training programs should provide them with the means to opt for a transparent and stable organization around discussions and negotiations regarding the use of AI with their collaborators. Managers thus have a key role to play in ensuring a harmonious relationship between humans and machines, eliminating any form of oppressive algorithmic management, and promoting trust-based management rather than surveillance-based management.

19.

Support the creation of an «AI relay» network

Establishing an «AI Relay Network» within companies typically involves employees with various technical and operational expertise in the field of AI, data experts, and key users in different departments. This contributes to building a collective competence based on a common AI grammar that stems from the work of all employees. This collective competence presents an opportunity for social engineering across various sectors, facilitating the adoption and integration of AI within the company by enabling knowledge sharing, technical support, and promoting the effective use of AI tools.

In conjunction with the supervision committee and the Data Protection Officer (DPO), it acts as a catalyst for innovation and digital transformation, providing training, resources, and operational support for AI implementation. Its role is to provide technical solutions that enable employees to influence the configuration of AI solutions, that organize and condition their activities.

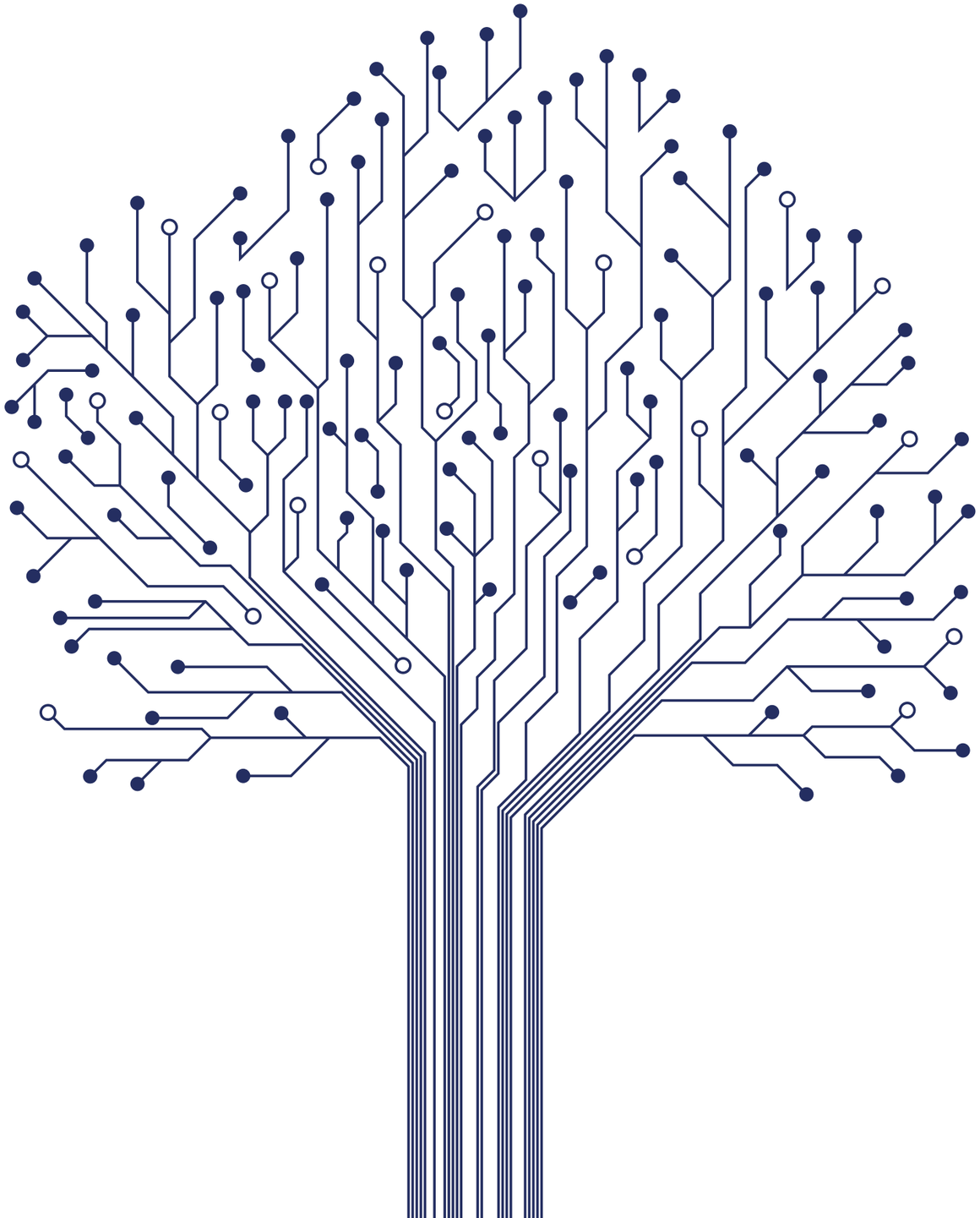
20.

