Livre Blanc
édité par COOPERTEAM

MESSAGERIE ÉLECTRONIQUE : RISQUES ET ENJEUX POUR L'ENTREPRISE

Par Maître Olivier ITEANU
Avocat à la cour d'appel de Paris
SELARL ITEANU Avocats

Témoignage client

de Sylvain Lebarbier
Chargé de mission - Conformité et Déontologie - AG2R

Table des matières

PRÉFACE

Il est urgent d'agir !

par Maître Olivier ITEANU,
Avocat à la Cour d'Appel de Paris

L'événement des 15 dernières années est l'arrivée massive d'Internet dans les entreprises et les foyers européens. Cependant, on n'a pas toujours analysé en profondeur les effets de cette révolution. Ce temps est désormais venu.

Car Internet, ce sont des dizaines de services différents et, parmi les plus utilisés, la messagerie électronique et le Web qui tiennent une place de choix dans l'évolution de nos sociétés et leurs usages. Cette messagerie électronique sous-tend une nouvelle économie de flux à l'entrée et à la sortie des systèmes d'information de l'entreprise. Ainsi, on estime que plus de 70 % des données des entreprises sont acheminées par le système dit de messagerie électronique.

Ces nouveaux flux créent de nouveaux usages : avant la messagerie électronique, il était rare que les collaborateurs soient destinataires de courriers personnels sur leur lieu de travail. La messagerie électronique a brisé cette pratique. Les courriels personnels affluent désormais dans les boîtes aux lettres électroniques des salariés. Quels sont les droits et devoirs de l'employeur au regard de ces contenus ?

Ces nouveaux flux créent aussi de nouvelles responsabilités juridiques. Avant, il était rare que les moyens mis à disposition de l'entreprise soient détournés pour l'importation, l'usage de contenus illicites, par exemple l'introduction dans l'entreprise de vidéos pédopornographiques. L'on sait malheureusement que cet usage est bien réel dans l'environnement en ligne, que ce contenu illicite peut par exemple être annexé à un courriel, et l'employeur n'a pas toujours conscience que cette situation l'expose en terme de responsabilités juridiques. Pour ces raisons, les questions de traçage et traçabilité doivent être aujourd'hui au centre des préoccupations des entreprises de toutes tailles.

Avant l'avènement du numérique, la question de l'archivage se posait peu quant au support utilisé : le papier. La dématérialisation et l'archivage électronique des contenus natifs du monde numérique font régulièrement la une de l'actualité.

Le grand mérite de ce livre blanc, initié par la Société COOPERTEAM , est d'avoir compris que ces questions ne sont pas exclusivement techniques ou organisationnelles : elles sont également juridiques.

A l'inverse, la seule dimension juridique des problèmes traités est notoirement insuffisante. La technique et l'organisation sont préalables. Aussi, il est urgent que les compétences diverses se parlent pour que l'entreprise évolue dans ce nouvel environnement en toute sécurité, en toute confiance.

Il est urgent d'agir et ce livre blanc est un outil pour y parvenir. Reste maintenant à l'entreprise à se mettre en conformité avec la Loi au moyen de cet outil et avec les bons partenaires.

Section 1

Messages électroniques en entreprise, un statut juridique méconnu

La messagerie électronique (courriels, chat) est un formidable outil de développement pour l'entreprise et ses collaborateurs.

Cet outil est même devenu indispensable à l'activité de l'entreprise : quelle entreprise peut aujourd'hui se passer de messagerie électronique ? Nous ne sommes même qu'au début de cette mutation déjà bien avancée.

Mais du fait de cette omniprésence, la messagerie électronique est également devenue un objet de droit.

Comme nous allons le voir, **la messagerie électronique engage l'entreprise.** Elle est susceptible de faire courir de nouveaux risques à l'activité de l'entreprise, voire de faire courir à l'entreprise et à ses dirigeants de nouveaux risques juridiques.

Un cadre de notre entreprise a passé commande par courriel d'un service, sans avoir obtenu l'accord de son supérieur hiérarchique : sommes- nous tenus par cette commande faite par courriel ?

La réponse est par principe oui, à charge de l'entreprise de se retourner ensuite contre son salarié pour n'avoir pas respecté la procédure interne et prendre éventuellement des sanctions proportionnées.

I. Les messages électroniques engagent l'entreprise

Peu d'entreprises le savent, mais un simple courriel est susceptible d'engager l'entreprise vis-à-vis d'un prospect, d'un client, d'un fournisseur ou d'un partenaire.

Cette évolution majeure tient à ce que le droit français a décidé d'accueillir le support électronique comme mode de preuve à l'égal du courrier papier.

Ainsi, un simple courriel de commande est-il l'égal dans la Loi, d'un courrier de commande sur papier en tête de l'entreprise, signé en original et empruntant la voie postale ?

La loi du 13 mars 2000[1] qui a réformé en profondeur le droit de la preuve a été amorcée en portant adaptation de la preuve aux technologies de l'information. Cette Loi a redéfini la preuve littérale et a consacré **la force probante de l'écrit électronique**.

L'article 1316-3 du Code civil dispose en effet que : « *L'écrit sur support électronique a la même force probante que l'écrit sur support papier.* »

1 Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Certes, **pour que l'écrit numérique soit admis comme moyen de preuve**, l'article 1316-1 du Code Civil prévoit que la messagerie doit respecter trois conditions[2]:

- la personne dont émane l'écrit doit être dûment identifiée.
- l'écrit doit être établi dans des conditions de nature à en garantir l'intégrité.
- l'écrit électronique doit être conservé dans des conditions de nature à en garantir l'intégrité.

Cependant, ces conditions préalables sont théoriques. Le fait est que, désormais, un juge ne peut refuser un courriel comme preuve au seul motif que le support électronique ne le convainc pas. Si le juge rejette la preuve, il ne pourra le faire que si l'une des parties soulève cette irrecevabilité et démontre que les trois conditions précitées ne sont pas remplies. En d'autres termes, le juge n'est pas en droit de rejeter un courriel sauf s'il motive ce rejet.

A ce jour, aucune jurisprudence n'a été publiée sur l'application de l'article 1316-1 du code civil.

Tout courriel est donc par principe admissible à titre de preuve.

II. La messagerie électronique fait courir un risque à l'activité de l'entreprise

Comme nous l'avons dit en introduction, l'utilisation des nouvelles technologies, notamment de la messagerie électronique, sur le lieu de travail est un formidable outil au service de l'entreprise.

La messagerie électronique facilite également le travail des collaborateurs et est ainsi un moyen d'améliorer leurs conditions de travail.

Parmi les abus connus et susceptibles d'être sanctionnés par la justice, sous réserve qu'on puisse les identifier et les prouver, on peut citer :

- l'atteinte aux droits de propriété intellectuelle de l'entreprise, par la diffusion de programmes, de données, de bases de données appartenant à l'entreprise.
- l'envoi d'informations confidentielles à des

2 « L'écrit sous forme électronique est admis en preuve au même titre 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. »

boîtes aux lettres privées, à la concurrence, etc.

