

RETROSPECTIVE 2017

L'ACTUALITÉ ET LA PRATIQUE EN DROIT DES AFFAIRES

Droit des nouvelles technologies

Droit de la concurrence

Droit de la distribution / Franchise



SOMMAIRE

TITRE I: LÉGISLATION ET TEXTES JURIDIQUES

1/ Les principales lois adoptées en 2017

2/ Les principaux décrets en 2017

3/ Les principaux arrêtés du ministre des finances en 2017

4/ Les principales circulaires de la Banque Centrale de Tunisie en 2017

TITRE II: ETUDES JURIDIQUES

1/ Droit des nouvelles technologies

« 1.1 / "La reine des cryptomonnaies" » le Bitcoin

1.2 / Le big data l'enjeux de la décennie

1.3 / Le Contrat cloud computing : fiche pratique

2/ Droit de la concurrence / Droit de la distribution / Franchise

2.1/ Le cadre juridique et réglementaire de la franchise

2.2/ Les tendances du conseil de la concurrence année 2015, 2016, 2017

TITRE III: JURISPRUDENCE : L'approche du Conseil de la concurrence en matière de prix excessivement bas (année 2017)

Titre I : LÉGISLATION ET TEXTES JURIDIQUES

1/ Les principales lois adoptées en 2017

- [Loi organique n° 2017-7 du 14 février 2017, modifiant et complétant la loi organique n° 2014-16 du 26 mai 2014 relative aux élections et référendums.](#)
- Loi n° 2017-8 du 14 février 2017, portant refonte du dispositif des avantages fiscaux.
- [Loi organique n° 2017-19 du 18 avril 2017, modifiant et complétant la loi organique n° 2016-34 du 28 avril 2016, relative au conseil supérieur de la magistrature.](#)
- Loi n° 2017-28 du 25 avril 2017, portant approbation du plan de développement (2016-2020) .
- Loi n° 2017-39 du 8 mai 2017, portant modification de la loi n° 92-52 du 18 mai 1992, relative aux stupéfiants.
- Loi n° 2017-41 du 30 mai 2017, modifiant certaines dispositions du code des hydrocarbures.
- [Loi organique n° 2017-45 du 7 juin 2017, modifiant et complétant la loi n° 75-40 du 14 mai 1975, relative aux passeports et documents de voyage.](#)
- [Loi n° 2017-47 du 15 juin 2017, modifiant la loi n° 2004-71 du 2 août 2004, relative à l'institution d'un régime d'assurance maladie.](#)
- Loi n° 2017-48 du 15 juin 2017, modifiant la loi n° 2013-47 du 1er novembre 2013, relative aux dispositions dérogatoires concernant les procédures de changement de vocation des terres agricoles, de déclassement des terrains relevant du domaine forestier de l'Etat et de l'aménagement et de l'urbanisation des terrains, situés à l'extérieur des zones couvertes par des plans d'aménagement et affectés pour l'exécution du programme spécifique pour le logement social et à la création des zones industrielles et la poursuite de l'application des procédures dérogatoires qu'elle comporte
- [Loi n° 2017-51 du 28 juin 2017, portant dispositions dérogatoires de mise à la retraite avant l'âge légal dans la fonction publique.](#)
- [Loi n° 2017-52 du 4 juillet 2017, relative à la modification des dispositions de la loi n° 95-21 du 13 février 1995, relative aux immeubles domaniaux agricoles.](#)
- [Loi organique n° 2017-62 du 24 octobre 2017, relative à la réconciliation dans le domaine administratif.](#)

2 / Les principaux décrets de 2017

- Décret n°2017-268 du 1^{er} février 2017 relatif à la fixation des règles d'intervention, d'organisation et de fonctionnement du fonds de garantie des dépôts bancaires et des conditions d'adhésion et d'indemnisation des déposants.
- [Les Décrets n°2017-388, n°2017-389, n°2017-390 du 9 mars 2017,](#) pris en application de la loi sur l'investissement.

3 /Les principales circulaires de 2017

- Circulaire aux banques n°2017-02 du 10 mars 2017 relative à la mise en œuvre de la politique monétaire de la Banque Centrale de Tunisie
- Circulaire aux banques et aux établissements financiers n°2017-06 du 31 juillet 2017 relative au reporting comptable, prudentiel et statistique à la Banque Centrale de Tunisie
- Circulaire aux banques et aux établissements de crédit n°2017-08 du 19 septembre 2017 relative aux règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme.



1/ Droit des nouvelles technologies

L'innovation financière conjuguée avec les progrès technologiques vont bouleverser d'ici quelques années tout le paysage financier et économique dans le monde.

Les cryptomonnaies, les protocoles blockchain et les ICO (Initial Coin Offering) sont désormais considérés comme une nouvelle forme de la finance.

Qu'est ce qu'une ICO ?

Il s'agit d'un processus de levée de fonds utilisant des tokens comme actifs émis par une société, et des cryptomonnaies comme valeur d'échange pour acheter ces tokens. Le principe emprunte au fonctionnement d'une introduction en Bourse. Originellement, une ICO est une opération réalisée par une société travaillant dans l'orbite de la blockchain permettant de financer, le plus généralement, la recherche et le développement dans les protocoles de blockchain ou dans les usages de ces protocoles, mais aussi parfois pour lancer un fonds d'investissement non régulé. Le concept doit être reconnu pertinent par la communauté blockchain pour que l'ICO soit un succès.

L'entreprise va alors émettre des jetons, représentant le plus souvent un droit sur des revenus futurs liés au développement de son projet. La valeur initiale de ce jeton est calculée en fonction de l'espérance de revenus attendus. Si le projet se révèle être un succès, le jeton prend alors de la valeur sur le marché secondaire, où il peut s'échanger sur des places de marchés.

Qu'est ce qu'une cryptomonnaie ?

Au sens économique du terme, une cryptomonnaie est un mode de paiement. Il s'agit d'un logiciel p2p ou un programme construit à partir d'une source de code unique ou cloné à partir d'une autre source de code, comme litecoin, peercoin, ou bien sûr bitcoin. Elle est « émise » dans le cadre d'une blockchain, généralement en rémunération d'un travail (le minage)

Qu'est ce qu'un jeton "token" ?

Un token répond à de larges fonctionnalités, pouvant aller jusqu'à conférer des droits sur des revenus, voire sur la gouvernance d'un projet. En effet, il représente un actif sous-jacent, qu'il s'agisse d'un droit sur des biens sous-jacents, des revenus futurs ou d'échange contre services.

Ainsi, la différence majeure entre une cryptomonnaie et un jeton tient à leur structure : les premières sont des modes (ou monnaies) d'échange liés à leur propre protocole blockchain, alors que les jetons ne sont pas liés à un protocole blockchain spécifique mais à chaque entreprise émettrice.

Qu'est ce qu'une blockchain ?

La blockchain est une technologie qui permet de stocker et transmettre des informations de manière transparente, sécurisée et sans organe central de contrôle.

Elle repose sur une architecture décentralisée, c'est-à-dire qu'elle n'est pas hébergée par un serveur unique mais par une partie des utilisateurs. Il n'y a aucun intermédiaire pour que chacun puisse vérifier lui-même la validité de la chaîne. Les informations contenues dans les blocs (transactions, titres de propriétés, contrats...) sont protégées par des procédés cryptographiques qui empêchent les utilisateurs de les modifier a posteriori.

La blockchain peut être utilisée de trois façons : pour du transfert d'actifs (monnaie, titres, actions...), pour une meilleure traçabilité d'actifs et produits et pour exécuter automatiquement des contrats (des "smart contracts").



1-1/ "La reine des cryptomonnaies", le Bitcoin

"How to buy a bitcoin?" telle était la question de l'année en 2017. A l'heure actuelle, le bitcoin est la plus connue et la plus utilisée des nombreuses crypto-monnaies en circulation¹

En effet, Avant l'apparition du bitcoin, de nombreuses monnaies précurseurs ont existé, par exemple, les technologies développées par David Chaum et Stefan Brands (ecash), Adam Back (hashcash), Wei Dai (b-money), Nick Szabo (bit-gold)². Aucune n'a eu le succès du bitcoin.

Créé en 2009 par Satoshi Nakamoto³, le bitcoin⁴ est une unité de compte virtuelle stockée sur un support électronique permettant à une communauté d'utilisateurs d'échanger entre eux des biens et des services sans avoir à recourir à la monnaie légale.

Ainsi, dans sa conception, le bitcoin est une unité de compte créée, en nombre limité, selon un algorithme, et stocké au sein d'un « coffre-fort » électronique sur l'ordinateur.

Le bitcoin a été créé pour remplir les trois fonctions traditionnelles de la monnaie : (i) il représente une unité de compte⁵ ; (ii) il facilite les transactions commerciales et (iii) il permet de stocker une valeur pouvant être utilisée dans le futur⁶.

Permettant de s'affranchir des aléas des monnaies étatiques, le bitcoin comporte des avantages certains, mais il présente également des dangers relatifs principalement aux risques de spéculation et de blanchiment.

Mais est-ce une monnaie ? Un instrument de paiement ? Un instrument financier ? Un bien ? Quels dangers du bitcoin ? faut-il le réglementer ?

Le bitcoin a suscité ainsi un certain nombre d'interrogations qu'il est possible de synthétiser autour de trois axes : Quels sont les principes techniques sur lesquels reposent le bitcoin ? (I), Quels sont les dangers du bitcoin (II) et qu'elle est la qualification juridique du bitcoin ? (III).



a. Les principes techniques du bitcoin

Les principaux principes du processus d'émission et des transactions en bitcoins sont les suivantes⁷ :

-La quantité de monnaie créée par le système est limitée par le programme à 21 millions de bitcoins, limite qui pourrait être atteinte aux alentours des années 2140

- Le rythme de création des bitcoins est régulé et fluctue pour tenir compte du nombre de mineurs (miners) et de l'évolution de la capacité de calcul des unités informatiques connectées. En effet, le bitcoin est créée au sein d'une communauté d'internautes qu'on appelle « mineurs », qui ont installé sur leurs unités informatiques connectées à internet un logiciel libre. Celui-ci va créer, selon un algorithme, les unités de compte bitcoin qui seront ensuite allouées à chaque mineur en récompense de sa participation au fonctionnement du système. Une fois créés, les bitcoins sont stockés au sein d'un « coffre-fort » électronique sur l'ordinateur, la tablette ou le portable de l'utilisateur. Il est ensuite possible de les transférer via internet, en tout anonymat, entre les membres de la communauté.

-Le transfert s'opère en dehors du circuit de paiement traditionnel. Des plates-formes internet proposent, sans aucune garantie de prix ni de liquidité, l'achat/vente de bitcoins contre des devises ayant cours légal.

¹ SYLVAIN MIGNOT, Le bitcoin : nature et fonctionnement, Banque & Droit n° 159 janvier-février 2015

² Id

³ En 2008, un certain Satoshi Nakamoto publia un article de recherche dans une mailing list concernant la cryptographie, dont le titre était : Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto, 2008). Il faut noter que ce Satoshi Nakamoto n'était connu d'aucun des utilisateurs de cette liste de diffusion. De fait, il a rapidement été établi qu'il n'existe pas en tant que personne, ce nom n'étant rien d'autre qu'un pseudonyme. Il pourrait être le pseudonyme utilisé par une personne ou une équipe de programmeurs.

⁴ C'est un terme anglais composé de « bit » : unité d'information binaire et de « coin » : pièce de monnaie

⁵ Une unité standardisée qui permet de mesurer la valeur des flux et des stocks de biens, des services ou d'actifs

⁶ V. Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », Focus n° 10, 5 déc. 2013

⁷ SYLVAIN MIGNOT, Le bitcoin : nature et fonctionnement, Banque & Droit n° 159 janvier-février 2015

b. Les dangers du bitcoin

L'anonymat est l'un des principaux dangers liés au développement du bitcoin. Le bitcoin favorise ainsi le contournement des règles relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

L'anonymat des transferts de bitcoin constitue donc un risque d'utilisation de cette monnaie virtuelle à des fins criminelles ou plus précisément à des fins de blanchiment ou de financement du terrorisme⁸.

