Sciences humaines
& entreprises

Cybersécurité : entre exigence de conformité, protection du patrimoine de l'entreprise et management

2019

Compte rendu

L'Anvie

Asso_Anvie

Anvie, 8, rue d'Athènes, 75009 Paris
Tel : 01 42 86 68 80 / Fax : 01 42 86 58 90
E-mail : claudine.touboul@anvie.fr
www.anvie.fr

Piratage d'ordinateurs, vol de données personnelles ou stratégiques et non-nominatives, atteintes à la propriété intellectuelle et au savoir-faire, ransomware, sans parler d'attaques aux risques systémiques... Les entreprises sont de plus en plus exposées au cyber-risque. Dans ce contexte, les réglementations - nationales et internationales - sur la sécurité se sont multipliées.Est-ce suffisant ? Paradoxalement, pour une victime, la conformité réglementaire de lutte contre les cyberattaques s'impose. Les entreprises se trouvent alors en quelque sorte, entre le marteau et l'enclume. Au-delà des réponses techniques et organisationnelles à mettre en œuvre pour garantir la sécurité des systèmes d'information et de la mise en conformité règlementaire, comment tirer parti des leviers juridiques pour dégager un avantage concurrentiel, instaurer une culture de la sécurité au sein de l'organisation et préserver le patrimoine immatériel de l'entreprise.

Les points à retenir

1. Si les dernières années ont été largement consacrées à la question des données personnelles avec l'entrée en application du RGDP le 25 mai 2018, c'est aujourd'hui la cybersécurité qui représente le défi majeur des organisations face à la recrudescence des cyber-activités malveillantes qui occasionnent des pertes considérables pour les entreprises comme pour les particuliers. Dans près d'un cas sur deux, les attaques ont des impacts concrets sur l'activité des entreprises touchées (indisponibilité du site, arrêt de la production, pertes en chiffre d'affaires, amendes règlementaires, rappels de produits, faillite même) avec un taux d'élucidation juridique faible. La cybersécurité est donc devenue une priorité d'Etat, impliquant une vraie spécialisation administrative et un nouvel arsenal juridique. Au sein du secteur privé, elle devient un marché en pleine expansion tant dans le domaine de la R&D que de celui des assurances et des prestations de gestion de crise.
2. Face aux risques liés à la cybersécurité, se mobilise tout un écosystème d'acteurs : l'ANSSI, les GIRs et le Parquet de Paris étant considérés comme les plus légitimes en France sur le plan juridique.
3. Pour sécuriser les systèmes d'information, les fonctions techniques et juridiques doivent fonctionner en tandem : la collaboration réussie entre le RSSI et DPO est un facteur clé de succès.
4. Les entreprises doivent désormais se préparer à la gestion de cyber-crises. On note de ce fait la souscription de plus en plus courante aux services de cyber-assurances, d'expertise judiciaire, d'investigation numérique et de simulateurs d'attaques. La collecte de preuves dans ce domaine est une tâche d'une grande ampleur.
5. Dans une vision prospective, il est souhaitable que le droit s'ouvre aux évolutions technologiques afin d'édicter des normes servant de repères éthiques tout en restant le plus simple et plastique possible afin de pouvoir traiter un maximum de situations. Il s'agit aussi de peser contre une tendance des grands Groupes consistant à se dégager des risques juridiques à travers leurs CGU.
6. Si la plupart des incidents constatés relèvent d'erreurs humaines, le facteur humain peut cependant être perçu non plus comme une menace, mais sous l'angle stratégique, en misant sur lui pour assurer la protection du patrimoine immatériel de l'entreprise.

Animateur scientifique

Olivier ITEANU, Avocat
Chargé d'enseignement, Université Paris I Panthéon Sorbonne et Université Paris XI
Vice-président, Hexatrust
Membre de l'Agora 41, espace de réflexion mis en place par l'Anssi

Intervenants

Nicolas ARPAGIAN, Directeur de la stratégie et des affaires publiques, Orange Cyberdéfense

Alain BOUILLÉ, Vice-président, Cesin

Matthieu BOURGEOIS, Avocat associé, KGA Avocats

Gaël BOUQUET, Directeur juridique, Centre des constructeurs français d'automobiles

Laurence CLAYTON, expert judiciaire en informatique, LCA-ICSI

Mathieu COULAUD, Head of Legal, Microsoft France

Jean-Louis FIAMENGHI, Directeur de la sûreté, Veolia

Ezechiel SYMENOUH, Cyber Risks Practice Leader, Gras Savoye Willis Tower Watson

Christian SOMMADE, Délégué général, Résilience France

Sylvie SCHLANGER, Avocat général, Chef du Service civil, Cour d'Appel de Paris

Sylvain STAUB, Avocat, Barreau de Paris, CEO, Data Legal Drive

Yves VERHOEVEN, Sous-directeur Stratégie, Anssi

L'Appel de Paris pour la confiance et la sécurité dans le cyberespace

Le 12 novembre 2018, à l'occasion de la réunion à l'UNESCO du Forum de gouvernance de l'Internet (FGI), le Président de la République, Emmanuel Macron, a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Cette déclaration de haut niveau en faveur de l'élaboration de principes communs de sécurisation du cyberespace a déjà reçu l'appui de 564 soutiens, parmi lesquels 67 États, 358 entités du secteur privé et 139 organisations internationales et de la société civile.

