

DONNEES PERSONNELLES

Citation : Caprioli & Associés, Données personnelles, www.caprioli-avocats.com
Première publication : juin 2005.

La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise

Eric A. CAPRIOLI, Docteur en droit, Avocat à la Cour de Paris, Caprioli & Associés (Paris, Nice)

www. caprioli-avocats.com
contact@caprioli-avocats.com

Plan

I/ REGIME JURIDIQUE DE L'ENTREPRISE QUALIFIEE DE FOURNISSEUR D'ACCES

II/ NOUVEAUX RISQUES, NOUVELLES RESPONSABILITES POUR L'ENTREPRISE

La Cour d'appel de Paris a rendu une décision particulièrement importante pour les entreprises qui fournissent des accès à l'internet à leurs salariés, alors qu'elles n'en fournissent pas à des personnes externes (Cour d'appel de Paris, 4 février 2005) [1]. Ces entreprises pourraient désormais être qualifiées de fournisseur d'accès à l'internet (FAI) au sens de l'article 43-7 de la loi du 30 septembre 1986, introduit par la loi du 1er août 2000 et, en vertu de cette qualité, être assujetties aux obligations et responsabilités qui pèsent sur cet intermédiaire technique, spécialement en ce qui concerne celle de la conservation des données de connexion pendant une durée d'un an maximum selon les cas. Cette obligation a été introduite par la loi sur la sécurité quotidienne (LSQ) du 15 novembre 2001 [2]. Passé ce délai, ces données relatives au trafic doivent être effacées ou anonymisées conformément à la loi, devenu l'article L.34 -1 du Code des Postes et communications électroniques (C.P.C.E.) après l'adoption de la loi du 9 juillet 2004 (J.O. du 10 juillet 2004) [3]. Cette disposition du C.P.C.E. a une application plus large étant donné qu'elle vise " *les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* ".

Dès lors que l'entreprise peut être responsable en cas de non fourniture des données de nature à permettre l'identification d'une personne en vertu de textes récents établissant le régime juridique des prestataires techniques [4], on peut s'interroger sur les conditions d'application des principes de responsabilité civile à l'entreprise du fait des fautes de ses salariés au cours de l'exécution de leurs contrats de travail.

En effet, outre ces obligations et responsabilité susceptibles d'être applicables à l'entreprise si la qualité de fournisseur d'accès était retenue, il est important d'identifier et de mesurer les risques juridique générés par l'utilisation de l'internet et des réseaux numériques par les salariés. Si ces risques se caractérisent par leur nouveauté, leur généralisation et les évolutions techniques rapides, ils restent régis par les règles de droit commun de la responsabilité civile (articles 1382 et suivants du code civil), inchangées ou presque depuis l'origine du code civil. Il appartient à la jurisprudence d'en faire une interprétation adaptée au nouveau contexte de l'entreprise communicante.

I/ REGIME JURIDIQUE DE L'ENTREPRISE QUALIFIEE DE FOURNISSEUR D'ACCES

Dans l'affaire de la Cour d'appel de Paris, deux agents commerciaux ont décidé de ne plus travailler avec la société qu'ils représentaient en Autriche et aux Etats-Unis d'Amérique après la perte de confiance en ladite société provoquée par la réception par chacun d'eux d'un mail anonyme selon lequel la société de presse en ligne (World Press Online) allait fermer. Les deux courriers électroniques avaient été envoyés à partir d'une adresse gratuite, et l'enquête auprès du fournisseur d'adresse a permis l'obtention de l'adresse IP de leur expéditeur : celle utilisée par le salarié d'une banque qui s'est avérée être celle d'un **routeur** de ladite banque.

La société demanda donc à la banque de lui communiquer les données d'identification de l'expéditeur de ces messages. Ses demandes restant sans réponse, la société assigna la banque en référé pour obtenir ces informations sur le fondement des articles 43-7 et 43-9 de la loi du 30 septembre 1986. Le 12 octobre 2004, le Tribunal de commerce de Paris a ordonné à la banque de " *communiquer l'identité et plus généralement de toute information de nature à permettre l'identification de l'expéditeur du message* ". En appel, la juridiction confirme l'ordonnance en ces termes : " *la demande de la société ne se heurte à aucune contestation sérieuse*

alors qu'en sa qualité, **non contestée**, de prestataire technique au sens de l'article 43-7 de la loi du 1er août 2000, la banque est tenue, en application de l'article 43-9 de ladite loi, d'une part, de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisition judiciaire. " Mais, la Cour tempère l'ordonnance en ce que " la loi du 1er août 2000 ne lui fait pas (à la banque) obligation de traiter les données qu'elle doit conserver et communiquer ni de procéder elle-même à l'identification de l'auteur du message litigieux, et d'autre part, qu'une telle recherche relève de toute évidence d'une mesure d'instruction que le juge des référés ne peut ordonner que sur un autre fondement que ceux sur lesquels il a été saisi dans le cadre de la présente instance. " Ainsi, l'objectif qui consistait à identifier l'auteur des messages pour d'éventuelles suites judiciaires n'est pas atteint ! On peut penser qu'en se fondant sur les articles 145 et 11 du N.C.P.C., il eut été possible de permettre cette mesure d'instruction visant à identifier une personne ayant contribué à un contenu[5] avant l'introduction de toute procédure contentieuse.

