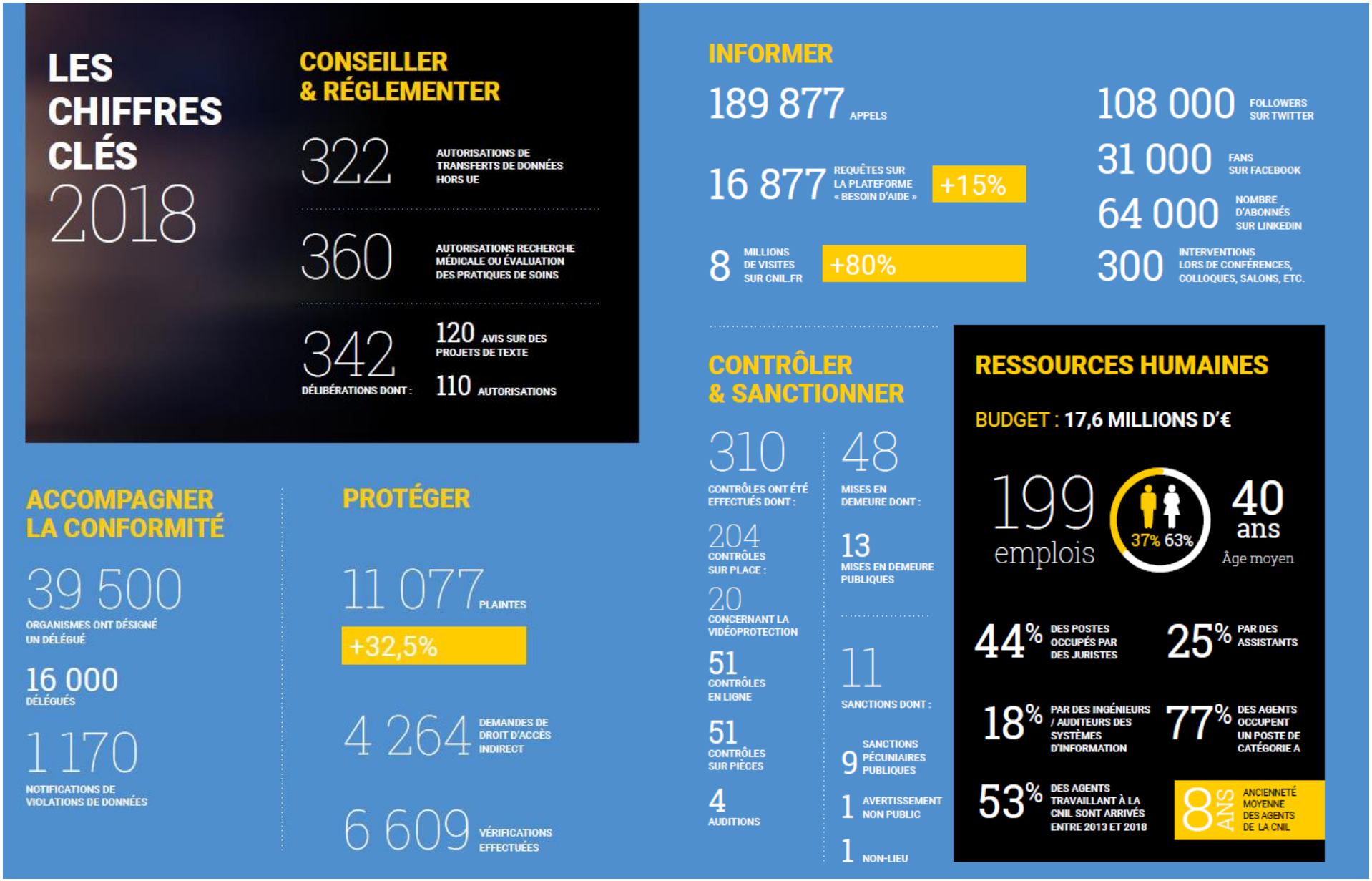
CONFÉRENCE DE PRESSE

15 avril 2019

Rapport d'activité 2018 et enjeux 2019

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Chiffres clés de l'année 2018



Temps forts 2018

Janvier

06/01 > **40 ans** et toujours dans l'air du temps

09/01 > **Darty :** sanction pécuniaire pour une atteinte à la sécurité des données clients

