Quel cadre juridique pour une IA de confiance ?

Dès le 9 décembre 2023[1], les médias ont relayé l'annonce d'un accord du trilogue européen sur des règles globales du futur IA Act.

Si cette information a été perçue plutôt comme une bonne nouvelle, notamment par les défenseurs des libertés et des droits fondamentaux, d'autres voix se sont élevées pour dénoncer le choix de l'UE de réglementer l'intelligence artificielle au lieu de soutenir les entreprises européennes dans leurs efforts d'innovation.

En réalité, ce règlement s'inscrit dans un ensemble plus large de plusieurs textes européens cohérents et constituant une traduction législative de la stratégie numérique de l'Union européenne.

Cette stratégie européenne tient compte d'un constat préoccupant pour l'Europe :
- Une course à l'innovation en matière d'IA et un retard de l'UE dans ce domaine
- Une accélération des usages de l'IA nécessitant une protection renforcée des libertés et droits fondamentaux pour prévenir les risques de dérives dans les usages.

Partant de ce constat, le législateur européen s'est fixé pour objectif de répondre à ce double impératif : assurer un équilibre entre le soutien à l'innovation (I) et la protection des personnes contre les risques de l'IA (II)

I. Les instruments de soutien à l'innovation en matière d'IA

l'IA fait l'objet d'une course à l'innovation à l'échelle mondiale. Une étude publiée par l'OMPI en 2019[2] révèle une forte accélération depuis 2013 du nombre de demandes de brevets en lien avec des technologies de l'IA. Mais les entreprises européennes sont quasi absentes de la liste des principaux déposants. Le palmarès est dominé par les Etats-Unis et la Chine[3].

Cette domination du secteur par les Etats-Unis et la Chine ne signifie pas pour autant que l'Europe n'innove pas. Au contraire, de nombreuses Startup émergent en Europe comme partout ailleurs dans le monde et lancent sur le marché des technologies innovantes en matière d'IA. Cependant, aucune n'arrive à se développer suffisamment au point de pouvoir concurrencer les GAFAM et représenter une alternative pour les utilisateurs. Deux explications à cette situation que le législateur européen entend corriger.

La première explication réside dans la difficulté de disposer d'un volume de données suffisant pour entrainer et perfectionner les algorithmes qui sont au coeur des systèmes d'intelligence artificielle.

---

[1] https://www.lemonde.fr/economie/article/2023/12/09/ai-act-l-union-europeenne-pionniere-dans-la-regulation-de-l-intelligence-artificielle_6204830_3234.html

[2] https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

[3] https://fr.statista.com/infographie/24982/innovation-intelligence-artificielle-nombre-brevets-ia-machine-learning-par-entreprises/

La deuxième, intrinsèquement liée à la première, réside dans les stratégies déployées par les G.AF.AM. pour maintenir leur domination du marché et bloquer l'accès aux données pour les concurrents potentiels.

Outre le déploiement d'investissements financiers conséquents[4], ces obstacles pourraient être surmontés par deux types de mesures : l'accès aux données (A) et le rétablissement du libre jeu de la concurrence (B)

A. L'accès aux données

Deux règlements européens le Data Act[5] et le Data Governance Act[6] ont été adoptés en vue de faciliter pour les entreprises européennes :

- le partage des données captées par les objets connectés
- l'accès à des données particulières détenues par le secteur public

1. L'accès aux données captées par les objets connectés

1.1. Constat : on assiste à une multiplication d'objets connectés dans tous les domaines de la vie, allant de la montre connectée pour le suivi du bien être ou de la santé, du GPS dans la voiture permettant d'analyser le trafic en temps réel pour détecter l'itinéraire le plus rapide, au tracteur connecté muni de nombreux capteurs collectant d'innombrables données sur l'état des sols ou la météo.

1.2. Problème : la valeur issue de l'exploitation des données n'est pas partagée. Ces données restent dans les mains de ceux qui les captent de façon accessoire à l'objet ou service vendu. Les utilisateurs du service ou de l'objet n'ont aucun contrôle sur ces données et ne peuvent les transférer à d'autres entreprises.

1.3. Solution : adoption du Data Act, règlement européen dont l'objectif est de permettre une répartition équitable de la valeur tirée de l'utilisation des données issues des objets connectés. Il prévoit des mesures visant notamment à :
- accorder aux utilisateurs d'objets connectés un contrôle sur leurs données
- favoriser le transfert de ces données entre fournisseurs de services
- protéger les PME contre les clauses contractuelles abusives. Des clauses contractuelles type seront élaborées par la Commission.

