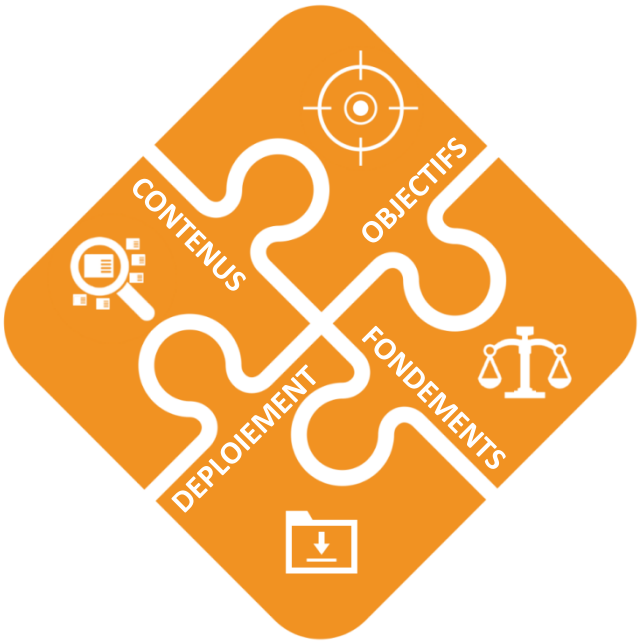
Olfeo France

LE GUIDE DE LA CHARTE

DES SYSTEMES D'INFORMATION

Co-écrit avec le cabinet d'avocats

Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées



Sommaire

Ce guide a pour objectif d'aider les directions informatiques dans l'élaboration de leur Charte des systèmes d'information, souvent appelée de manière générique « Charte informatique ».

Olfeo ne peut en aucun cas fournir une Charte informatique type à personnaliser dans la mesure où il n'existe pas de Charte type de par la diversité des entreprises.

Il s'agit donc ici d'aborder pourquoi et comment mettre en œuvre une Charte, les lignes directrices de son contenu, et quelles sont les éléments à mettre en œuvre pour qu'elle soit juridiquement opposable aux utilisateurs.

Le Guide de la Charte Informatique Olfeo a été co-écrit avec le cabinet d'avocats Alain Bensoussan. Le cabinet Alain Bensoussan Avocats assiste ses clients depuis 1978 dans le domaine du droit de l'informatique.

Deux avocats spécialisés dans le Droit des technologies du cabinet d'avocats Alain Bensoussan ont participé à ce guide : **Maître Polyanna Bigle**, Avocate et Directeur du Département Sécurité des Systèmes d'Information et Dématérialisation et **Maître Eric Barbry**, Avocat et Directeur du pôle Droit Numérique.

I. CHAPITRE 1 : LA DEMARCHE DE LA CHARTE

Cette première partie a pour objectif de comprendre pourquoi, aujourd'hui, il est nécessaire de mettre en place une Charte informatique.

I.1 QU'EST-CE QU'UNE CHARTE INFORMATIQUE ?

La Charte informatique définit les conditions générales d'utilisation du système d'information et de communication et notamment des accès Internet, des réseaux et des services multimédias au sein d'une entreprise ou d'une administration.

Ainsi, le terme « système d'information » englobe les systèmes informatiques et les moyens de télécommunications.

Ce document recense l'ensemble et, par là même, leurs droits. Sa mise en place permet d'éviter toute forme d'abus de l'usage des outils informatiques et constitue une règle de référence en cas de conflit si elle est correctement déployée.

In fine, l'objectif est, pour un établissement public ou privé, d'optimiser la gestion technique du matériel et du système d'information au sens large, et par là même sa gestion financière, mais également d'apporter de la sécurité juridique et technique au système d'information et aux données qui y sont contenues.

Enfin, la Charte permet d'informer les utilisateurs de la collecte de leurs données à caractère personnel pour les besoins du système d'information et de la mise en œuvre des outils informatiques en application de :

- **L'article L.1222-4 du Code de travail** qui dispose que :

> *« Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance »*

- **Loi Informatique et Libertés** qui dispose au nom du principe de Transparence que :

> *« La loi garantit aux personnes l'information nécessaire relative aux traitements auxquels sont soumises des données les concernant et les assure de la possibilité d'un contrôle personnel. Le responsable du traitement de données personnelles doit avertir ces personnes dès la collecte des données et en cas de transmission de ces données à des tiers. »*

I.2 LES FONDEMENTS JURIDIQUES D'ADOPTION D'UNE CHARTE

I.2.a RAISON N°1 : INFORMER LES UTILISATEURS CONFORMEMENT A LA LOI

La Charte informatique doit être adoptée principalement pour informer les utilisateurs et les sensibiliser aux enjeux liés au système d'information.
Les autorités comme l'Anssi (Agence Nationale pour la sécurité des Systèmes d'information ou la Cnil, (Commission Nationale de l'Informatique et des Libertés), recommandent l'adoption d'une Charte informatique dans le but de :

> *« Sensibiliser les salariés ou les agents publics aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration »*[1].

Les règlements intérieurs et les contrats de travail ne se suffisent plus à eux-mêmes.

D'autre part, si l'établissement public ou privé collecte des données à caractère personnel, les utilisateurs doivent en être informés dès la mise en place d'un outil de contrôle ou de surveillance, notamment un outil de filtrage.
Cette information porte sur les traitements réalisés des données à caractère personnel, sur les modalités d'accès à Internet ou d'utilisation des réseaux sociaux, sur les

[1] Rapport de la Cnil sur la cybersurveillance, édition mars 2004 : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/044000175/0000.pdf

éventuelles sanctions en cas de non-respect des règles déterminées dans la Charte.

I.2.b RAISON N°2 : RESPONSABILISER L'EMPLOYEUR ET L'EMPLOYE ET LIMITER LEUR RESPONSABILITE

L'employeur a la responsabilité du bien-être de ses employés. Mais il en a également la responsabilité notamment du fait des moyens qu'il met à leur disposition.
Ainsi, un employeur pourrait être responsable des faits causés par ses salariés, même par négligence, imposant la mise en place de moyens pour éviter les dérives et les dommages.

