Transparence et réglementation européenne

L'innovation technologique constitue bien souvent un véritable défi pour le législateur. Pris au dépourvu, il peine couramment à en saisir la complexité technique quand il n'adhère pas pleinement au laissez-faire de l'économie libérale. Dans ce texte, Nayla Glaise fait le point sur les récents textes juridiques européens relatifs à l'économie numérique, plus promptes à protéger le bon fonctionnement du marché que les droits des travailleurs.

L'Acte sur l'intelligence artificielle, l'acte sur le marché numérique, l'acte sur les services numériques, l'acte sur la gouvernance des données, la proposition de directive relative à l'amélioration des conditions de travail dans les plateformes numériques… ces dernières années ont été marquées par l'adoption de multiples lois, dont le but est d'encadrer les algorithmes et de mieux protéger les données des citoyens.

Décryptage des avancées obtenues et des lacunes de cette « vague » législative.

Le RGPD : Règlement général de protection des données

Entré en vigueur le 25 mai 2018, il est considéré comme la législation la plus complète au monde en matière de protection des données, en créant un large éventail de nouveaux droits concernant les données personnelles pour toutes les personnes physiques de l'Union européenne (UE).

Toute organisation qui "traite" les données à caractère personnel de personnes situées dans l'UE doit se conformer à la réglementation, même si elle n'y est pas elle-même située. L'employeur qui exploite des données personnelles est tenu de respecter plusieurs obligations, notamment : recueillir l'accord de la personne concernée, l'Informer de son droit d'accès, de modification et de suppression des informations collectées.

La loi sur l'Intelligence Artificielle ou Artificial Intelligence Act

Elle est une des premières adoptées par un grand organisme de réglementation dans le monde. Cette loi classe les applications de l'IA en trois catégories de risques :

Premièrement, les applications et les systèmes qui créent un risque inacceptable, tels que les scores sociaux gérés par le gouvernement, comme ceux utilisés en Chine, sont interdits.

Ensuite, les applications à haut risque, telles qu'un outil de balayage de CV qui classe les candidats à l'emploi, sont soumises à des exigences légales spécifiques.

Enfin, les applications qui ne sont pas explicitement interdites ou répertoriées comme étant à haut risque ne sont généralement pas réglementées.

À l'instar du RGPD, la loi européenne sur l'IA pourrait devenir une norme mondiale, déterminant dans quelle mesure elle a un effet positif plutôt que négatif sur votre vie, où que vous soyez. Elle fait déjà des émules à l'échelle internationale : ainsi le Congrès brésilien a-t-il adopté, fin septembre, un projet de loi qui crée un cadre juridique pour l'IA.

Compte tenu de la puissance des Big Tech, une gouvernance démographique et anticipatrice de l'IA n'est réalisable que si tous les acteurs sociaux s'engagent systématiquement. Les représentants des travailleurs, comme les autres, devraient participer pleinement aux discussions et leurs contributions être intégrées de manière significative.

La proposition de loi comporte plusieurs lacunes et exceptions. Avec une approche fondée sur le risque, l'impact de l'IA sur les droits fondamentaux, les droits des travailleurs et l'environnement, ainsi que la nécessité d'anticiper son évolution future, ne sont pas suffisamment pris en compte.

Les utilisations à haut risque sont autorisées pour autant que le fournisseur, sur la base d'une auto-évaluation, soit en mesure de cocher les cases de ce qui est une liste de contrôle essentiellement procédurale. La liste des utilisations à haut risque de l'IA couvre des aspects essentiels de la vie et du travail des citoyens européens (de l'éducation à l'emploi et à l'accès aux services, au crédit, à la justice, etc.) et peu de choses sont faites pour les limiter ou les interdire. Les fournisseurs n'ont pas à éliminer le risque, ils sont simplement censés le remarquer, le surveiller et fournir des informations à son sujet. La raison pour laquelle certaines utilisations sont placées dans cette catégorie n'est pas décrite et semble donc arbitraire.

Les risques résiduels sont considérés comme "acceptables" tant que les mesures de gestion des risques sont suffisantes et que le système d'IA est utilisé conformément à sa destination ou dans des conditions de "mauvaise utilisation raisonnablement prévisible". La seule obligation est leur communication

La liste des utilisations interdites est courte, semble définitive et aucune disposition n'est prévue dans le règlement pour la mettre à jour et l'étendre.

Malgré le fait que le règlement IA classe parmi les utilisations à haut risque "l'emploi, la gestion des

travailleurs et l'accès au travail indépendant", nous demandons une directive spécifique sur l'utilisation de l'IA dans l'emploi dans le but de mieux prendre en compte les questions liées à la responsabilité de l'employeur dans la prévention des risques liés à l'IA, les règles sur la protection des données, la transparence et l'explication des algorithmes, la surveillance et le rôle des organisations syndicales.