Les signataires rappellent que le cyberespace est un lieu d'opportunités mais également de nouvelles menaces. Le développement de la cybercriminalité et d'activités malicieuses peuvent aussi bien mettre en danger nos données privées que certaines infrastructures vitales.Afin de faire respecter les droits des personnes et les protéger en ligne comme dans le monde physique, les États doivent donc agir de concert et s'associer à des partenaires dusecteur privé, du monde de la recherche ou encore de la société civile.

La cybersécurité, un enjeu désormais majeur pour les Etats et les organisations

« *La cybersécurité est un terme neuf* » rappelle Olivier Iteanu, avocat à la Cour d'appel de Paris et chargé d'enseignement à l'Université Paris I Panthéon Sorbonne et à l'Université Paris XI. Avant l'arrivée d'Internet, la sémantique se limitait au terme de « fraude informatique », avec notamment l'introduction, le 5 janvier 1988, d'un chapitre au Code pénal consacré à la fraude au traitement automatisé de données. Dans les années 2000 apparaît le préfixe « cyber », avec en 2001 l'ouverture de la Convention de Budapest sur la Cybercriminalité, premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques. De prime abord, l'Etat a donc instauré une réponse d'ordre judiciaire à ce phénomène criminel en développement.

Or dans les faits, la protection contre ces actes délictuels attend des réponses plus larges, se situant sur un plan préventif, organisationnel, technique et humain - autant de champs que recouvre aujourd'hui la « cybersécurité ». La cybersécurité est désormais devenue une notion majeure au niveau étatique et stratégique pour les organisations, suscitant collaboration entre les pouvoirs publics, le secteur privé et la société civile. C'est ainsi qu'a été lancé, au mois de novembre 2018, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, (ci-contre). Par ailleurs, au mois d'octobre 2019, l'assemblée générale du Cigref a cité la cybersécurité au premier plan de ses préoccupations, constatant que ses membres subissaient quotidiennement l'assaut de cyber-activités malveillantes, nécessitant une vaste mobilisation intersectorielle.

Evolution du cadre réglementaire, exigence de conformité : quels défis ?

Cybercriminalité : de quoi parle-t-on ?

Selon Sylvie Schlanger, avocate générale, chef du Service civil à la Cour d'Appel de Paris, et représentant le Parquet dans le domaine de la cybersécurité, « *c'est le rapport de Marc Robert rendu en 2014 par le Groupe de travail interministériel sur la lutte contre la cybercriminalité qui marque le point de départ d'une série de mesures destinées accroître l'efficacité de la répression dans ce domaine* ».

La cybercriminalité n'est pas une infraction en soi mais regroupe la masse d'infractions commises par les délinquants divulguant leur identité et leurs actions par le biais d'Internet. Cette pluralité intrinsèque de champs d'action rend difficile le suivi de son évolution par les magistrats et policiers. Autre difficulté consubstantielle à cette délinquance : son aspect international. Face à ce constat, la Justice a su s'adapter, en développant à la fois des outils internes et des outils cohérents de coopération avec les Etats européens et au-delà.

Il n'existe pas de définition de la cybercriminalité dans le code pénal, mais le rapport Robert propose la suivante : « l*a cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet* ». Les préjudices occasionnés aux entreprises et aux particuliers dans ce domaine sont édifiants. La demande de rançon, l'attaque virale générale, le vol de données, le phishing et l'arnaque au président sont les cyberattaques les plus fréquentes répertoriées depuis 2018 à l'encontre des entreprises (étude Opinionway-Cesin). Par ailleurs, l'AMF a estimé à 1 milliard d'euros la somme totale escroquée aux Français entre le 1er juillet 2017 et le 30 juin 2019 en matière d'épargne détournée sous une identité frauduleuse.

Face à ce constat, les pouvoirs publics ont renforcé tant la visibilité dédiée à la cybercriminalité au sein des institutions juridiques que la législation pénale spécifique à ce domaine.

- Des services dédiés à la cybercriminalité ont été créés à tous les niveaux de la Justice, tout d'abord au sein des GIRs (Groupes d'Intervention Régionaux luttant contre la délinquance financière, issus de la loi du 9 mars 2004 portant adaptation de la justice à l'évolution de la criminalité), mais aussi au sein du Parquet de Paris, qui dispose désormais

d'assistants spécialisés en cybercriminalité, même s'ils travaillent au sein d'équipes pluridisciplinaires. Le Procureur de la République de Paris a également créé une cellule spéciale auprès de lui, devenue une section, dédiée à la poursuite et à la recherche des cyber-infractions.

- Au plan législatif, un aspect procédural très important tient à l'article 706 72.1 du code de procédure pénale intégré dans ce dernier par la loi du 3 juin 2016. Cet article statue qu'en matière de criminalité organisée, le Procureur de la République, le Pôle de l'Instruction, le Tribunal Correctionnel et la Cour d'Assises de Paris exercent une compétence concurrente à celle qui résulte de l'application des articles sur la compétence territoriale. Par exemple, si une cyber-infraction est détectée à Lyon, le Parquet de Paris a la possibilité de gérer cette enquête concurremment avec le Procureur de Lyon.
- De nouveaux outils procéduraux ont été mis à la disposition des policiers afin de collecter des preuves. Ils comptent les réquisitions d'experts (en bornage, en géolocalisation, interception de fichiers des données numériques) ; l'infiltration dans les réseaux par les policiers, y compris sous pseudonyme ; l'interception des données électroniques à distance.

