Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

JURISTENDANCES INFORMATIQUE ET TELECOMS

n° 155 – Mars 2015

LE CODE SOURCE DU LOGICIEL SIMULANT L'IMPOT SUR LE REVENU EST COMMUNICABLE

L'avis de la Commission d'accès aux documents administratifs

▪ Un chercheur s'étant vu refuser l'obtention du code source du logiciel simulant le calcul de l'impôt sur les revenus des personnes physiques, pour le réutiliser dans ses travaux universitaires, s'est adressé à la CADA. Dans sa réponse on ne peut plus claire, la Commission d'accès aux documents administratifs a répondu dans un avis du 8 janvier 2015 (1) :

▪ « *Le code source d'un logiciel est un ensemble de fichiers informatiques qui contient les instructions devant être exécutées par un micro-processeur. Elle estime que les fichiers informatiques constituant le code source sollicité, produits par la direction générale des finances publiques dans le cadre de sa mission de service public, revêtent le caractère de documents administratifs, au sens de l'article 1er de la loi du 17 juillet 1978. Ce code est, de ce fait, communicable à toute personne qui le demande, conformément à l'article 2 de la même loi, dès lors, compte tenu des dispositions du g du 2° du I de l'article 6 de cette loi, que sa communication ne paraît pas porter pas atteinte à la recherche des infractions fiscales. En application de l'article 4, il doit être communiqué, au choix du demandeur et dans la limite des possibilités techniques de l'administration, par la délivrance d'une copie sur un support compatible avec celui qu'elle utilise, aux frais du demandeur, ou par courrier électronique et sans frais. En vertu de l'article 10 relatif à la réutilisation des informations publiques, et à moins que des tiers à l'administration détiennent des droits de propriété intellectuelle sur ce code, il peut être utilisé par toute personne qui le souhaite à d'autres fins que celles de la mission de service public de l'administration fiscale, notamment pour les besoins de la recherche en économie, telle celle à laquelle le demandeur consacre ses travaux.*

▪ *En réponse à la demande qui lui a été adressée, le directeur général des finances publiques a indiqué à la commission que le code source de l'application de calcul de l'impôt sur le revenu des personnes physiques se composait de nombreux fichiers nécessitant un lourd traitement pour être rendus exploitables, de sorte que le document sollicité devait être regardé comme inexistant, en l'absence de traitement automatisé d'usage courant susceptible d'en produire une version compréhensible.*

▪ *La commission rappelle que si toute personne est en principe fondée à obtenir communication d'un document administratif, en vue de la réutilisation des informations publiques qu'il comporte, dans le format le plus propre à cette réutilisation, lorsque l'administration le détient dans différents formats ou peut obtenir par un traitement automatisé d'usage courant le format souhaité, la loi du 17 juillet 1978 ne fait pas obligation à l'administration d'élaborer un nouveau document, notamment un document qui n'existerait pas en l'état et ne pourrait être obtenu que par une opération excédant un simple traitement automatisé d'usage courant.*

▪ *La commission considère, en revanche, que l'appréciation de l'administration selon laquelle la réutilisation envisagée se heurterait à des difficultés techniques, voire à une impossibilité matérielle, ne saurait fonder le refus de communiquer le document sollicité dans l'état où l'administration le détient.*

▪ *La commission émet donc un avis favorable à la communication à Monsieur X du code source sollicité, sous la forme sous laquelle l'administration le détient. Le demandeur est libre de le réutiliser dans les conditions fixées à l'article 12 de la loi du 17 juillet 1978, en l'absence de droits de propriété intellectuelle détenus par des tiers à l'administration, dont le directeur général des finances publiques ne fait pas état* ».

Les enjeux

Le code source d'un logiciel utilisé par une autorité publique est un document administratif communicable à toute personne qui le demande, conformément à la loi CADA du 17 juillet 1978.

(1) Avis CADA 2014-4578 - Séance du 8-1-2015.

Le conseil

La loi prévoit depuis 2005, la possibilité de réutiliser les informations publiques à d'autres fins que celles pour lesquelles elles sont détenues ou élaborées.

Si leur obtention occasionne un coût pour l'administration ou si elle souhaite obtenir une rémunération de ses droits de propriété intellectuelle, celle-ci peut demander le paiement d'une redevance après avoir conclu une licence de réutilisation.

ISABELLE POTTIER

VERS UNE REFORME DE LA CONNAISSANCE DES RESEAUX.

La réglementation actuelle

▪ L'article D. 96-6-3 du Code des postes et communications électroniques (CPCE) prévoit que l'Etat et les collectivités territoriales peuvent demander aux opérateurs de réseaux des informations relatives :

- aux infrastructures d'accueil des réseaux de télécoms (artère de génie civil, pylônes, locaux, armoires etc.) ;

  aux équipements passifs de réseaux télécoms (câbles, éléments de connexion et d'interconnexion).

▪ L'idée force qui sous-tend cette **obligation de communication** est que pour que les collectivités territoriales puissent correctement exercer leurs pouvoirs dans le domaine de l'aménagement numérique du territoire, elles doivent pouvoir connaître la **situation des réseaux existants** ou en cours de déploiement, afin d'intégrer les données qui en résultent dans la mise au point de leur schémas directeurs territoriaux d'aménagement numérique (SDTAN).

