

ASSEMBLÉE NATIONALE

22 mars 2024

PRÉVENIR LES INGÉRENCES ÉTRANGÈRES - (N° 2343)

Commission	
Gouvernement	

Rejeté

AMENDEMENT

N° 106

présenté par

M. Lachaud, Mme Abomangoli, M. Alexandre, M. Amard, Mme Amiot, Mme Amrani, M. Arenas, Mme Autain, M. Bernalicis, M. Bex, M. Bilongo, M. Bompard, M. Boumertit, M. Boyard, M. Caron, M. Carrière, M. Chauche, Mme Chikirou, M. Clouet, M. Coquerel, M. Corbière, M. Coulomme, Mme Couturier, M. Davi, M. Delogu, Mme Dufour, Mme Erodi, Mme Etienne, M. Fernandes, Mme Ferrer, Mme Fiat, M. Gaillard, Mme Garrido, Mme Guetté, M. Guiraud, Mme Hignet, Mme Keke, M. Kerbrat, M. Laisney, M. Le Gall, Mme Leboucher, Mme Leduc, M. Legavre, Mme Legrain, Mme Lepvraud, M. Léaument, Mme Pascale Martin, Mme Élisabeth Martin, M. Martinet, M. Mathieu, M. Maudet, Mme Maximi, Mme Manon Meunier, M. Nilor, Mme Obono, Mme Oziol, Mme Panot, M. Pilato, M. Piquemal, M. Portes, M. Prud'homme, M. Quatennens, M. Ratenon, M. Rome, M. Ruffin, M. Saintoul, M. Sala, Mme Simonnet, Mme Soudais, Mme Stambach-Terreiro, Mme Taurinya, M. Tavel, Mme Trouvé, M. Vannier et M. Walter

ARTICLE 3

Supprimer cet article.

EXPOSÉ SOMMAIRE

Cet amendement vise à supprimer l'article 3 qui prévoit d'élargir les finalités permettant aux services de renseignement de recourir à la technique du renseignement dite de l'algorithme. Jusqu'alors, ce recours était strictement circonscrit aux « seuls besoins de la prévention du terrorisme ».

Actuellement l'algorithme « défense » est un instrument de détection ciblée des signaux faibles. Cette détection est ciblée en ce qu'elle est effectuée en fonction de paramètres déterminés, dans un seul objectif (révéler une menace terroriste ...). L'enjeu crucial consiste à être en mesure de détecter une menace dont les auteurs et les modes opératoires ne sont pas connus – auteurs qui ne peuvent, par définition, faire l'objet d'une surveillance ciblée a priori –, ce afin de caractériser et d'évaluer cette menace. Cependant, le recours à cette technique est extrêmement opaque, le fonctionnement des algorithmes n'est en effet pas connu. Bien que la loi prévoit que l'identification des personnes ne puisse se faire au moment de la captation des données, Bastien Le Querec (Quadrature du net) alerte

: ""Les boîtes noires font du chalutage de données pour découvrir une menace. A partir d'une URL, on va cibler un réseau, un quartier, une résidence"".

En vertu de l'élargissement de ces finalités, les services spécialisés de renseignement pourraient ainsi être autorisés à détecter des connexions susceptibles de révéler « toute forme d'ingérence étrangère ou de tentative d'ingérence étrangère ». Or, cette dernière notion est trop vague et peut permettre la création d'un algorithme qui aura pour finalité de révéler des activités au delà des enjeux de défense. La nouvelle rédaction de l'article L851-3 du code de la sécurité intérieure ainsi proposée ouvrirait la voie à une confusion dangereuse entre ingérence étrangère, et simple influence ou intervention d'acteurs étrangers, y compris celle d'acteurs non-étatiques telles que les organisations non-gouvernementales, et quelles que soient les finalités de ces interventions. De plus, elle permettrait un usage de ces techniques de renseignement à l'encontre de groupements politiques associatifs ou informels.

En outre, si le seul recours élargi à ces traitements automatisés ne devrait pas permettre l'identification par les services spécialisés des personnes auxquelles les données détectées se rapportent, la nouvelle version de l'article L851-3 permettrait bien l'« identification de la ou les personnes concernées et le recueil des données y afférente » en cas de détection de « données susceptibles de caractériser l'existence d'une menace ». Or, cette nouvelle rédaction, qui ne précise pas le type de menace concernée soulève à nouveau le risque d'arbitraire et de probables violations aux droits et libertés mentionnés. De plus, la confiance que l'on place dans nos technologies de renseignement est toujours risqué pour les droits et libertés d'une part, et n'a jamais en soi prouvé son efficacité. Le renseignement doit nécessairement, et avant tout, passer par du travail humain.

Plus généralement, l'élargissement de ces finalités apparaît problématique, tant il a été maintes fois documenté que le recours aux techniques de renseignement algorithmiques est attentatoire aux les libertés individuelles. De façon générale, il a été montré que la surveillance, qu'il s'agisse de la collecte massive de données ou de la collecte ciblée de données, interfère directement avec la vie privée, dont le droit est constitutionnellement garanti, et la sécurité, nécessaires à la liberté d'opinion et d'expression. Cette interférence peut être directe ou indirecte, par exemple par un effet d'auto-censure des acteurs. C'est le constat émis dans une résolution A/C.3/71/L.39/Rev.1 l'Assemblée générale des Nations Unies sur le droit à la vie privée à l'ère numérique (2016), qui pointe que la crainte de la divulgation involontaire d'une activité en ligne, telles que la recherche et la navigation, dissuade probablement les individus d'accéder à des informations, en particulier lorsque cette surveillance conduit à des résultats répressifs. Cette même surveillance peut également avoir un effet paralysant sur la liberté du travail journalistique et sur le secret des sources, et donc sur la liberté de la presse, reconnue à valeur constitutionnelle.

Nous souhaitons rappeler que la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement prévoyait que l'usage des techniques de renseignement prévues à l'article L. 851-3 du code de sécurité intérieure ferait l'objet d'un rapport en juillet 2024. Nous pensons que ce rapport devra permettre un débat de fond et éclairé sur le sujet.

Enfin, nous rappelons notre opposition ferme au recours à la surveillance algorithmique. Le développement de la « technopolice » qui s'est déployé ces dix dernières années : caméras-piétons, caméras embarquées, drones, transmission des images en temps réel, utilisation d'algorithmes « intelligents », etc., doit prendre fin. Notre programme l'Avenir en Commun propose de mettre un

terme à cette fuite en avant et nous reviendrons à des méthodes de police et d'investigation qui mettent le savoir-faire humain au cœur du dispositif, dans le respect de la vie privée des citoyen-nes.

Pour toutes ces raisons, le présent amendement propose la suppression de cet article 3.