Auto-incrimination et notification de violation des données

Julien Levis, le 17 avril 2021

La présente note revisite les fondements de la protection contre l'auto-incrimination ainsi que ceux de la procédure de notification des violations de données. Elle en déduit que la sanction prononcée sur le fondement d'un rapport de violation des données ne procède pas d'une forme d'auto-incrimination.

Le principe *nemo tenetur* (protection contre l'auto-incrimination) fait-il échec à l'utilisation du rapport sur la violation des données prévu à l'art. 33 du Règlement général sur la protection des données (RGPD) par une autorité de supervision ?

C'est la thèse récemment développée par un responsable du traitement (Hôpital d'Amsterdam) à l'occasion de poursuites engagées à son encontre devant l'Autorité de Protection des données néerlandaise (*Autoriteit Persoonsgegeven*) au titre d'une violation de données.

La décision a été commentée par Célian Hirsch. Ce dernier s'est montré sensible à un argument développé par l'Hôpital d'Amsterdam au soutien de sa défense : en vertu du principe de protection contre l'auto-incrimination l'*Autoriteit Persoonsgegeven* n'aurait – selon l'Hôpital – pas dû prononcer de sanction sur le fondement du rapport de violation des données (transmis par ce dernier en application de l'art. 33 RGPD).

La présente note ne reviendra pas sur la décision néerlandaise, mais se concentrera sur l'argument relatif à l'auto-incrimination. Un tel examen offrira en effet tout à la fois l'occasion de :

- Spécifier les circonstances visées par le principe *nemo tenetur*- limitées selon nous à l'exercice déloyal par des autorités de poursuite de leurs prérogatives – (I) mais aussi ;
- Préciser les bénéficiaires de la règle nemo tenetur (II), et enfin ;
- S'interroger sur la nature de l'obligation mise en place par l'art. 33 du RGPD (III). Envisager l'application du principe *nemo tenetur* au rapport de violation des données suppose une lecture répressive de l'art. 33 RGPD. Il nous apparaît par contraste important de souligner la dynamique collaborative mise en place par l'art. 33 RGPD entre

responsable du traitement et autorité de supervision.

I. Le principe *nemo tenetur*, garde-fou face aux autorités de poursuite (et non face au législateur)

La protection prétorienne contre l'auto-incrimination déduite par la Cour européenne des droits de l'homme (CourEDH) de l'art. 6 de la Convention européenne des droits de l'homme (CEDH) ne semble devoir s'appliquer que lorsqu'une contrainte a été exercée par une autorité de poursuite ou équivalente. Ceci ressort de la jurisprudence de la CourEDH en la matière : les décisions concernées visent en effet des menaces et manipulations intervenues au cours et à l'occasion de poursuites judiciaires[1].

Le rapport de violation des données visé à l'art. 33 RGPD est requis par le législateur communautaire et non sur demande d'une quelconque autorité étatique. La notification de violation de données constitue dès lors l'accomplissement spontané d'une obligation légale d'information et non un aveu de culpabilité obtenu sous l'effet d'une contrainte déloyale exercée par les autorités de poursuite.

L'utilisation de ce rapport par une autorité de supervision ne nous paraît à ce titre pas attentatoire au principe *nemo tenetur*.

La considération de la sanction assortissant l'obligation légale ne suffit du reste pas à faire de celle-ci la menace déloyale visée par la CEDH : la simple énonciation d'une obligation législative ne saurait par hypothèse constituer une menace illégitime.

II. Le principe *nemo tenetur,* règle destinée à protéger des personnes physiques (et non des personnes morales)

Si les garanties offertes par l'art. 6 CEDH sont en général applicables aux personnes morales, la question de cette applicabilité se pose concernant la protection contre l'auto-incrimination. Il semble d'ailleurs que toutes les décisions notables rendues par la CourEDH au visa de ce principe concernent des personnes physiques.

L'interdiction de l'auto-incrimination puise sa justification dans le souci d'éviter que l'autorité judiciaire n'use avec déloyauté de ses prérogatives et n'exerce une pression psychologique ou n'use de menaces ou de subterfuges pour provoquer des déclarations auto-incriminantes. Cette protection contre diverses formes de manipulation apparaît caractériser des menaces visant des personnes physiques et non morales[2].

En théorie, l'on peut imaginer une pression psychologique exercée sur des représentants de l'entreprise aux fins de les conduire à admettre la culpabilité de la personne morale.

