La Tribune du DPO de l'année 2020, par Isabelle Dubois, in ICTjournal (rédac. Chef R. Koller)
https://www.ictjournal.ch/ https://adhocresolution.ch/

- Lorsque l'écologie rejoint la protection des données (janvier 2020)

On me dit souvent que c'est « peine perdue » pour les tenants de la protection des données, car les technologies permettant le traitement de données personnelles se multiplient, les bases de données s'interconnectent, les scandales en la matière montrent l'impuissance des autorités de contrôle à faire respecter les réglementations. Je réponds qu'une chose reste possible, c'est de multiplier les sensibilisations et les formations sur les règles à respecter en la matière, de manière que chacun d'entre nous puisse agir à son niveau. De bonnes pratiques simples à mettre en œuvre et sans coût existent que je résume dans une attitude de sobriété dans la communication. Il s'agit de supprimer définitivement les courriels devenus inutiles, les versions bêta des documents, mais aussi de privilégier l'envoi d'un nouveau courriel à la réponse à un courriel qui répond lui-même un courriel,..., de répondre à la personne concernée uniquement plutôt qu'à toute la république, enfin de ne communiquer que l'essentiel et de pseudonymiser ou d'anonymiser les informations quand cela est possible. De cette manière, en limitant le traitement, l'exploitation, la communication, la conservation d'informations personnelles on limite de fait les violations des règles applicables.

Or, voilà que ces mesures participent également à la sauvegarde de la planète : la sobriété numérique est prônée comme une des mesures simples que tout un chacun peut prendre pour limiter les coûts environnementaux de l'hyper connectivité. Ne serait-ce pas le début d'un cercle vertueux que je vois poindre ?

- Compteurs intelligents : quels enseignements tirer de la mise en demeure de la CNIL ? (Février 2020)

Comme ICTjournal le rapporte (voir p. 33), deux grands fournisseurs d'électricité se sont fait épingler pour ne pas avoir correctement traité la question du consentement des utilisateurs, et prévu des durées de conservation trop longues. En Suisse, rappelons que la loi sur l'approvisionnement en électricité a été modifiée en deux phases, avec l'ouverture progressive du marché régulé par l'Etat, d'abord aux grands consommateurs, puis aux petites entreprises et aux ménages. La multiplication des acteurs augmente le risque relatif au traitement des données personnelles, mais la loi sur l'électricité renvoie expressément à la LPD.

Les lecteurs de la Tribune savent désormais que tout traitement doit respecter les principes de licéité, finalité, proportionnalité, exactitude, bonne foi, transparence et sécurité. Le consentement du consommateur relève de la licéité, mais aussi de la finalité et de la transparence : le client doit comprendre ce qui sera collecté, à quelle(s) fin(s), quelle sera la

durée de conservation et si des tiers pourront y accéder. Chaque finalité doit faire l'objet d'un consentement (qui doit donc être spécifique), et tous les consentements doivent être donnés en pleine connaissance des tenants et aboutissants (donc éclairés). Il convient également de distinguer les données qui sont nécessaires à l'approvisionnement en électricité et déterminantes pour la facturation, de celles qui visent d'autres fins. C'est à cette catégorie qu'appartiennent les données de consommation dites fines (à la demi-heure), or elles peuvent révéler des informations sur la vie privée (heures de lever/coucher, périodes d'absence, le nombre de personnes présentes dans le logement). Là le consentement doit être spécifique, éclairé, et express. Le Préposé fédéral a fait une fiche sur le sujet :

https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/l_utilisation-de-compteurs-electriques-intelligents.html

- Le sens de l'équilibre (mars 2020)

C'est une situation historique que nous vivons, dont nous nous serions bien passés. Nos repères ont disparu, on hésite sur le comportement à avoir. La peur pousse les uns à la retenue, les autres aux excès, le courage devient témérité, voire inconscience.

En protection des données l'on connaît le principe de proportionnalité : le traitement des données personnelles doit être nécessaire, adéquat et apte à atteindre l'objectif, et proportionnel au résultat attendu. La gestion de crise connaît également la pesée des intérêts lorsque, les faits établis, la gouvernance apprécie la situation et définit les mesures à prendre.

