UBIFRANCE
L'Agence française pour le développement international des entreprises

CHARTE

UTILISATION DU SYSTEME D'INFORMATION

GUIDE JURIDIQUE DE L'UTILISATEUR

Table des matières

AVANT-PROPOS

1. Ubifrance a déployé une charte d'utilisation du système d'information.

2. Afin de faciliter la bonne compréhension de cette charte, Ubifrance a rédigé le présent document intitulé « guide juridique », dont l'objectif est de présenter les règles de droit qui ont présidé à la rédaction de cette charte, ainsi que les risques liés au non-respect de ces règles.

3. Il est donc recommandé à chaque utilisateur de procéder à une lecture attentive de ce guide.

4. Ce guide, bien qu'il s'efforce d'être exhaustif, ne saurait cependant être considéré comme limitatif. En effet, compte tenu de la multiplicité des règles relatives au bon usage des ressources informatiques et de communication électronique, il appartient avant tout à l'utilisateur d'adopter en toutes circonstances un comportement prudent et avisé, en sollicitant au besoin l'aide du Directeur des systèmes d'information.

5. Chaque utilisateur est supposé avoir pris connaissance du présent guide accessible sur l'Intranet d'Ubifrance.

1 PREAMBULE

6. Ubifrance met à la disposition des utilisateurs, dans le cadre de leur activité professionnelle, des ressources informatiques et de communication électronique, dont l'usage est source de responsabilité.

7. Les faits commis sont en effet susceptibles d'entraîner la mise en cause de sa responsabilité civile[1] ou pénale[2] tant d'Ubifrance que des utilisateurs.

8. Il est, en revanche, important de préciser que le statut de salarié[3] ne protège en aucune manière l'utilisateur d'une mise en cause de sa responsabilité civile ou pénale en cas d'utilisation illicite de ces moyens.

9. Il existe donc une obligation pour Ubifrance de définir les règles d'utilisation de ses ressources informatiques et de communication électronique aux fins de la préserver, ainsi que les utilisateurs, de toute mise en cause de leur responsabilité respective.

10. Il s'agit précisément de l'objet de la charte dont les fondements juridiques sont exposés dans le présent guide juridique.

11. L'utilisation desdits moyens doit ainsi répondre à un référentiel qui inclut notamment :

- la législation et la réglementation en vigueur ;
- la jurisprudence ;
- les recommandations d'organismes compétents ;
- les meilleures pratiques du domaine.

[1] Article 1384 du Code civil : « 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, ou des choses que l'on a sous sa garde. Toutefois, celui qui détient, à un titre quelconque, tout ou partie de l'immeuble ou des biens mobiliers dans lesquels un incendie a pris naissance ne sera responsable, vis-à-vis des tiers, des dommages causés par cet incendie que s'il est prouvé qu'il doit être attribué à sa faute ou à la faute des personnes dont il est responsable. Cette disposition ne s'applique pas aux rapports entre propriétaires et locataires, qui demeurent régis par les articles 1733 et 1734 du code civil. Le père et la mère, en tant qu'ils exercent l'autorité parentale, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux. Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ; Les instituteurs et les artisans, du dommage causé par leurs élèves et apprentis pendant le temps qu'ils sont sous leur surveillance. La responsabilité ci-dessus a lieu, à moins que les père et mère et les artisans ne prouvent qu'ils n'ont pu empêcher le fait qui donne lieu à cette responsabilité. En ce qui concerne les instituteurs, les fautes, imprudences ou négligences invoquées contre eux comme ayant causé le fait dommageable, devront être prouvées, conformément au droit commun, par le demandeur, à l'instance. »

[2] L'article L. 121-2 du Code pénal dispose : « Les personnes morales, à l'exclusion de l'État, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants. (…) 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. »

[3] Cette mise en garde est également valable pour les stagiaires, intérimaires, intervenants extérieurs tels que les consultants, prestataires ou auditeurs.

12. Sans que cette liste ait un caractère exhaustif, les réglementations applicables sont relatives :

- à la protection des systèmes d'information, et notamment à la fraude informatique, qu'il s'agisse de l'intrusion dans un système d'information ou de l'altération des informations qu'il contient, étant précisé que ces actes sont passibles de sanctions pénales ;

- à la propriété intellectuelle, et notamment aux droits d'auteur qu'il s'agisse de créations multimédia, de logiciels, de textes, de photos, d'images ou d'œuvre de toute autre nature ;

- aux libertés individuelles, et notamment aux dispositions légales en matière de traitements de données à caractère personnel ;

- au respect des règles d'ordre public en matière de contenu des informations qui seraient susceptibles d'être mises en ligne sur le réseau, telles que des informations à caractère pornographique ou portant atteinte à l'intégrité ou à la sensibilité d'un autre utilisateur par accès à des messages, images ou textes provocants ;

- au respect des principes de liberté du commerce et de l'industrie, ainsi que de liberté de la concurrence, qui sont limités par l'interdiction d'utiliser tous procédés contraires aux usages loyaux du commerce nuisant notamment à un concurrent (dénigrement, utilisation de signes distinctifs, imitation de produits concurrents, divulgation et exploitation de savoir-faire, appropriation de clientèle, débauchage de personnel, , etc..).

13. Ces dernières années, la Cour de cassation a rendu de nombreuses décisions sur l'utilisation des ressources informatiques et de communication électroniques à des fins personnelles[4], ainsi que sur la preuve de la faute du salarié par des procédés informatiques.

14. A plusieurs reprises, la Cour de cassation s'est prononcée sur la problématique de l'usage professionnel et l'usage non professionnel de ces moyens.

15. Deux organismes œuvrent également à la réflexion sur, d'une manière générale, la problématique de la cybersurveillance dans le domaine du travail, à savoir la Commission nationale de l'informatique et des libertés (Cnil)[5] et le Forum des droits sur l'internet[6].

16. La Cnil a publié en 2008 un guide, présenté sous formes de fiches pratiques sur des thématiques clés, à destination des employeurs et des salariés[7]. Ces fiches traitent des données à caractère personnel dans l'univers spécifique des dispositifs de contrôle des salariés liés aux

[4] Un arrêt a marqué le développement du contentieux en la matière en ce qu'il est considéré comme l'arrêt fondateur du concept de « vie privée résiduelle », soit : Cass. soc.2-10-2001 n° 99-42942 dit arrêt « Nikon ».
[5] Le site internet de la Cnil est accessible à l'adresse suivante : www.cnil.fr.
[6] Le Forum des droits sur l'internet est une association, participant à la corégulation de l'internet. Il associe, dans une structure de gouvernance innovante, représentants de l'État, du secteur privé et de la société civile. Son domaine de compétence couvre l'ensemble des aspects de politique publique liés au développement de la société numérique sur le plan des contenus et des usages (http://www.foruminternet.org).
[7] Guide pour les employeurs et les salariés, Cnil, 2008.

nouvelles technologies. L'objectif est, d'une part, de répondre à un souci de transparence et de confiance à l'égard des salariés, et d'autre part, de garantir la sécurité juridique pour les entreprises, en leur qualité de responsables de traitement.

17. Le 12 octobre 2009, la Cnil a publié sur son site web « 10 conseils pour sécuriser votre système d'information ».[8]

18. Sans entrer dans le détail de ces 10 conseils, il convient de relever que les conseils n°9 et 10, respectivement « anticiper et formaliser une politique de sécurité du système d'information » et « sensibiliser les utilisateurs aux risques informatiques et à la loi informatique et libertés », suggèrent à l'entreprise d'aller au-delà de la simple rédaction d'une charte et de mettre en place une véritable gouvernance de la sécurité, les utilisateurs du système d'information devant être particulièrement sensibilisés aux risques informatiques.

19. Le Forum des droits sur l'internet s'est, quant à lui, intéressé dès 2001 à l'impact du développement des nouvelles technologies sur les relations du travail et a publié l'année suivante un rapport sur les relations du travail et internet[9]. Il posait les jalons d'une réflexion sur les règles et usages à développer. Il estimait alors vain de vouloir prohiber un usage personnel d'internet par les salariés et esquissait les limites de cet usage en rappelant le pouvoir de contrôle de l'employeur, dès lors qu'il est guidé par les principes de proportionnalité et de loyauté posés par le Code du travail.

20. Il en ressort, par ailleurs, des meilleures pratiques en ce domaine qu'il est opportun d'extraire des règlements intérieurs, les règles relatives à l'usage des ressources informatiques et de communication électronique, lesquelles doivent faire l'objet d'un document spécifique.

21. Les nécessaires évolutions de ce référentiel, et notamment de la loi et de la jurisprudence dominante, expliquent qu'Ubifrance se réserve le droit de faire évoluer, dans un souci de conformité, la charte sur l'utilisation des ressources informatiques et de communication électronique.