10/01 > **Innovation dans le secteur social-logement :** un pack de conformité pour les produits et services de la silver économie

22/01 > **Admission post-bac (APB) :** clôture de la mise en demeure

23,24/01 > La CNIL au 10e forum international de la cybersécurité (FIC)

31/01 > La CNIL et INRIA décernent le prix protection de la vie privée 2017 à une équipe de recherche européenne

Février

27/02 > **SNIIRAM :** la CNAMTS mise en demeure pour des manquements à la sécurité des données

Mars

21/03 > **Cambridge Analytica :** les autorités de protection européennes se saisissent du sujet

27/03 > **Direct Energie :** mise en demeure pour une absence de consentement concernant les données issues du compteur communicant Linky

Avril

10/04 > Publication du guide de sensibilisation sur le RGPD pour les TPE/PME avec Bpifrance

Mai

25/05 > **Entrée en application du RGPD**

Juin

07/06 > **Optical center :** sanction de 250.000 € pour une atteinte à la sécurité des données des clients du site internet www.optical-center.fr

28/06 > Sanction de 75 000 euros pour une atteinte à la sécurité des données de demandeurs de logements

Juillet

19/07 > **Applications mobiles :** mises en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire

20/07 > **Jouets connectés :** clôture de la procédure de mise en demeure à l'encontre de la société genesis industries limited

24/07 > **Vidéosurveillance excessive :** mise en demeure de l'institut des techniques informatiques et commerciales (ITIC)

31/07 > **OPH de Rennes :** sanction pécuniaire pour une utilisation du fichier des locataires incompatible avec la finalité initiale

Août

02/08 > **Dailymotion :** sanction de 50.000€ pour une atteinte à la sécurité des données des utilisateurs

07/08 > Entrée en vigueur de la nouvelle loi informatique et libertés et de son décret d'application

09/08 > Étude réalisée à partir de messages postés sur twitter par EU DisinfoLab : la CNIL est saisie du dossier

Septembre

03/09 > **Biométrie sur le lieu de travail :** la CNIL lance une consultation publique sur le futur règlement type

19/09 > La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo

20/09 > **Biométrie au travail illégale :** sanction de 10.000 €

26/09 > **Montres connectées pour enfants :** quels enjeux pour leur vie privée ?

27/09 > **Alliance française Paris Ile de France :** sanction de 30.000 € pour une atteinte à la sécurité des données des utilisateurs

Octobre

04/10 > **Applications mobiles :** clôture de la mise en demeure à l'encontre de la société Teemo

17/10 > Dispositifs de mesure d'audience et de fréquentation dans des espaces accessibles au public : la CNIL rappelle les règles

18/10 > Mise en demeure de cinq sociétés d'assurance pour détournement de finalité des données des assurés

25/10 > **Direct Energie :** clôture de la mise en demeure

30/10 > **Vidéosurveillance excessive :** mise en demeure de l'école 42

Novembre

07/11 > **Pratiques abusives « mise en conformité RGPD » :** comment s'en prémunir avec la CNIL et la DGCCRF ?

6/11 > Publication d'une liste des traitements pour lesquels une analyse d'impact est requise

16/11 > **Données génétiques :** les réserves de la CNIL sur l'amendement portant sur l'élargissement du FNAEG

25/11 > Premier bilan 6 mois après l'entrée en application du RGPD

29/11 > **Gestion commerciale et gestion des impayés :** la CNIL lance une consultation publique sur les futurs référentiels

29/11 > **Applications mobiles :** clôture des mises en demeure

Décembre

03/12 > **Jouets connectés :** quels conseils pour les sécuriser ?

05/12 > Signature d'une convention triennale sur la protection des données personnelles dans les usages numériques de l'éducation

19/12 > Publication de l'ordonnance de réécriture de la loi informatique et libertés

20/12 > **Enceintes intelligentes :** des assistants vocaux connectés à votre vie privée

20/12 > **Uber :** sanction de 400.000€ pour une atteinte à la sécurité des données des utilisateurs

26/12 > **Parcoursup** et les établissements d'enseignement supérieur : questions-réponses

27/12 > **Bouygues Telecom :** sanction pécuniaire pour manquement à la sécurité des données clients

28/12 > **Transmission des données à des partenaires à des fins de prospection électronique** : quels sont les principes à respecter ?