- l'achat ou la vente de produits ou services illégaux de type fichiers vidéos ou musicaux pirates attachés à des messages.
- la réception ou l'émission de contenus illicites.
- de mauvaises pratiques pénalisant le réseau (réception des virus informatiques, charge sur le réseau etc.).

III. La messagerie électronique fait courir un risque juridique à l'entreprise et à ses dirigeants

Enfin, pour l'ensemble des actes illicites commis à partir de la messagerie électronique de l'entreprise, et notamment ceux énoncés au paragraphe précédent, l'entreprise peut voir sa responsabilité juridique engagée.

Cette responsabilité peut tout d'abord être engagée en tant qu'employeur du salarié, l'employeur peut voir sa responsabilité civile engagée sur le fondement de l'article 1384, alinéa 5 du Code civil pour des faits civils ou pénaux commis par le salarié préposé.

Sa responsabilité sera engagée dès lors que trois conditions cumulatives sont réunies :

- le salarié a agi sous la subordination de son employeur.
- ce salarié a causé un dommage à l'occasion de l'exercice de ses fonctions.
- ce salarié a utilisé les outils de l'entreprise conformément à leur destination.

En clair, l'employeur « *ne s'exonère de sa responsabilité que si son préposé a agi* ***hors des fonctions*** *auxquelles il était employé,* ***sans autorisation****,* ***et à des fins étrangères*** *à ses attributions* ».

Cette solution aboutit donc à obliger l'entreprise à dédommager des victimes pour des actes qu'elle n'a pas commis et auxquels elle n'a pas participé. Aussi critiquable soit-elle sur le plan de l'équité, il n'en reste pas moins que **l'employeur risque d'être tenu pour responsable dans la mesure où il a donné au salarié délinquant les moyens matériels pour commettre un délit en ligne.**

Ce d'autant que les tribunaux ont pour ligne constante d'appréhender de manière très lâche la condition relative à l'exercice *dans ou hors des fonctions*.

Un arrêt de la Cour d'Appel d'Aix en Provence a ainsi confirmé la condamnation d'un employeur pour avoir mis à disposition d'un salarié les moyens techniques nécessaires à la mise en ligne d'un site internet contrefaisant celui d'une autre société[3].

Ainsi, la Cour a estimé que le simple fait que le salarié ait utilisé l'accès Internet et les logiciels mis à sa disposition suffisait à rendre l'employeur responsable solidairement avec son salarié des faits qui lui étaient reprochés. Cette jurisprudence a été abondamment commentée mais n'a pas été jusqu'à ce jour clairement contredite.

Ce qui est vrai pour l'accès Internet l'est également pour les logiciels de messagerie, dans la mesure où il s'agit de la mise à disposition de moyens et leur contrôle qui est en cause.

Il faut être conscient que la messagerie électronique est un nouveau facteur de risque pour l'activité de l'entreprise.

La messagerie crée, avec l'extérieur, des *flux entrants* et *sortants* et les actifs de l'entreprise peuvent emprunter cette voie pour être dilapidés, pillés.

3 Arrêt de la Cour d'appel d'Aix en Provence 13 mars 2006, Lucent Technologies c/ Escota, Lycos France, Nicolas B.

Section 2

L'entreprise réagit par le contrôle : méthodes et bonnes pratiques

Face aux nouveaux risques juridiques et financiers que constitue l'introduction dans l'entreprise de la messagerie électronique, **l'entreprise doit réagir pour se prémunir** et conserver l'usage de cet outil qui est tout à la fois un élément important de sa productivité et un espace de liberté pour les collaborateurs.

I. Le contrôle légitime de l'entreprise

Au titre de ses attributions et de son pouvoir de direction, **le chef d'entreprise peut légitimement contrôler l'activité professionnelle de ses salariés.**

L'article L 120-2 du Code du travail dispose que les restrictions aux droits et libertés des salariés sont possibles dans la mesure où celles-ci sont justifiées par la nature de la tâche à accomplir et proportionnées au but recherché.

En d'autres termes, **ce contrôle est possible sous condition de respecter deux grands principes que sont le principe de transparence et le principe de proportionnalité :**

- **Le principe de transparence :** L'article L.121-8 du Code du travail dispose qu'aucune *« information concernant personnellement un salarié (…) ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi ».*

  Cette information doit être effective, compréhensible et mise à jour afin que les salariés aient une réelle connaissance du dispositif en place.

  En outre, l'employeur doit recueillir l'avis, et non l'accord, des représentants du personnel. En particulier, l'article L.432-2-1 du même code prévoit une information du comité d'entreprise dans le but de recueillir son avis.

- **Le principe de proportionnalité :** L'article L.120-2 du Code de travail dispose que : *« nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».*

  Les moyens mis en œuvre ne peuvent apporter de restrictions aux libertés individuelles des salariés que si elles sont justifiées par un intérêt légitime de l'employeur *(sécurité des systèmes de messagerie, par exemple)* et proportionnées aux finalités du contrôle visé.

Aussi, tout procédé de contrôle du système de messagerie et notamment des contenus transitant par les serveurs de l'entreprise, ne pourra être mis en place qu'après information préalable des salariés, avis préalable des représentants du personnel et en respectant le principe de proportionnalité.

II. Le cas du courrier électronique personnel

Depuis plusieurs années, la question du contrôle des messageries électroniques se heurte à celle, légitime, du respect de la vie privée des salariés sur leur lieu de travail. Il faut dire que la violation d'une correspondance privée est sanctionnée par l'article 226-15 alinéa 2 du Code pénal à une peine de 45.000 Euros et un an d'emprisonnement.[4]

La question du contrôle des messageries électroniques a connu une évolution majeure en 2006 : La Cour de Cassation, dans deux arrêts du 18 octobre 2006, a considéré que les « fichiers de travail », notamment électroniques, *« sont présumés, sauf si le salarié les identifie comme personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors de sa présence ».*[5]

De l'avis général, ces deux arrêts s'étendent à la messagerie électronique. Les applications à ces arrêts de principe ne se sont pas fait attendre.