22. Enfin, la complexité, tant sur le plan juridique que technique, des règles en question explique qu'Ubifrance ait pris l'initiative de diffuser deux documents explicatifs, soit le présent guide et son pendant technique, le livret des procédures qui a pour objectif d'exposer sur un plan pratique les principes de mise en œuvre des règles définis dans la charte.

2 PORTEE ET OPPOSABILITE

23. En application de l'article L. 1321-1 du Code du travail :

- « Le règlement intérieur est un document écrit par lequel l'employeur fixe exclusivement :

1° Les mesures d'application de la réglementation en matière de santé et de sécurité dans l'entreprise ou l'établissement, notamment les instructions prévues à l'article L. 4122-1 ; (…)

[8] 10 conseils pour sécuriser votre système d'information, Cnil, 12-10-2009.
[9] Relations du travail et internet, Forum des droits sur l'internet, 17-9-2002.

3° Les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions que peut prendre l'employeur. »

24. L'article L. 1321-5 dispose notamment :

- « Les notes de service ou tout autre document comportant des obligations générales et permanentes dans les matières mentionnées aux articles L. 1321-1 et L. 1321-2 sont, lorsqu'il existe un règlement intérieur, considérées comme des adjonctions à celui-ci. Ils sont, en toute hypothèse, soumis aux dispositions du présent titre. »

25. En ce qu'elle définit des « obligations générales et permanentes » aux fins de garantir notamment la sécurité des ressources informatiques et de communication électronique mis à disposition par Ubifrance, obligations sanctionnées le cas échéant sur le plan disciplinaire, la charte d'utilisation du système d'information constitue annexe au règlement intérieur. [10]

26. Elle a été portée à la connaissance des utilisateurs, et est entrée en vigueur, dans les conditions fixées par Ubifrance dans l'article « entrée en vigueur » de ladite charte.

27. En ce sens, elle ne doit pas être assimilée à un accord d'entreprise autorisant l'expression syndicale par voie électronique[11].

3 DOMAINE D'APPLICATION DE LA CHARTE

28. Le périmètre de l'application de la charte d'utilisation du système d'information mise à disposition par Ubifrance est défini au regard des trois paramètres exposés ci-après.

3.1 Personnes concernées

29. Une distinction doit être opérée ici entre les personnels d'Ubifrance et les personnels extérieurs.

30. La charte, sous réserve de respecter la procédure d'opposabilité évoquée plus haut, s'applique en l'état aux salariés d'Ubifrance.

31. Des personnes extérieures à Ubifrance peuvent également avoir accès aux ressources informatiques et de communication électronique, et à ce titre, doivent en faire un usage légitime.

[10] Notamment : information et consultation préalable des instances représentatives du personnel ; communication à l'inspection du travail ; dépôt au secrétariat du Conseil des Prud'hommes ; publicité et affichage au sein d'Ubifrance.

[11] Art. L.2142-6 du Code du travail : « Un accord d'entreprise peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mis en place sur l'intranet de l'entreprise, soit par diffusion sur la messagerie électronique de l'entreprise. Dans ce dernier cas, cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne doit pas entraver l'accomplissement du travail. L'accord d'entreprise définit les modalités de cette mise à disposition ou de ce mode de diffusion, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou de refuser un message. »

32. L'opposabilité de la charte à ce type d'utilisateur répond à des mécanismes différents :

- pour les prestataires techniques : dans les contrats d'assistance technique, l'entreprise prestataire doit se porter fort du respect par son personnel des règles applicables à Ubifrance, et notamment de son règlement intérieur et de sa charte d'utilisation du système d'information ; par ailleurs, ce règlement intérieur et cette charte pourraient être annexés au contrat liant Ubifrance et le prestataire technique ;

- pour les autres catégories (travailleurs indépendants, stagiaires, etc.) : ils doivent individuellement accepter cette charte.

33. Enfin, la charte d'utilisation du système d'information d'Ubifrance a été complétée par une charte des droits d'administration.

34. En effet, la pratique[12] conduit à la mise en place d'une charte spécifique car ils bénéficient d'habilitations étendues d'administration. La charte des droits d'administration crée des obligations spécifiques, notamment une obligation de confidentialité renforcée sur les données ou informations que les administrateurs recueillent dans le cadre de leur activité.

3.2 Moyens concernés

35. La charte vise toutes les ressources informatiques et de communication électronique utilisées à des fins professionnelles :

- mises à disposition par Ubifrance,
- personnelles aux utilisateurs mais dont l'utilisation a été expressément autorisée par Ubifrance.

3.3 Usages concernés

36. Il s'agit de définir la « localisation » de l'utilisation des ressources informatiques et de communication électronique, à savoir :

- dans les locaux d'Ubifrance quels qu'ils soient ainsi que les bureaux en France (par exemple les Chambres de commerce et de l'industrie) et à l'étranger (les Missions Economiques) ;

- dans le cadre d'un usage dit nomade (ordinateur portable par exemple) ;

- le cas échéant en accès distant quelque soit le lieu de la connexion (rendez-vous extérieur, domicile, etc.).

37. Les deux dernières hypothèses impliquent de la part des utilisateurs une particulière vigilance. La vulnérabilité des moyens, ainsi que des informations qu'ils contiendraient ou

[12] Par exemple, la fiche 7 du guide de la Cnil pour les employeurs et les salariés est consacrée aux administrateurs réseau.

seraient amenés à diffuser, est en effet plus grande que pour les moyens fixes et/ou utilisés dans les locaux d'Ubifrance, sous le contrôle permanent de cette dernière.

4 REGLES D'UTILISATION DU SYSTEME D'INFORMATION

38. La problématique majeure est la distinction entre l'usage professionnel et l'usage non professionnel des ressources informatiques et de communication électronique mis à disposition par Ubifrance en vue de l'accomplissement des tâches confiées aux utilisateurs.

39. Par deux décisions du 18 octobre 2006[13], la Cour de cassation a précisé que les dossiers et fichiers créés par un salarié, grâce aux outils informatiques et de communication électronique mis à sa disposition par son employeur pour l'exécution de son travail, sont présumés, sauf si le salarié les identifie comme personnels, avoir un caractère professionnel. Il en résulte que l'employeur peut y avoir accès hors sa présence.

40. De fait, si la Cour de cassation légitime, d'un côté, le droit d'accès de l'employeur aux fichiers et aux messages électroniques reçus et émis par ses salariés, elle légitime, de l'autre côté, l'utilisation de ces mêmes outils à des fins personnelles, au nom du principe communément dénommé « vie privée résiduelle »[14].

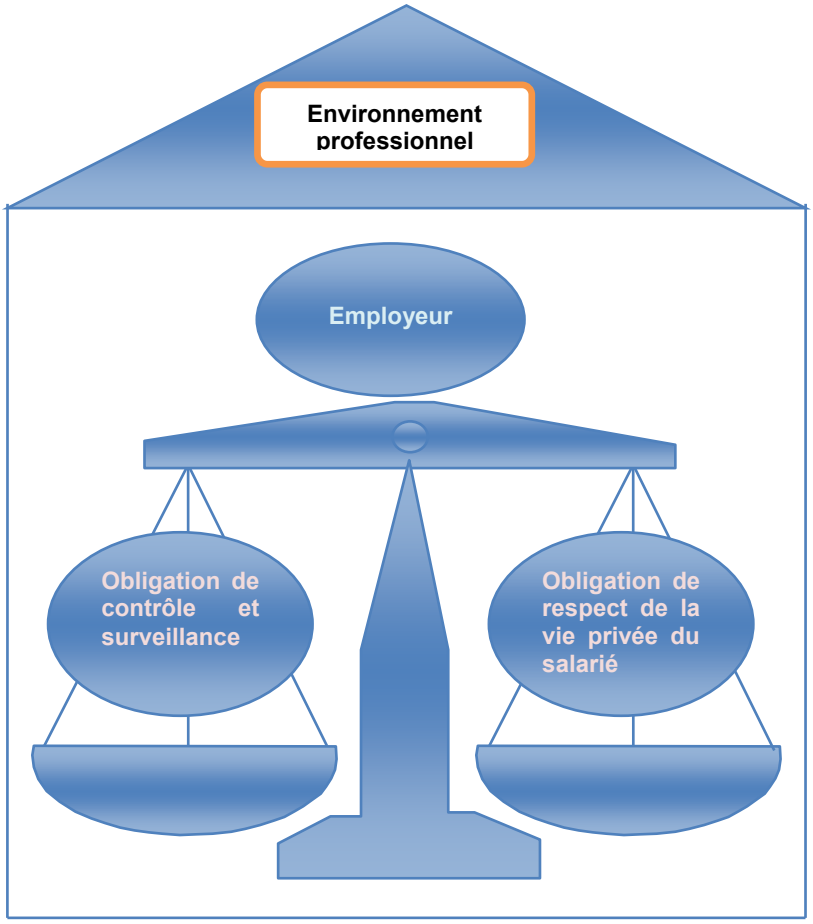
41. La Cour de cassation concilie les intérêts de l'employeur, pouvant mettre en place des dispositifs de contrôle de l'activité de ses salariés afin de réduire les risques d'engagement de sa responsabilité, et les droits fondamentaux des salariés tenant entre autre au respect de leur vie privée, principe protégé tant au niveau national[15] qu'au niveau européen[16].

