Semaine 2. Le mail, un objet à risque

Sommaire

Intervenants (dans l'ordre alphabétique)

Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés

Franck ASTOLFI, Responsable du projet d'archivage ReMIND chez Bouygues Construction

Philippe BAZIN, Avocat associé, Avocat au Barreau de Rouen

Christophe BINOT, Responsable de la Gouvernance de l'Information du Groupe Total

Anne BURNEL, Directrice des Archives du Groupe La Poste

Richard CAZENEUVE, Président du CR2PA

Marie-Anne CHABIN, Expert, membre fondateur du CR2PA

Vincent CLAUDON, Secrétaire Général de l'Agence de services et de paiement

Bruno DANVIN, Vice-président du CR2PA

François DELION, Coordinateur de projet conservation des données Bouygues Telecom

François-Xavier FERRARIO, Retraité, ancien Inspecteur général d'Oséo-BPIFRANCE

Roger GRASS, Conseiller à la Cour de cassation, Ancien secrétaire général et greffier de la Cour de justice de l'Union européenne

Ludovic GUERRA, Étudiant Enseeiht

Dr. Fernando LAGRAÑA, Directeur, Programme DBA, Webster Genève

Marie LAPERDRIX, Chef du service des archives du ministère de l'Economie et des Finances

Eric LAURENT-RICARD, Président Experact – Expert près la Cour Pénale Internationale

Hélène LEGRAS, CIL/DPO Groupe AREVA et Vice-Présidente de l'ADPO

Dijana LEKIC, Étudiante Paris 8

Corentin MACIAS, Étudiant Enseeiht

Nathalie MORAND-KHALIFA, Directeur du département Information Management de la Recherche et Innovation de L'Oréal

Cyrille TESSER, Expert à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Textes des vidéos

S2A — Les e-mails de Hillary Clinton

Marie-Anne CHABIN, Expert, membre fondateur du CR2PA

Avec l'affaire des e-mails de **Hillary Clinton**, l'histoire internationale de ces dernières années nous offre **une illustration très complète de la manière dont une personnalité publique expérimentée peut se trouver piégée par la messagerie électronique.**

En mars 2015, la future candidate à l'élection présidentielle américaine est accusée d'avoir dissimulé des e-mails liés à son activité de Secrétaire d'État entre 2009 e 2013. Le point central de l'affaire est que, pour correspondre avec ses interlocuteurs dans l'exercice de ses **fonctions gouvernementales**, elle a utilisé une **boîte de messagerie personnelle** y compris pour transmettre des informations confidentielles, notamment au sujet de l'attaque du consulat américain de Benghazi (Lybie) en septembre 2012.

De façon tout à fait déconnectée du jugement sur le fond du dossier et de la question politique de l'élection – qui n'est pas notre propos – il est intéressant de retrouver dans cette affaire les concepts et les ingrédients principaux de la problématique du mail. Toutes les questions fondamentales sur le fonctionnement du mail, ses subtilités et ses risques sont présents dans ce dossier, ainsi qu'on peut le voir au travers de **quelques citations de la presse française**.

> **1) Depuis 2009, les membres de l'administration ont l'obligation de conserver tous leurs e-mails pour une éventuelle utilisation par des parlementaires ou des historiens.**
> *Les Échos*, 5 mars 2015

Hillary Clinton est devenue Secrétaire d'État l'année de cette nouvelle réglementation et ne l'a pas appliquée ; ses prédécesseurs fonctionnaient avec une **adresse mail privée** et elle n'a pas la seule à avoir poursuivi cette pratique, ce qui montre bien qu'il faut un certain temps pour qu'une réglementation se mette en place, d'autant plus l'usage d'une boîte gouvernementale n'était pas strictement obligatoire avant 2013, même s'il était fortement conseillé.

> **2) À moins d'être classés confidentiels ou secret-défense, ces échanges peuvent être consultés par toute personne qui en fait la demande au nom de la loi sur la liberté d'information (*Freedom of Information Act*)**.
> *Le Monde*, 12 août 2015

On voit ici le principe de **transparence** des archives du gouvernement avec une restriction pour certains documents qui seraient confidentiels ; il est intéressant de noter le concept qu'il y a derrière ce *Freedom of Information Act*, parce qu'on a souvent eu en France le principe du secret avec des dérogations pour l'accès à l'information.

> **3) « Les responsables gouvernementaux n'ont pas le droit d'emporter avec eux des courriels ou des documents sans qu'ils aient été préalablement examinés par le gouvernement, qu'ils soient personnels ou professionnels », a affirmé Tom Fitton, président de *Judicial Watch*.**
> *Les Échos*, 13 septembre 2015

La remarque est parfaitement juste mais dans le cas présent, Hillary Clinton n'a pas emporté des documents du gouvernement, elle les a **créés à l'extérieur**. Elle ne les a pas rapportés au gouvernement. Il y a là une nuance intéressante qui est la conséquence de la facilité des échanges électroniques.

> **4) En quatre ans, la secrétaire d'État a envoyé et reçu 62 320 courriels par le biais de son adresse personnelle. Depuis que cette pratique a été révélée en mars, la candidate démocrate a dû restituer pour archivage, à la demande du département d'État, les 30 490 courriels qu'elle considère comme professionnels. Concernant les 31 830 courriers restants, Mme Clinton a estimé qu'ils relevaient de sa vie personnelle et les a effacés.**
> *Le Monde*, 8 septembre 2015

Ce qui est intéressant ici d'abord, ce sont les **statistiques** parce qu'on a assez peu d'éléments chiffrés sur les pratiques des uns et des autres. Deuxièmement, c'est la question de savoir **qui décide** du statut personnel ou professionnel d'un mail ? et cette question est d'autant plus difficile que pour l'instant on peut constater que Hillary Clinton est **juge et partie**, ce qui pose un problème : elle-même a décidé que tel mail était professionnel ou était personnel ou, mais elle ne peut rien prouver ni sur l'exhaustivité des mails produits au départ et elle ne peut pas non donner la possibilité de revoir ce statut puisqu'elle les a supprimés. On voit bien qu'il y a, là, une **urgence à avoir des règles**, et à les appliquer à la création du mail.

> **5) À la demande du département d'État, Hillary Clinton a livré 55.000 pages [de messages] il y a deux mois. Mais la liste n'est pas exhaustive, et nul ne sait si des messages compromettants n'ont pas été supprimés**
> *Les Échos*, 5 mars 2015

Des chiffres encore. Mais ces 55000 **pages** ne veulent pas dire grand-chose. Elles correspondent en réalité aux 30000 messages qui sont une unité de compte assez précise, tandis que les pages ne veulent pas dire grand-chose car il s'agit de l'impression de ces 30000 messages et on voit

bien que le **vocabulaire** pour parler des mails n'est pas encore tout à fait adapté.

> **6) En tant que responsable de la diplomatie américaine, Hillary Clinton envoyait et recevait une très grande quantité d'informations confidentielles et sensibles.**
> *Le Monde*, 12 août 2015

Confidentiel et sensible : les deux mots sont employés un peu comme Dupont et Dupond ; il faudrait préciser qu'est-ce qui est **confidentiel** et qu'est-ce qui est **sensible** et progresser dans la catégorisation des messages, ce qui n'est pas fait.

> **7) Les documents examinés, s'ils contenaient bien des informations classifiées, n'étaient pas identifiés comme tels.**
> *Le Monde*, 12 août 2015

Nous voici avec cette question sur le point fondamentale de la **qualification** des messages. Il est important que les messages soit qualifiés pour pouvoir statuer, après, sur leur devenir. La qualification peut être faite, devrait être faite par l'auteur en fonction des **procédures** qu'il doit appliquer et en fonction de sa propre appréciation des contenus. La qualification peut être réalisée également par une **tierce personne** qui est soit dans l'équipe administrative du responsable en question, soit par quelqu'un chargé de l'archivage de ces messages après coup. Mais il faut avoir cette qualification, sinon on ne peut rien conclure.

> **8) Hillary Clinton assure que [ces informations] n'étaient pas officiellement confidentielles à l'époque.**
> *Courrier international*, 2 septembre 2015

La remarque est particulièrement pertinente parce que – je ne juge pas les propos de Hillary Clinton en tant que tels – la confidentialité en tant que telle est **une notion évolutive**. Quelque chose qui n'était pas confidentiel peut le devenir, dans un contexte différent, par exemple politique, au bout d'un an ou deux, parfois moins. Et quelque chose qui était confidentiel à un certain moment peut ne plus l'être du tout. Donc cette notion de confidentialité attachée au mail doit être statuée dès la création du mail puis doit accompagner le mail, comme « **métadonnée** de confidentialité », pendant tout son cycle de vie.

