CONFERENCE DE PRESSE

10 avril 2018

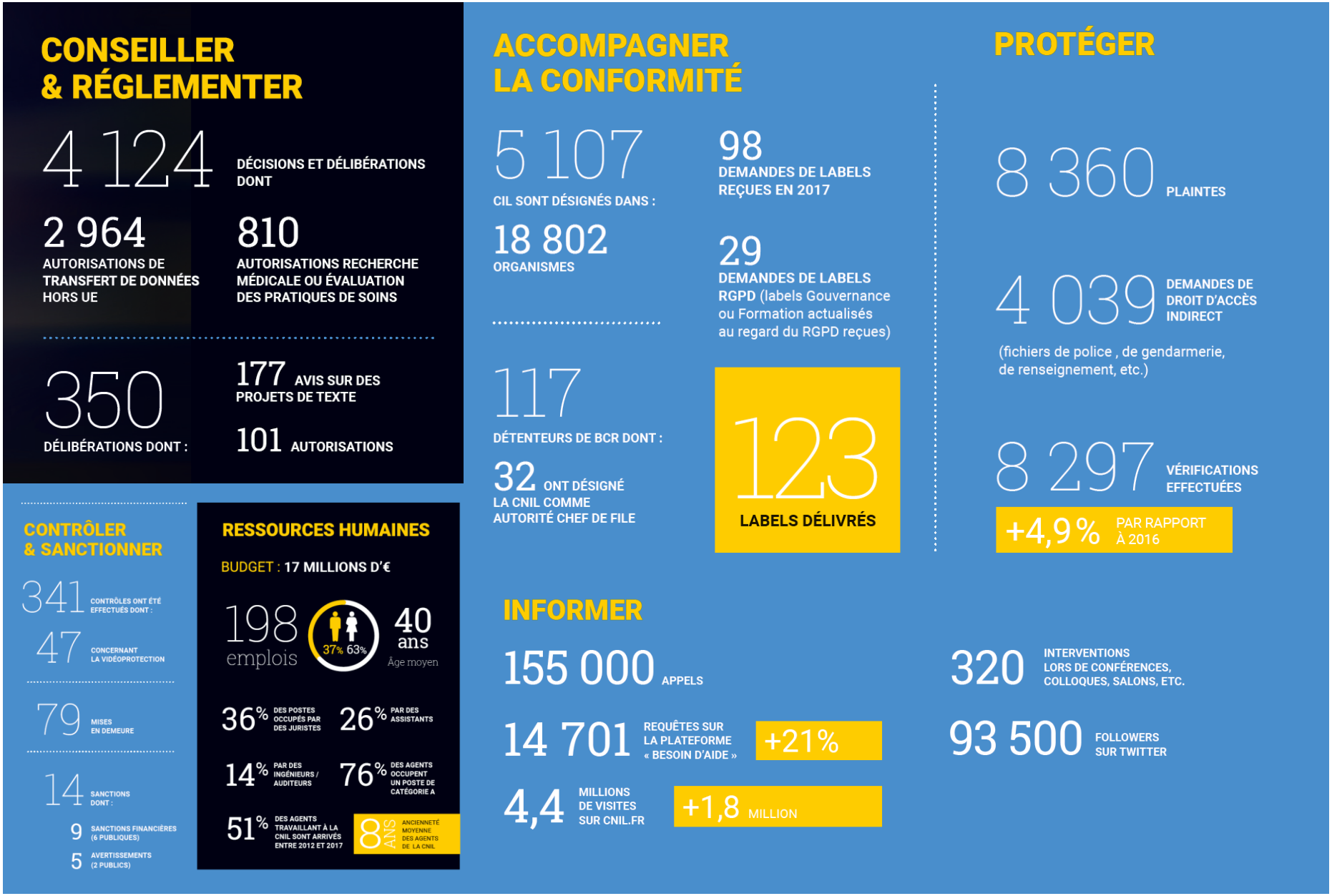
Présentation du 38ème

Rapport d'activité 2017

et des enjeux 2018

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Chiffres clés de l'année 2017



Temps forts 2017

Janvier 2017

09/01
Caméras-piétons utilisées par les forces de l'ordre : l'avis de la CNIL

27/01
Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers

Février

17/02
Règlement européen : une nouvelle consultation sur le profilage, le consentement et la notification de violations

Avril

18/04
Création du système national des données de santé (SNDS) : quels usages avec quelles garanties ?

