The European Data Governance Forum – CNIL

European Data Governance Forum – CNIL

Le G29 et la CNIL organisaient le 8 décembre une conférence internationale qui se tenait à l'UNESCO. La conférence avait pour thème : Protection des données, innovation et surveillance : quel cadre éthique pour l'Europe ?

2015 est une année charnière pour la protection de la vie privée, avec l'adoption du règlement de l'Union Européenne sur la protection des données, la poursuite des négociations commerciales internationales et les décisions finales à prendre sur la gouvernance de l'internet. Cette période est cruciale pour l'Europe qui, dans le nouvel environnement numérique, doit promouvoir haut et fort les valeurs sociétales qui sont les siennes et définir des actions prioritaires pour le futur.
Une réponse d'ensemble à ces défis internationaux ne saurait être élaborée par des acteurs agissant en ordre dispersé. La complexité des problèmes posés demande une réflexion collective de la part de l'ensemble des parties prenantes.
La conférence du 8 décembre organisée par le G29 (groupe des autorités européennes de protection des données) et la CNIL était placée sous le patronage de l'UNESCO et de la Délégation permanente française auprès de l'UNESCO. Elle réunssait des représentants et experts d'horizons divers – institutions nationales, européennes et internationales, industrie, ONG et société civile – qui ont présenté leur point de vue sur les défis actuels de la surveillance numérique et sur la manière d'y répondre de manière adéquate dans une société démocratique.
La conférence s'est achevée par la présentation d'une Déclaration adoptée par le G29 qui était endossable par les parties prenantes qui le souhaitaient. Cette Déclaration soulignait la responsabilité collective de toutes les parties prenantes dans la définition et le respect d'un cadre éthique pour la collecte et l'utilisation de données personnelles dans l'économie numérique. Elle a défini les principes essentiels à inclure dans un tel cadre ainsi que les actions clés à entreprendre par toutes les parties prenantes, des secteurs public et privé, pour garantir le respect des règles.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.newspress.fr/Communique_FR_284395_1332.aspx

La protection des données personnelles, « atout pour la France », selon Manuel Valls

La protection des données personnelles, « atout pour la France », selon Manuel Valls

« Je mesure l'audace d'inviter un ancien ministre de l'intérieur parler de protection des données, cela peut paraître risqué » : surprise, c'est le premier ministre, Manuel Valls, qui a prononcé le discours d'ouverture de l'« European data governance forum », organisé lundi 8 décembre à Paris.

Cette journée de conférence au siège de l'Unesco a été mise en place par le G29, qui rassemble les autorités européennes de protection des données, afin de réfléchir à un « cadre éthique et juridique » sur la question des données personnelles.

Le chef du gouvernement a souligné à plusieurs reprises le rôle que doivent jouer, selon lui, les autorités européennes et les Etats : « Il serait erroné de penser que toute régulation tue l'innovation. La régulation, c'est le rôle des Etats. Les valeurs de la démocratie doivent peser sur le monde numérique, la loi doit s'y appliquer. »

Projet de loi sur le numérique

« En 2015 et 2016, la loi réaffirmera de manière solennelle le droit à la vie privée et à la protection des données personnelles, ainsi que le contrôle des actes des services de renseignement », a expliqué le premier ministre. Sans préciser si cette question sera abordée dans le cadre du projet de loi numérique, en 2015, ou s'il fera l'objet d'un texte distinct.

Manuel Valls et Mme Falque-Pierrotin, la présidente de la CNIL, ont également rappelé que 2015 serait l'année du règlement sur les données personnelles, adopté au printemps par le parlement européen et qui doit désormais faire l'objet d'un accord entre les Etats membres. Sur ce sujet, le premier ministre a souligné « le soutien de la France à la réflexion sur le règlement sur les données », tandis que Mme Falque-Pierrotin a estimé qu'il y avait « urgence à nous doter de cet instrument juridique unique pour toute l'Union ».

Sur la question très sensible de l'inclusion – ou non – de la lucrative question des données personnelles dans les négociations sur les traités de libre-échange actuellement en négociation notamment entre l'UE et les Etats-Unis, M. Valls s'est voulu rassurant : « La France veillera, dans les négociations sur les traités de libre-échange, à ce que le standard européen soit préservé. »

« DÉFICIT DE CONFIANCE »

Le gouvernement français en est convaincu, a martelé Manuel Valls : la protection des données est un atout économique. « L'Europe doit faire de la protection des données personnelles un argument d'attractivité et de compétitivité. L'utilisateur doit pouvoir faire ses choix sur ses propres données en toute connaissance. Cela a un potentiel économique énorme. »

Un avis partagé par Mme Falque-Pierrotin : « Il ne faut pas que le déficit de confiance se transforme en méfiance » générale au sein de l'écosystème numérique. « Le monde a changé. Certains voudraient faire croire que la vieille histoire de la protection des données est dépassée », a conclu Manuel Valls. « Chaque époque a son combat : le droit des femmes, l'abolition de la peine de mort… La France y a tenu sa place. C'est parce que la France est le pays des droits de l'homme qu'elle doit faire de la protection des données un grand combat pour les droits humains. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/pixels/article/2014/12/08/la-protection-des-donnees-personnelles-atout-pour-la-france-selon-manuel-valls_4536408_4408996.html par Martin Untersinger

Attention, la CNIL contrôle votre site Web sans vous en informer et rédige des PV

Attention, la CNIL contrôle votre site Web sans vous en informer et rédige des PV

La CNIL peut désormais contrôler des sites web hors la présence de l'organisation concernée. Le responsable du traitement n'est informé qu'après coup. En octobre dernier, la CNIL a publié le mode d'emploi pour ce nouveau type de contrôle. Analyse de Bénédicte Querenet-Hahn, associée, et Grit Karg, collaborateur au sein du cabinet d'avocats GGV.

