



## LES ENJEUX CONTRACTUELS DU CLOUD HYBRIDE

### Une réalité technique protéiforme, une définition ISO très large

- Lors du **premier salon Interconnect** organisé par **IBM** à Las Vegas en février 2015 (1), " Big blue " a exposé sa **stratégie** pour le cloud laquelle doit être centrée autour du **cloud hybride**. A suivre les présentations faites à cette occasion, il apparaît que le cloud hybride recouvre techniquement une **réalité hétérogène** recouvrant d'une part le fait d'avoir des données ou applications provenant de l'extérieur, d'autre part la structure technologique de la plateforme cloud, elle-même, permettant de discriminer entre espace dédié ou public, avec une localisation physique, des niveaux de sécurité différents.
- La **multiplicité des formes** concrètes du " cloud hybride " est à l'origine d'une controverse entre les différents prestataires et même entre experts.
- Après un peu plus de **deux ans de travaux** les organismes de **normalisation** UIT-T et ISO ont approuvé trois nouvelles normes (2) dont la norme ISO 17788 laquelle définit le cloud hybride comme un modèle de développement utilisant au moins deux modèles de développement du cloud et permettant entre eux une interopérabilité et une portabilité des données et des applications. Pour un candidat à une offre de cloud hybride, une telle définition ne permet pas de s'engager sereinement.

### La nécessité d'un encadrement contractuel précis

- **Faire référence aux normes ISO** précitées et obtenir la garantie de leur respect durant toute la durée d'exécution du contrat est un minimum. Cependant, cela ne saurait suffire pour sécuriser le candidat à une offre de cloud hybride.
- La clause " **prix** " et généralement l'annexe financière associée doivent faire l'objet d'une attention toute particulière : le coût des services pouvant varier fortement selon le type de service utilisé. Si certains prestataires ne facturent pas le trafic entre différents centres de données dans le cloud hybride, ce n'est pas le cas de tous.
- Les dispositions contractuelles sur la **sécurité**, les **garanties** de performance revêtent un caractère crucial, de même que celles sur la **réversibilité**. A ce titre, compte tenu de la complexité de l'architecture " hybride " envisagée, il est indispensable d'exiger un plan de réversibilité dès la signature du contrat avec mise à jour à intervalle régulier.
- Les **annexes au contrat** et en particulier les annexes techniques et de sécurité doivent également faire l'objet d'un soin particulier. Il importe en effet que l'architecture technique soit particulièrement précise et compréhensible par tout homme de l'art. L'annexe sécurité proposera un vrai **plan d'assurance sécurité** comprenant le PSSI, les plans de continuité et de reprise d'activité.
- Enfin, alors qu'une **norme ISO sur les niveaux de services** (SLA) doit être publiée dans les prochains mois (3), prévoir un mécanisme de benchmark avec possibilité de révision du contrat peut être une sage précaution pour ne pas risquer de se trouver avec un contrat sur des prestations de cloud hybride trop rapidement obsolètes par rapport à l'état de l'art.

### Les enjeux

Une réalité technique protéiforme

Une définition par la norme ISO insuffisante en soi et sans caractère contraignant

(1) <https://www-950.ibm.com>

(2) JTIT n°153-2015

### L'essentiel

Fixer le caractère obligatoire des normes ISO sur le cloud

Convenir de clauses sur la sécurité, les performances et la réversibilité adaptée à l'architecture « cloud hybride ».

S'assurer de leur mise en œuvre par des SLA avec pénalités applicables de plein droit.

(3) Projet de norme ISO 19086.

ERIC LE QUELLENEC

### Un déséquilibre significatif dans les droits et obligations des parties prohibé

- L'abus lors des négociations est sanctionné. Y compris dans les relations entre professionnels, qui sont pourtant gouvernées par le principe de liberté contractuelle.
- Ainsi, « **soumettre ou de tenter de soumettre** un partenaire commercial à des obligations créant un **déséquilibre significatif** dans les droits et obligations des parties » engage la responsabilité de son auteur ([C.com. art. L 442-6](#)).
- Cette **notion** de « déséquilibre significatif » - bien qu'elle ait été jugée conforme tant à la Constitution qu'à la Convention européenne des droits de l'Homme – est souvent considérée comme floue et imprécise.
- Il s'agit pourtant d'une notion bien connue en droit de la consommation, ayant donné lieu à une jurisprudence importante, constituant « un **précédent légal** facilitant la compréhension du texte ». Pour autant, les solutions retenues en la matière ne sont pas purement transposables, par analogie, aux rapports entre professionnels, « les rapports de force [étant] différents de ceux existants entre professionnels et consommateurs » (1).
- Cette qualification relève d'une **appréciation au cas par cas** faite par le juge, qui pourra, au besoin, consulter la Commission d'examen des pratiques commerciales.
- Dans **deux arrêts du 3 mars 2015** (2), la Cour de cassation a précisé que les juges du fond devaient apprécier non seulement les clauses qui leur sont soumises, mais également le contexte dans lequel le contrat est conclu et son économie afin de procéder à une analyse globale et concrète de celui-ci.
- En l'espèce, les critères mis en avant par les juges du fond – validés par la Cour de cassation - pour caractériser un déséquilibre significatif étaient (i) **l'absence de réciprocité** des dispositions contractuelles, (ii) **l'absence de contrepartie**, et (iii) **l'absence de négociation effective** des clauses, aucune suite n'ayant été donnée aux réserves et avenants aux conditions générales d'achat des fournisseurs.

### Les bonnes pratiques à adopter

- Si les décisions intervenues en matière de **déséquilibre significatif** sont limitées et concernent essentiellement le secteur de la grande distribution, ces règles ont déjà trouvé application dans le secteur informatique (3).
- Par ailleurs, force est de constater que la **rupture brutale des relations commerciales** établies, prohibée par l'alinéa 5 du même texte, est désormais très **fréquemment sanctionnée** par les tribunaux, indépendamment du secteur d'activité des parties au contrat.
- Rien ne permet de présager un tel avenir au « déséquilibre significatif ». Pour autant, mieux vaut, dans un but de **sécurité juridique**, tenter de se prémunir contre un tel risque en adoptant les pratiques suivantes :
  - éviter que ses contrats types (CGA et CGV) instaurent un déséquilibre manifeste entre les droits et obligations des parties ;
  - prohiber toute **clause purement potestative**, qui conditionne la naissance ou l'exécution d'une obligation à la volonté discrétionnaire d'une des parties ;
  - assurer une certaine **réciprocité** quant aux modalités et conditions des clauses dites sanction (pénalités, résiliation anticipée) ;
  - permettre une véritable **négociation** des contrats.