Bilan 2018

Une année exceptionnelle pour la CNIL marquée par l'entrée en application du RGPD

L'entrée en application du RGPD a marqué une prise de conscience inédite des enjeux de protection des données auprès des professionnels et des particuliers. Cela s'est logiquement traduit par une augmentation considérable des plaintes adressées à la CNIL, avec une tendance à la hausse qui s'installe. La CNIL a aussi reçu un afflux de demandes d'information de la part des professionnels souhaitant s'approprier ce nouveau cadre, et ce, tous canaux confondus : appels téléphoniques, consultations du site web, comptes réseaux sociaux, demandes de conseil ou d'intervention, etc.

BILAN D'ACTIVITE 2018

1. La CNIL au service des citoyens

Un nombre record de plaintes qui s'explique par l'effet médiatique inédit du RGPD et des citoyens de plus en plus sensibilisés

En 2018, la CNIL a reçu 11 077 plaintes, ce qui représente un record de plaintes et une augmentation de plus de 32% par rapport à 2017 (8300 en 2017). Cette tendance à la hausse est confirmée sur les premiers mois de l'année 2019. Cette augmentation s'explique par une médiatisation importante du RGPD et une plus grande sensibilité aux questions de protection des données. En effet, selon un sondage IFOP réalisé pour la CNIL en avril, **62%** des Français ont entendu parler du RGPD et **70%** se disent plus sensibles que ces dernières années à la protection de leurs données personnelles.

Avec l'entrée en application du RGPD, la CNIL a constaté la mise en ligne de plus en plus fréquente par les organismes de « Politique de protection des données », « Politique de confidentialité » ou autre *Privacy Policy*.

Comment ces plaintes sont-elles traitées ?

Pour les plaintes les plus simples, la CNIL rappelle aux citoyens leurs droits, où trouver les informations dédiées à ces droits et comment les exercer et aux responsables de fichiers leurs obligations. Pour exercer ses droits, la personne doit d'abord s'adresser au responsable du fichier ou au Délégué à la protection des données (DPO) s'il y en a. Ce n'est qu'en cas de refus ou d'absence de réponse dans un délai d'un mois que la CNIL peut intervenir.

Pour les plaintes plus complexes (soit plus de 9000), la CNIL intervient auprès du responsable du fichier mis en cause, par écrit, pour l'interroger sur les conditions de mise en œuvre de son traitement de données, lui rappeler ses obligations et demander le respect des droits des personnes. Ces plaintes peuvent également donner lieu à un contrôle sur place et dans des cas plus rares à une mesure correctrice (mise en demeure, injonction, sanction pécuniaires etc.).
Lorsque les traitements de données personnelles sont transfrontaliers au sein de l'Union Européenne, les plaintes sont désormais traitées en coopération avec les autorités de protection de données des autres pays concernés. **20% des plaintes environ font désormais l'objet d'une coopération européenne**.

- **35,7% des plaintes concernent la diffusion de données sur internet.** Les personnes demandent de supprimer des données sur internet (nom, prénom, coordonnées, commentaires, photographies, vidéos, comptes, etc.). Ces plaintes traduisent les difficultés rencontrées par les personnes pour maitriser leur vie numérique, et notamment leur réputation en ligne. 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.

La CNIL a reçu **373 demandes de déréférencement**. Ce droit, désormais consacré par le RGPD, permet de demander à un moteur de recherche de supprimer certains résultats de recherche associés à ses nom et prénom. En cas de refus, la CNIL saisie par un particulier, fera la balance entre les intérêts du public à avoir accès au contenu via les moteurs de recherche et les droits fondamentaux de la personne. La CNIL prend notamment en compte le caractère récent du contenu en cause, sa pertinence, son caractère exact, journalistique ou légal et le rôle joué par la personne dans la vie publique.

Par ailleurs, plusieurs centaines de plaintes ont été reçues contre l'association belge « EU Disinfonlab » à l'occasion de son étude portant sur les tweets concernant « l'affaire Benalla ». Ces plaintes sont traitées, dans le cadre du mécanisme de coopération par l'autorité belge de protection des données.