En ces temps troublés, où les procédures et organisations habituelles sont dépassées, inadaptées, il est important de pondérer les intérêts des uns et des autres : préserver la santé publique, préserver les collaborateurs, préserver les emplois, et agir dans le cadre légal. Notons que le droit, lui aussi, connaît les situations d'urgence. L'Etat d'urgence décrété par les autorités permet de prendre des mesures que la crise seule justifie. Ce n'est pas la loi de la jungle pour autant, car les mesures prises le sont à titre provisoire, et l'urgence ne signifie pas absence de procédures, mais nouvelles procédures.

Ainsi, l'on traitera les données personnelles, y compris sensibles, qui sont nécessaires en l'occurrence, pour préserver les intérêts jugés prépondérants, sans omettre de définir, d'ores et déjà, la durée du traitement – ou l'évènement à la survenance duquel le traitement prendra fin -, les mesures prises pour sécuriser les données, et leur suppression une fois la finalité atteinte.

Ainsi donc, se préoccuper du respect des droits fondamentaux durant la crise reste légitime, et restreindre ces droits dans la mesure nécessaire à la sauvegarde de la santé publique l'est

tout autant. Aujourd'hui, les coupeurs de cheveux en quatre sont tout autant à craindre que les hors-la-loi.

Oui, en temps de crise, il faut avoir le sens de l'équilibre.

- Bonnes – et moins bonnes – pratiques en télétravail (mai 2020)

Le télétravail a beaucoup d'avantages, plus de liberté, moins de places physiques de travail, plus de place dans les transports publics, moins de pollution, plus de temps, moins de perte de temps, etc., et la crise a démontré qu'il est possible, même dans des environnements qui ne l'envisageaient ou ne le souhaitaient pas. Mais s'il doit durer il doit être durable au sens socio-économique du terme.

Notons que les droits et obligations des uns et des autres – les employeurs et les employé-es-ne changent pas au motif que le mode de travail change. Et c'est dans la mise en œuvre de ces droits et obligations qu'il faut être attentif.

Le travailleur a droit au respect de sa sphère privée et de ses droits de la personnalité, au versement du salaire contre une prestation définie et un horaire respectueux des lois. L'employeur a le droit d'obtenir le rendement attendu, de donner des instructions et d'obtenir leur respect, il a droit à la diligence et à la fidélité des salarié-es. Ces droits se transforment en obligations comme par effet de miroir. Alors comment les mettre en œuvre, sachant que l'employeur est le garant de la santé et de la sécurité au travail de ses employées ?

En définissant par écrit le cadre dans lequel le télétravail s'inscrit. En choisissant des outils fiables, sûrs, respectueux des règles applicables aux données personnelles, qu'il s'agisse des outils de travail en eux-mêmes – plateformes d'échange, vidéoconférence, supports de données, ou des mesures de surveillance du rendement. En disant ce que l'on fait et en faisant ce que l'on dit. En gardant à l'esprit que certains outils gratuits ont un coût. En bannissant les logiciels expions.

Dans le contexte du télétravail, le choix du CYOD plutôt que du BYOD, et l'élaboration d'un règlement interne respectueux des droits et obligations de chacune et chacun sont gages de réussite et de durabilité. Les lecteurs trouveront une information utile du SECO sur l'ergonomie au télétravail ici.

- Flux transfrontières de données avec les Etats-Unis : appeler un chat un chat (septembre 2020)

Lorsqu'un responsable de traitement souhaite transférer des données personnelles à l'étranger, il doit s'assurer avant toute chose que le pays destinataire possède une législation d'un niveau sensiblement identique à celui de l'Union européenne ou de la Suisse. Sinon, il

doit prendre des mesures complémentaires, parmi lesquelles on compte les clauses contractuelles. Bon. Pour faciliter le flux transfrontière avec les Etats-Unis tout en garantissant un niveau suffisant de sécurité, ont dès lors été élaborés tout d'abord le Safe Harbor puis, en vigueur jusqu'il y a quelques semaines, le Privacy Shield, soit un ensemble de clauses de protection conventionnelles négociées par les autorités.

Pourquoi ces cadres de sécurité ont-ils été annulés ? Parce qu'un examen judiciaire des garanties offertes par ces outils en a révélé l'insuffisance. Le premier, le Safe Harbor, ne permettait pas l'exercice du droit d'accès par les personnes concernées, réservant ce droit aux seuls ressortissants américains. Le second, le Privacy Shield, n'empêche pas la violation des droits des personnes concernée : Selon la Cour, les limitations de la protection des données qui découlent de la réglementation interne des États-Unis sur l'accès et l'utilisation, par les autorités publiques américaines, des données transférées depuis l'Union, ne sont pas suffisamment encadrées et violent le principe de proportionnalité, car les programmes de surveillance des autorités américaines ne sont pas limités au strict nécessaire.

