_swissprivacy.law

La décision France Travail, ou le prix du risque identifié mais non traité

Philippe Zanon, le 26 août 2026

Le 22 janvier 2026, la CNIL a infligé une amende de EUR 5 millions à FRANCE TRAVAIL pour plusieurs défauts de sécurité que l'opérateur avait lui-même identifiés, sans les corriger à temps. L'occasion de revenir sur cette décision au vu de la récente cyberattaque révélée cette mi-août contre la DGFiP.

5 millions d'euros d'amende, 36,8 millions de personnes touchées et un constat implacable : chacune des défaillances sanctionnées avait été identifiée par FRANCE TRAVAIL lui-même, avant que les mesures censées y répondre ne soient différées.

La délibération n° SAN-2026–003 du 22 janvier 2026 détaille, grief par grief, ce qui était concrètement attendu de l'opérateur au titre de son obligation de sécurité au sens de l'art. 32 RGPD, et ses enseignements dépassent la seule frontière française. Un peu de contexte avant d'entrer dans le détail qui servira pour la suite.

FRANCE TRAVAIL est une institution nationale publique dotée de la personnalité morale et de l'autonomie financière (cf. art. L. 5312–1 du code du travail). Le décret n° 2022–1161 du 17 août 2022 a créé un traitement des données de santé nécessaires à l'accompagnement adapté des demandeurs d'emploi en situation de handicap, dont l'opérateur et les organismes de placement spécialisés CAP EMPLOI sont conjointement responsables (cf. art. D. 5312–51 du code du travail).

FRANCE TRAVAIL a ainsi ouvert son applicatif métier à environ 2'300 salariés des 98 structures CAP EMPLOI, associations autonomes et indépendantes de l'opérateur.

Entre le 6 février et le 5 mars 2024, des cyberattaquants ont usurpé plusieurs de ces comptes au moyen de techniques dites d'ingénierie sociale. Concrètement, ces derniers ont manipulé des salariés pour obtenir leurs identifiants et mots de passe, sans forcer la moindre barrière technique.

Une activité anormale avait été relevée le 29 février sur le système de mesure des performances, mais l'alerte n'a été prise en compte que le 4 mars en fin de journée et les investiga-

tions engagées le lendemain. 25 gigaoctets de données concernant 36’820’828 personnes ont été exfiltrés, notamment des données relatives à l’état civil, le numéro de sécurité sociale (NIR) ou encore l’adresse postale, les coordonnées de contact et le statut de demandeur d’emploi. Étaient visées les personnes inscrites au cours des vingt dernières années, mais aussi les simples titulaires d’un espace candidat. La violation a été notifiée le 8 mars 2024 et un contrôle sur place a suivi.

La co-responsabilité n’allège pas la charge de celui qui maîtrise le système

FRANCE TRAVAIL soutenait que les CAP EMPLOI, co-responsables du traitement, devaient assumer une part des mesures de sécurité, la documentation contractuelle leur attribuant expressément la charge de leur propre environnement de travail. En s’appuyant sur l’arrêt IAB Europe (CJUE, 7 mars 2024, IAB Europe, C-604/22 ; pour une analyse de l’arrêt, cf. swiss privacy.law/303/), la CNIL confirme que celle-ci ne se traduit pas nécessairement par une responsabilité équivalente. En effet, la Commission rappelle que le niveau de responsabilité de chacun s’apprécie au regard des circonstances de l’espèce.

Or, l’examen des conventions révèle que FRANCE TRAVAIL s’engageait à mettre en œuvre les mesures de sécurité technique des outils mis à disposition, à contrôler le respect des règles d’habilitation et à ordonner, le cas échéant, la déconnexion des environnements insuffisamment sécurisés. Force est par conséquent de constater que c’est bien FRANCE TRAVAIL qui était réellement responsable de la sécurité du système d’information, ce que la CNIL retient à juste titre en jugeant que « c’est à FRANCE TRAVAIL que revient en premier lieu l’initiative du déploiement et du pilotage des mesures destinées à assurer la sécurité de son système d’information ». La conclusion s’imposait : celui qui conçoit, héberge et administre le système en détermine les règles de sécurité.

Ce que la CNIL reproche concrètement à FRANCE TRAVAIL

L’obligation de sécurité au titre de l’art. 32 RGPD est une obligation de moyens. Il s’agit non pas d’empêcher toute attaque, mais de déployer des mesures appropriées au risque. En l’espèce, le risque était considérable entre volumétrie du traitement, NIR et données de santé. C’est au regard d’un tel risque que la formation restreinte de la CNIL a examiné les quatre manquements retenus, qui procèdent tous de cette seule et même obligation.

