JTIT Internationale n° 2 – décembre 2012
Special international issue – December 2012
ALAIN BENSOUSSAN
Juristendances Informatique et Télécoms
Le réseau Lexing vous informe – The Lexing Network informs you

ACTUALITE DE LA PROTECTION DES DONNEES PERSONNELLES

LATEST DATA PROTECTION NEWS IN EACH COUNTRY

Une riche actualité

▪ L'actualité, en France, dans le domaine de la protection des données personnelles est très riche :

- l'augmentation considérable des contrôles de la CNIL,
- l'augmentation du nombre de Cil,
- la publication du bilan annuel de la CNIL,
- les recommandations de la CNIL sur le cloud computing,

sont autant d'actualités qui impactent l'activité des entreprises.

▪ Qu'en est-il dans les autres pays ? Les membres du réseau Lexing® vous en informent.

A highly-topical theme

▪ *Data privacy, in France, is an exciting sector with an action-packed agenda:*

- *the significant increase in the number of CNIL controls,*
- *the growing number of Data Protection Officers,*
- *the publication of the CNIL annual report,*
- *the CNIL recommendations about cloud computing*

are all events that deeply affect business world.

▪ *What about the other countries? The Lexing® network members inform you.*

A propos de Lexing®

Lexing® est le premier réseau international d'avocats technologues dédié au droit des technologies avancées.

Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

About Lexing®

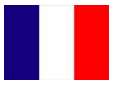
Lexing® is the first international network of lawyers dedicated to technology law.

Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

CHLOE TORRES

FRANCE

ALAIN BENSOUSSAN-AVOCATS



▪ De nombreuses entreprises françaises ont adopté une approche « Privacy by Design » **(1)** consistant 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.

▪ Le concept de « Privacy by Design » implique également le respect de ces valeurs tout au long du cycle de vie du produit ou service concerné.

Ce concept est une tendance très marquée, principalement dans les groupes internationaux, et est amené à se développer de plus en plus.

▪ La pratique du Privacy by Design constitue en effet, un nouvel outil de différenciation face à la concurrence et un gage supplémentaire de qualité et de confiance pour les clients.

▪ Cette tendance est appelée à se généraliser, dans la mesure où elle correspond à l'esprit du projet de règlement européen visant à réformer la directive n°95/46/CE relative à la protection des données à caractère personnel **(2)**. La Commission européenne prévoit ainsi de rendre obligatoire l'approche « protection des données personnelles dès la conception » et propose l'adoption du Privacy by Design pour tous les produits, services et systèmes exploitant ce type de données.

REFERENCES

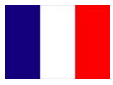
(1) Chloé Torrès, « Privacy by Design » Juristendances Informatique et Libertés, n°45 – Mai-Juin 2012 (page 1)

(2) Proposition de Règlement général sur la protection des données

Cf. également Blog tendances «Informatiques et libertés» de Chloé Torrès

FRANCE

ALAIN BENSOUSSAN-AVOCATS



▪ *A large number of French companies have adopted a "Privacy by Design" approach **(1)** meaning that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.*

▪ *Adopting a PbD approach is a very visible trend in international groups and such a trend is expected to grow by leaps and bounds.*

▪ *Privacy by Design can serve as a new tool to stand out from competitors and be a further mark of quality and trust for clients.*

▪ *It will become pervasive, to the extent that it is in line with the spirit of the draft EU General Data Protection Regulation that is expected to amend Data Protection Directive 95/46/EC **(2)**. The European Commission is indeed planning to make the Privacy by Design approach compulsory and proposes to adopt Privacy by Design for all products, services and systems involving personal data.*

REFERENCES

(1) Chloé Torrès, « Privacy by Design » Juristendances Informatique et Libertés, n°45 – Mai-Juin 2012 (page 1)

(2) Proposal for a General Data Protection Regulation

See also Data privacy blog of Chloé Torrès

ALLEMAGNE

BUSE HEBERER FROMM

REFERENCES

▪ En Allemagne, une récente décision de l'*Oberlandesgericht* **(1)** (cour d'appel régionale de Munich, juridiction placée directement sous la cour de cassation fédérale allemande) a semé la confusion et donné quelques sueurs froides aux entreprises spécialisées dans le secteur des newsletters électroniques.

▪ Aux termes de cet arrêt rendu fin septembre dernier, un courrier électronique envoyé dans le cadre d'une procédure de « double opt-in » (« opt-in confirmé », email demandant à l'utilisateur de confirmer son abonnement à une newsletter en cliquant sur un lien de confirmation) a été considéré comme une publicité non sollicitée, donc comme du spam, et dès lors comme devant être interdit.

▪ Dans l'hypothèse où cette décision viendrait à être généralisée, le secteur du e-marketing serait confronté à un problème épineux dans la mesure où la procédure de « double opt-in » est devenue la norme, jusque-là acceptée par les tribunaux, pour obtenir et prouver le consentement des utilisateurs à recevoir des messages publicitaires. Si une décision de la cour de cassation allemande serait la bienvenue pour rétablir la sécurité juridique quant aux meilleures pratiques acceptables en la matière, elle ne semble pourtant pas d'actualité à ce jour.

▪ Pour l'instant, la leçon à tirer de l'analyse des magistrats de Munich et posant (à leur yeux) problème dans l'espèce qu'il leur était déférée est la suivante : vous devez toujours être en mesure de prouver que vous avez obtenu le consentement de la personne à qui vous envoyez des messages publicitaires, c'est-à-dire qu'il faut conserver et documenter ce consentement et être capable de le produire à tout moment (ce qui ne semble pas avoir été le cas dans l'affaire concernée). Ainsi, les entreprises doivent veiller à se constituer des dossiers adéquats et à mettre en place un système pertinent d'archivage leur permettant de disposer non seulement de l'heure et de l'adresse IP liées à la prise d'abonnement à une newsletter, mais aussi de l'heure et l'adresse IP liées à la confirmation de l'abonnement, et du contenu de l'email de confirmation envoyé.