- **L'article 1383 du Code civil** prévoit en effet que :

> *« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »*

- **L'article 1384 du Code civil** pose la responsabilité spécifique des employeurs du fait de leurs employés :

> *« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre […] les maîtres et les commettants du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés »*

- **L'article 121-2 du Code pénal** prévoit la responsabilité des personnes morales responsables de leurs employés :

> *« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.*
>
> *Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.*
>
> *La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3 ».*

La jurisprudence[2] condamne le libéralisme excessif de l'employeur, sur le fondement de la responsabilité des « commettants du fait des préposés[3], » lui imposant la réparation des dommages causés aux tiers par ses salariés au moyen des outils de communications électroniques mis à leur disposition.

Toutefois, la Charte doit obéir au principe de proportionnalité[4] qui s'applique en matière de restrictions aux libertés individuelles ou collectives, ainsi qu'il a été jugé

[2] CA Aix en Provence, 2ème ch., 13 mars 2006, Lucent Technologies c/ Escota, Lycos France et autre.
[3] Code civil, art. 1384 al. 5.
[4] Code du travail art. L1321-3.

par les juridictions judiciaires ou administratives à propos des règlements intérieurs.

Il est donc plus que nécessaire d'organiser la responsabilité de l'employeur en le responsabilisant et de lui donner, dans le même temps, les moyens de preuve de sa diligence, de l'information de ses employés sur les bonnes utilisations des moyens informatiques et de communication.

I.2.c Raison n°3 : Repondre a des exigences non prevues par la loi

Tous les usages ne sont pas interdits par les dispositions légales ou réglementaires, bien au contraire. Dès lors, la Charte informatique s'impose comme la meilleure façon de répondre à des exigences de l'entreprise ou de l'établissement.

Il s'agira par exemple, de l'interdiction de la visualisation ou du téléchargement de contenus érotiques, pornographiques ou même humoristiques car cela serait contraire à l'éthique de l'entreprise ou de l'établissement, de l'interdiction de transmettre ses codes d'accès à un tiers, même à l'administrateur, car cela engendrerait une forte insécurité pour le système, ou encore de l'interdiction de regarder sur Internet des chaînes de télévision ou d'écouter la radio car ces pratiques sont consommatrices de bande passante.

I.2.d RAISON N°4 : UNE BONNE PRATIQUE ADMISE PAR TOUS

Aujourd'hui, la majorité des établissements privés et publics ont une Charte informatique et cela engendre forcément un impact juridique. Étant donné que 80% des établissements disposent aujourd'hui d'une Charte, il pourra être reproché de ne pas avoir mis en œuvre cette bonne pratique.
On trouve le mot « Charte » dans les cas de jurisprudence, les établissements privés et publics utilisant ce terme pour qualifier ce document.

On peut notamment citer les cas des entreprises AIS 2, Zetès France, ou encore Coca-Cola™ :

- **Le cas de jurisprudence AIS2**[5]

Mme X, employée en qualité de responsable d'agence au sein de l'entreprise AIS 2 a été licenciée pour faute grave le 25 octobre 2010. La salariée passait plus d'une heure par jour sur Internet pour son usage personnel, violant ainsi le règlement intérieur et la Charte informatique en place dans l'entreprise.

Le règlement intérieur précisait que les matériels informatiques, leurs supports et logiciels, ainsi que les accès intranet et internet mis à la disposition du personnel devaient être utilisés conformément à leur objet et aux besoins de la fonction. La Charte informatique indiquait quant à elle que l'usage abusif de l'Intranet et/ou de l'accès à Internet à des fins personnelles notamment l'accès à des sites de rencontre,

[5] CA Aix en Provence, ch. 17, 13-01-2015, Mme X / AIS 2.

shopping, jeux en ligne à plusieurs joueurs relevait « d'agissements proscrits ».

La Cour d'appel d'Aix en Provence a relevé que le comportement de la salariée caractérisait une violation délibérée et répétée de la Charte informatique en vigueur au sein de son entreprise.

- **Le cas de jurisprudence Zetes France™[6]** :

En 2007, la société Zetes France a licencié un de ses collaborateurs suite à la découverte de l'installation de logiciels sur le poste de travail de celui-ci, ce qui était formellement interdit par la Charte informatique de l'entreprise.

La Cour d'appel de Paris a relevé que le salarié avait procédé à un usage anormal de l'outil informatique qui lui était confié, nuisant au bon fonctionnement du système, et ne respectant pas la Charte informatique.

Dans ces deux cas, une Charte informatique avait été déployée comme un règlement intérieur et a donc été reconnue juridiquement opposable aux salariés.

- **Le cas de jurisprudence Coca-Cola France™[7] :**

M. X, employé de la société Coca-Cola comme délégué commercial, a été licencié pour faute grave le 10 août 2004 en raison de la découverte sur son ordinateur portable de 480 fichiers à caractère pornographique.

[6] CA Paris, pôle 6 ch. 5, 19-1-2012 RG n° 07/01754, M. X. c/ SAS Zetes France.
[7] Cass. soc., 15-12-2010, n° 09-42.691, M. X. c/ Coca-Cola.

Suite à une opération de maintenance sur son ordinateur, il a été découvert que M. X avait utilisé sa messagerie professionnelle pour la réception et l'envoi de documents à caractère pornographique et avait conservé, sur son disque dur, un nombre conséquent de tels fichiers, ce qui constitue un manquement délibéré et répété du salarié à l'interdiction posée par la Charte informatique mise en place dans l'entreprise et intégrée au règlement intérieur, de détenir de tels fichiers.

La Cour a estimé que le fait de détenir et d'envoyer des fichiers à caractère pornographique en violation des dispositions de la Charte informatique mise en place, était constitutif d'une cause réelle et sérieuse du licenciement de l'employé.

I.3 LE MECANISME DE LA CHARTE

Une Charte s'inscrit dans une démarche d'explication et de sensibilisation quant aux enjeux et aux risques. L'objectif est de faire adhérer les utilisateurs. Il faut donc que la Charte soit claire et à la portée de tous.

Pour mettre en place une Charte pertinente, voici le mécanisme à maîtriser :

- La connaissance des risques,
- L'apprentissage de la problématique,
- La responsabilisation des acteurs,
- Définir des moyens techniques,
- Mettre en place une politique de contrôle et d'audit,
- Et enfin pouvoir de sanctionner.

Il s'agit de définir une politique cohérente entre réalité technique et politique des ressources humaines afin de maîtriser l'ensemble des risques.