### Les enjeux

Assurer, côté client et prestataire, la mise en œuvre effective des dispositions contractuelles.

Eviter les sanctions associées (dommages et intérêts, nullité des clauses concernées, voire du contrat dans son ensemble, cessation de la pratique incriminée, et paiement d'une amende civile).

(1) [CA Paris, Pôle 5, Ch. 4, 1-10-2014](#), RG 2009F00729, Ministre de l'économie / Carrefour

(2) Cass. com, 3-3-2015, [n° 13-27525](#) Ministre de l'économie / Eurauchan, et [n° 14-10907](#) Ministre de l'économie / Provera

(3) Pour une illustration en matière de contrat informatique : [CEPC, Avis n°15-1](#) et [n°15-3](#) du 22-1-2015

### Les conseils

Organiser une revue des contrats types, Conditions Générales d'Achat et de Vente.

Négocier avec soin les clauses « sensibles » en particulier : les conditions financières (révision du prix et conditions de paiement), les pénalités, la responsabilité et la réparation du préjudice, le dédit et la résiliation anticipée.

[JEAN-FRANÇOIS FORGERON](#)

[SOPHIE DUPERRAY](#)

## LA RESPONSABILITE CONTRACTUELLE D'UNE SOCIETE MERE POUR IMMIXTION EN PHASE PRECONTENTIEUSE

### Le principe de l'autonomie d'une personne morale au sein d'un groupe

- Une société n'ayant pu obtenir de son ancienne partenaire commerciale, filiale d'un groupe, le règlement de **factures impayées**, avait assigné en paiement la **société mère** du groupe et avait obtenu en appel la condamnation de cette dernière à lui régler la somme due par la filiale.
- La Cour d'appel avait souverainement apprécié que l'**immixtion de la société mère**, au stade précontentieux, avait été de nature à créer une apparence propre à faire croire qu'elle se substituait à sa filiale et qu'elle devait par là même répondre des dettes de cette dernière. En effet, outre le fait que les deux sociétés du groupe possédaient une adresse électronique similaire, le même domicile ainsi que le même dirigeant, la société mère avait émis une lettre dans laquelle elle répondait à la mise en demeure de régler des factures impayées, adressée par la société cocontractante de sa filiale, ce qui avait convaincu la Cour d'appel que la société mère avait **entretenu une confusion** avec les intérêts de sa filiale.
- Le pourvoi formé par la société mère reprochait à l'arrêt d'appel de l'avoir condamnée à régler les dettes de sa filiale alors qu'en vertu du principe de l'**autonomie de la personne morale**, une société ne saurait être tenue des dettes d'une autre société du même groupe. La Haute juridiction **confirme l'arrêt d'appel**.
- Dans le cas présent la société mère ne s'était immiscée ni dans la conclusion, ni dans l'exécution du contrat, jusqu'à la mise en demeure délivrée par la société défenderesse. De cette intervention au stade précontentieux « *lorsque le créancier s'apprêtait à saisir la juridiction en paiement de la créance, à plusieurs reprises, pour discuter le montant de l'obligation, en proposant notamment d'obtenir un montant moindre tiré de remises consenties à l'occasion de commandes précédentes, et tenter d'obtenir un paiement amiable, la société mère a laissé ainsi croire à la société* » créancière, à un moment où la société filiale avait encore des actifs, qu'elle se substituait à cette dernière dans l'exécution du contrat.

### Les contours de la notion d'« immixtion » dans les relations contractuelles

- En principe, une société mère ne sera pas tenue pour responsable des engagements contractés par sa filiale fût elle intégralement contrôlée. Il en résulte que le contractant de la filiale ne saurait agir directement contre la société mère afin d'obtenir le paiement des commandes passées pour le compte de la filiale (2).
- Il en va néanmoins différemment lorsque la société mère s'immisce dans les affaires de la filiale, créant ainsi une apparence fautive d'unicité d'entreprise.
- Pour apprécier cette apparence, les juridictions se fondent sur un **faisceau d'indices**. Des éléments tels que l'identité d'adresse électronique, de domicile ou de dirigeant, couplés au fait, pour une société mère, d'intervenir au stade précontentieux opposent sa filiale et le cocontractant de cette dernière.
- Pour la Cour de cassation, si le principe reste l'**indépendance entre une maison mère et ses filiales**, l'apparence d'une immixtion de la maison mère dans les affaires de sa filiale entraîne la responsabilité contractuelle de la maison mère, peu important que cette immixtion ne soit jamais intervenue au stade de l'exécution du contrat, mais uniquement au niveau précontentieux. Ainsi en principe, une société mère ne sera pas tenue pour responsable des engagements contractés par sa filiale fût elle intégralement contrôlée. Il en résulte que le contractant de la filiale ne saurait agir directement contre la société mère afin d'obtenir le paiement des commandes passées pour le compte de la filiale.

### Les enjeux

Le principe de l'autonomie d'une personne morale au sein d'un groupe souffre d'exceptions, parmi lesquelles l'immixtion de la société mère en phase précontentieuse de nature à créer une apparence de substitution à sa filiale, qui peuvent conduire à tenir une société mère pour responsable du paiement des dettes de sa filiale.

(1) [Cass. com. 3-2-2015, n°13-24895](#).

(2) Cass. com., 8-12-1997, *Bull. Joly Sociétés* 1998, p. 472, § 162, note J.-J. Daigre.

### Les conseils

Dans un groupe de sociétés, la société mère qui souhaite être dissociée des dettes dues par ses filiales au titre de l'exécution d'un contrat auquel elle est tiers, doit éviter au stade précontentieux opposant sa filiale et le cocontractant, de créer l'apparence d'une substitution entraînant sa responsabilité contractuelle.