Le premier grief porte sur la robustesse de l’authentification.

En effet, la politique en vigueur imposait des mots de passe d’au moins huit caractères combi-

nant trois types de caractères, ce qui correspond au second cas prévu par la recommandation de la CNIL relative aux mots de passe et autres secrets partagés (délibération n° 2022-100 du 21 juillet 2022) et appelle donc une mesure de restriction complémentaire.

Or le compte n'était verrouillé qu'après 50 tentatives infructueuses (sic !), contre 10 au maximum selon cette recommandation, sans qu'aucun autre mécanisme (exemple : un captcha) ne compense ce seuil. La CNIL relève que cette vulnérabilité n'a pas été exploitée par les attaquants, mais retient toutefois le manquement à l'obligation de sécurité au sens de l'art. 32 RGPD en raison du risque qu'il fait peser.

Ce premier grief mérite qu'on s'y arrête car il est le plus instructif !

Les attaquants disposaient des identifiants et des mots de passe. De ce fait, le seuil de 50 tentatives n'a joué aucun rôle dans la survenance de la violation. Le manquement a toutefois été retenu car la CNIL a suivi le raisonnement de la jurisprudence de la Cour de justice de l'Union européenne, selon laquelle la survenance d'une violation ne suffit pas à caractériser un manquement à l'art. 32 RGPD, pas plus que son absence ne démontre la conformité (en ce sens, CJUE, 14 décembre 2023, VB c. Natsionalna agentsia za prihodite, C-340/21 ; pour une analyse des conclusions de l'avocat général, cf. swissprivacy.law/230/).

Cela amène à considérer que la conformité s'apprécie au regard du caractère approprié des mesures déployées, et non à la lumière du scénario d'attaque effectivement réalisé. Ainsi, un contrôle déclenché par un incident peut aboutir à sanctionner des vulnérabilités entièrement étrangères à cet incident, ce que la CNIL rappelle avoir déjà fait, par exemple s'agissant du stockage de mots de passe en clair (en ce sens, délibération n° SAN-2022–018 du 8 septembre 2022) ou encore en cas d'absence de politique d'habilitation (en ce sens, délibération n° SAN-2021–019 du 29 octobre 2021).

Le deuxième grief (le plus lourd) tient à l'absence d'authentification multifacteur.

En effet, les analyses d'impact réalisées en 2022 identifiaient précisément le risque et prévoyaient un déploiement pour 2023 que la CNIL avait accueilli favorablement dans son avis. Toutefois, la mesure a été repoussée à avril 2024, FRANCE TRAVAIL faisant valoir que la fourniture des seconds terminaux incombait contractuellement aux CAP EMPLOI. Or, selon la formation restreinte, il appartenait à FRANCE TRAVAIL en sa qualité de développeur et d'hébergeur de l'outil d'apprécier la faisabilité de la solution retenue et de l'adapter, par exemple, par la distribution de calculettes OTP. Est également rejetée l'idée qu'une telle mesure aurait été inopérante face à l'ingénierie sociale dès lors qu'elle aurait rendu l'authen-

tification des attaquants extrêmement difficile.

À ce stade, il convient de préciser que cette doctrine est antérieure à la délibération n° 2025-019 du 20 mars 2025 relative à l'authentification multifacteur qui l'a consolidée. La nécessité d'une telle mesure avait déjà été soulignée par l'ANSSI dans ses recommandations relatives à l'authentification multifacteur et aux mots de passe de 2021, puis par la CNIL en 2022 (cf. délibération n° 2022-100 précitée) et en 2024 dans son guide de la sécurité des données personnelles, et la formation restreinte avait même retenu dès 2018 qu'elle aurait été de nature à empêcher une violation de données (cf. délibération n° SAN-2018–011 du 19 décembre 2018).

Le troisième grief vise l'exploitation des journaux d'activité de l'applicatif métier, c'est-à-dire l'enregistrement horodaté des opérations effectuées par les utilisateurs dans l'outil.