L'entreprise doit mettre en place un contrôle des messageries en respectant les conditions suivantes :

➪ INFORMER *préalablement les salariés, par publication sur les panneaux d'affichage obligatoires et par note de services.*

➪ AVISER *les représentants du personnel en collectant leur avis.*

➪ MOTIVER *dans l'information préalable et l'avis des représentants du personnel, le recours à ce contrôle, notamment par les risques que fait courir la messagerie à l'activité de l'entreprise.*

4 pour avoir « commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »

5 Cass. Soc. 18 octobre 2008

Lors d'une action en justice, *l'employeur pourra toujours faire valoir les courriers électroniques indiquant leur nature personnelle (mais pas leur contenu), ainsi que leur nombre grâce aux données de connexion conservées.*

Tout dispositif de contrôle *devra faire l'objet d'une déclaration à la* **CNIL** *et devra préciser la durée pendant laquelle les messages sont conservés.*

La Cour de Cassation a ainsi jugé récemment que :

> *« Attendu que pour juger le licenciement sans cause réelle et sérieuse, la cour d'appel a retenu que les deux messages électroniques du 16 avril 2002 adressés par M. X. à une de ses collaboratrices sur le lieu de travail ne comportant aucun élément professionnel, constituent de la correspondance privée ; qu'il n'appartient pas à l'employeur de prendre connaissance des messages personnels émis ou reçus grâce à l'outil informatique mis à la disposition du salarié pour son travail.*
>
> *Qu'en statuant ainsi, sans rechercher si les fichiers ouverts sur le matériel mis à sa disposition par l'employeur avaient été identifiés comme personnels par le salarié, la cour d'appel n'a pas donné de base légale à sa décision ».* [6]

Ainsi donc, **l'employeur est en droit de prendre connaissance des messages professionnels de son salarié hors de sa présence, à condition de s'assurer qu'il ne s'agit pas de messages personnels.**

Le problème reste que le caractère personnel d'un courriel est avant tout déterminé par rapport à son contenu.

L'employeur peut procéder au contrôle de la messagerie professionnelle de son salarié hors de sa présence à condition que ces messages ne soient pas personnels. *Le caractère personnel des messages se déduit de mentions pouvant figurer dans le sujet telles que « personnel », « mes documents », ou toutes mentions qui démontrent clairement un caractère personnel (un prénom, un lieu de villégiature, etc.). Si l'employeur prend connaissance par erreur d'un message qu'il croyait professionnel et qui se révèle personnel par son contenu, il lui reste à détruire l'édition papier de ce message, dans tous les cas à ne pas l'utiliser d'une quelconque manière que ce soit et à considérer que le contenu dont il a pris connaissance est strictement confidentiel, et à ne le révéler donc à quiconque.*

III. Contrôle : les bonnes pratiques

Pour la Direction Informatique :

→ *Moyens techniques de contrôle*

Pour assurer l'exercice de son pouvoir de contrôle sur les messages électroniques, l'employeur devra utiliser des outils techniques lui permettant d'accéder au contenu du courrier électronique en toute légalité.

A ce titre, il pourra :

- mettre en place un dispositif technique susceptible de détecter certains mots clés dans l'objet des messages, et dont la liste ne devra pas être divulguée aux salariés de l'entreprise.
- mettre en place un dispositif permettant de limiter l'envoi ou la réception de certains messages du fait de leur taille ou volume ou du fait de la nature des pièces jointes.
- faire une copie de sauvegarde et/ou archivage des messages envoyés ou reçus par le salarié, dans l'hypothèse où ce dernier n'aurait pas conservé le message.

Pour la Direction Générale :

→ *Mesures d'ordre organisationnel*

Il est primordial que tout employeur sensibilise le personnel de son entreprise aux questions de criminalité informatique, y compris sur les aspects légaux par la formation et l'information du personnel de l'entreprise.
Cette formation pourra se réaliser par la fixation de directives à l'attention des salariés et pourrait contenir :

- une description des comportements risqués, des pratiques interdites et les activités considérées comme suspectes sur le réseau.
- les conséquences possibles d'une violation de la sécurité.
- les sanctions en cas de non-respect des directives fixées.

→ *Outils juridiques*

L'introduction de nouvelles technologies nécessite que l'employeur adapte les règles de fonctionnement de l'entreprise. Dans cette situation, la question du choix de l'instrument se pose.

6 Ch. soc., 30 mai 2007, Société The Phone House c/ Monsieur X.

Il est fortement conseillé à la ***DIRECTION INFORMATIQUE*** *de :*

⇨ BLOQUER

toutes les applications non autorisées et d'interdire aux employés de les télécharger et de les installer,

⇨ CONFIGURER

le pare-feu ainsi que les filtres de courrier électronique afin de bloquer les messages contenant des exécutables cachés ou visibles,

⇨ IDENTIFIER

et assurer le suivi de chaque ordinateur, chaque serveur, chaque périphérique et chaque application présents sur le réseau.

❖ Les Chartes

Pour fixer les règles de déontologie et de sécurité relatives à l'usage des outils informatiques, la CNIL recommande la rédaction de certains documents, et notamment de **chartes** d'usage Internet ou informatique.
Ces chartes ont généralement pour but de fixer des lignes de conduite, qui cumulent souvent des interdictions générales directes ou indirectes avec des règles d'usage pratique. Ce sont, à la base, des outils pédagogiques sans valeur juridique.

Elles doivent préciser de manière exhaustive les comportements interdits au sein de l'entreprise : consulter des sites pédophiles ou pornographiques, télécharger de la musique, des films ou tout autre programme, développer un site Internet à partir de son poste de travail, dialoguer sur des chats ou forums à des fins non professionnelles, etc.
Pour que cette charte soit opposable aux salariés, celle-ci doit être intégrée dans une norme juridique existante (contrat de travail, règlement intérieur, éventuellement notes de services).

❖ Le règlement intérieur

Inscrite dans le règlement intérieur, l'obligation de ne pas utiliser les TIC à titre personnel et notamment l'accès privé à la messagerie électronique pourra, en cas de non respect, fonder l'exercice du pouvoir disciplinaire de l'employeur. Toutefois, pour être opposable, la règle qui n'a pas été respectée doit figurer dans le règlement intérieur.

L'employeur devra également s'attacher à la protection de son réseau informatique. A ce titre, la Cnil considère « *qu'un usage raisonnable, susceptible de ne pas amoindrir les conditions d'accès professionnel au réseau et ne mettant pas en cause la productivité paraît généralement et socialement admis par la plupart des entreprises ou administrations.*»

L'employeur devra prévoir une clause autorisant une utilisation personnelle, ponctuelle et raisonnable des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs, et qui ne met pas en cause l'intérêt ou l'image de l'entreprise.

Toutefois, il est fortement conseillé d'imposer une interdiction formelle de toute utilisation de l'Internet à des fins personnelles. Cette mesure permettra de garantir l'employeur contre de telles pratiques tout en permettant d'accorder une certaine tolérance. Elle est en réalité nécessaire à ce jour, et compte tenu de la jurisprudence aujourd'hui majoritaire qui semble considérer que dès l'instant où l'employeur autorise un tel usage personnel, même en tentant de le borner, il endosse une responsabilité juridique consécutive à cet usage personnel.

❖ Les notes de procédures complémentaires valant notes de services

L'employeur pourra également élaborer des notes de procédure à l'attention des administrateurs réseaux notamment, dans lesquelles les modalités, les finalités et les limites du contrôle des systèmes d'information pourraient être définies.