[MARIE-ADELAÏDE  
MONTIVAUT-JACQUOT](#)

## CONFIDENTIALITE ET SECURITE DU VOTE ELECTRONIQUE DANS L'ENTREPRISE

- Confidentialité et sécurité informatique sont des problématiques centrales des dispositifs de vote électronique. Par un arrêt rendu le [11 mars 2015](#), le Conseil d'Etat apporte des précisions importantes sur les obligations de toute entreprise procédant aux **élections des représentants du personnel** par vote électronique.
- Dans cette affaire, une société s'était vue reprocher par la Cnil des manquements à ses obligations de veiller à la sécurité et à la confidentialité du système de vote électronique choisi. L'entreprise contestait la délibération de la Cnil devant le Conseil d'Etat. Rejoignant la Cnil, le Conseil d'Etat rejette l'argumentaire des requérants pour trois motifs.

### Expertise indépendante préalable à chaque scrutin

- « Préalablement à sa mise en place ou à toute modification substantielle de sa conception, le système de vote électronique est soumis à une **expertise indépendante** » ([art. R.2314-12](#) et [R.2324-8](#) Code du travail). Le requérant soutenait qu'il n'était pas tenu d'organiser une expertise avant chaque scrutin et que le dépôt préalable d'une copie du logiciel auprès d'un huissier de justice constituait une garantie de sécurité suffisante.
- Selon la Cnil, en l'absence d'expertise indépendante préalable au vote et d'« éléments permettant une comparaison effective » entre le logiciel de vote utilisé et la version déposée, l'organisateur du scrutin manquait à son obligation de sécuriser les **données personnelles des électeurs** ([art. 34 loi n°78-17 du 6-1-78](#)).
- Le Conseil d'Etat reprend cette analyse : « l'utilisation d'un système de vote électronique pour l'élection des délégués du personnel est subordonnée à la réalisation d'une expertise indépendante (...) préalablement à chaque scrutin recourant au vote électronique ».

### Envoi des codes personnels d'authentification selon un procédé sécurisé

- Le système doit assurer la sécurité de l'adressage des moyens d'authentification ([art. R.2314-9](#) et [R.2324-5](#) du Code du travail) afin d'éviter une **usurpation de la qualité d'électeur**. Or, les identifiants et mots de passe avaient été envoyés par lettres simples et sur le mél professionnel des électeurs.
- Réponse du Conseil d'Etat : « la transmission aux électeurs des identifiants et mots de passe leur permettant de participer au vote doit faire l'objet de **mesures de sécurité spécifiques** permettant de s'assurer que les électeurs en sont les seuls destinataires ». La Cour de cassation avait déjà jugé dans le même sens (Cass. soc. 27-2-2013, n°[12-14415](#)) : « l'envoi des codes personnels d'authentification (des électeurs) sur la messagerie professionnelle, sans autre précaution destinée notamment à éviter qu'une personne non autorisée puisse se substituer frauduleusement à l'électeur, n'est pas de nature à garantir la confidentialité des données transmises ».

### Chiffrement ininterrompu des bulletins de vote

- « Les données du vote font l'objet d'un **chiffrement dès l'émission du vote** sur le poste de l'électeur " ([arrêté du 25-4-2007 pris en application du décret n°2007-602 du 25-4-2007](#)). La Cnil recommande de ne déchiffrer le bulletin de vote durant le processus électoral « à aucun moment, même de manière transitoire » ([Délib. Cnil n°2010-371 du 21-10-2010 relative à la sécurité des systèmes de vote électronique](#)), ce qui n'était pas le cas en l'espèce.
- Le Conseil d'état en déduit que le système de vote électronique en cause méconnaissait l'obligation de chiffrement ininterrompu des bulletins de vote.

## L'enjeu

Sécuriser le dispositif de vote électronique dans l'entreprise

## Les conseils

Adapter la rédaction du cahier des charges de vote électronique aux nouvelles conditions de sécurité et de confidentialité.

Réaliser une expertise indépendante du dispositif de vote électronique avant chaque scrutin.

Communiquer l'identifiant et le mot de passe de l'électeur sur des supports distincts et sécurisés.

Choisir un procédé de chiffrement ininterrompu des bulletins de vote, de leur émission par l'électeur à leur dépouillement.

[EMMANUEL WALLE](#)  
[ETIENNE MARGOT-DUCLOT](#)

## COMMENT REAGIR EN CAS DE FAILLES DE SECURITE ?

### Les actions à mettre en œuvre au sein de l'entreprise

- Qu'elles proviennent d'une **erreur**, d'une **négligence** ou de **procédés illicites**, les failles de sécurité représentent aujourd'hui l'une des préoccupations majeures des entreprises. Aussi, dès la découverte d'une faille de sécurité, et préalablement à toute action contentieuse, plusieurs actions doivent rapidement être mises en œuvre.
- En interne d'abord, il est recommandé au RSSI, au DSI, ou, le cas échéant, à la société d'expertise informatique, d'**identifier la faille**, de **la corriger** avant de mettre en place un **audit de sécurité** et de procéder aux mises à jour des procédures internes.
- Parallèlement, il est vivement conseillé au RSSI, au DSI ou à la société d'expertise informatique de réaliser un **dossier de preuve technique**, comprenant a minima un rapport d'incident et les logs de connexion aux serveurs.
- A l'appui de ces éléments, il sera possible de qualifier juridiquement les faits et de les rattacher notamment aux infractions suivantes : **accès frauduleux dans un STAD**, **maintien frauduleux dans un STAD**, introduction, modification ou suppression frauduleuses de données dans un STAD, extraction, détention, reproduction ou transmission de données contenues dans un STAD, détention de programmes informatiques conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions d'atteintes aux STAD, association de malfaiteurs informatiques, usurpation d'identité numérique, escroquerie, **vol d'informations**.

