CONFÉRENCE DE PRESSE

8 AVRIL 2016

Présentation du

Rapport d'activité 2015

#DirectCNIL

Sommaire

Chiffres clés de l'année 2015

Les particuliers et la CNIL

Plus de 13 790 demandes individuelles adressées à la CNIL

- 7 908 plaintes (2000 de plus qu'en 2014, **+ 36 % par rapport à 2014**)
  - Dont 36% concernent l'e-réputation.
- 5 890 demandes de droit d'accès indirect (fichiers de police, de gendarmerie, de renseignement, FICOBA, etc.)
  - **+ 12 % par rapport à 2014.**

L'action de contrôle et de sanction

- 510 contrôles (dont 155 contrôles en ligne et 87 contrôles vidéoprotection)
- 93 mises en demeure

10 sanctions

Dont :

- 7 avertissements
- 3 sanctions financières

L'encadrement et la mise en conformité des acteurs

- **2 571 décisions et délibérations** adoptées
- 244 autorisations
- 150 avis
- 12 463 déclarations relatives à des systèmes de vidéosurveillance
- 6 852 déclarations relatives à des dispositifs de géolocalisation
- 359 autorisations de systèmes biométriques
- 96 323 dossiers de formalités **dont 50 339 formalités simplifiées**
- 16 406 organismes ont désigné un correspondant informatique et libertés (CIL), soit 4 321 CIL.
- 73 labels ont été délivrés depuis 2012
- 78 groupes ont adopté des BCR

Temps forts 2015-2016

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

Avril 2015

- Publication de l'avis sur la création du fichier des auteurs d'infractions terroristes (FIJAIT)

Juin 2015

- Interdits de stade : mise en demeure du PSG FOOTBALL
- Mise en demeure adressée à Google lui demandant de procéder aux déréférencements sur toutes les extensions du moteur de recherche
- Projet de règlement européen : avis du G29 dans la perspective du trilogue
- Cookies et autres traceurs : premier bilan des contrôles

Juillet 2015

- Étude d'impacts sur la vie privée : publication de la méthode PIA de la CNIL
- Relations clients : mise en demeure de la société BOULANGER pour commentaires excessifs
- Données traitées par les sites de rencontre : 8 mises en demeure

Septembre 2015

- Internet Sweep Day : une protection insuffisante sur les sites pour les enfants
- Droit d'accès au traitement d'antécédents judiciaires (TAJ) : clôture de la mise en demeure des ministères de l'intérieur et de la justice
- Interdits de stade : clôture de la mise en demeure du PSG FOOTBALL

Octobre 2015

- Invalidation du *safe harbor* par la Cour de Justice de l'Union européenne
- Organisation de la convention des CIL, à l'occasion de leurs 10 ans d'existence
- *Safe harbor* : le G29 demande aux institutions européennes et aux gouvernements d'agir sous 3 mois

Novembre 2015

- Relations clients : clôture de la mise en demeure de la société BOULANGER pour commentaires excessifs
- Le premier label « Gouvernance Informatique et Libertés » a été délivré
- Défaut de sécurité de données clients : sanction de 50 000 € à l'encontre d'Optical Center
- Lire, écouter, regarder et jouer en ligne à l'heure de la personnalisation : publication du nouveau cahier IP

Décembre 2015

- Politique de confidentialité de Facebook : 5 autorités européennes prennent position
- Projet de loi République numérique : publication de l'avis de la CNIL
- Consensus sur le Paquet européen protection des données personnelles

Janvier 2016

- La CNIL participe au Forum international de la cybersécurité (FIC)

Février 2016

- Safe harbor : le G29 analyse les conséquences de la décision de la CJUE
- La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi Informatique et Libertés

Mars 2016

- Avertissement public de la société NC NUMERICABLE pour erreur dans la transmission de données d'identification sur ses abonnés
- Éducation au numérique : le Ministère de l'Éducation nationale et la CNIL signent une convention de partenariat
- En route vers un pack de conformité consacré aux véhicules connectés
- Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre de Google

Bilan 2015 : un nombre record de plaintes

L'année 2015 est marquée par une forte augmentation de l'activité de la CNIL, avec 13 790 demandes provenant de particuliers : 7908 plaintes dont 36% concernent l'e-réputation et 5 890 demandes de droit d'accès indirect. Cette évolution témoigne de la volonté des citoyens de reprendre leurs droits en main au bénéfice de plus de transparence et de sécurité, notamment dans la gestion de leur e-réputation.

1. Protéger sa vie privée en ligne : de la préoccupation à la responsabilisation

En 2015, la CNIL a enregistré 7 908 plaintes, soit 2000 de plus qu'en 2014 (36 % de hausse).

