Auteur : Lionel GUILLET
Expert en Management de la Sécurité de l'Information

DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL A L'OBLIGATION GENERALE DE SECURITE

L'EVOLUTION DE LA LEGISLATION ET DE LA REGLEMENTATION EST UN LEVIER DE DEVELOPPEMENT DE LA SECURITE DE L'INFORMATION

Les enjeux politiques, stratégiques et économiques liés à la sécurité des systèmes d'information sont tels désormais qu'il s'agit pour les États d'obliger les entreprises[1], toutes les entreprises, sans distinction de secteur ou de taille, à mettre en œuvre les moyens d'assurer la protection de leur patrimoine informationnel. La démarche, initiée depuis longtemps, s'accélère avec le développement de la numérisation de toutes les activités et la dépendance sans cesse accrue de nos Sociétés au bon fonctionnement de ce nouvel écosystème.

Le moyen pour y parvenir, il est juridique au nom, tout à fait justifié, de la préservation des libertés individuelles et des données personnelles. Mais il poursuit logiquement un objectif plus large que l'on ne peut que partager, inciter, contraindre s'il le faut, les entreprises à se mettre en place une véritable protection de leur système d'information pour garantir leur efficacité et leur performance individuelles et collectives.

La généralisation de l'obligation de déclarer les atteintes aux données à caractère personnel est en chemin.

Le Règlement de l'Union Européenne 611-2013 mis en place fin août 2013 publie l'obligation de déclarer les violations de données à caractère personnel auprès d'une autorité nationale compétente (la CNIL, en France).

Elle consolide des dispositions déjà publiées. D'une directive 2002/58/CE de juillet 2002, enrichie en 2009, elle fait une règle, une règle transposée dès 2011 dans la législation française, notamment par l'article 34 bis de la Loi 78-17 dite "Loi Informatique et Libertés".

Pour l'instant, cette obligation ***s'adresse aux seuls gestionnaires de réseaux et de services de communications électroniques au public***. En France, les opérateurs déclarés auprès de l'Autorité de Régulation des Communications électroniques et des Postes, l'ARCEP[2].

[1] Par "entreprise", il faut comprendre toutes les formes d'organisations intéressées par le sujet, administrations, services publics, entreprises du secteur privé, associations …

[2] Tout comme les autres autorités de régulation L'ARCEP participe au respect de la conformité juridique dans son périmètre de responsabilité. Aussi, puisque nous nous intéressons au renforcement progressif de la réglementation en matière de protection de l'Information, est-il intéressant de savoir qu'elle a été rétablie dans son pouvoir de sanction par une ordonnance 2014-329 du 12 mars 2014, après en avoir été privée sur décision du Conseil Constitutionnel mi 2013 sur une question prioritaire de constitutionnalité.

Mais, cette nouvelle réglementation ne manque pas de faire valoir sa ***conformité avec le futur "règlement sur la protection des données" dans l'UE qui portera extension de cette obligation à tous les responsables de traitements de données à caractère personnel.*** Nous l'évoquerons plus loin.

Elle s'inscrit dans un principe général, l'obligation de protection des données de l'entreprise

La nouvelle règle européenne ne se limite pas à publier l'obligation de protection des données, ***elle précise également les moyens à mettre en œuvre pour la satisfaire.***

C'est ainsi qu'elle rappelle, dans ses considérants, que le chiffrement ou le hachage des informations ne suffit pas pour répondre, attention, notez bien, à …" ***l'obligation générale de sécurité*** énoncée à l'article 17 de la directive 95/43/CE" sur la protection des données à caractère personnel.

C'est l'affirmation ***d'un principe fondamental de protection de l'Information***, l'obligation générale de sécurité ***dans laquelle s'inscrit les données personnelles***, principe repris depuis, sous une forme ou sous une autre, dans les directives et les règles subséquentes publiées dans le domaine.

La transposition française de ce principe se retrouve notamment dans la Loi 78-17 qui précise, dans son article 34, qu'***un "responsable de traitement est tenu de prendre toutes précautions utiles***, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès".

La protection des données de l'entreprise, désormais une obligation majeure pour les responsables de traitement

Le "responsable de traitement est tenu de prendre toutes précautions utiles" dit la Loi. Ainsi, très clairement, ***l'enjeu n'est plus seulement de se mettre en conformité avec la règlementation. Il s'agit maintenant de pouvoir justifier, en cas d'accident de sécurité, que toutes les démarches ont été accomplies pour*** identifier et suivre l'évolution des risques, et que les mesures de protection en conséquence ont été mises en œuvre.

Ainsi, parmi d'autres mesures, l'analyse des risques, un plan de continuité d'activité, le suivi des évènements de sécurité font partie des actions indispensables à ***la maîtrise des risques*** dont le responsable de traitement doit désormais justifier.

Le responsable de traitement, en général, c'est le chef d'entreprise

En effet, toujours selon la Loi de janvier 1978, le responsable de traitement c'est "la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens de ce traitement".

Or, dans une entreprise qui décide de la finalité et des moyens de traitement de données si ce n'est ***le chef d'entreprise lui-même***.

Ainsi, pour résumer, il faut retenir que les données à caractère personnel ne sont pas dissociables du système d'information de l'entreprise placé sous la responsabilité de son (ses) dirigeant(s) qui doi(ven)t prendre toutes les dispositions pour en assurer la protection et pouvoir le prouver si nécessaire.

