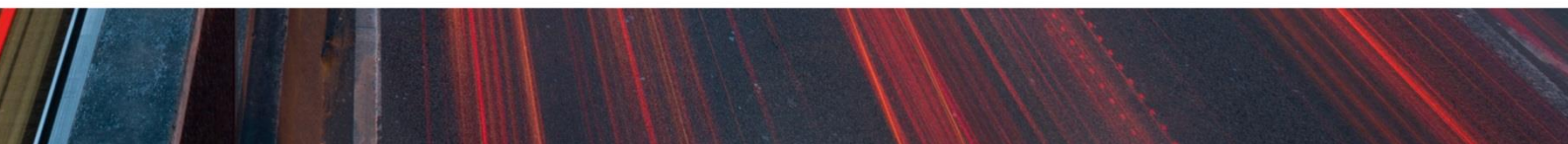
Filtrage et Internet au bureau

LIVRE BLANC JURIDIQUE VOL. IV :

Plan de déploiement d'une solution de filtrage

Olfeo
La sécurité positive

Lexing
Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées



VOLUME IV

PLAN DE DEPLOIEMENT D'UNE SOLUTION DE FILTRAGE

Note : les paragraphes marqués de ce marque-page rouge sont des nouveautés par rapport à la 3ème édition du livre blanc juridique Olfeo.

ETAPE 1 : LE CHOIX DE LA SOLUTION

Une solution de filtrage pertinente doit être capable de proposer :

- Des **catégories pertinentes qui correspondent au droit pénal** du pays et segmentées en fonction **des centres d'intérêts** des utilisateurs
- Un **taux de reconnaissance** élevé (aptitude à reconnaître les sites visités par les utilisateurs)
- Une **qualité du classement** pertinente (choix de la bonne catégorie pour un site au regard de la législation et de la culture du pays)

LE BON CHOIX DES CATEGORIES

La législation, les centres d'intérêts varient d'un pays à un autre.

Or, il est important de s'assurer que la solution de filtrage que l'on souhaite mettre en place permette à l'entreprise de se défendre conformément au droit pénal applicable dans le(s) pays dans le(s)quel(s) elle donne accès à Internet. Pour cela la solution de filtrage doit permettre d'exclure précisément les sites et protocoles illicites.

De même il est indispensable que celle-ci prenne en compte les centres d'intérêts extra-professionnels des internautes afin d'apporter une simplicité de création des politiques de filtrage et que celles-ci soient efficaces.

Il faut savoir choisir un outil adapte à son besoin et répondant aux obligations légales et qui collecte des données non discriminatoires

L'IMPORTANCE DU TAUX DE RECONNAISSANCE

En effet, si les URL référencées ne correspondent pas à l'usage du web tel qu'il est fait par l'organisation, cette base ne sera pas pertinente quelle que soit sa taille. Le taux de reconnaissance est l'indicateur le plus fiable pour mesurer l'efficacité d'un outil de filtrage.

Les solutions américaines à vocation mondiale embarquent des bases très volumineuses mais qui incluent les sites les plus regardés dans le monde avec une très grosse proportion de sites anglo-saxons.

Pour le marché français, des sites français comme « tf1.fr » ou « fnac.com » seront référencés mais pas forcément des sites à audience plus locale comme des pages pornographiques sur des blogs français.
Il est intéressant de noter que les 100.000 premiers sites regardés de France représentent 98% du trafic et que 70% d'entre eux sont francophones.

LA QUALITE DU CLASSEMENT : LES SITES DANS LES BONNES CATEGORIES

Le troisième critère d'évaluation est la qualité de classement. L'analyse automatique à base de mots clés ou d'intelligence artificielle conduit trop souvent à des évaluations erronées qui se traduisent par du sur-filtrage et donc à un mécontentement des utilisateurs.

Il est important que le classement effectué par l'éditeur soit juste, c'est-à-dire que le site soit classé dans la catégorie dont il est le plus proche. Des pages différentes d'un même site peuvent d'ailleurs être classées dans des catégories différentes (exemple : les portails sont par nature multi-catégories).

L'appréciation de l'appartenance d'un site à une catégorie plutôt qu'à une autre nécessite :

- Une analyse humaine (nous avons vu que les techniques d'intelligence artificielle ne sont pas encore assez performantes)

- Un jugement de valeur qui soit basé sur un référentiel culturel très proche de l'entreprise utilisatrice

Ce dernier point est très important et favorise aussi les solutions locales. Des éditeurs américains peuvent, par exemple, classer des syndicats dans la catégorie terrorisme/activisme car c'est sincèrement dans cette catégorie que leur jugement de valeur les place. L'impact de ces erreurs de classement peut se traduire, au minimum par du temps pour reclasser certains sites et au pire par des difficultés sociales.

L'utilisation du filtrage est non seulement légale mais apparaît dans bien des cas comme étant imposée par la loi.

Sa mise en œuvre doit s'inscrire dans le respect des obligations légales que constituent principalement :

- Le droit « Informatique et Libertés »
- Le droit du travail

ETAPE 2 : LE RESPECT DU DROIT INFORMATIQUE ET LIBERTES

LES PRINCIPES DE LA LOI INFORMATIQUE ET LIBERTES

La Loi Informatique et Libertés, vise ce que l'on nomme les données à caractère personnel et les traitements de données à caractère personnel.

En vertu **de l'article 2 alinéa 2 et 3 de la loi Informatique et Libertés** :

- **Constitue une donnée à caractère personnel « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

- **Constitue un traitement de données à caractère personnel: « toute opération ou tout ensemble d'opérations portant sur de telles données**, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

L'article 8 I de ladite loi précise également des **interdictions en matière de collecte ou de traitement de certaines données** :

- « **Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement** ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. »

En application **de l'article 6 de la loi Informatique et Libertés,** un traitement de données à caractère personnel ne peut porter que sur des données :

- **Collectées de manière loyale** et licite

- **Adéquates, pertinentes**, **complètes, exactes, mise à jour** si nécessaire et non excessives eu égard à la finalité du traitement

- **Conservées sous une forme permettant l'identification des personnes** concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées

Dans la mesure où les outils de filtrage permettent d'identifier les comportements de personnes physiques, les informations qu'ils comportent constituent bien des données à caractère personnel au sens de la loi.

Les données des outils de filtrage peuvent être collectées, saisies, enregistrées, consultées, éditées. Elles font donc l'objet d'un traitement.

Par conséquent, un dispositif de filtrage constitue un traitement soumis à la législation relative à la protection des données à caractère personnel.

LES PRINCIPES DU REGLEMENT 2016/679 RELATIF A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES, ET ABROGEANT LA DIRECTIVE 95/46/CE (RGPD)

Le Parlement européen a adopté le 14 avril 2016 le règlement général sur la protection des données personnelles 2016/679 (dit « RGPD »). L'objectif du règlement est d'instaurer des mécanismes visant à assurer une application cohérente de la législation en matière de protection des données dans l'ensemble de l'Union européenne. Ce règlement sera applicable à compter du 25 mai 2018.