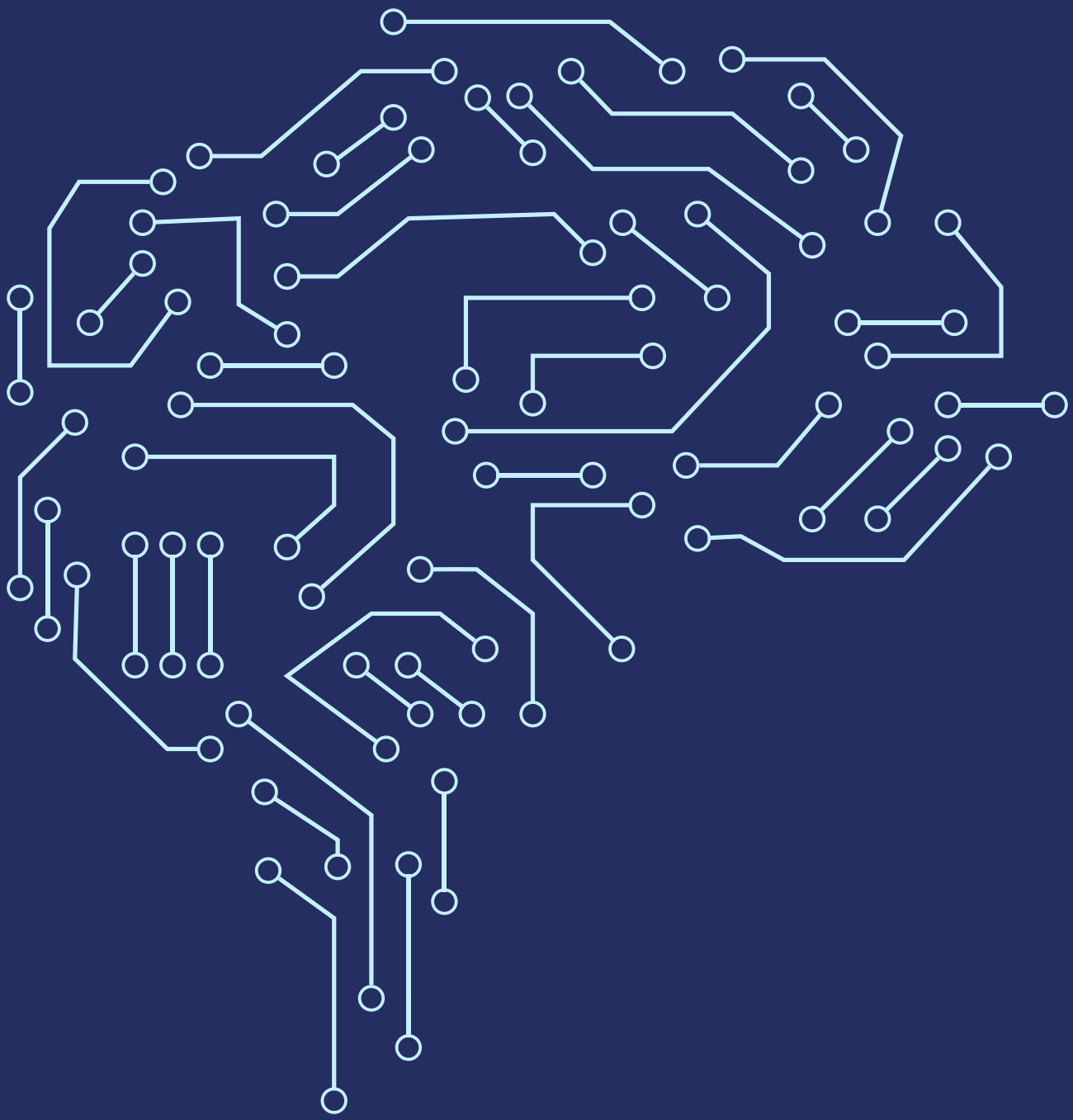
Protecting the independence of Data Protection Officers (DPOs)

When the Data Protection Officer (DPO) is an employee of the company, they may come across such strong pressures that they cannot remain truly independent. While the GDPR stipulates that the DPO cannot be penalized for reasons inherent to their role, this system provides little protection in case of dismissal or potential sanctions. This justifies additional guarantees beyond the GDPR, including granting the DPO protected employee status. The Court of Justice of the European Union recently reiterated that Member States can provide greater protection for DPOs, for example, by limiting the possibility of dismissing an employee DPO to cases of gross misconduct or requiring authorization from labour inspection.

In all cases, the legislator should ensure that the Works Council (CSE) is mandatory informed of the appointment of their DPO to ensure their working conditions and independence. Companies and administrations must also formally commit to ensuring their independence and specify this to the CNIL (French data protection authority) upon appointment (for example, by allowing direct communication with management).

Finally, when the DPO position is external to the company, the internal regulations should ensure that the service contract is precise and detailed to avoid any conflicts of interest.





7 passage Tenaille
75014 Paris — France
Tel : 01 40 52 82 77

contact@fo-cadres.fr
fo-cadres.fr
FOCADRES FO-CADRES

Graphic design: Clara Luneau