La loi du 17 mars 2014 relative à la consommation, également appelée loi Hamon, a introduit à l'article 44 de la loi Informatique et Libertés un nouveau mode de contrôle. Elle prévoit que la CNIL procède à toute constatation utile, en dehors des contrôles sur place et sur convocation.

Les données imprudemment accessibles
La CNIL peut à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations.

La CNIL n'a pas besoin de se déplacer pour effectuer le contrôle, qui peut être effectué sans que l'organisme contrôlé en ait connaissance, à tout moment, et sans que le responsable des locaux puisse s'y opposer.

Procès verbal
Une fois un contrôle effectué, la CNIL rédigera un procès-verbal factuel décrivant la méthodologie appliquée et précisant l'environnement technique du contrôle ainsi que les éléments vérifiés. Ce procès-verbal sera ensuite adressé au responsable du traitement qui disposera alors d'un délai fixé par la CNIL afin de faire part de ses observations.
Un contrôle à distance peut être combiné avec tout autre moyen dont dispose la CNIL, telles que les auditions ou visites. En cas d'infraction à la réglementation constatée, un contrôle en ligne peut donner lieu à une mise en demeure ou, le cas échéant, à l'ouverture d'une procédure de sanction.

Finalités de la collecte de données
Les vérifications en ligne portent notamment sur la pertinence des données collectées au regard des finalités pour lesquelles elles sont collectées, les mentions obligatoires relatives à la collecte de données à caractère personnel, la sécurité des données collectées et traitées, le respect des formalités déclaratives auprès de la CNIL.

Selon la CNIL, un accent est également mis sur la vérification du respect des règles relatives aux « cookies » et à d'autres traceurs. La CNIL vérifiera le nombre et la nature des cookies déposés sur le poste informatique de l'internaute, les modalités d'information à destination du public en matière de cookies, la qualité et la pertinence de l'information et les modalités de recueil du consentement de l'internaute.

Répression des fraudes
Par ailleurs, la loi Hamon renforce la coopération de la CNIL avec les agents de la DGCCRF (la direction générale de la concurrence, de la consommation et de la répression des fraudes). Tout manquement constaté par l'autorité sera en effet transmis à la CNIL pour qu'elle puisse prendre les mesures nécessaires.

La communication systématique d'informations entre la CNIL et la DGCCRF a déjà été mise en place dans le domaine du e-commerce par la signature, le 6.1.2011, d'un protocole de coopération afin d'améliorer l'échange d'informations relatif à la protection des données personnelles.

Eviter tout risque de sanction
Au regard de ce renforcement des moyens de contrôles et de la volonté affichée de la CNIL de vérifier systématiquement les sites web, il appartient aux marchands s'assurer de la conformité de leurs sites avec la réglementation en vigueur, afin d'éviter tout risque de sanction.
Pour en savoir plus, nous vous recommandons notre article « Nouvelles exigences de la loi Hamon – Comment mettre à jour votre site e-commerce » : http://www.francoallemand.com/fileadmin/ahk_frankreich/Dokumente/recht/publications-droit/DF/4-2014-F-D-Nouvelles-exigences-de-la-loi-Hamon.pdf.

Contrôles dans l'entreprise
Pour rappel, selon l'article 44 de la loi Informatique et Libertés, les agents de la CNIL sont habilités à effectuer des contrôles au sein des entreprises. Ces contrôles sont en général réalisés suite à une plainte auprès de la CNIL et en présence d'une personne responsable des locaux, éventuellement assisté d'un conseil.
Le responsable des locaux doit par ailleurs être informé de son droit d'opposition à la visite. En cas d'exercice de ce droit, la visite ne peut avoir lieu qu'avec l'autorisation du juge des libertés et de la détention du TGI (Tribunal de Grande Instance) compétent. En cas d'urgence toutefois ou de risque de destruction de documents, la CNIL peut procéder à la visite, sur l'autorisation du juge, sans que l'entreprise ne puisse s'y opposer.
Lors de tels contrôles, la CNIL peut demander la communication de tous les documents nécessaires, en prendre copie, recueillir tout renseignement utile, et accéder aux programmes informatiques et aux données.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.larevuedudigital.com/2014/12/expert/attention-la-cnil-controle-votre-site-web-sans-vous-en-informer/

Droit à l’oubli : Où en sont les traitements des demandes à Google 6 mois plus tard…

Droit à l’oubli : Où en sont les traitements des demandes à Google 6 mois plus tard…

En juin, Google satisfaisait 57% des demandes de déréférencement (transmises par Reputation VIP). En octobre, c'est le non qui l'emporte désormais largement dans 71% des cas, ce en moyenne 26 jours après la demande.