▪ Néanmoins, les opérateurs de réseaux de communications électroniques bénéficient des **interdictions de communication** d'informations visées par les dispositions du décret du 15 janvier 2010 (1), lorsque les informations concernent :

- la localisation des emprises de desserte et des systèmes de raccordement situés dans le périmètre autour d'**installations d'importance vitale** et d'installations classées ;
- la localisation précise des **nœuds et relais des réseaux** télécoms de collecte ;
- le tracé des infrastructures d'accueil géographiquement isolées et dédiées aux **réseaux télécoms longue distance** ou à la desserte spécifique de clients professionnels.

Les modifications attendues

▪ Le **projet de décret en cours** d'adoption a pour objectif de supprimer la première des trois interdictions sus visées, et ce, afin de faciliter les conditions de mise en œuvre, par l'Etat et les collectivités territoriales de leurs droits à communication d'informations.

▪ L'Autorité de régulation des postes et communications électroniques, saisie de ce projet de décret, vient de publier l'**avis** (2) qu'elle a rendu à son propos.

▪ L'Autorité note que « les dispositions du projet de décret visent à **simplifier** la mise en œuvre du **droit à la connaissance des réseaux** de l'Etat, des collectivités territoriales et de leurs groupements, lesquels sont, par ailleurs, soumis au respect de la **confidentialité** des **informations sensibles** dont ils sont destinataires en application de l'article 6 de la **loi n° 78-753 du 17 juillet 1978** (3) portant diverses mesures d'amélioration des relations entre l'administration et le public et des articles L. 33-7 et D. 98-6-3 du Code des postes et communications électroniques ».

▪ Elle indique qu'elle n'a pas d'observations particulières à formuler dans la mesure où les conditions de la **préservation de la confidentialité** des informations transmises par les opérateurs continuent à être assurées conformément aux dispositions de la loi du 17 juillet 1978 et du CPCE.

L'enjeu

L'existence des interdictions dont bénéficient les opérateurs s'explique principalement par des raisons de protection de la confidentialité des informations commerciales des opérateurs de réseaux de télécoms, d'une part, mais aussi par des considérations de maintien du secret de la localisation et du tracé de certaines infrastructures télécoms, pour des raisons de protection du territoire et de ces infrastructures contre des actes malveillants, terroristes ou de guerre, d'autre part.

Les conseils

Les opérateurs devront modifier leurs procédures internes de communication d'informations pour tenir compte de la suppression de l'interdiction dont ils bénéficiaient jusqu'à présent.

(1) Décret 2010-57 du 15 01 2010.
(2) Avis Arcep 2014-0472 du 17 04 2014
(3) Loi 78-753 du 17 07 1978

FREDERIC FORSTER

DE LA RECEVABILITE DES PIECES DANS UNE PROCEDURE D'APPEL AVEC REPRESENTATION OBLIGATOIRE

La recevabilité des pièces dans la procédure d'appel

▪ Dans **deux importants arrêts**, l'Assemblée plénière de la Cour de cassation (1) précise le sort de la communication des pièces dans une procédure d'appel **avec représentation obligatoire** (2).

▪ Dans le premier arrêt, la Cour d'appel a refusé d'écarter des débats, les pièces communiquées par l'appelante 18 jours après le dépôt et la notification des conclusions dans les délais procéduraux, au motif que la preuve d'une atteinte aux droits de la défense n'a pas été rapportée. L'intimée a en effet pu conclure trois fois suite au dépôt des pièces et avant la clôture de l'instruction.

▪ Le pourvoi a contesté cette décision au motif que, lorsque la partie adverse le demande, le retrait des pièces non communiquées simultanément au dépôt des conclusions doit être fait de manière automatique par le juge.

▪ La Cour de cassation rejette le pourvoi et estime que la Cour d'appel a jugé à bon droit que les pièces communiquées quelques jours après le dépôt et la notification des conclusions avaient néanmoins permis à l'intimé de répondre souverainement à ces pièces qui avaient été communiquées en temps utile.

▪ Dans la seconde affaire, le juge d'appel a déclaré les conclusions de l'intimé irrecevables car communiquées postérieurement au délai de deux mois (art. 909 CPC), mais a refusé d'étendre cette irrecevabilité aux pièces produites en même temps que les conclusions, en l'absence de dispositions spécifiques dudit article.

▪ Le pourvoi a contesté ce refus au motif que les pièces produites en même temps que des conclusions irrecevables doivent être écartées des débats.

▪ La Cour de cassation fait droit à l'argumentaire du pourvoi tout en le rejetant, la cour d'appel ne s'étant pas fondée sur les pièces pour forger son intime conviction.

Dans quel cas les pièces communiquées hors délais sont irrecevables ?

▪ La Cour de cassation apporte une réponse distincte à la **défaillance d'une partie** dans la communication des pièces en appel selon que la communication des conclusions aient été ou non faite dans des délais procéduraux impératifs.

▪ Le Code de procédure civile pose uniquement le principe de la **communication simultanée des pièces** avec les conclusions, sans impartir de délais (art. 906).

▪ En revanche, il impose des délais applicables, soit à l'appelant, soit à l'intimé, pour le dépôt de leurs conclusions (art. 908, 909 et 910). Ainsi, de la combinaison de ces dispositions, l'Assemblée plénière opère la distinction suivante :

- si les **conclusions** elles-mêmes ont été **signifiées dans des délais** procéduraux impératifs mais que les pièces ne le sont qu'ultérieurement, alors il appartiendra aux juges d'appel de les écarter ou non après avoir analysé si la partie adverse a ou non disposé du temps nécessaire pour pouvoir répondre à ces pièces communiquées tardivement ;

- en revanche, si les conclusions elles-mêmes ont été **signifiées en dehors des délais** procéduraux impératifs, alors les pièces communiquées à l'appui des conclusions irrégulières doivent automatiquement être écartées des débats.

