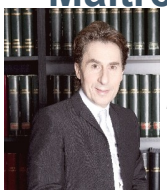
Maître Bensoussan répond à vos questions



Le site Copwatch ayant pour objectif de surveiller la vie tant publique que privée des policiers et gendarmes, a créé une véritable polémique, en octobre denier, à tel point que le ministère de l'Intérieur a déposé un référé visant à obtenir le blocage de ce site Internet, demande acceptée le 14 octobre 2011. Vous promettiez alors de revenir sur ce sujet…

La décision est dans le prolongement de mon premier commentaire. Il est évident que la diffusion de propos injurieux et diffamatoires et la collecte et la diffusion de données personnelles en violation de la loi Informatique et libertés ont été reconnues par le tribunal. Nous avons donc une application classique de l'article 6-I.8 de la LCEN[1] qui permet au juge des référés de faire cesser de tels actes dans ce domaine. Par contre, l'innovation repose sur le fait que le tribunal a prévu qu'en compensation, l'État devra dédommager les fournisseurs d'accès Internet (FAI) pour la mise en place de ces mesures de filtrage. C'est donc une très grande avancée dans ce domaine ; nous allons voir comment ceci va pouvoir s'appliquer, et s'il va notamment y avoir appel.

Plus d'une trentaine de sites miroirs, c'est à dire des copies du site Copwatch, ont vu le jour, depuis, relayant les informations qu'il contenait...

En ce qui concerne ces sites miroirs, un des grands problèmes de l'Internet est qu'il n'existe pas de convention internationale pouvant empêcher ce phénomène. En conséquence de quoi, la façon de gérer ce type de problématique est très différente entre les pays anglo-saxons et les pays romano-germaniques. Si nous prenons l'exemple des Etats-Unis, la question de la liberté d'expression apparaît dès le Premier Amendement de la Constitution des États-Unis d'Amérique. Nous ne pouvons donc que constater une grande disparité dans l'interprétation de cette liberté, une certaine limite quant à une décision nationale- en témoignent cette grande résistance, via tous ces sites miroirs- et toute la difficulté de la régulation par le droit d'Internet.

La Communauté urbaine de Strasbourg déploie la technologie du paiement sans contact, en commençant par ses 765 horodateurs, qui vont être progressivement équipés d'une solution de paiement sans contact par carte de crédit ou téléphone portable. Ayant bénéficié d'une dérogation exceptionnelle de l'Etat, elle envisage d'utiliser cette technique pour gérer des informations ou des services d'accès dans les domaines des transports, de la culture, du tourisme ou des services à la personne. Cette avancée technologique est-elle suffisamment bien cadrée juridiquement et ne comporte t'elle pas de risques ?

Dans le domaine des micro-paiements, l'équilibre est recherché entre la sécurité juridique et la baisse extrêmement importante des coûts que permet le recours à la technologie du sans contact. L'approche est assez similaire à celle qui a été menée dans le domaine des cartes bancaires, même si les montants sont plus élevés et la sécurité plus importante. Les cartes bancaires sont parvenues à un tel haut niveau de sécurité qu'on peut parler de fiabilité. Pour le micro-paiement et le paiement sans contact, si le niveau de sécurité requis est plus faible, il n'en est pas moins important. Mais, le point le plus délicat, dans ce type de technologie, n'est pas le couple « sécurité/fraude » mais « sécurité/confidentialité » (notamment les aspects relatifs à la vie privée).. La capacité, pour une technologie de type NFC sans contact (Near Field Communication), de se déployer de manière sereine, est directement liée à la maîtrise des aspects de confidentialité par l'ensemble des acteurs impliqués dans le dispositif.

Par exemple, il convient de veiller à ce qu'il y ait une attribution d'un alias (identification unique d'un mobile) différent pour chaque fournisseur de services de façon à ce que le recoupement d'informations sur les services utilisés ne puisse être effectué[2].

