Données du franchisé : comment y accéder et comment les utiliser ?

Jean-Baptiste Gouache (Avocat – Associé)
Membre du collège des experts de la Fédération Française de la Franchise

Jessica Mansuy (Avocat)

Les données collectées ou produites par le franchisé jouent un rôle stratégique pour le franchiseur.

Sans ces données, le franchiseur ne peut :

- comprendre son marché,
- analyser la performance de son réseau,
- animer son réseau,
- déceler les difficultés de son franchisé et l'aider à prévenir les contentieux,
- conduire des actions marketing ou commerciales en utilisant le fichier client du franchisé.

Le droit organise la collecte, l'usage et la propriété des données.

En effet, la loi soumet le traitement de données à caractère personnel à des conditions de licéité et le responsable du traitement de ces données à certaines obligations.

Si la collecte donne lieu au traitement d'une base de données mais que le traitement est réalisé par le franchisé, le franchiseur doit être contractuellement autorisé à accéder aux fichiers, à les utiliser, et à les conserver pour tous usages.

A défaut, le promoteur de réseau est susceptible d'engager sa responsabilité pénale, le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données étant puni de 2 ans d'emprisonnement et de 30.000 euros d'amende (**I**).

Par ailleurs, l'utilisation des données du franchisé par le franchiseur peut être constitutive du délit pénal d'abus de confiance, de manœuvres déloyales et ne doit pas permettre une ingérence dans la gestion du franchisé (**II**).

La jurisprudence admet l'existence d'une clientèle appartenant au franchiseur et plus récemment d'une clientèle appartenant au franchisé.

Le Code de la Propriété Intellectuelle organise la protection des droits du producteur de bases de données.

Il est cependant difficile de déterminer qui du franchiseur ou du franchisé est titulaire du droit de producteur de bases de données.

Il convient dès lors de déterminer les droits du franchiseur dans le contrat de franchise (**III**).

I. La collecte des données

La finalité de la loi « Informatique et Liberté » est de concilier la liberté de circulation des données avec le droit au respect de la vie privée, en raison de la généralisation de l'outil informatique, du développement des nouvelles technologies dans le quotidien.

Les informations et les données qui nous concernent font l'objet chaque jour d'opérations de collecte, de transfert, et plus généralement de traitement, que ce soit chez le médecin, lors d'achats de biens et de services, d'octroi de prêts bancaire, au travail, sur Internet.

La loi « Informatique et Liberté » s'applique tant à l'égard des franchiseurs que des franchisés dès lors qu'ils effectuent un traitement de données à caractère personnel.

A. Champ d'application et notions

1. *Champ d'application de la loi « Informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004*

a) Principe

La loi s'applique aux :

- traitements automatisés de données à caractère personnel : c'est-à-dire, aujourd'hui, un traitement informatisé de données à caractère personnel,
- traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers : c'est-à-dire, un traitement manuel ou manuscrit dès lors que les données sont appelées à figurer dans des fichiers.

b) Exception

La loi ne s'applique pas aux :

- traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles (art. 2),
- copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises (art.4).

2. *Notions*

a) Notion de donnée à caractère personnel

La définition est particulièrement large.

L'article 2 de la loi définit une donnée à caractère personnel comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son*

identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

Une donnée à caractère personnel est une donnée qui permet d'identifier directement ou indirectement une personne physique.

b) Notion de traitement de données à caractère personnel

L'article 2 de la loi définit un traitement de données à caractère personnel comme « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* » .

La loi s'applique à toute manipulation ou opération portant sur les données personnelles.

c) Notion de fichier de données à caractère personnel

L'article 2 de la loi donne une définition large d'un fichier de données à caractère personnel comme « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés*».

B. Régime du traitement de données à caractère personnel

1. <u>Personnes soumises à la loi</u>

a) Le responsable du traitement et le sous-traitant : définitions

i. Responsable du traitement

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, « *la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* » (art.3).

Le responsable du traitement a un rôle fondamental dans la mesure où c'est sur lui que pèse l'ensemble des exigences prévues par la loi et qui encourt les sanctions en cas de violation de ces dispositions.

La loi s'applique au responsable :

- établi sur le territoire français,
- sans être établi sur le territoire français ou sur celui d'un autre état membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français (à l'exception des traitements utilisés qu'à des fins de transit).

ii. Sous-traitant du traitement

La loi s'applique également à toute personne traitant des données à caractère personnel pour le compte du responsable du traitement (art.35).

La loi précise que les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité.

Le contrat liant le sous-traitant au responsable du traitement doit ainsi comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoir que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

b) En droit de la franchise : qui du franchiseur ou du franchisé est le responsable du traitement de données

i. Franchisé sous-traitant du franchiseur

Si le franchisé est sous-traitant du franchiseur, la collecte des données interviendra par son intermédiaire mais seul le franchiseur sera considéré comme le responsable du traitement au sens de la loi.

Dans cette hypothèse, le contrat de franchise devra comprendre une clause prévoyant :

- l'obligation pour le franchisé de n'agir que sur instructions du franchiseur,
- l'obligation pour le franchisé de mettre en place des mesures afin d'assurer la sécurité ainsi que la confidentialité des données.

Il est également recommandé de prévoir l'obligation pour le franchisé de supprimer les données du fichier à l'issue du contrat.

ii. Franchiseur et franchisé responsables de leurs propres traitements

Dans cette hypothèse, le franchiseur et le franchisé ont chacun avoir leur propre base de données.

Ils seront ainsi responsables de leur propre traitement.

La base du franchisé pourra également venir s'intégrer à la base générale du franchiseur.

Le franchiseur devra déclarer sa base globale à la CNIL et le franchisé devra déclarer sa propre base et le fait qu'elle alimente la base du franchiseur.

En pratique : les parties devront organiser la gestion des données dans le contrat de franchise et prévoir chacune leur obligation au regard de la collecte et de la transmission des données.

Il conviendra également de prévoir dans le contrat de franchise une clause permettant d'organiser l'accès et l'utilisation par le franchiseur des données et des fichiers du franchisé à toutes fins et à titre gratuit.

c) Cession des données à des tiers

Les contrats d'échange, de location ou cession de fichiers privés à des tiers à des fins commerciales sont autorisés à condition :

- d'informer les personnes concernées de ces opérations,
- de leur donner le droit de s'y opposer,
- que ce droit d'opposition soit effectif.

Il est possible de prévoir ce droit dès le départ : la déclaration devra prévoir dans ce cas que les données peuvent être mises à disposition de sociétés tierces.

Le fait que les données soient cédées entre sociétés d'un même groupe est indifférent, le droit d'opposition demeure (Décisions de la CNIL « Vivendi Canal + » n° 01-040 du 28 juin 2001).

La finalité devra être la même que celle contenue dans la déclaration.

En pratique, il existe des risques :

- pour le cessionnaire si les données mises à disposition ont été collectées par le cédant de manière déloyale ou pour une autre finalité,
- pour le cédant en cas de détournement de finalité celui-ci pouvant être responsable pour traitement non conforme.

Le contrat de cession devra donc prévoir les garanties nécessaires.

