Compte-rendu du séminaire du 11 mars 2022 présenté par Dominique DURANT

Protection des données personnelles

M. DURANT a commencé par présenter son travail. Il est DPO (Data Protection Officer ou Délégué à la protection des données) chez FM Logistic, une entreprise de logistique basée à Phalsbourg, en Lorraine. Un DPO est une personne chargée de la protection des données personnelles au sein d'une organisation. Le travail d'un DPO est basé sur le RGPD (Règlement Général sur la Protection des Données), un règlement sur la protection des données personnelles, voté en avril 2016 et entré en vigueur le 25 mai 2018. Le RGPD s'applique à tous les pays membres de l'Union Européenne.

M. DURANT nous a ensuite énoncé les différentes obligations d'une entreprise concernant les données personnelles de leurs clients. Ces données identifient directement ou non une personne physique (nom, prénom, adresse, empreinte, etc). Les entreprises ont le droit d'utiliser ces données si le client l'autorise, mais il a le droit de modifier/demander la suppression de ces données. Des sanctions sont mises en place pour les entreprises ne respectant pas la réglementation. Une entreprise qui ne respecte pas cela ou qui utilise les données à d'autres fins sont passibles de sanctions allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel dans le cas d'une entreprise.

L'organisme qui s'occupe de vérifier que ce règlement est bien respecté se nomme la CNIL (Commission Nationale de l'Informatique et des Libertés). Elle s'occupe de vérifier que le RGPD est appliqué par les entreprises, mais également aider et accompagner les entreprises dans l'utilisation et le respect du RGPD.
Une entreprise peut également sous-traiter l'utilisation des données, sous l'autorité d'un responsable de traitement (personne qui détermine les finalités et les moyens d'un traitement). En général, tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel va sous-traiter les données.
Un sous-traitant qui traite des données pour le compte d'une organisation n'est pas responsable de ces données. En cas de litige, le responsable est la personne qui a décidé de mettre en place le traitement des données. Par conséquent, sous-traiter des données ne permettent pas d'échapper à des sanctions en cas de litige.
Un litige peut avoir lieu si les données collectées sont disproportionnelles ou si leur utilisation est disproportionnelle, par exemple si l'entreprise vend ces données à d'autres entreprises. De plus, un employeur n'a pas le droit de surveiller n'importe comment ses employés : il n'a pas le droit d'utiliser de key logger ni de surveillance des mouvements de la souris. Il n'a pas non plus le droit de regarder les mails ou messages marqués comme étant privés même si l'employé utilise en appareil fourni par l'entreprise.
En plus de l'amende, une entreprise peut voir son image dégradée car la CNIL partage les litiges importants.

L'entreprise doit permettre aux personnes d'être informées de ce que l'on fait de leurs données : comment elles sont utilisées, pourquoi, et qui y a accès. Les personnes disposent de nombreux droits concernant ces données, notamment le droit d'opposition au traitement,

le droit de rectification des données erronées ou encore le droit d'accès aux données.
De plus, s'il n'y a eu aucune interaction avec l'utilisateur depuis 2 ans, ses données doivent être supprimées. Les données ont donc une durée de conservation et sont limitées dans le temps. Dans un premier temps, les entreprises peuvent rendre les données anonymes pour de ne pas savoir à qui elles appartiennent avant de passer à un archivage définitif où l'on supprime définitivement les données.

Enfin, une entreprise n'a absolument pas le droit d'utiliser des données personnelles si la personne concernée n'est pas consentante. Ce consentement doit être un acte positif clair et univoque. De plus, l'utilisateur doit avoir la possibilité de retirer son consentement à tout moment. Si l'utilisateur est mineur, il doit avoir l'accord de ses parents.

Aujourd'hui, de plus en plus d'organismes utilisent nos données quotidiennement. Il est donc normal et nécessaire de règlementer ces utilisations pour éviter des abus et d'avoir le droit de savoir comment ces données sont utilisées. Malheureusement, le RGPD ne s'applique actuellement qu'au sein de l'Union Européenne et de nombreux abus qu'il est impossible d'arrêter ont encore lieu au-delà de ses frontières. Il est donc primordial d'étendre l'utilisation du RGPD partout dans le monde, pour le bien de tous.