▪ Dans cette seconde hypothèse, la cassation n'est cependant pas encourue s'il est prouvé que la cour d'appel ne s'est pas fondée sur les pièces litigieuses pour prendre sa décision.

Les enjeux

Dans la procédure d'appel en matière contentieuse avec représentation obligatoire, les pièces sont écartées des débats si l'on ne maîtrise pas parfaitement les règles.

(1) Cass. Ass. plén. 5-12-2014, n° 13-19674 et n° 13-27501

(2) En principe, en matière civile, un justiciable ne peut intervenir directement devant la cour d'appel et doit être représenté par un avocat, par exemple : demandes de dommages et intérêts, contentieux contractuels, etc.

Les conseils

Dans une procédure d'appel avec représentation obligatoire, la priorité doit être de signifier les conclusions, dans les délais impartis par les articles 908 et suivants du Code de procédure civile, et ce même si les pièces le sont ultérieurement.

MARIE-ADELAÏDE DE MONTLIVAULT-JACQUOT
LAURE LALOT

QUAND L'AUDIT DEGENERE…

Continuité, confidentialité et outils de mesure intrusifs

▪ Après avoir diligenté **plusieurs audits**, un célèbre éditeur de logiciels s'est vu rejeter par les titulaires de licences les **demandes de régularisation** qui en ont découlées. Il a donc décidé de porter les affaires en justice, considérant que ses clients outrepassaient leurs droits acquis en vertu des contrats de licences.

▪ La première décision (1), rendue en référé, apporte de précieux enseignements relatifs à l'emploi d'outils de mesure des utilisations d'un logiciel par un client.

▪ Le juge rejette la demande de l'éditeur visant à ordonner l'exécution de scripts sur le système d'information du client, considérant que les pouvoirs dont il dispose en vertu des articles 145 du Code de procédure civile et L.332-1-1 du Code de la propriété intellectuelle ne lui permettent pas d'ordonner une telle mesure.

▪ En revanche, et compte tenu de la probabilité démontrée d'un écart entre le nombre de licences acquises et leur utilisation réelle, la demande légitime d'expertise judiciaire de l'éditeur a été accueillie. Il appartiendra le cas échant à l'expert désigné par le tribunal d'inviter le client à passer ces scripts, après avoir pris les précautions nécessaires pour garantir la continuité de fonctionnement du système d'information de l'audité, et la confidentialité des informations recueillies non indispensables à sa mission.

▪ Le tribunal affirme également que l'éditeur ne démontrait, ni même alléguait l'existence d'une obligation contractuelle d'exécution de ces outils informatiques de collecte d'information. Il n'en faut pas moins pour apercevoir dans cette décision les premiers contours d'un principe de continuité du système d'information et de confidentialité des données stratégiques comme limite à l'obligation contractuelle de coopérer à un audit…

Qualification des écarts et abus de droit d'auditer

▪ Dans la seconde affaire (2), ce même éditeur a, suite à plusieurs audits et tentatives de rapprochement amiable infructueuses, assigné son client sur le terrain notamment de la contrefaçon. Il sollicitait dans ce cadre la condamnation de ce dernier à lui verser plus de 10 millions d'euros pour utilisation non autorisée de logiciels et de services de support associés.

▪ La juridiction, statuant au fond, relève tout d'abord que le logiciel en question avait été livré par l'éditeur suite à la commande d'une solution globale par le client et installé par un intégrateur tiers. Après avoir préféré la qualification contractuelle à celle de contrefaçon, le tribunal conclut que l'éditeur ne pouvait pas légitimement soutenir que le logiciel n'était pas inclus dans le périmètre du contrat de licence et rejette ses demandes

▪ L'utilisation d'un logiciel hors du périmètre du contrat ne peut faire l'objet d'une action en contrefaçon, mais seulement d'une action en responsabilité contractuelle. Cependant, le tribunal mentionne explicitement le fait que l'éditeur ne soutenait pas que le client ait « utilisé un logiciel cracké ou implanté seul un logiciel non fourni », ni même que le nombre de licences ne correspondait pas au nombre d'utilisateurs effectifs du logiciel. Dans ces hypothèses, la question majeure de la qualification de contrefaçon ou de manquement contractuel reste donc entière…

▪ Le tribunal affirme enfin que la pratique consistant à multiplier des audits à des fins de pression commerciale fait dégénérer ce droit en abus sans pour autant condamner l'éditeur, faute pour le client de démontrer le préjudice en découlant.

L'essentiel

L'utilisation d'outils de mesure des licences intrusifs ne peut être imposée ni par le juge des référés, ni par l'éditeur.

Un droit d'audit peut dégénérer en abus et les écarts qu'il révèle ne relèvent pas nécessairement de la contrefaçon.

(1) TGI Nanterre réf, 12-6-2014, Oracle Corp., Oracle France c. Carrefour Org. et Systèmes Gpe

(2) TGI Paris 3e ch. 1re sect. 6-11-2014, Oracle Corp., Oracle Fce c. AFPA

L'enjeu

Piloter efficacement les audits et maitriser les risques de dépassement des licences.

