Le devoir d'informer l'autorité et le principe *nemo tenetur*

Célian Hirsch, le 24 mars 2021

Selon l'autorité néerlandaise de protection des données, l'obligation de lui transmettre le rapport d'une fuite de données n'est pas contraire au principe *nemo tenetur*.

Décision de l'*Autoriteit Persoonsgegeven* (Pays-Bas) du 26 novembre 2020 contre Stichting OLVG

Un hôpital situé à Amsterdam annonce à l'autorité néerlandaise de protection des données (*Autoriteit Persoonsgegeven*) qu'il a été victime d'une « violation de données », conformément à son obligation prévue par l'art. 33 par. 1 RGPD d'informer l'autorité compétente lors d'une fuite de données. Concrètement, l'hôpital transmet à l'autorité deux rapports de fuite de données concernant l'accès du personnel et des étudiants aux dossiers électroniques des patients.

L'autorité ouvre alors une enquête pour violation, par l'hôpital, de la sécurité du traitement au sens de l'art. 32 RGPD. En résumé, elle lui reproche de n'avoir pas prévu une authentification à deux facteurs lorsqu'un employé de l'hôpital voulait accéder aux dossiers électroniques des patients. Or l'hôpital traite des données extrêmement sensibles sur la santé d'environ 500'000 patients. Afin de protéger ces données de manière adéquate, un système de double authentification était nécessaire.

Pour sa défense, l'hôpital soulève la violation du principe *nemo tenetur ipsum accusare*, à savoir le droit de ne pas s'auto-incriminer (art. 48 de la Charte européenne des droits de l'homme et art. 6 CEDH).

Avant d'exposer l'argument de l'hôpital, il convient de rappeler la portée de ce principe ainsi que les obligations du responsable du traitement lorsqu'il est victime d'une fuite de données.

Selon la jurisprudence de la CourEDH, le droit de ne pas s'auto-incriminer est violé lorsqu'un suspect, qui est menacé de subir des sanctions pénales s'il ne collabore pas, livre les informations demandées ou est puni précisément pour avoir refusé de le faire.

En droit européen, lorsqu'un responsable découvre qu'il a été victime d'une « violation de données », il doit transmettre dans les 72 heures un rapport de la fuite à l'autorité compé-

tente (art. 33 par. 1 RGPD). Ce rapport doit décrire la nature de la violation, ses conséquences probables ainsi que les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation (art. 33 par. 3 RGPD).

S'il ne respecte pas cette obligation, il peut être sanctionné d'une amende pouvant s'élever jusqu'à EUR 10'000'000 ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total (art. 83 RGPD).

En l'espèce, selon l'hôpital, l'enquête a été ouverte uniquement en raison des rapports de fuite de données, lesquels ont été remis sous la menace d'une peine (art. 33 par. 1 RGPD *cum* art. 83 RGPD). Or sanctionner une personne grâce à des documents remis sous la contrainte est contraire au principe selon lequel personne n'est obligé de s'auto-incriminer.

Même si la jurisprudence de la CourEDH reconnaît que le principe *nemo tenetur* ne s'applique pas aux documents existant indépendamment de la volonté de la personne concernée, les rapports de fuite de données ne constitueraient pas de tels documents selon l'hôpital. En effet ces rapports auraient été établis précisément afin de respecter le devoir d'informer l'autorité de la fuite selon l'art. 33 par. 1 RGPD. Ils ont donc été établis sous la contrainte d'une sanction pénale, à savoir l'amende prévue par l'art. 83 RGPD.

L'autorité néerlandaise de protection des données rejette cette argumentation dans la décision commentée ici.

Premièrement, elle affirme que les deux rapports de fuite de données ont eu pour seul effet d'inciter l'ouverture d'une enquête contre l'hôpital. Ils n'ont toutefois pas servi de moyens de preuve de violation par l'hôpital de ses obligations de sécurité du traitement des données (art. 32 RGPD). Par ailleurs, l'art. 33 par. 5 RGPD prévoit que le responsable du traitement doit documenter toutes les violations de données. Les rapports de fuite constituent dès lors des documents existant indépendamment de la volonté de la personne concernée.

En outre, l'autorité néerlandaise n'a pas formellement demandé les rapports, même si elle a demandé un complément d'information suite au premier rapport. Le simple fait que le courrier de l'autorité contienne une référence au droit de l'autorité d'ordonner au responsable « de lui communiquer toute information dont elle a besoin pour l'accomplissement de ses missions » (art. 58 par. 1 RGPD) n'y change rien. Les informations n'ont donc pas été obtenues sous la contrainte.

