CONFÉDÉRATION FRANÇAISE DE L'ENCADREMENT-CGC

Draft of the EU Commission on a European AI regulation
(Artificial Intelligence Act) 21 April 2021

La **Confédération française de l'encadrement - Confédération générale des cadres** (**CFE-CGC**) est un syndicat français de salariés fondé le 15 octobre 1944 sous le nom de Confédération générale des cadres (CGC), qui présente la caractéristique de défendre les intérêts d'une catégorie professionnelle spécifique, l'encadrement. Cette spécificité en fait un syndicat catégoriel ouvert aux cadres, ingénieurs, agents de maîtrise et forces de ventes tant dans le secteur privé que public.

La CFE-CGC est adhérente de la Confédération européenne des cadres (CEC Euro Managers) et, depuis juin 2014, observatrice de la Confédération européenne des syndicats indépendants (CESI), qui regroupe essentiellement des organisations du secteur public en Europe.

La CFE-CGC se définit comme un syndicat de proposition prônant avant toute chose le dialogue et la négociation.

La CFE-CGE s'intéresse depuis 2018 aux impacts de l'IA sur l'emploi. Nous avons organisé des tables rondes et un cycle de conférence « Y voir Clair » afin d'initier le débat et de comprendre les enjeux. Ensuite, nous avons travaillé à l'élaboration d'une charte pour répondre à la question éthique posée par l'intelligence artificielle dans le domaine RH.

En effet, l'intelligence artificielle se développe très largement dans le monde professionnel avec des impacts qui restent encore aujourd'hui difficiles à mesurer.

Tous les métiers se retrouveront à terme impactés par l'IA, soit de façon positive avec une réallocation des tâches à forte valeur ajoutée vers des emplois augmentés, soit de façon négative avec un risque de suppression de certains emplois, dont toutes les tâches deviendraient automatisables.
Il est donc important de mesurer régulièrement ces impacts réels de l'IA sur les emplois à l'échelle de chaque secteur et de chaque entreprise.

L'IA va aussi modifier les processus industriels de façon partielle ou totale s'ils peuvent être intégralement dématérialisés.
Nous pensons que l'hybridation deviendra la norme dans l'industrie du futur, ce que nous commençons à voir avec l'intégration de l'IA dans la maintenance prédictive ou dans les relations clients fournisseurs (optimisation des processus logistiques).

Ces optimisations apportent des gains de productivité qu'il est important de mesurer afin de permettre une répartition équitable entre les facteurs de production.
C'est dans ce but que nous avons initié avec d'autres syndicats européens le projet SecoIADeal, financé par Horizon2020. Ce dernier a également pour objectif de définir quelles compétences seront nécessaires aux managers pour la maîtrise du big data et de l'apprentissage automatique.

Pour terminer, nous constatons que l'IA bouleverse les processus RH à la fois au moment du recrutement et tout au long de la vie du salarié dans l'entreprise. Il faut donc en priorité définir un cadre éthique à ces pratiques.

Pour rappel, la CFE-CGC avait déjà répondu à la consultation de février 2020 sur la proposition du HLEG. Nous avions proposé une approche Social By Design en complément de celle dite du X by design. L'idée forte était de sensibiliser les équipes d'experts en méga données aux impacts sociaux de leur travail.

Nous avions aussi été interviewés par un consultant mandaté par la Commission européenne sur la pertinence de l'AI Assessment List. Pour nous, cet outil était une base de travail intéressante à finaliser.

Aujourd'hui, La CFE-CGC salue la proposition de règlement de la Commission européenne établissant un cadre de régulation en matière d'intelligence artificielle.

C'est pour nous une bonne chose qu'un cadre réglementaire vienne encadrer les pratiques dans les entreprises avec l'arrivée du management dit « algorithmique ».
Les enjeux sont grands en termes de responsabilité et de liberté avec des outils d'aide à la décision qui peuvent se révéler opaques et générateurs de biais.
Créer des obligations et des pénalités associées, dans la logique de ce qui avait été fait sur le RGPD, permet de responsabiliser les fournisseurs d'IA, tout en informant et en protégeant les utilisateurs d'IA.

