La responsabilité des prestataires informatiques à l'épreuve des cyber-risques

par Corinne Thiérache, Avocat Associé
SELARL CARBONNIER LAMAZE RASLE & Associés
Pôle Nouvelles Technologies – Propriété Industrielle

Journée formation organisée le 18 octobre 2016 par la CNEJITA Experts sur le thème « Sécurité informatique : l'expert face aux actes de cybermalveillance»

CNEJITA EXPERTS

Carbonnier Lamaze Rasle & associés
SOCIETE D'AVOCATS - PARIS

MARCALLIANCE
FOR GLOBAL LAW & TAX PRACTICES

INTRODUCTION

1) ETAT DE LA SITUATION

Règles simples à garder à l'esprit :

- ***Pour lutter contre les cybermalveillances, la technique n'est rien sans le droit, le droit n'est rien sans la technique***
- ***« Pas de sécurité absolue mais une sécurité au juste niveau» (Guillaume Poupard, Directeur de l'ANSSI)***

Evolution lente des mentalités

- La cybercriminalité affecte de plus en plus les entreprises quelle que soit leur activité ou leur importance
- De plus en plus d'entreprises disent avoir été victimes de cyberattaques (intrusions dans leur système d'information, phishing, vol en ligne d'argent ou d'informations, altération de leur site Internet, ou infection de leurs machines par un virus ou un programme malveillant, réseau télécom piraté, ordinateurs cryptolockés, revenge spam)

L'importance de l'enjeu n'est pas toujours saisie par les entreprises

- Rôle clé joué par le responsable informatique, RSSI ou DSI pour sensibiliser leur hiérarchie mais sont-ils en réalité entendus? (prob budgétaire et délégations de pouvoirs) La cybersécurité n'est pas un coût, c'est un investissement
- Rappel article 34 de la loi du 6 janvier 1978 (état de l'art / coûts raisonnables + Notification de violations de données personnelles à la CNIL et aux personnes concernées élargie par le nouveau règlement européen
- Pourtant, les dommages que la cybercriminalité peut engendrer, ou qu'elle engendre déjà, peuvent être considérables et de différentes natures et ne concernent pas que l'entreprise mais tous les acteurs qui lui confient leurs données.
- Actualités récentes (Affaires SONY, Orange, Ebay, piratage des données du site de rencontres adultères Ashley Madison, Yahoo) et leurs conséquences (clients, prospects, salariés de l'entreprise)

2) LES ACTEURS EN PRÉSENCE

Diversité des prestataires informatiques confrontés aux cyber-risques

- Externes à l'entreprise : Fabricants (hardware et software) et des intermédiaires avec des prestations de services (nouvelles fonctions des intégrateurs) avec des compétences concurrentes
- Internes à l'entreprise : Rôle du RSI, RSSI et de la DSI

Synergie (convergence) ou conflits de compétences entre les prestataires informatiques et les prestataires en télécommunication

- Problématiques de gestion des flux, de l'interopérabilité (ex: accès à des plateformes)
- **Multiplicité des prestataires informatiques et télécoms = potentiel conflit entre les obligations de chacun** en fonction des business modèles choisis : entre internalisation, sous-traitance partielle ou externalisation complète (rôle du SSII ou ESN)

3) DIFFICULTÉS A SURMONTER

Identification du responsable de la sécurité et donc de la « faille » :
Concours de responsabilités, principe de responsabilité distributive en fonction des obligations de chacun (rôle des experts judiciaires et clauses contractuelles)

le droit toujours en retard face aux nouvelles technologies

- Lois Godefrain de 1988 (STAD)
- Vol d'information ou de la copie non autorisée d'un fichier informatique (Cass crim 20 mai 2015)
- Article L. 323-3 du Code pénal depuis la loi du 13 novembre 2014 sur la lutte contre le terroriste

➢ Attention au statut du lanceur d'alerte

(I) Etendue des obligations des prestataires informatiques externes à l'entreprise avec le cas particulier des prestataires du cloud

(II) Etendue des obligations de la Direction des systèmes d'information (DSI) ou de la Direction informatique interne à l'entreprise

III) Focus sur les principales règles de recevabilité de la preuve au civil et au pénal

IV) Obligations issues du nouveau règlement européen sur la protection des données personnelles