Cela fait désormais plusieurs mois que Google a mis en ligne son formulaire permettant à un internaute européen de demander l'application de l'arrêt de la CUJE relatif au droit au déréférencement.
Spécialiste de l'e-réputation, la société Reputation VIP, au travers de Forget.me, joue ainsi le rôle d'intermédiaire entre ses clients et Google, le premier moteur de recherche en Europe et donc le plus concerné par ces requêtes.
De quoi ainsi établir des statistiques, différentes cependant de celles publiées officiellement par Google – Forget.me représente environ 5% des demandes Google selon l'éditeur. De ces données, il ressort que le moteur a manifestement industrialisé le processus de traitement des requêtes.

Plus rapide, mais plus de non au terme du traitement
La durée de traitement des demandes s'est nettement accélérée au cours des six mois écoulés. En juin, Google mettait en moyenne 56 jours pour traiter une demande de déréférencement d'URLs. En octobre selon Reputation VIP, la durée moyenne est de 26 jours.

Un autre paramètre a très significativement évolué : la nature des réponses de Google. Le rapport entre Oui et Non s'est même clairement inversé. En juin, Google apportait une réponse positive dans 57% des cas. La proportion de Oui a reculé de manière quasi continue pour tomber à 29% en octobre.
En clair sept demandes de déréférencement sur dix adressées à Google (dont 54% portent sur des atteintes à la vie privée) aboutissent à un refus de la part du moteur – qui n'est pas tenu de justifier sa décision.

Dans leur guide d'application du droit au déréférencement, les autorités de protection ont cependant demandé aux services concernés de publier « la liste des critères qu'ils utilisent », mais aussi les « statistiques détaillées sur leurs décisions. »
Par ailleurs, en cas de refus du moteur, les internautes disposent toujours de recours et peuvent notamment déposer plainte, en France, auprès de la CNIL. En fin de semaine dernière, l'autorité de protection faisait état de 110 plaintes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/droit-a-l-oubli-google-dit-de-plus-en-plus-souvent-non-39810627.htm

Sites e-commerce: Le contrôle commence

	Sites e-commerce: Le contrôle commence

Seulement 22% des sites web affichent une mention relative à la protection des données personnelles conforme aux exigences de la loi.

Le gendarme de l'e-commerce a commencé ses opérations de contrôle. La Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), la CNIL au Maroc, a passé sous la loupe plusieurs catégories de sites web.

Des sites d'annonces, voyage et hôtellerie, cabinets de recrutement et emploi, vente en ligne, deals, marketing, organismes publics, organismes de prévoyance sociale, jusqu'aux concessionnaires de services publics, en passant par l'immobilier, les banques et les sociétés de financement, les assurances, le transport et logistique, la santé, les télécoms et même la location de voitures. Cette opération de contrôle a montré que seulement 22% des sites web au Maroc affichent une mention relative à la protection des données personnelles conforme aux exigences de la loi. «La mention est présente, mais incomplète dans 28% des cas», a indiqué la CNDP qui a mené cette première campagne de contrôle, précisant que 50% des sites contrôlés n'affichent pas de mention relative à la protection des données à caractère personnel.
Les résultats du contrôle, publiés en septembre dernier, démontrent que «très peu de sites web au Maroc, à peine 1%, se soucient de recueillir le consentement des internautes à collecter et traiter leurs données personnelles. Dans 80% des cas, le site web n'évoque nulle part la demande de consentement, et dans 19% des cas, la présence de la demande est aléatoire, puisqu'elle ne figure pas sur la totalité des formulaires de collecte des données», selon la CNDP.
L'opération de contrôle de la CNDP montre que l'obligation d'informer les personnes concernées au moment de la collecte de leurs données personnelles dans les termes prévus par la loi est très rarement respectée avec 1%.
Une lettre, accompagnée de la fiche de synthèse et du document, a été adressée aux responsables de traitement, afin de les inviter à procéder à la mise en conformité de leur site web, selon la CNDP. Et à l'expiration du délai fixé par la Commission, les sites web seront à nouveau contrôlés afin de permettre à la CNDP de prendre les mesures légales qui s'imposent. Il s'agit notamment de la relance du responsable du traitement, la mise en demeure et, en l'absence d'une réponse positive, l'ouverture d'une procédure disciplinaire qui pourrait déboucher sur un avertissement, un avertissement public, un blâme, ou même le transfert du dossier à la justice.
Créée par la loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, la CNDP est chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'Homme. Cette loi a pour objectif de doter l'arsenal juridique marocain d'un instrument juridique de protection des particuliers contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée, et d'harmoniser le système national de protection des données personnelles à celles de ses partenaires, tel que défini par les instances européennes.
Pour mieux protéger les internautes, la loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel a prévu des sanctions. Ainsi, et sans préjudice de la responsabilité civile des personnes ayant subi des dommages du fait de l'infraction, est puni d'une amende de 10.000 à 100.000 dirhams quiconque aura mis en œuvre un fichier de données à caractère personnel sans la déclaration ou l'autorisation exigée ou aura continué son activité de traitement de données à caractère personnel malgré le retrait du récépissé de la déclaration ou de l'autorisation.

