Compte-rendu : « Midis du GFII »
Déjeuner-débat du 22 mai 2012
Isabelle Falque-Pierrotin, présidente de la CNIL
Diffusion restreinte

1. Evolution des rôles et missions de la CNIL

Elargissement du périmètre des missions
La CNIL est une institution composée de plus de 170 personnes : non seulement des juristes, mais aussi de plus en plus des techniciens capables de réaliser des audits de sécurité et de répondre aux demandes toujours plus complexes des industriels comme des clients. Le périmètre des missions de la CNIL s'est considérablement élargi ces dernières années, en réponse au développement des technologies et des usages. L'autorité est désormais compétente pour traiter les dossiers liés à la vidéo protection, à la création de labels, aux failles de sécurité… La CNIL est insérée dans un réseau international et européen. Les sujets traités sont de plus en plus internationaux et la CNIL a acquis l'expérience et la légitimité pour traiter avec les grands acteurs de l'internet et se faire entendre à un niveau international.

Le passage au « Big Data » modifie la problématique des données personnelles
La question de la protection des données personnelles a connu un changement de nature depuis 6 ans. Le développement de l'économie numérique et la dématérialisation lient, dans un continuum, univers physique et virtuel. Smart grid, ville intelligente, services mobiles : toutes ces innovations reposent sur le traitement de données personnelles. Celles-ci sont le véritable « carburant » de l'économie numérique, au cœur de ce nouvel écosystème. Avec l'accélération des process et la diminution du coût des outils, le volume de données disponibles sur les réseaux double tous les 18 mois. Les données ne sont plus une valeur rare, mais produites et échangées en quantité exponentielle, en permanence et par tous : les entreprises, les pouvoirs publics, et les citoyens. Le foisonnement de ces données a des conséquences importantes pour les industriels et les instances de régulation.

Les données personnelles : une priorité stratégique
Pour les industriels, la CNIL a longtemps été considérée comme un « mal nécessaire », éloigné des réalités de la sphère marchande. Mais les données personnelles doivent désormais être considérées comme une priorité stratégique. En effet, la manière dont les données personnelles sont traitées par les entreprises peut être un facteur de différenciation concurrentiel. L'acceptabilité sociale des services et technologies de demain sera liée à leur caractère non-intrusif pour les citoyens. L'innovation dépend donc de la capacité des industriels à fournir des garanties aux consommateurs. De même, la protection des données des salariés peut être utilisée comme un levier pour la confiance et la cohésion interne aux entreprises.

La CNIL évolue vers une instance d'aide au pilotage de la conformité
Pour le régulateur, l'univers est différent de celui qui existait lors de la création de la CNIL. Il s'agissait à l'époque de grands fichiers publics dont l'utilisation devait être encadrée. Le rôle de la CNIL était d'abord un rôle de vérification des obligations déclaratives liées aux traitements, associé à un pouvoir de sanction. Aujourd'hui, la CNIL doit sortir de son rôle de seule « gardienne du temple et des grands principes » et ajuster ses méthodes pour privilégier la prévention et le conseil, sans renoncer à exercer son pouvoir de sanction qui doit rester une arme de dissuasion.
En effet, face à la complexité de l'univers des données, l'approche répressive ne suffit plus. Il faut remonter en amont dans la chaîne d'utilisation des données afin de mieux comprendre les besoins et fournir aux industriels

des clés opérationnelles déclinées par secteur d'activité. Pour la CNIL, le passage d'une pédagogie des risques à une pédagogie des solutions est un changement considérable de culture. Cette nouvelle priorité a un impact très fort sur les moyens et le fonctionnement de l'institution. Par exemple, le rôle des CIL (Correspondants Informatiques et Libertés) doit évoluer de simple référent à celui de « Compliance Officer » : personne chargée d'accompagner son organisation dans la mise en place d'une gouvernance des données personnelles conforme à la loi Informatique et Libertés.

2. La Révision de la directive 1995 (axe de travail n°1)

Inquiétudes sur la gouvernance voulue par la Commission Européenne

La directive 1995/46/CE, qui fixe le cadre légal en matière de protection des données à caractère personnel, est aujourd'hui obsolète. Dans le cadre de la révision de cette directive, la Commission européenne a publié un projet de règlement européen le 25 janvier dernier[1]. Le nouveau texte devrait être adopté avant 2014. Il convient d'observer une grande vigilance car ce texte encadrera la protection des données personnelles pour les prochaines années. On constate un changement de paradigme en termes de régulation : on passe d'un principe de régulation a priori à un principe de régulation a posteriori assorti d'une responsabilisation croissante des responsables de traitement.