I-ÉTENDUE DES OBLIGATIONS DES PRESTATAIRES INFORMATIQUES EXTERNES

➢ 1.1 Obligations applicables à l'ensemble des prestataires informatiques

✓ **Obligation de délivrance conforme :** obligation de résultat (CA Versailles 20 janvier 2011)

✓ **Obligation d'information sous deux volets** :

❑ Obligation de renseignement et de mise en garde : information circonstanciée et personnalisée (Cass.civ. 2 juillet 2014) avec prise en compte des caractéristiques du système préexistant et informations sur la comptabilité entre les installations (CA Rennes 9 mai 2006)

❑ Obligation de conseil : portée variant en fonction des compétences propres du client mais ne disparaissant jamais même en présence de compétences techniques internes (installation de logiciels spécifiques Cass com 6 mai 2003)

➢ 1.1 Obligations applicables à l'ensemble des prestataires informatiques

✓ **Distinction classique entre obligation de moyens et de résultat reposant sur l'existence d'un aléa**

❑ Rôle actif du client dans la réalisation du projet = obligation de moyens (CA Lyon 21 déc. 2006)

❑ Conséquence sur la charge de la preuve reposant sur le client

➢ 1.1 Obligations applicables à l'ensemble des prestataires informatiques

✓ **Applications jurisprudentielles de l'obligations d'information en fonction de la prestation informatique fournie par le prestataire**

- Contrat de maintenance : obligation renforcée quand mainteneur tiers par rapport au matériel et système mis en place dont il n'est pas le fabricant (Cass com 5 fév. 2013) + mission d'assistance générale (mise à jour des logiciels, évolutions techniques, mot de passe (CA Versailles 25 mars 2014 + TC Nanterre 5 fév. 2015 : responsabilité engagée en cas de piratage de lignes téléphoniques ou Internet)

- Contrat de conseil en informatique: obligation de moyen parfois renforcée (CA Paris 23 janv. 1990)

- Fourniture d'un système informatique « clés en main » : devoir de conseil accru (Cass civ 31 mars 1992) (Etude d'Huissier)

1.2 Obligations particulières mises à la charge du prestataire de Cloud

- **Garantie de sécurité, confidentialité, intégrité et disponibilité des données**

- **Respect de la législation et réglementation applicable au traitement des données personnelles :** Loi du 6 janvier 1978 modifiée, Safe Harbor annulée par la CJUE et remplacée par le Privacy Shield, mise en place de BCR), préparation au nouveau règlement européen sur les données personnelles effectif en mai 2018

- **Information sur les différents lieux d'hébergement des données** (question de la protection équivalente, difficultés s'agissant de contrats d'adhésion et d'acteurs US)
- Engagement sur l'absence de **collecte et de stockage** de données de connexion autre que pour les **besoins de sécurité des systèmes**

- Souscription d'une **assurance professionnelle** couvrant les risques subis par le client
- **Attention : recours à la sous-traitance et responsabilité conjointe (G29)**

II- ETENDUE DES OBLIGATIONS DE LA DIRECTION DES SYSTÈMES D'INFORMATION INTERNE À L'ENTREPRISE

➢ 2.1 Missions de la DSI

❑ **Détection de la législation applicable avec mise en œuvre des dispositifs adéquats + sensibilisation du personnel et des prestataires extérieurs**

- Sécurité du système informatique,
- Gestion et utilisation des moyens informatiques (postes de travail, serveurs, équipements de réseau, BYOD, systèmes de stockage, de sauvegarde et d'impression, logiciels, services de télécommunication, Internet, etc.) ;
- Traitement des données personnelles ;
- Relations avec les prestataires (détermination des besoins, des référentiels et cahiers des charges, clauses de garantie et de responsabilité)

➢ 2.2 Types de responsabilités encourues

- ❑ **Responsabilité civile contractuelle ou délictuelle**
- ❑ **Responsabilité pénale**

✓ Points de vigilance particuliers (ex: délit de marchandage et délit de prêt illicite de main d'œuvre)

✓ Possibilité de cumul avec la responsabilité de la personne morale pour laquelle la DSI a agi

Ex: délit de fraude informatique (article L. 323-2 du Code pénal) comme fondement d'une condamnation au pénal d'un informaticien qui a, pour se venger d'une procédure de licenciement dont il faisait l'objet, modifié le mot de passe dont il assurait jusqu'alors la maintenance (Paris 8 juin 2012),

