IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

www.irsem.fr

Brève stratégique - 70

3 juin 2024

Extension de la loi FISA

La « souveraineté numérique » européenne loin des préoccupations américaines

Clotilde Bômont

La portée extraterritoriale de certaines lois américaines permet aux agences de renseignement d'accéder aux données de citoyens et d'organisations européens sans leur consentement, faisant fi des réglementations de l'UE et allant à l'encontre de la « souveraineté numérique » européenne. Vivement critiquée des deux côtés de l'Atlantique, l'extension de la loi FISA votée fin avril 2024 est une entrave à la coopération UE-US dans le domaine numérique à la veille des élections européennes et américaines.

Boom de l'IA générative, campagnes de désinformation, recrudescence des cyberattaques soutenues par les gouvernements russe (APT28, APT29) et chinois (APT31), régulation des contenus et responsabilisation des plateformes… Face à ces sujets d'actualité, le renouvellement fin avril 2024 de la loi américaine FISA est passé relativement inaperçu en France. Pourtant, à la veille des élections européennes et américaines, cette mesure sur la captation de données numériques pose plus largement la question de la coopération transatlantique dans un contexte de réaffirmation de la « souveraineté numérique » européenne.

Adopté par le Congrès américain en 1978, le Foreign Intelligence Surveillance Act (FISA) régit la surveillance physique et électronique des personnes physiques et morales étrangères, sur le territoire américain et à l'étranger. À la suite de nombreuses atteintes à la vie privée et à la sécurité des données de citoyens américains, en particulier dans le cadre du programme de surveillance massive Stellar Winds, et afin de légaliser l'action des services secrets américains, la loi est amendée en 2008. La section 702 de l'amendement indique alors que les agences de renseignement américaines sont en droit d'exiger des opérateurs de communication et de services numériques qu'ils leur fournissent toutes données jugées utiles, sans que cette demande s'appuie nécessairement sur un mandat. Elle précise que cette mesure ne peut cibler les ressortissants américains. Alors que le FISA devait expirer en décembre 2023, sa validité avait été prolongée de quelques mois par le président américain Joe Biden, avant que son renouvellement pour deux ans ne soit voté par le Sénat le 20 avril 2024.

Défendu par l'administration Biden, le projet de loi a suscité de vifs débats aux États-Unis, dépassant les clivages entre républicains et démocrates. Tandis que certains défendent l'utilité de la loi pour la sécurité nationale et la lutte contre le terrorisme, en particulier dans le contexte de la rivalité sino-américaine et des conflits en Ukraine et au Proche-Orient, d'autres dénoncent de sérieuses atteintes aux libertés individuelles. Ce sont d'abord les nombreux abus qui sont pointés du doigt, la Foreign Intelligence Surveillance Court (FISC) – Cour fédérale veillant au respect du FISA – ayant elle-même dénoncé les violations répétées de la loi par le FBI. Des analystes auraient notamment eu recours à la section 702 pour accéder sans mandat aux données de citoyens américains lors des mouvements Black Lives Matter en 2020 et lors de l'assaut du Capitole le 6 janvier 2021. L'ancien président des États-Unis, Donald Trump lui-même, a accusé avec véhémence la NSA et le FBI d'avoir eu recours à la loi de manière abusive lors des présidentielles de 2016 afin de nuire à sa campagne, et haranguait ses soutiens sur son réseau social Truth Social le 10 avril 2024, incitant à « tuer le FISA ».

C'est donc ensuite le rejet des propositions visant à mieux encadrer la saisie des données qui a mécontenté les opposants au texte. En effet, à l'issue d'un vote serré mi-avril, la Chambre des représentants a rejeté la disposition prévoyant la demande de mandat lors d'enquêtes impliquant indirectement des ressortissants américains (lors d'un échange entre la personne étrangère surveillée et un citoyen américain, par exemple).

Le durcissement de la loi, enfin, est une autre pierre d'achoppement. Deux amendements prévoient d'étendre l'applicabilité de la section 702 aux voyageurs étrangers sur le sol américain et aux trafiquants de drogue internationaux. Un troisième, davantage contesté, porte sur la mise à jour de la définition des opérateurs de communication et de services. Bien que la FISC souligne la nécessité d'adapter cette définition aux évolutions technologiques, la nouvelle définition est jugée trop large par diverses parties prenantes, y compris par les grands industriels du numérique. Elle comprend effectivement dorénavant toute entité « ayant accès à des équipements qui sont ou peuvent être utilisés pour transmettre ou stocker des communications filaires ou électroniques ». Cela étend considérablement le champ des entreprises, organisations ou même individus tombant sous le coup de la loi, la simple fourniture d'une connexion Wifi répondant en théorie à cette définition. Le libellé exclut néanmoins les logements, les établissements publics et les établissements commerciaux de restauration et d'hébergement.