C'est d'ailleurs la réelle raison d'être d'une Charte. Cette Charte doit être déployée en annexe du règlement intérieur si le souhait de l'entreprise est de contrôler et de sanctionner les collaborateurs.

II. CHAPITRE 2 : LE CONTENU DE LA CHARTE

La Charte doit obéir au principe de proportionnalité[8] qui s'applique en matière de restrictions aux libertés individuelles ou collectives. Cela signifie proportionnel à un but recherché.

Ce principe est à manier avec précaution, in concreto notamment en fonction du secteur d'activité concerné et des tâches et missions confiées dans, par exemple, un établissement financier, établissement médical ou entreprise de textile.

Ainsi, un certain nombre de thèmes devront être traités comme, par exemple, le contrôle et l'audit de l'employeur de l'activité des utilisateurs, la vie privée résiduelle, le filtrage, l'image de marque ou les responsabilités.

En outre, la Cour de cassation a posé le principe du droit à la vie privée résiduelle qui contraint l'employeur à organiser un savant équilibre entre les libertés individuelles du personnel au sein de l'entreprise et son pouvoir hiérarchique et disciplinaire.

Nous allons traiter, dans ce guide de Charte quelques aspects précis à aborder dans la Charte informatique.

[8] Code du travail art. L1321-3.

II.1 ZOOM : EQUILIBRE VIE PRIVEE RESIDUELLE / DROIT DU TRAVAIL

La Cour de cassation, avec l'arrêt Nikon du 2 octobre 2001[9], est venue préciser qu'un employeur ne pouvait pas interdire à ses salariés ou agents d'utiliser les outils mis à leur disposition par l'employeur à des fins personnelles.
La Charte doit donc définir avec précision la frontière entre l'utilisation professionnelle et l'usage privé résiduel. Toute règle qui viserait à interdire purement et simplement l'utilisation privée des outils informatiques et d'Internet entraînerait la nullité même de la Charte ou en tout cas en obèrerait gravement l'opposabilité.

A l'inverse tout n'est pas permis ou possible pour l'utilisateur et il est normal pour l'employeur, maître de son système d'information d'en définir les règles.

Ainsi, l'employeur est en droit de limiter et d'encadrer les conditions d'utilisation à des fins personnelles de moyens de communication professionnels. L'usage personnel doit dans tous les cas être limité à des usages « socialement admis ».

La jurisprudence est venue préciser le périmètre de la vie privée résiduelle en la limitant à quatre attributs spécifiques que sont la vie sentimentale, la santé, la vie sexuelle et la vie financière[10].

[9] Cass. soc. 2-10-2001, n°99-42942 - « Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; que celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».
[10] CA Rennes, 3ème Chambre des Appels Correctionnels, 14-01-2010, n° 08-02209.

Il s'agit par exemple de décrire des contextes socialement admis (appeler l'école si un enfant est malade, faire une déclaration à son assurance suite à un accident…) et ce qui ne l'est pas : on peut interdire ici l'utilisation de l'adresse e-mail professionnelle sur Internet.

Cependant, le droit à une vie privée résiduelle et l'utilisation par le salarié ou l'agent des moyens de communication mis à la disposition de l'employeur, telle que l'adresse email professionnelle, pour accomplir ses obligations légalement admissibles ont des limites. Ainsi, il a été jugé par la Cour de cassation[11] que n'est pas admissible le fait, pour un salarié, d'utiliser sa messagerie électronique professionnelle afin de tenir des propos antisémites et constitue une faute grave.

Afin que les documents, e-mail, fichiers et autres supports aient un caractère privé opposable à l'employeur, il revient à l'utilisateur de les identifier comme privé (en utilisant le terme « privé ») aussi bien pour les éléments stockés que les courriers électroniques entrants ou sortants.

Il faut spécifier également que la « zone privative », ne veut pas dire que l'employé a le droit de tout y faire.

Heureusement l'établissement public ou privé peut contrôler ces zones privées et particulièrement le DSI, les administrateurs… L'employeur a le droit d'avoir accès aux fichiers, documents ou adresses électroniques identifiés comme « privé » si l'utilisateur est présent ou en cas d'absence s'il a été dument appelé et ce en cas de risque particulier notamment de sécurité, de continuité de service, ou d'un risque grave de voir sa responsabilité engagée[12].

[11] Cass, soc, 02-06 2004, n° 03-45269.
[12] Cass. soc., 17-05-2005, n°03-40017.

Encore faut-il le préciser dans la Charte informatique et surtout avoir la preuve que l'activité d'un salarié dans sa zone privée met en cause la bonne marche du système d'information en cas de litige.

II.2 ZOOM : IMAGE DE MARQUE / RESEAUX SOCIAUX

Concernant les réseaux sociaux, la jurisprudence est encore très indécise, mais il apparaît tout de même que les utilisateurs se doivent d'adopter un comportement loyal vis à vis de leur employeur lors de l'utilisation des réseaux sociaux, que ces réseaux sociaux soient professionnels (Linkedin, Viadéo ou autre) ou non professionnels (Facebook, Pinterest, Twitter).

Il a ainsi été jugé que le fait de publier des informations préjudiciables à son employeur sur un blog constituait un manquement à son obligation de loyauté. Cette solution est applicable lors de l'utilisation des réseaux sociaux par les salariés ou par les utilisateurs de système d'information au sens large, vis à vis de l'entité qui met à leur disposition des moyens informatiques[13].

Le 17 janvier 2012, la 17ème chambre correctionnelle de Paris, a considéré qu'un salarié s'était rendu coupable d'injure publique pour avoir publié sur le profil Facebook d'une représentation syndicale présente dans son entreprise, estimant que «les expressions utilisées excédaient les limites

[13] CA Besançon, 15-11-2011, n° 10-02642

de la critique admissible, y compris lorsqu'elle s'exerce dans un cadre syndical»[14].

L'établissement public ou privé devra ici se positionner quant à sa visibilité sur les réseaux sociaux. Il convient d'aborder ici les risques par rapport à l'image, l'e-réputation, la concurrence déloyale… Ainsi, doivent être ici précisées les **interdictions de communication sur et au nom de l'établissement, aussi bien dans la sphère privée,** dans le respect du principe de la liberté d'expression, **que professionnelle**, et la possibilité d'effectuer des signalements d'éventuels abus de la part d'un tiers.