[13] Cass. soc. 18-10-2006 n°04-48025 : « Les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence » ; Cass. soc. 18-10-2006 n°04-47400 : « Les documents détenus par le salarié dans le bureau de l'entreprise mis à sa disposition sont, sauf lorsqu'il les identifie comme étant personnels, présumé avoir un caractère professionnel, e sorte que l'employeur peut y avoir accès hors de sa présence ».

[14] Cass. soc.2-10-2001 n° 99-42942 dit arrêt « Nikon »: « (…) 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 ».

[15] Soit notamment le Code civil (art.9 et 1384), le Code pénal (art. 226-15 et 432-9), le Code du travail (art.L. 2323-13) et la loi dite « Informatiques et libertés ».

[16] Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (art. 8).



42. Il convient ici de relever que le droit au respect de la vie privée, en ce compris le respect des correspondances privées, s'applique non seulement dans la relation entre l'employeur et ses salariés, mais également dans les relations entre salariés sous peine d'engager sa responsabilité civile et pénale, et de subir des sanctions disciplinaires.

43. Il est donc indispensable pour les entreprises de bien déterminer la frontière entre l'usage professionnel et l'usage personnel des outils qu'elles mettent à disposition.

44. En pratique, deux grandes tendances coexistent au sein des entreprises :

- certaines d'entre elles ont défini une règle de nommage des fichiers et messages électroniques personnels, en imposant à leurs salariés d'utiliser un terme prédéfini pour qualifier ces éléments de « personnel » (le terme le plus répandu étant « privé ») ;

- d'autres entreprises ont fait le choix de considérer que l'adresse électronique fournie par elles est exclusivement réservée à un usage professionnel, tout en permettant et en facilitant l'utilisation de services internet gratuits de type webmail[17].

[17] Le webmail est une interface web rendant possible l'émission, la consultation et la manipulation de courriers électroniques directement sur le web depuis un navigateur

45. Pour des raisons de sécurité, Ubifrance a opté pour une définition des règles de nommage.

46. Il n'en demeure pas moins que l'usage des ressources informatiques et de communication électronique à des fins personnelles, quelles qu'en soient les modalités pratiques, doit demeurer exceptionnel.

4.1 Utilisation professionnelle

47. Dans la droite ligne de la jurisprudence évoquée plus haut, la charte d'utilisation du système d'information pose le principe de sa mise à disposition des utilisateurs réservée à un usage professionnel exclusif.

48. En pratique, cette règle concerne essentiellement :

- la messagerie électronique professionnelle, en l'occurrence « [.]@ubifrance.fr » ;
- internet, et en particulier les services en ligne (sites web, blogs, forum, chats, etc..).

49. La présomption du caractère professionnel de l'usage de ces moyens emporte comme conséquence principale qu'Ubifrance peut y avoir accès, même en dehors de la présence de l'utilisateur en cause. Les conditions d'accès à la messagerie électronique professionnelle sont précisées dans le livret des procédures.

50. Tout service de type Web 2.0 (Twitter, Facebook, etc..) utilisé depuis Ubifrance est présumé être professionnel, en cas d'ouverture d'un compte, les identifiants de connexion doivent être communiqués au responsable hiérarchique de l'utilisateur et à la DSI/RSSI.

4.2 Utilisation privée résiduelle

4.2.1 Principes généraux

51. L'usage du système d'information à des fins non professionnelles est simplement toléré et ce faisant strictement encadré :

- il doit demeurer exceptionnel et raisonnable tant dans la fréquence que dans la durée ;

- il ne doit perturber ni l'activité de l'utilisateur, ni celle de son département, ni celle d'Ubifrance en général ;

- il ne peut être ni lucratif, ni ludique ;

- il ne peut permettre la circulation d'informations professionnelles ;

- il ne doit pas échanger des propos indécents, injurieux ou dénigrants susceptibles de porter atteinte à l'image d'un membre d'Ubifrance, d'Ubifrance elle-même.

52. En cas d'abus avéré, Ubifrance se réserve le droit de suspendre cette tolérance, et de prendre le cas échéant toute sanction adéquate.

53. L'usage des ressources informatiques et de communication électronique à des fins personnelles relève de la seule responsabilité de l'utilisateur, à l'encontre duquel Ubifrance pourra donc se retourner si sa propre responsabilité venait à être recherchée dans ce cadre.

4.2.2 Règle de nommage des données informatiques personnels

54. Les fichiers, répertoires et messages personnels pour être identifiés comme tels doivent comporter la mention « PRIVE ».

55. La conséquence directe de cette mention, qui doit apparaître clairement, est que contrairement aux fichiers professionnels, Ubifrance ne peut, en principe, y accéder sauf dans un certain nombre d'hypothèses.

56. Toutefois, l'identification du caractère privé des dossiers, fichiers ou messages pourrait ne pas dépendre systématiquement de la seule apposition de la mention « personnel ».

57. Une jurisprudence de la Cour de cassation du 8 décembre 2009 a considéré que les fichiers contenus dans un dossier avec le prénom du salarié ne sont pas de nature personnelle.[18]

4.2.3 L'accès aux données informatiques personnels

58. Il ressort de la jurisprudence le principe général selon lequel l'employeur est autorisé à accéder aux fichiers personnels de ses salariés en présence d'un risque avéré en termes notamment de sécurité, de continuité de service, ou d'un risque grave de voir sa responsabilité engagée.[19]

59. Ceci explique que la charte prévoit un tel accès en cas de risque ou évènement particulier.

60. En outre, cet accès est justifié par le principe général de continuité du service qui permet :

- que ces éléments fassent l'objet de conservation technique dans le cadre des procédures de back up (sauvegarde informatique) ou de plans de continuité ou reprise d'activité mises en œuvre au sein d'Ubifrance ;

- à un administrateur ou toute personne « habilitée », d'accéder à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des ressources informatiques et de communication électronique, ce notamment dans le cadre d'opération de maintenance[20].

[18] Cass. soc. 8-12-2009 Alain B. c/ FNGDSB … « ni le code d'accès à l'ordinateur connu des informaticiens de l'entreprise et simplement destiné à empêcher l'intrusion de personnes étrangères à celle-ci dans le réseau informatique, ni l'intitulé des répertoires et notamment celui nommée « Alain », ne permettaient d'identifier comme personnels les fichiers litigieux et n'interdisait leur ouverture en l'absence du salarié (…). »

[19] Cass. soc. 17-5-2005 n°03-40.017 : « Sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

[20] Fiche n°7 du guide pour les employeurs et les salariés, 2008, de la Cnil : « Les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ils sont conduits par leurs fonctions même à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique

61. Enfin, Ubifrance pourra, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'elle y est autorisée par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.)[21].

5 CONDITIONS D'ACCES ET D'IDENTIFICATION

62. Ubifrance définit :

- les conditions d'accès aux ressources informatiques et de communication électronique mises à disposition par elle ;

- les conditions de suspension et de retrait de cet accès dont elle informera, dans la mesure du possible, l'utilisateur concerné.

63. Une fois cet accès autorisé, l'utilisateur se voit attribuer un identifiant.

64. Compte tenu des enjeux en termes de sécurité, ledit accès est strictement encadré et relève de la seule responsabilité de l'utilisateur.

65. L'utilisateur doit ainsi respecter toutes les consignes de sécurité (changement régulier, choix en dehors de toute référence à l'environnement familier, etc.) diffusées par Ubifrance.

66. Une vigilance accrue est demandée aux bénéficiaires d'un accès à distance, qui doivent suivre toutes les prescriptions complémentaires qui leur seraient signifiées.

67. L'identifiant est strictement confidentiel. Ceci emporte pour conséquence que l'accès aux ressources informatiques et de communication électronique via cet identifiant est réputé avoir été réalisé par le titulaire, qui devra donc assumer la responsabilité d'usage non conforme, sauf à démontrer avoir demandé, préalablement, une suspension ou une suppression de son droit d'accès.

68. En particulier, un usage non conforme peut être assimilé à une atteinte aux systèmes d'information, en tant que systèmes de traitement automatisé de données. Une telle atteinte relève de la réglementation sur la fraude informatique qui sanctionne, entre autre, l'accès illicite, c'est-à-dire toute pénétration dans un système d'information par une personne non autorisée[22].

69. Il n'existe pas d'exception au caractère confidentiel de l'identifiant cependant la Direction des systèmes d'information ou un administrateur du système d'administration pour des raisons de protection, de sécurité ou de continuité du service peut passer outre l'identifiant via un code administrateur.