L'article 43-7 de la loi de 1986 précitée définit le FAI comme suit : " *Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communications en ligne autre que de correspondance privée (...)*". Or, étant donné que cet article a été abrogé par la Loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 [6], il convient de se pencher sur la nouvelle définition donnée à l'article 6 -I-1° de la LCEN " *les personnes dont l'activité est d'offrir un accès à des services de communications au public en ligne(...)*. " Elle vise clairement les FAI et on peut, en première analyse, supposer qu'une solution identique serait rendue sous l'empire de la LCEN étant donné que l'entreprise donne à ses salariés un accès vers l'internet. Pourtant, le caractère " *non contesté* " de la qualité de FAI par la banque devra être médité par les juristes. Envisagé sous cet angle, on peut penser que la qualification retenue et les conséquences en découlant sont susceptibles d'être entendues différemment par d'autres juridictions dans la mesure où les entreprises en général et les banques en particulier (mais aussi pourquoi pas, les collectivités publiques, telles que les administrations ou les collectivités locales), n'ont en aucune façon pour activité de fournir des accès à l'internet ou d'héberger des contenus autres que ceux liés à son activité économique. L'activité d'une entreprise est indiquée dans l'objet de ses statuts et elle se retrouve dans le code APE de ladite entreprise. Si la qualification de prestataire technique devait être retenue pour chaque entreprise proposant en interne d'accéder à l'internet, les obligations juridiques seraient considérables et les dommages pour les entreprises françaises seraient difficilement mesurables. Par conséquent, l'entreprise devrait conserver toutes les données de connexion relatives aux échanges et être en mesure de les communiquer à tout moment à l'autorité judiciaire. Une telle analyse extensive de la qualification de fournisseur d'accès ne nous semble pas conforme à la réalité juridique, même s'il faut en tempérer la portée dans la mesure où les données sont également susceptibles d'être conservées pour des besoins de facturation et pour la sécurité des réseaux. La traçabilité des échanges réalisés à partir des postes de travail appartenant à et sous la responsabilité de l'ent reprise nous semble une précaution juridique particulièrement importante en terme de sécurité des systèmes d'information.

II / NOUVEAUX RISQUES, NOUVELLES RESPONSABILITES POUR L'ENTREPRISE

L'obligation de détention et de conservation des données permet l'identification de toute personne ayant contribué à la création d'un contenu de services découlant de l'article 43-9 de la loi de 1986 par un prestataire technique a donné lieu à un jugement du TGI de Paris du 16 février 2005 [7]. Les données communiquées par le prestataire technique étaient pour le moins fantaisistes : " *Nom : Bande Prénom : Dessinée Date de naissance : 25/03/1980 Adresse : Rue de la BD Code postal : 1000 Ville : Bruxelles Adresse email de confirmation : pitbullteam@hotmail.com* " ; le tribunal juge qu'elles ne " *sont pas de nature à permettre l'identification de l'auteur du site litigieux* ". Elles ne sont pas conformes au texte. " *En manquant ainsi à l'obligation légale que lui imposait l'article 43-9, la société Tiscali Média a commis une négligence au sens de l'article 1383 du code civil et engagé dès lors sa responsabilité délictuelle envers les sociétés demanderesse. Cette faute a directement conduit à priver les demanderesse de la possibilité d'agir en réparation des actes de contrefaçon dont elles ont été victimes à l'encontre de leur auteur.* "

Le prestataire technique (ici un fournisseur d'hébergement) a manqué à son obligation légale de détenir et de conserver les données d'identification des personnes dont il héberge les contenus. Il aurait dû prendre un minimum de précaution en vérifiant les données d'identification fournies lors de l'enregistrement de l'abonné au service d'hébergement. A ce titre, le juge ordonne au prestataire technique d'indemniser les éditeurs de BD victimes de contrefaçon, du montant des dommages -intérêts auquel les sociétés demanderesse auraient pu prétendre si l'auteur du site contrefaisant avait pu être identifié.