> **9) Son compte e-mail aurait donc dû faire l'objet de mesures de protection particulièrement importantes. Mais le compte personnel qu'elle utilisait, et qui fonctionnait avec plusieurs serveurs – dont l'un situé à son domicile –, ne bénéficiait pas de ces mesures, et était donc aisément vulnérable à un piratage. Plus grave, certaines mesures élémentaires de protection n'étaient semble-t-il pas respectées – l'un des domaines liés au compte utilisait un certificat de sécurité invalide […] Aucune preuve d'un piratage d'ampleur n'a cependant été apportée pour l'instant.**
> *Le Monde*, 12 août 2015

La question de la **sécurité informatique** est au cœur de la gestion des mails, en général, très souvent et dans cette affaire en particulier. Ceci dit, il faut distinguer le **risque théorique** et le **risque avéré**. Et on sait – l'actualité nous le montre régulièrement - que les serveurs les plus sécurisés ne sont pas exempts d'attaques des cybercriminels.

> **10) Quinze courriels envoyés par la responsable de la diplomatie américaine à Sidney Blumenthal, vieil ami et conseiller de Mme Clinton, ne figuraient pas dans le fichier [transmis par Mme Clinton]– M. Blumenthal avait transmis des copies de tous ses échanges avec Mme Clinton à la commission d'enquête, à sa demande.**
> *Le Monde*, 8 septembre 2015

Ce point, qui est **plus rarement commenté** dans la presse, est pourtant essentiel, en tout cas dans le cadre de notre MOOC. Il vient rappeler, à juste titre, **qu'un mail est un échange, qu'il y a au minimum, deux exemplaires**, deux personnes, chacune ayant le sien. Donc vous-même avez détruit le message que vous avez envoyé, sachez que celui à qui vous l'avez envoyé peut l'avoir gardé. Il fallait vraiment rappeler cela.

S2B — Risques tous @zimuts

Christophe BINOT, Responsable de la Gouvernance de l'Information du Groupe Total

Le mail est un point d'entrée important de virus et d'attaque. On a des systèmes antivirus qui filtrent les e-mails (toutes les entreprises ont ça). Il y a bien sûr des campagnes de ***phishing***, faites par des hackeurs et des cybercriminels et on essaie de sensibiliser les utilisateurs à cette notion de *phishing*, en particulier en faisant nous-mêmes des campagnes de *phishing* pour voir quels sont les **utilisateurs qui cliquent** sur les mails et qu'est-ce qui les attirent et les fait cliquer sur différents liens, et en les éduquant en expliquant : si vous avez cliqué sur tel lien, ça a téléchargé tel malware sur votre boîte mail qui s'est ensuite répercuté dans différents fichiers. Donc, c'est aussi des **campagnes de sensibilisation** en termes de cybersécurité parce que le mail, comme les clés USB, est un des deux principaux points d'entrée de toutes les attaques informatiques actuellement.

Fernando LAGRAÑA, Directeur, Programme DBA, Webster Genève	Le mail peut être dangereux non seulement par rapport à son contenu mais aussi par rapport à la liste des personnes qui le reçoivent. On voit ainsi **des attitudes contraires à l'éthique** où lorsqu'on envoie un courrier à un collègue, celui-ci fera mine de ne pas l'avoir reçu. C'est le cas par exemple lorsqu'on lui rappelle qu'il y a un délai à tenir et que la personne a des difficultés, mais plutôt que de le signaler, de révéler éventuellement une faiblesse ou un problème, la personne préférera ignorer que le mail est arrivé. Parfois même, on voit des situations dans lesquelles le **déni** est tel que lorsque celui qui aura envoyé le premier message réclamera, celui qui a reçu le mail prétendra ne pas l'avoir reçu, en utilisant diverses excuses, telles que celle-ci, la plus fréquente : « Pardon, j'ai trouvé ça dans mon courrier-poubelle, je ne comprends pas comment ça s'est passé », mais en réalité, c'est une façon de ne pas recevoir. **Pire encore sont les situations dans lesquelles on met à l'écart un collaborateur dans une entreprise** ; c'est ce qu'on appelle le silence, dans lequel on sortira sciemment quelqu'un d'une liste de distribution, on refusera de répondre à ses courriers, bref, on le mettra à l'écart ; si on compare cette situation à celle de la relation entre individus, c'est la **première étape du harcèlement**. Lorsqu'on isole l'individu, qu'on ne répond pas à ses attentes, à ses questions. Malheureusement, le courrier électronique, puisqu'il est une façon intermédiée par l'ordinateur de dialoguer est un outil puissant, et les gens se sentent protégés derrière l'ordinateur et ils ont tendance à adopter des comportements moins éthiques que dans la vie quotidienne.
Roger GRASS, Conseiller à la Cour de cassation, Ancien secrétaire général et greffier de la Cour de justice de l'Union européenne	Il est certain qu'un mail peut présenter un **risque médiatique**. Pour les institutions que je connais, ce risque médiatique est toutefois limité mais je peux imaginer des institutions plus exposées. Pour l'entreprise , **un mail peut être interprété dans les médias de manière assez dramatique pour elle**, il suffit à cet égard de songer à un mail maladroit sur des opérations de licenciements ou des déplacements d'unités de production. Il peut y avoir une certaine facilité à écrire un mail faisant une proposition conditionnelle de telle manière que, sorti de son **contexte**, il puisse être **interprété** ou lu comme une proposition définitive, et donc comme un engagement de volonté qu'il suffit d'accepter pour le contrat soit parfait.
Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex	Je reçois beaucoup de mails, ou de courriels, qui sont manifestement adressés par des machines et non pas par des interlocuteurs personnes physiques, autrement dit par des **robots**. Quelle est la valeur juridique de ces robots ? Pardon, Quelle est la valeur juridique de ces messages ? Réponse très simple : un robot n'a pas de personnalité juridique. Celui qui a une personnalité juridique, c'est la **société qui gère les robots**, la société qui réunit les moyens pour que ces messages soient envoyés. Par conséquent, le message reçu émanant d'un robot engage la société qui gère le robot, c'est-à-dire le représentant légal de cette société.
Richard CAZENEUVE, Président du CR2PA	On constate en entreprise que le risque documentaire n'était pas parmi les risques majeurs du temps de l'ère papier ; aujourd'hui, les choses ont

changé, puisque **le mail constitue un des risques majeurs et transverses de l'entreprise, car tous les collaborateurs sont parties prenantes**. Donc, le top management se doit de s'approprier ce risque documentaire, d'en assurer, par des prescriptions, des politiques, un certain nombre d'exigences auprès de collaborateurs et se doit également d'ailleurs, au-delà de la sensibilité , de les former à une **meilleure maîtrise**, une **meilleure écriture**, une meilleure conservation, ou destruction d'ailleurs, de leur production.

Dijana LEKIC, Étudiante Paris 8

Les avantages de la messagerie électronique, il y en a plusieurs. Je l'ai vu pendant mon alternance aussi dans le cadre professionnel, c'est rapide : envoyer une information et communiquer avec quelqu'un très rapidement ; ça laisse aussi la possibilité à la personne de garder cette information, comme une preuve, une forme d'engagement ; c'est pratique, facile d'utiliser une messagerie électronique. Les inconvénients existent aussi : j'ai eu certains cas : ma messagerie principale a été **hackée**, des personnes sont entrées dans ma messagerie ; de ce point de vue, il y a des risques par rapport aux informations qu'on envoie ; ma pratique est par exemple, quand j'envoie des pièces jointes du type **carte d'identité**, d'enlever, supprimer plutôt que laisser dans ma messagerie électronique. Voilà. Donc il y a des risques derrière, peut-être plus au niveau personnel, individuel, qu'au niveau professionnel.

S2C — Le message de l'ANSSI sur les risques du mail

Richard CAZENEUVE, CR2PA

Le numérique est agile mais fragile.

Cyrille TESSER, Expert à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Il existe beaucoup de risques liés aux mails et ils sont très variés. Je vais vous donner quatre exemples. Avant de les énumérer, il faut bien comprendre que ces risques sont issus majoritairement de « **clics de souris** par l'utilisateur » sur des liens ou des PJ malveillantes présents dans les courriers électroniques reçus ; mais cela peut aussi se produire automatiquement sans que l'utilisateur ne fasse quoi ce soit, s'il dispose d'équipements et/ou logiciels mal configurés, voire pire s'il utilise des logiciels avec des failles de sécurité. **On est donc sur des critères d'éducation, de sensibilisation et d'information des gens pour avoir une posture « normale » vis-à-vis des emails**.

1) Premier exemple de risque avec ce que l'on appelle le ***phishing***, ou **hameçonnage** en français, qui consiste à vous appâter et vous faire envie de réagir au message que vous venez de recevoir. Tous les stratagèmes sont utilisés pour vous faire répondre ou vous faire cliquer sur des PJ ou sur des liens (argument sentimental, argent, etc.) mais dont le but se résume bien souvent à du vol de données personnelles ou plus directement à des fins de détournement financier. La cible est votre porte-monnaie. Pour mémoire, je rappelle que les banques, les impôts, les

fournisseurs d'électricité ne demanderont jamais de ressaisir vos coordonnées bancaires ni vos identifiants pour un remboursement...

2) le deuxième exemple est un cas particulier de phishing qui concerne les messages de type « **arnaque de l'ami à l'étranger** ». Les escrocs usurpent les identités mail de vos proches dans le but de vous demander de l'argent. Ils vous font croire qu'ils ont un problème à l'étranger et qu'ils ont rapidement besoin d'un virement bancaire ou de fond. Un coup de fil à cette personne vous permettra de dédouaner très vite la situation.

