ACN
Alliance pour la confiance numérique

***Prise de position de l'ACN***
***27 août 2026***

# FUITES DE DONNEES : SORTIR DE LA FATALITE ET RESPONSABILISER LES DIRIGEANTS PUBLICS POUR PASSER A L'ACTION

***Les intrusions et violations de données récemment rendues publiques au sein de la Direction générale des Finances publiques et de l'Éducation nationale viennent allonger une longue série devenue particulièrement préoccupante. Ces incidents ne peuvent plus être considérés comme des accidents isolés : ils révèlent une fragilité structurelle dans la protection des données confiées aux administrations et, plus largement, dans la gouvernance de la cybersécurité. La France est ainsi devenue le 2ème pays le plus ciblé au monde, avec plusieurs dizaines de millions de comptes compromis au premier semestre 2026. De quoi mettre à mal la confiance des citoyens dans la capacité de l'Etat à protéger leurs données.***

***L'Alliance pour la Confiance Numérique (ACN) appelle l'État à cesser de traiter la cybersécurité comme un aléa et à faire de la sécurisation des données des citoyens et du renforcement de la souveraineté numérique une véritable priorité nationale, au-delà des discours.***

***Il est urgent de tirer les leçons de ces évènements, d'engager systématiquement la responsabilité des décideurs publics concernés, de mettre en œuvre sans retard des plans et stratégies élaborés depuis des années et de capitaliser sur la filière française de la confiance numérique pour y parvenir.***

**La responsabilité en question : des solutions connues mais aucune sanction à ce jour**

La fuite de données de la DGFIP ne révèle rien de nouveau. Comme l'a justement rappelé le Premier ministre, nous « ne redécouvrons pas la lune » à chaque incident de sécurité. Les solutions existent depuis des années : les rapports se sont accumulés, les stratégies ont été formulées. Pourtant, face à cette cascade de fuites, aucune sanction n'a été prononcée. Le message ainsi envoyé est que finalement laisser fuiter les données sensibles de millions de citoyens n'est pas en soi constitutif d'une faute. A contrario, lorsque les citoyens confient leurs données aux pouvoirs publics, ils s'attendent, à bon droit, à ce que tout soit mis en œuvre pour les protéger. Cette obligation de moyens est une responsabilité qui doit peser sur les épaules de chaque décideur public et privé.

*« Lorsqu'une fuite de cette ampleur se produit, c'est un symptôme d'une faille dans la gouvernance et la responsabilisation. Il est temps que chaque décideur, public comme privé, intègre que la protection effective des données sensibles et personnelles relève de sa responsabilité. Rompre avec l'absence ou la dilution des responsabilités est une condition sine qua non pour quitter la logique de fatalité et entrer dans celle de l'action réelle. En ce sens, nous soutenons pleinement l'initiative de création d'une commission d'enquête à l'Assemblée nationale, proposée par le député Philippe*

*Latombe, afin d'établir les diverses responsabilités dans les fuites de données récentes* » déclare Grégory Wintrebert, Président de l'ACN.

**Transposition de NIS2 : une priorité stratégique à géométrie variable ?**

La transposition chaotique de la directive NIS2 est un autre exemple de la différence entre une priorité de façade et l'action réelle. Sur un sujet aussi stratégique que la résilience de notre pays, cette directive devait être transposée avant… octobre 2024. A ce jour, et malgré les efforts répétés des Présidents des commissions spéciales ayant examiné ce texte au Sénat (Olivier Cadic) et à l'Assemblée (Philippe Latombe), le projet de loi « Résilience » n'a toujours pas été inscrit à l'agenda parlementaire et Bruxelles a ouvert une procédure à l'encontre de la France pour sanctionner son inaction ! NIS2 n'est pourtant pas un caprice bureaucratique : elle crée un cadre légal qui oblige les entités essentielles et importantes à renforcer leur sécurité numérique et leur résilience. L'ACN appelle à aligner les paroles et les actes et à inscrire ce projet de loi à l'agenda législatif, sans délai supplémentaire. Chaque jour de retard aggrave notre exposition, renforce les critiques légitimes de Bruxelles, décourage les acteurs de la confiance numérique et renvoie, là-aussi, le message d'une priorité finalement un peu secondaire.

