

16ème législature

Question N° : 9411	De M. Christophe Naegelen (Libertés, Indépendants, Outre-mer et Territoires - Vosges)	Question écrite
Ministère interrogé > Transition numérique et télécommunications		Ministère attributaire > Numérique
Rubrique >numérique	Tête d'analyse >Encadrement de l'utilisation des « deepfakes »	Analyse > Encadrement de l'utilisation des « deepfakes ».
Question publiée au JO le : 27/06/2023 Réponse publiée au JO le : 09/01/2024 page : 240 Date de changement d'attribution : 21/07/2023 Date de renouvellement : 03/10/2023		

Texte de la question

M. Christophe Naegelen attire l'attention de M. le ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications, sur l'encadrement de l'utilisation des « *deepfakes* ». Cet anglicisme désigne une technique de synthèse s'appuyant sur l'intelligence artificielle. Le *deepfake* permet notamment la superposition de fichiers audio ou vidéo réels sur d'autres fichiers de manière à créer de faux contenus d'apparence très réalistes. En 2019, il existait environ 15 000 *deepfakes* en ligne, nombre qui est amené à augmenter d'environ 900 % chaque année selon les estimations du Forum économique mondial. De fait, il existerait aujourd'hui des millions de *deepfakes* en ligne. Si ces nouvelles intelligences artificielles peuvent représenter de véritables innovations, il convient toutefois de rappeler les dangers potentiels de celles-ci en fonction de l'utilisation qui en est faite. En effet, ces techniques peuvent notamment conduire à l'utilisation de l'image ou de la voix d'une personne sans son consentement, à des fins parfois mensongères et trompeuses. De plus, ces faux contenus créés par intelligence artificielle sont désormais particulièrement difficiles à différencier d'un contenu authentique, ce qui représente un fort risque de désinformation pour les citoyens. En outre, au delà d'être de plus en plus réalistes, les intelligences artificielles capables de produire des *deepfakes* sont désormais accessibles, en ligne, au plus grand nombre et sont assez simples d'utilisation. En 2021, le Gouvernement a mis en place une stratégie nationale avec un plan d'action en 5 ans sur l'intelligence artificielle, dont l'un des axes est destiné à promouvoir un modèle éthique équilibré entre innovation et protection des droits fondamentaux. Il existe en effet déjà un fort encadrement de l'utilisation des intelligences artificielles, tant au niveau national qu'au niveau européen. Cependant, il n'existe à ce jour aucune législation spécifique concernant les *deepfakes*, les abus constatés dans l'utilisation qui est faite de ces derniers étant souvent rapprochés, en fonction des situations, du champ de la diffamation, de l'atteinte au droit à l'image, de l'usurpation d'identité ou de l'escroquerie. Pourtant, l'encadrement de l'usage qui est fait de ces nouvelles technologies constitue un double enjeu, à la fois de lutte contre la désinformation, mais également de protection des données et de la vie privée des individus. Ainsi, il demande ce que le Gouvernement compte mettre en place pour renforcer l'encadrement des pratiques de *deepfake*.

Texte de la réponse

Le Gouvernement est très sensible à la nécessité de lutter contre la propagation de contenus truqués, dont la faisabilité, l'accessibilité et la diffusion se trouvent facilitées du fait de l'essor de l'intelligence artificielle. Il soutient activement l'adoption de mesures spécifiques en faveur de la prévention et de la transparence des contenus d'hypertrucages dans le règlement relatif à l'intelligence artificielle actuellement en cours de négociations à Bruxelles, lesquelles sont en passe d'aboutir. Ce projet de règlement prévoit notamment une obligation pour les utilisateurs d'un système d'intelligence artificielle qui génère ou manipule des images ou contenus audio ou vidéo qui présentent une ressemblance avec des personnes, des objets, des lieux, etc. et pourraient être perçus à tort comme authentiques ou véridiques, d'indiquer que ces contenus ont été générés ou manipulés artificiellement. La France se mobilise pour que les contenus ainsi visés ne soient pas limités aux seuls contenus présentant une ressemblance avec des personnes, comme proposé par le Parlement européen, afin de couvrir tous les hypertrucages. La France soutient également l'extension de cette obligation d'information aux personnes physiques qui utiliseraient de tels systèmes d'intelligence artificielle en dehors d'un cadre professionnel, afin de pouvoir également lutter contre la création et dissémination d'hypertrucages par des individus agissant de leur propre fait. Cette disposition viendra compléter celles déjà prévues par le règlement sur les services numériques, entré en vigueur le 25 août 2023, qui impose aux plateformes en ligne de traiter promptement les contenus illicites qui leur sont signalés, dont relèvent potentiellement les pratiques abusives en matière d'hypertrucage. Les très grandes plateformes doivent aussi lutter contre les risques systémiques, de désinformation notamment, et prendre toute mesure d'atténuation nécessaire. Par ailleurs, le cadre national permet déjà de lutter en partie contre ces pratiques. Ainsi, la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information impose aux opérateurs de plateforme en ligne de mettre en œuvre des mesures afin de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité de certains scrutins. Elle a aussi créé un référé spécifique pour faire stopper en urgence la diffusion « délibérée, artificielle ou automatisée, et massive » d'une information manifestement fausse (« inexacte ou trompeuse ») et susceptible d'altérer la sincérité d'un scrutin. Enfin, le Gouvernement a présenté dans son projet de loi sur la sécurisation de l'espace numérique (SREN) deux mesures d'encadrement des « deepfakes ». Premièrement, le projet de loi adapte les interdictions de trucages prévues au sein du code pénal aux nouveaux outils d'intelligence artificielle. En effet, les hypertrucages générés par l'intelligence artificielle sans support préalable n'étaient pas compris pas dans la catégorie du « montage » telle que définie par le code pénal. Le projet de loi SREN modifie l'article 226-8 de ce code pour réguler ces nouvelles réalités qui représentent une part croissante des hypertrucages. Deuxièmement, la très grande majorité des hypertrucages recensés sont des hypertrucages à caractère sexuel. Ils concernent majoritairement les femmes et sont souvent utilisés pour nuire à leur réputation. Le projet de loi SREN crée un nouvel article 226-8-1 au sein du code pénal pour sanctionner tout hypertrucage à caractère sexuel diffusé sans consentement, même s'il est précisé qu'il s'agit d'un hypertrucage. De tels hypertrucages sont sanctionnés d'une peine d'emprisonnement de deux ans et de 60 000 € d'amende. Ces dispositions ont été adoptées de façon conjointe par le Sénat et l'Assemblée nationale. L'ensemble de ces dispositifs tant au niveau européen que national renforcent substantiellement l'encadrement et la répression des pratiques d'hypertrucages illicites, en visant particulièrement celles s'appuyant sur l'intelligence artificielle.