Aussi, est puni d'une amende de 20.000 à 200.000 dirhams par infraction, tout responsable de traitement de données à caractère personnel refusant les droits d'accès, de rectification ou d'opposition. La loi n° 09-08 a également prévu une peine d'emprisonnement de trois mois à un an et d'une amende de 20.000 à 200.000 dirhams ou de l'une de ces deux peines seulement, quiconque effectue un transfert de données à caractère personnel vers un Etat étranger.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.aujourdhui.ma/geeks/nouvelles-technologies/sites-e-commerce-le-controle-commence-114695#.VHxhLNKG8t4
Par Atika Haimoud

Droit à l’oubli : les 13 critères dégagés par la CNIL

Droit à l’oubli : les 13 critères dégagés par la CNIL

Soucieuse de ne pas laisser Google et ses concurrents fixer eux-mêmes leurs propres conditions d'application du droit à l'oubli, la CNIL a publié une liste de 13 critères à prendre en compte dans la décision de donner ou non satisfaction à une demande de déréférencement.

Le 13 mai 2014, la Cour de Justice de l'Union Européenne (CJUE) a rendu son déjà célèbre arrêt Google Spain qui oblige Google à donner satisfaction aux internautes qui demandent la censure de résultats qui les concernent, consacrant ainsi l'existence d'un « droit à l'oubli » sur Internet. Toutefois la CJUE avait aussitôt nuancé cette obligation en prévenant Google qu'il fallait étudier les demandes au cas par cas, pour refuser les requêtes d'un individu lorsqu'il « il existe des raisons particulières, telles que le rôle joué par cette personne dans la vie publique, justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations ».

La CJUE demandait que l'appréciation soit réalisée par Google lui-même, au regard de « la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à recevoir cette information ». La cour confiait ainsi à une entreprise privée le soin d'interpréter et appliquer le droit, à la place d'un juge dont c'est le métier et la fonction.
Or en signant cet arrêt inattendu qui contredisait l'avis de son avocat général, la cour de Luxembourg a fait naître un conflit inédit d'influence entre le secteur privé et des autorités publiques. D'un côté, Google a sauté sur l'occasion pour prendre un bout de souveraineté aux Etats et affirmer sa capacité autonome à déterminer ses propres critères jurisprudentiels, en mettant sur pieds un comité consultatif privé. De l'autre côté, les CNIL européennes qui se croyaient investies du pouvoir de faire respecter le droit à l'oubli avaient immédiatement annoncé leur intention de fixer elles-mêmes des critères, qu'elles appliqueraient en dernier recours si un internaute se plaint de ne pas avoir eu satisfaction. Elles ont ainsi boudé les réunions publiques de Google, n'acceptant pas d'être doublées.

C'est donc dans cet esprit que le G29, qui réunit la CNIL et tous ses homologues européens, a publié ce jeudi une première liste de critères généraux à prendre en compte dans l'acceptation ou le refus d'une demande de droit à l'oubli. Le document (.pdf) détaille chacun des critères à l'aune de l'arrêt de la CJUE. Les voici résumés (nos commentaires en italique) :

1. **Les résultats de recherche sont-ils relatifs à une personne physique ? Le résultat apparaît-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ?**
Seules les recherches du nom ou du pseudonyme d'un particulier entrent dans le champ de l'arrêt Google Spain.
2. **S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?**
Outre la détermination de ce qu'est un « rôle dans la vie publique », La CNIL ajoute un critère supplémentaire qui est de distinguer selon que l'information elle-même est une information pertinente au regard de cette vie publique, ou s'il s'agit d'une information d'ordre purement privé.
3. **Le plaignant est-il mineur ?**
Par principe si la réponse est oui le droit à l'oubli doit être respecté, au nom de 'l'intérêt supérieur de l'enfant » consacré par la Charte des droits fondamentaux de l'Union européenne.
4. **Les données sont-elles exactes ?**
En cas d'inexactitude, le droit à l'oubli joue le rôle d'un droit brutal de rectification. C'est toutefois à l'internaute d'apporter la preuve de l'inexactitude.
5. **Les données sont-elles pertinentes et/ou excessives ?**
Plusieurs sous critères sont ici ajoutés :