Proposition de directive relative à l'amélioration des conditions de travail dans les plateformes numériques

Le 9 décembre 2021, la Commission européenne a présenté la proposition de directive relative à l'amélioration des conditions de travail des travailleurs des plateformes. Les dispositions prévoient, entre autres, la mise en place d'une présomption réfragable de salariat pour les travailleurs des plateformes sous certains critères, complétée par un renversement de la charge de la preuve.

La proposition introduit des lois qui obligeront les plateformes de travail numériques à montrer le fonctionnement de leur algorithme aux travailleurs et à leurs syndicats sur les questions relatives aux conditions de travail et à la gestion du travail. Jusqu'à présent, les algorithmes ne font pas l'objet d'un examen public sous prétexte de protéger le secret commercial.

Cette directive, si elle est adoptée, constitue une amélioration notable sur la transparence des algorithmes même si nous considérons qu'il y a moyen de l'améliorer sur ce point notamment avec une définition plus globale de la gestion des algorithmes pour ne pas limiter sa portée qu'aux systèmes entièrement automatisés.

La loi sur les Données ou le Data Governance Act

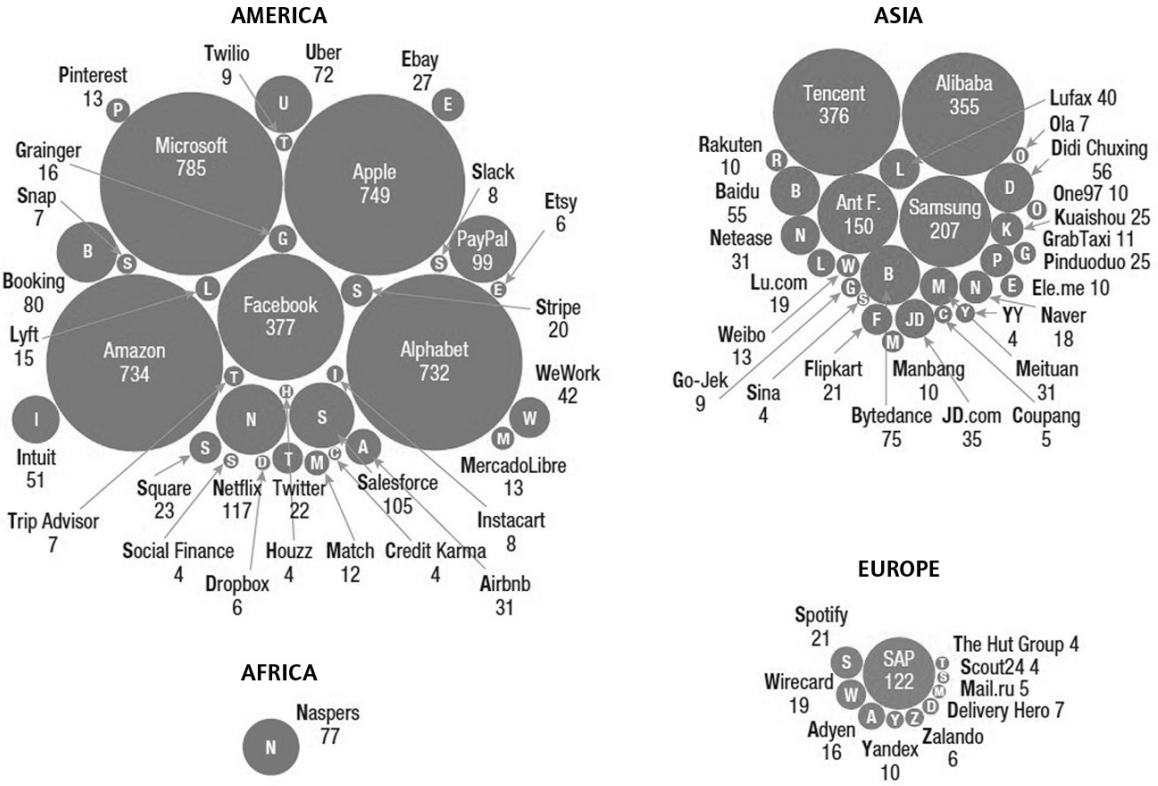
« Si le RGPD concerne la protection des données personnelles, d'autres données en disent aussi beaucoup sur nous, comme celles générées par l'utilisation d'appareils connectés ou celles produites par les logiciels qui les font tourner. Faut-il les protéger comme des données personnelles ? Ou sont-elles un bien commun, quitte à faire l'impasse sur leur propriété intellectuelle ? C'est la voie suivie par la Commission européenne avec le projet de Data Act. Il tend ainsi à nous rendre le contrôle et la propriété de ces données, aujourd'hui dans les mains des fabricants. Les fichiers contenus dans les PC, Smartphone ou autres tablettes ne sont pas concernés : ces appareils ne font que les stocker (ou les diffuser si c'est un média), elles ne les produisent pas (et l'utilisateur les contrôle déjà).