Cette augmentation importante s'explique par la prise de conscience croissante des citoyens, notamment pour la gestion de leur réputation en ligne. Cela se traduit par la pratique régulière de l'*ego-surfing*, qui est souvent à l'origine de demandes de retraits de contenus ou de déréférencement. En cas de refus de l'éditeur du site ou du moteur de recherche, la CNIL peut être saisie d'une plainte. A titre indicatif, la CNIL a ainsi reçu près de 700 plaintes depuis l'été 2014 et la consécration par la Cour de justice de l'Union européenne d'un droit au déréférencement. Enfin, la médiatisation d'affaires touchant à la sécurité des données tend aussi à sensibiliser les citoyens à cette problématique croissante.

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

Afin de faciliter les démarches des personnes qui la saisissent et de fiabiliser leurs demandes, la CNIL a amélioré en avril 2015 son service de plaintes en ligne en déployant une cinquantaine de scénarios correspondant aux plaintes les plus fréquentes.

Les 5 typologies principales

Internet / téléphonie (36 % des plaintes)

Quels motifs ? Opposition à la diffusion de données personnelles (nom, coordonnées, commentaires, photos) sur un annuaire, un site marchand, un site de rencontres, un réseau social, un blog ou un forum etc.

La diffusion de ces données porte atteinte à la réputation des personnes concernées qu'il s'agisse d'un contexte personnel ou professionnel, notamment dans le cadre de la recherche d'emploi.

Un arbitre amateur s'étonne auprès de la CNIL de pouvoir accéder en ligne, sur le site web d'un district à un procès-verbal de commission ayant prononcé une sanction disciplinaire à son encontre. Interrogée par la CNIL, la fédération a demandé aux ligues et aux districts de retirer de leur site web tous les procès-verbaux et autres relevés de décisions à caractère disciplinaire.

Quels motifs ? Sollicitations par SMS ou téléphone et à l'inscription au fichier PREVENTEL (liste noire en matière d'impayés commune à la plupart des opérateurs).

Commerce/marketing (26% des plaintes)

Quels motifs ? Radiation de fichiers publicitaires, conservation coordonnées bancaires sans accord préalable, opposition à recevoir des courriels publicitaires ou spam.

Les personnes ne souhaitent pas que leurs adresses soient publiées ou récupérées lorsqu'elles déposent des annonces en ligne. Elles s'inquiètent également de la conservation sans leur accord des informations relatives à la carte bancaire qui sont susceptibles d'être réutilisées pour réaliser des achats frauduleux.

A la suite d'un achat en ligne auprès d'une société française, Monsieur G. reçoit des sollicitations par courriel plusieurs fois par jour. Il s'oppose à ce démarchage via le lien de désabonnement indiqué dans les courriels, mais sans succès. Le plaignant est agacé par ces sollicitations répétées et adresse une plainte à la CNIL en joignant la copie d'écran de sa demande auprès de la société. La CNIL est intervenue auprès de la société et M. G a enfin été supprimé des listes de diffusion.

Gestion des ressources humaines (16% des plaintes)

Quels motifs ? La moitié des plaintes (500 environ) concernent des dispositifs vidéo filmant les salariés sur leur lieu de travail, souvent de manière disproportionnée. De nouveaux dispositifs de vidéosurveillance au travail se développent : surveillance des chaînes de production pour des raisons d'hygiène ou de sécurité, application pour surveiller les magasins et les employés depuis le smartphone de l'employeur, webcam pour surveiller la présence en télétravail, etc.

Les autres cas concernent la géolocalisation des véhicules ou des smartphones, l'accès à la messagerie, la prise de contrôle à distance des postes de travail etc.

Les employés sont souvent insuffisamment informés des dispositifs mis en place par leur employeur. Certains employeurs refusent de communiquer au salarié les informations en lien avec son dossier professionnel.

Madame T. signale à la CNIL un transfert automatique de tous les courriels reçus sur son adresse professionnelle vers l'adresse de sa supérieure hiérarchique, et ce sans information préalable. La CNIL est intervenue auprès de l'employeur, en lui rappelant que de tels envois systématiques étaient excessifs au regard du droit à la vie privée du salarié sur le lieu de travail. L'organisme a cessé ces transferts automatiques, non prévus par la charte informatique, et dont les salariés n'étaient pas informés.

Banque/crédit (10% des plaintes)

Quels motifs ? Absence de levée de l'inscription au fichier des incidents de crédit et de paiement (FICP) ou au fichier central des chèques et cartes après régularisation (FCC).

Ces levées d'inscription tardives des fichiers gérés par la Banque de France, obtenues après l'intervention de la CNIL, et bien que les personnes ont régularisé leur situation, entraînent des préjudices importants. Ainsi, une inscription au FICP ne permet souvent pas aux personnes de se voir attribuer des moyens de paiement (chéquier, carte bancaire) et l'inscription au FCC entraîne les mêmes désagréments.

