Quelle sécurité dans un monde de transformation numérique ?

Compte rendu des Rencontres Cyberlex du 15 janvier 2018

Pour ouvrir les rencontres annuelles Cyberlex 2018, organisées au Palais du Luxembourg sous le parrainage de Monsieur Philippe Adnot, sénateur de l'Aube, Élise Dufour, présidente de Cyberlex, a souligné comme la transformation numérique est devenue un enjeu stratégique majeur pour les entreprises. En outre, les incidents de sécurité connus notamment par SFR, Darty et Hertz, ont montré que la question est aujourd'hui primordiale et ne peut être ignorée. L'objectif de ce colloque était de donner la parole à tous les acteurs concernés et de s'interroger sur les solutions juridiques pouvant être apportées.

I. ASPECTS SOCIÉTAUX ET ÉCONOMIQUES

Monsieur Mounir Mahjoubi, secrétaire d'État au Numérique, a ouvert ces rencontres. Après avoir souligné que l'un des enjeux de la sécurité numérique était de sensibiliser tous les citoyens, il a développé plusieurs piliers d'action en la matière. Le premier pilier concerne la constitution de champions économiques du numérique en France et la manière de les créer. Il s'agit de définir les moyens pour faire grandir les sociétés du numérique et de l'innovation, afin de transformer des *start-up* en grands groupes de demain. Le deuxième est la transformation numérique de l'État. En effet, pour que la France devienne l'un des leaders mondiaux du numérique, la création de champions nationaux ne suffira pas. L'État doit également montrer l'exemple. L'objectif fixé par le gouvernement est de dématérialiser toutes les démarches d'ici 2022. Cette première étape doit être suivie par l'instauration d'une nouvelle philosophie dans la façon de rendre le service public. On pense notamment à la simplification judiciaire et à la justice numérique. Enfin le dernier pilier est fortement relié aux deux premiers. Le mouvement initié ne doit pas laisser pour compte certains citoyens : il sera donc impératif d'accompagner les 20 % de Français qui aujourd'hui ne maîtrisent pas le numérique afin de les y intégrer. De même, les TPE-PME qui aujourd'hui utilisent peu le numérique devront être intégrées au projet et être accompagnées en ce sens.

CYBER LEX
L'association du Droit et des Nouvelles Technologies

Gilles Rouvier, vice-président et secrétaire général ; **Emmanuelle Cornet-Ricquebourg**, vice-présidente et trésorière ; **Blandine Allix, Jérôme Legrain, Laures Landes, Marc Amal, Marc Pic,** membres du Conseil d'administration.

Ce projet de transformation nécessite une forte sécurité car, sans confiance en la technologie, le numérique ne peut se développer. Cette problématique, qui était jusqu'à présent réservée aux experts, doit être prise à bras-le-corps et diffusée dans la société et notamment dans les entreprises. Or, les menaces à la sécurité numérique n'ont jamais été aussi prononcées et diverses qu'aujourd'hui. Les attaques sont complexes et peuvent toucher un grand nombre d'entreprises simultanément. Elles ne sont plus ciblées comme auparavant. Il est donc impératif de s'adapter. Mounir Mahjoubi voit deux scénarios possibles. Le premier est un renoncement face à ces attaques très sophistiquées et bien plus développées que nos systèmes de défense actuels. Le second est une réglementation du cyberespace en y amenant une « *paix* », en en faisant un espace de confiance. Afin d'atteindre l'objectif de confiance, plusieurs axes sont envisagés. Le premier est la transposition de la directive « *NIS* »[1] qui va ramener le sujet de la cybersécurité au cœur des débats, ce qui permettra de sensibiliser les entreprises et de rappeler les grands principes en la matière. Le deuxième est celui des données, 2018 étant l'année du Règlement pour la protection des données personnelles (RGPD) qui contient un engagement pour la sécurisation des données personnelles allant dans le sens d'une sécurité numérique accrue. *Fake news*, crypto-monnaies… les sujets sont nombreux et complexes. Ils demanderont une réflexion poussée afin que des décisions hâtives ne soient pas prises.