II.3 ZOOM : MOBILITE ET BYOD

Les modes d'utilisation des outils au bureau sont en pleine révolution. Il ne s'agit plus seulement d'utiliser des infrastructures informatiques dans les bâtiments de l'entreprise.

L'entreprise doit prendre en considération les nouveaux usages mobiles : ordinateurs portables, smartphones, tablettes, télétravail. Ces nouveaux usages nécessitent une adaptation des règles et usages traditionnels, notamment au regard des problématiques de sécurité et de la confidentialité des données échangées.

A la marge de ces évolutions d'usage est né le « BYOD » (« Bring your own device » ou en français « Apportez vos appareils personnels »). Il s'agit pour un salarié d'utiliser un appareil personnel dans le cadre professionnel. Le BYOD

[14] TGI Paris, 17-01-2012, n° 1034008388

concerne davantage les appareils nomades que non nomades.

La décision d'accepter ou non le BYOD au sein de l'entreprise appartient à l'employeur. En revanche il ne peut l'imposer.

En effet, selon l'article L.4121-1 du Code du Travail, l'employeur a l'obligation de fournir à ses employés les moyens adaptés et nécessaires à l'exécution de leurs tâches professionnelles.

Si l'entreprise fait le choix de ne pas l'accepter, alors il est recommandé en tout état de cause d'indiquer dans la Charte informatique que le recours au BYOD est interdit et de prévoir les sanctions en cas d'infraction à cette règle (« BYOD » sauvage dans l'hypothèse où un salarié mettrait par exemple sa carte SIM professionnelle dans son téléphone personnel).

Si l'entreprise l'accepte alors la Charte informatique devra être amendée. Cette Charte, ou un document spécifique, devra définir les règles d'usage, d'acceptation et de sortie du BYOD. Ces règles peuvent figurer dans la Charte si le BYOD est accessible à tous les salariés. Si le byod est réservé à une certaine catégorie (par exemple l'encadrement) alors les règles devront être précisées dans un document spécifique.

Dès lors que l'employeur l'autorise, il peut imposer aux salariés la mise en place de moyens de sécurité concernant les données et applications professionnelles. Ceux-ci doivent néanmoins respecter la vie privée des employés qui utilisent des équipements personnels dans le cadre de leur activité professionnelle. D'un point de vue sécurité des informations professionnelles, il paraît donc nécessaire que l'utilisateur

accepte d'ajouter des solutions de sécurisation sur son système informatique.

En outre, l'employeur doit définir les conditions de contrôle sur toutes les données professionnelles qui sont utilisées par le salarié sur son système informatique personnel, utilisé pour son travail, afin d'éviter que la confidentialité des informations sensibles de l'entreprise soit menacée.

Afin d'assurer une sécurité maximale pour les systèmes d'information de l'entreprise, les responsables des systèmes informatiques pourront procéder aux actions suivantes :

- Limiter à certaines catégories de personnes uniquement le « droit » au BYOD
- Limiter le nombre ou le type de terminaux accessibles au BYOD
- Limiter le nombre ou le type d'usages
- Imposer des mesures ou applications particulières tel que le MDM ou une application de sécurité
- Imposer la mise en place d'un contrôle de la partie professionnelle du terminal
- Définir les règles d'utilisation du BYOD
- Définir le processus à suivre pour bénéficier du BYOD

II.4 ZOOM : FLUX SECURISES

La problématique des flux (entrants ou sortants) est devenue une question prioritaire pour l'entreprise et singulièrement pour la direction des systèmes d'information.

On peut distinguer les flux sécurisés des flux non sécurisés. Pour les flux non sécurisés, il n'existe de limites à leur analyse

et à leur contrôle que celles relevant d'une violation de la vie privée. Encore faudrait-il être capable, notamment sur les accès internet, de distinguer les accès professionnels des accès personnels.

La Cour de cassation estime d'ailleurs que les connexions internet d'un salarié sont présumées être professionnelles. De fait l'employeur peut les contrôler hors la présence du salarié.

La question est plus complexe s'agissant des flux sécurisés. Ces flux sécurisés (https) sont de plus en plus nombreux. Ils posent une question particulière dans la mesure où ces flux sont cryptés et que le contrôle desdits flux nécessite une intervention de déchiffrement/rechiffrement.
L'entreprise peut-elle déchiffrer les flux sécurisés sur son réseau ? Dans quelle mesure le chiffrement/déchiffrement est-il encadré ?

La Cnil a annoncé sa position en mars 2015[15] et l'ANSSI a publié une recommandation[16] en la matière.

Pour la Cnil, « ce déchiffrement est légitime du fait que l'employeur doit assurer la sécurité de son système d'information », mais il doit l'encadrer.

L'ANSSI considère que « l'employeur est légitime à déchiffrer les contenus de flux chiffrés transitant sur les postes de travail de ses salariés, mais uniquement de façon encadrée en raison des risques juridiques liés au déchiffrement ». Cette

[15] Cnil, Analyse de flux https : bonnes pratiques et questions

[16] ANSSI, Note technique - Recommandations de sécurité concernant l'analyse des flux HTTPS, 9 10 2014

position est justifiée du fait que l'employeur pourrait voir sa responsabilité engagée d'une part « en raison d'agissements délictueux qui pourraient être commis par les salariés grâce aux moyens qu'il leur a fournis (matériels, accès internet, etc.) et dissimulés grâce au chiffrement » et d'autre part « en raison du non-respect d'obligations liées à la sécurité (des données, de l'accès à Internet, etc.) ».

Les flux chiffrés qui appartiennent à l'entreprise peuvent être décryptés.

Les flux privés échangés sur le réseau de l'entreprise n'appartiennent pas à l'entreprise (par exemple banque ou Webmail). Le déchiffrement des flux sécurisés vers les webmails est interdit. Si l'entreprise ne souhaite pas que son salarié accède à son webmail, alors cette interdiction doit être prévue dans la Charte.

II.5 ZOOM : CONTROLE ET AUDIT DE L'EMPLOYEUR

Le Code du travail permet à un employeur de contrôler l'activité de son employé et notamment le respect des temps et conditions de travail. Mais il impose que l'employé soit préalablement informé de l'existence d'opérations de contrôle et surtout que le non-respect de ces règles peut aboutir à une sanction.