---

des sites visités, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…). »

[21] Cass. soc. 23-5-2005 n°05-17818

[22] Art. 323-1 et suivants du Code pénal.

70. D'autre part, aux termes de la jurisprudence, dans l'hypothèse notamment de l'absence prolongée pour maladie ou congé sabbatique, il peut être demandé à l'utilisateur son identifiant, dont la rétention constituerait de la part de ce dernier un acte d'insubordination justifiant son licenciement pour faute grave[23].

71. Une cour d'appel a ainsi jugé que repose sur une cause réelle et sérieuse le licenciement prononcé à l'encontre de la salariée qui[24] :

- « en refusant de répondre favorablement à une demande d'information isolée alors que, s'agissant d'un numéro de code d'accès informatique, elle était en mesure d'y répondre sans investigation préalable et savait pertinemment que son refus mettait en difficulté la personne qui la remplaçait et son employeur, la salariée a manqué aux obligations de bonne foi et de loyauté qui lui incombait et n'étaient pas supprimées pendant la suspension de son contrat de travail. »

72. Dans un arrêt du 18 mars 2003[25], la Cour de cassation a retenu la notion de la continuité du service pour sanctionner la non-communication des codes d'accès informatique en considérant que :

- « si le salarié n'est pas tenu de poursuivre une collaboration avec l'employeur durant la suspension de l'exécution du contrat de travail provoquée par la maladie ou l'accident, l'obligation de loyauté subsiste durant cette période et le salarié n'est pas dispensé de communiquer à l'employeur, qui en fait la demande, les informations qui sont détenues par lui et qui sont nécessaires à la poursuite de l'activité de l'entreprise ;

- d'où il suit qu'en statuant comme elle l'a fait, sans rechercher si l'employeur avait effectivement la possibilité, sans recourir à la salariée, d'avoir communication du mot de passe informatique et si de ce fait, comme le soutenait l'employeur en demandant la confirmation du jugement, la salariée n'avait pas eu une volonté de bloquer le fonctionnement de l'entreprise, la cour d'appel a violé les textes susvisés. »

6 GESTION DES ABSENCES ET DES DEPARTS

73. L'utilisation des ressources informatiques et de communication électronique permet l'optimisation de la production au sein d'Ubifrance et une mutualisation de l'information concernant les disponibilités de chacun.

74. Chaque utilisateur doit en conséquence veiller à ce que la continuité du service soit assurée conformément aux modalités d'organisation du service telles que définies par Ubifrance.

75. En cas d'absence d'un utilisateur, quelle qu'en soit la cause et la durée, Ubifrance peut, et ce conformément à la jurisprudence évoquée ci-avant :

[23] Cass. soc. 30-10-2007 n°06-44727 ; V. aussi CA Aix-en-provence 10-4-1997 Trambouze c/ Sarl Technolift.
[24] CA Limoges 22-11-2000 EURL Cabinet de podo orthopédie c/ Badefort.
[25] Cass. soc. 18-3-2003 n°01-41.343.

- accéder aux éléments présents au sein des ressources informatiques et de communication électronique mises à disposition de l'utilisateur concerné, en ce qu'ils sont présumés professionnels ;

- accéder, sous certaines conditions, aux fichiers, répertoires et messages informatiques clairement dénommés « PRIVE » ;

76. A l'annonce du départ d'un utilisateur, Ubifrance peut modifier les droits d'accès et les conditions d'utilisation des ressources informatiques et de communication électronique de ce dernier.

77. Lors de son départ, l'utilisateur perd tout droit d'accès au système d'information et de communication sauf décision contraire de l'autorité hiérarchique de l'utilisateur et s'interdit donc tout accès non autorisé au système d'information et de communication d'Ubifrance au risque de voir sa responsabilité engagée.

7 PRESERVATION DE LA CONFIDENTIALITE ET DU SECRET

7.1 Protection des informations confidentielles

78. La sauvegarde du patrimoine et des intérêts d'Ubifrance passe par le respect, par tous, d'une obligation générale et permanente de confidentialité et de discrétion, à l'égard des informations et documents disponibles au sein d'Ubifrance.

79. Cette obligation de loyauté impose aux utilisateurs le respect d'une discrétion et confidentialité absolue s'agissant de toutes les informations relatives à l'activité d'Ubifrance ou de ses clients et des documents confidentiels de toute nature appartenant à Ubifrance

80. Tout salarié en particulier est tenu, tant pendant l'exécution de son contrat de travail qu'après son départ, pour quelque cause que ce soit (maladie, retraite, démission ou licenciement), à une obligation de loyauté envers son employeur.

81. La violation de cette obligation est passible des sanctions disciplinaires prévues par la loi n°82-689 du 4 août 1982 relative aux libertés des travailleurs dans l'entreprise, dite « loi Auroux ». Les tribunaux ont par exemple jugé qu'un salarié commet une faute grave après avoir communiqué des informations confidentielles depuis sa messagerie professionnelle à une banque concurrente[26].

82. L'utilisateur doit avoir conscience que la révélation d'une information à caractère secret dont il est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende, (article 226-13 du Code pénal).

[26] CPH Nanterre 15-09-2005 RG 03/02028.

7.2 Respect du secret des correspondances

83. L'utilisateur doit s'interdire de prendre connaissance des courriers postaux ou électroniques qui ne lui sont pas adressés, à l'exception de ceux présentant un caractère professionnel et sous réserve qu'il soit habilité à le faire par l'autorité hiérarchique.

84. Constitue une infraction le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende, (article 226-15 du Code pénal).

85. Est également puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

7.3 Respect du régime de la cryptologie

86. Le régime juridique de la cryptologie est réglementé par la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite « loi LCEN ».

87. L'utilisation de moyens de cryptologie est libre depuis la loi LCEN.

88. En revanche, la fourniture, le transfert depuis un état membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à déclaration préalable au Premier ministre, sauf exceptions.

89. L'utilisateur est informé de la possibilité d'utiliser les moyens de cryptologie autorisés par Ubifrance sous réserve du respect des exigences et des conditions d'intégrité et de confidentialité fixées par Ubifrance.

90. La mise en œuvre de systèmes de cryptologie est recommandée tant au titre de la sécurité que pour l'intégrité et la confidentialité dans la transmission de données que de la preuve de ces mêmes données.

91.L'utilisateur ne doit cependant pas utiliser un moyen de cryptologie pouvant perturber l'activité d'Ubifrance.

92. Par ailleurs le régime de la liberté d'utilisation des moyens de cryptologie n'existe pas dans tous les pays. L'utilisateur devra préalablement à toute importation de données cryptées dans un pays étranger vérifier le régime en vigueur pour éviter tout risque de confiscation desdites données.

8 SECURITE DU SYSTEME D'INFORMATION

8.1 obligation générale de sécurité

93. La loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité dispose que « la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ».

94. De même, la loi dite « Informatique et libertés » pose le principe selon lequel le responsable du traitement de données à caractère personnel est tenu de prendre toutes précautions, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et notamment d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

95. Ces obligations pesant Ubifrance justifient les règles de conduite et les interdictions édictées par la charte d'utilisation du système d'information.

96. Il est enfin rappelé qu'un usage non conforme peut être assimilé à une atteinte aux systèmes d'information, en tant que systèmes de traitement automatisé de données. Une telle atteinte relève de la réglementation sur la fraude informatique[27] qui sanctionne notamment :

- L'accès ou le maintien dans un système

97. L'accès illicite, c'est-à-dire toute pénétration dans un système d'information par une personne non autorisée, tel que la connexion pirate, tant physique que logique, l'appel d'un logiciel ou d'un fichier, alors que l'on ne dispose pas de l'habilitation pour le faire.

98. Le maintien frauduleux, c'est-à-dire le maintien au sein d'un système d'information, après un accès illicite et après avoir pris conscience du caractère « anormal » de ce maintien.

99. Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende, (article 323-1 du Code pénal).

100. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende, (article 323-1 du Code pénal).

- L'entrave au fonctionnement

101. L'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système d'information. L'entrave au système est appréhendée de manière extensive, car il suffit d'une influence « négative » sur le fonctionnement du système pour que l'entrave soit retenue. Il en est ainsi pour les bombes logiques, l'occupation de capacité mémoire, la mise en place de codifications, de barrages ou de tous autres éléments retardant un accès normal à un système d'information.

[27] Art. 323-1 et suivants du Code pénal.

102. Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende, (article 323-2 du Code pénal).

- L'altération des informations

103. L'altération des informations est matérialisée par la suppression, la modification ou l'introduction de données pirates, avec la volonté de modifier l'état du système et ce, quelle que soit l'influence.
104. Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende, (article 323-3 du Code pénal).

- La détention de virus

105. Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 du Code pénal est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

9 PLAN DE CONTINUITE D'ACTIVITE

106. L'obligation à la charge d'Ubifrance d'assurer la continuité du service lui confrère le droit, en présence de toute situation susceptible de remettre en cause cette continuité (sinistre, incident majeur, etc.), de prendre toute mesure adéquate[28].