### Les recours légaux

- **Dépôt de plainte.** Une plainte devra être déposée auprès du procureur de la République territorialement compétent, qui diligentera une enquête préliminaire confiée aux services de police ou de gendarmerie spécialisés que sont :
  - la brigade d'enquêtes sur les fraudes aux technologies de l'information (**Befiti**), service de la Police Judiciaire dévolu aux infractions informatiques en région parisienne ;
  - la sous-direction de lutte contre la cybercriminalité relève de la Direction centrale de la police judiciaire (**SDLC**), compétente pour les attaques à l'encontre d'un système d'information situé à l'extérieur du périmètre d'intervention de la Befiti ;
  - l'Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication (**OCLCTIC**), compétente sur tout le territoire français.
- **Notification à la Cnil.** Si l'atteinte porte sur des traitements de données personnelles mis en œuvre par une entreprise fournissant un service de communications électroniques (opérateurs de télécommunications et FAI), le responsable de traitement devra la notifier à la Cnil sans délai à compter de la constatation de la violation. La Cnil peut alors décider de procéder à une mission de contrôle, à l'issue de laquelle des recommandations ou des sanctions peuvent être prononcées (avertissement public, par exemple). Pour les autres organismes (privés ou publics), la notification de violation des données personnelles n'est pas obligatoire.
- La Cnil peut aussi, en cas de non-respect de l'obligation de sécurité de l'article 34 de la loi Informatique et libertés, **dénoncer au procureur** de la République les infractions à la loi Informatique et libertés, prévues aux articles 226-16 à 226-24 du Code pénal.
- Si la répression des atteintes au système d'information a été largement renforcée par la loi 2014-1353 du 13 novembre 2014 introduisant le délit d'extraction de données dans un STAD et par l'**arrêt** « Bluetouff » de la Cour de cassation du 20 mai 2015 qui consacre le vol de données, la **sécurisation du système d'information** reste le meilleur moyen de lutter contre les failles de sécurité.

### Les enjeux

Les enjeux sont importants : piratage des systèmes de traitement automatisé de données (STAD), perte d'informations confidentielles et stratégiques, vol de données personnelles, et lourds de conséquences sur le plan financier. A cet égard, l'entreprise victime devra vérifier sa police d'assurance pour vérifier si elle est couverte pour les risques informatiques.

### Les conseils

L'entreprise confrontée à une atteinte à son système informatique ayant conduit à une violation des données personnelles devra communiquer sur cet incident en interne et auprès de toutes personnes susceptibles de la solliciter (journalistes ou clients) et réagir très rapidement pour éviter toute diffusion d'information erronée ou inexacte, toute atteinte à sa réputation, ou encore mauvaise appréciation de l'impact de l'événement sur son activité économique.

VIRGINIE  
BENSOUSSAN-BRUE  
SASKIA BOUROVITCH

## BREVET EUROPEEN A EFFET UNITAIRE : LA CJUE REJETTE LES RECOURS EN ANNULATION FORMES PAR L'ESPAGNE

### La fin d'une épée de Damoclès sur le brevet européen à effet unitaire

- Alors que l'Europe connaît un système de dépôt unitaire par le biais de l'Office européen des brevets (OEB) depuis quarante ans, il aura fallu autant d'années de négociations pour **aboutir à un système unifié** de protection au sein de l'Union.
- L'opposition persistante de certains Etats, a conduit les Etats membres à recourir au système de la "**coopération renforcée**" pour permettre l'adoption du "**paquet brevet unitaire**" composé de trois textes distincts :
  - le **règlement UE n°1257/2012** du 17 décembre 2012 mettant en œuvre la coopération renforcée dans le domaine de la création d'une protection unitaire conférée par un brevet européen déposé auprès de l'OEB ;
  - le **règlement UE n°1260/2012** du 17 décembre 2012 portant sur le régime linguistique applicable au brevet européen à caractère unitaire et prévoyant que les demandes de brevets européens à effet unitaire devront être soumises dans l'une des langues trois officielles du système, à savoir l'anglais, le français ou l'allemand à l'exclusion de toute autre traduction ;
  - un **accord relatif à une juridiction unifiée du brevet** du 19 février 2013 et ayant pour objet la création d'un système juridictionnel unifié spécifique ayant compétence exclusive pour connaître des actions relatives à la contrefaçon ou la validité de brevets européens à effet unitaire.
- **S'opposant** au système et, notamment au **régime linguistique adopté**, l'Espagne a formé, devant la Cour de justice de l'Union européenne, deux recours tendant à l'annulation des Règlements adoptés.

### Le rejet des recours par la Cour de justice de l'Union européenne

- **Affaire C-146/13**(1) : le premier recours vise le règlement instaurant la protection unitaire elle-même. L'Espagne fait valoir qu'il ne peut porter sur un brevet déposé et délivré par l'OEB, institution échappant au contrôle juridictionnel de l'Union.
- La **Cour rejette le recours** rappelant la distinction entre les conditions de délivrance d'un brevet européen fixées par la Convention sur le brevet européen (CBE) et les modalités de sa protection ; le règlement européen n'a pas pour objet d'encadrer la délivrance du brevet, mais uniquement de fixer les conditions dans lesquelles, une fois délivré par l'OEB, il peut bénéficier d'un effet unitaire au sein des Etats participants à la coopération renforcée.
- **Affaire C-147/13**(2) : le second recours porte sur la remise en cause du **système linguistique**, à savoir l'adoption de trois langues officielles pour réduire les coûts d'obtention et de délivrance d'un brevet en Europe. Aujourd'hui la protection d'un brevet dans les pays signataires de la CBE implique sa traduction dans les langues officielles de chaque pays désigné entraînant des frais souvent trop lourds à supporter et la renonciation à solliciter une protection pour l'ensemble des pays initialement désignés dans la demande de brevet.
- L'Espagne invoque une **rupture d'égalité** pour les personnes dont la langue n'est pas l'une des langues officielles. **La Cour rejette le recours**, ce choix poursuivant un objectif légitime (faciliter l'accès des PME à cette protection) et le traitement différencié étant, en pratique, atténué par la mise en place de mécanismes permettant de préserver l'équilibre de traitement entre les opérateurs économique (période transitoire, système de remboursement des frais de traduction, etc.)

### Les enjeux

L'invalidation du « paquet brevet unitaire » instauré par les Règlements UE [1257/2012](#) et [1260/2012](#) du 17-12-2012 et l'[Accord relatif à une juridiction unifiée du brevet](#) du 19-2-2013.

- (1) [CJUE gde ch. C-146/13](#), Royaume d'Espagne c/ Parlement européen et Conseil de l'Union européenne, 5-5-2015.
- (2) [CJUE gde ch. C-147/13](#), Royaume d'Espagne c/ Conseil de l'Union européenne, 5-5-2015

### Les conseils

Anticiper l'entrée en vigueur du système de brevet européen à effet unitaire en :

- auditant le portefeuille de brevets existant ;
- analysant l'opportunité d'une transformation des brevets européens existants en brevets européens à effet unitaire ;
- définissant une politique de protection pour les brevets à venir.