Si la CNIL reconnait des avancées substantielles pour les droits des citoyens et un allègement des formalités pour les entreprises dans le projet de la Commission Européenne, elle reste néanmoins inquiète sur le mode de gouvernance que cette dernière souhaite mettre en place. La gouvernance est pour le moment trop centralisée. La CNIL estime que dans le texte actuel, la Commission dispose d'un pouvoir normatif trop important. Une partie des prérogatives de la Commission devraient plutôt être transférées au G29 (groupe des 27 CNIL européennes) ou aux autorités locales (la CNIL et ses homologues). Par ailleurs, dans le cas où une société dispose d'un établissement principal en Europe, c'est l'autorité de l'établissement principal qui gèrera la question des données personnelles de manière centralisée. Dans ces conditions, on peut craindre que la protection de la vie privée s'éloigne du citoyen[2]. Son autorité locale n'étant plus, dans bien des cas, compétente. La CNIL souhaite un dispositif plus souple, moins bureaucratique, pour garder la diversité des situations et des spécificités nationales. Il faut un marché unifié des données personnelles mais pas à n'importe quel prix.

Les pistes envisagées

Les pistes actuellement envisagées par la Commission européenne prévoient :

- d'alléger le système des formalités préalables pour les entreprises
- de renforcer les pouvoirs de sanction des autorités nationales
- de responsabiliser et accompagner les acteurs dans leur démarche de conformité (« accountability ») :
  - Evolution du rôle du CIL vers celui de « Compliance Officer» : celui qui diffuse les méthodes, les outils et les bonnes pratiques en matière de gestion des données personnelles dans l'organisme.
- de reconnaître de nouveaux droits pour les citoyens (portabilité et droit à l'oubli).

Enjeux : préserver l'avantage concurrentiel de l'UE

La CNIL se soucie de l'ingénierie du dispositif mis en place par la Commission : quel sera le rôle du G29 ? Des autorités nationales ? Quelle place pour la collaboration entre les autorités ? Il ne s'agit pas pour la CNIL de défendre son pré-carré mais d'anticiper les disfonctionnements et d'alerter les acteurs.

[1] http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_fr.pdf
[2] http://www.cnil.fr/la-cnil/actualite/article/article/projet-de-reglement-europeen-la-defense-de-la-vie-privee-seloigne-du- citoyen-1/

L'enjeu est important : un dispositif inadapté risquerait de faire perdre à l'UE l'avantage concurrentiel qu'elle a acquis dans le domaine du traitement des données personnelles. A l'international, l'UE reste perçue comme un territoire offrant un haut niveau de protection pour les données. Mais les autres « puissances » se mettent en ordre de bataille et scrutent le modèle que l'UE va développer pour les années à venir. Ainsi, les Etats-Unis commencent à réguler (initiatives « Safe Harbor » et « decrees» signés avec Google et Facebook). La FTC (Federal Trade Commission) est désormais très vigilante par rapport aux grands acteurs de l'internet. De même, l'Asie a construit à marche forcée un environnement juridique favorable aux transferts internationaux de données personnelles au sein de l'APEC (marché commun asiatique).
La CNIL, de par son expérience, doit être moteur au niveau européen et rassembler l'ensemble des acteurs autour d'une proposition cohérente et prospective. Il faut renforcer les principes fédérateurs communs ainsi que la coopération et le dialogue entre les autorités.

3. Accompagner l'innovation (axe de travail n°2)

Cloud computing : une nécessaire clarification du cadre juridique

Le Cloud représente une extraordinaire opportunité pour les clients et les développeurs de solutions. Cependant, le recours par les entreprises à ces services pose des questions nouvelles en termes juridiques et de gestion des risques. Afin de préciser le cadre applicable, la CNIL a lancé une consultation publique auprès des acteurs du Cloud, et a publié en juin des recommandations pratiques et des clauses contractuelles types à destination des entreprises qui recourent aux solutions de Cloud.[3]

Big data : prévenir les menaces (mining, informatique prédictive, reconnaissance faciale, …)