107. Ces mesures sont exceptionnelles, et mises en œuvre pour la durée qu'Ubifrance estime nécessaire pour assurer un retour à un fonctionnement normal de son système d'information.

108. Les utilisateurs sont informés dans la mesure du possible de la nature et de la durée envisagée de la ou des mesures mises en place.

109. Dans tous les cas, ils doivent, sans délai, apporter leur concours, selon les directives fournies, à cette mise en place.

10 MOBILITE ET MATERIELS MIS A DISPOSITION PAR UBIFRANCE

110. Dans le cadre de ses déplacements professionnels, peu importe leur durée ou leur fréquence, l'utilisateur se doit d'adopter une attitude de prudence et de réserve accrue dans l'usage des ressources informatiques et de communication électronique d'Ubifrance.

[28] La charte d'utilisation des moyens informatiques et de communication électronique vise en son article 7 comme mesure entre autre la dégradation de service, la suppression temporaire de l'accès à certaines ressources du système d'information, la mise en œuvre de contraintes exceptionnelles comme le télétravail.

111. A titre d'illustration, l'utilisateur a le devoir de respecter les règles suivantes :

- s'informer, auprès d'Ubifrance, des mesures particulières de sécurité et de sûreté à observer en fonction de sa destination, s'il s'agit d'un pays étranger ;

- adopter la plus stricte discrétion sur Ubifrance et ses activités au sein de celle-ci lorsqu'il est dans des lieux publics, et notamment ne pas travailler sur ou discuter d'éléments confidentiels, secrets, sensibles ou stratégiques en de tels lieux ;

- veiller à utiliser tous les moyens de prévention de vol (câble antivol, coffres d'hôtels) et de protection d'informations disponibles (chiffrement, écrans polarisés) et ne pas laisser ses affaires professionnelles sans surveillance, afin de réduire la probabilité d'un vol de matériel ou d'information et d'en limiter les conséquences ;

- alerter Ubifrance dans les plus brefs délais de tout événement suspect (déplacement d'ordinateur portable ou d'objets personnels dans la chambre d'hôtel, fouille et saisie temporaire d'ordinateurs au contrôle des douanes, intérêt manifeste et questionnement sur Ubifrance de la part de voyageurs tiers, etc.), ainsi qu'en cas de perte ou de vol de matériel.

112. L'utilisateur est, par ailleurs, averti du fait que les formalités douanières de certains pays étrangers (USA et Chine notamment) permettent, en toute légalité, aux agents assermentés de ces pays, de procéder à une saisie temporaire des matériels informatiques afin d'en examiner le contenu et d'en établir une copie intégrale. L'utilisateur doit se soumettre à ces formalités sans réserve. Toutefois, afin de limiter les conséquences potentielles pour Ubifrance, il est expressément recommandé aux utilisateurs de réduire au strict nécessaire la quantité d'informations confidentielles, secrètes, sensibles ou stratégiques présentes sur ces matériels lors de tels déplacements. Dans certains cas, il sera préférable d'utiliser un support de stockage distant mis en place par Ubifrance (disque virtuel, accès aux serveurs de fichiers par tunnel chiffré) pour stocker de telles informations lors d'un déplacement.

11 OUTILS COLLABORATIFS ET PLATES-FORMES DE COMMUNICATION COLLECTIVES

113. La mise en place des outils collaboratifs et plate-formes de communication collectives ne peut se faire que sur autorisation écrite et préalable de l'autorité hiérarchique, à défaut d'autorisation, cette mise en place pourra donner lieu à des sanctions.

114. L'utilisateur s'interdit tout propos pouvant porter atteinte à Ubifrance au risque de voir sa responsabilité engagée.

115. A titre d'exemple, le Tribunal de grande instance de Paris a condamné un salarié pour la création d'un blog portant atteinte aux droits de l'employeur.[29]

[29] TGI Paris 23-1-2007.

116. La participation des utilisateurs à un service de type web2.0 dans le cadre de ses activités professionnelles est interdite, sauf autorisation expresse de la hiérarchie.

117. Ubifrance ne saurait interdire à l'utilisateur de participer auxdits services hors dans son activité professionnelle, or dans ce cadre il s'interdit de diffuser tout propos relatif à l'activité d'Ubifrance.

12 PROTECTION DES DONNEES A CARACTERE PERSONNEL

12.1 Traitement et collecte des données à caractère personnel

118. En matière de protection des données à caractère personnel, les principaux textes applicables sont :

- la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés », modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004 et ses décrets d'application ;

- la convention n°108 du Conseil de l'Europe du 28 janvier 1980 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel ;

- la directive n°95/46 des communautés européennes du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ses données.

119. La loi « informatiques et libertés » organise la protection des données à caractère personnel relative aux personnes physiques.

120. Les dispositions de cette loi s'appliquent aux traitements de données à caractère personnel mis en œuvre par toutes les entreprises et organismes, quel que soit leur secteur d'activité. Ces dispositions s'appliquent également quelque que soit la technologie utilisée, qu'il s'agisse d'outils de bureautique (fichiers du personnel ou fichiers de clients), ou de toute autre technologie (autocommutateurs téléphoniques, contrôle d'accès par badge, systèmes de vidéosurveillance utilisés pour la constitution de fichiers nominatifs).

121. Par données à caractère personnel, il y a lieu d'entendre les informations qui permettent, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent et notamment les adresses électroniques de correspondants.

122. La loi du 6 janvier 1978 a créé un dispositif juridique, pour encadrer la collecte et la mise en œuvre des traitements des données à caractère personnel, en vertu duquel :

- d'une part, il est interdit, sauf exceptions limitativement énumérées, 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 ;

- d'autre part, toute personne auprès de laquelle sont collectées (oralement ou par écrit) des informations mises en œuvre dans un système automatisé de traitement doit être informée :

  - de l'identité du responsable du traitement ;

  - de la finalité du traitement ;

  - du caractère obligatoire ou facultatif des réponses ;

  - des conséquences d'un défaut de réponse ;

  - des destinataires des informations ;

  - de l'existence d'un droit d'interrogation, d'accès, de rectification, d'opposition pour motifs légitimes, sur les données à caractère personnel les concernant détenues et gérées par des tiers ;

  - le cas échéant, des flux transfrontières de données à caractère personnel.

123. Ainsi, selon le type de traitement ou de données, il s'agira, soit de réaliser une déclaration (ou une déclaration simplifiée) auprès de la CNIL, soit d'obtenir une autorisation de celle-ci. A noter que certains traitements sont exempts de ces formalités et en particulier lorsqu'un correspondant à la protection des données à caractère personnel (CIL) est nommé

124. L'attention de l'utilisateur est attirée sur le fait qu'il existe des règles particulières concernant certains types de traitements et certaines catégories de données (par exemple, les données dites « sensibles »). Ainsi, toutes collectes ou traitements de 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, sont interdites.

125. La violation enfin de la législation relative au traitement des données à caractère personnel est passible de sanctions pénales.

126. Compte tenu de ces risques pesant sur Ubifrance et ses utilisateurs, il est légitime que la charte d'utilisation du système d'information impose aux utilisateurs de respecter les finalités des traitements à caractère personnel.

12.2 Obligations du responsable du traitement

127. Le responsable du traitement est la personne qui détermine les finalités et les moyens du traitement.

128. Le responsable du traitement est tenu de procéder à une collecte loyale et licite, étant précisé que les finalités de la collecte doivent être déterminées, explicites et légitimes. En toute hypothèse, la collecte doit respecter le principe de proportionnalité : les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités

annoncées. En toute hypothèse, les données doivent être exactes, complètes, mises à jour et conservées.

129. Indépendamment de ce qui précède, il appartient au responsable du traitement de procéder, avant tout traitement de données à caractère personnel, aux formalités requises auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

130. Le responsable du traitement est tenu, de surcroît :

- de corriger les données collectées inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ;
- de conserver les données 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 ;
- d'assurer la sécurité et la confidentialité des données à caractère personnel, y compris dans le cas où le traitement serait sous-traité à un tiers, ce dernier devant présenter des garanties suffisantes formalisées dans un contrat écrit ;
- d'informer, la personne dont les données ont été collectées (oralement ou par écrit) comme indiqué ci- dessus. [30]

12.3 Droits de la personne concernée par le traitement

131. La personne concernée par le traitement de données à caractère personnel est la personne physique à laquelle se rapportent les données qui font l'objet du traitement.

132. Cette personne est la personne centrale que la loi informatique et libertés du 6 janvier 1978 entend protéger.

133. Cette personne bénéficie :

- d'un droit d'opposition, qui lui permet de s'opposer pour des motifs légitimes à ce que ses données fassent l'objet d'un traitement ;
- d'un droit d'accès, qui lui permet d'obtenir la communication d'un certain nombre d'informations relatives aux données à caractère personnel traitées ;
- d'un droit de modification ou de suppression de ses données.

