**Association Nationale des Directeurs des Systèmes d'Information**
www.andsi.fr

# Règlement européen sur la protection des données – Droit à la déconnexion

## Compte rendu de la présentation du 10 janvier 2017, à Châteauform' City Monceau Velasquez

Compte rendu rédigé par Laure MUSELLI & ANDSI

## En bref…

André MEILLASSOUX, Avocat spécialisé dans les technologies de l'information, associé chez ATM Avocats et Président de l'AFDIT, présente le contexte d'adoption du nouveau règlement européen sur la protection des données, les enjeux qu'il revêt pour les Etats et les changements qu'il occasionne pour les entreprises. Il revient également sur les détails de la mesure concernant le droit à la déconnexion de la loi Travail, entrée en vigueur en janvier 2017. Trois DSI viennent compléter cet exposé juridique, en décrivant les pistes suivies par leurs entreprises respectives pour la mise en œuvre de cette mesure.



### *Règlement européen sur la protection des données*

### *Un débat sociétal*

Le règlement européen sur la protection des données s'inscrit dans un débat sociétal autour de la question de la volonté de protéger nos données ou pas, qui marque une opposition frontale en l'Europe et les Etats-Unis, et leurs deux conceptions de ce sujet. **La question de la société dans laquelle nous souhaitons vivre est aujourd'hui primordiale à l'heure du Big Data.**

**La problématique du « Big Business » :**
Il existe une problématique concernant le droit des citoyens face à des géants de l'internet, des sociétés américaines surpuissantes souhaitant imposer un système fondé sur la fin de la vie privée. Il s'agit d'un modèle économique reposant majoritairement sur la vente des données personnelles, dans lequel les utilisateurs se sont engouffrés, attirés par la gratuité des services proposés. En réalité, pour les utilisateurs, le prix en a été la perte de leurs données personnelles et de leur vie privée : les grandes entreprises du net ont récupéré pendant plusieurs années les données personnelles des utilisateurs, les ont stockées, croisées et les revendent aujourd'hui à des entreprises publicitaires et commerciales sans leur accord. Selon une étude du cabinet Gartner, les services gratuits d'internet représentent 192 milliards de dollars et la vente des données personnelles pèse pour plus de 95% dans le chiffre d'affaires de ces sociétés.
**La problématique du « Big Brother » :**
Il s'agit de savoir si nous acceptons la société de surveillance généralisée, contre laquelle un certain nombre d'acteurs s'élève. La Quadrature du Net, une association, se bat contre une appropriation du net par les grandes sociétés et pour sa neutralité. E. Snowden, ancien employé de la CIA et spécialiste de l'informatique, risque aujourd'hui la peine de mort pour trahison et passage à l'ennemi, pour avoir révélé les détails de surveillance de masse par les Etats-Unis, comme le présente le film documentaire « Citizen 4 », qui retrace les toutes premières heures de ses révélations au monde.

## *Contexte de la rédaction du règlement :*

**La loi informatique et libertés de 1978 :**

La loi Informatique et Liberté du 6 janvier 1978 a été prise à l'occasion d'un scandale d'Etat baptisé à « Affaire Safari », du nom d'une base unique décidée par l'Etat, regroupant les bases de données de tous les services secrets français. Cette décision avait occasionné un lever de bouclier tant elle paraissait destinée à espionner la population.
Sous la pression de l'opinion publique, le gouvernent a fait voter **la loi du 6 janvier 1978, instaurant la CNIL** et **consacrant la protection des données personnelles**.
Si la France a été pionnière en la matière, aujourd'hui, la quasi-totalité des pays a ensuite adopté le même système : (à l'exception des Etats-Unis, qui se sont toujours refusés à prendre une réglementation sur les données personnelles) et a adopté le même système :

- Une **loi qui pose le principe de la protection des données personnelles**
- Une **autorité indépendante comme la CNIL**, qui a le monopole de la poursuite des infractions aux données personnelles : qui reçoit les plaintes, réalise ses enquêtes et transmet ses conclusions au procureur de la république, qui peut mettre en œuvre l'action pénale.

En 2004, une directive européenne modifie légèrement les règles de fonctionnement de la CNIL, en privilégiant les contrôles a posteriori.