- ❑ **Mesures disciplinaires :** cas de violation de son contrat de travail, du règlement intérieur, de la charte informatique etc. pouvant aller jusqu'au licenciement

➢2.2 Types de responsabilités encourues

- ❑ Importance des délégations de pouvoirs : points d'attention dans leur rédaction

- ❑ Types d'agissements susceptibles d'engager sa responsabilité :

- ✓ utilisation d'un logiciel sans licence d'utilisation,
- ✓ absence de mesures de sécurité raisonnables pour la protection du système informatique,
- ✓ détournement des données personnelles des salariés, fourniture aux salariés des moyens ayant permis la réalisation d'une infraction,
- ✓ négligence ou une imprudence dans le fonctionnement du système informatique,
- ✓ négligence de la direction des systèmes informatiques s'agissant de la sécurisation de l'utilisation des BYOD,
- ✓ défaut de sécurisation des données personnelles

III - FOCUS SUR LES PRINCIPALES RÈGLES DE RECEVABILITÉ DE LA PREUVE AU CIVIL ET AU PÉNAL

- **Problématique : dans quelle mesure les preuves facilitant l'identification de l'auteur de la cyber-attaque ou de l'origine de la faille dans le système d'information sont-elles recevables en justice ? La fin justifie-t-elle les moyens ?**

➢3.1 Grands principes de la recevabilité de la preuve au civil

- En présence d'un fait juridique : en principe, la preuve est libre (sauf exceptions légales)

- En présence d'un acte juridique, la preuve est régie par l'article 1359 nouveau du Code civil qui prévoit qu'il faut une preuve littérale chaque fois que l'acte juridique dépasse une certaine valeur (actuellement, 1.500 €).

➢3.1 Grands principes de la recevabilité de la preuve au civil

- **Précisions : L'article 1366 nouveau du Code civil** prévoit que « *l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

- **L'article 1379 nouveau du Code civil** prévoit que « *la copie fiable a la même force probante que l'original. La fiabilité est laissée à l'appréciation du juge. Néanmoins est réputée fiable la copie exécutoire ou authentique d'un écrit authentique***.**

« *Est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'État. Si l'original subsiste, sa présentation peut toujours être exigée.* **»**

3.1 Grands principes de la recevabilité de la preuve au civil

- **Exceptions :** Dans un certain nombre de cas, la preuve d'un acte juridique est libre même si sa valeur est supérieure à 1500€ à savoir liberté de preuve en matière commerciale

- ✓ commencement de preuve par écrit,
- ✓ impossibilité de produire un écrit, s'il est d'usage de ne pas établir d'écrit ou lorsque l'écrit a été perdu par force majeure (C. civ., art 1360 nouveau).

- **Exemples d'autres moyens de preuve recevables :**

- ✓ l'attestation ou le témoignage qui doit obéir aux conditions de forme de l'article 202 du code de procédure civile à condition qu'il soit bien précisé que l'auteur est conscient qu'il établit l'attestation en vue de sa production en justice.
- ✓ Le procès-verbal de constat dressé par un huissier de justice
- ✓ Le journal du DSI : prob se constituer une preuve à soi-même
- ✓ Le rapport d'un expert judiciaire

➢ 3.1 Grands principes de la recevabilité de la preuve au civil

❑ **Précision en matière du droit du travail :** Pas de dispositions propres -> règles de preuves régies par le Code civil et le Code de procédure civile.

La preuve des faits par l'employeur et la protection de la vie privée des salariés :

✓ **Principe : Arrêt NIKON, Cass.soc., 2 oct. 2001 n° 99-42942 :** « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

✓ **Précision sur les fichiers « personnels** » : tous les fichiers et dossiers stockés sur le lieu de travail, que ce soit sur support papier ou dans un ordinateur, sont présumés être de nature professionnelle. Ils peuvent donc être librement consultés par l'employeur. Toutefois, le salarié a la possibilité d'identifier ses fichiers et dossiers privés par la mention « *personnel* ». Ces documents ne pourront alors être consultés par l'employeur qu'en présence du salarié (Cass. Soc., 18 octobre 2006, n° 04-47400 et 04-48025) sauf en cas de force majeure.