Il résulte de ces mesures une efficacité accrue de l'écosystème juridique : près de 2 220 condamnations pénales ont ainsi été prononcées en 2012 dans le domaine de la cybercriminalité. On peut également souligner une nouveauté de taille qui tient à la volonté de s'unir et d'assumer un rôle préventif : le Parquet de Paris et l'AMF ont conclu un accord afin de mener des actions d'information et de prévention concernant les attaques en pleine recrudescence ciblant les particuliers mais aussi les entreprises et les administrations.

Les pouvoirs publics luttent contre la cyberciminalité

Si la justice ne peut agir qu'en réponse à un dommage, d'autres acteurs peuvent agir en amont. C'est notamment le cas de l'ANSSI, créée en 2009. « *Le risque de cyberattaque a en effet été identifié en France en 2008 comme un des trois risques majeurs contre la Défense et la Sécurité nationale* » relate Yves Verhoeven, sous-directeur à la stratégie de l'ANSSI. La cyberdéfense et la protection des systèmes d'information sont devenues une priorité nationale, portées au plus haut niveau de l'Etat. Etant donné l'ampleur de sa mission, les activités de l'ANSSI ne cessent de se développer depuis sa création. Afin de sensibiliser l'ensemble des organisations, elle diffuse des guides bonnes pratiques en cybersécurité et a développé une méthode d'analyse du risque cyber destinée aux entreprises. Elle a mis au point un label en matière de cybersécurité et a participé à la mise en place de la plateforme cybermalveillance.gouv.fr, destinée à orienter les victimes des cyberattaques vers des réponses concrètes et des prestataires de proximité. Depuis 2013, la France a renforcé son cadre juridique : elle est ainsi passée pionnière en matière de protection des opérateurs d'importance vitale (OIV) pour la nation. L'Etat a en effet promulgué une loi imposant aux OIV de mettre en œuvre des mesures strictes de sécurité vis-à-vis de leurs systèmes d'information critiques et de se soumettre à des contrôles effectués par l'ANSSI. A ce cadre est venu se rajouter en 2018 la « loi sécurité des réseaux et des systèmes d'information », d'origine européenne, qui concerne de façon plus large les opérateurs jouant un rôle essentiel pour le bon fonctionnement quotidien de l'économie et de la société : transports, établissements pénitenciers, scolaires, énergie, santé, banque. On peut s'attendre dans un avenir proche à l'établissement de standards européens en matière certification en cybersécurité.

Avec l'ANSSI, l'Etat français lutte contre les cyberattaques

L'ANSSI a été créée avec la mission première de préserver la souveraineté et l'autonomie de décision et d'action de la France dans les domaines politique, diplomatique et militaire et de protéger l'ensemble de ses infrastructures critiques sur le terrain. Son approche, strictement défensive, repose sur la prévention, la protection, la régulation et la formation. Elle regroupe 600 experts et accompagne également les organisations en fonction de leur profil par des actions de conseil, de politique industrielle et de réglementation afin de rendre disponibles des produits de sécurité et des services de confiance ou de les aider à comprendre les cyberattaques dont elles font l'objet. Elle revêt enfin un rôle de protection des particuliers en développant des actions de sensibilisation et de formation. L'ANSSI intervient également en soutien technique des services enquêteurs du Ministère de l'Intérieur (DGSI) et du Parquet de Paris.

En moyenne, elle traite 10 à 20 cyberattaques majeures par an, dont les plus connues ont concerné le Ministère de l'Economie et des Finances en 2011, le géant pétrolier Saudi Aramco en 2012, TV5 Monde en 2015 et le malware de sabotage NotPetya en 2017 qui occasionna à l'entreprise Saint-Gobain une perte de 250 M€ en chiffre d'affaires.

La cybersécurité est donc devenue une priorité d'Etat, impliquant une vraie spécialisation juridique et administrative. Au sein des entreprises, comment s'organise-t-elle ? Comment répartir les rôles entre responsables de la sécurité des systèmes d'information (RSSI), délégués à la protection des données (DPO) et directions juridiques ?

Organiser la collaboration entre RSSI, DPO et les services juridiques

Alain Bouillé est RSSI du groupe Caisse des Dépôts. « *Face au constat de solitude du RSSI au sein des organisations, j'ai fondé en 2012 le CESIN, Club des Experts de la Sécurité de l'Information et du Numérique, qui compte aujourd'hui 520 membres et dont je suis aujourd'hui le vice-président* » indique-t-il. Autrefois réservé aux grandes entreprises, le poste de RSSI est en développement et figure désormais à plein temps dans nombre d'entreprises de moins de 2 000 employés. Les conséquences des failles de sécurité observées durant ces dernières années ont en effet souligné l'utilité de la cybersécurité, phénomène totalement exacerbé par la digitalisation de l'ensemble des processus et la cloudification, qui rend d'autant plus nécessaire le fait de classifier la donnée, afin de la protéger contre la criminalité et les espions.