Quels motifs ? Plaintes relatives aux cartes bancaires sans contact (NFC).

Les clients ne sont pas informés de manière satisfaisante de la mise en place de ce dispositif et ont du mal à faire désactiver la fonction sans contact activée par défaut.

La CNIL s'est rapprochée des établissements financiers qui ont depuis amélioré l'information auprès de leurs clients, diminué le nombre de données disponibles sur la carte et facilité la désactivation du sans contact.

Libertés publiques (5% des plaintes)

Quels motifs ? Demandes d'anonymisation ou d'opposition à la diffusion en ligne d'articles de presse (132 plaines en 2015),

Dans le cadre des élections régionales : e-mailing politique ou appels effectués par des automates, détournements de fichiers (utilisation de fichiers d'associations ou de la collectivité pour de l'e-mailing politique).

Les réactions des personnes démarchées dans le cadre d'élections sont très vives, surtout lorsqu'il s'agit d'un appel téléphonique provenant d'un candidat dont elles ne partagent pas les idées. Ces personnes s'interrogent sur l'origine des données.

C'est nouveau ! A suivre ...

Les plaintes reçues permettent à la CNIL d'identifier de nouvelles tendances telles que : la géolocalisation des salariés non plus via leur véhicule mais via des bracelets connectés ou leur smartphone, de nouvelles techniques de vidéosurveillance des salariés via une application sur smartphones ou une webcam.

Des municipalités invitent leurs administrés à leur envoyer des photos ou du son pour signaler des incivilités (déjections canines, stationnement abusif, tapage nocturne, dépôt d'ordure, affichage sauvage, etc).

Gros plan sur le droit au déréférencement

Face à la pratique généralisée consistant à rechercher des informations sur une personne via les moteurs de recherche, contrôler sa réputation sur internet constitue une préoccupation grandissante des citoyens.

Deux démarches sont possibles :

- soit, s'adresser au site qui est à l'origine de la diffusion de l'information, c'est-à-dire exercer son droit d'opposition auprès du site ;
- soit effectuer une demande de déréférencement, c'est à dire demander aux moteurs de recherche la suppression de certains liens de la liste des résultats affichés par le moteur de recherche (ce droit a été reconnu par une décision de la cour de justice de l'union européenne - CJUE - du 13 mai 2014).

En 2015, la CNIL a reçu près de 450 plaintes de personnes physiques qui se sont vu opposer un refus à une demande de déréférencement effectuée auprès d'un moteur de recherche.

Ces personnes demandent principalement la suppression de liens (URLs) diffusés sur des annuaires, des blogs, pages web perso, des sites marchands, des sites de presse et des réseaux sociaux. Au total, **plus de 700 plaintes ont été reçues par la CNIL depuis juin 2014 en matière de déréférencement**.

La CNIL est intervenue auprès des moteurs de recherche pour leur demander un déréférencement dans 30% des dossiers traités. A cet égard, de nombreuses demandes de déréférencement adressées à la CNIL n'entrent pas dans le cadre de la décision de la CJUE (les données concernent des personnes morales et non des personnes physiques ou la demande porte sur le respect des droits d'auteur). Les demandes de la CNIL ont été suivies d'effets dans 76% des cas, le solde étant, soit encore en cours de traitement, soit ayant fait l'objet de nouveaux échanges entre la CNIL et les moteurs de recherche.

> ***Monsieur T.*** *demande le déréférencement de deux liens renvoyant vers la fiche descriptive de son brevet déposé en 2006, et diffusant ses prénom, nom ainsi que son adresse personnelle. Il invoque à l'appui de sa demande qu'il ne paye plus ses annuités et que le brevet est désormais caduc. En outre il ne souhaite pas que ses coordonnées personnelles soient diffusées en ligne. Le déréférencement a été demandé au motif que les informations sont inexactes, pas à jour, et la publication de ces informations ne répond pas à une obligation légale. La diffusion des coordonnées personnelles de Monsieur T. comporte un risque d'atteinte à sa vie privée. En conséquence, l'inclusion de ces informations dans les résultats du moteur de recherche Google n'est pas pertinente au regard de l'intérêt du public à en connaître.*

> ***Monsieur B.*** *souhaitait faire déréférencer un lien renvoyant vers une interview qu'il a donnée en 2015 dans le cadre de son activité professionnelle. Après analyse, l'information est apparue exacte, récente et relative à la vie professionnelle de Monsieur B. En outre, le contenu a été publié à des fins journalistiques, la personne ne pouvait ainsi ignorer que ces propos seraient diffusés. Dès lors, la CNIL a considéré que l'inclusion de cet article dans les résultats des moteurs de recherche restait pertinente.*

2. Des demandes de droit d'accès indirect toujours en hausse

En 2015, la CNIL a reçu **5890 demandes de droit d'accès indirect, soit une augmentation de 12% par rapport à 2014**. Ces demandes reçues représentent un total de 8377 vérifications à mener concernant par ordre d'importance : le fichier FICOBA de l'administration fiscale, le fichier TAJ des antécédents judicaires de la police et de la gendarmerie et les fichiers de renseignement.