Au niveau international, le Groupe d'action financière (GAFI) a adopté et publié à la suite de sa réunion des 19 et 21 juin 2013 des lignes directrices relatives aux nouvelles méthodes de paiement qui mentionnent également les risques de lutte contre le blanchiment des capitaux et le financement du terrorisme, liés aux monnaies virtuelles échangeables ou remboursables.

La spéculation est un autre danger que présente également le bitcoin. Dans ce sens, on a considéré que : « Même si le bitcoin ne remplit pas à ce jour les conditions pour devenir un support d'investissement crédible et poser ainsi un risque significatif pour la stabilité financière, il représente un risque financier certain pour les acteurs qui le détiennent. En raison de la progression limitée et déterminée du nombre de bitcoins en circulation, le bitcoin peut constituer un support spéculatif. En outre, il peut apparaître à certains investisseurs comme une valeur « refuge », comme lors de la crise chypriote »⁹.

D'autres dangers et risques du bitcoin peuvent être soulignés :

- Aucune autorité ne veille à la mise en place des conditions nécessaires pour assurer la sécurité des « coffres-forts » électroniques qui permettent le stockage des bitcoins. En cas de vol de leurs bitcoins, les détenteurs n'ont aucun recours contre les pirates informatiques (hackers) ;
- La convertibilité des bitcoins dans différentes monnaies ayant cours légal, nécessaire pour tirer les bénéfices d'une spéculation, n'est également garantie par aucun organisme centralisé. Les investisseurs ne peuvent récupérer leurs fonds en devises que si d'autres utilisateurs désirent acquérir des bitcoins. Ainsi, le système peut à tout moment s'effondrer lorsque les investisseurs veulent dénouer leurs positions mais se retrouvent détenteurs de portefeuilles devenus illiquides¹⁰.

En conclusion, les risques du bitcoin ont été exposés comme suit¹¹ :

- Un commerçant ne pourra pas accepter de manière significative les paiements en bitcoins sans s'exposer à des risques substantiels.
- Risque de liquidité, lié à la faible profondeur du « marché des changes » des bitcoins,
- Risque financier lié à la volatilité du cours du bitcoin,
- Risque opérationnel lié notamment à l'absence de sécurité des « coffres-forts » permettant le stockage des unités de bitcoins et de garantie financière en cas de fraude.

c. La qualification juridique du bitcoin

L'analyse juridique du bitcoin n'est pas aisée. En effet, le bitcoin n'entre dans aucune définition juridique préexistante. Ainsi, si le bitcoin n'est pas une monnaie, il peut toutefois être envisagé à la fois comme bien et comme objet de transactions¹².

Mais comment peut-on justifier que le bitcoin n'est pas une monnaie ?

Le bitcoin ne possède pas de pouvoir libératoire universel comme la monnaie

Au sens juridique du terme, une monnaie est un bien particulier, émis par l'État et dont la valeur est garantie par l'État. La monnaie se singularise, par son pouvoir libératoire universel: le débiteur se trouve libéré de sa dette de sommes d'argent une fois qu'il a remis à son créancier la quantité d'unité de monnaie (ayant cours légal à l'endroit où il se situe) qu'il lui doit; ce dernier est réputé satisfait, dès qu'il est entré en possession de la due quantité de monnaie, et sa créance se trouve alors automatiquement éteinte¹³.

Le pouvoir libératoire de monnaie est dit « universel », car il n'y a pas besoin d'un accord du créancier pour que la remise des unités monétaires libère le débiteur à son égard. L'effet libératoire se produit de plein droit, compte tenu du pouvoir attaché à la monnaie par la loi

Le bitcoin ne possède pas de pouvoir libératoire universel. Le débiteur d'une somme d'argent qui veut payer sa dette en bitcoins doit avoir obtenu l'accord de son créancier d'être réglé de la sorte, pour être juridiquement considéré comme libéré¹⁴.

Le bitcoin n'exige pas la remise de fonds comme la monnaie électronique

Juridiquement, la monnaie électronique constitue une créance sur son émetteur et offre à son détenteur un droit au remboursement (garanti) opposable à celui-ci¹⁵.

En fait, la monnaie électronique est émise contre la remise de fonds et les unités de monnaie électroniques alors créées ont une contre-valeur égale à la somme remise lors de leur émission.

Le bitcoin est émis à l'issue d'une programmation informatique qui n'est nullement conditionnée par une remise de fonds. De sorte que, le bitcoin se présente plutôt comme un mode de paiement conventionnel, qui dépend de l'unique volonté des parties de l'accepter comme tel¹⁶.



⁸ V.Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », Focus n° 10, 5 déc. 2013.

⁹ Id.

¹⁰ Id.

¹¹ Id.

¹² M. Roussille, Le bitcoin : objet juridique non identifié, Banque & Droit n° 159 janvier-février 2015

¹³ Id.

¹⁴ Id.

¹⁵ Id.

¹⁶ Id.

1-2 / Le Big data, l'enjeu de la décennie

Les « big data » se présentent comme des ensembles de données numériques gigantesques détenus par les sociétés ou les Gouvernements ou n'importe quelle autre grande organisation. Ces données sont ensuite analysées en profondeur, grâce à des algorithmes informatiques.

Il s'agit alors de différentes catégories de données hétérogènes qui regroupent à la fois des données structurées et non structurées.

Le Big Data se définit donc comme une méga base de données qui ne cesse de se développer avec le temps. En effet, les hommes interconnectés interagissent et génèrent des traces numériques qui sont captées, croisées et interprétées instantanément, en temps réel. Ces données sont ainsi le carburant de l'économie numérique, le pétrole de l'internet, l'or noir des big data¹⁷.

Comme il faut bien stocker les big data pour les analyser, on utilisera de grands data centers ou encore des centres de traitement de données. Ces centres seront, sans doute, souvent externalisés dans des clouds.

En somme, on peut identifier un Big Data dès lors que l'on est en présence :

- d'un grand Volume de données (généralement plus de 100 téraoctets),
- d'une Variété de données (c'est-à-dire de différents formats de données)
- d'un flux continu de données (on parle alors de Vitesse des

données ou encore de Vélocité).

- Ajoutons deux autres V, un pour Valeur (qualification des données) et un pour Validité (conformité des données)

L'intérêt pratique des big data tient, en effet, à leurs nombreuses applications potentielles : analyse financière, connaissance du client, identification de tendances à long terme, mais également et spécialement ses capacités prédictives.

Certes, la capacité prédictive des Big data est un atout majeur mais elle constitue également une source de dangers et de risques :

A cet égard, les exemples ne manquent pas : Google Maps sait où on est parti en vacances. Google traite, les requêtes des internautes et dresse une infographie. Si Google sait ce qu'on a fait cet été, il pourrait aussi bien connaître les idées politiques, les convictions religieuses, déterminer le nombre de femmes enceintes ou le nombre d'homosexuels qui vivent dans le pays. L'on pourrait imaginer aussi des applications politiques ou militaires. Il existe en outre d'importants risques de détournement de fichiers et d'interconnexion de données¹⁸.

Dans quelle mesure alors, l'encadrement des big data permet de minimiser sinon de limiter ces risques ?

Certes, la protection des données personnelles est une limite majeure aux risques des big data (I), mais il ne faut pas perdre de vue que les big data peuvent également avoir un côté obscur que représente la cybercriminalité (II).

a. Le défi des big data : la protection des données personnelles¹⁹

La protection des données personnelles est un droit fondamental. En effet, en vertu de l'article 24 de la constitution tunisienne de 2014 : « L'État protège la vie privée, l'inviolabilité du domicile et le secret des correspondances, des communications et des données personnelles ».

Dans ce sens, l'article premier de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel (ci-après loi 2004) : «- Toute personne a le droit à la protection des données à caractère personnel relatives à sa vie privée comme étant l'un des droits fondamentaux garantis par la constitution et ne peuvent être traitées que dans le cadre de la transparence, la loyauté et le respect de la dignité humaine et conformément aux dispositions de la présente loi. »

De plus, l'article 9 de la même loi dispose que : «Le traitement des données à caractère personnel doit se faire dans le cadre du respect de la dignité humaine, de la vie privée et des libertés publiques. Le traitement des données à caractère personnel, quelle que soit son origine ou sa forme, ne doit pas porter atteinte aux droits des personnes protégés par les lois et les règlements en vigueur, et il est, dans tous les cas, interdit d'utiliser ces données pour porter atteinte aux personnes ou à leur réputation.»

Reste à savoir qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information qui permet d'identifier ou de rendre identifiable une personne.

C'est ainsi que l'article 4 de la loi 2004 définit les données à caractère personnel comme suit : « Au sens de la présente loi, on entend par données à caractère personnel toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne physique ou la rendent identifiable, à l'exception des informations liées à la vie publique ou considérées comme telles par la loi ».

Selon cette définition, les données à caractère personnel ne peuvent donc se rapporter qu'aux personnes physiques ; sont donc exclues, du champ d'application de ces données, les données relatives aux personnes morales.

Dans ces conditions, même si le champ d'application de la notion de « big data » se recoupe avec celui de données à caractère personnel, ce premier est beaucoup plus étendu, en intégrant aussi bien des données à caractère personnel que des données relatives à des personnes morales.



¹⁷ Les big data — littéralement « grosses données ».

¹⁸ Les exemples des risques que présentent les big data sont nombreux et concernent l'internet des objets IOT, les données sur le terrorisme, les données sur les consommateurs, les données sur le marché, les données de santé¹⁹ Id.

¹⁹ Revue Lamy Droit de l'Immatériel, N° 97, 3608 - Enjeux stratégiques et financiers de collecte des données, 1^{er} octobre 2013 21 M. Roussille, Le bitcoin : objet juridique non identifié, Banque & Droit n° 159 janvier-février 2015

De plus, une donnée qui peut au départ être anodine, n'ayant pas de caractère personnel, parce qu'elle se rapporte à une personne totalement anonyme, qui ne peut être ni identifiée, ni identifiable, peut vite se transformer en donnée à caractère personnel, et ce grâce aux recoupements, aux traitements personnalisés et subjectifs effectués par le biais d'algorithmes informatiques sophistiqués sur lesquels reposent les données massives.

La notion de « big data » dépasse celle de données à caractère personnel, ces deux notions tendent à se croiser, mais ne se confondent pas totalement²⁰.

Il importe alors de déterminer l'encadrement des big data s'ils portent sur des données à caractère personnel.

Tout traitement²¹ des données à caractère personnel a un but, C'est le pourquoi du traitement ou encore sa finalité.

Cette finalité doit être légale, déclarée, loyale et respectueuse de la dignité humaine. En effet, aux termes de l'article 10 de la loi 2004 : « La collecte des données à caractère personnel ne peut être effectuée que pour des finalités licites, déterminées et explicites. »

Dans la même optique l'article 11 de la loi 2004 dispose que : « Les données à caractère personnel doivent être traitées loyalement, et dans la limite nécessaire au regard des finalités pour lesquelles elles ont été collectées. Le responsable du traitement doit également s'assurer que ces données sont exactes, précises et mises à jour. »

En outre, le traitement des données à caractère personnel ne peut être effectué pour des finalités autres que celles pour lesquelles elles ont été collectées sauf dans les cas suivants²² :

- si la personne concernée a donné son consentement.
- si le traitement est nécessaire à la sauvegarde d'un intérêt vital de la personne concernée
- si le traitement mis en œuvre est nécessaire à des fins scientifiques certaines.

Donc, les données sont collectées pour des finalités déterminées, explicites et légitimes. Ces données ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités initiales.

