Maître Bensoussan répond à vos questions

"Privacy by Design", DAS, INDECT, big data, drones… le spécialiste en droit des technologies avancées, Maître Alain Bensoussan vous révèle tout sur les grandes tendances en matière de technoprotections.

Quelle est l'actualité dans le domaine de la protection des données personnelles à l'heure où nombre d'entreprises françaises sont en train de réfléchir à une approche "PbD" ?

Des entreprises anticipent la prochaine adoption du projet de règlement européen dont la règle du « Privacy by Design » (PbD) sera une exigence essentielle. Cette règle du « Privacy by Design » est appelée à se généraliser dans la mesure où elle est expressément prévue dans le projet de règlement européen visant à réformer la directive n° 95/46/CE relative à la protection des données à caractère personnel (article 23).

L'idée sous-tendue est que la réglementation Informatique et libertés n'est pas une problématique de « formalité » mais bien une problématique de « conformité ». Ainsi, en contrepartie de la suppression des obligations administratives de déclarations préalables, les entreprises vont devoir garantir la conformité des traitements à la loi et concevoir des logiciels (et leur paramétrage) conformément à la nécessité de protéger les données personnelles. Le potentiel intrusif de certaines technoprotections exige en effet que la vie privée et la protection des données personnelles soient prises en compte dès le départ, c'est-à-dire dès la conception de la nouvelle technologie et tout au long de son cycle de vie. La règle du « Privacy by Design » consiste à concevoir des produits et des services en prenant en compte dès leur conception, les aspects liés à la protection de la vie privée et des données à caractère personnel.

Elle implique également le respect de ces valeurs tout au long du cycle de vie de la technologie concernée. Ce qui a pour conséquence que les dossiers de spécifications fonctionnelles, les cahiers des charges des utilisateurs, les dossiers d'analyse fonctionnelle, c'est-à-dire les spécifications générales et les spécifications détaillées qui vont servir au paramétrage ou au développement spécifique, vont devoir tenir compte des contingences Informatique et libertés qui sont au nombre de trois :

- le caractère adéquat, pertinent et non excessif des données collectées et traitées. Ce caractère va être remplacé par des dossiers minima, c'est-à-dire que dans la nouvelle réglementation, il faudra justifier de la nécessité de traiter de manière nominative certaines données ;
- l'intégration dans les traitements des mécanismes de consentement des personnes. La réglementation Informatique et libertés en Europe impose, sauf exception, un mécanisme de consentement qui n'est généralement pas intégré dans les phases de collecte ;
- une durée de péremption, donnée par donnée, au regard de chacun des traitements. Une donnée peut être gérée dans un seul traitement comme dans plusieurs traitements. Sa durée de péremption est donc à envisager à travers le couple « données-traitement ».

Bon nombre d'entreprises ont d'ores et déjà adopté cette approche qui sera dans les tout prochains mois rendue obligatoire, le projet de règlement devant aboutir à une publication fin 2013, début 2014 *(Lire aussi la proposition de règlement 2012-0011 (COD) 25-1-2012 : http://www.alain-bensoussan.com/wp-content/uploads/226468461.pdf)*.

S'agissant d'un règlement européen, il ne fera pas l'objet d'une transposition dans les droits nationaux et sera applicable tel quel dans toute l'Union européenne deux ans après sa publication, soit début 2016.

Comment trouver un juste équilibre entre protection de la vie privée et évolutions des technoprotections dans ce domaine ?

Après les événements du 11 septembre 2001, il est clair que la vidéosurveillance a laissé place à la vidéoprotection. La demande sociale a évolué pour mettre en avant des préoccupations de protection plutôt que de libertés individuelles *(Lire aussi "De la vidéosurveillance aux technoprotections", Le Figaro Blog expert du 20-7-2010 : http://blog.lefigaro.fr/bensoussan/2010/07/de-la-videosurveillance-aux-technoprotections.html)*.

