Conférence de presse
16 avril 2015

Présentation du 35ème rapport d'activité 2014

Contact presse : 01 53 73 22 13

#DirectCNIL

Sommaire

Chiffres clés de l'année 2014

Les particuliers et la CNIL

Plus de 11 000 demandes individuelles adressées à la CNIL

- 5 825 plaintes
  - Dont 39% concernent l'e-reputation.
- 5246 demandes de droit d'accès indirect (fichiers de police, de gendarmerie, de renseignement, FICOBA, etc.)
  - **+ 22 % par rapport à 2013**.

L'action de contrôle et de sanction

- 421 contrôles (dont 88 contrôles vidéoprotection et 58 contrôles en ligne)
- 62 mises en demeure
- 18 sanctions

Dont :

- 7 avertissements
- 8 sanctions financières
- 3 relaxes

L'encadrement et la mise en conformité des acteurs

- **2277 décisions et délibérations** adoptées
- 390 autorisations, dont 15 autorisations uniques
- 100 avis
- 11 892 déclarations relatives à des systèmes de vidéosurveillance
- 6123 déclarations relatives à des dispositifs de géolocalisation
- 401 autorisations de systèmes biométriques
- 92 663 dossiers de formalités dont 50 000 engagements de conformité
- 14 400 organismes ont désigné un correspondant informatique et libertés (CIL)
- 44 labels ont été délivrés depuis 2012

Temps forts 2014-2015

Janvier 2014

- La formation restreinte de la CNIL prononce une sanction pécuniaire de 150 000 € à l'encontre de la société GOOGLE Inc. et l'enjoint de procéder à la publication d'un communiqué relatif à cette décision sur la page d'accueil de Google.fr, sous huit jours à compter de la notification de la décision. Google fait un recours devant le Conseil d'Etat, avant de se désister début 2015.

Février 2014

- Nouveau collège de la CNIL : élection du Président et des vice-présidents.
- Election d'Isabelle Falque-Pierrotin à la présidence du G29.
- Création d'un nouveau label pour les services de coffre-fort numérique.
- Publication de l'avis de la CNIL sur le projet de loi relatif à la géolocalisation.

Mars 2014

- La loi du 17 mars 2014 relative à la consommation donne à la CNIL la possibilité de procéder à des contrôles en ligne. Les premiers contrôles en ligne interviennent en octobre 2014.

Avril 2014

- Adoption de l'avis du G29 sur PRISM et la surveillance.

Mai 2014

- Décision de la Cour de Justice de l'Union européenne qui confirme l'application du droit de la protection des données aux moteurs de recherche. Elle en déduit que les internautes peuvent demander, sous certaines conditions, la suppression des liens vers des informations portant atteinte à la vie privée, sous le double contrôle des autorités de protection des données et du juge. C'est le droit au déréférencement.
- Publication du Cahier innovation et prospective consacré au quantified self et au corps connecté. Organisation d'une table-ronde et d'ateliers avec les professionnels.

Juin 2014

- Le G29 annonce l'élaboration de lignes directrices et de critères communs pour une approche européenne commune du droit au déréférencement.
- 1er pack de conformité pour les compteurs communicants, élaboré en collaboration avec la FIEEC.

Juillet 2014

- Réunion avec le G29 et les moteurs de recherche dans le cadre de la mise en œuvre du droit au déréférencement
- Pack de conformité pour le logement social pour aider les bailleurs sociaux à mieux comprendre et appliquer la loi « Informatique et Libertés ».

Septembre 2014

- Cookie sweep day : action européenne d'audit en ligne sur les pratiques en matière de cookies
- Politique de confidentialité de Google : le G29 propose un pack de conformité

Octobre 2014

- Avis du G29 sur l'internet des objets
- Premiers contrôles en ligne

Novembre 2014

- Le G29 adopte des lignes directrices sur le droit au déréférencement et des critères communs d'analyse des plaintes

Décembre 2014

- Le G29 et la CNIL organisent le 8 décembre *The European Data Governance Forum* à l'UNESCO qui réunit 350 personnes.
- Présentation de la déclaration adoptée par le G29 qui réaffirme les valeurs communes de l'Europe et propose des actions concrètes pour élaborer un cadre éthique européen.
- Présentation des résultats du projet Mobilitics, en partenariat avec Inria, sur les smartphones Android et leurs applications

Janvier 2015

- Remise des premiers Trophées Educnum
- Publication des propositions de la CNIL sur les évolutions de la loi « informatique et libertés » dans le cadre du projet de loi numérique.

Février 2015

- Mise en demeure du ministère de l'intérieur et du ministère de la justice pour non respect des délais légaux dans le traitement des demandes de droit d'accès indirect à TAJ.
- Désignation de la personnalité qualifiée par la CNIL parmi ses membres, en charge du contrôle du blocage administratif de sites internet

Mars 2015

- Publication de l'avis de la CNIL sur le projet de loi relatif au renseignement

Bilan 2014 : les données personnelles au cœur du débat public et des préoccupations des Français

L'année 2014 a une fois encore montré une activité de la CNIL en croissance avec 11000 demandes provenant de particuliers : 5825 plaintes dont 39% concernent l'e-réputation et 5240 demandes de droit d'accès indirect. L'actualité nationale et internationale a placé les données personnelles au centre du débat public : consécration du droit au déréférencement, projet de loi sur le numérique, projet de loi relatif au renseignement, rapport du Conseil d'Etat, négociations du règlement européen, etc. La CNIL accompagne la transition numérique des acteurs professionnels en développant des outils de conformité plus souples. Elle favorise aussi la responsabilisation des individus en leur proposant des outils pour mieux maîtriser leurs données personnelles.

_____

1. Protéger sa vie privée en ligne : une préoccupation croissante des citoyens

En 2014, la CNIL a enregistré environ **5825 plaintes**, ce qui correspond à une légère hausse des demandes (+3%). **39% de ces plaintes concernent des problématiques d'e-réputation** : suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne, la réutilisation de données publiquement accessibles sur internet, etc. Depuis la décision de la Cour de Justice de l'union Européenne en mai 2014, la CNIL a reçu **200 plaintes consécutives à des refus de déréférencement** par les moteurs de recherche.

