ethos

Ethos Engagement Paper

Responsabilité numérique des entreprises

>20 ANS | D'INVESTISSEMENT SOCIALEMENT RESPONSABLE

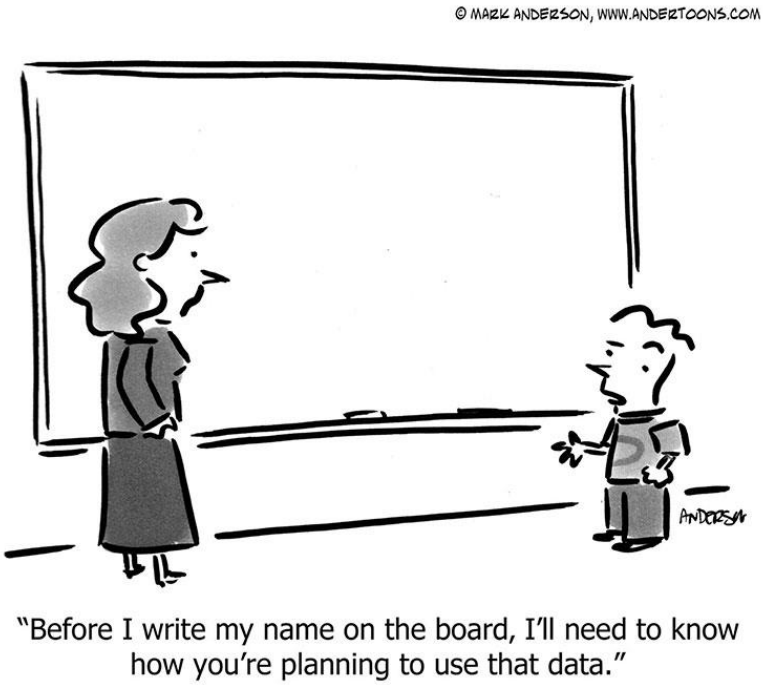
Novembre 2020

La Fondation Ethos regroupe plus de 220 caisses de pension et institutions suisses exonérées fiscalement. Créée en 1997, elle a pour but de promouvoir l'investissement socialement responsable et de favoriser un environnement socioéconomique stable et prospère.

La société Ethos Services assure des mandats de gestion et de conseil dans le domaine des investissements socialement responsables. Ethos Services propose des fonds de placement socialement responsables, des analyses d'assemblées générales d'actionnaires avec recommandations de vote, un programme de dialogue avec les entreprises ainsi que des ratings et analyses environnementales, sociales et de gouvernance des sociétés. Ethos Services appartient à la Fondation Ethos et à plusieurs membres de la Fondation.

www.ethosfund.ch

Cet engagement paper se base notamment sur les travaux dirigés par Jean-Henry Morin (Université de Genève), Johan Rochel (Ethix Lab for Innovation Ethics) et Eva Thelisson (AI Transparency Institute).
White paper, *Towards a Digital Responsibility Index*, à paraitre décembre 2020.



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Imprimé sur « RecyStar », 100% à base de vieux papiers sans azurant optique.

Sommaire

1 Introduction

1.1 Contexte

La numérisation représente l'un des trois grands enjeux sociétaux du 21ème siècle aux côtés du changement climatique et de l'accroissement des inégalités sociales. Elle offre un potentiel de développement économique considérable pour les entreprises et leurs actionnaires ce qui fait que le phénomène est souvent qualifié de 4ème révolution industrielle. Au-delà des améliorations de productivité des industries traditionnelles, la numérisation a permis en 20 ans l'émergence des géants de la technologie, communément appelé GAFAM aux Etats-Unis (Google, Amazon, Facebook, Apple et Microsoft). A fin septembre 2020, les capitalisations boursières cumulées des GAFAM atteignait près de USD 6'000 milliards et représentaient 14% de l'indice mondial MSCI World, alors que les 54 sociétés du secteur de l'énergie ont une capitalisation boursière cumulée représentant moins de 3% de ce même indice.

Cette révolution numérique ouvre également de nouveaux défis pour les entreprises et leurs actionnaires. De nombreux scandales, dont notamment l'affaire Cambridge Analytica, ont mis en lumière les abus qui peuvent résulter de l'exploitation des données privées à des fins commerciales et politiques. Cela implique de nouveaux risques éthiques, juridiques, financiers et de réputation pour les entreprises.

Au vu de l'impact de la numérisation sur l'économie et la société en générale, Ethos considère que ce thème est devenu un sujet majeur de l'investissement responsable et de l'analyse environnementale, sociale et de gouvernance (ESG). Les entreprises de tous les secteurs d'activités doivent être proactive et mettre en place des politiques de responsabilité numérique. Ce concept implique que les entreprises identifient de manière large et exhaustive les enjeux de la numérisation et mettent en place des politiques de gestion et de transition qui respectent les intérêts de l'ensemble de leurs parties prenantes (« stakeholders »).