- **Article 1 :** L'informatique doit être au service de chaque citoyen et ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la loi.
- **Article 2 :** Une donnée à caractère personnel est toute donnée qui peut se rapporter à une personne physique.

**Le Big Data face aux 5 principes de la loi Informatiques et Libertés**

- **Principe de collecte loyale et licite** : il est par exemple impossible de collecter les données d'une personne sans lui avoir demandé son avis. L'implication immédiate concerne l'obligation de l'« opt in »», c'est-à-dire la nécessité d'un consentement éclairé, clair et indiscutable, par opposition au « opt out », qui consiste pour la personne à se manifester a posteriori pour indiquer son opposition à la collecte de ses données.
- Aujourd'hui, le débat concerne le fait de savoir si demander de cliquer sur un bouton « j'accepte » pour accepter des conditions d'utilisation d'un service respecte le principe de collecte loyale et licite. Les conditions d'utilisation de Facebook, par exemple, comportent 80 pages au milieu desquelles apparaît une clause établissant un droit de licence mondial gratuit et transférable des données personnelles, et où il est précisé que l'objectif poursuivi est la récolte, le stockage, le traitement et la revente des données personnelles (nom, profil, photos…) aux annonceurs.
- **Principe de finalité :** il est nécessaire de déclarer à la CNIL la finalité de la récolte des données. Il est impossible de changer de finalité au cours du temps. Pour toute nouvelle finalité, une nouvelle déclaration est nécessaire.
- **Principe de proportionnalité et de pertinence :** il est interdit de collecter une quantité de données disproportionnée ou abusive. La CNIL a par exemple lancé à l'Université de Lille une interdiction de mettre en place un système de reconnaissance biométrique auprès d'un millier d'étudiants pour sécuriser l'entrée sur le site, qu'elle jugeait disproportionné.
- **Principe d'exactitude :** respect du droit des personnes, c'est-à-dire un droit d'accès, de rectification et de suppression des données collectées.
- **Principe d'une durée de conservation limitée** des données : indiquer une durée de conservation des données justifiée.

Aujourd'hui, 70% des données du Big Data sont des données personnelles et les 50 milliards d'objets connectés promis en 2020 vont permettre une plus grande accumulation de données supplémentaires. Cette collecte massive constitue un risque pour la vie privée, dans la mesure où les données et opinions sont stockées afin d'affiner le profilage psychologique réalisé par des robots d'intelligence artificielle. Pourtant, le **Big Data n'est compatible avec aucun des cinq piliers de la CNIL**. Le Big Data constitue en effet une inversion de la logique, puisqu'auparavant, les systèmes d'information étaient créés pour générer des données, alors qu'aujourd'hui, les données sont collectées puis stockées sans qu'on ne connaisse à l'avance l'usage qui pourra en être fait. Sur le fond, le droit positif français est ainsi régulièrement bafoué par les acteurs américains : la finalité est impossible à déclarer, la collecte n'est pas loyale et licite puisque la totalité des données est stockée, la proportionnalité et la pertinence ne peuvent être

contrôlées, l'exactitude ne peut être vérifiée dans une telle quantité de données et le droit d'accès des personnes relève de l'impossible.

**L'absence de qualification juridique des données personnelles** contribue largement à cette dérive. Est-on propriétaire d'une donnée ? Le Conseil d'Etat a été saisi par Axelle Lemaire à ce sujet le 7 octobre 2016, dans le cadre de son projet de loi sur la République Numérique, et notamment sur la question du statut juridique d'une donnée et le fait qu'elle soit susceptible d'une patrimonialisation.
Le Conseil d'Etat, sur cette question, a répondu qu'il n'existe pas de droit de propriété, ni d'inviolabilité, comme dans le cas du corps humain, mais qu'il faudrait un principe à l'autodétermination informationnelle. La loi du 7 octobre 2016 reprend cette position, en réaffirmant que les citoyens n'ont pas la propriété, mais le droit de contrôle de leurs données personnelles. En ce sens, elle va contre la pratique généralisée des entreprises américaines, qui prônent un droit de propriété et par conséquent la possibilité de leur céder ce droit.