En plus d'internet, les autres secteurs concernés par les plaintes sont les suivants :

- **Commerce** (16% des plaintes reçues) : radiation de fichiers publicitaires, conservation coordonnées bancaires, fichiers clients, opposition à recevoir des courriels publicitaires ;

M. F a réalisé un achat sur internet auprès de la société B. A la suite de cet achat, il a reçu de nombreux courriels de prospection commerciale. Un lien de désabonnement étant proposé, il l'utilise pour ne plus recevoir de prospection mais continue à recevoir les courriels. Deux mois après avoir exercé son droit d'opposition à recevoir de la prospection commerciale auprès de la société, il sollicite la CNIL afin que sa demande soit prise en compte. La CNIL a rappelé à la société que toute personne physique a le droit de s'opposer à ce que ses données soient utilisées à des fins de prospection. M. G n'a plus reçu de messages commerciaux de la société B.

- **Gestion des ressources humaines** (14% des plaintes reçues qui émanent de salariés ou de syndicats) : vidéosurveillance (300 plaintes), géolocalisation, accès au dossier professionnel, cybersurveillance ;

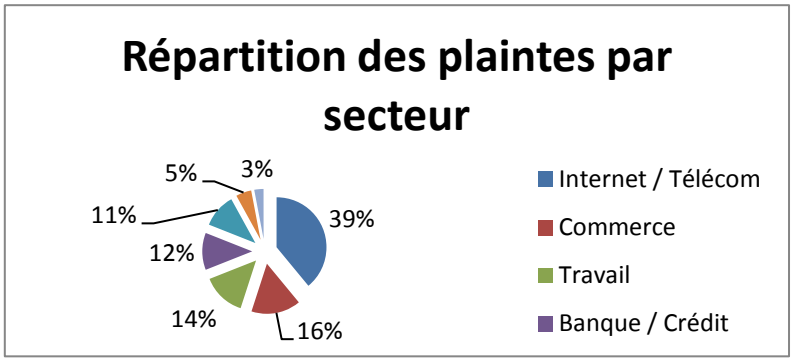
Une monitrice d'auto-école saisit la CNIL car son employeur a mis en place, sur sa voiture, un système de géolocalisation alors qu'elle est autorisée à l'utiliser en dehors de son temps de travail. La CNIL a effectué un contrôle sur place à l'issue duquel le gérant a enlevé le dispositif de géolocalisation.

- **Banque** (12% des plaintes reçues) : le motif principal de plainte est la contestation de l'inscription au FICP (fichier national des incidents de remboursement des crédits aux particuliers, ou au FCC (fichier central des chèques et des retraits de cartes bancaires).

A la suite de sa perte d'emploi, Mme G a eu des difficultés pour payer son prêt à la consommation. Après deux mensualités impayées, sa banque l'a inscrite au FICP. Mme G a retrouvé un emploi et a remboursé intégralement sa dette. Un an après, elle a sollicité un prêt immobilier auprès d'une autre banque qui le lui a refusé au motif qu'elle était inscrite au FICP. Mme G n'arrivant pas à obtenir sa radiation du fichier d'incident a sollicité la CNIL.
La CNIL a rappelé à la banque qu'elle devait procéder à la radiation de l'incident immédiatement après le remboursement intégral de la dette par l'intéressé. Mme G a finalement été défichée.

- **Libertés publiques et collectivités locales** (11% des plaintes reçues) : élections municipales, presse en ligne, diffusion par les collectivités locales de documents publics sur internet, réutilisation de données publiques.

Un propriétaire dont le bien a été vendu aux enchères retrouve l'ensemble des documents concernant la vente, en ligne, sur le site d'un cabinet d'avocat. La CNIL est intervenue auprès de ce professionnel du droit pour lui rappeler ses obligations en matière de confidentialité des données. Les éléments ont été supprimés du site.



L'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de plaintes, ainsi que l'exercice du droit d'accès.

Un nouveau service de plaintes en ligne depuis avril 2015

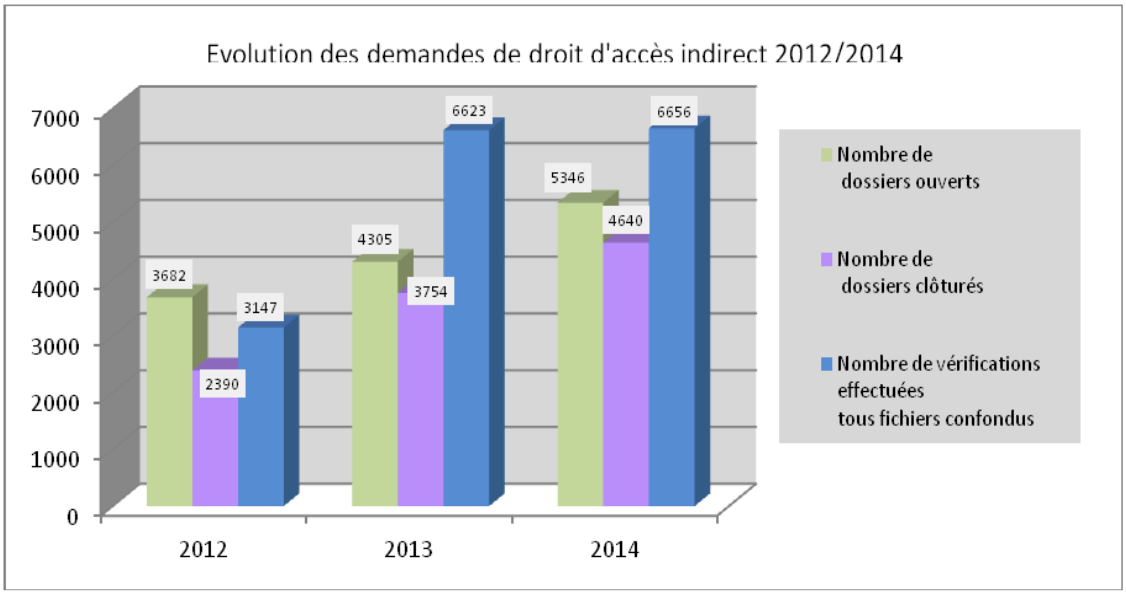
Les plaintes en ligne ont été étendues à de nouveaux cas de plaintes. Désormais, les internautes peuvent naviguer parmi une cinquantaine de cas correspondant aux plaintes les plus fréquentes.

Le service permet ainsi de répondre :

- aux difficultés liées à la suppression de données personnelles sur des sites, blogs, forums, réseaux sociaux ou des moteurs de recherches ;
- aux problèmes liés au spam et à la prospection commerciale par courrier, courriel ou par téléphone ;
- aux questions de surveillance des salariés ;
- aux inscriptions dans les fichiers d'incidents de paiement (Préventel, FICP, FCC chèques ou cartes bancaires).