1.2 Aperçu des attentes d'Ethos

La Fondation Ethos a pour but de promouvoir l'investissement socialement responsable et de favoriser un environnement socio-économique stable et prospère. A ce titre, elle attache une importance particulière à l'éthique des affaires et aux questions de bonne gouvernance.

Ethos plaide ainsi en faveur de la mise en place d'une stratégie de responsabilité numérique des entreprises qui soit exhaustive et qui aborde l'ensemble des problématiques énumérées au chapitre 2 de ce document. Les différentes attentes d'Ethos envers les entreprises sont détaillées au chapitre 3.

Les principes d'Ethos en matière de responsabilité numérique

1. Mettre en place un code de responsabilité numérique
2. Assurer une transparence auprès des parties prenantes sur les pratiques et l'empreinte numériques
3. Respecter les plus hauts standards en matière de traitement et de protection des données
4. Mettre en place des principes éthiques d'utilisation de l'intelligence artificielle (IA)
5. Exclure les activités sensibles liées à la numérisation
6. Assurer une transition sociale juste et responsable
7. Contribuer à réduire l'empreinte environnementale de la technologie numérique

2 Enjeux de la numérisation

2.1 Gouvernance numérique

La définition de la stratégie et l'identification des risques des entreprises doivent tenir compte de la numérisation. Cela suppose une adaptation de la gouvernance des entreprises et un suivi régulier du conseil d'administration de l'évolution technologique pouvant affecter l'entreprise. Cela concerne aussi bien les produits et services de l'entreprise que les modes de production, d'approvisionnement et de distribution. Cela implique enfin de suivre la pertinence de la stratégie en intégrant de manière régulière les risques et les opportunités liés à la numérisation.

Au vu du caractère « disruptif » et de l'évolution rapide des technologies, le conseil d'administration doit s'assurer que l'entreprise investit suffisamment de ressources dans ce domaine, tout en respectant les plus hauts standards éthiques, environnementaux et sociaux. Etant donné la complexité de la problématique, le conseil d'administration doit s'assurer d'avoir les connaissances nécessaires à la compréhension de ces enjeux. Il doit également veiller à ce que la direction gère les différents enjeux et mette en place des politiques et des procédures qui respectent les meilleures pratiques.

2.2 Transparence numérique

Les entreprises doivent informer les utilisateurs et les personnes concernées de la collecte de données à caractère personnel qu'elles effectuent. Cette transparence est indispensable, mais de loin pas généralisée. Les utilisateurs ne sont pas toujours conscients du stockage et de l'utilisation de données les concernant. Les entreprises doivent anticiper et être transparentes pour créer une relation de confiance. Les données stockées devraient être obtenues par consentement libre et éclairé (« opt in »).

Les entreprises doivent permettre aux utilisateurs de leurs services et produits de facilement consulter et interagir avec les données les concernant qui sont collectées (modifier ou effacer). Cette autonomie des utilisateurs doit être facilitée au maximum par les entreprises.

Certaines données peuvent avoir une très grande valeur. Il est donc essentiel que les entreprises qui détiennent ces données mettent en place les plus hauts standards de sécurité pour éviter une commercialisation, une fuite ou un vol de données.

Si, malgré tout, les données ont pu être exploitées par un tiers non autorisé, les entreprises doivent s'engager à informer les détenteurs de ces données sans délai. Ces derniers doivent en effet pouvoir prendre leurs dispositions pour éviter d'être victime d'une utilisation abusive de leurs données personnelles (fraude, rançonnage, utilisation des mots de passe, de cartes de crédit, profilage, etc.).

2.3 Gestion des données et politique de cyber sécurité

Les données sont devenues aujourd'hui une ressource essentielle de nombreuses entreprises. Les sociétés actives dans les secteurs technologiques et publicitaires sont les principales concernées, mais elles ne sont de loin pas les seules. En effet, toute entreprise ayant à sa disposition des données sur ses clients, employés, fournisseurs, actionnaires ou encore ses concurrents est concernée par l'utilisation, voire la commercialisation potentielle des données

L'importance des données pour les entreprises et l'économie génère un enjeu de cyber sécurité ainsi que de réglementation.