2. Conditions de licéité du traitement de données personnelles

a) Conditions propres aux données

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont à cinq (5) conditions cumulatives :

- les données sont collectées et traitées de manière loyale et licite. En pratique, cette condition correspond essentiellement au respect par le responsable du traitement de son obligation d'information : est déloyal tout traitement effectué à l'insu des intéressés. Le non-respect de cette condition peut faire l'objet de sanctions administratives (amendes) et pénales cinq (5) ans d'emprisonnement et 300.000 euros d'amendes (art. 226-18 du Code pénal).

- elles sont collectées pour des finalités déterminées, explicites et légitimes, leur traitement ultérieur ne pouvant être incompatible avec ces finalités, sauf s'il est poursuivi à des fins statistiques, scientifiques ou historiques, sous réserves qu'ils respectent les autres dispositions de la loi et qu'ils ne soient pas utilisés pour prendre des décisions à l'égard des personnes concernées. Tout détournement de finalité est passible de cinq (5) ans d'emprisonnement et de

300.000 euros d'amende (art. 226-21 du Code pénal) et susceptible de sanctions administratives (avertissements, interruption de traitement, amendes).

Exemples : opérations relatives à la gestion des clients (pour les contrats, commandes, livraisons factures, programme de fidélité), opérations relatives à la prospection (réalisation d'opérations de sollicitation), élaboration de statistiques, organisation de jeux-concours, gestion des dossiers contentieux et des impayés, la gestion des salariés.

- elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieur. Le non-respect de ce principe de proportionnalité peut donner lieu à des sanctions administratives.

- elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées. Le fait pour un responsable de traitement de ne pas procéder à la rectification, à la mise à jour, au verrouillage ou à l'effacement de données appartenant à une personne qui en a fait la demande est puni d'une amende de 1.500 euros et peut faire l'objet de sanctions administratives (avertissements, amendes).

- elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. Les données doivent donc être supprimées des fichiers au terme de la durée déclarée. Toute conservation des données pour une durée supérieure à celle déclarée est punie de cinq (5) ans d'emprisonnement et de 300.000 euros d'amende et peut faire l'objet de sanctions administratives.

  En pratique, quelle est la durée de conservation ?

  - lorsque les données sont celles d'un prospect : 3 ans
  - lorsque les données sont celles d'un client existant : durée de la relation contractuelle dans les limites de la prescription légale : 5 ans.

  La loi prévoit cependant que les données peuvent être conservées au-delà de la durée nécessaire au traitement :

  - en vue d'être traitées à des fins historiques, statistiques ou scientifiques,
  - pour des fins autres que historiques, statistiques ou scientifiques à condition que :
    - soit le responsable du traitement a obtenu l'accord exprès de la personne concernée,
    - soit une autorisation de la CNIL a été obtenue,
    - soit, pour les données dites sensibles, si l'intérêt public l'impose et que le traitement a été autorisé par la CNIL ou par décret en Conseil d'état après avis publié et motivé de la Commission.
  - lorsqu'elles sont mises en œuvre aux seules fins de journalisme ou d'expression littéraire ou artistique.

b) Condition relative au consentement préalable de la personne concernée

Principe : le responsable d'un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée avant tout traitement.

En pratique : le régime de l'opt in/l'opt out

Deux procédés permettent d'obtenir le consentement de la personne concernée par le traitement :

- l'opt in : la personne va donner son consentement explicite pour que ses données soient ultérieurement utilisées à des fins commerciales en cochant une case.

- l'opt out : la personne qui reçoit un message commercial a la possibilité de s'opposer à ce que ces données soient utilisées à des fins commerciales en cliquant sur un lien de désinscription directement accessibles sur les messages commerciaux ou en cochant une case pour ne pas recevoir de messages ultérieurs.

Dérogation : le responsable du traitement n'est pas tenu d'obtenir le consentement préalable de la personne concernée dans cinq (5) hypothèses :

- lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (ex : obligations déclaratives pesant sur l'employeur au titre de la réglementation fiscale ou sociale),

- lorsque le traitement mis en œuvre tient à la sauvegarde de la vie de la personne concernée,

- lorsque le traitement est nécessaire à l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement (fichiers de police ou justice),

- lorsque le traitement est nécessaire à l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci.

  Exemple :
  - la collecte de données dans le cadre de formulaires bancaires que doit remplir la personne demandant l'ouverture d'un compte.
  - collecte de l'adresse postale pour les besoins de la livraison
  - coordonnées bancaires, pour les nécessités du paiement d'un achat comme du versement d'un salaire
  - individu sollicite un vendeur en vue de lui adresser une offre de produits. Sont traitées à cette occasion les coordonnées de la personne, pour une durée devant toutefois rester limitée
  - demande de devis pour une assurance-automobile, l'assureur étant amené dans ce cas à recueillir des informations, par exemple, sur la date de mise en circulation du véhicule

- lorsque le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

c) Condition relative à la nature des données personnelles traitées

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

Dérogation : Possibilité de déroger à ce principe si la finalité du traitement l'exige et dans certains cas limitativement énumérés :

- les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée ;
- les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
- les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :
    - pour les seules données sensibles correspondant à l'objet de ladite association ou dudit organisme ;
    - sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;
    - et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
- les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;
- les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;
- les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels ;
- les traitements nécessaires à la recherche dans le domaine de la santé.

L'interdiction peut être en outre écartée si :

- les données personnelles traitées sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation,
- si les traitements sont justifiés par l'intérêt public.

d) Condition relative au transfert des données vers un Etat non membre de la Communauté européenne

Définition : Le transfert de données à caractère personnel se définit comme la communication, la copie ou le déplacement de données par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex. d'un disque dur d'ordinateur à un serveur) depuis le territoire européen vers un ou des pays ni membres de l'Union européenne, ni membres de l'Espace économique européen.

Exemples : Les données des salariés d'une multinationale sont centralisées par la société mère située aux Etats-Unis. Les données personnelles des salariés français font donc l'objet d'un transfert vers les Etats-Unis. Les données des clients sont transférées par un Master Franchisé ou une filiale française vers le franchiseur situé aux Etats-Unis. Les données personnelles des clients français font donc l'objet d'un transfert vers les Etats-Unis.

Principe : Les données ne peuvent être transférées vers un Etat non membre de la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. La CNIL peut interdire le transfert de données si un niveau de protection suffisant n'est pas assuré dans l'Etat destinataire.

Dérogation : Un transfert des données est possible si la personne concernée a consenti expressément au transfert ou si le transfert est nécessaire :

- à la sauvegarde de la vie de cette personne,
- à la sauvegarde de l'intérêt public,
- au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice,
- à la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime,
- à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci (exemple d'une commande transférée par le responsable du traitement à un fournisseur situé hors Communauté européenne),
- à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

La CNIL peut également autoriser le transfert lorsque le traitement garantit un niveau de protection suffisant, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

En pratique : En cas de transfert de données hors de la Communauté européenne, il est nécessaire de sécuriser un tel transfert :

- par la mise en place d'un contrat de transfert de données selon le modèle de contrat établi par la Commission européenne,

  La Commission européenne propose 2 modèles de contrat disponibles sur le site de la CNIL :

- un encadrant le transfert de données entre 2 responsables de traitement,
- un encadrant pour le transfert de données entre 1 responsable et 1 sous-traitant.

Ces modèles de contrat prévoient, à titre d'exemple, les obligations l'exportateur et de l'importateur :

- l'exportateur des données s'engage à avoir respecté et à continuer à respecter les dispositions applicables à la collecte de données
- l'importateur de données s'engage à assurer la sécurité et la confidentialité des données qui lui sont transférées.