A noter : exclusion de la directive de 96 sur le droit des producteurs des bases de données
Calendrier : adoption le 15 novembre 2023, entrée en vigueur 20 mois après son entrée en vigueur.

[4] https://digital-strategy.ec.europa.eu/fr/news/commission-awards-eu41-million-contract-develop-infrastructure-common-european-data-spaces

[5] https://data.consilium.europa.eu/doc/document/PE-49-2023-INIT/fr/pdf

[6] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020PC0767

2. L'accès à certaines données détenues par les établissements publics

2.1. Constat : la directive de 2016 sur l'open data a permis aux entreprises d'accéder aux données ouvertes détenues par les établissements du secteur public. Mais certaines données ne sont pas concernées par la directive. Il s'agit **de données protégées** (informations commerciales confidentielles, propriété intellectuelle, données personnelles) dont la divulgation risque de porter atteinte aux droits des tiers.

2.2. Problème : comment rendre ces données disponibles sans porter atteinte à la protection dont font elles font l'objet, soit au titre du RGPD, soit au titre de droits de propriété intellectuelle?

2.3 Solution : adoption du Digital Governance Act (DGA), règlement européen visant à compléter la directive de 2016 sur l'open data. Ce règlement prévoit des mécanismes permettant de :

- favoriser le partage sécurisé des données personnelles et non personnelles par la mise en place de structures d'intermédiation entre les détenteurs de données et les utilisateurs potentiels de ces données

- faciliter la réutilisation de certaines catégories de données détenues par des organismes du secteur public (informations commerciales confidentielles, propriété intellectuelle, données personnelles, etc.)

Condition pour les structures d'intermédiation : une certification obligatoire pour les fournisseurs de services d'intermédiation de données. Elle sera facultative pour les organismes pratiquant l'altruisme en matière de données

Calendrier du DGA : entrée en vigueur le 23 juin 2022, applicable depuis septembre 2023.

B. Le rétablissement du libre jeu de la concurrence

1. L'adaptation de l'article 22 du règlement sur les concentrations

1.1. Constat
L'innovation dans le domaine de l'IA en Europe existe. L'UE dispose d'un niveau élevé de compétences en matière d'IA. Cependant, ces entreprises sont rachetées par les géants de la tech dans le cadre d'opérations de concentration dès qu'ils détectent un potentiel de croissance, et ce, dans le but de :

- récupérer les compétences
- s'approprier les technologies développées
- neutraliser la concurrence

Ces opérations de concentration dites « killer acquisitions » ne concernent d'ailleurs pas que les entreprises européennes mais toutes les entreprises présentant un potentiel soit en termes de nombre d'utilisateurs donc de données, soit en termes technologique.

Exemples de killer acquisitions permis les nombreuses acquisitions[7] :

- achat par Meta : Instagram, Whatsapp
- achat par Alphabet : Deepmind, YouTube, Double-click, Androïd, Nest , Picasa, Waze
- achat par Microsoft : Linkedin, Skype

1.2. Problème

Comment permettre à la commission de contrôler tout projet de concentration susceptible de produire des effets significatifs » sur la concurrence dans l'Union même pour les opérations n'atteignant pas les seuils prévus par l'article 22 du règlement sur les concentrations?

1.3 Solution :

Le 31 mars 2021[8], la Commission européenne publie de nouvelles lignes directrices sur l' interprétation de l'article 22 du règlement du 20 janvier 2004. Cette nouvelle interprétation lui permettra de contrôler désormais tous les projets de concentration qui lui seront soumis par les Etats membres, même si les opérations n'atteignent pas les seuils prévus par le règlement.

2. L'adoption d'un texte ad hoc visant les grandes plateformes ou « gatekeepers »

2.1. Constat :

Parallèlement aux phénomènes des concentration, les géants du net qui bénéficient déjà d'une position de monopole mettent en oeuvre des pratiques anti-concurrentielles visant à empêcher les concurrents d'accéder au marché de la donnée.

2.2. Problème

La sanction de ces comportements qualifiés d'abus de position dominante intervient après de longues procédures pouvant prendre plusieurs années[9] [10]. Il était impératif de mettre en place un mécanisme de contrôle a priori permettant aux autorités d'empêcher la mise en oeuvre de ces pratiques?

2.3. Solution :

Le Digital Market Act (DMA)[11] : Il s'agit d'un règlement ayant pour objectif de limiter et contrôler le pouvoir exercé par les plateformes appelées « gatekeepers » sur le marché numérique.