(1) Oberlandesgericht (OLG) Munich, 29.09.2012
(en allemand)

GERMANY

BUSE HEBERER FROMM

REFERENCES

▪ *In Germany, a recent decision by the Higher Regional Court of Munich **(1)** (being a rather important court directly below the German Federal Supreme Court) has led to some confusion and scare among businesses providing email-newsletters.*

▪ *The court decided in late September, that an initial email sent out in the course of a double opt-in (aka confirmed opt-in) procedure, i.e. the email asking the user to confirm his subscription of the newsletter by clicking the confirmation link, was to be regarded as unrequested advertising and therefore (impermissible) spam.*

▪ *If this was generally true, it would pose a real problem to all kinds of email marketing, because the double opt-in procedure has become the factual – and until now, accepted by the jurisdiction – standard for obtaining and demonstrating the users' consent with receiving advertising emails. To regain security as to what is the legally acceptable best practice in this regard, a decision by the German Federal Supreme Court will be necessary, but is not yet in sight.*

▪ *For the time being, it is advisable to orientate on what the Munich court has pointed out as being the central problem (in their eyes) with the confirmation email in the case they had to decide: It shall always be required to prove that you have the consent from the individual that you send advertising emails to, i.e. you must save and document such consent and be able to print it out at any time (which is what the defendant was not able to accomplish). That means, businesses have to make sure that they have an adequate documentation and archiving process in place, covering such information as the time and IP-address relating to the registration for the newsletter, the time and IP-address relating to the confirmation, and the content of the confirmation email sent out).*

(1) Oberlandesgericht (OLG) Munich, 29.09.2012
(in German)

BELGIQUE

PHILIPPE & PARTNERS

REFERENCES

▪ Par deux lois du 21 juin 2012 **(1)**, la Belgique a finalisé la transposition du troisième paquet télécom. Une des mesures importantes de cette nouvelle législation au regard de la vie privée est la modification apportée à l'article 129 de la loi du 13 juin 2005 relative aux communications électroniques, lequel vise les informations stockées dans les équipements terminaux d'un utilisateur final, soit ce qui est plus communément appelé les « cookies ».

▪ Alors que prévalait jusqu'alors un système d'opt-out – installation de cookies autorisée par défaut, à charge de l'utilisateur de s'y opposer – la modification législative a pour conséquence de conditionner l'installation d'un cookie à l'obtention, par le prestataire, du consentement préalable de l'utilisateur, soit un système d'opt-in. Aucun détail n'est donné dans la loi sur la façon dont le consentement doit être obtenu ou conservé. Or, l'on imagine assez peu qu'un pop-up apparaisse préalablement à la visite de chaque site web pour demander l'autorisation d'installer tel ou tel type de cookies.

▪ Il ressort toutefois de plusieurs déclarations concordantes d'autorités de protection de la vie privée ainsi que de la Commissaire Européenne Neelies Kroes **(2)**, qu'une distinction doit être opérée entre des « cookies » pratiques – comme ceux qui permettent de maintenir connecté l'utilisateur à un site web ou de retenir la langue dans laquelle il souhaite accéder au site – et les « cookies » invasifs qui traquent l'utilisateur dans ses pérégrinations sur la Toile à des fins publicitaires. La Commissaire européenne plaide donc pour l'implémentation dans les navigateurs d'un standard technique « DNT - Do Not Track » (laquelle option est maintenant disponible dans la plupart des navigateurs répandus) activé par l'utilisateur et qui permettrait aux opérateurs de site de savoir si oui ou non ils peuvent installer un « cookies » traqueur sur l'ordinateur de l'internaute.

▪ Si cette solution parait effectivement simple et pratique, il s'agit en fait d'un système d'opt-out qui n'est pas conforme au prescrit législatif belge. L'interrogation demeure quant à la manière d'appliquer ce texte. Nous attendons le ou les arrêtés d'exécution.

(1) Loi portant des dispositions diverses en matière de communications électroniques (10.07.2012)
et Loi modifiant la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges (10.07.2012)

(2) Neelies Kroes, Why we need a sound Do-Not–Track standard for privacy online (20.01.2012)

BELGIUM

PHILIPPE & PARTNERS

REFERENCES

▪ *By two laws of 21 June 2012* ***(1)****, Belgium has completed the transposition of the third telecom package. One of the important steps of this new legislation with regard to the privacy is the modification of Article 129 of the Law of 13 June 2005 on electronic communications, with respect to the information stored in the terminal equipment of a user, or what is more commonly known as "cookies"*

▪ *While prevailed a system of opt-out (by default authorization of the installation of cookies) the legislative modification has the effect to require the consent of the user prior to install any cookie. No details are given in the law on how consent must be obtained or stored. One cannot imagine a pop-up appears before visiting each website to request permission to install a particular type of cookies.*

▪ *However, it appears from statements of data protection authorities and from the EU Commissioner Neelies Kroes* ***(2)****, that a distinction must be made between "cookies" strictly necessary to the service the user has already asked for - like those that keep the user connected to a website or retain the language in which they wish to access the site - and "cookies" that track user in his wanderings on the Internet for advertising purposes. European Commissioner therefore calls for the implementation in browsers of a technical standard "DNT - Do Not Track" (which option is now available in most popular browsers) activated by the user and allowing website operators to know whether or not they can install a "cookie" on the user's computer.*

▪ *If this solution seems simple and effective, it is actually an opt-out system which is not in accordance with Belgian legislation. The issue is therefore not yet solved. We are waiting for the implementing decrees.*

(1) Loi portant des dispositions diverses en matière de communications électroniques (10.07.2012)
et Loi modifiant la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges (10.07.2012)

(2) Neelies Kroes, Why we need a sound Do-Not–Track standard for privacy online (20.01.2012)

CANADA

LANGLOIS, KRONSTRÖM, DESJARDINS

REFERENCES

▪ En janvier 2012, un tribunal canadien a reconnu pour la première fois l'existence d'un délit fondé sur « l'intrusion dans la vie privée » **(1)**. Selon la Cour d'appel de l'Ontario, l'intrusion dans la vie privée est caractérisée par des intrusions intentionnelles, non autorisées et significatives dans des affaires privées pour lesquelles une personne est raisonnablement en droit d'attendre une protection de sa vie privée, et lui causant détresse, humiliation ou angoisse. Bien que la portée de cet arrêt soit limitée à l'Ontario, il revêt une importance particulière pour les employeurs de l'ensemble du territoire canadien, dans la mesure où les autres tribunaux canadiens seront bien évidemment susceptibles d'être saisis de demandes similaires visant à obtenir la même solution.

