DÉCEMBRE 2012

n°375

EXPERTISES

DES SYSTÈMES D'INFORMATION

LE MENSUEL DU DROIT DE L'INFORMATIQUE ET DU MULTIMÉDIA

INTERVIEW

GUILLAUME TEISSONNIÈRE

DE LA CONVERGENCE NUMÉRIQUE À LA CONVERGENCE DES DROITS

DOCTRINE

TÉLÉMÉDECINE

Cadre juridique des systèmes d'information et de la confidentialité des données

JURISPRUDENCE

DROIT D'AUTEUR

Validité des liens profonds

EXPERTISES
DES SYSTÈMES D'INFORMATION

SOMMAIRE n°375

ÉDITORIAL

INCONCILIABLES

Le pouvoir politique doit-il s'emparer de la question de la copie privée pour mettre fin à cet affrontement permanent qui oppose les ayants droit aux industriels et aux consommateurs depuis 2006 au sein de la commission éponyme ? C'est ce que pense Jean-Noël Tronc, directeur général de la Sacem. Pour cet ex-conseiller technique NTIC de Lionel Jospin, l'enjeu n'est plus juridique mais politique. Et il appelle le gouvernement à empêcher les industriels de torpiller le système de la rémunération pour copie privée. De leur côté, les industriels demandent aux pouvoirs publics de réformer un système jugé non conforme au droit communautaire, obsolète, anti-démocratique et anti-économique. Mais le gouvernement Ayrault qui n'a semble-t-il pas envie de s'en mêler fait la sourde oreille. Comme ses prédécesseurs du reste. Pourtant la situation s'aggrave et pourrait aboutir à une impasse. Faute d'avoir été entendus sur leur revendication de réforme du système et sur leur critique des nouveaux barèmes proposés par les ayants droit, cinq des six représentants du collège des industriels siégeant à la commission de la copie privée ont démissionné de leur fonction.

Celle-ci pourra-t-elle fonctionner sans une partie de ses membres (deux représentants du collège des consommateurs menacent de suivre l'exemple des industriels) ? De nouveaux barèmes doivent en effet être adoptés avant le 21 décembre 2012, échéance fixée par la loi du 20 décembre 2011. Les ayants droit pensent que c'est possible. C'est également l'avis de la ministre de la Culture Aurélie Fillipetti qui fustige cette politique de la chaise vide. Mais les industriels vont probablement dénoncer la décision devant le Conseil d'Etat. En vertu de la théorie de la « formalité impossible » appliquée en droit administratif, le Conseil pourrait cependant considérer la condition de la complétude impossible à remplir et rejeter ainsi le recours.

Les industriels attaquent sur un autre front, celui du Conseil constitutionnel. A la suite de l'arrêt Canal+ du Conseil d'Etat qui a jugé que les usages professionnels doivent être exclus du dispositif de compensation, la loi du 20 décembre 2011 avait laissé un délai d'un an pour remédier à la question de l'exonération des professionnels. Dans une décision du 17 octobre 2012, la Cour de cassation a jugé recevable la question prioritaire de constitutionnalité posée sur le II de l'article 6 de la loi de 2011.

Le système, que les ayants droit bénéficiaires de la rémunération souhaitent conserver tel quel, semble à bout. Depuis 2006, la guerre entre les membres de la commission est déclarée : cinq de ses décisions ont été annulées par le Conseil d'Etat et deux autres font l'objet d'un recours. Le dialogue est désormais impossible. Et la table-ronde organisée par la commission des affaires culturelles de l'Assemblée nationale, animée par Patrick Bloche (député PS), et qui s'est tenue le 21 novembre 2012, n'a dégagé aucune solution. Le système peut-il encore perdurer alors qu'il est censé fonctionner sur la base de la corégulation ? Une réponse politique s'impose.

Cybersécurité
Le partage « volontaire » de données personnelles avec les gouvernements

Suite au rejet par le Congrès américain d'un projet de loi sur le Partage et la protection de la cyber-intelligence, William B. Bierce présente les principales questions juridiques que pose tout projet de partenariat public-privé sur la cybersécurité : les divulgations volontaires de "bonne foi", les limitations de responsabilité pour de telles divulgations, la portée des droits du gouvernement d'utiliser toute information divulguée (y compris des données privées externalisées), et les conflits de droit avec des régimes juridiques étrangers.