3) Troisième exemple de risque pouvant passer par le mail, les « **prises de contrôle à distance** » de l'ordinateur : pour voler les informations dans votre ordinateur, pour détourner de la puissance de calcul, pour rebondir sur votre machine et se cacher derrière votre adresse IP avant de commettre une attaque en déni de service, pour diffuser du SPAM ou des malwares, pour stocker des images pédopornographiques, pour poster des messages diffamatoires, d'incitation à la haine raciale ou de terrorisme, etc.

4) Le quatrième et dernier exemple concerne les **rançongiciels** (***ransomware*** en anglais). Phénomène de plus en plus inquiétant car cette fois-ci, les clics de souris vont déboucher sur un chiffrement de toutes les données de vos ordinateurs, tablettes, ordiphones/smartphones, puis un message va apparaitre vous demandant une rançon financière, si vous souhaitez récupérer toutes vos données. Les rançons sont demandées sous forme de monnaie virtuelle : bitcoin, etc. avec des mécanismes de chiffrement dont l'intérêt principal pour l'attaquant est l'anonymat pour ne pas être tracé. Mais attention, payer la rançon ne garantit pas la récupération de l'intégralité de vos données.

Pour éviter d'en arriver là, je vous recommande de prendre quotidiennement connaissance des **bulletins d'alerte du CERT-FR** comme celui dédié aux rançongiciels/ransomwares sur son site web.

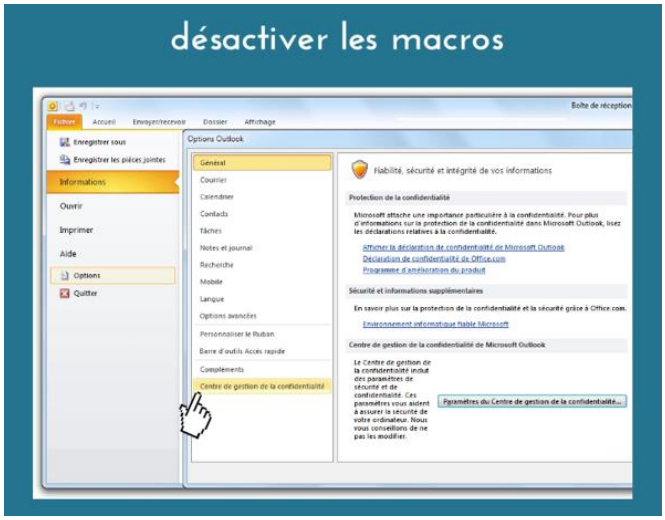
Il y a au moins quatre recommandations ou règles :

1) La première concerne les **bons comportements** à adopter lorsque l'on reçoit des messages piégés. N'ouvrez pas les messages dont la provenance ou la forme est douteuse. Ne vous fiez pas aux apparences. Apprenez à distinguer des emails piégés en deux minutes sur le **site web de la « Hack-academy**. Toujours réfléchir avant de cliquer. Voici quelques critères d'attention : orthographe, langue utilisée, présentation, adresse email de l'émetteur, adresse email de réponse … demander confirmation à l'émetteur du mail par un autre moyen, vérifier les adresses réelles des liens affichés dans le message, etc.

2) Deuxième règle, effectuez et tester vos **sauvegardes** régulièrement. Ne laissez pas votre périphérique de sauvegarde branché en continu sur votre installation. Sortez physiquement la sauvegarde de votre réseau et placez là en lieu sûr. Assurez-vous aussi qu'elle fonctionne. *Idem* pour les sauvegardes dans le Cloud, déconnectez-vous une fois l'opération terminée. Pour les moyennes et grandes entreprises, on recommande la mise en place de politiques de sauvegarde.

3) Troisième règle, les rançongiciels utilisent les vulnérabilités des applications pour se propager. Il faut donc impérativement **mettre à jour** ses principaux logiciels et outils comme : Windows, iOS, Android, anti-virus, lecteur PDF, navigateur WEB, JAVA, Silverlight ... et si possible, désactiver les macros exécutables des solutions « Office ». Je prends l'exemple d'un outil de messagerie très répandu.

Pour **désactiver ses macros**, je vais dans : fichier – options – centre de gestion de la confidentialité – Paramètre du centre de gestion de la confidentialité – paramètre des macros – et je choisi : Notifications pour les macros signées numériquement, toutes les macros sont désactivées.



4) Quatrième règle, ne travaillez pas en tant qu'**administrateur** de votre poste. Une fois que celui-ci a été configuré, créer un compte utilisateur et n'utiliser que celui-ci. Pour les grandes structures les équipes informatiques ont déjà tout préparé, mais pour les particuliers ou les petites entreprises, cette règle est trop rarement appliquée. Dans l'immédiat, elle empêchera l'escroc d'avoir tous les privilèges sur votre machine s'il arrive à la compromettre.

En synthèse, je pense qu'il est possible de se protéger de tous ces cas de figures par des règles simples et qui ne coûtent que du « bon sens ». Vous retrouverez toutes ces informations de façon détaillée, et bien d'autres, sur le site web de l'ANSSI.

De façon générique, je vous recommande deux documents :

ANSSI : www.ssi.gouv.fr et CERT-Fr : www.cert.ssi.gouv.fr

Bulletin d'alerte du CERT-FR dédié rançongiciel / ransomware : http ://www.cert.ssi.gouv.fr/site/CERTFR-2016-ACT-016/index.html

Apprendre à détecter un mail piégé en 2 minutes https ://www.hack-academy.fr/candidats/willy

S2D

L'utilisateur du mail prend des risques

Fernando LAGRAÑA, Directeur, Programme DBA, Webster Genève

Une des questions qui se posent vis-à-vis du mail, c'est le risque dans son utilisation, et **il y a des risques au niveau de l'individu et au niveau de l'entreprise** ; ils sont variés. Au niveau de l'individu, il y a des risques liés à la confidentialité : bien souvent, quand on écrit un mail à un collègue, un pair, un client, il nous arrive de considérer que ce mail est individuel mais il y a le risque que ce mail soit réutilisé, **retransmis** à l'ensemble de l'entreprise ou à d'autres personnes et de ce fait on se trouve engagé par le mail que l'on a envoyé et, en pensant le faire d'une manière individuelle, on se retrouve en train d'engager par exemple une entreprise. L'autre type d'élément de risque lié au mail est le fait que beaucoup d'individus utilisent le mail comme ils utiliseraient **le chat** ; ils ont le sentiment d'être dans une conversation animée à bâtons rompus.

Or, le mail n'est pas une chose orale, n'est pas verbal ; c'est un élément écrit même s'il est écrit de manière électronique et, dans ce sens là, les paroles s'en vont et **les écrits restent**, et bien souvent les gens, à nouveau, sont engagés alors qu'ils pensaient être dans une conversation anonyme. Un autre élément est celui de l'entreprise, et c'est peut-être plus général au niveau de l'utilisation de tous les outils électroniques. Les entreprises fournissent des **équipements électroniques** à leurs collaborateurs et ceux-ci quittent l'entreprise, **voyagent**, ne protègent pas nécessairement leur système électronique, par négligence, par manque de connaissances et parfois les entreprises s'exposent, par le biais de courriers électroniques notamment ; on a vu beaucoup de cas de **SCAM**, de méthodes qui permettent de capturer, d'obtenir de manière illicite de l'information par le biais d'un système de courrier électronique ; on connaît les systèmes des virus, des bots, etc. qui exposent les entreprises. Il y a aussi des

