

Classement

Une technologie qui se met en garde contre elle-même



Voitures autonomes, chirurgie et médecine, ChatGPT: l'intelligence artificielle est désormais dans notre quotidien.

© DALL·E 2

Par Monica Fahmy et Ruth Brüderlin

ChatGPT, voitures autonomes, IA en médecine: l'intelligence artificielle est entrée dans notre quotidien. Et avec elle se posent de nombreuses questions éthiques et juridiques. L'intelligence artificielle fascine, facilite notre quotidien et pose en même temps à l'humanité des défis juridiques complexes. Même ChatGPT est de cet avis, comme l'a découvert le député démocrate américain Ted Lieu, l'un des trois seuls députés à être diplômé d'une université en informatique. Dans son commentaire publié en janvier 2023 dans le New York Times sur le thème «L'avenir avec l'IA», il a laissé ChatGPT écrire le premier paragraphe.

Le robot y décrit un monde dans lequel des armes commandées par des ordinateurs capables d'apprendre circulent dans les rues et décident elles-mêmes quand elles doivent faire feu. Et voici ce que ChatGPT écrit: «Les progrès rapides de l'IA ont clairement montré qu'il est maintenant temps d'agir pour s'assurer que cette technologie soit utilisée d'une manière sûre, éthique et utile à la société.» Pour sa part, le député américain indique ressentir à la fois de l'enthousiasme et de la peur vis-à-vis de l'IA, surtout celle «qui n'est pas surveillée ou réglementée».

Une chose est claire: il faut des lois. L'évolution en matière d'intelligence artificielle est fulgurante. Des questions de responsabilité se posent déjà aujourd'hui dans différents domaines. Mais les processus politiques sont difficiles et longs.

Qui est responsable en cas d'erreur de diagnostic?

Prenons l'exemple du secteur de la santé. La Food and Drug Administration américaine a autorisé les outils d'IA, notamment pour le diagnostic d'attaques et d'hémorragies cérébrales, la détection de fibrillation auriculaire et l'interprétation d'images IRM du cerveau. Cela comporte des risques juridiques, par exemple sur la question de la responsabilité en cas d'erreur de diagnostic ou si l'IA effectue un traitement inutile, voire nuisible. Qui est responsable? L'entreprise qui fabrique l'IA? Si oui, peut elle être tenue pour responsable, par exemple lorsque son siège se trouve dans un pays qui ne

donne pas suite à une demande d'entraide judiciaire de la Suisse? L'institution qui utilise l'IA, par exemple l'hôpital, est-elle responsable? Quels employés? Le responsable informatique qui a acquis la technologie? Le personnel médical qui l'a utilisé? Ou l'IA elle-même?

Dans sa publication L'intelligence artificielle dans le quotidien médical, la Fédération des médecins suisses (FMH) écrit que le médecin peut être tenu pour responsable de ce qu'il a identifié, influencé et dont il est responsable en raison de ses compétences professionnelles. La décision de recourir à des systèmes d'IA pour le diagnostic et le traitement d'un patient, ou d'y renoncer, en fait partie.

Aux États-Unis, les fabricants d'IA peuvent être considérés comme responsables. Le cabinet d'avocats The Eisen Law Firm (Cleveland, Ohio), spécialisé dans les erreurs médicales, estime que l'IA n'est pas un acteur médical agréé et ne peut donc pas être poursuivie juridiquement en cas d'erreur, mais ajoute que l'IA est aussi un produit et «si un produit ne fonctionne pas et cause des dommages, les victimes peuvent poursuivre le fabricant en justice». Une autre possibilité pour les patients serait de porter plainte pour faute professionnelle parce que le médecin a mal utilisé l'IA ou s'est trop fié à elle.

La responsabilité en cas de collision avec une voiture autonome

L'utilisation de l'IA est déjà un standard dans l'industrie automobile, des fonctions de conduite autonome aux systèmes avancés d'assistance à la conduite. Ce point a été abordé dans «[Jusletter.ch](#)», une revue juridique suisse en ligne. Sous le titre «Intelligence artificielle: nécessité d'agir en droit suisse», les auteurs écrivent: «La clarification de la responsabilité civile en cas de dommage et la garantie de la responsabilité pénale constituent un défi central.»