[VIRGINIE BRUNOT](#)

## QUELLES PROPOSITIONS POUR DEVELOPPER LA TELEMEDECINE ?

### Le déploiement insuffisant de la télémédecine

- Sur l'impulsion de la Commission Européenne et des professionnels de santé, la France s'est dotée d'un **véritable cadre juridique** pour la télémédecine, avec la loi du 21 juillet 2009 et le décret du 19 octobre 2010 (1). Les actes de télémédecine, déjà reconnus par la loi du 13 août 2004 (2) sont ainsi définis : " *les actes médicaux, réalisés à distance, au moyen d'un dispositif utilisant les technologies de l'information et de la communication* ".
- Il existe **cinq types d'actes** : la téléconsultation, la téléexpertise, la télésurveillance médicale, la téléassistance médicale et la réponse médicale. Le décret est venu préciser les conditions spécifiques de mise en œuvre de ces actes, en sus des règles déontologiques communes à tout acte de médecine.
- Si le cadre juridique est posé, les modalités d'accès à la télémédecine et l'organisation de cette activité restent encore à affiner.
- Ainsi le **groupe de travail, dit "GT 33"**, a été réuni dans le cadre du CSF Santé (3) et du CSIS (4), au sein du CNI (5), instance consultative associant l'Etat, l'industrie et les partenaires sociaux. Il doit son nom à la 33e mesure proposée, dans le cadre du Contrat de Filière Industries et Technologies de Santé du 5 juillet 2013.
- La **mesure 33** visait à faciliter le développement de la télésanté - télémédecine, et à " *permettre l'émergence d'une stratégie industrielle en matière de e-santé, au soutien de la politique de santé publique, en associant les industriels* ".
- Dans son rapport du **30 mars 2015 intitulé " Lever les freins au développement de la télémédecine "** (6), le GT 33 a édicté sept propositions d'actions concrètes en vue d'un déploiement plus important de la télémédecine.

### Sept actions concrètes à mettre en œuvre

- La première action porte sur le " **kit de démarrage d'un projet** de télémédecine " composé de cinq fiches pédagogiques établies par la Direction Générale de l'Offre des Soins, qui permet, en répondant à plusieurs questions (type d'actes, coopération, etc.), de déterminer la nature du projet et de le qualifier juridiquement.
- Il est ensuite préconisé de réaliser une **évaluation** a priori du potentiel médico-économique d'un projet, à l'aide du cadre d'évaluation proposé par la HAS (7) dans son rapport du 18 juillet 2013 (8).
- Pour les **aspects juridico-administratifs**, plusieurs actions sont envisagées :
  - Clarification du processus de contractualisation avec chaque ARS (9), par un décret annoncé pour le premier semestre 2015 ;
  - Simplification des autorisations des protocoles de coopération et amélioration de la visibilité de ceux-ci au moyen du site COOP-PS ;
  - Amélioration du circuit de traitement des dossiers de télémédecine par les ARS (guichet unique, structures de maîtrise d'ouvrage régionales).
- Pour les **aspects techniques**, une simplification de la procédure d'agrément hébergeur de données de santé et la mise en avant de solutions d'authentification forte, alternatives à la Carte de professionnel de santé, sont préconisées.
- Enfin, sont essentielles **l'implication d'experts** et l'intégration par la HAS de la télémédecine dans les recommandations professionnelles, dans la droite ligne de ce qui est prévu dans le projet de loi de santé.

### Les enjeux

Des mesures en vue de la promotion et l'amélioration de l'accès à la télémédecine.

- (1) Loi 2009-879 et décr. 2010-1229.
- (2) Loi 2004-810.
- (3) Comité Stratégique de Filière Santé.
- (4) Conseil Stratégique des Industries de Santé
- (5) Conseil National de l'Industrie.
- (6) [Rapport du GT 33 du 27-3-2015](#).
- (7) Haute Autorité de Santé.
- (8) [Rapport de la HAS du 18-7-2013](#).
- (9) Agence Régionale de Santé.

### L'essentiel

Sept actions recommandées afin de lever les freins au développement de la télémédecine.

[MARGUERITE BRAC DE LA PERRIERE](#)  
[AUDE LATRIVE](#)

## ATTENTION A LA REQUALIFICATION FISCALE DES MANAGEMENT PACKAGES

### Le régime fiscal des gains issus des management packages

- Un dirigeant salarié ou toute autre personne en relation d'affaires avec un groupe de sociétés, peut bénéficier d'**option de souscription** ou d'**achat d'actions** en dehors du dispositif légal, ou se voir offrir la possibilité d'acheter et/ou de revendre dans des **conditions préférentielles** des titres d'une société.
- L'administration fiscale se réserve alors le droit de **requalifier le gain réalisé** à cette occasion et de le taxer non pas dans la catégorie des plus-values de cession sur valeurs mobilières mais dans celle correspondant effectivement à la nature de l'opération réalisée.
- Dans ce cas, l'imposition est effectuée au **barème progressif de l'impôt** sur le revenu :
  - soit dans la catégorie des **traitements et salaires** (ou dans celle de l'article 62 du CGI) si la prestation rendue en contrepartie de l'offre des titres peut-être rattachée à l'exécution d'un contrat de travail ou, à l'exercice de fonctions dirigeantes dont la rémunération est imposable dans la catégorie des traitements et salaires (ou dans celle de l'article 62 du CGI) ;
  - soit dans la catégorie des **bénéfices non commerciaux** (CGI, art. 92-1) lorsque l'avantage a pour contrepartie une activité déployée à titre personnel (le service ainsi rémunéré peut consister par exemple en des opérations d'entremise ou de négociation dans le cadre de la restructuration d'un groupe) ;
  - soit en tant que **revenu distribué** si l'avantage consenti est occulte, ou résulte d'un acte de gestion anormal de la société, ou a pour effet de porter la rémunération totale du bénéficiaire à un montant exagéré (1).