Le point 36 du règlement préconise de classer les applications d'IA liées au monde du travail comme à haut risque. Il couvre bien l'ensemble des situations (candidats, salariés, indépendants) et tous les risques associés aux populations discriminables.
La Commission européenne a bien identifié que le lien de subordination crée une asymétrie entre le salarié et l'employeur avec une possibilité pour les employeurs d'imposer ces systèmes d'IA de façon unilatérale ou par un consentement volontaire vicié. Cette asymétrie est encore plus forte pour les candidats, qui disposent seulement des droits sur leurs données accordées par le RGPD.

Nous attirons cependant l'attention de la Commission européenne sur l'éventualité de se retrouver face à des applications identifiées comme doublement à haut risque, c'est-à-dire liées au monde du travail (Annexe 3 point 4) et utilisant des procédés de reconnaissance biométrique (Annexe 3 point 1), et dont les obligations pour le fournisseur ou opérateur d'IA ne seront pas claires.

Par ailleurs, de façon plus courante, nous serons confrontés à des applications liées au monde du travail (Annexe 3 point 4) et ayant des obligations sur la transparence des algorithmes visées par l'article 52, car utilisant des systèmes de reconnaissance des émotions. Nous trouvons aujourd'hui ce type d'application pour le recrutement, par exemple[1]. L'optimisation du processus de recrutement se fait par des systèmes de reconnaissance des émotions, afin d'évaluer au mieux les candidats. Nous pouvons imaginer que ce type de système va se pérenniser pour, entre autres, tester leur résistance au stress. Ces applications font aussi une analyse de la voix du candidat à travers son rythme et son intensité (prosodie). La voix est considérée comme une donnée biométrique, car elle permet d'idendifier la personne, et peut donc être soumise aux obligations associées (Annexe 3 point 1).

C'est une des limites de l'approche par le risque proposée par la Commission européenne. Il aurait été plus pertinent de s'appuyer sur celle du Federal Government's Data Ethics Commission ("Datenethikkommission"), fondée sur la criticité, beaucoup plus précise[2]. En effet, une granularité plus fine des risques aurait permis une simplification du modèle et donc, des obligations associées.
Pour ce faire, il faudrait définir des sous-niveaux par criticité dans les modèles à haut risque afin d'ajouter des obligations claires inhérentes aux outils utilisant des données biométriques, par exemple.
Dans le cas des applications de recrutement avec utilisation de données biométriques, on peut supposer que les fournisseurs d'IA devront remplir toutes les obligations liées à l'article 16 et aux obligations de transparence de l'article 52 (système de reconnaissance des émotions). Les obligations liées aux systèmes d'IA utilisant la voix dépendront de la finalité recherchée et définie par fournisseur d'IA.
Que se passera-t-il pour ceux qui auront omis de déclarer l'une des obligations en prétextant la bonne foi ? C'est une des limites du modèle auto-déclaratif proposé par le règlement.

Pour la CFE-CGE, l'autoévaluation des systèmes à haut risque par les fournisseurs d'IA n'est pas suffisante dans la régulation proposée, même si les obligations et pénalités associées semblent assez contraignantes pour eux.
Nous préconisons que des autorités tierces veillent à la conformité des systèmes d'IA avant la mise sur le marché, et que ces conformités soient systématiquement fournies aux représentants des salariés lors des informations ou consultations liées à une introduction de système d'IA dans le monde professionnel.
Ces autorités devraient aussi avoir la possibilité d'auditer ces systèmes d'IA afin de vérifier la conformité des produits tout au long de leur cycle de vie.
Ceci est déjà rendu possible par la demande d'une autorité nationale compétente de l'article 16 (point j).
Il faut donc rendre obligatoires ces demandes pour les applications à haut risque concernant le monde professionnel.
Pour toutes les applications déjà sur le marché dans le domaine des RH et du monde du travail en général, celles-ci devront passer par un processus d'évaluation strict vu les dérives que nous constatons déjà en France et en Europe.