3.2 Grands principes de la recevabilité de la preuve au pénal

- **Principe : la preuve est libre mais encadrée :** principe du contradictoire et appréciation de la valeur probante par le juge**.**

- **Article 427 du Code de procédure pénale :** « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui.* »

- **Tous les moyens de preuve sont recevables devant le juge pénal** tels que les indices, les aveux, un écrit (obligatoire en matière de contrat), un témoignage, etc.

A RETENIR : Le principe fondamental de légalité et de loyauté de la preuve : fait partie des principes essentiels du procès équitable.

IV- OBLIGATIONS DU NOUVEAU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

➢ 4.1 Adoption du nouveau règlement européen

- ❑ le 27 avril 2016 : adoption d'un règlement général sur la protection des données + directive relative à la protection des données à caractère personnel à des fins répressives. Le règlement sera applicable à partir du 25 mai 2018.

- ❑ Le règlement européen renforce les obligations des entreprises en matière de traitement des données pour une meilleure protection de celles-ci (cible privilégiée des pirates informatiques en sus du savoir-faire, des secrets des affaires, secret de fabrique ou actifs immatériels).

  → Conséquence : Révision de la politique de conformité informatique et libertés par les responsables des systèmes d'informations et des prestataires

➢ 4.2 Eclairage sur certaines nouvelles obligations

- **Principe du « *Privacy by design* » (Règlement, art. 25, paragraphe 1) :** l'obligation de respecter la protection des données dès la conception des produits services et systèmes exploitant des données à caractère personnel.

  → Cela implique que la protection des données soit intégrée par la Direction des systèmes informatiques dès la conception d'un projet informatique (gestion en mode agile)

- **Principe de la sécurité par défaut ou « *Security by default* » (Règlement, art. 25, paragraphe 2):** l'obligation de disposer d'un système informatique ayant les fonctionnalités minimales requises en matière de sécurité à toutes les étapes (enregistrement, exploitation, administration, intégrité et mise à jour) et dans tous ses éléments, physiques ou logiques (contrôle d'accès, prévention contre les failles de sécurité, anonymisation, etc.).

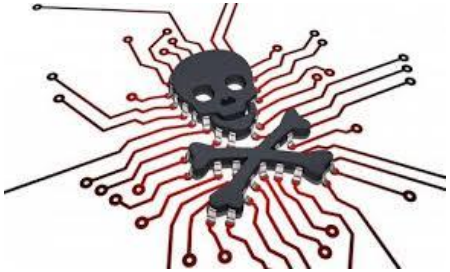
  → Cela implique que la sécurité des données soit intégrée par la Direction des systèmes informatiques dès la conception d'un projet informatique (gestion en mode agile)

- **Règles d'accountability (obligation de documentation) (Règlement, art. 24) :** l'obligation mise à la charge du responsable de traitement de documenter l'ensemble des actions de sa politique de protection des données pour démontrer aux autorités de contrôle ou aux personnes concernées leur conformité avec le règlement européen.

  → Cela implique : tenue de la documentation, mise en œuvre des obligations en matière de sécurité, réalisation d'une analyse d'impact, audits réguliers

➢ 4.2 Eclairage sur certaines nouvelles obligations

- **Notification des failles de sécurité est élargie et obligatoire dans un délai de 24 h à la CNIL (Règlement, art. 33 et 34)** « *en cas de défaillance dans les obligations de sécurité et de protection* » + *si cette défaillance est susceptible d'affecter les personnes concernées, information des personnes concernées dans un délai de 24h* **(Règlement, art. 29).**



- **L'étude d'impact (Règlement, art. 35) :** l'obligation mise à la charge du responsable de traitement ou du sous-traitant d'effectuer une analyse d'impact relative à la protection des données personnelles préalablement à la mise en œuvre des traitements présentant des risques particuliers d'atteinte aux droits des libertés individuelles.

→ Parmi ces traitements à risque figurent : les traitements de données sensibles, la surveillance des espaces publics et des traitements utilisés pour faire du profilage automatique

➢ 4.2 Eclairage sur certaines nouvelles obligations

- **La désignation obligatoire d'un *Data Protection Officer* (DPO – Délégué à la protection des données : Quid du CIL en France ?) (Règlement, art. 37) :** concerne les entreprises traitant des données à caractère personnel de manière régulière et à une échelle importante, et celles dont les activités consistent en un traitement à grande échelle des données dites «sensibles» ou relatives à des condamnations (-> les entreprises doivent déterminer si elles entrent dans le champ d'application de cette obligation).