Vérifier si la notion « big data » respecte le principe de finalité permet de délimiter l'utilisation des données personnelles collectées pour une finalité déterminée au préalable, et ce principalement afin de protéger les intérêts de la personne concernée. Par ailleurs, en acceptant les utilisations ultérieures pour des finalités compatibles, on permet au responsable de traitement une certaine flexibilité et une souplesse nécessaires au cours du processus de traitement.

Il n'en demeure pas moins qu'aucun traitement n'est possible sans le consentement de la personne concernée. De sorte que la personne permet le traitement de ses données personnelles à travers un consentement éclairé, donné sur la base d'une connaissance de l'opération de traitement²³.

En outre, ce consentement doit être donné de manière explicite et peut être réversible²⁴.

L'importance de ce dispositif est qu'il est sanctionné pénalement par l'emprisonnement et l'amende.

Ainsi, aux termes de l'article 87 de la loi 2004 : « Est puni d'un emprisonnement de deux ans et d'une amende de dix mille dinars, celui qui viole les dispositions de l'article 13 ainsi que le paragraphe premier de l'article 14, le paragraphe premier de l'article 28, le paragraphe premier de l'article 63 et les articles 70 et 71 de la présente loi. Est puni également des mêmes peines prévues au paragraphe précédent, celui qui viole les dispositions du paragraphe premier de l'article 27 ainsi que les articles 31, 44 et 68 de la présente loi. »

Dans le cadre de traitement des données à caractère personnel, la loi 2004 assure également un droit d'accès, un droit de mise à jour des données, un droit à l'oubli et un droit de sécurisation des données



²⁰ La notion de « big data » est étroitement liée également aux données de sources publiques qui sont régies par des principes différents de ceux qui régissent les données à caractère personnel.

Les données de sources publiques sont « open data » (l'open data désigne le mouvement visant à rendre accessible à tous via le web les données publiques non nominatives, ne relevant ni de la vie privée ni de la sécurité, collectées par les organismes publics.), elles sont disponibles, accessibles et même réutilisables.

²¹ Selon l'article 6 de la loi 2004 : « Au sens de la présente loi, on entend par :

- traitement des données à caractère personnel : les opérations réalisées d'une façon automatisée ou manuelle par une personne physique ou morale, et qui ont pour but notamment la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation, l'utilisation, l'expédition, la distribution, la diffusion ou la destruction ou la consultation des données à caractère personnel, ainsi que toutes les opérations relatives à l'exploitation de bases des données, des index, des répertoires, des fichiers, ou l'interconnexion.

- le responsable du traitement : toute personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel.

- tiers : toute personne physique ou morale ou l'autorité publique ainsi que leurs subordonnés, à l'exception de la personne concernée, le bénéficiaire, le responsable du traitement, le sous-traitant ainsi que leurs subordonnés.

- sous-traitant : toute personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement. »

²² Article 12 de la loi 2004

²³ Art. 31 de la loi 2004 - Après l'expiration du délai fixé par l'article 7 de la présente loi pour l'opposition de l'Instance, il faut informer au préalable et par n'importe quel moyen laissant une trace écrite les personnes concernées par la collecte des données à caractère personnel de ce qui suit :

- la nature des données à caractère personnel concernées par le traitement ;
- les finalités du traitement des données à caractère personnel ;
- le caractère obligatoire ou facultatif de leur réponse ;
- les conséquences du défaut de réponse ;
- le nom de la personne physique ou morale bénéficiaire des données, ou de celui qui dispose du droit d'accès et son domicile ;
- le nom et prénom du responsable du traitement ou sa dénomination sociale et, le cas échéant, son représentant et son domicile ;
- leur droit d'accès aux données les concernant ;
- leur droit de revenir, à tout moment, sur l'acceptation du traitement ;
- leur droit de s'opposer au traitement de leurs données à caractère personnel ;
- la durée de conservation des données à caractère personnel ;
- une description sommaire des mesures mises en œuvre pour garantir la sécurité des données à caractère personnel .
- le pays vers lequel le responsable du traitement entend, le cas échéant, transférer les données à caractère personnel .

La notification s'effectue par lettre recommandée avec accusé de réception ou par n'importe quel moyen laissant une trace écrite dans un délai d'un mois au moins avant la date fixée pour le traitement des données à caractère personnel.

²⁴ Art. 27 de la loi 2004

- **Le droit d'accès**

Toute personne qui donne ses données personnelles ne s'en dessaisit pas, elle peut revendiquer à n'importe quel moment le droit d'y accéder .

Dans ce sens, l'article 32 dispose: « Au sens de la présente loi, on entend par droit d'accès, le droit de la personne concernée, de ses héritiers ou de son tuteur de consulter toutes les données à caractère personnel la concernant, ainsi que le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer lorsqu'elles s'avèrent inexactes, équivoques, ou que leur traitement est interdit. Le droit d'accès couvre également le droit d'obtenir une copie des données dans une langue claire et conforme au contenu des enregistrements, et sous une forme intelligible lorsqu'elles sont traitées à l'aide de procédés automatisés ».

- **Le droit à la mise à jour des données**

Les données personnelles servent de base à la prise de décision concernant les personnes concernées Le responsable du traitement est tenu de mettre à jour continuellement ces données et les effacer si elles s'avèrent inexactes.

A cet égard, l'article 21 précise « Le responsable du traitement et le sous-traitant doivent corriger, compléter, modifier ou mettre à jour les fichiers dont ils disposent, et effacer les données à caractère personnel de ces fichiers s'ils ont eu connaissance de l'inexactitude ou de l'insuffisance de ces données ».

- **Le droit à l'oubli**

C'est le droit pour le citoyen de voir ses données personnelles gardées pour un temps limité, celui nécessaire pour atteindre la finalité à la base de leur collecte. C'est ainsi que l'article 45 de la loi 2004 impose que : «- Les données à caractère personnel doivent être détruites dès l'expiration du délai fixé à sa conservation dans la déclaration ou l'autorisation ou les lois spécifiques ou en cas de réalisation des finalités pour lesquelles elles ont été collectées ou lorsqu'elles deviennent inutiles pour l'activité du responsable du traitement. Il est établi un procès-verbal par huissier de justice et en présence d'un expert désigné par l'Instance. Les honoraires de l'expert fixés par la l'Instance et les frais de l'huissier de justice sont à la charge du responsable du traitement. »

- **Le droit d'opposition**

Selon l'article 42 de la loi 2004: la personne concernée, ses héritiers ou son tuteur, a le droit de s'opposer à tout moment au traitement des données à caractère personnel le concernant pour des raisons valables, légitimes et sérieuses, sauf dans les cas où le traitement est prévu par la loi ou est exigé par la nature de l'obligation. En outre, la personne concernée, ses héritiers ou son tuteur, a le droit de s'opposer à ce que les données à caractère personnel la concernant soient communiquées aux tiers en vue de les exploiter à des fins publicitaires. L'opposition suspend immédiatement le traitement ».

Il ressort de cet article que la personne concernée, ses héritiers ou son tuteur a le droit de s'opposer au traitement de ses données personnelles . Cette opposition peut intervenir à n'importe quel moment mais elle doit se baser sur des raisons valables, sérieuses et légitimes. C'est ainsi qu'on ne peut s'y opposer si le traitement est prévu par la loi.

- **Le droit à la sécurisation des données**

Les données personnelles sont « confiées » à la personne responsable du traitement qui doit prendre toutes les mesures nécessaires pour assurer la sécurisation.

A cet effet, l'article 18 de la loi 2004 précise que « Toute personne qui effectue, personnellement ou par une tierce personne, le traitement des données à caractère personnel est tenue à l'égard des personnes concernées de prendre toutes les précautions nécessaires pour assurer la sécurité de ces données et empêcher les tiers de procéder à leur modification, à leur altération ou à leur consultation sans l'autorisation de la personne concernée. ».

L'importance de ce dispositif de protection est assurée par des sanctions pénales. Dans ce sens l'article 94 de la loi 2004 punit « de trois mois d'emprisonnement et d'une amende de mille dinars quiconque viole les dispositions des articles 12, 18, et 19, ainsi que les paragraphes premier et deuxième de l'article 20, et les articles 21, 37, 45, 64 et 74 de la présente loi. »

Il y'a également d'autres limites au transfert et à la communication des données. Les données sont fournies au responsable, il ne peut les communiquer et les transférer sans consentement²⁵.



²⁵ Article 47. Loi 2004 «Il est interdit de communiquer des données à caractère personnel aux tiers sans le consentement exprès donné par n'importe quel moyen laissant une trace écrite, de la personne concernée, de ses héritiers ou de son tuteur sauf si ces données sont nécessaires à l'exercice des missions confiées aux autorités publiques dans le cadre de la sécurité publique ou de la défense nationale, ou s'avèrent nécessaires à la mise en œuvre des poursuites pénales ou à l'exécution des missions dont elles sont investies conformément aux lois et règlements en vigueur.

L'Instance peut autoriser la communication des données à caractère personnel en cas du refus, écrit et explicite, de la personne concernée, de ses héritiers ou de son tuteur lorsqu'une telle communication s'avère nécessaire pour la réalisation de leurs intérêts vitaux, ou pour l'accomplissement des recherches et études historiques ou scientifiques, ou encore en vue de l'exécution d'un contrat auquel la personne concernée est partie, et ce, à condition que

la personne à qui les données à caractère personnel sont communiquées s'engage à mettre en œuvre toutes les garanties nécessaires à la protection des données et des droits qui s'y rattachent conformément aux directives de l'Instance, et d'assurer qu'elles ne seront pas utilisées à des fins autres que celles pour lesquelles elles ont été communiquées. »

Art. 51.loi 2004 «Le transfert vers un autre pays des données personnelles faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si ce pays assure un niveau de protection adéquat apprécié au regard de tous les éléments relatifs à la nature des données à transférer, aux finalités de leur traitement, à la durée du traitement envisagé, et le pays vers lequel les données vont être transférées ainsi que les précautions nécessaires mises en œuvre pour assurer la sécurité des données. Dans tous les cas, le transfert des données à caractère personnel doit s'effectuer conformément aux conditions prévues par la présente loi ».

b. Le Côté obscur du Big Data : la cybercriminalité

Ce côté obscur du Big Data, se révèle par différentes pratiques²⁶ qui tombent sous le coup de l'incrimination. Il en est ainsi du phishing, du skimming, de la fraude au président, du cryptolocker et de certaines cyberattaques.

• Le phishing

Le phishing (hameçonnage, en français) est un phénomène récent, issu de l'association de techniques de spam, d'usurpation de sites web et d'intégration sociale. Il met ainsi en œuvre l'envoi massif de courriers électroniques émanant, apparemment, d'institutions financières reconnues, vers des destinataires supposés être des clients de la banque émettrice.

Le message, sous divers prétextes (mise à jour de logiciel, sécurité des clients, vérification...) demande au destinataire de se connecter sur le site internet de la banque dont l'adresse figure dans le message pour y opérer certaines vérifications.

Les utilisateurs dupés, croyant se connecter sur le site de la banque, sont alors redirigés vers un site web frauduleux, qui est généralement une réplique parfaite du site authentique. Parvenus sur ce site, les utilisateurs pensent mettre à jour leurs informations personnelles (numéro de comptes bancaires, mots de passe, etc.). Une fois ces informations personnelles obtenues, l'escroc peut alors utiliser l'identité volée pour vider les comptes bancaires de sa victime, ou faire procéder, au nom de la victime, à l'ouverture de nombreux comptes créditeurs d'achats en ligne.

Il s'agit donc le plus souvent d'arnaquer financièrement les internautes naïfs. Il peut aussi s'agir de récupérer les identifiants (login et mots de passe) d'autres internautes naïfs pour envoyer du spam depuis une adresse réelle via plate-forme de courrier saine. Enfin, il peut s'agir de comptes sur des plates-formes en ligne comme Facebook ou des sites de jeu en ligne (poker...). Pour cela, des campagnes de spam sont mises en place. Les messages envoyés massivement aux victimes potentielles ressemblent en tous points avec ceux émanant d'administrations ou d'entreprises et incitent le lecteur à cliquer sur un lien souvent trafiqué (par exemple le lien affiché n'est pas le lien réel). La page associée au lien réel propose alors de saisir des coordonnées (bancaires le plus souvent), coordonnées qui sont collectées par les criminels.

