Des données personnelles d'agents Insee en libre accès sur des serveurs à l'Insee, c'est possible ?
Oui ! Et la direction de l'Insee ne fait rien pour stopper cela !

Il s'agit de données administratives, parfois très sensibles comme des arrêts maladie, des coordonnées personnelles, des documents d'embauche pour les enquêtrices et enquêteurs, des comptes rendus d'évaluation, de déclarations de grève, …
Incroyable ?

Ce que nous trouvons incroyable c'est la légèreté avec laquelle la direction nous a répondu depuis 2020, quand nous avons dénoncé les premiers faits. Voici la liste des instances auxquelles nous nous sommes adressés :

- la direction régionale où ont été faites les premières découvertes ;
- la direction nationale en GT et en CTR ;
- l'unité dédiée à la sécurité des données ;
- le directeur général ;
- la Cnil.

Quelle place y aurait-il pour des lanceurs ou lanceuses d'alertes à l'Insee sur un sujet où l'Insee joue gros : la confiance de la population à nous confier ses données de manière sûre ? Aucune, à moins d'imaginer que c'est le seul fait que nous soyons des syndicats qui aient rendu la direction si désinvolte (qui pourrait l'imaginer ?), il y a tout lieu de croire que la direction de l'Insee, dans son sentiment de puissance, ne pouvait juste pas penser que de telles données pouvaient être laissées sans limitation d'accès.

Nous n'osons imaginer que maintenant, connue l'ampleur du problème, elle ne fera rien.

Lors du GT du 6 septembre dernier nous avons apporté en séance la preuve, dûment anonymisée, que sur des serveurs ouverts à toutes et tous figuraient (entre autres) des comptes rendus d'entretien professionnel réalisés par la secrétaire générale en 2012.
Ces serveurs ont été fermés peu de temps après...mais il en reste d'autres !

L'Insee se doit d'être irréprochable sur la sécurité des données. C'est un domaine en perpétuelle évolution technique mais dont une des failles les plus fréquentes sont les défauts d'organisation humaines et les « erreurs » qui s'ensuivent.

Or lors du CTR du 19 octobre où ce sujet a été traité, et malgré la litanie des exemples, la direction a ramené nos explications à de simples cas isolés de dysfonctionnements.
Rien qui ne montre de sa part le début d'une analyse de ce qui a amené à la situation actuelle et qui devrait être changé, rien qui ne mentionne les moyens et l'organisation en interne qui est à revoir.

C'est pourquoi nous redemandons :

- un plan de sécurisation mentionnant les moyens nécessaires, au long cours, modifiable au vu de l'évolution des outils et technologies ;
- une remise à plat des règles ;
- un plan de formations et informations régulières à tous les agents sur ces règles.

La direction ne s'est pas franchement engagée sur ces points : nous redisons solennellement que des données personnelles sont encore accessibles sur serveur, trois semaines après le CTR.
Si leur accessibilité à tous les agents n'est pas supprimée d'ici une semaine, nous ressaisirons la Cnil.

Chronologie

Voici toute l'histoire : de premières découvertes…qui en amènent d'autres

Tout a débuté après le premier confinement en 2020 : des agents d'une DR ont découvert sur un serveur partagé la présence d'un fichier nominatif avec les numéros de téléphone des agents, accessible à toutes et tous. Des données confidentielles dont la direction avait pourtant annoncé un traitement limité pendant le confinement.
Le fichier a été supprimé dès que signalé.

Mais par curiosité nous sommes allés voir dans d'autres dossiers, en accès libre : il y avait d'autres données, là plus grave : des données d'embauches d'enquêtrices et enquêteurs (adresses, dates de naissance...) jusqu'à...l'extrait de casier judiciaire non vide d'un candidat enquêteur qui n'a pas été embauché.
Nous avons à nouveau demandé la suppression de ces données, ce qui a tardé pendant l'été 2020 mais a été fait à l'automne.
De fait, à partir de ce moment nous avons refusé de simplement « signaler » les fichiers ne respectant pas une sécurisation minimum mais avons demandé plus largement :

- La réalisation d'un audit sur les serveurs de la DR.
- La rédaction d'une note permettant une connaissance par tous les agents des règles de mise à disposition des fichiers contenant des données personnelles.
- L'octroi de moyens afin que la vérification des accréditations et des contenus des fichiers soit réellement faite régulièrement.