- par la vérification du destinataire des données au Safe Harbor (pour un transfert aux Etats-Unis).

Définition : Il s'agit d'un ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne.

Ces principes, négociés entre les autorités américaines et la Commission européenne en 2001, sont essentiellement basés sur ceux de la Directive 95/46 du 24 octobre 1995 :

- information des personnes,
- possibilité accordée à la personne concernée de s'opposer à un transfert ou à une utilisation des données pour des finalités différentes,
- consentement explicite pour les données sensibles,
- droit d'accès et de rectification,
- sécurité des données.

En pratique :

Vous pouvez trouver la liste des entreprises ayant adhéré aux principes du Safe Harbor sur le site internet du Département du Commerce américain.

Vous devez vérifier sur ce site que l'adhésion de l'entreprise est bien à jour (« current ») et qu'elle couvre bien le transfert envisagé (ex : catégorie de données traitées).

L'adhésion au Safe Harbor permettant de garantir un niveau de protection suffisant au transfert de données en provenance de l'Union européenne vers une entreprise située aux Etats-Unis, ce transfert n'est pas soumis à une décision d'autorisation de la CNIL. La formalité que vous devez accomplir est celle qui est applicable au traitement principal (déclaration normale, demande d'autorisation ou demande d'avis). Le transfert de données vers les Etats-Unis et la garantie qui encadre le transfert, ici le Safe Harbor, devront être mentionnés dans le formulaire.

3. ***Obligations du responsable du traitement***

a) Obligation de déclaration

i. Données soumises à déclaration normale

Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la Commission nationale de l'informatique et des libertés (CNIL).

La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

La commission délivra sans délai un récépissé, le cas échéant, par voie électronique.

Le demandeur peut mettre en œuvre le traitement dès réception de ce récépissé. Il n'est exonéré d'aucune de ses responsabilités.

ii. Données soumises à déclaration simplifiée

Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, et correspondant à une de normes publiées par la CNIL, le responsable du traitement peut effectuer une déclaration simplifiée.

Exemples :
Norme simplifiée n° 48 : Délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects
Norme simplifiée n° 46 : Délibération n°2005-002 du 13 janvier 2005 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels

iii. Dispense de déclaration

La CNIL a défini des catégories de traitements qui sont dispensés de déclaration (ex : les opérations courantes de l'entreprise (comptabilité, fichiers de fournisseurs, gestion des paies, registre unique du personnel, déclarations sociales obligatoires, etc.), sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (blog), traitements automatisés de données à caractère personnel mis en œuvre par des organismes à but non lucratif).

iv. Exonération de déclaration

Sont exonérés de déclaration, les traitements pour lequel le responsable a désigné un correspondant à la protection des données chargé d'assurer de manière indépendante le respect des obligations prévues par la loi, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.

b) Obligation de solliciter une autorisation préalable

Une autorisation préalable de la CNIL est obligatoire pour les traitements qui présentent des risques particuliers d'atteinte aux droits et aux libertés.

Il en est ainsi des :

- traitements statistiques réalisés par l'INSEE ou l'un des services statistiques ministériels,
- traitements portant sur des données sensibles, lorsqu'elles sont anonymisées ou justifiées par l'intérêt public,
- traitements portant sur les données génétiques, sur les données biométriques nécessaires au contrôle de l'identité des personnes,
- traitements automatisés ou non des données relatives aux infractions, condamnations ou mesures de sûreté.

La demande d'autorisation fait l'objet d'un examen approfondi de la part de la CNIL, qui a 2 mois pour se prononcer à compter de la réception de la demande. Si la CNIL ne s'est pas prononcée dans ce délai, la demande d'autorisation est réputée rejetée.

Le non-accomplissement des formalités auprès de la CNIL est sanctionné de cinq (5) ans d'emprisonnement et de 300.000 euros d'amende (art.226-16 du Code pénal).

c) Obligation d'information

Certaines informations exigées par la loi doivent être portées à la connaissance de la personne concernée par le traitement de données :

- l'identité du responsable du traitement ou de son représentant ;
- la finalité du traitement de données ;
- le caractère obligatoire ou facultatif des réponses ;
- les conséquences d'un défaut de réponse ;
- les destinataires ou catégories de destinataires des données ;
- ses droits d'accès, d'interrogation, d'opposition de rectification et de suppression ;
- le transfert des données envisagées dans un état non membre de la Communauté européenne.

Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1.500 euros par infraction constatée et 3.000 euros en cas de récidive (art. 131-13 du Code pénal).

d) Obligation de sécurité et de confidentialité

i. Obligation de sécurité

Le responsable du traitement de données personnelles doit prendre toutes précautions utiles pour assurer la sécurité des données adaptées à la nature des données et aux risques présentés par le traitement (sécurité des locaux et des systèmes d'information) pour empêcher que les fichiers soient endommagés, altérés, détruites ou que des tiers non autorisés y aient accès.

En pratique :

Il devra en effet assurer la sécurité des données adaptées à la nature des données et aux risques présentés par le traitement (sécurité des locaux et des systèmes d'information) pour empêcher que les fichiers soient endommagés, altérés, détruites ou que des tiers non autorisés y aient accès.

Pour sécuriser les locaux : il devra installer des alarmes et retreindre l'accès aux locaux susceptibles d'héberger du matériel contenant des données au moyen de portes verrouillées ou sas d'accès pour les équipements plus critiques.

Pour les utilisateurs, il :
- devra s'assurer que chaque salarié n'a accès qu'aux données nécessaires pour sa mission avec identifiant et un mot de passe,
- mettre en place un système de définition de niveaux d'habilitation d'un utilisateur dans le système et d'un moyen de contrôle des permissions d'accès aux données,
- sensibiliser les utilisateurs au moyen par exemple d'une charte informatique annexée au règlement intérieur.

Pour sécuriser les postes de travail, il devra :

- limiter le nombre de tentatives d'accès à un compte. En fonction du contexte, ce nombre peut varier entre trois et dix. Lorsque la limite est atteinte, il est préférable de bloquer la possibilité d'authentification à ce compte temporairement ou jusqu'à l'intervention d'un administrateur du système ;
- installer un «pare-feu» (firewall) logiciel, et limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail ;
- utiliser des antivirus régulièrement mis à jour ;
- prévoir une procédure de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.
- prévoir d'afficher, lors de la connexion à un compte, les dates et heures de la dernière connexion.

Pour sécuriser l'informatique mobile (smartphones, clés usb, ordinateurs portables), il devra prévoir des moyens de chiffrement pour les espaces de stockage des matériels informatiques mobiles.

Il devra enfin :

- Effectuer des sauvegardes fréquentes pour éviter la perte d'information et prévoir de stocker les supports de sauvegarde sur un site extérieur.

- Prévoir un système de journalisation des activités des utilisateurs, des anomalies et des évènements liés à la sécurité.

- Sécuriser le réseau et le serveur.

- Mettre en place des détecteurs de fumées et extincteurs et surélever les matériels informatiques en cas d'inondation.

- Prévoir un engagement de confidentialité dans contrat de travail.

Le non-respect de l'obligation de sécurité est sanctionné de cinq (5) ans d'emprisonnement et de 300.000 euros d'amende (art. 226-17 du Code pénal).

ii. Obligation de confidentialité

Le responsable du traitement est également tenu d'assurer la confidentialité des données. Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et les tiers autorisés qui détiennent une autorisation spéciale et ponctuelle (ex : police, services des impôts).