Quatre grands principes structurent le règlement RGPD (articles 5 et 6) :

- le principe de légalité, les données à caractère personnel devant être traitées de manière licite, loyale et transparente au regard de la personne concernée
- le principe de finalité, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités
- le principe de légitimité, les données traitées doivent être exactes, adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Ces données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées
- le principe de proportionnalité, les traitements doivent être proportionnés au regard de la finalité

L'article 4 du RGPD reprend des termes similaires à ceux du droit français pour définir la notion de donnée à caractère personnel qui renvoie alors à « toute information se rapportant à une personne physique identifiée ou identifiable (est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale) ».

Ce même article 4 défini le terme de traitement « comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le

rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ». Comme pour la définition de la notion de données à caractère personnel, la définition de ce type de traitement en droit européen est aussi très proche de la définition de la loi française. Le règlement RGPD ajoute la structuration comme opération appliquée à des données à caractère personnel, opération qui n'est pas mentionnée dans l'article 4 de la loi Informatique et Libertés.

LES DEMARCHES PREALABLES A METTRE EN OEUVRE

Schématiquement, pour qu'un outil de filtrage soit mis en œuvre conformément à la loi Informatique et Libertés et/ou au RGPD, 3 grands principes doivent être respectés :

- Le droit des personnes
- Les formalités et actions à accomplir
- La sécurité des données

Le droit des personnes

Tant la loi Informatique et Libertés que le RGPD prévoit des obligations relatives au droit des personnes.

Les personnes concernées par un traitement de données à caractère personnel disposent de cinq droits au titre de la loi Informatique et libertés:

- Le droit à l'information
- Le droit d'accès
- Le droit d'interrogation
- Le droit d'opposition
- Le droit de rectification

Le RGPD ajoute, dans son article 13, le droit à l'effacement (oubli numérique), le droit à la limitation du traitement et le droit à la portabilité des données.

La personne dont les données à caractère personnel font l'objet d'un traitement doit être informée, au plus tard au moment de la collecte des données[1] :

- De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant
- De la finalité poursuivie par le traitement
- Du caractère obligatoire ou facultatif des réponses
- Des conséquences éventuelles, à son égard, d'un défaut de réponse
- Des destinataires ou catégories de destinataires des données
- Des droits qu'elle détient
- Des transferts de données à destination d'un Etat non-membre de la Communauté européenne

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art.32.

L'article 13 du RGPD ajoute à cette liste l'obligation d'informer sur :

- l'intérêt légitime poursuivi par le responsable du traitement
- le droit de retirer son consentement à tout moment
- la durée de conservation des données ou les critères permettant de la déterminer
- le droit de réclamation auprès de l'autorité de contrôle
- l'existence ou non d'une prise de décision automatisée, y compris un profilage, et, au moins des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Cette information peut être réalisée par le biais de la charte lorsqu'il s'agit d'employés par exemple.

Les entités responsables du traitement devront mettre en place une procédure afin de garantir aux personnes concernées l'exercice de leur droit de rectification, d'interrogation et de leur droit d'accès conformément à l'article 39 de la loi Informatique et Libertés. Ces entités devront aussi prévoir les procédure permettant l'effacement et la portabilité des données à caractère personnel.

Ces dernières ont en effet le droit d'interroger le responsable du traitement en vue d'obtenir :

- « **La confirmation que des données** à caractère personnel les concernant font ou **ne font pas l'objet d'un traitement**

- **Des informations relatives aux finalités du traitement** ou catégories de données à caractère personnel traitées et **les destinataires** ou catégories de destinataires auxquels les données sont communiquées

- Le cas échéant, **des informations relatives aux transferts de données à caractère personnel** envisagés à destination d'un Etat non-membre de la Communauté européenne

- La communication, sous une forme accessible, des **données à caractère personnel qui la concernent** ainsi que de toutes **informations disponibles quant à l'origine** de celles-ci

- « **Les informations permettant de connaître et de contester** la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à son égard. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. »[2]

Ces droits ont pour but « d'encourager la transparence dans l'exploitation des données à caractère personnel »[3].

Les personnes concernées par le traitement ont en outre le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement[4].

[2] Loi 78-17 du 6 1 1978, art. 39.
[3] Alain Bensoussan, « Informatique, télécoms, internet » éd. 2014, n°1639.
[4] Loi n° 78-17 du 6 1 1978,art. 38

Formalités en application de la loi Informatique et libertés : la déclaration CNIL

De fait, toute entité qui met en œuvre un outil de filtrage doit procéder aux formalités préalables imposées par la CNIL.

On peut s'interroger sur le type de démarches préalables à mettre en œuvre.

L'article 22 de la loi Informatique et Libertés prévoit que les traitements automatisés de données à caractère personnel **doivent faire l'objet d'une déclaration auprès de la CNIL.** Lorsque ceux-ci ne relèvent pas des dispositions prévues aux articles 25, 26 et 27 de la loi relatifs aux demandes d'autorisation.

Dès lors que le dispositif de filtrage permet un contrôle individuel, celui-ci doit faire l'objet d'une **déclaration dite « normale** » auprès de la CNIL.

Selon l'article 30 de la loi informatique et Libertés, cette déclaration doit notamment préciser :

- L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre État membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande
- La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions
- Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements
- Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement
- Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées
- Les destinataires ou catégories de destinataires habilités à recevoir communication des données
- La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit

  Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant
- Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5
- La durée de conservation des données établie, étant précisée que la CNIL considère qu'une durée de conservation de six mois paraîtrait suffisante dans la plupart des cas
- L'indication de la date à laquelle les instances représentatives du personnel ont été consultées sur la mise en place des outils de filtrage

La déclaration normale portera en général sur la mise en œuvre de l'ensemble des outils de surveillance et particulièrement sur les outils de filtrage. Si l'outil de filtrage est le seul traitement de contrôle individuel des employés, alors il fera l'objet d'une déclaration normale en tant que tel.

La déclaration pourra alors être transmise par Internet, par un dépôt direct auprès de la CNIL, ou par un envoi par lettre recommandée avec accusé de réception.

La déclaration normale a la CNIL ne fait que 4 pages et peut être réalisée en ligne. L'enregistrement de la déclaration auprès de la CNIL sera effectif dès réception du récépissé portant le numéro de déclaration. Dès réception de ce récépissé, le traitement peut être mis en œuvre.

En revanche, si l'entreprise dispose d'un correspondant Informatique et Libertés[5], elle se trouvera dispensée de la déclaration normale[6].

Si le dispositif de filtrage ne permet pas de contrôle individuel, il est possible de procéder à une déclaration simplifiée du traitement. En effet, une norme simplifiée n°46 relative à la gestion du personnel permet de procéder à une déclaration simplifiée auprès de la CNIL des outils informatiques liés à la gestion des personnels.

