FAIRE PROGRESSER LA SCIENCE POUR LA SOCIÉTÉ : SANTÉ, MIGRATIONS ET TECHNOLOGIES
SOMMET DES ACADÉMIES DES SCIENCES DU S7 | 6-8 MAI 2025 | OTTAWA (ONTARIO), CANADA

TECHNOLOGIES AVANCÉES ET SÉCURITÉ DES DONNÉES

DÉFINITION DE LA QUESTION

Les deux dernières décennies ont vu s'élargir de façon remarquable la quantité, la portée, l'utilité et les finalités des systèmes de collecte des données1 ainsi que des technologies de traitement et d'archivage, notamment les systèmes d'IA, qui utilisent des données pour faire des déductions ou effectuer des opérations. Selon le Rapport scientifique international sur la sécurité des systèmes avancés d'IA (*International Scientific Report on the Safety of Advanced AI*), les possibilités qu'offre l'IA de rendre service à l'humanité sont contrebalancées par plusieurs risques potentiellement graves2. Par conséquent, une approche multiniveau, holistique, centrée sur l'humain et intelligente de la gouvernance et de la réglementation doit être employée pour éviter d'étouffer les avantages de ces technologies tout en s'attaquant aux problèmes qu'elles posent. Dans ce document, l'expression « sécurité des données » est utilisée pour désigner cet ensemble de préoccupations interconnectées.

CONTEXTE

Ainsi que l'a documenté le groupe d'experts responsable du *Rapport scientifique international sur la sécurité des systèmes avancés d'IA*, l'énorme potentiel que recèlent les progrès anticipés de l'IA, notamment en ce qui concerne la disponibilité et la qualité des données produites pour des raisons légitimes telles que la recherche dans des domaines essentiels à l'amélioration de la condition humaine, est contrebalancé par les risques potentiellement graves de dérapages, de violations des droits de la personne, de perturbation du marché du travail, de perte de moyens de subsistance et de dommages climatiques/environnementaux que pose la mauvaise utilisation intentionnelle de ces données (p. ex. la désinformation et d'autres menaces pour la démocratie). De grandes incertitudes subsistent quant à l'ampleur des perturbations à prévoir et à leur chronologie, mais le manque de préparation des secteurs scientifique, informatique et politique de la société fait consensus. Suivant le principe de précaution, il serait par conséquent essentiel d'investir dans la sécurité des données ainsi que dans les recherches qui permettraient d'exploiter et de maîtriser adéquatement les systèmes d'IA avancés. Des innovations sociales, politiques et technologiques seraient nécessaires à tous les niveaux pour identifier et maximiser les avantages collectifs et pour s'assurer que les garde-fous requis pour bien anticiper, prévenir et atténuer les risques sont continuellement maintenus et actualisés.

La mise en place de mesures de gouvernance et de réglementation à l'échelle nationale et internationale, et la coordination ces mesures, jouera un rôle important dans l'atténuation de ces risques. Les organismes de gouvernance et de réglementation doivent définir leurs attentes et des lignes directrices techniques et organisationnelles afin de s'assurer que les risques et les avantages sont correctement identifiés et pris en compte. Ils doivent mettre en place des régimes de conformité et d'application réactifs qui protègent les personnes et la planète sans étouffer l'innovation et la prospérité économique. Nous considérons qu'une gouvernance et une réglementation efficaces, tout autant que des politiques innovantes, doivent être mises en place afin que les bénéfices soient partagés plus équitablement entre les différents groupes de la société et que soit établi le cadre nécessaire pour favoriser une innovation responsable et une utilisation de la technologie qui permette d'atteindre des objectifs sociétaux souhaitables. Les

1 Ces systèmes comprennent les téléphones intelligents, les dispositifs portables et autres dispositifs personnels, les systèmes de domotique et d'automatisation industrielle, les compteurs intelligents, les dispositifs médicaux, les véhicules autonomes et les systèmes de surveillance publics et privés.