[30] L'article 35 de la loi n°78-17 énonce en effet que :
« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.
Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.
Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »

12.4 Atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques

134. L'utilisateur doit être parfaitement conscient que tout traitement opéré sur des données à caractère personnel (données susceptibles d'identifier directement ou indirectement une personne) est soumis à une réglementation très stricte et que le non-respect de celle-ci l'expose à des sanctions pénales.

135. Ainsi, le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les règles posées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, constitue une infraction.

13 PROTECTION DE LA PROPRIETE INTELLECTUELLE

136. L'utilisation des ressources informatiques et de communication électronique d'Ubifrance implique le respect des droits de propriété intellectuelle.

137. Ces droits recouvrent la propriété littéraire et artistique (droit d'auteur, droits voisins du droit d'auteur..) et la propriété industrielle (marques, dessins et modèles, inventions et connaissances techniques…).

138. La violation des droits de propriété intellectuelle par un utilisateur est susceptible d'entraîner la mise en cause de sa responsabilité mais aussi celle d'Ubifrance en application de l'article L. 336-3 du Code de la propriété intellectuelle :

- « La personne titulaire d'un accès à des services de communication au public en ligne à l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par le droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

139. La tendance législative actuelle est d'ailleurs un renforcement des contrôles du respect de ces règles et des sanctions de la contrefaçon :

- les contrôles sur les parcs de licence des entreprises se multiplient afin d'identifier les téléchargements de licences sans autorisation, et ce faisant, se sont multipliés en 2008 les contentieux dans ce domaine ;

- les sanctions en matière de contrefaçon sont régulièrement aggravées par le législateur comme l'illustre la loi n°2009-1311 du 28 octobre 2009 sur la protection pénale de la propriété littéraire et artistique sur Internet dite prévoyant entre autres comme sanctions la suspension du compte de l'internaute fautif.

140. L'utilisateur doit donc veiller à la protection des droits de propriété intellectuelle des tiers. En outre, Ubifrance doit mettre en place des moyens de sécurisation offerts par le

fournisseur d'accès pour veiller à ce que l'accès Internet ne soit pas utiliser pour reproduire ou représenter des œuvres sans autorisation de l'auteur.

13.1 Protection par la propriété littéraire et artistique

- Règles de protection du droit d'auteur

141. En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit originale jouit, sur cette œuvre, du seul fait de sa création, "d'un droit de propriété incorporel et exclusif opposable à tous".

142. Cette disposition s'applique à toutes les œuvres de l'esprit, quel qu'en soit le genre, la forme d'expression, le mérite ou la destination. Sont considérées ainsi comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle et notamment de l'article L. 112-2, les œuvres suivantes :

- "les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
- les conférences, allocutions, serments, plaidoiries et autres œuvres de même nature ;
- les œuvres dramatiques et dramatico-musicales ;
- les œuvres chorégraphiques ;
- les œuvres musicales avec ou sans paroles ;
- les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensemble œuvres audiovisuelles ;
- les œuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;
- les œuvres graphiques et typographiques ;
- les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
- les œuvres d'art appliqué ;
- les illustrations, les cartes géographiques ;
- les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;
- les logiciels, y compris le matériel de conception préparatoire...".

143. Toute forme d'utilisation, de reproduction, de représentation ou de mise à disposition du public de l'œuvre est ainsi soumise à l'autorisation préalable du titulaire des droits sur les œuvres.

144. L'utilisateur est donc informé qu'à défaut d'une autorisation expresse du titulaire, il lui est interdit d'utiliser, reproduire, représenter ou mettre à disposition du public une œuvre.

145. L'utilisateur ne doit pas via l'accès internet mis à sa disposition par Ubifrance reproduire ou représenter des œuvres de l'esprit sans l'autorisation des titulaires des droits. [31]

[31] L'article L.336-3 du Code de la propriété intellectuelle énonce que : « La personne titulaire d'un accès à des services de communication au public en ligne à l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par le droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

146. La contrefaçon d'une œuvre de l'esprit est civilement et/ou pénalement sanctionnée.

- Logiciels

147. Les logiciels sont protégés par le droit d'auteur.

148. Toute utilisation, reproduction, représentation ou mise à disposition du public du logiciel n'est autorisée que sous réserve du consentement du titulaire des droits sur ledit logiciel.

149. L'étendue et les caractéristiques des droits conférés sont définies, en général, par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation du logiciel visé.

150. L'utilisateur d'un logiciel s'expose à des sanctions civiles, voir à des sanctions pénales prévues par le Code de la propriété intellectuelle, lorsqu'il utilise le logiciel sans autorisation (ou au-delà des limites visées dans les contrats de licence).

151. Par exemple, les atteintes aux droits d'auteur d'un logiciel sont passibles d'une peine d'emprisonnement de trois ans et d'une peine d'amende de 300 000 euros.[32]

152. Par ailleurs, les utilisateurs sont informés que de tels actes exposent également Ubifrance à des risques importants, notamment en termes de sécurité informatique.

153. A ce titre, les utilisateurs doivent notamment :

- utiliser les logiciels mis à leur disposition dans le cadre de leurs missions, dans le respect des droits et obligations stipulées aux licences d'utilisation souscrites par Ubifrance ;
- ne pas reproduire ou diffuser les logiciels mis ainsi à leur disposition.

154. L'utilisateur ne peut, par exemple, enregistrer ou télécharger un programme auquel il a eu accès dans le cadre de ses fonctions, afin de l'enregistrer sur son propre poste pour toute autre utilisation hors du cadre de ses fonctions et/ou hors des locaux d'Ubifrance.

155. De la même manière, l'utilisateur ne peut installer ou télécharger sur des équipements d'Ubifrance des logiciels sur lesquels des droits lui auraient été concédés à titre personnel (contrat de licence souscrit par lui-même pour ses besoins personnels) et dont l'utilisation à des fins professionnelles au sein d'Ubifrance ne rentrerait pas dans le cadre de l'étendue des droits conférés sur l'œuvre en question.

156.Par ailleurs les logiciels dits « libres » comme par exemple les logiciels « shareware » sont en libre essai mais non libres de droits.

Il convient donc de rappeler aux utilisateurs qu'ils doivent veiller à la protection des droits de propriété intellectuelle des tiers. En outre, Ubifrance doit mettre en place des moyens de sécurisation offerts par le fournisseur d'accès pour veiller à ce que l'accès internet ne soit pas utilisé pour reproduire ou représenter des œuvres sans autorisation de l'auteur.

[32] Art. L. 335-5 du Code de la propriété intellectuelle.

157. Il existe des licences associées notamment la licence « GPL » qui est une licence qui contient des droits et obligations à la charge de l'auteur et de l'utilisateur.

- Textes, images et sons

158. De la même façon, les textes, les images et les sons, sont, dès lors qu'ils présentent une certaine originalité, protégés en principe par le droit d'auteur.

159. A cet égard, certains textes ou images portent les mentions copyright ou ©, qui rappellent que ceux-ci sont protégés par des droits d'auteur. Toutefois, l'absence des mentions copyright ou © ne signifie pas que l'utilisation des textes ou images est libre, le droit français n'impose pas de telles mentions pour reconnaître l'existence d'un droit d'auteur sur une œuvre.

160. L'autorisation écrite du titulaire des droits est ainsi nécessaire pour leur utilisation, reproduction, représentation et mise à disposition du public.

161. Le non-respect des droits de l'auteur sur ces éléments est constitutif de contrefaçon et est donc civilement et/ou pénalement sanctionnable.

162. D'une manière générale, la difficulté à connaître précisément l'origine de tels éléments transmis et, donc, les droits y afférents, en particulier avec le développement des moyens d'échange d'informations en réseau ouvert comme Internet, oblige les utilisateurs à la plus grande prudence.

163. Les utilisateurs doivent donc s'interdire d'utiliser les éléments sur lesquels ils ne disposeraient pas d'autorisation expresse d'utilisation.

- Bases de données

164. On entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

165. Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, sont soumises aux dispositions du Code de la propriété intellectuelle.

166. Par ailleurs, les données contenues dans ces bases sont protégées par le droit sui generis lequel fait obstacle :

- à toute extraction par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;
- à la réutilisation, par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle que soit sa forme.

167. A ce titre, un utilisateur des bases de données d'Ubifrance ne peut pas utiliser par exemple un fichier d'adresses dont cette dernière est propriétaire à des fins personnelles et ne

saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

13.2 Protection par la propriété industrielle

- Marques

168. Le Code de la propriété intellectuelle protège toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale.

169. Peuvent être utilisés à titre de marque, toutes les dénominations et signes figuratifs ou sonores, tels que les mots, assemblages de mots, noms patronymiques, noms géographiques, pseudonymes, lettres, chiffres, sigles, emblèmes, photographies, dessins, empreintes, logos ou la combinaison de certains d'entre eux.