### La qualification fiscale du gain de cession d'actions

- Le **Conseil d'Etat** s'est prononcé récemment sur la qualification fiscale du gain de cession d'actions résultant de l'exercice d'options d'achat d'actions consenties à un dirigeant en dehors du cadre légal des options d'achat d'actions (**stock-options**).
- A cette occasion, le Conseil d'Etat a confirmé la décision de la Cour administrative d'appel de Paris et donc la position de l'administration.
- Il a validé la requalification en  **salaire d'une plus-value de cession de titres** réalisée par un dirigeant après l'exercice d'une option d'achat d'actions (2).
- Le Conseil d'Etat a considéré sans autre précision, que l'écart entre le prix de cession des actions et le prix fixé dans la convention (**management package**) correspondait, dans sa totalité, à un revenu qui trouvait sa source dans les conditions dans lesquelles l'option d'achat des actions lui avait été consentie et avait le caractère d'un **avantage en argent, imposable** dans la catégorie des traitements et salaires.
- Bien que cette décision s'inscrive dans la continuité de la **doctrine administrative** rappelée ci-dessus, il est toutefois regrettable que le Conseil d'Etat n'ait pas profité de l'occasion qui lui était offerte pour clarifier les critères de requalification en salaire des gains en capital réalisés par un dirigeant.

### Les enjeux

L'administration se réserve le droit de requalifier en salaire les gains réalisés sur des cessions de titres normalement imposables dans la catégorie des plus-values de cession.

(1) [BOI-RSA-ES-20-10-20-50-20140818](#).

(2) [CE 26-9-2014 n°365573](#).

### Les conseils

Le régime fiscal des plus-values de cession des titres sociaux pour les stock-options n'est pas applicable en dehors du cadre légal des plans de stock-options.

[PIERRE-YVES FAGOT](#)

# Prochain petit-déjeuner

## Informatique et libertés : Bilan d'activité de la Cnil: 9 septembre 2015

- Alain Bensoussan animera un petit-déjeuner débat consacré à la présentation du bilan d'activité de la Cnil pour l'année 2014.
- L'année 2014 a confirmé la tendance observée depuis quelques années quant à l'augmentation des activités de contrôle et de sanction de la Cnil. Pour 2015, la Commission se fixe un objectif d'environ 550 contrôles se décomposant de la façon suivante :
  - environ 350 vérifications sur place, dont un quart sur les dispositifs de vidéoprotection ;
  - 200 contrôles en ligne.
- Parmi les thématiques prioritaires des contrôles figurent les « Binding Corporate Rules » (BCR). Ce qui permettra à la Commission d'avoir un éclairage sur l'impact du dispositif au regard de la protection des données et du respect de la vie privée au sein des groupes concernés.
- De plus, le nombre de plaintes est toujours aussi important : 5800 plaintes enregistrées en 2014.
- Au-delà de ces chiffres, l'année 2014 se caractérise par les initiatives de la Cnil pour accompagner les entreprises dans leur démarche de conformité à la réglementation Informatique et libertés :
  - publication du label « Gouvernance Informatique et Libertés » ;
  - élaboration du pack de conformité assurance.
- L'année 2015-2016 s'annonce également riche en actions pour la Cnil, au vu du programme des contrôles annoncés.
- Nous vous proposons, dans le cadre de ce petit-déjeuner débat, de préciser les actions à mettre en œuvre par les entreprises pour assurer la conformité de leur activité à la réglementation Informatique et libertés et anticiper l'adoption du projet de règlement européen en matière de protection des données qui devrait être adopté fin 2015.
- **Lieu** : de 9h30 à 12h00 (accueil à partir de 9h00) dans [nos locaux](#), 58 bd Gouvion-Saint-Cyr, 75017 Paris.
- **Inscription gratuite** (sous réserve des places disponibles). L'enregistrement en ligne est obligatoire pour y assister : [formulaire en ligne](#).

## NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

### Suspension administrative : attention au licenciement déguisé



- **Charles Wagner** du cabinet Langlois Kronström Desjardins LLP, rappelle les dispositions de la *Loi sur les normes du travail* en matière de licenciement abusif à propos de la décision du 6 mars 2015 rendue par la Cour suprême du Canada (la « CSC ») dans l'affaire *Potter* (1).
- Dans cette affaire, deux mois après sa suspension, le salarié, qui ne connaissait toujours pas les motifs de cette suspension malgré une demande écrite pour les obtenir, a intenté une action pour licenciement déguisé.
- Son employeur avait cessé de lui verser son salaire et ses avantages sous le prétexte que ce dernier avait démissionné de son poste en intentant une action.
- Or, puisque le salarié avait été suspendu pour une période indéfinie, que son employeur ne lui avait pas communiqué de motifs valables et qu'il avait l'intention de le congédier, la Cour a conclu qu'il y avait bel et bien eu un acte unilatéral de la part de l'employeur représentant une modification substantielle des conditions de travail du salarié.

(1) [Actualité du 15-5-2015.](#)

Lexing Canada  
[Langlois Kronström Desjardins LLP.](#)

### La protection des données personnelles dans le monde



- **Françoise Gilbert** publie la 17<sup>ème</sup> édition du « Global Privacy and Security Law 2015 » édité par Aspen Publishers (2).
- Cet ouvrage auxquels participent bon nombre de membres du réseau Lexing®, analyse les lois de protection de la vie privée, les usages et les tendances de 66 pays sur tous les continents (Europe, Afrique, Moyen-Orient, Asie-pacifique et Amérique du Nord et du Sud).
- Chaque pays contributeur traite la législation de son Etat sur la protection des données et la confidentialité des données.
- La première édition date de janvier 2009. L'ouvrage est actualisé trois fois par an sous la direction de Françoise Gilbert.
- Dans cette 17<sup>ème</sup> édition parue en mai 2015, il convient de signaler :
  - un nouveau contributeur pour l'Inde (Rahul Matthan) ;
  - l'adoption par la Russie d'une loi en décembre 2014 ;
  - l'introduction en Slovaquie (loi n ° 307/2014 Coll) et en Turquie (nouveau E-Commerce Code), de législations qui ont des répercussions sur les questions de protection des données ;
  - l'entrée en vigueur en Lituanie, en Janvier 2015, d'une nouvelle loi sur la sécurité cybernétique.

(2) [Actualité sur la 17<sup>ème</sup> édition.](#)

Lexing Etats-Unis  
[IT Lawgroup](#)

## Liste d'opposition au démarchage téléphonique

▪ Un décret du **19 mai 2015** précise le fonctionnement de la liste d'opposition au démarchage téléphonique (1). La mise en œuvre et la gestion de ce traitement automatisé sont confiées à un organisme de droit public ou de droit privé désigné dans les conditions prévues à l'article L. 121-34 du Code de la consommation, pour une durée maximale de cinq ans.