---

[7] https://fr.statista.com/infographie/9418/gafam-rachats-et-acquisitions-de-startups-ia/

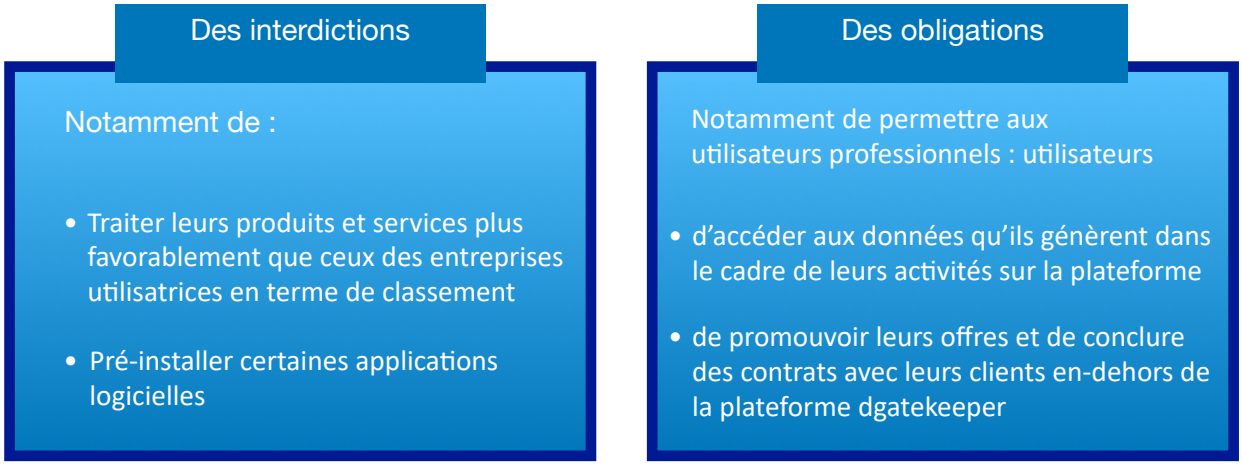
[8] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52021XC0331(01)

[9] Affaire google shopping : https://curia.europa.eu/juris/document/document.jsf?text=&docid=250881&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=826021

[10] Affaire google Android : https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220147fr.pdf

[11] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R1925

Le DMA prévoit pour ces gatekeepers :



Les sanctions : en cas de manquement, ils encourent une amende de 10% de leurs CA mondial et 20% en cas de récidive. 22 plateformes ont déjà été désignées comme gatekeepers.
L'autorité de contrôle est la Commission

Calendrier : le DMA est entré en vigueur depuis en novembre 2022, applicable aux grandes plateformes depuis le 03/07/2023, à partir de mars 2024 pour les autres plateformes.

II. Les instruments de protection des libertés et droits fondamentaux

A. Protection générale contre les traitements automatisés

1. Par le RGDP et la directive police

1.1. Principes
- Interdiction de traiter les données biométriques (article 9 du RGPD)
- Droit de ne pas faire l'objet une décision résultant d'un traitement automatisé (article 22 du RGPD)

1.2. Conséquences
- Interdiction de l'utilisation de la reconnaissance faciale dans l'espace public
- Droit de s'opposer à une décision résultant d'un traitement automatisé[12]

1.3. Exceptions
- Consentement express de la personne concernée
- Dans l'Intérêt public, en cas de nécessité absolue

[12] CJUE 16/03/2023 SCHUFA : « le RGPD consacre un « droit » de la personne concernée de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé, y compris le profilage » l'avocat général

2. Par le Digital service Act (DSA)[13]

2.1 Principe général de *transparence algorithmique* *(article 27 du règlement)*

2.2. Conséquences

2.2.1. Pour les personnes, le droit de :

- comprendre comment et pourquoi certains contenus leur sont suggérés
- pouvoir modifier les paramètres des algorithmes de recommandation

2.2.2. Obligation pour les plateformes :

- d'expliquer le fonctionnement des algorithmes qu'elles utilisent pour recommander certains contenus publicitaires en fonction du profil des utilisateurs.
- de proposer un système de recommandation de contenus non-fondé sur le profilage
- de fournir les algorithmes de leurs interfaces à la Commission et aux autorités nationales compétentes

B. Protection spécifique contre les risques liés aux SIA

L'IA Act[14] est un projet de règlement européen visant à encadrer la mise sur le marché de systèmes d'IA avec une approche fondées sur les risques.