A. Réglementation en matière de protection des données

L'utilisation abusive des données privées a poussé certains Etats à imposer de nouvelles règles sur la manière dont les données sont stockées, gérées et utilisées. En Europe, le « Règlement Général sur la Protection des Données- RGPD [1] » est ainsi entré en vigueur en 2018. Cette loi européenne va bien plus loin que la plupart des législations de par le monde et reconnaît la sensibilité du sujet. Les entreprises

[1] http://gdpr-text.com/de/read/article-1/

actives au sein de l'Union européenne (UE) ou qui traitent des données de ressortissants de l'UE doivent veiller à respecter cette législation. La violation du RGPD peut conduire à des amendes significatives pouvant s'élever jusqu'à EUR 20 millions ou 4% du chiffre d'affaires global.

Après plus de 3 ans de discussions, le parlement suisse a approuvé en septembre 2020 une modernisation de la « Loi fédérale sur la protection des données (LPD)[2] » avec l'objectif de la rendre compatible avec le régime du RGPD. La loi suisse renforce le cadre de protection des utilisateurs et l'obligation d'information des entreprises. Les deux textes s'accordent sur les 7 principes liés à la récolte des données. Cela concerne la licéité, la bonne foi, la proportionnalité, la finalité, l'exactitude, la sécurité et la transparence. Les deux lois divergent cependant sur plusieurs aspects, notamment en matière de sanction. La LPD prévoit des sanctions financières largement inférieures à ce qui est prévu en Europe. Il n'est à ce stade pas certain que l'UE acceptera l'équivalence. Les entreprises suisses ont donc un intérêt certain à respecter les meilleures pratiques et les plus hauts standards règlementaires et donc s'aligner volontairement sur le RGPD.

La Californie a également légiféré dans le domaine de la protection des données avec l'entrée en vigueur au 1er janvier 2020 du California Consumer Privacy Act[3] qui reprend plusieurs éléments clés du RGPD, notamment les obligations de transparence en matière de collecte de données, de vols de données, ainsi que la protection des données privées.

B. Respect de la vie privée

L'exploitation des données par les entreprises permet de proposer des services personnalisés aux utilisateurs ou de mettre ces données à disposition de tiers à des fins commerciales. L'exploitation des données privées a en effet permis à certaines entreprises de développer de nouveaux modèles d'affaires et a notamment révolutionné l'industrie des services. La personnalisation des services qui en découle peut être positive et bénéfique pour les utilisateurs, mais elle risque bien souvent d'être effectuée au détriment du respect du caractère privé de certaines données. La publicité ciblée est un exemple d'utilisation des données souvent effectuée en violation du respect de la sphère privée des parties prenantes de l'entreprise. En moins d'une décennie, les données privées à disposition de Google et Facebook leur ont permis de devenir les principaux acteurs publicitaires, se répartissant désormais la grande part des recettes de ce secteur.

La personnalisation des services sur la base de l'utilisation de données privées devrait être un choix de l'utilisateur et pas l'option par défaut des services (« privacy by default »). Les appareils et services utilisant des données privées doivent être conçus de sorte qu'ils respectent la vie privée et ne puissent pas automatiquement exploiter les données (« privacy by design »). Ce concept est d'ailleurs un élément clé du RGPD.

C. Minimisation des données

Le principe de respect de la vie privée dès la conception nécessite que les systèmes de traitement des données soient conçus pour traiter le moins de données à caractère personnel possible. Ce principe de minimisation des données suppose de mettre en œuvre un paramétrage par défaut favorable au respect de la vie privée, de limiter l'accès aux renseignements personnels à ce qui est strictement nécessaire pour fournir le service et de mettre en place des outils permettant aux utilisateurs de mieux protéger leurs données à caractère personnel (contrôles de l'accès, cryptage, etc.).

D. Cyber sécurité

La cybercriminalité est l'un des risques majeurs que rencontrent actuellement les organisations de toutes tailles et de tous secteurs. Les attaques informatiques peuvent aller jusqu'à mettre à mal la survie même de certaines entreprises et nécessitent la mobilisation de ressources importantes pour assurer la cybersécurité et des plans de restauration des systèmes.

La cybercriminalité peut avoir plusieurs origines, allant de la malveillance à l'espionnage. Les cibles les plus fréquentes sont les organisations qui

[2] https://www.parlament.ch/centers/eparl/curia/2017/20170059/Texte%20pour%20le%20vote%20final%203%20NS%20F.pdf

[3] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

peuvent présenter un intérêt financier, comme les banques par exemple ou les organisations qui collectent et stockent un nombre important de données. Cependant, toutes les entreprises peuvent être victimes de détournements de fonds, cryptage de données contre rançon, infractions contre des systèmes de paiements ou destructions des bases de données et des programmes clés de l'entreprise.

La stratégie de cybersécurité des entreprises doit également prévoir une information rapide aux autorités et aux utilisateurs dans le cas où une cyberattaque devait compromettre la sécurité et confidentialité des données. Le RGPD prévoit ainsi que toute fuite de données doit être rapportée à l'autorité de tutelle dans les 72 heures.

