Parlement européen

60, rue Wiertz / Wiertzstraat 60
B-1047 Bruxelles / Brussel

**M. Sébastien Lecornu**
Premier ministre
Hôtel Matignon
57 rue de Varenne
75007 Paris
France

*Bruxelles, le 19 août 2026*

Monsieur le Premier ministre,

La cyberattaque ayant touché la Direction générale des finances publiques, révélée le 13 août dernier et affectant plus de 700 000 particuliers et professionnels ne constitue malheureusement pas un fait isolé. Elle s'inscrit dans une série préoccupante d'incidents touchant l'administration centrale depuis le début de l'année 2026 : le piratage du fichier Ficoba en janvier (environ 1,2 million de comptes bancaires), puis trois intrusions distinctes visant le ministère de l'Éducation nationale – le système COMPAS en mars (243 000 agents), le service annexe à ÉduConnect en avril (données de plusieurs millions d'élèves), et le système de formation des personnels fin juillet (données d'agents en poste depuis 2001, incluant des numéros de sécurité sociale).

Cette accumulation révèle une vulnérabilité structurelle de nos administrations face à la menace cyber, à attribuer à la fois aux « dettes techniques » décrites par le Ministre des comptes publics cette semaine et au retard pris dans la transposition de la **directive européenne concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS 2 »**. Échue depuis le 17 octobre 2024, cette transposition demeure bloquée dans le circuit parlementaire, la France faisant désormais l'objet d'un recours de la Commission européenne devant la Cour de justice de l'Union depuis le 8 juillet 2026. Or NIS 2 impose précisément les standards qui ont fait défaut dans ces incidents en termes de gestion des risques et de gouvernance de la sécurité des systèmes d'information critiques.

Je salue les premières annonces de votre Gouvernement, comme la mission d'audit confié à l'ANSSI sur la sécurisation des systèmes d'information de la DGFiP, la création d'une taskforce dédiée et l'accélération du plan de sécurisation des administrations lancé en avril dernier. Ces mesures vont dans le bon sens, mais en matière cyber, la prévention vaut mille remèdes.

Contact : francois.kalfon@europarl.europa.eu

Parlement européen

60, rue Wiertz / Wiertzstraat 60
B-1047 Bruxelles / Brussel

Parmi les pistes que la France doit d'urgence suivre pour se mettre à niveau face à l'ampleur de la menace qui pèse sur nos administrations, j'identifie en premier lieu les suivantes :

1. **Transposer d'urgence la directive NIS2** en inscrivant le projet de loi « Résilience » à l'ordre du jour de la prochaine session du Parlement ;

2. **Soutenir à Bruxelles l'ambition du Cybersecurity Act 2**, notamment ses dispositions généralisant les schémas européens de certification de cybersécurité et permettant la désignation de « fournisseurs à haut risque », à l'image de Huawei, pour sécuriser l'infrastructure numérique européenne ;

3. **Élargir les missions et les moyens de l'ANSSI** dès la loi de finances pour 2027 ;

4. **Renforcer, dans le cadre de France 2030, le soutien aux filières françaises de cybersécurité et d'hébergement souverain des données**, condition de notre autonomie stratégique numérique en matière cyber.

Face à une menace qui doit rassembler toutes les forces de la Nation, je me tiens à votre disposition et celle du Gouvernement dans les prochaines semaines, pour en échanger de vive voix.

Je vous prie de recevoir, Monsieur le Premier ministre, l'expression de ma haute considération.

**François Kalfon**
*Député européen*

Contact : francois.kalfon@europarl.europa.eu