Une collaboration parfois difficile

L'information n'est pas neutre : elle génère des risques et des profits. Elle est un actif de l'entreprise. Si le RGPD a donné un coup de projecteur sur les données à caractère personnel, dans les faits, « *le DPO doit gérer l'ensemble des données, et non seulement celles à caractère personnel* » estime Matthieu Bourgeois, avocat associé chez KGA Avocats, spécialisé en Droit des nouvelles technologies, auteur de l'ouvrage « Droit de la donnée – principes théoriques et approche pratique » (LexisNexis, novembre 2017), et président du Cercle de la Donnée. « *La grande affaire du siècle naissant est de professionnaliser l'usage de la donnée. Toutes les organisations se doivent de nommer un DPO afin d'acquérir la compétence en interne s'assurant de la conformité de la donnée. Le DPO fait le lien entre le service juridique et le RSSI.* » Au mois de mai 2019, deux ans après la création de ce poste, on dénombrait en France 53 000 entités juridiques ayant désigné des DPO et près de 19 000 DPO, certains étant mutualisés.

Le RSSI doit donc désormais cohabiter aux côtés du juriste et du DPO : une coopération parfois difficile. La principale difficulté tient surtout au profil du délégué à la protection des données. Du fait de la jeunesse de ce métier, les DPO peuvent parfois être très théoriques dans leur action. Ils appliquent toute la panoplie de procédures exigées par la CNIL, qui peut manquer de pragmatisme et entraîner de la lourdeur dans les process. « *Il faut un rééquilibrage du DPO par le RSSI car la conformité à la réglementation n'est pas égale à la sécurité* », rappelle Alain Bouillé. L'enjeu est d'opérationnaliser la conformité.

« *La moitié des DPO sont des RSSI* », souligne Matthieu Bourgeois. « *Dans ce cas, cela ne fonctionne que s'il y a un référent RGPD à la direction juridique* ». Dans le cas contraire, si le DPO a un profil juridique, il aura « *besoin d'un bras droit, qui soit un RSSI* », analyse-t-il. Par exemple, lorsqu'il s'agit de réaliser des analyses d'impact ou d'évaluer les mesures de sécurité, le DPO juriste est totalement démuni. L'un des problèmes des juristes est qu'ils n'ont pas été formés à la gestion de projets et à la priorisation. La meilleure solution consiste à prévoir un tandem. « *Le métier de RSSI existe depuis plus de 30 ans. Le RSSI avait déjà l'habitude de travailler sur ces sujets de règlementation, alors qu'un DPO qui a un profil juridique ne va pas rattraper la compétence technique du RSSI sur l'aspect sécurité* », explique Alain Bouillé. De plus, DPO et RSSI doivent disposer d'une expérience humaine et d'excellentes capacités de communication, pour être capables de s'entretenir aussi bien avec la direction générale qu'avec le terrain, quand il s'agit de conduire une enquête. Enfin, plus le RSSI sera indépendant de la DSI, plus il aura la capacité d'agir.

Vers un commissariat à la donnée ?

En tout état de cause, « *le rôle du DPO devrait évoluer* », estime Matthieu Bourgeois. Il envisage notamment la création d'un « commissaire aux données », qui serait alors une profession réglementée. Une idée « intéressante », selon Olivier Iteanu. « Comme le commissariat aux comptes, cela va entrer dans la culture ». On peut noter à cet égard que certains DPO sont issus du métier de l'audit. A terme, il vaut mieux séparer l'action et le contrôle.

Et en cas d'incident, comment procéder ?

Quels acteurs impliquer ?

En cas de cyberattaque, de litige, de manquement, « *tout le monde doit être convoqué à la réunion de gestion de crise : DPO, RSSI, directeur juridique, etc.* », recommande Laurence Clayton, expert judiciaire en informatique au sein du cabinet LCA-ICSI et commissionné auprès de la Cour de Versailles. « *Si les objectifs de l'attaque ne sont pas de consulter les données personnelles, il n'y a pas forcément besoin de convoquer le DPO* ». Cependant, « *la CNIL a une autre opinion* », prévient Olivier Iteanu. Quant à la décision de notifier ou non l'incident à la CNIL, « *elle reviendra au DPO* », souligne Sylvain Staub, avocat au barreau de Paris et CEO de la plateforme Data Legal Drive.

Comment gérer un incident ?

Les étapes de gestion d'un incident sont les suivantes. Dès le début de la mise en place de la cellule de crise, il s'agit d'établir l'ampleur de l'attaque, sa propagation, et de collecter sa preuve technique, vaste chantier en soi. Il faut analyser beaucoup de données et les traces enregistrées dans les systèmes (serveurs, firewalls) pour comprendre ce qui s'est passé. Une

difficulté de cette étape consiste à ne pas effacer la preuve en tentant de restaurer le système. La conservation des traces est également limitée dans le temps. Bien souvent, la preuve a disparu car l'incident résulte d'une attaque ayant débuté six mois plus tôt et peu d'entreprises sont capables de stocker un tel historique de leurs données. La question se pose ensuite d'arbitrer entre restauration rapide du système pour reprendre l'activité de l'entreprise et blocage du système pour collecter la preuve. La personne la plus à même d'avoir intérêt à bloquer le système est le directeur juridique, seul responsable pouvant peser face à la direction générale pour plaider en faveur d'une pause dans l'activité de l'entreprise. Les grandes entreprises disposent parfois d'une capacité de doublage de leurs systèmes d'information, leur permettant de basculer en un temps record sur une plateforme dédiée à la reprise de l'activité, tout en conservant les preuves intactes par ailleurs. Mais la plupart ne peuvent assurer cette continuité, ne disposant pas de traces assez anciennes. Et un autre écueil est celui de l'excès de données à traiter.