Mai

16/05
Facebook sanctionné pour de nombreux manquements à la loi Informatique et Libertés

Juin

29/06
Windows 10 : clôture de la procédure de mise en demeure à l'encontre de Microsoft corporation

Juillet

11/07
Observations de la CNIL sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme

20/07
Lancement de la vidéo du YouTuber Kevin Tran de sensibilisation aux usages responsables d'Internet et à la protection des données auprès des jeunes en partenariat avec MGEN

27/07
Hertz France : sanction pécuniaire pour violation de données personnelles

Septembre

13/09
Les données génétiques : premier titre de la nouvelle collection point CNIL

28/09
Admission post-bac (APB) : mise en demeure pour plusieurs manquements

Novembre

22/11
RGPD : un logiciel pour réaliser son analyse d'impact sur la protection des données (PIA)

Décembre

04/12
Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité

13/12
La CNIL publie son avis sur le projet de loi relatif à la protection des données personnelles

15/12
Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle

18/12
Transmission de données de Whatsapp à Facebook : mise en demeure publique pour absence de base légale

Bilan 2017

L' « effet RGPD » : une année de préparation active de la transition, doublée d'une très forte attente des particuliers et des professionnels

L'année 2017 se caractérise par une préparation active de la transition vers le futur cadre juridique européen. La CNIL a participé aux réflexions sur le projet de loi relatif à la protection des données et proposé de nombreux outils pratiques pour permettre aux professionnels de s'approprier ce nouveau règlement. Une très forte demande s'est exprimée en ce sens. Tout en s'adaptant à ce nouveau contexte, la CNIL a dû aussi faire face à l'afflux des demandes des particuliers avec un nombre record de plaintes.

BILAN D'ACTIVITE 2017

1. La CNIL au service des citoyens

Un nombre record de plaintes et des citoyens de plus en plus concernés

En 2017, la CNIL a reçu 8 360 plaintes, ce qui représente un record de plaintes (7900 en 2015 / 7703 en 2016). En règle générale, la CNIL constate **une préoccupation croissante des personnes** quant à l'utilisation qui est faite de leurs données. Elles posent de nombreuses questions sur la collecte de données personnelles via des applications ou des sites, sur la pertinence des données qui leurs sont demandées.

- **27% des plaintes concernent la diffusion de données personnelles sur Internet** (site, blog, réseau social) et principalement leur suppression ou leur rectification, ce qui demeure une démarche difficile. Dans la majorité des cas, les personnes s'adressent à la CNIL car elles n'ont pas obtenu de réponse de la part de l'organisme ou de la personne à l'origine de la diffusion de l'information, qu'il n'existe pas de procédure en ligne, qu'elles ont reçu un refus non motivé de la part de l'organisme ou enfin que l'information erronée a été dupliquée à de nombreuses reprises. Dans ce dernier cas de figure, la personne a plutôt intérêt à supprimer l'information à la source. La CNIL diffuse de nombreux conseils pratiques pour sensibiliser les personnes à la maîtrise de leurs données personnelles en ligne : réglages des paramètres de confidentialité, minimisation des données transmises, recours à des pseudonymes, ego-surfing pour vérifier les informations en ligne, fermetures des comptes non actifs, etc.

La CNIL a reçu **335 demandes de déréférencement**, à la suite de refus de la part des moteurs de recherche. Ce sont donc 1335 demandes reçues depuis 2014. Pour apprécier le bienfondé de ces demandes, la CNIL met en balance les droits fondamentaux de la personne concernée avec l'intérêt du public à avoir accès au contenu à partir des nom et prénom de cette personne. Elle prend notamment en compte le caractère récent du contenu en cause, son caractère exact, journalistique ou légal et le rôle joué par la personne dans la vie publique. Ces demandes ont été suivies d'effets par les moteurs de recherche dans 75% des cas. Le Conseil d'Etat a saisi la cour de justice de l'UE sur la possibilité pour les moteurs de recherche de traiter des données sensibles et des données d'infraction ce qui entraine une suspension du traitement de certaines plaintes déréférencement concernant ce type de données.

- **25% des plaintes concernent le secteur marketing/commerce** et principalement la prospection par courriel, téléphone ou courrier. Afin de limiter la prospection commerciale non sollicitée, la CNIL dispense de nombreux conseils pratiques et notamment la création d'adresses électroniques dédiées aux usages : achats en ligne, réseaux sociaux, jeux, relations amicales, échanges

professionnels. Pour agir plus efficacement contre le spam, la CNIL a changé en 2017 sas méthodes d'instruction et renforcé sa collaboration avec l'association Signal spam.

- **Les autres secteurs concernés par les plaintes sont :**

  - les ressources humaines (16%) : vidéosurveillance excessive, géolocalisation, refus de communication du dossier professionnel) ; Ces demandes proviennent de salariés, de syndicats ou d'inspecteurs du travail.
  - la banque et le crédit (12%) : absence de levée de l'inscription au Fichier national des Incidents de remboursement des Crédits aux Particuliers ou fichier central des chèques et cartes bancaires ;
  - le secteur santé et social (8%) : difficultés à accéder au dossier médical ou social, Pôle emploi.