MARIE SOULEZ

NICOLAS DUBOSPERTUS

VALIDITE DES CLAUSES LIMITATIVES DE RESPONSABILITE SUR LA PERTE DE DONNEES.

La clause limitative de responsabilité pour les contrats de maintenance

▪ En matière de contrats de maintenance informatique, le prestataire peut éviter d'engager pleinement sa responsabilité s'il perd les données de son client par l'effet d'une clause limitative à ce titre.

▪ **Perte de données et clause limitative de responsabilité.** La validité d'une clause limitative de responsabilités pour perte de données a été analysée dans un jugement relatif aux contrats de maintenance informatique.

▪ Lors d'une intervention de maintenance d'un parc informatique, un prestataire a perdu les données sauvegardées sur les serveurs de sa cliente. En se référant au contrat, les juges ont appliqué la clause limitative de responsabilité et condamné la société de maintenance à indemniser sa cliente de la somme dérisoire de 7 280 €. Le préjudice réel était chiffré à 158 345,95 € (1).

▪ **La perte de données n'est pas, à elle seule, une faute lourde.** Les juges auraient pu écarter la clause en considérant que la perte des données par la société de maintenance informatique constituait une faute lourde.

▪ Celle-ci est caractérisée par une négligence d'une extrême gravité confinant au dol et dénotant l'inaptitude du débiteur de l'obligation à l'accomplissement de sa mission contractuelle. Les juges ont considéré qu'aucun comportement exceptionnellement grave n'avait été démontré (2).

▪ **L'obligation essentielle du contrat doit être maintenue, même s'il contient une clause limitative de responsabilité.** Les clauses limitatives sont appréciées de façon subjective, par référence aux circonstances de la clause.

▪ Les juges prennent en considération l'absence de contradiction entre la clause et la substance de l'obligation essentielle (3). Ce point n'a pas été retenu dans la décision rendue par le Tribunal de commerce Nanterre en mai 2014 (1).

La clause limitative de responsabilité pour les contrats cloud

▪ Une obligation essentielle des contrats cloud est assurément que le prestataire maintienne les données dans les serveurs sous sa responsabilité. Dans ce cadre, il est probable que la solution précitée diverge dans un contrat cloud.

▪ Cependant, plutôt que de discuter d'une telle clause devant un juge, il est préférable de le faire **avant de signer tout contrat**.

▪ En conséquence, pour être indemnisé à hauteur du préjudice subi, tout client souhaitant migrer ses données dans le cloud doit impérativement veiller à **négocier soigneusement la clause** écartant ou limitant la responsabilité du prestataire à ce titre.

▪ Dans une perspective de nécessaire recherche d'un **équilibre**, le plafond de responsabilité doit être évalué **en fonction des risques réels** encourus et des incidences concrètes pour l'utilisateur.

▪ Le cabinet propose une démarche de type **benchmark** permettant de trouver la solution la plus adaptée.

Les enjeux

La clause limitative de responsabilité s'applique en cas de perte de données dans le cadre de l'exécution d'un contrat de maintenance.

(1) TC Nanterre 2e ch. 2-5-2014.
(2) JTIT n° 152 – Décembre 2014, p 5
(3) Cass. com. 29-6-2010 n°09-11841.

Les conseils

Négocier avec soin les clauses responsabilité et préjudice.

Prévoir un montant d'indemnité forfaitaire, évalué en fonction du risque réel.

ERIC LE QUELLENEC
DANIEL KORABELNIK

LES NOUVELLES PRECISIONS DE L'ADMINISTRATION SUR LE FICHIER DES ECRITURES COMPTABLES

La comptabilité au moyen de systèmes informatisés

▪ Depuis le **1er janvier 2014**, les contribuables qui tiennent leur comptabilité au moyen de systèmes informatisés ont l'obligation, **en cas de contrôle fiscal**, de présenter leurs documents comptables sur support dématérialisé en remettant au vérificateur un fichier des écritures comptables (FEC) devant satisfaire à différentes normes (1).

▪ L'administration a mis en ligne sur son site internet www.impot.gouv.fr à la rubrique « le contrôle fiscal et la lutte contre la fraude » un document sur le FEC sous la forme d'une liste de questions/réponses apportées par le service du contrôle fiscal aux différentes questions portées à son attention.

▪ Ce document publié pour la première fois au mois d'avril 2014 a été dernièrement actualisé le 19 **décembre 2014** et comporte des précisions et de nouvelles tolérances administratives sur les points suivants.

Les nouvelles tolérances administratives

▪ **Auto-entrepreneur.** L'auto-entrepreneur est dispensé de présenter un fichier des écritures comptables (FEC) lorsqu'il tient sa comptabilité au moyen de systèmes informatisés.