En effet, FRANCE TRAVAIL disposait d'une journalisation conservée un an et d'un centre des opérations de sécurité, mais aucun dispositif ne générait d'alerte. Les anomalies étaient pourtant considérables, qu'il s'agisse des horaires et de la fréquence des requêtes, du taux d'erreur de 69 % sur l'un des comptes usurpés ou encore, pour la seule journée du 6 février 2024, des neuf gigaoctets extraits (soit l'équivalent de plus de treize millions de fiches pour un unique conseiller !). La collecte des traces ne suffit toutefois pas. C'est la CNIL elle-même qui l'exige dans sa recommandation relative à la journalisation (délibération n° 2021-122 du 14 octobre 2021), laquelle réclame un système de traitement et d'analyse permettant de générer des alertes. Circonstance aggravante, elle avait déjà appelé l'attention de l'opérateur sur ce point en 2022.

Enfin, le quatrième grief concerne les habilitations.

En ce sens, les conseillers CAP EMPLOI pouvaient consulter l'ensemble des données de tous les demandeurs d'emploi (y compris ceux qui ne bénéficiaient pas de l'obligation d'emploi) et modifier de leur seule initiative le périmètre géographique de recherche sans limitation. Si la CNIL admet l'utilité de ces accès, elle juge leur périmètre supérieur à ce qui est strictement nécessaire.

En définitive, la formation restreinte conclut que l'opérateur n'a pas mis en place des mesures techniques et organisationnelles adéquates et proportionnées aux exigences de l'art. 32 RGPD, alors même qu'il avait identifié la plupart de ces risques avant la mise en œuvre du traitement. Le constat est d'autant plus sévère que son système d'information a vocation à s'ouvrir à davantage d'acteurs du réseau pour l'emploi.

Sanctionner un établissement public : possible, mais discuté

De nombreux manquements étant constatés, restait la question de la sanction. FRANCE TRAVAIL a tenté de s'en sortir autrement. L'opérateur contestait en ce sens le principe même de l'amende, l'art. 20 de la loi Informatique et Libertés excluant les traitements « mis en œuvre par l'État ».

Toutefois, la formation restreinte interprète strictement cette exception et lui oppose la notion voisine de traitement mis en œuvre « pour le compte de l'État », qui n'en bénéficie pas. En effet, la CNIL relève que l'opérateur dispose de la personnalité morale et d'un budget financé pour un tiers seulement par l'État, le reste provenant de contributions obligatoires des employeurs. L'amende était donc possible, sans qu'une mise en demeure préalable soit requise. Sur le quantum, la CNIL retient une négligence grave au sens de l'art. 83 RGPD dès lors que les analyses d'impact avaient listé les risques exacts qui se sont matérialisés plus de deux ans plus tard. Les 5 millions d'euros, pour un plafond légal de dix millions, s'accompagnent d'une injonction de justifier la mise en conformité sur les quatre points, sous astreinte de 5'000 euros par jour de retard, ainsi que d'une publication qui n'identifiera plus l'opérateur à l'expiration d'un délai de deux ans.

Cette sanction appelle cependant de nombreuses réserves et laisse sceptique. Une amende infligée par une autorité publique à un opérateur public dont le budget provient, directement ou indirectement, de la collectivité interroge sur son effet réellement correctif, dès lors que c'est, in fine, le contribuable qui règle la facture.

Un passage moins commenté mérite pourtant l'attention. FRANCE TRAVAIL demandait à la formation restreinte, plutôt qu'une amende, de lui enjoindre d'allouer une somme déterminée à la sécurisation de son système d'information, ce qui est une proposition plutôt séduisante pour un organisme dont chaque euro provient de la collectivité. Elle est toutefois écartée en deux temps. D'une part, l'injonction et l'amende ont des objets distincts, la première visant à faire cesser une pratique, la seconde à sanctionner des manquements passés. D'autre part, il n'appartient pas à l'autorité de contrôle de flécher les attributions budgétaires de l'organisme qu'elle contrôle.

Ce qu'il faut en retenir, en France comme en Suisse

Quatre réflexes se dégagent de cette décision.

D'abord, une analyse d'impact qui identifie un risque et planifie une mesure crée une véri-

table dette de conformité. En effet, si elle est en principe conçue comme un outil de maîtrise des risques, une analyse d'impact se mue en pièce à charge lorsque les mesures qu'elle annonce restent lettre morte. Tout report doit donc être daté, motivé et compensé par une mesure intermédiaire, faute de quoi il documente la négligence au lieu de la prévenir.

