LES DOSSIERS TECHNIQUES

Vade-mecum*

Obligations juridiques liées aux systèmes d'information

* *Vade-mecum : Recueil contenant des renseignements sur les règles d'un art ou d'une technique à observer ou sur une conduite à suivre et qu'on garde sur soi ou à portée de main pour le consulter.*
(Trésor de la Langue Française)

Juin 2017

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS
11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

CYBERLEX
4 avenue HOCHE – 75008 Paris
Tél. : +33 1 43 18 16 50
cyberlex@cyberlex.org – www.cyberlex.org

Table des matières

1 Présentation des auteurs

La présente contribution est le fruit de la réflexion collective d'un Groupe de travail composé de membres de l'association Cyberlex, Association du droit et des nouvelles technologies, et du CLUSIF, Club de la sécurité de l'information français.

PRÉSENTATION DE CYBERLEX

Cyberlex réunit, depuis 1996, des juristes d'entreprise, des avocats, des professeurs de droit, des magistrats ainsi que des professionnels du marché de l'internet et des technologies numériques.

Cyberlex ne représente pas une opinion, mais des opinions, à l'image de la diversité de ses membres, excluant tout lobbying. L'ambition de Cyberlex est de contribuer à mieux comprendre le monde des nouvelles technologies et l'évolution des usages, appréhender les différents aspects du droit et ainsi participer à sa meilleure lisibilité.

PRÉSENTATION DU CLUSIF

Le CLUSIF est une association de professionnels de la sécurité dont la mission principale consiste à favoriser les échanges d'idées et de retours d'expériences au service d'une sécurité des systèmes d'information (SSI) efficace.

Le CLUSIF a pour finalité d'agir pour la sécurité de l'information, facteur de pérennité des entreprises, administrations centrales et collectivités locales. L'enjeu actuel est donc de contrôler l'exposition au risque général associé au système d'information en particulier.

MÉTHODOLOGIE ADOPTÉE

Un groupe de travail composé de membres de Cyberlex et du CLUSIF, disposant de compétences juridiques et techniques nécessaires à la compréhension des enjeux des systèmes d'information du point de vue de la sécurité et de la protection des données de l'entreprise, a donc été mis en place sous la direction conjointe d'Amélie PAGET et de Patrick BLUM, membres du CLUSIF, et de Corinne THIERACHE, ancienne Présidente et membre de Cyberlex et de Gilles ROUVIER, Vice-Président et Secrétaire général de Cyberlex, afin de coordonner les différents travaux (ci-après le Groupe de travail Cyberlex - CLUSIF).

Les réflexions qui ont alimenté ces travaux et les recommandations qui en ont découlé, reprises dans le présent rapport, sont proposées par les membres du Groupe de travail en toute indépendance et n'engagent que ces derniers. Elles ne sauraient donc engager leurs employeurs ou leur organisme.

Une vingtaine de réunions mensuelles de réflexion ont été tenues par le Groupe de travail Cyberlex - CLUSIF entre septembre 2015 et septembre 2017.

Remerciements

Le CLUSIF et Cyberlex tiennent à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement (par ordre alphabétique) :

Membres de Cyberlex contributeurs :

François	**COUPEZ**	*ATIPIC AVOCAT*
Sandrine	**MONDIN-SIMON**	*SNCF*
Gilles	**ROUVIER**	*LAWWAYS AVOCATS*
Julie	**RUELLE**	*IDEA AVOCATS*
Corinne	**THIERACHE**	*ALERION Société d'Avocats*

Membres du CLUSIF contributeurs :

Antoine	**BAJOLET**	*TDF*
Patrick	**BLUM**	*ESSEC*
Benoît	**FUZEAU**	*CASDEN BANQUE POPULAIRE*
Garance	**MATHIAS**	*MATHIAS AVOCATS*
Sophie	**MICHAS**	*AGIRC-ARRCO*
Nicolas	**MOREAU**	*SPM*
Amélie	**PAGET**	*HSC BY DELOITTE*
Lazaro	**PEJSACHOWICZ**	*CLUSIF*
Ludovic	**PETIT**	*ALTRAN*
Blandine	**POIDEVIN**	*JURIS-EXPERT AVOCATS*
Marine	**SOUCHARD**	*PAYNAME*

Sont vivement remerciés les autres participants du Groupe de travail pour leur soutien au présent rapport :

Jean	**CHERIN**	*HSC BY DELOITTE*
Hoji	**FARHAT**	*ATEXIO*
Jean-Marc	**GREMY**	*CLUSIF*
François	**NOMICHIT**	*ENGIE*

Et un grand merci à Florence Hanczakowski, chargée de mission au CLUSIF, pour son aide logistique.

2 Contexte et objectifs

2.1 Nouveaux risques et évolution de la fonction sécurité

L'origine du poste de Responsable de la Sécurité des Systèmes d'Information (RSSI) remonte au milieu des années 1980. Il était alors perçu comme un expert technique « *chasseur de virus* » et bâtisseur de murailles, une fonction essentiellement opérationnelle, la raison en incombait à la nature des risques pesant sur les systèmes d'information (SI) d'alors.

Tant que l'architecture des SI était basée sur des architectures majoritairement propriétaires et des applications développées en interne, l'organisme attendait de son RSSI qu'il connaisse les mécanismes de sécurité à mettre en œuvre, qu'il en vérifie régulièrement la bonne application et qu'il traite des problématiques de continuité d'activité.

Dans les années 90, l'avènement de l'internet a permis l'accélération du développement de l'informatique en réseaux au sein des entreprises, accompagné des premiers programmes malveillants à large diffusion, et marquant sans doute un changement de paradigme de la SSI avec l'ouverture des SI sur l'extérieur.

Le XXIe siècle est marqué par le développement de l'économie numérique. Essentiel aux activités supports et métiers, le SI supporte les processus de l'organisme et son patrimoine informationnel. Si la gestion du SI reposait à l'origine sur le matériel informatique, des enjeux de gouvernance apparaissent. Les évolutions du poste de RSSI reflètent parfaitement ces tendances.

La nature des risques a fondamentalement changé, en raison de la complexité accrue des SI et de l'ouverture des réseaux. Le RSSI doit traiter de nombreux domaines complémentaires comme les aspects juridiques et la communication, interne et externe. La transformation digitale des entreprises impose aux RSSI de changer leur façon d'appréhender les risques et leur manière de travailler.

Le périmètre d'action du RSSI sur la protection de l'information sous les trois dimensions, écrite, orale et numérique, s'élargit et lui impose de devenir un alchimiste qui doit interagir avec tous les niveaux (directeurs, managers, chef de projet, personnel d'accueil, etc.) et toutes les entités (Métiers, Informatique, Maîtrise d'ouvrage, Finance, Comptabilité, Marketing, Communication, Juridique, Achat, Gestionnaires de risques, Qualité, etc.) de son organisation. Sa position transversale joue un rôle primordial dans la réussite de ses missions.

Les risques ont évolué avec la généralisation des usages des SI et la professionnalisation des attaques. La combinaison classique disponibilité-intégrité-confidentialité-preuve doit maintenant s'étudier aussi au travers du prisme d'attaques organisées, voire mafieuses ou étatiques. La diffusion des SI dans tous les secteurs de la société (commerce, santé, industrie, défense…) a logiquement entraîné une évolution des textes encadrant les usages, mais aussi pénalisant les manquements.

En outre, l'ouverture des SI vers l'extérieur, le déploiement du numérique, l'émergence

des technologies (big data, objets connectés…), l'évolution des techniques de récupération d'informations, et la croissance exponentielle des actes de malveillance contre les entreprises et les administrations nécessitent la prise de conscience, par l'ensemble de leurs dirigeants et de leur personnel, de la nécessité de protéger le patrimoine informationnel.

Par ailleurs, la généralisation de l'externalisation de larges pans du SI des entreprises, historiquement sous la forme de contrats d'infogérance, puis aujourd'hui sous la forme de délocalisation dans le « cloud public », ainsi que l'évolution des méthodes de travail des collaborateurs (équipements nomades, BYOD, COPE, ...), conduit le RSSI à traiter des risques non plus uniquement sur le plan de la technique, puisque celle-ci lui échappe, mais également sur le plan contractuel, en prévoyant des clauses couvrant ces risques.

2.2 Omniprésence du droit

De nos jours, le développement de la numérisation des activités nous rend dépendants des technologies de l'information et de la communication (TIC), quelles qu'elles soient.

En conséquence, le cadre légal et réglementaire conditionne les moyens techniques à mettre en œuvre pour être conforme à la loi et préserver ou protéger ce qui est essentiel au développement des entreprises : leurs créations techniques, leur savoir-faire, leur secret des affaires[1].

Cette composante juridique, en très forte évolution, fait peser un nouveau risque sur les entreprises. Sa compréhension, son analyse et son traitement ont pris, depuis quelques années, une place croissante dans le métier du RSSI.

Qu'il s'agisse de données personnelles ou confidentielles, que vous soyez opérateur d'un site marchand ou hébergeur d'un blog de presse, que vous soyez un hôtel ou un restaurant offrant du wifi à ses clients, des exigences juridiques vous seront applicables.

Le Règlement général sur la protection des données (RGPD)[2] affirme la place du juridique dans la SSI. Avec des sanctions pouvant atteindre 20 millions d'euros ou 4 % du CA mondial et des répercussions importantes en termes d'image, les risques juridiques associés à la protection des données à caractère personnel ne peuvent plus être ignorés.

Le RSSI doit ainsi connaître la réglementation sur les données à caractère personnel ou encore sur la sécurité des SI et se conformer aux principes arrêtés par la Commission nationale de l'informatique et des libertés (CNIL), à ceux de l'Agence nationale de la sécurité de systèmes d'information (ANSSI), notamment pour les

[1] Qui seront à terme protégés dans les conditions prévues par la directive européenne du 8 juin 2016 (Directive (UE) 2016/943) et plus largement leurs informations stratégiques couvertes ou non par la propriété intellectuelle (droits d'auteur et droits voisins, marques, brevets, dessins & modèles, bases de données…).
Pour en savoir plus : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0943

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Pour en savoir plus : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

Opérateurs d'Importance Vitale (OIV), ainsi qu'aux directives d'autres autorités ou règlementations sectorielles (banque/assurance, santé, etc.). Il doit également appréhender certains fondements juridiques et le droit des contrats pour lui permettre, notamment, d'introduire des clauses de sécurité valables dans les contrats signés avec les partenaires et les fournisseurs, ou le droit de la responsabilité.

Face aux nombreux questionnements juridiques, et au manque de clarté de certains textes législatifs, si le RSSI peut compter en interne sur sa direction juridique - cette dernière pouvant faire appel à des avocats en soutien - il lui est nécessaire de disposer d'une sensibilité juridique pour discuter avec cette direction, expliquer son action aux dirigeants et la diffuser au sein de son entité.

Force est de constater que la règle de droit est omniprésente dans notre société et régit chaque rapport social et économique.

En présence de ces évolutions, les organismes, au travers de leur RSSI, mettent en place des politiques de sécurité des SI afin d'accompagner les entreprises et les administrations dans leur développement, tout en maîtrisant les risques SI, et guident ces entités afin de leur permettre de mieux assurer leur responsabilité de gestion des risques métiers liés aux SI.

Le souhait des entreprises et des administrations est, dans ce contexte mouvant, de développer, voire de créer une certaine aptitude à anticiper les questions juridiques et à en assurer la communication en interne notamment sur les sujets de cybersécurité.

Les directions générales facilitent cette évolution en étant sensibilisées, ne serait-ce que par l'actualité, aux questions de cyberdéfense et attendent des RSSI, compétents techniquement, d'être vigilants sur certains aspects juridiques et de s'imposer à leurs côtés dans l'entreprise sur ce sujet, en vue d'une solution globale.

2.3 Les professionnels visés par ce document

Dans ce contexte, ce document s'adresse à toutes les personnes préparant un projet faisant appel à un SI.

S'il vise en premier lieu les Directeurs des Systèmes d'Information (DSI) et les RSSI, il permettra néanmoins aux maîtrises d'ouvrage et maîtrises d'œuvre de mieux appréhender les exigences légales et ainsi anticiper le risque juridique.

Sont donc concernées, outre les métiers traditionnels liés aux SI, toutes les personnes intervenant dans le cadre de processus utilisant le SI (achats, gestion des ressources humaines, métiers, communication, marketing, etc.), sans oublier les correspondants informatique et libertés (CIL) et futurs délégués à la protection des données (DPD ou DPO pour *« Data protection officer »*) dédiés à la protection des données à caractère personnel.

2.4 Objectifs du document

Pour ces raisons, ce document a pour but de permettre à ces personnes et de manière générale à toute personne en charge des SI et de leur protection, ou préparant un projet faisant appel à un SI, d'appréhender la multiplicité des exigences légales et

réglementaires pour rendre possible une gestion des risques juridiques plus sereine en faisant appel à des compétences juridiques complémentaires une fois le problème identifié.

En effet, « *Disposer d'un savoir précis et pointu comme le juriste comporte une responsabilité : celle de rendre le droit accessible* » (Thibault Turchet, Juriste - Zero Waste France) et c'est la volonté de ce document.

Ce document a été pensé comme **un outil de pilotage des questions juridiques liées au SI**, permettant le développement de la culture juridique des RSSI et la prévention des risques juridiques par ces derniers. Il ne s'agit nullement d'un manuel de droit de la sécurité des SI, ni d'une consultation juridique.