Ce document contiendrait :

- les cas dans lesquels le contrôle des données globales de trafic est autorisé,
- les situations dans lesquelles le contrôle peut être individualisé,
- les personnes habilitées à requérir ce genre de contrôle.

Enfin, ce document pourrait clairement préciser que les courriels personnels ne doivent en aucun cas être ouverts.

Focus

Externalisation des systèmes de messagerie : à qui incombe la responsabilité ?

Dans un souci de gestion efficace des risques, les entreprises ont tendance à avoir recours à des prestataires extérieurs spécialisés en la matière. Les entreprises ont recours à l'externalisation des systèmes de messagerie afin de s'assurer la maîtrise des coûts et des services, surmonter la complexité de l'infrastructure technique liée à l'archivage des courriels et de s'assurer une garantie de sécurité grâce au recours à des prestataires spécialisés. Ces tiers vont permettre aux entreprises de leur assurer un système de messagerie fiable, sécurisé et performant.

Exemple : *Une société X héberge ses serveurs de messagerie dans une société d'infogérance*, la question est de savoir à qui incombe la responsabilité en cas de problèmes de messagerie ?*

** Une société d'infogérance est un prestataire de services informatiques qui propose l'externalisation de la gestion des systèmes d'informations.*

Lorsqu'une entreprise envisage une externalisation de son système de messagerie, il est impératif d'organiser contractuellement les relations entre l'entreprise, le donneur d'ordre et le prestataire externe.

Ce contrat devra comporter :

- les obligations incombant au prestataire :
  - assurer la protection du système de messagerie,
  - s'engager à conserver l'intégralité des données reçues, sous la forme et le format convenus avec l'entreprise puisque les données doivent pouvoir être restituées en fin de contrat ou en cas de cessation d'activité.
- des modes de suivi et de contrôle du système définis (périodicité, nature des tests sur les supports, opérations de transfert, etc.),
- une définition précise du niveau de service attendu (taux de disponibilité, performance du service, délai de restitution des données, etc.),
- des garanties spécifiques doivent être mises en œuvre afin de protéger les données du système de messagerie.

De son côté, l'entreprise, donneur d'ordre, devra procéder à un certain nombre de contrôles et notamment :

- la mise en place de procédures spécifiques pour définir les autorisations en matière d'intervention sur les systèmes de messagerie,
- la gestion des droits d'accès clairement établie (suivi des personnes habilitées : émission, pertes, d'accréditations, etc.),
- la détermination des responsabilités (accès non autorisé, etc.).

Section 3

L'entreprise réagit : la traçabilité des échanges électroniques, une obligation légale pour toutes les Entreprises

I. Pourquoi la question de la traçabilité est-elle devenue obligatoire pour les entreprises de toutes tailles ?

Du fait de l'ouverture des systèmes d'information des entreprises sur l'extérieur, la question de la traçabilité des échanges est devenue une affaire cruciale pour les directions générales pour au moins deux raisons.

D'une part, parce que cette traçabilité est exigée par les législations, comme c'est le cas dans la Loi française sous l'impulsion de directives communautaires. Nous détaillons ci-après cette obligation légale de traçabilité.

D'autre part, parce qu'il **est désormais de l'intérêt même des directions générales d'organiser la traçabilité des échanges au sein de l'entreprise.** En effet, comme nous l'avons vu, **ces flux sont porteurs de risques juridiques et il peut se trouver des cas où l'entreprise se disculpera d'une accusation en démontrant qu'elle n'est pas à l'origine d'un flux en litige.**

Exemple d'un cas où la DIRECTION GENERALE aurait dû mettre en place un système de traçabilité :

Une vidéo pornographique est retrouvée sur le serveur de l'entreprise. On soupçonne que cette vidéo a été introduite dans l'entreprise, attachée à un courrier électronique.

Une vidéo pornographique mettant en scène des mineurs est un délit en tant que tel.

L'article 227-23 du Code Pénal punit « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende. »

Mais le même article du Code Pénal comporte une sorte de « sous-délit » qui est « *Le fait de (…) détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30.000 euros d'amende.* »

Or, qui détient cette image, si ce n'est l'entreprise ?

Dans ce cas, le représentant légal peut encourir la peine … sauf s'il est capable d'attribuer la présence du fichier en litige par la traçabilité des échanges qu'il aura mis en place.

II. Les contours de l'obligation légale de traçabilité pour l'entreprise :

Toutes les entreprises sont concernées

Contrairement à certaines croyances, l'obligation de traçabilité n'est pas réservée par la Loi aux seuls opérateurs de communications électroniques, soit les anciens opérateurs de télécommunications et les fournisseurs d'accès Internet (FAI).

Créée après les attentats du 11 septembre 2001, cette obligation devait à l'origine être effectivement temporaire et ne concerner que les FAI. Toutefois, la Loi n° 2006-64 du 23 janvier 2006 relative à la Lutte contre le terrorisme a rendu cette mesure permanente et des textes de Lois ultérieurs ont étendu l'obligation de traçabilité bien au-delà des seuls opérateurs. Aujourd'hui elle concerne toutes les organisations fournissant un accès à un système de messagerie, qu'il s'agisse d'une entreprise pour ses employés, d'une université pour les étudiants et les professeurs, d'une organisation gouvernementale pour ses fonctionnaires, ou d'une association pour ses membres.

Deux textes de loi différents imposent la conservation des traces, communément appelées *données techniques de connexion*. Nous allons voir tout à la fois que les justifications apportées à ces obligations de « traçage » sont différentes selon les textes, que les populations concernées sont beaucoup plus diverses qu'on ne le croit et que les obligations en question concernent bien plus que de simples données de connexion. **La loi prévoit dans tous les cas des sanctions pénales (peines d'emprisonnement et amendes) pour les contrevenants.**

A. Les obligations des opérateurs de communication électronique

La première de ces obligations figure à l'article L34-1 du Code des postes et des communications électroniques (CPCE) : « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations », les opérateurs de communications se voient imposer de conserver « certaines catégories de données techniques ».

Dans la mesure où l'organisation fournit l'accès à son propre système de messagerie, elle a l'obligation de garantir la traçabilité des échanges électroniques réalisés par le biais de ce système.

La population concernée est parfaitement identifiée : il s'agit des opérateurs de communications électroniques et les fournisseurs d'accès Internet. Ces acteurs disposent d'un statut. Ils ont l'obligation de se déclarer auprès de l'Autorité de régulation des communications électroniques et des postes (Arcep), qui tient à jour la liste des opérateurs sur son site Web[7].