La sécurité de l'internet et de la vie privée touche aussi bien le cloud computing, (1) l'informatique mobile et l'internet des objets (avec des capteurs et des ordinateurs dans les voitures et les matériels électriques). La cybersecurité a des implications profondes sur les entreprises, les « infrastructures critiques » et les individus, qui en dépendent de plus en plus dans la vie commerciale, économique, sociale et personnelle.

Selon des experts de la cybersecurité, la grande majorité des intrusions ne sont pas divulguées aux autorités pour des « raisons de securité » ou afin d'éviter l'embarras, donc, la perte d'image de marque (2). Vu la croissance des risques et des dépendances, la question se pose de savoir dans quelle mesure les entreprises « devraient » participer à des programmes gouvernementaux de cybersecurité, et les conditions qui seraient mutuellement acceptables, et ce malgré le rejet par le Sénat américain d'un projet de loi portant sur « la participation volontaire » du secteur privé à la cybersecurité gouvernementale.

Le 2 août 2012, le Congrès américain a en effet rejeté un projet de loi qui aurait autorisé les professionnels de l'informatique du secteur privé - que ce soit en interne ou en mode externalisé - de partager des informations de cybersécurité avec les autorités de la sûreté nationale. Le projet de loi sur le Partage et la protection de la cyber-intelligence (3) (CISPA) aurait permis (sans obligation) à l'entreprise de partager, « de bonne foi », des informations sur la cybersécurité et les cybermenaces avec le Department of Homeland Security.

Suite au rejet du texte, les rumeurs ont circulé sur le fait que le Président Obama allait établir par ordonnance un comité interdépartemental pour permettre un partenariat public-privé pour la coopération (opt-in) volontaire (4) et la fourniture de « best practices » pour des sociétés gérant les « infrastructures critiques ». Une telle ordonnance prévoit d'établir un conseil gouvernemental qui déterminerait les industries privées constituant « une cyber infrastructure critique » pour inciter le secteur privé à adopter volontairement des mesures de cybersecurité. Nominalement volontaires, de telles « best practices » risquent de devenir obligatoires, par exemple, pour ceux qui souhaitent fournir des biens ou services au gouvernement ou sa chaîne de fourniture, ou en cas de menaces de contentieux. En annonçant de telles « best practices », le gouvernement inviterait pratiquement tous les autres Etats (par exemple, la Chine ou la Russie) à réglementer l'internet. Et une bureaucratie décrétant des « standards » fixes s'exposerait ainsi à des voies d'attaques. Une telle réglementation manquerait de souplesse, d'hétérogénéité et de vitesse nécessaires face à des menaces de plus en plus complexes.

Nonobstant le rejet de ce projet de loi aux USA, le thème reste toujours d'actualité (5). Cet article explore les principales questions juridiques pour tout projet de partenariat public-privé visant les risques et la cybersécurité : les divulgations volontaires de "bonne foi", les limitations de responsabilité pour de telles divulgations, la portée des droits du gouvernement d'utiliser toute information divulguée (y compris des données privées externalisées), et les conflits de droit avec des régimes juridiques étrangers. Ces questions se posent aussi au niveau international, en particulier dans le monde du cloud computing, invitant le secteur privé à exercer une vigilance constante pour prévenir une « cybervoracité » gouvernementale de type orwellien (en établissant des conditions limitatives) et à préserver la confiance fondamentale avec des engagements en matière de sécurité.

L'APPROCHE AMÉRICAINE ÉCHOUÉE : UN PARTENARIAT PUBLIC-PRIVÉ

Les conflits d'intérêts gouvernementaux et privés

Globalement, le gouvernement poursuit plusieurs intérêts fondamentaux en matière de cybermenaces sur le secteur privé. Fondamentalement, tel que prévu dans le projet de loi américain, le gouvernement visait à protéger la défense nationale et la « base industrielle de défense », ainsi que les « infrastructures critiques » privées (transports, opérations bancaires, l'électricité, l'eau et d'autres services publics). Une cybersécurité gouvernementale efficace favorise la continuité du gouvernement, la prospérité économique et la qualité de vie en général.

Dans l'Union européenne, les mêmes buts gouvernementaux peuvent prévaloir sur tout intérêt privé d'un citoyen ou tout intérêt national. Les Etats membres conservent le pouvoir souverain d'adopter des mesures législatives afin de limiter certains droits privés dans la mesure où ces restrictions sont « nécessaires, appropriées et proportionnées » dans une société démocratique afin de sauvegarder la sécurité nationale (à savoir la sécurité de l'Etat), la défense, la sécurité publique, et la prévention, l'investigation, la détection et la poursuite de délits ou de l'utilisation, sans autorisation préalable nécessaire des systèmes électroniques de communication (6).