**Passer à l'action : l'État n'y arrivera pas seul, la filière de confiance numérique est à ses côtés**

Face à cette urgence, un message doit être clair : l'État n'a pas besoin de chercher des solutions ailleurs. La France dispose d'une filière de confiance numérique, dont les compétences sont non seulement reconnues mondialement mais aussi attestées par l'État lui-même à travers un système de certifications et de qualifications. Pourtant, le constat est amer : l'État sous-utilise systématiquement cette filière et cherche trop souvent à réinventer en interne ce qui existe déjà par ailleurs dans la filière sans y recourir. Les appels d'offres demeurent fragmentés, ignorent les critères de souveraineté numérique, les délais s'éternisent, les projets sont repoussés… C'est une double perte : nous sacrifions notre souveraineté numérique et nous nous privons des compétences locales pourtant disponibles. Par ailleurs, les budgets dévolus à la sécurité des systèmes d'informations sont, dans la plupart des cas, très largement sous-dotés dans les projets numériques de l'Etat. Les priorités doivent changer ! Le projet de loi de finances à venir sera une véritable occasion de mesurer à quel point ce sujet est considéré comme prioritaire.

**Quatre priorités pour sortir de cette spirale**

Face à cette succession de crises, l'ACN, en tant que syndicat professionnel de la filière de la confiance numérique, souhaite s'adresser à la fois au Gouvernement, mais a aussi prévu de rencontrer l'ensemble des candidats à la prochaine élection présidentielle pour leur demander d'agir avec force sur tous les fronts :

1. Inscrire d'urgence le projet de loi « Résilience » à l'agenda parlementaire et transposer NIS2 sans délai supplémentaire. Ce retard inacceptable doit cesser.
2. Augmenter significativement les budgets de sécurisation des systèmes d'information publics dans les projets de loi de finances à venir (à commencer par le prochain). La cybersécurité ne peut plus être traitée en miettes budgétaires : il faut une vision cohérente et durable.
3. Recourir massivement aux solutions de la filière française et européenne de confiance et mettre en place une véritable politique industrielle en soutien de cette filière. Faire des appels d'offres publics des leviers de souveraineté et de résilience, plutôt que des corvées administratives. Déléguer l'expertise plutôt que de prétendre tout faire en interne.

4. Engager systématiquement la responsabilité des décideurs publics ou privés dont les entités subissent des fuites majeures. Chaque événement de cette gravité doit entraîner des conséquences visibles : audits obligatoires, sanctions, reddition de compte publique.

La fuite DGFIP est un moment de vérité. Elle doit forcer les décideurs à abandonner l'illusion qu'on peut traiter la cybersécurité par à-coups, à posteriori, avec des rapports et des déclarations. La confiance numérique, dans tous ses volets (résilience, sécurité, souveraineté), doit être érigée en priorité nationale et inscrite au plus haut niveau de la gouvernance de l'État. Dans la perspective des prochaines élections présidentielles, il est urgent d'expliquer à nos concitoyens comment l'Etat compte mettre fin à ces fuites à répétition et préciser les engagements de chacun pour enfin, protéger les données sensibles et personnelles que les citoyens confient chaque jour aux administrations. La filière de la confiance numérique est prête à participer à cette mobilisation collective. Nous avons les compétences, les certifications, l'expérience et la volonté. Il ne manque qu'une chose : que l'on cesse de considérer la cybersécurité comme un aléa climatique, que la protection des données soit une réelle responsabilité assumée par les dirigeants et que les actions nécessaires soient mises en œuvre en conséquence.

*A propos de l'ACN :*

***L'Alliance pour la Confiance Numérique (ACN) est le syndicat professionnel qui représente les entreprises du secteur de la confiance numérique*** *notamment celles de la cybersécurité, de l'identité numérique, de l'Intelligence Artificielle de confiance, de la blockchain et des infrastructures numériques de confiance.* ***La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue*** *grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur.* ***Selon l'Observatoire ACN de la Confiance Numérique 2026, le secteur emploie 114 000 personnes et pèse, en France, plus de 22,4 milliards d'euros de chiffre d'affaires, en forte croissance.*** *L'ensemble des données économiques du secteur est disponible dans l'édition 2025 de cet Observatoire en téléchargement sur le site ACN (www.confiance-numerique.fr).* ***Les 100 entreprises membres de l'ACN (dont plus de 85% sont des start up/PME/ETI) représentent plus 80% du chiffre d'affaires du secteur.*** *L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) du Campus Cyber et participe activement aux travaux des Comités Stratégiques de Filière (CSF) Industries de Sécurité et Solutions Numériques de confiance. Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).*