Autrement, comme indiqué précédemment, il convient de privilégier la réalisation d'une déclaration normale auprès de la CNIL, l'exercice n'étant d'ailleurs pas plus compliqué qu'une déclaration simplifiée.

Enfin en l'absence de données directement ou indirectement nominatives, le dispositif de filtrage ne constitue pas un traitement de données à caractère personnel et ne nécessite pas une déclaration à la CNIL.

Si les données relatives aux employés sont anonymisées, il convient de préciser les modalités de cette anonymisation afin de déterminer si l'anonymisation des données est absolue, c'est à dire si les données ne sont plus nominatives directement (nom, prénom…) et indirectement (adresse mél, adresse IP…).

L'anonymisation des données doit réellement permettre de faire perdre leur caractère personnel aux données afin de rendre impossible toute identification des personnes pour qu'aucune déclaration à la CNIL ne soit nécessaire. L'anonymisation doit donc être irréversible. Si elle est réversible, le dispositif de filtrage doit être déclaré.

Actions en application du RGPD : l'établissement d'un registre et l'analyse d'impact le cas échéant

A compter du 25 mai 2018, le RGDP fera disparaitre les formalités déclaratives auprès de la CNIL au bénéfice de l'obligation de tenir un registre dans les conditions de l'article 30 du règlement. Il conviendra également d'appliquer un nouveau principe, le principe de responsabilité (accountability) selon lequel le responsable du traitement est responsable du respect des principes essentiels du RGPD et doit être en mesure de démontrer que ceux-ci sont respectés (article 5).

[5] Tel que le prévoit l'art. 22-III de Loi n° 78-17 du 6 1 1978
[6] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010 p. 19

Le responsable de traitement devra ainsi tenir un registre des activités de traitement contenant l'identité et les coordonnées du responsable de traitement, les finalités, les catégories de personnes concernées, les catégories de données, l'existence ou non d'un transfert international, les délais prévus pour l'effacement et une description générale des mesures de sécurité techniques et organisationnelles qui ont été prises.

L'article 35 du RGPD obligera le responsable de traitement à effectuer, avant la mise en œuvre du traitement, une analyse d'impact « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ». L'analyse d'impact sera en particulier requise en cas « d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ». La CNIL pourra établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

Les dispositifs de filtrage peuvent déboucher sur un traitement automatisé de données à caractère personnel qui procède à une « évaluation systématique et approfondie » des connexions internet ; De surcroît, sur le fondement de ce traitement des décisions juridiques concernant directement les salariés peuvent être prises (sanction par exemple). Par conséquent, l'analyse d'impact semble requise en cas de mise en œuvre d'un dispositif de filtrage.

L'article 35 détaille les modalités de l'analyse d'impact. Cette dernière devra au moins contenir :

- une description générale des traitements envisagés et des finalités
- l'évaluation de la nécessité et de la proportionnalité des opérations de traitement
- l'évaluation des risques pour les droits et libertés des personnes concernées
- les mesures envisagées pour faire face aux risques.

La sécurité des données

Le principe de sécurité et de confidentialité des données prévoit une obligation de sécurité des données à caractère personnel.

Au titre de la loi Informatique et Libertés [7], le responsable d'un traitement de données à caractère personnel est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès. Des mesures de sécurité et de confidentialité adéquates devront donc être prises (mot de passe, sécurisation des accès physique et logique ainsi que des liaisons…).

La CNIL dispose d'une gamme de pouvoirs élargie pour vérifier que les dispositions de la loi Informatique et Libertés sont respectées. En cas de non-respect des dispositions, la CNIL peut sanctionner le responsable du traitement.

Cette obligation de sécurité des données et des traitements est reprise par les articles 25 et 32 à 34 du RGPD qui imposent la mise en œuvre de « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » telles que la pseudonymisation, l'anonymisation ou la minimisation des données par exemple.

[7] Loi n° 78-17 du 6 1 1978, art.34.

Le principe de minimisation vise à s'assurer que les données traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. L'application de ce principe au filtrage renvoie à ce que, dans l'hypothèse ou un traitement de données à caractère personnel est mis en œuvre afin d'identifier le comportement d'une personne, ne doivent être traitées que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du dispositif de filtrage (exemple : identité, fonctions et coordonnées de la personne concernée et faits signalés par le dispositif automatique de filtrage). La sécurité de ce dispositif sera d'autant plus renforcée si les données traitées sont anonymisées.

De surcroît, l'article 25-1 imposera l'obligation de Privacy by design. Ce principe signifie que les aspects de protection des données doivent être pris en compte dès la conception d'un traitement et maintenus en conformité tout au long du cycle de vie de la solution qui assure le traitement. Le Privacy by design est un gage de confiance vis-à-vis des salariés et des partenaires.

A titre d'exemple, il convient de prendre les mesures qui garantissent, par défaut, que les données à caractère personnel traitées au titre du filtrage ne sont rendues accessibles qu'à un nombre déterminé et restreint de personnes (dès la conception et tout au long du cycle de vie de traitement).

LES POUVOIRS DE LA CNIL

La modification de la loi Informatique et Libertés par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, a renforcé les pouvoirs de la CNIL.

L'article 11 de la loi Informatique et Libertés dresse la liste de ses pouvoirs :

- La CNIL informe de leurs obligations les personnes concernées par un traitement et les responsables de traitements en proposant notamment des guides, modèles sur son site Internet
- Elle veille à ce que les traitements soient mis en œuvre conformément aux formalités préalables de la loi Informatique et Libertés
- Elle dispose d'un pouvoir réglementaire pour encadrer ces traitements et peut élaborer des normes relatives à certaines catégories de traitements et édicter des recommandations
- Elle est consultée sur tout projet de loi ou décret relatif à la protection des personnes à l'égard des traitements
- Elle conseille les personnes et les organismes privés ou publics qui souhaitent mettre en œuvre ou envisage de mettre en œuvre des traitements
- Elle anime le réseau des Correspondants Informatique et Libertés (Cil)
- Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, après les avoir reconnus conforme à la loi Informatique et Libertés
- Elle dispose d'un pouvoir d'investigations et de contrôle des traitements mis en œuvre ;

- Elle peut prononcer des sanctions en cas de non-respect des obligations Informatique et Libertés

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a modifié l'article 45 de la loi Informatique et libertés afin d'accroître les pouvoirs de la CNIL en prévoyant que:

- la Cnil peut fixer le délai imparti à un responsable de traitement pour se mettre en conformité avec la loi à 24 heures en cas d'extrême urgence, au lieu de cinq jours au moins auparavant ;
- la Cnil est autorisé à prononcer une sanction pécuniaire sans mise en demeure préalable dans certaines circonstances alors qu'avant la sanction financière ne pouvait intervenir qu'après mise en demeure ;
- lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la loi Informatique et Libertés, la CNIL peut prononcer les sanctions suivantes, après mise en demeure et dans le cadre d'une procédure contradictoire : avertissement, sanction pécuniaire et injonction de cesser le traitement.