2 International AI Safety Report (DSIT 2025/001, 2025), https://www.gov.uk/government/publications/international-ai-safety-report-2025

parties qui doivent veiller à la sécurité des données incluent les praticiens (p. ex. le secteur privé et le secteur public), les chercheurs universitaires et le public, à l'échelle de l'individu comme des groupes (auto-) identifiés.

RECOMMANDATIONS EN MATIÈRE DE POLITIQUES

RECOMMANDATION 1

Comme les technologies avancées sont susceptibles de rapidement devenir des infrastructures essentielles, il est d'une importance capitale que leur gestion ne soit pas totalement abandonnée aux entreprises qui les développent, aux marchés et à l'adaptation de la société, et que la responsabilité de cette gestion ne soit pas transférée aux particuliers, qui seraient obligés de s'éduquer et de se former sur les risques qu'ils courent. Les entreprises, les marchés et l'éducation jouent tous un rôle crucial, mais une gouvernance et une réglementation efficaces sont indispensables :

a. pour protéger les personnes touchées par les possibilités et les effets différentiels des nouvelles technologies;
b. pour faire en sorte que ces technologies ne continuent pas de concentrer le pouvoir économique et politique et d'accentuer les inégalités existantes.

RECOMMANDATION 2

Réglementer la collecte et la conservation des données représente un défi de nature réglementaire et éthique. Ensuite, une fois les données recueillies, deux aspects très importants de l'utilisation des données méritent une réglementation minutieuse : la prévention des fuites de données involontaires et l'assurance de la qualité des données. La réglementation en émergence, comme la *Loi sur l'IA de l'UE*[3], reconnaît ces préoccupations, mais comporte certaines lacunes. Par exemple, cette réglementation recommande :

a. la pseudonymisation des données pour éviter les fuites involontaires – bien que les experts en protection de la vie privée aient montré que cela est souvent insuffisant et que des mesures plus fortes comme la protection différentielle de la vie privée sont nécessaires;
b. de veiller à ce que le profil démographique des données utilisées pour faire des déductions utiles (p. ex. pour former un modèle d'IA) corresponde à la population pour laquelle elles sont créées – mais ne précise pas comment cela pourrait se faire sans violer la confidentialité des données.

Pour combler ces lacunes, les décideurs politiques doivent collaborer plus étroitement avec les experts, y compris les universitaires, et avec les membres du public associés à ces données. Une communication bilatérale doit guider l'interprétation de la législation au regard des caractéristiques techniques à satisfaire, comme la garantie que les données démographiques pertinentes (p. ex. sur la langue, l'âge, la race, le genre) soient échantillonnées et sécurisées de manière adéquate afin de ne pas aggraver les inégalités. Elle doit également éclairer les orientations que les chercheurs universitaires ou du secteur privé doivent privilégier pour mettre au point des technologies qui facilitent le respect de la réglementation par les praticiens et son application par les autorités de réglementation (p. ex. par la mise au point d'approches d'analyse des données qui produisent des garanties vérifiables).

RECOMMANDATION 3

Comme les systèmes basés sur des données touchent maintenant tous les aspects de l'activité humaine, la « surface de menace » de ces systèmes s'est considérablement élargie. Des personnes de tous horizons interviennent désormais dans l'utilisation et la gestion de ces systèmes. Les actes, les omissions et les erreurs commis par ces personnes peuvent entraîner des failles de sécurité. Le nombre de cas où des erreurs humaines ont conduit à des attaques de raçongiciels ou d'autres provenances contre des infrastructures essentielles comme des hôpitaux illustre l'ampleur du problème. Un effort général et continu sera nécessaire pour développer une « littératie » sur la sécurité des données et la protection de la vie privée. Les décideurs politiques doivent encourager l'élaboration continue d'outils et de programmes de formation pour instaurer et améliorer en permanence cette littératie, ainsi que le développement de systèmes et de procédures parallèles de protection pour atténuer l'effet des erreurs humaines.