Une telle hypothèse ne devrait toutefois plus être qualifiée d'auto-incrimination : elle ne correspond pas à une hypothèse d'incrimination de la personne morale par elle-même mais par une personne physique qui lui est tierce – fût-elle son représentant. Cette personne physique – potentiellement soumise au jeu de sa propre responsabilité personnelle – agit comme représentante mais concurremment en son nom propre. Incriminer la personne morale pourrait d'ailleurs dans certaines hypothèses constituer pour lui/elle une stratégie de défense.

En conclusion sur ce point, si contraindre le représentant d'une personne morale à incriminer celle-ci semble susceptible de porter atteinte au droit des personnes morales à un procès équitable, cette forme de déloyauté ne paraît pas ressortir de la prohibition de l'auto-incrimination. Le grief de manipulation d'un témoin (le représentant de la personne morale) par l'autorité de poursuite constituerait peut-être une piste d'analyse mieux adaptée.

III. La notification de violation des données, mécanisme de collaboration (et non de répression)

La notification de violation de données semble pouvoir s'analyser non comme une déclaration (auto) incriminante, mais comme une modalité de collaboration entre responsable du traitement et autorité de supervision. L'énumération –contenue à l'art. 33 RGPD – des informations à communiquer dans le rapport semble corroborer cette lecture :

1. Les éléments collectés portent sur la fuite elle-même (plutôt que sur l'analyse de ses causes) ;
2. Ils apparaissent destinés à identifier le risque résiduel pour les personnes concernées, pas les carences du déclarant ;
3. Ils incluent une présentation des éventuelles mesures correctrices adoptées (éléments susceptibles de venir à la décharge du déclarant).

Le *Working Party 29* (prédécesseur de Comité européen sur la protection des données) a lui-même insisté sur cette dimension collaborative et souligné notamment la possibilité qu'offrait la notification au responsable du traitement d'obtenir un avis de l'autorité de supervision sur la nécessité éventuelle de notifier l'incident aux personnes concernées[3].

La notification permet d'échapper à des sanctions aggravées : non celles procédant des éven-

tuelles carences techniques et organisationnelles sous-jacentes, mais celles qui sanctionneraient le défaut de notification lui-même.

Concernant les carences sous-jacentes, force est de constater qu'elles ont vocation à être potentiellement connues même en l'absence de notification. La notion de fuite de données, souvent assimilée à celle de violation de données tant elle en est le cas le plus topique, implique une rupture de confidentialité susceptible de porter l'incident, voire les données affectées, à la connaissance du grand public. On pense notamment aux forums relatifs aux incidents de sécurité informatique. Il est fréquent que ces derniers publient, rapidement après l'incident, des informations détaillées, lesquelles peuvent ensuite être reprises par une presse plus généraliste.

En procédant à une notification, le responsable du traitement facilite l'action du régulateur et lui fournit notamment les moyens de protéger les personnes affectées voire de nouvelles victimes potentielles. Le délai court de 72h – alors qu'il est plus long pour la notification aux personnes concernées – semble illustrer cette logique : rapidement averti, le régulateur peut adopter des mesures destinées à limiter l'impact de l'incident.

A titre purement illustratif, on pourrait dresser un parallèle – limité[4] – entre la notification de violation des données et les procédures dites de « plaider coupable » connues notamment des droits américains, italiens ou français[5]. La personne poursuivie y bénéficie de sanctions allégées en considération de sa coopération. De tels régimes seraient privés de toute efficacité si se déclarer coupable mettait systématiquement le déclarant à l'abri de toute sanction pour les faits révélés.

Alors que nous concluons, notons incidemment que l'art. 24 al. 6 de la nouvelle Loi suisse sur la protection des données (nLPD) semble formuler une règle proche de celle proposée par l'Hôpital d'Amsterdam : l'impossibilité d'utiliser l'annonce de violation des données dans une procédure pénale initiée contre le responsable du traitement.

Cette règle nous paraît toutefois refléter une spécificité du droit suisse le distinguant du droit européen. À la différence du RGPD, la nLPD repose encore largement sur des procédures pénales pour sa mise en œuvre. L'autorité de supervision suisse (le Préposé fédéral à la protection des données et à la transparence) dispose – en comparaison de ses homologues européens – de pouvoirs correctifs et de sanctions limités. Dans ce contexte de procédure pénale au caractère largement inquisitoire, la référence du législateur suisse au principe *nemo tenetur* revêt une autre résonance.

Proposition de citation : Julien LEVIS, Auto-incrimination et notification de violation des données, 17 avril 2021 *in* www.swissprivacy.law/70