Mounir Mahjoubi conclut en indiquant que les enjeux à venir sont ceux de la structuration européenne autour de ces sujets. La France, l'un des pays actifs en Europe en matière de cybersécurité, apportera son expertise. Elle entend également augmenter la capacité technique, intellectuelle et humaine de la cybersécurité, aussi bien au niveau militaire que civil pour répondre aux enjeux actuels.

II. ASPECTS JURIDIQUES

Élise Dufour était chargée, quant à elle, d'éclairer le sujet d'un point de vue juridique. Elle indique que la transformation numérique, travail global de longue haleine, passe non seulement par une sécurité purement technique mais également par une sécurité juridique. En effet, chacun des acteurs sera impacté par cette révolution et le droit y prendra une part importante. Lors de la mise en place d'un plan de transformation numérique au sein d'une entreprise, les salariés seront directement concernés.

1. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

De nombreux sujets seront alors sur la table : droit à la déconnexion, télétravail, vote électronique, *e-learning*, bulletin de paye électronique, géolocalisation… Les problématiques sont pluridisciplinaires – incluant une composante juridique qu'il faudra maîtriser - et devront être toutes traitées pour réussir la transformation numérique. Au niveau des consommateurs, les problématiques sont également nombreuses. Contractualisation en ligne, archivage, gestion de la preuve… Ces sujets devront être éclaircis. Le RGPD va en ce sens, avec des procédures de sécurisation telles que la protection des données dès la conception et par défaut, en anglais le *privacy by default* et le *privacy by design*. En bref, la remise en perspective dans le monde numérique implique une revue de l'ensemble des process. Ce monde VUCA (*Vulnerability*, *Uncertain*, *Complex* et *Ambiguous*) est l'objet de cette conférence.

TABLE RONDE N° 1 - Quels sont les nouveaux enjeux de la sécurité dans la transformation numérique ?

Modérateur : Colonel Éric Freyssinet, chef de la Mission numérique de la Gendarmerie nationale

La transformation numérique actuellement en marche va engendrer de nombreux bouleversements et risques. Cela concerne aussi bien les citoyens, avec notamment le traitement de leurs données personnelles, que les entreprises, qui peuvent faire l'objet d'attaques. Nouveaux enjeux, nouvelles opportunités, l'objet de cette table ronde était de répondre de manière pratique aux interrogations actuelles. Pour traiter ces questions, Éric Freyssinet a réuni Nabil Bouzerna, Head of Cyber-security Labs & CHESS Platform Architect chez IRT SystemX, Olivier Laurelli, Hacker (affaire *Bluetouff*), Arnaud David, Chief Data Protection Officer chez CGI et Ludovic Petit, Groub Cyber Security chez Altran.

Éric Freyssinet introduit cette table ronde en rappelant que le poste qu'il occupe a pour objectif d'accompagner la transformation numérique au sein de la Gendarmerie. L'institution est confrontée à plusieurs enjeux. Le premier est l'ouverture de son système d'information qui reste aujourd'hui très fermé. Cette ouverture a pour corollaire l'augmentation des risques numériques, qu'il faudra savoir maîtriser. En outre, les données que la Gendarmerie traite sont par nature très sensibles et doivent être sécurisées. Il s'agira donc de transformer le système tout en protégeant ces données. Un autre enjeu est celui de la cybercriminalité. Cette menace pousse à la création de nouveaux outils pour lutter contre ces pratiques.

Pour **Ludovic Petit**, qui gère la cybersécurité chez Altran, l'un des principaux enjeux pour un directeur de la sécurité est de savoir passer du statut de technicien à celui de communicant. Ainsi, il est nécessaire d'adapter les métiers de l'entreprise à la composante numérique nouvelle. Pour ce faire, il convient de comprendre ces métiers et le secteur d'activité de l'entreprise concernée pour adapter l'approche sécurité. Le directeur de la sécurité a donc un rôle important au niveau de la sensibilisation et de la communication, pour faire le lien entre les métiers. La dimension technique reste bien évidemment primordiale mais elle ne prendra pas toute son importance si les parties prenantes n'en comprennent pas l'intérêt. Les directions juridiques et de la sécurité doivent donc avancer de concert. Le cadre légal va conditionner les moyens techniques pouvant être mis en œuvre. Le plus important est donc de développer un langage commun pour adapter les dispositions légales et réglementaires sur le plan technique. La confiance est l'élément essentiel de la réussite de la transformation numérique. Pour cela, il est impératif de démystifier les concepts et de clarifier les notions.