La communication des données à des personnes non-autorisées est punie de cinq (5) ans d'emprisonnement et de 300.000 euros d'amende. Par ailleurs, la divulgation d'informations commise par imprudence ou négligence est punie de trois (3) ans d'emprisonnement et de 100.000 euros d'amende (art.226-22 du Code pénal).

C. Les sanctions pénales encourues

1. Sanction spécifique à la loi « Informatique et Liberté »

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalable à leur mise en œuvre prévues par la loi est puni de cinq (5) ans d'emprisonnement et de 300.000 euros d'amendes. (Art. 226-16)

2. Le délit d'intrusion ou de maintien volontaire dans un système de traitement automatisé de données

Le fait pour un franchiseur de s'introduire sans autorisation dans le système de traitement automatisé de données utilisé par le franchisé constitue un délit pénal.

a) Définition

L'article 323-1, alinéa 1er du Code Pénal incrimine « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ».

L'accès frauduleux « *vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication* ». (CA Paris, 5 avril 1994 JCP E 1995, I, 461, obs. F. Vivant et C. Le Stanc).

Ex : l'ancien salarié qui accède frauduleusement dans le système informatique de son ancien employeur à l'aide de codes d'accès qui lui avaient été remis lors de son embauche constitue le délit *(CA Paris, 27 mars 2002 : JurisData n° 2002-180229)*

Le maintien frauduleux :

- la personne est habilitée à accéder au système de traitement automatisé de données, mais réalise des opérations par la suite qui ne le sont pas (ex : une personne procède, au moyen de vingt-cinq ordinateurs, à la copie de l'annuaire électronique de France Télécom afin de le

revendre à une clientèle spécialisée ((*T. corr. Brest, 14 mars 1995 : LPA 28 juin 1995, n° 77, note M.-G. Choisy)*

- la personne accède par hasard, erreur ou inadvertance, et se maintien volontairement dans le système par la suite, tout en sachant que celui-ci est interdit (l'utilisation pendant plus de deux ans d'un code permettant l'accès à une base de données accessibles aux seules personnes autorisées, alors que ce code a été remis à un salarié pour sa période d'essai" *(Cass. crim., 3 oct. 2007, n° 07-81.045)*

Système de traitement automatisé de données : le Code pénal ne donne pas de définition.

Une définition avait été proposée par le Sénat lors des travaux préparatoires à l'adoption de la loi *Godfrain (L. n° 88-19, 5 janv. 1988, préc.)* mais n'a pas été retenue par l'Assemblée nationale « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés* ».

Cette définition comporte donc deux (2) caractéristiques :

- *Un ensemble composé* d'éléments de nature diverse (unités de traitement, mémoires, logiciels, données, organes d'entrées et sorties, liaisons) dont les relations entre eux pouvaient résulter de la recherche d'un résultat déterminé (le traitement de données) ;
- *Un ensemble protégé* par des dispositifs de sécurité mais la jurisprudence ne subordonne pas l'application de l'article 323-1 à l'existence d'un dispositif de sécurité quelconque (*Cass. crim., 3 oct. 2007 : JurisData n° 2007-040853)*

Ex : le système carte bleue est un système de traitement automatisé de données dès lors que les terminaux de paiement sont conçus pour permettre de recevoir des paiements dans le cadre du réseau CB, qu'ils font l'objet d'une procédure d'agrément et de qualification pour répondre aux spécificités techniques et fonctionnelles "carte bleue", et qu'ils vérifient lors d'une transaction l'authenticité de la carte en effectuant un calcul de données sur celle-ci. (*TGI Paris, 25 février 2000, D. affaires 2000, p. 219, obs. X. Delpech).*

Le traitement automatisé se définit comme *"l'ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et d'une façon générale leur exploitation".*

b) Sanction

Le fait d'accéder ou se de maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux (2) ans d'emprisonnement et de 30 000 euros d'amende.

La peine est de trois (3) ans d'emprisonnement et de 45 000 euros d'amende lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système.

La peine est portée à cinq (5) ans d'emprisonnement et à 75 000 euros d'amende lorsque les infractions prévues ci-dessus ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat.

D. Projet de règlement européen sur la protection des données

Le 25 janvier 2012, la Commission européenne a rendu public un projet de règlement relatif à la protection des données à caractère personnel, qui refond l'ensemble du cadre juridique européen issu de la directive du 24 octobre1995.

Le projet a été adopté en première lecture par le Parlement européen le 12 mars 2014.

On attend la position du Conseil de l'UE qui devait être prévue pour juin 2014 et les négociations entre le Parlement et les gouvernements nationaux au Conseil qui devaient débiter en juillet 2014 pour un accord automne 2014. Mais il y a du retard.

Une fois définitivement adopté, il sera directement applicable dans tous les Etats membres 2 ans après sa publication.

Simplification : la loi applicable sera déterminé en fonction du lieu d'implantation de l'établissement principal du responsable du traitement combiné à système guichet unique : le responsable sera ainsi tenu de s'adresser qu'à une seule et même autorité nationale de protection de données à caractère personnel pour l'ensemble des traitements qu'il mette en œuvre.

Il sera également créé un comité européen de protection de données pour assurer l'homogénéité des traitements dans les différents pays.

Plus de sévérité :

- Le sous-traitant pourra directement engager sa responsabilité et il sera tenu d'une obligation renforcée en matière de sécurité et de confidentialité.
- Le responsable du traitement devra apporter la preuve de son respect de l'ensemble des dispositions du règlement.
- Avant de communiquer les données personnelles de citoyens européens à un pays tiers, toute entreprise (par exemple un moteur de recherche, un réseau social ou un fournisseur de services d'informatique en nuage) serait tenue de demander une autorisation préalable à une autorité nationale de protection des données dans l'UE. Les entreprises devraient également informer la personne concernée d'une telle demande.
- Les entreprises qui violent les règles devraient être sanctionnées par des amendes allant jusqu'à 100 millions d'euros ou équivalant à 5% de leur chiffre d'affaires annuel mondial, en fonction du montant le plus élevé.
- Protection renforcée sur Internet : droit à l'effacement des données, de nouvelles limites au "profilage" (une pratique utilisée pour analyser ou prédire les performances professionnelles d'une personne, sa situation économique, sa localisation, etc.), ou encore l'obligation d'utiliser un langage clair et simple pour expliquer les politiques sur le droit à la vie privée. Tout fournisseur de services Internet qui souhaite traiter des données à caractère personnel sera d'abord tenu d'obtenir le consentement libre, informé et explicite de la personne concernée.

Nouveau critère : la collecte devra être loyale, licite et « transparente ».

II. L'usage des données

Le franchiseur peut vouloir utiliser les données du franchisé en dehors de ce qui est prévu contractuellement. L'accès ou l'utilisation des données du franchisé par le franchiseur, sans son autorisation, peut constituer un délit pénal (**A**.). Il peut également donner lieu à des contentieux en matière de concurrence déloyale (**B**.). Enfin, l'usage des données du franchisé ne doivent pas aboutir à une ingérence dans la gestion du franchisé (**C**.).

A. Le détournement de fichiers clientèle : délit pénal d'abus de confiance

Le détournement de fichiers clients du franchisé par le franchiseur expose également ce dernier au délit d'abus de confiance.

