La Tribune du DPO 2022 - ICTJournal

2022 : #Proportionnalité et Responsabilité

En ce début de nouvelle année, pourquoi ne pas convenir de nous comporter de manière responsable et avec proportionnalité tant dans le traitement de l'information en général que dans celui des données personnelles en particulier ?

Il en va de l'avenir de notre planète tout comme de notre intégrité numérique. En attendant que l'autodétermination informationnelle devienne réalité, prenons la mesure de ce que nous communiquons et de ce que nous stockons, faisons le tri entre le nécessaire et l'utile, agissons de manière proportionnelle et responsable.

Appliquons cette réflexion aux petites choses du quotidien, lors de nos innombrables échanges courriels par exemple. Évitons les détails non pertinents, utilisons les initiales plutôt que le nom des personnes concernées par le sujet, ne communiquons qu'aux personnes ayant besoin d'en connaître, soyons brefs, évitons les enchaînements de courriels sans fin, nommons nos échanges de manière pertinente.

Appliquons-la également au classement de nos arborescences informatiques, au classement de nos documents et de nos archives, et à lors de l'utilisation de nos CRM. Vérifions, ante, que les solutions technologiques que nous envisageons nous permettent de mettre en œuvre cette proportionnalité, et prenons conscience de la responsabilité qu'impliquent nos choix.

Appliquons-la, enfin, dans l'usage de l'intelligence artificielle. La proportionnalité, en particulier dans le traitement des données personnelles, et la responsabilité – juridique, sociale -, nous impose de faire preuve de discernement. Posons le cadre éthique et légal sur toute utilisation de l'intelligence artificielle, de manière à ce qu'elle soit, et reste, au service de l'humanité et nous permette de nous améliorer collectivement. Alors les craintes de Stephen Hawkins auront été vaines : « La création d'une intelligence artificielle serait le plus grand évènement de l'histoire de l'Humanité. Mais il pourrait aussi être le dernier ». – janvier 2022

*

David contre Goliath

Selon la tendance majoritaire, c'est en vain que les autorités de protection des données et les DPO s'époumonnent depuis plusieurs années à dire que l'usage de Google Analytics n'est pas conforme aux règles applicables au traitement des données personnelles. Il serait vain de lutter contre les GAFAM, tout-puissants et sans réelle concurrence, le combat serait perdu d'avance, c'est David contre Goliath, et puis la conformité en protection des données c'est bon pour les institutions publiques qui se doivent d'être exemplaire, et qui n'ont pas besoin de la masse d'informations statistiques que Google est capable de livrer. Or, depuis peu, le vent tourne, puisque comme le mentionne l'article ci-contre deux autorités de protection des données ont déclaré Google Analytics non conforme, les autorités autrichienne et française, tels des sherpas ouvrant la voie. Pour quel motif ? Pour l'heure, le discours se concentre sur le flux transfrontière généré par l'utilisation de cet outil statistique à destination des États-Unis, et le fait que ces transferts ne reposent plus - depuis juillet 2020, tout de même - sur un cadre juridique garantissant un traitement conforme, toutes les mesures complémentaires,

notamment contractuelles, ne permettant pas de pallier cette non-conformité : la législation des États-Unis autorise l'accès à ces données sur simple réquisition des autorités. Moi, bien modestement, tel le pèlerin avec son bâton, je rappelle que quoi qu'il en soit la conformité suppose que l'on respecte les principes applicables au traitement des données personnelles en particulier celui de la proportionnalité. Qui impose que l'on choisisse le traitement le plus apte à atteindre l'objectif, en traitant aussi peu de données que possible mais autant que nécessaire (eh oui) et que lorsqu'on a le choix du traitement on doit prendre le moins intrusif. Un outil statistique permettant la conformité, donc. Et il en existe. Pour mémoire, David a gagné contre Goliath. - mars 2022

*

Un responsable qui s'ignore

À lire le rapport ci-contre, comme DPO on ne peut que s'interroger. Les administrateurs ont-ils bien conscience de leurs responsabilités ? Certes ils doivent mener de front des politiques diverses et les nouveaux défis ne manquent pas. On n'est donc pas surpris de trouver en haut de la liste des thématiques 2021 et 2022 la digitalisation et l'automatisation. De là à trouver en dernière position la conformité…

Pour certains types de conformité légale, il est vrai que les conseils d'administration ont déjà dû de longue date mettre en œuvre les procédures permettant d'affronter les audits, en particulier financiers, ce qui peut expliquer que ce n'est plus une préoccupation. Mais qu'en est-il de la conformité en protection des données ?