Il ne s'agit ni d'une information individuelle, ni d'une information détaillée sur les conditions de contrôle et encore moins une obligation d'avertir ledit employé avant le contrôle ; mais il s'agit d'une règle générale d'information, portée à l'attention de tous, que les conditions d'utilisation

du système d'information feront l'objet de contrôles qui eux-mêmes pourront aboutir à des sanctions.

La Cour de Cassation opère une distinction entre un système de contrôle et un audit, le premier ne pouvant être instauré qu'après information et consultation des institutions représentatives du personnel tandis que le second, qui a pour finalité d'apprécier, à un moment donné, l'organisation d'un service afin, par exemple, de faire des propositions d'amélioration d'un service ou pour optimiser son organisation, ne nécessite pas d'information et de consultation préalable des organes représentatifs[17].

L'objectif d'un audit est d'identifier les non-conformités qui pourraient mettre en danger l'entreprise et lui permettre de prendre les mesures correctives appropriées. L'audit se distingue du contrôle car il ne s'agit, à proprement parler, de vérifier la conformité ou non de tel ou tel utilisateur aux règles fixées par l'entreprise mais de réaliser une photographie plus générale, une appréciation d'ensemble de l'usage des systèmes d'information par les utilisateurs. L'audit est surtout destiné à optimiser ces usages alors que le contrôle est destiné à identifier l'existence ou non d'un écart ou d'une faute de l'utilisateur.
Les règles de l'audit sont souvent fixées par la direction de la qualité lorsqu'il en existe une et dictées par les certifications dont dispose l'entreprise.

Les règles du contrôle sont malheureusement souvent inexistantes. Elles n'ont pas à figurer dans la Charte des systèmes d'information. La Charte doit comporter une disposition relative au droit de contrôle mais n'a pas pour

[17] Cass. soc. , 12-07-2010, n° 09-66369.

vocation à expliciter les modalités de ce contrôle. En effet, ces modalités de contrôle ne relèvent que de la seule responsabilité de la direction générale, de la direction des ressources humaines et de la direction des systèmes d'information.

Pour un contrôle optimum, il est important qu'au-delà de la Charte, l'entreprise puisse disposer de deux autres outils que sont :

- Le guide des opérations de contrôle ;
- La charte administrateur (voir chapitre 3).

S'agissant plus précisément du guide des opérations de contrôle, son objectif est de fixer en interne les règles de ce type d'opérations et répondra à des questions aussi pratiques que :

- Qui a le droit de déclencher les contrôles ?
- Qui peut réaliser les contrôles ?
- La personne contrôlée doit-elle être présente et/ou prévenue ?
- Une entreprise peut-elle réaliser un contrôle à distance ?
- Quels types de preuve une entreprise doit-elle conserver et en quelles unités ?
- A quel moment une entreprise fait-elle appel à un huissier ?
- Faut-il prévenir la police ?
- A quel moment une entreprise doit-elle recourir à un juge ?

II.6 CE QUI EST A BANNIR

Une Charte « techno-captive » est à bannir. Pourquoi ?

Il s'agirait d'une Charte comprenant un ensemble de technologies, logiciels, et modes d'emploi techniques. En effet, à la vitesse de leurs évolutions, la Charte serait vite dépassée, imposant une mise à jour régulière. Or, cela signifie que son déploiement devrait être renouvelé à chaque nouvelle technologie qui imposerait une modification de la Charte.

De même, une **Charte « rappel de la loi »** est à bannir. Pourquoi ?

Il s'agirait de faire de la Charte un recueil de textes ou de dispositions légales. Or, d'une part, les dispositions légales impératives s'imposent à l'utilisateur même en l'absence de Charte.

D'autre part, une Charte « rappel de la loi » pourrait elle aussi se retrouver vite dépassée par l'évolution législative et réglementaire. Or, toute modification de la Charte imposerait ici aussi la mise en œuvre du processus de déploiement de la Charte modifiée.

III. CHAPITRE 3 : LE DEPLOIEMENT DE LA CHARTE

Ce document est destiné à être diffusé auprès de tous les utilisateurs des ressources informatiques.

III.1 L'OPPOSABILITE JURIDIQUE DE LA CHARTE INFORMATIQUE

Pour être opposable aux salariés, la Charte doit être déployée de la même manière qu'un règlement intérieur, dans le respect du code du travail.

Le Droit français établit clairement qu'une Charte déployée comme un règlement intérieur est considérée comme un règlement intérieur. Ce document s'impose donc à tous les utilisateurs soumis au règlement intérieur.

III.1.a LE PRINCIPE DE DISCUSSION COLLECTIVE

Il s'agit de soumettre la Charte aux instances représentatives du personnel (article L1321-4 du Code du travail). (Comité d'entreprise, le Comité technique, ou à défaut le délégué du personnel, ainsi qu'à l'avis du Comité d'hygiène et de sécurité).

Dans le secteur privé, l'article L2323-13 du Code du travail prévoit que un mois avant la consultation, les membres du Comité d'entreprise doivent avoir reçu les éléments d'information sur le projet et ses conséquences sur les conditions de travail, afin qu'ils puissent émettre un avis éclairé sur ce document.

Le dossier de présentation au Comité d'entreprise abordera notamment les fondements législatifs et jurisprudentiels de la Charte informatique, son champ d'application, ses principes, ainsi que son déploiement.

Le comité d'entreprise est consulté sur les aspects « organisation du travail » (article L. 2323-6 du Code du travail) et le CHSCT est quant à lui consulté pour avis au regard des aspects santé et bien-être (article L4612-8 et L4612-9 du Code du travail).

Un avis négatif n'empêche pas la mise en place de la Charte, en revanche l'absence de consultation constitue un délit d'entrave selon Article L2328-1 du Code du travail.

III.1.b LE PRINCIPE DE TRANSPARENCE

A la suite de l'avis rendu lors de la consultation des institutions représentatives du personnel, l'employeur pourra procéder à la mise en œuvre de la Charte, en procédant à la publicité de la charte par voie d'affichage.