Et, il s'agit bien d'***une obligation générale, pas seulement***, celle-ci***, applicable aux fournisseurs de réseaux et de services de télécommunications.***

Le futur règlement européen, Règlement général sur la protection des données, prévoit la généralisation de la notification de toute violation de données à caractère personnel et plus …

Cette fois, ce n'est plus une directive, soumise à interprétation, comme en 1995, c'est ***une réglementation qui s'imposera*** le moment venu à l'ensemble des États de l'Union, sans alternative. "***Règlement général sur la protection des données***", c'est son sous-titre. Il marque bien la portée des dispositions en préparation.

En effet, même si ce texte s'intéresse à la protection des personnes en matière de traitement des données à caractère personnel et de libre circulation des données, il le fait par référence à la protection des données dans son ensemble, et ce, pour les motifs développés précédemment.

Dans ces dispositions, figure bien sûr ***en bonne place, l'extension de la notification des violations des traitements des données personnelles à une autorité de contrôle en cas d'accident***, mais, en plus, ***le devoir d'en informer également les personnes concernées***, opération qui peut être lourde de conséquences en termes financiers et d'image pour l'entreprise.

Et nous ne parlerons pas de ***l'obligation de conserver une trace documentée de cet évènement***, ni de ***l'analyse d'impact préalable pour les traitements à risques particuliers pour les droits et les libertés des personnes***.

Alors … que faut-il de plus pour inciter les derniers hésitants à passer à l'acte, tracer les évènements de sécurité de l'information et leur résolution ?

Le futur règlement européen dans son parcours législatif. Un point à la date du … 17 mars 2014.

La Commission des Libertés Civiles de la Justice et des Affaires intérieures et le Parlement européens se sont prononcés sur la règlementation en préparation.

La Commission a défini sa position en octobre dernier, le 21 octobre précisément.

Le Parlement a voté le texte en 1ère lecture le 12 mars 2014, lors de sa dernière session plénière avant les élections prévues le 25 mai.

Ce vote des députés représente une étape décisive. Il valide le travail très important déjà accompli par les organes européens, un travail sous lobbying intense, avant sa transmission à la future Assemblée et l'ouverture des négociations avec le Conseil dont la position devrait être connue le 5 et 6 juin prochains.

Commission et Parlement se sont exprimés en faveur de la réglementation pour la protection des données à une très forte majorité tout en renforçant, à chaque fois, les dispositions initialement prévues, notamment sous l'influence d'une actualité qui rappelle en permanence les dérives d'usage et de contrôle des données personnelles et le développement de la cybercriminalité.
Aussi, ce contexte ne laisse aucun doute. Il faut se préparer dès maintenant, il faut être prêt avant que la législation l'impose.

En effet, législation ou pas, les risques et les enjeux sont tels, les enjeux économiques, mais aussi en termes d'image de marque et de confiance de la part des clients et des partenaires, qu'il n'est plus l'heure d'attendre encore.

Le renforcement progressif de la législation impose définitivement de mettre en place un système de management de la sécurité de l'information dont plan de continuité d'activité et dispositif de suivi des incidents sont parties intégrantes

Partageons, si vous le voulez bien, une évidence pour commencer ce chapitre.

Le principe de sécurité de l'information, la protection des données à caractère personnel, mais pas seulement, le principe de sécurité de l'information ***s'inscrit nécessairement dans une approche globale de la Sécurité de l'Information de l'entreprise*** non dissociable de son environnement.

Par conséquent, il impose de passer par la mise en place d'un véritable management de la sécurité de l'information et de ses outils, depuis l'analyse des risques au plan de récupération et de continuité d'activité en passant par un dispositif de gestion des incidents de sécurité dûment formalisé et autres.

Une démarche en cours de mise en place à effets collatéraux, une démarche conforme à son objectif, améliorer le niveau général de la sécurité des systèmes d'information dans toutes les entreprises …

C'est une évidence. Un peu plus tôt, un peu plus tard, mais il est sûr que l'obligation de notifier selon une procédure formelle les failles de protection à une autorité habilitée ne restera plus longtemps limitée aux seuls fournisseurs d'accès et de services de télécommunication.

J'ajouterais que lorsque la réglementation cible une catégorie d'acteurs économiques, que ce soit des services télécoms, des secteurs économiques d'activité déterminés ou des opérateurs d'importance vitale [3] …, c'est toute la chaîne d'activité concernée qui est impactée. Ce sont aussi les sous-traitants, prestataires et autres fournisseurs de services annexes compte tenu de l'interdépendance des

[3] (*) La loi de Programmation Militaire 2113-1168 du 18 décembre 2013 met à la charge des opérateurs d'importance vitale (OIV) de nouvelles obligations, notamment une obligation de notification, bien évidemment, mais, cette fois, il s'agit d'informer "sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information …" nous en reparlerons.

activités et des enjeux économiques et stratégiques en termes de continuité et d'efficacité issus de ces partenariats.

Par conséquent, encore une fois, les dirigeants d'entreprise doivent définitivement passer à l'acte si ce n'est pas encore fait afin de garantir la sécurité de l'Information de leur entreprise et être en conformité avec les évolutions de la règlementation.

Cela ne signifie pas forcément des investissements coûteux. Je le souligne notamment à l'attention des petites et moyennes entreprises.

Il s'agit d'abord de bien connaître les risques attachés à ses activités et les moyens de s'en protéger et de partager cette approche avec ses personnels, sans oublier de mettre en place les dispositifs de recours indispensables en cas d'accident. Plan de continuité d'activité, politique de sauvegarde, dispositif d'alerte et de gestion des évènements de sécurité … des dispositifs évoqués dans différents articles de ce site, proposés à votre attention.

Vos questions et observations auprès de guillet.lionel@gmail.com sont les bienvenues.