RECOMMANDATION 4

Les divers publics ne doivent pas être considérés comme un seul groupe indifférencié, qu'il s'agisse des « utilisateurs », des « consommateurs » ou des « gens ». Les groupes et les particuliers traitent avec des technologies avancées de collecte de données et de surveillance et en sont touchés de façons très variables, qui ont des conséquences qui peuvent aller du niveau le plus insignifiant au niveau le plus grave, depuis les améliorations mineures en tremes de commodité apportées par la livraison automatisée à domicile, jusqu'à des formes invisibles de discrimination, par exemple l'intégration de préjugés raciaux et sexistes dans les processus d'embauche automatisés ou de condamnation, et jusqu'à l'exclusion de pays entiers basée sur des listes d'interdiction de vol fondées sur des soupçons catégoriques, ou même à la mort, comme dans le cas de l'utilisation de systèmes d'armements ciblés basés sur l'intelligence artificielle. La « justice des données » – à savoir l'équité dans la manière dont les personnes sont catégorisées et traitées lors de la collecte et de l'utilisation des données – devra donc s'ajouter aux considérations de justice actuelles, à savoir les aspects juridiques, économiques, sociaux et environnementaux.

RECOMMANDATION 5

Certaines vulnérabilités particulières doivent également être prises en compte, par exemple les très jeunes, les personnes âgées, en particulier celles qui souffrent de troubles cognitifs, et les personnes malades, qui sont peut-être plus susceptibles d'être victimes d'une utilisation malveillante des technologies avancées, par exemple par des escrocs qui recrutent des personnes âgées, par

3 Loi sur l'IA de l'UE, https://www.europarl.europa.eu/topics/fr/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

l'utilisation de rançongiciels contre les hôpitaux et par des prédateurs qui ciblent les enfants. Toutefois, ces vulnérabilités ne doivent pas servir d'excuse à un élargissement injustifié et généralisé des mesures de surveillance et à une restriction des droits de la personne. Lorsque des mesures plus robustes de sécurité et de surveillance sont adoptées, elles peuvent contribuer à marginaliser davantage les groupes qui sont déjà victimes d'injustices liées aux données.

RECOMMANDATION 6

Les autorités de réglementation doivent intégrer à leurs mandats existants les considérations de sécurité des données associées aux technologies émergentes et, par conséquent, veiller à se doter de l'expertise et des capacités internes ainsi que des moyens de communication et de coordination requis. De nouveaux systèmes de gouvernance et de nouvelles entités de réglementation pourraient également se révéler nécessaires, tant au niveau national qu'international, pour coordonner les lignes directrices, les normes et les meilleures pratiques applicables à tous les secteurs et à toutes les parties intéressées, lorsque des technologies avancées entraîneront au sein de la société des changements systémiques et perturbateurs, comme c'est le cas avec l'IA. La sécurité des données est importante parce que les données et les technologies avancées sont désormais des médiateurs non seulement de l'innovation et de la prospérité, mais aussi de la santé, de l'éducation, de la créativité, des arts, de l'expression et de la connaissance.

RECOMMANDATION 7

Il faut clarifier les responsabilités de chaque entité de réglementation pour éviter qu'une éventuelle fragmentation du paysage réglementaire engendrée par la création de nouvelles entraîne des inefficacités. Le G7 constitue l'un de ces forums de coordination, mais une discussion beaucoup plus large doit aussi se tenir avec les organismes de réglementation existants reconnus (même si leurs responsabilités sont parfois contestées), par exemple l'UNESCO et l'Union internationale des télécommunications (UIT), les pays du Sud et les leaders économiques et technologiques hors du cercle du G7.

RECOMMANDATION 8

Nous reconnaissons que les technologies de pointe soulèveront inévitablement des enjeux de sécurité nationale, mais ce sera la responsabilité des académies et des gouvernements de défendre les intérêts de l'humanité et de la planète. La coopération pour la paix et la sécurité mondiales est nécessaire. Nous soutenons la création d'un « CERN pour l'IA » – qui permettrait aux chercheurs du monde entier d'avoir un accès généralisé et équitable à la puissance de calcul disponible pour constituer leurs ensembles de données, et qui favorisera également l'apprentissage réciproque entre les chercheurs du Nord et du Sud.

