La notion de protection des données dès la conception

Sylvain Métille, le 9 novembre 2020

Nous mettons en ligne, de manière périodique, les contributions d'auteurs externes nous ayant fait l'honneur d'accepter d'accompagner le lancement de Swissprivacy. Nous accueillons cette semaine la contribution de Sylvain Métille, Professeur associé à l'UNIL et avocat associé au sein de l'Étude HDC.

L'adoption le 20 octobre 2020 par le Comité européen de la protection des données des Lignes directrices 4/2019 sur la protection des données dès la conception et par défaut) est l'occasion de revenir sur la notion de protection des données dès la conception (« *privacy by design* »).

En bref, le responsable du traitement doit prendre, dès la conception du traitement, des mesures techniques et organisationnelles appropriées afin que le traitement respecte les principes relatifs à la protection des données et offre les garanties nécessaires afin de protéger les droits de la personne concernée (art. 25 RGPD, 7 nLPD et 5 LPDS).

Ce concept n'est pas nouveau. Il repose sur les sept principes développés notamment par Ann Cavoukian, ancienne Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada), qui ont été adoptés à fin 2010 par la 32e Conférence internationale des autorités de protection des données à Jérusalem (2010). Ceux-ci ont la teneur suivante :

1. prendre des mesures proactives et non réactives, des mesures préventives et non correctives (prévoir et prévenir les incidents liés à l'atteinte de la vie privée avant même qu'ils ne se produisent) ;
2. assurer la protection implicite de la vie privée (faire en sorte que les données personnelles soient protégées de manière automatique avec un paramétrage par défaut des nouvelles technologies assurant un niveau de protection maximum des données sans que l'utilisateur n'ait à définir de paramètres spécifiques) ;
3. intégrer la protection de la vie privée dans la conception des systèmes et des pratiques ;
4. assurer une fonctionnalité complète selon un paradigme à somme positive et non à somme nulle (assurer la protection de la vie privée sans nuire à la mise en œuvre d'autres fonctionnalités) ;

5. assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements ;
6. assurer la visibilité et la transparence (chaque élément intégré aux systèmes lié à la protection des données personnelles doit rester visible et transparent en cas de vérification indépendante) ;
7. respecter la vie privée des utilisateurs.

L'idée fondamentale de la protection des données dès la conception est de considérer que la majorité des violations de la sphère privée ne sont pas détectées. Plutôt que de chercher à réparer celles que l'on détecte, mieux vaut empêcher qu'elle ne se produise. Autre point important, il ne s'agit pas d'un jeu à somme nulle avec un gagnant et un perdant. La protection des personnes ne doit pas empêcher le traitement des données, mais il doit simplement garantir un traitement respectueux.

Cette obligation ne s'applique directement qu'au responsable du traitement, mais de fait elle doit aussi être prise en compte par les fabricants de produits, les prestataires de services et les développeurs d'applications. Plus on agit tôt, plus il est facile de rendre le traitement conforme.

Cette obligation n'est pas absolue, mais elle doit être proportionnée. Premièrement, les mesures prises doivent être aptes et efficaces. Deuxièmement, l'approche est basée sur la gestion du risque : on prendra compte de l'effort requis par ces mesures et des moyens techniques disponibles d'une part, ainsi que des risques que représentent le traitement pour les personnes d'autre part. Troisièmement, les mesures ne sont pas prises une fois pour toutes, mais doivent être mises à jour régulièrement.

Malgré le principe 2 ci-dessus, la protection des données dès la conception doit être distinguée de la protection des données par défaut, qui, dit de manière simplifiée, oblige le responsable du traitement à régler les paramètres par défaut sur le mode le plus protecteur de la sphère privée, l'utilisateur étant libre de les modifier. Pour des raisons pratiques évidentes, la concrétisation de ces deux principes est souvent traitée conjointement.

La protection des données dès la conception n'implique pas obligatoirement des mesures techniques compliquées. Par exemple, dans le cadre de l'obligation faite aux restaurateurs de collecter les coordonnées de leurs clients dans le cadre de la lutte contre l'épidémie de la COVID-19, le formulaire papier à l'entrée du restaurant qui expose toutes les informations des clients précédents n'est pas conforme. En revanche, le recours à des fiches individuelles à glisser dans une sorte de boîte aux lettres n'exige pas de mesures compliquées et seraient

un exemple concret de protection des données dès la conception.

Proposition de citation : Sylvain MÉTILLE, La notion de protection des données dès la conception, 9 novembre 2020 *in* www.swissprivacy.law/26

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