La preuve servira le cas échéant à notifier l'incident à la CNIL. Sylvain Staub rappelle à ce sujet le changement de régime de la preuve qu'a instauré le RGPD, qui fait désormais régner le principe d'accountability, obligation faite pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données (obligation de moyens). En cas de détournement de données de cartes bancaires d'un client par exemple, la question se posera de notifier la totalité des clients : dans les faits, si l'entreprise le fait, elle risque de faire faillite. Il conviendra donc de délimiter l'opération (période, type d'achat) afin de proportionner la notification à l'attaque.

Si l'entreprise a besoin de déposer plainte auprès de la gendarmerie, elle doit collecter des éléments suffisants pour constituer une preuve au sens judiciaire, qui pourront ensuite être apportés dans le cadre de la mise en œuvre d'une police d'assurance.

Quelques recommandations

Pour se prémunir des risques, Laurence Clayton recommande d'instaurer une stratégie de sauvegardes des données et d'effectuer une répartition claire des responsabilités en cas d'incident. Certains prestataires de services effectuent des simulations de cyberattaques permettant de tester la capacité à collecter une preuve en cas de crise. Et si un incident survient, il convient de prendre en compte le sujet au plus vite, d'en mesurer les enjeux et d'établir une stratégie de la preuve acceptée par tous, qui dépendra de l'intérêt ou non à collecter la preuve. Vis-à-vis de la CNIL, Sylvain Staub rappelle qu'il convient aussi de documenter de manière préventive l'ensemble des éléments permettant d'éviter les failles de sécurité (obligation de résultat), notamment en cas de sous-traitance d'un traitement. La difficulté est de cartographier la sûreté du puzzle de logiciels et de traitement d'information, métier par métier, au niveau Corporate-succursales-mandataires. Chaque version de logiciel utilisée doit être « privacy by design ». C'est à ce niveau très opérationnel et technique que résidera le cœur de la preuve.

Le rôle des assureurs

L'assurance dispose d'un véritable rôle à jouer aux côtés de l'entreprise en cas de gestion de cyberattaque. Comme Ezechiel Symenouh, Cyber Risks Practice Leader, du groupe Gras Savoye Willis Tower Watson l'indique, « *les contrats d'assurance cyber intègrent trois volets : l'assistance, la responsabilité civile et le dommage* ». L'assistance est le volet le plus important, car elle recouvre la prise en charge de trois types de frais :

- Frais d'IT Forensic, c'est-à-dire, des services d'investigation ;
- Frais juridiques : le cabinet d'avocat pouvant répondre aux questions se posant sur les besoins de notification, et aux rapports avec les clients, fournisseurs et partenaires ;
- Frais en relations publiques : auprès de qui communiquer et comment ?

Le Forensic

Le besoin en termes de cyberdéfense a glissé : on sait de mieux en mieux protéger, mais il faut maintenant savoir réagir en cas d'incident, trouver des preuves, des responsables, et sévir. Les services d'investigation numérique se démocratisent et peuvent être réalisés « à la carte » selon les situations. Le coût d'une enquête formalisée avec collecte méthodique de preuves et démasquage de fautifs reste bien inférieur à celui d'une éventuelle perte de brevet ou de données sensibles par exemple. Le principal problème réside dans la méthodologie : sans protocole d'investigation stricte, les informations obtenues ne sont pas ou peu recevables juridiquement parlant. Les services d'investigation numérique, plus communément appelés Forensic, sont proposés par de plus en plus de prestataires et pallient cette problématique. En confiant l'enquête à un professionnel, la société victime s'assure que tout est fait selon les règles. Il est cependant primordial de faire appel à un prestataire dont les méthodes d'investigation sont les mêmes que celles des autorités.

L'assureur effectue ensuite un calcul d'impact des préjudices de la crise en matière de responsabilité civile et de dommage. Il existe deux types de préjudices : ceux ayant trait à l'intégrité des données, et l'indemnisation des frais supplémentaires d'exploitation engagés pour reprendre le plus rapidement possible son activité (heures supplémentaires, pertes de CA, recours à d'autres serveurs).

Comment se déroule la gestion d'une cyberattaque avec l'aide d'un assureur ?

Dans le cas d'une entreprise ne disposant pas d'équipe en interne pour répondre à la crise, l'assureur effectue une préparation du client en amont (entraînement du client et fourniture d'un kit d'urgence). Si un incident intervient, le client doit appeler la hotline téléphonique disponible 7 jours sur 7 et 24 heures sur 24. Un coordinateur d'incidents, travaillant au sein d'un cabinet d'avocats, lui répond. Il a pour mission de mandater 3 experts en 2 heures (informatique, juridique et le consultant en relations publiques). La plupart du temps, l'assureur a négocié au préalable avec ces prestataires des tarifs et des délais d'intervention : il n'y a pas de contractualisation entre l'assuré et les prestataires. Si l'entreprise dispose déjà de prestataires, l'assurance fonctionne sur un mode de remboursement. Dans ce cas, la preuve de la cause de l'attaque est assez simple : les éléments demandés par l'assureur comportent l'historique des logs du serveur attaqué, les captures d'écran du message de chiffrement ou de la demande de rançon, le rapport d'analyse des réseaux, ou la plainte (par exemple dans le cas d'un vol de PC contenant des données confidentielles). Si l'entreprise dispose de ressources internes en sécurité IT, l'assureur peut en assumer la charge si des heures supplémentaires sont effectuées. Il est recommandé de tenir un tableau de bord ou d'ouvrir un compte de charge comptable listant l'ensemble des frais supplémentaires engagés pour la gestion de cette crise.