Qui doit assumer la responsabilité lorsqu'un véhicule autonome provoque un accident? Le conducteur, le constructeur automobile ou les développeurs du logiciel d'IA? Les lois et réglementations ne sont pas les mêmes dans tous les États. Si un véhicule autonome est autorisé dans un pays où les règles sont plus laxistes, mais qu'il provoque un accident dans un pays où les règles sont plus strictes, il serait intéressant de suivre le débat juridique.

En outre, des questions éthiques se posent. On peut par exemple imaginer que le logiciel de bord décide de lui-même, dans une situation d'urgence, qu'il est préférable de heurter un piéton plutôt qu'un autre usager de la route. D'un point de vue purement rationnel, cela pourrait avoir du sens. Mais cela serait-il aussi éthiquement défendable?

Qu'en est-il de la protection des données?

La protection des données représente un tout autre problème. Les systèmes d'IA collectent d'immenses quantités d'informations sur les patients, les automobilistes et les passagers, ainsi que sur chaque personne utilisant internet. On ne sait pas qui est responsable de la protection des données. Des normes uniformes, des règles claires pour leur collecte, leur utilisation et leur stockage font défaut. Le Préposé fédéral à la protection des données et à la transparence (PFPDT) renvoie la responsabilité aux personnes qui traitent les données. Elles doivent veiller à ce que les dispositions de la loi sur la protection des données soient respectées, en particulier les principes définis à l'article 4. Elles doivent aussi veiller à l'exactitude des données (art. 5) et à leur sécurité (art. 7).

Silvia Böhlen, du service de communication du PFPDT, reconnaît que c'est justement lors du traitement de grandes quantités de données que le risque existe que des données prétendument anonymes, par exemple de patients, puissent être identifiées. De plus, les données sur l'état de santé ne doivent pas être transmises aux assurances ou aux employeurs. «Les responsables doivent en tenir compte lors de la mise en place et de l'exploitation des systèmes, par exemple dans le cadre des

principes privacy by design et privacy by default explicitement ancrés dans la loi révisée sur la protection des données», explique-t-elle.

La loi sur la protection des données a été délibérément formulée de manière technologiquement neutre, explique Silvia Böhlen, de sorte que les principes formulés restent valables à tout moment. «Avec la révision totale de la loi sur la protection des données, qui entrera en vigueur le 1er septembre 2023, le législateur et le monde politique en ont tenu compte.»

L'homme rend l'IA raciste et misogyne

Les systèmes d'IA apprennent à partir des données dont ils sont nourris. Mais ils intègrent aussi, directement ou indirectement, des distorsions. Les technologies d'IA continuent d'être principalement développées par des hommes. Et elles utilisent principalement des données occidentales. L'IA reprend donc automatiquement les clichés et les préjugés, ce qui entraîne une inégalité de traitement entre les hommes et les femmes, ainsi qu'avec les personnes issues d'autres cultures.

Les auteurs d'une étude publiée en février 2021 par la chancellerie du canton de Zurich, la Faculté de droit de l'Université de Bâle et l'ONG Algorithmwatch.ch considèrent également la discrimination comme un risque majeur: «Les données peuvent être erronées ou incomplètes et reproduire ainsi d'anciens modèles de discrimination, voire en établir de nouveaux. Le manque de traçabilité est également considéré comme problématique. Il est parfois presque impossible de comprendre comment les algorithmes d'apprentissage parviennent à leurs résultats.»

Nadja Braun Binder est professeure de droit public à l'Université de Bâle et figure parmi les auteurs de l'étude. Interrogée sur les défis juridiques liés à l'IA dans l'État et l'administration, elle cite par exemple l'assurance des garanties de procédure: «Si une autorité utilise des processus d'apprentissage automatique pour prendre une décision, il faut s'assurer qu'elle puisse motiver sa décision.» Lors de l'utilisation de l'IA dans le secteur public, il faut en outre identifier quelles bases juridiques sont nécessaires. «Et il faut clarifier quelles sont les dispositions à prendre pour que les exigences légales puissent être satisfaites», ajoute-t-elle.