1. Définition et sanction du délit pénal d'abus de confiance

L'article 314-1 du Code pénal définit l'abus de confiance comme « *le fait, par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé* ».

L'abus de confiance est puni de trois (3) ans d'emprisonnement et de 375.000 euros d'amende.

2. Application du délit d'abus de confiance au détournement d'informations relatives à la clientèle

Le 16 novembre 2011, la chambre criminelle de la Cour de cassation a jugé que le délit pénal de l'abus de confiance, prévu et réprimé par les dispositions de l'article 314-1 du code pénal, s'appliquait aussi au détournement d'informations relatives à la clientèle :

> « *Vu l'article 314-1 du code pénal ;*
>
> *Attendu que les dispositions de ce texte s'appliquent à un bien quelconque, susceptible d'appropriation ;*
>
> *Mais attendu que les informations relatives à la clientèle constituent un bien susceptible d'être détourné […]* » (Cass. crim. 16 novembre 2011, n° de pourvoi 10-87866).

En l'espèce, une société reprochait à un de ses directeurs régionaux d'avoir détourné sa clientèle pour le compte d'une société concurrente, gérée par un de ses anciens salariés, en utilisant les renseignements dont il était dépositaire.

B. Etat de la jurisprudence en matière de concurrence déloyale

Le détournement de fichiers-clients a donné lieu à quelques arrêts.

Pour une meilleure compréhension de cette jurisprudence, il convient de distinguer les litiges :

- où une clause était prévue au contrat concernant l'utilisation des fichiers clients (**1**.)
- où une telle clause n'était pas prévue (**2**.)

1. Actions fondées sur l'existence d'une clause prévue au contrat concernant l'utilisation des fichiers clients

Il convient d'évoquer préalablement les cas d'espèce où une clause était prévue au bénéfice du franchisé (**a)** avant d'aborder les litiges où une clause était prévue au bénéfice du franchiseur (**b**.).

a) Clause prévoyant que les fichiers sont la propriété du franchisé

En présence d'une clause prévoyant que le fichier est la propriété exclusive du franchisé, la jurisprudence retient la qualification d'actes de concurrence déloyale en cas de détournement par le franchiseur du fichier-clients appartenant au franchisé.

- CA Paris, 24 janv. 2002, Société Audika, BRDA 2002, 8, n° 18 : Est condamné pour concurrence déloyale, un franchiseur qui avait détourné le fichier-clientèle d'un franchisé, postérieurement à la rupture du contrat, au mépris d'une clause prévoyant que ce fichier était la propriété exclusive du franchisé. Dans cette espèce, le franchiseur avait adressé des courriers aux clients du franchisé leur indiquant les nouveaux correspondants du franchiseur.

- CA Douai, 11 sept. 2008, n°07/04112 : Le fait d'adresser une invitation à des ventes privées à une cliente alors que le franchisé n'avait autorisé l'utilisation du fichier-clients que dans le cadre de son activité de vente à distance, constitue une faute de la part du franchiseur qui a indûment tiré profit de l'exploitation d'une clientèle dont il n'avait pas la propriété.

Ainsi, en présence d'une clause prévue au contrat de franchise limitant l'usage des fichiers au franchisé, le franchiseur ne peut, après la rupture du contrat, utiliser lesdits fichiers.

b) Clause prévoyant que les fichiers sont la propriété du franchiseur

La jurisprudence considère que le franchiseur ne commet pas de faute en adressant un courrier aux clients du franchisé après la cessation du contrat dès lors que la constitution du fichier-clients par le franchiseur était prévue au contrat de franchise et que le franchisé avait accepté les dispositions contractuelles relatives à la constitution de ce fichier.

CA Rennes, 22 janvier 2008, n°06/07220 : La Cour d'appel de Rennes a jugé que :

> - n'était « *pas critiquable le fait de donner une information objective* » et que l'utilisation d'un bon de réduction ne pouvait concerner, par hypothèse, que des clients attachés aux produits de la marque et donc au franchiseur ;
>
> - « *la constitution par Yves Rocher d'un fichier client à partir des achats de ses produits, même effectués au centre de beauté de sa franchisée, ne peut lui être non plus reproché compte tenu de l'objet même de la franchise, qui concerne la distribution à titre exclusif de produits de sa marque. Les premiers juges ont en outre justement souligné que la constitution d'un tel fichier découlait des dispositions contractuelles relatives notamment au système informatique et aux opérations publicitaires par publipostage initiées par le franchiseur, et avaient ainsi été acceptées par la franchisée* ».

Dans cette affaire, il était reproché à la société Yves Rocher d'avoir envoyé aux clients du centre de beauté du franchisé, un courrier les informant de sa prochaine fermeture et des coordonnées des centres Yves Rocher à proximité et leur offrant un chèque-cadeau de bienvenue.

Il est intéressant de noter que dans cette espèce, la Cour a considéré que la constitution par le franchiseur d'un fichier-clients à partir des achats effectués sur le point de vente de son franchisé ne pouvait lui être reprochée dès lors que le contrat de franchise comporte une clause de la distribution exclusive des produits de sa marque.

Ainsi, le franchiseur serait-il autorisé à utiliser le fichier clients du franchisé dès lors que ces fichiers concernent les produits de sa marque et que le franchisé a accepté la constitution, par le franchiseur, d'un tel fichier.

Le contrat a donc intérêt à prévoir l'usage non limité des données collectées par le franchisé et entrées par celui-ci dans le logiciel prescrit par le franchiseur.

2. Actions en l'absence de clause au contrat concernant l'utilisation des fichiers clients

Il convient de distinguer les cas d'espèce où les fichiers appartenaient au franchisé (**i**.) avant d'aborder les litiges où les fichiers appartenaient au franchiseur (**ii**.).

A la lecture de ces arrêts : on constate que la question de la propriété du fichier rejoint globalement la question de la propriété de la clientèle.

a) Fichier clients appartenant au franchisé

Lorsqu'aucune clause n'est prévue au contrat concernant l'utilisation des fichiers-clients, la jurisprudence a tendance à protéger les données du franchisé en cas de détournement de clientèle par le franchiseur/ou pour prévenir le risque de détournement de clientèle par ce dernier.

- CA Paris, 29 Avril 2014, n°13/04683 – n°13/04676 : Aux termes de deux (2) arrêts, la Cour d'appel de PARIS a confirmé deux (2) ordonnances de référé ayant jugé que l'accès par le franchiseur aux données nominatives des clients du franchisé, via le logiciel référencé exclusif, constituait un trouble manifestement illicite dès lors que le contrat n'avait pas prévu cette possibilité.
  Dans ces espèces, en application du contrat de franchise, les franchisés devaient mettre en place un logiciel informatique permettant la remontée de données financières du franchisé.

  Il avait par la suite été demandé aux franchisés d'acheter et d'installer un module informatique « *permettant chaque soir de relayer les informations commerciales et financières sur la base informatique du franchiseur* ».

  Les franchisés, considérant qu'il existait un risque de détournement de leur clientèle par le franchiseur dans la mesure où le contrat de franchise permettait au franchiseur d'accéder au fichier clients élaboré par les franchisés pendant la durée du contrat et de conserver une copie de ce fichier clients à l'expiration dudit contrat, avaient saisi le Président du Tribunal de Commerce de Paris pour suspendre l'effet desdites clauses en raison du dommage imminent.