Les tendances émergentes

Les plaintes reçues permettent à la CNIL d'identifier de nouvelles tendances :

- **Les objets connectés soulèvent des enjeux croissants** : compteurs communicants (plaintes, notamment de mairies, qui pointent un manque d'information sur l'installation des compteurs, les données collectées, leurs destinataires, les enceintes connectées ou assistants vocaux) ;
- **La réutilisation par des sites internet des données des auto-entrepreneurs publiées sur les annuaires professionnels :** des sites internet réutilisent les nom, prénom et adresses personnelles des auto-entrepreneurs à partir des informations disponibles sur Infogreffe ;
- **Les dispositifs de lecture automatisée de plaque d'immatriculation (« LAPI ») en lien avec la dépénalisation du stationnement payant** : absence d'information, caractère intrusif du dispositif, absence d'information sur la durée de conservation des données, sur les destinataires ;
- **Le manque de formation des personnels communaux chargés de la prise d'empreintes digitales de demandeurs de titres d'identité (« TES »)** qui ne sont pas informés de la possibilité de refuser la numérisation et l'enregistrement des empreintes et de la procédure prévue dans ce cas – le ministère a diffusé une circulaire explicative en ce sens ;
- **Le son couplé à la vidéoprotection** : cette tendance attentatoire à la vie privée des personnes s'inscrit dans un phénomène constant de déploiement de dispositifs permettant de surveiller les employés et leur activité sur le lieu de travail. La captation et l'enregistrement des conversations des employés s'effectuent souvent à leur insu (via des smartphones) et sont, a priori, disproportionnés ;
- **L'accès aux messageries professionnelles des salariés absents ou ayant quitté l'entreprise** : la messagerie doit être supprimée après le départ d'un salarié, un message indiquant les coordonnées d'un nouvel interlocuteur peut être mise en place.

L'offre grand public de la CNIL pour une meilleur maîtrise de sa vie privée

Le site de la CNIL a reçu **1,8 million de visites supplémentaires en 2017, soit 4,4 millions de visites**. (+59% de visiteurs).
Le service d'aide en ligne Besoin d'Aide a reçu 14 701 demandes (+21% par rapport à 2016) et dispose de plus de 500 questions/réponses.

Sur son site, la CNIL propose de nombreuses fiches pratiques et conseils à destination des particuliers :

- Les conseils pour un bon mot de passe est l'article le plus lu du site ;
- Enceintes connectées et assistants vocaux ;
- Jouets connectés ;
- Les données collectées et transmises par les compteurs communicants (Gaspar et Linky) ;
- Utilisation d'un WIFI public ;
- Prospection politique par automate d'appels ;

La vidéo « Protéger sa vie privée en 6 étapes » par Le Rire Jaune, en partenariat avec la MGEN a atteint plus de 4 millions de vues sur YouTube.

Les 4 comptes Twitter de la CNIL comptent 100 000 followers, le compte Facebook 29 000 fans et le compte LinkedIn 19 000 abonnés.

Le site Educ Num a également eu 100 000 visiteurs en 2017. Et une nouvelle édition des Incollables « Ta vie privée c'est secret ! », avec les Editions PlayBac, a connu un grand succès auprès des jeunes.
Les demandes d'informations et de conseils reçues par la CNIL émanant de particuliers portent principalement sur :

- la surveillance au travail (vidéosurveillance, géolocalisation, cybersurveillance, etc.) ;
- la suppression d'informations sur internet ;
- la réception intempestive de publicités (par sms, téléphone, courrier électronique).

Demandes de droit d'accès indirect : un léger infléchissement du nombre de demandes, sans doute provisoire, mais des vérifications en hausse

En 2017, la CNIL a reçu **4 039 demandes de droit d'accès indirect qui ont donné lieu à** plus de 8000 vérifications. Ces demandes reçues représentent un total de 7170 vérifications à mener concernant par ordre d'importance : le fichier TAJ des antécédents judiciaires de la police et de la gendarmerie, le fichier FICOBA de l'administration fiscale, et les fichiers de renseignement. **49 % des demandes reçues ont porté sur le fichier TAJ (1979 demandes)**.

Cette évolution s'explique par :

- La mise en place depuis 2016 d'un droit d'accès direct des héritiers à Ficoba ;
- La possibilité pour les services de police français de procéder, sous certaines conditions, à des échanges d'informations sur les données de ce fichier avec leurs homologues étrangers dans le cadre d'enquêtes administratives. Cette procédure évite aux personnes de devoir exercer leur droit d'accès indirect, puisque les données sont directement échangées entre les autorités compétentes. La CNIL avait reçu en 2016 400 demandes de ressortissants français souhaitant travailler sur le territoire suisse.
- Le nombre plus restreint de mesures dans le cadre des prolongations successives de l'état d'urgence (assignations à résidence, perquisitions administratives).

Mais, compte tenu de l'élargissement constant du périmètre des enquêtes administratives et du nombre croissant de fichiers consultés, la CNIL prévoit pour l'année 2018 une augmentation des demandes de droit d'accès indirect. Par exemple, le dispositif « grands événements » adopté en avril 2017 prévoit que toute personne autre qu'un spectateur ou un participant, notamment lestechniciens, fournisseurs, prestataire de services, journalistes, sponsor, etc. accédant à un grand événement, est soumise à une enquête administrative.
Enfin, depuis la mise en place effective par le Conseil d'Etat d'**une formation spécialisée pour le contentieux du droit d'accès indirect,** la CNIL a produit 189 requêtes, en qualité d'observateur. La formation spécialisée a rendu 79 décisions concluant majoritairement au rejet des requêtes formulées par des personnes souhaitant un droit à communication des données enregistrées dans les fichiers vérifiés par un magistrat de la CNIL dans le cadre du droit d'accès indirect.