Cependant, l'article L34-1 du CPCE ne précise ni la durée ni la nature exacte des données techniques qu'ils doivent conserver. Ces précisions ont été apportées par un décret du 24 mars 2006[8] pris en application de l'article L34-1 du CPCE : la durée de conservation des données techniques est fixée à un an à compter du jour de leur enregistrement. Au-delà, l'opérateur a l'obligation de les détruire. Le décret définit aussi les types de données concernées par la conservation, mais il est rédigé d'une telle façon que toutes les informations détenues par les opérateurs sont visées, y compris les données purement administratives *(voir tableau 3.1).*

Tableau 3.1 Données de communications électroniques à conserver obligatoirement par les opérateurs (décret n° 2006-358 du 24 mars 2006)

a	Les informations permettant d'identifier l'utilisateur.
b	Les données relatives aux équipements terminaux de communication utilisés.
c	Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication.
d	Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.
e	Les données permettant d'identifier le ou les destinataires de la communication.
f	Pour la téléphonie seulement, en plus des données listées précédemment, celles permettant d'identifier l'origine et la localisation de la communication.

En réalité la traçabilité va bien au-delà des seules données strictement techniques. Dans la catégorie des « informations permettant d'identifier l'utilisateur », il semble que de simples données administratives, comme les données sollicitées par l'opérateur pour l'ouverture d'une ligne (nom, prénom, adresse), soient considérées comme des données techniques de connexion. Le décret oblige ainsi l'opérateur à conserver toutes les données en possession desquelles il se trouve et, surtout, à les produire sur demande : un juge d'instruction, le parquet ou un simple plaignant quel qu'il soit, autorisé en justice au vu d'une simple requête, peuvent obtenir en toute légalité ces informations d'un opérateur.

Le décret dispose que les opérateurs sont dédommagés par l'État lorsqu'ils sont requis par une autorité judiciaire pour fournir des données conservées. Enfin, l'article L30-3 du CPCE prévoit une peine d'emprisonnement maximale d'un an et une amende maximale de 75 000 euros pour les opérateurs qui ne respecteraient pas la conservation des données techniques de connexion dans les conditions légales.

B. Les obligations des organisations françaises fournissant un accès à des services de communication en ligne

Un second texte de loi impose la conservation des données :

Selon l'article 6, II, de la **Loi n° 2004-575 du 21 juin 2004 (LCEN)**, les personnes « *dont l'activité est d'offrir un accès à des services de communication au public en ligne* » et celles qui « assurent, même à titre gratuit, pour mise à disposition du public des services de communication au public en ligne » ont l'obligation de détenir et conserver « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

Dans ce texte, il s'agit en réalité de limiter les atteintes aux droits de tiers diffamés ou injuriés en public sur les réseaux.

Le texte prévoit des sanctions pénales d'un an d'emprisonnement et de 75 000 euros d'amende[9].

Le texte précise qu'un décret du Conseil d'État après avis de la CNIL viendra définir les données concernées, ainsi que leur durée et les modalités de leur conservation. À ce jour, aucun décret n'a été publié mais la loi s'applique en dépit de l'absence d'un décret.

À la différence des dispositions du CPCE, on se trouve dans une réglementation à la fonction

7 *www.arcep.fr.*

8 Décret n° 2006-358 relatif à la conservation des données des communications électroniques.

9 Article 6, VI, de la LCEN.

et non par rapport à un statut prédéterminé. En d'autres termes, toute personne qui endosse la fonction de fournisseur d'accès Internet ou de fournisseur d'hébergement est tenue par l'obligation de conservation. Et ce, même si, sur un plan technique, elle n'assure aucune de ces deux fonctions. **Dans de telles conditions, une entreprise vis-à-vis de ses salariés, un établissement scolaire vis-à-vis de ses élèves peuvent être considérés comme des « fournisseurs d'accès » ou des « hébergeurs » et se trouver débiteurs de l'obligation pénalement sanctionnée en cas de violation.**

C'est ce texte qui a été appliqué par la cour d'appel de Paris et qui a abouti à la condamnation de BNP Paribas.

III. Illustration de cette obligation par l'affaire BNP PARIBAS

Les faits de cette affaire

World Press Online est une agence de presse présente dans de nombreux pays. Le 8 décembre 2003, deux de ses agents, reçoivent un e-mail leur annonçant la fermeture prochaine de la société. L'information a de quoi surprendre. Elle est en fait erronée et a manifestement pour but de déstabiliser les relations de World Press Online avec ses agents.

L'adresse utilisée par l'émetteur de l'e-mail est distribuée par Yahoo! et est de type pseudo@yahoo.fr. World Press Online obtient de Yahoo! l'adresse IP du corbeau qui a créé le compte à partir duquel a été émis le message frauduleux. Cette adresse IP identifie l'ordinateur d'une banque, BNP Paribas. Pour retrouver le corbeau, il reste à World Press Online à trouver qui, à la BNP, a attribué cette adresse IP au jour et heure dits, probablement l'un de ses salariés.

Interrogée par lettre recommandée avec accusé de réception le 20 février 2004 puis par une sommation délivrée par huissier de justice le 24 juin 2004, BNP Paribas ne répond pas. World Press Online décide de saisir en procédure d'urgence (référé) le tribunal de commerce de Paris.

Le 12 octobre 2004, ce dernier fait droit à la requête et ordonne à la BNP « de répondre à la société World Press Online sous astreinte de 200 euros par jour de retard pendant trente jours passé un délai de huit jours après la signification de l'ordonnance […] en particulier de communiquer l'identité et plus généralement toute information de nature à permettre l'identification de l'expéditeur du message électronique du 8 décembre 2003 ».

En exécution de cette ordonnance, BNP Paribas adresse, le 2 novembre 2004, à World Press Online un courrier dans lequel elle indique ne pas être en mesure de dire à qui elle a attribué en interne l'adresse IP relevée par Yahoo! « dans la mesure où l'adresse IP [xxx] correspond à une machine qui concentre tous les flux de la navigation entre les postes du groupe BNP en France et pour partie à l'étranger ». BNP Paribas n'est donc pas en mesure d'aider World Press Online à identifier l'auteur du message en litige.

Par un arrêt de la Cour d'Appel de Paris du 4 Février 2005, les juges affirment :

> *« La société BNP Paribas est tenue, en application de la [Loi[10]], de détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisitions judiciaires. »*

La question posée à la justice, et à laquelle la cour d'appel de Paris répondra, est d'une portée qui dépasse le cadre de ce litige : toute entreprise, petite ou grande, a l'obligation de tracer tous les flux sortant de ses machines qui échangent en interne et avec l'extérieur.

10 article 43-9 de la loi du 1er août 2000 ancêtre de la LCEN du 21 Juin 2004 précitée

Section 4

L'archivage du contenu des messages électroniques : une obligation participant au respect de l'obligation de traçabilité

La Loi n°79-18 du 3 Janvier 1979, dite Loi sur les archives[11], définit l'archivage comme l'ensemble des actions, outils et méthodes mises en œuvre pour conserver, à moyen ou long terme, des informations dans le but de les exploiter. Cet archivage peut être électronique, la loi ne faisant pas de distinction entre les types d'archivage (papier ou électronique). La loi reconnaît même explicitement une valeur juridique au document électronique.