Olivier Laurelli souligne ensuite l'évolution de l'approche des entreprises en matière de sécurité des systèmes d'information. Ces dernières adoptent désormais une démarche d'anticipation afin de tester la sécurité de leurs systèmes, alors qu'auparavant les organismes réagissaient plutôt à la suite d'une attaque. Intervenue au cours des dix dernières années, cette approche proactive dénote une prise de conscience qu'il faut pérenniser. Par ailleurs, les entreprises ont aujourd'hui deux besoins : la résilience, d'une part, et la disponibilité de leurs systèmes d'information ainsi que de leurs données en cas d'attaque, d'autre part. À cet égard, Olivier Laurelli insiste également sur les procédures de mise à jour des logiciels dont le non-respect est souvent à la source de failles de sécurité.

Arnaud David revient sur l'impératif de sensibilisation du plus grand nombre à ces questions. Il considère qu'aujourd'hui, le débat est trop restreint. Ainsi, malgré l'arrivée du RGPD, les mesures de sécurité prévues sont trop générales. Il est nécessaire, de son point de vue, de prévoir un catalogue de mesures à mettre en œuvre et de les adapter aux différentes organisations, publiques ou privées, ainsi qu'aux relations avec les prestataires ou encore avec les clients. Ainsi, il convient d'ajuster les mesures de sécurité au regard des risques encourus. L'idée est de personnaliser la sécurité au cas par cas, *in concreto*, pour permettre une meilleure efficacité.

Au sein d'IRT SystèmeX, **Nabil Bouzerna** tente d'anticiper les enjeux de cybersécurité. Il convient selon lui pour ce faire de procéder de manière empirique, comme dans le cadre d'une expérimentation. En effet, la cybersécurité ne peut être considérée comme une science exacte avec des points définis à vérifier et des « *cases à cocher* ». Il est nécessaire de constamment réévaluer, chercher de nouvelles menaces potentielles pour déterminer et déployer les mesures appropriées visant à lutter contre ces menaces, et limiter les risques en résultant. En effet, la cybersécurité doit se *challenger* pour rester efficace. Il y a dans ce domaine un besoin de proactivité. Il n'est plus suffisant d'avoir une réaction rapide à la suite d'une attaque. Il faut désormais l'anticiper. Pour Nabil Bouzerna, la transformation numérique à l'œuvre aujourd'hui va multiplier les risques et le challenge s'annonce d'autant plus important pour les experts de la cybersécurité.

Ludovic Petit compare l'optimisation de la cybersécurité au travail du serrurier. Ce dernier, pour augmenter la sécurité d'une serrure, va tenter de comprendre comment on la crochète. Il va ensuite adapter le système pour que le crochetage ne soit plus possible. La cybersécurité fonctionne sur le même modèle. Il est nécessaire de tester de nouvelles « *solutions d'attaques* » pour anticiper des méthodes de crochetage non encore développées. Pour cela, il est intéressant de confronter ses approches

avec celles d'un concurrent ou d'un partenaire. L'objectif de la cybersécurité n'est pas d'être uniquement un support technique mais de concourir à faire la valeur d'une entreprise. À cette fin, le dialogue avec le service juridique est également indispensable. Ainsi, la cybersécurité doit prendre en compte la multiplication des plateformes de connexion des individus. Il ne s'agit plus aujourd'hui de placer un *firewall* dans un lieu physique déterminé : les surfaces d'attaque sont beaucoup plus étendues, notamment avec le développement des objets connectés, et la cybersécurité plus difficile à assurer. Au sein des entreprises, le maître mot est la sensibilisation des salariés pour impliquer tout le monde dans cette transformation et ainsi réduire les risques.