2.4 Algorithmes et intelligence artificielle

L'intelligence artificielle (IA) regroupe un ensemble de théories et de techniques pour développer des programmes informatiques complexes, capables de simuler certains traits de l'intelligence humaine (raisonnement, apprentissage, langage naturel, mouvement…). L'IA se base aujourd'hui principalement sur les technologies très avancées d'apprentissage automatique (« machine learning ») qui visent à donner aux ordinateurs la capacité d'« apprendre » à partir de données, c'est-à-dire d'améliorer leurs capacités à résoudre des tâches sans être explicitement programmés pour chacune d'entre elles. La méthode qui donne le plus de résultats actuellement est le « deep learning », ou apprentissage profond. Il s'agit d'une classe d'algorithmes d'apprentissage automatique utilisant plusieurs couches (« layers ») cachées de réseaux de neurones artificiels capables d'extraire, d'analyser et de classer des caractéristiques de plus en plus abstraites des données qui leur sont présentées.

L'IA peut apporter une forte valeur ajoutée dans le domaine de la santé, de la productivité et de l'environnement. Dans le domaine médical, par exemple, la radiologie, en tant que branche hautement technologique, a commencé très tôt à se pencher sur la technologie « intelligente », ce qui a permis, par exemple, de détecter des tumeurs dans les poumons à l'aide d'un algorithme informatique depuis plus de 10 ans.[4]

Le développement rapide de ces technologies durant ces dernières années a été rendu possible par l'explosion de la puissance de calcul des machines et la croissance de la quantité de données disponibles qui alimentent les algorithmes.

Ces développements simultanés permettent aux machines de surpasser des humains dans certains domaines comme par exemple dans le jeu de go. Au-delà de la performance de l'ordinateur, c'est le fait que le programme, basé sur un réseau de neurones artificiels, a appris à jouer seul qui est significatif de l'évolution de l'IA. En effet, celle-ci se développe de façon autonome de sa programmation « humaine », ce qui ne permet plus à son concepteur d'expliquer son processus décisionnel. Une IA inexplicable peut donc potentiellement prendre des décisions qui vont à l'encontre de sa programmation ou de l'intérêt général.

L'impact potentiel des algorithmes sur nos vies quotidiennes (voiture autonome, reconnaissance faciale, assistant vocal, etc.) ouvrent un débat important sur la responsabilité et l'éthique associées à ces machines.

Il n'existe à ce jour aucune réglementation encadrant le fonctionnement de l'IA et permettant de s'assurer que ces programmes devenus autonomes et indépendants des êtres humains n'enfreignent des règles éthiques. Certaines attentes éthiques par rapport à l'IA commencent cependant à émerger autour de 4 principes (transparence, impartialité, responsabilité et impact positif).

A. Transparence

L'attente de la société civile par rapport à la transparence des systèmes d'intelligence artificielle est grande. Il est attendu aujourd'hui que les entreprises soient transparentes sur les programmes qu'elles utilisent et comment ceux-ci sont utilisés. Cela peut être le cas dans de nombreux domaines, comme les ressources humaines, les services clientèles, le diagnostic médical, l'attribution de crédits ou d'assurances

[4] https://medicalforum.ch/fr/article/doi/fms.2019.08035

ou encore la sélection de prestataires. L'éventuel recours à de telles technologies devrait être transparent. En particulier, il devrait être possible de savoir comment et pourquoi un système a pris une décision ou agit d'une telle manière (IA explicable).

B. Egalité de traitement / impartialité

Le fonctionnement des systèmes d'intelligence artificielle est souvent opaque, notamment dans le domaine du « deep learning ». Les décisions ou recommandations effectuées à l'aide de programmes faisant appel à l'intelligence artificielle peuvent également se heurter à des dilemmes moraux et éthiques. La traçabilité du mécanisme décisionnel est donc indispensable pour garantir que les décisions prises par l'IA ne souffrent d'aucun biais ethnique, de genre ou d'autres sortes (« unbiased AI »). Cette neutralité doit être à la base de la conception des programmes pouvant aboutir à des mécanismes décisionnels autonomes. Elle dépend non seulement du code de l'algorithme, mais surtout des données qui vont alimenter les algorithmes. Les entreprises ont donc la responsabilité de vérifier que les résultats ou les prédictions de l'IA ne sont pas biaisés, notamment en raison de données de base de mauvaise qualité ou peu représentatives. Si une telle neutralité ne peut pas être garantie, alors la mise en service de tels logiciels ne devrait pas être possible.

