Chloé Berthélémy, Conseillère politique, European Digital Rights (EDRi)

Mais que fait l'Europe ?

La reconnaissance faciale se déploie à travers tout le continent. Souvent dans l'opacité, sans débat public. Parfois même de manière illégale. En réponse l'Union européenne (UE) a adopté en 2024 l'acte sur l'intelligence artificielle. Il vise à encadrer ces nouvelles technologies qui risquent de nous faire basculer dans une société de surveillance de masse. Malheureusement, au terme de nombreux compromis politiques, la loi échoue largement à enrayer la prolifération de ces technologies liberticides.

ÇA PARTAIT MAL : QUAND L'APPROCHE ÉCONOMIQUE DOMINE

En avril 2021, la Commission européenne révèle sa proposition législative pour un acte européen sur l'intelligence artificielle (AIA). Les mesures de protection des droits fondamentaux y sont modestes, largement inefficaces face aux risques présents et futurs que posent ces systèmes technologiques. Pas de surprise néanmoins, car la nature des débats précédents la publication annonçaient déjà la couleur.[1] L'objectif politique affiché et assumé est de réguler *a minima* le marché de l'intelligence artificielle (IA) en plein essor. Le mode d'ordre, c'est l'innovation.
Empêtrée dans un discours qui place l'UE dans une course technologique effrénée contre les États-Unis et la Chine et devant déjà « rattraper notre retard », la Commission favorise une régulation légère de l'IA. C'est un marché qu'il ne faudrait pas accabler par un trop-plein d'obligations juridiques contraignantes et coûteuses à respecter. Les start-ups européennes doivent pouvoir innover librement, devenir compétitives sur le marché mondial, et ainsi, contribuer à « *la souveraineté numérique européenne* ». On verra plus tard pour les coûts sociétaux, politiques et environnementaux.

Le texte donne par conséquent une grande place à l'auto-régulation et choisit une approche basée sur les risques posés par les systèmes d'IA. Quatre niveaux de risque (négligeable, limité, élevé et inacceptable) sont établis plus ou moins explicitement pour classer les types d'IA ou leur champ d'application (éducation, emploi, police, etc.). Les développeurs eux-mêmes sont chargés d'évaluer dans quelle catégorie tombent leurs systèmes. Ce seront donc les entreprises, avant tout motivées par le profit, qui déterminent quelles exigences elles doivent ou non respecter. Et il leur appartiendra aussi de juger si elles ont suffisamment satisfait à ces exigences fixées en matière de traitement des données, d'exactitude, de transparence, etc. Les mécanismes de supervision, qui par défaut interviennent a posteriori de la mise sur le marché et l'utilisation de l'IA, échoueront à systématiquement détecter les abus, les erreurs et les défauts de conformité et donc à prévenir les dommages.

En outre, les obligations ne sont vraiment pas strictes. Pour les IA à risques limités, un peu de transparence vis-à-vis des personnes qui interagissent avec elles. Pour les systèmes à hauts risques, il s'agit principalement de se mettre en conformité avec des standards techniques, définis par des organismes de standardisation de droit privé. Ces règles sont le fer de lance de la proposition de la Commission européenne et pourtant selon sa propre évaluation, elles ne toucheraient que de 5 à 15 % des systèmes d'IA mis sur le marché de l'UE.

Là s'illustrent toutes les lacunes de la loi. D'abord son approche purement économique qui traite l'IA comme un simple produit industriel passe sous silence un grand nombre de risques. Pensons notamment au renforcement des inégalités structurelles, des rapports de pouvoir, des

1 https://la-rem.eu/2024/03/loi-europeenne-sur-lia-une-reglementation-digne-de-con%ef%ac%81ance/

impacts environnementaux, des formes nouvelles d'exploitation sur le marché du travail, ou encore de l'extractivisme dans les pays du Sud Global. Sans parler de la dépendance croissante vis-à-vis des entreprises de la tech et la plus grande acceptation sociale de la surveillance de masse. Deuxièmement, elle ne tient pas compte de la complexité des systèmes d'IA et de l'importance du contexte pour pouvoir évaluer leurs impacts sur les droits fondamentaux et sur la société plus globalement. En se concentrant sur les critères à remplir du fournisseur de l'IA, et non des utilisateurs, le mécanisme est fondamentalement mal adapté pour identifier les risques dans le contexte du déploiement. Par exemple, un système de reconnaissance faciale déployé dans un centre commercial peut satisfaire aux exigences techniques spécifiées dans la loi, tout en constituant une violation importante des droits fondamentaux en compromettant la protection des données, violant la vie privée ou l'interdiction de discriminer.

L'ACTE SUR L'IA ET LA SURVEILLANCE BIOMÉTRIQUE : PROTECTEUR OU PERMISSIF ?

Au cours des négociations entre le Parlement européen et le Conseil des États-Membres, quelques règles ont tout de même été introduites pour pallier cette zone de quasi-non-droit pour les utilisateurs d'IA à hauts risques. Dans le texte final, on trouve donc des obligations en matière d'accessibilité (en particulier pour les personnes en situation de handicap) et de transparence (inscription dans un registre européen des buts de l'usage de l'IA et de sa logique de fonctionnement). De plus, les déployeurs devront mener une étude d'impact sur les droits fondamentaux et en publier un résumé. Les personnes affectées par les systèmes d›IA, quant à elles, obtiennent quelques voies de recours, bien que certainement peu efficaces dans la pratique.