Il est tout à fait notable que la liberté sans sécurité n'a pas vraiment d'existence. On s'aperçoit que les technologies nouvelles – biométrie, reconnaissance faciale, identification vocale, détections de comportements anormaux, vidéo… – sont des outils qui permettent, non seulement d'organiser la surveillance, mais d'assurer la « tranquillité » des personnes. Tout ce qui était considéré comme liberticide est aujourd'hui revu et corrigé à travers le prisme de la « liberté ». Cette dernière reste prédominante, mais elle va bien au-delà de la protection : il s'agit du droit à la tranquillité. L'évolution des technologies de protection s'oriente vers cela. C'est une tendance que l'on retrouve dans beaucoup de législations où ses outils doivent bien sûr être au service de la lutte contre les agressions, mais également de la prévention de ces dernières. Il semble que l'on évolue de la « réaction » à la « prévention » par exemple, lorsqu'il s'agit d'effectuer une levée de doute et ainsi limiter les interventions humaines. L'usage des drones à des fins civiles mais aussi de la vidéoprotection, permet de garder une zone calme par dissuasion plutôt que de calmer une zone par répression.

L'usage civil des drones ou robots aériens sans personnes à bord permet, à la fois, d'assurer la surveillance et la sécurité de certains lieux inaccessibles ou à risque : surveillance des ouvrages d'art, diagnostic de barrages, secours aux victimes, protection civile, sécurité urbaine, etc. Bien qu'il n'y ait pas de cadre juridique spécifique pour ce type d'usage en France, les robots aériens sont néanmoins soumis aux mêmes contraintes réglementaires que les systèmes de vidéosurveillance compte tenu de leur potentiel considérable en termes d'observation, d'acquisition et de transmission de données, ainsi que de géolocalisation.

Cette situation a d'ailleurs conduit la Cnil à entamer une réflexion prospective sur l'usage des drones va se généraliser aux usages civils. Ces derniers peuvent aujourd'hui surveiller une forêt pour vérifier qu'il n'y a pas de feu et surveiller aussi la tranquillité. Ils peuvent aussi surveiller une manifestation pour anticiper des débordements. Les technoprotections sont à mon sens, les éléments clé pour préserver la démocratie et respecter la liberté dans un monde sécurisé *(Lire aussi l'article Cnil du 30-10-2012 : http://www.alain-bensoussan.com/avocats/drones-et-robots-aeriens-cadre-juridique-et-ethique-a-definir/2013/04/19)*.

Avec le Big data et l'analyse comportementale, que devient l'anonymat au sein de l'espace public ? Quelle place vont prendre les projets de recherche DAS de la police de New York et INDECT au niveau européen ?

Le droit à la tranquillité qui est une exigence tout aussi importante que le droit à la sécurité impose aux pouvoirs publics d'intervenir, voire même de prévenir l'infraction, « Voir et Éviter ». Partant de ce constat, les projets DAS (Domain Awareness System : littéralement, Système de connaissance du domaine) ou INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment : littéralement Système d'information intelligent soutenant l'observation, la recherche et la détection pour la sécurité des citoyens en milieu urbain) sont des projets qui ont vocation à intervenir sur réaction mais aussi d'anticiper.

Ils visent à détecter les comportements suspects ou anormaux à l'aide d'un réseau de caméras et de capteurs et ont en commun de laisser des systèmes automatisés définir ce qui est suspect et ce qui ne l'est pas en d'autres termes, de faire du profilage. Aujourd'hui, ce sont quand même des projets de protection *via* les technoprotections, mais ce ne sont pas encore des projets de « technoprévention ». Les technologies peuvent en effet être classées en trois catégories selon la fonction assurée :

- la technosurveillance (loi Pasqua) ;
- la technoprotection (Loppsi 2) ;

Maître Bensoussan répond à vos questions *(suite)*

- la technoprévention dont relève notamment le projet américain DAS ; ce dernier comporte un logiciel capable de rechercher les zones d'infractions avant qu'elles ne soient commises.