2. Des demandes de droit d'accès indirect en forte croissance

En 2014, la CNIL a reçu **5246 demandes de droit d'accès indirect, soit une augmentation de 22% par rapport à 2013**. Ces demandes reçues représentent un total de 7577 vérifications à mener concernant par ordre d'importance : le fichier FICOBA de l'administration fiscale, les fichiers d'antécédents judicaires de la police et de la gendarmerie (fichier unique TAJ depuis le 1er janvier 2014) et les fichiers de renseignement.



Madame L a adressé à la CNIL une demande de droit d'accès indirect car, si dans le cadre d'une enquête de moralité réalisée dans la perspective du concours d'accès à l'Ecole Nationale de la Magistrature, un avis favorable a été émis, elle a appris à cette occasion qu'elle faisait l'objet d'une inscription dans le fichier d'antécédents judiciaires pour des faits qu'elle n'avait pas commis. Tel était bien le cas et cette affaire de «complicité d'escroquerie », qui aurait pu lui faire perdre le bénéfice de ce concours, a été effacée.

Monsieur D, a saisi la CNIL après que le Préfet de son département lui a signifié une probable abrogation de son agrément en qualité d'agent de police municipale au motif de son inscription dans le fichier d'antécédents judiciaires. Au terme des vérifications, l'affaire concernée (« refus d'obtempérer, mise en danger de la personne, défaut de permis de conduire ») a été supprimée dans la mesure où il n'était nullement le mis en cause, mais la victime.

Monsieur L., préoccupé par l'absence de réponse obtenue quant à la délivrance de sa carte professionnelle d'agent de sécurité privée a souhaité exercer son droit d'accès indirect. Aux termes des vérifications menées, une affaire de « violences volontaires et d'outrage à agent de la force publique » enregistrée à son nom dans ce fichier a été supprimée car, commise par un tiers qui avait usurpé son identité.

Gros plan sur FICOBA

Pourquoi cette augmentation des demandes d'accès à FICOBA ?

L'augmentation importante du nombre de demandes de droit d'accès indirect au fichier FICOBA dont la CNIL est désormais destinataire (**3264 demandes en 2014, soit + 50% par rapport à 2013**), trouve son origine dans la reconnaissance par le Conseil d'Etat dans une décision du 29 juin 2011 du droit d'accès des héritiers en leur qualité « d'ayant droit du solde des comptes bancaires détenus par la personne décédée ».

Que contient FICOBA ?

Ce fichier, détenu par l'administration fiscale, permet à l'héritier d'avoir un recensement des comptes détenus par le défunt sur le territoire national (établissement, numéro et nature du compte, date d'ouverture, de modification ou de clôture), de nature à faciliter ses démarches aux fins de règlement de la succession. Il ne comporte aucune donnée concernant l'historique des opérations bancaires effectuées ou le solde des comptes à une date donnée.

Vers une consultation de FICOBA par les notaires ? Les modalités d'accès à ce fichier vont être modifiées au 1er janvier 2016, date d'entrée en vigueur de la loi n°2014-617 du 13 juin 2014 relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence. Cette loi consacre, en effet, le droit pour les héritiers d'obtenir directement les données d'identification des comptes détenus par le défunt auprès de l'administration fiscale. Les notaires en charge d'une succession auront, quant à eux, non seulement un droit mais une obligation de l'interroger pour avoir communication de ces mêmes données. A compter de cette date, les héritiers et notaires ne devront donc plus s'adresser à la CNIL qui demeurera compétente, au titre du droit d'accès indirect, pour les seules demandes formulées à titre personnel (exemple : double détention de livret A).

Si on cumule les plaintes et les demandes de droit d'accès indirect, **ce sont donc plus de 11 000 demandes individuelles qui ont été adressées à la CNIL en 2014**, auxquelles s'ajoutent **133 000 appels téléphoniques reçus (contre 124 500 appels reçus en 2013).**

Ces chiffres témoignent donc de la sensibilité croissante des personnes quant à la protection de leurs données personnelles dans un univers numérique marqué par la très forte circulation de ces données.

3. Une action répressive avec des pouvoirs de contrôle renforcés

La logique de la loi et son application par la CNIL visent avant tout la mise en conformité des organismes mis en cause. A chaque phase d'instruction d'une plainte et/ou d'un contrôle, ceux-ci ont la possibilité de suivre les mesures recommandées par la CNIL pour se mettre en conformité. **Dans l'immense majorité des cas, la simple intervention de la CNIL se traduit par une mise en conformité de l'organisme.** Le prononcé de sanction par la CNIL permet de sanctionner des organismes qui persistent dans des comportements répréhensibles, et constitue donc un instrument de dissuasion important.

62 mises en demeure ont été adoptées (contre 57 en 2013), dont 69% d'entre elles ont donné lieu à une mise en conformité. Plusieurs mises en conformité sont encore en cours.
18 sanctions (contre 14 en 2013) ont été prononcées par la formation restreinte, dont 8 sanctions pécuniaires.

La CNIL a réalisé **421 contrôles** en 2014, dont **les premiers contrôles en ligne**.

A l'occasion de l'adoption de la loi relative à la consommation du 17 mars 2014, la CNIL s'est vue reconnaître la possibilité d'effectuer des contrôles en ligne, lui permettant de constater à distance, depuis un ordinateur connecté à internet, des manquements à la loi Informatique et Libertés.

Cette adaptation du pouvoir d'investigation de la CNIL au développement numérique, vient s'ajouter aux autres moyens d'enquête déjà existants : contrôles sur place au sein des organismes, auditions sur convocation à la CNIL et contrôles sur pièces.

Elle offre à la CNIL l'opportunité d'être plus efficace et réactive dans un univers en constante évolution. Elle peut ainsi plus rapidement constater et agir contre les atteintes à la protection des données et à la vie privée sur internet.

Au total, **58 contrôles en ligne** ont ainsi pu être effectué entre octobre et décembre 2014, sur plusieurs thématiques, dont :

- la conformité des pratiques des acteurs du web à la recommandation cookies et autres traceurs, adoptée par la CNIL le 5 décembre 2013 ;
- la publication des listes d'électeurs sur les sites web des Universités ;
- la sécurité relative aux formulaires de demande en ligne d'actes d'état civil sur les sites des communes.