(1) [Décret 2015-556 du 19-5-2015.](#)

## Rapport annuel 2014 de la Banque de France

▪ Le rapport annuel 2014 de la Banque de France publié en mai 2015, signale un accord conclu avec la Fédération des ventes à distance qui a permis l'inclusion en 2014 des achats par internet (2).

(2) [Rapport annuel 2014 de la Banque de France.](#)

## Lutte contre les discriminations en entreprise

▪ Remise au ministre du travail, de l'emploi, de la formation professionnelle et du dialogue social, le **19 mai 2015**, d'un rapport de synthèse des travaux du groupe de dialogue inter-partenaires sur la lutte contre les discriminations en entreprise. (3). Sont préconisées la mise en place d'une formation à la problématique des discriminations (RH, représentants syndicaux, managers), et l'introduction, dans les entreprises de plus de 300 salariés d'un « référent égalité des chances ».

(3) [Rapport de synthèse sur la lutte contre les discriminations en entreprise.](#)

## Tableau de bord de l'Union de l'innovation

▪ La Commission européenne a publié le **7 mai 2015**, son édition annuelle du « tableau de bord de l'Union de l'innovation » fournissant une évaluation comparative des performances des Etats membres en matière de recherche et d'innovation (4). Les demandes de brevets, les exportations de produits de haute technologie et les ventes de produits innovants sont en baisse.

(4) [Tableau de bord de l'Union de l'innovation 2015.](#)

## Secret professionnel et échanges d'informations entre administrations

▪ Une ordonnance du **7 mai 2015** relative à l'adaptation du secret professionnel dans les échanges d'informations entre autorités administratives et à la suppression de la production de pièces justificatives prévoit que les administrations ne peuvent plus s'opposer mutuellement le secret professionnel dès lors qu'elles sont, dans le cadre de leurs missions légales (5).

(5) [Ordonnance 2015-507 du 7-5-2015.](#)

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan.

Directeur de la publication : Alain Bensoussan - Responsable de la rédaction : Isabelle Pottier

Diffusée uniquement par voie électronique – gratuit -

ISSN 1634-0701

Abonnement à partir du site : <http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance>

©Alain Bensoussan 2014

# Formations intra-entreprise : 2<sup>e</sup> semestre 2015

LE CABINET A LA QUALITE D'ORGANISME DE FORMATION PROFESSIONNELLE DEPUIS 30 ANS.

## Archivage électronique public et privé

### Dates

<b><u>Gérer un projet d'archivage électronique</u></b> : Intégrer les prérequis juridiques dans la conduite du projet et garantir la conformité des systèmes d'archivage électronique.	12-02 et 21-05-2015
<b><u>Gérer les archives publiques électroniques</u></b> : Comprendre les spécificités des archives publiques électroniques.	27-01 et 14-04-2015
<b><u>Contrôle fiscal des comptabilités informatisées</u></b> : Prévenir et anticiper les contrôles fiscaux et gérer les contraintes liées à l'évolution des systèmes d'information.	30-01 et 16-04-2015

## Cadre juridique et management des contrats

<b><u>Cadre juridique des achats</u></b> : Comprendre les bases du droit de l'achat et gérer les étapes de la conclusion d'un achat, depuis les pourparlers jusqu'au précontentieux.	04-02 et 26-06-2015
<b><u>Manager des contrats d'intégration et d'externalisation</u></b> : Comprendre les particularités de l'intégration et de l'outsourcing et bien gérer l'exécution des contrats.	10-02 et 13-05-2015
<b><u>Contract management</u></b> : Comprendre les bases du droit des contrats et gérer les étapes de la conclusion d'un contrat, depuis les pourparlers jusqu'au précontentieux.	28-01 et 01-04-2015
<b><u>Sécurisation juridique des contrats informatiques</u></b> : Comprendre et mettre en œuvre les outils juridiques de sécurisation des contrats informatiques.	28-01 et 08-04-2015
<b><u>Garantir la pérennité et le succès d'un projet informatique grâce au contract management Niveau 2 Expert</u></b> : Gérer au sein d'un groupe de sociétés la signature et le bénéfice d'un contrat informatique.	30-01 et 31-03-2015
<b><u>Les clés pour réussir son projet « Cloud computing »</u></b> : Savoir définir une « cloud strategy »	04-02 et 19-05-2015

## Conformité et risque pénal

<b><u>Risque et conformité au sein de l'entreprise</u></b> : Cerner le rôle et la place de la conformité dans l'entreprise pour sécuriser l'activité de l'entreprise.	05-03 et 23-06-2015
<b><u>Gérer une crise en entreprise : le risque pénal</u></b> : Le risque et les principes. Comment s'annonce le risque et	20-03 et 19-06-2015

## Informatique

<b><u>Edition de progiciel : Etat de l'art et tendances juridiques</u></b> : Maîtriser le cadre juridique de l'édition logicielle pour gérer l'administration des parcs de progiciels.	16-01 et 10-04-2015
<b><u>Traitement et hébergement des données de santé à caractère personnel</u></b> : Identifier les problématiques complexes (contrats d'hébergement, contrats de sous-traitance, etc.) et bénéficier de recommandations spécifiques s'agissant des clauses des contrats.	06-02 et 20-05-2015

## Internet et commerce électronique

<b><u>Commerce électronique</u></b> : Acquérir les connaissances indispensables à la maîtrise des obligations principales d'un éditeur d'un site marchand.	29-01 et 18-03-2015
<b><u>Webmaster niveau 2 expert</u></b> : Présentation en 360° des risques juridiques d'une activité web 2.0 et web 3.0.	11-03 et 10-07-2015

## Innovation propriété intellectuelle et industrielle

<b><u>Audit du patrimoine intellectuel de l'entreprise</u></b> : Détecter les forces, points de faiblesses et risques juridiques et financiers d'un portefeuille « Propriété Intellectuelle ».	12-02 et 16-04-2015
<b><u>Protection d'un projet innovant</u></b> : Présenter les spécificités juridiques relatives à un projet innovant afin de gérer les étapes d'une protection adaptée.	17-03 et 16-06-2015
<b><u>Sensibilisation à la protection d'un portefeuille marque et nom de domaine</u></b> : Acquérir la connaissance minimale pour assurer la protection d'une marque et d'un nom de domaine de la création à l'échéance tout en assurant le maintien et la défense.	24-03 et 02-07-2015
<b><u>Droit des bases de données</u></b> : Conclure des licences adaptées à ses besoins et connaître et prévenir les risques liés à l'exploitation d'une base de données.	22-01 et 12-03-2015
<b><u>Droit d'auteur numérique</u></b> : Acquérir les bons réflexes pour protéger son patrimoine intellectuel et ne pas porter atteinte aux droits d'autrui.	03-02 et 29-05-2015
<b><u>Lutte contre la contrefaçon</u></b> : Anticiper les difficultés liées à la contrefaçon sur internet et cerner les spécificités face aux technologies de l'information et de la communication.	27-03 et 25-06-2015