**Du « Safe Harbor » au « Privacy Shield »**

C'est ce qu'illustre l'affaire Max Schrems, qui a donné lieu à un arrêt de la Cour de Justice de l'Union Européenne en octobre 2015. Max Schrems a utilisé une loi autrichienne stipulant que les entreprises devaient donner un droit d'accès aux données. Il a demandé à Facebook de lui fournir les informations le concernant et a reçu un dossier de 35 000 pages de données personnelles. Il a saisi le tribunal de Vienne ainsi que la Cour de Justice de Vienne et a perdu. La Cour de Cassation autrichienne a suspendu son jugement et interrogé la Cour de Justice. Cette dernière a validé la condamnation de Facebook au motif que la quantité d'informations collectées sans l'accord de la personne était abusive. Elle a également constaté que Facebook avait bénéficié, comme la plupart des entreprises américaines, d'un certificat « Safe Harbor » de complaisance et par conséquent, a annulé le traité « Safe Harbor ».

La Commission Européenne émet une liste des pays dont le niveau de protection des données est équivalent à celui de l'Union Européenne et vers lesquels les données personnelles peuvent être transférées. Les Etats-Unis n'ayant pas de loi sur la protection des données, les transferts des données personnelles vers les Etats-Unis étaient interdits, ce qui empêchait les multinationales américaines de transférer les données de leurs filiales européennes vers les Etats-Unis. A partir de 2001, la Commission Européenne a négocié avec le Département d'Etat américain un traité nommé « Safe Harbour », permettant aux entreprises américaines souhaitant collecter et stocker des données de solliciter du Département d'Etat un certificat « Safe Harbor », prouvant que l'entreprise est apte à collecter des données et à les protéger, et les autorisant à faire du transfert de données personnelles. Toutes les sociétés américaines avaient obtenu le certificat « Safe Harbor », en ayant pourtant collaboré avec la NSA, installé des backdoors dans les systèmes et livré les données.

Suite à l'**annulation du traité « Safe Harbor »**, les entreprises américaines avaient jusqu'au 31 décembre 2015 pour régulariser leur situation, ces dernières n'ayant plus aucun fondement juridique pour transférer les données aux Etats-Unis. A partir du 2 janvier 2016, l'Allemagne a donc commencé à mettre à l'amende les sociétés américaines n'ayant pas régularisé la situation. Dans ce contexte, la Commission a annoncé la négociation d'un nouveau traité se substituant au « Safe Harbor » : le **« Privacy Shield »** (bouclier de protection de la vie privée), finalement adopté le 21 juillet 2016, stoppant de fait les poursuites. Selon certains Etats et citoyens, ce traité comporte les mêmes failles que le « Safe Harbor ».

## *Le règlement de 2016*

**Il était donc nécessaire de réaffirmer les principes de la loi Informatique et Libertés.**
Là où les Etats ont été défaillants dans la protection des données personnelles, L'Europe a réaffirmé le principe selon lequel la protection des données personnelles et de la vie privée est un droit fondamental à protéger absolument, car il n'existe pas de démocratie sans des espaces privés réservés.
En mars 2012, la Commission Européenne a présenté un projet de règlement européen sur la réglementation et la protection des données personnelles. La **différence entre une directive et un règlement européen** tient au fait qu'une directive impose aux Etats de prendre une loi sur la base de la directive, alors qu'avec le règlement, plus coercitif, la Commission propose et le Conseil des Ministres puis le Parlement adoptent un texte qui devient immédiatement applicable tel quel, sans que les Etats ne puissent faire de réserves.

Ce règlement a été adopté 4 ans et demi plus tard, en avril 2016, à une quasi-unanimité, après avoir été extrêmement débattu, avec plus de 4 200 amendements déposés, et un lobbying fort contre le texte. Il existe en effet une guerre homérique entre la conception que l'Europe voulait imposer et la conception commerciale anglo-saxonne et conception européenne.

**Le texte réaffirme les principes de protection de la loi Informatique et Libertés de 1978** et affirme que les **sanctions prononcées par les CNIL européennes peuvent se monter à 20 millions d'euros et jusqu'à 4% du CA mondial des entreprises** condamnées.