Il s'agit de diffuser la Charte auprès des utilisateurs, au même titre que la diffusion du règlement intérieur (article L1321-5 du Code du travail) individuellement et collectivement par affichage (R1321-1 Code du travail) à une place convenable et aisément accessible dans les lieux de travail ainsi que dans les locaux et à la porte des locaux où se fait l'embauche. A la lecture de cet article, un affichage par voie papier pourra être complété par une diffusion par intranet de la Charte.

En dehors de l'affichage réglementaire, tout type de mise à disposition complémentaire ou de diffusion sur la charte

auprès des salariés est la bienvenue. L'usage aujourd'hui de l'intranet ou du réseau social d'entreprise est une voie particulièrement adaptée pour assurer cette diffusion.

Même si ce n'est pas une obligation légale, dès lors que la Charte a été validée collectivement avec les institutions représentatives du personnel, il est possible et sans doute même souhaitable de mettre en œuvre une solution imposant à l'utilisateur de déclarer avoir bien pris connaissance de la charte. En pratique, il s'agit de solutions comme celles développées par Olfeo permettant l'affichage d'un message à la première connexion de l'utilisateur ou lors de la mise à jour de la charte permettant de présenter la charte et imposant la confirmation par l'utilisateur de sa prise de connaissance de la Charte.

Dans le déploiement d'une telle solution il convient d'être très attentif à la terminologie employée sur l'interface web. Il faut éviter des formules comme « j'accepte la charte » ou « j'adhère à la charte », mais opter pour des formules beaucoup plus neutres comme « j'ai pris connaissance de la Charte » voire s'abstenir de toute information particulière avec une mention comme « continuez ».

<u>Les démarches supplémentaires à destination des entreprises et des administrations employant des agents de droit privé :</u>

Plus généralement, comme prévu par les articles R1321-2 et R1321-4 du Code du travail, si les salariés dépendent du code du travail, il est également nécessaire de :

- déposer la Charte au Greffe du **Conseil des prud'hommes**,

- transmettre la Charte à **l'Inspection du travail** en deux exemplaires.

III.1.c LA MODIFICATION DE LA CHARTE

A chaque modification de la Charte, l'ensemble de cette procédure doit être à nouveau déployée.

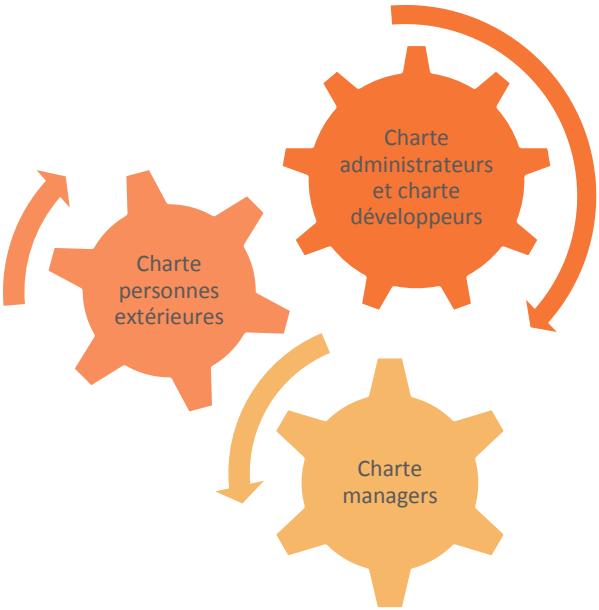
Pour le Livret Technique ou Guide Juridique, l'avantage non négligeable de ces différents documents est qu'ils n'ont pas besoin d'être soumis aux Instances Représentatives du Personnel.

III.2 LES AUTRES CHARTES SPECIFIQUES A CERTAINS GROUPES DE PERSONNES

Il pourra parfois être nécessaire de prévoir des règles spécifiques à certaines catégories de personnes : les développeurs, les managers, la hiérarchie ou les personnes extérieures à l'établissement.

Ces personnes n'ont pas les mêmes accès au système d'information. Par exemple, un accès plus étendu pour les développeurs ou les manager et un accès plus limité pour les personnes extérieures qui ne sont pas soumises au règlement intérieur de l'établissement mais celui de leur propre employeur ou aucun s'il s'agit d'un professionnel indépendant.

Ces règles pourront se traduire par des Chartes spécifiques :



III.3 LES AUTRES GUIDES ET CODES

III.3.a GUIDE DES OPERATIONS DE CONTROLE

La Charte informatique, la Charte administrateurs, le Livret et le Guide Juridique sont les quatre piliers qui permettent :

- de responsabiliser les salariés quant à l'usage des ressources informatiques ;
- le cas échéant, de sanctionner les comportements illicites ou inappropriés.

Si ce socle est un préalable indispensable à toute opération de contrôle, il n'a pas pour objectif ni pour vocation de déterminer, en pratique, les conditions matérielles et opérationnelles d'un contrôle sur le poste informatique (fichier et/ou messagerie) d'un salarié.

Or, l'opération de contrôle est une opération risquée sur le plan juridique.

Toute erreur dans l'opération de contrôle peut aboutir :

- au mieux à ce que les preuves ainsi obtenues ne soient pas opposables au salarié ;

- au pire, à ce que l'opération se retourne contre l'employeur et que celui-ci soit sanctionné, par exemple pour la violation du secret de correspondances.

De fait, en plus des documents socles susvisés, il est indispensable de déterminer, en amont, le processus opérationnel que la personne en charge du contrôle devra suivre scrupuleusement pour éviter, autant que faire se peut, que la responsabilité de l'entreprise soit engagée.

Le guide des opérations de contrôle est donc, comme son nom l'indique, un mode opératoire.

C'est un guide important en cas de litige. Il définit les conditions d'accès à la preuve et les conditions de maintien de la preuve. C'est ici qu'il sera expliqué comment, selon les cas, l'accès à la preuve se fera en présence ou non d'un salarié, avec un huissier, avec les autorités … Par exemple, le guide des procédures comporte des indications sur le déclenchement de la procédure, les personnes habilitées à

déclencher la procédure, le recours à un huissier de justice, le recours à une autorisation judiciaire si besoin, les modalités pratiques du contrôle telle que les éléments conservés, les éléments communiqués, ou encore le nombre de copie de preuve effectué.