Il n'existe pas de sanction spécifique à la non-conservation des documents d'entreprise. En fonction des circonstances, l'entreprise peut être condamnée à des peines de nature fiscale et/ ou pénale.

En matière fiscale, l'article 1734 du Code général des impôts dispose que « *L'absence de tenue, la destruction avant les délais prescrits ou le refus de communiquer les documents soumis au droit de communication de l'administration entraîne l'application d'une amende de 1 500 euros.* »

Depuis le 1er janvier 2006, l'article 1746-1° du Code général des impôts précise que quiconque met « *les agents habilités à constater les infractions à la législation des impôts dans l'impossibilité d'accomplir leurs fonctions est puni d'une amende de 25 000 euros* » (de 75 à 7 500 euros pour les infractions antérieures au 1er janvier 2006), prononcé par le tribunal correctionnel. En cas de récidive, le tribunal peut prononcer une peine de six mois de prison.

En matière pénale, l'article 322-2 du nouveau Code pénal prévoit que la destruction, la dégradation ou la détérioration d'un registre, d'une minute ou d'un acte original de l'autorité publique est punie de trois ans d'emprisonnement et de 45 000 € d'amende.

11 Publication au JORF du 5 janvier 1979, version consolidée au 24 février 2004.

Les articles L. 441-1[12] et suivants du nouveau Code pénal sanctionnent la constitution de faux et l'usage de faux.

Si l'entreprise fait disparaître des documents comptables ou n'a pas tenu une comptabilité complète ou régulière, celle-ci peut être déclarée coupable de banqueroute dans le cadre de l'ouverture d'une procédure de redressement ou de liquidation judiciaire[13].

Enfin, l'article 1746 du Code général des impôts prévoit notamment que toute entrave à l'exercice de la mission des agents habilités à constater les infractions aux obligations légales existantes en matière fiscale est puni d'une amende de 25.000 Euros.

I. Un moyen probatoire stratégique pour l'Entreprise

Grâce à la loi du 13 mars 2000[14], une réforme en profondeur du droit de la preuve a été amorcée en portant adaptation de la preuve aux technologies de l'information. Cette Loi a redéfini la preuve littérale et a consacré **la force probante de l'écrit électronique**.

L'article 1316-3 du Code civil dispose en effet que : «*L'écrit sur support électronique a la même force probante que l'écrit sur support papier.* »

L'archivage électronique ne disqualifie donc pas l'information archivée qui est reconnue comme preuve au même titre que l'écrit établi sur support papier.

12 L'article L. 441-1 du nouveau Code pénal dispose :
« Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende. »

13 L'article 654-2 du Code de Commerce dispose :
« En cas d'ouverture d'une procédure de redressement judiciaire ou de liquidation judiciaire, sont coupables de banqueroute les personnes mentionnées à l'article L. 654-1 contre lesquelles a été relevé l'un des faits ci-après :
1° Avoir, dans l'intention d'éviter ou de retarder l'ouverture de la procédure de redressement judiciaire, soit fait des achats en vue d'une revente au-dessous du cours, soit employé des moyens ruineux pour se procurer des fonds ;
2° Avoir détourné ou dissimulé tout ou partie de l'actif du débiteur ;
3° Avoir frauduleusement augmenté le passif du débiteur ;
4° Avoir tenu une comptabilité fictive ou fait disparaître des documents comptables de l'entreprise ou de la personne morale ou s'être abstenu de tenir toute comptabilité lorsque les textes applicables en font obligation ;
5° Avoir tenu une comptabilité manifestement incomplète ou irrégulière au regard des dispositions légales. »

14 Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Pour que l'écrit numérique soit admis comme moyen de preuve, l'article 1316-1 du Code Civil dispose que : « *L'écrit sous forme électronique est admis en preuve au même titre 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*. »

Trois conditions doivent être respectées pour qu'un document électronique soit recevable comme moyen de preuve :

1. la personne dont émane l'écrit doit être dûment identifiée,
2. l'écrit doit être établi dans des conditions de nature à en garantir l'intégrité,
3. l'écrit électronique doit être conservé dans des conditions de nature à en garantir l'intégrité.

Cependant, quelle que soit la forme de la preuve, le juge conserve son pouvoir souverain d'appréciation et pourra toujours l'évincer.

C'est d'ailleurs la raison pour laquelle, une sauvegarde opérée par l'intermédiaire d'un professionnel réputé, utilisant des standards du marché, peut influencer un juge non convaincu.

Cette question de la preuve est importante puisque l'entreprise doit respecter certaines obligations légales de conservation[15].

II. L'Entreprise est tenue au respect des durées de conservation de documents fixées par la Loi

Dans une délibération du 11 octobre 2005, la Commission Nationale de l'Informatique et des Libertés (CNIL) a défini l'archivage électronique de données à caractère personnel comme *« les pratiques de conservation des données visées à l'article 2 de la Loi du 6 janvier 1978 modifiée, que celles-ci soient collectées, reçues, établies ou transformées sous forme électronique, par toute personne, service ou organisme privé dans l'exercice de son activité »* (CNIL, Délib. n° 2005-213, 11 oct. 2005 : Journal Officiel 23 Novembre 2005).

A- Des obligations légales variées en matière d'archivage

Tout d'abord, la limitation de la durée de conservation est justifiée par la volonté de préserver le principe du «droit à l'oubli» consacré par la Loi de 1978[16] et destiné à garantir que les données archivées sur les clients, fournisseurs ou salariés ne soient pas conservées, dans les entreprises, pour des durées qui pourraient apparaître comme manifestement excessives.

Par ailleurs, lorsque certaines données sont conservées, de façon légitime, sur de longues durées, il importe que les modalités pratiques de cet archivage garantissent les personnes contre, notamment, tout détournement de finalité.

Les obligations en matière de durée de conservation des documents archivés sont multiples en fonction de la nature du document invoqué à titre de preuve :

En outre, la **Loi du 21 Juin 2004**[17] a introduit dans le Code de la consommation l'article L. 134-2 qui dispose que : *« Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à [120 euros][18], le contractant professionnel assure la conservation de l'écrit qui le constate pendant [5 ans à compter de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate »] et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande. »*

Dans le cas contraire, le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de cinq ans à compter de celle-ci.

Par ailleurs, la Loi impose également la conservation des données de connexion pour les opérateurs de communication électronique (article du CPCE) mais aussi pour l'identification de toute personne ayant contribué à la création du contenu ou de l'un des contenus des services (de communications électroniques) dont on est prestataire.

---

15 La CNIL, réunie en séance plénière le 11 octobre 2005, a adopté une recommandation visant à sensibiliser les professionnels sur certaines règles générales de bonnes pratiques à mettre en œuvre.