170. L'enregistrement de la marque confère à son titulaire un droit de propriété sur cette marque pour les produits et services qu'il a désignés.

171. L'utilisateur ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque pour des produits et services identiques à ceux désignés dans l'enregistrement ou encore supprimer ou modifier une marque régulièrement apposée.

172. L'utilisateur ne peut, par ailleurs, sauf autorisation du propriétaire, s'il existe un risque de confusion dans l'esprit du public :

- reproduire, utiliser ou apposer une marque pour des produits ou services similaires à ceux désignés dans l'enregistrement ;

- imiter une marque et l'utiliser, pour des produits ou services identiques ou similaires à ceux désignés lors de l'enregistrement.

173. Dans ces conditions, l'utilisateur ne saurait notamment, dans le cadre de ses fonctions, utiliser une marque pour laquelle Ubifrance ne détient pas l'autorisation expresse d'utilisation.

174. Il ne saurait, en outre, utiliser à des fins personnelles, toute marque dont Ubifrance serait titulaire.

- Brevets et dessins et modèles

175. Certaines inventions et autres créations sont susceptibles d'être protégées par :

- le droit des dessins et modèles ;
- le droit des brevets.

176. Par conséquent, l'utilisateur s'interdit de les utiliser sans l'autorisation expresse de leurs titulaires.

- Secrets de fabrique

177. Les secrets de fabrique qui sont tous procédés de fabrication mais également toutes innovations non-brevetables issus d'une expérience technique ainsi que le savoir-faire ou know-how, peuvent appartenir à Ubifrance ou à des tiers.

178. Au sens juridique du terme, un secret de fabrique s'applique également à la fourniture de services.

179. Sa divulgation est sanctionnable pénalement.

180. L'utilisateur doit donc se montrer particulièrement vigilant et est parfaitement informé du caractère extrêmement confidentiel et de la valeur des secrets de fabrique d'Ubifrance et s'interdit une quelconque atteinte à ces derniers. [33]

13.3 Autres protections

- Dénominations non protégées par un droit de propriété intellectuelle

181. Certaines dénominations, qui ne sont pas protégées par un droit de propriété intellectuelle, bénéficient d'une protection et ne peuvent, par conséquent, être utilisées sans autorisation :

- une dénomination sociale ou raison sociale ;
- un nom commercial ou une enseigne ;
- un nom de domaine.

182. Par conséquent, l'utilisateur s'interdit de les utiliser sans l'autorisation expresse de son propriétaire.

- Noms de domaine

183. Un nom de domaine permet d'identifier et d'authentifier l'auteur d'un site sur Internet.

184. Le titulaire d'un nom de domaine dispose sur celui-ci d'un droit d'usage.

185. Par conséquent, l'utilisateur s'interdit de déposer un nom de domaine identique ou similaire à des noms de domaine antérieurement déposés.

14 AUDIT ET CONTROLE

14.1 Fondements juridiques

[33] Le secret de fabrique est une technique, un tour de main, une formule de composition d'un produit que le concepteur décide d'ériger en secret. L'article L.1227-1 (ex article L152-7) du Code du travail énonce que « le fait, par tout directeur ou salarié d'une entreprise où il est employé, de révéler ou de tenter de révéler un secret de fabrique est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. (…) »

186. Il pèse sur Ubifrance une obligation générale de sécurité, qui lui confère le droit de contrôler l'activité des utilisateurs.

187. La surveillance et le contrôle des salariés sur le lieu et pendant le temps de travail font partie des prérogatives reconnues à l'employeur, pour autant que les procédés utilisés ne soient pas illicites.

188. Ces prérogatives sont notamment justifiées par ses pouvoirs disciplinaires et de direction, mais aussi par l'obligation générale de sécurité qui lui incombe.

189. C'est dans ce cadre que s'inscrivent les audits et contrôles que peut être amenée à réaliser Ubifrance aux fins notamment de vérifier la conformité de l'usage des ressources informatiques et de communication électronique qu'elle met à disposition.

190. Ces audits et contrôles peuvent avoir également pour finalités d'optimiser l'utilisation des ressources informatiques et de communication électronique, et l'analyse statistique.

14.2 Contrôle du système d'information : traçabilité et filtrage

191. Au titre des procédés de contrôle, Ubifrance a informé les utilisateurs dans la charte d'utilisation du système d'information la mise en place d'outils de traçabilité[34] et de filtrage[35].

192. Les données issues de ces dispositifs sont de deux types :

- le « log » qui peut être défini comme la journalisation de données informatiques résultant de l'utilisation d'une application ;

- la « trace » qui est une donnée informatique témoignant de l'existence d'une opération au sein d'une application.

193.Ainsi la Cour de cassation dans un arrêt du 8 juillet 2009 a jugé que l'employeur peut rechercher et identifier les sites internet sur lesquels un salarié a surfé pendant son temps de travail et le sanctionner sans que cela porte atteinte à l'intimité de sa vie privée. [36]

14.3 Contrôle de la messagerie

[34] Journaux de connexions de l'ensemble des moyens informatiques et de communication électronique.
[35] Filtrage des contenus, des URL, protocolaire, etc. permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre ou d'interdire l'accès à internet ou à certaines catégories de sites internet.
[36] Cass.soc 8-7-2009, dans cette affaire un informaticien consacrait, parfois, jusqu'à 4 heures par jour à l'entretien d'une messagerie et à des consultations internet à des fins purement privées et ludiques. Il avait, en outre, sollicité l'informaticien sous ses ordres pour pouvoir se connecter anonymement sur internet, tout en ignorant que le numéro d'identification des machines restait enregistré. Or, l'utilisation privée d'une connexion Internet d'entreprise doit rester « raisonnable », au même titre que le téléphone ou les photocopies, le salarié étant tenu d'une obligation de loyauté vis-à-vis de son employeur (art. L.1222-1 du Code du Trav.). En cas d'abus, la sanction peut être très sévère, comme en l'espèce, jusqu'au licenciement pour « faute grave ».

194. Ubifrance peut accéder à tout élément issu des moyens informatiques et de communication électronique, présumé professionnel aux termes de la jurisprudence, ce en dehors de la présence de l'utilisateur concerné.

195. En ce qui concerne les fichiers électroniques clairement revêtus de la mention « PRIVE », ils peuvent être consultés par Ubifrance en dehors de la présence de l'utilisateur en présence uniquement d'un risque ou d'un événement particulier.

196. L'employeur peut également, indépendamment de la présence de l'utilisateur et/ou en cas d'opposition de ce dernier, accéder aux fichiers électroniques personnels de ce dernier si un juge l'y autorise, sur le fondement de l'article 145 du Code de procédure civile[37]. Il est en effet possible de demander sur requête ou en référé que des mesures d'instruction soient ordonnées, s'il existe un motif légitime de conserver ou d'établir, avant tout procès, la preuve des faits dont pourrait dépendre la solution d'un litige. La Cour de cassation considère que le respect de la vie privée du salarié ne constitue pas en lui-même un obstacle à l'application de mesures d'instruction afin de conserver des preuves.[38]

197. Ubifrance pourra le cas échéant demander à des personnes tierces, telles qu'un huissier de justice, d'être présentes lors de ces opérations de contrôle.

198. Ceci explique que les utilisateurs doivent s'assurer que toutes les opérations réalisées sous couvert de leur identifiant, l'ont été par eux.

199. Ces audits et contrôles relèvent des compétences de la Direction des systèmes d'information qui a la charge de la qualité et de la sécurité des services informatiques fournis aux utilisateurs.

200. A ce titre, les personnels de la Direction des systèmes d'information sont conduits, de par leur fonctions, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexion à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

201. Ces personnels, dûment mandatés pour mener ces démarches, garderont toutefois confidentielles les informations qu'ils pourraient être amenés à connaître à cette occasion. Ils ne peuvent en tout état de cause utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

14.4 Contrôle des consommations de téléphonie fixe et mobile

202. Les utilisateurs sont informés dans la charte d'utilisation du système d'information qu'Ubifrance a mis en place un autocommutateur ou PABX qui enregistre, à partir de chacun des postes téléphoniques fixes, les éléments de la communication (date, heure, durée, coût et numéros appelés).

[37] Art.145 du Code de procédure civile : « S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. »
[38] Cass. soc. 23-5-2007 n°05-17818.

203. L'enregistrement en revanche des conversations téléphoniques est interdit sauf à en informer préalablement l'interlocuteur, ainsi que de ses droits en cas de traitement des données à caractère personnel, conformément à la loi dite « Informatique et libertés ».

204. Les mêmes informations sont disponibles via les opérateurs téléphoniques pour les moyens informatiques et de communication électronique nomades (téléphone portable, BlackBerry, etc.).

