La Tribune du DPO de l'année 2019, par Isabelle Dubois, in ICTjournal (rédac.chef R. Koller)[1]

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

- Quand les extrêmes ne se rejoignent pas (Février 2019)

L'un part, l'autre reste. Le premier, docteur en droit, s'est mis au service de la protection des données il y a 38 ans, avec flegme et rigueur, fermeté et cordialité, compétence et persévérance. Jean-Philippe Walter a quitté à fin janvier 2019 sa fonction de Préposé fédéral suppléant à la protection des données et à la transparence. Il a co-fondé – et préside actuellement- l'Association francophone des autorités de protection des données, il a participé à la création de la plateforme de sensibilisation thinkdata.ch avec la soussignée et bien d'autres, et on lui doit aussi la Journée annuelle de la protection des données personnelles, qui se tient tous les 28 janvier. Il reste heureusement actif, en particulier auprès du Conseil de l'Europe. Bon vent, Jean-Philippe, et chapeau bas. Le second est sans nul doute un ingénieur astucieux et créatif, pour qui le respect de la sphère privée n'a aucun sens ni aucun intérêt- surtout lorsqu'il concerne les autres- sauf l'intérêt commercial qui, bon an mal an, le conduit à faire amende honorable. On reconnaîtra à Marc Zuckerberg le mérite de n'avoir jamais caché son jeu, et ceux qui s'émeuvent des dernières affaires le concernant ont la mémoire courte car *the Social network* a toujours eu pour ambition d'interconnecter toutes les informations que ses utilisateurs jugent bon de communiquer.

À quand un réseau social protégeant les données personnelles dès la conception et par défaut ?

- Les objets connectés, et moi et moi et moi (Mars 2019)

Toutes sortes d'objet sont aujourd'hui connectés avec ou sans fil. Cela a commencé par le calcul de nos pas et des calories dépensées, cela s'est glissé ensuite dans nos montres, puis nos maisons. Enfin, certaines, car ce n'est pas demain que mon frigo passera commande pour moi, je vous le dis. Le DPO se préoccupe de la sécurité de ces objets et je vais y venir, mais le citoyen ferait bien de s'interroger aussi sur l'aspect philosophique des choses : sommes-nous encore connectés à notre conscience ?

Et puis les jouets de nos petits ont été connectés aussi, et là, on ne rigole plus. Quelles mesures prendre pour éviter le pire en termes de violation des droits de la personnalité ? J'en vois deux, à notre portée. D'une part, se préoccuper des fonctionnalités de l'objet telles que le constructeur les a prévues, et privilégier les objets paramétrables. D'autre part, sécuriser l'accès par un mot de passe, désactiver le partage automatique des données, éteindre l'objet ou l'appareil quand il ne sert pas. L'attention doit être renforcée pour les jouets connectés, car si nounours a des capteurs, il va sans doute collecter des images ou conversations intimes. Las !

- Du nouveau en Protection des données (Avril 2019)

Ce 1er mars 2019 est entrée en vigueur la Loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS), du 28 septembre 2018.

[1] Une chronique de 2000 caractères insérée dans ICTjournal depuis début 2019

AD HOC RESOLUTION

ICTjournal

Les lecteurs se souviennent peut-être que le Parlement avait choisi de scinder en deux la modification de la LPD, et de s'atteler dans un premier temps aux modifications nécessaires à l'intégration de l'acquis de Schengen (soit le traitement des données personnelles par les organes fédéraux à des fins pénales). Conçue comme une loi de transition, cette loi comprend diverses nouvelles dispositions. C'est ainsi que le Préposé fédéral obtient de nouvelles compétences d'enquête et de décision, et que plusieurs définitions ont été revues et complétées. Le *profil de la personnalité* s'appelle désormais, comme dans le RGPD, *profilage*. Que recouvre cette notion ? toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation, et cætera. Pour ce type de traitement le consentement exprès, éclairé, de la personne est requis. À cela s'ajoute l'obligation, déjà prévue par le RGPD et reprise dans la deuxième phase de modification de la LPD, de s'assurer de la conformité du traitement dès sa conception. C'est dans ce contexte légal que le projet de Migros d'offrir à ses clients des offres personnalisées découlant directement de l'analyse de leur panier d'achat s'inscrit. Bien sûr, dans ce profilage-là, le client est volontaire et c'est son propre panier d'achat qui est analysé pour une offre qui n'est adressée qu'à lui. Reste que la sécurité des données, le droit d'accès et leur suppression sur demande devront être garanties. À suivre, donc.