“ ***Monsieur R., 34 ans**, dirigeant d'une société de surveillance et de gardiennage, titulaire depuis 2005 de l'agrément préfectoral requis a adressé à la CNIL une demande de droit d'accès indirect après avoir reçu du CNAPS (Conseil National des Activités Privées de Sécurité), désormais compétent en ce domaine, un courrier faisant état d'infractions de nature à faire obstacle au renouvellement de son agrément et, de fait, au maintien de son activité. Au terme des vérifications menées par la CNIL, les deux faits concernés ont été supprimés, en accord avec le procureur de la République, car il avait bénéficié de suites judiciaires favorables (classement sans suite pour insuffisance de charges).*

“ ***La mère de Monsieur D., mineur,** a souhaité alerter la CNIL sur la situation de son fils après son interpellation et placement en garde à vue alors qu'il était passager d'une moto, acquise récemment par le père de l'un de ses amis. Au terme des vérifications, l'enregistrement dont il faisait l'objet pour « recel de bien provenant d'un vol » a été supprimé car il n'était nullement mis en cause. En l'occurrence, le père de son ami avait acheté, à son insu, une moto volée.*

“ ***Madame H.** 27 ans, confrontée à des difficultés d'exercice de sa profession dans le domaine de la restauration qui l'amène régulièrement à intervenir en zones aéroportuaires, a souhaité mettre en œuvre son droit d'accès indirect. En l'occurrence, elle était mise en cause pour une affaire de « vol en réunion » pour s'être emparée, pour répondre à un défi d'intégration lors de ses études, de décorations de Noël sur une place publique. Cette affaire a été requalifiée en « vol simple » et immédiatement supprimée en raison de l'expiration du délai de conservation associé (5 ans).*

Les effets des attentats et de l'état d'urgence sur les demandes de droit d'accès indirect

La CNIL a reçu ces derniers mois près de 155 demandes de droit d'accès indirect liées au contexte de l'état d'urgence (perquisitions administratives, assignations à résidence, retrait de badges aéroportuaires ou de cartes professionnelles). Ces demandes portent notamment sur le Traitement d'Antécédents Judiciaires (TAJ) et les fichiers des services de renseignement du ministère de l'intérieur.

Le renforcement des effectifs au sein des forces de sécurité depuis les attentats du 13 novembre 2015 (création annoncée de 8500 postes dans la police, la gendarmerie, la douane et l'administration pénitentiaire) et l'accroissement du nombre de candidats à ces fonctions contribuent également à accroître le nombre demandes de droit d'accès indirect au fichier TAJ, consulté dans le cadre des enquêtes administratives menées pour l'accès à ce type d'emplois.

Au premier trimestre 2016, la CNIL a déjà constaté une augmentation de 18 % des demandes d'accès au fichier TAJ par rapport au premier trimestre 2015.

3. Une action répressive en hausse, notamment grâce aux contrôles en ligne

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 sanctions par la CNIL permet de sanctionner des organismes qui persistent dans des comportements répréhensibles, et constitue donc un instrument de dissuasion important.

L'année 2015 se caractérise par une forte augmentation du nombre de mises en demeure adoptées par la Présidente de la CNIL. En effet, **93 mises en demeure** ont été adoptées contre 62 en 2014. Cette hausse s'explique par la possibilité de réaliser des contrôles en ligne et par le fait que des contrôles s'inscrivaient dans des thématiques ayant révélé de nombreux manquements : cookies (40 mise en demeure), sites de rencontre (8 mise en demeure), services dématérialisés d'actes d'été civil (20 mise en demeure).

10 sanctions ont été prononcées par la formation restreinte, dont 3 sanctions pécuniaires.

La CNIL a réalisé **501 contrôles** en 2015, dont **87 contrôles portant sur des dispositifs vidéo**.

155 contrôles en ligne ont été réalisés sur de nombreuses thématiques telles que :

- les sites de tirage de photos ou de créations d'albums photo,
- de conseil de santé en ligne,
- de crédit en ligne,
- d'adhésion à des partis politiques,
- de demande d'actes d'état civil,

28 contrôles en ligne réalisés en 2015 ont conduit à une mise en demeure en 2015, 2 procédures de sanction ont été engagées et toujours en cours.

4. Les données personnelles, au cœur de l'actualité législative en France et en Europe

En 2015, l'actualité législative s'est fortement structurée autour de la protection des données personnelles et des libertés numériques, comme en témoignent les 122 avis que la CNIL a rendus.

