La Tribune du DPO de l'année 2021, par Isabelle Dubois, in ICTjournal (rédac. Chef R. Koller)

https://www.ictjournal.ch/ https://adhocresolution.ch/

- Une obscure clarté (janvier 2021)

On peut, bien sûr, saluer l'effort déployé par d'aucuns pour communiquer de manière visuelle le message concernant le traitement de nos données, par des pictogrammes, si l'on considère qu'il s'agit d'un travail en cours d'élaboration. On peut aussi, à l'instar de la fédération romande des consommateurs, que je rejoins, se montrer pour le moins dubitatif sur le résultat de cet effort, pour plusieurs raisons.

Remémorons-nous les principes qui gouvernent le traitement des données personnelles : licéité, finalité, proportionnalité, exactitude, transparence, bonne foi et sécurité, auquel s'ajoute le droit d'accès. Par transparence, le législateur entend que les personnes concernées soient clairement informées sur les tenants et aboutissants du traitement considéré : quelles sont les données traitées, à quelles fins le sont-elles, comment, durant combien de temps et où les conserve-t-on, les transmet-on ou non à des tiers, cas échéant à qui et sur quelle base ; le droit d'accès suppose quant à lui que l'on sache quels sont nos droits et comment les faire valoir.

Las ! Soyons honnêtes, il faudra remettre l'ouvrage sur le métier. À l'exclusion peut-être du pictogramme se référant à la géolocalisation – reprenant un visuel connu des citoyennes et citoyens pour signaler la localisation – j'imagine que certains lecteurs et lectrices seront comme moi bien en peine de décrire par des mots les principes qui se cachent dans ces images. En outre, une trop grande simplification est source d'incomplétude, et pas forcément de conformité. Or, la personne concernée doit être pleinement informée et le traitement respectueux de tous les principes. En l'état, un texte reste indispensable.

Ayant commencé cette chronique par un oxymore (cette figure de style qui consiste à opposer des contraires pour renforcer l'effet) je m'autoriserais à l'achever par une citation : « ce qui se conçoit bien s'énonce clairement », écrivait Pascal. Pas très visuel, mais tellement parlant.

- Un mal pour un bien ? (avril 2021)

Selon les résultats d'une enquête, la pandémie a eu pour effet, dans les entreprises, de mettre l'IT au premier plan : plus de technologie est nécessaire pour commercialiser les biens et les services, pour répondre aux besoins générés par le télétravail et par les entretiens et conférences à distance, pour augmenter la numérisation, avec pour corolaire un besoin accru en personnel et en sécurité, particulièrement en cyber sécurité, ainsi que le recours à l'IA. La protection des données n'est pas oubliée, et l'on peut espérer qu'elle soit mise à sa juste place, à savoir au cœur des préoccupations à chaque fois que les technologies permettent, incluent

ou induisent le traitement de données personnelles, qu'il s'agisse de celles des collaborateurs et collaboratrices ou des clients et fournisseurs.

Pour ce faire, la mise en œuvre des projets devra être le fait d'équipes pluridisciplinaires. Seule la collaboration entre l'IT, le juridique, les RH, si possible coordonnée et accompagnée par un DPO, interne ou externe, permettra de garantir de l'efficacité, de la performance, de la rentabilité dans le respect des droits de la personnalité des uns et des autres. Le chef de projet aura à cœur de mettre en œuvre les exigences légales, en procédant à la protection des données dès la conception et par défaut, l'analyse d'impact en cas de risque élevé pour les droits de la personnalité, la mise à jour des conditions générales et clauses contractuelles avec tous les nouveaux sous-traitants, producteurs de solutions par lesquelles transiteront des données personnelles, sans oublier la formalisation des processus et la rédaction de règlements internes sur l'usage des outils et leur surveillance.

Tous ces changements et innovations sont aussi l'occasion de faire le ménage (suppression d'outils et applications obsolètes, destruction sécurisée de vieux dossiers). Si les entreprises jouent le jeu, alors on pourra dire que ce fut un mal pour un bien.

- Comparaison n'est pas raison, mais … (mai 2021)

On l'a vu, l'Union européenne se dote d'un cadre juridique ambitieux pour faire face aux défis de l'intelligence artificielle. A quel type d'autorité faudra-il confier sa mise en œuvre et le contrôle de la conformité ? Le débat s'initie déjà.
Jusqu'à présent j'étais plutôt favorable à la création d'une autorité de surveillance ad hoc en matière d'IA plutôt qu'à confier ces tâches aux autorités de surveillance en matière de protection des données. Mais pour de mauvaises raisons. Parce qu'elles n'ont pas en leur sein, aujourd'hui, les compétences et profils nécessaires.