▪ **Micro-entreprise**. Pour les contribuables imposables à l'impôt sur le revenu dans la catégorie des micro-bénéfices industriels et commerciaux (BIC) et micro-bénéfices non commerciaux (BNC), qui tiennent un état récapitulatif de leurs recettes sur un registre papier ou un tableau et confient la tenue de leurs comptabilité à un tiers, ce dernier peut saisir en comptabilité ces opérations par récapitulation au moins mensuelle, et non trimestrielle, des totaux de ces opérations. Il est donc toléré, sous conditions, que le fichier des écritures comptables (FEC) ne comporte pas le détail des écritures comptables des recettes. Cependant, le contribuable devra être en mesure de présenter, quelle qu'en soit la forme, papier ou tableur, le détail de ses recettes, ainsi que les pièces justificatives afférentes (par exemple, les rouleaux de caisse enregistreuse). En revanche, si le contribuable, quel que soit son régime d'imposition, enregistre, pour partie, ses écritures comptables dans un logiciel comptable et transfère ses données à un tiers pour que ce dernier tienne sa comptabilité de manière dématérialisée, le FEC doit comprendre, dans ce cas, le détail des écritures comptables hors écritures de centralisation.

▪ **Transcodage et libellé en langue étrangère**. L'administration avait initialement indiqué qu'à compter de l'exercice 2014, le transcodage des écritures ne respectant pas les normes comptables françaises, ne sera plus accepté et la comptabilité devra être tenue conformément aux normes comptables françaises et en langue française. Par mesure de souplesse, la tolérance est prolongée aux exercices clos en 2014. Cependant, à compter des exercices clos en 2015, le transcodage ne sera plus admis dans le FEC de même que les libellés en langue étrangère.

▪ **Société Civile Immobilière (SCI)**. Les SCI sont tenues de fournir un FEC en cas de vérification de comptabilité dès lors qu'elles tiennent leurs documents comptables sous une forme informatisée. Par mesure de tolérance, les SCI soumises exclusivement aux revenus fonciers et qui ne comportent que des associés personnes physiques sont dispensées de présenter un FEC.

Les enjeux

Pour les contrôles pour lesquels l'avis de vérification est adressé depuis le 1er janvier 2014, les contribuables qui tiennent leur comptabilité au moyen de systèmes informatisés doivent la présenter sous forme de fichiers dématérialisés (FEC).

Les conseils

Pour vous aider dans la mise en œuvre de ce fichier des écritures comptable (FEC), l'administration a établi sur son site une liste de questions /réponses et mis à disposition des entreprises un outil logiciel pour vérifier la conformité de leur fichier des écritures comptables avec les normes exigées.

(1) CGI LPF, art L 47 A-I et A 47 A-1.

PIERRE-YVES FAGOT

L'EMPLOYEUR PEUT LIRE LES SMS SUR LES TELEPHONES PROFESSIONNELS

Présomption de caractère professionnel des SMS

▪ Tout salarié est présumé savoir que son employeur est en droit d'accéder pour un motif légitime au contenu de son téléphone portable professionnel et notamment à ses SMS. Ainsi peut être interprété l'**arrêt rendu le 10 février 2015** par la chambre commerciale de la Cour de cassation (1).

▪ En l'espèce, afin de prouver un **débauchage illicite**, un employeur avait produit en justice les SMS échangés par son salarié avec des tiers au moyen de son téléphone portable professionnel.

▪ Le salarié soutenait que l'accès de l'employeur aux SMS enregistrés sur son téléphone portable professionnel, sans en être informé au préalable, était attentatoire à sa vie privée (2) et constituait donc une **preuve illicite**.

▪ La Cour de cassation considère que « les messages écrits (SMS) envoyés ou reçus par le salarié au moyen du téléphone mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère **professionnel**, en sorte que l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ».

Un droit d'accès pour un « motif légitime »

▪ Ce faisant, la Cour de cassation **transpose aux SMS** les solutions dégagées sur d'autres supports numériques, dossiers, fichiers sauvegardées sur l'ordinateur professionnel, méls échangés sur la messagerie électronique de l'employeur. Ils sont présumés être professionnels sauf s'ils sont identifiés comme personnels.

▪ L'employeur doit justifier d'un « motif légitime » pour accéder au contenu des SMS enregistrés sur les téléphones professionnels de ses employés. En l'espèce, des **soupçons de débauchage** ont été jugés constitutifs d'un **motif légitime**.

▪ Le salarié contestait avoir été informé du droit de l'employeur de lire les SMS enregistrés sur son téléphone professionnel. En effet, l'employeur ne l'avait pas expressément informé de ce droit et la charte des systèmes d'information de l'entreprise ne le prévoyait pas expressément.

▪ Pour rejeter cet argument, la Cour de cassation a probablement pris en compte le fait qu'aucun dispositif de contrôle a priori des SMS n'avait été mis en place dans l'entreprise, l'employeur n'était donc pas tenu à une information préalable.

▪ La solution dégagée est cohérente avec l'**état actuel du droit** : de même que l'employeur peut prendre connaissance d'une correspondance laissée sur le bureau d'un salarié, d'un fichier informatique enregistré sur son poste de travail ou des méls échangés par sa messagerie professionnelle, il peut accéder aux SMS enregistrés sur le mobile mis à la disposition de son employé, sauf à démontrer que ceux-ci sont identifiés comme étant « personnels ».

▪ Ce **pouvoir de contrôle de l'employeur** ne saurait en revanche être admis sur un téléphone personnel, sauf si l'entreprise a mise en place une politique d'utilisation des appareils personnels à des fins professionnelles (« Byod ») et une solution logicielle permettant de séparer les usages personnels et professionnels de l'appareil (exemple : « Mobile management device » ou « MDM »).