Il peut permettre au RSSI d'identifier et d'apprécier dans les grandes lignes les principales questions juridiques liées aux obligations de sécurité de l'information et en particulier les questions cruciales – celles susceptibles de remettre en cause l'existence même de projets faisant appel à un SI. Sous forme de fiches pratiques, il contient les premiers éléments de réponse afin de privilégier une approche pragmatique et accessible et ainsi acquérir les bons réflexes en matière de gestion des exigences légales et réglementaires.

Il a donc pour ambition de fournir les clefs de lecture du cadre juridique en matière de sécurité de l'information et de délivrer les points de vigilance afférents.

Mais ce document ne prétend pas à l'exhaustivité et ne dispense pas de recourir à un conseil juridique spécialisé, qu'il soit interne ou externe à l'organisme. Il ne présente que les obligations générales de sécurité de l'information dans le cadre légal en application à date de publication de ce document. Ainsi, s'il est fait référence parfois au RGPD applicable au 25 mai 2018, il conviendra d'attendre une version réactualisée de ce document pour en avoir une appréciation plus détaillée et pragmatique.

Enfin, ne sont pas traitées les dispositions spécifiques s'ajoutant généralement au régime général (OIV, administrations, hébergeurs de données de santé, établissements financiers, FAI, etc.). Dans cette perspective, il a été décidé de ne traiter ni de la gestion des incidents, ni de celle du contentieux.

3 Principes généraux

3.1 Hiérarchie des normes et des contrats

Dans les sociétés occidentales, le droit est construit selon le principe pyramidal dit de la « hiérarchie des normes » formulée par le théoricien du droit Hans Kelsen. Ainsi une norme de niveau supérieur s'impose à celle de niveau inférieur. Le législateur et l'administration doivent donc s'assurer qu'une règle nouvelle respecte les règles antérieures de niveau supérieur dans la hiérarchie. En revanche, une règle nouvelle peut modifier les règles antérieures de même niveau et entraîne ainsi, en toute logique, l'abrogation des règles inférieures contraires.

Avec le développement du droit de l'Union européenne[3] qui irrigue de plus en plus souvent de nombreux aspects de notre droit national, il convient de s'interroger sur l'articulation de ce droit (règlement, décision de la Cour de Justice de l'Union européenne et directive) avec le droit français.

Ce dernier est composé de quatre blocs au sommet duquel se situe le bloc constitutionnel (i), vient ensuite le bloc législatif (ii), puis le bloc réglementaire (iii) et le bloc contractuel (iv) auxquels s'ajoute la prise en compte des usages.

(i) Le bloc constitutionnel est composé de la Constitution du 4 octobre 1958, du préambule de la Constitution du 27 octobre 1946, de la Déclaration des droits de l'Homme et du Citoyen du 26 août 1789 ainsi que des lois organiques (lois qui structurent l'organisation des pouvoirs administratifs). Les Traités de l'Union européenne sont intégrés dans ce bloc, ainsi que les différents Traités internationaux et conventions internationales bilatérales ratifiés et signés par la France (par ex : Convention de Budapest sur la cybercriminalité du 23 novembre 2001 ou les accords de l'Organisation Mondiale du Commerce).

(ii) Le bloc législatif comprend les lois ordinaires votées par le Parlement, les décisions du Président de la République, la directive européenne non transposée mais parvenue à date d'applicabilité pouvant être évoquée dans un procès, la directive européenne transposée par une loi, voire une ordonnance ratifiée, ainsi que le règlement communautaire directement applicable dans le droit interne. Ainsi, les directives et les règlements (tels que le règlement eIDAS[4] sur l'identification électronique et les services de confiance pour les transactions électroniques, ou encore le RGPD) ont une force supra-législative. Si les directives fixent les principes que les lois nationales doivent transposer, les règlements, en revanche, s'appliquent tels quels aux législations des États membres et annulent et remplacent les lois portant sur les sujets qu'ils concernent.[5]

[3] On n'utilise plus en droit l'expression de « droit communautaire » depuis l'entrée en vigueur du traité de Lisbonne en 2009. Depuis cette date, les « Communautés » n'existent plus, on parle désormais de « Droit de l'Union européenne ».

[4] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (**E**lectronic **I**dentification **a**nd trust **S**ervices (eIDAS))

[5] **Pour aller plus loin** : Il convient également de distinguer la directive d'harmonisation minimale, de la directive d'harmonisation maximale. Alors que l'harmonisation maximale établit les mêmes règles dans tous les États membres de l'Union européenne, l'harmonisation minimale permet aux États membres plus de latitude quant à

Ici doivent être mentionnés **les principes généraux du droit** que sont les règles dégagées par la jurisprudence (pouvoir d'interprétation de la loi par le juge), qui se situent à la même hauteur que la loi. Ainsi, le terme de « jurisprudence » s'applique à l'ensemble des jugements et des arrêts qu'ont rendu les Tribunaux et les Cours pour la solution d'une situation juridique donnée. Il est de principe que les Tribunaux ne peuvent rendre « *des arrêts de règlement* » imposant une règle générale applicable dans un même cas donné : ils ne peuvent se substituer ni au pouvoir législatif ni à celui de l'autorité administrative disposant du pouvoir réglementaire pour définir une telle règle obligatoire. Mais si la règle du précédent n'a pas cours en France, il est cependant évident que plus on monte dans la hiérarchie judiciaire, plus les décisions qui sont prises par les juridictions supérieures, ont de l'influence sur les juridictions inférieures avec une tendance à « s'aligner » sur les décisions des Cours d'appel et sur celles de la Cour de cassation. En effet, le rôle de cette Cour suprême, à l'instar du Conseil d'État, est d'uniformiser la jurisprudence afin d'éviter la disparité des jugements et des arrêts dans une matière donnée.

Pour rappel, la Justice est organisée en France en deux ordres depuis la Révolution française :

- **un ordre judiciaire** pour résoudre les conflits entre les personnes (individus, associations, entreprises, etc.) et les infractions à la loi pénale.

Les juridictions civiles de l'ordre judiciaire sont situées sur une échelle à deux degrés :

- les juridictions de première instance, c'est-à-dire celles qui rendent des jugements susceptibles d'appel, appartiennent toutes au premier degré, tels le Tribunal d'instance, le Tribunal de grande instance, le Tribunal de commerce, le Conseil de prud'hommes. Parallèlement, en matière pénale, nous trouvons le Tribunal correctionnel ;

- les juridictions du second degré que sont les Cours d'appel.

La Cour de cassation n'est pas un troisième degré de juridiction, car elle n'examine pas les faits. Son rôle, capital, mais limité, consiste à vérifier la conformité au droit dans certaines conditions.

- **un ordre administratif** pour les litiges entre une personne privée et une personne publique (administration, collectivité territoriale, personne privée chargée d'une mission de service public) ou entre administrations (Tribunal administratif, Cour administrative d'appel et Conseil d'État).

En cas de conflit de compétence entre les deux ordres, le Tribunal des conflits désigne l'ordre compétent[6].

Enfin, la « *question prioritaire de constitutionnalité* », qui existe depuis la réforme constitutionnelle du 23 juillet 2008 est le droit reconnu à toute personne qui est partie devant une juridiction de soutenir qu'une disposition législative porte atteinte aux droits et libertés que la Constitution garantit. Sous réserve de la recevabilité de la question, il

l'atteinte de l'objectif poursuivi par le texte

[6] **Pour en savoir plus** : https://www.legifrance.gouv.fr/Sites/Juridictions

appartient au Conseil constitutionnel, sur renvoi par le Conseil d'État ou la Cour de cassation, de se prononcer et, le cas échéant, d'abroger la disposition législative[7].

(iii) Le bloc réglementaire vise les ordonnances (avant leur ratification), les décrets (en conseil des Ministres, en Conseil d'État ou simples par le Premier Ministre), les arrêtés ministériels ou interministériels et les arrêtés préfectoraux émanant du Préfet.

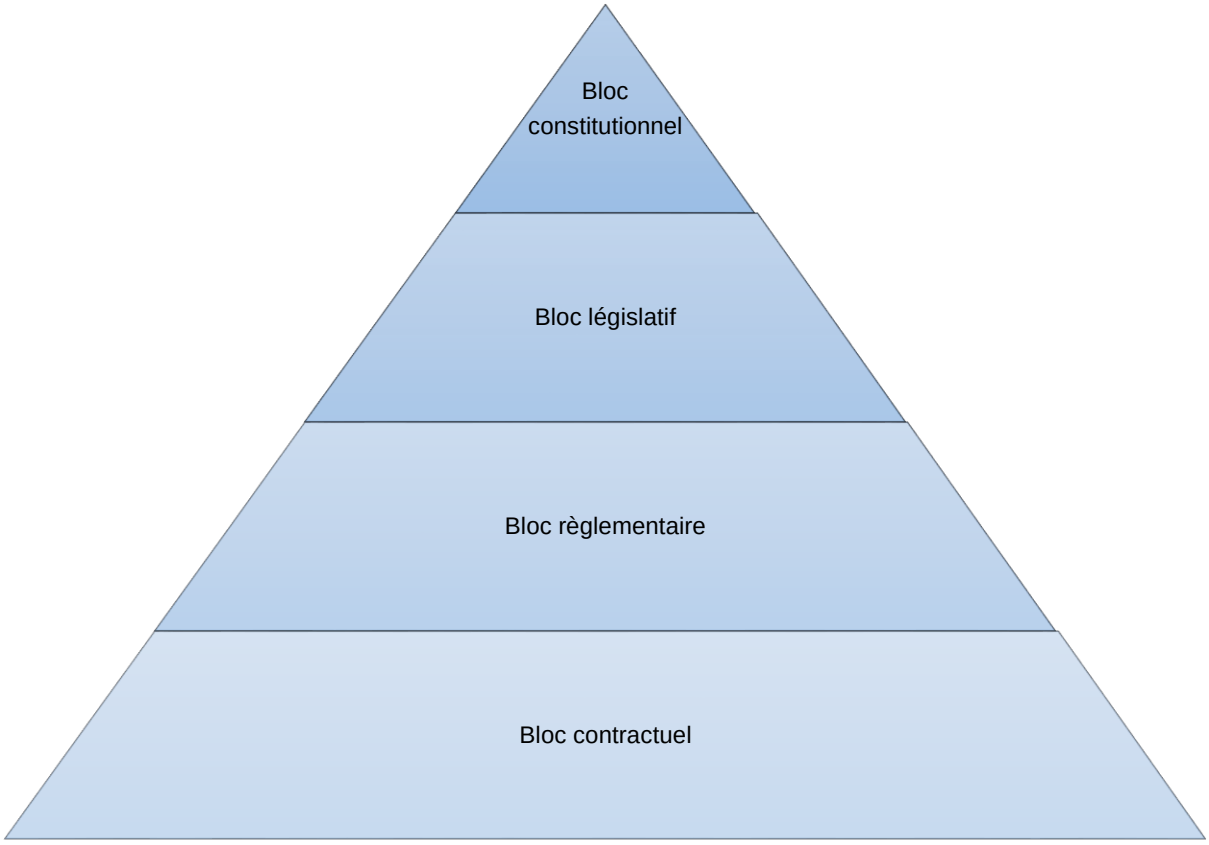
(iv) Le bloc contractuel vise les contrats qui tiennent lieu de lois entre les parties qui les ont signés.

L'usage est une pratique dont l'emploi constant, général et relativement ancien dans le monde des affaires, dans la profession ou un secteur d'activité précis (état de l'art) en fait une règle non écrite qui s'impose aux parties et aux juges. Les circulaires et instructions ne s'imposent pas au juge et sont en principe dépourvues de valeur réglementaire. De même, les recommandations de la CNIL n'ont pas en principe valeur de loi, ou de décret, mais constituent des documents relevant les bonnes pratiques que la CNIL (s'appuyant elle-même sur la loi n° 78-17 du 6 janvier 1978 modifiée dite « Loi Informatique et Libertés »), en tant que régulateur, souhaite voir respectées par les professionnels. Il est toutefois patent que la CNIL a de plus en plus tendance à se reposer sur ces recommandations pour fonder ses condamnations (ex : délibération n° 03-034). Enfin, la CNIL fait directement référence à certaines de ses recommandations dans les normes simplifiées qu'elle élabore à destination des entités et auxquelles ces dernières peuvent faire un engagement de conformité (ex : délibération n° 2016-264 du 21 juillet 2016).

Pour mémoire, les codes, généralement publiés tous les ans, rassemblent de façon cohérente des textes épars dans une partie législative et une partie réglementaire avec une rédaction harmonisée et actualisée pour faciliter l'accès aux règles de droit en fonction des domaines concernés. Certains sont visés par le législateur, d'autres ne sont que des « compilations » réalisées à l'initiative d'un éditeur.

[7] **Pour en savoir plus** : http://www.conseil-etat.fr/Conseil-d-Etat/Question-prioritaire-de-constitutionnalite

Présentation récapitulative de la hiérarchie des normes



1. Bloc constitutionnel : • Constitution du 4 octobre 1958 • Préambule de la Constitution du 27 octobre 1946 • Déclaration des droits de l'Homme et du Citoyen du 26 août 1789 • Lois organiques • Traités internationaux et conventions internationales bilatérales
2. Bloc législatif • Règlements européens • Directives européennes parvenues à date d'applicabilité • Lois ordinaires • Ordonnances ratifiées • Décisions du Président de la République • Jurisprudence
3. Bloc réglementaire • Ordonnances non ratifiées • Décrets pris en conseil des Ministres, en Conseil d'État ou simples par le Premier ministre • Arrêtés ministériels ou interministériels, arrêtés préfectoraux
4. Bloc contractuel • Conventions, contrats, protocoles, avenants, bons de commande, devis acceptés, etc.)