  La Cour d'appel de Paris a ainsi jugé que :

- les parties n'avaient pas convenu, initialement, que le franchiseur pourrait avoir accès aux données personnelles et nominatives des clients du franchisé,
- le logiciel dont l'installation était demandée entrainait la transmission automatisée des données nominatives du fichier clients du franchisé au franchiseur,
- le changement de logiciel conduisait à mettre à disposition du franchiseur un élément essentiel du fonds de commerce du franchisé, avec le risque de détournement de sa clientèle au terme du contrat,
- il en résultait une modification de l'économie du contrat caractérisant un trouble manifestement illicite et un dommage imminent, celui de la perte de propriété des données,
- la mise en place et l'utilisation du module informatique constituait une modification substantielle de l'économie du contrat et créait un déséquilibre manifeste entre les obligations contractuelles respectives des parties,
- il convenait en conséquence de suspendre les clauses litigieuses dans l'attente de la décision du juge du fond saisi de la question de la licéité desdites clauses.

- CA Aix-en-Provence, 14 mars 2013, JurisData n°2013-005765 : Il a été jugé, suite à une cession de fonds de commerce, que constituait un acte de concurrence déloyale ayant pour effet de désorganiser l'entreprise cessionnaire, le détournement du fichier client par le cédant, ce dernier ayant conservé le carnet de réservation du cessionnaire suite à une cession de fonds de commerce. En l'espèce, le simple fait d'avoir conservé le fichier clients est déloyal alors qu'aucun acte effectif de démarchage n'a été prouvé.

La jurisprudence considère cependant usuellement qu'en l'absence de preuve d'utilisation du fichier de la clientèle du franchisé, il ne peut être reproché au franchiseur d'avoir commis des manœuvres déloyales.

- CA Rennes, 12 janv. 2010, n°17, 09/02312 : La Cour d'appel de Rennes a jugé que :
  - la lettre circulaire adressé à la clientèle du franchisé, postérieurement à la cessation du contrat de franchise, afin d'annoncer à cette clientèle que le franchisé avait quitté le réseau, qu'une nouvelle direction allait se mettre en place en Loire-Atlantique et que les contacts devaient désormais être obtenus en composant un nouveau numéro de téléphone, *« revêtait un caractère purement informatif et* ***était exempt de manœuvres déloyales*** »,
  - rien ne démontrait que « *l'envoi de ce courrier circulaire avait été réalisé au moyen d'un fichier de la clientèle [du franchisé] obtenu dans des circonstances reprochables ».*

  Elle a donc confirmé l'ordonnance ayant rejeté les demandes d'interdiction sous astreinte d'entretenir la moindre relation avec sa clientèle et de publication au motif que l'existence du trouble manifestement illicite allégué n'était pas démontré.

- CA Paris, 2 oct. 2014, n° R.G. 12/22621 : la Cour d'appel de Paris a récemment adopté la même position concernant un contrat de concession exclusive.

Elle a en effet jugé que le nouveau concessionnaire étant devenu revendeur du concédant (la société Xerox), il pouvait faire connaître à la clientèle qu'il distribuait désormais les produits Xerox sur le territoire qui lui était contractuellement dévolu et que le fait d'adresser aux clients de l'ancien concessionnaire un courrier annonçant à la fois la résiliation du contrat de concession et sa qualité de revendeur agréé du concédant, n'était pas constitutif d'actes de concurrence déloyale dès lors qu'il ne commettait **ni manœuvre déloyale ni dénigrement**.

Elle a également ajouté que « *rien ne démontrait que [le nouveau concessionnaire] avait utilisé pour ses envois, non son propre fichier, mais un fichier appartenant à [l'ancien concessionnaire] que lui aurait fourni la société Xerox* ».

A contrario, on pourrait se demander si du fait de cet ajout, la Cour n'aurait pas considéré qu'en présence de la preuve de l'utilisation, par le franchiseur, du fichier-clients du franchisé, le fait d'adresser un courrier à la clientèle du franchisé, postérieurement à la cessation du contrat de franchise, afin d'annoncer à cette clientèle que le franchisé a quitté le réseau, pouvait être constitutif de manœuvres déloyales.

b) Fichier clients appartenant au franchiseur

La jurisprudence considère que le fait, pour le franchiseur, de procéder à l'envoi de courriers à la clientèle attachée à sa marque à partir de l'exploitation de son propre fichier, n'était pas constitutif d'un détournement de clientèle.

- CA Rennes, 28 juin 2011, n°270, 10/00903 : L'envoi, grâce à l'exploitation de son propre fichier, de courriers circulaires informant la clientèle consommatrice de produits Yves Rocher de l'ouverture du nouveau centre de beauté ouvert sous l'enseigne Yves Rocher ne saurait constituer une manœuvre destinée à capter la clientèle de son ancien franchisé.

  Le franchisé reprochait en l'espèce à la société Yves Rocher d'avoir détourné sa clientèle par l'exploitation du fichier des clients.

  La Cour a jugé que « *le fait que le franchisé ait pu développer une clientèle locale attachée à son fonds n'exclut pas que le franchiseur a de son côté développé une clientèle nationale attachée à la notoriété de l'enseigne* » et qu'il « *n'était pas discuté que le fichier des clients a été mis en place et exploité par la société Yves Rocher qui ne s'est nullement obligée à l'utiliser en direction des clients de son franchisé après la rupture de relations contractuelles* ».

- Cass. com, 6 mai 2008, n° 06611968 - 06612178 : Un ancien concessionnaire considérait que constituait des actes de concurrence déloyale le fait pour un concédant d'avoir utilisé son fichier clients qu'il s'était attribué illégalement en copie grâce au système informatique qu'il avait mis en place.

  La Cour de cassation a jugé que *« la clientèle constituée par le concessionnaire pour l'exploitation de la marque Peugeot est attachée à cette marque* ».

La jurisprudence considère également que le franchiseur ne commet pas de détournement de la clientèle de son franchisé en utilisant les fichiers de cartes fidélité dans la mesure où les clients titulaires de la carte fidélité sont attachés à l'enseigne du franchiseur.

- CA Chambéry, 2 oct. 2007, JurisData n° 2007-353925 : La Cour d'appel a considéré qu'il résultait des éléments du dossier que le franchisé n'était pas titulaire du fichier de cartes de fidélité détenues par les clients de son magasin et que l'avantage financier offert aux clients du magasin titulaires de la carte de fidélité n'était pas, à terme, supporté par le magasin lui-même mais par la direction d'enseigne Intermarché.

  La Cour en a donc déduit que *« la clientèle du magasin titulaire de la carte de fidélité Intermarché est une clientèle attachée à l'enseigne Intermarché et que la direction d'enseigne Intermarché ne commet aucun détournement de clientèle en utilisant les fichiers des titulaires de cartes de fidélité* ».

Dans ces trois (3) espèces, le détournement de clientèle n'a pas été admis notamment car les juges sont partie du postulat que la clientèle appartenait au franchiseur.

C. L'accès et l'utilisation aux données du franchisé ne doit pas aboutir à une ingérence du franchiseur dans les affaires du franchisé

L'accès aux données du franchisé ne doit pas permettre au franchiseur de s'immiscer dans la gestion du franchisé.