C. Responsabilité

L'impartialité de l'IA est centrale mais ne permet pas forcément de résoudre l'ensemble des dilemmes moraux auxquels pourrait être confrontée l'intelligence artificielle. Il est donc essentiel que l'intervention humaine reste en tout temps possible. En cas de problème, la question de la responsabilité doit également être clarifiée. Est-ce que la responsabilité incombe au vendeur, au propriétaire, au concepteur de l'algorithme ou passe directement au système ?

Les principes éthiques actuels ont pour conditions préalables au développement de l'IA que celui-ci soit effectué de manière responsable, sûre et utile, que les machines conservent le statut d'outils et que les personnes physique ou morales gardent à tout moment le contrôle et la responsabilité de ces machines.

D. Impact positif

L'IA peut représenter un élément central pour résoudre certains défis actuels comme le changement climatique, la perte de biodiversité, la santé ou les inégalités. L'IA devrait avant tout être développée dans le but d'avoir un impact environnemental et social positif.

2.5 Produits et services sensibles

Le rapide développement des nouvelles technologies rend possible des activités qu'Ethos considère comme incompatibles avec sa Charte et les bases du développement durable. Cela concerne en particulier les activités de surveillance par reconnaissance faciale ou visant à restreindre la liberté d'expression ainsi que le développement ou l'utilisation d'armes autonomes, la promotion de contenus sensibles ou prohibés voir même les activités visant à influencer le comportement humain de façon cachée.

A. Surveillance

Les nouvelles technologies d'analyse et de traitement des images peuvent contribuer à prévenir la diffusion sur internet de contenus violents et sensibles ou à détecter des agressions dans les lieux publics. Ces systèmes peuvent cependant être utilisés pour surveiller les citoyens et, dans le cas d'utilisation par des régimes autoritaires, nuire à la liberté d'expression et aux droits humains. Les entreprises doivent donc veiller à la manière dont leurs technologies et services sont utilisés par les clients. Elles devraient définir les limites acceptables pour garantir que leurs produits et services ne nuiront pas directement ou indirectement aux droits humains.

B. Armes autonomes

L'IA permet le développement de nouveaux types d'armements autonomes qui sélectionnent et engagent des cibles sans intervention humaine. Les enjeux sont élevés : les armes autonomes ont été décrites comme la troisième révolution dans la guerre, après la poudre à canon et les armes nucléaires.

Contrairement aux armes nucléaires, les armes autonomes ne nécessitent pas de matières premières coûteuses ou difficiles à obtenir, de sorte qu'elles pourraient rapidement arriver sur le

marché noir et aux mains de terroristes, de dictateurs cherchant à mieux contrôler leur population, de seigneurs de guerre désireux de perpétrer un nettoyage ethnique, etc. En étant dépourvues d'humanité, les armes autonomes seraient idéales pour des tâches telles que les assassinats, la déstabilisation des nations, la soumission des populations et le génocide[5].

Les entreprises doivent veiller à ce que leurs produits, technologies ou propriété intellectuelle ne contribuent pas de manière spécifique, directement ou indirectement, au développement d'armement autonome.

2.6 Impact social

Les évolutions technologiques ont et vont continuer à avoir un impact majeur sur l'emploi et les modèles sociétaux actuels. Au fur et à mesure que les systèmes d'IA se développent et que de nouveaux modèles d'affaires apparaissent, des emplois ou des types de tâches vont disparaitre ou être fortement réorganisés. Les bénéficiaires de cette révolution numérique pourraient être les entreprises et les actionnaires qui pourront bénéficier d'une augmentation de la productivité. Cependant, les gains pour les actionnaires pourraient être limités au court terme si la transition ne s'effectue pas de manière responsable. En particulier, le système de prévoyance suisse pourrait souffrir si le nombre d'actifs diminue drastiquement ou que le développement de l'économie de services (« gig economy ») transforme les employés en entrepreneur indépendants (« uberisation »).

Pour assurer une transition juste, il est essentiel de mettre en place des politiques d'entreprise qui garantissent la responsabilité des entreprises par rapport aux suppressions et aux déplacements d'emplois, comme des programmes de reconversion, de formation continue et des possibilités de changement d'emploi. A ce titre, une veille technologique permet d'anticiper les évolutions techniques et les besoins correspondant en compétences. Cette veille permettrait ainsi d'assurer une transition responsable des compétences.

Les systèmes d'IA, associés à la transition plus large vers l'économie numérique, exigeront que les travailleurs à tous les niveaux et dans toutes les professions aient accès à la sécurité sociale et à la formation continue tout au long de leur vie pour rester employables. Il est de la responsabilité des États et des entreprises de trouver des solutions qui assurent à tous les travailleurs, dans toutes les formes de travail, le droit et l'accès aux deux.