Le Data Act ne concerne que des données brutes, pas celles retravaillées, traitées et exploitées par le fabricant qui contiendront son savoir-faire. Il prévoit le droit de les porter vers une autre entreprise en vue d'un service (on pense à du big data, à l'intelligence artificielle…). Les entreprises ne pourront pas s'échanger les données sur leurs produits et sur leur utilisation dans le dos de l'utilisateur sans une demande de sa part »[1]

Toutefois, le RGPD gardera toujours préséance si les données visées par le Data Act ont un caractère personnel. Les Pme bénéficieront d'une protection contractuelle particulière : toute clause relative à un échange de données qui serait jugée en leur défaveur serait déclarée caduque en cas de conflit. Les très petites entreprises sont même exemptées de partager les données d'utilisation de leurs produits ou logiciels. Tout le monde ne pourra pas en bénéficier : en seront exclues les organisations qui tombent sous la coupe du Digital Market Act (Dma), comme Google ou Facebook qui s'approprient déjà les données sur leurs marchés et les verrouillent.

Lois sur les marchés et les services numériques : Digital Market Act (DMA) et Digital Service Act (DSA)

Afin de garantir que les plateformes numériques n'imposent des conditions inéquitables aux entreprises ou discriminatoires, la Commission a adopté deux propositions de réglementation : la loi sur les services numériques (Dsa) et la loi sur les marchés numériques (Dma).



Répartition géographique des plateformes mondiales (capitalisation en milliards de dollars) [Source UNCTAD 2019]

Ces propositions approuvées sous la présidence française ont deux objectifs de nature économique et éthique : freiner la stratégie hégémonique des grands acteurs (principalement américains) du numérique et rechercher une modération plus efficace des contenus.

Le Digital Service Act vise à responsabiliser tous les intermédiaires, mais surtout les plus grandes plateformes. Elles devront modérer le contenu qu'elles hébergent sur leurs sites web et coopérer avec les autorités des États membres. Le Digital Market Act imposera des contraintes spécifiques aux acteurs "systémiques", avec pour objectif principal d'empêcher les Gafam de profiter de leur taille et de leur capitalisation boursière pour fausser la concurrence.

Directive sur la Sécurité des réseaux et de l'Information : Network and Information

Security 2 (NIS2)

Entrée en vigueur le 3 juin dernier, cette nouvelle directive est une mise à jour de la directive de 2016 sur la sécurité des réseaux et de l'information (NIS 2). Élargie à la gestion de crise et aux réponses aux incidents, elle comprend des dispositions visant à réglementer l'utilisation efficace du chiffrement, les tests de sécurité et la gestion et la divulgation des risques. Les organisations doivent signaler les incidents de cybersécurité aux autorités compétentes dans les 24 heures. Point crucial, le texte garantira la sécurité tout au long des chaînes d'approvisionnement, en introduisant la responsabilité des cadres supérieurs en cas de non-respect des obligations en matière de cybersécurité.

NIS 2 s'inscrit ainsi dans une stratégie numérique européenne plus large avec, comme nous l'avons vu, les lois sur les services numériques, sur le marché numérique et sur l'intelligence artificielle. Au sein de cette vague législative, NIS 2 se concentre sur la modernisation de la sécurité des services critiques, et sera liée à la future loi sur la cyber-résilience. Couvrant des secteurs tels que l'énergie, les transports, les marchés financiers, la santé et les infrastructures numériques, la directive renforcera les exigences de sécurité en imposant une approche de gestion des risques et des mesures de surveillance exigeantes pour les autorités nationales. En outre, le texte vise à harmoniser les régimes de sanction dans les États membres tout en contribuant à accroître le partage d'informations et la coopération en matière de gestion des cybercrises au niveau national et européen.

Dans sa « Boussole numérique pour 2030 » la Commission européenne utilise le concept d'«écosystème de confiance » affirmant que les citoyens devraient faire confiance à la technologie, et que la fiabilité est également une condition préalable à son adoption. Ces multiples législations européennes ont une énorme influence sur la politique mondiale sur le traitement des données notamment aux Etats Unis et en Amérique du Sud. Mais dans toutes ces propositions numériques de la Commission européenne, nous identifions un problème récurrent : l'emploi est systématiquement négligé. L'accent est mis sur le marché et non sur la protection des droits des travailleurs, ainsi dans tous ces textes l'abus de pouvoir algorithmique n'est pas traité.

Notes de bas de page :

[1]
https://www.lemonde.fr/idees/article/2022/04/13/le-data-act-entend-rendre-le-controle-et-la-propriete-des-donnees-industrielles-sans-frais-et-en-temps-reel_6121994_3232.html

Pour citer cet article :

Nayla Glaise, « Transparence et réglementation européenne », *Silomag 15*, juillet 2022. URL : https://silogora.org/transparence-et-reglementation-europeenne/