▪ La Cour ne précise pas la manière d'identifier le caractère « **personnel** » d'un SMS. On peut supposer qu'en apposant la mention « [Personnel] » au début de chaque message, le salarié puisse interdire à l'employeur d'ouvrir ce message hors sa présence. Et si l'employeur passe outre cette mention en ouvrant le SMS sans en avertir au préalable le salarié, la preuve ainsi obtenue serait jugée déloyale et devrait être écartée des débats judiciaires.

L'enjeu

Avoir connaissance du contenu des téléphones portables mis à disposition du personnel.

Respecter la vie privée des salariés.

Lutter contre les actes de débauchage et de concurrence déloyale.

(1) Cass. com. 10-2-2015, n°13-14779.
(2) Code civil, art. 9.

Les conseils

- Encadrer l'usage du téléphone portable (heures de disponibilité, autorisation de l'utiliser à des fins personnelles).

- Mettre en place des solutions de type MDM (Mobile Device Management) afin de séparer les usages professionnels et privés du téléphone.

- Prévoir dans la charte des systèmes d'information une mention exprès sur le droit de l'entreprise d'accéder aux SMS échangés sur les téléphones portables professionnels.

- Mettre en place une charte « Byod » (« Bring your own device »).

EMMANUEL WALLE
ETIENNE MARGOT-DUCLOT

HEBERGEMENT DE DONNEES DE SANTE : IMPACT DU PROJET DE LOI DE SANTE.

La procédure d'agrément en vigueur

▪ La règlementation en vigueur impose aux professionnels de santé (PS), aux établissements de santé (ES) et à la personne concernée de recourir à un hébergeur agréé à cet effet, en cas d'externalisation de l'hébergement de données de santé à caractère personnel (1).
▪ Les ES et PS hébergeant eux-mêmes les données de santé des patients dont ils assurent la charge sont dispensés de la procédure d'agrément.
▪ A ce jour, la personne qui confie à l'hébergeur des données (le déposant) est tenue de recueillir le consentement exprès de la personne concernée au titre de l'hébergement, des modalités d'accès et des modalités de transmission (1).
▪ Ce consentement n'est pas requis dès lors que seul le déposant accède aux données de santé hébergées (1).
▪ Le projet de loi de santé n°2302 déposé à l'Assemblée nationale le 15 octobre 2014 modifie cette procédure.

La nouvelle procédure

▪ Les articles 25 et 51 du projet de loi modifient l'article 1111-8 CSP et en particulier habilitent le gouvernement à prendre par voie d'ordonnance des mesures de simplification de la procédure dans un délai de douze mois à compter de la promulgation.
▪ La loi sera a priori d'application immédiate, et l'ordonnance modifiant le décret hébergement sera prise dans le délai susvisé. A l'issue de ce délai, un référentiel précisant le contenu du dossier devrait être établi (2).
▪ Le régime transitoire ne dispensera pas de la nécessité de disposer d'un agrément.
▪ Le projet de loi supprime la référence aux PS, ES et personne concernée de sorte que **tout responsable de traitement de données de santé à caractère personnel** doit respecter l'obligation de recourir à un tiers agréé pour l'hébergement de données de santé (art.25-IV).
▪ L'hébergement sera réalisé après que « *la personne en a été dûment informée et sauf opposition pour un motif légitime* » (art.25-IV). Cette nouvelle disposition **dispense le déposant du recueil d'un consentement exprès** tel que prévu dans le régime actuel, sous réserve de la délivrance d'une information préalable.
▪ L'ordonnance définira les **conditions dans lesquelles le médecin de l'hébergeur peut accéder aux données de santé à caractère personnel**. Les contrats devront donc être mis à jours afin d'intégrer ces conditions (art.51-I-5).
▪ L'attestation de la conformité de l'hébergement aux exigences légales et règlementaires ne se traduira plus par la délivrance d'un agrément par l'Asip santé mais par celle d'une accréditation par l'instance nationale d'accréditation (art.51-I-5).
▪ Enfin, le projet de loi entend harmoniser cette nouvelle procédure d'accréditation et les dispositions du Code du patrimoine relatives à l'archivage (3) afin d'éviter que les établissements publics de santé et les établissements de santé privé d'intérêt collectif soient soumis à une double obligation lorsqu'ils confient les données de santé et leur archivage à un tiers hébergeur (art.51-I-5).
▪ En tout état de cause, l'objectif du projet de loi est toujours d'assurer la **confidentialité et la sécurité des données de santé.** Dès lors, **les conditions techniques nécessaires pour ce faire telles que mises en œuvre par les hébergeurs agréés à ce jour ne seront pas impactées**.

Les enjeux

Simplifier le système de santé et en particulier la procédure relative à l'hébergement des données de santé.

(1) CSP art.1111-8.

L'essentiel

L'hébergement externalisé de données de santé devra être accrédité, et non plus agréé.

Le consentement exprès du patient n'est plus requis.

(2) Décr. 2006-6 du 4-1-2006.
(3) C.patrimoine art.L.212-4.

MARGUERITE BRAC DE LA PERRIERE
ALIX D'OMEZON

Prochains petits-déjeuners

Les applications mobiles dans tous leurs états : 11 mars 2015

▪ . Céline Avignon animera un petit-déjeuner débat sur les applications mobiles et les risques pour l'entreprise au regard de la Cnil.
▪ Si les applications mobiles envahissent le quotidien de chacun en B to C (Réseaux sociaux Messagerie instantanée, Jeux, Vie pratique tel que météo et Google maps), elles s'attaquent également au marché dédié à l'entreprise avec des applications professionnelles et d'affaires (B to B) connectées au système d'information.
▪ Elles représentent un champ d'investigation pour la Cnil :
- Quels sont les principes qui doivent être respectés au regard de la loi Informatique et libertés ?
- Comment concevoir dans une démarche « privacy by design » efficace ?
- Quelle politique de confidentialité mettre en œuvre ?
- Comment assurer la gestion des données personnelles et l'information des personnes concernées ?
- Comment utiliser des cookies et autres traceurs en toute légalité ?