– Les données sont-elles relatives à la vie professionnelle du plaignant ?
une réponse positive joue en défaveur du droit à l'oubli, qui doit être utilisé pour la protection de la vie privée)
– L'information est-elle potentiellement constitutive de diffamation, d'injure, de calomnie ou d'infractions similaires à l'encontre du plaignant ?
la réponse positive doit reposer en priorité sur une décision judiciaire qualifiant les accusations, mais un critère de « contenu excessif » peut aussi s'appliquer par la CNIL
– L'information reflète-t-elle une opinion personnelle ou s'agit-il d'un fait vérifié ?
La CNIL vise ici le déréférencement de « campagnes de dénigrement » qui pourrait être accordé, ce qui semble flirter très dangereusement avec la ligne rouge de la censure pure et simple d'une opposition politique.
6. **L'information est-elle sensible au sens de l'article 8 de la Directive 95/46/CE ?**
Le fait que la page web dont la censure est demandée contient des informations sur l'origine raciale, la religion, les opinions politiques, l'orientation sexuelle, etc., doit jouer en faveur du droit à l'oubli.
7. **L'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ?**
La CNIL est ici favorable à ce qu'une information devenue obsolète puisse être supprimée, y compris (c'est un cas explicité) s'il s'agit par exemple d'une condamnation en première instance annulée en appel.
8. **Le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ?**
Il s'agit d'un critère de proportionnalité. La CNIL est par exemple favorable au déréférencement de pages qui relateraient une « infraction mineure » et qui posent problème pour la recherche d'un emploi, ou celui de photos intimes.
9. **Les informations issues du moteur de recherche créent-elles un risque pour le plaignant ?**
Sont visées ici les informations telles que des coordonnées bancaires, n° de passeport, adresse personnelle, etc., qui pourraient être utilisées par des tiers à mauvais escient.
10. **Dans quel contexte l'information a-t-elle été publiée ?**
A nouveau plusieurs sous-critères :
– Le contenu a-t-il volontairement été rendu public par le plaignant ?
Contrairement à ce que l'on pourrait croire, la CNIL estime que la réponse positive joue en faveur du droit à l'oubli, car il faut respecter le fait que la personne ne souhaite plus voir référencé un contenu qu'elle avait mis en ligne. Mais l'on doute que la réponse négative puisse jouer en sa défaveur. Dès lors, est-ce vraiment un critère ?
– Le contenu devait-il être public ? Le plaignant pouvait-il raisonnablement savoir que le contenu serait rendu public ?
La mise en ligne à l'insu de la personne joue en faveur du déréférencement (ce qui rejoint notre point précédent)
11. **Le contenu a-t-il été rendu public à des fins journalistiques ?**
La CNIL refuse d'en faire véritablement un critère. Tout en reconnaissant qu'il faut « prendre en considération » le caractère journalistique de l'information dont la censure est demandée, la CNIL minimise au maximum sa portée par rapport aux autres critères.
12. **La publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ?**
Si oui, le droit à l'oubli sera en principe refusé, sauf si d'autres critères priment (tels que le préjudice subi)
13. **L'information est-elle relative à une infraction pénale ?**
Si la condamnation a été effacée par l'amnistie prévue par la loi, le droit doit être systématiquement accordé. Sinon, c'est la gravité et la date de l'infraction qui entrent en considération.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.numerama.com/magazine/31424-droit-a-l-oubli-les-13-criteres-degages-par-la-cnil.html
par Guillaume Champeau

Registre National du Commerce et des Sociétés gratuitement ouvert et partagé : ce que le projet de loi a visiblement

négligé

Registre National du Commerce et des Sociétés gratuitement ouvert et partagé : ce que le projet de loi a visiblement négligé

Le projet de loi du gouvernement: « pour la croissance et l'activité » ambitionne, et c'est louable, de renouer avec la croissance de moderniser l'économie en simplifiant les règles qui, aujourd'hui, constituent un frein à la création et à l'innovation.

Pour ce faire le gouvernement fait l'exercice d'une attaque en règle des professions réglementées, qualifiées de tous les maux de la terre et qui méritent toutes la guillotine législative propre à les assainir!
Les greffiers des Tribunaux de Commerce, qualifiés notamment de rentiers ne sont pas épargnés!
L'une des propositions pour atteindre les objectifs envisagés s'inscrit dans la vague, très trendy, de l'open data. Dans cet esprit le gouvernement envisage de permettre l'ouverture et le partage gratuit des données du Registre National du Commerce et des Sociétés.
Pour les non initiés il est bon de rappeler le rôle de ce Registre tenu par l'Institut National de la Propriété Intellectuelle.

L'INPI est en charge de la centralisation au niveau national, sous forme de documents originaux, des informations et actes provenant des Registres du Commerce et des Sociétés (RCS) tenus localement par chacun des greffes de Tribunaux de commerce et des greffes des Tribunaux civils à compétence commerciale. L'ensemble de ces informations et actes forme le Registre National du Commerce et des Sociétés (RNCS).

A l'origine, un des objectifs de cette mission de centralisation par l'INPI du RNCS était la sécurisation de l'information légale sur les entreprises. La centralisation d'un second original de chaque acte et pièce déposés dans les différents RCS permettait de parer au risque de déperdition physique de cette information en cas par exemple d'incendie entraînant la destruction des archives papier d'un greffe.

14 millions d'euros versés à l'INPI
A l'heure de la dématérialisation et de la tenue électronique des registres légaux, la nécessité de cette sécurisation physique s'est significativement estompée. Aujourd'hui le rôle de l'INPI dans la tenue du RNCS se résume à archiver l'ensemble des actes et pièces transmis et à distribuer, de manière payante, 2 licences de données (IMR et bilans) pour les sociétés de renseignements commerciaux, ces licences étant constituées par le GIE Infogreffe pour le compte de l'INPI…

Pour être complet sur le sujet il convient de rappeler que les entreprises acquittent à chaque formalité une taxe de 5.90€ reversée à l'INPI par les greffiers. En 2013 le montant collecté s'est élevé à 14 M€ d'euros. Pour faire quoi? On peut encore s'interroger… Dans la mesure où la base de données de l'INPI et les licences ne sont autres que celles fournies par le GIE Infogreffe.