## Management des litiges

<b><u>Médiation judiciaire et procédure participative de négociation</u></b> : Comprendre le déroulement de la procédure de médiation judiciaire et de la procédure participative.	22-01 et 03-04-2015
--	---------------------

## Presse et communication numérique

<b><u>Atteinte à la réputation sur Internet</u></b> : Gérer les difficultés d'application de la loi sur la presse aux nouveaux vecteurs de communication de la pensée.	23-01 et 17-04-2015
--	---------------------

## Informatique et libertés

<b><u>Informatique et libertés (niveau 1)</u></b> : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	24-07 et 13-11-2015
<b><u>Cil (niveau 1)</u></b> : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	14-01 et 02-04-2015
<b><u>Informatique et libertés secteur bancaire</u></b> : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	20-01 et 04-03-2015
<b><u>Informatique et libertés collectivités territoriales</u></b> : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	15-04 et 24-06-2015
<b><u>Sécurité informatique et libertés</u></b> : Connaître les exigences issues de la réglementation Informatique et libertés en matière de sécurité des données personnelles et sensibiliser aux risques liés à une faille de sécurité.	20-01 et 26-03-2015
<b><u>Devenir Cil</u></b> : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	06-03 et 03-06-2015
<b><u>Cil (niveau 2 expert)</u></b> : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	05-02 et 17-06-2015
<b><u>Informatique et libertés gestion des ressources humaines</u></b> : Donner aux membres de la direction des ressources humaines les clés pour utiliser les outils et les traitements de données personnelles mis en œuvre en matière de gestion des ressources humaines.	15-01 et 18-03-2015
<b><u>Flux transfrontières de données</u></b> : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	11-02 et 19-03-2015
<b><u>Contrôles de la Cnil</u></b> : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle).	13-02 et 10-04-2015
<b><u>Informatique et libertés secteur santé</u></b> : Sensibiliser aux risques Informatique et libertés liés aux traitements du secteur santé et assurances et apporter des éléments de benchmark permettant de positionner son niveau de conformité.	27-01 et 25-03-2015
<b><u>Informatique et libertés à l'attention du comité exécutif</u></b> : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité.	Selon demande



## Une gestion innovante de la réclamation clients

Zbynek Loebel  
CEO Youstice (\*)

### En quoi consiste exactement l'innovation de votre société Youstice ?

Youstice est un nouveau service que les entreprises peuvent mettre à la disposition des consommateurs afin de résoudre de façon simple et efficace les incidents et requêtes pouvant naître à l'occasion d'un achat en ligne. Cette idée m'est venue en 2012 afin de répondre au besoin d'avoir un outil simple et de bon sens pour optimiser la gestion des difficultés pouvant naître avec un consommateur à l'occasion de l'achat d'un produit ou d'un service.

Notre plateforme est disponible sur le marché européen depuis l'automne 2014 et offre des solutions personnalisées dans le secteur du commerce de détails (e-commerce), des transports, des jeux en ligne, avec un développement vers d'autres secteurs prévu dans le courant de l'année.

### Comment fonctionne votre plateforme de gestion des réclamations clients ?

Le fonctionnement est simple. Il appartient aux entreprises d'ajouter notre application sur leur site marchand pour permettre à leurs clients d'y accéder par un simple clic. Les clients insatisfaits par un achat ou un service sélectionnent parmi une liste de problèmes celui qui les concerne et suggèrent une solution pour mettre un terme au litige. Cela ne prend que quelques minutes seulement.

La société prestataire est notifiée par email et peut visualiser la liste des plaintes sur son tableau de bord dédié et ainsi les traiter, soit en acceptant la solution proposée par le consommateur, soit en en proposant une autre. Pour les clients qui n'acceptent pas la contre-proposition de la société, nous avons une option que nous appelons "l'escalade", qui permet de soumettre la plainte à un tiers professionnel neutre qui tranchera.

### Pourquoi avoir choisi de mettre en place un tel service ? comment s'insère-t-il dans les nombreuses dispositions légales de protection des consommateurs ?

Cette offre est pertinente pour tout commerçant qui souhaite traiter les plaintes de ses clients à moindre coût, d'une façon plus efficace, et qui souhaite entretenir une relation de PARTENAIRES avec ses clients. Je considère qu'il s'agit d'un outil créateur de confiance et de loyauté pour les détaillants et prestataires de services.

Nous croyons également en la possibilité pour notre service de devenir un outil très demandé en raison de sa conformité à la nouvelle réglementation européenne relative au règlement extrajudiciaire des litiges de consommation. Cette nouvelle réglementation va recommander des règles plus strictes en matière de protection des consommateurs au sein des états membres de l'union européenne. Les entreprises peuvent anticiper cette nouvelle réglementation en intégrant cet outil marketing.

### Quels autres avantages les entreprises peuvent-elles tirer de ce service ?

Il y a plusieurs avantages que je souhaiterais évoquer. Tout d'abord, nous offrons un outil de service client « dédié » qui va désengorger les opérations, minimiser le temps passé à traiter des incidents et être ainsi plus rentable. De plus, nous avons pour objectif d'aider les commerçants à construire et maintenir une bonne réputation en tant qu'entreprise de confiance grâce à un outil permettant de résoudre des problèmes de façon très efficace - et minimiser les retours clientèles négatifs.

A côté de cela, les sociétés françaises qui développent leur commerce dans différents pays, ou envisagent de le faire, peuvent, grâce à notre plateforme, offrir à leurs clients un service multilingue, garantissant des services support de haut niveau pour les consommateurs en difficulté. Enfin, dernier élément mais non des moindres, Youstice est également un outil intelligent de conformité permettant aux entreprises de se conformer à la nouvelle réglementation européenne relative au règlement des litiges de consommation

(\*) <http://www.youstice.com/fr/>