▪ Ce petit-déjeuner sera l'occasion de faire le point sur les risques juridiques et les moyens de garantir la protection du consommateur et de ses données personnelles dans les applications mobiles.

▪ **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.

Failles de sécurité : bilan et tendances : 25 mars 2015

▪ Virginie Bensoussan-Brulé et Chloé Torres animeront un petit-déjeuner débat sur les bons réflexes et les actions à mettre en œuvre en matière de failles de sécurité.
▪ L'obligation de notification des failles entraînant la divulgation ou l'accès non autorisé à des données personnelles pose une série de questions dont la résolution est d'importance du fait des sanctions pénales :
- Quelles sont les personnes soumises à cette obligation ?
- Qu'est-ce qu'une violation de sécurité : une faille ou un défaut ?
- Comment informer la Cnil et notifier les clients et partenaires?
- Quelles sont les » mesures de protection appropriées » et les actions qui doivent être mises en œuvre ?
- Quels sont les recours et sanctions en cas d'exploitation d'une faille de sécurité ?
- Comment ce cyber risque est-il couvert par les assureurs ?

▪ Ce petit-déjeuner sera l'occasion de dresser un état des lieux et de préciser les actions à mettre en œuvre par les entreprises en matière de failles de sécurité.

▪ **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.

Réalité virtuelle : 15 avril 2015

▪ Alain Bensoussan et Marie Soulez animeront un petit déjeuner débat sur l'impact des technologies immersives dites de « réalité virtuelle » ou « réalité de synthèse » sur le plan technique, économique et juridique.
▪ Dès 1997, alors que la réalité virtuelle semblait encore relever de la science-fiction, l'American Dialect Society qui détermine chaque année « the Word of the year » retient parmi les mots pertinents, « virtual » qu'elle associe à l'expression « virtual reality », rendant ainsi hommage à l'émergence d'une nouvelle technologie.
- Quel est l'état du droit positif ?
- Comment assurer la protection des environnements immersifs ?
- Comment assurer la protection des données personnelles des utilisateurs comme celles sur la géolocalisation ?

▪ Ce petit déjeuner sera l'occasion de faire le point sur le statut de la réalité virtuelle, ses risques juridiques et les moyens de garantir la protection de l'innovation, de l'utilisateur et de ses données personnelles.

▪ **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

La protection des données en Espagne: Questions les plus fréquentes

- **Lexing Espagne** a élaboré le chapitre espagnol sur la protection des données dans de la prestigieuse revue internationale « Data Protection and Privacy 2015 » éditée par Law Business Research Ltd.
- Cet ouvrage couvre une trentaine de législations sur la protection des données et la confidentialité des données.
- Chaque étude traite des questions les plus fréquentes en matière de violations de la protection des données, d'exemptions, d'autres lois connexes, de la notion de traitement légitime, des notifications de failles, des obligations de sécurité et des violations, des formalités d'enregistrement, des pénalités, des transferts et de l'utilisation d'Internet et des communications électroniques.

Télécharger le chapitre

Lexing Espagne, Marc Gallardo

Champ d'application territorial du règlement sur la protection des données

- **Lexing Belgique** annonce une **journée d'étude le 27 mars 2015** consacrée au droit international privé au quotidien.
- Le Comité National Belge de l'Union internationale des avocats (UIA) a décidé, en partenariat avec l'Ordre français des avocats du barreau de Bruxelles, de consacrer une journée d'étude à cette problématique d'actualité cruciale en Belgique, à savoir le droit international privé.
- Cette journée comprend deux volets : le premier abordera des questions touchant à la sphère économique, le second sera consacré à des questions relevant du droit familial et notamment à la protection des données personnelles.
- **Jean-François Henrotte** définira l'application territoriale du règlement 2006-2004 et les conséquences de la vaste réforme qui en est proposée par la Commission.

Programme de la journée d'étude du 27-3-2015.

L'appropriation de standards techniques par le droit des brevets : un abus de position dominante ?

- **Lexing Belgique** analyse les conclusions de l'Avocat Général Melchior Wathelet présentées le 20 novembre 2014 devant la Cour de justice de l'union européenne (CJUE, Huawei Technologies Co. Ltd, C-170/13) sur la question des liens étroits existant entre la **propriété intellectuelle** et le **droit de la concurrence**, en particulier dans le contexte de la normalisation technique.
- Cette affaire est à mettre en lien avec des arrêts précédents de la Cour de Justice (CJUE 2 mai 2012, affaire C-406/10), concernant l'**absence de protection des fonctionnalités d'un programme** d'ordinateur par le droit d'auteur.
- Dans les deux cas, l'on constate une tension entre l'intérêt du progrès technique et industriel (les entreprises doivent pouvoir réutiliser des fonctionnalités et se baser sur des normes techniques) et l'intérêt des titulaires de droit de propriété intellectuelle.

Alexandre CASSART, Actualité du 16-2-2015.