	dangers au niveau de la relation entre individu et son entreprise : en effet, **beaucoup d'utilisateurs du mail considèrent que le mail est une chose privée. Or, dans la plupart des pays du monde, ce n'est pas le cas**, alors que dans l'ère du téléphone, il y avait ce qu'on appelait la confidentialité de la communication téléphonique. Ici, le mail, les plateformes appartenant aux entreprises, le courrier électronique est la propriété de l'entreprise, et dans le cadre des conflits qui peuvent exister entre un individu et son employeur, l'employeur aura accès à l'ensemble des courriers qui auront pu être émis par un individu. Donc les risques sont effectivement multiples.
Nathalie MORAND-KHALIFA, Directeur du département Information Management de la Recherche et Innovation de L'Oréal	Le fait d'utiliser un mail, notamment lors de négociations contractuelles, n'est pas un problème en soi, que ce soit au plan légal, technique ou de traçabilité des échanges qui ont pu avoir lieu. Ce qui pose un problème, c'est le fait que **ce document-mail est un document virtuel.** Auparavant, lorsque j'échangeais avec mon partenaire ou mon futur partenaire, j'avais des documents papier, et quand j'envoyais un courrier, quand j'envoyais un compte rendu, je gardais une copie que j'allais ranger dans mon dossier papier qui avait trait à l'affaire. De la même façon, quand je recevais un courrier ou une réponse, ou des éléments constitutifs du dossier contractuel, j'allais le ranger dans le dossier ; donc je gardais une trace physique. Aujourd'hui **la messagerie pose un problème de responsabilité.** Les traces de la négociation restent dans les boîtes individuelles car très rares sont les entreprises qui ont mis en place des boîtes génériques ou partagées (pour des raisons d'efficacité). Comme souvent, les **objets** sont très **mal libellés**, on ne sait pas qui est le destinataire et qui est en charge du dossier. Donc, ça arrive dans nos **messageries personnelles**. Je traite l'affaire, le collaborateur en charge du dossier va répondre à la demande mais, en général, va oublier ou ne va pas prendre le temps (parce qu'il n'en a pas) de classer ce document dans le dossier électronique concerné.
Marie LAPERDRIX, Chef du service des archives du ministère de l'Economie et des Finances	**La confidentialité des mails est une utopie** puisqu'un mail, vous l'envoyez à quelqu'un, vous pouvez éventuellement mettre des personnes en copie ; donc un mail est une trace écrite et, comme toute trace écrite, elle peut rebondir (c'est le concept de **mail boomerang**) et revenir quelques années après ou quelques mois après l'avoir écrit, et vous porter préjudice. De ce fait, il faut être particulièrement vigilant sur la confidentialité des mails, si ces derniers traitent de sujets liés aux ressources humaines.
Richard CAZENEUVE, Président du CR2PA	Effectivement, chacun, par expérience, a connu **le clic malheureux**. Or, on sait qu'une fois le message diffusé, il est très difficile d'en effacer les conséquences, qui peuvent être désastreuses, en particulier en entreprise. Donc, **la prévention est fondamentale en matière d'utilisation du numérique et du mail.**
Dijana LEKIC (Paris8), Étudiante Paris 8	Les pratiques de mon côté, peut-être parce que je suis dans le domaine et que je me méfie un peu concernant la gestion des informations et des documents qu'on échange par mail, je pense toujours à ce que je connais ou que j'ai vu pendant mes cours, notamment le master, et au travail

pendant l'alternance. Sinon, je pense que les gens, **les jeunes ne sont pas trop conscients de cet engagement via le mail et des envois de documents et de partage** ; mais les pratiques d'usage des mails, je pense qu'on a tous les mêmes pratiques au niveau de la quantité d'échanges ; **on échange tous beaucoup**, les jeunes surtout, dans le cadre de leurs études, entre eux, les amis. On a des pratiques qui se ressemblent avec des différences au niveau de la sécurité, des astuces que moi peut-être je connais plus ; combien de temps je vais garder un mail ? Je me dis : je vais quand même le garder, on ne sait jamais, et ma sœur, elle va le supprimer tout de suite…

S2E

Les mails ne sont pas anodins : témoignages d'entreprises

Vincent CLAUDON, Secrétaire Général de l'Agence de services et de paiement

Les incidents liés aux mails peuvent être nombreux, importants et avoir des conséquences assez néfastes pour un établissement, pour une organisation. Le premier aspect néfaste d'un mail que je peux considérer est celui de **s'adresser à la mauvaise personne** : on envoie un mail et on n'a pas vu qui était en copie, et cela peut avoir des conséquences assez fâcheuses en termes de discrétion, en termes de portée des éléments qui sont dans ce mail. C'est le premier point. Le deuxième souci que je verrais dans les incidents liés aux mails, c'est la **réponse compulsive** : on reçoit un mail, on est agacé, on répond tout de suite ; cela peut avoir aussi des dommages assez importants. Pour ma part, dans ma pratique, quand il y a des éléments un peu difficiles ou un agacement qui peut poindre en moi par rapport aux éléments qui sont apportés, j'essaie toujours de me laisser du temps ; je ne réponds jamais, quand il y a des choses négatives à dire, s'il y a des choses à rappeler, je ne le fais jamais dans l'instant, **j'attends un peu, je me laisse de la réflexion, de la maturation, pour ne pas créer d'impair**, parce qu'on voit… Peut-être que les gens se sont un peu disciplinés ces derniers temps mais on a vu au début de l'usage des mails des conversations qui pouvaient monter très vite , très fort, très haut, et qui peuvent nuire aux relations au sein de l'établissement, au sein de l'entreprise et qui peuvent avoir des conséquences assez fâcheuses.

Franck ASTOLFI, Responsable du projet d'archivage ReMIND chez Bouygues Construction

En fait, on a fait le constat que **les mails engageants dans le domaine de la construction n'apparaissaient plus, comme ça devrait être le cas, dans les archives**.

Les service travaux sont amenés à archiver tous types de documents, y compris des correspondances. Il y a 15 ans, la majorité des correspondances étaient du papier, acheminé par la Poste, des mails imprimés et mis dans des boîtes d'archives. À cette époque-là, les chargés d'affaire du Service Après Vente qui sont amenés à consulter ces documents trouvaient les échanges de courrier pour comprendre le déroulement d'un chantier, surtout pour des dommages-ouvrages ou

des contentieux, il est important de pouvoir se référer à ces correspondances.

Plus récemment, on s'est rendu compte que les mails augmentaient et que la partie correspondance papier diminuait ; les gens n'imprimaient plus ; les mails étaient conservés **dans les messageries**, classés ou pas. Dans la mesure où ils n'étaient **pas classés**, si le responsable travaux changeait de poste ou partait, sa messagerie était fermée et c'était la **disparition** complète de ses mails, ce qui était un vrai souci.

Christophe BINOT, Responsable de la Gouvernance de l'Information du Groupe Total

Oui, il y a beaucoup de mails qui apparaissent de manière totalement anodine, par exemple un ingénieur qui dit : il s'est passé cela sur tel sujet ou sur tel outil, ou voilà le compte rendu d'une opération, mais après, plusieurs années après, replacés dans un contexte de judiciarisation d'un certain nombre d'opérations ou de procès, de litiges, ces mails, qu'on appelle des ***smoking guns*** aux États-Unis, font les choux gras des avocats lors des procès, parce qu'ils montrent que tel ou tel collaborateur était au courant de telle ou telle pratique que l'entreprise a cherché à cacher ou à masquer. Cela fait partie vraiment d'une éducation, d'une sensibilisation des utilisateurs, en disant : **ne gardez que les mails essentiels et assurez-vous que ces mails essentiels ne comportent pas d'informations qui seraient susceptibles de mettre l'entreprise en péril lors de procès**.

S2F

Les mails ne sont pas anodins : témoignages d'avocats

Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés

Les courriers électroniques sont à la base de nos dossiers de plaidoirie. Ils permettent d'intégrer les cas de droit dans un contexte factuel. Ils permettent de dire que telle personne à répondu à telle autre et, avec tous ces éléments, nous pouvons reconstruire une histoire. **En fait, ce qu'il faut savoir, est que le juge n'attend pas la vérité ; il attend l'histoire la plus plausible.** Dès le moment où nous pouvons fixer la trame, la **chronologie** d'une histoire, eh bien, sachez que nous pouvons emporter la conviction de ce juge ; il cherche la logique et la **vraisemblance** de l'histoire, c'est-à-dire si je considère que mon histoire, elle a un trou à un moment donné, quand il y a un trou, là, on sait très bien que le juge va poser des questions sur le trou. On met un peu de sel sur la plaie et on dit : ça fait mal, là ? Et c'est exactement cela.

Le fait d'assurer la **traçabilité** des courriers électroniques, justement, permet de limiter ces trous béants dans une argumentation. Les éléments de traçabilité du courrier électronique se retrouvent à l'article **L34-1 du code des Postes et télécommunications électroniques**. Il y a par exemple l'adresse de courrier électronique, il y a la date d'envoi du courrier électronique, des éléments qui ont trait au terminal qui va les recevoir, des éléments qui ont trait à l'adresse IP du destinataire. Tous ces éléments se retrouvent listés pendant un certain temps vis-à-vis

	justement des autorités qui devraient avoir à déterminer qui a envoyé quoi et comment.
Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex	J'ai adressé un mail mais il n'est pas arrivé à son correspondant ; et, symétriquement, j'ai reçu un mail qui ne m'était pas destiné. Comment ça se passe ? Il faut se rappeler que **l'Internet, c'est la foire d'empoigne, l'Internet, c'est tout sauf la confidentialité.** Par conséquent, si je veux assurer la confidentialité des messages et dans une certaine mesure la fiabilité dans leur acheminement, il ne faut pas que j'utilise les circuits publics de l'Internet ; il faut que j'utilise ce qu'on appelle les **réseaux privés virtuels**, **VPN** en anglais. À cette condition-là, on a des chances raisonnables que le risque de recevoir quelque chose qui ne nous est pas destiné, et le risque que ce que l'on a envoyé n'arrive pas soit, sinon neutralisé, du moins très réduit. Mais, si je me trouve dans l'hypothèse où, précisément, j'ai envoyé un courriel à quelqu'un qui ne devait pas le recevoir, c'est comme si j'avais mis une mauvaise adresse, **je dois assumer les conséquences du risque que j'ai pris**. Et symétriquement, celui qui m'a envoyé un message et qui n'a pas pris la précaution de, même s'il met en bas de son mail que ce message est à usage… patati et patata, la confidentialité aujourd'hui ne lie que les professions réglementées. Moi, je suis avocat et j'appartiens à une profession réglementée, lorsque nous échangeons entre avocats, toutes nos correspondances sont présumées confidentielles, et ce n'est pas pour rien, c'est une des raisons pour lesquelles nous sommes réglementés, c'est que nous avons une **déontologie** et une interdiction de pouvoir diffuser les courriels que l'on reçoit entre avocats ; celui qui prend le risque d'utiliser un réseau non sécurisé pour adresser des mails prend le risque que ceux-ci soient diffusés et utilisés par les gens qui en sont, de fait, les destinataires, même si ce ne sont pas les destinataires voulus.
Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés	En fait, **la valeur juridique des courriers électroniques va dépendre avant tout de leur contenu**. Si je me retrouve avec un courrier électronique qui contient **une démission**, je pourrai l'utiliser, lorsque je suis l'employeur, comme démontrant cette démission. Un arrêt de la cour de cassation nous montre effectivement que lorsque le salarié envoie une démission de deux pages –c'est important, ce n'est pas juste un petit entrefilet qui démontrerait que c'est fait sur un coup de tête – eh bien, cette démission est tout à fait acceptable. Il y a un point qui est très important : **en matière de relations de travail, en matière de droit du travail, la preuve est libre**, c'est-à-dire qu'un courrier électronique pourra très bien être utilisé si je peux démontrer que c'est bien telle personne qui en est l'auteur et que l'intégrité est bien respectée. C'est-à-dire que tout ce qui va concerner la démission, tout ce qui va concerner des avertissements, le fait de les communiquer, de les transmettre par courrier électronique est tout à fait envisageable. Ce sont des points qui sont importants.

