FNEC FP 53

PIRATAGE DE L'ÉDUCATION NATIONALE : DONNÉES DES PERSONNELS, DES ÉLÈVES ET DES FAMILLES EXPOSÉES, SERVICES BLOQUÉS, CONDITIONS DE TRAVAIL DÉGRADÉES, ET ENCORE LE DÉMERDENTIEL…

À QUELQUES JOURS DE LA RENTRÉE, L'ÉDUCATION NATIONALE DE NOUVEAU DANS LE CHAOS

La colère monte dans les écoles, les établissements et les services de l'Éducation nationale.

De très nombreux personnels enseignants et non enseignants (personnels administratifs des services, chefs d'établissement, AESH…) se retrouvent privés d'accès à leurs outils professionnels, parfois depuis plusieurs semaines : messagerie académique, applications de gestion, outils administratifs et systèmes d'information nécessaires au fonctionnement du service public.

Les remontées du terrain sont alarmantes : des collègues ne peuvent plus accéder à leur messagerie professionnelle ou aux applications nécessaires à leur travail ; des remplaçants ne peuvent pas être missionnés normalement ; des directrices et directeurs d'école n'ont plus accès aux outils de gestion des élèves (ONDE…) ; des personnels des DSDEN ayant repris le travail se retrouvent bloqués et avec des conditions de travail dégradées ; des chefs d'établissement et les personnels administratifs sont confrontés aux mêmes difficultés, la gestion des avancements et promotions est bloquée…

Et alors que la paie doit être préparée, le ministère doit répondre immédiatement : le versement des salaires pourra-t-il être assuré normalement la semaine prochaine ?

À une semaine de la rentrée, ce sont encore les personnels qui paient les conséquences de cette situation.

Le 31 juillet, le ministère de l'Éducation nationale reconnaissait officiellement avoir été victime d'une intrusion frauduleuse dans l'un de ses systèmes d'information, susceptible d'avoir conduit à l'exfiltration de données personnelles concernant un nombre important d'agents. Le ministère indiquait alors que les investigations se poursuivaient.

Depuis, la situation apparaît beaucoup plus grave et des données personnelles auraient été massivement exfiltrées, exposant ainsi les agents de l'Éducation nationale. D'après les éléments dont nous disposons, en dépit du silence du ministère, l'attaque pourrait concerner bien au-delà des seuls personnels : élèves, enseignants, personnels administratifs mais également parents et responsables légaux.

Environ **1,22 million d'élèves distincts, 4,35 millions d'identifiants de personnels et environ 602 000 comptes académiques** pourraient apparaître dans les données revendiquées. **L'ampleur exacte de la compromission n'est toujours pas établie par le ministère.**

Mais le problème est suffisamment grave pour que la question soit posée publiquement. Le risque est réel : une telle accumulation de données peut faciliter les tentatives d'hameçonnage ciblé, l'usurpation d'identité, les fraudes et les attaques visant directement les personnels, les élèves et leurs familles.

Comment l'État peut-il demander aux personnels, aux élèves et aux familles de faire confiance aux outils numériques de l'Éducation nationale lorsque leurs données les plus personnelles sont ainsi exposées ?

Alors, qui est responsable ?

Si les hackers sont responsables de l'attaque, cela ne dispense en rien l'État et le gouvernement de leurs responsabilités.

Depuis des années, les gouvernements successifs imposent suppressions de postes, réductions de moyens et réorganisations permanentes à l'Éducation nationale.

Pendant ce temps, l'administration dépend toujours davantage d'outils numériques complexes et interconnectés pour faire fonctionner les écoles, les établissements et les services.

Qui a décidé de supprimer des milliers de postes dans l'Éducation nationale ?
Qui organise depuis des années la réduction des moyens humains et matériels du service public ?
Qui porte la responsabilité de garantir la sécurité et la continuité des systèmes d'information de l'État ?
Qui doit garantir la protection des données personnelles des agents, des élèves et des familles ?

Le ministère rappelle lui-même qu'il est responsable de nombreux traitements de données personnelles. Ce même ministère a recours très régulièrement à des sous-traitants pour la gestion de ces données. Le recours à des prestataires ne fait pas disparaître la responsabilité du ministère : **l'État doit garantir la sécurité et la protection des données dont il assure le traitement.**

Et ce n'est malheureusement pas la première alerte. En mars 2026, le ministère avait déjà reconnu une intrusion dans son système RH COMPAS. **Environ 243 000 agents, stagiaires ou titulaires** étaient concernés par l'exfiltration de données personnelles comprenant notamment des éléments d'identité et des coordonnées.

Combien faudra-t-il encore de fuites de données pour que le gouvernement prenne la mesure de la situation ?

« Qui aurait pu prédire ? »

Le gouvernement peut toujours expliquer qu'une cyberattaque est imprévisible. Mais qui pouvait ignorer que des systèmes informatiques concentrant les données de millions de personnes constituent une cible majeure ?

Qui pouvait ignorer que la sécurisation de ces systèmes nécessite des personnels qualifiés, des moyens techniques et humains, des investissements et non une politique d'austérité continue ?

Réduction drastique des moyens, suppression des postes, fragilisation des services publics, transferts des responsabilités… c'est bien le gouvernement qui organise les conditions d'un fonctionnement dégradé.

Après les salaires insuffisants, les milliers de suppressions de postes, la dégradation continue des conditions de travail par des contre-réformes imposées aux personnels…

Voici maintenant un État qui n'est même plus capable, à une semaine de la rentrée, de garantir à ses agents l'accès normal à leurs outils de travail et qui doit répondre à de graves interrogations concernant la protection de leurs données personnelles et celles des élèves et des familles.

La fédération FO de l'enseignement en Mayenne exige :

- le rétablissement immédiat et complet des accès aux outils professionnels nécessaires au fonctionnement des écoles, des établissements et des services ;
- qu'aucun personnel ne soit tenu responsable des conséquences des dysfonctionnements informatiques qu'il ne maîtrise pas ;
- une information transparente et complète des personnels, des élèves et des familles sur la nature exacte des données compromises ;
- que chaque personne concernée soit individuellement informée des risques et des mesures de protection à prendre ;
- la mise en œuvre de toutes les mesures nécessaires pour garantir la sécurité des données ;
- la transparence totale sur les systèmes concernés, les conditions de l'intrusion et les éventuels recours à des prestataires ou sous-traitants ;
- les moyens humains et financiers nécessaires pour assurer la sécurité et la continuité du service public ;
- **l'augmentation des salaires**
- **l'arrêt des suppressions de postes et des politiques d'austérité qui désorganisent l'Éducation nationale**

La FNEC-FP FO 53 refuse que les personnels soient une nouvelle fois sommés de *« faire avec »*.

Elle n'acceptera pas que les agents soient rendus responsables d'un chaos dont ils ne sont pas responsables.

Salaires, postes, conditions de travail, sécurité des données et continuité du service public : les personnels ont toutes les raisons d'être en colère.

La FNEC-FP FO 53 est à leurs côtés et organise la résistance pour défendre les droits et les conditions de travail des personnels de l'Éducation nationale. **Pas de moyens, pas de rentrée scolaire !**

A Laval, le 20/08/26

FNEC-FP ***FO*** 53, syndicats ***FO*** de l'enseignement, de la culture et de la formation professionnelle
6 rue Souchu Servinière, 53000 Laval
06 52 32 30 45 – @ : 53@fo-fnecfp.fr