RECOMMANDATION 9

Nous recommandons aux décideurs politiques de soutenir par des mesures incitatives le recours au modèle ouvert (*open-source*) afin de remédier à la difficulté de devoir former les experts nécessaires pour voir à l'application de la réglementation. De telles mesures incitatives pourraient prendre la forme d'un financement ciblé et d'une allocation de ressources qui aideraient la communauté des développeurs exploitant le modèle ouvert à assurer le maintien des logiciels et à garantir leur intégrité. Les projets populaires de logiciels basés sur des codes sources ouverts ont montré que l'ouverture et la transparence peuvent également conduire à un renforcement de la sécurité. Toutefois, les décisions liées à l'autorisation ou à la restriction du développement et de l'exploitation libres des puissants systèmes d'IA doivent faire l'objet d'un contrôle démocratique et les règles de sécurité qui s'appliquent aux systèmes exclusifs doivent également s'appliquer aux systèmes ouverts.

RECOMMANDATION 10

Les modèles d'IA générative peuvent produire des médias d'une qualité impressionnante et être utilisés à mauvais escient et à des fins de tromperie. Ces modèles inondent également le Web d'éléments de mésinformation, dont l'inexactitude n'est pas nécessairement intentionnelle, mais qui constituent de fausses informations qui peuvent à leur tour être utilisées et recyclées par les modèles d'IA, ce qui entraînera à la fois la dégradation du modèle et la génération de nouvelles fausses informations. Les textes de réglementation, comme la Loi sur l'IA de l'UE, ont pour but de répondre à cette préoccupation4. La méthode du « filigrane », qui consiste à intégrer dans les contenus générés par l'IA des éléments permettant de les identifier comme tels5 est une solution envisageable, mais fragile. Les filigranes vérifiés par les propriétaires des modèles d'IA peuvent ne pas suffire à endiguer les préjudices causés par les données trompeuses générées par l'IA et ne modifient pas nécessairement le comportement des personnes qui interagissent avec les données – en particulier dans les sociétés qui recourent fortement à la technologie. Les décideurs politiques doivent encourager l'exploration des différentes techniques de vérification de la provenance des données.

RECOMMANDATION 11

Enfin, les technologies d'IA infonuagiques, telles que les grands modèles de langage (GML), ont un impact direct important sur le climat de la planète. Par exemple, la consommation d'électricité résultant d'une requête effectuée sur ChatGPT est bien plus intense que celle d'une simple recherche sur le Web. Les affirmations non vérifiées selon lesquelles l'augmentation de la consommation d'électricité soutiendrait l'accélération du passage à des sources d'électricité durables ne peuvent constituer une réponse à ce problème. La gouvernance et la réglementation des données et de leur traitement doivent être coordonnées avec la mise en œuvre de politiques de durabilité environnementale et énergétiques.

4 Loi sur l'IAde l'UE, https://www.europarl.europa.eu/topics/fr/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

5 https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/

CANADA

La Société royale du Canada

RSC SRC

ALAIN-G. GAGNON

FRANCE

Académie des sciences

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

FRANÇOISE COMBES

GERMANY

German National Academy of Sciences Leopoldina

Leopoldina
Nationale Akademie der Wissenschaften

BETTINA ROCKENBACH

ITALY

Accademia Nazionale dei Lincei

ACCADEMIA NAZIONALE DEI LINCEI

ROBERTO ANTONELLI

JAPAN

Science Council of Japan

MAMORU MITSUISHI

UNITED KINGDOM

The Royal Society

THE ROYAL SOCIETY

ADRIAN SMITH

UNITED STATES

National Academy of Sciences

NATIONAL ACADEMY OF SCIENCES

MARCIA McNUTT