Aux termes de l'article 33 du RGPD et en cas de violation de données à caractère personnel, le responsable du traitement doit notifier la violation en question à la CNIL si cette violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Aux termes de l'article 34 de la loi Informatique et Libertés, cette obligation de notification n'est applicable qu'aux fournisseurs au public de services de communications électroniques. Cette obligation s'applique donc à tous responsables de traitement, y compris aux sous-traitants qui effectuent un traitement de données à caractère personnel.

LES SANCTIONS

Les sanctions administratives et pécuniaires que la CNIL peut prononcer sont :

- Un avertissement
- Une mise en demeure
- Une sanction pécuniaire
- Une injonction de cesser le traitement
- Un retrait de l'autorisation de mise en œuvre du traitement

Les sanctions pécuniaires prononcées par la CNIL font l'objet depuis la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique d'un plafonnement à hauteur de 3 millions d'euros.

Le non-respect des obligations de la loi Informatique et Libertés constitue également des infractions et peut conduire les tribunaux à prononcer des sanctions pénales.

La sanction encourue varie en fonction de l'obligation non respectée et peut être une contravention ou un délit. La peine maximale encourue est de 5 ans d'emprisonnement et 300 000 euros d'amende[8].

Pour les personnes morales, l'amende encourue est le quintuple de celui prévu pour les personnes physiques.

[8] Code pénal, art. 226-16 et suivants.

La loi pour une République numérique intègre, comme le RGPD, le principe de proportionnalité du montant de la sanction pécuniaire par rapport à la gravité des manquements commis et aux avantages tirés de ces manquements. L'article 47 de la loi Informatique et Libertés précise dorénavant que « la formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission ».

En application des articles 83 et 84 du RGPD, la CNIL pourra imposer, en cas de non-respect du règlement, une amende administrative de 10 000 000 d'euros ou 2% du chiffre d'affaire annuel mondial dans les cas suivants :

- absence de protection des données dès la conception et protection des données par défaut
- absence de représentant établi dans l'union
- absence de registre des activités de traitement
- absence de coopération avec l'autorité de contrôle
- absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation des données
- absence d'analyse d'impact.

L'amende administrative pourra s'élever à 20 000 000 d'euros ou 4% du chiffre d'affaire annuel mondial dans les cas suivants :

- non-respect des principes de base d'un traitement (licéité, loyauté, légitimité, adéquation et pertinence des données, consentement, données sensibles, etc.)
- non-respect du droit des personnes
- non-respect des règles relatives aux transferts de données à caractère personnel.

LE SAVIEZ-VOUS ?

L'OUTIL DE FILTRAGE DOIT FAIRE L'OBJET D'UNE DECLARATION PREALABLE A LA CNIL. L'ACCES AUX DONNEES DE L'OUTIL DOIT ETRE SECURISE.

ETAPE 3 : LE RESPECT DU DROIT DU TRAVAIL

La mise en place d'une solution de filtrage constitue à la fois :

- **Un outil de contrôle** de l'activité des employés, et doit à ce titre **être porté à leur connaissance**[9]
- Une nouvelle technologie introduite au sein de l'entreprise, et doit en conséquence faire l'objet **d'une consultation des institutions représentatives du personnel**[10]

SIMPLE « DOCUMENTS » D'INFORMATION ET/OU CHARTE INFORMATIQUE ?

Dès lors que l'outil de filtrage engendre la collecte des données à caractère personnel, un document doit être rédigé pour informer les salariés de la mise en place de cet outil.

Il n'existe pas de présentation obligatoire quant à la forme permettant d'assurer une telle information.

Ce document peut être une charte communément appelée « charte d'usage des systèmes d'information » ou « charte informatique ».

Cependant, implémenter au sein de l'entreprise ou de l'établissement une telle charte peut nécessiter plus de temps.

Ainsi, dans le but de simplifier ces démarches d'information, il est possible de rédiger un document présentant à minima la nouvelle technologie, les objectifs recherchés, les règles d'utilisation ainsi que la durée de conservation des données collectées.

L'implémentation de ce document simplifié consiste pour l'employeur à respecter les démarches minimum suivantes :

- **Transmettre le document à chaque salarié** individuellement à travers par exemple une note de service, un courrier accompagnant la fiche de paie, un lien inséré sur le site intranet de l'entreprise ou de l'établissement, un outil de diffusion de charte qui permet d'afficher celle-ci à la première connexion Internet du collaborateur…
- **Afficher le document** à une place accessible sur le lieu de travail

[9] C. trav. art. L. 1222-4. : « Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »
[10] C. trav. art. L. 2323-13

- **Soumettre** la proposition d'installation de la solution **à l'avis du comité d'entreprise**[11] ou technique dans les administrations, à défaut, des délégués du personnel et à l'avis du comité d'hygiène, de sécurité et des conditions de travail[12]

Il convient de préciser qu'un avis négatif de ces comités ne fait pas obstacle à la mise en place de la solution. En revanche, l'absence d'avis rendu, positif ou négatif, empêche la mise en œuvre du logiciel de filtrage.

Si cette démarche simplifiée permet de mettre en place rapidement l'outil de filtrage, le document ainsi implémenté n'est pas opposable à l'employé en ce sens qu'il ne permet pas à l'employeur d'utiliser les informations résultant de l'utilisation de l'outil de filtrage pour prendre une sanction à l'égard du personnel.

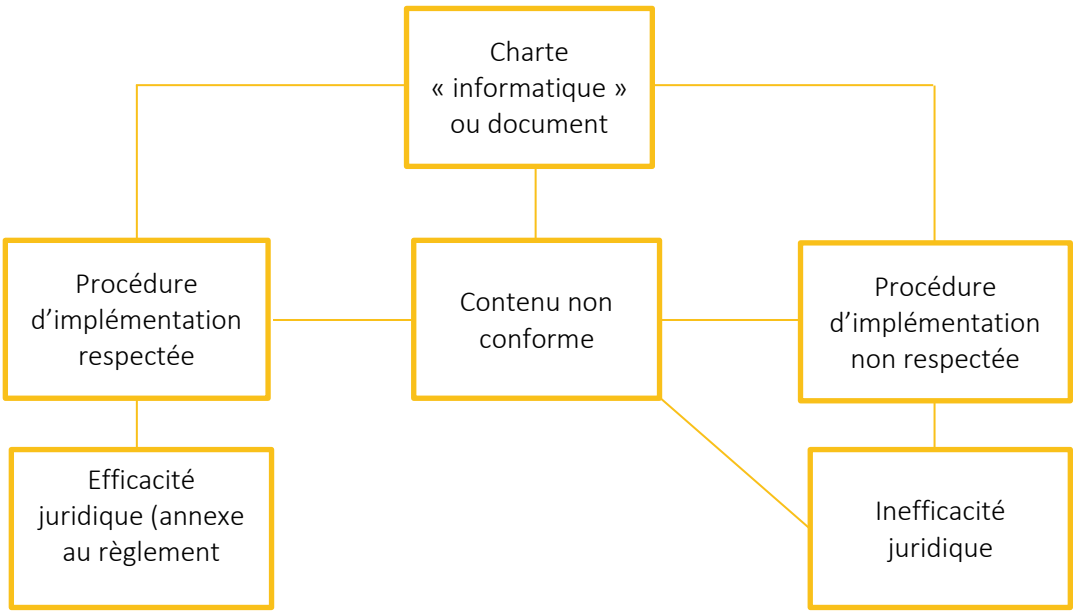
Dans le but de rendre une charte « utilisateurs » opposable aux employés et donc « efficace » juridiquement, une procédure d'implémentation spécifique doit alors être suivie. Eu égard à son objet, consistant notamment à poser des obligations générales et permanentes concernant les conditions d'utilisation des équipements de travail et à la sécurité au sein de l'entreprise, elle doit être considérée comme une adjonction au règlement intérieur[13], si un tel règlement existe déjà.