**Une conception européenne opposée à la conception américaine**

**L'approche européenne** encadre la collecte et le traitement des données selon des principes fondamentaux protecteurs et impératifs issus d'une législation générale. C'est dans cette logique que le **Règlement général sur la protection des données personnelles** réaffirme la volonté de sauvegarder les données des individus contre l'appétit des grands acteurs de l'internet, américains pour la plupart.

**Les Etats-Unis** sont à l'inverse soucieux de ne pas entraver le développement de leurs grandes entreprises, se basent quant à eux, sur un **principe de liberté et d'autorégulation des entreprises qui définissent elles-mêmes leur politique en matière de données personnelles**. Il s'agit plutôt de protection des consommateurs contre les abus, sous le contrôle de la *Federal Trade Commission (FTC*), autorité fédérale indépendante. Cette approche permissive est adaptée au modèle des GAFA : pas de déclaration, pas de consentement, pas d'entraves aux traitements et à la réutilisation ultérieure des données, qui constitue leur business model.

L'adoption, le 27 avril 2016, du Règlement général de l'Union Européenne a été anticipée et ressentie, notamment aux Etats-Unis, comme une entrave au modèle des grandes entreprises du Net, sociétés quasiment toutes américaines. En décembre 2015, B. Obama a prononcé dans la Silicon Valley un discours très virulent mettant en avant l'idée qu'internet aurait été inventé et porté par les USA, et que des mauvais perdants souhaitaient imposer des dispositifs légaux pour empêcher les sociétés américaines de recueillir les fruits de leur travail : « *L'internet, nos sociétés l'ont créé, agrandi, perfectionné…. Et ce qui est présenté comme de nobles positions est juste conçu pour défendre les intérêts commerciaux de nos concurrents".* D.Trump a pour sa part menacé l'Europe de mesures de rétorsion, invitant toutes les entreprises américaines du net à supprimer les services gratuits, ce qui entraînerait une perte de 3% de PIB à la Communauté Européenne.

**Changements pour les entreprises**

L'approche retenue par le règlement européen, qui entrera en vigueur en mai 2018, est celle d'un **Droit doux, mou et flou**. Il **pose des principes, mais ne prévoit pas de sanction**, l'idée étant plutôt d'aller vers une responsabilisation des responsables de traitement, en imposant une voie à suivre.

Parmi ces principes, on trouve :

- La politique de **Privacy by design**, qui impose la conformité à la réglementation des données personnelles dès la conception du système d'information. Les entreprises devront concevoir des fonctionnalités par défaut (c'est-à-dire sans aucune intervention humaine) et des produits de sorte à collecter et traiter le moins possible de données à caractère personnel.
- La politique de **Security by default**, qui impose une conformité à la réglementation des données personnelles au niveau de l'infrastructure sécuritaire du réseau. Les outils permettant le traitement de Big Data et la création de données secondes issues des données initiales ne devront donc pas permettre de croiser des données ou générer des traitements qui seraient contraires à la réglementation des données à caractère personnel.

Le règlement impose donc un double contrôle : a priori, dès la conception du traitement des données, et a posteriori, avec une capacité à auditer et à contrôler le processus de traitement des données.

Le règlement prévoit également la **nomination obligatoire d'un Data Protection Officer (DPO, ou Délégué à la Protection des Données** en français), qui remplace le Correspondant Informatique et Libertés (CIL), dans les entreprises ou organismes dont les activités de base requièrent un suivi régulier et systématique. Aux tâches déjà accomplies par le CIL s'ajoutent entre autres, pour le DPO, celles de notification et d'enregistrement des violations de données personnelles, ainsi que des analyses d'impact de ces violations.

Par ailleurs, le Règlement introduit, la **notion de réutilisation compatible des données avec les finalités initiales** : les réutilisations de données pour de nouvelles finalités sont possibles avec le consentement de la personne concernée, sur une base légale, ou si les finalités ultérieures sont déclarées compatibles avec celles initialement définies.