* **Encadrer les archives courantes, intermédiaires et définitives**
* **Respecter le principe du « droit à l'oubli » (A**rticles 6-5° et 24 de la loi du 6 janvier 1978 modifiée en août 2004)
* **Eviter la « dilution » des données archivées dans le système informatique de l'entreprise (**Article 34 de la loi du 6 janvier 1978 modifiée)
* **Utiliser des procédés d'anonymisation en cas de conservation à long terme de documents d'archives**
* **Développer, dans les entreprises, des procédures formalisées**

Disponible à l'adresse suivante : http://www.cnil.fr/index.php?id=1888

16 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifiée en août 2004

17 Loi n°2004-575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique, Publication au JORF du 22 juin 2004.

18 Décret n°2005-137 du 16 Février 2005 pris pour l'application de l'article L 134-2 du code de la consommation.

❖ **pour les documents comptables :**

	Délai de conservation	Textes applicables
livres et registres comptables	10 ans à compter de la clôture du livre ou du registre	Article L.123-22 du Code de commerce
factures, bons de commande, de livraison etc.	10 ans à compter de la clôture de l'exercice comptable	Article L.123-22 du Code de commerce

❖ **pour les documents civils et commerciaux (contrats, documents bancaires etc.) :**

	Délai de conservation	Textes applicables
Contrats conclus entre commerçants et entre commerçants et non commerçants Documents établis pour le transport de marchandises Documents bancaires (relevés bancaires, talons de chèque, etc.)	5 ans	Article L. 110-4 du Code de commerce
Contrats d'acquisition et de cession de biens immobiliers et fonciers	30 ans	Article 2272 du Code civil
Correspondance commerciale (bons de commandes, bons de livraison, etc.) Factures clients et/ou fournisseurs	10 ans à compter de la clôture de l'exercice comptable	Article L. 123-22 alinéa 2 du Code de commerce

❖ **pour les documents sociaux :**

	Délai de conservation	Textes applicables
Comptes annuels (bilan, compte de résultat et annexe)	10 ans à compter de la clôture de l'exercice considéré	Article L. 123-22 alinéa 2 du Code de commerce
Convocations, feuilles de présence et pouvoirs Rapports du gérant ou du conseil d'administration Rapports des commissaires aux comptes	3 ans	Article L. 235-9 du Code de commerce
Ordres et registres de mouvements de titres	5 ans	Article 2224 du Code civil
Statuts, annexes et pièces modificatives	5 ans à compter de la radiation de la société du RCS	Article 2224 du Code civil
Registre des procès verbaux d'assemblées et/ou de conseil d'administration	5 ans à compter du dernier PV enregistré	Article 2224 du Code civil

B- Des exigences supplémentaires pour les entreprises cotées en bourse

La Loi n° 2003-706 du 1er août 2003 de sécurité financière

En France, la Loi n° 2003-706 du 1er août 2003 de sécurité financière[19] dispose que la direction

19 J.O n° 177 du 2 août 2003, page 13220.

générale doit rendre compte, dans un rapport présenté chaque année aux actionnaires lors de l'assemblée amenée à statuer sur les comptes de l'exercice, des procédures de contrôle interne mises en place au sein de l'entreprise et assurant une meilleure transparence.

La notion de contrôle interne ne fait pas l'objet d'une définition juridique.

L'Ordre des Experts Comptables français définit le contrôle interne comme l'ensemble des politiques et procédures mises en œuvre par la direction d'une entité en vue d'assurer, dans la mesure du possible, la gestion rigoureuse et efficace de ses activités. Cette définition est particulièrement large et n'est pas limitée aux informations comptables et financières.

L'archivage de l'information doit être effectué sérieusement et doit permettre de garantir :

- l'intégrité de l'information conservée et ceci pendant toute la durée de conservation, qui peut être longue puisque le Code de Commerce impose de conserver la comptabilité pendant une durée de 10 ans et le Code Général des Impôts pendant une durée de six ans. La notion d'intégrité implique que le support d'archivage ne peut admettre aucune possibilité de modification de l'enregistrement initial.

- la traçabilité de l'information, c'est-à-dire la possibilité de repérer si les informations ont été manipulées depuis leur origine et par quelles personnes.

Ces procédures impliquent notamment le respect des politiques de gestion, l'exactitude et l'exhaustivité des enregistrements comptables, ou encore l'établissement en temps voulu d'informations financières ou comptables fiables. Le contrôle interne général doit être accompagné d'un contrôle interne informatique.

Au regard de la mise en œuvre des procédures de contrôle interne et afin de contrôler la pertinence de l'information financière communiquée, l'entreprise générique doit être en mesure de disposer de moyens pertinents en termes d'archivage et de recherche de l'information. En effet, l'archivage, lorsqu'il est effectué dans certaines conditions, est un moyen de vérifier que les informations comptables, financières et de gestion communiquées aux organes sociaux de la société reflètent avec sincérité l'activité et la situation de la société.

III. Les recommandations de la CNIL en matière d'archivage

Dans sa recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel, la CNIL rappelle que les responsables de traitements doivent mettre en œuvre les mesures techniques et d'organisation adéquates pour protéger les données archivées notamment contre la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite.

A cet égard, la CNIL recommande un encadrement des archives et notamment que :

- **l'accès aux archives intermédiaires**[20] soit limité à un service spécifique (par exemple un service du contentieux) et qu'il soit procédé, *a minima*, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations).
- les **archives définitives** soient conservées sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives (par exemple la direction des archives de l'entreprise).

Elle recommande de mettre en œuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées ainsi que de mettre en oeuvre des dispositifs de traçabilité des consultations des données archivées.

Elle recommande enfin que les entreprises définissent, dans le cadre de procédures formalisées, des règles d'archivage répondant à l'ensemble des préconisations précitées et qu'une information puisse être fournie à la demande exprimée par les personnes faisant l'objet des traitements archivés (V. CNIL, Délib. préc. n° 45).

20 La CNIL, dans sa Délibération n° 2005-213, 11 oct. 2005, Journal Officiel 23 - Novembre 2005, a donné sa propre définition des archives courantes, intermédiaires et définitives.

- doivent être considérées comme «courantes», les archives constituées par les données d'utilisation courante par les services concernés dans les entreprises, organismes ou établissements privés (par exemple : les données concernant un client dans le cadre de l'exécution d'un contrat) ;
- doivent être considérées comme «intermédiaires» les archives constituées par les données qui présentent encore pour les services concernés un intérêt administratif, comme par exemple en cas de contentieux, et dont les durées de conservation sont fixées par les règles de prescription applicables ;
- doivent être considérées comme «définitives» les archives constituées par les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction (V. CNIL, Délib. préc.).