Le renseignement et la lutte contre le terrorisme

La CNIL s'est prononcée sur **14 projets de dispositions législatives ou réglementaires directement relatives au traitement de données à des fins de renseignement ou de lutte contre le terrorisme**. Des dispositifs d'une nouvelle ampleur, en termes de volume de données traitées comme de modalités de collecte, ont été légalisés. De nouveaux fichiers ont été créés, certains fichiers existants ont été modifiés, de nouvelles techniques d'enquête et de recueil de données ont été utilisées pour surveiller et contrôler des communications.

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 ». Alexandre Linden, la personnalité qualifiée désignée par les membres de la CNIL, présentera un rapport dédié à cette activité.

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 pas été suivie d'effet.

Le projet de loi pour une République numérique conforte et renforce l'action de la CNIL

La CNIL s'est prononcée, lors de la séance plénière du 19 novembre 2015, sur l'avant projet de loi pour une « République numérique », dans sa version alors envisagée par le Gouvernement. Le projet de texte adopté en première lecture à l'Assemblée nationale comporte de nombreuses modifications, qui tiennent notamment compte de l'avis de la CNIL. La CNIL a insisté dans son avis sur la nécessaire cohérence avec les autres textes en préparation et particulièrement le règlement européen qui sera d'application directe en 2018.

Le projet de loi tend également à **renforcer les pouvoirs de la CNIL et à conforter ainsi son engagement dans la régulation du numérique** et son activité d'accompagnement des particuliers, des entreprises et des administrations.

La loi du 26 janvier 2016 sur la modernisation de notre système de santé

La CNIL a été sollicitée sur le projet de loi et a participé à de nombreuses auditions.

En Europe

Au plan international, la finalisation du projet de règlement européen sur les données personnelles qui a fait l'objet d'un accord à l'issue du trilogue en décembre 2015 et l'arrêt de la CJUE d'octobre 2015 invalidant le *Safe Harbor* ont très fortement mobilisé la CNIL. La Présidente de la CNIL a été réélue à la présidence du G29 (groupe des CNIL européennes) en février 2016, pour un mandat de deux ans.

Les enjeux pour 2016 (1) : assurer la mise en œuvre du règlement européen

La fin de l'année 2015 marque un tournant majeur dans la protection des données, avec l'adoption du règlement européen en décembre. Il devrait être voté avant l'été 2016 et être applicable au premier semestre 2018.

L'adoption du règlement européen sur la protection des données personnelles en décembre 2015 constitue l'aboutissement de quatre années de travail et de négociations intenses et marque un tournant majeur dans la régulation des données personnelles. En effet, il s'agit de passer d'un cadre national à un cadre prioritairement européen. Il faudra donc que la CNIL intègre, dans l'ensemble de son fonctionnement, la dimension européenne de la régulation.

Cette adoption signifie aussi le début d'un compte à rebours qui va durer deux ans, jusqu'à la mise en œuvre effective du règlement en 2018. La CNIL devra adapter ses procédures, ses outils et le rôle de la formation plénière mais aussi suivre de près la refonte de la loi Informatique et Libertés qui s'appliquera encore pour les traitements des autorités publiques et pour certains traitements de santé.

L'exercice est complexe puisqu'il s'agit de changer complètement de logiciel tout en continuant d'ici à 2018 de veiller à la bonne application du cadre juridique actuel. Pour autant, cette période de transition constitue une opportunité pour la CNIL, afin de lui permettre de mettre à jour ses doctrines, ses pratiques, et ses outils.

Le texte tel qu'adopté en décembre prévoit, notamment :

- **Pour le citoyen**, un renforcement des droits existants, notamment en lui permettant de disposer d'informations complémentaires sur le traitement de ses données mais également de les obtenir sous une forme claire, accessible et compréhensible. Le droit à l'oubli est conforté et un nouveau droit, le droit à la portabilité, est prévu, rendant ainsi plus effective la maîtrise de ses données par la personne. Les mineurs font également l'objet d'une protection particulière.
- **Pour les entreprises,** une simplification des formalités, la possibilité d'un interlocuteur unique pour toutes les autorités de protection des données européennes et d'une mise à disposition d'une boite à outils de conformité dont certains seront nouveaux (ex : code de conduite, certification). Ces outils pourront être modulés en fonction du risque sur les droits et libertés des personnes. (ex : tenue d'un registre, consultation des autorités de protection, notification des failles de sécurité).
- **Pour les autorités de protection**, une affirmation de leurs compétences dès lors qu'il existe un établissement sur le territoire de l'Union ou que leurs citoyens sont affectés par le traitement, mais également un renforcement de leurs pouvoirs, notamment répressifs avec la possibilité de prononcer des sanctions administratives pouvant aller jusqu'à 4% du chiffre d'affaire mondial de l'entreprise concernée. Surtout, les « CNIL » européennes pourront désormais prononcer des décisions

conjointes, aussi bien pour constater la conformité d'un organisme que pour prononcer une sanction. Cette intégration européenne renforcera ainsi la protection des personnes et la sécurité juridique pour les entreprises.

