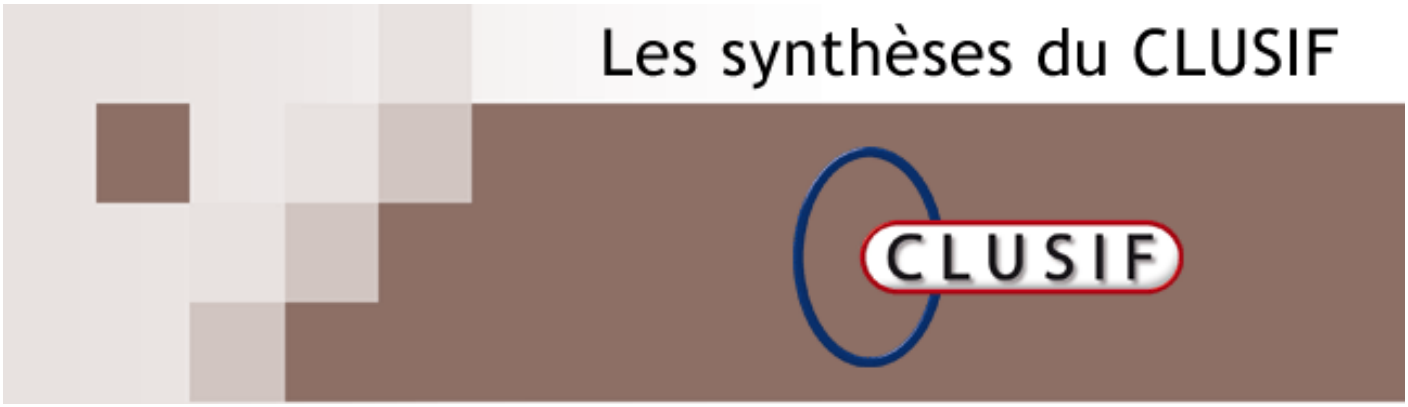

Droit et société de l'information : point sur la réglementation - *Synthèse de la conférence thématique du CLUSIF du 6 décembre 2017.*

La multiplication de textes ayant un impact sur les responsables des systèmes d'informations, qu'ils soient le fait du législateur français ou de l'Europe, peuvent inquiéter. Pourtant, l'environnement législatif peut devenir un atout permettant à la fois de porter les demandes des services informatiques et de soutenir l'activité de l'entreprise. Depuis deux ans, le Club de la sécurité de l'information français (CLUSIF) et CYBERLEX (Association du Droit des Nouvelles Technologies) travaillent conjointement à l'élaboration d'un document permettant aux juristes et aux responsables de la sécurité des systèmes d'information de mieux appréhender les tenants et aboutissants, tant techniques que juridiques, des textes de loi.

Au cours d'une conférence dont le thème était **« Droit et société de l'information : point sur la réglementation »** qui s'est déroulée mercredi 6 décembre 2017, professionnels du droit et acteurs de la sécurité de l'information se sont succédé pour présenter ce « *vademecum* » des obligations juridiques liées aux systèmes d'information, et, pour évoquer plus largement les moyens à mettre en œuvre pour adresser cette problématique.

Vademecum - Obligations juridiques liées aux systèmes d'information

« L'environnement réglementaire est de plus en plus riche et il va au-delà du Règlement européen sur la protection des données (RGPD), c'est pourquoi il nous a semblé nécessaire d'associer CYBERLEX et le CLUSIF dans un travail commun, permettant de faire le point sur ce sujet », a indiqué en introduction **Thierry Chiofalo, administrateur du CLUSIF**.

« Pour comprendre le mieux possible la portée de ces textes et les exigences qu'ils font peser sur les systèmes d'information il est indispensable d'amener les bons acteurs à communiquer facilement entre eux, notamment DSI et juristes » a-t-il précisé. Avant d'ajouter qu' « il convient aussi de ne pas développer de conformité en silo mais d'identifier toutes les synergies possibles : PIA (Privacy Impact Assessment) et analyse de risque ne sont après tout qu'une même méthode déclinée selon deux finalités, sécurité de l'organisme d'une part et sécurité du citoyen d'autre part»,.

Réaliser un outil pratique pour les opérationnels. Telle était la priorité du groupe de travail, a expliqué **Gilles Rouvier (avocat et membre de CYBERLEX)**. « Une dizaine de personnes ont travaillé sur le sujet pendant deux ans et nous présentons aujourd'hui, une série de fiches pratiques, un *vademecum* qui doit servir de fil d'Ariane pour se retrouver dans cette accumulation de textes. Il fallait utiliser un langage commun aux directions des systèmes d'information et des juristes, quelque chose qui réponde aux besoins des métiers et du business en général », a expliqué l'avocat.

Pour **Ludovic Petit, directeur de la sécurité d'Altran et membre du CLUSIF**, il s'agissait de comprendre les enjeux des systèmes d'information en matière de sécurité et de protection des données de l'entreprise, de disposer de cas d'usage, d'outils pédagogiques. « Il ne faut pas perdre de vue que le cadre réglementaire conditionne aussi les

déploiements techniques », a-t-il souligné. « Le cadre légal est une composante incontournable du travail des responsables de la sécurité informatique », a-t-il souligné.

Le document du groupe de travail aborde de nombreux sujets qui ont été débattus tant par les juristes que par les responsables des systèmes d'information : responsabilité civile et pénale, notion de droit de la preuve, risques, surveillance des utilisateurs, sécurité des contrats, protection des données personnelles, … S'il ne vise pas l'exhaustivité, le document publié mercredi 6 décembre sera amendé et mis à jour au fil des ans et constitue, de l'aveu de tous les intervenant, une « boussole ».