▪ Dans une affaire pénale relative à l'exclusion d'éléments de preuves **(2)**, la Cour suprême du Canada a rendu un arrêt posant le principe selon lequel l'attente raisonnable d'une salarié en matière de respect de sa vie privée à l'égard des données à caractère personnel stockées sur son ordinateur professionnel devait être appréhendée au regard des faits particuliers de chaque espèce, indépendamment de l'existence d'une charte informatique et libertés au sein de l'entreprise. En l'espèce, la haute juridiction a estimé que la police avait violé les droits de l'accusé et que la saisie d'un ordinateur par les forces de police nécessitait la délivrance d'une ordonnance par le tribunal, et ce quand bien même l'employeur avait consenti à la saisie.

▪ Les entreprises canadiennes seront prochainement tenues de notifier les failles de sécurité (violations de données à caractère personnel), dès l'adoption par la Chambre des communes des amendements proposés à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), déposés en septembre 2011 (Projet de loi C-12) **(3)**.

▪ Sur le front législatif, l'actualité phare des prochains mois sera constituée par l'entrée en vigueur de la Loi Anti-spam **(4)** instaurant un régime de consentement express (opt-in) à l'égard des messages électroniques commerciaux non sollicités et un régime de consentement implicite (opt-out) à l'égard des cookies.

▪ Enfin, il convient de signaler la publication par le Commissariat à la protection de la vie privée du Canada d'une « Position de principe » **(5)** sur l'application de la LPRPDE à la collecte et à l'utilisation de données concernant les activités sur le Web des personnes à des fins de publicité comportementale en ligne. Dans ce document, il se prononce en faveur d'un régime de opt-out.

(1) Jones c/ Tsige, 08 01 2012 (2012 ONCA 32) (en anglais)

(2) R. c/ Cole, 19 10 2012 (2012 SCC 53) (en anglais)

(3) Projet de loi C-12 modifiant la Loi sur la protection des renseignements personnels et les documents électroniques

(4) Canada's Anti-Spam Act (CASL) (en anglais)

(5) Position de principe sur la publicité comportementale en ligne

CANADA

LANGLOIS, KRONSTRÖM, DESJARDINS

REFERENCES

▪ *In January 2012, a Canadian Court recognized a breach of privacy as a civil cause of action (tort) for the first time **(1)**. The intrusion upon seclusion tort recognized by the Ontario Court of appeal will require proof of intentional, unauthorized, and significant intrusions upon private matters regarding which an individual has a reasonable expectation of privacy in circumstances that lead to distress, humiliation or anguish. Although limited in its application to Ontario, the judgment bears importance for all Canadian employers, as Canadian Court are likely to be seized of cases seeking to obtain recognition of similar causes of action.*

▪ *In a criminal case pertaining to an exclusion of evidence application **(2)**, the Supreme Court found that the determination of whether an employee had a reasonable expectation of privacy with regard to the personal data stored on an employer's computer depended on the circumstances of a particular situation, despite the existence of a work place policy. In this instance the court found that the police had infringed the accused's rights and that the seizure of the computer by the police forces required the issuance of a court order regardless of the employers consent.*

▪ *Canadian organizations will soon be subject to an obligation to disclose data breaches, when the proposed amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA), introduced in the House of Commons in September 2011 (Bill C-12) **(3)** comes into force.*

▪ *On the legislative front the upcoming months should see the coming into force of the Anti spam Act **(4)** which sets forth an express opt-in regime with regards to unsolicited electronic commercial communication and an op-out framework pertaining to cookies.*

*Finally the Canadian privacy commissioner has published a Policy Position **(5)** on the Application of PIPEDA to the collection and use of data about an individual's Internet activities for the purposes of online behavioral advertising, calling for the possibility of opting-out of the practice before any data is collected.*

(1) Jones v. Tsige, 08 01 2012 (2012 ONCA 32)

(2) R. v. Cole, 19 10 2012 (2012 SCC 53)

(3) Bill C-12 to amend the Personal Information Protection and Electronic Documents Act

(4) Canada's Anti-Spam Act (CASL)

(5) Policy Position on Online Behavioral Advertising

ESPAGNE

ALLIANT ABOGADOS

REFERENCES

▪ En Espagne, l'année 2012 a été marquée par la modification de la loi sur la protection des données dans trois domaines en particulier :

1) Amendes. En 2011 il avait été procédé à la refonte du régime de sanction instauré par la loi sur la protection des données espagnole afin d'y inclure, notamment, un système d'avertissement en cas de violations mineures, destiné à se substituer aux sanctions économiques, particulièrement lourdes en Espagne (pour preuve, le montant total des amendes infligées en 2011 est de plus de 20.000.000€, soit le montant le plus élevé appliqué par une autorité de protection des données dans l'UE). Toutefois, l'autorité de protection des données espagnole (AEPD) n'a pas automatiquement recours à ce système et subordonne son bénéfice à une analyse au cas par cas. En effet, depuis mars 2011, date d'entrée en vigueur de ce système d'avertissement, et janvier 2012, l'AEPD ne l'a utilisé que dans 44% de ses résolutions constatant une infraction à la loi **(1)**. Une autre disposition importante concerne l'introduction du **principe de responsabilité** (« accountability ») permettant de réduire les sanctions en cas de violation de la loi sur les données personnelles. A cette fin, il appartient au responsable du traitement ou au sous-traitant de démontrer deux éléments : a) la mise en œuvre de procédures nécessaires pour la collecte et le traitement de données avant la survenance de la violation, et b) une violation dont la cause se trouve dans un fonctionnement anormal desdites procédures et non dans un défaut de diligence **(1)**.