La charte constitue alors une annexe au règlement intérieur, dès lors que sa procédure d'implémentation est la même que celle prévue pour la mise en œuvre d'un tel règlement.

Cette procédure d'implémentation de la charte consiste alors à :

- **La soumettre à l'avis du comité d'entreprise ou technique dans les administrations**, à défaut, des délégués du personnel ainsi que, pour les matières relevant de sa compétence, à l'avis du comité d'hygiène, de sécurité et des conditions de travail[14]
- **L'afficher 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[15]
- **Pour les entreprises et les administrations qui emploient des agents de droit privé,** deux étapes supplémentaires sont nécessaires :
    - **La déposer au greffe du conseil de prud'hommes** du ressort du siège social de l'entreprise[16]
    - **La transmettre à l'inspecteur du travail en deux exemplaires**[17]

[11] C. trav. art. L. 2323-13
[12] C. trav. art. L. 4612-8.
[13] C. trav. art. L. 1321-5.
[14] C. trav. art. L. 1321-4.
[15] C. trav. art. R. 1321-1.
[16] C. trav. art. R. 1321-2.
[17] C. trav. art. R. 1321-4.



Par ailleurs, si l'employeur souhaite apporter des **modifications ultérieures** à ce document, il devra de **nouveau respecter la même procédure**.

En ce qui concerne les personnes tierces à l'entreprise qui ont accès à Internet, la charte informatique, constituant une annexe au règlement intérieur, n'est pas par principe opposable aux tiers qui ne sont pas des salariés de l'entreprise.

Dans la catégorie des tiers, il faut distinguer entre :

- **Les tiers intervenant sous contrat de prestations** (exemple : contrat de sous-traitance sur place)
- **Les tiers** pour lesquels il n'y a **pas** nécessairement **de contrat** (par exemple intervention occasionnelle d'un travailleur indépendant)

Concernant les premiers, il est nécessaire d'insérer une clause dans le contrat de prestation de service visant la charte informatique, à charge pour l'employeur principal de la personne de faire respecter la charte.

Concernant les seconds, la seule solution est l'acceptation individuelle de la charte informatique.

La procédure d'acceptation individuelle peut être :

- Ecrite
- Par voie électronique suite à l'ouverture d'une session informatique, le cas échéant

Idéalement, il est conseillé de rédiger à côté de la charte du système d'information applicable aux salariés/agents, une « charte des droits d'accès » pour les tiers de l'entreprise. La charte des droits d'accès est un document quasi-identique à la charte informatique mais adaptée aux utilisateurs tiers de l'entreprise et qui prévoit notamment des sanctions adaptées pour cette catégorie d'utilisateurs en cas de non-respect de la charte.

L'adoption d'une charte à destination des personnels ne règle cependant pas tous les problèmes.

Elle ne règle pas le problème des conditions dans lesquelles les personnels des directions informatiques et particulièrement les administrateurs systèmes peuvent ou non déployer les outils, les paramétrer, ou encore accorder à telle ou telle personne une dérogation temporaire ou définitive.

La particularité des chartes dans les administrations

Le dépôt de la charte informatique au greffe du conseil des prud'hommes est sa transmission à l'inspecteur du travail ne concerne que les personnes soumises au Code du travail.

La procédure d'implémentation d'une charte informatique dans l'administration n'est pas homogène. Elle dépend de la catégorie d'utilisateur au sein de l'administration et de la fonction publique à laquelle il appartient (fonction publique de l'Etat, fonction publique territoriale, fonction publique hospitalière).

Il existe de multiples statuts au sein de l'administration. Il ne sera abordé ci-dessous que la procédure d'implémentation relative aux agents titulaires de l'Etat (fonctionnaires) et aux agents non titulaires de l'Etat (agents contractuels).

S'agissant des agents titulaires de l'Etat, ces derniers sont notamment soumis à :

- La loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et son article 4 dispose que : « le fonctionnaire est, vis à vis de l'administration dans une situation statutaire et réglementaire ». Leur situation est donc régie de façon statutaire et réglementaire

  En conséquence, leur situation est modifiable par le législateur ou l'autorité administrative détenant le pouvoir réglementaire. Leurs droits et avantages peuvent donc être accrus et leurs obligations et sujétions aggravées en fonction des exigences de l'intérêt général et des besoins du service, et ce par voie législative ou réglementaire

- La loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat

L'article 28 de la loi n°83-634 « portant droits et obligations des fonctionnaires » dispose que :

- « Tout fonctionnaire, quel que soit son rang dans la hiérarchie, est responsable de l'exécution des tâches qui lui sont confiées. Il doit se conformer aux instructions de son supérieur hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public

- Il n'est dégagé d'aucune des responsabilités qui lui incombent par la responsabilité propre de ses subordonnés. »

Ce principe d'obéissance est ainsi associé à un principe de la responsabilité du fonctionnaire dans la mesure des tâches et des prérogatives qui lui sont confiées.
L'obéissance hiérarchique impose au fonctionnaire de se soumettre aux mesures prises par le chef de service pour le fonctionnement et l'organisation du service qu'elles soient générales (circulaires, instructions, notes de service...) ou particulières (comme les décisions d'affectation).

La jurisprudence reconnaît au chef de service un pouvoir autonome d'organisation dans le respect de la hiérarchie des normes :

- «Considérant que si, même dans le cas où les ministres ne tiennent d'aucune disposition législative un pouvoir réglementaire, il leur appartient, comme à tout chef de service, de prendre les mesures nécessaires au bon fonctionnement de l'administration placée sous leur autorité [...] dans la mesure où l'exige l'intérêt du service»[18].

L'acte réglementaire est un acte :

- Général
- Impersonnel ou non nominatif
- Visant une fonction, une institution, ou une situation[19]

En l'espèce une charte informatique a vocation à entrer dans la catégorie de l'acte réglementaire, dans la mesure où elle s'applique :

- De manière générale
- Sans distinguer les catégories de destinataires
- A toutes personnes placées dans la situation d'utilisateur des Systèmes d'information

La charte informatique ne doit pas comporter de disposition manifestement illégale, ou compromettante gravement un intérêt public. En conséquence, la charte devrait s'imposer au fonctionnaire, en tant qu'acte réglementaire pris dans le cadre de l'organisation du service.