En ce qui concerne le **droit des citoyens**, le règlement renforce les droits existants et en apporte de nouveaux pour une meilleure maîtrise de ses données. Ainsi, il consacre **le droit à l'oubli,** introduit le **droit à la portabilité des données** en cas de changement de prestataire, ou encore celui, pour tout individu, à **s'opposer à son profilage.**

Enfin, une disposition du règlement est vivement critiquée. Il s'agit de celle qui **autorise un traitement des données à d'autres fins que celles auxquelles les utilisateurs ont souscrit** si « le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ». Le flou autour de la notion d'intérêt légitime pose un problème dans ce cas, la réalisation de bénéfices étant un intérêt légitime pour les entreprises commerciales.

## *Droit à la déconnexion*

### *Les principes du texte*

En matière de droit à la déconnexion, la **loi Travail du 8 août 2016, entrée en vigueur le 1er janvier 2017**, a réaffirmé des principes qui existaient déjà :

- Dans une **directive du Parlement Européen de 2003** qui traitait de l'aménagement du temps de travail et contenait l'idée que le salarié n'est pas subordonné sur son temps de repos et n'a donc pas à répondre aux sollicitations de l'employeur.
- Ce principe avait déjà été affirmé par la **Chambre sociale de la Cour de Cassation, notamment en 2004**, en statuant qu'on ne pouvait pas demander à un employé de répondre à ses mails pendant le week-end.

Dès le début des années 2000, les outils numériques viennent bouleverser le cadre spatio-temporel des travailleurs du savoir, avec le télétravail et le nomadisme, ainsi qu'une surcharge informationnelle liée à une connexion permanente via téléphones portables et mails. Le Professeur Jean-Emmanuel Ray en appelle alors à un « droit à la déconnexion », qu'il considère comme « le droit à la vie privée du XXIème siècle ».

Alors que le rapport Mettling préconise l'instauration d'un droit et d'un devoir de déconnexion pour le salarié et l'employeur, **la loi du 8 août 2016 ne retient que le droit, sans imposer d'obligation**.

**Le texte pose ainsi un principe mais ne donne pas les moyens, et surtout ne prévoit pas de sanction.** Il impose aux employeurs de **négocier sur le droit à la déconnexion dans le cadre d'accords collectifs ou, à défaut, d'une charte de bonnes pratiques**. Une charte informatique est négociée librement au sein de l'entreprise avec les institutions représentatives du personnel et permet de régler de nombreux problèmes potentiels. Il peut s'agir, pour le DSI, d'un outil très utile qu'il doit utiliser de façon proactive, afin de ne pas être tenu pour responsable en cas de problème qui pourrait comporter une dimension technique. Pour ce faire, la bonne pratique consiste à constituer un dossier de correspondances avec la direction des RH, la direction juridique, voire la DG, informant ces dernières des points liés à l'évolution de la technique, qui nécessiteraient d'intégrer de nouvelles dispositions dans la charte informatique.

Finalement, il existe une différence entre déconnexion technique et déconnexion intellectuelle, la déconnexion étant d'abord une question de formation, d'organisation, individuelle et surtout collective. « Il s'agit autant d'une éducation au niveau individuel que d'une régulation d'entreprise », comme l'affirme le rapport Mettling.

Quelques exemples de mise en œuvre :

- Chez Volkswagen : mise en veille des serveurs et des smartphones professionnels entre 18h15 et 7h.
- Chez Daimler-Benz : option de renvoi des mails vers des contacts disponibles pendant les congés, et la suppression de ces mails de la boîte, pour éviter toute surcharge au retour de vacances.
- Chez Michelin : accord d'entreprise mettant en œuvre un dispositif dissuasif d'alerte des supérieurs en cas de dépassement de non-respect du nombre d'heures de repos légal.

### *Exemples de mise en œuvre du droit à la déconnexion par trois DSI :*

**Premier DSI :**

A partir de janvier 2017, il est nécessaire de commencer à travailler avec les organisations syndicales représentatives sur des négociations concernant l'égalité professionnelle et la qualité de vie au travail. Ces négociations devront porter sur les modalités d'exercice par le salarié de son droit à la déconnexion et sur la mise en place par l'entreprise des mesures concernant les outils numériques, en vue d'assurer les temps de repos et de congé, ainsi que la vie personnelle et familiale.