En outre, dans un monde où la précarisation et l'individualisation du travail s'accroît, tous les travailleurs, quelle que soit leur forme de travail, doivent avoir des droits sociaux et fondamentaux identiques et solides. Tous les systèmes d'IA doivent prévoir un contrôle et un équilibre permettant de vérifier si leur déploiement et leur augmentation vont de pair avec les droits des travailleurs tels qu'ils sont définis dans les dispositions garantissant les droits de l'homme, les conventions de l'Organisation internationale du Travail (OIT) et les conventions collectives.

2.7 Impact environnemental

La révolution numérique actuelle a également des enjeux environnementaux importants à l'heure où notre société doit réduire drastiquement ses émissions de gaz à effet de serre pour limiter le réchauffement climatique. La révolution numérique voit cependant son empreinte carbone croître exponentiellement et son impact environnemental augmenter fortement.

Une étude de GreenIT.fr[6] a chiffré que, en 2019, l'univers numérique était constitué de 34 milliards d'équipements (smartphones, télévisions, écrans d'ordinateurs et objets connectés, etc.). En tenant compte de l'ensemble du cycle de vie des équipements informatiques, la contribution de l'empreinte numérique à l'empreinte de l'humanité est loin d'être négligeable. Toujours selon GreenIT.fr, ces 34 milliards d'équipements informatiques, les différents réseaux (11 milliards de box DSL/fibre, 10 millions d'antennes relais 2G à 5G et environ 200 millions d'autres équipements actifs réseau WAN) ainsi que les quelques milliers de centres informatiques (« data center ») (avec plus 67 millions de serveurs hébergés)

[5] https://futureoflife.org/open-letter-autonomous-weapons/

[6] https://www.greenit.fr/wp-content/uploads/2019/10/2019-10-GREENIT-etude_EENM-rapport-accessible.VF_.pdf

contribuaient en 2019 à l'empreinte écologique de l'humanité de la manière suivante :

- 4.2% de la consommation d'énergie primaire (6800 TWh)
- 3.8% des émissions de gaz à effet de serre (1400 millions de tonnes de GES)

La crise du coronavirus, qui a conduit plus de 3 milliards de personnes à rester confinées chez elles et à faire appel à des services informatiques, n'a fait qu'augmenter cette tendance avec une explosion encore plus marquée des flux de données.

Au vu de la croissance effrénée de l'utilisation d'objets connectés, des réseaux informatiques et d'une économie centrée sur les données, l'empreinte numérique va encore augmenter exponentiellement ces prochaines années. Il est nécessaire que les entreprises, les consommateurs et les États agissent dans ce domaine.

3 Attentes d'Ethos

Ethos attend des entreprises dont elle est actionnaire ou vis-à-vis desquelles elle agit en tant que représentant d'autres investisseurs institutionnels qu'elles veillent à appliquer les principes suivants.

Les principes d'Ethos en matière de responsabilité numérique

1. Mettre en place un code de responsabilité numérique
2. Assurer une transparence auprès des parties prenantes sur les pratiques et l'empreinte numériques
3. Respecter les plus hauts standards en matière de traitement et protection des données
4. Mettre en place des principes éthiques d'utilisation de l'IA
5. Exclure les activités sensibles liées à la numérisation
6. Assurer une transition sociale juste et responsable
7. Contribuer à réduire l'empreinte environnementale de la technologie numérique

Principe 1 : Mettre en place un code de responsabilité numérique public

Le conseil d'administration doit veiller à ce que l'entreprise se dote d'un code de responsabilité numérique (« Digital Responsibility Code ») couvrant les principaux enjeux auxquels l'entreprise fait face en pondérant leur matérialité par rapport au secteur d'activité et aux spécificités de l'entreprise. Le conseil d'administration a la responsabilité de couvrir l'ensemble des enjeux numériques et de vérifier annuellement que la couverture est pertinente. Le code devrait couvrir au minimum les enjeux suivants :