- Cybersécurité et Protection des données, des cousins par alliance (Mai 2019)

J'entends souvent dire en entreprise que l'on respecte la protection des données *puisque* l'on fait de la cybersécurité. Les responsables de la sécurité de l'information s'occupent effectivement de la sécurité des données personnelles de l'entreprise dans le cadre de leur fonction. Mais j'aime à rappeler que le principe de sécurité en protection des données personnelles, qui doit conduire le responsable de traitement à garantir la confidentialité, la disponibilité et l'intégrité des données, n'est qu'un des sept principes applicables au traitement des données personnelles. Par ailleurs, ce que l'on entend par donnée personnelle n'est pas toujours clair, pour qui n'a pas été formé. Et la distinction entre les données personnelles et les données sensibles est rarement maîtrisée. Souvent les données fiscales ou salariales sont considérées par ces mêmes responsables de la sécurité de l'information comme des données sensibles ou très sensibles. Or, la protection des données ne connaît pas de données plus ou moins sensibles, et liste les catégories de données personnelles qui sont qualifiées de sensibles et qui doivent être traitées avec plus de circonspection : uniquement si le traitement est nécessaire et qu'il repose sur une base légale ou sur le consentement exprès de la personne concernée. Enfin, comme son nom l'indique la cybersécurité couvre la problématique de la sécurité de l'information numérique, alors que la loi sur la protection des données vise un traitement conforme pour toute donnée personnelle, quel que soit le support dans lequel elle est structurée. Si les cartothèques papier n'existent pratiquement plus, il n'est pas rare en entreprise ou en organisation d'avoir encore en format papier les dossiers du personnel, ou les dossiers des bénéficiaires ou des usagers. Ainsi, les domaines d'application de la cybersécurité et de la protection des données, s'ils s'interconnectent, ne se recouvrent pas.

AD HOC RESOLUTION

ICTjournal

- RGPD, le verre à moitié plein ou à moitié vide (Juin 2019)

On peut constater les effets négatifs induits par le RGPD – baisse de confiance des utilisateurs, mesures insuffisantes de mise en conformité ou au contraire usines à gaz coûteuses et peu durables, ou réduire le Conseiller en protection des données en entreprise suisse à un simple « déclareur de fichiers » – ce qui revient à méconnaître la loi - et minimiser son rôle par rapport au DPO, ou délégué à la protection des données du RGPD. On peut voir le verre à moitié vide, mais selon moi, ces constats ou *avis d'experts* plus ou moins pertinents sont chose normale en période de transition.

Pour ma part, je préfère voir le verre à moitié plein : on parle, enfin, de protection des données, même si pour beaucoup de petites entreprises suisses seule la loi fédérale s'applique ; on revoit les procédures de travail, désormais conscient des risques et enjeux. Les obligations légales en matière de protection des données, c'est avant tout du bon sens, de la conscience professionnelle, une saine gestion des actifs, et le respect d'autrui. Ainsi, un an après le RGPD, je constate une prise de conscience salvatrice des entreprises suisses de petite et moyenne taille, et un réel plaisir à prendre ensemble le chemin vers la conformité, en toute sérénité quand l'accompagnement est adapté au contexte. Car cette mise en conformité permet au dirigeant de reprendre la main sur ses données, et cela est rassurant.