- **Une nouvelle architecture de coopération entre les autorités de protection avec un nouvel organe européen** : le Comité Européen de la Protection des Données (CEPD) en charge d'arbitrer les différends entre les autorités et également d'élaborer une doctrine « européenne ». Cette entité, qui prend la suite du G29, verra son indépendance renforcée et pourra rendre des avis contraignants, notamment dans le cadre de procédures de sanctions.

La Directive

L'année 2015 a aussi été marquée par l'aboutissement de la phase de négociations ou «trilogue» entre les trois institutions européennes (la Commission, le Parlement et le Conseil de l'UE) en décembre 2015 sur le texte de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

La directive doit encore être formellement adoptée par les institutions européennes mais l'accord sur le texte intervient quasi-simultanément avec celui sur le projet de règlement sur la protection des données et répond à la demande des autorités de protection des données de traiter ces deux textes comme un « paquet ».

Les enjeux de 2016 (2) : accompagner et faciliter la transition numérique des acteurs privés comme publics

Bien que déjà engagé ces dernières années, ce tournant s'accentuera en 2016, notamment parce que la loi pour une République numérique confère à la CNIL de nouvelles missions. La CNIL doit accompagner le développement de la confiance dans les services numériques dans une logique de conformité et de respect des droits des personnes.

Alors que la CNIL s'est fortement engagée ces dernières années sur l'accompagnement du secteur privé, le secteur public a également entamé sa transition numérique. L'enjeu est considérable à la fois au regard du volume des données traitées, de l'ouverture croissante des données publiques, renforcé par le projet de loi sur la République numérique, et du potentiel développement de traitements de « big data » publics.

Qu'est-ce que le projet de loi pour une République numérique va changer pour la CNIL ?

L'ouverture des données publiques devient la règle

Le projet de loi ne remet pas en cause l'équilibre entre transparence administrative et protection de la vie privée et des données personnelles. En effet, les critères de communicabilité n'ont pas changé, et la publication – donc la réutilisation – est subordonnée au caractère librement communicable du document.

Pour autant, en passant d'une logique de la demande à une logique de l'offre, le projet de loi vise clairement à démultiplier le nombre de fichiers, y compris contenant des données personnelles, mis en open data. Ceci va donc se traduire par un accroissement sensible des demandes de conseil d'une part, de formalités d'autre part, et de réclamations individuelles, enfin, liées à l'open data pour la CNIL. En effet, alors que la législation sur la transparence de la donnée publique avait été conçue autour de la problématique de la communicabilité, l'ouverture massive des données, notamment personnelles, pose la question de leur usage *a posteriori*. Or, en la matière, toute réutilisation de données personnelles est soumise au « droit commun » informatique et libertés, ce qui implique une implication croissante de la CNIL dans l'accompagnement de l'open data.

Dans ce contexte, et afin de promouvoir une ouverture des données publiques respectueuse de la vie privée, la CNIL a décidé de lancer une concertation pour élaborer un « pack de conformité » en matière de données publiques. Elle a ainsi sollicité la Commission d'accès aux documents administratifs (CADA) et la mission Etalab du SGMAP pour définir, avec les administrations concernées, les bonnes pratiques en la matière.

Le rôle de la CNIL est conforté en matière d'anonymisation

Dans la version du texte issue de l'Assemblée nationale, l'article 30 prévoit que la CNIL pourra certifier des méthodologies d'anonymisation dans la perspective de leur mise en ligne et de leur réutilisation – comme elle pourra d'ailleurs le faire pour les processus d'anonymisation de traitements du secteur privé. L'anonymisation des bases de données est en effet essentielle à leur ouverture ou à leur partage : elle permet en effet de prémunir les

personnes de tout risque de réidentification, et les acteurs (administrations émettrices de données, réutilisateurs, entreprises privées qui réalisent des recherches notamment statistiques), de toute mise en cause de leur responsabilité en la matière. L'homologation de méthodologies d'anonymisation par la CNIL sera ainsi un gage de protection des personnes et de sécurité juridique pour les acteurs.

Les missions de la CNIL sont élargies ou clarifiées sur plusieurs points (art. 29 du PJL) :

Le champ de la saisine pour avis de la CNIL sur les projets de lois et de décrets est élargi et clarifié, puisque, outre les dispositions relatives à la protection des données à caractère personnel, sont ajoutés les dispositions relatives au traitement de telles données.