L'étape suivante est celle de la quantification des pertes. Il est actuellement complexe de quantifier la perte d'exploitation subie par l'entreprise. L'arrêt total du système d'information pendant 3 ou 4 jours peut occasionner des pertes de revenus, d'opportunité, d'image… Certains clients peuvent décider de résilier leur contrat. L'entreprise doit être en mesure de fournir des éléments comptables des 3 dernières années pour pouvoir effectuer des comparaisons objectives. Ces éléments constitueront la base de l'indemnisation, effectuée par dires d'experts.

Il est recommandé à l'entreprise de pouvoir documenter et retracer l'événement du début à la fin, y compris lorsque des serveurs sont situés en Ukraine, au Portugal ou en Grèce… La personne la plus compétente pour gérer cette crise est le risk manager, s'il existe, car il doit travailler en mode projet pour collecter et mobiliser les ressources internes.

La cyberdéfense est donc en permanente évolution. On peut se demander à quoi ressemblera le monde de demain, encore plus connecté et technologique… Comment anticiper les évolutions liées au développement des nouvelles technologies et les risques sécuritaires et juridiques à venir ? Quelles problématiques juridiques posent les nouvelles technologies ? Quelle contribution les juristes apporteront-ils en termes d'approche et de valeur ?

Droit et révolution numérique : quelles interactions ?

Des entreprises productrices de nouvelles normes

Selon Nicolas Arpagian, Directeur de la stratégie et des affaires publiques d'Orange Cyberdéfense, enseignant à l'Ecole nationale de la Police et à l'Ecole nationale de la Magistrature, fondateur de l'Institut National des Hautes Etudes de la Sécurité et de la Justice et auteur d'une dizaine d'ouvrages, « *on peut s'attendre à ce que les technologies à venir changent la donne juridique actuelle* ». Le Droit a toujours été jusqu'à présent un élément structurant de la cybersécurité. Il définit aujourd'hui la panoplie des risques, en détermine un périmètre, fixe des responsabilités et des sanctions. Par ailleurs, en France, à l'opposé des pays anglo-saxons, le principe de précaution est inscrit dans la Constitution : si une technologie implique des effets collatéraux incertains, il faut éventuellement la brider au regard des risques potentiels. L'arbitrage entre le bien-fondé et les risques d'une innovation relève des prérogatives de l'Etat.

Or si le cadre est jugé trop contraignant, on risque de décourager les innovateurs ou d'entraîner leur exportation. Par exemple, à l'opposé des chercheurs européens qui se le sont interdits, les innovateurs chinois ont mis en place une expertise en matière de reconnaissance faciale ou conduit des actions de clonage sur des animaux. En outre, le caractère privé du financement permet d'abolir le cadre éthique posé en général par les financements publics. Les grandes fortunes privées actuelles financent des programmes de recherche en direction d'une vie magnifiée par le transhumanisme : vie sur la Lune, homme augmenté, homme millénaire…

Auparavant, les Etats étaient les uniques producteurs de normes. Désormais, les grands acteurs économiques créent leurs propres conditions d'utilisation : ce sont eux qui décident si l'usage par les utilisateurs est conforme à leurs intérêts. Un navigateur a par exemple considéré que le tableau « l'origine du monde » de Gustave Courbet n'était pas conforme à sa propre éthique et l'a effacé de tous ses serveurs. La limite des préjudices sera désormais appréciée à l'aune d'acteurs économiques ayant leur propre stratégie, fondée sur leurs intérêts purs ou la raison d'être dont ils se sont dotés. De la même façon que l'armée française a pris la décision de ne pas développer de robots ou de drones tueurs, car elle considère que c'est contraire à son éthique, les entreprises se fixent des règles par rapport à une innovation technologique placée dans un contexte. Avec une société de plus en plus technologique, c'est aussi l'échelle des risques qui progressera, dans le cadre de processus technologiques engageant la vie humaine. Aujourd'hui, un industriel transfère une partie de la responsabilité à son utilisateur. Or plus il y aura de dépendance numérique, plus les liens géographiques seront distendus

entre les infrastructures et ceux en charge de les piloter, diluant la capacité à prendre la main sur les événements. Sur les écrans, tout pourra sembler normal aux opérateurs alors qu'une opération de piratage est en cours. Il sera donc nécessaire de développer des systèmes de capteurs. Les innovations auront pour but en général de baisser les coûts et d'accélérer les processus dans une logique de déconcentration des innovations. Gageons que le marché sera assez mûr pour que les entreprises ne fassent pas l'économie de réfléchir à la sécurité de ces nouvelles formes d'organisation, en intégrant cette dimension dans les prix et les investissements.

Cybersécurité et véhicule autonome : sujet sensible ?

Pour illustrer ces lignes générales d'évolution, Gaël Bouquet, aujourd'hui directeur juridique du Centre des Constructeurs Français d'Automobiles, présente les enjeux liés à la cybersécurité dans le cas du véhicule connecté et autonome. Au préalable, il convient de prendre conscience qu'étant donné l'accroissement en autonomie des véhicules, celle des conducteurs sera de plus en plus faible : ils seront soumis à une certaine prescriptivité.