3.2 Responsabilités

En termes de responsabilité juridique, il convient de distinguer la responsabilité civile **(1)** de la responsabilité pénale **(2)**, chacune étant régie par des règles propres.

3.2.1 Responsabilité civile

La responsabilité civile, du point de vue juridique, peut être appréhendée comme le mécanisme par lequel une personne ayant causé un dommage est tenue d'en réparer les conséquences, par l'attribution notamment de dommages et intérêts.

La responsabilité civile se subdivise en deux sous-catégories que sont la responsabilité civile contractuelle et la responsabilité civile délictuelle (ou extra-contractuelle).

La responsabilité civile contractuelle s'applique dès lors que l'une des parties à un contrat a mal, ou pas, exécuté ses obligations vis-à-vis de l'autre partie (exemple : le taux de disponibilité que l'hébergeur d'une application en mode SaaS garanti par contrat n'est pas atteint). Le régime de responsabilité contractuelle sera largement dépendant de la volonté des contractants et des termes exacts des dispositions de leur contrat. Elle répond à un régime juridique distinct de celui de la responsabilité délictuelle.

La responsabilité civile délictuelle s'applique dans le domaine civil lorsqu'il n'existe pas de relations contractuelles entre la victime et l'auteur du dommage (exemple : un pot de fleurs tombe d'une fenêtre et blesse un passant).

Ainsi ces deux formes de responsabilité civile s'excluent l'une de l'autre et sont soumises à des règles et des régimes juridiques distincts. Elles interdisent à celui qui subit le dommage de choisir entre l'un ou l'autre des fondements (principe de non-cumul des responsabilités).

Ceci est illustré par des dispositions du Code civil spécifiques à chacune de ces formes de responsabilité civile, à savoir :

- la responsabilité contractuelle, désormais régie par les articles 1231 à 1231-7 du Code civil (anciennement articles 1146 à 1155 du même Code) depuis le 1er octobre 2016, date d'entrée en vigueur de l'ordonnance n° 2016-131 du 10 février 2016 (JO 11 févr.2016) **;**
- la responsabilité délictuelle, désormais régie par les articles 1240 à 1244 du Code civil (anciennement articles 1382 à 1386 du même Code) depuis le 1er octobre 2016, date d'entrée en vigueur de l'ordonnance n° 2016-131 du 10 février 2016 (JO 11 févr.2016).

3.2.1.1 La responsabilité contractuelle

Gérard Cornu définit la **responsabilité contractuelle** comme « *l'obligation pour le contractant qui ne remplit pas (en tout, en partie, ou à temps) une obligation que le contrat mettait à sa charge, de réparer (en nature si possible ou, à défaut, en argent) le dommage causé à l'autre partie (le créancier), soit par l'inexécution*

totale ou partielle, soit par l'exécution tardive de l'engagement contractuel »[8].

➢ **Clauses limitatives et exonératoires de responsabilité**

En vertu de la liberté contractuelle, les parties peuvent valablement stipuler des clauses afin d'alourdir leur responsabilité ou au contraire de la restreindre en cas de manquement constaté.

Tel est notamment le cas des clauses élusives ou limitatives de responsabilité qui visent à exclure la responsabilité ou à limiter le montant de la réparation en cas d'inexécution ou de mauvaise exécution par l'un des contractants.

La **clause limitative de responsabilité** est la clause qui limite ou détermine les cas dans lesquels il sera possible d'engager la responsabilité des contractants.

On utilise le terme de « **clause pénale** » pour désigner une clause prévoyant automatiquement une sanction financière en cas de manquement à ses obligations, étant entendu qu'en cas d'application de cette sanction financière, il n'y aura pas de dommages-intérêts supplémentaires ultérieurs (la clause est exclusive de toute autre réparation du dommage).

La **clause de non-responsabilité**, quant à elle, exclut toute responsabilité.

Ces clauses sont, en principe, valables. Toutefois, leur validité peut être remise en cause :

- lorsqu'elles mettent en échec une garantie légale ;
- lorsqu'elles limitent ou excluent la responsabilité d'un professionnel dans un contrat conclu avec un consommateur. La clause sera réputée non écrite sur le fondement de l'article L. 132-1 du Code de la consommation ;
- en cas de faute lourde du débiteur, sur le fondement de l'article 1231-3 du Code civil (anciennement article 1150 du Code civil) et en application de la célèbre jurisprudence Chronopost : « *seule la faute lourde caractérisée par une négligence d'une extrême gravité confinant au dol et dénotant l'inaptitude du débiteur de l'obligation à l'accomplissement de sa mission contractuelle*, *peut mettre en échec la limitation d'indemnisation prévue au contrat type* » (Ch. Mixte 22 avril 2005 Chronopost III),
- et encore lorsqu'elles visent une obligation essentielle du contrat (Cass. com., 22 oct. 1996, JCP G 1997, II, n° 22881). En effet, si l'obligation essentielle qui sous-tend le contrat perd toute sa portée, elle prive le créancier de toute contrepartie et le contrat n'a plus de raison d'être. A cet égard, l'article 1170 du Code civil dispose désormais que « *toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite* ».

Enfin, il convient de noter que l'article 1171 du Code civil, directement inspiré de la notion de clauses abusives prévues dans le Code de la consommation, énonce que : « *Dans un contrat d'adhésion, toute clause qui crée un*

[8] Extrait du « Vocabulaire juridique », Gérard Cornu, PUF

déséquilibre significatif entre les droits et les obligations des parties au contrat est réputée non écrite » (1er alinéa).

3.2.1.2 La responsabilité extra-contractuelle/délictuelle

La responsabilité extra-contractuelle (ou encore appelée responsabilité délictuelle) s'articule autour de trois concepts :

- la faute (ou la simple négligence) ;
- le dommage ;
- et le lien de causalité existant entre cette faute et le dommage subi.

Ainsi, dans l'exemple vu précédemment, la personne qui pose le pot de fleurs sur le rebord de sa fenêtre, sans s'assurer qu'il ne peut pas tomber, commet une faute. Le pot de fleurs tombe et blesse un passant qui subit par la même un préjudice. Le lien de causalité est donc établi : c'est bien la faute qui a causé le dommage.

Il convient de préciser que la responsabilité délictuelle repose notamment sur l'article 1240 du Code civil (ancien article 1382 du même Code), qui dispose que « *Tout fait quelconque de l'homme, qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé, à le réparer* ». Le Code civil prévoit certains régimes de responsabilité dits « objectifs », qui s'appliquent qu'il y ait faute ou non. De tels cas de mise en cause « objective » de la responsabilité, sans faute particulière, se retrouvent notamment en matière d'accidents de la circulation, de commercialisation de produits défectueux ou de responsabilité de l'employeur en raison des actes commis par ses salariés.

Cette distinction instaurée entre la responsabilité contractuelle et la responsabilité délictuelle a des implications directes notamment :

- en termes de charge de la preuve : pour la victime en responsabilité délictuelle, il est nécessaire d'apporter la preuve de la faute commise par le débiteur, alors que pour la responsabilité contractuelle il suffit de démontrer la simple inexécution, qui est alors présumée et c'est alors le débiteur qui doit prouver qu'il n'est pas en faute ;
- en termes de gravité de la faute comme fait générateur (n'importe quelle faute pour la responsabilité délictuelle, contre un manquement d'une certaine gravité pour la responsabilité contractuelle) ;
- en termes de prescription : durée de cinq ans de droit commun désormais alignée pour la responsabilité délictuelle et la responsabilité contractuelle (sauf exception) avec points de départ différents (cf. Tableau ci-dessous) ;
- en termes d'étendue de la réparation : selon l'article 1231-3 du Code civil (ancien article 1150 du même Code), la réparation ne sera limitée qu'au dommage prévisible au moment de la formation du contrat, qui pour la responsabilité contractuelle, dépend du contrat et du respect de la volonté des parties (clause limitative de responsabilité,...).

	Responsabilité contractuelle	Responsabilité délictuelle
Charge de la preuve	Simple inexécution faisant présumer la faute ; au débiteur d'apporter la preuve qu'il n'est pas responsable d'un manquement contractuel	Preuve de la faute apportée par la victime
Gravité de la faute	Manquement contractuel (obligation de moyen, de moyen renforcée ou de résultat)	Faute constituée par un acte ou une abstention. Abus de droit
Prescription	5 ans à compter du manquement (sauf exception)	5 ans à compter de la connaissance du fait délictueux
Étendue de la réparation	Dommage prévisible au moment de la formation du contrat	Dommage subi

Les distinctions initiales existant entre les responsabilités contractuelle et délictuelle, bien que classiques et cardinales, sont aujourd'hui brouillées.

Ainsi, la réforme globale de la responsabilité civile à venir pour compléter la récente réforme du droit des obligations, envisage de clarifier les régimes de responsabilité : « *Le régime de la responsabilité contractuelle sera donc modernisé dans le cadre du futur projet de réforme globale de la responsabilité civile, qui détaillera les dispositions communes aux responsabilités contractuelle et extra-contractuelle, et les dispositions propres à chacun de ces deux régimes* » (Rapport au président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats).

3.2.1.3 Responsabilités spécifiques

- **Responsabilité des employeurs du fait de leurs salariés vis-à-vis des tiers**

La responsabilité des commettants du fait de leurs préposés est un type de responsabilité du fait d'autrui. Il s'agit de la situation dans laquelle un employé cause un dommage à un tiers et engage dès lors la responsabilité délictuelle de son employeur. Ce régime de responsabilité est prévu à l'article 1242 du Code civil (ancien article 1384 du même Code) dont l'alinéa 5 dispose que *« Les maîtres et les commettants, (sont solidairement responsables) du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ».*

En tout état de cause, le commettant peut se dégager de sa responsabilité civile du fait de son préposé si ce dernier a agi hors des fonctions auxquelles il était affecté, sans autorisation et à des fins étrangères à ses attributions.

- **Responsabilité des employeurs vis-à-vis de leurs salariés**

Le contrat qui lie un employeur à ses salariés est le contrat de travail, auquel s'ajoutent la convention collective applicable en fonction du secteur d'activité concerné et les réglementations spécifiques du droit du travail (codifiées dans le Code du travail).

L'employeur aura sa responsabilité engagée vis-à-vis de ses salariés en cas de non-respect de ses obligations. Ainsi, en tant que dépositaire de données à caractère personnel concernant le salarié (notamment pour l'établissement des bulletins de paie), l'employeur est responsable en cas de pertes de données ou vols de données à caractère personnel de son salarié en raison d'absence de mesures prises pour sécuriser l'accès à ces données parfois sensibles (numéro de sécurité sociale, données de santé, etc.).

- **Responsabilité des salariés vis-à-vis de leurs employeurs**

Les principes décrits ci-dessus s'appliquent également dans ce cas. C'est le contrat de travail avec la convention collective et le Code du travail qui constituent le socle des obligations du salarié vis-à-vis de son employeur, notamment s'agissant du principe de loyauté et l'engagement de ne rien entreprendre dans le cadre de la société pouvant mettre en danger les autres salariés ou l'entreprise, voire son dirigeant.

- **Responsabilité de la personne morale**

Les personnes morales, dotées de la personnalité juridique, sont responsables sur le plan civil : en droit civil, leur responsabilité tant contractuelle que délictuelle peut être engagée au même titre qu'une personne physique.

- **Responsabilité des dirigeants**

La responsabilité personnelle des dirigeants peut être engagée lors de l'exercice de leurs fonctions de direction.

Pour les différentes sociétés commerciales, les dispositions du Code de commerce sont applicables. Pour les sociétés à responsabilité limitée (SARL) : arts. L.223-22 et L.223-24 du Code de commerce, pour les sociétés par actions (SA) : arts. L.225-249 à L.225-254 du Code de commerce. À défaut de règles spécifiquement prévues par le droit des sociétés, c'est alors le droit commun qui aura vocation à s'appliquer, tant en matière délictuelle qu'en matière contractuelle.

Ainsi, il convient de se référer aux articles 1240 et 1241 du Code civil (anciennement articles 1382 et 1383 du même Code) s'agissant de la responsabilité des dirigeants à l'égard des tiers et à l'article 1231-1 du Code civil (anciennement article 1147 du même Code) pour la responsabilité des

dirigeants à l'égard de la société et des associés.

Les dirigeants sont responsables à l'égard de la société, des associés et actionnaires.

- S'agissant de la société, ils doivent répondre des fautes liées à l'exercice de leurs fonctions (violation des dispositions législatives ou réglementaires applicables à la société, non-respect de l'objet social, faute de gestion comprenant l'imprudence, la négligence ou des manœuvres frauduleuses).
- S'agissant des associés et actionnaires, ils peuvent être poursuivis pour manquement à leur devoir de loyauté.

Ils sont également responsables à l'égard des tiers. Dans la plupart des cas, la société constitue un paravent et assume seule la responsabilité de l'action ou l'omission fautive du dirigeant social qui de ce fait n'engage pas sa responsabilité. Cependant, le législateur et la jurisprudence ont instauré une responsabilité des dirigeants à l'égard des tiers, si le dirigeant a commis personnellement une faute séparable de ses fonctions.