Et lorsque des utilisateurs exigent qu'on supprime leurs données, c'est non par défiance mais par *ras-le-bol* d'être traités comme une marchandise. Car la bonne nouvelle dans ces nouvelles règles, et celles encore à venir, c'est que l'on reparle des droits fondamentaux : la dignité humaine, la liberté personnelle et le respect de la vie privée. N'oublions pas en effet que ces règles viennent d'une Convention internationale à vocation universelle (Convention 108+), dont le préambule porte sur la nécessité de garantir l'autonomie personnelle.

- WhatsApp Messenger. What else ? (Septembre 2019)

Le phénomène se répand dans tous les milieux : dans les loisirs, en sport, entre collègues, entre amis, entre membres d'une même famille, entre copains d'école. Il touche tous les milieux professionnels, scolaires, sociétaux : on crée un groupe WhatsApp pour partager des informations qui vont du banal au confidentiel, de l'indispensable à l'inutile. Des entreprises demandent même à leurs dirigeants de fixer leurs objectifs hebdomadaires et de les partager avec leurs collègues sur un groupe WhatsApp (cf ci-contre).

Loin de moi l'idée de critiquer *le fait* de se regrouper ainsi dans un outil de messagerie instantanée. Mais que tant de personnes - 1,5 milliard d'utilisateurs actifs dans le monde à ce jour pour WhatsApp- l'utilisent sans se poser de questions est inquiétant. L'on sait que les noms, prénoms et numéros de téléphone sont des données personnelles, et qu'elles doivent être traitées selon certains principes en particulier la licéité, proportionnalité, la sécurité. On comprend donc l'importance de connaître les tenants et aboutissants de l'utilisation de moyens technologiques avant d'y livrer diverses informations. Que deviennent ces informations ? Comment sont utilisées les données personnelles collectées directement des contacts de l'utilisateur ? À qui sont-elles communiquées ? Pour mémoire WhatsApp a été racheté par Facebook en 2014, pour qui la transparence et les échanges sont de mise. Dans certains cas cela est anodin, mais lorsque des mineurs sont concernés, ou que les informations



échangées portent sur des données de santé ou sur la sphère intime, la responsabilité individuelle, en particulier des dirigeants, impose de proposer des outils plus respectueux dans le traitement des données personnelles. Et il y en a, que l'on songe à Signal, Telegram ou Threema par exemple.

- Solutions techniques de collaboration, quelles bonnes pratiques pour le Responsable de traitement ? (Octobre 2019)

Mettre à disposition des collaborateurs un espace de travail collaboratif, ergonomique et sûr à la fois est tendance, et permet d'améliorer l'efficience et d'alléger les processus de travail. De tels espaces de stockage, partage et élaboration coopérative de documents permettent souvent également de résoudre les questions et incidents par conversation en ligne (*chat).*

Dans le choix des solutions qui s'offrent aux entreprises, le respect de la protection dès la conception et par défaut (*privacy by design and by default*), obligation prévue par le RGPD et reprise dans le projet modifiant la LPD (déjà en vigueur pour les organes fédéraux, voir la LPDS), doit être un des critères retenus. Beaucoup de solutions étant proposées par des entreprises américaines, cette règle impose de vérifier quelles mesures techniques et organisationnelles ont été prises, qui permettront au Responsable de traitement de garantir le traitement conforme des données personnelles. Les données de sauvegardes, à tout le moins, étant transférées sur le territoire des USA, on vérifiera bien sûr que l'entreprise est inscrite au *privacy shield*, avec toute la relative sécurité que cela induit, puisqu'il a été constaté que certaines entreprises s'auto-certifient sans évaluation externe (cf. 1er rapport du PFPDT). Une garantie supplémentaire est obtenue lorsque l'entreprise est certifiée ISO 27001, puisque cette norme de sécurité de l'information contient des exigences relatives aux données personnelles. Et pour les institutions publiques cantonales et communales, attention à ne pas utiliser cet espace pour le traitement des prestations – à traiter idéalement par le guichet universel sécurisé – sachant que le traitement d'informations couvertes par le secret de fonction ne peut pas être confié à un sous-traitant. Pour ces institutions, l'élaboration d'un Règlement de traitement peut s'avérer utile.