Cependant, dans le cas où l'acte réglementaire affecterait les droits et obligations statutaires des fonctionnaires ou les prérogatives dont ils bénéficient de par leur appartenance à leur corps, il pourrait faire l'objet d'un recours pour excès de pouvoir « ouvert même sans texte contre tout acte administratif et qui a pour effet d'assurer, conformément aux principes généraux du droit, le respect de la légalité »[20]

La charte doit être adoptée après consultation du comité technique[21] et le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail[22]. Ces comités n'ont qu'un pouvoir consultatif et la décision revient en dernier ressort à l'autorité hiérarchiquement compétente. Néanmoins, leur consultation étant obligatoire dans le cadre d'une charte informatique, le défaut de consultation entacherait la charte d'illégalité.

S'agissant des agents contractuels de l'Etat, ces derniers ne sont pas des fonctionnaires car leur mission prend nécessairement fin, soit par une cessation d'emploi dans la fonction publique, soit par une poursuite d'emploi dans la fonction publique à la suite d'une intégration.

Un agent lié à l'administration peut être un agent public ou un salarié de droit privé.

S'il s'agit d'un agent public, le droit applicable est le droit est le droit public et le juge compétent pour connaître de tout litige est le juge administratif.

[18] CE sec.7-2-1936 n° 433211 Jamart
[19] Jurisclasseur administratif, fascicule 106-10 Notion d'acte administratif n°10.
[20] CE sec. 17-2-1950 n° 86949 Dame Lamotte.
[21] Article 15 de la loi n°84-16 du 11 janvier 1984
[22] Article 16 de la loi n°84-16 du 11 janvier 1984

Les agents publics non titulaires sont soumis au décret n°86-83 du 17 janvier 1986, et notamment aux **articles 43, 43-1, 43-2, 44** du titre relatifs à la suspension et la discipline.

Selon les dispositions desdits articles, l'agent non titulaire est soumis, , à l'obligation d'obéir aux instructions qui lui sont données, sauf en ce qui concerne les ordres manifestement illégaux et de nature à compromettre l'ordre public[23].

En conséquence, l'agent non titulaire devra se conformer à la charte informatique, de la même manière que le fonctionnaire.

S'il s'agit d'un agent de droit privé, sa situation s'apparente à celle d'un salarié travaillant dans une entreprise. Il est soumis au Code du travail. La procédure d'implémentation de la charte est la même que celle relative aux salariés.

La particularité du personnel informatique

Les meilleures pratiques en la matière consistent donc à côté de la charte destinée à l'ensemble des personnels, à **adopter une charte spécifique dite « charte administrateur »** ou encore **« charte des droits d'administration »**.

Il apparaît nécessaire de responsabiliser l'administrateur aussi bien par la technologie (filtrage, contrôle des accès et des usages) que par un encadrement de la règle du jeu sur un plan contractuel.
La charte administrateur est un complément indispensable à la charte des utilisateurs car si tout administrateur est un utilisateur, tous les utilisateurs ne sont pas des administrateurs ou dotés de droits d'administration.

De fait, il convient de déterminer les droits et obligations des administrateurs et des personnes disposant d'un droit d'administration : **ils doivent pouvoir être protégés de tous risques d'atteintes à la vie privée** mais également pouvoir être sanctionnées en cas d'abus des moyens dont ils disposent.

La charte administrateur ne repose sur aucune réglementation en particulier, et s'inscrit dans le cadre de la meilleure pratique du moment dans le domaine de la responsabilisation des acteurs de la sécurité des Systèmes d'information.

Le recours à la contractualisation de l'obligation de confidentialité pesant sur l'administrateur, notamment dans une charte administrateur est également consacré par la Commission Nationale de l'Informatique et Libertés dans le cadre du guide pour les employeurs et les salariés Edition 2008 et particulièrement de la fiche pratique n° 7.

La charte administrateur, faisant l'objet d'une acceptation par l'administrateur, doit nécessairement aborder au minima les thématiques suivantes : les prérogatives, les engagements et les responsabilités de l'administrateur.

Elle permet également de responsabiliser les administrateurs pour leur propre usage étant rappelé que la jurisprudence a déjà sanctionné :

- Un administrateur du réseau informatique pour la présence de fichiers en provenance d'Internet approchant les 6 GO d'images, de sons, de vidéos et de progiciels laissant présager un téléchargement 24h/24 et 7 jours/7 depuis le poste administrateur[24]

[23] Jursiclasseur Administratif Fascicule 193 Agents non titulaires n°65

- Un administrateur réseau pour atteinte à un système de traitement automatisé de données alors même que l'accès a été rendu possible du fait de sa fonction d'administrateur[25]

L'IMPLEMENTATION « COLLECTIVE »

La charte informatique est destinée à être diffusé auprès de tous les utilisateurs des ressources informatiques.

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.

Le principe de discussion collective

Il s'agit de soumettre la Charte aux instances représentatives du personnel (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 Internet, son champ d'application, ses principes, ainsi que son déploiement.

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.

Le principe de transparence

Il s'agit de diffuser la Charte auprès des utilisateurs, comme un règlement intérieur s'il en existe un (article L1321-5 du Code du travail) :

- individuellement, avec le bulletin de salaire ou grâce à un outil de diffusion individuelle de la Charte en ligne par exemple,

[24] CA Paris 22ème chambre, 4 10 2007.
[25] TGI Rennes 21 2 2008 n°03-52216

- collectivement, à une place facilement accessible sur le lieu de travail et/ou sur l'intranet.

Les démarches supplémentaires à destination des entreprises et des administrations employant des agents de droit privé :

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.

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.

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 (ou la hiérarchie), 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) soit comme 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.

CE QU'IL FAUT RETENIR

ADOPTER UNE CHARTE QUI INTEGRE LE FILTRAGE. LA CHARTE NE SE DECLARE PAS A LA CNIL

LA PROTECTION DES LANCEURS D'ALERTE

La personne, administrateur ou non, en charge de la gestion du filtrage et des éventuelles alertes mises en œuvre peut être confrontée à une situation la conduisant à dénoncer des faits, notamment répréhensibles, à son supérieur hiérarchique ou à une autorité tierce à l'entreprise (exemple : signalement d'un délit commis sur internet). Dans cette hypothèse ladite personne pourrait être qualifiée de lanceur d'alerte. Un régime spécial de protection doit alors s'appliquer conformément à la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Un lanceur d'alerte est « une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice

graves pour l'intérêt général, dont elle a eu personnellement connaissance » (article 6 de la loi n° 2016-1691).