- **Gouvernance** : La manière dont les enjeux numériques de l'entreprise sont gérés doit être prévue dans le code. Le conseil d'administration doit traiter de la thématique de manière régulière et s'assurer que ses membres comprennent les opportunités, les risques et les enjeux de la numérisation. La direction générale devrait nommer un responsable dédié aux questions de numérisation (« chief digital officer ») et avoir la responsabilité de la mise en œuvre du code et de son respect.
- **Veille technologique** : Le code doit mentionner la manière dont le conseil d'administration et la direction de l'entreprise surveillent les évolutions technologiques pertinentes aux activités de la société. Cela suppose une veille constante et une prise en compte des évolutions dans la définition de la stratégie et des risques de l'entreprise.
- **Cybersécurité** : Le code devrait inclure une section sur la façon dont l'entreprise gère ce risque. La stratégie de cybersécurité devrait être revue par le comité d'audit et la direction devrait nommer un « Chief Security Officer ». Au vu de la sensibilité de la thématique, il est évident que les détails de la politique de sécurité doivent rester confidentiels. Cependant, il est important que l'entreprise confirme qu'elle procède de manière régulière à des audits de sécurité et qu'une sensibilisation de tous les utilisateurs de systèmes est effectuée.
- **Respect de la vie privée et des données** : Les entreprises doivent confirmer dans leur code qu'elles s'engagent à respecter la protection des données et la vie privée de leurs parties prenantes (voir principe 3 ci-dessous).
- **Règles éthiques d'utilisation de l'intelligence artificielle (IA)** : Le code doit prévoir une section détaillée ou faire référence à des principes plus précis sur les règles d'utilisation de l'IA (voir principe 4 ci-dessous).
- **Responsabilité sociale de la transition numérique** : L'impact de la transition numérique sur les employés de l'entreprise doit également faire partie du code (voir principe 6 ci-dessous).
- **Principe de réduction de l'empreinte environnementale numérique** : Les entreprises doivent stipuler dans leur code de responsabilité numérique la manière dont les impacts environnementaux des biens et services numériques ainsi que des données et réseaux de l'entreprise sont minimisés (voir principe 7 ci-dessous).

Principe 2 : Assurer une transparence auprès des parties prenantes

La mise en œuvre du code de responsabilité numérique devrait être vérifiable par les parties prenantes de l'entreprise (clients, fournisseurs, actionnaires, société civile, etc.). Cela nécessite une transparence complète, facilement accessible sur le site internet et dans le rapport annuel et compréhensible, notamment sur les points suivants :

- Le code de responsabilité numérique devrait être **disponible sur internet** et dans les langues des pays dans lesquels l'entreprise déploie son activité.
- Les utilisateurs doivent **savoir quelles données sont collectées** et pouvoir les consulter. Les lieux de stockage des données doivent également être communiqués, ainsi que la manière dont les données privées sont cryptées.
- Les règles de confidentialité des données doivent être **intelligibles et facilement accessibles** par les utilisateurs.
- **L'utilisation d'IA** dans les processus décisionnels doit être clairement communiquée.
- Une attaque compromettant la sécurité des données doit être **communiquée sans délai.** Les utilisateurs dont les données ont été compromises doivent également être informés.

Principe 3 : Respecter les plus hauts standards en matière de traitement et protection des données

Les sociétés doivent appliquer les plus hauts standards dans ce domaine pour minimiser les risques légaux et financiers. Les entreprises devraient notamment se conformer aux points suivants :

- Les produits et services des entreprises doivent être conçus de manière à pouvoir en tout temps respecter la vie privée des utilisateurs (« **privacy by design** ») et toujours offrir un mode par défaut respectueux de la vie privé (« **privacy by default** »).
- Les personnes dont les données sont collectées doivent expressément donner leur consentement libre et éclairé avant toute utilisation de leurs données (« **opt in** »).
- Les entreprises ne doivent pas utiliser les données privées dans le cadre d'une surveillance des comportements.
- Aucune donnée ne doit être collectée et stockée sans une raison déterminée (finalité).
- Les entreprises doivent respecter le principe d'une collecte et d'une possession strictement minimale des données (proportionnalité). Elles devraient mettre en place des technologies leur permettant de s'assurer du respect de ce principe (Technologies améliorant la confidentialité ou TAC) dans le cadre de leurs services en ligne et de leur site internet.

Principe 4 : Mettre en place des principes éthiques d'utilisation de l'IA

L'utilisation de l'IA nécessite la mise en place d'un code d'éthique et de déontologie qui devrait aborder les principes suivants :

- Les entreprises qui développent des systèmes d'IA doivent s'assurer que ceux-ci sont développés dans le but d'avoir **un impact positif pour la société et la planète**.
- Les technologies autonomes peuvent refléter et renforcer certains biais ou préjugés selon la qualité de la programmation et des données qui alimentent les algorithmes. **Les entreprises doivent garantir l'égalité de traitement et la non-discrimination par l'IA** qu'elles développent et utilisent. Cette dernière ne devrait pas avoir des effets injustes sur les personnes, en particulier ceux liés à des caractéristiques sensibles telles que l'ethnicité, le sexe, la nationalité, le revenu, l'orientation sexuelle, les capacités et les orientations politiques ou religieuses (« unbiased AI »).
- Les entreprises doivent pouvoir **expliquer à tout moment le fonctionnement de leurs systèmes d'IA** et pouvoir tracer le processus décisionnel (IA explicable).
- L'utilisation d'une décision de l'IA par l'entreprise devrait faire l'objet d'une **approbation humaine** et être soumise à un droit de recours (« human in the loop »)
- Les entreprises doivent s'assurer qu'il est possible à tout moment de choisir un **mode manuel** dans les programmes et que ce mode a le dessus sur le mode autonome.