4. Les données personnelles, au cœur du débat public

En 2014, le débat public s'est fortement structuré autour de la protection des données personnelles et des libertés numériques en France et ailleurs. On peut citer notamment le rapport du Conseil d'Etat sur le numérique ou la consultation du CNNum sur le projet de loi numérique, auxquels la CNIL a largement contribué. Elle a publié en janvier 2015 ses propositions qui comportent notamment : un droit à l'oubli pour les mineurs, des sanctions renforcées, la saisine systématique de la CNIL dans le cadre des propositions de loi.
Ce débat se poursuit en 2015 avec le projet de loi relatif au renseignement au sujet duquel l'avis de la CNIL a été rendu public, à la demande du Président de la Commission des Lois de

l'Assemblée Nationale. La CNIL a aussi été très attentive au projet de loi santé, et notamment son article 47 relatif aux modalités d'ouverture des données de santé.

Au plan international, les suites des révélations d'Edward Snowden et les débats autour du droit au déréférencement consacré par la CJUE ont alimenté les discussions. En 2015, le projet de règlement européen sur les données personnelles sera un enjeu central, de même que les mesures visant à une lutte coordonnées de l'Europe contre le terrorisme (PNR, etc.).

La CNIL, comme le G29, dont la CNIL occupe la Présidence pour deux ans, sera très active dans l'ensemble de ces débats et s'attachera à garantir **un équilibre entre libertés, sécurité et innovation.**

Les enjeux pour 2015 (1) : libertés et sécurité, quel équilibre ?

Depuis les révélations d'Edward Snowden et à nouveau, avec les attaques terroristes perpétrées en janvier 2015 en France, l'équilibre entre libertés et sécurité est débattu. Même si les impératifs d'ordre public sont forts et légitimes, ils ne doivent pas conduire à la mise en place d'une surveillance généralisée et indiscriminée des personnes, incompatible avec l'Etat de droit.

En 2013, E. Snowden a levé le voile sur la surveillance massive et généralisée de l'ensemble de la population par des acteurs privés, pour le compte d'acteurs publics. Ses révélations questionnent toutes les démocraties et les réponses que celles-ci élaborent face à une menace terroriste croissante. Les attaques terroristes de janvier 2015 ont de nouveau placé en haut de l'agenda des gouvernements le renforcement des moyens de lutte contre le terrorisme.

Pour trouver de réelles voies d'action pour faire face à la situation actuelle, il faut sortir d'une opposition binaire entre sécurité et liberté. Le respect des libertés fondamentales n'est pas contradictoire avec l'impératif de sécurité : c'est le garde-fou de nos démocraties,. Libertés et sécurité sont donc indissociables, et leur équilibre dépend des garanties et des modalités de contrôles dont elles sont assorties. Le propre d'un Etat de droit est en effet de se doter des outils légaux nécessaires pour répondre aux menaces, mais en les assortissant de garanties suffisantes pour rester fidèle aux principes et aux valeurs qui le fondent.

C'est précisément le rôle de la CNIL de contrôler cet équilibre fragile et de prévenir les dérives éventuelles, au plan national comme sur les dossiers européens. Pour ce faire, trois leviers d'action sont possibles :

Nous rassembler entre européens autour de nos valeurs communes. C'est ce que le groupe des CNIL européennes, le « G29 », a proposé dans une déclaration le 8 décembre dernier à l'occasion d'une conférence internationale à l'UNESCO. Cette déclaration pose le principe d'un nécessaire équilibre entre protection des données personnelles, innovation et surveillance, et met en avant la nécessité de mettre en œuvre des dispositifs ciblés et non massifs en matière de surveillance. Elle propose également un certain nombre de mesures opérationnelles, notamment en matière d'ordre public.

Exiger un niveau de garantie élevé pour prévenir les risques d'abus de dispositifs par nature intrusifs. C'est une exigence absolue de nos Etats de droit. L'annulation de la directive sur la rétention des données de connexion par la Cour de Luxembourg en 2014 conforte le besoin d'une approche proportionnée et accompagnée de garanties effectives pour mettre en œuvre ces dispositifs. C'est à la lumière de ces mêmes principes que la CNIL a été saisie par le Gouvernement sur le PNR français qui permet la collecte de données des passagers aériens lors des vols à destination et en provenance du territoire national. Elle a, dans le cadre de l'examen du décret publié le 26 septembre 2014, demandé et obtenu des garanties fortes (information des personnes, durée de conservation limitée, absence de données « sensibles », etc.).

Renforcer le contrôle en aval de ces dispositifs. Une personnalité qualifiée au sein de la CNIL est chargée depuis février 2015 de contrôler le blocage administratif des sites provoquant des actes de terrorisme ou en faisant l'apologie ainsi que les sites à caractère pédopornographique. Ce contrôle vise à s'assurer que le blocage n'est pas disproportionné afin d'éviter tout « sur blocage ».

Dans le cadre du projet de loi relatif au renseignement, la CNIL a rendu un avis le 5 mars 2015, dans lequel elle a été très attentive aux modalités de contrôle des fichiers de renseignement. Ces fichiers bénéficient actuellement d'un cadre législatif spécifique interdisant le contrôle de leur régularité du point de vue de la loi Informatique et Libertés. Or, un tel contrôle général constitue une exigence fondamentale afin d'asseoir la légitimité démocratique de ces fichiers dans le respect des droits et libertés des citoyens.

La CNIL a proposé que le projet de loi lui permette d'exercer un tel contrôle, selon des modalités particulières, adaptées aux activités des services de renseignement, et en coopération avec la CNCTR (Commission Nationale de Contrôle des Techniques de Renseignement). Cette proposition n'a pour l'heure pas été suivie d'effet.

THE EUROPEAN DATA GOVERNANCE FORUM

UNESCO-PARIS 8 DÉCEMBRE 2014 / 8 DECEMBER 2014

DÉCLARATION COMMUNE DES AUTORITÉS EUROPÉENNES DE PROTECTION DES DONNÉES RÉUNIES AU SEIN DU GROUPE DE L'ARTICLE 29

1 **La protection des données à caractère personnel est un droit fondamental**. Les données personnelles ne peuvent pas être traitées comme un simple objet de commerce, un actif économique ou un bien de consommation.

2 **Les droits des personnes au regard de la protection de leurs données doivent être combinés avec les autres droits fondamentaux**, notamment la prohibition de toute discrimination et la liberté d'expression, qui sont de valeur égale dans toute société démocratique. Ils doivent également être articulés avec l'impératif de sécurité.