Ensuite, la répartition contractuelle des rôles entre co-responsables n'exonère pas celui qui développe et héberge le système. Ainsi, des clauses dans un contrat qui répartissent les coûts ne déplacent pas l'initiative des mesures de sécurité, laquelle demeure attachée à la maîtrise effective de l'outil.

En outre, la journalisation ne vaut que par son exploitation. Ainsi, collecter des traces sans les analyser en continu ne protège de rien.

Enfin, une politique d'habilitation se mesure au périmètre effectivement consultable par chaque utilisateur, non aux profils théoriquement définis.

Les lecteurs suisses auraient tort de n'y voir qu'une affaire française, car chacune des défaillances sanctionnées trouve un répondant en droit suisse.

En effet, l'exigence d'une authentification robuste et d'une sécurité adaptée au risque découle de l'art. 8 LPD, dont le Conseil fédéral a précisé les exigences minimales aux art. 1 à 6 OPDo. Le besoin d'en connaître, qui fonde le quatrième grief, est formulé presque à l'identique à l'art. 3 OPDo, qui impose de restreindre l'accès de chaque personne autorisée aux seules données nécessaires à l'accomplissement de ses tâches. La journalisation défaillante du troisième grief correspond à une obligation expresse de l'art. 4 OPDo, applicable aux organes fédéraux et, notamment en cas de traitement automatisé de données sensibles à grande échelle, aux personnes privées. Quant à la détection tardive de l'attaque, elle aurait directement mis à l'épreuve l'obligation d'annoncer au PFPDT, dans les meilleurs délais, toute violation entraînant vraisemblablement un risque élevé (art. 24 LPD).

La différence décisive tient à l'aval. La LPD ne connaît pas la sanction administrative dès lors que l'art. 61 let. c LPD punit d'une amende de 250'000 francs au plus la violation intentionnelle des exigences minimales de sécurité, mais cette sanction pénale vise la personne physique responsable, l'entreprise ne pouvant être condamnée à sa place que dans des cas précis (art. 64 LPD renvoyant à la Loi fédérale sur le droit pénal administratif, RS 313.0). Surtout, ces dispositions pénales ne visent que les personnes privées.

Transposée en Suisse, une telle affaire se dénouerait donc tout autrement. En effet, un

organe fédéral placé dans la situation de FRANCE TRAVAIL n'encourrait aucune sanction, et la menace pénale pèserait plutôt sur les épaules de ses collaborateurs, une divulgation de données personnelles secrètes relevant du secret des fonctions (art. 320 CP). A défaut, le devoir de discrétion au titre de l'art. 62 LPD prendrait le relais.

Le PFPDT, dont la surveillance s'étend pourtant aux traitements des organes fédéraux (art. 4 LPD), devrait quant à lui s'en tenir aux mesures administratives telles que la modification, la suspension ou encore la cessation du traitement (art. 51 LPD).

Ce résultat tient d'ailleurs moins au silence de la loi qu'à un renoncement assumé. Le Conseil fédéral a effectivement écarté l'idée d'armer le préposé d'un pouvoir de sanction contre les organes fédéraux lors des travaux de révision totale, estimant que la faculté d'interdire ou de suspendre leurs traitements et le renforcement du volet pénal de la loi suffisaient (en ce sens, Message LPD, FF 2017 6565, 6589). Le débat français sur la légitimité d'une sanction pécuniaire entre entités publiques est ainsi réglé en amont, par un choix délibéré du législateur Suisse.

L'exigence matérielle reste pourtant comparable. Un responsable suisse qui aurait, comme l'opérateur français, identifié le besoin d'une authentification multifacteur puis différé sa mise en œuvre pour des motifs budgétaires pourrait difficilement soutenir avoir assuré une sécurité adéquate au risque encouru.

L'actualité immédiate donne du reste à la décision un écho particulier, et une raison de s'en souvenir. Le 14 août 2026, le ministère de l'Économie et des Finances a signalé une violation affectant le système d'information de la Direction générale des finances publiques (DGFiP), et la CNIL a indiqué le 18 août être saisie et pouvoir procéder à des vérifications. Cette fois, l'exception tenant aux traitements mis en œuvre par l'État pourrait bien trouver à s'appliquer. La décision France Travail n'en conserverait que davantage sa valeur d'étalon : celle de ce que l'obligation de sécurité exige, concrètement, d'un grand opérateur public.

Proposition de citation : Philippe Zanon, La décision France Travail, ou le prix du risque identifié mais non traité, 26 août 2026 *in* www.swissprivacy.law/416