2) Cookies. En mai 2012, l'Espagne s'est dotée d'une « Loi sur les cookies » **(2)** par l'adoption d'amendements à la loi sur la société de l'information et le commerce électronique (34/2002). Ce nouveau texte, très similaire au dispositif en place dans d'autres Etats membres, permet aux exploitants de sites Web d'utiliser des cookies à condition que les personnes aient donné leur consentement, après avoir reçu une information claire et complète sur l'utilisation et les finalités des cookies. Des exceptions ont été aménagées pour les cookies « techniques » et « nécessaires ». Un document d'orientaiton devrait être publié par l'AEPD afin de clarifier le champ d'application des nouvelles mesures (mentions, formulaires d'obtention du consentement, exemptions).

▪ **3) Cloud Computing**. L'AEPD a formulé des lignes directrices sur le Cloud Computing **(3)**, destinés particulièrement aux cabinets d'avocats, dans l'objectif de favoriser le respect de la loi lors du stockage de données personnelles dans le cadre de services « cloud ». L'AEPD adhère ainsi à l'approche du Groupe « Article 29 » **(4).**

(1) Rapport d'activités annuel 2011 de l'AEPD (en espagnol)

(2) Décret-loi royal 13/2012 du 30 mars 2012 (en espagnol)

(3) Lignes directrices de l'AEPD sur le Cloud Computing (en espagnol)

(4) Groupe de travail "article 29", Avis 05/2012 sur l'informatique en nuage (WP196) du 1er juillet 2012

SPAIN

ALLIANT ABOGADOS

REFERENCES

▪ *During 2012 Spanish Data Protection Law (SDPL) has experienced a remarkable evolution in three main areas:*

▪ ***1) Fines**. The sanction regime under SDPL was reviewed in 2011 to include, among other measures, a warning system for minor infringements as an alternative to economic sanctions, especially severe in Spain (i.e. total amount of fines imposed in 2011 was more than € 20.000.000, the highest compared to the rest of DPA in the EU). But the benefits of this system are not automatically granted by the SPDA, which will assess its application under a case-by-case approach. Since the warning system entered into force in March 2011 to January 2012, the SPDA has applied the warning system on 44% of the resolutions declaring an infraction of SDPL **(1)**. Another important provision is the one that incorporates the **accountability principle** as a criterion to reduce the sanctions for an infringement of the SDPL. The data controller or data processor must demonstrate two elements: a) that he applied adequate procedures when collecting and processing personal data before the infringement occurred, and b) that the infringement is due to an abnormal functioning of said procedures and not of his lack of diligence **(1)**.*

***2) Cookies**. In May 2012, Spain implemented the "Cookie Law" through amendments to its law on Information Society and Electronic Commerce (34/2002) **(2)**. This new provision is very similar to other EU countries and allows website operators to serve cookies provided individuals have given consent after having been given clear and comprehensive information about the use and purpose of cookies. Exemptions are also foreseen in case of "technical" and "necessary" cookies. It is expected the SDPA will issue Guidelines on Cookies to clarify the scope of this new provision (i.e. notices, forms of obtaining valid consent and exemptions.).*

▪ ***3) Cloud Computing**. The SDPA has issued Guidelines on Cloud Computing **(3)** in order to make it easier for data controllers (focusing on law firms) to comply with the SDPL when using cloud services to store personal data. The SDPA also fully supports the Opinion issued by Art. 29 Working Group on Cloud Computing **(4)**.*

(1) AEPD Annual Report Rapport (2011) (in Spanish)

(2) Royal decree-law 13/2012 of 30 March 2012 (in Spanish)

(3) AEPD Guidelines on Cloud Computing (in Spanish)

(4) Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing (WP196) of 1 July 2012

Affaire « Google 2 »