Quels que soient les lieux de ses activités commerciales, le secteur privé peut être confronté à des conflits d'intérêts, surtout pour ce qui touche à la confidentialité, avec ceux du gouvernement. Par exemple en matière de commerce B2B et B2C, chaque entreprise recueille et stocke des informations confidentielles de tiers, qui leur font confiance pour ne pas les diffuser sans autorisation. Tout transfert "B2G" « volontaire » de ces informations privées au gouvernement comporte des risques d'abus (que ce soit par négligence ou par intention) d'utilisation de l'information à des fins sans rapport avec les informations B2B et B2C.

Suivant sa localisation et son activité, chaque entreprise définit ses propres politiques de protection des données, les conditions de sécurité et de divulgation conformément à la classification des données. Celles-ci peuvent être soumises à des régimes juridiques différents. Ainsi elles peuvent être classées comme (i) des secrets commerciaux internes, (ii) des secrets commerciaux externes (les informations de tiers qui sont confidentielles, protégées par des obligations contractuelles de non-divulgation), (iii) des informations sur les employés, qui peuvent figurer dans un fichier d'emploi et un fichier de réglementation du droit du travail, (iv) des informations sur les activités ordinaires sur les transactions avec des clients (y compris des infos personnellement identifiables [PII], (v) des informations relatives aux cartes de crédit et à la démographie, et (vi) des informations relatives à la conformité de l'entreprise avec les lois, comme par exemple les documents comptables, fiscaux et réglementaires. En sus, des lois étrangères peuvent s'appliquer (tels que les directives de l'Union européenne) aux PII et aux accords entre les contrôleurs de données (« data controllers » et les responsables de traitement (« data processors »).

Les conditions préalables à une limitation de responsabilité pour des divulgations volontaires de l'information sur la cybersécurité

Le projet de loi CISPA aurait octroyé une exemption générale contre toute réclamation de toute personne concernant la divulgation de renseignements confidentiels dans le cadre d'un échange volontaire de données avec le gouvernement en matière de cybersécurité. Les entreprises privées aurait eu une immunité illimitée contre toutes actions civiles ou pénales devant les tribunaux américains intentées contre une entité ou ses dirigeants, employés ou agents qui révèleraient « de bonne foi » des informations sur leur usage des systèmes de cybersécurité ou l'identification de cybermenaces. Cette limitation de responsabilité avait été conçue comme une incitation des acteurs du secteur privé à contrôler la robustesse de leurs propres systèmes et réseaux ainsi que ceux de leurs clients et à partager des informations sur les cybermenaces et les vulnérabilités afin de mieux protéger leur systèmes.

De la « bonne foi »

Pour éviter d'éventuels abus, le projet de loi CISPA aurait limité cette exonération à des cas de « bonne foi ». La preuve de cette « bonne foi » aurait été un élément indispensable à toute exonération légale.

Le critère de la « bonne foi » aurait cependant exposé le secteur privé à des aléas, des coûts et des détournements. Il aurait été susceptible de générer des litiges. Ce critère était trop flou, trop vague et trop imprévisible dans chaque cas de « divulgation volontaire ». Les tribunaux aurait été obligés de se prononcer sur la légitimité et la portée de la responsabilité dans des cas particuliers, tels que les cas d'intentions "mixtes" bonnes et « non autorisées ».

Des intentions de poursuivre la cybersecurité

Pour cerner la limitation de la responsabilité, le projet de loi aurait exigé que l'entreprise privée ait une intention expresse de soutenir la cybersecurité, particulièrement pour surveiller ses systèmes ou réseaux afin d'identifier et d'obtenir des informations sur des cybermenaces. Tout autre but n'aurait pas justifié une immunité de poursuite judiciaire par des tiers. Comme la « bonne foi », cette limitation souffre d'ambiguïté. Comme dans la preuve d'un délit, les intentions délictuelles de l'acteur seraient mises en cause.

De nouveaux risques pour les entreprises, les individus et le gouvernement

Un tel projet de loi aurait également exposé les fournisseurs de technologies de l'information et de l'information à des coûts, des risques et de la confusion.