Pour ces nouveaux services, la question est de savoir comment trouver l'équilibre entre protection, accompagnement de l'innovation et réalisme ? Les algorithmes existent depuis longtemps. Ce qui change aujourd'hui, c'est la puissance de calcul, la baisse des coûts d'accès et la montée en force des offres de solutions analytiques permettant de dégager des connaissances inédites à partir de très gros volumes de données. Des données non personnelles peuvent, après croisements et interprétation, permettre au responsable de traitement d'identifier une personne physique et présenter de facto un caractère personnel.
Le projet Watson d'IBM[4], qui permet d'établir des corrélations par intuition et par expérience, est un bon exemple des progrès du « data mining ». La fouille de données, croisée aux technologies de géolocalisation, permet de dégager de nouvelles informations sur les personnes et d'anticiper les comportements sur la foi d'analyses prédictives. Or, cette démultiplication des possibilités de profilage soulève d'importantes questions éthiques. On peut également citer le développement d'outils d'analyse de flux de voitures connectés aux dispositifs de vidéosurveillance à Singapour : la prédiction permet de prodiguer des conseils aux conducteurs en temps réel avec une réelle granularité du profilage dans le service rendu. On trouve aussi le projet « e-boarders » (« frontières intelligentes ») au Royaume Uni où, à partir du croisement de données diverses collectées sur le passager (où le billet a été acheté ? comment ? par qui ? quels bagages ? quelle provenance ? quel poids ?), est attribué un « profil de dangerosité » aux individus. Ceux qui reçoivent un profil de dangerosité supérieur font l'objet d'un contrôle accru à la frontière. Dans un autre registre, le réseau social Facebook a récemment racheté la start-up Face.com, spécialisée dans la reconnaissance faciale[5]. Facebook est déjà propriétaire d'Instagram et il existe de nombreuses applications permettant la publication et le partage

[3] http://www.cnil.fr/la-cnil/expertise/actualite-expertise/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/
[4] http://www-03.ibm.com/innovation/us/watson/index.html

d'images via Facebook (PhotoFinder et PhotoTagger). Le croisement de ces données peut aboutir à un profilage commercial et une reconnaissance systématique des utilisateurs à leur insu.

Transparence et éducation numérique

Concernant les données personnelles, les personnes doivent pouvoir faire leurs choix en toute connaissance de cause. La législation doit forcer les acteurs à aller vers plus de transparence et à simplifier leurs messages. Les utilisateurs ignorent le plus souvent la manière dont leurs traces numériques sont utilisées, parce que les conditions générales d'utilisation des web services ne sont pas suffisamment explicites ou trop nombreuses.
Il faut repenser les principes de la citoyenneté à l'aune de la nouvelle réalité numérique. L'éducation au numérique doit être une priorité nationale, par exemple dans les cours d'éducation civique. Ce message n'est pas encore suffisamment pris en compte par les pouvoirs publics[6].

4. Création de labels (axe de travail n°3)

La loi "informatique et libertés" permet à la CNIL depuis 2004 de délivrer des labels "à des produits ou des procédures". Cette compétence est seulement effective depuis 18 mois, depuis la modification du règlement intérieur. Il s'agit d'un nouveau métier pour la CNIL qui la rapproche d'une activité de régulation économique. Il faut être vigilant pour ne pas fausser la concurrence. A la demande d'organisations professionnelles et d'institutions, la CNIL a créé en 2011 deux référentiels : un pour des procédures d'audit "Informatique et libertés", et un pour des formations "Informatique et libertés". C'est sur la base de ces deux référentiels que les labels sont délivrés. Le label CNIL permet aux entreprises de se distinguer par la qualité de leur service. Pour les utilisateurs, c'est un indicateur de confiance dans les produits ou procédures labellisés leur permettant aisément d'identifier et privilégier ceux qui garantissent un haut niveau de protection de leurs données personnelles. Pour la CNIL, c'est un moyen d'encourager les organismes à adopter des pratiques respectueuses de la protection des données à caractère personnel et de garantir une meilleure application de la Loi (5 labels ont été délivrés en juin 2012).

5. Questions / Discussions avec la salle

Quid des « données rendues publiques » pour l'intelligence économique ?

La Cour de cassation a rendu un avis sur les données « rendues publiques » : si une donnée est rendue publique par un individu de son propre chef, cette donnée peut être réutilisée à d'autres fins. Il convient donc de lister ce que sont les données « rendues publiques » : un mur Facebook est considéré par exemple comme un espace public. La CNIL a conscience que ces données sont la matière première des acteurs de l'Intelligence Economique. Des paramétrages fins doivent être trouvés pour garantir le respect des droits des citoyens et les intérêts des acteurs économiques.

Quid du rapprochement des fichiers STIC et JUDEX ?