Devant la Cour d'appel de Toulouse, un franchisé a invoqué l'ingérence permanente de son franchiseur dans sa gestion en raison de la seule demande de transmission de fichier clients.

Dans cette espèce, la Cour a cependant rejeté la demande du franchisé dans la mesure où le franchisé n'apportait la preuve du grief allégué, la communication critiquée ayant été sollicitée par un seul message électronique dans le cadre d'un concours auquel le franchisé était libre de ne participer. (CA Toulouse, 12 septembre 2012, n°11/00206).

III. La propriété des données

A. La propriété de la clientèle en droit de la franchise : consécration du principe de possession d'une clientèle propre au franchisé

1. Refus de l'admission d'une clientèle propre aux franchisés

Jusqu'au 27 mars 2002, la jurisprudence considérait que le franchisé ne pouvait bénéficier du statut protecteur des baux commerciaux car il ne disposait pas de clientèle autonome et donc de fonds de commerce.

Dès 1962, la Cour d'appel de Montpellier avait refusé de reconnaître à un franchisé le bénéfice de la propriété commerciale au motif que la clientèle était attirée par la marque du franchiseur (CA Montpellier, 19 janvier 1962, D.1963, jur., p.172, F. Givord).

Aux termes d'un arrêt remarqué du 6 février 1996, la Cour d'appel de Paris aconsidéré que le franchisé ne disposait pas de clientèle propre s'il n'apporte pas la preuve que son activité personnelle ou son droit au bail l'emportait sur la marque dans l'attrait de la clientèle : « *pour qu'un locataire franchisé ou concessionnaire d'une marque soit considéré comme ayant un fonds de commerce en propre, il faut qu'il apporte la preuve de ce qu'il a une clientèle liée à son activité personnelle indépendamment de son attrait en raison de la marque du franchiseur ou du concédant, ou bien, qu'il démontre que l'élément du fonds qu'il apporte, le droit au bail, attire la clientèle de manière telle*

qu'il se prévaut sur la marque » (CA Paris, 6 février 1996, JCP 1997, II, 22818, note B. Boccara, JurisData n°1996-020370).

Le franchisé ne se voyait donc reconnaître que très rarement une clientèle personnelle, la propriété de la clientèle étant reconnue au franchiseur, titulaire de la marque.

2. Reconnaissance de l'autonomie de la clientèle des franchisés

Dans deux (2) arrêts postérieurs, la Cour d'appel de Paris est cependant revenue sur cette position en décidant que le propriétaire d'un fonds de commerce est celui qui assume la charge des risques pour attirer la clientèle, c'est-à-dire la « *perte des investissements qu'il a faits pour l'acquérir, la maintenir et la développer* ». Elle ajoutait également que « *Dans le cas d'une exploitation de fonds après signature d'un accord de franchise, il faut observer que la sanction d'une éventuelle perte de clientèle, voir insuccès total, frappe directement le franchisé au point le cas échéant de mettre en péril l'existence de son fonds de commerce. Dans ce cas de figure, le franchiseur n'est atteint que d'une manière différé et de manière limitée dans le temps […] Qu'il faut voir là la preuve que la clientèle attachée au fonds est celle du franchisé, laquelle est autonome par rapport à celle du franchiseur* ». (CA Paris, 4 octobre 2000, JCP 2001, 11.10467, Note B.Boccara, JurisData n° 2000-126109).

Le 27 mars 2002, la Cour de cassation a consacré le principe d'une clientèle propre au franchisé.

Dans cette espèce, des propriétaires avaient notifié à leur preneur leur refus de renouvellement du bail et de paiement de l'indemnité d'éviction. La Cour d'appel d'Agen avait fait droit à la demande du preneur tendant au paiement d'une indemnité d'éviction au motif qu'il était bien propriétaire d'un fonds de commerce et que les parties avaient reconnu au locataire le bénéfice du statut des baux commerciaux aux termes d'un accord.

Devant la Cour de cassation, les bailleurs contestaient que le franchisé puisse être propriétaire d'un fonds de commerce car il ne démontrait pas avoir développé une clientèle propre indépendante de l'attrait exercé par la marque du franchiseur.

La Cour de cassation décide que le franchisé dispose d'une clientèle propre s'il met en œuvre à ses risques et périls un ensemble de moyens corporels et incorporels pour conquérir une clientèle: « *si une clientèle est au plan national attachée à la notoriété de la marque du franchiseur, la clientèle locale n'existe que par le fait des moyens mis en œuvre par le franchisé, parmi lesquels les éléments corporels de son fonds de commerce, matériel et stock, et l'élément incorporel que constitue le bail, que cette clientèle fait elle-même partie du fonds de commerce du franchisé puisque, même si celui-ci n'est pas le propriétaire de la marque et de l'enseigne mises à sa disposition pendant l'exécution du contrat de franchise, elle est créée par son activité, avec des moyens que, contractant à titre personnel avec ses fournisseurs ou prêteurs de deniers, il met en œuvre à ses risques et périls […]* ». (Cass.3ème civ., 27 mars 2002, Bull. civ. 2002, III, n°77, JurisData n°2002-013175).

La Cour de cassation distingue ainsi l'existence d'une clientèle locale appartenant au franchisé en raison des moyens mis en œuvre par ce dernier et d'une clientèle nationale attachée à la notoriété de la marque du franchiseur.

B. Critères de détermination de la propriété des bases de données

Le Code de la Propriété Intellectuelle organise la protection des droits du producteur de bases de données.

L'article L. 341-1 du Code de la Propriété Intellectuelle défini le producteur d'une base de données comme « *la personne qui prend l'initiative et le risque des investissements correspondants* ».

Le titulaire de la protection organisée par ledit code est donc celui qui prend l'initiative et le risque des investissements correspondants à cette base de données.

Pour bénéficier de la protection de ce régime, les textes exigent cependant que les investissements revêtent certains critères.

Aux termes de l'article L. 341-1 du Code de la Propriété Intellectuelle, le producteur d'une base de données bénéficie en effet *« d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel*. ».

Le producteur de la base de données doit donc attester d'un investissement, financier, matériel et humain (**1**) et qui soit substantiel (**2**).

1. Un investissement financier, matériel et humain

De manière générale, les investissements financier, matériel et humain sont cumulativement consentis lors de l'élaboration d'une base de données.

En pratique, les investissements sont justifiés par :

- le personnel mis en place pour constituer et vérifier la base de données,
- les prestations informatiques exclusivement consacrés à ladite base de données,
- les vérifications et mises à jour permanentes des bases de données.

Aux termes d'un arrêt rendu le 23 mars 2010, la Cour de cassation a jugé que « *la base de données avait été constituée par un apport intellectuel de la société France Télécom, chiffré par l'expert en effort d'investissement de sept cent trois hommes par mois de travail correspondant à 10,6 millions d'euros entre 1992 et 2000* » (Cass., com., 23 mars 2010, n° 08-20427, n°08-21768).

2. Un investissement « substantiel »

L'article L. 341-1 du Code de la Propriété Intellectuelle subordonne la protection des bases de données à la preuve d'un investissement « substantiel ». Ce critère est soumis à l'appréciation des juges du fond.

Les contours de ce critère restent cependant difficiles à définir en raison d'un contentieux encore peu nourri et de décisions de valeurs inégales.

