IMPACT DU RGPD SUR LA SÉCURITÉ DE L'INFORMATION

suite à la Conférence-débat du 19 mars 2018 animée par Dominique Doquang

Mayeul Obel Okeli
Mayeul.obelokeli@gmail.com

Résumé :

Cet article analyse l'impact et l'influence du RGPD (Règlement Général de la Protection des Données) sur la sécurité de l'information des entreprises.

Mots-clés :

RGPD, Sécurité, Union Européenne, CNIL

Aux aurores du 25 mai 2018, tous les acteurs des tissus économique et social de l'Europe se réveillent sous les premiers sons de cloche du nouveau Règlement Général de la Protection des Données (RGPD) initié par l'Union européenne.

En effet, les retentissements de ces cloches annoncent la mise en application du règlement précité, symbole de la reconnaissance du mauvais traitement des données personnelles par les entreprises et les collectivités publiques.

Dans une démarche de simplification, cet article ne traitera que l'impact ou l'influence du RGPD sur la sécurité de l'information des entreprises à but lucratif.

OBJECTIFS

Le RGPD affiche trois objectifs principaux :

- renforcer le droit des personnes ;
- responsabiliser les acteurs traitant des données ;
- crédibiliser la régulation.

SANCTIONS PRÉVUES PAR LE RGPD

Le RGPD prend ainsi la forme d'un fouet destiné principalement aux entreprises, en préconisant des sanctions financières contre les entreprises en cas de non-respect des clauses prévues par ce nouveau règlement, garant du droit des données personnelles.

Parmi les sanctions envisagées par le RGPD, on peut citer :

- 4 % du Chiffre d'Affaires (CA) mondial ou 20 millions d'euros, le législateur prenant en compte le montant maximum des deux ;
- indemnisation de toute personne lésée matériellement ou moralement ;
- suspension des flux partant hors Union européenne (UE).

RGPD ET LE DROIT NATIONAL

Les Européens concernés par le RGPD se sentent désormais dotés des manettes pour gérer leurs données personnelles, mais ne disposent pas d'éléments pour apprécier, à ce jour, l'efficacité ni l'efficience de cette nouvelle réglementation dans la vraie vie.

Certains diront que c'est trop tôt pour porter des jugements. En revanche, d'autres se perdent dans la définition de la frontière des rôles du RGPD et de leur institution nationale de protection contre l'atteinte de l'identité humaine, par exemple en France la CNIL (Commission Nationale de l'Informatique et des libertés).

Le RGPD empiète-t-il sur certains rôles attribués à ces institutions nationales ?

Pour le commun des mortels, cette question est une équation à plusieurs inconnues.

Pour illuminer la lanterne, il importe de savoir que le RGPD n'est pas une institution, c'est un règlement européen que chaque pays européen s'engage à faire respecter sur son territoire. Dans le cas de la France, la CNIL est le garant de la mise en application et du respect du RGPD.

Au point de vue juridique, le RGPD est un règlement qui s'impose à tous les états de l'Union européenne (UE). Si ces états veulent aller plus loin, ils le peuvent. Le droit national peut ainsi renforcer la protection des données personnelles.

L'essence du RGPD est dans la convergence et l'unicité, pour renforcer non pas les lois existantes au niveau national, mais la directive 95 existant au sein de l'UE.

BUSINESS, RGPD ET SÉCURITÉ DE L'INFORMATION

Le RGPD porte l'étendard de la protection des données personnelles.

Les données personnelles constituent une déclinaison de l'identité d'une personne. Cela concerne aussi bien les employés et partenaires que les clients d'une entreprise. Par client, il faut entendre toute personne qui bénéficie d'un service gratuit ou payant d'une entreprise.

La problématique de la protection des données personnelles dénonce la pratique de la sécurité informatique des entreprises et collectivités publiques. Nous le savons tous, la sécurité informatique d'une organisation est un thème débattu et pris à cœur par les entreprises depuis bien des décennies.

Dans le livre intitulé « Sécurité informatique et réseaux » de Solange Ghernaouti, édité en 2013, on peut lire :

- « La sécurité informatique est un processus continu destiné à prévenir des événements dommageables ou à en limiter des effets ».
- « Pour une organisation, l'objet de sa sécurité est de contribuer à préserver les valeurs, les forces et les moyens organisationnels, humains, financiers et techniques dont elle s'est dotée pour réaliser ses objectifs ».

De ces deux définitions, on peut comprendre que la sécurité de l'information se focalise sur les informations stratégiques d'une entreprise dont la vulgarisation est en mesure de contraindre l'activité de cette entreprise.