1. Principe général de prévention des risques posé par l'IA Act

Quatre niveaux de risque ont été définis :

- **Risque inacceptable** : les SIA considérés comme une menace évidente pour la sécurité, les moyens de subsistance et les droits des personnes seront interdits. Ex. Notation sociale

- **Risque élevé** : SIA utilisés dans le transport, l'éducation, la formation, l'emploi, la santé, composants de produits de sécurité, le service public...

  Obligation de mettre en place :
  une procédure de contrôle de conformité avant la mise sur le marché
  Des mesures de surveillance humaine continue après la mise sur le marché (système équivalent à la procédure de mise sur le marché de médicaments)

- **Risque limité** : SIA assortis d'obligations de transparence lors de leur utilisation. Exemple : cas d'interaction avec un agent conversationnel (Chatbot)

- **Risque minimal ou nul** : Pas d'obligation mais il est recommandé de réaliser une analyse d'impact pour pouvoir confirmer l'absence de risque

Obligations de transparence spécifiques pour l'IA générative. Exemple : obligation de le préciser si le contenu proposé a été généré par par l'IA.

[13] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2065

[14] https://www.consilium.europa.eu/fr/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

2. Deux régimes de responsabilité

2.1. **Responsabilité générale du fait de produits**
Projet de modernisation de la directive du 25 juillet 1985 sur les produits défectueux à l'ère numérique[15].

2.1.1 Objectif : étendre la notion de produit aux mises à jour des logiciels, aux systèmes d'intelligence artificielle ou aux services digitaux (robots, drones, ou les systèmes domestiques intelligents)

Il s'agit d'une responsabilité objective, c'est à dire sans faute, seule le caractère défectueux du produit doit être produit par la victime.

Un produit doit être considéré comme étant défectueux lorsqu'il représente un danger pour le consommateur en général. Les défauts peuvent être liés à plusieurs facteurs, tels que la conception du produit, ses instructions, ses caractéristiques techniques, ses éventuels usages ainsi que les effets que d'autres produits peuvent avoir sur lui. Sa durée de vie et ses capacités d'apprentissage peuvent aussi être mises en cause[16].

2.1.2. Conséquences, permettre aux victimes de :

- prétendre à des dédommagements pour des dégâts psychologiques établis sur le plan médical. Ils doivent nécessiter un traitement médical ou psychologique.et réparation des dommages corporels, des dommages aux biens ou des pertes de données causées par des produits défectueux (drôles, robots)
- demander une compensation en cas de destruction ou de piratage de données irréversible (ex. suppression de documents sur un disque dur)

2.2. Responsabilité spécifique du fait des SIA

2.2. 1. Principe
Régime de responsabilité pour faute prévu par une proposition de directive européenne « relative à l'adaptation des règles en matière de responsabilité civile extra-contractuelle au domaine de l'intelligence artificielle (Directive sur la responsabilité en matière d'IA)[17].

2.2.2. Objectif
Ensemble de règles visant compléter le projet de règlement IA Act pour permettre aux victimes « de dommages causés par le résultat d'un système d'IA ou l'incapacité de ce système à produire un résultat qui aurait dû l'être » d'intenter une action civile en réparation contre le fournisseur du système d'IA en cause.

---

[15] https://single-market-economy.ec.europa.eu/system/files/2022-09/COM_2022_495_1_EN_ACT_part1_v6.pdf

[16] https://www.europarl.europa.eu/news/fr/headlines/economy/20231023STO08103/mise-a-jour-des-regles-europeennes-pour-les-produits-defectueux

[17] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52022PC0496

2.2.3 Spécificité

Allègement de la charge de la preuve pour les victimes et leurs ayant droits grâce à :

- présomption réfragable de non-respect des obligations de vigilance prévues par l'IA Act par le fournisseur (article 3). Possibilité pour les juridictions de contraindre le défendeur à divulguer les éléments de preuves nécéssaire à une action en réparation

- Présomption réfragable d'un lien de causalité en cas de faute du défendeur et le résultat produit (article 4).

Conclusion :

S'appuyant sur l'effet structurant et la portée internationale du RGPD, l'UE privilégie la voie du Règlement pour traduire sur le plan législatif la volonté de bâtir une stratégie européenne pour relever les nombreux défis soulevés par l'intelligence artificielle. L'analyse de ces différents textes permet de relever que, parallèlement à la recherche de cet équilibre entre le soutien à l'innovation et la protection des personnes, un troisième objectif apparaît en continu : limiter autant que possible la fragmentation du marché européen numérique et construire un marché unique de la donnée.

Synthèse