➢ **Responsabilité des sous-traitants/donneurs d'ordre**

Dans l'hypothèse de la sous-traitance[9], seul le soumissionnaire/entrepreneur principal va contracter avec le maître d'ouvrage et sera ensuite l'unique responsable vis-à-vis de ce dernier. Il assurera les relations contractuelles avec les sous-traitants qui ne se connaîtront pas nécessairement les uns les autres.

En termes de responsabilité, le sous-traitant n'engagera sa responsabilité contractuelle que par rapport à son donneur d'ordre (lequel est le soumissionnaire cocontractant du client). En cas de faute de sa part entraînant un préjudice à l'égard du client final, ce dernier aura alors le choix entre la mise en cause en cascade des responsabilités contractuelles successives du co-contractant principal puis du sous-traitant vis-à-vis de celui-ci, ou agir directement contre le sous-traitant. Mais ce choix sera exclusif en raison du principe de non-cumul des responsabilités contractuelles et délictuelles (ou extra-contractuelles) pour une même faute.

NOTA BENE : Notons enfin que la réforme récente du droit des contrats et des obligations ne traite pas directement de la responsabilité civile. Celle-ci fera l'objet d'un projet de loi ultérieur. Un projet de réforme du droit de la responsabilité civile a été rendu public le 13 mars 2017[10].

[9] Selon la loi n° 75-1334 du 31 décembre 1975 relative à la sous-traitance: « *la sous-traitance est définie comme l'opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant, l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché public conclu avec le maître de l'ouvrage* ». A ne pas confondre avec la notion de sous-traitant au sens de la Loi Informatique et Libertés et du RGPD : « *Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre* ».

[10] http://www.textes.justice.gouv.fr/textes-soumis-a-concertation-10179/projet-de-reforme-du-droit-de-la-responsabilite-civile-29782.html

Ainsi, il est encore trop tôt pour étudier les apports de cette réforme. Selon certains auteurs, l'avant-projet « *semble osciller entre simple mise en forme de solutions jurisprudentielles acquises et innovations plus ou moins audacieuses* ».

3.2.2 Responsabilité pénale

La responsabilité pénale est celle encourue vis-à-vis de l'État en raison du trouble à l'ordre public causé par l'auteur d'une infraction, qu'il soit une personne physique et/ou morale (entreprise, association, etc.). La responsabilité des personnes morales a été étendue par principe à toutes les infractions au 1er janvier 2006.

Une infraction n'existera et ne sera sanctionnée pénalement que si trois éléments sont réunis cumulativement :

- l'**élément légal** : consiste en l'existence d'un texte sanctionnant un type d'action (principes de légalité et d'interprétation stricte de la loi pénale) : en l'absence de loi, pas d'infraction ;
- l'**élément matériel** : est un acte positif, au minimum un commencement d'exécution, ou un acte négatif (ex : omission d'exécuter une action telle que la non-assistance à personne en danger) ;
- l'**élément moral ou intentionnel** : l'auteur a eu pleinement conscience de l'acte commis ; en revanche, peu importe qu'il ait été conscient des conséquences. Il existe toutefois des exceptions (on parle de « délits objectifs »), comme la détention d'images pédophiles pour laquelle l'intention n'a pas à être démontrée.

Ce n'est que lorsque ces trois conditions sont remplies que la responsabilité pénale de l'auteur peut être engagée. Dans le cas, par exemple, d'un virus infectant un poste informatique d'une entreprise et transformant celui-ci en poste zombie attaquant une entreprise tierce, la responsabilité pénale de l'entreprise infectée par le virus ne pourrait être recherchée en vertu du texte réprimant les piratages informatiques : il manque ici l'élément intentionnel de l'infraction (en revanche, ceci n'est pas un obstacle pour rechercher la responsabilité civile).

➢ Responsabilité de la personne morale

En droit pénal, la personne morale est responsable des infractions commises pour son compte par un représentant de la société dès lors que l'infraction a été commise en son nom et dans l'intérêt de l'entreprise (article 121-2 du Code pénal). Par exemple, un représentant ou un organe agit dans le cadre de la direction de la personne morale et en son nom. Le champ des infractions susceptibles de conduire à la mise en cause de la responsabilité pénale des personnes morales était initialement cantonné aux « *cas prévus par la loi ou le règlement* ». Les entreprises sont désormais potentiellement justiciables des mêmes infractions que les particuliers.

➢ **Délégation de pouvoirs**

Définition : Le mécanisme de la délégation de pouvoirs permet à une autorité (le délégant) de transférer une partie des pouvoirs qu'il tient de son mandat social ou de son contrat de travail, à un subordonné (le délégataire). Le délégataire pourra ainsi, par exemple, conclure des contrats au nom de la société, prérogative qui relève en principe de la seule compétence du représentant légal de l'entreprise.

Ce transfert de pouvoirs s'accompagne d'un transfert des obligations et des responsabilités attachées auxdits droits. Le délégataire devient responsable en lieu et place du délégant.

Pour exonérer le chef d'entreprise ou le délégant, la délégation de pouvoirs doit être certaine, précise et dépourvue d'ambiguïté. Toutefois, le fait de prévoir ce transfert de responsabilité par écrit n'est pas suffisant, et ce même si le délégataire l'a expressément accepté.

En vertu de l'article 121-1 du Code pénal, selon lequel « *nul n'est responsable pénalement que de son propre fait* », le transfert de responsabilité implique en outre que le préposé soit pourvu de la compétence, de l'autorité et des moyens nécessaires pour veiller au respect des règles faisant l'objet de la délégation par le chef d'entreprise ou le délégant.

Ainsi, la validité de la délégation de pouvoirs suppose que les conditions cumulatives suivantes soient réunies :

- une délégation de pouvoirs certaine, précise et dépourvue d'ambiguïté ;
- le délégataire est obligatoirement un salarié de l'entreprise ;
- il doit faire partie du personnel d'encadrement ;
- il doit expressément accepter la délégation (un écrit est préconisé) ;
- il doit avoir l'autorité, la compétence (c'est-à-dire des diplômes, des aptitudes et de l'expérience dans la fonction occupée) et les moyens nécessaires aussi bien matériels que financiers.

Une sous-délégation est possible dans les conditions de fond et de forme ci-dessus envisagées, la chaîne des délégations ne devant pas conduire à diluer les responsabilités.

En conclusion, la rédaction de la délégation de pouvoirs doit faire l'objet d'un soin tout particulier, afin qu'elle puisse résister à l'examen des juges.

3.3 Droit de la preuve

Dans ce domaine également, la réforme du droit des obligations et du droit de la preuve par l'ordonnance n° 2016-131 précitée (applicable depuis le 1er octobre 2016) a conduit à revoir formulations et numérotation des articles, mais sans en bouleverser les principes généraux.

3.3.1 Notion de preuve

Il est essentiel de garder en mémoire qu'en droit, toute prétention (ce logiciel m'appartient, j'ai tous les droits sur ce site web, etc.) nécessite que l'on puisse être **en mesure de justifier des droits allégués** (un ancien adage dit ainsi « *Ne pas être ou ne pas être prouvé, c'est tout un* ») sauf à ce que la loi prévoit des aménagements pour protéger par exemple certaines personnes (les auteurs, les salariés, etc.) en leur accordant des présomptions : en matière de droit à la consommation, les règles du Code de la consommation s'interprètent en faveur du consommateur ; en matière de vente, toute ambiguïté du contrat s'interprète au détriment du vendeur, etc.

Cette nécessité d'apporter la preuve de ses prétentions est formalisée dans l'article 1353 du Code civil : « *Celui qui réclame l'exécution d'une obligation doit la prouver* ».

Ainsi, celui qui échoue à apporter cette preuve alors qu'il en a la charge, risque de perdre son procès. Le tribunal n'a en effet pas pour rôle de pallier la carence d'une partie dans ce domaine et le recours à une expertise judiciaire ordonnée à la demande d'une des parties par le tribunal selon le respect du contradictoire[11] (notamment en matière informatique) suppose qu'un certain nombre d'éléments pertinents soient versés aux débats. Au fur et à mesure des preuves apportées par l'une ou l'autre partie en fonction de leurs allégations réciproques, la charge de la preuve pèse alternativement sur chacune d'entre elles au cours du procès. Au final, « *l'incertitude ou le doute sont retenus au détriment de celui qui en a la charge* ».

Dans certains cas, les preuves peuvent être discutées et remises en cause par la partie adverse selon des procédures spécifiques propres au moyen de preuve utilisé. Ainsi, en matière de contrat établi par écrit, l'article 1373 du Code civil reprend le principe déjà existant en offrant la possibilité de « désavouer » sa signature pour contester être le signataire de ce contrat (y compris dans les hypothèses de signature électronique, une procédure de vérification d'écriture étant alors possible). Dans l'hypothèse où la réalité d'un fait ou d'un contenu ou bien encore l'existence d'un acte est discutée, c'est le juge qu'il faudra convaincre de la pertinence de ses arguments ou de la fiabilité des moyens techniques utilisés.

3.3.2 Régime juridique de la preuve

Les règles applicables en matière de droit de la preuve sont différentes suivant la branche du droit considérée.

Ainsi, en matière de **droit civil**, le système de preuve est prévu et encadré par la loi (articles 1353 à 1386-1 du Code civil) et seuls certains modes de preuve sont acceptés. En outre la preuve doit être loyale. En pratique, l'écrit prédomine, qu'il soit papier ou électronique, à partir du moment où il est signé par la partie qui s'engage.

[11] Ce qui est à distinguer d'une expertise non contradictoire

Une distinction fondamentale existe entre les « actes juridiques » et les « faits juridiques ».

- **Les « actes juridiques »**[12], tels les contrats, nécessitent le consentement des parties, se traduisant par leur signature du document, établi en autant d'exemplaires que de parties ayant un intérêt distinct, et conservé par chacune d'entre elles, « *à moins que les parties ne soient convenues de remettre à un tiers l'unique exemplaire dressé* » comme le prévoit l'article 1375 du Code civil.

Un acte juridique permet de se préconstituer une preuve dans l'hypothèse d'une contestation ultérieure de cet acte. À noter cependant que la validité de certains de ces actes (cessions de droit d'auteur, cautionnement, etc.) nécessite un formalisme spécifique prévu par la loi, généralement pour protéger l'une des parties.

Ainsi, l'acte authentique (écrit rédigé par un notaire) a la primauté en termes de valeur probante devant l'acte dit sous « seing privé » (rédigé par écrit par des particuliers).

Quant à l'aveu[13] ou le serment[14] (de la partie qui doit établir la preuve), ils ont pour des raisons historiques une valeur théoriquement égale.

Viennent ensuite le « commencement de preuve par écrit » (rendant acceptables d'autres commencements de preuve par écrit pour augmenter sa valeur probante, tel qu'un courrier électronique) ou les présomptions, déduites d'éléments de faits[15].

Par exception, actuellement, la preuve des actes juridiques portant sur une somme inférieure ou égale à 1 500 euros est libre, ce qui explique qu'un contrat de transport (taxi, bus, etc.) ne nécessite pas de document signé des deux parties pour être prouvé, tout comme la majorité des commandes passées sur des sites de e-commerce.

Le droit s'étant adapté aux évolutions technologiques, les contrats peuvent généralement être signés électroniquement, la signature électronique ayant la même valeur que la signature manuscrite à condition que le procédé de signature utilisé réponde aux exigences posées par les textes (cf. Règlement « eIDAS » n° 910/2014 du 23 juillet 2014 et ses actes d'exécution) ou que le magistrat saisi d'un contentieux considère que la signature électronique utilisée est « fiable » (sur la base d'une analyse technique ou de son intime conviction). La signature électronique doit ainsi permettre une identification renforcée du signataire et garantir l'intégrité de l'acte signé, lors de sa signature et dans le temps.

[12] L'acte juridique est une « *manifestation de volonté destinée à produire des effets de droit* » (article 1100-1 du Code civil).
[13] *« L'aveu est la déclaration par laquelle une personne reconnaît pour vrai un fait de nature à produire contre elle des conséquences juridiques* », article 1383 modifié du Code civil.
[14] Article 1384 et suivants modifiés du Code civil.
[15] « *Constitue un commencement de preuve par écrit tout écrit qui, émanant de celui qui conteste un acte ou de celui qu'il représente, rend vraisemblable ce qui est allégué* », article 1362 modifié du Code civil.

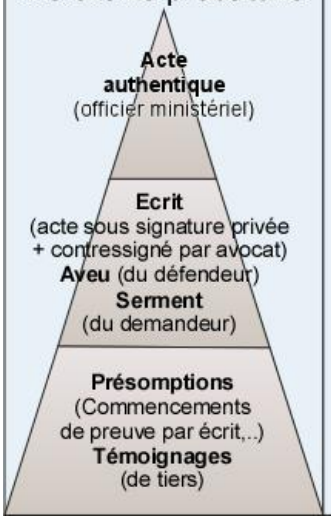
- À côté des actes juridiques, il existe des « **faits juridiques** »[16], c'est à dire des événements qui peuvent avoir des conséquences juridiques non recherchées à l'origine (attaque informatique, crash d'un serveur, remise d'un bulletin de paie, etc.). Il n'y a dans ces cas, et fort logiquement, pas d'écrit préconstitué : en droit civil, **la preuve de ces faits est donc libre et s'effectue par tout moyen.**

En droit commercial, c'est à dire dans les relations entre « commerçants » au sens juridique du terme (ce qui inclut la très grande majorité des entreprises), la preuve est dite « libre » : ainsi, **tous les modes de preuve sont acceptables par le juge. Reste que c'est à lui qu'il appartiendra de trancher en cas de litige et d'apprécier la force probante des preuves soumises**.