Dans la vraie vie, une entreprise ne saurait avoir le même niveau de sécurité dans toutes les couches de sa plateforme de système d'information, sachant que l'investissement en sécurité est proportionnel à la criticité de l'information à protéger. Cela explique le fait que les données personnelles sont considérées ou non comme critiques par l'entreprise.

Les avancées technologiques du Web et de la mobilité occasionnent et facilitent la collecte, par les entreprises, des données personnelles des acteurs économiques connectés au réseau Internet, à n'importe quel moment et partout.

Les entreprises ont vite compris qu'il est possible de tirer un profit des données personnelles, tant qu'elles apportent un revenu supplémentaire et ne compromettent pas leurs activités professionnelles. Face à la profusion de la pratique de vente des données personnelles par des

entreprises à l'insu des personnes concernées, l'intervention de l'Union européenne (UE) s'est exprimée par le caractère obligatoire de l'application du RGPD dans le but d'arrêter ou de réduire ce fléau de vente impropre. Une réglementation existait déjà en France (LIL) et dans la plupart des pays de l'UE, ainsi que des sanctions financières, certes moins élevées, mais ce n'était pas le vide juridique. La différence essentielle tient au fait qu'un règlement est d'application obligatoire, il a force de loi dans tous les pays de l'UE, alors que précédemment la directive devait être transposée par chaque pays de l'UE dans sa loi nationale.

Par ailleurs, la sécurité de l'information à 100% n'existe pas et cela n'est pas un secret. Aucune politique de sécurité, nul service de sécurité, aussi perfectionné soit-il, ne tient si l'intégrité des personnes se trouve mise en cause. En effet, le maillon faible de la sécurité est toujours l'humain.

Les résidents européens se réjouissent du protectionnisme RGPD et des indemnités prévues, mais on oublie que l'humain, employé d'une entreprise, peut occasionner le non-respect du RGPD en exfiltrant, involontairement ou volontairement, des données personnelles détenues par son entreprise.

Le RGPD n'a pas prévu de sanction contre un salarié dans un tel contexte. En fin de compte, c'est l'entreprise qui est sanctionnée pour l'erreur de son employé, et surtout pour l'absence de mise en place d'un dispositif adéquat empêchant ce vol de données.

Le RGPD ne préconise pas de solution technique de sécurité pour la protection des données personnelles. Il ne protège pas les données autres que les données personnelles détenues par une entreprise, que ce soient celles de ses clients, partenaires ou employés. L'entreprise elle-même, en tant que personne morale, ne possède pas de donnée personnelle.

Au point de vue sécurité, le RGPD est un vrai challenge pour les entreprises qui sont astreintes à proposer des solutions innovantes des services reposant sur des technologies modernes telles que le Cloud Computing, par exemple.

Dans le domaine du Cloud Computing, la maturité de la sécurité de l'information déployée par un fournisseur cloud n'est pas toujours rassurante. Il est avéré que la sécurité de l'information constitue l'un des freins de l'adoption du Cloud Computing par les entreprises, surtout sous le modèle cloud public.

L'inquiétude des entreprises concerne le fait de confier, à son partenaire fournisseur cloud, une partie ou la totalité de la sécurité des informations hébergées dans le cloud public d'une part et la capacité de celui-ci à se protéger des cyberattaques d'autre part. On est amené à se demander si le RGPD ne rendra pas difficile l'adoption du cloud par les entreprises.

EXERCICE

Je vous propose, sous forme d'exercice, une question à laquelle je n'ai pas pu trouver de réponse par moi-même.

Énoncé

La sécurité d'une solution cloud public SaaS est à 100% la responsabilité du provider de solutions Cloud.

Une entreprise A, cliente, souscrit une solution cloud public SaaS auprès d'une entreprise B, « fournisseur de solution Cloud ». Dans le jargon Cloud, l'entreprise A et l'entreprise B sont respectivement dénommées « cloud consumer » et « cloud provider ».

Suite à une cyberattaque visant le cloud provider, les données personnelles collectées par le cloud consumer avec sa solution SaaS et hébergées par le cloud provider sont exfiltrées et divulguées par un hacker.