Section 5

Les bonnes pratiques en matière de traçabilité et d'archivage électronique

La première recommandation à suivre pour toutes les entreprises Françaises est de se conformer à la Loi Française : or comme nous l'avons vu, toute entreprise offrant des services « on line » et utilisant des messageries électroniques pour ses collaborateurs, a l'obligation de recourir à la pratique de la traçabilité et de l'archivage électronique**.**

Nous recensons ci-après les quelques bonnes pratiques minimales qui nous semblent s'imposer en ce domaine:

Pour la Direction Informatique

- Mettre en place des outils techniques de contrôle des flux entrants et sortants de l'entreprise par la messagerie électronique.
- Mettre en place des outils techniques de contrôle des flux entrants et sortants de l'entreprise par les autres applications (serveur web, etc.) de l'entreprise accédant au réseau internet.
- Faire le choix d'outils techniques qui soient basés sur les standards du marché et recourir à des prestataires sérieux et pérennes, disposant de références.
- Conserver les traces des flux sur un support non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'information (par exemple la direction ou le service juridique).
- Procéder à la conservation de toutes données techniques transitant par les serveurs de l'entreprise en précédant cette procédure des mesures d'information et de recueil d'avis précités.

Pour la Direction Générale / Direction Juridique / Direction Ressources Humaines

- Préalablement à la mise en place des outils, informer les salariés de ce contrôle par voie d'affichage, sur les lieux d'affichage obligatoires et / ou par note de services – justifier le recours à ce contrôle, notamment par le risque juridique occasionné par ces flux pour l'entreprise.
- Recueillir l'avis des représentants du personnel sur ce contrôle.
- Déclarer à la CNIL le traitement consécutif à la collecte de données à caractère personnel dans le cadre de ce contrôle.
- Etablir une charte d'usage Internet encore appelée Charte informatique ou Code de bonne conduite ou autre, rédigée en coopération avec les personnes concernées dans l'entreprise, interdisant l'usage personnel des outils mis à disposition par l'entreprise, logiciels de messagerie et de navigation, accès Internet, notamment. La Charte comportera une première partie didactique, rappelant l'obligation de respecter les droits de l'entreprise, les droits des tiers, l'ordre public.
- Se tenir informé des lois, des décrets et des recommandations de la CNIL afin d'actualiser les outils et les mesures mises en place pour garantir la conformité des systèmes en fonction des évolutions.

Témoignage client

« L'exigence de traçabilité, qu'elle découle de la loi ou même simplement du bon sens, correspond au besoin plus global de la préconstitution de la preuve. La solution fournie par Cooperteam nous accompagne dans la gestion de cette preuve, et nous permet de garantir à la fois son intégrité et sa légalité; le choix de cette solution s'imposait donc de lui-même … »

Monsieur Sylvain Lebarbier

Chargé de mission - Conformité et Déontologie – AG2R

CHIFFRES CLÉS 2007

- Plus de 4 000 collaborateurs en France

- 8,40 milliards d'euros de CA

- 889 millions d'euros d'affaires nouvelles

MÉTIERS

1er assureur paritaire de personnes en France, 3 métiers caractérisent AG2R :

- la retraite complémentaire

- la protection des personnes

- l'épargne-retraite et l'épargne salariale.

ENJEU DU PROJET

Conserver les traces des échanges effectués par l'intermédiaire du système de messagerie électronique Lotus Domino

Ces traces doivent être juridiquement opposables

BÉNÉFICES

Traçabilité des flux de messagerie

- Gestion de la non-répudiabilité

- Impact minimal sur les serveurs de messagerie

- Stockage sécurisé des traces de la messagerie

Créé en 1951, AG2R est un acteur majeur de l'économie sociale et le premier assureur paritaire de personnes en France.

CONTEXTE DU PROJET

Le sens de l'Histoire numérique est celui d'une responsabilisation croissante des personnes morales et de leurs représentants, impliquant un besoin de traçabilité sans cesse renforcé. Les lois impactant cette responsabilité (Perben 2, LCEN…) combinées à la jurisprudence récente ont ainsi dû être rapidement prises en compte par AG2R.

De nouveaux risques ont en effet émergé de ce cadre légal, obligeant notamment tout organisme à conserver les traces générées par les services de communication en ligne dont il est considéré comme prestataire.

Dans ce contexte, AG2R a souhaité s'appuyer sur une solution de collecte des traces de tous les messages électroniques reçus et envoyés par le biais du système de messagerie IBM Lotus Notes Domino, cette opération devant permettre de conserver les informations exigées par la loi tout en garantissant le caractère incontestable de leur légalité.

Cette démarche ne pouvait par ailleurs être envisagée qu'à la condition expresse qu'elle ne soit pas susceptible de porter atteinte aux droits des utilisateurs, et que seules soient traitées les informations strictement nécessaires à l'application de la loi.

Mise en œuvre du projet

Après avoir reconnu la nécessité de mettre en œuvre une solution pérenne de traçabilité des échanges électroniques, AG2R a cherché à évaluer toutes les offres techniques disponibles afin de choisir la meilleure solution, l'objectif étant d'implémenter la solution de traçabilité la plus fiable et la plus sûre tout en garantissant un impact minimal sur ses serveurs de messagerie Domino.

Pour atteindre cet objectif **AG2R** a réalisé une étude technique et financière des solutions disponibles sur le marché.

Après analyse technique, le premier scénario a été écarté, AG2R souhaitant s'appuyer sur un outil ergonomique de restitution et d'exploitation des logs, plutôt que sur les outils natifs de Lotus Notes Domino.

L'étude reposait sur les deux scénarios suivants : la mise en place de la solution native de Lotus Notes Domino (journaling) ou l'utilisation de solutions tierces du marché.

Pour le deuxième scénario quatre solutions tierces du marché, dont la solution **Cooperteam,** ont été analysées et comparées sur des critères fonctionnels et techniques, l'offre de support et de prestation d'assistance ayant été également considérée. L'étude a distingué la solution de traçabilité des flux fournie par **Cooperteam** comme la seule solution répondant aux besoins d'AG2R : garantir la traçabilité des échanges en offrant les avantages suivants :

- ✓ Charge serveur très réduite et fiabilité technique de la solution.
- ✓ Sécurité accrue grâce à un stockage des informations sur un serveur hébergé à l'extérieur de la société.
- ✓ Taille réduite des données stockées (3Go/an pour 50 000 mail/j).
- ✓ Informations complètes, statistiques immédiates et modules de requête très performant.

La solution a été acquise auprès de COOPERTEAM et implémentée au cours du premier trimestre de l'année 2007, permettant à AG2R de remplir ses objectifs :

- Anticiper les risques de mise en cause de sa responsabilité en garantissant la traçabilité de tous les échanges électroniques réalisés à travers la messagerie Lotus Notes Domino.
- Démontrer que les traces ont été conservées dans des conditions assurant qu'elles sont restées intègres depuis leur production, en les externalisant chez un hébergeur tiers.

Edité par

COOPERTEAM

14 Avenue de l'Opéra
75001 Paris

Information :
+ 33 (0)4 97 13 87 00

info@cooperteam.com
www.cooperteam.fr

Corporate **Messaging** Management