	Quand on se retrouve avec **des mises en demeure**, on est plus sur le volet contrat électronique ; là aussi je peux très mettre en place une mise en demeure et envoyer la mise en demeure sous une forme électronique, dès le moment où j'ai l'habitude d'échanger par voie électronique avec mon co-contractant. C'est une décision de 2011 sur l'absence de couverture en matière de gestion de titres sur Internet. La morale de l'histoire est : on ne sait pas si le mail n'a pas de valeur juridique en tant que telle, c'est son contenu qui a une valeur juridique, et à ce titre ce seront des règles de preuve libre, ou des règles de preuve encadrée qui trouveront à s'appliquer. Donc c'est à juger au cas par cas ; c'est à mettre en avant dans le cadre d'une politique de gestion des courriers électroniques.
S2G	**Le mail engage**
François-Xavier FERRARIO, Retraité, ancien Inspecteur général d'Oséo-BPIFRANCE	Tous les mails n'ont pas la même valeur, c'est certain. Une partie des mails ne délivre qu'une information factuelle qui *a priori* n'est pas interprétée ou interprétable ; et dans l'autre cas, **les mails engageants, ceux-là emportent une responsabilité directe**, soit un engagement à l'égard de tiers, soit une action à réaliser qui est décidée par la hiérarchie par exemple. Dans l'univers des mails, il y a ceux qui comptent et ceux qui ne comptent pas beaucoup. Comment les différencier ? D'une part, il y a le sujet du **secret**, le sujet de la **responsabilité** inhérente à l'envoi de certains mails, et d'autre part, il y a ceux qui ne font qu'apporter une information, pour enrichir les connaissances, ces informations n'étant pas absolument indispensables à l'engagement d'une action ou à la maîtrise d'un phénomène ou d'un risque.
Roger GRASS, Conseiller à la Cour de cassation, Ancien secrétaire général et greffier de la Cour de justice de l'Union européenne	Un mail est-il engageant ? Oui, je pense qu'**un mail est engageant, plus particulièrement dans les relations externes**. On sait qu'un mail peut être un élément de preuve de la **responsabilité contractuelle** ou **délictuelle** d'une entreprise, les cours suprêmes dans la plupart des États occidentaux ayant admis qu'un mail pouvait être un élément de preuve. Et cela est d'autant plus important qu'avec l'avènement du courrier électronique, l'habitude a été prise d'engager les **relations pré-contractuelles** non pas par téléphone mais par mail. Un mail laisse des traces et le principe *verba volent, scripta manent* rappelle la dangerosité du mail dans un contentieux toujours possible.
Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex	Lorsque je rédige un courriel et que je l'adresse à quelqu'un, est-ce que je suis lié, est-ce que je suis engagé par le courriel que j'ai rédigé et envoyé. La réponse est assez simple puisque le courriel est considéré comme un écrit. L'écrit est quelque chose qui est dissociable de son support. Autrement dit, **que j'écrive une lettre sur un support papier ou**

	que j'écrive sur un support électronique, j'ai écrit. Donc, la réponse est simple : j'ai rédigé un mail, je suis engagé par ce mail. Toutefois, la loi prévoit que l'on puisse contester l'identité du message : non, ce courriel, je n'en suis pas l'auteur. Ou que l'on puisse contester l'intégrité du message : non, ce courriel ne correspond pas à celui que j'ai envoyé. Donc la réponse à la question est simple : un courriel est engageant au même titre qu'un écrit sur support papier, à condition que l'**identité** de son auteur ou l'**intégrité** du contenu du message soit ne sont **pas contestés**, soit ne soient contestables.
Marie LAPERDRIX, Chef du service des archives du ministère de l'Economie et des Finances	Un mail est engageant puisqu'il véhicule une **information** qui est **engageante** et, de fait, aujourd'hui, un certain nombre d'informations transitent par un mail, et ces décisions, des décisions extrêmement importantes pour les organismes qui les prennent sont prises **via un mail** et non plus par une note signée de manière manuscrite.
Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés	**Attention , un mail peut vous engager juridiquement**. Dans une affaire de la **cour de cassation** du 1er juillet 2015 qui opposait un commerçant à un expert comptable, la cour de cassation a considéré que les questions posées par mail par le professionnel étaient suffisamment précis pour valoir commande ; l'expert comptable avait répondu à des questions extrêmement précises concernant le régime fiscal des salariés expatriés en Tunisie. Ces questions étant précises, et les réponses l'étant tout autant, il avait envoyé dans le même courrier une facture d'honoraires. La personne qui avait demandé avait dit : Mais attendez, moi, ce que je demandais, c'était juste des renseignements généraux. La cour de cassation n'a pas fait droit à cette **demande** et a considéré qu'il y avait bien **commande**. La morale de l'histoire, parce que histoire en a toujours une , c'est qu'il faut faire attention à ce que l'on écrit par mail. Ce ne sont pas des paroles qui s'envolent mais bien des écrits qui restent.
Ludovic GUERRA (Enseeiht), Étudiant Enseeiht	Pour ce qui est de l'engagement des mails, j'estime qu'un mail est quelque chose d'écrit et comme tout ce qui est écrit, que ce soit une lettre, un SMS ou quoi que ce soit qui est écrit, c'est quelque chose qui est engageant parce qu'il y a **une trace écrite qui est gardée**. Si j'écris une information, par exemple un message de condoléances pour une personne, je m'engage. À partir du moment où je dis ce que je pense à une personne, qu'elle a une trace écrite qu'elle peut relire, réfléchir dessus, c'est quelque chose qui est très engageant. Donc, quand j'écris un mail, outre le fait de faire attention aux fautes d'orthographe (parce que ça donne une **image de soi** si on fait des fautes), le message que l'on fait passer est très important. La personne va le lire, peut-être le relire plus tard, y penser, répondre, donc, oui, on s'engage au niveau personnel ou niveau du travail ; je décide de faire ça, par exemple d'engager une personne pour mon boulot, un stagiaire ou autre, le mail qu'on envoie est engageant. Lorsqu'on discute pour un contrat et que l'on souhaite négocier pour son salaire et que la

	personne dit : « Je vous envoie un mail récapitulant tout ce qu'on a dit, par exemple : vous aurez 100 euros par mois de remboursement pour la voiture », la personne qui envoie ce mail est engagée car elle dit : voilà ce que je vais faire. C'est une preuve écrite et si elle ne respecte pas ses engagements, on peut se faire valoir devant la loi. Donc, oui, pour moi, il est engageant dans tous les contextes.
Corentin MACIAS, Étudiant Enseeiht	Oui, c'est vrai que je pense **avoir conscience du fait de s'engager**, que ce soit dans les médias sociaux ou dans des e-mails, et même plus que conscience car du point de vue de la loi française un mail vaut comme une preuve. En étant vice-président de l'association étudiante de mon école, on a eu recours à des juristes pour des fournisseurs qui n'avaient pas été honnêtes avec nous et on a pu arriver avec des preuves grâce aux e-mails.