L'avis de la CNIL sur un projet de loi est désormais rendu public.

Deux nouvelles missions seraient confiées à la CNIL

Conduire une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques, en impliquant des personnalités qualifiées et en organisant des débats publics.

Régulateur des données personnelles, et à ce titre au cœur du numérique, la CNIL incarne, y compris par sa composition, la nécessité de prendre en compte la pluralité des regards et les problématiques éthiques en matière de numérique. Toutefois, il ne lui appartient pas de déterminer des positions éthiques en la matière. Son rôle serait plutôt celui d'animatrice et de facilitatrice de ce débat, impliquant tous les acteurs concernés (chercheurs, entrepreneurs, administration, société civile). Elle compte faire en sorte que cette réflexion puisse être l'occasion d'une appropriation par les citoyens des débats liés aux enjeux éthiques du numérique.

Promouvoir, dans le cadre de ses missions, l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

Enfin, les pouvoirs de sanction de la CNIL sont considérablement renforcés, par anticipation sur le règlement européen qui prévoit des sanctions pouvant atteindre 4% du chiffre d'affaires mondial.

Quel accompagnement des acteurs privés et publics ?

Le respect de la loi « informatique et libertés » implique une mise en conformité dynamique. Il ne s'agit pas en effet seulement de démarches administratives – dont une bonne partie va disparaître avec le règlement européen –. Il s'agit de respecter, pendant toute la vie d'un traitement de données, les principes, droits et obligations posées par la loi, notamment les droits des personnes, tout en les déclinant de manière opérationnelle. Les avantages de la conformité pour les professionnels sont en outre nombreux : assurer une sécurité juridique aux acteurs ; tirer parti du droit pour en faire un facteur de succès ; accroître le capital de confiance vis-à-vis des interlocuteurs. La CNIL a développé une gamme d'outils complémentaires permettant d'accompagner aux mieux les différents métiers et secteurs d'activité.

Les packs de conformité

Depuis deux ans, la CNIL a lancé un nouvel outil : les « packs de conformité ». Ces packs, élaborés en concertation étroite avec les acteurs d'un secteur, permettent de promouvoir auprès de ceux-ci des bonnes pratiques, de décliner les obligations légales de manière opérationnelle et de simplifier les formalités administratives. Il s'agit donc d'un outil ancré dans la réalité des métiers. 2015 a vu le lancement des packs du secteur bancaire et du secteur social et médico-social. Par ailleurs, l'accompagnement se poursuit sur les packs adoptés en 2014 : compteurs communicants, secteur des assurances, logement social.

En 2016, deux nouveaux packs seront lancés, respectivement dédiés à l'open data pour le secteur public et au véhicules connectés, dans le droit fil des réflexions engagées dés 2014.

Sur la base du dialogue établi avec les professionnels de l'assurance s'est formé un Club de conformité qui permet d'assurer un dialogue suivi avec les entreprises. Ce Club permet ainsi d'aborder les questions nouvelles qui se posent notamment quant à l'utilisation des réseaux sociaux pour la recherche des bénéficiaires des contrats d'assurance vie en déshérence ou encore la mutualisation des fraudes en matière de sinistres automobiles.

Les labels

80 labels ont été délivrés par la CNIL.

Créé il y a un an, le label « Gouvernance » est un gage de sécurité juridique et informatique et un instrument de valorisation. Il constitue l'une des principales applications du principe d'*accountability* (principe de responsabilité) prévu par le projet de règlement européen. Ce texte encourage d'ailleurs, de façon très explicite, la création et le développement des labels, certifications, et marques de protection des données, notamment à l'échelle de l'Union Européenne. Dans la perspective du règlement européen, de nouvelles formes de labellisation pourraient donc être envisagées.

Des outils d'autoévaluation

La responsabilisation accrue des acteurs dans le cadre du règlement implique en effet, en l'absence de formalités préalables, des modes d'intervention et d'évaluation innovants. La CNIL prévoit donc de mettre à disposition des questionnaires d'autoévaluation, notamment à destination des PME/PMI.

Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement ?

La question de l'équilibre entre protection des données personnelles, innovation technologique et surveillance est au centre de nombreuses préoccupations, tout particulièrement depuis les révélations d'Edward Snowden sur la surveillance de masse. Elle se pose aujourd'hui avec acuité suite aux demandes faites par le FBI auprès de la société APPLE, afin de pouvoir contourner les solutions de chiffrement à la main des utilisateurs, c'est-à-dire dont ils sont les seuls à détenir la clé de déchiffrement.