- Le 16 novembre 2012, à l'issue d'une brève audience, le tribunal fédéral du district nord de Californie a donné son feu vert à la transaction amiable proposée par Google et la Federal Trade Commission (« FTC ») dans l'affaire qui les opposait (affaire « Google 2 ») **(1)**, mettant ainsi fin aux allégations selon lesquelles Google avait fait de fausses déclarations aux utilisateurs du navigateur Safari concernant l'utilisation de cookies publicitaires de suivi et l'affichage de publicités ciblées, et ce en violation d'un accord conclu en octobre 2011 entre la FTC et Google. Aux termes de cette transaction, la firme de Mountain View devra s'acquitter d'une amende civile record d'un montant de 22,5 millions de dollars, soit l'amende la plus élevée jamais prononcée dans l'histoire de la FTC pour violation d'une décision administrative. Google s'est également engagée à désactiver l'ensemble des cookies de suivi qu'elle avait, en dépit de déclarations contraires, installés sur les ordinateurs des consommateurs, et à attester auprès de la FTC de son respect de cette mesure.
- **Spécificités**. Au contraire de plusieurs autres décisions, la décision rendue dans l'affaire Google 2 **(2)** ne s'articule pas uniquement autour de la violation de promesses faites. Sa spécificité est d'être également axée sur le non-respect, par Google, d'une transaction antérieurement conclue avec la FTC (octobre 2011) **(3)**. Par là même, cela témoigne des efforts continus entrepris par le régulateur américain du commerce dans le but de s'assurer que les entreprises respectent bien les engagements en matière de vie privée pris non seulement à l'égard des consommateurs mais également à l'égard de la FTC. En effet, lorsqu'une société contrôlée par la FTC s'engage à adopter certaines pratiques pendant une certaine durée, 20 ans en l'espèce, la FTC est en droit de s'assurer du bon respect de cet engagement.
- **Engagements en matière de vie privée**. Un aspect essentiel de l'affaire Google 2, tel qu'il ressort de la transaction et de la plainte associée **(4)**, réside dans le constat que des promesses en matière de vie privée peuvent être faites partout, et pas seulement dans une politique de vie privée en ligne. Elles peuvent se trouver, par exemple, dans des déclarations faites par la société dans les documents qu'elle dépose auprès d'organismes réglementaires, ou encore dans ses documents marketing ou promotionnels. A titre d'illustration, le premier volet de l'affaire, Google 1, concernait les promesses et déclarations faites par Google dans son dossier d'adhésion au Safe Harbor. L'affaire Google 2, quant à elle, a trait aux promesses et déclarations faites par Google dans son engagement de conformité au Code d'autorégulation du Network Advertising Initiative (NAI), une association regroupant différents prestataires de services de marketing en ligne.
- **Evolution de la doctrine de la FTC.** Google 2 est révélateur d'une évolution de la doctrine de la FTC en matière de vie privée. Au fur et à mesure de l'évolution de la notion de respect de la vie privée, la FTC a en effet affiné et élargi la nature de ses enquêtes. Dans les affaires précédentes dont elle a été saisie, l'attention de la FTC se cristallisait sur les violations des promesses contenues dans les politiques de vie privée mises en ligne par les entreprises. Puis, plus récemment, et notamment dans l'affaire Google 1 **(5)**, la FTC a élargi son champ d'action aux violations du Safe Harbor, c'est-à-dire l'ensemble de principes de protection des données personnelles négociés entre le Département américain du commerce et la Commission européenne. Désormais, avec Google 2, la FTC agrandi de nouveau ses compétences en y incluant la violation de déclarations faites dans le cadre du Code d'autorégulation du NAI. Cette tendance va probablement se confirmer, et les prochaines décisions de la FTC enrichiront certainement l'éventail du référentiel au regard duquel la FTC procède à ses contrôles.
- **Quel impact pour les entreprises ?** Les entreprises mettent souvent en avant leur adhésion à des groupements et des associations prônant le respect de la vie privée afin d'en faire la vitrine de leurs valeurs et engagements dans ce domaine. Cependant, celles-ci devraient prendre garde car les promesses données dans le cadre de ces organismes ne sont pas de simples déclarations marketing : le public les lit, tout comme la FTC et les autres régulateurs. Les programmes en matière de vie privée, tels que le Safe Harbor ou le Code NAI, ont leurs règles spécifiques. Si les engagements pris ne sont pas conformes aux mesures réellement appliquées, ce décalage pourrait exposer l'entreprise concernée à des plaintes pour pratiques déloyales et trompeuses, ou, comme dans le cas de Google, à des amendes substantielles pour absence de respect à une ordonnance par consentement renfermant des engagements sur les déclarations faites en matière de vie privée.

(1) Proposition de transaction entre la FTC et Google dans l'affaire Safari (« Google 2 »)
(en anglais)

(2) Ordonnance par consentement de l'affaire Google 2
(en anglais)

(3) Transaction entre la FTC et Google datée d'octobre 2011 (« Google 1")
(en anglais)

(4) Plainte (en anglais)

(5) Transaction dans l'affaire Google 1
(en anglais)

Google 2

▪ *On Nov. 16, 2012, after a brief hearing on the terms of the settlement, a federal court in the Northern District of California approved the FTC's proposed settlement with Google in the Safari matter (Google 2)* ***(1)****. The settlement resolves allegations that Google made misrepresentations to Safari users about the placement of advertising tracking cookies and serving of targeted advertisements in violation of the FTC's October 2011 Order against Google. Under the settlement, Google will pay a $22.5 million civil penalty, the largest in the FTC's history for violation of an administrative order. Google must also disable all tracking cookies that it had said it would not place on consumer's computers, and report to the FTC on how it has complied with this remediation requirement.*

▪ .***Google 2 Unique Aspects****. Unlike most consent orders published by the FTC, the Google 2 Consent Order* ***(2)*** *does not address primarily the actual violations privacy promises made. Rather, it addresses the fact that Google's activities allegedly violate a prior settlement with the FTC, dated October 2011 (Google 1)* ***(3)****. As such, beyond evidencing the FTC's ongoing efforts to ensure that companies live up to the privacy promises that they make to consumers, Google 2 clearly shows that the FTC takes seriously the commitments that it requires from companies that it has previously investigated. When an FTC consent decree requires a 20-year commitment to abide by certain practices, the FTC may, indeed, return and ensure that the obligations outlined on the consent decree are met.*

▪ ***Privacy Promises are made everywhere****. A significant aspect of the proposed Google 2 Consent Order and related Complaint* ***(4)****, is that privacy promises are made in numerous places beyond a company's online privacy statement. They are found, as well as, in other representations made by the company, such as through its regulatory filings, or in its marketing or promotional documents. In the Google 1 enforcement action* ***(5)****, the FTC looked at the promises and representations made in Google's Safe Harbor self-certification filings. In the Google 2 enforcement action, the FTC looked at the promises and representations made in Google's statements that it complied with the Self-Regulatory Code of Conduct of the Network Advertising Initiative (NAI).*

▪ ***Evolution of the FTC Common Law.*** *Google 2 shows a clear evolution of the FTC "Common Law" of Privacy. As the concept of privacy compliance evolves, the nature of the FTC's investigations becomes more refined and more expansive. In its prior cases, the FTC first focused on violations of companies' privacy promises made in their public Privacy Statements. Then, more recently, in several consent orders – including Google 1 - the FTC expanded the scope of its enforcement action to include violations of the Safe Harbor Principles outlined by the US Department of Commerce and the EU Commission. Now, with Google 2, the FTC expands again the scope of its enforcement actions to include potential violation of representations made of compliance with the NAI Self Regulatory Code of Conduct. This trend is likely to continue, and in future cases, we should expect to see an expansion of the FTC investigations into verifying compliance with statements made that a company follows other self-regulatory industry standards.*

▪ ***What consequences for Businesses.*** *Companies often use their membership in industry groups or privacy programs as a way to show their values, and to express their commitment to certain standards of practice. These promises are not just statements made for marketing purposes. The public reads them, and so do the FTC and other regulators. Privacy programs such as the Safe Harbor or the NAI Code have specific rules. If the disclosures and promises made are not consistent with the actual practices and procedures, such deficiency would expose the company to claims of unfair and deceptive practice; or in the case of Google, to substantial fines for failure to comply with an existing consent decree barring future misrepresentation.*

REFERENCES

(1) FTC's proposed settlement with Google in the Safari matter (Google 2)

(2) Google 2 Consent Order

(3) Settlement with the FTC, dated October 2011 (Google 1).