Il est important, alors que le texte du projet de loi est dans les mains de juristes éminents au Conseil d'Etat, de faire un peu de droit. Alors tentons d'expliquer, sans passion ni dogme, les difficultés auxquelles se heurtent le texte actuel.

La volonté de vouloir mettre en données ouvertes les données des entreprises afin de faciliter leur réutilisation dans le but de favoriser le développement économique ne ressort pas du simple postulat. Si aucun pays européen ne l'a encore mis en œuvre c'est que à cette liberté s'oppose des règles de droit dont l'essentiel ont pour but de protéger les individus.

Les données personnelles des dirigeants sont protégées
Ainsi le sujet de la propriété des données personnelles issues du RCS et du RNCS est le premier écueil qui doit être analysé pour déterminer les conditions de distribution de ces données.
L'article 2 de la loi informatique et libertés et la directive 95/46/CE définissent les données personnelles comme les données permettant d'identifier ou de rendre identifiable une personne physique. Cette définition concerne l'intégralité des informations des dirigeants des sociétés immatriculées au Registre du Commerce et des Sociétés. La nationalité, la date et lieu de naissance et bien sûr les noms, prénoms et adresses sont mentionnés.

La généralisation des transactions sur les données personnelles dont la collecte est la contre partie obligée de l'accès à un très grand nombre de services a répandu cette croyance infondée.

Ces données personnelles ne sont pas susceptibles d'appropriation, ce principe a été rappelé par le Conseil d'Etat dans son rapport: le numérique et les droits fondamentaux: « 50 propositions du Conseil d'Etat pour mettre le numérique au service des droits individuels et de l'intérêt général « .

Dans ce rapport le Conseil d'Etat promeut un droit à: « l'autodétermination informationnelle » décrit comme un « objectif » qui donne sens à tous les droits préexistants.

Les données personnelles peuvent être cédées après accord explicite
Mais le projet de loi gouvernemental soulève un autre problème de légalité. L'article 6 de la directive 95/46/CE dispose que « de telles informations ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ».
Or, les données personnelles des personnes physiques n'ont été collectées que pour une seule raison: celle de figurer au RCS et au RNCS et pour les seules finalités induites par ces mêmes registres. Ces données n'ont jamais été collectées pour qu'elles puissent ultérieurement figurer dans « une licence ouverte » à tous sur internet notamment pour être « googliser ». Les commerçants de base de données, les opérateurs de ces nouveaux marchés ne peuvent pas en principe réutiliser ces données personnelles.
L'article 7 de la Directive 95/46/CE dispose que « Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement ».

Le même principe est posé par l'article 7 de la loi dite Informatique et Libertés.
Si le RCS et le RNCS sont légalement « dispensés » du recueil de ce consentement, il n'en va nullement de même si les données sont ensuite sorties du RCS ou du RNCS pour être communiquées au public en vue de leur réutilisation.

Les données doivent être rendues anonymes
L'article 13 de la loi n°78-753 du 17 juillet 1978 dite CADA dispose que « Les informations publiques comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet ».
La CNIL exige également, au visa de la loi Informatique et Libertés, une anonymisation des données à caractère personnel figurant dans les documents administratifs.
En clair, chaque dirigeant, administrateur de société, chaque commerçant délivre son identité, son adresse et son âge. Ce sont autant de données personnelles. Si comme le prévoit le projet de loi gouvernemental, ces données devaient être exploitées à des fins commerciales, ce ne serait possible qu'avec l'accord de l'intéressé.
Gageons que le Conseil d'Etat relèvera ces obstacles qui, a priori, ont échappé au rédacteur du projet de loi et démontrent la non conformité des licences, aujourd'hui payantes, délivrées par l'INPi aux réutilisateurs professionnels.

Et la propriété intellectuelle des fichiers?
Tout comme il pourra constater qu'il n'est pas juridiquement possible de demander aux greffiers et à leur GIE Infogreffe d'abandonner leur droit de propriété intellectuelle issu de leur qualité de producteur de bases de données (Directive 96/9/CE du 11 mars 1996 – Article L 341-1 du Code de la propriété intellectuelle – Article L 112-3 du Code de la propriété intellectuelle).
En clair, selon la loi, seuls les Greffiers sont en droit d'autoriser une extraction de leurs bases de données et une diffusion de leurs données. Le projet de loi, en ce qu'il ne recueille pas l'accord des Greffiers sur la réutilisation de leurs droits, constituerait une spoliation.
Au plan du droit, une telle situation de fait exige un dispositif indemnitaire. Or, la loi impose une protection des producteurs de bases de données pendant 15 ans à compter du dernier investissement. Ce point n'a pas échappé au Rapporteur, Richard Ferrand, qui l'a clairement évoqué dans son rapport sur le projet de loi. Enfin il serait cocasse de voir l'Etat contraint, par les règles de droit, de payer une indemnité pour assurer une diffusion gratuite des données du RNCS!