Lexing Belgique Philippe & Partners

Lutte contre le terrorisme : renforcement des dispositifs d'échanges d'information

▪ Le **décret 2015-174 du 13 février 2015** portant amélioration des échanges d'information dans le cadre de la lutte contre le terrorisme vise à renforcer les échanges d'information entre les autorités policières nationales et internationales (1).

(1) Décr. 2015-174 du 13-2-2015

Modernisation de l'Etat : un centre interministériel de services informatiques

▪ Le **décret 2015-144 du 9 février 2015**, paru au Journal officiel du 11 février 2015, crée un service à compétence nationale (SCN) à caractère interministériel dénommé « centre interministériel de services informatiques relatifs aux ressources humaines » (2).

(2) Décr. 2015-144 du 9-2-2015.

Dématérialisation des échanges avec les juridictions financières

▪ Le **décret 2015-146 du 10 février 2015** relatif à la dématérialisation des échanges avec les juridictions financières pose le principe de la dématérialisation des échanges de données et de la transmission des actes dans le cadre des procédures des juridictions financières (3).

(3) Décr. 2015-146 du 10-2-2015.

Fichier national des interdits de gérer

▪ Le **décret 2015-194 du 19 février 2015** définit les modalités d'inscription et de radiation des données du fichier national des interdits de gérer, ainsi que leur durée de conservation. Ce fichier national, créé afin de **lutter contre les fraudes** (4).

(4) Décr. 2015-194 du 19-2-2015.

Une nouvelle fiche technique portant sur les marchés négociés

▪ La DAJ a publié une nouvelle fiche technique sur son site Internet sur les marchés négociés de l'article 35 du code des marchés publics (5). Cet outil détermine le droit applicable à chaque hypothèse de marché négocié.

(5) DAJ, Fiche technique Conseil aux acheteurs du 12-2-2015.

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

Formations intra-entreprise : 1e semestre 2015

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

Archivage électronique public et privé	Dates
Gérer un projet d'archivage électronique : Intégrer les prérequis juridiques dans la conduite du projet et garantir la conformité des systèmes d'archivage électronique.	12-02 et 21-05-2015
Gérer les archives publiques électroniques : Comprendre les spécificités des archives publiques électroniques.	27-01 et 14-04-2015
Contrôle fiscal des comptabilités informatisées : 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	
Cadre juridique des achats : 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
Manager des contrats d'intégration et d'externalisation : Comprendre les particularités de l'intégration et de l'outsourcing et bien gérer l'exécution des contrats.	10-02 et 13-05-2015
Contract management : 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
Sécurisation juridique des contrats informatiques : Comprendre et mettre en œuvre les outils juridiques de sécurisation des contrats informatiques.	28-01 et 08-04-2015
Garantir la pérennité et le succès d'un projet informatique grâce au contract management Niveau 2 Expert: Gérer au sein d'un groupe de sociétés la signature et le bénéfice d'un contrat informatique.	30-01 et 31-03-2015
Les clés pour réussir son projet « Cloud computing » : Savoir définir une « cloud strategy »	04-02 et 19-05-2015
Conformité et risque pénal	
Risque et conformité au sein de l'entreprise : 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
Gérer une crise en entreprise : le risque pénal : Le risque et les principes. Comment s'annonce le risque et	20-03 et 19-06-2015
Informatique	
Edition de progiciel : Etat de l'art et tendances juridiques : Maîtriser le cadre juridique de l'édition logicielle pour gérer l'administration des parcs de progiciels.	16-01 et 10-04-2015
Traitement et hébergement des données de santé à caractère personnel : 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	
Commerce électronique : Acquérir les connaissances indispensables à la maîtrise des obligations principales d'un éditeur d'un site marchand.	29-01 et 18-03-2015
Webmaster niveau 2 expert : 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	
Audit du patrimoine intellectuel de l'entreprise : Détecter les forces, points de faiblesses et risques juridiques et financiers d'un portefeuille « Propriété Intellectuelle ».	12-02 et 16-04-2015
Protection d'un projet innovant : Présenter les spécificités juridiques relatives à un projet innovant afin de gérer les étapes d'une protection adaptée.	17-03 et 16-06-2015
Sensibilisation à la protection d'un portefeuille marque et nom de domaine : 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
Droit des bases de données : 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
Droit d'auteur numérique : Acquérir les bons réflexes pour protéger son patrimoine intellectuel et ne pas porter atteinte aux droits d'autrui.	03-02 et 29-05-2015
Lutte contre la contrefaçon : 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	
Médiation judiciaire et procédure participative de négociation : Comprendre le déroulement de la procédure de médiation judiciaire et de la procédure participative.	22-01 et 03-04-2015
Presse et communication numérique	
Atteinte à la réputation sur Internet : 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	
Informatique et libertés (niveau 1) : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	24-07 et 13-11-2015
Cil (niveau 1) : 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
Informatique et libertés secteur bancaire : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	20-01 et 04-03-2015
Informatique et libertés collectivités territoriales : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	15-04 et 24-06-2015
Sécurité informatique et libertés : 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
Devenir Cil : 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
Cil (niveau 2 expert) : 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
Informatique et libertés gestion des ressources humaines : 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
Flux transfrontières de données : 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
Contrôles de la Cnil : 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
Informatique et libertés secteur santé : 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
Informatique et libertés à l'attention du comité exécutif : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité.	Selon demande