Au vu de nos saisines répétées nous avons également déclaré la direction responsable de tels dysfonctionnements. Aucune consigne claire n'ayant été donnée, tant à la GIIR qu'aux agents, nous avons estimé qu'aucun-e agent-e « lambda » ne devait être tenu-e pour responsable des fichiers non protégés.

Nous avons saisi la direction nationale et avons signalé en GT en septembre 2020 de nombreux autres problèmes dans la gestion de la sécurité des données en interne : tel directeur qui met son calendrier Outlook accessible à tous permettant d'anticiper la nomination de responsables, l'ouverture totale aux fichiers tampons des mopieurs pourtant censés être sécurisés par mots de passe, et évidement les serveurs partagés.
Nous avons signalé également que les solutions pratiques pour échanger des données statistiques en interne étaient peu pratiques, peu connues, et aboutissaient trop souvent à des solutions non sûres.

Autant de petits accrocs à la bonne sécurisation des données qui montraient selon nous qu'un gros travail devait être fait par la direction de l'Insee.

La saisine et l'intervention de l'Unité « *Innovation et stratégie du système d'information* » (Unissi) de la DSI

Mais au printemps 2021, nous découvrons de nouveaux fichiers non sécurisés sur serveur : cette fois il s'agit de la découverte d'archives mél (2 à 3 giga de .pst) de la gestion administrative de tous les agents de la direction régionale . Tous les échanges mél du Sar avec les agents depuis plusieurs années : beaucoup d'administratif basique (récupérer les certificats d'abonnement de transport) des régularisations Sirhius mais aussi des scans d'arrêt maladie signés de médecins.

- Nous avons donc fait un courrier solennel au directeur général le 27 mai 2021, et sans réponse de sa part nous avons déposé une « plainte » à la Cnil en juin 2021 pour non respect du Règlement général sur la protection des données (RGPD).

- Après de nombreuses relances (il est vrai dans une période difficile avec confinements) l'« Unissi » a procédé à un audit des serveurs de la DR. Cet audit a conclu en août 2021 que la gestion des droits était « *conforme aux recommandations* ».
  Petit hic : les rapporteurs ont examiné le serveur de partage appelé « U: » et pas celui d'archives nommé « M: » (qui sert pourtant de base de travail à certaines unités), et qui était celui sur lequel figuraient des données personnelles des agents.

L'intervention de la Cnil en 2022 : un résultat ponctuel mais toujours pas d'électrochoc général

Cette intervention de la Cnil n'a eu lieu dans les locaux de la DR qu'en mars 2022. Ne voyant rien bouger après cette visite nous la sollicitons à nouveau à l'été 2022.
C'est seulement à ce moment que l'accessibilité des serveurs à toutes et tous est coupé.

Mais tout est loin d'être résolu : par manque de réponse de la direction, nous sommes allés voir sur des serveurs ouverts ce qui pouvait bien y être accessible. Nul besoin de connaissances en informatique pour cela.
Nous y avons découvert sur un serveur de la DG, entre autres, l'entièreté des archives courrier (un .pst) du secrétariat général entre 2009 et 2012. Y figuraient par exemple les comptes-rendus d'évaluation de hauts cadres de l'époque. La direction a fermé le serveur après que nous avons pointé l'anomalie.

Mais dans certaines DR on trouve encore en clair un tableau de compte rendu d'évaluation, dans une autre un accès à des archives méls d'une boîte qui ne devrait en aucun cas être accessible.

Nous n'avons pas fait d'examen systématique mais trop d'exemples montrent des accessibilités énormes : ce n'est pas à nous de faire ce travail de vérification, c'est à la direction de l'organiser : et après tant d'alertes nous considérons que la direction nationale en est responsable, pas les collègues qui n'ont pas eu de règles claires ni de consignes à appliquer !

Le 9 novembre 2022