Mais la réglementation proposée par la commission européenne et celle applicable au traitement des données personnelles ont de nombreuses similitudes. Leur but, déjà : donner un cadre de conformité, avec au centre le respect des droit fondamentaux, tout en favorisant ou permettant la circulation des idées versus des données. Les principes directeurs, ensuite, dont ceux de la sécurité, de la transparence, de la responsabilité, applicables sur tout le cycle de vie de la donnée, leur sont communs. Les outils à disposition pour contribuer à la conformité, que sont les analyses d'impact ou de risque, les systèmes de management de la qualité, les codes de conduite et certifications. Certaines obligations comme l'obligation de documenter les traitements, l'enregistrement des systèmes IA versus le recensement des traitements, l'obligation d'informer les personnes concernées. Et, enfin, le traitement de données personnelles.
Car si l'on exclut certains traitements peu risqués, les systèmes d'IA à haut risque – a fortiori ceux impliquant un risque inacceptable, interdits- auront tous comme base le traitement de données personnelles, voire sensibles pour le traitement desquels le RGPD s'applique.

Se doter d'une autorité de surveillance unique aux compétences et ressources renforcées aurait un avantage précieux : permettre d'éviter des conflits de compétence, positifs ou, pire, négatifs.

- La confiance à l'ère du numérique, un vœu pieux ? (été 2021, article complet)

Au début du siècle, les indices étaient au vert : technologies en forte expansion, innovation fulgurante, outils de travail performants. La douce illusion bercée d'insouciance que tout irait de mieux en mieux fut douchée par les révélations de lanceurs d'alerte. Et la confiance fut rompue. A jamais ?

Sans doute pas, mais…Si tout le monde s'accorde à dire qu'il faudrait restaurer la confiance des utilisateurs que nous sommes vis-à-vis des solutions technologiques qui nous sont proposées, deux écoles semblent co-exister quant à la faisabilité de cette mission.
Pour les uns, c'est peine perdue. Nous dépendons trop, parfois totalement, de systèmes et solutions informatiques créés par des géants en perpétuelle lutte concurrentielle, et leur modèle économique rend vaine cette quête.
Pour les autres, c'est possible car la technologie le permet, manque la volonté, y compris politique, d'investir dans le développement de solutions labellisables, et la nécessité de viser, en fonction de la sensibilité des données concernées, le bon niveau de sécurité[1].

Pour ma part, mon cœur balance, entre éternel optimisme et dure réalité et, s'il existe, le chemin pour restaurer la confiance à l'ère du numérique me semble semé d'embûches.

Tout d'abord, la notion de confiance doit être prise au sérieux, et l'on doit faire en sorte que le fond et la forme se rejoignent, que les termes utilisés soient bien descriptifs des processus et non de pure façade. Combien de solutions nous ont été vendues en jouant sur le pouvoir des mots – dans mon domaine, des outils « RGPD conformes » vendus très cher par des commerciaux devenus pour l'occasion spécialistes de la conformité.

Ensuite, la conformité est une condition sine qua non. J'aime constater qu'une fois encore revenir aux principes qui président au traitement des données personnelles, que je rappelle en toute occasion, comme une litanie dans l'espoir qu'ils s'impriment dans les consciences, serait un bon fil rouge. Ainsi, traiter les données pour une finalité connue et légitime, autant que nécessaire mais aussi peu et longtemps que possible, de manière sécurisée et selon une confidentialité dictée par la finalité et la nature des données, dire ce que l'on fait et faire ce que l'on dit, est indispensable pour (re)créer la confiance.

[1] Exprimé en particulier par Jean-Henry Morin in La Responsabilité numérique – restaurer la confiance à l'ère du numérique, éd. fyp, 2014, qui évoque également le prérequis de conformité que je mentionne ici

Dans l'ensemble des données informatiques à considérer se trouve un nombre significatif de donnés qualifiées par la réglementation de personnelles. Restaurer la confiance suppose donc d'être capable et déterminé à traiter les données personnelles d'une manière conforme aux règles de protection des données. Dans ce cadre, c'est tant le Responsable de traitement, organe décidant des finalités et des moyens du traitement, que le sous-traitant qui sont responsables de la conformité du traitement, le second dans la mesure de la part de traitement qui lui a été déléguée. Le principe de la protection des données dès la conception et par défaut – obligation figurant tant dans le RGPD que dans la LPD modifiée – sera donc incontournable.

Cette conformité dépendant non seulement du prestataire mais également du client, elle n'est pas si facile à atteindre. Mais si de co-responsables ils deviennent co-acteurs de la conformité, alors la confiance sera restaurée.

*