S2H — Propriété du mail et responsabilité

Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex	Quand on reçoit un mail, on peut se demander à qui il appartient, en fait **qui en est le propriétaire ?** Pour répondre à la question, il faut d'abord avoir à l'esprit que un mail, c'est exactement comme une lettre sur support papier. Si je reçois une lettre sur support papier, j'aurai tendance à considérer qu'elle m'appartient, bon ; alors qu'en réalité il faut distinguer deux hypothèses : **1)** Le **support** lui-même, c'est-à-dire l'objet courrier, c'est un meuble et en fait de meuble il y a un adage du droit qui dit « possession vaut titre » qui veut dire que lorsqu'on possède un objet mobilier, on est présumé en être le propriétaire ; sur le plan matériel, le mail appartient incontestablement à son destinataire. **2)** Sur le **plan intellectuel**, la réponse est plus nuancée. Si le mail se limite à faire une description ou à être simplement informatif, il n'a aucune originalité, il ne laisse place à aucune protection intellectuelle, et à ce moment-là, il appartient à son destinataire. En revanche, s'il possède un contenu innovant, il contient une création originale, à ce moment-là, il devient une œuvre de l'esprit et alors, malgré le fait qu'il ait été adressé à quelqu'un, par exemple un message, une poésie, un roman ou une nouvelle ; à ce moment-là, c'est une œuvre de l'esprit protégeable en tant que telle, à ce moment-là, il appartient à l'émetteur du mail et non pas à son récepteur.
Bruno DANVIN, Vice-président du CR2PA	**Tout ce que j'écris de ma boîte professionnelle appartient à l'entreprise parce que le message l'engage.**
Anne BURNEL, Directrice des Archives du Groupe La Poste	Dans l'univers professionnel, à mon sens, il est indéniable que **les courriels appartiennent à l'entreprise** ou à l'organisme pour lequel nous travaillons. On peut noter qu'il existe une relative tolérance sur

l'usage à titre privé de la messagerie professionnelle, comme c'est le cas pour le téléphone.

Cela dit, lorsque l'on est amené à créer un **message à titre personnel,** il est préférable de le classer dans un répertoire spécifique intitulé « personnel » ou « privé ». L'intérêt de procéder de la sorte est que, dans le cas où votre employeur aurait besoin d'accéder à votre messagerie, cela lui permettra d'identifier ces messages qui seront isolés dans un **répertoire spécifique** et, de cette façon-là, l'employeur n'ira pas consulter ces messages d'ordre privé.

Ce que l'on peut dire est que le **besoin de l'employeur** d'accéder à vos messages professionnels peut se produire par exemple dans le cas d'un départ non anticipé de collaborateur, donc le besoin pour les collègues ou la hiérarchie d'accéder à vos messages que vous n'aurez peut-être pas eu le temps de transmettre à votre successeur sur le poste. Il est donc important de savoir, lorsqu'on produit un message dans le cadre professionnel, qu'il appartient à votre entreprise.

Pour conclure, j'ajouterai que finalement, comme pour tout document de travail, **le courriel est un document d'archives qui appartient au patrimoine documentaire de l'entreprise** et non pas au collaborateur à titre individuel.

Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex

Écrire des messages électroniques, cela comporte des risques. Pour qui est le risque lorsque un salarié rédige un courriel et l'expédie ? S'il s'agit du **risque civil**, la réponse est assez simple, parce que le salarié est présumé mandaté par son employeur et, par conséquent, dès lors que **le courriel émane d'une boîte professionnelle, il est engageant pour la société**, sauf si la société arrive à démontrer que le destinataire du courriel ne pouvait pas ignorer que la personne qui lui a écrit n'avait pas le pouvoir de l'engager. Mais c'est une théorie qui est très très peu retenue , les tribunaux ayant tendance à considérer que **le collaborateur est le mandataire apparent**, c'est-à-dire qu'il agissait de bonne foi et qu'il faudrait vraiment qu'il ait agi de manière tellement inconsidérée par rapport à la manière habituelle de procéder que le destinataire ne pouvait pas ignorer qu'il n'était pas mandaté.

En revanche, pour l'aspect pénal, la réponse est plus nuancée. Si on considère que le courriel a été rédigé sur le lieu de travail, avec les outils fournis par l'employeur, là, l'employeur sera civilement responsable car les tribunaux considèrent que dès lors que ce sont les outils de travail qui ont été utilisés, que les choses se sont faites sur le lieu de travail, à ce moment-là, l'employeur doit répondre des dommages causés par ses salariés. En revanche, **sur le plan pénal**, la réponse est différente parce que, par exemple, un salarié qui ferait une contrefaçon d'un morceau de musique, ou téléchargerait des fichiers illégaux ; à ce moment-là, le salarié pourrait être poursuivi à titre individuel et l'employeur ne le serait pas, sauf dans une hypothèse que je n'ai jamais vue vérifiée, mais qui techniquement parlant et juridiquement parlant est possible, c'est celle qui consisterait à

	poursuivre l'employeur sur le terrain de la complicité, c'est-à-dire celui qui a fourni les moyens pour commettre l'infraction.
Bruno DANVIN, Vice-président du CR2PA	**Un mail reçu est aussi un objet à risques.**

S2I — Vous avez dit *disclaimer* ?

Marie-Anne CHABIN, Expert, membre fondateur du CR2PA	On appelle « disclaimer » dans le contexte de la messagerie électronique ces **quelques lignes d'avertissement** ajoutées assez fréquemment à la fin des messages d'entreprise ou de certaines personnes.
Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés	En droit français, les *disclaimers* ne servent pas à grand-chose. Il faut avoir à l'esprit, par contre, qu'un courrier électronique peut être considéré comme un papier officiel d'une entreprise. À ce titre, certaines mentions doivent y figurer, au sens des articles R123-237 et R123-238 du code de commerce. La cour d'appel de Nîmes en 2011 a eu à juger indirectement de la **valeur juridique d'un *disclaimer***, ou plutôt de son absence mais cette question, bien qu'évoquée, n'a pas été traitée par les magistrats de la cour d'appel de Nîmes. On peut conclure, sur la question du *disclaimer*, que si elle est **de peu d'intérêt** en droit national, elle peut revêtir, en fonction de la nationalité du destinataire, une importance tout autre. Les éléments relatifs à la confidentialité sont autant d'éléments qui peuvent être impactants pour certains pays comme les États-Unis.
Philippe BAZIN, Avocat associé, Avocat au Barreau de Rouen	Alors , je reçois, vous recevez, nous recevons des courriels qui sont assez exotiques dans la mesure où figure en bas de page une mention plus ou moins longue, plus ou moins en plusieurs langues, sur le thème : ce mail, ce courriel n'a pas de valeur engageante ; il n'aura de valeur que s'il est suivi d'un courrier papier. Cette formule peut être tentante pour se dire : tout ce que j'écris par courriel finalement ne m'engage pas. Sauf que c'est **un faux ami**. Pourquoi ? Parce que si je ne double pas le courriel d'une lettre recommandée AR (puisqu'avec une lettre simple, je n'aurai pas plus la preuve que la lettre est arrivée), donc si je ne double pas le courriel d'une lettre recommandée avec accusé de réception, je n'aurai pas plus de preuve et par conséquent mon correspondant aura beau jeu de me dire : « Mais, Monsieur, vous m'avez dit que ce courrier n'avait pas de valeur mais comme vous n'avez pas, par ailleurs et ensuite, adressé un courrier papier, je suis amené à considérer que c'est **ce courrier qui vous engage, dès lors que son identité n'est pas contestée, dès lors que son intégrité n'est pas contestée**.

Marie-Anne CHABIN, Expert, membre fondateur du CR2PA

Disclaimer signifie à proprement parler « **Avis de non-responsabilité** » (en anglais) ; il est parfois intitulé « Avis de confidentialité » ou « Post-scriptum ».

On trouve dans ces différents *disclaimers* des contenus très très variés qui sont révélateurs de la réalité du monde numérique.

À partir de ma collection personnelle de disclaimers, j'ai identifié **quatre groupes assez représentatifs** de ce qu'on peut rencontrer.

1) Le 1er groupe est un rappel de la **confidentialité** et de la **propriété** du message, et on pourrait très bien imaginer que cette information soit ajoutée à l'intérieur même du message, de manière non systématique mais plutôt opportune, de la même façon que l'on peut ajouter un tampon « confidentiel » sur un document papier.

> ***Ce message et toutes les pièces jointes sont établis à l'intention exclusive des destinataires et sont confidentiels.***
>
> ***Ce message est protégé par les règles relatives au secret des correspondances (message d'un particulier) ou Ce message, y compris toute pièce jointe, est confidentiel et couvert par le secret professionnel (*disclaimer *d'un avocat).***
>
> ***Le présent courriel, y compris tout fichier qui y serait joint, est propriété de [l'entreprise].***
>
> ***Les idées et opinions présentées dans ce message sont celles de son auteur, et ne représentent pas nécessairement celles de [l'entreprise].***
>
> ***Il peut également contenir des informations à usage restreint, soumises à droits d'auteur ou à d'autres dispositions légales.***

2) Le 2e groupe concerne des mentions d'ordre **technique** qui sont positives ou négatives qui mettent en évidence la fragilité du medium « messagerie » :

> ***L'intégrité de ce message n'étant pas assurée sur internet, la société expéditrice ne peut être tenue responsable de son contenu ni de ses pièces jointes.***
>
> ***Ce message a été vérifié et ne contient pas de programme malveillant.***

3) Un 3e groupe vise certains messages qui finalement sont assez peu crédibles et qui ressemblent plutôt à **des vœux pieux** :

> ***Sous réserve de tout accord conclu par écrit entre vous et [l'entreprise], son contenu ne représente en aucun cas un engagement de la part de [l'entreprise].***

Un certain nombre de mails sont aujourd'hui engageants, de fait, et ce ne serait sans doute pas très efficace de produire un *disclaimer* disant « je ne suis pas engagé » dans une procédure contentieuse.