2. La CNIL conseille les pouvoirs publics

En 2017, la CNIL a rendu 4124 décisions et délibérations dont **177 avis** portant notamment sur différents champs d'activité :

- **Les impôts** : Les modalités de mise en œuvre de la réforme du **prélèvement à la source de l'impôt sur le revenu** ;
- **La santé** : le décret encadrant l'évolution de la procédure d'agrément des hébergeurs de données de santé au profit d'un dispositif de certification ;
- **La régulation du numérique** : le décret sur la confidentialité des correspondances électroniques dans lequel la CNIL rappelle que le consentement requière la manifestation d'une volonté libre,

spécifique et éclairée ; la CNIL a rendu un avis sur **le projet de loi relatif à la protection des données personnelles**. Elle a insisté sur le nécessaire renforcement de la lisibilité de ce texte qui constitue une étape majeure pour la protection des données personnelles des citoyens et la sécurité juridique des acteurs économiques.

- **La sécurité** : la CNIL n'a pas été saisie du **projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme** mais elle a néanmoins choisi d'examiner ce texte en formation plénière. Elle a notamment estimé que les garanties relatives aux modalités de saisie et d'exploitation de données informatiques dans le cadre des visites et à la surveillance des communications hertziennes devraient être renforcées. Elle a demandé que des précisions soient apportées concernant l'obligation de déclarer les numéros d'abonnement et les identifiants des moyens de communication électronique prévue dans certaines hypothèses, pour clarifier les finalités et garantir la proportionnalité de telles mesures.
  La CNIL a rendu un avis en mai 2017 sur **le traitement ACCRED (automatisation de la consultation centralisée de renseignements et de données)** : elle a souligné que, pour garantir la stricte proportionnalité du dispositif, la liste des traitements susceptibles d'être consultés doit être adaptée aux nécessités spécifiques de l'enquête administrative réalisée.

La CNIL a également participé à une vingtaine d'auditions parlementaires et accueilli dans ses murs des parlementaires de l'Assemblée Nationale.

3. La CNIL accompagne les professionnels dans la transition au RGPD

La permanence de renseignement juridique par téléphone de la CNIL a reçu 67 128 appels en 2017.
Au 1er trimestre 2018, les consultations de « besoin d'aide » sur cnil.fr sont en très nette augmentation par rapport à 2017, avec +64%.

Les professionnels peuvent d'ores et déjà s'appuyer sur de nombreux outils de préparation et de mise en conformité au RGPD, disponibles sur le site internet de la CNIL :

- **La méthode en 6 étapes** pour se préparer permet aux organismes de s'assurer qu'ils ont anticipé et mis en œuvre l'essentiel des mesures nécessaires pour être prêts en mai 2018.
- **Un modèle de registre**
- Le G29 (groupe des CNIL européennes) a déjà adopté plusieurs **lignes directrices**, qui assurent une compréhension et une interprétation communes des points clés du RGPD au niveau européen. Des lignes directrices relatives à l'autorité chef de file, au délégué à la protection des données, au droit à la portabilité et aux analyses d'impact sur la protection des données (PIA), au profilage, à la notification des violations, ont déjà été adoptées.
- Des foires aux questions (FAQ) disponibles sur le site et dans la rubrique « besoin d'aide » permettent aux professionnels comme au public de prendre connaissance, rapidement et simplement, des principales nouveautés issues du RGPD.
- Des outils pratiques, **comme le logiciel PIA**, qui facilite la réalisation des analyses d'impact sur la protection des données, ou encore un modèle de registre (30 000 téléchargements).
- Un formulaire de désignation du délégué à la protection des données, etc.

Dès 2012, la CNIL a anticipé le règlement en développant des outils de conformité tels que le correspondant informatique et libertés, les labels, les études d'impact sur la vie privée ou les packs de conformité qui sont aujourd'hui consacrés. Les entreprises françaises ayant déjà intégré ces outils pourront aborder le règlement de façon plus sereine puisqu'elles ont déjà fait une bonne partie du chemin vers l'*accountability*, clé de voûte de la conformité à l'heure du règlement.

Du CIL au futur délégué à la protection des données
Alors que la désignation d'un correspondant informatique et libertés est optionnelle, 18 800 organismes ont déjà désigné un CIL. Le règlement européen consacre la place du délégué en le plaçant au cœur des nouvelles

obligations des professionnels, en véritable pilote de la conformité. On estime à **80 000** le nombre d'organismes qui devront désigner un DPO.