- **21% des plaintes concernent le secteur marketing/commerce**. La CNIL a constaté une très forte hausse des plaintes concernant la prospection par SMS. Les personnes se plaignent de recevoir des sollicitations sans que leur consentement préalable n'ait été recueilli et que l'envoi de « STOP » à l'expéditeur fasse cesser la réception de publicités. La publicité par courrier électronique reste une source importante de plaintes. Le travail mené en lien avec l'association « Signal Spam » devra porter ses fruits dans les mois à venir, notamment en raison des nouveaux pouvoirs de la CNIL créés par le RGPD et la nouvelle loi Informatique et Libertés.

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

  - les ressources humaines (16,5%) : 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 (8,9%) : 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 (4,2%) : difficultés à accéder au dossier médical ou social, Pôle emploi. Depuis la sanction de 10 000€ prononcée en 2017 à l'encontre d'un professionnel de santé, une amélioration des pratiques est perceptible puisque le nombre de plaintes relatives au droit d'accès au dossier médical a baissé de près de 30% par rapport à 2017.

Les tendances émergentes

- **Le visionnage à distance des images issues des dispositifs vidéo**, notamment par l'employeur (depuis son ordiphone ou tablette), pointant un risque de surveillance excessive des employés ;
- **L'installation de caméras dans des unités de soin**, filmant ainsi des personnes vulnérables (patients, personnes dépendantes, mineurs, etc.) pour leur « sécurité » ;
- Le souhait des clients de banques ou de services en ligne de contenus **d'utiliser leur droit à la portabilité de leurs données** ;
- **La sécurité de ses données personnelles**, et pas seulement sur internet (accès à ses données par des collègues dans des établissements hospitaliers ou par un ancien conjoint lors d'un conflit familial ; documents papiers jetés non broyés dans les poubelles ; confidentialité de ses données en qualité de copropriétaire gérées par un syndic, etc.) ;
- Des craintes quant aux **données auxquelles les applications mobiles accèdent** dans son ordiphone.

Une modification importante des modalités d'exercice des droits pour certains fichiers de l'Etat

Le décret du 1er août 2018 portant application de la loi Informatique et Libertés prévoit désormais, pour certains fichiers comme le Traitement d'Antécédents Judiciaires (TAJ) de la police et de la gendarmerie nationales, un **principe direct de l'exercice des droits** : accès, rectification, effacement voire limitation. Ce droit s'exerce auprès du responsable du traitement, **sous réserve des restrictions applicables** à chacun des fichiers, qui doivent être définies par le décret les régissant.

La CNIL n'est donc plus l'interlocutrice première des personnes pour la majeure partie des fichiers qui étaient jusqu'à présent soumis au régime du droit d'accès indirect

Toute personne souhaitant exercer ses droits pour les fichiers concernés doit désormais effectuer directement une demande auprès de l'administration gestionnaire. Ce n'est que si, au terme d'un délai de deux mois, ce dernier lui oppose une restriction ou ne lui apporte aucune réponse, qu'elle a alors la possibilité, en deuxième ligne, de saisir la CNIL au titre de l'exercice indirect des droits. Elle peut également engager un recours auprès des juridictions administratives contre la décision de restriction opposée par le responsable du traitement.

4264 demandes de droit d'accès indirect ont été adressées à la CNIL en 2018 portant majoritairement sur le TAJ et le fichier FICOBA. 1344 d'entre-elles reçues avant le 1er août 2018 (soit 31,50%) ont fait l'objet d'un transfert total ou partiel vers les différents gestionnaires à la suite de l'entrée en vigueur du décret du 1er août 2018.

2. La CNIL conseille les pouvoirs publics

Le collège de la CNIL a rendu 120 avis sur des projets de texte d'origine gouvernementale concernant la protection des données personnelles ou créant de nouveaux fichiers et 110 autorisations.
Les **avis** ont porté notamment sur :

- le projet d'ordonnance de réécriture de la loi « informatique et libertés » ;
- le décret d'application de la loi « informatique et libertés » ;
- certaines dispositions du projet de loi d'orientation des mobilités.

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

3. La CNIL aide les professionnels à s'approprier le RGPD

La CNIL : une source d'information de référence pour les professionnels

« L'effet RGPD », déjà ressenti en 2017, s'est accentué en 2018. Dès le premier trimestre 2018, le nombre des sollicitations émanant des professionnels a augmenté de manière significative pour atteindre sur certaines périodes des chiffres inédits (+ de 25 000 appels pour le seul mois de mai). Les responsables de traitement, en particulier les petites et moyennes entreprises, désireux de se conformer à la nouvelle réglementation souhaitent de plus en plus être accompagnés et rassurés, en raison notamment du renforcement des pouvoirs de sanction.