Le manque de confiance du client

Cette loi risquait d'ébranler les liens de confiance entre la société commerciale

(ou les fournisseurs ou gérants de systèmes d'informations tels que les fournisseurs d'accès à internet) et son client. Sans autorisation contractuelle, les fournisseurs, les prestataires et les gérants auraient été placés en difficulté face à leurs obligations de non-divulgation. Chaque prestataire et chaque licencié aurait dû obtenir l'accord préalable pour faire de telles divulgations. Et les fournisseurs auraient naturellement voulu être indemnisés pour toute réclamation dans le cadre d'un tel partage avec le gouvernement.

Une avalanche de contentieux

Le principe législatif d'une telle exonération de responsabilité aurait provoqué des contentieux contre toute société partageant les informations relatives à la cybersecurité avec le gouvernement. Dans un système juridique permettant des « class actions », pour protéger des victimes de la même violation de droits, des avocats créatifs auraient pu intenter des procès, demander des audiences préliminaires et harceler le « volontaire » selon la procédure civile de la « découverte » avant la présentation du cas au décideur des faits (la « divulgation » de preuves ou d'informations susceptibles de mener à des preuves) . Dans le cas du projet de loi CISPA, de tels frais de justice aurait été à la charge de l'accusé, même pour défendre une action en justice légalement empêchée. En bref, le secteur privé aurait été toujours menacé d'avancer les frais de justice et de consacrer du temps pour se défendre contre de telles poursuites.

Les réclamations financières contre le gouvernement

Quelle aurait été la responsabilité financière du gouvernement pour dédommager de ses erreurs ou de ses abus, en se fondant sur une loi qui autorise le partage volontaire d'informations et qui engage le gouvernement à ne pas abuser de secrets commerciaux ou de données confidentielles ? Selon le projet de loi CISPA, si le gouvernement avait abusé des informations ainsi reçues dans le cadre de la cybersecurité, il aurait été responsable des dommages réels et tenu de payer les frais d'avocat. Le projet de loi aurait ouvert les portes à des contentieux contre le gouvernement, en cédant volontairement sa souveraineté à des fins limitées, modifiant ainsi le « Federal Tort Claims Act ». Quel cadeau pour les avocats qui auraient pu porter plainte contre les victimes de ces cas de divulgations ou d'utilisations fautives ! Quelle charge pour le contribuable et le Trésor public !

Des risques d'abus gouvernementaux

Deux types d'abus gouvernementaux sont envisageables dans un partenariat public-privé pour la cybersecurité. En premier lieu, les citoyens ne pourraient ni savoir ni prouver des manquements gouvernementaux. Le projet de loi aura interdit au gouvernement d'utiliser l'information privée à des fins autres que la cybersécurité. Mais une telle utilisation aurait été presque impossible à vérifier, sinon prouver. Le « partenariat » dévaluerait la confiance des clients, des individus, des employés, des prestataires, des cédants de licences, etc. dans leurs propres secrets commerciaux. Certains ont conclu que les informations gouvernementales auraient été suffisamment protégées, mais pas les informations personnelles identifiables (PII). Personne ne pourrait dire si la divulgation volontaire de renseignements auto-incriminants pourrait entraîner une poursuite réglementaire concernant des défaillances ainsi portées à l'attention du gouvernement.

En deuxième lieu, le projet de loi aurait pu permettre des abus gouvernementaux de données personnelles collectées indûment dans le cadre d'une divulgation sur la cybersecurité. Le gouvernement fédéral aurait pu utiliser les informations privées pour d'autres fins gouvernementales (quoique légitimes), à la seule condition qu' « au moins un but important » de l'utilisation par le gouvernement de l'information ait été dans le cadre la cybersécurité ou de la sécurité nationale des Etats-Unis. Cette exception a été un facteur dans la défaite de ce projet de loi, car elle aurait ouvert la boîte de Pandore avec des conséquences imprévues pour l'entreprise privée.

Des risques d'abus privés

Le projet de loi CISPA aurait permis au secteur privé de partager sans limite l'information avec le gouvernement. Il n'y aurait pas eu de restrictions quant à la nature, le volume ou le but (dès l'instant qu'il y avait le degré minimum préalable de « bonne foi » dans l'intention de protéger les données). En l'absence de telles restrictions, toute entité privée aurait pu librement divulguer au gouvernement beaucoup d'informations, sans prendre de précautions pour modérer les divulgations non nécessaires à la cybersecurité.