Si ce raisonnement devait être repris pour les " *entreprises fournisseurs d'accès* " pour leurs propres besoins, cela pourrait vouloir signifier que ces dernières - en cas de non respect de cette obligation[8] - pourraient se voir condamner en lieu et place du salarié (non identifiable) auteur d'un comportement délictueux au paiement de dommages-intérêts du fait de ce comportement.

Enfin, plus généralement, il faut garder à l'esprit une autre donnée juridique essentielle : la responsabilité civile du commettant du fait de ses préposés telle que prévue à l'article 1384, al.5 du code civil. En effet, une fois le salarié identifié, la société ayant subi un préjudice du fait des communications électroniques est non seulement fondée à agir en réparation des préjudices subis contre celui-ci, mais également contre son employeur sur ce fondement certes classique, mais **facteur de nouveaux risques juridiques importants pour les entreprises** qui mettent à disposition de leurs salariés des connexions à l'internet et des services de messageries électroniques. A ce titre, on se rappellera que dans une affaire similaire, le TGI de Marseille avait jugé solidairement responsable une société qui avait fourni un accès à l'internet à l'un de ses salariés qui avait

diffusé des contenus préjudiciables sur l'internet par le biais de pages personnelles (TGI Marseille du 11 juin 2003) [9]. Les risques liés à ces nouveaux usages des outils (ordinateur, téléphones fixes et portables) et moyens informatiques et de communication électroniques (courriers électroniques, Sms, Mms, ...) sont nombreux : introduction de virus, enregistrements sur les postes de travail et diffusion de fichiers illicites ou sans droit, ..., ils varient en fonction du contexte et de l'organisation de l'entreprise.

Dès lors, pour les entreprises qui entendent se conformer à la présente décision, et plus largement pour une bonne gestion des risques juridiques, la solution consistera certainement à mettre en place, afin d'appréhender l'ensemble des dimensions, juridique, technique et organisationnelle, d'une part, des procédures de traçabilité et de conservation des données de connexion et des données échangées sur les réseaux utilisés par l'entreprise (intranet, extranet, internet, ...) [10] et d'autre part, des règles d'utilisation des moyens de communications électroniques et informatiques. A n'en point douter, la charte d'utilisation des moyens informatiques et de communications électroniques sera un instrument adapté à la résolution de ces difficultés [11], mais il faudra prendre en compte d'autres aspects tels que notamment, la politique de sécurité des systèmes d'information de l'entreprise et sa charte/politique relative aux données personnelles et au respect des droits fondamentaux.

Notes

[1] Disponible sur le site : www.foruminternet.org.

[2] En fait, il pourra être différé pour une durée maximale d'un an aux opérations tendant à effacer ou rendre anonymes certaines catégories de données techniques pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou pour les besoins de la facturation et du paiement des prestations de communications électroniques (art. L. 34-1 II et L. 34-III du Code des Postes et Communications Electroniques).

[3] Un décret en Conseil d'Etat, pris après avis de la CNIL, est attendu. Il doit déterminer les catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées, à ce titre, à la demande de l'Etat, par les opérateurs.

[4] On a estimé, à la suite de la directive européenne du 8 juin 2000, que les intermédiaires techniques (les prestataires de services à l'internet) devaient disposer d'un régime de responsabilité spécifique, adapté à leur situation.

[5] V. en ce sens, un des attendus de l'ordonnance de référé du TGI de Paris du 2 février 2004 (affaire Métrobus c./Ouvaton), disponible sur www.legalis.net, qui propose cette utilisation combinée des articles 145 et 11 du NCPC.

[6] JO du 22 juin 2004. Sur la LCEN, v. l'ouvrage sous la direction d'Eric Caprioli, La Loi pour la confiance dans l'économie numérique (LCEN), à paraître aux éditions L.G.D.J. en 2005.

[7] Disponible sur le site www.legalis.net.

[8] On peut penser que le non respect de l'obligation figurant à l'article 43-9 de la loi de 1986 s'entend de sa mauvaise exécution (conservation de données d'identification insuffisantes voire fantaisistes) mais aussi de son inexécution (absence de détention de ces données).

[9] TGI Marseille, 11 juin 2003, www.foruminternet.org et D. 2003, obs. Cédric Manara.

[10] Eric A. Caprioli, Responsabilité des prestataires de commerce électronique et conservation de données aux fins de traçabilité in Traçabilité et responsabilité, sous la responsabilité de Philippe Pédrot, éd. Economica, 2002, p. et sur le site : www.caprioli-avocats.com.

[11] Eric A. Caprioli, Cybersurveillance des salariés : du droit à la pratique des chartes " informatiques ", P. Aff. du 29 septembre 2004, p. 7 et s. et l'article de Nicolas Ivaldi " La cybersurveillance des salariés et charte informatique ", dans ce numéro.