Ces outils interviennent quand même en mode « réaction » – service d'urgence – mais à travers la prise en compte de la vitesse de réaction, d'intervention et de répression. En couplant la vidéoprotection et, de manière générale, la connaissance du terrain et l'usage des données collectées et traitées en grand nombre (big data), l'idée est de donner une réponse la plus mesurée possible et la plus rapide possible à un acte délinquant.

C'est bien dans le domaine mi-protection, mi-sécurité que ce type de services se développe. Il est clair que ce type de projets est appelé à se développer à condition d'en contrôler les éventuelles dérives. Ils sont à la tranquillité ce que sont les études épidémiologiques à la santé. Il existe en effet un lien fort entre sécurité et santé ; dans l'un comme dans l'autre, il faut réagir le plus rapidement possible et pour cela, ne pas uniquement regarder l'étude de cas. On va essayer d'utiliser toutes les informations que l'on a sur la maladie pour pouvoir éviter le développement épidémiologique. De la même manière ici, on va disposer d'un ensemble d'informations pour permettre d'arrêter le plus rapidement l'infraction, mais surtout pour protéger les victimes.

La légitimité de ce type de projets est d'être efficace sur le terrain de la sécurité, mais surtout sur celui de la tranquillité. Bien évidemment, il faudra mettre en place des garde-fous car si la légitimité de ces services s'inscrit dans le cadre de la demande sociale de protection et de sécurité, il faut qu'il y ait des barrières éthiques et juridiques pour encadrer d'éventuelles dérives. Il est vrai que le Droit se trouve légèrement en retard en ce qui concerne l'encadrement de ce type de pratiques. Il faudra mettre en place des chartes de comportement et surtout des règles pour sanctionner les dérives.

Il n'est pas question de renoncer à ce type de services qui correspond à la demande sociale mais il faut être sûr que le niveau d'encadrement soit suffisant pour éviter des comportements liberticides. Il est clair qu'actuellement, il y a un déficit juridique. Notamment l'utilisation dans les espaces publics des technologies de big data entraîne la possibilité de pouvoir anticiper des comportements. Ces outils sont des outils intermédiaires qui vont aller de la protection vers la prévention. Suspecter l'ensemble de la population n'a aucun sens. En revanche, utiliser le Fichier national des empreintes génétiques (FNEG) ou des fichiers comportementaux, permettrait d'accélérer l'intervention et de ne pas attendre qu'un individu passe à l'acte. Le couplage des technoprotections en temps réel avec les fichiers de police généraux ou segmentés, constitue un défi pour les libertés. On ne peut pas admettre une société dans laquelle on est tous suspect ; en revanche, il n'est pas admissible, de ne pas intervenir alors qu'on dispose de tous les éléments qui rendent vraisemblables la réalisation d'une infraction par un récidiviste.

Il faut redéfinir un principe de proportionnalité. On peut supposer que le principe de prévention rend admissible le recours à la vidéoprotection pour intervenir avant qu'il y ait une nouvelle victime. Les outils algorithmiques de calcul permettent de détecter un coefficient de suspects mais ces technologies doivent être encadrées et ne pas faire de chacun d'entre nous un suspect.

Internet est un formidable outil de partage à l'échelle mondiale. Quid du respect de la vie privée à l'épreuve de l'informatique ?

L'Internet est un monde virtuel dans lequel il n'y a pas d'atteinte et de violation de droits fondamentaux particuliers, notamment celui de la vie privée. Le bonheur est dans l'Internet. Il s'agit d'un monde comme un autre avec ses embûches ; on ne peut empêcher des personnes en embuscade qui utilisent les nouvelles technologies dans un cadre qui n'est pas adapté. Mais la vie privée est tout aussi bien défendue, sinon mieux, dans le monde virtuel que dans le monde réel.