---

[1] https://www.nouvelobs.com/economie/20191029.OBS20418/recale-d-un-job-apres-un-entretien-video-vous-n-avez-peut-etre-pas-plu-a-l-ia.html
[2] https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html;jsessionid=AC45E5C2DA3EA6D4BEBC9FE46A1C36E5.2_cid297

Qu'en est-il pour les systèmes d'IA développés par un éditeur puis déployés dans l'entreprise par une équipe interne ou par une société de services ?
Qui sera responsable de l'évolution, de l'optimisation et du réglage du système d'IA dans le contexte local d'une entreprise ? Fournisseur, utilisateur, distributeur ?
De plus, pour entraîner le modèle, que cela soit en mode bac à sable ou en production, quelles seront les contraintes sur les données et qui en sera responsable au dernier niveau ? Fournisseur, utilisateur, distributeur ?
On peut supposer que le fournisseur d'IA à haut risque devra répondre aux obligations liées à la solution générique, puis que chaque entreprise utilisatrice (utilisateur d'IA) devra à son tour remplir ses obligations en termes de données et de cycle de vie du système d'IA.
Aujourd'hui, cela n'est pas clair dans la régulation proposée.
En tout état de cause, le résultat attendu pour les fournisseurs d'IA dans le chapitre 1.4.3 ne sera pas atteint :
« Les fournisseurs d'IA devraient bénéficier d'un ensemble d'exigences minimal, mais clair, créant une sécurité juridique et garantissant l'accès à l'ensemble du marché unique. »

La CFE-CGE considère que les obligations d'information pour les systèmes d'IA à haut risque sont insuffisantes pour les salariés.
L'article 13 du règlement proposé oblige les fournisseurs d'IA à communiquer aux utilisateurs des informations sous forme d'une notice d'utilisation sur son système d'IA.
La définition d'un utilisateur d'IA est donnée par l'article 3 :

« Toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel. »

Nous supposons que les salariés pourraient être considérés comme un utilisateurs de la solution au même titre que l'employeur. Les opérateurs de solution d'IA n'ont donc pas d'obligation précise de communiquer les impacts des systèmes d'IA sur les salariés et peu de salariés seront informés de l'existence d'une notice utilisation.

Nous pensons aussi qu'il aurait fallu définir une analyse relative à la protection des données (AIPD) dédiée au jeu de données des systèmes d'IA.
En effet, une AIPD au sens de RGPD couvre les données propres à la personne, mais qu'en est-il des métadonnées utilisées dans les modèles d'apprentissage des logiciels de reconnaissance d'émotion humaine utilisés par exemple dans les applications de recrutement à distance et faisant appel à des systèmes d'IA ?
De même, les processus d'anonymisation sont-ils suffisants pour garantir l'intégrité des données des personnes ?
Qu'en est-il de la durée de conservation de ces données ou métadonnées sachant que ces modèles d'apprentissage sont plus pertinents et précis si les jeux de données sont importants ?
De plus, quid des procédures de réclamation pour les salariés auprès des autorités compétentes ?

Nous pensons qu'il manque aussi dans l'article 13 la notion d'explicabilité.
La transparence des systèmes d'IA ne pourra pas être totale que si une explicabilité des systèmes d'IA est apportée.

Pour l'ensemble des modèles d'apprentissage automatique, l'explicabilité devra s'appliquer sur tous les éléments du système d'IA : jeu de données, algorithme d'apprentissage, modèle, prédiction du modèle.
Il est évident que certains systèmes d'IA basés sur des réseaux de neurones entraînent une opacité par un effet boîte noire. Il conviendra alors de s'appuyer sur les travaux en cours pour trouver la meilleurs stratégie d'explicabilité : explicabilité par construction, explications a posteriori.
En tout état de cause, il existe des solutions pour expliquer les modèles proposés et ne pas risquer d'exposer les salariés à des décisions arbitraires.

La CFE-CGC considère que la sécurité des données des salariés est fondamentale.
L'article 15 du règlement proposé vient préciser les obligations des fournisseurs d'IA en matière de robustesse et de cybersécurité.
Cependant, aucune obligation de test d'intrusion n'est faite à ces fournisseurs d'IA et on ne leur fournit aucun référentiel technique ou qualification de sécurité en annexe.
Nous considérons que le règlement ne permet à ces fournisseurs d'IA de respecter les obligations énoncées dans l'article 15.

Pour terminer, il est annoncé en propos liminaire que les droits fondamentaux des salariés seront renforcés (article 31 de la charte des droits fondamentaux) par le présent règlement.
En l'état du règlement proposé et à la suite de l'ensemble de nos remarques, la CFE-CGC s'interroge sur le renforcement réel de ces droits pour les salariés.
Pour nous, les garde-fous nécessaires à leur garantie tels que définis par l'article 31 ne sont pas suffisants.
Nous espérons que les travaux portés par le Conseil de l'Europe sur l'IA viendront compléter le règlement pour une intelligence artificielle éthique.