L'ensemble des obstacles relevés démontre, à l'évidence, que le projet ne peut être maintenu en l'état.
La raison voudrait qu'une solution viable pour tous soit envisagée. C'est pourquoi nous proposons de diffuser en licence ouverte les données par exemple sur le site d'ETALAB. Ce choix d'un projet phare du gouvernement éviterait le doublon que représente la solution INPI. Qui de mieux placé que les greffiers dont la mission est de recevoir, contrôler, saisir et valider les informations, actes et documents déposés par les entreprises lors de l'accomplissement de leurs formalités légales pour en assurer une diffusion en données ouvertes respectueuses du droit.
Nous y sommes prêts.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.huffingtonpost.fr/bernard-bailet/ouverture-et-partage-gratuit-des-donnees-du-registre-national-du-commerce-et-des-societes-ce-que-le-projet-de-loi-a-visiblement-neglige_b_6232202.html?utm_hp_ref=france
par Bernard Bailet Président du G.I.E. Infogreffe

Les CNIL européennes veulent

imposer leur droit à l’oubli au monde entier

Les CNIL européennes veulent imposer leur droit à l’oubli au monde entier

Les établissements européens de protection des données personnelles ont publié un ensemble de règles encadrant le droit à l’oubli. Ils réclament notamment l’extension de la mesure à la version américaine de Google.

L’Europe milite pour un droit à l’oubli sans frontières. Le G29, le groupe européen des autorités de protection des données personnelles, a adopté mecredi un ensemble de recommandations pour encadrer cette mesure. Parmi leurs griefs, les CNIL européennes réclament l’extension du droit à l’oubli à tous les noms de domaine des moteurs de recherche, y compris en .com. Le premier site visé est Google, qui représente près de 90% du marché de la recherche en Europe.

135.000 demandes en quatre mois

Le droit à l’oubli est apparu en Europe en mai, à la suite d’une décision de la Cour de justice européenne. Cette dernière avait alors estimé que les moteurs de recherche, dont Google, étaient responsables du traitement des données à caractère personnel. En conséquence, les citoyens européens peuvent désormais obtenir, sous certaines conditions, le déréférencement de pages Internet qui contiennent des informations «inappropriées, hors de propos ou qui n’apparaissent plus pertinentes.»
Même si tous les moteurs de recherche en Europe sont touchés par la mesure, Google est le premier concerné. En quatre mois, le groupe américain a reçu plus de 135.000 demandes de droit à l’oubli, via un formulaire mis en ligne pour l’occasion. En cas de refus de la part de Google, les internautes peuvent s’adresser à leur CNIL nationale, qui pourra juger leur cas grâce aux critères adoptés mercredi. «Il s’agit d’avoir une mise en oeuvre harmonisée et une interprétation commune de l’arrêt de la Cour», explique Gwendal Le Grand, directeur des technologies et de l’innovation à la CNIL.

Pour le G29, Google n’en fait pas assez

Les règles proposées par le G29 risquent de relancer un débat que Google tente vainement d’apaiser. Actuellement, lorsqu’un internaute obtient le déréférencement d’un contenu en ligne portant sur sa vie privée, il est retiré des résultats de recherche de la version du moteur de son pays d’origine. Une protection jusqu’alors jugée adéquate par Google, qui géolocalise l’adresse IP de ses utilisateurs. Les internautes français sont par exemple automatiquement redirigés vers les résultats de Google.fr, même s’ils tapent Google.com sur leur barre de navigation. Il est tout de même possible d’accéder au résultats de recherche de Google.com, en cliquant sur un bouton prévu à cet effet sur l’écran d’accueil, ou en remplaçant simplement le «.fr» par «.com» dans la barre de navigation. Google est donc sommé d’étendre le droit à l’oubli «sur tous les noms de domaine en .com».

Les CNIL européennes ne sont pas tendres avec le groupe américain et considèrent qu’il n’en fait pas assez pour assurer le respect du droit des citoyens. «La loi européenne ne doit pas être contournée», prévient le groupe. «Les actions de Google sont sujettes aux décisions des autorités de protection des données personnelles et des juges», ajoute Gwendal Le Grand. Si Google n’adapte pas ses pratiques, les CNIL seront désormais en droit de lui réclamer le respect de ses nouvelles règles.
Contacté par le Figaro, Google a indiqué qu’il analyserait «attentivement» ces recommandations dès leur publication officielle.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lefigaro.fr/secteur/high-tech/2014/11/27/01007-20141127ARTFIG00320-les-cnil-europeennes-veulent-imposer-leur-droit-a-l-oubli-au-monde-entier.php#xtor=AL-201
Par Lucie Ronfaut

Utilisation abusive de la

messagerie électronique : licenciement sans cause réelle et sérieuse en l’absence de déclaration préalable à la CNIL

	Utilisation abusive de la messagerie électronique : licenciement sans cause réelle et sérieuse en l’absence de déclaration préalable à la CNIL

Poursuivant sa construction jurisprudentielle extrêmement protectrice des droits personnels du salarié, la Cour de Cassation a rendu un nouvel Arrêt le 8 octobre 2014 (Cass. Soc 8 oct 2014 n° 13-14991) encadrant strictement le contrôle par l'employeur, de l'activité des salariés au travail.

En l'espèce, une salariée avait envoyé et reçu un peu plus de 1 200 mails personnels via sa messagerie professionnelle sur une période de deux mois.
L'employeur avait licenciée ladite salariée pour faute, au motif d'une utilisation excessive de sa messagerie professionnelle à des fins personnelles .