Selon les RH, il n'y a **pas d'obligation de résultat, mais uniquement une obligation de moyens**. Il n'existe pas de risque de poursuites ou de sanctions, mais il faut arriver à trouver avec les instances représentatives du personnel un

accord et des actions sur le sujet. Aucune mesure concrète n'a encore été prise, mais **les RH ont une préférence pour une approche souple et une sensibilisation des collaborateurs et du management, avec une solution de type charte** et la mise en œuvre d'actions de formation et de sensibilisation des personnels, y compris d'encadrement et de direction. De leur côté, les **partenaires sociaux ne trouvent pas cela suffisant et réclament des actions plus concrètes, comme l'arrêt des serveurs à 18h.**

Pour l'instant, le DSI préférerait une charte sur le comportement, plutôt que quelque chose « qui pourrait ressembler à une usine à gaz » et se refuse à faire des propositions techniques. La société étant de plus en plus internationale, avec de nombreux collaborateurs en déplacement, l'arrêt des serveurs de messagerie n'est pas envisageable pour des questions de décalage horaire. En revanche, la solution de Michelin, consistant à repérer les personnes connectées trop longtemps et trop souvent pourrait être une approche intéressante, mais ces données peuvent être considérées comme des données privées.

**Deuxième DSI :**

L'entreprise dispose d'un climat social apaisé, avec des instances représentatives du personnel qui ne sont pas en attente de plus de règles.

Les mesures pour assurer le droit à la déconnexion des salariés s'arrêtent à la phrase suivante en **signature de mail : « Si ce mail vous arrive en période de congés ou d'absence, merci de n'y répondre qu'à votre retour ».**

Une simple sensibilisation semble être suffisante, comme dans le cas du harcèlement.

**(Pierre DELORT)** : Pour l'entreprise, un des enjeux de la déconnexion est, en cas de licenciement, de se **protéger contre une attaque judiciaire de la part des employés**. Le risque tient en effet à une possible requalification en heures supplémentaires du temps de travail du soir ou du week-end, basée sur les mails reçus et envoyés.

**Troisième DSI :**

Le groupe est international, avec des usines partout dans le monde, et de nombreux employés multi-fuseaux horaires qui se déplacent beaucoup. Au mois de septembre, le DSI, identifiant la problématique de la déconnexion, s'est adressé à la Directrice des Relations Sociales, qui lui a précisé le contenu des obligations légales et du contexte de la mesure.

L'idée du DSI était de comprendre et de mesurer le phénomène de connexion en dehors des heures de travail. Trois éléments permettent de **détecter lorsque les employés travaillent chez eux** :

- L'utilisation du **téléphone professionnel**, sujet sur lequel il est compliqué d'obtenir des données ;
- L'utilisation de la **messagerie**, pour laquelle il est possible de voir quand les mails arrivent, partent, ou sont ouverts, mais difficile d'obtenir des données, le système étant externalisé.
- Un **outil de sécurité permettant de contrôler les accès depuis l'extérieur aux systèmes de l'entreprise**, en dehors de la messagerie, qui est un système à part. Cela permet de voir qui s'est connecté à quel système et à quelle heure. Les logs ont été étudiés sur une durée d'un mois, avec un focus sur les personnes basées en France. Les résultats ont montré que les personnes en déplacement utilisaient l'accès pour travailler sur des systèmes de production le soir et le week-end. Les premiers week-ends du mois sont plus chargés que les autres. Sur une cinquantaine de sites en France, quatre réalisent 75% des connexions, et une très grosse partie en dehors des horaires 08h-20h et le week-end.

Les conclusions du DSI sont les suivantes :

- Des populations de type **finance, qui gèrent les clôtures de comptes** dont la remise est impérative le premier lundi se connectent le week-end depuis chez eux, ce qui est plus confortable que de se déplacer sur le lieu de travail.
- Des populations au **profil R&D ou industriel travaillant sur des programmes de démarrage d'usines ou de produits**, qui se connectent à des horaires atypiques, soit à l'étranger lorsqu'ils sont en déplacement, soit en France lorsqu'ils doivent interagir avec des sites étrangers impliquant un décalage horaire.

L'hypothèse que de mauvaises pratiques de non-déconnexion puissent être reliées à des problématiques de sécurité au travail, éventuellement occasionnées par une défaillance du management, a été soulevée avec la Directrice des Relations Sociales. Il peut s'agir entre autres de sollicitations abusives, de pression trop forte, ou encore de ressources insuffisantes. Une pratique de connexion abusive de la part d'un salarié peut donc constituer un signal d'alarme à prendre en compte pour prévenir un éventuel problème de santé.