(4) Complaint

(5) Google 1 enforcement action

ITALIE

STUDIO LEGALE ZALLONE

REFERENCES

▪ La loi italienne sur la protection des données est en vigueur depuis bientôt quinze ans, quinze années au cours desquelles les entreprises ont su se montrer de plus en plus sensibles aux problématiques qui y sont potentiellement associées. Si aujourd'hui les entreprises n'hésitent plus à utiliser Internet à grand échelle afin de fidéliser davantage leur clientèle et accroître leur chiffre d'affaires, elles sont également plus attentives à l'image qu'elles renvoient au public en termes de protection des données, pleinement conscientes de l'impact positif qu'une démarche respectueuse de la vie privée peut avoir sur le marché et, à terme, sur la clientèle.

▪ Deux thèmes sont particulièrement d'actualité en Italie : l'exploitation des nouvelles technologies sur le lieu de travail et l'utilisation des réseaux sociaux.

▪ Correctement utilisés, les réseaux sociaux représentent une source formidable de données que les entreprises peuvent utilement exploiter pour prendre en compte les besoins du marché, comprendre les attentes des consommateurs et s'ouvrir des opportunités commerciales. Pour autant, l'utilisation des données issues des réseaux sociaux peut s'avérer être assez complexe et délicate, et des précautions particulières doivent être prises afin d'agir dans le respect de la loi.

▪ En Italie, il est possible de contrôler les activités des salariés sur leur lieu de travail afin de protéger l'entreprise en cas d'actes illégaux, mais uniquement dans le strict respect des limites posées par le droit du travail. En effet, si des contrôles peuvent être menés, l'employeur se doit de suivre une procédure claire et spécifique conformément à la loi, particulièrement restrictive en la matière. L'autorité italienne de protection des données, le Garante **(1)**, a adopté plusieurs décisions soulignant fermement la nécessité du strict respect de la loi s'agissant du contrôle des salariés. En mars 2007, le Garante a publié un document d'orientation **(2)**, par ailleurs controversé, traitant de l'utilisation d'internet et de la messagerie électronique sur le lieu de travail. Par la suite, le Garante a été saisi de plusieurs affaires et a notamment, par une décision n°1712856 datée du 24 février 2010 **(3)**, limité l'accès aux fichiers personnels d'un salarié soupçonné d'utiliser illégalement Internet sur son lieu de travail, tout en confirmant le droit de l'employeur de prononcer des sanctions à son encontre. La cybersurveillance des salariés est donc une tendance très marquée, amenée à se développer de plus en plus, compte tenu de l'utilisation exponentielle des nouvelles technologies dans le monde du travail.

(1) Autorité italienne de protection des données (Garante)

(2) Document d'orientation de l'autorité italienne de protection des données du 1er mars 2007 disponible
-en italien :
doc. web n. 1387522
-en anglais
doc. web n. 1408680

(3) Décision n°1712856 datée du 24 février 2010 (en italien)

ITALY

STUDIO LEGALE ZALLONE

REFERENCES

▪ *Data Protection Law has been in force in Italy for fifteen years now, and companies are now more and more aware of the potential issues related to it. In addition, companies are starting to leverage the use of the Internet to a significant extent, in order to foster customer fidelization and revenue growth. Companies that are privacy aware tend to pay more attention to their corporate image towards the public, knowing that this will positively reflect in their approach to the market and, ultimately, in better customer acceptance.*

▪ *The attention is now focusing also on two other areas: labor environment and use of social networks. Social networks, when used correctly, are an amazing source of data that companies can use to better address market needs, understand their customer base and open new business opportunities.*

▪ *The use of these data can be quite complex and tricky, and therefore the utmost attention is made to act in compliance with the law.*

*In Labor environment, the main attention is to the possibility to control illicit activities from the employees, within the strict boundaries marked by labor laws, which are quite restrictive in these filed. This does not mean controls cannot be implemented, but that there is a very clear and mandatory path to follow in order to protect the company's assets. In this area the Italian Authority (Garante) **(1)** has issued several decisions, all of them remarking and underlying the need to proper compliance with the law. In March 2007 the Garante has published a controversial document, Guidelines on the use of Internet and e-mail in employment context **(2)**. After that, several cases have been brought to the attention of the Garante: among others, the decision No. 1712856 **(3)** laid down on Feb. 24, 2010 while confirming the right of the employer to take disciplinary sanctions against an employee accused of illicit use of the Internet while at work, has also limited the access to the employees personal files. This trend of surveillance is bound to continue in the future, as new technologies are implemented in the every day's companies activities.*

(1) Italian data protection authority (Garante)

(2) Italian Authority Guidelines of March 1, 2007, available:
-in Italian:
doc. web n. 1387522
-in English:
doc. web n. 1408680

(3) Decision No. 1712856 dated 24 February 2010 (in Italian)

MEXIQUE

LANGLET, CARPIO Y ASOCIADOS

REFERENCES

▪ Au Mexique, la Loi fédérale sur la protection des données personnelles détenues par des particuliers ("LFPDPPP") **(1)** promulguée en 2010 est venue remplacer l'ancien système sous l'empire duquel les données personnelles étaient protégées par l'introduction d'action civile devant les tribunaux compétents.

Le Code civil fédéral (article 1910) et les Codes civils de chaque Etat fédéré renferment effectivement une disposition spécifique en matière de « dommage moral » suffisamment large pour couvrir la protection des données personnelles ainsi que le droit à l'autodétermination informationnelle. Le concept de dommage moral et ses règles d'indemnisation sont exposés dans l'article 1916 du Code civil fédéral. Dans ce cadre, et certains cas, un acte ou une omission peuvent être considérés comme une infraction pénale, sanctionnée au niveau fédéral ou local.