• Le skimming

C'est l'utilisation frauduleuse de numéros de cartes bancaires sur internet.

Le skimming consiste à manipuler les automates et terminaux de paiement (bancomats, distributeurs de billets et terminaux de paiement dans les commerces, les stations-service, la restauration, etc.). Pour ce faire, les escrocs se servent d'un équipement spécial introduit dans les automates ou à proximité, qui copie les données contenues sur la piste magnétique de la carte bancaire, de débit ou de crédit et enregistre le code NIP. Les malfaiteurs agissent généralement en bandes organisées.

• La fraude au président

Elle consiste à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers (le fraudeur) pour obéir à un prétendu ordre du dirigeant.

• Le cryptolocker

C'est un logiciel malveillant qui se propage par courrier électronique à l'ouverture d'un lien ou d'une pièce jointe. Les

données sont alors « prises en otage » par le pirate qui demande le paiement d'une rançon dans un délai imparti pour que la personne puisse récupérer ses données.

• Les cyberattaques

Les cyberattaques peuvent aussi bien venir de l'intérieur de l'entreprise que de l'extérieur.

En matière de Big Data, les entreprises ont leurs propres serveurs, mais peuvent aussi avoir recours au Cloud computing pour héberger leurs données.

Les cyberattaques peuvent avoir lieu aussi bien sur les serveurs internes de l'entreprise que sur les serveurs externes de leurs prestataires en Cloud.

Il existe en fait différents types d'attaques possibles. On parle ainsi de « scans », de « spoofing », de « sniffing », de « chevaux de troie », de « cracks » de mots de passe, ou encore d'attaque de type « DOS » (« Denial of Service » ou « déni de service »).

En effet, toute attaque commence par un sondage de la future victime ; ce que l'on appelle « scan ». Ce sondage va balayer chaque port IP afin de connaître les services offerts par le système.

- **Les attaques de type « Dos »** visent à saturer un système d'information ou de communication afin de l'empêcher de fournir le service attendu. Le but est de rendre impossible l'utilisation de certains services en saturant le système concerné. L'objectif ainsi poursuivi par les pirates par une telle intrusion dont est victime le site web de l'entreprise est de nuire à son image de marque. Plus spécialement, la performance et la disponibilité sont deux facteurs essentiels pour mettre en œuvre et assurer la pérennité de sites web prospères ; un défaut de performance ou une absence de disponibilité pouvant avoir comme conséquence immédiate, par exemple, une perte de clientèle et de revenus.
- **Les attaques de sites (« suck sites »)** Lorsqu'un site web est attaqué par des pirates, sa page d'accueil originale se trouve supprimée au profit d'une page de leur cru. Celle-ci comporte généralement les trois éléments suivants : un message (à caractère technique, humoristique, politique, sexuel...) ; une revendication qui tente d'expliquer les motivations réelles ou non des pirates quant au choix du site attaqué et une signature qui est un marque promotionnelle. Celle-ci peut d'ailleurs, comme tout autre élément informatique, être piratée, ou détournée, par d'autres pirates encore moins respectueux des règles établies. Il faut signaler qu'il existe un second type d'attaques au cours de laquelle les pirates se contentent de construire un second site web, sous leur contrôle, et dont le contenu peut n'avoir aucun rapport avec le site original.
- **Dans le cas du « spoofing »**, l'adresse IP d'une machine est utilisée pour identifier une machine sur internet. Ce genre d'attaques est utilisé pour s'introduire dans le réseau d'une entreprise.
- **Le « sniffing »** vise une méthode qui consiste à « écouter » le réseau afin d'intercepter des logins et des mots de passe. Il y a « cracks » de mots de passe lorsque le hacker prend une série de mots qui lui semblent pouvoir correspondre au mot de passe et compare le résultat encrypté au mot de passe stocké sur la machine.

²⁶ Gérard Haas, La cybercriminalité à la fois côté obscur et face cachée du Big Data, Dalloz IP/IT 2016 p.21



1-3 / Fiche Pratique - Le Contrat cloud computing

Le Cloud computing, c'est quoi?

Le Cloud Computing ou Informatique dans les nuages ou encore « informatique dématérialisée ». est né du constat que de nombreux serveurs dans le monde ne sont pas utilisés au plein de leur capacité et que le besoin d'une entreprise en puissance et capacité de stockage peut varier dans le temps.

Le Cloud Computing consiste donc à mutualiser ces serveurs et considérer la puissance de calcul et de stockage des serveurs. Ainsi, cela permet, sur demande, de bénéficier d'une puissance de calcul et de stockage conforme aux besoins à un moment donné.

Le client peut donc, en fonction de ses besoins, recourir à des services de cloud, depuis le simple usage d'un espace de stockage de fichiers ou d'une application de télé-sauvegarde jusqu'à une infogérance totale de son système d'information²⁷.

Les services de cloud, quelles spécificités?

les spécificités des services de cloud résident d'une part, dans tout ce qui touche au transfert, au traitement et à la conservation des données dont le client abandonne la maîtrise entre les mains du prestataire et, d'autre part, dans le fait que cela se réalise à distance au travers de l'interconnexion de réseaux numériques ouverts.

Ainsi, l'informatique dématérialisée permet

- De mutualiser les Ressources tout en les gardant isolées
- Une élasticité
- Un large accès réseau
- Un Prix déterminé en fonction de l'usage fait

Quels sont les types de Cloud?

Il existe:

Des Clouds privés (l'infrastructure Cloud est exploitée pour une seule entreprise),

Des Clouds communautaires (l'infrastructure Cloud est accessible à des personnes ayant une communauté d'intérêt),

Des Clouds publics (l'infrastructure Cloud est accessible au public de manière large),

Des Clouds hybrides (deux ou plusieurs Clouds composent l'infrastructure Cloud).

Quels sont les modèles de Cloud?

Trois modèles de Cloud Computing existent :

- Infrastructure as a Service (ou IaaS), l'Infrastructure as a Service (IaaS) consistant en une offre d'infrastructures en ligne permettant la mise à disposition de ressources informatiques virtualisées de calcul ou de stockage en ligne (telles que des serveurs, processeurs, infrastructure réseau)
- Platform as a Service (PaaS) consistant en une offre d'applications intégrées en ligne (telles qu'un CRM ou un ERP) ;
- Software as Service (SaaS). consistant en une offre de logiciels en ligne (tels qu'une messagerie ou un logiciel bureautique)

Quels sont les risques et les avantages du Cloud?

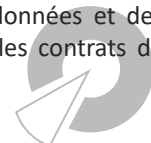
Les avantages sont:

- **Réduction des coûts:** Les PME auront la possibilité de ne plus gérer directement l'ensemble de leur système d'information. Les grandes entreprises peuvent réorganiser complètement leurs systèmes d'information en réalisant d'importantes économies d'échelle grâce à leur externalisation auprès d'un prestataire spécialisé. Le Cloud permet donc à toute entreprise de ne pas investir dans des logiciels, du matériel informatique ou encore dans des contrats de maintenance puisque cet ensemble de besoins est régi par le prestataire cloud. Le client se contente de payer les coûts d'usage de l'ensemble des moyens techniques et applicatifs dont le prestataire de cloud le fait bénéficier.
- **Simplification de la gestion:** Le recours à une solution cloud permet à une entreprise de s'exonérer des contraintes de la gestion et de la maintenance de ressources informatiques internes.
- **Une bonne disponibilité:** L'entreprise peut accéder à son application n'importe quand et de n'importe où. Il suffit juste à l'utilisateur d'établir une connexion internet.

Les risques sont:

- **Délocalisation:** Le cloud oblige l'entreprise à se déposséder de la maîtrise technique de son système d'information et d'accepter que ses données soient hébergées chez le prestataire, ce qui peut parfois inquiéter le management et faire reculer certains devant la décision.
- **La protection des DP:** Les données ou les applications du client se trouvent partiellement ou totalement stockées dans des centres informatiques (data centers) situés dans d'autres pays dont la législation relative à la protection des données personnelles peut être insuffisante.
- **La sécurité des données:** La sécurité des données et des applications est également un risque dans les contrats de cloud.

²⁷ C'est-à-dire la délocalisation de l'ensemble de ses serveurs, de ses applications et de ses données et leur gestion technique par le prestataire de cloud.



Un contrat cloud, quelle qualification?

La qualification de la relation client-prestataire dépendra des obligations contractuelles de ce dernier.

Les qualifications rejetées:

- **La vente:** Aucun transfert de propriété, ni corporelle ni incorporelle, ne résulte du contrat de cloud.
- **La location:** Les contrats de cloud (comme les contrats de SaaS en particulier) se traduisent généralement par la mise à disposition.
- **Le Dépôt:** Les contrats de stockage dans le cloud portent sur des données. Etant immatérielles, elles sont incompatibles avec la qualification de contrat de dépôt.

La qualification la mieux adaptée:

- **Un contrat de louage de service:** La qualification du contrat cloud comme un contrat de louage de service ou contrat d'entreprise semble être la mieux adaptée et la plus représentative des multiples particularités des contrats de cloud.

Quelles sont les obligations des parties dans un contrat Cloud?

Les obligations du prestataire

- Garantir la sécurité, la confidentialité, l'intégrité et la disponibilité des données :
- Garantir la continuité avec le système antérieur, dont il assure la reprise des données ;
- Respecter la législation applicable au traitement des données personnelles;
- Informer le client sur les différents lieux de stockage des données et de tous les traitements de données effectués dans le cadre de la prestation fournie;
- S'engager à ne pas collecter ni stocker au-delà des seuls besoins temporaires de sécurité des systèmes, des données de connexion relative à l'utilisation par le client de ses données et des applications auxquelles il a accès dans le cloud;
- Souscrire une assurance garantissant sa responsabilité civile professionnelle à raison de son intervention sur le système informatique du client et à cause de tous les risques qui pourraient nuire au bon fonctionnement dudit système.

Les obligations du client

- Obligation de collaboration avec le prestataire
- Payer le prix de la prestation de service

Quelle responsabilité pour le prestataire?

- La responsabilité du prestataire est une responsabilité de droit commun reposant sur la qualification d'obligation de moyens ou de résultat.
- L'obligation sera de moyen lorsqu'il sera question de la disponibilité du service alors qu'elle sera de résultat s'agissant de la récupération des données hébergées. En ce cas, seul un cas de force majeure pourra exonérer le prestataire de sa responsabilité.
- Néanmoins, il est possible d'aménager la responsabilité du prestataire par des clauses spécifiques au contrat telles que des clauses limitatives de responsabilité.

Quelles sont les principales clauses d'un contrat cloud computing?²⁸

1. Objet du contrat

Il est nécessaire de bien définir les caractéristiques essentielles des prestations de cloud computing que le prestataire va mettre en œuvre au profit de son client, à savoir:

- Définition de la prestation d'hébergement des données ;
- Définition de la prestation de fourniture d'applications en ligne ;
- Définition des différentes prestations connexes;
- type de cloud mis en œuvre.

2. La clause de qualité du service attendu Service Level Agreement SLA

Il s'agit d'un document dans lequel le prestataire formalise la qualité du service et précise notamment les modalités, la performance du service (temps de réponse, temps de transmission des données ...), la disponibilité des applications (horaires d'ouverture et de fermeture, périodes d'indisponibilités...).

Le prestataire doit être tout particulièrement vigilant à la rédaction et surtout à la lecture de cette clause dans la mesure où elle constitue en majeure partie une des causes de mise en jeu de sa responsabilité.