Sur la base de ces résultats, la DRH a décidé de lancer un process avec les DRH filiales, afin de leur rappeler le risque lié à de mauvaises pratiques par rapport aux obligations légales. L'idée consiste, à partir des particularités identifiées au sein du groupe, d'arriver à trouver une **politique homogène, éventuellement de type charte ou aménagement de la charte informatique**, qui puisse s'appliquer à tous les sites.

Le process devrait aboutir à une charte ou à l'aménagement de la charte informatique, avec éventuellement, à côté de l'obligation légale, des éléments intéressants d'évaluation de management. Un top 50 des managers qui abusent pourrait par exemple être intéressant, s'il devenait un indicateur qualité affiché.

Débat

**Intervenant :** Quel profil voyez-vous pour le DPO ? Est-ce un informaticien ? Un juriste ?

**André MEILLASSOUX :** Le DPO ne peut pas être le DSI, car une dualité est nécessaire entre le DSI en charge de la mise en place des outils, et le DPO qui doit rappeler que des contraintes doivent être intégrées. Il existe donc une incompatibilité avec le poste de responsable informatique. Ce sont souvent des juristes, mais des ingénieurs peuvent aussi prendre ces positions.

**Int. :** Est-ce au DPO de faire l'inventaire de tous les fichiers d'une société, pour vérifier s'il existe des problèmes de données privées ? Qui doit faire cela ?

**A.M. :** Le règlement général impose la tenue d'un registre. Il y a eu des recommandations CNIL de tenir un registre de toutes les fuites de données, pour, en cas de contrôle, fournir l'historique de la société, ainsi que les actions prises. Je pense que c'est une mission extrêmement délicate. On est en conflit d'intérêt entre la position que l'on accepte et le lien que l'on est censé devoir entretenir avec la CNIL, qui a comme contrepartie un allègement important des formalités. Je vois mal un salarié aller dénoncer son entreprise à la CNIL et je pense qu'il s'agit donc d'une position très difficile. Mais je pense que c'est un poste à définir, car extrêmement nouveau : il y a très peu de CIL dans les entreprises françaises, sauf dans certaines sociétés très fortement exposées aux données personnelles.

**Int. :** Est-ce que ce règlement n'est pas un boulet pour l'Europe, qui doit courir le 100 mètres ?

**A.M. :** C'est le grand grief qui lui est fait, mais la question a été tranchée par le Parlement Européen. Nous avons dit : « En Europe, nous tenons à nos principes fondamentaux et nous les affirmons ».

**Int. :** Est-ce que ce n'est pas un sparadrap sur une jambe de bois ? Ces sociétés sont-elles vraiment préoccupées par ces lois qui ne vont pas aussi vite qu'elles ?

**A.M. :** Je pense que la question est sur la table, mais on peut constater que ces entreprises américaines ont incroyablement modifié leur comportement. Par exemple, Apple dit aujourd'hui « vos données sont nos données, la prunelle de nos yeux, et jamais nous ne les donnerons à qui que ce soit. Si la NSA ou la CIA nous le demandent, nous saisirons la justice ». C'est un nouveau discours, mais qu'en penser ? Je pense qu'il était tout de même nécessaire de réaffirmer ces principes démocratiques.

**Int. :** Finalement, la loi donne des orientations et les métiers doivent inventer les pratiques ?

**A.M. :** L'approche du droit doux, mou, flou est une incitation. On met sur la table un sujet, on dit qu'il faut le faire, il n'y a pas de sanction, mais il y a quand même une réprobation si on ne le fait pas. Par exemple, dans le cas du règlement européen, on incite très fortement les gens à faire des études d'impact. Si les études d'impact ne sont pas faites, il n'y a pas de sanction, mais en cas de problème, l'absence d'étude d'impact sera reprochée. C'est une incitation forte à ce que les problématiques avancent et que les gens les traitent, avec une injonction à aller dans une direction assez librement, pour améliorer les pratiques.