Enfin, l'autorité souligne que, même si elle devait écarter certaines preuves découlant du

rapport, celui-ci contient des documents qui existaient déjà avant le rapport de fuite. Ils constituent en tout état de cause des documents indépendants. Par la suite, l'autorité a également recueilli des documents d'employés, auxquels le droit de garder le silence avait été rappelé.

Pour ces diverses raisons, l'autorité néerlandaise considère que l'amende infligée à l'hôpital ne contrevient pas au principe *nemo tenetur*.

Le raisonnement de l'autorité néerlandaise est-il entièrement convaincant ? Nous avons quelques doutes.

Premièrement, l'hôpital a été, selon nous, contraint de s'auto-incriminer. En effet, il n'avait que deux options : soit respecter son devoir d'informer l'autorité de la fuite (art. 33 RGPD), soit violer ce devoir et risquer une amende importante, laquelle doit être considérée comme de nature pénale au sens de la jurisprudence de la CourEDH (jurisprudence Engel c. Pays-Bas). L'hôpital n'a donc pas établi et transmis librement le rapport de fuite.

Deuxièmement, l'exception des *pre-existing documents* (documents existant indépendamment de la volonté de la personne concernée) est sujette à débat. La jurisprudence de la CourEDH reconnaît cette exception pour « les documents recueillis en vertu d'un mandat, les prélèvements d'haleine, de sang et d'urine ainsi que de tissus corporels en vue d'une analyse de l'ADN » (Saunders c. Royaume-Uni [GC], par. 69). Cette exception est justifiée par le fait que l'autorité peut dans tous les cas état saisir ces données, même si le suspect refuse de collaborer. Il est donc admis que même si l'autorité « contraint » une personne à lui fournir ces informations, le principe *nemo tenetur* ne s'applique pas pour ces documents.

À notre avis, il n'est pas convaincant d'appliquer cette exception aux rapports de fuite de données. En effet, ceux-ci sont établis précisément afin d'informer l'autorité compétente, voire les personnes concernées, de la fuite. Bien que certains documents du rapport puissent exister avant la fuite, ils ne deviennent intéressants pour l'autorité, et permettent de documenter la fuite, qu'une fois qu'ils sont liés à d'autres documents. Cet ensemble de documents, et le travail qui est déployé pour établir ce rapport, ne permet donc pas de considérer que certains documents, voire le rapport tout entier, constituent des *pre-existing documents*.

Enfin, il nous parait difficilement soutenable de prétendre que l'autorité aurait pu sanctionner l'hôpital sans les rapports de fuite de données. En effet, sans une quelconque information de la fuite, l'autorité n'aurait probablement jamais examiné si l'hôpital respectait le principe de la sécurité des traitements de données (art. 32 RGPD).

Notons que le législateur allemand, conscient de ce problème, a précisément adopté l'art. 43 al. 4 BDSG afin que le rapport de fuite de données ne puisse pas être exploité par l'autorité de contrôle afin de sanctionner le responsable du traitement.

À notre avis, cette même solution devrait s'imposer aux autres États membres de l'Union européenne. En effet, le fait d'utiliser le rapport de fuite de données contre le responsable du traitement constitue une violation de l'art. 48 de la Charte européenne des droits de l'homme et de l'art. 6 CEDH. Ce rapport devrait ainsi toujours être déclaré inexploitable dans une procédure visant à sanctionner le responsable du traitement (art. 83 RGPD).

Qu'en est-il de la situation helvétique ? Contrairement à l'avant-projet, la nLPD ne prévoit aucune sanction pénale lors d'une violation du devoir d'informer le Préposé fédéral d'une fuite de données (art. 24 nLPD). L'avant-projet avait d'ailleurs précisément été critiqué sur ce point. Selon nous, notre législateur a choisi une solution convaincante à cet égard : selon l'art. 24 al. 6 nLPD, le rapport de fuite ne peut pas être utilisé dans le cadre d'une procédure pénale contre la personne tenue d'annoncer la fuite, à moins que celle-ci y donne son consentement.

Proposition de citation : Célian Hirsch, Le devoir d'informer l'autorité et le principe *nemo tenetur*, 24 mars 2021 *in* www.swissprivacy.law/64

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.