Sur le terrain on ne peut que constater le bas niveau de maturité de la plupart des entreprises dans ce domaine. De plus, même si l'information ne fait pas la Une des journaux, on ne peut plus ignorer que la législation suisse a été modifiée, et que d'autres obligations légales attendent les responsables de traitement. La modification de la LPD ayant été publiée en automne 2020, avec certes une date d'entrée en vigueur à définir et qui est reportée à nouveau, on peut s'étonner que cette thématique soit négligée à ce point en 2021 et 2022.

Car qui sont les responsables de traitement ? Les actuels *maîtres de fichier* ? Aux termes de la loi suisse, il s'agit de la personne qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles. Dans les sociétés anonymes, nombre de traitements sont donc directement de la responsabilité du conseil d'administration. Et quand on décide de basculer du papier au numérique, ou d'atteindre le 100 % numérique, quand on vise l'automatisation ou la robotisation à l'aide de l'intelligence artificielle par exemple, on décide de nouveau traitement de données personnelles. Et le conseil d'administration répond des non conformités. – mai 2022

*

Ecologie et Conformité font la paire

Evidemment, ceux qui visent la prospérité trouveront cette chronique ennuyeuse car, c'est bien connu, on ne peut être heureux sans prospérité. Mais, comme le monde est toujours divisé en deux, elle plaira peut-être à celles et ceux qui pensent que 1) le bonheur ne se mesure pas à l'aune du compte en banque, 2) on peut être créatif, innovant et éco-responsable, et 3) l'écologie et la protection des données font bon ménage.

Et je le prouve. D'abord, la sobriété, que je prône en protection des données, est une alliée précieuse de la conformité, car moins l'on traite de données personnelles et pour la durée la plus courte, moins on stocke les données dans des pays lointains, moins on transfère d'informations non pertinentes ou à des personnes non directement concernées, et moins on court de risques dommageables de violations de données. C'est aussi une alliée de l'écologie car en économisant nos échanges électroniques et autres transfert numériques on agit sur la consommation en énergie et on limite les effets de serre. Pour aider la planète, on peut donc réfléchir à deux fois avant de prendre l'avion, mais aussi revoir nos habitudes dispendieuses de communication à tout va. Elles ont aussi en commun le bon sens, qui est un bon guide en protection des données : si l'on accepte de se remettre en question et de réévaluer nos pratiques en analysant, en amont, les besoins et les traitements nécessaires pour les combler, on arrive assez bien à respecter les principes applicables au traitement des données personnelles. Il en va de même pour les développements de la 5 G, de la smart city, de l'intelligence artificielle (très gourmands en énergie), qu'il ne s'agit ni d'interdire ni d'exclure mais d'intégrer intelligemment, après réflexion et dans l'intérêt commun.

En tous cas, il est certain qu'installer des serveurs sur la lune, comme en rêve une start-up américaine, ce n'est pas une solution. Ni pour l'écologie ni pour la protection des données. -juin 2022

*

On reprend les bases

Comme les lecteurs de la Tribune le savent bien, parmi les principes applicables au traitement des données personnelles on trouve le principe de sécurité, qui comprend trois aspects : la confidentialité, l'intégrité et la disponibilité des données.

Beaucoup de questionnements portent ces derniers temps sur la possibilité d'externaliser les données dans les clouds des grands fournisseurs de solutions américains, et leurs serveurs européens, en raison de l'inadéquation de la législation américaine et des risques de non-conformité. Si, pour les acteurs de la protection des données, la question se tranche par la négative s'agissant des autorités publiques qu'elles soient fédérales ou cantonales, elle doit être tranchée par le Responsable de traitement dans les organisations privées, qui en assume le risque. Or, désormais, ce n'est plus seulement la confidentialité voire l'intégrité des données personnelles qui doit nous inquiéter, mais également la disponibilité des données, possiblement mise à mal par la crise énergétique qui nous attend et les coupures d'électricité qui pourraient être ordonnées par la confédération.

Dans ce contexte, on rappellera les obligations et responsabilités des sous-traitants, telles que la nouvelle ordonnance sur la protection des données les décrits. Les sous-traitants doivent être connus mais également agréés par les Responsables de traitement, ils répondent, pour la partie qui leur est déléguée, de la conformité du traitement et de la sécurité des données et ils doivent participer activement au droit d'accès et à l'annonce des violations.

Au vu de ces risques de nature diverse et aux responsabilités qui y sont rattachées, il conviendra non seulement de bien choisir ses partenaires et sous-traitants, mais de bien délimiter les responsabilités des uns et des autres. Et de bétonner les clauses contractuelles. - Octobre 2022

*