3 **La technologie est un moyen qui doit demeurer au service de l'homme**. Le fait qu'un traitement de données soit techniquement faisable, n'implique pas qu'il soit de ce fait acceptable sur les plans social et éthique, ni qu'il soit conforme à la loi.

4 **La confiance du public dans les produits et services de l'économie numérique** dépend en grande partie du respect des règles de protection des données par l'industrie. Le respect de ces règles constitue un facteur concurrentiel fondamental pour les acteurs économiques.

5 **La prise de conscience et les droits des personnes** doivent être renforcés pour leur permettre de limiter leur exposition à un risque de surveillance excessive par les acteurs publics ou privés. L'éducation au numérique peut y contribuer.

6 **La surveillance secrète, massive et indiscriminée** est inacceptable sur le plan éthique.

7 **L'accès à des données personnelles aux fins de sécurité n'est pas acceptable dans une société démocratique** dès lors qu'il est massif et sans condition.

8 **Le traitement de données personnelles dans le cadre d'activités de surveillance** doit faire l'objet d'un **contrôle indépendant et effectif**, auquel les autorités de protection des données doivent être associées selon leurs compétences.

9 L'autorité publique d'un Etat non membre de l'Union ne peut par principe **accéder directement à des données personnelles couvertes par les règles européennes**, quelles que soient les conditions de cet accès ou la localisation de ces données. Des demandes d'accès émanant de l'étranger ne peuvent être adressées directement aux sociétés soumises au droit de l'Union.

10 Aucune des dispositions figurant dans les **instruments européens visant à encadrer les transferts internationaux de données** entre acteurs privés ne peut servir de base légale à des transferts de données vers les autorités de pays tiers pour des finalités de surveillance massive et indiscriminée.

11 **Le stockage de ces données sur le territoire de l'Union** est un moyen de faciliter le contrôle effectif par une autorité européenne indépendante.

12 **Les projets européens de règlement et de directive relatifs à la protection des données doivent être adoptés en 2015**. Ces textes doivent assurer un haut niveau de protection des données, conforme aux valeurs et droits fondamentaux de l'Europe.

13 Le niveau européen de protection des données ne peut être érodé, en tout ou partie, par des accords bilatéraux ou internationaux, **y compris des accords commerciaux** sur les biens et services à conclure avec des pays tiers.

14 Les règles de protection des données de l'Union doivent être considérées comme des principes internationaux impératifs en **droit international public et privé**.

15 L'équilibre à établir entre protection des données, innovation et surveillance n'implique **ni de reconstruire les frontières internes de l'Union ni de fermer les portes de l'Europe** à des partenariats étrangers.

16 Le Groupe de l'article 29 ouvre cette Déclaration aux commentaires **de toute partie intéressée**, qu'elle soit de statut public ou privé. Ces commentaires peuvent lui être adressés par l'intermédiaire du site Web disponible à l'adresse **www.europeandatagovernance-forum.com**. Le Groupe tiendra compte de ces commentaires dans ses activités de l'année 2015.

ARTICLE 29
Data Protection Working Party

CNIL
Commission Nationale de l'Informatique et des Libertés

Les enjeux de 2015 (2) : la protection des données, clé de voûte de l'innovation

Alors que les innovations numériques reposent de plus en plus sur le traitement de données personnelles, une protection optimale de ces données constitue non seulement un impératif pour nos concitoyens, mais aussi un avantage concurrentiel sur des marchés disputés. Loin d'opposer artificiellement innovation et protection des données, il faut au contraire voir dans la seconde la condition de réussite de la première, dans le cadre d'un accompagnement adapté de la CNIL.

Nombreux sont ceux qui, ces dernières années, ont tenté d'opposer artificiellement innovation et protection des données, voyant dans la loi « informatique et libertés » un obstacle potentiel au développement de nouveaux services ou technologies, notamment liés au « big data ».

Or, loin d'une telle affirmation stérile et erronée, l'expérience concrète des projets montre que **la protection des données personnelles et l'innovation sont aujourd'hui indissociables à l'ère numérique**. La confiance des consommateurs dans l'économie numérique et les nouveaux services qui leur sont proposés est en effet subordonnée à la protection effective de leurs données. Une illustration en est fournie en matière de *cloud* : à la suite des révélations de M. Snowden, un rapport de l'Information Technology and Innovation Foundation a évalué les pertes pour les sociétés américaines à $22 milliards de dollars. Dans le même temps, les sociétés américaines ou européennes comprennent désormais qu'il ne s'agit pas seulement d'une question d'image, mais aussi d'une question de compétitivité.

Au-delà des mots, c'est dans l'accompagnement concret de services opérationnels que la CNIL est quotidiennement engagée. Ainsi, si certains font valoir une nouvelle « révolution » du big data, permettant de croiser de manière quasi-universelle des volumes considérables de données pour faire émerger de nouveaux services il apparaît que le « big data » présente certes un caractère inédit par son échelle, mais s'inscrit dans le prolongement de processus classiques de croisements de données à des fins de profilage. **Ce ne sont pas nécessairement les principes Informatique et Libertés qu'il faut remettre en cause mais c'est assurément les outils de la régulation qu'il faut adapter.**

C'est donc dans **un état d'esprit pragmatique, ouvert et soucieux d'accompagner l'innovation** que s'inscrit la CNIL.

Elle a, à cet égard, organisé ses services et adapté ses modes de travail pour être au plus près de ses publics et des innovations. En promouvant le passage d'une logique de formalités administratives à une logique de conformité tout au long de la vie du traitement de données, la CNIL positionne ainsi l'innovation au cœur de son action et de son fonctionnement.

Quelques exemples en témoignent :

- La constitution d'un « pôle innovation et prospective », depuis plus de trois ans, porte ses fruits : la CNIL est désormais en contact avec de très nombreuses start-up ou pépinières de talents, qu'elle conseille dès la conception de leurs produits pour une protection optimale des données ;

- La CNIL mène par ailleurs une activité de recherche, souvent en liaison avec des laboratoires, pour tester les dispositifs innovants ou proposer des solutions. Ainsi, le projet Mobilitics avec Inria constitue le premier projet d'expérimentation dans des conditions réelles permettant de connaître tous les échanges de données entre un smartphone et des entités tierces. De même, le logiciel Cookieviz, développé en open source par la CNIL, a été téléchargé plus de 100 000 fois et permet à des internautes de voir concrètement, et tous navigateurs confondus, la face cachée de leur navigation.