On peut imaginer des scénarios typiques de bavure ou de divulgation grossièrement excédentaire. Ainsi, un hôpital aurait pu transférer au gouvernement certaines données sensibles du malade, sans prendre de précautions pour nettoyer ou effacer des données médicales qui pourraient être utilisées dans le cadre d'une discrimination illégale en matière d'emploi (par exemple, les maladies sexuellement transmissibles, l'orientation sexuelle, SIDA, les troubles génétiques, des caractéristiques ethniques, le cancer ou autre maladie potentiellement mortelle ou une condition médicale relative à un handicap). Cela comportait un risque de piratage et d'utilisation non autorisée.

Une telle approche dépasserait les limites des mesures nécessaires à la protection de la vie privée selon le droit de l'Union européenne et de celui du Canada, par exemple (7). Donc, une « solution » législative « à l'américaine » aurait entravé le commerce international de prestations américaines de traitement de données européennes ou canadiennes, sans mentionner de pays tiers.

Les limitations de la souveraineté : des conflits de loi

Dans un monde intégré, les incidences juridiques de toute « divulgation volontaire » d'informations sur la

cybersécurité et les cybermenaces dépassent les frontières nationales. Tout octroi par un gouvernement (par exemple, les Etats-Unis) d'exonération de responsabilité n'équivaut pas à une immunité dans d'autres pays. Une société américaine aurait été confrontée à un risque de poursuite par des gouvernements étrangers et ses clients, ses fournisseurs étrangers et sa chaîne de la valeur ajoutée étrangère. Une telle limitation légale de responsabilité soulèverait des questions de réciprocité, de reconnaissance et de représailles par tout autre gouvernement. Selon la loi entre Etats souverains, un pays peut empêcher ses ressortissants de continuer l'exportation de données aux USA, comme le font certains pays cherchant à limiter la prolifération nucléaire.

L'APPROCHE EUROPÉENNE DURABLE

Des alternatives moins contraignantes. Le débat américain sur le partage volontaire d'informations privées pour la cybersecurité (et incidemment sur l'impact sur la vie privée) invite à une recherche d'alternatives moins intrusives et plus équilibrées.

Conseils inter-gouvernementaux

Dans l'Union européenne, une approche de conseils « indépendants » intergouvernementaux existe pour ces questions, mais cela concerne en premier lieu la protection de la vie privée. Le groupe de travail de l'article 29 (« G29 ») sur la protection des données à caractère personnel, qui dispose d'un pouvoir consultatif, rédige des avis et des rapports indépendamment de la Commission européenne. Le G29 a été établi par l'article 30 de la directive 95/46/EC du Parlement européen et du Conseil européen du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement de données personnelles. Ses membres représentent les autorités de contrôle de chaque Etat membre. Il a établi son propre règlement de procédure interne (8). Il vient justement de rendre un avis à la Commission en février 2012 sur le cloud computing.

Associations commerciales

Aux Etats-Unis, les associations commerciales sont habilitées à organiser une action en concertation pour plaider leurs intérêts communs devant le Congrès. Les « lobbies » peuvent donc promouvoir des approches favorisant les prestataires ou les entreprises (les responsables de traitements).

Adoption de standards

Les organismes nationaux et internationaux cherchent déjà des standards pour la transparence, le libre-échange de données et la sécurité des échanges, du traitement et des supports de données.

Des alternatives plus contraignantes

Des conventions internationales. Les conventions internationales peuvent adopter de nouveaux standards juridiques dans le droit de l'internet (9). Vu les limites de la souveraineté pour exonérer le secteur privé de sa responsabilité civile pour des manquements aux obligations liées à la vie privée, les chefs d'Etats pourraient penser à une stratégie diplomatique par la voie d'une convention internationale. Les contours d'une telle solution existent déjà avec la notion de « protection adéquate » pour les données de la vie privée d'après l'Union européenne (10).Selon un accord entre les USA et l'UE, les manquements d'une société américaine à ses obligations (volontairement souscrites dans le cadre de l'accord sur le Safe harbor) la soumettraient à des procédures administratives et judiciaires du gouvernement américain. En vertu des Binding corporate rules (contrats-type entre responsables de traitement et prestataires), les sociétés commerciales présentes dans plusieurs pays s'engagent à respecter des normes internationales de la directive sur la protection des données à caractère personnel. Reste à décider les conditions substantives des obligations et droits des citoyens et de sociétés sous une telle convention. Ce serait la déclaration d'une nouvelle guerre froide, entre « blocs » de pays, ciblant des pays ou blocs « voyous » et les cellules terroristes.

