Synthèse de la conférence thématique du CLUSIF du 12 décembre 2013.

Les textes et projets législatifs consacrés aux nouvelles technologies se multiplient, tant à l'échelle nationale que régionale : protection des données personnelles, obligation de sécurité, notification des incidents, interception des informations numériques, autant de sujets désormais couverts par le droit. Ainsi, les professionnels de la sécurité informatique ne peuvent plus ignorer ces questions juridiques. Le 12 décembre 2013, le CLUSIF a consacré une conférence au droit de la SSI afin de **présenter le cadre légal actuel**, mais aussi, par-delà l'accumulation des textes, d'**identifier les tendances.** L'objectif était d'**anticiper les évolutions législatives**, en permettant ainsi d'inscrire les projets SSI dans le long terme[1]. Six orateurs sont intervenus : Annabelle TRAVERS-VIAUD (BULL), Olivier JOFFRAY (AiBiZU DSX), Garance MATHIAS (Cabinet d'Avocats Mathias), Myriam QUEMENER (Ministère de la Justice) et, en animateur de la table ronde, Jean-Marc GREMY (Cabestan Consultants et Vice-Président du CLUSIF).

Une protection des données personnelles renforcée[2]

Le projet de règlement européen sur la protection des données personnelles a été déposé devant le Conseil en octobre 2013. Il a vocation à remplacer l'actuelle directive européenne. L'objectif du Parlement européen est une adoption en 2015, pour une application effective deux années plus tard. Ce texte prévoit **une mutation du poste de Correspondant Informatique et Libertés (CIL) vers celui de Délégué à la Protection des Données (DPO ou *Data Protection Officer*)**. La mission première de ce dernier sera de contrôler la conformité des traitements de données personnelles aux exigences légales, rapprochant ainsi cette fonction de celle de commissaire aux comptes. Prônant la transparence, le projet vise également à **renforcer les droits des personnes concernées**. Enfin, le texte fera peser sur les organismes **une lourde obligation de sécurité** impliquant une analyse d'impact, une sécurisation dès la conception, une documentation détaillée, des contrôles de sécurité et des certifications. Les audits et les produits certifiés joueront alors un rôle important en matière de **preuve de conformité « informatique et libertés »**.

[1] Lazaro PEJSACHOWICZ, Président du CLUSIF

[2] Olivier JOFFRAY (AiBiZU DSX), « Règlement européen sur les données personnelles : J-18mois – Quelles exigences et quels moyens pour s'y conformer ? »

Le développement de la sécurisation des systèmes d'e-paiement[3]

Depuis les années 2000, un cadre normatif consacré aux moyens de paiement en ligne se développe. Il s'organise autour de deux textes : un standard technique PCI-DSS[4] et une recommandation de la Banque Centrale Européenne (BCE[5]), dont l'objectif commun est de **lutter contre la fraude**. Ces normes s'adressent aux **prestataires de services de paiement** (PSP) et érigent des **exigences de sécurité** communes, telles que la séparation des rôles et responsabilités ou le chiffrement des flux. Pour autant, certaines différences persistent quant au champ d'application, rendant ainsi ces **textes complémentaires**. La démarche adoptée diffère également : la BCE opte pour le « *comply or explain* », qui s'oppose à la conformité stricte côté PCI-DSS. Enfin, si la conformité à PCI-DSS peut être exigée par les clients, seules les recommandations de la BCE s'imposent aux PSP en vertu de la directive européenne sur les services de paiement. **Deux nouvelles recommandations** sont d'ailleurs en cours d'élaboration, l'une consacrée aux PAAS (*Payments Account Access Service*) et l'autre au paiement mobile.

La captation de données informatiques par les services de l'État[6]

L'actualité abondante autour de PRISM a réveillé la crainte des citoyens européens quant à la protection de leur vie privée face à d'éventuels abus des États-Unis, et a placé le ***Patriot Act*** au cœur du débat public. Cette loi d'exception permet aux autorités américaines d'investigation de capter toutes les données transitant sur le territoire américain. Une **définition large du terrorisme** a permis d'étendre son application à des affaires de droit commun. Les informations et fichiers électroniques peuvent être transmis, après autorisation d'un juge, mais sans que les prestataires sollicités puissent en informer quiconque, en vertu de la **clause dite du « bâillon »**. Quant aux données de connexion, si l'ordre de bâillonnement ne s'y applique pas, leur communication n'est soumise à aucun contrôle préalable du juge. Ces dispositions inquiètent et poussent les prestataires à exiger une localisation des données au sein l'Union Européenne. Pour autant, avec le **projet de loi de programmation militaire**, certains dénoncent un « **PRISM à la française** ». Contrairement au *Patriot Act*, ce texte ne fixe aucune limite temporelle à son application. Il permettrait aux agents habilités de demander aux opérateurs, FAI et hébergeurs la communication en temps réel des informations circulant ou conservées sur leurs réseaux et services, et ce, sans autorisation ni contrôle d'un juge. Cette loi vient d'être adoptée par le Parlement, mais elle pourrait être soumise à un contrôle de constitutionnalité avant sa promulgation.

L'organisation de la lutte contre la cybercriminalité[7]

Confrontée à une hausse de la cybercriminalité, la justice ne peut plus ignorer les évolutions technologiques. On assiste à une prise de conscience des institutions nationales et européennes. En 2001, la **Convention de Budapest** est venue tracer les lignes directrices pour les États souhaitant développer une législation nationale en la matière, et améliorer la coopération internationale. Depuis, les **structures européennes** telles que l'ENISA, Interpol et Eurojust se mobilisent. En janvier 2013, l'EC3, centre européen consacré à la lutte contre la cybercriminalité rattaché à Europol, a été créé. Les **textes européens relatifs à la sécurité des réseaux se multiplient**. On peut ainsi citer la directive relative aux attaques contre les systèmes d'information, le projet de règlement sur la protection des

[3] Annabelle TRAVERS-VIAUD (BULL), « Recommandations de la BCE pour la sécurisation des paiements sur internet et PCI-DSS »
[4] PCI-DSS : *Payment Card Industry – Data Standards Security*
[5] BCE : Banque centrale européenne, *Recommendations for the security of internet Payments*
[6] Garance MATHIAS (Cabinet d'Avocats Mathias), « Mythes et réalités du *Patriot Act* et… de ses équivalents »
[7] Myriam QUEMENER (Ministère de la Justice), « Cybercriminalité et cybersécurité : réponses européennes et internationales »

données personnelles, ou encore le récent projet de directive relatif à la protection du secret des affaires. En droit interne, les textes législatifs et les services spécialisés fleurissent. La mise en œuvre de ces dispositifs s'organise progressivement. Au-delà des textes, une **véritable politique pénale** doit être définie. C'est tout l'objet du **Programme européen de lutte contre la cybercriminalité** lancé en février 2013. L'objectif est de fixer une approche commune en matière de sécurité des réseaux, de lutte contre la criminalité en ligne et de protection des consommateurs. En France, le **prochain rapport interministériel sur la cybercriminalité** devrait proposer une esquisse de notre politique pénale.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF
http://www.clusif.fr/fr/infos/event/#conf131212.