En Europe non plus, le renouvellement de la loi FISA n'a pas été bien accueilli. Elle compte en effet, aux côtés du Patriot Act voté en 2001 et du CLOUD Act adopté en 2018, parmi les lois américaines menaçant directement la sécurité des données européennes. Leur portée extraterritoriale permet au gouvernement américain de contraindre les entreprises de services numériques étatsuniennes à fournir les données de leurs clients, même si ces dernières ne quittent pas le sol européen. Or, compte tenu de la situation oligopolistique du marché, les grandes entreprises américaines du numérique interviennent presque inéluctablement dans les chaînes de valeurs des services numériques, exposant ainsi une large part des données européennes aux indiscrétions des agences de renseignement américaines. Ces dispositions, en sus de limiter la maîtrise de leurs données par les Européens, entrent en concurrence avec les règlements en vigueur au sein de l'UE, à commencer par le Règlement général sur la protection des données (RGPD). Si des mesures ont été proposées au sein de l'UE pour limiter l'emprise de ce type de lois, elles ne font pas toujours consensus. C'est ce qu'ont montré les débats autour du schéma européen de certification pour les services cloud (EUCS) dont la seconde version prévoyait d'inclure une clause garantissant que les offres certifiées au plus haut niveau de sécurité ne seraient pas soumises à des juridictions non européennes. Si cette clause a été retirée dans la dernière version du texte, le renouvellement du FISA pourrait rouvrir les discussions.

Par ailleurs, la reconduction du FISA souligne les ambivalences de la relation euro-américaine en matière numérique. Le renouvellement de la loi intervient en effet peu de temps après la signature, le 10 juillet 2023, d'un nouvel accord de transfert de données entre les États-Unis et l'UE (le Data Privacy Framework, DPF). Cet accord est le troisième de ce type, le Safe Harbor puis le Privacy Shield ayant été invalidés par la Cour de justice de l'Union européenne (CJUE) en 2015 et en 2020 au motif qu'ils ne garantissaient pas suffisamment la protection des données personnelles des Européens. La Commission européenne avait déjà été vivement critiquée en mars 2022, lorsqu'avait été annoncé l'accord de principe sur le DPF. La présidente de la Commission, Ursula von der Leyen, a notamment été accusée de céder aux pressions des États-Unis qui ont utilisé l'argument de la guerre en Ukraine et de la sécurité européenne pour accélérer l'adoption du DPF alors que l'UE tenait tête à Washington depuis près de deux ans. En signant le DPF sans obtenir de garanties solides sur la sécurité des données européennes alors que le FISA arrivait à son terme, l'UE aurait ainsi perdu son levier pour demander une révision de la loi américaine.

La décision américaine sur le FISA est, en outre, de mauvais augure pour l'avenir du Conseil EU-US du commerce et des technologies (Trade and Technology Council, TTC) dont l'efficacité est de plus en plus mise en question. Mis en place en 2021, le TTC a permis de renouer le dialogue transatlantique après la présidence de Donald Trump, attestant les volontés de coopération bilatérale et les nombreux intérêts économiques et stratégiques communs. Cependant, la défense de ses intérêts nationaux conduit parfois Washington à négliger son partenaire européen. En adoptant de manière unilatérale et sans tenir compte de l'impact pour l'UE des mesures telles que l'Inflation Reduction Act (IRA), le contrôle des exportations de semi-conducteurs vers la Chine, les sanctions contre l'entreprise de télécommunications Huawei ou encore le durcissement de la loi FISA, les États-Unis montrent que la relation américano-européenne n'est pas une priorité dans leur agenda.

Aussi, même si les contestations exprimées au sujet du renouvellement du FISA aux États-Unis semblent converger avec les intérêts européens, il convient de garder à l'esprit qu'elles sont avant tout motivées par des préoccupations nationales. Le durcissement de la loi FISA rappelle avec force la nécessité pour l'UE de s'affirmer face à l'allié américain et de réduire sa dépendance structurelle vis-à-vis des États-Unis. En dépit de réelles avancées en matière de « souveraineté numérique » européenne ces cinq dernières années, l'UE doit encore accélérer le développement de ses capacités industrielles et de Recherche & Développement et faire de la préservation de son marché une priorité. Les élections de juin 2024 sont une opportunité de (re)définir les ambitions de la politique numérique européenne. ■

Clotilde Bômont *est chercheuse en géopolitique du numérique (IRSEM).*
Contact : clotilde.bomont@irsem.fr

Avertissement : l'IRSEM a vocation à contribuer au débat public sur les questions de défense et de sécurité. Ses publications n'engagent que leurs auteurs et ne constituent en aucune manière une position officielle du ministère des Armées.