**Int. :** Est-ce que la formation à l'usage des outils numériques n'est pas une problématique ?

**DSI 3 :** Aujourd'hui, les employés de moins de trente ans qui entrent chez nous veulent travailler comme à la maison. C'est donc un vrai sujet, et la loi, qui est une loi de protection, bénéficie in fine à tout le monde, car un employé fatigué ne travaille pas bien. On a également un problème culturel. Les vieux comme moi souhaitent faire semblant de fonctionner comme leurs enfants pour être modernes : on est en temps réel permanent, on décroche tout le temps, etc… Ce n'est pas un acte délibéré de faire travailler les gens, mais on se fait prendre par cette tendance, et la pression fait que la réponse le dimanche à 15h, c'est mieux que le lundi à 08h. On a besoin d'une formation, mais elle s'adresse à une élite : la masse ne sera jamais formée, sauf implicitement.

**Int. :** Est-ce qu'on sait combien ça va coûter aux entreprises européennes de mettre en place une telle réglementation ? On parle de DPO, d'analyses, d'impact, etc… Il y a des coûts, des audits…

**A.M. :** Je ne sais pas répondre à cette question, et je pense que les opposants ont fait valoir que les coûts occasionnés n'étaient pas gérables et les contraintes immenses. Par exemple, quand vous dites aux chasseurs de tête qu'ils n'ont pas le droit de prendre de décision sur un cv qui soit automatique, et qu'une intervention humaine est obligatoirement requise, ils sont furieux. Pour prendre des informations personnelles sur les candidats, on n'avait pas LinkedIn et Facebook avant, mais on le faisait quand même. C'est donc purement hypocrite.

**Int. :** Quand vous parlez de droit mou, je trouve que c'est un mot parfaitement approprié. Selon la CNIL, on n'a pas le droit de garder une donnée relative à une personne plus de 12 mois, si cette personne ne se reconnecte pas pendant les 12 mois. Si la personne revient sur le site au bout de 9 mois, le compteur est remis à zéro. Et tout va être fait pour que la personne revienne, même quelques secondes, par exemple en lui envoyant un email. Par ailleurs, les coordonnées d'une personne qui achète un produit garanti trois ans sur un site de e-commerce ne peuvent être effacées, étant donné qu'elle est liée par un contrat de cinq ans. De fait, la contrainte des 12 mois n'existe plus et la CNIL ne peut rien dire. Imaginons que cette personne soit en contact avec un ministère, avec des documents officiels bancaires, par exemple. Le code général des impôts oblige alors à garder les informations bancaires pendant 10 ans. Moi je l'aime bien, ce droit mou, parce qu'on peut faire ce que l'on veut, en réalité.

**A.M. :** Tous les cas que vous mentionnez sont des exceptions. Si vous allez dans une banque contracter un emprunt sur 20 ans, on ne peut pas demander à la banque d'effacer vos données au bout de trois ans. Par ailleurs, il existe toujours l'exception d'obligation légale de conservation des documents, comme 10 ans pour les factures, ou 30 ans pour les fiches de paye. J'ai organisé en 2008 un panel sur la question de la régulation des entreprises du net. Le responsable des données personnelles pour Google y avait participé et on lui avait demandé combien de temps il conservait les données, à une époque où le business model de l'entreprise n'était pas aussi clair. Il avait répondu que la durée de conservation devait être de deux ans. C'était du pur mensonge, car on sait aujourd'hui qu'ils n'ont jamais effacé une seule donnée. Lorsque dans la salle, quelqu'un a posé la question du point de départ des deux ans, il a répondu que les deux ans couraient à partir de la dernière connexion. Les délais de trois ans pour les prospects commerciaux ou de treize mois pour les cookies, débutent toujours à partir de la fin de la relation.

**Présentation de l'orateur**

**André MEILLASSOUX**

André MEILLASSOUX est un Avocat spécialisé dans les technologies de l'information, la propriété intellectuelle (IT/IP) et les contrats. Il est associé chez ATM Avocats. Il est l'actuel Président de l'AFDIT (Association Française de Droit de l'Informatique et de la Télécommunication), président sortant de l'IFCLA (International Federation of Computer Law Associations) et le correspondant pour la France de l'International Technology Law Association (ITechLaw).