RGPD

# Accès non-autorisé aux données : qui est responsable de quoi ?

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les différentes autorités de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question de la responsabilité dans le cas d'un accèsnon-autorisé par un employé aux données médicales d'un autre employé.

La plupart des obligations prévues par le RGPD pèse sur le responsable du traitement, défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul (...), détermine les finalités et les moyens du traitement* » (art. 4.7 RGPD).

L'article 32 du même texte indique que le responsable du traitement est tenu de mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ». En d'autres termes, le responsable du traitement est le garant de la sécurité des données personnelles qu'il traite dans le cadre de l'exercice de son activité. À ce titre, il lui appartient notamment de s'assurer que seules les personnes autorisées ont accès aux données personnelles, à savoir uniquement les personnes ayant besoin d'en connaître dans le cadre de l'exercice de leurs fonctions au sein de l'organisme.

L'article 33 du RGPD ajoute qu'« *en cas de violation de données à caractère personnel* », le responsable du traitement « *en notifie la violation en question à l'autorité de contrôle compétente (...), dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* ».

## L'affaire[1]

Ayant appris que sa supérieure hiérarchique avait eu accès à son dossier de santé avant de la licencier, la salariée d'un établissement de santé a déposé une plainte auprès de l'autorité belge de protection des données (l'APD) contre son employeur. L'enquête a montré que la supérieure hiérarchique avait consulté le dossier médical de la plaignante afin de vérifier que cette dernière était dans un état adéquat dans l'optique de lui annoncer son licenciement. Elle aurait agi en totale autonomie sans instruction de la part de l'établissement de santé.

Dans la mesure où la plaignante invoquait, l'illicéité de la consultation de son dossier médical pour défaut de base légale (article 6 du RGPD), la question se posait de savoir si l'établissement de santé, contre qui la plainte était dirigée, pouvait être considéré comme le responsable du traitement. L'APD a répondu par la négative, considérant que cette qualification devait être attribuée à la supérieure hiérarchique. « *Lorsque l'employé d'une organisation opère des traitements de données à caractère personnel dans le cadre des activités de celle-ci, le traitement est réputé avoir lieu sous l'autorité de l'organisation, a expliqué l'APD. Toutefois, il est des situations exceptionnelles dans lesquelles l'employé peut définir lui-même les finalités d'un traitement de données à caractère personnel outrepassant ainsi de manière illicite l'autorité*

*qui lui a été confiée (...).* » Plusieurs éléments ont été retenus par l'autorité de protection des données pour qualifier la supérieure hiérarchique de responsable du traitement : le fait que la décision de licenciement émanant de l'établissement de santé ne s'appuyait pas sur des éléments qui auraient été collectés lors de la consultation du dossier médical de la plaignante ; le fait que l'accès au dossier médical avait eu lieu à un horaire qui ne constitue pas un « *horaire de travail ordinaire* » ; et enfin le fait que l'établissement de santé avait entamé, du fait de cet accès non-autorisé, une procédure disciplinaire à l'encontre de la supérieure hiérarchique.

Ainsi, s'il n'était pas possible de sanctionner l'établissement de santé en raison de l'illicéité de l'accès au dossier médical par la supérieure hiérarchique, la plaignante estimait qu'une sanction devait être prononcée à l'encontre de son employeur qui n'avait pas notifié à l'APD cet incident. Son raisonnement était le suivant : l'établissement de santé est responsable du traitement concernant les activités liées à la gestion, au sein de l'hôpital, des dossiers patients. Il se devait donc, compte tenu de l'atteinte à la confidentialité des données de la plaignante du fait de cet accès non-autorisé, de notifier l'incident en ce qu'il constituait une violation de données.

L'APD a rappelé sa position, selon laquelle la notification est « *de principe* » et le fait de ne pas notifier la violation est « *l'exception* », étant précisé que : (i) pour se prévaloir de cette exception, le responsable doit démontrer que « *les conditions d'application sont effectivement réunies dans une situation donnée* » ; (ii) « *dans un souci de prudence et une perspective protectrice des droits et libertés des personnes concernées, un responsable du traitement devrait toujours, en cas de doute, notifier à l'APD une violation de données (...), même dans les cas où il considère pour plusieurs raisons que la violation n'est pas susceptible d'engendrer de risque pour les droits et libertés de la personne concernée, mais qu'eu égard aux circonstance de l'espèce, il ne peut pas en être tout à fait certain.* »

En l'espèce, l'APD a estimé que l'établissement de santé aurait dû notifier la violation de données : d'une part, parce que l'accès non-autorisé a porté sur des données de santé, sachant que la perte de confidentialité de ce type de données représente un risque pour la plaignante ; d'autre part, parce que l'établissement de santé ne pouvait pas être certain que la supérieure hiérarchique n'avait pas opéré cet accès pour des « *raisons cachées* » (même si cette dernière avait indiqué avoir été guidé par des motivations apparaissant comme « *louables* »).

Cela étant dit, l'APD a estimé que ce manquement – le défaut de notification - ne serait pas retenu contre l'établissement de santé, dans la mesure où à la date des faits (2020), le CEPD n'avait pas encore publié ses lignes directrices 01/2021 relatives aux violations de données et que, par conséquent, « *le niveau de la connaissance et de la pratique concernant la gestion des violations de données à caractère personnel ne se trouvait pas au même niveau qu'aujourd'hui* ».

## Quelles recommandations ?

On peut dire que l'établissement de santé s'en tire plutôt bien dans cette histoire. Il aurait dû notifier la violation de données, mais, pour autant, il n'est pas sanctionné parce qu'au moment des faits la connaissance sur ce sujet n'était pas celle d'aujourd'hui. À méditer...

Il convient de noter également que l'autorité belge de protection des données n'a pas challengé le responsable du traitement sur les mesures techniques et organisationnelles qui étaient en vigueur au moment où l'accès non-autorisé s'est produit. N'oublions pas que l'établissement de santé est tenu de garantir la sécurité des données et donc leur confidentialité. Il est étonnant que l'APD n'ait pas cherché à comprendre, au regard des règles d'habilitation en vigueur au sein de l'établissement, comment la supérieure hiérarchique a pu consulter le dossier médical de la plaignante. N'y a-t-il pas de surcroît une problématique d'atteinte au secret médical ?

**Alexandre FIEVEE**
*Avocat Associé*
*DERRIENNIC ASSOCIES*

Notes

(1) APD, Chambre contentieuse, 64/2025, 1re avril 2025.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

**Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info**