Protection des donnÃ©es et Ã©thique : lâ□□importance de lâ□□IA Act europÃ©en
Internet
PostÃ© par : JPilo
PubliÃ©e le : 24/5/2023 14:00:00

En avril 2022, la Commission EuropÃ©enne (CE) a votÃ© la dÃ©cision de mettre en place le premier cadre juridique mondial pour rÃ©guler la commercialisation et lâ□□usage de lâ□□Intelligence Artificielle (IA).

AprÃ¨s des mois de discussions pour les lÃ©gislateurs, la proposition de loi devrait Ãªtre votÃ©e au Parlement EuropÃ©en prochainement. Avec la prÃ©sence grandissante de lâ□□IA dans tous les aspects de la vie quotidienne, et celle des applications telles que ChatGPT, qui a connu une croissance spectaculaire, les risques et dÃ©rives qui sâ□□y rapportent sont plus que jamais au cÅ□ur des dÃ©bats, et ce projet de loi devenu nÃ©cessaire.

Pour Neil Thacker, RSSI EMEA chez Netskope, rÃ¨glementer lâ□□usage de lâ□□Intelligence Artificielle est essentiel pour protÃ©ger les donnÃ©es, mais cela doit se faire avec des prÃ©ceptes lÃ©gaux prÃ©cis et transparents, qui Ã©voluent avec les technologies, afin dâ□□Ã©viter les vides juridiques, tout en respectant des principes Ã©thiques.

Â« Avec lâ□□IA Act, les lÃ©gislateurs tendent Ã mesurer l'impact potentiel de l'intelligence artificielle sur la sociÃ©tÃ©, plus particuliÃ¨rement sur les droits des citoyens, et le cadre lÃ©gislatif inhÃ©rent pour les protÃ©ger.

La loi permettra aux organismes de surveillance d'exiger le retrait ou la modification d'un modÃ¨le d'IA s'il prÃ©sente un risque Ã©levÃ©. Le schÃ©ma est donc similaire Ã celui du RGPD.

Si ce dernier se concentre sur les donnÃ©es personnelles, leur utilisation et leur traitement responsables, lâ□□IA Act le complÃ¨tera en garantissant le respect des exigences et de la lÃ©gislation existante en matiÃ¨re de droits fondamentaux par les nouvelles technologies gÃ©nÃ©ratives.

De ce fait, les organisations devront se conformer aux deux, et pourront potentiellement subir des rÃ©percussions conjointes : par exemple, une mauvaise hygiÃ¨ne en matiÃ¨re de protection des donnÃ©es entraÃ®nerait une nÃ©gligence aussi en termes dâ□□IA, si elle utilisait des donnÃ©es auxquelles elle ne devrait pas avoir accÃ¨s.

La nouvelle lÃ©gislation devrait ainsi garantir l'Ã©tablissement, la mise en Å□uvre, la documentation et le maintien de systÃ¨mes, de processus et de la gestion des risques. Les entreprises devront dÃ©terminer si leurs systÃ¨mes d'IA sont catÃ©gorisÃ©s Ã risque Ã©levÃ©, et pourront faire l'objet d'une Ã©valuation rÃ©guliÃ¨re.

Certains systÃ¨mes, notamment sâ□□ils exploitent les personnes vulnÃ©rables en raison de leur situation sociale ou Ã©conomique, ou mettent en place des "scores sociaux", comme reprÃ©sentÃ© dans un Ã©pisode de la sÃ©rie TV Black Mirror, sont dâ□□ores et dÃ©jÃ interdits par la proposition discutÃ©e en ce moment mÃªme au Parlement EuropÃ©en.

De plus, ce rÃ¨glement devrait Ã©galement obliger les organisations Ã communiquer quand et comment l'IA a Ã©tÃ© intÃ©grÃ©e dans la prise de dÃ©cisions, et leur influence sur ces derniÃ¨res.

L'une des questions cruciales de ce cadre lÃ©gislatif repose sur la dÃ©finition de ce qui se rapporte Ã la nÃ©gligence ou dâ□□un acte commis intentionnellement en cas dâ□□entrave Ã la loi, susceptible alors dâ□□engager la responsabilitÃ© pour faute.

Lâ□□enjeu sera en effet de dÃ©finir sâ□□il est question dâ□□une erreur liÃ©e Ã une nÃ©gligence involontaire en matiÃ¨re de protection des donnÃ©es ou encore si par exemple elle est le fruit dâ□□une pratique discriminatoire basÃ©e sur des informations dont la partialitÃ© est connue. Ainsi, les leÃ§ons tirÃ©es du RGPD - y compris en matiÃ¨re dâ□□hygiÃ¨ne des donnÃ©es, de normes et de processus - seront extrÃªmement utiles pour se conformer Ã lâ□□IA Act.

Seulement, ce dernier rÃ©glemente aussi la mÃ©thodologie relative Ã la prise de dÃ©cision, et les donnÃ©es sur lesquelles elles sont basÃ©es, ce qui va donc bien plus loin que la seule gestion de ces donnÃ©es.

Au-delÃ de la question de lâ□□Ã©thique, l'exfiltration des donnÃ©es n'est de fait plus la seule cybermenace. Lâ□□IA peut en effet devenir une porte dâ□□entrÃ©e pour les cybercriminels qui chercheraient Ã voler les donnÃ©es utilisÃ©es par cette technologie. Or, si la compromission de l'intÃ©gritÃ© des informations incite l'intelligence artificielle Ã prendre une dÃ©cision diffÃ©rente et contraire Ã lâ□□Ã©thique, les hackers pourraient se servir de ce risque pour nuire Ã l'organisation ciblÃ©e.

Une prise de dÃ©cision Ã©clairÃ©e est cruciale pour mettre en place une intelligence artificielle Ã©thique et qui rÃ©pond aux exigences de lâ□□IA act. ConnaÃ®tre et documenter lâ□□utilisation de la technologie est un moyen simple de comprendre et dâ□□anticiper les failles pour les donnÃ©es critiques de lâ□□entreprise, tout en garantissant une utilisation responsable de lâ□□IA.

La transparence suscite en effet la confiance, câ□□est pourquoi une visibilitÃ© complÃ¨te sur les technologies permet leur protection. Toutefois, une IA en open source semble difficile Ã contraindre, par sa nature libre, car il parait compliquÃ© dâ□□imposer une morale sans autoritÃ© supÃ©rieure. Â»