De la surveillance interne gouvernementale

Au lieu d'un partenariat public-privé, on peut imaginer que les Etats optent pour des solutions utilisant les méthodes d'espionnage, peut-être soutenues par des « conseils » ou « best practices », inspirées de l'exemple chinois de surveillance généralisée. Le législateur canadien étudie actuellement un projet de loi qui permettrait le cyberespionnage des communications internes canadiennes, soit avec une autorisation judiciaire, soit par ordonnance du gouvernement (11). L'administration canadienne pourrait prendre des mesures de cyberespionnage sans autorisation judiciaire, moyennant une appréciation préalable de plusieurs considérations d'ordre public :

a) « *la mesure dans laquelle l'exemption est susceptible de nuire à la sécurité nationale ou au contrôle d'application des lois ;*

b) le fait que les opérateurs de télécommunications visées ont la capacité ou non d'exécuter les obligations en cause ;

c) le fait que les dépenses liées au respect des obligations en cause auraient ou non des effets négatifs injustifiés sur les activités commerciales des opérateurs de télécommunications ;

d) le fait que l'exécution des obligations en cause entraverait ou non sérieusement la prestation de services de télécommunication aux Canadiens ou la compétitivité de l'industrie canadienne des télécommunications (12) ».

UNE STRATÉGIE DE MANAGEMENT EN INFORMATIQUE ET TÉLÉCOMS

Les avocats dans le domaine des systèmes d'information peuvent aider les entreprises, les PME, les prestataires et les multinationaux en matière de cybersecurité. Toute proposition de régime volontaire de partage d'informations liées à la cybersécurité pose quelques questions pour l'avenir de l'externalisation et de la chaîne d'approvisionnement fiable pour les entreprises mondiales. La profession juridique peut poser des scénarios et les conseiller sur leurs interêts dans ce type de législation.

• Quelle est la responsabilité des prestataires de service pour les politiques de l'entreprise client ?
• Quelles conditions générales s'y appliqueraient, si le prestataire de service estimait bon de promouvoir le partage volontaire avec le gouvernement ?
• Comment peut-on limiter la responsabilité civile ? Une divulgation « volontaire » peut-elle être justifiable en cas d'événement de «force majeure» ?
• Serait-il plus prudent d'attendre une obligation légale ? Et de séparer les données privées des autres données sur la plateforme et les logiciels y afférents ?

Bref, le conseil juridique a un intérêt à connaître la structure technique des plateformes et à guider le client dans les évolutions de ces projets de lois.

UNE SYMBIOSE INÉLUCTABLE

En conclusion, l'expérience législative américaine suggère que la coopération « volontaire » privée avec les forces de police et de la sécurité nationale serait une mauvais idée, que ce soit aux USA ou ailleurs, pour les entreprises, les fournisseurs de données privées ou les titulaires de droits de propriété intellectuelle.

En Europe, l'ancienneté des directives sur la protection des données personnelles (1995) et celle sur le commerce électronique (2000) démontre qu'il existe un équilibre qui favorise les libertés de la vie privée, mais qui protège pourtant les intérêts gouvernementaux. Suite à cette tentative législative aux USA, les autres pays devraient réfléchir avant de s'embarquer sur un « partenariat » avec le secteur privé en matière de cybersecurité.

Peut-être que les USA devraient repenser la structure débridée et labyrinthique de leurs lois sur la vie privée (sous l'autorité de plusieurs agences publiques habilitées) visant à protéger le consommateur (13), le consommateur financier (14), le malade (15), l'employeur ou tout autre victime (16) d'un accès non autorisé à des systèmes d'information privés, l'individu européen (17), la défense nationale ou n'importe qui (18). Ou bien les Américains devraient s'organiser pour placer les intérêts privés au-dessus des intérêts gouvernementaux. Le rejet de ce projet de loi démontre qu'ils parcourent un chemin plus en faveur de la vie privée et de la protection des secrets commerciaux, mais qu'un juste équilibre reste un rêve des services gouvernementaux.