Le DPO ne sera pas nécessairement un employé du responsable de traitement des données mais il devra impérativement être désigné sur la base de ses connaissances du droit et des pratiques en matière de protection des données personnelles.

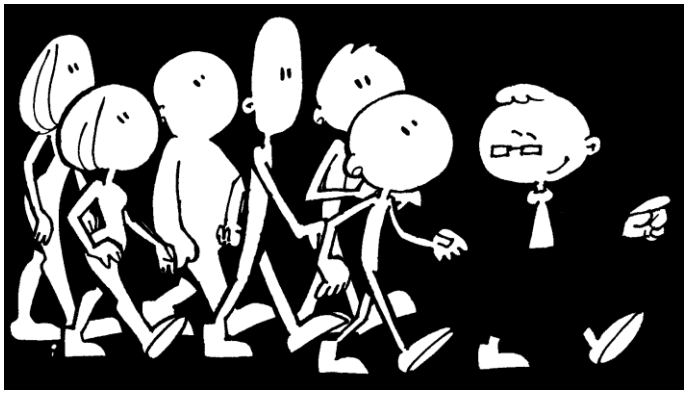
- + Distinction CIL et responsable de traitement : Le CIL est irresponsable au niveau pénal. Seul le responsable de traitement est responsable (Règlement, art. 4).

➢ 4.2 Eclairage sur certaines nouvelles obligations

- **Consécration de la responsabilité conjointe : (Règlement, art. 26) :** en cas de pluralité de responsables de traitement déterminant conjointement les finalités et les moyens du traitement.

Les sous-traitants peuvent également assumer une responsabilité directe au même titre que les responsables de traitement (-> formaliser les obligations des sous-traitants et les rôles respectifs de chacun dans des conventions pour leur appliquer une responsabilité propre)

Les prestataires Cloud et les développeurs de logiciels sont également concernés puisqu'ils seront tenus de respecter les dispositions du règlement.



➢ 4.2 Eclairage sur certaines nouvelles obligations

❑ **Des sanctions déjà augmentées par anticipation par la loi Lemaire relative à la République du numérique du 7 octobre 2016.**

Le plafond maximal des sanctions de la CNIL **passe de 150.000 € à 3 millions €** (anticipation sur l'augmentation du plafond du montant des sanctions prévu par le règlement européen qui sera applicable le 25 mai 2018 et prévoit un plafond jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial).

Aucune modification quant aux sanctions pénales (articles 226-16 à 226-24 du Code pénal : jusqu'à 5 ans de prison et 300.000 € d'amende)

CONCLUSION

Comment agir pour prévenir ?

Devant ces nombreux difficultés et obstacles, la stratégie doit s'opérer en trois volets qui allient à la fois la technique (notamment par le recours à des experts en informatique) et le juridique:

- A l'égard d'un tiers malveillant : sensibilisation de tous les collaborateurs et charte de bonne conduite
- A l'égard d'un sous-traitant ou d'un prestataire extérieur : vérifier les accords contractuels passés pour évaluer la prise en compte réelle de ces risques par les sous-traitants ou prestataires extérieurs + insertion de clauses spécifiques : garanties et responsabilités, sécurisation des accès contre intrusion de tiers, clauses de sécurité.
- A l'égard d'un salarié malveillant : surveillance du réseau internet dans le respect du droit du travail et du règlement intérieur

Recommandations : Faire réaliser les audits ou revues techniques et juridiques indispensables (revues de gouvernance et de sécurité) - Nécessité de se faire accompagner et, au vu de l'évolution des nouvelles technologies, de réaliser ces audits ou revues de compliance de manière récurrente (pas un one shot au moment d'une acquisition ou d'une cession).

Contact :

Corinne THIERACHE
cthierache@carlara.com

Avocat Associé
SELARL CARBONNIER-LAMAZE-RASLE & ASSOCIES
Responsable du Pôle « *Nouvelles Technologies - Propriété Industrielle* »

Carbonnier Lamaze Rasle & associés
SOCIETE D'AVOCATS - PARIS

CARBONNIER LAMAZE RASLE & Associés
8, rue Bayard – 75008 PARIS
01 53 93 61 41