- Enfin, la CNIL organise chaque année des rencontres thématiques réunissant l'ensemble d'un écosystème numérique : après une journée dédiée à l'open data, la CNIL a ainsi organisé en janvier 2015 une matinée dédiée à la voiture connectée, qui a rassemblé pour la première fois l'ensemble des acteurs de la filière.

Pour la CNIL, l'innovation n'est donc ni un mot, ni une notion abstraite : c'est une réalité, expérimentée et accompagnée quotidiennement dans le cadre d'outils innovants. En effet, au-delà de la connaissance de nouvelles pratiques ou technologies, la CNIL innove dans les modalités d'accompagnement de ces acteurs.

C'est ainsi que la Commission a mis en place un nouvel outil de régulation, les « **packs de conformité** ». Elaborés en concertation avec les acteurs d'un secteur, ces packs regroupent des bonnes pratiques permettant de décliner les droits et obligations de la loi informatique et libertés pour les acteurs du secteur en question, et des instruments de simplification des formalités administratives (normes simplifiées, autorisations uniques, dispenses de déclarations, etc.). L'objectif est ainsi de fournir un cadre juridique et pratique sûr et adapté aux besoins d'un secteur donné. Plusieurs « packs » ont déjà été adoptés, pour les assurances, le logement social ou la domotique. Deux autres (banque et secteur social) sont en cours d'élaboration.

Prolongeant les packs, la CNIL a également mis en place des « **clubs conformité** », qui réunissent de manière informelle les acteurs d'un secteur pour mieux identifier les innovations et les questions pratiques émergentes.

Les **labels** s'inscrivent dans la même logique de responsabilisation des acteurs et de simplification.

Lucidité sur les enjeux, expérience concrète de l'innovation, ouverture aux acteurs et nouveaux modes de régulation sont donc les orientations de la CNIL **pour accompagner le développement d'un numérique durable**.

Les enjeux de 2015 (3) : Quels nouveaux droits pour mieux maîtriser ses données ?

Pour être durables, les nouveaux modèles numériques doivent se construire autour de l'utilisateur, de ses usages et des ses attentes. La protection des données personnelles en fait partie : l'utilisateur s'attend désormais à détenir une véritable capacité de maîtrise, de choix et d'arbitrage sur ses données. Comment atteindre cet objectif dans un environnement en évolution permanente ? C'est l'objet du projet de règlement européen en cours de négociations.

Si les utilisateurs ne font pas confiance aux services de l'économie numérique, ils ne les utiliseront pas. Cette exigence de confiance est fondamentale, mais elle est encore loin d'être satisfaite à en croire plusieurs études menées par la Commission européenne : ainsi, plus de 90% des Européens s'inquiètent du fait que des applications mobiles collectent leurs données sans leur consentement *.

Le projet de règlement sur la protection des données, en cours de négociations à Bruxelles, vise à favoriser le développement de cette confiance en Europe, en particulier en renforçant la capacité des citoyens à contrôler l'usage de leurs données. Pour ce faire, le projet de texte prévoit un véritable « droit à l'oubli », un « droit à la portabilité » des données, ainsi que le droit des personnes d'être informées des failles ayant affecté leurs données personnelles.

Le « droit à l'oubli » permettra d'obtenir la suppression des données de l'utilisateur si celui-ci souhaite qu'elles ne soient plus traitées et s'il n'y a pas de motif légitime pour qu'une entreprise les conserve. Appliqué aux moteurs de recherche, ce droit à l'oubli s'entend comme un « droit au déréférencement » sur lequel la CNIL et ses homologues européens ont adopté des lignes directrices communes en 2014. Une idée fausse encore répandue consiste à soutenir que ce droit permet d'effacer le passé ou de restreindre la liberté de la presse. Tel n'est pas le cas. Le droit à l'oubli permet aux personnes de contrôler l'impact de la diffusion de leurs données sur leur vie personnelle et professionnelle. La pratique quotidienne de la CNIL et de ses homologues européens attestent de l'importance sociale de ce droit.

Le texte vise également à **garantir aux personnes un accès libre et aisé à leurs données personnelles**, pour qu'elles puissent voir plus facilement quelles sont celles dont disposent les entreprises et les pouvoirs publics et qu'elles puissent transférer leurs données facilement et gratuitement d'un prestataire de services à un autre – c'est le principe de « **portabilité des données** ». Il s'agit de permettre aux personnes de ne pas demeurer captives d'un seul écosystème numérique et de pouvoir migrer vers d'autres, notamment quand ceux-ci s'avèreraient plus protecteurs en matière de vie privée.

* SPECIAL EUROBAROMETER 359 - Attitudes on Data Protection and Electronic Identity in the European Union (June 2011)

Le texte prévoit enfin **une obligation de notification des failles**, **en imposant aux organisations d'informer les intéressés et l'autorité compétente** en matière de protection des données dans les meilleurs délais – dans la mesure du possible, dans les 24 heures – si des données sont accidentellement ou illégalement détruites, perdues, altérées, consultées par des personnes non autorisées ou divulguées à de telles personnes. Aujourd'hui, seuls les opérateurs de communication électronique sont soumis à cette obligation de notification des failles.

La CNIL et ses homologues européens apportent leur plein et entier soutien aux nouveaux droits prévus par le texte.

De façon plus opérationnelle et afin de donner aux citoyens la possibilité d'exercer pleinement leurs droits, la CNIL a pris plusieurs initiatives :

- Mise en ligne, le 28 janvier 2015, à l'occasion de la journée européenne de la protection des données, d'un nouvel espace entièrement dédié aux droits des citoyens en matière de données personnelles. La CNIL y explique les droits et propose de nombreux conseils pour les exercer plus facilement.

- Ouverture en avril 2015 d'un nouveau service de plaintes en ligne étendu à de nouveaux cas de plaintes.

- Lancement à partir de mai 2015 d'un service de réponses en ligne pour les particuliers pour les accompagner au quotidien dans l'exercice de leurs droits.

Droit au déréférencement : état des lieux un an après la décision de la Cour de Justice de l'Union Européenne

Le 13 mai 2014, la Cour de Justice de l'Union européenne a rendu un important arrêt qui consacre pour les personnes la possibilité d'obtenir des moteurs de recherche le déréférencement de certaines de leurs données, dans certaines conditions.

Le 13 mai 2014, la Cour de Justice de l'Union européenne a rendu un arrêt majeur dans une affaire "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (C-131/12).