Néanmoins, à la lumière des premiers contentieux, les juges du fond ont dégagé deux (2) critères : les coûts de collecte et de gestion (**a**) et le caractère accessoire ou dérivé de l'activité de développement de la base de données (**b**).

a) Coûts de collecte et de gestion

L'investissement pris en compte par la loi est celui qui a été rendu nécessaire à la constitution, à la vérification ou à la présentation du contenu de la base :

- les investissements liés à la collecte des données : la Cour de Justice de l'Union Européenne indique que la notion d'investissement est liée à l'obtention du contenu de la base de données et indique que cette notion désigne « *les moyens consacrés à la recherche d'éléments existants et à leur rassemblement* » dans ladite base (CJCE, 9 nov. 2004, aff. C-203/02 ; Cass. 1ère civ., 5 mars 2009, Jurisdata n°2009-047354).

- les investissements liés à la vérification des données : la Cour de Justice de l'Union Européenne indique que la notion d'investissement s'entend de « *moyens consacrés, en vue d'assurer la fiabilité de l'information contenue dans ladite base, au contrôle de l'exactitude des éléments recherchés* » lors de la constitution et pendant la période de fonctionnement de la base (CJCE, 9 nov. 2004, aff. C-203/02 ; Cass. 1ère civ., 5 mars 2009, Jurisdata n°2009-047354).

- les investissements liés à la présentation des données : la Cour de Justice de l'Union Européenne indique que *« le rassemblement des données, leur agencement systématique ou méthodique au sein de la base, l'organisation de leur accessibilité individuelle et la vérification de leur exactitude tout au long de la période de fonctionnement de la base* », peuvent nécessiter un investissement substantiel, alors même que la recherche de données et la vérification de leur exactitude au moment de la constitution de la base « *ne requièrent pas, en principe, de la personne qui constitue cette base la mise en œuvre de moyens particuliers puisqu'il s'agit de données qu'elle a créés et qui sont à sa disposition* ». (CJCE, 9 nov. 2004, aff. C-203/02).

La notion d'investissement exclut cependant les investissements liés à la création de données. (CJCE, 9 nov. 2004, aff. C-203/02).

La Cour de cassation a ainsi considéré que les moyens consacrés par le créateur du site pour l'établissement d'annonces immobilières publiées dans différentes éditions du journal Ouest France « *ne correspondaient pas à un investissement lié à la constitution de la base de données dans laquelle elles étaient intégrées mais à la création des éléments constitutifs du contenu de cette base et à des opérations de vérification, purement formelle, pendant cette phase de création* ». (Cass. 1ère civ., 5 mars 2009, Jurisdata n°2009-047354). En l'espèce, l'investissement correspondant à la vérification des données et à leur présentation dans une base faisait défaut. Cette base ne pouvait donc bénéficier de la protection instaurée par l'article L.341-1 du Code de la Propriété Intellectuelle.

Sont également exclus les investissements liés à la vérification au cours de la phase de création d'éléments qui sont par la suite rassemblées dans une base de données.

Par un arrêt rendu le 20 décembre 2013, la Cour d'appel de Paris a ainsi jugé que « *la société Protagoras se doit de rapporter la preuve d'investissements humains et financiers spécifiques qui ne se confondent pas avec ceux qu'elle consacre à la création des éléments constitutifs du contenu de sa base de données et à des opérations de vérification, purement formelle, pendant cette phase de création consistant à les collecter auprès de professionnels et à les diffuser tels que recueillis de ses clients* » et qu'en l'espèce, notamment, « *la gestion des demandes de stages s'analyse en un travail de vérification préalable intervenant dans la phase de création de la liste afférente à l'activité en cause*

et constitue un investissement lié à la création de données et non à la vérification du contenu de la base de données. » (CA Paris, 20 décembre 2013, n° R.G. 12/20260)

b) L'indifférence du caractère accessoire ou dérivé de l'activité de développement de la base de données

La Cour de Justice de l'Union Européenne considère qu'il importe peu que l'activité sous laquelle la protection est demandée soit simplement accessoire : « *la circonstance que la constitution d'une base de données soit liée à l'exercice d'une activité principale dans le cadre de laquelle la personne qui constitue la base est également le créateur d'éléments contenus dans cette base n'exclut pas, en tant que telle, que cette personne puisse revendiquer le bénéfice de la protection par le droit sui generis, à condition qu'elle établisse que l'obtention desdits éléments, leur vérification ou leur présentation, ont donné lieu à un investissement substantiel sur le plan quantitatif ou qualitatif, autonome par rapport aux moyens mis en œuvre pour la création de ces éléments* » (CJCE, 9 nov. 2004, aff. C-203/02).

=>Le producteur de la base de données se voit attribuer un monopole d'exploitation lui permettant d'interdire toute extraction totale ou partielle ainsi que toute utilisation abusive. Il a donc le droit d'interdire l'extraction et la réutilisation de tout ou partie du contenu d'une base de données sur un autre support peu importe le moyen utilisé ou la forme que cela revêt.

Durée de la protection : La protection d'une base de données court à compter de l'achèvement de la fabrication de la base et expire 15 ans après le 1er janvier de l'année civile qui suit celle de l'achèvement

Si la base de données protégée fait l'objet de nouveaux investissements, une nouvelle durée de protection court pendant 15 ans après le 1er janvier de l'année civile suivant celle de ce nouvel investissement.

Sanction : En cas d'atteinte aux droits des producteurs d'une base de données, est prévu une peine de trois ans d'emprisonnement et une amende de 300 000 euros d'amende, les peines étant portées à 5 ans d'emprisonnement et 500 000 euros d'amende en cas de bande organisée.

****

A ce jour, la jurisprudence n'a pas fixé lequel du franchisé ou du franchiseur avait la qualité de producteur de base de données. Cette détermination est casuistique car les investissements sont souvent partagés.

Les données peuvent en effet résulter d'une production conjointe.

C'est notamment le cas pour la publicité nationale et locale ou pour le logiciel.

Exemple pour le logiciel :

Critères	**Qui**	
	Franchiseur	**Franchisé**
Investissements financiers	Logiciel Maintenance du logiciel	Maintenance du logiciel Paiement de la redevance

Investissements matériels	Logiciel	Matériel informatique
Investissements humains	Déplacements sur le lieu de vente pour maintenance du matériel (mise à jour)	Personnel Entrée des données

C. Objectif du contrat de franchise : déterminer les droits du franchiseur sur les données

Afin de pouvoir accéder, utiliser et conserver les données du franchisé en toute légalité, l'insertion de certaines clauses est recommandée dans les contrats de franchise. :

- Reconnaître conventionnellement la qualité de producteur de données au franchisé et autoriser conventionnellement l'accès du franchiseur aux données du franchisé ainsi que la possibilité pour ce dernier d'utiliser les fichiers et données à toutes fins, à titre gratuit pour tenir compte des investissements du franchiseur.

- Autoriser conventionnellement au franchiseur un droit d'usage et d'exploitation desdites données, pour une durée de vingt-cinq (25) années suivant la cessation des effets du contrat, incluant le droit pour le franchiseur de céder ces données, pour tenir compte de la contribution du franchiseur à la notoriété de la marque, qui a permis et facilité la collecte desdites données.

- Prévoir la possibilité pour le franchiseur, en cas de cessation du contrat pour quelque cause que ce soit, d'adresser un courrier à l'ensemble des clients du franchisé pour les informer de la cessation du contrat de franchise.