Si, à l'approche de l'entrée en application du RGPD, la majorité des questions a porté sur la nécessité ou pas d'effectuer des formalités auprès de la CNIL, les problématiques ont évolué depuis et deviennent de plus en plus complexes. La CNIL est ainsi régulièrement interrogée sur les paramétrages des cookies, la conformité de logiciels au RGPD, l'interprétation de certaines dispositions du RGPD (base légale, consentement, modalités d'information des personnes, etc.), sans oublier tout ce qui a trait aux modalités concrètes d'exercice du droit des personnes.

- 189 877 appels reçus (+ 22% par rapport à 2017)
- 283 742 consultations des Questions/Réponses en forte hausse (+59% par rapport à 2017)
- 8 millions de visites sur cnil.fr en 2018 (+80% par rapport à 2017)

- Environ 215 000 comptes suivent la CNIL de près ou de loin sur les réseaux sociaux. En 12 mois, l'audience de la page LinkedIN de la CNIL a été multipliée par trois pour atteindre 70 000 abonnés.

Les professionnels peuvent s'appuyer sur de nombreux outils de mise en conformité au RGPD proposés par la CNIL et disponibles depuis son site:

- **Le guide TPE/PME** élaboré avec bpifrance ;
- **La méthode en 6 étapes** permet aux organismes de s'assurer qu'ils ont mis en œuvre l'essentiel des mesures pour être en conformité ;
- **Un modèle de registre simplifié ;**
- **Des exemples de mention d'information ;**
- **Des éclairages sur les notions clés :** consentement, profilage, guichet unique, violation de données, transferts, etc.
- La liste des traitements pour lesquels une analyse d'impact sur la protection des données est obligatoire ;
- Un **logiciel** qui facilite la réalisation des analyses d'impact sur la protection des données téléchargé 150 000 fois et traduit en 18 langues ;
- Une formation en ligne (MOOC) sur les principes clés du RGPD : **27.500 personnes** ont créé leur compte depuis 1 mois et 10% poursuivent jusqu'à l'obtention d'une attestation

ARNAQUES RGPD

À l'approche du 25 mai, la CNIL a mis régulièrement en garde les professionnels sur des démarchages agressifs et abusifs pour des prestations de « conformité RGPD » frauduleuses, en diffusant des messages de vigilance sur son site ou les réseaux sociaux. Elle a signalé ces pratiques à la DGCCRF. Elle constate encore aujourd'hui de telles pratiques, notamment actuellement à destination de médecins, dentistes ou pharmaciens.

Les nouveaux outils au service de la conformité

Le délégué à la protection des données

Le règlement européen consacre la place du délégué en le plaçant au cœur des nouvelles obligations des professionnels, en véritable pilote de la conformité. Le positionnement du DPO est fortement affirmé ainsi que ses ressources afin qu'il puisse accomplir pleinement son métier qui implique une capacité à se poser en pilote de la conformité.

- 51.000 organismes ont désigné un délégué à la protection des données, ce qui représente 17.000 délégués (par effet de la mutualisation)
- 1/3 sont des organismes publics

Deux référentiels en matière de certification de DPO ont été adoptés :

- un référentiel de certification qui fixe notamment les conditions de recevabilité des candidatures et la liste des **17 compétences et savoir-faire attendus pour être certifié** en tant que DPO ;
- un référentiel d'agrément qui fixe les critères applicables aux organismes qui souhaitent être habilités par la CNIL à certifier les compétences du DPO sur la base du référentiel de certification élaboré par la CNIL ;

Les cadres de référence

La CNIL élabore des cadres de référence permettant de guider les organismes dans la mise en conformité de leur traitement. Ces instruments de régulation ont vocation à donner davantage de sécurité juridique aux organismes. Ils sont élaborés en concertation avec les acteurs ou secteurs concernés : règlement type « biométrie sur les lieux de travail et les référentiels sur la gestion clients, la gestion des impayés ou les ressources humaines.

Les notifications de violations de données

L'entrée en application du RGPD le 25 mai 2018 a imposé, à tous les organismes qui traitent des données personnelles, de mettre en place des mesures pour prévenir les violations de ces données.
Une violation de données à caractère personnel est constituée par toute action, intentionnelle ou non, portant atteinte à la confidentialité, l'intégrité ou la disponibilité de ces données.