Les packs de conformité

Elaborés en étroite concertation avec les acteurs d'un secteur, ils permettent de promouvoir des bonnes pratiques et de décliner de façon opérationnelle les obligations. En 2017, deux packs, intégrant déjà les principes du RGPD ont été finalisés : les packs véhicules connectés et Silver économie.

Les labels

123 labels ont été délivrés depuis 2012.

En 2017, la CNIL a reçu 98 demandes de labels, ce qui constitue un nombre record. Afin d'anticiper l'entrée en application du RGPD, la CNIL a procédé à l'actualisation des référentiels « Gouvernance » et « Formation ».

4. L'activité répressive : vérifier la conformité pour sécuriser les données

Les contrôles

La CNIL a réalisé **341 contrôles** en 2017, dont **:**

- **256 contrôles sur place (dont 47 contrôles portant sur des dispositifs vidéo)**.
- **65 contrôles en ligne**
- **20 contrôles sur pièces et sur convocation**, adaptés notamment aux organismes établis hors de France

Les actions menées par la CNIL en 2017 au titre de ses pouvoirs de contrôle et de sanction ont notamment tourné autour de trois axes :

1. **La sécurité des données**

La CNIL reçoit chaque semaine un à deux signalements concernant des failles de sécurité. Pour chacun d'entre eux, les services vérifient la réalité de l'incident de sécurité et prennent des mesures afin qu'il soit résolu au plus vite. C'est ainsi que la CNIL a mis fin en 2017 à près de 80 violations de données (soit par des prises de contact avec le responsable de traitement, des contrôles, des mises en demeure ou des sanctions). Parmi ces incidents de sécurité, cinq ont donné lieu à des sanctions pécuniaires compte tenu notamment du nombre de personnes concernées ou de la nature des données (ex : **Darty, Hertz France**).

2. **La défense des droits des personnes**

Un nombre conséquent de contrôles a été mené concernant directement le respect des droits des personnes (environ 15% des vérifications). Il s'est agi notamment de vérifier la prise en compte des droits de rectification ou d'opposition de plaignants. Environ 15% des mises en demeure de la CNIL concernent également ce point. On peut notamment citer la mise en demeure **APB** (article 10, information insuffisante et non-respect du droit d'accès). Enfin à deux reprises, la formation restreinte de la CNIL a pris des sanctions, une fois pour un défaut de réponse à une demande de droit d'accès (**cabinet dentaire**), l'autre pour non mise à jour des données (**Carrefour Banque**).

3. **La coopération avec les homologues européens**

Dans la continuité des années précédentes, la CNIL a veillé à mener des actions sur des acteurs internationaux en coopération avec ses homologues européens. C'est en 2017 que la CNIL a rendu une sanction pécuniaire à l'encontre de la société **Facebook** concernant notamment l'absence de base légale à la combinaison massive de données et l'utilisation de dispositifs de traçage déloyaux (cookies DATR). Toujours sur la base d'une coopération européenne, la CNIL a également adopté deux mises en demeure publique contre **WhatsApp** (transfert massif de données sans consentement) et sur les jouets connectés conçus par une société chinoise. Enfin, la CNIL a initié ses vérifications concernant la faille **UBER**.

Les contrôles ont été réalisés sur de nombreuses thématiques, et plus particulièrement dans le cadre du programme annuel sur :

- **La confidentialité des données de santé traitées par les sociétés d'assurance** : Il ressort des premiers éléments constatés que les organismes d'assurance, conscients de la sensibilité des données

qu'ils traitent, ont mis en place certaines mesures de nature à préserver la confidentialité et la sécurité de telles données. Toutefois, la CNIL poursuit son analyse afin de déterminer si les garanties apportées sont suffisantes.

- **Les fichiers de renseignement :** Pour l'ensemble des fichiers (les fichiers dits de renseignement territorial, mis en œuvre par les services centraux et locaux de police et de gendarmerie, STARTRAC, PASP et GIPASP, EASP) les investigations menées ont principalement eu pour objet d'analyser les modalités de gestion des fichiers par les services centraux, et d'exploitation par leurs utilisateurs. Les constats ont plus particulièrement porté sur la doctrine d'utilisation de tels fichiers, la pertinence des données enregistrées, le respect des durées de conservation ainsi que les modalités de partage entre services de renseignement. Les constats opérés font actuellement l'objet d'une instruction par les services de la CNIL.
- **Les télévisions connectées (« Smart TV »)** : Les contrôles ont notamment permis de révéler la grande variété des données collectées par ces différents acteurs telles que les coordonnées du téléspectateur couplées à l'historique détaillé des programmes visualisés. La CNIL poursuit ses travaux afin de déterminer si les données ainsi collectées sont proportionnées aux finalités poursuivies, si les durées de conservation appliquées sont justifiées, et si l'information des téléspectateurs ainsi que les mesures de sécurité mises en œuvre sont suffisantes.