III.3.b CODE ETHIQUE, POLITIQUE D'ARCHIVAGE, POLITIQUE DE DEMATERIALISATION

Il est également recommandé d'éditer des codes éthiques, des politiques d'archivage, politique de dématérialisation pour la gestion des documents électroniques et des signatures électroniques.

IV. CHAPITRE 4 : LA SOLUTION, UNE STRUCTURE DOCUMENTAIRE

IV.1 UN LIVRET TECHNIQUE OU LIVRET DES PROCEDURES

Pour les raisons expliquées ci-dessus, la Charte informatique ne devrait pas comporter, même à titre d'illustration, de références technologiques ou d'instructions techniques.

A l'inverse, il est indispensable d'expliquer aux utilisateurs comment utiliser les outils mis à leur disposition.

C'est la raison pour laquelle il est préconisé d'adopter, en complément de la Charte informatique, un « Livret technique utilisateur ».

Le Livret technique utilisateur est un document à vocation opérationnelle et technique. De fait, il n'est pas considéré comme un outil de sanction en tant que tel et n'a pas, par principe, à faire l'objet d'une consultation des instances représentatives du personnel.

Son objectif est d'aborder les bonnes pratiques par type de technologie. Par exemple : comment renouveler son login/mot-de-passe, comment doit être composé le mot-de-passe : lettres, chiffres, nombre de caractères, majuscules, minuscules…

IV.2 UN GUIDE JURIDIQUE POUR LES UTILISATEURS

Comme développé plus haut, la Charte informatique ne devrait pas comporter, même à titre d'illustration, de références légales ou jurisprudentielles.

A défaut, la Charte risque vite de devenir obsolète ou de ne pas être en phase avec l'évolution légale ou jurisprudentielle et donc de devoir être fréquemment modifiée et (re)présentée devant les instances représentatives du personnel.

A l'inverse, informer les utilisateurs sur les raisons qui ont présidées à la rédaction de telle ou telle dispositions de la Charte présente deux intérêts : un intérêt pédagogique d'abord, mais également un moyen pour l'entreprise de démontrer qu'elle n'a pas manqué à son obligation d'information à l'égard de ses utilisateurs comme le souhaitent de nombreux acteurs au premier rang desquels figure la Cnil ou encore l'Hadopi.

C'est la raison pour laquelle il est préconisé d'adopter en complément de la Charte informatique un « Guide juridique Utilisateur ».

Il présente la législation applicable et les jurisprudences dominantes s'il en existe. Il traite également lorsque c'est nécessaire la position d'une autorité en particulier (Cnil, Hadopi, DGCCRF, AMF, …).

Le « guide juridique utilisateur » n'est que l'illustration juridique et jurisprudentielle de la Charte. De fait, il n'est pas

considéré comme un outil de sanction en tant que tel et n'a pas, par principe, à faire l'objet d'une consultation des instances représentatives du personnel.

Il présente donc l'avantage de pourvoir être actualisé en temps réel et les versions successives peuvent aisément être adressées aux utilisateurs soit par mél soit via l'intranet de l'entreprise.

IV.3 UNE CHARTE ADMINISTRATEUR

La Charte administrateur vient en complément de la Charte informatique, afin de préciser les conditions dans lesquelles les administrateurs systèmes, applications ou réseaux doivent agir.

De même, la Charte administrateur a vocation à responsabiliser les personnels disposant des droits étendus sans nécessairement être des administrateurs statutaires.

Si ces collaborateurs sont assurément soumis aux mêmes règles que les autres employés (Charte informatique), ils ont des moyens et/ou des obligations professionnelles plus sensibles que les autres.

Ils ont, par exemple, la possibilité de passer outre les logins et mots de passe et d'accéder à des données susceptibles de relever de la vie privée résiduelle des utilisateurs.

De même, ils peuvent réaliser une prise en main à distance du poste de l'utilisateur.
Enfin, ils ont accès à l'ensemble des informations relatives aux utilisateurs, tel que les fichiers de journalisation (logs).

Les administrateurs ne peuvent, en principe, se livrer à aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications, des informations dont ils peuvent avoir connaissance dans l'exercice de leurs fonctions.

Il est d'usage de considérer que les administrateurs sont tenus à une obligation de discrétion professionnelle, à défaut de secret professionnel.

Ils doivent donc être protégés de tous risques, notamment, d'atteintes à la vie privée, telle la violation des correspondances privées.

Si, à l'inverse, ils abusent des moyens dont ils disposent, ils doivent pouvoir être sanctionnés.

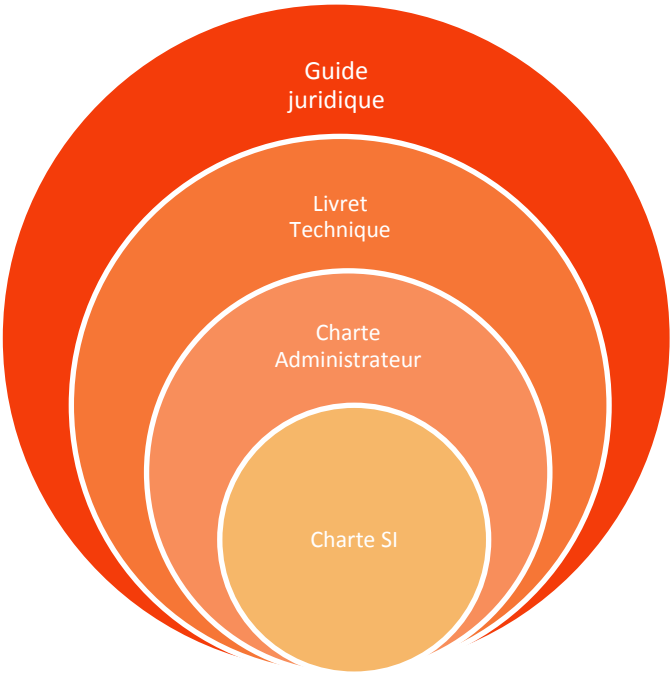
De plus, ce sont souvent les administrateurs qui, seuls, en cas de contrôle ou d'enquête, pourront communiquer les données de trafic à l'autorité habilitée.

Pour l'ensemble de ces raisons, la plupart des entreprises publiques ou privées qui disposent d'une équipe de plusieurs administrateurs internes ou externes ou d'une équipe informatique significative font le choix d'adopter une Charte administrateur.