La CNIL a reçu **1170 notifications** en 2018. Ces notifications sont dues en très grande majorité **à des atteintes à la confidentialité des données.**

La CNIL privilégie l'accompagnement lors de la réception des notifications dans les délais impartis. Cette approche a pour but d'aider les professionnels concernés à prendre les mesures pour limiter les conséquences d'une violation. L'objectif est avant tout d'élever le niveau global de cybersécurité et de permettre aux personnes de se protéger lorsqu'une violation s'est produite.

Pour autant, une violation qui serait massive (volume de données) ou qui porterait sur des traitements à fort enjeu (données sensibles, données bancaires, acteur régalien…) est susceptible d'entraîner, si la situation l'exige, une réponse répressive, quand bien même la procédure de notification serait respectée. Par ailleurs, la CNIL adoptera une approche répressive en cas de non-respect de l'obligation de notification dans les 72h.

Lors des contrôles la CNIL vérifiera systématiquement que les organismes ont bien mis en place des procédures et un registre des violations.

4. L'activité répressive au service de la sécurité des données

La CNIL a réalisé **310 contrôles** en 2018, dont **:**

- **204 contrôles sur place (dont 20 contrôles portant sur des dispositifs vidéo)**.
- **51 contrôles en ligne**
- **51 contrôles sur pièces**
- **4 auditions**

L'entrée en application du RGPD ne change pas la manière dont les contrôles de la CNIL sont effectués. La CNIL continue de vérifier, sur place, en ligne ou sur audition, la conformité des traitements de données à caractère personnel, aux dispositions de la loi « Informatique et Libertés » et du RGPD. Deux nouveautés ont néanmoins été introduites lors de la modification de la loi « Informatique et Libertés » le 20 juin 2018. Désormais, la CNIL peut « inviter » des agents d'autres autorités de protection des données de l'Union européenne à participer à des contrôles sur le territoire français. Elle peut aussi effectuer des contrôles en ligne sous identité d'emprunt.

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

- Les pièces justificatives demandées par les agences immobilières
- Les traitements liés au recrutement
- Les traitements liés au stationnement payant
- La collecte de données dans les centres d'appels téléphoniques

- Le détournement de finalités des données des assurés commis par des sociétés d'assurance
- La mise à jour des données inscrites au FAED (fichier Automatisé des Empreintes Digitales)
- La gestion des durées de conservation dans le secteur médico-social

Les sanctions et mises en demeure

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.**

49 mises en demeure ont été adoptées en 2018. **Deux secteurs ont été particulièrement concernés :**

- celui des assurances, avec 5 décisions adoptées ;
- celui des entreprises spécialisées dans le ciblage publicitaire par le biais d'une technologie (SDK) installée dans des applications mobiles, avec 4 décisions adoptées.

Ces mises en demeure ont toutes fait l'objet d'une clôture.

11 sanctions ont été prononcées par la formation restreinte, dont 10 sanctions pécuniaires (dont 9 publiques) et 1 avertissement non public et un non-lieu. **7 sanctions pécuniaires prononcées concernaient des atteintes à la sécurité** des données personnelles.

La CNIL reçoit un grand nombre de 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. Ce sont presque **90 violations de données qui ont pu être résolues**, soit par une prise de contact immédiate avec le responsable de traitement, soit, pour les cas les plus graves, par des contrôles, des mises en demeure ou des sanctions. La majorité des sanctions prononcées en 2018 a concerné des incidents de sécurité (7 sur 10). Figurent parmi les organismes sanctionnés sur ce thème : Uber, Bouygues Télécom, Dailymotion ou Optical center. Ce n'est pas l'incident en tant que tel que la CNIL a sanctionné, mais les carences et insuffisances dans les mesures de sécurité dont cet incident n'a été qu'une traduction.

5. Une coopération européenne opérationnelle

Le RGPD a institué au niveau européen un nouveau modèle de gouvernance et une série de mécanismes de coopération formels entre autorités nationales de protection des données, plus particulièrement pour les traitements dits transfrontaliers. Sur ces aspects, des outils et des procédures ont été mis en place durant l'année 2018 afin de rendre opérationnel ce nouveau cadre de coopération et organiser en pratique le travail des autorités.