Un autre sujet est celui de l'ergonomie de la sécurité. Pour qu'elle soit à la portée de tous, les interfaces doivent être améliorées. Il faut prendre en compte le facteur humain et bannir le jargon technique. C'est pourquoi il convient de développer la cybersécurité en s'entourant d'équipes pluridisciplinaires et en confrontant les modes de pensées. Cela renvoie aussi au besoin de formation des parties prenantes. En effet, les failles de sécurité qui occasionnent des pertes de données sont souvent les résultantes de comportements humains fautifs (intentionnels ou non). Il convient donc de faire en sorte que tous soient concernés par ces questions de sécurité numérique. Voilà un enjeu de la transformation numérique : faire en sorte que chaque employé se sente concerné par le sujet et pense en termes de sécurité.

La donnée personnelle est également un sujet d'actualité avec la prochaine entrée en application du RGPD. Pour autant, se focaliser uniquement sur celle-ci est une erreur. En effet, l'utilisation de la donnée ne s'attache pas qu'à la donnée personnelle. Il s'agit également de réfléchir à l'utilisation de toutes les données et aux modèles de gouvernance. Les nouvelles règles vont permettre à terme d'harmoniser l'ensemble des manipulations de données et d'élever le niveau d'exigence.

Les objets connectés soulèvent également des questions de sécurité. En effet, lorsque l'on commercialise une nouvelle technologie, la sécurité est rarement la priorité : les objets connectés n'ont pas échappé à cette règle et aujourd'hui, des millions d'objets de ce type, très vulnérables aux attaques, sont en service. La transformation numérique devra également apporter des solutions en la matière. Les utilisateurs devront aussi changer leurs habitudes afin de protéger au maximum les données utilisées par ces objets, car la multiplication de ceux-ci entraîne une augmentation potentielle de la surface exposée aux attaques.

Pour **Ludovic Petit**, il y a sur ce point deux dimensions à prendre en compte. Premièrement, la dimension technique : pour gérer ces objets, il faut des infrastructures, ce qui n'a pas forcément été anticipé. Les modèles techniques doivent donc évoluer. Deuxièmement, il faudra identifier les interlocuteurs et les responsabilités, notamment en termes de sécurité.

Pour terminer concernant les enjeux, **Nabil Bouzerna** attire l'attention sur le fait que s'agissant des données, il convient de développer la traçabilité (cf. accès, actions, modifications,… sur les données et sur les informations de manière générale). De nombreuses expérimentations sont faites aujourd'hui pour utiliser la *blockchain* qui permet de se passer de tiers de confiance. Cette technologie permet de tracer les données de manière certaine, de chiffrer et de rendre les données confidentielles.

TABLE RONDE N° 2 - Le droit comme outil de sécurisation ?

Modératrice : Thaima Samman, avocat à la Cour, associée du cabinet Samman

Comme cela a été soulevé lors de la première table ronde, le technicien seul ne suffit plus aujourd'hui à assurer la sécurité numérique. L'expert juridique, de son côté, ne sera qu'un maillon et ne constituera qu'une partie de la chaîne nécessaire. Pour traiter ces problématiques, Thaima Samman a réuni Mathieu Coulaud, Head of Legal chez Microsoft France, Guillaume Vautrin, Senior Legal Counsel chez Google, Alexandra Bensamoun, Professeur de droit privé à l'Université Rennes 1 et Philippe Laurier, Responsable des activités de quantification du risque Cyber chez IRT SystemX. Les intervenants ont également pu interagir avec le député Éric Bothorel, présent à la table-ronde.

Éric Bothorel, député des Côtes-d'Armor et coauteur du rapport d'information parlementaire sur la couverture numérique du territoire, qui aborde notamment les questions de cyber sécurité, plaide en introduction de cette table ronde pour un encouragement de la libre circulation des données tout en définissant un encadrement légal et réglementaire. Sur le sujet brûlant de la cybersécurité, il écarte l'idée d'un processus de certification de masse des objets connectés qui nécessiterait des ressources considérables. Il envisage plutôt une approche par la donnée et l'évaluation de sa sensibilité. La sécurité serait alors envisagée en fonction de la nature de la donnée plutôt qu'en fonction de celui qui l'émet.