Le cadre juridique en matière de protection des données au Mexique comprend la LFPDPPP, son Règlement d'application (RLFPDPPP) **(2)** et les résolutions prises par l'autorité mexicaine de protection des données (Institut fédéral d'accès à l'information et à la protection des données, ou « IFAI ») **(3)**. Des sanctions civiles et pénales peuvent être infligées, en sus des sanctions administratives prévues par la LFPDPPP.

▪ La dernière actualité au Mexique dans le domaine informatique et libertés concerne la non-conformité d'une politique de confidentialité. Par une déclaration en date du 3 décembre 2012 **(4)**, l'IFAI a en effet mis en cause une des plus grandes chaînes de vente au détail de médicaments au Mexique, la société Pharma Plus, S.A. de C.V., exploitant la marque Farmacias San Pablo®. En résumé, Pharma Plus, S.A. de C.V. n'a pas respecté la loi sur la protection des données et les règlements y associés car a) sa politique de confidentialité ne précisait pas les informations concernant l'identité et l'adresse du responsable du traitement et b) la vente de médicaments psychotropes était subordonnée à l'ordonnance médicale contenant le nom et l'adresse du patient. Pharma Plus, S.A. de C.V. a ainsi écopé de deux amendes : i) une pour violation des dispositions de la LFPDPPP (notice et légalité), à hauteur de 115.000 dollars américains et ii) une autre pour défaut d'information sur l'identification du responsable du traitement dans la politique de confidentialité, à hauteur de 38.000 dollars américains.

(1) Loi fédérale sur la protection des données personnelles détenues par des particuliers (LFPDPPP) et
(2) son Règlement d'application (RLFPDPPP)
(en espagnol)

(3) Autorité de protection des données mexicaine (IFAI)

(4) Communication du 3 décembre 2012 sur Pharma Plus, S.A. de C.V. (Comunicado 166 - IFAI/166/12)

MEXICO

LANGLET, CARPIO Y ASOCIADOS

REFERENCES

▪ *Before the enactment of our Law on the Protection of Personal Data held by Private Parties ("Mexican Privacy Law or MPL") **(1)** in 2010, our legal system protected personal data by means of a civil action before the competent courts.*

The Federal Civil Code (article 1910) and the corresponding Civil Codes of each of the States of the country have a specific provision regarding "moral damage" which was comprehensive to protect personal data and the informational self-determination right in a primary stage. The Federal Civil Code elaborates and furthermore establishes in article 1916 the concept of moral damage and the rules for the determination of the indemnification. And in some case, the act or omission can be considered as a crime or felony, either in the State or in the Federal scope.

*The legal framework regarding the protection of personal data in Mexico includes the MPL, the Rules to the MPL **(2)** and the resolutions issued by the Federal Institute for Access to Public Information **(3)**. Civil and Criminal provisions may be used in addition to the Administrative provisions contained in the MPL.*

▪ *The latest case regarding the infringement of data protection rights in Mexico involves the company Pharma Plus, S.A. de C.V. which uses the brand Farmacias San Pablo® and is one of the largest drug retailing chains in Mexico. On December 3, 2012 the Federal Institute for Access to Public Information issued a Statement **(4)** which refers to the Pharma Plus, S.A. de C.V. case. In a nutshell, Pharma Plus, S.A. de C.V. did not comply with the MPL and its rules: a) because the Privacy Notice lacked the information regarding the identity and domicile of the Data Controller and b) because the sale of psychotropic drugs was conditioned to the medical prescription containing the name and address of the patient. As a consequence thereof, the Federal Institute for Access to Public Information issued a resolution imposing Pharma Plus, S.A. de C.V. two fines: i) for the infringement of the principles (notice and legality) in the MPL in the amount of $115,000.00 and ii) for the infringement of the Identity Element of the Privacy Notice in the amount of $38,000.00.*

(1) Law on the Protection of Personal Data held by Private Parties (LFPDPPP) and
(2) its Rules (RLFPDPPP)
(in Spanish)

(3) Mexican data protection authority (IFAI)

(4) Statement of 3 December 2012 on Pharma Plus, S.A. de C.V. (Comunicado 166 - IFAI/166/12)

TUNISIE

YOUNSI & YOUNSI INTERNATIONAL LAW FIRM

▪ En Tunisie la protection des données personnelles trouve son fondement dans l'article 9 de la Constitution, telle que modifiée en 2002 **(1)**. Deux ans après, la loi N°2004-63 du 27 Juillet 2004 relative à la protection des données à caractère personnel **(2)** fut promulguée pour garantir la protection des données personnelles et l'impératif de les traiter dans la transparence, la loyauté et le respect de la dignité humaine.

▪ Il faut souligner le rôle important joué par l'Instance Nationale de Protection des Données Personnelles (INPDCD) **(3)**, créée en vertu de cette même loi et organisée par deux décrets **(4)**, dans la mesure où elle assure la sécurisation des opérations de transfert de données et le respect de leur confidentialité en protégeant les droits des personnes concernées et en s'assurant de leur accord explicite. Toute opération de traitement des données personnelles est soumise à une déclaration préalable auprès de cette instance. Pour lui garantir l'efficacité et l'indépendance requises pour l'accomplissement de sa mission, la loi a doté cette instance d'une personnalité morale et de l'indépendance financière.

▪ Quatre ans plus tard, le décret-loi du 26 mai 2011 relatif à l'accès public aux documents administratifs **(5)** a été promulgué dans le but de mettre les nouvelles technologies de l'information et de la communication au service de la consécration des valeurs de démocratie et du rapprochement de l'information du citoyen qui constitue un partenaire essentiel dans le contrôle des performances de l'administration et l'amélioration de son rendement.

▪ L'INPDCD a organisé les 28 et 29 juin dernier, avec le concours de la Commission Européenne, une rencontre internationale axée sur « la loi relative à la protection des données personnelles en Tunisie et sur l'impératif de son amendement ». Cette rencontre s'inscrit dans le cadre de l'amendement de la loi organique n°2004-63, dès lors que la majorité des dispositions de cette loi ne sont pas conformes aux normes internationales. Elle a pour objectifs de permettre à l'INPDCD de s'acquitter convenablement de sa mission, tout en étant totalement indépendante du pouvoir exécutif, et de repérer les lacunes et les défaillances que recèle la loi organique actuelle.