> ***Tout usage de ce message par une personne autre que son destinataire est strictement interdit, ou Si vous n'êtes pas le destinataire de ce message, il vous est interdit de le copier, de le faire suivre, de le divulguer ou d'en utiliser tout ou partie.***

Une personne qui a reçu un message en est *de facto* destinataire ; c'est une lapalissade. On voit donc qu'**il y aurait des nuances à introduire dans la notion de destinataire**, en distinguant : la personne à qui l'émetteur souhaite envoyer son message (le destinataire **intentionnel**), la personne à qui l'émetteur a envoyé son message par erreur en cliquant trop vite sur une adresse proposée par l'outil (le destinataire **involontaire**) et la personne qui, sans que l'émetteur puisse le savoir, par suite d'un bug quelque part (le destinataire **inconnu**). va de fait recevoir le message.

4) Le 4e groupe concerne les *disclaimers* **écologiques** qui sont parfois inutiles et parfois pédagogiques selon le niveau de culture numérique du récepteur :

> ***Avant d'imprimer, pensez à l'environnement ! Please consider the environment before printing !***
>
> ***Le stockage des messages électroniques sur des serveurs, où qu'ils soient, consomme de l'énergie. Pensez à faire le tri de vos boîtes aux lettres électroniques (professionnelle et privée) régulièrement et à jeter les courriels inutiles.***

Le *disclaimer* ajouté au message par le serveur de messagerie d'une entreprise lors de l'expédition du message (l'auteur du mail ne le voit pas forcément) ne doit pas être confondu avec **les publicités** parfois ajoutées par certains **opérateurs de messagerie gratuite**.

Ces informations additionnelles se trouvent visuellement au même endroit du document pour le récepteur, c'est-à-dire en fin de message, pour le récepteur, et ne sont pas connue de l''émetteur. Il m'est arrivé un jour une **anecdote** assez intéressante : un de mes interlocuteurs répond à un de mes message en utilisant, pour une raison technique quelconque, sa messagerie personnelle, en l'occurrence **Voila**, qui a disparu du paysage depuis. Je prends connaissance du message et mon regard a été attiré à la fin du message par une phrase, pour le moins inattendue dans le contexte et qui disait en substance : « Savez-vous qui est ce ministre qui vit avec une femme plus jeune que lui de 30 ans ? », avec un petit bouton à cliquer pour avoir la réponse. Intriguée (plus par le fonctionnement de la messagerie que par la vie privée des ministres), j'ai cliqué et découvert la réponse sur le site pipol où me conduisait le lien. J'ai alors réalisé que mon interlocuteur était totalement étranger à cette histoire, alors que pour moi, il faisait partie de la lecture de ce qu'il m'écrivait. Je veux juste souligner par là que finalement le message s'était arrêté entre la boîte de messagerie de l'émetteur et la mienne en tant que récepteur ; il avait fait une pause sur le serveur de messagerie de l'opérateur pour prendre ce petit bagage publicitaire inopportun qui pour moi fait partie du contenu

	intellectuel, de la lecture du message que j'ai reçu, alors que pour l'émetteur, il ne faisait pas partie du message qu'il avait voulu me transmettre. **Je pense qu'il y a là une intrusion qui est un peu gênante dans la correspondance entre nos deux personnes.**
S2J	**Mails pro/mails perso**
Bruno DANVIN, Vice-président du CR2PA	**Le mail c'est comme le téléphone : tantôt privé, tantôt public.**
Christophe BINOT, Responsable de la Gouvernance de l'Information du Groupe Total	Le mail est un système individuel : oui et non... Le mail n'est pas un système individuel en tant que tel. On cherche à combattre cette idée chez nos collaborateurs : **la boîte mail, bien qu'elle soit à mon nom, n'est pas un espace privé, c'est un espace qui appartient à l'entreprise**. Nos systèmes d'archivage de mails sont des systèmes d'archivage dans lesquels tous les mails deviennent visibles par un ensemble de collaborateurs ou par une partie de l'entreprise. Ce n'est pas quelque chose de personnel qui appartient à l'utilisateur. Si l'utilisateur veut stocker ou archiver des mails qui sont purement personnels, il doit en fait les **tagger comme « privé »** ; autrement un système de messagerie d'entreprise n'est pas un système de boîtes mail personnelles mais **un système de boîtes de collaborateurs qui traitent des mails appartenant à l'entreprise et qui sont la propriété de l'entreprise**.
François DELION, Coordinateur de projet conservation des données Bouygues Telecom	Qu'est-ce qui fait qu'un mail est personnel ou professionnel ? À mon sens, c'est **l'adresse** que je vais utiliser pour rédiger ce mail. Mon entreprise me fournit une adresse mail professionnelle… mais on est loin de la **réalité de terrain**… Lorsque j'ai un mail à rédiger au bureau en vitesse, je ne vais pas pas ouvrir ma boîte mail externe laposte.net, je vais utiliser mon Outlook qui me tend les bras sur mon poste de travail. Alors il a fallu trouver une solution pour les mails personnels à partir des adresses professionnelles. Le consensus généralement adopté est d'utiliser **l'objet** en écrivant un mot du type « **privé** » ou « **personnel** ».
Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés	Oui, une adresse de courrier électronique professionnelle peut être considérée comme **une donnée personnelle**. Je vous donne un exemple : l'adresse p.agosti@caprioli-avocats.com; c'est mon adresse de courrier électronique professionnelle ; comme vous le comprenez, elle m'identifie ; mon nom, Agosti, est bien identifié Dès le moment où j'en ai plusieurs à traiter, et même une seule, on peut considérer que c'est un traitement de données à caractère personnel, et à ce titre, c'est un traitement qui est soumis à la loi Informatique et Libertés. *A contrario*, l'adresse contact@caprioli-avocats.com est une **adresse générique** ; on ne peut identifier une personne ; ce n'est pas une

	donnée à caractère personnel. Comme on le comprend, le fait d'avoir une adresse professionnelle n'est pas quelque chose qui permet avec certitude d'**être identifié** ; il est tout à fait envisageable qu'il y ait des homonymes ou des personnes qui usurpent votre identité. À ce titre, il y a une mesure de sécurité à prendre pour être sûr que mon interlocuteur est bien untel. On peut par exemple penser à ce qu'une personne ait l'habitude de m'écrire à cette adresse professionnel et saura que c'est bien moi qui est en face ; c'est **le courant habituel de relation**. **L'adresse IP peut être considérée comme une donnée à caractère personnel.** En tout cas, c'est ce qui est dit par certaines décisions. Si on retrouve face à une personne qui fraude, c'est normal de pouvoir retrouver l'adresse IP de la personne qui fraude.
Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex	Il m'arrive de recevoir, dans ma boîte aux lettres électronique, des courriels qui, dans l'objet, précisent « **personnel** ». Moi, je suis un avocat libéral, mais quand on est salarié, c'est le genre de chose dont il faut effectivement faire l'économie . Pourquoi ? Parce que si mon correspondant a pris la peine de marquer dans l'objet « personnel », c'est la manière qu'ont actuellement les tribunaux de qualifier, de caractériser le courriel personnel, quand l'objet mentionne qu'il est , personnel. Donc si l'émetteur du courriel a pris la peine de préciser dans l'objet « personnel », dans ma boîte, il apparaîtra « objet personnel » et effectivement il aura un caractère personnel, ce qui signifie, au regard du droit du travail, que l'employeur ne peut pas en prendre connaissance. En revanche, **si l'émetteur adresse un message pour évoquer un sujet personnel mais qu'il ne précise pas dans l'objet du message qu'il s'agit d'un objet personnel, à ce moment-là, mon employeur sera autorisé à prendre connaissance** du message puisque, ni de près ni de loin, il ne pouvait savoir que le message contenu à l'intérieur de l'enveloppe était effectivement un message qui abordait un sujet personnel.
Richard CAZENEUVE, Président du CR2PA	**Il n'y a plus de rupture entre la sphère personnelle et la sphère professionnelle.**

S2K — Le mail au travail : zoom sur l'@rrêt Nikon

Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés	Nous allons parler du régime juridique des courriers professionnels et des courriers personnels au sein de l'entreprise. C'est une vaste question qui, depuis 2001 ; défraie la chronique jurisprudentielle. Nous sommes le 2 octobre **2001**. La cour de cassation, chambre sociale, nous sort un arrêt qui est un arrêt de principe, **l'arrêt Nikon**, que tous les étudiants de droit étudient depuis lors et qui explique que, même

pendant mon temps de travail, sur mon lieu de travail, j'ai le droit à une vie personnelle résiduelle et je peux par exemple envoyer des mails personnels sur mon lieu de travail. Cette sphère privée résiduelle va poser de gros problèmes pour les entreprises. Une entreprise doit pouvoir surveiller, justement, la bonne activité de son entreprise, et s'assurer que le salarié est rentable ; c'est quelque chose de logique dans une économie libérale.