En droit pénal, également, la preuve est libre.

Enfin, sauf exception, la preuve est également libre en **droit administratif**, la force que le juge attachera à celle-ci dépendant de son intime conviction.

Les règles de preuves peuvent se résumer selon le schéma suivant, étant entendu que la preuve des faits étant libre dans tous les cas et pour tous les régimes de preuve, ce schéma ne concerne que les actes juridiques :

<table>
<tr><th colspan="3">Régime de droit commun de la preuve
Classification de la valeur des preuves entre elles</th><th rowspan="2">Droit commercial, Droit administratif, Droit pénal, etc</th></tr>
<tr><th>Par défaut</th><th>Contrat de vente inférieur ou égal à 1 500 EUR</th><th>« Contrat sur la preuve »</th></tr>
<tr><td>Hiérarchie probatoire
 
</td><td>Preuve libre
(donc écrit non-signé ou « mal signé » suffisant)</td><td>Les Parties au contrat fixent elles-mêmes, grâce à un contrat antérieur, une hiérarchie probatoire différente ou prévoient l'acceptation d'autres moyens de preuve (dans certaines limites)</td><td>Preuve libre entre commerçants (tout moyen de preuve est recevable) / convention sur la preuve possible
-
Sauf exceptions, en droit administratif, la preuve est libre et la force probante dépend de l'intime conviction du juge</td></tr>
</table>

[16] Les faits juridiques sont des « *agissements ou des événements auxquels la loi attache des effets de droit* » (cf. article 1100-2 du Code civil). Ils étaient également définis historiquement comme des faits quelconques « *auquel la loi attache directement des effets juridiques, indépendamment de la volonté individuelle* ».

3.3.3 La question de la « preuve à soi-même »

La Cour de cassation a déjà eu l'occasion d'affirmer le principe selon lequel « *nul ne peut se pré-constituer preuve à soi-même* ».

Il convient de modérer l'interprétation qui pourrait être tirée à tort de cet adage, qui n'existe que pour éviter les manipulations qui pourraient être faites par une partie au détriment de l'autre.

En effet, cet adage ne s'applique qu'aux actes juridiques (essentiellement les contrats) et non aux faits juridiques (les traces informatiques…), comme l'a récemment rappelé la Cour de cassation (Civ. 3e, 10 mars 2016, n° 15-13.942)

En matière de preuve des faits juridiques, les tribunaux peuvent considérer, par exemple, que des documents émanant d'une personne morale (notamment ceux issus de son SI) sont parfaitement acceptables à titre de preuve. Un débat sur la fiabilité d'un système informatique dont émaneraient ces documents reste évidemment toujours possible.

Ainsi, la Cour de cassation a eu l'occasion d'affirmer à plusieurs reprises[17] que des enregistrements informatiques établis par la société qui s'en prévaut ou encore des relevés de communications téléphoniques (dans le cas de France Télécom[18]) étaient parfaitement acceptables et bénéficiaient d'une présomption simple de véracité des faits allégués.

C'est la raison pour laquelle un système informatique permettant l'enregistrement des logs voire l'archivage de documents électroniques pourra être utilisé dans les contentieux et présenté par la partie qui les a réalisés, sans risquer la censure *in fine* de la Cour de cassation.

Reste que c'est la fiabilité du système informatique lui-même qui pourra être discutée par la partie à qui on oppose les enregistrements réalisés. Il convient en conséquence, afin de donner la plus grande force probante possible à ces enregistrements, de prévoir une auditabilité et des politiques claires et transparentes concernant l'enregistrement, le traitement, l'intégrité, la confidentialité ou encore les conditions de conservation des informations stockées.

Ajoutons, pour conclure, que ces enregistrements informatiques, pour qu'ils soient acceptés devant les juridictions civiles, doivent avoir été constitués conformément aux textes applicables en ce qui concerne la protection des données à caractère personnel : ces données utilisées en tant que preuves doivent ainsi avoir été recueillies, traitées, sécurisées ou encore transmises uniquement aux personnes prévues ou autorisées, conformément à la loi.

[17] Cf. Cass.civ.1ère 13 juillet 2004 01-11.729
[18] Cf. Cass.civ. 1ère 7 mars 2000 n° 98-12.397

4 Les Fiches thématiques

4.1 La protection des données à caractère personnel (ou « données personnelles »)

PROTECTION DES DONNÉES PERSONNELLES*[19]	
➢ **Conformité des traitements de données personnelles – L'essentiel**	**N° 1.1**

CONTEXTE

Si la loi « informatique et libertés » est de plus en plus connue, peu d'organismes ont une vision complète des obligations qui en découlent quant à la gestion des données personnelles. Ainsi, la plupart des organismes pensent que cela se résume à la réalisation de formalités administratives lourdes auprès de la CNIL. Or la gestion des données personnelles dans le respect des exigences légales et réglementaires implique un processus parfois ardu d'identification et d'encadrement des traitements de l'organisme.
Le RGPD, entré en vigueur le 25 mai 2016 et entrant en application le 25 mai 2018, modifie sensiblement ce contexte juridique.

OBJECTIFS

La présente fiche vise à lister les principales étapes de ce processus permettant d'intégrer les exigences de la loi « informatique et libertés ».

TEXTES APPLICABLES

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Code pénal, articles 226-16 à 226-24
- Règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD, entré en vigueur le 25 mai 2016, qui entrera en application le 25 mai 2018)

RISQUES

Les principaux manquements aux obligations érigées par la loi « informatique et libertés » sont susceptibles de constituer des infractions pénales. Les peines encourues sont les suivantes : cinq ans d'emprisonnement et 1 500 000 euros d'amende pour une personne morale.

Indépendamment, la CNIL peut également, de son côté, mettre en demeure puis prononcer les sanctions administratives suivantes en cas de manquement à la loi « informatique et libertés » :

- un avertissement ;

[19] Les mots ou expressions comportant un astérisque (*) sont définis dans le glossaire en fin de document.

- une sanction pécuniaire de 3 millions d'euros (depuis la loi pour une République numérique) ;
- une injonction de cesser le traitement ou un retrait d'autorisation.

Lors de l'entrée en application du RGPD, le montant maximal des sanctions sera porté à 20 millions d'euros ou 4 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu.

Les impacts, en termes d'image, peuvent également être très importants. En effet, la CNIL peut également rendre publics les avertissements, les mises en demeure et les sanctions qu'elle prononce. Ces publications sont souvent relayées par la presse, grand public ou spécialisée TIC. De plus, depuis la loi « Pour une République numérique », la CNIL peut ordonner une communication de ses décisions directement auprès des personnes concernées.

RECOMMANDATIONS

<u>En phase projet :</u>

- Identifier, dès la phase projet :
  - les traitements de données personnelles* ;
  - le responsable de traitement* ;
  - les éventuelles données personnelles sensibles* ;
  - un interlocuteur pour chaque traitement ;
- Déterminer les finalités poursuivies par chacun de ces traitements ;
- Fixer les durées de conservation des différentes catégories de données personnelles ;
- Identifier les catégories de destinataires des données ;
- S'assurer que les traitements font l'objet de mesures de sécurité adaptées à la nature des données et aux risques présentés par le traitement ;
- Identifier les sous-traitants intervenant sur les traitements ;
- Encadrer strictement les relations contractuelles avec ces sous-traitants* ;
- Identifier les éventuelles interconnexions de traitements ;
- Identifier les transferts de données personnelles hors de l'Union européenne ;
- Mettre en place l'information préalable des personnes concernées et, le cas échéant, le recueil de leur consentement ;
- Réaliser les formalités préalables adéquates auprès de la CNIL ;
- Gérer les demandes d'accès, de rectification, de suppression et d'opposition des personnes concernées[20].

<u>En phase opérationnelle :</u>

- Désigner un CIL (Correspondant informatique et libertés) : cela peut simplifier certaines obligations. Dans le cadre du RGPD, la fonction de CIL disparaitra. Elle sera remplacée par celle de Délégué à la Protection des Données (DPD ou DPO pour *Data protection officer*) et sera obligatoire dans certains cas ;
- Gérer les incidents de sécurité impactant les traitements, le cas échéant, notifier les violations de données personnelles
- Veiller à l'actualisation des traitements et des formalités préalables.

[20] Dans le cadre de la loi pour une République numérique, voir également la question des données post-mortem.

PROTECTION DES DONNÉES PERSONNELLES*[19]	
➢ **Conformité des traitements de données personnelles – L'essentiel**	**N° 1.1**
POUR EN SAVOIR +	
- Guide du CIL, CNIL, éd. 2011 - Recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud Computing*, CNIL - Guide Mesures pour traiter les risques sur les libertés et la vie privée, CNIL, éd. 2012 Site de la CNIL : - https://www.cnil.fr/fr/declarer-un-fichier - Transfert de données hors Union européenne - Modèles de mentions légales - Notification de violation de données personnelles	

PROTECTION DES DONNÉES PERSONNELLES	
➢ **Mon projet implique-t-il un traitement de données personnelles ?**	**N° 1.2**

CONTEXTE

Depuis la loi « informatique et libertés » de 1978, les contraintes juridiques en matière de protection des données personnelles* ne cessent de croître et de se complexifier. Dans le même temps, les sanctions encourues en cas de manquement à ces exigences se renforcent. Le RGPD, entré en vigueur le 25 mai 2016 et applicable à compter du 25 mai 2018, encourage la mise en œuvre d'une véritable gouvernance des données personnelles. À ce titre, certaines notions et procédures présentées dans cette fiche sont impactées par ce texte européen.
Ainsi, il importe d'intégrer, dès la phase projet, la gestion des données personnelles. Cela passe d'abord par l'identification de ces données, l'appréciation de leur sensibilité et l'intégration des mesures techniques nécessaires à leur sécurisation dans les processus de gestion (principe de « *Privacy by Design* »).

OBJECTIFS

La présente fiche vise à vous guider dans l'identification des données à caractère personnel et déterminer leur sensibilité.

TEXTES APPLICABLES

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Code pénal, articles 226-16 à 226-24
- Règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD, entré en vigueur le 25 mai 2016, qui entrera en application le 25 mai 2018)

RISQUES

Les principaux manquements aux obligations érigées par la loi « informatique et libertés » sont susceptibles de constituer des infractions pénales. Les peines encourues sont les suivantes : cinq ans d'emprisonnement et 1 500 000 euros d'amende pour une personne morale.

Indépendamment, la CNIL peut également, de son côté, mettre en demeure puis prononcer les sanctions administratives suivantes en cas de manquement à la loi « informatique et libertés » :

- un avertissement ;
- une sanction pécuniaire de 3 millions d'euros (depuis la loi pour une République numérique) ;
- une injonction de cesser le traitement ou un retrait d'autorisation.

Lors de l'entrée en application du RGPD, le montant maximal des sanctions sera porté à

20 millions d'euros ou 4 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu.

Les impacts, en termes d'image, peuvent également être très importants. En effet, la CNIL peut également rendre publics les avertissements, les mises en demeure et les sanctions qu'elle prononce. Ces publications sont souvent relayées par la presse, grand public ou spécialisée TIC. De plus, depuis la loi « Pour une République numérique », la CNIL peut ordonner une communication de ses décisions directement auprès des personnes concernées.

RECOMMANDATIONS

1 - Mon traitement comporte-t-il des données à caractère personnel ?

Les données traitées permettent-elles d'identifier directement ou indirectement les personnes physiques ou sont-elles relatives à des personnes physiques directement ou indirectement identifiables ?

Exemple de données personnelles : nom, prénom, numéro de sécurité sociale, numéro de badge individuel, adresse électronique individuelle, photographie, empreinte digitale, lieu de naissance, données de localisation, enregistrement vidéo, adresse IP, etc.

=> Si oui : continuer l'étude pour évaluer la sensibilité des données personnelles.

Focus : Les données sont-elles anonymisées* ?
Si oui, mon projet ne porte pas sur des données personnelles, ces données anonymisées ne permettant pas d'identifier une personne physique.
Néanmoins, il sera important de veiller, eu égard aux évolutions technologiques, aux recoupements (Big Data) et aux éventuels ajouts d'informations à venir, à ce que les données demeurent anonymes dans la durée. Il est également complexe de remplir l'ensemble des exigences, notamment celles de la CNIL et du G29, en matière d'anonymisation.
En effet, l'anonymisation doit être entendue comme étant un traitement opéré sur des données personnelles dans le but d'empêcher **irréversiblement** l'identification de la personne concernée.
L'anonymisation ne doit pas être confondue avec la pseudonymisation qui n'empêche pas toute identification d'une personne physique de manière irréversible. La pseudonymisation* consiste à remplacer la valeur d'un attribut par une autre. La personne concernée est donc susceptible d'être identifiée indirectement.

2 - Les données personnelles font-elles l'objet d'un traitement ?

Eu égard à la définition légale particulièrement large de la notion de traitement, dès lors que votre projet implique des données personnelles, alors il y a traitement de données personnelles. La Cour de cassation a précisé qu'un fichier contenant des données personnelles concernant une seule personne, stocké sur le réseau d'un organisme, devait être considéré comme un traitement (voir « Pour en savoir + »).
Exemples de traitement : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme.

PROTECTION DES DONNÉES PERSONNELLES	
➢ **Mon projet implique-t-il un traitement de données personnelles ?**	**N° 1.2**

=> Si Oui, la loi « Informatique et libertés » (LIL) pour la protection des données s'applique à mon projet.