De nombreux commentateurs de cet arrêt ont souligné son caractère inédit, le présentant comme consacrant un « droit à l'oubli ». Telle n'est pourtant pas la réalité du droit consacré par la Cour : **il s'agit en réalité, pour les personnes, de la possibilité d'obtenir des moteurs de recherche le déréférencement de certaines de leurs données, dans certaines conditions.** Ce droit au déréférencement ne constitue pas davantage une révolution juridique : il est la déclinaison, pour le cas particulier des moteurs de recherche, des droits d'accès, d'effacement et d'opposition, que consacre la loi « Informatique et Libertés » en France depuis 1978, et la directive dans l'ensemble de l'Union européenne depuis 1995.

Pour autant, l'arrêt comporte des éléments d'importance fondamentale pour le droit européen en matière de protection des personnes au regard du traitement de leurs données personnelles.

Applicabilité de la directive 95/46/CE aux moteurs de recherche

L'arrêt de la Cour qualifie les activités des moteurs de recherche de « traitements de données à caractère personnel » au sens de la directive Européenne.

En retenant cette qualification, la Cour a écarté l'argument des moteurs selon lesquels ceux-ci, n'étant pas à l'origine des données accessibles à travers leurs services, ne sauraient voir peser sur eux aucune responsabilité au sens de ce texte – argument que le G29 contestait depuis plusieurs années déjà.

Applicabilité du droit européen à la société Google Spain, bien que le serveur à partir duquel sont traitées les données du plaignant se trouve aux Etats-Unis

L'arrêt retient la pleine application des règles européennes de protection des données aux moteurs de recherche, au motif que ceux-ci sont établis sur le territoire européen du fait du modèle économique de leurs activités.

Possibilité pour toute personne physique de demander que ses données ne soient plus accessibles via un moteur de recherche sur le fondement du droit européen

L'arrêt permet aux personnes d'obtenir d'un moteur de recherche la suppression d'un ou plusieurs résultats de la liste de résultats associés à leurs données personnelles (en pratique, leurs nom et prénom).

Les lignes directrices du G29 et les critères communs pour l'instruction des plaintes

Le 26 novembre 2014, Le G29 a adopté deux documents pour permettre la mise en œuvre du droit au déréférencement : d'une part, une interprétation commune de l'arrêt, d'autre part, des critères communs pour l'instruction des plaintes qui leurs sont adressées à la suite d'un refus de déréférencement.

Les critères retenus consistent en une série de questions qui, combinées entre elles, permettent de déterminer si l'information figurant dans le moteur de recherche doit ou non être déréférencée. Ces critères portent tant sur la personne qui exerce son droit au déréférencement que sur le contenu incriminé lui-même, ou sur le contexte de sa mise en ligne. Depuis cette date, la CNIL utilise cette boîte à outils pour examiner les **200 plaintes** qui lui ont été soumises par les internautes et confirmer, ou non, les décisions de refus de déréférencement que ceux-ci ont essuyées de la part des moteurs de recherche.

S'agissant de **la portée territoriale du droit au déréférencement**, le G29 considère que, pour donner plein effet à l'arrêt de la Cour de justice, les décisions de déréférencement doivent être mises en œuvre de manière à garantir effectivement la protection des droits fondamentaux des personnes et à ne pas permettre leur contournement.

Cela signifie donc, en pratique, que le déréférencement doit être effectif sur toutes les extensions d'un nom de domaine, européennes, ou non, y compris (mais non seulement) l'extension .com.

Depuis mai 2014, Google indique s'être prononcé sur le déréférencement de plus de 800 000 URL qui correspondant à moins de 300000 demandes (mars 2015). **Dans la moitié des cas, les demandes de déréférencement ont été acceptées par Google.**

Un ressortissant français travaillant à l'international et d'origine extra-européenne a demandé le déréférencement de contenus diffamants et injurieux le concernant. Le moteur de recherche concerné a accepté leur déréférencement mais uniquement à partir de l'extension française. Pour autant, les proches de cette personne vivant encore dans son pays d'origine ainsi que ses relations professionnelles situées hors de France continuaient à accéder aux informations incriminées, sur la base de la saisie de son nom. C'est pourquoi la personne a décidé de saisir la CNIL pour obtenir un déréférencement global.

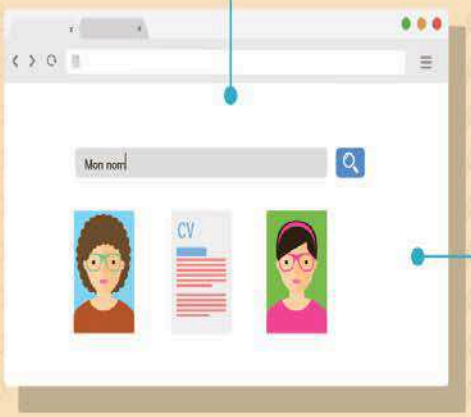
À la suite d'une demande de déréférencement ayant fait l'objet d'un refus auprès de Google, M.H s'est tourné vers la CNIL qui a décidé d'appuyer sa demande de déréférencement auprès de Google. M.H souhaitait en effet le déréférencement d'une URL menant à un article datant de la fin des années 90 et qui mentionnait son échec à un examen à la suite d'une garde à vue.Cette information, n'étant plus d'actualité et fortement préjudiciable au regard de sa vie professionnelle, a fait l'objet d'un second examen, qui s'est révélé positif, de la part de Google.

CNIL.

COMMENT DÉRÉFÉRENCER UNE INFORMATION ME CONCERNANT SUR UN MOTEUR DE RECHERCHE

Depuis 2014, les citoyens enropéens peuvent s'adresser aux moteurs de recherche pour **demander le déréférencement d'un contenu** web associé à leurs nom et prénom.

Ne plus associer mon nom à un contenu dans un moteur de recherche



POUR DÉRÉFÉRENCER UN CONTENU

Contactez d'abord le moteur de recherche via le formulaire dédié ou par courrier.

Motivez votre demande

Le contenu lié à cette URL
me concerne car
Il a été publié par une autre personne que moi
Il me porte préjudice car
Il est sensible, inexact et/ou obsolète car

Joignez une pièce d'identité

2 mois

Le moteur de recherche a deux mois pour répondre mais la demande peut être traitée en quelques jours.