Pour **Thaima Samman**, ce qui a changé dans le débat autour de la cybersécurité, c'est l'émergence de l'idée de dialogue et de collaboration. Aujourd'hui, l'enjeu est autant l'échange et la confiance entre les parties prenantes - et notamment entre les acteurs privés et le régulateur pour assurer la sécurité - que la technique pure.

La cybersécurité recoupe la notion d'intelligence artificielle (IA). **Alexandra Bensamoun** distingue IA et robot. Selon elle, une IA n'a pas impérativement une enveloppe corporelle. Par ailleurs, en tant que juriste, elle n'est pas satisfaite des définitions qui fleurissent aujourd'hui et considère que la précision ne nous servira pas sur ce point car la technique est évolutive. Comme rappelé par ailleurs, il n'existe pour le moment que ce qu'on appelle des IA « *faibles* » qui reposent sur trois piliers : des données, des algorithmes qui les traitent et des puissances de calculs. Ainsi, il n'y a pas d'indépendance de réflexion des IA, pas de conscience. En outre, si la cybercriminalité pose un problème au niveau de l'identification des auteurs d'intrusions, l'IA, dans la même veine, fait peur et il existe un risque plus important de captation des données. C'est la raison pour laquelle il est primordial de travailler la confiance. Pour la développer, deux éléments sont nécessaires : l'éthique et la responsabilité.

L'éthique de l'IA est très présente dans les débats récents. C'est un cadre de régulation envisageable qui pourrait être constitué de chartes, de codes de conduite… L'IA deviendrait éthique dès sa conception et le resterait lors de son utilisation. Mais qu'est-ce que l'éthique ? Il s'agit de droit, mais également, selon Alexandra Bensamoun, de « *non-droit* ». L'éthique renvoie souvent aux grands principes tels que ceux de diversité culturelle, de dignité de la personne humaine… Les initiatives dans ce domaine sont variées et d'origine aussi bien publique que privée. Ce foisonnement fait que l'éthique est difficile à appréhender. Pour autant, l'éthique présente des avantages. Elle renvoie à du droit souple qui peut en ce sens évoluer facilement et plus rapidement qu'une loi. Son développement peut permettre la promotion de principes larges et transnationaux et devenir une norme acceptée plutôt qu'imposée. Mais le revers est qu'il y a peu de sanctions au non-respect de l'éthique et qu'il faut se méfier d'un risque de privatisation de norme et de désengagement de l'État.

Mathieu Coulaud insiste sur l'importance de la demande du client en matière d'éthique. Pour rendre technique l'éthique, il faut la traduire en langage algorithmique. Cette éthique est nécessaire pour donner confiance. Pour instaurer cette confiance, il faut développer la transparence du système. Mais qu'est-ce que la transparence ? Elle revient à produire une visibilité dans le fonctionnement des produits et dans les encadrements contractuels. Elle va s'obtenir à travers le droit souple et le droit dur, qui devront s'adapter aux différentes situations. Ce mélange de droits doit permettre d'assurer la sécurité numérique qui entraînera la confiance nécessaire à la transformation numérique.

Guillaume Vautrin voit également le droit comme un outil de sécurisation de la technologie. À ses yeux, le cadre juridique passera principalement par le contrat qui permettra de définir les responsabilités, notamment en cas de perte de données. La responsabilité délictuelle existera mais ne pourra s'adapter aux cas concrets aussi facilement que l'encadrement contractuel.

Pour **Philippe Laurier**, la responsabilité délictuelle va cependant conserver une importance déterminante. En effet, lorsqu'il y a un dysfonctionnement mineur au niveau de la fourniture de service et d'assistance qui fait augmenter les coûts d'une attaque informatique et retarde par exemple de quelques jours la remise en fonctionnement, la responsabilité contractuelle ne s'appliquera pas automatiquement. C'est la responsabilité délictuelle qui permettra alors d'engager la responsabilité d'un prestataire en cas de dommage étranger à toute faute contractuelle. C'est la combinaison des deux types de responsabilité qui permettra d'assurer une sécurité optimale.