Cette clause fait partie intégrante du contrat de cloud et fait le plus souvent l'objet d'une annexe.

Les engagements contenus dans le SLA portent tant sur les services applicatifs que sur leur accès par le biais des liaisons télécoms. La question du niveau de disponibilité est, en particulier, critique pour une exploitation à distance puisque le client qui a externalisé ses données et les applications nécessaires à leur traitement recherche un système qui continue à être disponible dans les mêmes conditions que ce sur quoi il pouvait compter avant l'externalisation.

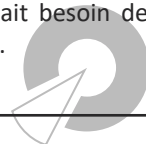
De manière générale, le SLA établira des seuils garantis quant à la disponibilité de l'application et du réseau, la vitesse de transfert des données, les délais maximum d'interruption, la fréquence des backups, les délais de restauration des données et des applications, la performance et la sécurité du système et les procédures de contrôle de ces éléments.

Cette clause doit également prévoir comment les services seront contrôlés, avec quels outils, suivant quelle procédure d'audit, par qui, à quelle fréquence etc.,

Des outils de support à toutes ces procédures doivent également être pointés, leur niveau et nature (helpdesk, combien d'opérateurs y sont disponibles, de quelle heure à quelle heure, quel jour, qui sont les personnes payées pour répondre à toute question, qui est responsable pour le « service clientèle »).

Cette clause peut donc organiser un mécanisme de sanctions acceptables par les deux parties mais qui doit en tout état de cause être incitatif pour le prestataire et suffisamment prévisible pour le client pour permettre un véritable contrôle de qualité.

Dès lors, le prestataire sera sanctionné lorsque le seuil de performance n'est pas atteint sans que le client ait besoin de rapporter la preuve d'un quelconque manquement.



Cette clause de SLA revêt ainsi le caractère d'une clause pénale.

S'agissant du type de sanction, l'Information Technology Association of America (ITAA) précise quelles sont les sanctions couramment envisagées dans le cadre de SLA.

Selon ces recommandations, les sanctions peuvent inclure des rabais mensuels (en pourcentage) sur les montants dus, en proportion de la performance réalisée par le prestataire dans le mois précédent, des réductions spécifiques, préagrées, en cas de non-atteinte des seuils de performance et la résiliation du contrat en cas de violation chronique des SLA.

3. La clause de propriété intellectuelle

Elle sera nécessaire lorsque des développements sont confiés au prestataire mais également lorsque des outils mis à disposition du client par le prestataire sont utilisés, comme par exemple une plate-forme de développement ou des structures de bases de données. Si le prestataire utilise des logiciels standards en libre accès sur le marché ou sous licence libre, il n'y aura pas de risque pour le client.

En revanche, si les technologies utilisées appartiennent au prestataire de cloud, il conviendra de prévoir une clause relative à la propriété intellectuelle du prestataire.

Par exemple, il conviendra d'inclure dans le contrat, une sous-licence sur les logiciels standards utilisés dans le cadre du cloud et une licence sur le logiciel/ programme/application qui a été créée.

La clause de propriété intellectuelle d'un contrat de cloud doit énumérer précisément les modalités de l'utilisation des applications par le client final, qui se limitent le plus souvent à un droit de « piloter » à distance les fonctionnalités choisies. Toute autre utilisation, non prévue au contrat constituera, une contrefaçon.

Elle doit également préciser que le prestataire n'acquiert, du fait de l'exécution du contrat, aucun droit de propriété intellectuelle sur les données que le client lui transfère et qui sont traitées à distance par les serveurs, et éventuellement les applications, du prestataire.

Le contrat de cloud comportera une clause exonérant et garantissant le prestataire contre une condamnation pour contrefaçon en raison du contenu des données appartenant à son client qu'il aurait stocké.

4. La clause de confidentialité

Cette clause doit, au minimum, contenir les éléments suivants :

- Une reconnaissance de principe du caractère entièrement confidentiel de toutes les données stockées et de toutes les opérations et traitements réalisés par le client sur et par le truchement des serveurs et de l'infrastructure du prestataire ; En conséquence, l'interdiction au prestataire de prendre connaissance du contenu de ces données ou de ces opérations et traitements, au-delà de ce qui leur est absolument nécessaire de connaître pour pouvoir assurer leurs prestations .

- L'engagement du prestataire de faire respecter cet engagement par tous ses salariés ou commettants et de communiquer à des tiers non autorisés ou de les laisser accéder à ces données et informations confidentielles du client ;
- L'engagement du prestataire de mettre en œuvre des moyens de sécurité (à définir en annexe technique) pour assurer la sécurité et la confidentialité des données et informations dont le client a confié la garde et l'hébergement au prestataire ;
- L'obligation imposée au prestataire de prévenir le client de tout incident ayant mis en cause la confidentialité de ses données ou traitements.

5. La clause relative à la protection des données personnelles

En France, le Syntec²⁹ recommande un article consacré aux données personnelles ainsi rédigé :

« Si les Données transmises aux fins d'utilisation des Services applicatifs comportent des données à caractère personnel, le Client garantit au Prestataire qu'il a procédé à l'ensemble des obligations qui lui incombent au terme de la loi du 6 janvier 1978 dite "Informatique & Libertés", et qu'il a informé les personnes physiques concernées de l'usage qui est fait desdites données personnelles. À ce titre, le Client garantit le prestataire contre tout recours, plainte ou réclamation émanant d'une personne physique dont les données personnelles seraient reproduites et hébergées via le Service applicatif. »

Complétée éventuellement par le paragraphe suivant :

« Dans le cas où les Données sont stockées sur des serveurs localisés dans des pays hors du territoire de l'Union Européenne, une autorisation spécifique de transfert des données doit être obtenue auprès de la CNIL. Le Prestataire s'engage à informer le Client de la localisation des Données et plus généralement, à communiquer toutes les informations utiles et nécessaires pour réaliser les déclarations. Le Client, en tant que responsable du traitement s'engage à conclure le standard contractuel établi par une décision de la Commission européenne du 5 février 2010 et à obtenir l'autorisation adéquate auprès de la CNIL ».

6. La clause de réversibilité

Il est recommandé de prévoir dans le contrat une clause de réversibilité qui permet au client de "reprenre ou de faire reprenre son informatique externalisée par un autre prestataire, afin d'assurer la continuité de l'activité sans dégradation de la qualité".

Dans la plupart des cas, la récupération des données se fera via des fichiers intermédiaires (type fichiers plats) lesquels permettent de préserver le savoir faire et les droits de propriété intellectuelle du prestataire.

Toutefois, l'inconvénient lié à cette pratique est le surcoût pour le client. Si cela semble justifié lorsque le client a pris la décision de changer de système, elle l'est moins lorsqu'il a été contraint de prendre cette décision en cas de faillite du prestataire ou en cas de manquement grave du prestataire à ses obligations. La réversibilité est un élément essentiel qui doit garantir au client

²⁹ La Fédération Syntec regroupe des syndicats professionnels spécialisés dans les professions de l'ingénierie, du numérique, des études et du conseil, de la formation professionnelle et de l'événementiel dont les sociétés sont rattachées à la Convention collective nationale des bureaux d'études techniques, des cabinets d'ingénieurs-conseils et des sociétés de conseils

la possibilité de pouvoir reprendre le contrôle exclusif de ses données et de ses applications et qui doit pouvoir, pour ce faire, compter sur la coopération technique de son prestataire.

7. La clause d'audit

Pour pallier la relative dépossession technique qu'induit pour le client le recours à une prestation de cloud, il est également conseillé d'introduire dans le contrat une clause d'audit permettant au client de procéder en cours d'exécution du contrat à des vérifications par un tiers extérieur de la conformité de la prestation aux stipulations contractuelles, et notamment aux engagements de niveau de service, de sécurité et de protection des données.

8. Clauses financières

Les solutions de cloud, qu'il s'agisse de fournir de l'espace de stockage, de la puissance de calcul pour les applications propres du client ou un logiciel en particulier, ont pour particularité le paiement de la prestation de cloud « à l'usage » ou « à la consommation ».

Le contrat prévoit ainsi un prix fondé sur une variable consommable (quantité de données stockées, bande passante, puissance de calcul décidée, utilisateurs connectés...) et le prestataire se livre à une facturation périodique.

Il conviendra donc de prévoir dans le contrat un système permettant d'avertir le client en cas de dépassement du seuil de sa consommation afin d'éviter des factures élevées.

9. La clause de modification unilatérale

Le droit positif admet la possibilité pour une partie de définir ou de modifier unilatéralement certains aspects du contrat.

Cette résiliation unilatérale va être souvent ouverte au prestataire.

Pour le client, cette clause lui permettra de modifier unilatéralement le périmètre des prestations fournies par le prestataire ou d'opter pour des options définies préalablement.

Pour le prestataire, cette clause lui permettra d'adapter son infrastructure technique comme il le souhaite.

Il convient de ne pas oublier de prévoir l'impact des ces modifications sur le prix du contrat. Cela pourra se traduire par une clause prévoyant:

- les prix de toutes les modifications envisageables ;
- que la modification du prix sera liée à l'augmentation des coûts pour le prestataire ou à l'amélioration du service pour le client ;

- que le prix sera fonction du prix du marché (le contrat prévoira alors la méthodologie pour choisir et comparer les prix proposés par les concurrents pour des prestations équivalentes).

10. La loi applicable et la juridiction compétente

Les contrats de cloud sont des contrats fréquemment internationaux, ce qui implique l'application des règles de droit international privé régissant ces contrats dont l'exécution s'effectue généralement sur un territoire distinct de celui du client, voire du prestataire lui-même.

Il est recommandé d'introduire dans le contrat de cloud une clause prévoyant la loi applicable en cas de litige ainsi qu'une clause d'attribution de juridiction du pays de l'entreprise afin d'éviter les difficultés liées à la saisine de tribunaux étrangers.

Selon l'article 62 CDIP : « Le contrat est régi par le droit désigné par les parties »

En l'absence de clause spécifique, les règles suivantes s'appliquent:

- s'agissant de la loi applicable, il conviendra d'appliquer l'article 62 al 2 CDIP qui dispose que «A défaut par celles-ci de désigner la loi applicable, le contrat est régi par la loi de l'Etat du domicile de la partie dont l'obligation est déterminante pour la qualification du contrat, ou celle du lieu de son établissement, lorsque le contrat est conclu dans le cadre de son activité professionnelle ou commerciale. »
- S'agissant de la compétence juridictionnelle, il conviendra d'appliquer les articles suivants:

L'article 3 du CDIP : « Les juridictions tunisiennes connaissent de toute contestation, civile et commerciale entre toutes personnes quelle que soit leur nationalité, lorsque le défendeur a son domicile en Tunisie ».

Toutefois, d'après l'Article 4 CDIP, les juridictions tunisiennes sont compétentes si les parties au litige les désignent comme telles, ou, si le défendeur accepte d'être jugé par elles..

Il n'en demeure pas moins que l'article 5 du même code apporte une précision en ces termes : «Les juridictions tunisiennes connaissent également :

Si l'action est relative à un contrat exécuté ou devant être exécuté en Tunisie, sauf clause attributive de compétence en faveur d'un for étranger. »



2 / Droit de la concurrence / droit de la distribution

2.1 / Franchise : Cadre législatif et réglementaire

- **La loi n° 2009-69 du 12 août 2009, relative au commerce de distribution a consacré un chapitre aux contrats de franchise.**

L'article 14 a défini le contrat de franchise et le réseau de franchise :

Le contrat de franchise: est un contrat par lequel le propriétaire d'une marque ou d'une enseigne commerciale accorde le droit de son exploitation à une personne physique ou morale dénommée franchisé, et ce, dans le but de procéder à la distribution de produits ou à la prestation de services moyennant une redevance. Le droit d'exploitation de la franchise comprend le transfert des connaissances acquises, le savoir faire et l'exploitation des droits de la propriété intellectuelle.