REFUS

Contestez ce refus auprès de la CNIL via son formulaire de plainte en ligne

ET / OU

Saisissez la justice afin qu'elle vérifie et ordonne les mesures nécessaires

ACCEPTATION

En France

48%

des requêtes ont été déréférencées de Google.fr

(mai 2014)

Retrouvez vidéos, tutoriels et modèles de lettre sur www.cnil.fr

Projet de loi relatif au renseignement

Ce projet de loi, adopté par le Conseil des ministres du 19 mars 2015, est en cours de discussion devant le Parlement. La CNIL a rendu un avis lors de la séance plénière du 5 mars qu'elle a publié, à la demande du Président de la Commission des Lois de l'Assemblée nationale. Le texte a beaucoup évolué depuis que la CNIL s'est prononcée, prenant en compte plusieurs de ses recommandations. Elle reste cependant très attentive aux modifications proposées par les parlementaires.

_____

L'avis de la CNIL a permis de resserrer le texte et de limiter ainsi le caractère massif de la surveillance. Des garanties substantielles ont été apportées sur les points suivants :

- **S'agissant des interceptions de sécurité**, le projet de loi a été précisé afin de limiter les personnes pouvant faire l'objet de telles " écoutes ". Il prévoit dorénavant la nécessité d'une autorisation expresse pour intercepter les correspondances des personnes qui ne font pas l'objet d'une surveillance particulière mais qui appartiennent à l'entourage d'une personne surveillée et qui sont susceptibles de jouer un rôle d'intermédiaire ou de fournir des informations essentielles.
- **S'agissant du recueil de données en temps réel sur les réseaux des opérateurs**, le projet de loi précise que de telles opérations ne peuvent porter que sur les données techniques de connexion, et en aucun cas sur le contenu des correspondances échangées (téléphone, courriel, contenu des SMS, etc.).
- **Les conditions de mise en œuvre et de contrôle des dispositifs techniques de proximité** (dits " IMSI catcher ") ont été précisées. La nature des données pouvant être recueillies par ces dispositifs a été limitée et des conditions de conservation plus rigoureuses ont été prévues s'agissant des correspondances.
- Enfin, **les techniques actuellement dévolues à la seule police judiciaire**, et particulièrement intrusives (pose de balises de localisation, de micros ou utilisation de key-loggers), ne pourront être utilisées par les services de renseignement qu'en dernier ressort, si aucun autre moyen n'est utilisable. De même, les durées de mise en œuvre de ces techniques et de conservation des données ainsi recueillies ont été réduites.

La CNIL reste cependant particulièrement vigilante à l'occasion des discussions à venir au Parlement. Elle insiste notamment sur les modalités de contrôle des fichiers de renseignement :

Ces fichiers bénéficient actuellement d'un cadre législatif particulier interdisant de fait le contrôle de leur régularité du point de vue de la loi " Informatique et Libertés ". Or, le contrôle de ces fichiers constitue une exigence fondamentale afin d'asseoir la légitimité de ces fichiers dans le respect des droits et libertés des citoyens.

Le projet de loi prévoit des dispositions encadrant la collecte des renseignements mais n'a pas prévu de contrôle, en aval, sur l'utilisation des fichiers ainsi alimentés.

Dans ce contexte, la Commission a proposé que le projet de loi lui permette d'exercer un tel contrôle, selon des modalités particulières, adaptées aux activités des services de

renseignement, et en coopération avec la Commission Nationale de Contrôle des Techniques de Renseignement.

Cette proposition n'a pour l'heure pas été suivie d'effet.

Projet de règlement européen : point d'étape

L'année 2014 a été marquée par un tournant politique important et de réelles avancées sur le projet de Règlement. D'abord au Parlement Européen avec le vote à l'unanimité des amendements proposés au projet de la Commission européenne, puis au Conseil de l'UE avec une progression notable sur plusieurs aspects essentiels du projet de Règlement. La CNIL, toujours vigilante à garantir un haut niveau de protection pour les citoyens, a suivi avec la plus grande attention l'avancée de ces travaux.

_____

Après l'accord politique obtenu au Parlement Européen en mars 2014, le Conseil de l'UE a vu le rythme de ses travaux s'accélérer sous l'égide de la présidence grecque puis italienne.

Ainsi, les ministres de l'UE lors des Conseils de juin, d'octobre, puis celui de décembre 2014, se sont mis d'accord sur les points suivants :

- Le champ d'application territorial du Règlement ;
- Le chapitre relatif aux transferts (Chapitre V) avec l'introduction de nouveaux outils d'encadrement des transferts (codes de conduite et mécanismes de certification approuvés);
- Le chapitre relatif aux obligations des responsables de traitement et des sous-traitants (chapitre IV) avec une approche par les risques comme outil de modulation des obligations applicables aux responsables de traitement et aux sous-traitants ;
- Les dispositions relatives au secteur public.

A la suite des événements de janvier 2015, la CNIL ainsi que le G29, a réitéré l'impératif à voir le projet de Règlement adopté en 2015. C'est en sens que la nouvelle Présidence Lettone a poursuivi ses travaux et qu'un accord général partiel sur le chapitre relatif aux principes (Chapitre II) et le guichet unique (Chapitres VI et VII) a été obtenu lors du dernier Conseil JAI du 13 mars 2015

Concernant **le guichet unique**, ses éléments constitutifs sont les suivants :

- Pour les cas transfrontaliers, c'est-à-dire relatifs à un traitement concernant plusieurs établissements dans l'UE ou affectant des personnes dans plusieurs Etats membres, une coordination entre une autorité chef de file et les autres autorités de protection concernées est nécessaire ;
- Pour les cas locaux (ex : plaintes/ manquement non général aux dispositions du règlement) concernant un traitement transfrontalier, les autorités nationales restent compétentes dès lors que le traitement est mis en œuvre dans un seul Etat membre ou n'affecte les personnes que d'un seul Etat membre ;
- L'EDPB (futur G29) dispose de la personnalité morale et de la possibilité d'adopter des décisions contraignantes.
- Les citoyens disposent de la possibilité d'exercer leur recours devant leur juridiction nationale.

La CNIL continue de sensibiliser les pouvoirs publics et s'attache également à défendre ses positions dans le cadre du G29.

Elle a ainsi contribué activement à l'élaboration de plusieurs documents en lien avec l'avancée des travaux communautaires, notamment sur les éléments clés du guichet unique, les transferts et l'approche basée sur les risques.

L'année 2015 s'avèrera cruciale car elle devrait être celle du trilogue et de l'adoption finale du projet de Règlement, nouveau modèle européen en matière de protection des données. En effet, le règlement devra à terme remplacer le texte fondateur actuel, la Directive 95/46/EC et l'ensemble des lois nationales de transposition contraires.