L'accès au droit est un enjeu de la confiance qu'il faut instaurer. Une PME, en raison du coût et de la lenteur des procédures, n'aura pas forcément intérêt à faire sanctionner un comportement fautif. C'est pourquoi la mise en place d'organismes et d'autorités, en capacité de pouvoir interroger l'éthique des algorithmes, permettra d'augmenter la confiance et la transparence des processus. Les PME bénéficieront de ces contrôles. On tendrait alors vers de l'« *éthique by design* ». **Éric Bothorel** envisage même la création d'un parquet national du numérique, qui deviendrait alors la 33e chambre. L'éthique ne reposerait alors plus uniquement sur de l'autoévaluation mais également sur l'interrogation par des autorités des modèles algorithmiques en place.

Alexandra Bensamoun voit également se développer à l'avenir la logique d'*accountability* sur le modèle du RGPD, avec une gouvernance interne au sein des entreprises de l'IA. Sans changer complètement la substance juridique, l'approche d'un cadre avec des grands principes et le choix des moyens pour les faire respecter permettrait de responsabiliser les acteurs.

Le droit ne doit pas devenir une source d'insécurité mais doit accompagner la technologie sans constituer un frein à la croissance des futurs champions du numérique que l'on souhaite voir émerger.

En conclusion, pour **Thaima Samman** le droit de la sécurité numérique est en construction et va sans doute imposer une modification profonde de philosophie. Il s'agira de passer d'un droit procédural (on coche la case de la mesure procédurale imposée) à un droit principiel combiné à la responsabilisation des acteurs. Pour le député Éric Bothorel également, le recours à la *soft law* est l'outil le plus adapté à notre économie en bouleversement.

CLÔTURE

Par Monsieur Jean Lessi, Secrétaire général de la CNIL

La CNIL a conclu ces rencontres, en soulignant deux points fondamentaux : l'importance des données personnelles dans le débat sur la cybersécurité et la nécessité d'une approche complète du sujet de la sécurité. La sécurité des données personnelles est importante d'un point de vue économique et social. La digitalisation de nos sociétés crée des tensions sur la vie privée car elle entraîne le décloisonnement de nos vies. Le recoupement de la multitude des informations désormais disponibles sur un individu permet de le rendre moins "flou" aux yeux des autres même s'il ne le souhaite pas. Avant même de parler de sécurité des données ou de leur violation, l'enjeu du respect de la vie privée est exacerbé par la digitalisation croissante. La violation des données entraîne quant à elle, encore plus brutalement, une levée du flou sur les individus. La cybersécurité agit directement sur le lien social de l'individu et donc sa protection. Le problème est de taille, mais il existe des solutions, notamment en adoptant une démarche de sécurité complète, à 360 degrés. La sécurité relève d'une double responsabilité, individuelle et collective. Individuelle, car c'est une obligation pour les responsables de traitement. Le RGPD a le mérite d'élargir le spectre, de saisir tous les acteurs de la chaîne de traitement des données en leur imputant leur responsabilité propre. Le responsable de traitement, les sous-traitants, ont chacun un rôle à jouer dans la sécurisation des données. Celle-ci sera, avec le RGPD, plus fortement contrôlée et sanctionnée. De même, des outils d'alerte tels que les notifications de violations de données seront développés. Mais la responsabilité individuelle n'est pas uniquement une responsabilité de sécurité. Elle concerne aussi l'étape de collecte des données et notamment l'objectif de minimisation de la donnée ainsi que celui de la proportionnalité dans la collecte. Autrement dit, si moins de données sont collectées, la question de la sécurité se posera de façon moins forte.

En plus de cette responsabilité individuelle, il existe une nouvelle responsabilité collective. En effet, il faudra accompagner les responsables de traitements et les sous-traitants dans leurs démarches. En ce sens, la CNIL cherche à développer des outils d'accompagnement, tels que le logiciel open source PIA pour procéder à des analyses d'impact sur la protection des données. La responsabilité collective renvoie également à tout l'écosystème de la sécurité. C'est en ce sens que la CNIL et l'ANSII, notamment, travaillent de concert et échangent au quotidien.

Enfin, l'information et l'implication du grand public seront un enjeu majeur de la transformation digitale. ■