Cela dit, le secteur privé n'existerait plus en cas de cyberguerre. Au niveau technique, les secteurs public et privé restent symbiotiques et interdépendants. Par exemple, le virus Stuxnet qui, selon les journaux, avait été développé par un ou deux gouvernements comme outil d'espionnage contre l'Iran, a également infecté le réseau informatique commercial de Chevron Corp. en 2010, et en riposte d'autres sociétés internationales ont été la cible de cyberattaques (19). Cette interdépendance mérite des engagements mutuels entre les deux secteurs, et peut-être des moyens de protéger les « volontaires » sur le plan international, sans nourrir la cybervoracité (et promouvoir des conséquences non intentionnelles) des gouvernements des masses de données externalisées, qui ne sont pas indispensables à la cybersecurité.

William B. BIERCE

Membre des barreaux de New York et du New Jersey
Licencié en droit français (Grenoble)
Cabinet Bierce & Kenerson, P.C. (New York)

(1) Article 29 Working Party, Avis 05/2012 sur le Cloud Computing, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Selon cet avis, "When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor i.e., according to Directive 95/46/EC "the natural or legal person, public authority, agency or any other body that alone or jointly with others, processes personal data on behalf of the controller." p. 8 (version anglaise).
(2) R. King, "Virus Aimed at Iran Infected Chevron's Computer Network," Wall Street Journal, le 9 nov. 2012, p. B1, cols. 1-2; p. B2, cols. 1-2 (ci-dessous "Virus Aimed at Iran").
(3) "Cyber Intelligence Sharing and Protection Act." D'autres abus de l'Internet, telles que les contrefaçons, ont suscité d'autres propositions régimes réglementaires, tel que la Stop Online Piracy Act ("SOPA") et la Protect IP Act ("PIPA"). Ils auraient permis les propriétaires de droits d'auteur à bloquer les sites sans examen judiciaire préalable (ou minimalement) et à demander des dommages-interêts de toute partie contractant avec de telles sites. Comme CISPA, PIPA et SOPA ont été rejetés.
(4) J. Blagdon, "After CISPA's failure, White House considers executive order to implement cybersecurity law," The Verge blog, http://www.theverge.com/2012/9/8/3303258/cybersecurity-executive-order-obama-white-house. Opinion editorial, "Harry Reid's Virus," Wall St. Journal, le 16 nov. 2012, p. A16, cols. 1-2, prévoyant le schéma du Cybersecurity Act of 2012, S. 3414, 112eme Cong., 2d Sess.
(5) Le Représentant Michael Rogers (R-Mich.), Président de la US House Intelligence Committee, cherche à poursuivre la discussion, nonobstant l'echec. https://rt.com/usa/news/cispa-rep-bill-rogers-937/ .
(6) Art. 15(1), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), JO (UE) Official Journal L 201 , 31/07/2002 P. 0037 – 0047, "32002L0058," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.
(7) Voir le "Personal Information Protection and Electronic Documents Act" ("PIPEDA"), gérée par le Commissariat à la Protection de la Vie Privée du Canada, http://www.priv.gc.ca/leg_c/frame/index_e.asp.
(8) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/rules-art-29_en.pdf, adopté le 10 février 2010.
(9) Voir, par exemple, le Anti-Counterfeiting Trade Agreement du 2 oct. 2010, signé par l'Australie, les Etats-Unis, le Japon, le Maroc, la Nouvelle Zélande, la Republique du Corée et le Singapour, portant sur les contrefaçons de droit d'auteur par des services de l'Internet. http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/intellect_property.aspx?view=d.
(10) Voir le protocole internationale sur les "Safe Harbor Privacy Principles" entre le Departement du Commerce et la Communauté européenne en matière de la protection de données personnelles en provenance de la CE, le 21 juillet 2000, http://ita.doc.gov/td/ecom/menu.html (ci-dessous, "Safe Harbor").
(11) "An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts," Bill C-30, First Session, Forty-first Parliament, 60-61 Elizabeth II, 2011-2012 (Feb. 14, 2012), http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5380965 (texte bilingue).
(12) Id., l'art. 32(2).
(13) Voir la législation de presque chaque état sur la "security breach notification" (la notification aux autorités et aux clients de la perte de confidentialité) en cas de brèche de dossiers sur au moins 5,000 personnes par incident.
(14) Voir la Bureau of Consumer Financial Protection, établie sous la Dodd-Frank "Consumer Financial Protection Act" de 2010.
(15) Health Insurance Portability and Accountability Act de 1996 ("HIPAA"), et ses réglement sur la "securité" et la "privacy," 45 CFR 160 et 164, établissant des standards nationaux afin de protéger les archives médicaux d'individus et d'autres renseignements personnels, et qui s'applique aux prestataires de service médicaux, des échanges "clearinghouses" pour les transactions médicales, et d'autres qui communiquent de tells informations électroniquement.
(16) Voir la Computer Fraud and Abuse Act of 1986, 18 USC 1030.
(17) Voir "Safe Harbor" ci-dessus.
(18) Voir le role de la Federal Trade Commission et des Attorneys-General des états, par exemple.
(19) Voir la note 1 supra, "Virus Aimed at Iran."