Ces mesures supplémentaires sont très loin d'être suffisantes et sont truffées d'exceptions. La transparence, oui, mais que pour les autorités publiques car le « secret des affaires » doit être préservé avant tout. Il n'y a pas de comptes à rendre non plus dans les domaines migratoire et de contrôle des frontières. L'UE poursuit son régime d'exceptionnalisme envers les migrant·es et demandeur·ses d'asile, qui se retrouvent à nouveau avec moins de protection que le reste de la population. Enfin, la police, elle aussi, est exemptée de tout devoir de transparence envers le public et peut même déployer une IA à haut risque avant d'en avoir obtenu l'autorisation au nom de la « sécurité publique ».

Mais qu'en est-il des IA présentant des risques inacceptables ? Si demain la police belge veut déployer de la reconnaissance faciale dans les rues, que dit le règlement ? Malgré sa liste de systèmes d'IA interdits, le cadre légal européen reste globalement permissif vis-à-vis de toute une série d'usages, dont les effets néfastes sont pourtant bien connus et documentés. À nouveau, à peine a-t-on établi une règle, qu'on en restreint immédiatement la portée en créant de multiples exceptions.

Le recours à « l'identification biométrique à distance en temps réel », telle que la reconnaissance faciale déployée sur les passant·es d'un centre-ville pour repérer celleux qui figurent une liste de surveillance, n'est interdit que pour la police dans les espaces accessibles au public.[2]

Toutefois elle pourra l'utiliser dès lors qu'il s'agit de retrouver des personnes disparues ou des victimes d'enlèvement ou de la traite sexuelle, en cas de « menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques », ou encore pour prévenir une menace terroriste.

2 https://www.laquadrature.net/2024/01/19/le-reglement-europeen-sur-lia-ninterdira-pas-la-surveillance-biometrique-de-masse/

Non seulement ces motifs peuvent être facilement abusés et leur définition élargie, comme c'est déjà le cas des politiques antiterroristes en Europe qui mènent systématiquement à la sur-répression des communautés musulmanes, mais la liste peut rapidement s'allonger dans le futur.

Pourtant les expérimentations montrent déjà tous les effets dystopiques de ces systèmes. En plus de faire des erreurs souvent lourdes de conséquences (surtout pour les personnes racisées[3]) en dépit de taux d'exactitude élevés affichés[4], ils décuplent le pouvoir étatique de surveillance. Les personnes qui tentaient d'éviter de passer devant les caméras de Londres, ou qui exerçaient leur droit légitime de leur résister en se couvrant le visage, ont été arrêtées et, dans certains cas, condamnées à une amende.[5]

Pire encore, au lieu de tracer des lignes rouges face aux risques sociétaux en jeu, l'AIA ouvre potentiellement la voie à la légalisation de certaines utilisations de ces systèmes pour la première fois dans l'UE. Les exceptions en série donnent le signal que certaines formes de surveillance biométrique de masse ou de discrimination alimentée par l'IA sont légitimes dans certaines circonstances.

C'est le cas des systèmes de reconnaissance des émotions – ces IA qui prétendent par exemple pouvoir déterminer sans aucune validation scientifique crédible si quelqu'un·e ment - qui sont interdits seulement sur les lieux de travail et dans l'enseignement. Sauf pour des « raisons médicales ou de sécurité ». Ils sont aussi permis dans le cadre des missions de police. Une exception en cache une autre.

Il est prohibé d'utiliser des méthodes de catégorisation biométrique (qui peuvent supposément classer les personnes sur la base de leurs caractéristiques physiques) pour déduire la race, les opinions politiques, l'orientation sexuelle, et autres. Mais c'est tout à fait possible pour le genre, le statut de santé, ou la situation de handicap. Et encore une fois, l'interdiction ne concerne pas la police ni les autorités d'immigration. Par conséquent, dans les faits, il sera possible sous droit européen d'autoriser la police à classer les personnes filmées par des caméras de vidéosurveillance en fonction de leur couleur de peau. Cela semble impossible à réconcilier avec la législation européenne en vigueur contre la discrimination.

Ceci témoigne de la volonté de l'UE de laisser les personnes les plus marginalisées de la société devenir les cobayes de tests technologiques les plus intrusifs et déshumanisants.

Malgré quelques outils donnés au combat contre la surveillance biométrique[6], l'AIA est passé à côté d'une grande opportunité de protéger les personnes, les communautés, la société et l'État de droit contre ses dangers. Cette loi met en évidence les fondements idéologiques de l'UE, concentrés sur le marché intérieur et la croissance économique. Elle ne met pas les droits fondamentaux au premier plan, même si c'est ce qu'elle prétend.

3 https://londonnewsonline.co.uk/news/police-facial-recognition-system-has-potential-to-entrench-racial-bias/

4 La police londonnienne a déclaré que leur système était efficace à 70 % pour repérer les suspects recherchés et qu'il identifiait faussement une personne recherchée dans un cas sur mille. Mais le professeur Pete Fussey de l'université d'Essex qui a mené un examen indépendant a constaté que le système n'était exact que dans 19 % des cas. https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras

5 https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

6 https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/#part-1