Les irrégularités récurrentes en matière de vidéoprotection portent sur :

- l'information du public (panneaux absents, peu lisibles ou incomplets) ;
- le non-respect de l'interdiction de filmer l'intérieur des immeubles d'habitation ;
- le non-respect des durées de conservation ;
- la sécurité (accès aux images et aux enregistrements insuffisamment protégé) ;
- l'autorisation préfectorale (défaut d'autorisation ou autorisation expirée).

Le programme des contrôles 2018 sera examiné en séance plénière le 12 avril.

Les sanctions

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.**

79 mises en demeure ont été adoptées en 2017 portant notamment sur les jouets connectés, APB, la transmission de données de Whatsapp à Facebook. **59** mises en demeure relevaient des manquements à la sécurité.
14 sanctions ont été prononcées par la formation restreinte, dont 9 sanctions pécuniaires et 5 avertissements. 4 sanctions ont porté sur la **non coopération avec la CNIL** et 8 sanctions concernaient des **manquements à la sécurité**.

5. L'animation d'un débat public sur les enjeux éthiques des algorithmes

Chargée par la loi pour une République numérique de mener une réflexion sur les questions éthiques et de société posées par les nouvelles technologies, la CNIL avait choisi en 2017 le thème des algorithmes à l'heure de l'intelligence artificielle.

Elle a publié, le 15 décembre dernier, le rapport de synthèse du débat public ouvert et décentralisé qu'elle a animé de janvier à octobre 2017 et ayant impliqué 60 partenaires partout en France (institutions publiques, associations, entreprises etc.).

La CNIL a ainsi proposé deux principes qui pourraient s'inscrire dans une nouvelle génération de garanties et droits fondamentaux à l'ère numérique, des « droits-système » organisant la gouvernance mondiale de notre univers numérique :

- Un principe de **loyauté** des systèmes d'IA selon lequel tout algorithme, qu'il traite ou non des données personnelles, devrait être loyal envers ses utilisateurs, non pas seulement en tant que consommateurs, mais également en tant que citoyens, voire envers des communautés ou de grands intérêts collectifs dont l'existence pourrait être directement affectée ;
- Un principe de **vigilance**, s'appliquant à l'ensemble des maillons de la « chaîne algorithmique » (développeurs, entreprises, utilisateurs), consistant à organiser une forme de questionnement régulier, méthodique et délibératif à l'égard des systèmes d'IA. Ce principe constitue une réponse directe aux exigences qu'imposent ces objets technologiques du fait de leur nature imprévisible, du caractère très compartimenté des chaînes algorithmiques au sein desquels ils s'insèrent et, enfin, de la confiance excessive à laquelle ils donnent souvent lieu.

Le rapport propose également la déclinaison opérationnelle de ces principes au travers de 6 recommandations à destination tant des pouvoirs publics que des diverses composantes de la société civile (entreprises, grand public, etc.) : former à l'éthique tous les acteurs impliqués dans les chaînes d'IA, rendre les systèmes algorithmiques plus compréhensibles, travailler le *design* desdits systèmes, constituer une plateforme nationale d'audit des algorithmes, encourager la recherche sur l'IA éthique et lancer une grande cause nationale participative autour d'un projet de recherche d'intérêt général et, enfin, renforcer la fonction éthique au sein des entreprises.

Les enjeux pour 2018 (1) : accompagner les professionnels dans leur transition au règlement jusqu'au 25 mai et après

Depuis plusieurs mois, la CNIL propose aux organismes publics et privés, quelle que soit leur taille, un accompagnement pour leur permettre de comprendre ce que change le règlement et conduire cette transition vers le RGPD de manière méthodique. Cet accompagnement se poursuivra après le 25 mai avec notamment l'élaboration de référentiels au niveau européen.

Une évolution substantielle du cadre juridique

Le règlement, s'il reste fidèle aux principes fondateurs de la protection des données en Europe, modifie profondément les obligations pesant sur les organismes, publics ou privés, qui traitent des données. Ce nouveau cadre repose sur une **logique de responsabilisation** des organismes qui traitent des données, qu'ils soient responsables de traitements – donneurs d'ordre – ou sous-traitants.

Cette notion de responsabilisation (*accountability*) se traduit tout d'abord par l'affirmation de deux principes : la prise en compte de la protection des données dès la conception du service ou du produit et par défaut (souvent connues sous leur nom anglais de ***privacy by design* et *by default***). Concrètement, cela signifie qu'à la fois en termes d'organisation interne, de configuration des services ou des produits et de nature et volume de données traitées, les responsables de traitements devront mettre en place des processus et mesures permettant de garantir une protection optimale des données et une minimisation de la collecte.

Le respect de la nouvelle législation européenne implique, pour les administrations comme les entreprises, une adaptation profonde de leurs outils, de leur méthodes et, au-delà, de leur culture en matière de protection des données. Il s'agit d'un **enjeu majeur en termes de confiance** des personnes et, par conséquent, de compétitivité pour les entreprises.