Enjeux et impacts de la réglementation

Il est vrai que pour les DSI, les enjeux et impacts ne manquent pas, comme l'a noté **l'avocate Garance Mathias** : contrats, règlements européens, identification et évaluation des risques, protection des SI, conformité, données à caractère personnel, secret des affaires, traçabilité…

Garance Mathias a rappelé le calendrier qui s'impose à tous : le 9 mai 2018 marquera le délai maximum de transposition de la directive NIS (Network and Information Security). Le 25 mai, ce sera l'application du RGDP. Le 9 juin marquera pour sa part le délai maximum de transposition de la directive sur le secret des affaires. Et le règlement sur la e-Privacy suivra dans un avenir relativement proche.

> « Tous ces textes ont des finalités différentes mais un objectif commun : assurer un niveau élevé de sécurité, de protection des secrets d'affaires, de protection des données à caractère personnel, de protection de la vie privée et des communications électroniques ».

Une vision opérationnelle de l'impact de la réglementation a été apportée par **Thierry Henniart, correspondant informatique et libertés d'une Collectivité territoriale et membre du CLUSIF**. « Pour notre part, en tant que collectivité, nous avons déjà dû nous adapter au Référentiel Général de Sécurité (RGS), au règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS », à la qualification des prestataires et des services ou à la Politique de sécurité des SI de l'État ». Thierry Henniart voit le RGPD comme une sorte d'opportunité. En effet, le règlement a généré une forte couverture médiatique et tout le monde en parle à l'intérieur des organisations. De la direction générale au service juridique, marketing, communication, les métiers sont tous impactés et alertés. Les demandes des responsables des systèmes d'informations seront donc entendues, selon lui.

> « La réglementation, ce sont des contraintes mais aussi des opportunités. Ce sont des briques, des cadres, sur lesquels on peut s'appuyer pour avancer et pour nous, ce cadre profite à l'e-administration et à la e-démocratie. Si les réglementations ont des finalités différentes, elles partagent toutes des moyens communs qui tendent à améliorer la sécurité des systèmes d'information des collectivités territoriales et à renforcer la confiance des citoyens envers leurs administrations publiques ».

De nombreuses évolutions législatives sont venues renforcer le droit en matière numérique, a pour sa part **rappelé la magistrate Myriam Quéméner**, actuellement détachée au sein du ministère de l'Intérieur comme conseiller juridique de Jean-Yves Latournerie, Préfet en charge de la lutte contre les cyber-menaces.

« Ce fut par exemple le cas de la Loi pour la république numérique qui mentionne l'utilisation d'un traitement algorithmique dans le cadre d'une décision administrative et la possibilité pour l'usager d'en demander les principales règles. Mais aussi la loyauté des plateformes en ce qui concerne la transparence de l'information pour les consommateurs et la régulation des avis en ligne », a rappelé la magistrate. Ce texte a également « multiplié par 20 le plafond des sanctions que peut prononcer la Commission nationale informatique et libertés (CNIL) et protégé les

citoyens qui détecteraient des failles informatiques et les portent à la connaissance de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) ».

En matière de législation, « Il faut trouver un équilibre entre une régulation-bâton (pénal) et le développement du numérique comme levier économique, tout en assurant la confiance. Le point commun de tous ces textes est de renforcer la sécurité tout en favorisant le développement. De même, il y a un équilibre à trouver entre la volonté de transparence et le secret des affaires », a souligné Myriam Quéméner. Pour la magistrate, il faut également éviter de vouloir créer de nouvelles lois à tout prix pour combler de supposés vides juridiques quand une simple adaptation de lois existantes suffirait.

Enfin, Myriam Quéméner a rappelé que le Paquet Cyber avait été présenté le 13 septembre dernier. Il prévoit notamment la transformation de l'ENISA en agence européenne de sécurité, la création d'un label européen pour les entreprises qui produisent les dispositifs informatiques qui pilotent les infrastructures clefs et une lutte renforcée contre la fraude aux moyens de paiement.

Dialogue autour de la réglementation des systèmes d'informations

Au cours d'une table ronde qui a suivi les interventions, **Pierre Desmarais, avocat**, a souligné l'intérêt d'une l'harmonisation et du développement de référentiels internationaux qui sont un atout pour les entreprises à l'exportation. Pour **Corinne Thiérache, également avocate et membre du groupe de travail**, le *vademecum* permet d'utiliser un langage commun, « on obtient plus d'adhésion lorsque tout le monde comprend le sens et la portée des textes ». Tous ces textes vont « pousser les entreprises à devenir des acteurs actifs de la sécurité, c'est un investissement sur l'avenir qui permettra d'éviter des problèmes d'image qui ont un impact sur l'activité », a-t-elle souligné.

Adèle Adam a pour sa part expliqué les impacts sur son entreprise, **Claranet**, qui est à la fois sous-traitant et responsable du traitement des données informatiques. « On héberge des données santé, ou des données critiques et les exigences des clients sont fortes. Elle a souligné, surtout, l'importance d'intégrer l'ensemble de ces exigences autour d'un tronc commun. En l'espèce, le SMSI ISO 27001 constitue un socle de conformité auquel sont ajoutées des briques au fil du temps et des nouvelles exigences réglementaires ».

Clara Petit, avocate du cabinet Iteanu a enfin souligné que le mot « risque », bien connu des RSSI et DSI habitués à les identifier et les évaluer, faisait son chemin dans les textes juridiques. Ainsi, elle a relevé qu'il apparaissait 78 fois dans le RGPD. « Les pirates informatiques ont un train d'avance. Il ne faut pas nier le risque mais apprendre à faire avec, faire preuve de bon sens et réfléchir ».