- Les entreprises **doivent tester de manière régulière** la performance et la qualité de leurs systèmes d'IA.
- Les entreprises doivent s'assurer que le développement de l'IA est responsable, sûr et utile, que **les machines gardent le statut d'outil** et que les personnes conservent le contrôle et la responsabilité de ces machines.

Principe 5 : Exclure les activités sensibles liées à la numérisation

Les entreprises doivent définir quelles activités liées à l'IA doivent être proscrites. Ethos est d'avis que les systèmes de gestion des risques des entreprises doivent prendre en compte que de tels biens, services ou programmes ne doivent pas contribuer, notamment, au développement ou au fonctionnement des activités suivantes :

- Systèmes de surveillance des personnes qui vont à l'encontre des droits fondamentaux
- Systèmes visant à limiter ou réduire la liberté d'expression
- Systèmes conçus pour créer des addictions
- Armes autonomes
- Systèmes contribuant à manipuler un marché ou à influencer de manière cachée le comportement d'un marché ou d'une population
- Systèmes diffusant des contenus sensibles, racistes, sexistes, illégaux ou permettant l'accès à des contenus et activités inappropriés aux mineurs

Principe 6 : Assurer une transition sociale juste et responsable

Pour assurer une transition juste, il est essentiel de mettre en place des politiques qui garantissent la responsabilité des entreprises par rapport aux déplacements ou aux suppressions d'emplois :

- Les entreprises doivent prévoir des programmes de développement personnel et de reconversion en offrant des systèmes de formation continue, ainsi que des possibilités de changement d'emploi.
- Les entreprises doivent prévoir des systèmes d'IA au service de l'humain et limiter les réductions d'emplois en répartissant de manière équitable les gains de productivité.
- Dans le cas de l'utilisation des données des collaborateurs ou de l'IA dans la gestion des ressources humaines, les employés doivent être informés et avoir le droit d'exiger la transparence des décisions et des résultats des systèmes d'IA ainsi que des algorithmes sous-jacents.[7]
- Le développement de nouveaux modèles d'affaires grâce à la transformation numérique et l'IA ne devrait pas permettre aux entreprises de se soustraire à leurs obligations envers les employés ou servir à contourner les conventions collectives ou les systèmes de sécurité sociale.
- Les entreprises doivent conduire une activité de veille technologique pour planifier leurs besoins en compétences et privilégier les reconversions et les transitions de compétences.
- Les entreprises doivent consacrer une partie de leur rapport de durabilité à expliquer leurs démarches pour préserver l'emploi (nombre de reconversions, nombre d'heures de formation continue, nombre d'emplois supprimés ou remplacés par des systèmes, mesures de redistribution des gains de productivité).

Principe 7 : Contribuer à réduire l'empreinte environnementale du numérique

La révolution numérique a un impact environnemental majeur, en particulier si l'on tient compte de l'empreinte des produits connectés sur l'ensemble de leur cycle de vie et de l'explosion de la quantité de données stockées et consommées. L'utilisation à large échelle d'algorithmes complexes implique également une puissance de calcul toujours plus importante et, par conséquent, une consommation d'énergie exponentielle. Les entreprises peuvent toutes agir

[7] Top 10 principles for Ethical artificial intelligence, UNI Global Union, Principe 1

pour réduire l'empreinte environnementale de leurs solutions numériques. Il s'agit en particulier de :

- Augmenter la durée de vie des équipements et allonger la durée de garantie légale.
- Réduire les besoins des services numériques par leur écoconception.
- Favoriser le remploi et le recyclage des produits numériques.
- Prévoir l'utilisation de centres de stockage de données conçus de manière efficiente et alimentés par de l'énergie renouvelable.
- Sensibiliser les clients sur l'utilisation limitant au maximum l'empreinte environnementale des produits connectés produits par l'entreprise.
- Publier des données pertinentes dans le rapport de durabilité comme par exemple le recyclage, la durée de vie moyenne des produits connectés, l'énergie consommée par les systèmes informatiques, les quantités de données stockées ou d'autres indicateurs environnementaux pertinents afin de permettre une comparaison et une évolution dans le temps.
- Evaluer régulièrement et tenir compte de l'impact environnemental lors de la décision d'internaliser ou d'externaliser les services informatiques.

Ethos
Place de Pont-Rouge 1
Case postale 1051
1211 Genève 26
Suisse

T + 41 (0)22 716 15 55
F + 41 (0)22 716 15 56

Bureau de Zurich
Bellerivestrasse 3
8008 Zurich
Suisse

T + 41 (0)44 421 41 11
F + 41 (0)44 421 41 12

info@ethosfund.ch
www.ethosfund.ch