Les organismes qui traitent des données devront ainsi :

- **se doter, le plus souvent, d'un délégué à la protection des données,** véritable chef d'orchestre de la conformité en interne, qui exercera une mission de conseil et de contrôle interne en la matière. Les administrations devront obligatoirement en désigner un ; de très nombreuses entreprises également.

Le règlement devrait se traduire, en France, par la désignation d'un délégué à la protection des données dans 80 000 à 100 000 organismes au minimum.

- **tenir un registre** des traitements mis en œuvre avec une documentation complète, facilitant ainsi l'information des personnes et l'éventuel contrôle par la CNIL ;
- **mener des études d'impact sur la protection des données (PIA) pour les traitements à risque** ;
- **notifier les failles** de sécurité à la CNIL et, le cas échéant, aux personnes concernées.

Une adaptation accompagnée par la CNIL

Afin d'aider les entreprises établies en France, qu'elles soient nationales ou transnationales, la CNIL met en place un dispositif d'accompagnement depuis plusieurs mois, qu'ils s'agissent d'outils élaborés au niveau européen ou national (voir page 7).

Les outils ou initiatives à venir avant mai

- Des **modèles-type de mentions** d'information ou de formulaires de recueil du consentement ;
- Un nouveau modèle de **registre simplifié** ;
- Une information sur les **droits des personnes** ;
- **Des dossiers thématiques à destination des professionnels du marketing et du commerce en ligne** ;
- Un guide élaboré en partenariat avec la BPI à **destination des TPE-PME** ;
- **Un plan d'accompagnement à destination des start-ups** :

La CNIL a décidé d'optimiser ses efforts à destination de ces acteurs très particuliers par leurs moyens comme par leurs objectifs vis-à-vis des enjeux de régulation. Ils sont souvent très agiles du point de vue du numérique, et sans ressources propres à dédier aux questions de protection des données. Dans l'univers économique du numérique, les start-ups jouent souvent un rôle de pionniers et d'éclaireurs vis-à-vis du reste du marché. Un écosystème réunissant de multiples parties prenantes (investisseurs, mentors, incubateurs/accélérateurs, acteurs publics) s'est d'ailleurs structuré pour les accompagner et favoriser leur développement.

La CNIL est convaincue que les startups ont un rôle déterminant à jouer dans le succès de l'application du RGPD par leur capacité à innover, proposer, inventer et mettre en œuvre avec souplesse et rapidité des solutions nouvelles et créatives répondant aux enjeux de conformité (*privacy by design*).

La CNIL a déjà de nombreuses occasions d'entrer en contact avec ces entrepreneurs pour les sensibiliser aux questions informatique et libertés, surtout par des actions ad hoc. Ce plan d'accompagnement consiste à :
- **Mieux structurer des contenus et messages** existants afin de faire monter en compétence tout cet écosystème ;
- **Animer des ateliers** réunissant des entrepreneurs intéressés. La CNIL a déjà dans les dernières semaines organisé, dans le cadre du programme French Tech central animé à Station F par la mission French Tech, et ailleurs 3 *masterclass* réunissant chacune une centaine d'entrepreneurs et 5 ateliers thématiques réunissant une à deux dizaines d'entrepreneurs ;
- **Etre à l'écoute et tirer parti des qualités d'innovation** des startups au profit de nos recommandations et des outils de conformité, en particulier le *privacy by design*.

Offrir un cadre juridique sécurisé : vers l'élaboration de référentiels et une clarification des exigences liées au analyses d'impact

La modification de la loi « informatique et libertés » va offrir à la CNIL de nouveaux outils de régulation dont des référentiels. Ces textes permettront à la CNIL de décliner, dans un secteur d'activité précis, les grands principes portés par le RGPD : ils offriront ainsi un cadre juridique clair et sécurisé permettant aux responsables de traitement concernés de savoir ce qu'attend le régulateur dans leur champ d'intervention. La conformité à certains de ces référentiels permettra également aux responsables de traitement concernés soit de ne pas avoir à faire d'analyse d'impact, soit de ne pas avoir à obtenir une autorisation de la CNIL pour le traitement de données de santé.

La CNIL prépare activement la rédaction de ces **référentiels** dont certains seront prêts dès l'entrée en vigueur du RGPD. Ils s'appuieront, pour partie, sur la doctrine établie par la CNIL depuis de nombreuses années (autorisations uniques, normes simplifiées, packs de conformité, etc.) en l'actualisant au regard des nouvelles exigences issues du RGPD. Ces référentiels seront portés par la CNIL au niveau européen pour que les

entreprises installées en France puissent bénéficier d'un niveau d'exigence uniforme sur tout le territoire de l'Union.

Concernant les analyses d'impact la CNIL travaille à l'élaboration de deux outils prévus par le RGPD :
- la liste des traitements obligatoirement soumis à la réalisation d'une analyse d'impact ;
- et la liste des traitements pour lesquels, au contraire, aucune analyse n'est requise.