Le chiffrement : élément de la sécurité du patrimoine informationnel

Internet est un réseau public, ouvert, devenu le support de la majorité de nos communications. Dans un contexte de numérisation croissante de nos sociétés et d'accroissement exponentiel des cybermenaces, le chiffrement est un élément vital de notre sécurité. Il contribue aussi à la robustesse de notre économie numérique et de ses particules élémentaires que sont les données à caractère personnel, dont la protection est garantie par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

Il est dès lors primordial de :

- protéger les personnes et leur vie privée afin de garantir leurs droits fondamentaux ;
- protéger les systèmes d'information des entreprises et des États, car les atteintes à ces systèmes peuvent occasionner de graves préjudices économiques, politiques, ou en termes de sécurité publique ;
- promouvoir l'essor de l'économie du numérique, au travers des notions de confiance et de sécurité, pour stimuler l'innovation et la croissance ;
- maintenir la compétitivité des acteurs nationaux du domaine de la cybersécurité pour soutenir l'économie.

La cybersécurité est un vecteur de confiance et d'innovation. Protéger les données personnelles dans l'univers numérique, à l'aide notamment du chiffrement, c'est aussi protéger un droit fondamental et, au-delà, l'exercice des libertés individuelles dans cet univers.

Les accès aux données dans le cadre des procédures judiciaires

En France, il existe d'ores et déjà une réglementation relative aux moyens de cryptologie et un cadre légal bien établi concernant différents types d'accès aux données informatiques dans le cadre de procédures judiciaires.

Ce cadre autorise notamment les réquisitions numériques, l'accès aux données de connexion, les interceptions de correspondances, les enregistrements audio-visuels, la captation de données informatiques affichées à l'écran ou introduites au clavier, ou encore le recours à des experts techniques dans le cas de données chiffrées. Ces dispositions sont applicables sans préjudice de la possibilité, pour les autorités judiciaires, de s'appuyer sur les moyens techniques dont disposent les organismes de police judiciaire.

L'obligation, pour les personnes, de coopérer avec les autorités

En outre, le droit pénal contient des incitations concernant la remise des clés de déchiffrement, s'agissant des personnes mises en cause ou des tiers tels que les prestataires de services de cryptographie s'ils ont connaissance de la convention secrète de déchiffrement.

En effet, le droit permet d'exiger de toute personne la communication de toute donnée, informatique ou non, quel que soit son support (logiciel, fichier, traitement, cloud, etc.). Il en est de même pour la fourniture des clés de déchiffrement ou des informations déchiffrées aux autorités judiciaires, par les personnes concernées ou par des tiers, et des peines renforcées sont prévues pour les personnes refusant de les remettre.

Toutefois ces dispositions ne peuvent pas conduire à obliger les personnes mises en cause à fournir les informations utiles à l'enquête. En effet, le droit de ne pas s'auto-incriminer est un droit fondamental qui trouve son origine dans la Convention européenne des droits de l'homme et dans la jurisprudence de la Cour européenne.

Les limites de l'usage de portes dérobées

L'actualité récente a conduit à un débat sur la pertinence de l'introduction, par le droit national, de portes dérobées (*backdoors*) ou d'une clé maitre permettant *in fine* d'accéder à des données contenues dans un système protégé par une solution de chiffrement présentée comme à la main de l'utilisateur. Un tel dispositif soulèverait de nombreuses questions :

- il créerait un risque collectif tendant à affaiblir le niveau de sécurité des personnes face à l'ampleur du phénomène cybercriminel, alors qu'il n'empêcherait pas, techniquement, des personnes malveillantes de continuer à utiliser des solutions de chiffrement à titre individuel pour protéger la confidentialité de leurs communications et de leurs données stockées ;
- il serait vraisemblablement peu robuste dans le temps, face aux attaques des États ou du crime organisé, d'autant plus qu'il serait nécessaire d'échanger entre autorités le secret ou les clés ;
- il serait très complexe à mettre en œuvre, de manière sûre, alors que les applications sont globalisées et mondialisées.

Les solutions de chiffrement robustes, sous la maîtrise complète de l'utilisateur, contribuent à l'équilibre et à la sécurité de l'écosystème numérique. L'introduction de portes dérobées ou de clés maîtres conduirait à affaiblir la sécurité des solutions techniques aujourd'hui déployées, ce qui serait préjudiciable au patrimoine informationnel des entreprises, à la stabilité de l'écosystème de l'économie du numérique et à la protection des libertés des personnes.

En conséquence, la CNIL considère que

- le chiffrement contribue à la résilience de nos sociétés numériques et de notre patrimoine informationnel ;
- dans le cadre des procédures judiciaires, il existe déjà de nombreuses voies permettant aux autorités d'accéder et d'analyser les contenus intéressant l'enquête ou utiles à la manifestation de la vérité ;
- les personnes mises en cause et les tiers ont obligation de coopérer avec les autorités ;
- la mise en place de portes dérobées ou de clés maîtres fragiliserait l'avenir de l'écosystème du numérique.