Le lanceur d'alerte bénéficie d'un régime de protection particulier :

- il n'est pas pénalement responsable s'il « porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte » (article 122-9 du code pénal);
- les procédures mises en œuvre pour recueillir les alertes doivent garantir une stricte confidentialité de l'identité du lanceur d'alerte, des personnes visées par l'alerte et des informations recueillies par l'ensemble des destinataires de l'alerte (article 9 de la loi n° 2016-1691);
- le lanceur d'alerte « ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir signalé une alerte » (article 10 de la loi n° 2016-1691).

L'article 8 de la loi n° 2016-1691 précise enfin que « le signalement d'une alerte est porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci ». Si le supérieur ne prend aucune mesure dans un délai raisonnable afin de traiter l'alerte, l'alerte peut être adressée à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. En dernier ressort, l'alerte pourra être rendue publique.

ETAPE 4 : L'ADMINISTRATION ET PARAMETRAGE DE LA SOLUTION

Une fois l'implémentation juridique de la mise en œuvre des outils de filtrage traitée (droit du travail et droit Informatique et Libertés en particulier), encore faut-il que les modalités d'utilisation même de la solution soient respectueuses des dispositions réglementaires.

Plusieurs autres zones de risque juridique sont ici à traiter :

- **Le niveau de paramétrage** et la qualité des listes d'exclusions
- **Le traitement égalitaire des utilisateurs**
- **L'utilisation précontentieuse ou contentieuse** des éléments issus des de filtrage utilisés.

LE NIVEAU DE PARAMETRAGE ET LA QUALITE DES LISTES D'EXCLUSION

Sur la première problématique, il faut rappeler que la constitution de listes d'exclusions n'est pas un acte aussi anodin qu'il n'y paraît.

S'il est normal, voire obligatoire d'interdire l'accès à un certain nombre de contenus (pédopornographie, racisme, révisionnisme, terrorisme, contrefaçon…) certaines restrictions portent en elle l'essence même d'une discrimination.
Ainsi, créer des listes d'exclusion autour de thématiques telles que l'homosexualité pourrait être considéré comme attentatoire aux libertés les plus fondamentales des individus voire discriminatoires ou encore homophobes.

LE TRAITEMENT EGALITAIRE DES UTILISATEURS

Sur la seconde problématique, qui découle de la première, il est essentiel d'assurer le même niveau de paramétrage de la solution pour tous les utilisateurs occupant un même poste, afin de ne pas discriminer les utilisateurs.
Cependant, si de par l'utilisation qu'il fait d'Internet, un utilisateur mettait en péril la sécurité du système d'information de l'entreprise ou de l'établissement, ce motif pourrait justifier une éventuelle intervention de l'administrateur visant à limiter les accès Internet de cet utilisateur.

Sur ce point, il conviendra d'avoir préalablement informé l'employé de cette possibilité, par exemple en prévoyant un paragraphe spécifique dans la charte « utilisateur » à cet effet.

LA CONSERVATION DES PREUVES

Sur la troisième problématique, il faut préciser que le droit de la preuve en matière précontentieuse ou contentieuse est un droit extrêmement rigoureux qui ne laisse la place à aucun doute particulièrement quand il s'agit de sanctionner un employé en application du code du travail.

Les conditions dans lesquelles ces éléments de preuve peuvent être apportés doivent être rigoureusement définies au sein de l'entreprise, dans ce que l'on peut appeler un guide de maintien des preuves.

Ce document est destiné à centraliser l'ensemble des meilleures pratiques en la matière (appel à un huissier, saisine des autorités compétentes, présence du personnel lors d'opérations de contrôle, conditions dans lesquelles des copies peuvent être réalisées…) et doit donc comporter des mentions particulières s'agissant des informations et données traitées à travers les outils de filtrage.

ETAPE 5 : LA GESTION DES LOGS

Il convient de regarder une combinaison de dispositions afin de répondre précisément à la question de savoir si l'employeur doit conserver les données relatives à l'utilisation d'Internet par ses salariés.

Cette difficulté résulte en particulier de la combinaison des dispositions :

- **Du Code des postes et des communications électroniques, modifié par la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme** et portant disposition diverses relatives à la sécurité et aux contrôles frontaliers
- **De l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004** et son décret d'application du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne[26]

Ces dispositions visent en partie les mêmes acteurs, dont le fournisseur d'accès, mais selon des approches différentes, qui ne coïncident pas.

L'article 6-I.-1 de la LCEN fait référence notamment aux « personnes dont l'activité est d'offrir un accès aux services de communication ».[27]

De son côté, **l'article L. 34-1 du Code des postes et communications électroniques** vise :

- Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, dans son alinéa 1er
- Mais également les acteurs « assimilés » à des opérateurs de communications électroniques qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, à l'alinéa 3 du paragraphe II

La définition de l'opérateur telle que prévue par **l'article L. 34-1 du Code des postes et communications électroniques** apparaît donc beaucoup plus large que celle posée à l'article 6 de la LCEN et il est difficile de déterminer les frontières de la notion de fournisseur d'accès.

Ces difficultés d'interprétation sont d'ailleurs accentuées par l'incertitude persistante quant au champ d'application desdits textes, et leur applicabilité aux employeurs.
Comme il a déjà été précisé, la question n'est en effet toujours pas tranchée s'agissant de la qualification possible de fournisseur d'accès d'un employeur donnant accès à Internet à ses employés, comme le rappelle la jurisprudence[28].

[26] Décret modifié par le Décret n ° 2014-1576 du 24 12 2014
[27] Renvoyant à la LCEN, art 6 I.1°

En pratique, afin de préserver sa responsabilité et donc pouvoir de contrôle et de direction, l'employeur doit être capable de retrouver a posteriori si l'origine d'un dommage ou d'un acte illicite ou contrevenant à la charte des Systèmes d'information, provenait de son organisation interne.

Dans ce contexte, et en l'absence de réponse jurisprudentielle claire, il est possible de relever que :

- **Le décret n° 2011-219 relatif à la conservation et à la communication des données** permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne du 25 février 2011 : portant application de l'article 6 de la loi n° 2004-575 du 25 juin 2004 pour la confiance dans l'économie numérique prévoit dans son article 3 **une durée d'un an** à compter du jour de la création des contenus
- **La CNIL** préconise une durée de conservation de **six mois** s'agissant de la conservation de données permettant le contrôle par l'employeur de l'utilisation d'Internet faite par ses employés (logs de connexions)[29]

Aux termes du **décret n° 2011-219 relatif à la conservation et à la communication des données**, les fournisseurs d'accès à Internet doivent conserver **pendant un an** à compter du jour de la création des contenus, pour chaque connexion de leurs abonnés, les données suivantes:

- L'identifiant de la connexion
- L'identifiant attribué par les fournisseurs d'accès à Internet à l'abonné
- L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès
- Les dates et heures de début et de fin de la connexion
- Les caractéristiques de la ligne de l'abonné

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement doivent aussi **conserver pendant un an** à compter du jour de la résiliation d'un contrat ou de la fermeture d'un compte par un utilisateur, les informations fournies lors de sa souscription ou lors sa création à savoir :

- Au moment de la création du compte, l'identifiant de cette connexion
- Les nom et prénom ou la raison sociale
- Les adresses postales associées
- Les pseudonymes utilisés
- Les adresses de courrier électronique ou de comptes associés
- Les numéros de téléphone
- Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour

Enfin, lorsque la souscription d'un contrat ou d'un compte est payante, les fournisseurs d'accès à Internet et les fournisseurs d'hébergement doivent **conserver pendant un an** à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement, les informations suivantes :

[28] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005.
[29] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010 p. 18

- Le type de paiement utilisé
- La référence du paiement
- Le montant
- Date et heure de la transaction

ETAPE 6 : LE MAINTIEN EN CONDITIONS OPERATIONNELLES

Il est indispensable d'assurer un maintien en conditions opérationnelles de la solution de filtrage et de sa conformité au droit.