3 - Les données personnelles relèvent-elles d'une catégorie particulière ?

3.1 Certaines données personnelles sont-elles sensibles* ?

a) Il s'agit de données énumérées à l'article 8.I de la LIL : information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle

Si oui, il faut veiller à entrer dans le cadre de l'art. 8.II de la LIL et obtenir une autorisation préalable de la CNIL. Veiller au moment de la collecte à recueillir le consentement exprès (écrit) des personnes, dans le strict cadre de la finalité du traitement. Pour les traitements du secteur public, la CNIL doit être saisie pour avis, préalablement à l'autorisation donnée par décret.

b) Il s'agit de données énumérées à l'article 25.I de la LIL.
Exemple : données génétiques, données biométriques, numéro de sécurité sociale, difficultés sociales.
Ces données impliquent un régime d'autorisation préalable de la CNIL ou bien d'autorisation unique.

c) Il s'agit des données énumérées à l'art. 9 de la LIL. Le traitement porte sur des données judiciaires* ?
Leur traitement ne peut être mis en œuvre qu'après autorisation de la CNIL, et que par :
- les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;
- les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;
- les personnes morales habilitées pour agir dans le cadre du processus HADOPI.

À savoir : avec le RGPD, les données sensibles évoluent. Elles englobent aussi les traitements de profilage à grande échelle, de surveillance des zones accessibles au public et de données concernant des mineurs.

=> Si Oui, certaines données personnelles sont sensibles.

Leur traitement est soumis à un régime particulier. Il peut notamment nécessiter le consentement préalable des personnes concernées, une autorisation préalable de la CNIL (procédure pouvant être fastidieuse et longue et ainsi retarder le projet), et des mesures de sécurité renforcées.
Sous l'égide du RGPD, un tel projet de traitement implique probablement la réalisation préalable d'une analyse d'impact sur les données personnelles.

3.2 - Aucune donnée personnelle n'est considérée comme sensible.

Le traitement est alors soumis au régime commun de protection des données personnelles.

PROTECTION DES DONNÉES PERSONNELLES	
➢ **Mon projet implique-t-il un traitement de données personnelles ?**	**N° 1.2**
Régime déclaratif de droit commun : la déclaration normale/inscription au registre tenu par le CIL, mention légale d'information, etc. Sous l'égide du RGPD, le traitement doit être inscrit dans le registre des activités de traitement.	
POUR EN SAVOIR +	
Avis du G29 4/2007 du 20 juin 2007 sur le concept de Données à caractère personnel Avis du G29 05/2014 du 10 avril 2014 sur les Techniques d'anonymisation Cass. crim. 8 septembre 2015, n° 13-85.587	

PROTECTION DES DONNÉES PERSONNELLES	
➢ **Se préparer à un contrôle de la CNIL**	**N° 1.3**

CONTEXTE

Depuis 2004, la loi « Informatique et Libertés » prévoit que la CNIL dispose d'un pouvoir de contrôle sur place dans les locaux du responsable de traitement*, qu'elle utilise très largement, ses visites se comptant par centaines chaque année. En outre, depuis 2014, la CNIL peut également procéder à des contrôles en ligne, sur des sites internet par exemple.

Par ailleurs, la CNIL a établi un protocole avec la DGCCRF dont les agents peuvent non seulement vérifier si l'entreprise est en conformité avec le droit du commerce, mais aussi si elle respecte la loi en matière de protection des données personnelles fournies par les consommateurs.

Les contrôles de la CNIL peuvent être entrepris selon plusieurs motivations : dans le cadre du programme annuel de la CNIL, à la suite de plaintes, ou en fonction de l'actualité.

C'est donc une nécessité, pour le responsable de traitement, d'être prêt à accueillir une visite d'agents de la CNIL : il ne suffit pas de faire ses meilleurs efforts pour protéger les droits des personnes par une application pertinente des dispositions de la loi ; il faut également pouvoir prouver que ces droits sont respectés, y compris dans le cas d'une visite impromptue.

L'organisme contrôlé a l'obligation de permettre le bon déroulement de la mission, mais dispose aussi de certains droits face aux pouvoirs de contrôle de la CNIL.

Au sein de l'organisme contrôlé, les investigations de la CNIL doivent être accompagnées selon une procédure stricte, afin d'éviter d'entraver l'intervention de la CNIL, ce qui pourrait constituer un délit, tout en assurant la protection des intérêts légitimes de l'organisme.

Il faut également se préparer aux suites du contrôle. Il est important de conserver une trace du déroulement du contrôle et être très vigilant sur la lettre de mission et le procès-verbal.

OBJECTIFS

La fiche explique succinctement :
- en quoi consiste le contrôle sur place de la CNIL
- comment s'organiser pour y répondre

TEXTES APPLICABLES

- Loi 78-17 du 6 janvier 1978 modifiée le 6 août 2004 relative à l'informatique, aux fichiers et aux libertés, dite « loi Informatique et Libertés »
- Décret n° 2005-1309 du 20 octobre 2005 (modifié) pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés
- Loi n° 2014-344 du 17 mars 2014 relative à la consommation, dite « Loi Hamon » (contrôles

PROTECTION DES DONNÉES PERSONNELLES	
➢ **Se préparer à un contrôle de la CNIL**	**N° 1.3**

de la DGCCRF et contrôles en ligne)

RISQUES

En cas d'anomalie constatée lors du contrôle, la CNIL peut faire des recommandations, des mises en demeure de faire cesser le manquement, voire infliger des sanctions telles que : avertissement, injonction d'arrêter le traitement, sanction pécuniaire, avec ou sans publicité dans la presse. En cas de violations graves, elle peut également dénoncer l'organisme au Procureur de la République.

Le plus souvent, le contrôle ne conduit pas directement à des sanctions : la CNIL demande d'abord à l'organisme d'apporter des compléments ou de prendre des mesures correctives, dans un délai généralement très court (quelques semaines).

Dans tous les cas, la meilleure attitude consiste à collaborer avec les agents de la CNIL, et à faire preuve de bonne volonté. Les cas de sanctions font généralement suite à des comportements négligents, voire désinvoltes, vis-à-vis de la CNIL.

RECOMMANDATIONS

Avant le contrôle

- produire un guide/une procédure de gestion des contrôles de la CNIL, le communiquer et sensibiliser le personnel intéressé (agents de l'accueil, agents de sécurité, le DG et son secrétariat, responsable juridique, etc.).

C'est le principe de responsabilité (accountability*), qui sera applicable dans le cadre du RGPD, qui oblige à identifier les documents permettant d'assurer les preuves.

- l'organisme n'est généralement pas prévenu à l'avance. Cependant, s'il y a un CIL, celui-ci est parfois prévenu, 24 ou 48 heures avant le contrôle.
- demander la lettre de mission et vérifier son périmètre et la carte professionnelle de l'agent de la CNIL.
- l'organisme dispose d'un droit d'opposition à la visite, sauf à ce que les agents disposent d'une ordonnance du juge des libertés et de la détention. Il n'est toutefois pas conseillé de faire usage de ce droit sans motif valable.
- en pratique, l'accueil des agents de la CNIL est primordial : il peut donner le ton du contrôle. D'où l'intérêt d'avoir rédigé un guide du contrôle pour informer toutes les personnes concernées.

Pendant le contrôle

- prévoir l'accompagnement des agents de la CNIL durant toute la durée du contrôle, de préférence à raison d'une personne par représentant de la CNIL, dont le CIL.
- désigner les personnes qui tiendront un compte-rendu exhaustif du déroulement des opérations.
- prévoir les conditions d'accueil : locaux, téléphone, postes de travail, imprimante, personnels techniques à la disposition de la CNIL pour les demandes de manipulation.
- la CNIL peut accéder à tous les locaux de l'organisme, et prendre copie de tout document qu'elle juge utile pour l'accomplissement de sa mission, en particulier le registre des traitements tenu par le CIL, mais aussi les dossiers d'architecture applicative, d'analyse, les schémas de bases de données, les chartes, etc.

PROTECTION DES DONNÉES PERSONNELLES	
➢ **Se préparer à un contrôle de la CNIL**	**N° 1.3**

- en fin de contrôle, la CNIL rédige et fait signer un procès-verbal : il est possible d'y inscrire des remarques avant signature.

Après le contrôle

- faire rapidement un compte-rendu interne avec les personnes qui ont participé au contrôle et prévoir les réponses qu'il faudra donner à la CNIL

Les suites du contrôle peuvent être :

- une clôture de la procédure, pouvant être accompagnée de recommandations ;
- une demande d'informations complémentaires ;
- une mise en demeure ;
- l'instruction d'une procédure de sanctions par la CNIL ;
- la dénonciation au parquet.

POUR EN SAVOIR +

- Comment se passe un contrôle de la CNIL ? - sur le site Web de la CNIL

4.2 Cyber surveillance des utilisateurs

CYBER SURVEILLANCE DES UTILISATEURS*	
➢ **La charte informatique**	**N° 2.1**

CONTEXTE

La sécurité de l'information est aujourd'hui un enjeu majeur pour tout organisme. Ce dernier, en tant que personne morale, peut voir sa responsabilité civile ou pénale engagée, du fait d'un utilisateur, suite à un incident de sécurité ou à un usage non conforme du SI* de l'organisme.

OBJECTIFS

Le document appelé en pratique « charte informatique » se réfère dans la plupart des cas à une annexe du règlement intérieur rappelant aux employés leurs droits et obligations en tant qu'utilisateurs du SI et encadrant leur usage des ressources numériques par des règles opposables aux salariés et à leur employeur.
La charte est également l'occasion de sensibiliser les utilisateurs et de les informer sur la collecte et l'utilisation de leurs données personnelles, de définir le cas échéant les usages personnels autorisés du SI et le droit à la déconnexion.
La charte participe à la démonstration de la conformité de l'organisme en matière de sécurité de l'information et de protection des données personnelles. Souvent exigée par les partenaires, clients, auditeurs, régulateurs et assureurs, la charte s'inscrit ainsi dans une démarche de responsabilité de l'organisme.
Des chartes spécifiques peuvent par ailleurs exister pour encadrer l'usage du SI par certains types d'utilisateurs : administrateurs, utilisateurs de terminaux personnels (BYOD*), etc.
La charte doit être révisée périodiquement (tous les trois ans en moyenne).
La présente fiche vise à indiquer les axes clefs concernant une charte informatique.

TEXTES APPLICABLES

- Code civil : article 9 (droit à la vie privée)
- Code du travail : articles L. 1121-1 (droits et libertés dans l'entreprise), L. 1222-3 et L. 1222-4 (information des employés), L.2323-32 (information – consultation du CE)
- Code pénal : art. 226-15 (atteinte au secret des correspondances), 226-16 à 226-24 (atteintes aux données personnelles), 323-1 à 323-8 (délits informatiques), 432-9 (atteinte au secret des correspondances, secteur public)
- Loi « informatique et libertés » : articles 32 (obligation d'information préalable des personnes concernées) et 34 (obligation de sécurité des données personnelles)
- Règlement 2016/679/UE du 27.04.2016

N. B. La liste de ces textes n'est pas exhaustive

CYBER SURVEILLANCE DES UTILISATEURS*	
➢ **La charte informatique**	**N° 2.1**

RISQUES

En l'absence de charte parfaitement adaptée à l'organisme (complète, à jour, bien formulée, compréhensible, et opposable aux utilisateurs) les risques sont :

- Mise en cause de la responsabilité civile ou pénale de l'organisme (ou de son représentant), du fait d'actes malveillants ou de négligences ;
- Manquement de l'organisme à ses obligations légales de sécurité de l'information, car il est dans l'impossibilité de démontrer la sensibilisation de ses utilisateurs et l'existence de règles de sécurité opposables à ces derniers ;
- Remise en cause de la sanction d'un comportement inapproprié, abusif ou dangereux du fait de preuves qui pourraient être considérées comme illicites (exemple : pas d'information préalable des utilisateurs du SI) ;
- Désorganisation des services, et diminution de la productivité des salariés en cas d'utilisation abusive des outils informatiques à des fins personnelles (utilisation abusive de la bande passante pour des jeux, visionnage de films, activité professionnelle tierce, voire concurrente, etc.) ;
- Refus par l'assurance, de prise en charge des réparations d'un incident résultant d'une utilisation inappropriée, abusive ou dangereuse ;
- ….

RECOMMANDATIONS

La charte doit être aussi complète que possible, compte tenu du contexte de l'organisme, et faire l'objet d'une révision régulière afin de s'adapter à l'évolution des technologies, des usages et de la jurisprudence.

Afin d'atteindre l'ensemble de ses objectifs, la charte informatique englobe généralement les axes suivants :

- Le message de la Direction
  - Contexte et enjeux de la charte, et plus globalement de la sécurité du SI
  - Objectifs et engagements de l'organisme en matière de sécurité de l'information
  - Le rôle des utilisateurs dans l'accomplissement de ces objectifs

- La sensibilisation
  - Rappeler les bonnes pratiques de sécurité aux utilisateurs

- La responsabilité
  - Fixer les règles (obligations et interdictions) d'utilisation des ressources informatiques opposables aux utilisateurs
  - Rappeler le rôle d'alerte des utilisateurs lorsqu'ils ont connaissance de faits anormaux dans le SI

CYBER SURVEILLANCE DES UTILISATEURS*	
➢ **La charte informatique**	**N° 2.1**

- Le respect de la vie privée
  - Encadrer les usages personnels du SI
  - Informer les utilisateurs des moyens de protection du SI et de surveillance mis en place

- La protection des données personnelles
  - Informer les utilisateurs des traitements des données personnelles les concernant, réalisés dans le cadre de la gestion du SI
  - Rappeler aux utilisateurs leurs obligations, en tant que personne accédant et participant à certains traitements de données personnelles.