Dans d'autres parties du monde, les choses avancent: le 27 janvier 2023, les Etats-Unis et l'Union européenne ont signé un «accord administratif sur l'intelligence artificielle pour le bien commun». Il vise à faire progresser l'IA de manière «responsable». Florent Thouvenin est juriste et, en tant que professeur extraordinaire, titulaire de la chaire de droit de l'information et de la communication à l'Université de Zurich, il déclare: «En l'état actuel des choses, contrairement à l'EU AI Act, il faut partir du principe qu'aucune réglementation globale ne sera édictée en Suisse.»

Il pense plutôt que le droit en vigueur dans notre pays sera adapté de manière ponctuelle, par exemple pour garantir la transparence, pour appréhender la discrimination et dans le domaine de la responsabilité. «Il semble largement admis que ces règles doivent être neutres sur le plan technologique, explique-t-il. C'est-à-dire qu'elles ne doivent pas s'appliquer uniquement en cas de dommage causé par l'utilisation de l'IA ou lorsque quelqu'un est victime de discrimination, mais qu'elles couvrent tout dommage et toute discrimination, indépendamment du fait que la cause soit un humain, une machine ou une interaction entre un humain et une machine.»

Mauvais diagnostics, décisions erronées, discrimination et violations de la protection des données: l'intelligence artificielle est humaine. Et elle dispose d'un potentiel de nuisance considérable. Début avril, Europol, l'autorité policière européenne basée à La Haye, a expressément mis en garde contre les possibilités d'utilisation criminelle de ChatGPT. Grâce à sa capacité à imiter la manière dont un groupe de personnes communique, cette technologie peut être utilisée de manière optimale pour la fraude, le phishing, la désinformation et d'autres crimes dans le domaine de la cybercriminalité.

Des mesures ont été prises. L'Italie est le premier pays à avoir bloqué l'accès à ChatGPT, le 30 mars 2023, avec effet immédiat, invoquant comme motif la violation de la protection des données. L'autorité italienne de protection des données a ainsi suivi la recommandation de ChatGPT. Le robot avait écrit dans le New York Times: «Il est maintenant temps d'agir. Sinon, les risques de l'IA pourraient l'emporter, de loin, sur ses avantages.»

«Il est maintenant temps d'agir. Sinon les risques de l'IA pourraient l'emporter, de loin, sur ses avantages.»

Cinq domaines à risques de l'IA

C'est dans ces domaines que Florent Thouvenin, juriste et professeur à l'Université de Zurich, voit les plus grands défis juridiques liés à l'utilisation de l'intelligence artificielle:

Transparence: Le droit doit garantir la reconnaissance et la traçabilité de l'utilisation de l'IA. Les personnes doivent pouvoir reconnaître lorsqu'elles interagissent avec un système d'IA (par exemple un chatbot) et comprendre dans une certaine mesure comment une décision a été prise, par exemple lors de la sélection de candidatures pour un emploi.

Confidentialité/protection des données: Les défis de l'IA peuvent être relevés par la législation actuelle en matière de protection des données. Mais les solutions ne sont pas toujours judicieuses et la protection des données peut également constituer un obstacle majeur au développement et à l'utilisation de l'IA.

Discrimination: La Suisse n'a pas de loi générale contre la discrimination ou l'inégalité de traitement. Seules les discriminations fondées sur le sexe ou un handicap sont interdites. Les discriminations liées à l'origine, par exemple, ne peuvent pas être combattues. Les nouvelles normes doivent être neutres sur le plan technologique, c'est-à-dire qu'elles doivent couvrir les discriminations causées par les hommes et les machines.

Manipulation: L'IA peut influencer les personnes dans leur pensée et leur action. Les systèmes de recommandation de contenus, comme sur YouTube, en sont un exemple typique. Il n'est pas clair si et dans quelles conditions une influence peut être qualifiée de manipulation, y compris sur le plan juridique. Des recherches fondamentales sont nécessaires dans ce domaine.

Responsabilité: Les normes actuelles en matière de responsabilité doivent être adaptées afin de couvrir également de manière adéquate les dommages causés par l'utilisation de systèmes d'IA. Cela vaut en particulier pour le droit de la responsabilité du fait des produits (LRFP), mais aussi pour la responsabilité extracontractuelle générale.