Dans le monde automobile une rupture technologique concernant l'architecture logicielle, le réseau et l'électronique à bord, représentant plusieurs centaines de millions de lignes de codes - un montant bien supérieur à celui de l'aviation. En effet, la complexité des interactions au niveau routier est bien supérieure à celle du transport aérien. En 2040, le système embarqué pourrait représenter la moitié du coût du développement du véhicule. Au niveau le plus élevé d'autonomie, le conducteur n'aura plus les mains sur le volant. Il pourra même se trouver à l'extérieur du véhicule. Cette situation soulève de nombreuses questions sur le plan juridique, ce qui freine encore le lancement des véhicules totalement autonomes sur les marchés.

Les futures fonctionnalités concerneront les aides à la conduite, les outils de conduite autonome en situation d'embouteillage ou d'autoroute, le stationnement automatisé. Par ailleurs, le véhicule disposera de modes de communication avec les autres véhicules et avec les infrastructures visant à améliorer la sécurité routière, l'empreinte écologique et le développement de services, impliquant un accès aux données.

Ces évolutions technologiques soulèvent plusieurs questions.

- Les conditions préalables de l'accès aux données. Comment faire en sorte que les utilisateurs puissent récupérer leurs données ? Comment rendre les différents systèmes opérables entre eux ? Comment protéger les données, malgré la dispersion des accès ?
- Le risque de cyberattaques. Le hacker peut accéder aux données personnelles et/ou manipuler le système d'information. Il peut user du véhicule comme d'une arme pour des actions criminelles et terroristes.

La réponse à cet environnement est de deux ordres.

- Au niveau technique, la filière automobile prévoit un véhicule étendu, c'est-à-dire segmenté en différentes interfaces (une interface pour l'accès réglementé des informations liées au diagnostic à distance, une interface nécessaire au développement de services Web tels que la maintenance à distance et une interface dédiée aux communications sans fil critiques pour les appareils connectés au wifi du véhicule).
- Du point de vue de la régulation, tous les Etats sont conscients du besoin de développer des standards : cybersecurity act et Draft C-ITS delegated act au sein de l'Union européenne, cybersecurity law, encryption law et SAC/TC/SC 34/WG cyber en Chine, tenue du world forum for harmonization of vehicle regulations à l'ONU avec une proposition de régulation en cours, etc.

Vers un droit plus plastique ?

Mathieu Coulaud, Head of Legal chez Microsoft France et enseignant à l'ESCP Europe souligne que dans le monde numérique, le Droit se doit d'être pragmatique, plastique, guidé par la réalité. « *Soit on considère que le Droit embrasse tout, soit on laisse l'environnement digérer les usages, les comportements et on laisse le Droit s'emparer des questions qui se posent* » précise-t-il. Comme le montre l'exemple du téléchargement dans le domaine musical, un Droit qui embrasse tout et trop vite commet des erreurs. Le téléchargement en France a ainsi été introduit dans un texte de loi comme une infraction. Or trois ans plus tard, le téléchargement était déjà remplacé par le streaming… Le texte de loi était figé et est donc devenu obsolète. Le Droit doit donc davantage se fonder sur des principes que sur des technologies précises. Le législateur doit prendre en compte les sciences, l'évaluation du risque, la conformité (compliance), et doit travailler en partenariat avec les ingénieurs, assureurs et gens du chiffre. La loi Informatique et libertés, par exemple, est extrêmement plastique, alors que le RGPD tient plus de l'outil économique contre la Chine et les Etats-Unis.

L'intelligence artificielle aura un impact sur de nombreux pans du Droit. Elle repose sur des algorithmes et des données, lesquels s'enrichissent l'un l'autre automatiquement. Beaucoup d'éléments de ces strates ne sont en fait pas protégés par la propriété intellectuelle. Il faudra donc y pallier, probablement en recourant à des aménagements de CGU. Les algorithmes, l'accroissement du nombre de données, le développement des objets connectés auront un impact sur le droit pénal, le droit de la preuve, le droit de la distribution numérique, le droit informatique, le droit de l'environnement, des assurances et de l'urbanisme.

C'est l'ingénieur qui produit le changement, et non le juriste, mais les juristes apporteront de la valeur en élaborant des normes, des codes de conduite, et en les faisant respecter. Par exemple, la norme Afnor PINS a pour but de créer un standard de qualité en matière de protection des données. Elle intègre le RGPD, mais constitue une valeur ajoutée par rapport à celui-ci.

De façon générale, les juristes peuvent fournir des réponses aux questions que se posent les opérationnels. Comment construire un green data center ? A cette question, les normes (européennes, notamment) fournissent des réponses substantielles. Le juriste dispose par ailleurs d'un rôle de formation des salariés et des populations. Enfin, il peut contribuer à la réflexion éthique en entreprise. Microsoft a par exemple créé un comité d'éthique sur toutes les questions que pose l'intelligence artificielle. Ce comité traite notamment des questions de recrutement, de reconnaissance faciale, de santé, de place de l'humain dans la responsabilité des décisions, afin d'éviter toute violation du droit de la personne.