Dans le monde virtuel, je peux restreindre mon compte et rester complètement anonyme très facilement. Témoin, la récente décision de la cour de Cassation qui place Facebook dans la sphère privée, dès lors que les propos sont diffusés au sein d'un groupe fermé auquel l'accès n'est possible que sur invitation de l'administrateur (Cass. civ. 10-4-2013, n° 01-19530). Or, aujourd'hui, il est possible de photographier un passant dans la rue et trouver son nom en déposant la photo sur le net et en lançant une recherche sur Google images.

Les nouveaux dangers proviennent de la coordination des potentialités du monde physique avec les potentialités du monde de l'Internet. Ce qui est effectivement dangereux, c'est la possibilité de croiser n'importe qui dans la rue, de le photographier, d'avoir son image et d'obtenir à son insu son nom, ses coordonnées ou toute autre information le concernant. La réunion des deux mondes fait naître une dangerosité qui n'est pas égale à l'addition des deux mondes. Il s'agit d'un danger « co-substantiel » supérieur à l'addition.

Face à la multiplication et à la diversité des traitements de données conjuguées à leur conservation illimitée sur le web, des réponses peuvent être apportées par l'instauration du droit à l'oubli numérique (ou au remords) (NDLR : en octobre 2010, la charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche a été signée. Cette charte – à laquelle a participé Me Bensoussan – a été initiée par la secrétaire d'Etat chargée de la prospective et du numérique. *Lire aussi http://www.alain-bensoussan.com/wp-content/uploads/262249.pdf*) ou le « Privacy by Design » (NDLR : les nouvelles formes de régulation comme le "Privacy by Design" permettront de régler ces questions ; c'est d'ores et déjà une tendance très marquée, principalement dans les groupes internationaux, et qui est amené à se développer de plus en plus chez les éditeurs de produit informatiques). Mais la véritable réponse serait d'élaborer une convention internationale consacrant trois droits qui pour moi sont fondamentaux :

- le droit à la dignité numérique ;
- le droit à la souveraineté ;
- et le droit à la propriété des données à caractère personnel par la personne concernée.

La réponse aux difficultés de couplage entre le monde réel et le monde virtuel, c'est l'émergence de nouveaux droits universels évoqués ci-dessus. Ces derniers devront être consacrés dans le monde entier pour pouvoir organiser une vie binaire et une vie physique en toute tranquillité. Cette voie est encore émergente aujourd'hui.

Les dispositifs de vidéoprotection se rapprochent des techniques d'enregistrements de données biométriques. Ils permettent, par exemple, d'analyser la démarche des passants ou d'identifier des comportements humains "anormaux" pour donner l'alerte. Pour devenir de plus en plus efficaces, devront-ils être nécessairement couplés à une base de données biométriques ?

La biométrie fait l'objet d'un encadrement où seule la biométrie de sécurité est privilégiée par rapport à la biométrie de confort (NDLR : au sens de la Cnil, la biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire "comportementales").

Le couplage des technologies d'analyse de comportement avec des technologies biométriques est la prochaine étape. Cela commence à se faire et il serait dommage de se priver de la reconnaissance faciale pour éviter un acte délinquant. Le problème est que les interconnexions entre bases de données devront être limitées à des actes importants pour ne pas violer l'intimité de la vie privée.

Aujourd'hui, par exemple, les interceptions de communications ne peuvent s'effectuer que dans l'intérêt de l'Etat et pour des infractions dont la sanction encourue est supérieure à deux ans de prison. De même, en matière de vidéoprotection, la conservation des images ne peut pas dépasser 1 mois, sauf procédure judiciaire en cours, la victime perd donc un élément d'identification extrêmement important. Les règles ont été posées pour trouver un équilibre entre vie privée et tranquillité. De la même manière, le couplage biométrie et détection des comportements anormaux en temps réel, s'il devait être mis en place, devrait s'accompagner d'un cadre juridique beaucoup plus contraignant que celui qui existe actuellement.