Toutefois, face à ce courant jurisprudentiel, on a considéré que c'est un peu libre, ce qui n'est pas le cas du tout. Depuis 2001, et avec deux grosses dates (2007 et 2011), la cour de cassation et la chambre sociale ont cherché à rééquilibrer, dans un autre sens, ce **balancier** qui était allé trop loin vers la vie privée. En gros, on se retrouve avec la possibilité, on pose le principe de la professionnalité des mails que le salarié envoie, ou reçoit, via son adresse de courrier professionnel, sauf si ces mails qui ne sont pas professionnels, sont marqués, j'ai bien dit « marqués » comme étant personnel. Le principe est : mon mail est professionnel ; je l'ai marqué comme étant personnel, il est personnel !

C'est le principe qui a fait jour depuis 2011 et, petit à petit, on a continué à le développer. Premier cas, le mail sortant : lorsque le **mail** est **sortant**, c'est facile : le salarié tape dans l'objet « personnel ». Par contre, lorsque le **mail** est **entrant**, on peut se retrouver avec des mails personnels ou professionnels, et dans ce cadre-là, il faudra le gérer au cas par cas. Il faut avoir à l'esprit que mail professionnel et mail personnel, ce n'est pas le même combat. Qu'est-ce qui va se passer ? Eh bien, l'entreprise va réguler cela en mettant en place une **charte d'utilisation des outils informatiques**. Et cette charte est reconnue par la jurisprudence en 2006 et en 2009. Cette charte nous dit : voilà exactement ce qu'il faut faire : tous les mails qui sont personnels, vous devez les marquer comme étant personnels. S'il n'est pas personnel, moi, l'employeur, je peux le contrôler. C'est un point important. Il faut savoir désormais que l'employeur peut accéder à ces mails professionnels hors de la présence du salarié. De la jurisprudence a fait jour également par rapport à un huissier de justice qui est venu contrôler cela et qui a pu le faire au motif de la professionnalité de ces mails.

Hélène LEGRAS, CIL/DPO Groupe AREVA et Vice-Présidente de l'ADPO

Donc , c'est vrai qu'il y a eu une **évolution sur la notion de mail personnel et mail professionnel**, dans le sens où une entreprise met à disposition de son personnel un ordinateur et une messagerie avec une adresse mail professionnelle et c'est vrai que, a priori, l'usage que devrait en faire le salarié est uniquement professionnelle.

Cependant dans **la vie de tous les jours**, si on a un dégât des eaux ; on ne va pas attendre le soir et on va utiliser son téléphone professionnel ou son mail professionnel pour un usage personnel. Sur cette question, il y a eu le déclic de **l'arrêt Nikon**. Nous sommes en **2001** et un salarié a utilisé sa messagerie professionnelle mais en indiquant que son mail était personnel. La cour de cassation a émis cet arrêt qui a fait grand bruit, du bruit dans Landerneau (pourtant on n'était pas en Bretagne

mais à Paris…) : désormais, on dit qu'**un salarié peut utiliser sa messagerie professionnelle pour un usage personnel**. Et cela a été confirmé en 2005.

Par contre, ensuite, il y a eu d'autres arrêts de la cour de cassation qui sont venus compléter l'arrêt Nikon et qui ont dit qu'**un mail créé par le salarié grâce à l'outil informatique mis à sa disposition par l'entreprise est présumé professionnel** et l'entreprise a le droit de l'ouvrir (c'était l'arrêt **Techni-Soft**) ; ensuite elle a émis un autre arrêt (l'arrêt **Cathnet-Science**) où elle précise que si on veut ouvrir un mail personnel, par exemple on présume que le salarié fait de la concurrence déloyale, qu'il y a un danger, par exemple que le mail est vérolé et qu'il risque que véroler toute la messagerie de l'entreprise et donc qu'il faut arrêter les dégâts mais là, par sécurité, on va **ouvrir le mail devant le salarié** ; c'est ça l'arrêt Cathnet- Science.

Il y a **beaucoup de jurisprudence** ; ce n'est pas la loi qui a dit : il y a des mails professionnels et il y a des mails personnels, c'est la jurisprudence et l'arrêt Nikon « a fait ce qu'on appelle jurisprudence » puisqu'il était unique en son genre en 2001 et que depuis il a fait des petits, il a confirmé ce précepte. Et c'est pour ça que maintenant les entreprises, sur les grands de **la CNIL** d'ailleurs qui met à disposition des personnes des modèles de chartes, dans des chartes informatiques, les entreprises précisent l'usage à faire des outils informatiques. Par contre, dans une charte informatique, **il ne faut jamais quantifier l'usage** personnel et l'usage professionnel car on risquerait de tomber dans des excès.

S2L — Trace et traçabilité des messages électroniques

Nathalie MORAND-KHALIFA, Directeur du département Information Management de la Recherche et Innovation de L'Oréal

Le mail est un document comme un autre, c'est la trace d'une action, d'une décision, d'une prise de responsabilité. Pour autant, comme tout autre document, il doit être contextualisé, il faut faire extrêmement **attention aux destinataires** ; il faut faire attention à l'objet si on veut que le destinataire le lise immédiatement ; il faut faire attention à ne pas mettre deux ou trois destinataires car on ne saura pas qui doit faire l'action. De la même façon, ne jamais oublier de mettre les bonnes personnes en copie, qui doivent avoir connaissance que les négociations contractuelles continuent, sont sur la bonne voie ou qu'il y a un problème.

Eric LAURENT-RICARD, Président Experact – Expert près la Cour Pénale Internationale

Il arrive fréquemment dans les expertises, en particulier judiciaires, d'être confronté à des fournitures d'informations, de messages édités et imprimés. **Il faut savoir que la valeur d'un message électronique imprimé est pratiquement nulle** car il est très facile, avant d'imprimer le message, de pouvoir en modifier le contenu et de venir prétendre que quelqu'un vous a envoyé telle ou telle information, ou telle ou telle

	menace, alors qu'en fait, c'est la personne qui a reçu le message qui l'a altéré avant de l'imprimer et de le présenter de cette façon-là. Aussi, il est toujours délicat d'affirmer la valeur probante d'un message ; pour ce faire, il faut (je reviens à ce qu'on a expliqué précédemment sur la traçabilité des messages) que **l'intégrité** du message puisse être vérifiée– grâce à la signature électronique par exemple ; analyser les en-têtes qui vont permettre de définir **quel chemin** a été utilisé par le message. Donc, quand on a une problématique de ce type-là, il faut toujours être capable de revenir au message électronique lui-même et à sa forme électronique, de façon à pouvoir en extraire les informations spécifiques, en particulier les informations concernant la **traçabilité** voire l'intégrité.
Pascal AGOSTI, Avocat associé, Docteur en droit, Cabinet Caprioli & Associés	Le 22 mars 2011, la chambre sociale de la **cour de cassation** a eu à se pencher sur l'**absence de traçabilité** de certains mails. À l'occasion d'une contestation de licenciement, le salarié licencié avait indiqué que certains mails mettaient en exergue le harcèlement moral de l'employeur : la cour de cassation a considéré que, puisque les mails en question ne figuraient pas dans la boîte mail du dirigeant, ils n'avaient pas cette valeur ; ils n'existaient pas ; ils pouvaient être des faux. Donc, ils ne se sont pas appuyés sur ces mails dont la trace était inconnue pour faire droit à la demande du salarié. La morale de l'histoire est que la décision d'appel a été confirmée en cassation.
Philippe BAZIN, Avocat au Barreau de Rouen, Cabinet Numerilex	Alors , quand un avocat est confronté au problème de la preuve, aujourd'hui, il aime bien les courriels. Il aime bien les courriels et il aime bien l'informatique en général, parce que si vous voulez vraiment avoir des relations confidentielles, n'utilisez surtout pas l'informatique. **Il n'y a pas plus traçable que l'informatique !** Dans la mesure où l'informatique garde en mémoire les coordonnées de l'émetteur, l'heure, le jour, l'appareil dont cela émane, le circuit qu'il a suivi, si d'aventure, en plus, vous passez par un serveur d'horodatage qui aura pour mission de conserver la trace de l'émission et la trace de réception, bref, sur le plan de la traçabilité, un objet informatique est **un objet extrêmement traçable**, par tous les moyens. Et n'oublions pas que la traçabilité désigne non seulement ce qui est **visible** (en d'autres termes, le contenu lisible par l'homme, le message) mais lorsque **j'efface** un contenu informatique, lorsque je le fais disparaître de mon ordinateur, eh bien, en fait, il ne disparaît pas, il ne disparaît que de mes yeux, mais il **reste inscrit** sur l'ordinateur et les experts, et pas seulement les experts puisqu'il existe des logiciels dans le commerce qui sont très simples pour ça, permettent de faire remonter le contenu du message, un peu comme on fait remonter une photo sur **un révélateur**, pour ceux qui ont connu l'époque où on faisait de la chambre noire et où la photo, après que le papier ait été « imprimé » apparaissait progressivement grâce au révélateur.

	Donc, un objet informatique est traçable, hypertraçable, et un conseil : si vous voulez de la relation confidentielle, surtout, revenez au papier .
Richard CAZENEUVE, *Président du CR2PA*	**Pour éviter une grande claque, ayez le bon clic !**

Suite avec la **Semaine 3. Écrire, lire, classer**