La jurisprudence bien établie de la Chambre Sociale de la Cour de Cassation considérait déjà qu'à défaut de déclaration à la CNIL d'un traitement automatisé d'information nominative en place dans l'entreprise, le licenciement fondé sur un tel grief est sans cause réelle et sérieuse.
Tel est le cas notamment du licenciement d'un salarié qui refuse d'utiliser le système de badge ou de pointeuse à l' entrée et sortie de l'entreprise: faute de déclaration préalable à la CNIL du système mis en place dans l'entreprise, l'employeur ne peut valablement sanctionner le salarié sur ce motif (Cass. Soc 6 avr. 2014 n° 01-45227)

Dans la présente espèce, l'employeur avait précisément réalisé cette déclaration à la CNIL.
Il avait toutefois déclaré le système de surveillance de la messagerie, non pas dès sa mise en service mais près de deux mois et demi après .
Or, ce dispositif avait servi, dès son installation, à mettre en lumière l'utilisation excessive par la salariée concernée de sa messagerie professionnelle à des fins professionnelles.
La Cour de Cassation a trouvé, dans cette espèce, l'occasion de durcir encore davantage sa jurisprudence en invalidant le licenciement de la salariée fondé sur une utilisation abusive de la messagerie électronique durant les deux mois ayant précédé la déclaration du dispositif de surveillance à la CNIL.
La Cour considérant que le système de surveillance étant antérieur à la déclaration à la CNIL, le moyen de preuve de l'employeur quant à la matérialité du motif de licenciement était donc illicite.

La Cour de Cassation indiquant précisément que :
« Constitue un moyen de preuve illicite les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL ».

Cet arrêt ne fait qu'ajouter à l'arsenal existant de protection des droits des salariés dans l'entreprise à commencer par l'art L1222-4 du Code du travail qui dispose qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance ou encore le fondamental art L1121-1 du Code du travail.

La Cour de Cassation s'estimant garante, en droit du travail, de la protection des droits fondamentaux des salariés poursuit sa jurisprudence protectrice des droits individuels du salarié qui ne s'arrêtent pas une fois la porte de l'entreprise franchie.
Par Me Sandrine PARIS-FEY
Avocat au Barreau de NANTES
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.juritravail.com/Actualite/motifs-personnels-de-licenciement/Id/172011

La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés…

La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés…

La firme à la pomme a été épinglée plusieurs fois par la Commission pour sa pratique abusive des caméras de surveillance, même dans les espaces de repos des salariés.

Il fut un temps où Apple dénonçait à grands coups de publicités la surveillance généralisée d'une société, comme dans 1984. La firme à la pomme semble aujourd'hui avoir zappé ces beaux principes…

La Cnil annonce en effet avoir mis en demeure Apple Retail France pour sa pratique abusive des caméras de surveillance dans ses boutiques et pour le manque d'information des salariés. Les caméras « ne sont pas orientées uniquement vers les zones sensibles (apporte d'accès ou coffre-fort) mais filment de manière directe et constante les postes de travail » mais aussi la salle de repos d'une des boutiques.

Cette surveillance, « est disproportionnée au regard de la finalité de prévention des atteintes aux personnes et aux biens. Si la surveillance de zones sensibles est justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut intervenir que dans des circonstances exceptionnelle », assène la Commission.

Surveillance disproportionnée

Ce n'est en fait pas la première fois que la firme est épinglée par la Commission informatique et Libertés. En décembre 2013, elle faisait déjà l'objet d'une mise en demeure portant sur le dispositif de vidéosurveillance des salariés installé au sein de l'Apple Store d'Opéra à Paris. « Il était notamment demandé à la société de réorienter certaines caméras qui filmaient en permanence des salariés et de leur délivrer une information complète », explique la Cnil.

En février 2014, la société a justifié s'être mise en conformité avec ses obligations pour le magasin, entraînant la clôture de la mise en demeure. Mais des contrôles menés en mai et juin derniers dans d'autres magasins français du géant « ont révélé que la société n'avait pas adopté des mesures de conformité similaires à l'ensemble de ses magasins. L'information des salariés sur le dispositif demeurait lacunaire et certaines caméras continuaient à filmer des salariés à leur poste de travail sans justification particulière ».

« La persistance de ces manquements » a conduit la Commission à mettre à nouveau en demeure la société « de modifier l'intégralité des dispositifs de vidéosurveillance de ses 16 magasins sur le territoire national ».

« Aucune suite ne sera donnée à cette procédure si Apple France se conforme à la loi dans le délai de deux mois qui lui est imparti », ajoute la Cnil. Dans le cas contraire, la firme pourrait écoper de sanctions financières.

Voila de quoi tendre encore un peu plus les relations entre Apple et ses salariés français. En 2012 déjà, ces derniers s'étaient mis en grève. En cause, des revendications sur les salaires et les conditions de travail. Les syndicats négociaient avec la direction la mise en place de différents dispositifs, dont l'attribution de tickets restaurant et d'un 13e mois. Les salariés ont finalement obtenu une concession : des tickets restaurant d'un montant de 8,50 euros…

Par Olivier Chicheportiche

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://www.zdnet.fr/actualites/la-cnil-met-en-demeure-apple-france-accuse-de-surveiller-en-permanence-ses-salaries-39808739.htm