Le réseau de franchise: Est l'ensemble des commerces indépendants exerçant sous la même marque et selon des méthodes commerciales unifiées dont notamment l'aménagement des locaux, les modes de gérance, l'exposition, le marketing et les sources d'approvisionnement.

Les articles 16 et 17 fixent les obligations des parties :

Les obligations du franchiseur:

Il doit être titulaire de la marque ou de l'enseigne commerciale, fournir au franchisé durant la relation contractuelle l'assistance commerciale et technique et toutes les informations sincères sur le réseau de franchise.

Les obligations du franchisé:

Le franchisé est tenu de fournir au franchiseur les données relatives à ses ventes et à sa situation financière et d'autoriser le franchiseur ou ses délégués, à accéder à ses locaux pendant les horaires habituels d'ouverture ou du travail.

L'article 15 fixe, sous peine de nullité, les différentes conditions exigées à la signature du contrat :

Le contrat de franchise doit être écrit. Le franchiseur est tenu dans un délai minimum de vingt jours avant la signature du contrat de mettre à la disposition du franchisé un projet de contrat et un document mentionnant les informations relatives au franchiseur et à son secteur d'activité. Les clauses minimales obligatoires faisant partie du contrat et les données minimales que doit contenir le document susvisé seront fixées par décret. Est considéré nul tout contrat contraire aux dispositions du présent article.

L'article 15 renvoi au décret d'application (Décret n° 2010-1501 du 21 juin 2010) qui énumère les clauses minimales obligatoires du contrat de franchise et du document d'information y relatif :

- **Décret n° 2010-1501 du 21 juin 2010, portant fixation des clauses minimales obligatoires des contrats de franchise ainsi que des données minimales du document d'information l'accompagnant.**

Les clauses minimales obligatoires des contrats de franchise :

Art. 2 - Le contrat de franchise doit inclure les droits et les obligations du franchiseur et du franchisé et notamment les mentions suivantes :

- les services rendus par le franchiseur au franchisé notamment en ce qui concerne le transfert de l'expérience acquise, du savoir faire et de l'exploitation des droits de la propriété intellectuelle,
- les royalties exigées du franchisé,
- la durée du contrat et les conditions de son renouvellement,
- les conditions d'exploitation de la marque ou de l'enseigne commerciale,
- les conditions de résiliation du contrat,
- les clauses d'exclusivité d'approvisionnement,
- les clauses de non concurrence,
- la délimitation de la zone géographique exclusive d'exploitation de la marque ou de l'enseigne commerciale,
- l'obligation du franchisé à la confidentialité des données divulguées par le franchiseur,
- le plan d'investissement à exécuter par le franchisé,
- Les conditions de répartition des dépenses de publicité,
- la communication au franchiseur des données relatives à la vente et à la situation financière du franchisé,
- les procédures d'autorisation du franchiseur ou de ses délégués pour accéder aux locaux du franchisé,
- la possibilité pour le bénéficiaire d'un contrat d'exclusivité de représentation couvrant tout le territoire de la République Tunisienne, de conclure avec des franchisés des contrats d'exploitation couvrant des zones géographiques limitées.



Les données minimales du document d'information :

Art. 3 - Le document d'information accompagnant le contrat de franchise, visé par l'article 15 de la loi n° 2009-69 du 12 août 2009 relative au commerce de distribution inclut des données relatives au franchiseur et son secteur d'activité et notamment les mentions suivantes :

- la forme juridique de l'entreprise et la nature de son activité,
- l'identité du franchiseur et son adresse pour les personnes physiques,
- l'identité du représentant légal, l'adresse du siège social, la liste des dirigeants et le capital pour les personnes morales,
- l'historique de l'entreprise,
- le numéro d'inscription dans le registre de commerce ou toute donnée équivalente,
- la preuve des droits de propriété de la marque ou de l'enseigne commerciale,
- les données relatives à l'inscription au registre national des marques,
- les données sur le réseau des franchisés,
- listes du réseau des franchisés en Tunisie, leurs adresses, la date de leur adhésion au réseau et la liste des franchisés exclus du réseau,
- les données sur le secteur d'activité de l'entreprise et les opportunités de développement du secteur dans les zones où la marque est représentée ainsi qu'en Tunisie,
- la spécification de la nature, du montant des dépenses et des investissements spécifiques de la marque ou de l'enseigne commerciale,
- les états financiers de l'entreprise.

Art. 4 - Les contrats de franchise ne doivent pas comporter des clauses anticoncurrentielles relatives à :

- l'imposition des prix de revente ou de prestation de service,
- la fixation d'un chiffre d'affaires minimum.

Art. 5 - En application des dispositions des articles 5 et 6 de la loi de la concurrence et des prix susvisée, sont fixées par arrêté du ministre chargé du commerce, les activités objet de contrats de franchise qui bénéficient systématiquement de l'autorisation prévue par l'article 6 de la même loi.

Les contrats de franchise peuvent être un terrain propice au développement de pratiques anticoncurrentielles et surtout des ententes prohibées par l'article 5 de la loi relative à la réorganisation de la concurrence et des prix. Cet article sanctionne par la nullité tout engagement, convention ou clause contractuelle se rapportant à l'une des pratiques prohibées. Toutefois l'article 6 offre une marge de manœuvre permettant d'éviter la nullité :

• Loi n° 2015-36 du 15 septembre 2015, relative à la réorganisation de la concurrence et des prix

Art. 5 - Sont prohibées, les actions concertées, les cartels et les ententes expresses ou tacites ayant un objet ou un effet anticoncurrentiel et lorsqu'elles visent à :

1. faire obstacle à la fixation des prix par le libre jeu de l'offre et de la demande,
2. limiter l'accès au marché à d'autres entreprises ou le libre exercice de la concurrence,
3. limiter ou contrôler la production, les débouchés, les investissements, ou le progrès technique,
4. Répartir les marchés ou les sources d'approvisionnement.

Est également prohibée, l'exploitation abusive d'une position dominante sur le marché intérieur ou sur une partie substantielle de celui-ci, ou d'un état de dépendance économique dans lequel se trouve une entreprise cliente ou fournisseur qui ne dispose pas de solutions alternatives, pour la commercialisation, l'approvisionnement ou la prestation de service (.....)

Est nul, de plein droit, tout engagement, convention ou clause contractuelle se rapportant à l'une des pratiques prohibées en vertu des paragraphes 1 et 2 du présent article.

Art. 6 - Sont exemptés de l'application des dispositions de l'article 5 de la présente loi, les accords, pratiques ou catégories de contrats dont les auteurs justifient qu'ils sont indispensables pour garantir un progrès technique ou économique et qu'ils procurent aux utilisateurs une partie équitable du profit qui en résulte, à condition qu'elles ne conduisent pas à :

- imposer des restrictions qui ne sont pas indispensables pour atteindre les objectifs visés,
- éliminer complètement la concurrence sur le marché en cause ou sur une partie substantielle de ce marché.

Cette exemption est accordée par un arrêté motivé du ministre chargé du commerce après avis du conseil de la concurrence et est publiée au Journal Officiel de la République Tunisienne.

Le ministre chargé du commerce peut déterminer la durée de l'exemption ou la soumettre à une révision périodique. Il peut retirer l'exemption en cas de non respect par les parties concernées des conditions de son octroi.

Les procédures de présentation des demandes d'exemption et la durée de celle-ci sont fixées par décret gouvernemental sur proposition du ministre chargé du commerce après avis du conseil de la concurrence.



• **Décret gouvernemental n° 2016-1204 du 18 octobre 2016, portant fixation des procédures de présentation des demandes d'exemption et de sa durée en application de la loi n° 2015- 36 du 15 septembre 2015, relative à la réorganisation de la concurrence et des prix.**

Art. 1 - Le présent décret gouvernemental a pour objectif de fixer les procédures de présentation des demandes d'exemption et la durée de celle-ci, conformément à l'article 6 de la loi n° 2015-36 du 15 septembre 2015, relative à la réorganisation de la concurrence et des prix.

Art.2 - Les personnes concernées par l'exemption doivent présenter aux services spécialisés du ministère chargé du commerce un dossier en trois exemplaires, comprenant des éléments permettant de prouver un progrès économique ou technique de la pratique ou de l'accord ou des catégories de contrats et les effets probables. Le dossier comprend :

- une demande contenant des informations sur le demandeur de l'exemption, sa forme juridique, sa nationalité et son adresse,
- une copie du registre du commerce et de l'acte de constitution de la société ou la carte d'identité du demandeur de l'exemption,
- une étude sur le secteur et la structure du marché dans laquelle exerce la société ou l'organisme concerné,
- la pratique ou l'accord ou les catégories de contrats objet de la demande d'exemption,
- une note explicitant les avantages économiques de l'exemption et ses effets sur le bien être du consommateur et sur l'emploi,
- les programmes d'investissement et les états financiers, toute information ou document pouvant appuyer la demande de l'exemption.

Après vérification de la constitution du dossier, le ministre chargé du commerce transmet une copie du dossier comportant les éléments sus-indiqués au conseil de la concurrence pour avis. Le conseil doit rendre son avis dans un délai ne dépassant pas deux mois à compter du jour de la transmission.

Art. 3 - Le ministre chargé du commerce doit répondre à la demande d'exemption dans un délai de trois mois à compter du jour de la réception d'un dossier comportant tous les éléments énumérés à l'article 2. Le cas échéant, des informations additionnelles peuvent être demandées avec sursis du délai jusqu'à leur communication. En cas de non présentation des informations demandées dans les délais, la demande d'exemption est considérée nulle.

La réponse du ministre se fait par un arrêté motivé comportant soit l'accord sur l'exemption dans les conditions présentées, soit l'accord sous réserves de changement de quelques conditions soit le refus.

Art. 4 - L'exemption est accordée pour une période ne dépassant pas cinq ans renouvelables. La personne concernée par l'exemption désirant la renouveler présente une demande de renouvellement comprenant une mise à jour des éléments composant le dossier énumérés à l'article 2 ci-dessus, et ce, dans un délai de trois mois avant la fin de la durée de l'exemption. Le ministre chargé du commerce, après avis du conseil de la concurrence, répond à la demande de renouvellement avant la fin de la durée de l'exemption.

Art. 5 - Le ministre de l'industrie et du commerce est chargé de l'exécution du présent décret gouvernemental qui sera publié au Journal Officiel de la République Tunisienne.

• **Arrêté du ministre du commerce et de l'artisanat du 28 juillet 2010, portant l'octroi systématique, à certains contrats de franchise, de l'autorisation prévue par l'article 6 de la loi n° 91-64 du 29 juillet 1991, relative à la concurrence et aux prix.**

En application des dispositions de l'article 6 de la loi sur la concurrence et aux prix, cet Arrêté énumère dans un tableau la liste des secteurs bénéficiant d'une exemption systématique de l'interdiction générale des ententes et des pratiques prohibées de l'article 5 de la même loi :

1- Les marques nationales : tous secteurs confondus,

2- Les marques étrangères : les secteurs suivants : Secteurs de distribution - Parfumerie, produits de beauté et cosmétique - Prêt à porter - Chaussures - Maroquinerie - Articles et chaussures de sport - Produits diététiques - Horlogerie - Articles de cadeaux - Lunetterie - Articles de ménage grand public - Meubles - Plantes d'intérieur et fleurs - Quincaillerie et articles sanitaires - Matériel électronique et informatique - Librairie - Biens d'équipement pour divers secteurs Secteur touristique - Location de voiture - Aires de loisir - Gestion des hôtels Secteur de la formation - Formation professionnelle Autres activités économiques - Service de dépannage - Salons de coiffure de beauté et d'hygiène corporelle - Services de réparation et de maintenance (auto, électronique ...) - Services d'appui à l'abandon du tabagisme - Services de soins dans les hôtels - Thalasso thérapie.