- L'intelligence artificielle, l'éthique et Edgar Snowden (Novembre 2019)

« Avec les progrès de l'intelligence artificielle dans les domaines tels que la reconnaissance faciale et la reconnaissance des formes, le plus grand danger est devant nous » confie Edgar Snowden dans sa biographie[2]. Et de citer les caméras réagissant *a priori* à des comportements évoquant une infraction – un deal, à cause d'un échange de poignée de mains ou d'une embrassade, un gang, en raison d'une réunion de jeunes portant des vêtements d'une même coupe et même couleur – réaction due à un biais que toute application systématique et sans discernement de règles générales aux cas particuliers contient. Le risque de décision automatisée biaisée n'est pas moins grand dans le domaine RH, sans parler du domaine médical.

Alors oui des règles éthiques sont indispensables. On s'inspirera avec bonheur de la charte de la CEPEJ[3] applicable à l'utilisation de l'IA dans le monde judiciaire, qui prévoit comme principes essentiels : le respect des droits fondamentaux – parmi eux la liberté personnelle et le respect de la sphère privée -, la non-discrimination, l'exigence de qualité et sécurité des données, les principes de transparence,

[2] Mémoires vives, p. 219
[3] Commission européenne pour l'efficacité de la justice

neutralité, intégrité intellectuelle – on y retrouve les principes de protection des données - et la maîtrise par l'utilisateur. Donc une charte éthique, qui repose sur les droits fondamentaux et les règles de protection des données, car si un traitement automatisé doit être éthique, il doit avant toutes chose être légal.

Mais ce qui manque cruellement, en amont, comme le relève le précité, c'est « un débat public digne de ce nom ». N'est-ce pas aux citoyennes et citoyens de décider dans quel monde ils souhaitent vivre, en connaissance des tenants et aboutissants ? Les experts en protection des données plaident quant à eux pour l'autodétermination informationnelle. Il y a encore loin de la coupe aux lèvres.

- Vacances de Noël, et si on méditait sur notre avenir d'êtres humains ?

L'ONG Amnesty international vient de publier un rapport percutant sur la surveillance de Google et Facebook et la violation des droits humains qui en découle. Tout le monde est concerné par le problème et fait partie de la solution : les Etats, les individus, les entreprises. Dans ce rapport, publié le 20 novembre dernier, l'ONG constate que plus de la moitié des humains sont connectés, et que l'accès à Internet est devenu indispensable à la communication, à l'apprentissage, à l'économie, à la vie sociale et politique, et à la mise en œuvre des droits humains. Et les *4 milliards* d'êtres humains qui l'utilisent le font essentiellement au travers des outils de ces deux entreprises, et par le truchement de leur téléphone, appareil qui révèle une foultitude d'informations sur nos habitudes, nos intérêts, nos déplacements. Or, au début, l'usage de ces outils n'impliquait pas la surveillance des utilisateurs, mais avec le temps les deux entreprises ont développé un véritable *business model* de surveillance, contrepartie sournoise de la gratuité des services offerts.

Amnesty international relève que les violations de la sphère privée générées par cette surveillance se doublent de risques de manipulation des populations, car ces deux entreprises ont aujourd'hui une position dominante qui les rend quasiment incontrôlables. Par conséquent, l'ère d'autorégulation touche à sa fin. L'Internet n'a pas besoin de la surveillance pour offrir ses services, et la surveillance *urbi et orbi* n'est pas une fatalité. Des solutions négociées par tous les groupes concernés sont à trouver pour rendre à nouveau les droits fondamentaux effectifs, avec l'appui des Etats qui ont l'obligation de protéger la population contre les violations de ses droits fondamentaux.

L'humanité arrivera-t-elle à faire mentir Richard Stallman, qui n'a pas de téléphone portable car « le téléphone portable, c'est le rêve de Staline [4]» ?

*



[4] Voir notamment l'entretien paru dans LaRevueDurable, n° 63, p. 50 et ss