A l'origine les fichiers STIC[7] et JUDEX[8] sont deux bases distinctes et séparées. Cependant, un article de la Loi d'Orientation et de Programmation pour la Sécurité Intérieure (LOPPSI) établit le principe de fusion des deux

[5] Information depuis confirmée : http://www.pcworld.fr/2012/06/19/business/facebook-rachete-face-com-specialiste-reconnaissance-faciale/529065/

[6] Depuis le déjeuner-débat, la **CNIL** souhaite inscrire dans la constitution le droit à la protection des données personnelles : http://www.cnil.fr/la-cnil/actualite/article/article/les-perspectives-pour-2012-2013-la-regulation-des-donnees-personnelles-au-service-dune-verita/ (10/07/12)

répertoires pour la constitution d'un super-fichier mutualisé (anciennement dénommé « ARIANE », puis TPJ (Traitement de Procédures Judicaires) puis TAJ (Traitement des Antécédents Judicaires). La CNIL s'était auto-saisie sur le TPJ en février 2011[9]. En effet, le ficher STIC présente un problème récurrent de manque de fiabilité des informations (victimes enregistrées comme auteurs d'infractions, etc.) avec des conséquences qui peuvent être dramatiques pour les personnes concernées (non-éligibilité à certaines fonctions, concours, etc.). On évalue à 1,3 million le nombre d'emplois concernés pas les procédures d'enquêtes administratives

Le Conseil Constitutionnel et le législateur ont entendu les réserves de la CNIL : le nouveau fichier TAJ (Traitement des Antécédents Judicaires), mis en œuvre par décret du 4 mai 2012[10], sera automatiquement alimenté par les décisions des juridictions via le traitement CASSIOPPEE, ce qui fournira aux citoyens des garanties sur la qualité des données. Néanmoins, la CNIL demeure inquiète sur certains points, notamment la mise à jour des fichiers STIC et JUDEX avant leur versement dans TAJ et les possibilités nouvelles offertes par TAJ aux autorités en termes de rapprochement de données et d'identification de personnes (fonctionnalités de reconnaissance faciale et d'analyse biométrique à partir des photographies des visages des personnes)[11]. L'encadrement des fichiers régaliens restent un axe de travail historique de la CNIL qui doit poursuivre la réflexion sur ces sujets.

Quel avenir pour la CNIL ?

A priori, on se dirige vers un renforcement du rôle et des pouvoirs de la CNIL. Le nouveau gouvernement est attendu en soutien sur les négociations avec la Commission européenne. Les moyens mis à disposition de la CNIL devraient également être réévalués, proportionnellement à l'élargissement du périmètre de ses missions (notification des violations de données à caractère personnel, contrôle de la vidéoprotection).

On observe une croissance des plaintes de 20 % par an. La pression de la société civile sur ces questions augmente de façon continue depuis la création de la CNIL Le gouvernement devra prévoir les budgets nécessaires. Pour autant, la réponse ne passe pas uniquement par l'augmentation des moyens budgétaires. Il faut ajuster les modalités d'intervention, multiplier les relais avec les entreprises et les acteurs publics, en travaillant en réseau.

Quelles sont les différences culturelles et les possibles convergences entre les CNIL européennes ?

Il y a des différences culturelles. D'abord, on constate que la logique économique prédomine dans les pays anglo-saxons, là où les pays de culture latine sont historiquement plus soucieux de la protection de la vie privée. La situation est plus contrastée dans les pays de l'Est. Ensuite, on observe des clivages dans la perception de ce qui relève d'un « donnée personnelle » ou pas, et sur les outils et démarches à mettre en place pour les protéger. Cependant, il y a une prise de conscience générale de la nécessité d'apporter une réponse commune : il faut légiférer et agir ensemble si l'on veut être crédible. Dès lors, la CNIL souhaite se rapprocher de ses homologues et favoriser une logique de coopération. Cependant, le cas de Google Street View a été très symbolique à cet égard. Les freins culturels en Europe sont nombreux. La diversité et les spécificités nationales doivent être prises en compte pour que le débat avance, ce que ne permet pas, en l'état, le dispositif de la Commission.

---

[7] ***« Système de Traitement des Infractions Constatées » :*** fichier informatisé du ministère de l'Intérieur regroupant les informations concernant les auteurs d'infractions interpellés par les services de la police nationale.

[8] *«Système Judiciaire de Documentation et d'Exploitation » :* équivalent de la Gendarmerie Nationale.

[9] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025804888&dateTexte=&categorieLien=id

[10] http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000025803463&dateTexte=&oldAction=rechJO&categorieLien=id

[11] http://www.cnil.fr/es/dossiers/police-justice/actualites/article/taj-traitement-dantecedents-judiciaires/