Boussayene Knani & Associés a jugé opportun de publier une sélection de décisions et avis récents et inédits dans un certain nombre d'affaires dont certaines ont été traitées par le Cabinet. La jurisprudence du Conseil de la Concurrence (2015-2016-2017) a permis à plusieurs reprises de clarifier des notions, de préciser leurs nuances et de dissiper les confusions. Cette publication essaye de rendre compte de l'évolution de la jurisprudence et des recommandations destinées à améliorer le fonctionnement concurrentiel des marchés.

Franchises et demandes d'exemption :

La démarche du Conseil de la concurrence en matière d'autorisation exceptionnelle des franchises

Les contrats de franchises constituent un terrain propice au développement des pratiques anticoncurrentielles prohibées par l'article 5 de la loi n° 2015-36 du 15 septembre 2015, relative à la réorganisation de la concurrence et des prix. Pour cette raison les parties au contrat de franchise peuvent se trouver dans l'obligation de demander l'exemption auprès du ministre chargé du commerce, conformément à l'article 6 de la loi précitée.

« Sont exemptés de l'application des dispositions de l'article 5 de la présente loi, les accords, pratiques ou catégories de contrats dont les auteurs justifient qu'ils sont indispensables pour garantir un progrès technique ou économique et qu'ils procurent aux utilisateurs une partie équitable du profit qui en résulte, à condition qu'elles ne conduisent pas à :

- imposer des restrictions qui ne sont pas indispensables pour atteindre les objectifs visés,
- éliminer complètement la concurrence sur le marché en cause ou sur une partie substantielle de ce marché.

Cette exemption est accordée par un arrêté motivé du ministre chargé du commerce après avis du conseil de la concurrence et est publiée au Journal Officiel de la République Tunisienne(...) »

Concrètement l'article 6 essaye de concilier entre deux impératifs contradictoires. Il s'agit de tolérer les ententes qui génèrent le progrès technique et l'investissement et permettent la création d'emploi, tout en continuant à se prémunir contre les effets négatifs des ententes verticales, inutiles pour l'économie et restrictives de la concurrence.

Le Conseil avait depuis une dizaine d'années donné son avis³⁰ sur les avantages et les inconvénients des franchises pour le franchisé tunisien et pour l'économie nationale :

Les avantages de la franchise

- Bien qu'il appartienne à un réseau de franchise, le franchisé est propriétaire de son entreprise. Il reste juridiquement indépendant tout en bénéficiant de l'image de marque et de la réputation de l'enseigne par rapport au consommateur.
- Le franchisé bénéficie d'un système de gestion commerciale expérimenté par le franchiseur, d'une assistance permanente et d'un transfert de savoir-faire.
- Le franchisé bénéficie de l'avantage compétitif dû à la synergie économique du réseau d'une part et à la capacité d'innovation du franchiseur d'autre part.

Contraintes de la franchise

- Bien que juridiquement indépendant, le franchisé doit se plier à la stratégie commerciale du franchiseur.
- Le franchisé est tenu de continuer à respecter les normes et standards imposés même s'il s'avère qu'ils ne sont pas efficaces sur le plan pratique.
- Le franchisé doit respecter les restrictions prévues lors de l'approvisionnement. Il est souvent obligé de s'approvisionner auprès du franchiseur ou des fournisseurs référencés.
- Le franchisé doit appliquer la stratégie d'investissement mise en œuvre par le franchiseur, même si elle s'avère contraire à ses intérêts.

Dans le cadre de sa mission consultative, le Conseil de la concurrence examine de plus en plus, depuis les trois dernières années, des demandes d'exemption en rapport avec des franchises qui sont le plus souvent relatives aux marchés pertinents de la restauration rapide, des cafés et des pâtisseries.

Les réseaux de franchises de la restauration rapide ont connu un développement remarquable depuis l'année 2012. A titre d'exemple, en 2015 le Conseil a été consulté à neuf reprises pour donner son avis sur des contrats de franchises se rapportant généralement à des marques de notoriété internationale opérant dans le marché du fast-food et des cafés.

Cette augmentation considérable des demandes d'octroi de l'autorisation exceptionnelle au sens de l'article 6 s'explique par le fait que le secteur de la restauration rapide n'est pas mentionné dans la liste des secteurs bénéficiant de l'autorisation systématique et qui sont prévus par l'arrêté du ministre du commerce et de l'artisanat du 28 Juillet 2010.

Dans ses avis, le Conseil commence généralement par la qualification du contrat de franchise comme étant un **contrat de représentation commerciale exclusive**. Il rappelle que ce type de contrat qui constitue une **entente verticale illicite**, était totalement prohibé par la loi de la concurrence et que des amendements ultérieurs ont introduit une certaine souplesse permettant d'exempter de l'application des dispositions prohibant les ententes, les contrats dont les auteurs justifient qu'ils sont indispensables pour garantir un progrès technique ou économique et qu'ils procurent aux utilisateurs une partie équitable du profit.

³⁰ Avis n°62160 du 1er février 2007 (voir surtout page 35-36 rapport 2007)

a. Avis n°162602 du 13 octobre 2016 "Burger King"

Le franchiseur : L'enseigne américaine de fast-food Burger King, classée 6^{ème} mondiale dans le secteur avec 13667 restaurants implantés dans 98 pays

Le Franchisé : First Food Services Tunisia SA

Analyse des clauses restrictives de la concurrence dans le contrat de franchise Burger King

Les clauses relatives à la durée du contrat

La durée du contrat fixée à 20 ans été jugée trop longue surtout pour un contrat impliquant plusieurs restriction à la concurrence.

La clause relative à la distribution exclusive

Cette clause qui doit être respectée sous peine de résiliation, impose au franchisé d'acheter, à titre exclusif, tous les produits soit directement auprès du franchiseur soit auprès d'autres fournisseurs énumérés dans une liste exhaustive figurant dans un manuel de procédure. **Le Conseil a considéré cette condition contraire au principe de liberté d'exploitation, corolaire de la liberté de commerce et de l'industrie. En outre, cette restriction permet au franchiseur de contrôler les débouchés. Elle est donc contraire à l'article 5.3 de la loi relative à la réorganisation de la concurrence et des prix.**

Les restrictions d'ordre intuitu personae

Cette clause interdit au franchisé, sauf autorisation préalable du franchiseur, de s'adonner à tout acte impliquant notamment une cession en tout ou en partie de son fonds de commerce. **Cette pratique a été jugée excessive et contraire à l'article 5.3 précité puisqu'elle permet au franchiseur d'avoir la main mise sur la stratégie d'investissement.**

Les clauses relatives au droit de préemption

Selon le décret n°2010-1501 du 21 juin 2010, le droit de préemption n'est pas une clause obligatoire devant être inscrite dans les contrats de franchises.

L'inscription de cette clause dans le contrat de franchise donne la priorité au franchiseur pour racheter le fonds de commerce du franchisé en cas de cessation de l'activité de ce dernier. L'entreprise pourra par la suite être revendue à un nouveau franchisé. Cette clause n'oblige en aucun cas le franchiseur à reprendre le site.

Le Conseil de la concurrence a exprimé sa réticence par rapport à cette clause limitant l'accès au marché à d'autres entreprises au sens de l'article 5.2 précité.

La clause de non-concurrence

La plupart des contrats de franchise prévoient une clause de non-concurrence par laquelle le franchisé s'interdit, pendant et après la fin de son contrat, de développer une activité concurrente de celle exercée dans le cadre de son contrat de franchise.

En introduisant de telles clauses, **le franchiseur cherche à protéger son réseau** en évitant que l'ex-franchisé continue, dans son activité future, de profiter du savoir-faire dont il a eu connaissance au cours du contrat de franchise.

Le Conseil de la concurrence a considéré cette clause comme une contrainte limitant au franchisé l'accès au marché au sens de l'article 5.2 précité.

En raison de toutes ces clauses restrictives de par leur objet ou leur effet³¹, le Conseil a remarqué que le contrat de franchise objet de la consultation constitue une entente illicite.

Toutefois, l'article 6 de la loi relative à la réorganisation de la concurrence et des prix autorise exceptionnellement ces ententes dont les auteurs justifient qu'elles sont :

- indispensables pour garantir un progrès technique ou économique
- et qu'elles procurent aux utilisateurs une partie équitable du profit qui en résulte

Et ce, à condition qu'elles ne conduisent pas à :

- imposer des restrictions qui ne sont pas indispensables pour atteindre les objectifs visés,
- éliminer complètement la concurrence sur le marché en cause ou sur une partie substantielle de ce marché.

Appréciation de l'applicabilité des critères d'exemption de l'article 6 au contrat de franchise Burger King :

Les critères de réalisation d'un progrès technique ou économique

- L'implantation en Tunisie de l'enseigne américaine Burger King dans le cadre d'une franchise à travers 15 restaurants permettra de renforcer la présence des marques notoires dans le secteur des fast-food en Tunisie et d'améliorer la qualité des services et des produits mis en vente, ce qui est de nature à garantir le progrès économique.
- Cette implantation permettra la création de 600 emplois directs et 200 emplois indirects.
- Le système de gestion commerciale expérimenté par le franchiseur, l'assistance permanente et le transfert de savoir-faire sont de nature à garantir le progrès technique.

Les critères de réalisation d'une partie équitable du profit aux utilisateurs :

- Le consommateur aura l'occasion de découvrir de nouveaux produits conformes aux standards internationaux et aura une large variété de choix grâce au transfert du savoir-faire.
- Ce contrat de franchise permet au franchisé de s'approvisionner de produits tunisiens à hauteur de 80%.

Avis du Conseil:

Au vu de ce qui précède, le Conseil considère l'ensemble des clauses restrictives de la concurrence indispensables pour garantir un progrès technique ou économique et qu'elles procurent aux utilisateurs une partie équitable du profit qui en résulte.

La durée d'exploitation exclusive de la marque Burger King doit pour autant être limitée à une période de 5 ans au lieu de 20 ans renouvelable une seule fois pour la même durée.

³¹ Dans l'affaire n° 2137 du 27 Mars 2003 le Conseil a rappelé l'approche alternative et s'est étalé longuement sur son explication. On peut lire dans cette décision :

« Les règles de la concurrence interdisent aux entreprises économiques toute sorte de concertation de nature à entraver l'équilibre général du marché, et ce, si l'entrave est intrinsèquement anticoncurrentielle de par son objet, ou si les effets qui en découlent le sont (.....). Le délit d'atteinte aux règles de la concurrence peut être établi par deux moyens :

- la conclusion d'un accord visant à perturber le fonctionnement normal du marché ;
- ou l'établissement de la preuve que cet accord a été concrétisé effectivement dans la pratique ».

Il en ressort selon le rapport du Conseil de la Concurrence, que « le délit d'atteinte à la concurrence en matière de pratiques prohibées ne suppose nullement le cumul entre l'acte juridique qu'est la conclusion de l'accord et l'événement effectif qu'est la concrétisation de l'accord. Il suffit de prouver l'un des deux éléments pour que le délit soit établi. La renonciation de l'entreprise concernée à la concrétisation de l'accord par la suite ne constitue aucunement une cause d'exonération, mais relève plutôt des circonstances atténuantes ».



b. Avis n°162622 du 29 décembre 2016 "Sharf coffe shop compagny"

Le franchiseur : L'enseigne autrichienne Sharf coffe shop compagny disposant de 298 points de vente dont 6 implantés au Maroc et 21 en Egypte.

Le Franchisé : Monsieur Saidi Karim

Le Ministre du commerce a demandé l'avis du Conseil de la concurrence en ce qui concerne l'implantation en Tunisie de l'enseigne autrichienne Sharf coffe shop compagny dans le cadre d'une franchise.

Le plan d'investissement prévoit l'ouverture de 3 espaces « coffeshop » durant les années 2016, 2017, 2018 et 2019 et la distribution de café de qualité supérieure importé d'Autriche et réalisé grâce à des machines spéciales importées.