Bien sûr, on ne peut pas dire – et encore moins écrire – que c'est la législation actuelle des Etats-Unis, et la volonté des autorités de surveiller largement la population comme les données d'où qu'elles viennent, qui empêche le transfert d'être conforme aux règles européennes, et que toutes les clauses contractuelles que des partenaires pourraient conclure n'y changeront rien. Mais on peut le penser.

- Nouvelle LPD, quoi de neuf pour les Responsables de traitement ?

Sous réserve d'un référendum, la LPD modifiée votée les 25 septembre dernier comporte quelques nouveautés, que les entreprises soumises également en tout partie au RGPD connaissent déjà.

L'obligation de déclarer certains fichiers au Préposé fédéral disparaît au profit d'une obligation de tenir le registre des traitements (il s'agit de référencer les fichiers ou applications contenant des données personnelles). Des exceptions pour les entreprises de moins de 250 personnes seront prévues par ordonnance, mais il s'agit d'un bon outil de gestion dont je recommande la tenue.

Les violations de données – vol, altération, accès indu à des données personnelles – devront être annoncées au Préposé fédéral dans les meilleurs délais (ainsi qu'aux personnes concernées selon les circonstances) et documentées.

Une analyse d'impact devra être effectuée pour tout nouveau traitement susceptible d'enfreindre les droits des personnes concernées. Une telle analyse est d'ailleurs déjà recommandée car elle permet de prendre les mesures techniques et organisationnelles

nécessaire à la conformité du traitement, avant de déployer la solution ou de la mettre sur le marché. On peut mettre cela en lien avec l'obligation – nouvelle en tant que concept – de protection des données dès la conception et par défaut. Celle-ci concerne tant le responsable de traitement – qui doit garantir et pouvoir établir la conformité du traitement – que le sous-traitant – qui doit permettre à son client d'être conforme en configurant le produit dans ce but. Le droit à l'information et le droit d'accès à ses données personnelles sont quant à eux renforcés, de même que l'exigence d'obtenir un consentement express pour le traitement des données sensibles, éclairé dans le sens que l'on comprend les tenants et aboutissants du traitement, et distinct pour chaque finalité.

Du neuf, donc mais rien d'insurmontable, et une heureuse harmonisation des notions avec le RGPD.

- Le casse-tête des bandeaux cookies

Ne pas en avoir, c'est discutable voire illégal. En mettre un « pour la forme », c'est pareil, même pire. Et casse-pied, il faut bien le dire. Un vrai casse-tête. Mais tout problème a sa solution. Et celle-ci réside dans la coopération entre l'organisationnel et la technique.

Revenons aux bases : on met un tel bandeau sur les sites internet parce que les internautes doivent savoir ce qui est traité les concernant, et pouvoir accepter ou non ce traitement lorsqu'il n'est pas indispensable. C'est pourquoi la phrase affirmative (nous utilisons des cookies …) ne laissant que le choix d'être d'accord (j'ai compris/J'accepte) n'est conforme que pour des cookies indispensables, dits fonctionnels (sont inclus les traceurs des paniers d'achat pour un site marchand, ou les mesures d'audience sans profilage). Si on utilise des cookies de traçage à des fins de publicité ciblée, alors on doit avoir le consentement des personnes concernées. Ce qui conduit à offrir le choix : l'internaute peut soit se dire réellement d'accord, soit tout refuser ou paramétrer lui-même les cookies. Et là, ça doit être du concret, pas une illusion : en un clic, l'internaute doit se retrouver sur une page lui permettant des décocher ce qui ne lui convient pas avec un effet réel et démontrable. Dans un tel cas de figure, la phrase doit mentionner les deux types de cookies et leur finalité, et l'internaute peut cliquer sur Tout accepter ou Paramétrer. Une fois le consentement obtenu, nul besoin de reposer systématiquement la question au même internaute. Certes, le consentement doit pouvoir être retiré en tout temps, mais un lien sur les cookies et leur paramétrage depuis les CGU suffira. Ah, parce qu'il faut des CGU ? Oui, transparence oblige…

AD HOC RESOLUTION ICTjournal

A noter que les outils de traçage et d'analyse ne sont pas un espace de jeu pour le marketing, mais doivent servir les intérêts bien compris du Responsable de traitement, avec sinon son impulsion, du moins son consentement éclairé.

*