Il s'agit en particulier de s'assurer de la conformité légale du paramétrage et des procédures permettant d'assurer l'utilisation précontentieuse ou contentieuse des éléments issus des outils de filtrage mis en œuvre.

LES REGLES D'OR DU FILTRAGE : COMMENT PROTEGER SON ORGANISATION DE L'USAGE D'INTERNET CONFORMEMENT AU DROIT ?

AVOIR LES MOYENS DE REGULER L'ACCES A CERTAINS SITES ET SERVICES (FILTRAGE)

AVOIR LES MOYENS TECHNIQUES D'AUTHENTIFIER ET DE CONSERVER LES LOGS

DANS UNE DÉMARCHE LÉGALE
EGALITAIRE ET NON DISCRIMINATOIRE

Déclaration CNIL de l'outil*

Choisir la déclaration normale pour tous les outils de surveillance et de contrôle individuel.

Il suffit de noter le numéro de récépissé pour mettre en œuvre la solution.

Discussion collective

Consulter les institutions représentatives du personnel concernant la charte et l'outil.

Un avis négatif n'empêche pas le déploiement de ladite charte et de la solution

Information des salariés

Rédiger une charte informatique et la diffuser individuellement et collectivement après l'avoir soumise pour avis aux institutions représentatives du personnel.

* Registre des traitements à partir du 25 mai 2018 (entrée en vigueur du RGPD)

POUR ALLER PLUS LOIN…

Découvrez nos 3 autres volumes sur les enjeux juridiques du filtrage Internet :

Volume I :
Droit de filtrer, droit de loguer

Volume II :
Nouveaux usages et filtrage

Volume III :
Ne pas filtrer, ne pas loguer :
conséquences

Disponibles au téléchargement via le lien suivant :
https://www.olfeo.com/proteger-votre-entreprise/maitriser-les-enjeux/juridique/demande-telechargement-du-livre-blanc

Le cabinet Alain Bensoussan et Olfeo publient également un guide de la charte informatique.

Découvrez dans ce guide quelles sont les bonnes pratiques en matière de charte, comment aborder la rédaction de la charte ? Comment la rendre opposable aux salariés ? …

http://www.olfeo.com/sites/olfeo/files/pdf/guide-charte-informatique-olfeo.pdf

A PROPOS D'OLFEO

Olfeo est éditeur de logiciel et expert de la sécurité web et du filtrage de contenus. Chez Olfeo, nous croyons que la sécurité positive est le meilleur moyen de vous protéger contre les nouvelles menaces du web tout en accompagnant les nouveaux usages chez vos collaborateurs.

Notre solution a aujourd'hui été adoptée par 2000 clients, représentant plus de 3 millions d'utilisateurs.

Il est dans notre ADN de considérer les projets de sécurité web au-delà des seuls aspects fonctionnels et techniques. Pour cela, nous proposons aux organisations exigeantes, la seule passerelle de sécurité Web basée sur une infrastructure proxy qui réunit à la fois l'expertise technologique, la conformité légale et culturelle ainsi que le facteur humain au service de la sécurité positive.

La sécurité positive doit être vue au sens large du terme. C'est l'approche novatrice d'Olfeo qui réunit ces trois enjeux fondamentaux de la sécurité Web dont deux d'entre eux sont trop souvent négligés dans beaucoup d'autres solutions. Olfeo est ainsi la seule solution qui peut réellement créer un environnement de confiance pour vos utilisateurs sur le Web.

Notre objectif est double : nous améliorons la fiabilité de votre sécurité web et nous accompagnons vos utilisateurs pour faire évoluer leurs pratiques et les responsabiliser dans leurs usages.

Notre passerelle de sécurité web, basée sur une infrastructure Proxy inclut les modules suivants :

- Proxy Cache QoS et déchiffrement SSL
- Filtrage d'URL
- Filtrage DNS
- Filtrage Protocolaire
- Antivirus de flux
- Portail Public

Retrouvez des actualités juridiques, métier et produit sur nos réseaux sociaux :

www.linkedin.com/company/olfeo

https://twitter.com/olfeo

www.youtube.com/user/OlfeoTV

www.facebook.com/societeolfeo

A PROPOS DU CABINET D'AVOCATS LEXING ALAIN BENSOUSSAN

Ce livre blanc a été co-écrit en collaboration avec le cabinet d'avocats Alain Bensoussan. 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.

Le cabinet a reçu le Premier prix dans la catégorie « Technologies de l'information – Médias & Télécommunications », Palmarès des cabinets d'avocats d'affaires en 2015, 2014 et 2013 (Le Monde du Droit) et le Client Choice Awards en 2014 dans la catégorie « Information Technology »

Deux avocats spécialisés dans le Droit des technologies et la Sécurité des Systèmes d'informations ont participé à l'élaboration de ce livre blanc juridique :

Maître Eric Barbry

Avocat au Barreau de Paris
Directeur du Pôle « Droit du numérique »

Maître Polyanna Bigle

Avocat au Barreau de Paris.
Directeur du Département « Sécurité des Systèmes d'information et dématérialisation »

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, entre autres, le premier traité de droit de l'informatique en 1985, puis « Informatique, Télécoms, Internet » (1997, 2001, 2004, 2008, 2012), « Informatique et Libertés » (2008, 2010, 2014) ou encore le « Code de la sécurité informatique et télécom » aux Editions Larcier en 2016. 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.

En 2015, la revue juridique américaine « Best Lawyers » confirme pour la 5ème 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.

Plus récemment, le cabinet a reçu le Premier prix dans la catégorie « Technologies de l'information – Médias & Télécommunications » du Palmarès
des cabinets d'avocats d'affaires en 2016, 2015, 2014 et 2013 (Le Monde du Droit) et le Client Choice Awards en 2014 et 2016 dans la catégorie « Information Technology »

Enfin, Alain Bensoussan a été distingué, en tant que Best Lawyer en Droit des Technologies de 2011 à 2015 et Law Firm of the Year pour l'année 2017 par la revue juridique américaine « Best Lawyers ».

www.alain-bensoussan.com

Réseau Lexing : network.lexing.eu/?lang=fr


www.youtube.com/channel/UC7xrTpr0LGPWVNbYxxDcFVQ