En tout état de cause, la ville de Strasbourg fait preuve d'une attitude innovante dans la façon de collecter les recettes publiques. Elle a en effet bénéficié d'une dérogation exceptionnelle de la Direction générale des finances publiques (DGFIP) pour permettre aux strasbourgeois de régler leur stationnement à l'aide d'une carte ou d'un téléphone mobile NFC / sans contact. Par ailleurs, nous disposons d'un recul technologique et des usages suffisants sur les puces NFC qui montrent que le système est parfaitement opérationnel.

Une proposition de loi relative à l'aggravation de la peine encourue pour l'usurpation d'identité commise par le biais de réseaux de communication électronique a été déposée, le 18 octobre dernier, par le Député UMP Jean Grenet. Pourriez-vous nous en expliquer l'objectif et le contenu ?

La tendance générale est de considérer que, dans cette période très particulière du développement d'un monde virtuel, la fraude électronique doit être sanctionnée de manière plus sévère, compte tenu de son absence de visibilité. Dans le monde réel, en général, la fraude est détectable dans un délai assez bref. Dans le monde virtuel, la fraude est assez transparente du fait de l'opacité des systèmes d'information. Elle peut prendre des formes très singulières et ne pas apparaitre immédiatement, empêchant alors la victime de réagir suffisamment vite. Il en est ainsi en matière d'usurpation d'identité. De plus, pour la plupart des infractions commises à travers Internet- c'est-à-dire sur le plan juridique un réseau de communication électronique ouvert ou non au public- l'élément matériel fait l'objet d'une aggravation de peine. Cette proposition de loi entend doubler les peines encourues lorsque l'usurpation est effectuée « au moyen d'un réseau de communication électronique » (et non pas seulement Internet), portant ces dernières à deux ans d'emprisonnement et 30 000 euros d'amende (contre actuellement : un an d'emprisonnement et 15 000 € d'amende ; ces mesures ont pour objectif de lutter contre l'absence de visibilité par la victime de la fraude, pendant un temps qui peut être très long. Par ailleurs, avec le développement des connaissances techniques par les particuliers et la faiblesse des systèmes de sécurité mis en œuvre, le risque devient très important et il convient de mettre en place une politique de dissuasion beaucoup plus forte tant dans le monde virtuel que ce qui peut exister dans le monde réel.

Le 3 novembre dernier, a été publié le décret d'application n° 2011-1431 [3], modifiant alors le code de procédure pénale en autorisant la conduite d'écoutes informatiques ou captations de données informatiques. Un juge d'instruction, après avis du procureur de la République, peut désormais requérir de différents services de police et de gendarmerie qu'ils procèdent à « l'installation des dispositifs techniques permettant la captation de données informatiques. » Quelles implications ce décret entraîne t-il?

Il est vrai que la Loppsi 2 (article 36) autorise le juge d'instruction, après avis du procureur, à permettre la mise en place d'un dispositif technique ayant pour objectif d'accéder à des données informatiques, sans avoir besoin du consentement des intéressés, de les enregistrer voire les transmettre. Un juge peut donc potentiellement valider l'installation d'un programme dit « espion », et détenir les matériels de captation informatique (comme le mouchard informatique). On voit bien que nous avons, dans ce domaine, la même situation que nous avions pour les réseaux de communication électronique. Aujourd'hui, chacun d'entre nous peut se transformer en un « James Bond Junior ». Il est très facile d'intercepter, d'espionner, de pirater un système car les technologies aujourd'hui disponibles, sont à la portée des utilisateurs, sans avoir besoin de connaissance technique importante. De ce fait, il était déterminant de fixer la liste des services habilités à détenir les matériels de captations informatiques (« mouchards informatiques ») et à procéder à leur installation. Le décret du 3 novembre 2011 désigne différentes entités, plus en termes de directions que de services. Certains auraient voulu qu'on restreigne davantage la liste pour permettre un contrôle plus direct, mais la fraude informatique prend une telle ampleur qu'il est bien évident que travailler à l'extérieur des organisations telles qu'elles existent aujourd'hui constituerait un frein à la lutte contre la criminalité binaire.

Sources

(1) Loi n° 2004-575 du 21 juin 2004
(2) Préconisation faite par la Cnil dès 2010 lors du déploiement des services sans contact mobile dans le cadre de l'expérimentation menée à Nice
(3) Décret n° 2011-1431 du 3 novembre 2011 :