Appréciation des critères d'exemption de l'article 6 :

- L'étude du marché pertinent a permis au Conseil de conclure que la concurrence est très limitée dans le secteur des salons de thé haut de gamme. Ce projet permettra donc de dynamiser et de moderniser ce secteur tant au niveau des services et de la qualité qu'au niveau esthétique et architectural. Cet alignement sur les standards internationaux offrira aux touristes des produits similaires à ceux fournis par la concurrence internationale.
- Le contrat de franchise objet de l'examen permet au franchisé de s'approvisionner de produits tunisiens à hauteur de 80%.
- Ce projet n'impliquera pas une exportation importante de devises dans la mesure où le financement sera réalisé essentiellement par le franchisé disposant de fonds propres en devise à l'étranger.

En l'espèce, le Conseil a décelé des clauses restrictives de la concurrence mais compte tenu des avantages de cette franchise pour l'économie et les consommateurs il a répondu favorablement à la demande d'exemption.

c. Avis n°152564 du 17 août 2015 "Paul"

Le franchiseur : L'enseigne française Paul spécialisée dans la finition, cuisson et vente de pains, viennoiseries et pâtisseries industriels.

Le Franchisé : شركة المخبز التونسي

Le Conseil a été consulté pour donner son avis sur la possibilité d'octroi de l'autorisation exceptionnelle de l'article 6 concernant l'implantation en Tunisie de l'enseigne française Paul dans la mesure où le secteur de la cuisson et vente de pains, viennoiseries et pâtisseries industriels n'est pas mentionné dans la liste des secteurs bénéficiant de l'autorisation systématique au sens de l'arrêté du ministre du commerce et de l'artisanat du 28 Juillet 2010.

L'étude du marché pertinent a permis au Conseil de constater que les boulangeries opérant dans le cadre de franchises et commercialisant leurs produits haut de gamme sous des marques notoires sont de plus en plus nombreux dans les quartiers huppés de la capitale depuis l'entrée en vigueur de la loi n° 2009-69 du 12 août 2009, relative au commerce de distribution : « Boulangerie Banette », « Chopain », « ERIC KAYSER ».

Le montage juridique prévoyait la signature de quatre contrats : un contrat de franchise, un contrat de transfert du savoir-faire « know-how », un contrat de distribution et un contrat de services. Ces contrats revêtent un caractère indissociable. La résiliation de l'un entraîne la résiliation de tous les autres.

Le Conseil a décelé plusieurs clauses prohibées et contraires à l'article 5 de la loi relative à la réorganisation de la concurrence et des prix. Toutefois, compte tenu des avantages de cette franchise pour l'économie et les consommateurs, la réponse à la demande d'exemption était positive.



d. Avis n°162599 du 13 octobre 2016 "Hard Rock Café"

Le franchiseur : L'enseigne américaine de fast-food Hard Rock Café

Le réseau Hard Rock Cafe est implanté dans 54 pays avec 198 restaurants et 16 hôtels et casinos. Cette marque opère spécialement dans le secteur de restaurants à thème et plus concrètement dans « la restauration à services complet informels »

Le Franchisé : Société D'investissement Hôteliers el Mouradi

Le Conseil a rappelé que ce contrat de franchise est qualifié comme un contrat de représentation commerciale exclusive en soulignant que ce type de contrat constitue une entente verticale illicite.

Analyse des clauses restrictives de la concurrence

L'examen de ce contrat de franchise a permis de déceler plusieurs clauses et pratiques restrictives de la concurrence et contraires aux principes fondamentaux de la liberté du commerce et de l'industrie et à l'article 5 de la loi relative à la réorganisation de la concurrence et des prix :

Les clauses d'exploitation exclusive de la marque :

Ce contrat de franchise interdit au franchiseur, durant toute la durée du contrat, de conclure de nouveaux contrats de franchise concernant les zones géographiques de Sousse, Gammarth, Djerba, Hammamet et le centre ville de Tunis.

Le Conseil souligne que cette clause est de nature à restreindre la concurrence en limitant l'accès au marché à d'autres entreprises. Toutefois, il remarque que cette restriction géographique est indispensable dans ce type de franchises.

Les clauses relatives à la durée du contrat

La durée du contrat fixée à 10 ans renouvelable une seule fois pour la même période, a été jugée trop longue surtout pour un contrat impliquant plusieurs restrictions à la concurrence.

La clause de non concurrence

Cette clause de non-concurrence post-contractuelle interdit au franchisé de concurrencer le réseau durant toute la période du contrat et pendant une année après sa fin, et ce, dans un rayon de 10 Miles (16 Km) à partir du lieu d'exploitation.

Le Conseil souligne que cette clause est de nature à restreindre la concurrence en limitant l'accès au marché à d'autres entreprises au sens de l'article 5.2 de la loi relative à la réorganisation de la concurrence et des prix.

Toutefois, existant dans la plupart des contrats de franchises, cette clause est selon le Conseil, indispensable pour la réalisation de l'investissement.

Appréciation des critères d'exemption de l'article 6 :

L'étude du marché pertinent a permis au Conseil de conclure que les restaurants de type Fast-food opérant sous le régime de la franchise sont de plus en plus présents en Tunisie. Cette présence sera renforcée par la l'implantation de la marque Hard Rock Café qui permettra de dynamiser et de moderniser le secteur tant au niveau des services que de la qualité.

Le Conseil a également constaté que l'investissement porte sur la création de 5 restaurants et impliquera la création de 375 emplois.

De surcroît, le contrat de franchise objet de l'examen permet au franchisé de s'approvisionner essentiellement de produits tunisiens.

Compte tenu des avantages de cette franchise pour l'économie et les consommateurs, la réponse du Conseil à la demande d'exemption était positive à condition de réduire la durée du contrat de 10 ans à 5 ans.



Affaire n°151379 du 16 mars 2017

(Marché du commerce en gros des viandes rouges à travers la participation aux appels d'offres)

Les agissements dénoncés avaient pour objet l'adoption par la société des viandes du Cap Bon d'une politique de prix excessivement bas au sens de l'article 5 paragraphe dernier de la nouvelle loi sur la concurrence et les prix qui dispose :

« Est également prohibée, toute offre de prix ou pratique de prix abusivement bas susceptible de menacer l'équilibre d'une activité économique et la loyauté de la concurrence sur le marché. »

Le Conseil a eu l'occasion de confirmer sa jurisprudence constante « Les prix excessivement bas sont ceux qui n'englobent pas les éléments du prix réel qui devrait inclure le coût fixe, le coût variable et la marge commerciale, ce qui engendre une atteinte à l'équilibre du marché »

En l'espèce, le Conseil a apporté la preuve des prix excessivement bas à partir d'un faisceau d'indices concordants reposant sur les critères suivants :

- Le critère de comparaison des prix de la requérante avec les estimations de l'acheteur public d'une part et avec les prix pratiqués par les sociétés ayant participé à l'appel d'offre d'autre part.
- Le critère de comparaison des prix de la requérante avec les prix adoptés à l'occasion de marchés publics similaires réalisés avec le même acheteur public ou avec des acheteurs publics différents.
- Le critère de comparaison des prix de la requérante avec les prix minimums pratiqués dans le marché et avec la moyenne générale des prix.

Le recours à ces critères a révélé sans conteste que la requérante pratiquait des prix excessivement bas.

L'enquête a également révélé que les prix pratiqués étaient parfois excessivement élevés et d'autres fois excessivement bas, ce qui pouvait laisser penser qu'il s'agissait d'une stratégie visant à exclure des concurrents du marché.

En effet, les prix étaient excessivement élevés quand la requérante participait seule aux appels d'offres et devenaient subitement excessivement bas quand il y avait des concurrents.

Généralement la mise en œuvre de cette stratégie n'est possible qu'avec une certaine complicité de l'acheteur public qui dévoile le secret des affaires en transmettant à chaque fois au participant à l'appel d'offre des informations relatives au nombre des participants à l'offre et à leurs prix.

Toutefois, en l'espèce le Conseil n'a pas retenu l'existence d'une entente illicite sur les prix entre l'acheteur public et l'entreprise visant à exclure les fournisseurs de viande rouge du marché. Le participant à l'appel d'offre a été cependant condamné.

L'approche du Conseil de la concurrence dans l'affaire n° 81159 du 31 décembre 2008, nous semble plus subtile. Des faits similaires ont été qualifiés d'entente illicite dans la mesure où l'adoption d'une politique de prix variant du simple au double, en fonction du nombre des participants à l'appel d'offres, ne peut être planifiée que grâce à la connivence de l'acheteur public.

Affaire n°151389 du 25 mai 2017 :

Henke c/ Argania Distribution

(Marché de la distribution de la lessive Ariel à travers les grandes et moyennes surfaces)

L'apport de cette décision a été considérable à double titre : le Conseil a été décisif non seulement dans l'affirmation des critères d'identification des prix excessivement bas, mais aussi en matière de compétence, et ce, à travers la détermination de la frontière entre les domaines d'intervention du Gouvernement et ceux du Conseil de la concurrence.

Le Conseil a entériné sa définition constante des prix excessivement bas prohibés par l'article 5 paragraphe dernier « Les prix excessivement bas sont ceux qui n'englobent pas les éléments du prix réel qui devrait inclure le coût fixe, le coût variable et la marge commerciale »

En l'espèce le Conseil a exclu l'adoption de la requérante d'une politique de prix excessivement bas, dans la mesure où la comparaison des prix d'importation du produit en tenant compte des majorations différentes prouve l'existence d'une différence positive pouvant couvrir la marge de bénéfice de la requérante.

En outre, cette décision précise « qu'il n'appartient pas au juge de la concurrence de contrôler si la société américaine Procter and Gamble qui produit la marque Ariel a engagé une politique de dumping³² en exportant ses produits en Tunisie à des prix prédateurs³³. L'ouverture de l'enquête relative à l'exportation de quantités importantes du produit Ariel au marché tunisien durant les années 2014 et 2015 à des prix tendant à la baisse relève de la compétence des services administratifs concernés ». Plus concrètement, « il appert de la loi n°99-9 du 13/02/1999, relative à la défense contre les pratiques déloyales à l'importation et de la loi n° 98-106 du 18 décembre 1998, relative aux mesures de sauvegarde à l'importation que la lutte contre le dumping relève des prérogatives du gouvernement »³⁴.



³² L'article 3 de la loi n°99-9 du 13/02/1999 relative à la défense contre les pratiques déloyales à l'importation a défini le dumping comme suit « un produit est considéré comme faisant objet d'un dumping, c'est-à-dire comme étant introduit sur le marché tunisien à un prix inférieur à sa valeur normale, si le prix à l'exportation de ce produit, est inférieur au prix comparable pratiqué, au cours d'opérations commerciales normales, pour le produit similaire destiné à la consommation dans le pays exportateur. »

³³ Le prix prédateur est défini par la Cour de cassation française comme étant le prix de vente unitaire d'un produit inférieur au coût variable unitaire de celui-ci (Cass.com.4-2-1997 : RJDA 5/97 n°663)

³⁴ Les articles 7 et 10 de la loi relative à la défense contre les pratiques déloyales à l'importation prévoient clairement le rôle du ministre chargé du commerce et de la branche de production nationale dans le déclenchement de la procédure :

Art.7 une enquête visant à déterminer l'existence, le degré, et l'effet de tout dumping prétendu ou de toute subvention alléguée n'est ouverte par le ministre chargé du commerce que sur plainte présentée par écrit par la branche de production nationale ou en son nom, sauf dans les circonstances visées à l'article 10.

Art. 10. le ministre chargé du commerce peut dans des circonstances exceptionnelles, décider d'ouvrir une enquête sans être saisi d'une demande écrite présentée par la branche de production nationale concernée ou en son nom, lorsqu'il est en possession d'éléments de preuve suffisants de l'existence d'un dumping ou d'une subvention, d'un dommage et d'un lien de causalité tel que prévu à l'article 7 pour justifier l'ouverture d'une enquête.