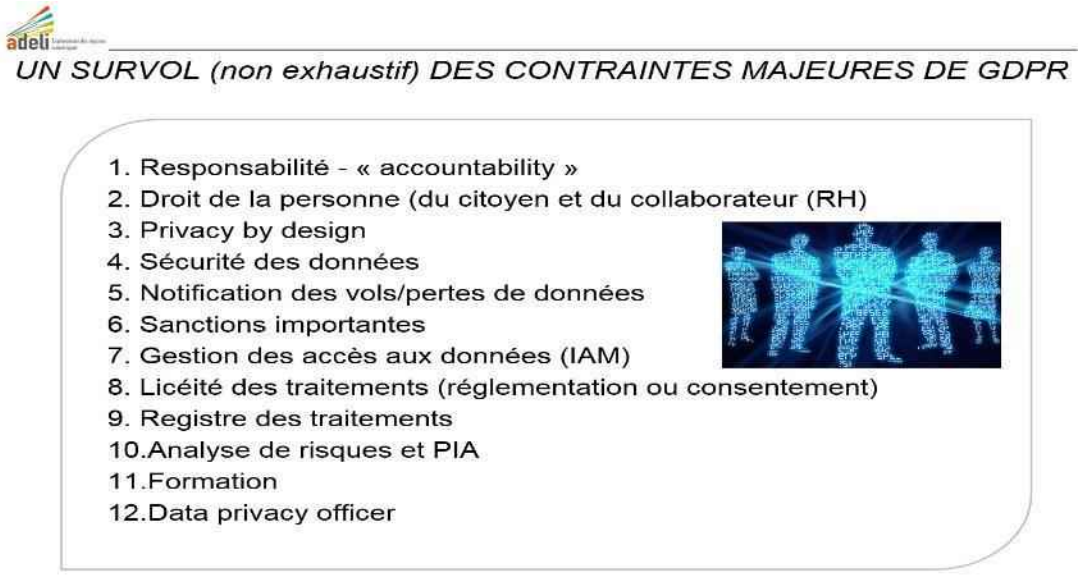
Question

Laquelle des deux entreprises A, cliente (cloud consumer) et B, fournisseur (cloud provider) doit être sanctionnée par le RGPD ? Qui peut m'aider à répondre à cette question ?

La rencontre « Autour d'un verre » organisée par ADELI

La rencontre « Autour d'un verre » du 19 mars 2018, organisée par ADELI sous le thème « RGPD » avait été présentée par Dominique Doquang, expert RGPD et membre du comité ADELI.

Je vous invite à regarder la vidéo de cette présentation sur ce lien Web : https://www.youtube.com/watch?v=4Ebk7rsJ3ks.



ADELI – Rencontre Autour d'un verre - Thème RGPD (ou GDPR en anglais)- Extrait de la présentation de M. Dominique Doquang

Je me suis rapproché de Monsieur Dominique Doquang, qui a accepté de me donner quelques éléments de réponse que je prends plaisir à partager avec vous. Je tiens à préciser que ces éléments de réponse ne sont pas exhaustifs.

Eléments de réponse par Dominique Doquang

Le RGPD n'a pas à donner la formulation de façon précise à de multiples questions telles que celle-ci. Il donne les éléments permettant d'appliquer le droit. Les entreprises A (cloud consumer) et B (cloud provider) pourraient être toutes les deux responsables, mais pas au même titre.

En tant que responsable de traitement, le mandataire (cloud consumer) n'a pas mis en place, le cas échéant, les mesures d'audit pour s'assurer de la qualité des mesures de sécurité mises en place par le sous-traitant, fournisseur de solution cloud (sous-traitant du cloud provider et éditeur de l'application cloud SaaS).

En tant que responsable de traitement, le fournisseur de solution cloud (cloud provider) n'a pas mis, le cas échéant, les mesures de sécurité suffisantes pour assurer la protection des données personnelles.

Le terme le cas « échéant » est important, car il peut y avoir plusieurs cas où la responsabilité, au sens RGPD, n'est pas en jeu (par exemple un acte de malveillance d'un des salariés).

Ce cas de figure donnera naissance à de multiples combats juridiques pour définir la répartition des responsabilités juridiques des deux parties en présence.

QUE DOIT-ON RETENIR ?

Le RGPD sanctionne les entreprises qui font preuve de mauvais usages des données personnelles. Il est l'expression d'un rappel aux entreprises des moyens à mettre en œuvre pour protéger les données personnelles critiques ou non contre les cyberattaques et les autres méthodes d'exfiltration de données.

En dernière analyse, le RGPD ne se limite pas à sanctionner les entreprises, il influence largement l'organisation ainsi que la stratégie d'une entreprise qui trouve son confort dans la sécurité informatique. Pas de sécurité informatique, pas de business.

Faut-il envisager un règlement européen portant sur les cas d'usage des autres données qui ne font pas partie de la famille des données personnelles ?