consentir à l'acquéreur d'un certain volume de licences une réduction sur le prix de celles-ci l'on été réalisé par le biais de Microsoft France (au droit de laquelle est venu Microsoft France) ;

Attendu que les relations se sont poursuivis avec Microsoft France au-delà de la souscription des licences et que le demandeur produit une série de courriels échangés entre Microsoft France et Creno Impex au cours des années 2009 et 2010 quand aux contrats de licence et de maintenance souscrits ;

Attendu que la demande de Creno Impex ne porte pas sur les conditions d'application ni le quantum des remises prévues par les contrats de 2004 et 2008, mais sur le comportement de Microsoft France à l'occasion de la vente des contrats de licences et de maintenance et que ces contrats de remises sur volume n'ont été qu'un élément des négociations commerciales ;

Attendu dès lors que d'un litige entre deux commerçants établis en France, les juridictions commerciales françaises sont compétentes, que Microsoft Business Solutions ayant fait élection de compétence devant le tribunal de commerce de Paris au titre du contrat de 2004, celui-ci est donc compétent pour connaitre de la demande d'annulation de licences de Creno Impex ;

Dès lors le tribunal rejettera l'exception d'incompétence soulevée par Microsoft en faveur des juridictions Irlandaises et se déclarera compétent pour connaitre du litige opposant Creno Impex et Microsoft France et à défaut de contredit dans les délais légaux le tribunal fait injonction à Microsoft France de conclure au fond dans un délai de six semaines et reverra la cause à l'audience collégiale du 26 novembre 2012 pour conclusions ;

Attendu que l'application de l'article 700 du cpc est sollicitée ; qu'il convient toutefois de surseoir à son application jusqu'à l'issue de la procédure au fond ;

Attendu que la société Microsoft France est déboutée, elle sera condamnée aux dépens de l'incident ;

DECISION

Par ces motifs le tribunal statuant publiquement par jugement contradictoire et en premier ressort :

- Dit l'exception d'incompétence soulevée par la société Microsoft France recevable mais mal fondée,
- Se déclare compétent pour connaitre du litige, et à défaut de contredit dans les délais légaux le tribunal fait injonction à Microsoft France de conclure au fond dans un délai de six semaines et reverra la cause à l'audience collégiale du 26 novembre 2012 pour conclusions,
- Droits et moyens réservés
- Condamne la société Microsoft France aux dépens de l'incident.

Le tribunal : *M. Ankri (président)*

Avocats : *Me Louvet, SCP August et Debouzy Avocats*

EXPERTISES

DES SYSTÈMES D'INFORMATION

54, rue de Paradis - 75010 Paris
Tél : 33 (0)1 40 59 60 61
Fax : 33 (0)1 40 38 96 43
expertises@expertises.info

Directeur de la publication : Raphaël d'Assignies Fondateur : Daniel Duthil Rédactrice en chef : Sylvie Rozenfeld sr@expertises.info Tribunes et chroniques : William B. Bierce - Sébastien Briois - Stéphanie Fauconnier Mélaine Lecardonnel - Myriam Quéméner - Sylvie Rozenfeld - Nicolas Samarcq - Guillaume Teissonnière Maquettiste : Odile Rogerg Diffusion et abonnements : abonnement@expertises.info Création graphique : Christine Dufaut pour l'Agence Adéquat Impression : Futurnet Imprimerie 156 rue Oberkampf, 75011 Paris

Formation : Cette publication peut être utilisée dans le cadre de la formation permanente.
11 numéros par an. France : 251,54 € dont TVA 2,10%. Etranger : 266,79 €. Voir le bulletin d'abonnement dans ce numéro. Publié par Celog - R.C. Paris B 308 950 260. N° commission paritaire publications et agences de presse : 0513 T 88093. Dépot légal : novembre 2012