205. Une décision récente de la Cour de cassation légitime ce type de procédé car elle a jugé que la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste édités au moyen de l'autocommutateur téléphonique de l'entreprise ne constitue pas un procédé de surveillance illicite, alors même que le salarié n'en avait été préalablement informé[39].

206. Ces dispositifs ne s'appliquent pas en revanche aux représentants du personnel.

207. Le traitement et la conservation des logs dans ce cadre de contrôle des utilisateurs peuvent enfin constituer un traitement de données à caractère personnel, et être à ce titre soumis aux formalités préalables imposées par la Cnil.

14.5 Vidéosurveillance

208. Les utilisateurs sont informés de la mise en place d'un système de vidéosurveillance dans les locaux d'Ubifrance.

209. La vidéosurveillance dite de « sécurité privée » est régie par :

- les principes directeurs de la loi « Informatique et libertés », dans la mesure où les activités de vidéosurveillance ne sont pas visées en tant que telles, à la différence, par exemple, des technologies de biométrie ;

- la délibération 94-056 du 21 juin 1994 portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et les lieux recevant le public. Cette disposition reste d'actualité, sous réserve des prescriptions de la loi 95-73 d'orientation et programmation relative à la sécurité du 21 janvier 1995 et de la refonte de la loi Informatique et libertés du 6 août 2008.

210. Ces dispositions visent :

- la prise de vue avec ou sans enregistrement ;
- la connexion avec des fichiers nominatifs.

211. Il est enfin rappelé que l'enlèvement ou la neutralisation des caméras de surveillance sans justificatif est strictement interdit.

[39] Cass. soc. 29-1-2008 n°06-45279.

15 REGLES EN MATIERE DE PROTECTION DES PERSONNES

212. Chacun a droit au respect de la vie privée.

213. Ainsi, la diffusion de toute information qui relève de la sphère privée d'une personne est susceptible d'engager la responsabilité civile de l'auteur de cette diffusion.

214. Par information qui relève de la sphère privée des personnes, il faut entendre notamment : des informations portant sur la vie sentimentale d'une personne, sur ses mœurs sexuelles, sur sa famille ou encore sur sa rémunération.

215. Par ailleurs, constitue une infraction, le fait, au moyen d'un procédé quelconque, de volontairement porter atteinte à l'intimité de la vie privée d'autrui :

- en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
- en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

216. Est également puni le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes visés ci-dessus.

217. Il est strictement interdit, par ailleurs, d'utiliser le nom, l'image ou encore la voix d'une personne sans son autorisation.

218. Un tel acte est susceptible d'engager la responsabilité civile de son auteur.

219. Constitue également une infraction le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

220.La loi prévoit des sanctions pénales et administratives en cas de non-respect de ces obligations, qui peuvent être infligées aussi bien aux personnes physiques qu'aux personnes morales[40].

16 REGLES EN MATIERE DE LIBRE CONCURRENCE

221. Les principes de liberté du commerce et de l'industrie et de liberté de la concurrence en matière commerciale sont limités par l'interdiction d'utiliser tous procédés contraires aux usages loyaux du commerce nuisant à un concurrent.

[40] Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du Code pénal, des infractions prévues à l'article 35 de la loi du 21 juin 2004. Les peines encourues par les personnes morales sont :

- L'amende, suivant les modalités prévues par l'article 131-38 du Code pénal ;
- Les peines mentionnées à l'article 131-39 du Code pénal.

222. Il en est ainsi à titre d'exemple du détournement de clientèle.

223. Ainsi l'utilisateur s'interdit, tout agissement déloyal (diffusion d'informations), imitation de produits concurrents, divulgation et exploitation de savoir-faire, appropriation de clientèle (démarche, détournement de fichiers et détournement de commandes), débauchage de personnel, organisation d'un réseau de débauchage, ainsi que l'exercice irrégulier d'une activité.

224. Les agissements déloyaux exposent leurs responsables au versement de dommages et intérêts au titre notamment de la concurrence déloyale.

17 LIBERTE D'EXPRESSION ET SES LIMITES

17.1 Principe de la liberté d'expression individuelle

225. Le principe de la libre communication des pensées et des opinions a été consacré notamment par l'article 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789.

226. La Convention européenne des droits de l'homme prévoit également un droit d'expression général en son article 10 alinéa 1.

227. Au niveau de l'entreprise, cette liberté est définie par le Code du travail et l'article L. 1121-1 qui dispose que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

17.2 Limites à la liberté d'expression

228. La liberté d'expression n'est toutefois pas sans limite et toute personne peut engager sa responsabilité civile et/ou pénale à raison de la violation de certaines règles considérées comme ayant une portée équivalente.

17.2.1 Les délits par la voie de la presse ou tout autre moyen de communication

- La diffamation

229. Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation.

230. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.

231. La diffamation commise envers les particuliers sera punie d'une amende de 12 000 euros, (article 32, loi du 29 juillet 1881 sur la liberté de la presse).

232. La diffamation commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée sera punie d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement.

233. Sera punie des peines prévues à l'alinéa précédent la diffamation commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.

- L'injure

234. Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure, (article 33, loi du 29 juillet 1881).

235. L'injure commise envers les particuliers, lorsqu'elle n'aura pas été précédée de provocations, sera punie d'une amende de 12 000 euros.

236. Sera punie de six mois d'emprisonnement et de 22 500 euros d'amende l'injure commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée.

237. Sera punie des peines prévues à l'alinéa précédent l'injure commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.

17.2.2 La dénonciation calomnieuse

238. L'attention de l'utilisateur est attirée sur le fait que la dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée :

- soit à un officier de justice ou de police administrative ou judiciaire,
- soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente,
- soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée,

est punie de cinq ans d'emprisonnement et de 45 000 euros d'amende, (article 226-10 du Code pénal).

239. La fausseté du fait dénoncé résulte nécessairement de la décision, devenue définitive, d'acquittement, de relaxe ou de non-lieu déclarant que la réalité du fait n'est pas établie ou que celui-ci n'est pas imputable à la personne dénoncée.

18 REGLES DE CONSERVATION ET D'ARCHIVAGE

18.1 Éléments présumés professionnels

240. Au même titre qu'un document papier, un document électronique doit être conservé et archivé puisqu'il peut constituer une preuve. [41]

241. Par ailleurs l'article 1316-3 du Code civil dispose que l'écrit sur support électronique a la même force probante que l'écrit sur support papier.

242. L'utilisateur doit :

- s'il existe une politique de conservation et d'archivage au sein de son service, la respecter,

- à défaut de politique de conservation et d'archivage, la définir au sein de chaque service avec son supérieur hiérarchique.

243. Les archives doivent répondre aux durées de conservation spécifiques aux documents qu'elles constituent.

244.La loi du 17 juin 2008 portant réforme de la prescription en matière civile a modifié les durées de prescription en matières civile et commerciale pour la fixer à une durée de cinq ans, notamment pour les obligations entre commerçants et non-commerçants[42]. S'agissant des contrats conclus par voie électronique d'une valeur égale ou supérieure à 120 euros, il pèse sur le contractant professionnel une obligation de conservation pour une durée de dix ans[43] à compter :

- de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate ;

- ou de la date de livraison du bien ou de l'exécution de la prestation.

18.2 Éléments privés

245. Les sauvegardes et back up réalisés par Ubifrance ne concernent pas les éléments du répertoire nommés « PRIVE », qui sont donc conservés sous la seule et entière responsabilité de l'utilisateur.

19 RESPONSABILITE ET SANCTIONS

[41] Art. 1316 du Code civil : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission. »
[42] Art. L. 110-4 du Code de commerce.
[43] Art. L. 134-2 du Code de la consommation.

246. Les ressources informatiques et de communication électronique mises à la disposition des utilisateurs permettent l'accès à de puissants moyens de communication. Or, de telles ressources ne doivent pas permettre de véhiculer n'importe quelle information.

247. Dans le cadre de son activité professionnelle, l'utilisateur engage sa responsabilité en ne se conformant pas aux termes de la charte d'utilisation du système d'information.

248. En cas de non-respect de ces règles, ce dernier s'expose à des sanctions civiles, pénales et disciplinaires s'agissant des salariés.

20 DEROGATIONS

249. Les dérogations sont exceptionnelles, et autorisées préalablement et expressément par le Directeur des systèmes d'information ou le Directeur général. Il s'agit là d'une prérogative discrétionnaire.

250. En tout état de cause, les utilisateurs sont informés qu'une dérogation n'a pas pour effet de leur accorder des droits acquis.

21 MISE A DISPOSITION DU GUIDE ET EVOLUTION

251. Le présent guide est mis à la disposition des utilisateurs sur l'Intranet d'Ubifrance.

252. Le présent guide sera régulièrement mis à jour et il appartient à l'utilisateur de prendre connaissance de toute nouvelle version du guide qui sera portée à sa connaissance par le biais de l'Intranet.

253. Une information sera communiquée à l'ensemble des utilisateurs à chaque nouvelle version du guide.