Ces listes permettront aux responsables de traitement concernés de savoir plus aisément s'ils sont ou non soumis à cette obligation. Ces listes devront également être soumises au mécanisme de coopération européenne afin d'assurer une harmonisation au niveau européen.

Un contrôle pragmatique du respect du RGPD à partir du 25 mai 2018

Dans les premiers mois de mise en œuvre du RGPD, la CNIL distinguera lors de ses contrôles deux types d'obligations s'imposant aux professionnels.

Les principes fondamentaux de la protection des données restent pour l'essentiel inchangés (loyauté du traitement, pertinence des données, durée de conservation, sécurité des données, etc.). Ils continueront donc à faire l'objet de vérifications rigoureuses par la CNIL.

En revanche, pour ce qui est **des nouvelles obligations ou des nouveaux droits résultant du RGPD** (droit à la portabilité, analyses d'impact, etc.), les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les organismes dans une courbe d'apprentissage vers une bonne compréhension et la mise en œuvre opérationnelle des textes.

Les enjeux de 2018 (2) : accompagner l'innovation

En 2018, la CNIL entend poursuivre ses efforts d'accompagnement de l'innovation initié depuis plusieurs années. Elle prolongera les travaux entrepris sur le cadre éthique et juridique de l'intelligence artificielle et entend porter la discussion sur la gouvernance éthique de l'IA à l'échelle internationale. Elle mènera également des réflexions sur la blockchain ou le design de la protection des données.

L'intelligence artificielle : passer à l'échelle sur le plan éthique et juridique et porter la réflexion au niveau international

Le rapport du député Cédric Villani publié en mars 2018, avant l'annonce par le Président de la République d'une stratégie nationale sur l'IA, confère une importance cruciale à la gouvernance éthique de l'intelligence artificielle. Les recommandations qu'il contient vont largement dans le sens de celles ayant émergé du débat public animé par la CNIL.

La CNIL s'en félicite et entend approfondir à l'échelle internationale le débat sur les principes de gouvernance éthique de l'intelligence artificielle. La Conférence Internationale des Commissaires à la Protection de la Vie Privée et des Données Personnelles, qui se réunira à Bruxelles en octobre 2018, a choisi l'intelligence artificielle comme sujet de travail. Sa réunion pourrait donner lieu à l'adoption par ses membres d'un texte précisant les grands principes sur lesquels devrait reposer le développement de l'intelligence artificielle.

La CNIL entend par ailleurs prolonger en 2018 les travaux qu'elle a déjà réalisés, notamment dans le cadre de son cahier IP consacré en 2017 à la « smart city », sur le cadre juridique du partage et de la mutualisation de données (portabilité citoyenne, plateformes de réutilisation des données, etc.) afin d'en faciliter la bonne appropriation par tous et le développement de projets de recherche en matière d'IA.

La blockchain

Il s'agit d'une technologie, au potentiel de développement fort, progressivement reconnu par **le droit français** (ordonnance relative aux bons de caisse, réforme en cours sur les titres financiers dans la blockchain, etc.) et pour laquelle une mission parlementaire d'information a été ouverte.

Certaines idées reçues circulent, notamment sur une **présumée « incompatibilité** » avec le RGPD et la CNIL a reçu **des demandes concrètes** d'acteurs privés comme publics, en particulier du secteur santé et des institutions financières

Les caractéristiques de cette technologie posent des questions réelles, et la CNIL souhaite proposer des **solutions et des lignes directrices concrètes et lisibles** pour les acteurs qui souhaiteraient l'utiliser dans le contexte d'un traitement de données personnelles.

Du privacy by design au design de la privacy

Le design sera au cœur des prochaines réflexions, avec l'idée d'explorer les enjeux informatique et libertés en mobilisant des champs disciplinaires peu utilisés jusqu'à présent. L'arrivée de services numériques reposant sur des modalités d'interaction « naturelles » (voix, geste) attire l'attention sur leur conception tout comme sur l'influence que les designers peuvent avoir sur les choix des personnes.

Les autorités de protection des données s'intéressent depuis longtemps à l'encadrement juridico-technique de l'utilisation des informations relatives à des personnes. A l'heure où les plateformes numériques investissent massivement dans les nouvelles interfaces hommes machines et l'interprétation des émotions, il devient tout aussi important de comprendre comment ces interfaces sont conçues et avec quelles intentions s'agissant de la manière dont elles influencent les utilisateurs.

La CNIL a entamé depuis plusieurs mois des travaux en lien avec des communautés actives sur les enjeux éthiques du design qu'elle poursuivra en 2018. L'objet de cette exploration est de comprendre comment il est

possible d'innover par le design. Il s'agira de s'interroger sur le rôle du design pour aider les utilisateurs à garder le contrôle et sur le rôle du designer pour accompagner l'utilisateur dans cette démarche.

Pour ces raisons, les intersections des différents champs disciplinaires design, sciences cognitives et comportementales sont des espaces que la CNIL va investiguer dans le cadre de ses activités d'innovation et de prospective pour mieux comprendre comment se forment les décisions au plus proche des individus.