ASSEMBLÉE NATIONALE

17ème legislature

Question N° : 1720	De **Mme Virginie Duby-Muller** (Droite Républicaine - Haute-Savoie)	**Question écrite**

Ministère interrogé > Intelligence artificielle et numérique	**Ministère attributaire** > Intelligence artificielle et numérique

Rubrique >numérique	**Tête d'analyse** >Impact des « deepfakes » sur la cybersécurité	**Analyse** > Impact des « deepfakes » sur la cybersécurité.

Question publiée au JO le : **05/11/2024**
Date de changement d'attribution : **24/12/2024**

Texte de la question

Mme Virginie Duby-Muller appelle l'attention de Mme la secrétaire d'État auprès du ministre de l'enseignement supérieur et de la recherche, chargée de l'intelligence artificielle et du numérique, sur l'impact de l'utilisation des *deepfakes* sur la cybersécurité. Un *deepfake* (abréviation de *deep learning* et *fake*) est une vidéo manipulée à l'aide de techniques d'intelligence artificielle (IA), où le visage, les mouvements et la voix d'une personne sont superposés sur une autre, donnant l'illusion qu'elle réalise des actions ou prononce des paroles qu'elle n'a jamais faites ou dites en réalité. Si ces nouvelles intelligences artificielles peuvent représenter de véritables innovations, il convient toutefois de rappeler les dangers de celles-ci sur la cybersécurité en fonction de l'utilisation qui en est faite. Ces manipulations vidéo peuvent semer la désinformation politique, entraîner des fraudes financières, le vol d'identité, voire influencer les marchés financiers. En Allemagne, le Gouvernement a exprimé une vive inquiétude face aux *deepfakes*, allant jusqu'à lancer une campagne de sensibilisation pour alerter les parents sur les dangers de ces technologies. Le 10 avril 2024 a été voté le projet de loi dit « SREN » pour mieux réguler l'espace numérique et protéger les internautes, notamment les plus jeunes, ainsi que les entreprises. Cette loi prend bien en compte les dangers liés à publication en ligne d'hypertrucages ou *deepfake* qui seront mieux réprimées. Néanmoins, selon un sondage IFOP, seulement un tiers des citoyens français estiment avoir la capacité de repérer un *deepfake* et à peine 6 % en sont totalement sûrs, illustrant ainsi le niveau élevé d'incertitude qui prévaut chez eux. Les jeunes et les hommes se montrent plus confiants : 55 % des 18-24 ans pensent pouvoir le faire, contre 28 % des plus de 35 ans, tandis que 40 % des hommes le croient possible, comparé à 28 % des femmes (source : Les Français et les jeunes face aux *deepfakes* - sondage IFOP). Les *deepfakes* utilisant le *machine learning* pour s'améliorer, ils risquent d'être de moins en moins détectables par une majorité de personnes. Récemment, les visages influenceurs et de personnalités publiques ont été utilisés pour la promotion de casinos en ligne, applications mobiles frauduleuses et cryptomonnaies douteuses. Les arnaqueurs usurpent l'identité de ces personnalités publiques, car elles ont une notoriété forte auprès du grand public. Des fausses vidéos sont ainsi propagées sur les réseaux sociaux, notamment TikTok, qui cible majoritairement les jeunes et se retrouvent à la merci de ces arnaques. Ainsi, elle lui demande ce que le Gouvernement compte mettre en place pour renforcer la sensibilisation et l'encadrement des *deepfakes*, cette problématique sérieuse étant de l'ordre de l'atteinte au droit à l'image, de l'usurpation d'identité et de l'escroquerie.