L'opposabilité de la Charte :

Pour être applicable, la charte informatique doit être opposable à tous les utilisateurs, par exemple :

- pour les salariés, stagiaires et apprentis, par une annexion au règlement intérieur selon les procédures ad hoc ;
- pour les fonctionnaires et agents publics, par le biais d'une décision de l'autorité administrative compétente ;
- pour les équipes des prestataires intervenant sur le SI, par son annexion au contrat de prestation précisant que le prestataire s'engage à ce que les membres de ses équipes respectent les dispositions de la charte ;
- dans la majorité des autres cas, elle peut être rendue opposable par voie contractuelle (validation en ligne, remise contre signature,...)

Il est déconseillé d'annexer la charte au contrat de travail : en effet, pour toute modification substantielle du contrat de travail, l'accord du salarié est requis. On peut donc arriver dans une situation où dans une entreprise, les salariés sont tenus de respecter des versions différentes de la charte.

La charte est le pendant juridique de la politique de sécurité des SI (PSSI). Ce sont deux documents distincts qui ne doivent pas être annexés l'un à l'autre. Ils sont d'égale importance en pratique et doivent être rédigés en parfaite cohérence.

Enfin, la présentation de la charte aux utilisateurs est primordiale pour qu'elle soit acceptée et comprise. À défaut, elle est susceptible de créer un mouvement de mécontentement chez les utilisateurs et sa fonction de sensibilisation sera inefficace.

La syntaxe de la charte :

Le document doit être pédagogique et simple à la lecture. Il ne faut donc pas recourir à un jargon trop technique ou juridique. Le style doit être direct et illustré (exemples pratiques et concrets) pour faciliter la lecture. Le plan doit être concis.

Il est conseillé d'exposer les principes généraux et de renvoyer à des notes ponctuelles pour chaque grand principe. Cela permet :

- d'éviter un document trop volumineux qui dissuaderait le lecteur ;
- d'avoir un contenu technologiquement neutre et pérenne.

CYBER SURVEILLANCE DES UTILISATEURS*	
➢ **La charte informatique**	**N° 2.1**

La charte fait appel à des compétences à la fois juridiques et techniques. Il est conseillé qu'elle soit rédigée avec la coopération de la DSI, de la Direction juridique, de la Direction des ressources humaines, du RSSI et du CIL/DPO.

Le contenu de la charte :

Les sujets récurrents pour la charte informatique applicable à l'ensemble des utilisateurs, sur l'ensemble du SI sont les suivants :

Généralités

- Préambule :
  - L'objectif de la charte
  - Les objectifs de sécurité du SI

- Champ d'application de la charte : géographique, technique et humain

- Modalités d'entrée en vigueur, d'opposabilité de la charte pour les différentes populations visées

- Les principaux interlocuteurs des utilisateurs pour :
  - Les demandes de matériel, logiciel, accès
  - Les dysfonctionnements
  - Les alertes
  - Les informations relatives aux données personnelles

- Principes généraux :
  - Les obligations de sécurité du SI et des informations
  - Le devoir d'alerte
  - Les contenus prohibés

Éléments récurrents :

- Le matériel informatique
- Les comptes utilisateurs
- Les logiciels
- Les fichiers
- La messagerie électronique
- La messagerie instantanée
- Les espaces de partage
- Les périphériques de stockage
- La navigation sur l'internet
- La communication sur l'internet
- La téléphonie
- Le BYOD (usage de matériels personnels à des fins professionnelles)

CYBER SURVEILLANCE DES UTILISATEURS*	
➢ **La charte informatique**	**N° 2.1**

- Le travail à distance
- La gestion des absences et des départs

Pour la majorité de ces éléments, l'ensemble des objectifs énumérés précédemment doivent être abordés :

- Quelles bonnes pratiques faut-il rappeler aux utilisateurs ?
- Quelles règles d'utilisation faut-il imposer aux utilisateurs ?
- Existe-t-il un espace de vie privée résiduel ? Un usage personnel est-il autorisé ? Comment les définir et les encadrer ?
- L'utilisation des ressources implique-t-elle un traitement de données à caractère personnel concernant les utilisateurs ?

POUR EN SAVOIR +

Jurisprudence :

- Cass. soc. 2 octobre 2001, n°99-42942 - Le salarié a droit, même au temps et au lieu du travail, au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances. L'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance du contenu des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ce, même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.
- Cass soc. 17 mai 2005, n° 03-40017 - 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.
- Cass. soc. 18 octobre 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. 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, présumés avoir un caractère professionnel, de sorte que l'employeur peut y avoir accès hors sa présence.
- Cass. soc. 17 juin 2009, n°08-40274 - Sauf risque ou événement particulier, l'employeur ne peut ouvrir les messages 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.
  La cour d'appel qui a ordonné à l'employeur d'organiser une enquête avec les délégués du personnel sur les conditions dans lesquelles avaient été consultées et exploitées les messageries de dix-sept salariés après l'envoi de lettres anonymes à la direction et notamment de rechercher si des messages qualifiés de personnels avaient été ouverts n'a pas violé ces dispositions

CYBER SURVEILLANCE DES UTILISATEURS*	
➢ **La charte informatique**	**N° 2.1**

- Cass. soc. 30 janvier 2013, n°11-23.891 - Doit être approuvée une cour d'appel qui, ayant constaté, que la procédure de demande d'explications écrites en vigueur dans l'entreprise, avait été mise en œuvre à la suite de faits qualifiés de refus d'obéissance et que les demandes formulées par l'employeur et les réponses écrites du salarié étaient conservées dans le dossier individuel de celui-ci, a retenu que cette mesure constituait une sanction
- Cass. soc. 12 février 2013, n°11-28649 - Une clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, est présumée utilisée à des fins professionnelles. En conséquence, les dossiers et fichiers non identifiés comme personnels qu'elle contient, sont présumés avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors la présence du salarié

CYBER SURVEILLANCE DES UTILISATEURS

➢ **Traitement des données personnelles concernant les utilisateurs du SI**	**N° 2.2**

CONTEXTE

La surveillance et la protection du SI imposent de journaliser l'activité de toutes les personnes qui y ont accès.

Cette traçabilité comporte des données à caractère personnel concernant les utilisateurs, et à ce titre, elle doit s'exercer dans le respect des exigences légales et réglementaires en vigueur, notamment de la loi « informatique et libertés » (et de son évolution dans le cadre du RGPD).

OBJECTIFS

Cette fiche présente les grands principes à respecter pour traiter les données personnelles concernant les utilisateurs du SI conformément aux exigences légales et réglementaires. Les données personnelles des utilisateurs, tout comme celles des clients, bénéficient de la protection offerte par la loi « informatique et libertés ».

La fiche permettra également d'attirer l'attention sur les dispositifs de surveillance du SI qui sont encadrés par les lois et règlements en vigueur (voir annexe de cette fiche).

TEXTES APPLICABLES

- Code civil : article 9 (droit à la vie privée)
- Code du travail : articles L. 1121-1 (droits et libertés dans l'entreprise), L. 1222-3 et L. 1222-4 (information des employés), L.2323-32 (information – consultation du CE)
- Code pénal : art. 226-15 (atteinte au secret des correspondances), 226-16 à 226-24 (atteintes aux données personnelles), 323-1 à 323-8 (délits informatiques), 432-9 (atteinte au secret des correspondances, secteur public)
- Loi « informatique et libertés » : articles 32 (obligation d'information préalable des personnes concernées) et 34 (obligation de sécurité des données personnelles)
- Règlement 2016/679/UE du 27.04.2016
- N. B. La liste de ces textes n'est pas exhaustive

RISQUES

Manquements aux exigences légales relatives à la protection des données personnelles :
- Infraction pénale
- Sanction CNIL (loi de 1978, modifiée par la loi « pour une République numérique »)
- Sanction CNIL, à compter du 25 mai 2018 (RGPD) : max. 4 % du CA annuel mondial ou 20 millions d'euros
- Impact réputationnel (publication des décisions sur le site de la CNIL, dans la presse)

CYBER SURVEILLANCE DES UTILISATEURS

➢ **Traitement des données personnelles concernant les utilisateurs du SI**	**N° 2.2**

Risque social :
- délit d'entrave (défaut de consultation des représentants du personnel)
- pas de preuve recevable (licite) devant les juridictions civiles contre un utilisateur (notamment pour les contentieux aux prud'hommes)
- perception par les utilisateurs d'une atteinte à leur vie privée

Risque financier :
- coût de la mise en conformité (refonte du système, régularisation des données déjà collectées,...)

Atteinte au secret des correspondances :
- Infraction pénale

RECOMMANDATIONS

L'employeur a le droit de surveiller l'activité des utilisateurs de son SI. Cette surveillance est encadrée et doit respecter certains principes :
- Informer et consulter, préalablement, les représentants du personnel (délégué du personnel, comité d'entreprise, CHSCT), notamment pour leur présenter les moyens de surveillance envisagés, leur finalité, leur justification (intérêt légitime, obligation légale) et leur proportionnalité
- mettre en place une charte informatique opposable (voir Fiche 2.1)
- informer les utilisateurs (notamment de la finalité du dispositif)
- veiller au respect de la vie privée des utilisateurs : accorder et respecter l'espace de vie privée résiduelle (voir Fiche 2.1)
- s'assurer de la licéité/conformité légale des moyens de surveillance, notamment le respect de la loi « informatique et libertés » : formalités préalables, durée de conservation, sécurité des données, etc. (voir Fiche 1.2).

A noter toutefois l'arrêt récent (Cass. soc. 1er juin 2017, n° 15-23522) qui conclut que « l'absence de déclaration simplifiée d'un système de messagerie électronique professionnelle non pourvu d'un contrôle individuel de l'activité des salariés, qui n'est dès lors pas susceptible de porter atteinte à la vie privée ou aux libertés au sens de l'article 24 de la loi « informatique et libertés », ne rend pas illicite la production en justice des courriels adressés par l'employeur ou par le salarié dont l'auteur ne peut ignorer qu'ils sont enregistrés et conservés par le système informatique ».

POUR EN SAVOIR +

Sur le site de la CNIL :
- Guide pour les employeurs et les salariés
- Fiche « Travail et Données personnelles »

CYBER SURVEILLANCE DES UTILISATEURS	
➢ **Traitement des données personnelles concernant les utilisateurs du SI**	**N° 2.2**

Jurisprudence :

- Cass. soc. 2 octobre 2001, n°99-42942 - Le salarié a droit, même au temps et au lieu du travail, au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances. L'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance du contenu des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ce, même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.
- Cass soc. 17 mai 2005, n° 03-40017 - 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.
- Cass. soc. 18 octobre 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. 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, présumés avoir un caractère professionnel, de sorte que l'employeur peut y avoir accès hors sa presence.
- Cass. soc. 17 juin 2009, n°08-40274 - Sauf risque ou événement particulier, l'employeur ne peut ouvrir les messages 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.
  La cour d'appel qui a ordonné à l'employeur d'organiser une enquête avec les délégués du personnel sur les conditions dans lesquelles avaient été consultées et exploitées les messageries de dix-sept salariés après l'envoi de lettres anonymes à la direction et notamment de rechercher si des messages qualifiés de personnels avaient été ouverts n'a pas violé ces dispositions
- Cass. soc. 30 janvier 2013, n°11-23.891 - Doit être approuvée une cour d'appel qui, ayant constaté, que la procédure de demande d'explications écrites en vigueur dans l'entreprise, avait été mise en œuvre à la suite de faits qualifiés de refus d'obéissance et que les demandes formulées par l'employeur et les réponses écrites du salarié étaient conservées dans le dossier individuel de celui-ci, a retenu que cette mesure constituait une sanction
- Cass. soc. 12 février 2013, n°11-28649 - Une clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, est présumée utilisée à des fins professionnelles. En conséquence, les dossiers et fichiers non identifiés comme personnels qu'elle contient, sont présumés avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors la présence du salarié

ANNEXE

De nombreuses applications/outils collectent des données personnelles sur les salariés (liste non exhaustive ci-dessous) :
Surveillance protection physique :

CYBER SURVEILLANCE DES UTILISATEURS	
➢ **Traitement des données personnelles concernant les utilisateurs du SI**	**N° 2.2**

- badge contrôle d'accès bâtiment
- contrôle d'accès biométrique
- registre d'accès (exemple : visiteurs, remise d'une clé,...)
- vidéoprotection/vidéosurveillance

Surveillance des flux réseaux :

- sonde (surveillance/écoute des flux internes)
- navigation sur l'internet y compris HTTPS
- messagerie électronique
- messagerie instantanée

Surveillance des postes de travail :

- antivirus (si journalisation des anomalies avec identification de l'utilisateur)
- analyse des programmes exécutés
- analyse des périphériques USB
- gestion des sauvegardes
- gestion des comptes utilisateurs (habilitations, journaux,...)
- téléphonie (taxation, liste appels)

Surveillance des terminaux mobiles (pro ou « BYOD ») :

- géolocalisation
- sauvegarde
- contrôle et effacement à distance (container ou complet)

Surveillance des accès d'administration (y compris prestataires) :

- gestion des comptes administrateurs (individuels, traçabilité)
- journalisation de toutes les commandes (texte, vidéo)

Analyse comportementale :

- détection automatique des comportements inhabituels de l'utilisateur (type de frappe clavier, lieu de connexion, etc.)