La Cnil recommande que l'obligation de confidentialité des administrateurs soit rappelée dans leurs contrats de travail ainsi que dans la Charte[18].

[18] Rapport de la Cnil sur la cybersurveillance, édition mars 2004 : http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf

REGULATION DU SI



CONCLUSION

La démarche de Charte informatique s'inscrit donc dans une logique de cohérence entre contraintes technique et politique des ressources humaines.

Dans les meilleurs pratiques, la Charte est accompagnée de différents livrets, guides, et codes pour la compléter.

Pour aller plus loin :

Retrouvez plus d'informations dans le Livre Blanc juridique Olfeo co-écrit avec le Cabinet d'avocats Alain Bensoussan :

« Filtrage et Internet au bureau : Enjeux et cadre juridique ».

Disponible sur :
http://www.olfeo.com/sites/olfeo/files/pdf/juridique.pdf

Testez vos connaissances juridiques en matière de Charte :
http://www.olfeo.com/proteger-votre-entreprise/maitriser-le-cadre-juridique/quiz-charte-informatique

A propos du cabinet d'avocats Alain Bensoussan

Le cabinet Alain Bensoussan Avocats assiste ses clients depuis 1978 dans le domaine du droit de l'informatique.

Depuis sa création, Alain Bensoussan Avocats a élargi ses domaines de compétence, du cœur de métier constitué par l'informatique et les télécommunications vers les technologies avancées.

Ces constantes évolutions technologiques ont été source de réflexion et de créativité l'amenant à rédiger le premier traité de droit de l'informatique en 1985, puis deux ouvrages phares aux Editions Francis Lefebvre, « Informatique, Télécoms, Internet » (1997, 2001, 2004, 2008, 2012) et « Informatique et libertés » (2008, 2010) et une collection d'une trentaine d'ouvrages aux éditions Hermès – Lavoisier entre 1991 et 2003. Novateur dans son organisation, sa gestion et son système qualité, son positionnement d'origine, centré sur le droit des nouvelles technologies, l'amène naturellement à intervenir dans tous les autres secteurs des technologies avancées au fur et à mesure de leur apparition et développement.

Installé à Paris, Alain Bensoussan Avocats ouvre de nouveaux bureaux en province en 1990 et se développe à l'étranger dès 1992 par des accords de correspondance organique conclus en Europe (notamment Allemagne, Suisse, Belgique), aux Etats-Unis et au Japon.

En janvier 2012, Alain Bensoussan Avocats crée Lexing ®, premier réseau international d'avocats technologues dédié au droit des technologies avancées. Toute son activité résulte d'un positionnement voulu par une stratégique d'innovation et de développement du droit du numérique qui lui valent d'obtenir la reconnaissance de ses pairs, tant au niveau national qu'international.

Dans sa nouvelle édition 2013, la revue juridique américaine « Best Lawyers » confirme pour la 3ème année consécutive, le positionnement d'Alain Bensoussan Avocats qu'il classe parmi les « avocats jugés incontournables » dans les catégories Technologies, Technologies de l'Information, et Contentieux.

De même, pour l'édition 2013 du guide professionnel « Chambers Europe » qui référence cette année encore Alain Bensoussan Avocats parmi les

leaders de la catégorie TMT: Information Technology – France : « The firm. This team is known across the market for its innovative work in IT law and is one of the largest teams in France to focus solely on IT-related matters. It recently worked with the European Commission on the Intelligent Transport Systems legal framework project ».

Site internet: www.alain-bensoussan.com
Chaine Youtube:
https://www.youtube.com/channel/UC7xrTpr0LGPWVNbYxxDcFVQ
Réseau Lexing : network.lexing.eu/?lang=fr

A propos d'Olfeo :

Avec plus de 10 ans d'expertise, Olfeo, éditeur français d'une solution de proxy et de filtrage de contenus Internet apporte une vision exclusive et innovante sur le marché de la sécurité grâce à une approche multi-locale.

La solution Olfeo permet aux entreprises et aux administrations de maîtriser les accès et l'utilisation d'Internet des utilisateurs en adéquation avec les exigences culturelles et législatives spécifiques d'un pays à travers 5 produits complémentaires : Proxy cache QoS, Filtrage d'URL, Filtrage protocolaire, Antivirus de flux, Portail public.

Olfeo dispose aujourd'hui d'une version française, suisse, belge, allemande, luxembourgeoise, marocaine, tunisienne et algérienne de sa solution. Cette approche locale garantit une protection juridique optimale, une qualité de filtrage inégalée et une haute sécurité du système d'information.

Les avantages exclusifs de version française de la solution Olfeo :

- Une protection juridique optimale à travers des catégories de filtrage reprenant l'intégralité du périmètre illégal français (Hadopi, Loppsi, Arjel, lois mémorielles…)

- Une facilité de création de vos politiques de filtrage grâce à des catégories en français conformes à la culture et aux centres d'intérêt des internautes français (débat sur les retraites, logos et sonneries…)

- Un taux de reconnaissance des sites visités par vos utilisateurs supérieur à 98% grâce à la connaissance des habitudes de surf des internautes français

- Une qualité de filtrage inégalée grâce au classement manuel du contenu par des équipes françaises polyglottes

- Le respect du code du travail grâce à la diffusion individuelle de la charte Internet et la conservation des logs utilisateurs ayant pris connaissance de la charte

- L'association des utilisateurs à votre politique de sécurité grâce à des fonctions exclusives de coaching, d'outrepassement et la possibilité de personnaliser les messages de blocage

- Une détection instantanée des attaques localisées sur le territoire français grâce à une double protection antivirale

- Un service client dédié et un interlocuteur unique pour accompagner chaque client tout au long de son abonnement

Olfeo propose également une version internationale de sa solution afin de répondre aux entreprises et administrations qui ont des besoins multi-pays.

Cette stratégie d'innovation est plébiscitée par plus de 2000 clients satisfaits, représentant plus de 3 millions d'utilisateurs.

http://www.olfeo.com

Suivre les actualités juridiques, clients et société Olfeo : http://www.olfeo.com/flux-rss-olfeo

Chaîne Youtube : http://www.youtube.com/user/OlfeoTV

Linkedin groupe : http://www.linkedin.com/groups/Olfeo-3986777
Linkedin entreprise : http://www.linkedin.com/company/olfeo