▪ Le dispositif judiciaire tunisien en matière de données personnelles garantit la protection requise et encourage, de ce fait, l'investisseur étranger à s'installer et investir en Tunisie.

REFERENCES

(1) Article 9 de la Constitution (modifiée par la loi constitutionnelle n°2002-51 du 1er juin 2002)

(2) Loi organique n°2004 - 63 du 27 Juillet 2004 portant sur la protection des données à caractère personnel

(3) Instance Nationale de Protection des Données Personnelles

(4) Décrets N° 2007-3003 & Décret N° 2007-3004 en date du 27 novembre 2007 définissant la mission, les prérogatives de l'INPDCD et les conditions et procédures de déclaration préalable et de demande d'autorisation pour le traitement des données à caractère personnel

(5) Décret-loi N° 2011-41 du 26 mai 2011 relatif à l'accès public aux documents administratifs (open-data) modifié par le décret-loi n°54 du 11 juin 2011 (disponibles sur http://www.iort.gov.tn/)

TUNISIA

YOUNSI & YOUNSI INTERNATIONAL LAW FIRM

▪ *In Tunisia everyone has the right to the protection of personal data related to his privacy as one of the fundamental rights guaranteed by article 9 of the Constitution, such as amended in 2002* ***(1)****. Two years later, the law N°2004-63 of July 27, 2004, relating to the protection of personal data* ***(2)*** *was enacted to guarantee the protection of personal data and the necessity to process them in transparency, fairness and respect of human dignity.*

▪ *It is necessary to underline the important role played by the National Authority for Protection of Personal Data (*INPDCD) **(3)***, established by the same law and organized by two decrees* ***(4)****, as far as it assures the safety of operations of transfer of data and the respect for their confidentiality by protecting the rights of the data subjects and by making sure of their explicit agreement. Any personal processing of personal data is subject to a preliminary declaration with this authority. To guarantee the efficiency and independence required for the fulfillment of its mission, the law endowed this authority with a legal personality and a financial independence.*

▪ *Four years later, the decree-law of May 26, 2011, concerning public access to administrative documents* ***(5)*** *was enacted to use the new information and communication technologies in the service of consecrating the values of democracy and easing access to information for the citizen, who is a vital partner in the control of the performances and improvement of the efficiency of the government.*

▪ *The INPDCD organized on June 28 and 29 of this year, with the cooperation of the European Commission, an international meeting centered on* ***"****the law relating to the protection of personal data in Tunisia and on the requirement of amending it". This meeting is in line with the amendment of the organic law No. 2004-63, since the majority of the provisions of this law are not in accordance with international standards. It has for objectives to allow the INPDCD to properly carry out its mission, while being totally independent from the executive power and identify any gaps and failures in the current organic law.*

▪ *The Tunisian data protection legal arsenal guarantees the required protection and therefore encourages foreign investors to settle down and to invest in Tunisia.*

REFERENCES

(1) Article 9 of the Constitution (modified by the constitutional law n°2002-51 of June 1st, 2002)

(2) National Authority for the Protection of Personal Data

(3) Organic Act n°2004-63 of July 27th, 2004 on the protection of personal data. (English translation)

(4) *Decree N° 2007-3003 & Decree N° 2007-3004 of November 27, 2007 which determine the mission and privileges of the INPDCD and the conditions and procedures of preliminary declaration and authorization request for the personal data processing*

(5) *Decree-law N ° 2011-41 of May 26th, 2011 concerning the public access to the administrative documents (open-data) (in French) modified by Decree-law n°54 of June 11th, 2011 (available on http://www.iort.gov.tn/)*

PAYS / COUNTRY	CABINET/ FIRM	CONTACT	TELEPHONE	EMAIL
France *France*	Alain Bensoussan-Avocats	Alain Bensoussan	+33 1 41 33 35 35	paris@alain-bensoussan.com
Afrique du Sud *South Africa*	Michalsons Attorneys	Lance Michalson John Giles	+27 (0) 21 300 1070	lance@michalsons.co.za john@michalsons.co.za
Allemagne *Germany*	Buse Heberer Fromm	Bernd Reinmüller Tim Caesar	+ 49 69 971097100	reinmueller@buse.de caesar@buse.de
Angleterre *UK*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	dpreiskel@preiskel.com
Argentine *Argentina*	Estudio Millé	Antonio Millé Rosario Millé	+ 54 11 5297 7000	antonio@mille.com.ar rosario@mille.com.ar
Belgique *Belgium*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Canada *Canada*	Langlois Kronström Desjardins	Jean-François De Rico	+1 418 650 7923	jean-francois.derico@lk
Espagne *Spain*	Alliant Abogados	Marc Gallardo	+ 34093 265 58 42	marc.gallardo@alliantabogados.com
Etats-Unis *USA*	IT Law Group	Françoise Gilbert	+ 1 (650) 804 1235	fgilbert@itlawgroup.com
Israël *Israel*	Livnat, Mayer & Co.	Russel D.Mayer	+972 2 679 9533	mayer@lmf.co.il
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	r.zallone@studiozallone.it
Liban *Lebanon*	Kouatly & Associée	Rayan Kouatly	+ 961 175 17 77	info@kouatlylaw.com
Luxembourg *Luxembourg*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Maroc *Morocco*	Bassamat & associée	Bassamat Fassi-Fihri	+ 212 522 26 68 03	contact@cabinetbassamat.com
Mexique *Mexico*	Langlet, Carpio y Asociados, S.C.	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	eochoa@lclaw.com.mx
Norvège *Norway*	Føyen Advøkatfirma DA	Arve Føyen	+ 47 21 93 10 00	arve.foyen@foyen.no
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	sebastien.fanti@sebastienfanti.ch
Tunisie *Tunisia*	Younsi & Younsi International Law Firm	Yassine Younsi	+216 71 34 65 64	cabinetyounsi_younsi@yahoo.fr

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 29, rue du colonel Pierre Avia 75015 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-juristendance