Autres :

- bonnes pratiques d'audit (tests d'intrusion, ingénierie sociale)

4.3 La sécurité des contrats

LA SÉCURITÉ DES CONTRATS	
➢ **Comment sécuriser les contrats ?**	**N° 3.1**

CONTEXTE

La sécurité des contrats informatiques est essentielle pour assurer une relation contractuelle sereine entre les co-contractants.

De manière générale, il convient d'être vigilant, voire d'éviter, les contrats « types » souvent imposés par les prestataires informatiques, et rédigés en faveur de ces derniers. Il ne faut donc pas hésiter à suggérer des modifications dans ces contrats afin de préciser les points peu clairs et compléter toutes les informations pertinentes et utiles.

OBJECTIFS

La clarté et l'exhaustivité du contrat et de ses annexes (exemple : cahier des charges, Plan d'Assurance Sécurité, etc.) permettent de gagner en prévisibilité, en sécurité juridique, mais aussi financière, afin de maîtriser les coûts liés à l'exécution ou l'inexécution du contrat concerné.

La mise en place d'engagements de qualité de service **et de dispositifs de mesure et de contrôle mutuellement acceptés** apparaît essentielle pour la clarté des engagements de chacune des parties (engagements de qualité de service ou *Service Level Agreement - SLA*, etc.).

Enfin, si des données à caractère personnel sont confiées par l'organisme qui les traite à son co-contractant, le RGPD précédemment cité impose la présence de clauses spécifiques dans le contrat, dédiées notamment à la sécurité de ces données.

Ces clauses ont également pour objectif d'encadrer strictement les relations contractuelles avec les prestataires éventuels du co-contractant : les obligations imposées au co-contractant doivent se retrouver dans les contrats que ce co-contractant conclut lui-même avec ses propres sous-traitants.

N. B. Cette fiche ne traite pas les contrats administratifs, notamment ceux passés dans le cadre des marchés publics.

TEXTES APPLICABLES

Code Civil : articles 1101 et suivants (sous-titre premier : Le contrat)

LA SÉCURITÉ DES CONTRATS	
➢ **Comment sécuriser les contrats ?**	**N° 3.1**

RISQUES

Un contrat mal rédigé sera sujet à interprétation, tant par les parties au contrat, qui chacune tentera de faire valoir ses arguments, que par le juge qui sera éventuellement saisi du litige.

Tour d'horizon de quelques problématiques éventuelles :

Côté interprétation par les parties :

- Désaccord entre les parties sur la non-exécution ou l'exécution non-conforme de la prestation (ex. : différence d'interprétation des délais de rétablissement du service ou les méthodes d'administration) ;
- Défaut de définition des modalités de fin de contrat, notamment la réversibilité et l'effacement des données qui doit être sécurisé et irréversible.

Côté interprétation par le juge :

- Clauses abusives réputées non-écrites (article 1171 du Code civil) : ces clauses sont celles entraînant un déséquilibre significatif entre les parties. Celles-ci sont réputées non-écrites dans les contrats d'adhésion (exemple : acceptation d'une offre standard en ligne) ;
- Inexécution ou mauvaise exécution du contrat (article 1217 du Code civil) : pourrait permettre le refus d'exécution des obligations de l'autre partie ;
- Vice du consentement : la remise en cause du consentement de l'une des parties peut entraîner la nullité du contrat ;
- En présence d'indivisibilité de plusieurs contrats expressément acceptée par les parties, telle qu'entre des contrats d'édition de logiciels et de maintenance, l'annulation d'un des contrats entraîne l'annulation de l'ensemble des contrats indivisibles ;
- Un changement de circonstances imprévisibles peut permettre à l'une des parties de demander la renégociation pendant l'exécution du contrat (article 1195 du Code civil) ;
- En présence d'un contrat révélant un abus de dépendance économique aboutissant à un avantage manifestement excessif (violence économique, article 1143 du Code civil), la partie « défavorisée » peut renégocier le contrat ou obtenir son annulation devant le juge ;
- Possibilité de fixation unilatérale du prix par le juge pour les contrats-cadres et les contrats de prestation de service (nouveaux articles 1164 et 1165 du Code civil) ;
- Inexécution ou mauvaise exécution du contrat (article 1217 du Code civil) : peut entraîner, sur décision du juge :
    - Exécution forcée ;
    - Réduction du prix ;
    - Résolution/Annulation du contrat ;
    - Indemnisation.

LA SÉCURITÉ DES CONTRATS

➢ **Comment sécuriser les contrats ?**	**N° 3.1**

Attention : En cas de mauvaises rédactions ou de rédactions inadaptées, le contentieux guette et ses inconvénients sont nombreux : perte de temps, d'argent et atteinte à l'image, insécurité de la solution qui sera rendue par le juge, blocage de la relation contractuelle qui empêche souvent d'avancer sur un projet, etc.

RECOMMANDATIONS

Dès le début de la relation contractuelle ou éventuellement dès le commencement des négociations, il convient d'adopter plusieurs réflexes pour assurer la sécurité des contrats informatiques :

S'assurer que les conditions de validité des contrats sont remplies (article 1128 du Code civil).

- S'assurer de la capacité de contracter : demander l'extrait de Kbis de l'organisme et les délégations de pouvoirs et de signature ;

S'assurer que la souscription du contrat est bien conforme aux politiques internes (achats, sécurité, etc.) afin d'éviter que des utilisateurs décident de leur propre initiative de souscrire à des produits logiciels ou à des services pour l'exécution de leur travail :

- En interne, mettre en place une procédure et de la sensibilisation afin de prévenir tout risque de consumérisation de l'IT menant au « *shadow IT* » ;
- Bannir la réalisation de prestations ou d'acquisition de contenus ou de licences illicites (exemple : achat de licences « pirates », utilisation d'une base de données formée en violation avec la réglementation sur la protection des données à caractère personnel, etc.).

S'assurer de la bonne foi du co-contractant :

- Négocier et conclure le contrat de bonne foi ;
- Prêter attention à la rupture des discussions avant signature : il faut respecter la bonne foi et, le cas échéant, la rupture ne doit pas être abusive (article 1112 du Code civil) ;
- Respecter le devoir d'information qui pèse sur le co-contractant (article 1112-1 du Code civil) :
    - Il concerne toute information pouvant être nécessaire (c'est-à-dire toute « *information dont l'importance est déterminante pour le consentement de l'autre partie* ») ;
    - Mais il ne porte pas sur la valeur du contrat (prix des prestations) ;
    - En cas de manquement, cela peut entraîner la nullité du contrat.

Spécifiquement, les prestataires informatiques ont une obligation d'information renforcée, de conseil et de mise en garde prenant en compte les besoins de leurs clients.

D'une façon générale, plus l'information donnée par chacune des parties sera claire et précise, moins il y aura de risque d'insécurité juridique du contrat concerné.

LA SÉCURITÉ DES CONTRATS

➢ **Comment sécuriser les contrats ?**	**N° 3.1**

S'assurer du droit applicable et des tribunaux compétents **(les remarques précédentes ne sont formulées qu'au regard du droit français)**.

Afin de minimiser les risques de contentieux subséquents, il faut sensibiliser les métiers, la direction des achats et la DSI à ces enjeux.

- Porter un soin particulier à la rédaction du cahier des charges qui doit définir précisément les besoins de l'organisme et rappeler son environnement informatique afin que la réponse apportée par le prestataire soit compatible et adéquate (contenu du contrat) : base essentielle pour juger du devoir d'information et de conseil à la charge du prestataire ;
- S'assurer de la traçabilité des négociations (ou de l'absence de possibilité de négocier) et de l'échange d'informations en sus d'un rappel exhaustif dans le préambule du contrat ou à titre de clause contractuelle autonome ;
- Le cas échéant, exiger du prestataire qu'il soit certifié (exemple : certification ISO/CEI 27001, label ANSSI,…) ;
- Prévoir des *SLA* (engagements à des niveaux de service avec des pénalités/bonus à la clé) ;
- Vérifier les limites de responsabilité ;
- Le cas échéant, prévoir la réversibilité des données et définir les conditions de celle-ci ;
- Consulter la direction juridique ou l'avocat en charge des contrats afin de ne pas exclure les contrats informatiques de leur champ de compétence et de contrôle ;
    - Penser à leur transmettre les annexes techniques qui ont valeur contractuelle et sont nécessaires à l'analyse juridique ;
- Mettre en place des référentiels de conformité/check-list internes afin de faciliter l'identification de points juridiques sensibles et des éventuelles modifications ;
- Garder en tête que la signature d'un (« simple ») devis ou d'un bon de commande entraîne généralement l'adhésion à des conditions contractuelles opposables.

POUR EN SAVOIR +

- Le CIGREF propose sur son site, un ensemble de dossiers sur les « relations fournisseurs »
- On pourra consulter en particulier le dossier 2015 du « Club Achats » CIGREF qui propose des fiches thématiques :

• Achats de services numériques : bonnes pratiques et points d'attention
• Contrats méthodes Agiles : bonnes pratiques et points d'attention
• Typologies d'optimisation logicielle : optimisation et outillage
• Audit de licences : fiche complétée par une mise à jour de la Charte de bonnes pratiques CIGREF.

5 Glossaire

« *Accountability* » (Responsabilité)	Dans le contexte du RGPD, le principe de responsabilité (« accountability ») stipule que le responsable de traitement est responsable du respect des principes relatifs au traitement des données, et qu'il est en mesure de le démontrer (Art. 5, 2.)
Anonymisation	L'anonymisation doit être entendue comme étant un traitement opéré sur des données personnelles dans le but d'empêcher irréversiblement l'identification de la personne concernée.
BYOD	L'acronyme « BYOD » est l'abréviation de l'expression anglaise « Bring Your Own Device » (en français : « Apportez Votre Équipement personnel de Communication » ou AVEC) qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel[21].
Donnée à caractère personnel (ou Donnée personnelle)	Au sens de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (« 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.
Donnée sensible	Cette expression n'existe pas en tant que telle dans la loi Informatique et Libertés. Elle est cependant souvent utilisée pour désigner les Données à caractère personnel* visées à l'article 8 de la loi Informatique et Libertés à savoir celles 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. Le RGPD y ajoute les données génétiques, les données biométriques et les données faisant apparaitre l'orientation sexuelle des personnes.
Données judiciaires	Au sens de la loi Informatique et Libertés (art. 9), il s'agit des données personnelles relatives aux infractions, condamnations et mesure de sûreté.
Interconnexion	L'interconnexion n'est pas définie par la loi Informatique et Libertés. La Commission Nationale de l'Informatique et des Libertés (CNIL) définit l'interconnexion comme la mise en relation automatisée d'informations provenant de fichiers ou Traitements* qui étaient au préalable distincts[22].

[21] Source : CNIL, « BYOD : quelles sont les bonnes pratiques ? », 19 février 2015
[22] *Fiche pratique de la CNIL, 05 avril 2011*

Pseudonymisation	La pseudonymisation consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par des données pseudonymes, de façon à ce qu'elles ne puissent plus être attribuées à une personne précise sans avoir recours à des informations supplémentaires conservées séparément et soumises à des mesures de sécurité. Cette technique permet la ré-identification ou l'étude de corrélations en cas de besoin particulier. Comme dans le cas de l'anonymisation, il faut être vigilant dans la mesure où une ré-identification peut intervenir à partir d'informations partielles (par exemple, la combinaison des données ville et date de naissance peut être suffisante)[23].
Responsable de Traitement	Au sens de la loi Informatique et Libertés, le responsable du traitement (de Données à caractère personnel*) est la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités du Traitement* et les moyens de ce Traitement*.
Sous-traitant	Au sens de la loi Informatique et Libertés, un sous-traitant est toute personne traitant des Données à caractère personnel* pour le compte du Responsable du Traitement*.
SI (Système d'information)	Cette notion recouvre : ● L'ensemble des matériels informatiques et téléphoniques, physiques ou virtuels, incluant notamment : postes de travail fixes et portables, serveurs, imprimantes, scanners, téléphones fixes et mobiles, fax, tablettes ; ● Les outils et logiciels permettant la création, la modification, l'échange, la diffusion, la reproduction, le stockage et la suppression des informations ; ● Les informations (écrits, images, sons et vidéos).
Traitement (de Données à caractère personnel*)	Au sens de la loi « informatique et libertés », un traitement de Données à caractère personnel* est 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. Remarque : même si avec la numérisation de la vie quotidienne, la plupart des activités de traitement sont liées à de l'informatique, un ensemble de fiches papier, classées par ordre alphabétique constitue également un traitement.
Utilisateurs	Pour un organisme, toute personne autorisée à accéder au SI de cet organisme. Sont notamment considérés comme utilisateurs les employés, les prestataires et les visiteurs.

[23] Le groupe de l'Article 29 qui regroupe les autorités de protection des données européennes, a publié un avis sur les principales techniques d'anonymisation, afin d'expliquer comment les mettre en œuvre (Avis 05/2014 sur les Techniques d'anonymisation).

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr

CYBERLEX

4 avenue HOCHE – 75008 Paris
Tél. : +33 1 43 18 16 50
cyberlex@cyberlex.org – www.cyberlex.org