« *Il y a peut-être une révolution à faire, consistant à imposer de la simplicité* », conclut Olivier Iteanu. « *Ce n'est pas la complexité qui crée la sécurité juridique*. » Au contraire, il conviendrait d'inciter le législateur à établir des textes fondateurs simples et généraux et à faire confiance aux juges, loin de la pression de l'actualité et de la complexité technologique. Enfin, sur l'équilibre à trouver entre soft law (contrat, éthique, CGU) et loi, une question philosophique demeure : la loi doit-elle être rédigée selon les comportements des individus ou selon le comportement qu'ils devraient avoir ? La loi doit-elle être supérieure à la technique ou la technique à la loi ? Il serait dommageable que le monde soit régi uniquement par des CGU ou que l'éthique cède le pas aux contraintes techniques.

Si certaines statistiques font ressortir qu'actuellement, dans 70 % des cas de cyber-malveillance, un sinistre est dû à une erreur humaine, comment considérer le facteur humain non plus comme une menace, mais sous l'angle stratégique, en misant sur lui pour assurer la protection du patrimoine immatériel de l'entreprise, préparer le management à la prévention du cyber-risque et créer les conditions de la résilience en cas d'attaque ?

L'humain comme facteur clé de succès à la gestion du risque de cyberattaque

Jean-Louis Fiamenghi est directeur de la sûreté chez Veolia depuis 2012. « *A cette date, l'enjeu principal de cette direction consistait à créer les conditions de la sûreté des salariés qui voyageaient dans les pays à risque* » se souvient-il. L'externalisation auprès de sociétés prestaires de sécurité était courante. La cybersécurité relevait de la DSI et présentait certaines faiblesses. En 2016, elle a été rattachée à la direction de la Sûreté, en coordination étroite avec la DSI.

La dimension humaine en cas de cyberattaque est essentielle. Des dispositifs de gestion de crise existent, mais face à l'incertitude, à l'urgence et à la fatigue, on se rend compte que les comportements changent. Les gestionnaires de crise peuvent avoir des réactions manquant d'ouverture envers le collectif. C'est donc plus à présent un dispositif de formation aux soft skills pour faire face à l'incertitude qui a été mis en place : gestion du stress, prise de conscience des effets de la fatigue sur la prise de décision, initiation au MBTI pour apprendre à mieux communiquer et création d'un climat de confiance. L'idée est de favoriser la prise de décision et le bon sens pour répondre à la crise, et de s'extraire de la seule conformité aux normes de gestion de crise.

Si les grands groupes disposent de moyens financiers pour se former à la gestion de crise, qu'en est-il des PME, PMI et ETI ? Afin de former ses équipes à la gestion de crise, on peut avoir recours aux services des consultants en gestion de crise, tel que le général Serge Garrigues, fondateur de SG Consultants, ancien chef d'État-major interministériel de zone auprès du préfet de police pour Paris et l'Ile-de-France.

« *Les crises touchent plus fortement les PME que les grands opérateurs* » constate Serge Garrigues. Comme le montre l'effet « Crue de Seine » de 2016 et 2018, l'ensemble des PME situées dans le centre-ville de Nemours et qui ne s'étaient pas préparées ont fait faillite. De plus, pour gagner certains marchés, il convient de prouver son PCA – Plan de Continuité d'Activité. Il faut par exemple sauvegarder ses données sur un serveur de secours situé au moins à 30 kilomètres de l'entreprise pour éviter de perdre toutes ses données. Mais une fois sensibilisées à la gestion de crise, les PME sont plus réactives et adaptables que les grands Groupes. Il suffit de professionnaliser deux ou trois personnes. Chez SG Consultants, les méthodes sont issues de raisonnements militaires tactiques, ayant pour objectif de trouver des solutions innovantes par rapport à des événements hors normes.

anvie
Sciences humaines & entreprises

Éclairer les pratiques, partager les expériences

De grandes entreprises et institutions de recherche ont fondé l'Anvie en 1990 sur une intuition simple : dans un monde traversé par de profondes mutations économiques, sociales et sociétales, les sciences humaines apportent aux entreprises un éclairage original sur les enjeux à l'œuvre.

Sur la base d'un travail de veille et d'analyse prospective, l'Anvie conçoit et propose des rencontres qui croisent apports de la recherche et témoignages d'entreprises et permettent aux participants de :

- Anticiper et prendre de la hauteur : ces événements proposent un temps de réflexion intense, efficace et précieux pour dépasser les effets de mode.
- S'inspirer et rencontrer : les participants nouent des contacts privilégiés avec d'autres professionnels engagés dans la transformation de leur entreprise.
- Progresser et diffuser : des enseignements et pistes d'action sont co-construits par les chercheurs, experts et participants.

Chaque année, environ 30 cycles de réunions mobilisent 100 chercheurs et 150 professionnels d'entreprises.

Petit-déjeuner débat, rencontre, groupe de travail, club… Différents formats sont utilisés en fonction de degré d'implication des participants requis par le sujet.

Enfin, l'Anvie organise également des formats sur mesure à la demande d'une entreprise.

Les entreprises adhérentes

GROUPE RENAULT · FDJ · BANQUE DE FRANCE EUROSYSTÈME · orange · MICHELIN · Rte
ECONOMIE d'ENERGIE · Caisse des Dépôts GROUPE · BNP PARIBAS PERSONAL FINANCE · GROUPE ADP · TOTAL · LE GROUPE LA POSTE · EDF
SOCIETE GENERALE · CA · SAINT-GOBAIN · GROUPE SEB · CA FÉDÉRATION NATIONALE DU CRÉDIT AGRICOLE · MAIF · SNCF
GROUPE nutriset · GRDF · VEOLIA · SAFRAN · pôle emploi · COVEA