Cyberattaque aux impôts : derrière la faille informatique, la question des moyens

La cyberattaque qui a frappé la Direction générale des finances publiques (DGFiP) cet été n'est pas un incident anodin. Pour la CGT, elle met en lumière les conséquences de politiques qui, depuis des années, suppriment des emplois, réduisent les moyens et fragilisent la maîtrise publique de compétences pourtant stratégiques. Ce piratage souligne aussi que la sécurité informatique est aujourd'hui plus que jamais une mission à part entière du service public.

Les chiffres donnent la mesure de la menace:en deux ans, les cyberattaques contre la DGFiP ont bondi de 170 %, passant de 2 579 en 2023 à 6 972 en 2025. Derrière ces attaques, des « données d'une sensibilité critique » (Schéma directeur du numérique 2026 : DGFiP), selon les propres termes de la direction. **Et une question : la DGFiP a-t-elle encore les moyens humains et techniques d'y faire face ?**

Cyberattaques à la DGFiP : la CGT avait alerté

Depuis janvier, les incidents informatiques se succèdent à la DGFiP : ordinateurs bloqués, applications indisponibles, données bancaires consultées frauduleusement… Dès le mois de mars, la CGT Finances publiques tirait la sonnette d'alarme : « Il n'y a pas de solution magique, il faut des moyens et notamment des moyens humains. »

Interrogée après le nouveau piratage, Fanny De Coster, secrétaire générale de la CGT Finances publiques a rappelé que la CGT avait « largement alerté » sur les risques liés notamment à la « dette informatique » accumulée aux Finances publiques. Elle pointe directement le manque de moyens : « Les moyens budgétaires pour développer la sécurité informatique sont largement insuffisants. »

Si former les agent·es et rappeler les règles de vigilance est nécessaire, la cybersécurité ne peut pas reposer sur leurs seules épaules. La direction reconnaît elle-même que protéger ses données exige des moyens techniques et humains. C'est précisément ce que la CGT revendique.

DGFiP : près d'un tiers des emplois de titulaires supprimé depuis 2008

Cette fragilité informatique doit aussi être replacée dans le contexte plus large de l'évolution des moyens de la DGFiP. Certes une cyberattaque ne s'explique pas par les seules suppressions d'emplois, **mais peut-on sérieusement sécuriser les données de millions de contribuables tout en réduisant, année après année, les effectifs et les moyens de la DGFiP ?**

Dans une lettre adressée aux député·es le 30 janvier 2026 sur la loi de finances, Fanny De Coster pointait l'ampleur des suppressions d'emplois : « Depuis sa création en 2008 jusqu'en 2026, la DGFIP aura subi 32 596 suppressions d'emplois temps pleins, correspondant à 29 % de ses emplois de titulaires. »

La CGT alertait déjà sur les conséquences de cette politique le 29 octobre 2024, dans son courrier d'interpellation des élu·es de l'Assemblée nationale et du Sénat : « Les suppressions d'emplois, les restrictions

budgétaires et la destruction du réseau de proximité de la DGFiP freinent sa capacité en termes d'action publique et dégradent les conditions de travail des agents. »

Des compétences stratégiques à préserver face aux cyberattaques

Sécuriser les données suppose aussi de disposer des compétences nécessaires. Or, face aux niveaux de rémunération proposés dans le privé, la fonction publique peine à recruter et surtout à fidéliser les spécialistes dont elle a un besoin croissant.

Aussi, la CGT demande « la revalorisation de toutes les carrières » pour restaurer l'attractivité des concours et donner à la DGFiP les effectifs nécessaires afin de « conserver la maîtrise de son Système informatique et développer une informatique au service des agent·es et des missions de service public ».

Cette bataille ne date pas d'hier. Dès janvier 2018, à l'occasion du lancement du programme gouvernemental Action publique 2022, la CGT réclamait « un recrutement d'informaticiens au niveau nécessaire à l'exercice des missions » et défendait une informatique « au service de tous les agents et de tous les contribuables ».

Cybersécurité : pour la CGT, l'État doit investir

La DGFiP continue d'investir dans l'informatique, mais la question est celle des priorités données à ces investissements. Pour Fanny De Coster, ils répondent avant tout à une logique d'« efficience », davantage tournée vers les économies d'emplois que vers la sécurisation des systèmes : « En langage administratif, ça veut dire qu'on investit pour pouvoir supprimer de plus en plus d'emplois. Ce n'est pas sur la cybersécurité. » (écouter l'émission " Cyberattaques : nos données ne sont-elles en sécurité nulle part ? " du 8 août 2026)

Le nouveau piratage donne une actualité particulière à ces revendications.

Sur le site La Vie Ouvrière, le 20 août 2026, Fanny De Coster estime que « les investissements depuis des années ne sont absolument pas à la hauteur des enjeux » et considère que « la cybersécurité devrait être un enjeu au plus haut niveau de l'État ».

Pour la responsable CGT, il faut donc s'attaquer aux causes structurelles plutôt que gérer les crises les unes après les autres : « Ils essayent d'éteindre des feux qu'ils allument eux-mêmes mais sans régler jamais le problème de fond. »

Et la réponse ne peut pas davantage consister à faire porter la responsabilité sur les personnels. À propos des mesures de formation et de sensibilisation annoncées après l'attaque, Fanny De Coster alerte dans le même entretien sur le risque de laisser penser que « ceux qui auraient failli dans l'histoire sont les agents des finances publiques ».

Protéger les données des contribuables, c'est donner des moyens à la DGFiP

Dès lors que l'État collecte et conserve les données personnelles de millions de contribuables, il a la responsabilité d'en garantir la protection. Pour assurer cette mission comme toutes celles du service public, les agent·es doivent disposer des moyens humains, techniques et financiers nécessaires. Protection des usager·es et moyens du service public vont de pair.

La réponse ne peut pas se limiter à demander davantage de vigilance aux personnels. La cybersécurité nécessite des emplois, des qualifications reconnues, des rémunérations permettant de recruter et de conserver les compétences, des investissements informatiques à la hauteur et la maîtrise publique des savoir-faire stratégiques.

Après des années de suppressions d'emplois et de restrictions budgétaires, il faut changer de logique : redonner à la DGFiP les moyens humains, financiers et techniques de protéger les données, les agent·es et le service public, aussi dans l'intérêt des usagers !