Dès le 25 mai, cette coopération s'est engagée :

- Cette coopération porte sur **des centaines de cas ou procédures** qui concernent plusieurs milliers de personnes (858 procédures en cours d'instruction). Par exemple : la CNIL est autorité chef de file pour 40 cas et autorité concernée pour 609 autres cas dont 498 plaintes et 53 violations de données.
- Même dans des cas où la coopération n'était pas obligatoire, la CNIL a coopéré : des échanges ont en effet eu lieu dans le cadre de l'instruction des plaintes collectives contre Google pour lesquelles le mécanisme de coopération n'était pas encore obligatoire, puisque Google ne disposait pas au moment de l'instruction d'un établissement principal en Europe.

Le CEPD a déjà rendu des avis ou des lignes directrices en matière de champ d'application territorial, de certification, de transparence, consentement, etc.

Les enjeux de 2019 (1) : réussir le RGPD, clé de voûte d'un numérique de confiance

L'année 2019 sera décisive pour crédibiliser le nouveau cadre juridique et transformer cet ambitieux pari européen en succès opérationnel. Les attentes de la société civile et des acteurs économiques sont très fortes et ce modèle suscite des intérêts à travers le monde. La CNIL articulera son action autour de deux axes principaux : la pédagogie et la dissuasion.

1. L'amplification des actions d'accompagnement des professionnels

La réussite de la mise en œuvre du RGPD par les professionnels passe par **une amplification des actions d'accompagnement** qui leur sont dédiées.

Pour les acteurs publics

- **La sensibilisation à destination des collectivités**

En 2019, la CNIL développera de nombreuses actions de sensibilisation à destination des collectivités territoriales et tout particulièrement des petites communes. Elle proposera au premier semestre un guide pratique, une rubrique dédiée sur son site avec des fiches thématiques permettant d'aller plus loin dans sa conformité, elle poursuivra ses échanges avec les têtes de réseau et les associations telles que l'ADF, l'AMRF, l'AMF, l'ANDAME, etc. Enfin, elle sera présente au Salon des Maires et des collectivités locales en novembre et enrichira son MOOC d'un module dédié aux collectivités.

- **La préparation des élections européennes et municipales en matière de communication politique**

Le RGPD n'a pas entrainé de changement quant à la qualification des opinions politiques comme des données sensibles et au principe d'interdiction de collecter et de traiter de telles données, ainsi qu'aux exceptions prévues. Néanmoins, en raison de la disparition des formalités préalables et de la création de nouveaux droits et obligations pour les acteurs de la vie politique, la CNIL a entamé une analyse approfondie qui la conduira à adapter prochainement ses recommandations de 2012.

Elle poursuivra aussi ses travaux s'agissant des nouveaux outils et usages mobilisés à des fins de communication politique dans le but d'affiner et d'asseoir sa doctrine.

La CNIL étendra également sa réflexion dans une dimension plus globale de la vie citoyenne. Elle réfléchit en particulier actuellement aux nouveaux usages numériques dans le champ de la démocratie locale et nationale et à l'impact des civic tech en matière de protection des données personnelles.

- **La publication d'un guide et de fiches pratiques sur l'ouverture des données publiques (open data) avec la CADA**

Le cadre juridique de l'open data et son articulation avec la réglementation relative à la protection des données personnelles a suscité de nombreuses interrogations de la part des différents acteurs concernés, par exemple sur les catégories de documents pouvant être publiés ou les conditions dans lesquelles ces mêmes documents peuvent être réutilisés.

Dans ce contexte, l'élaboration par la CNIL et la CADA d'un guide pratique sur la publication en ligne et la réutilisation des données publiques permettra de clarifier le cadre juridique applicable et de répondre aux principales problématiques rencontrées par les acteurs. La consultation ouverte pendant 6 semaines vient de s'achever. Elle a recueilli environ 120 contributions et 170 votes.

Pour les acteurs privés

- **L'accompagnement des start-ups et de la communauté des designers**

La CNIL a décliné une offre d'accompagnement à destination des startups. Elle a notamment formalisé un partenariat avec l'espace des services publics « French Tech Central » de Station F. Elle a organisé une vingtaine d'ateliers thématiques à Station F ainsi que dans d'autres lieux de l'innovation. Les thèmes abordés y ont notamment été : RGPD, Portabilité, Santé, Sécurité, Fintech, Silver Eco, PIA ou Objets connectés. Des contenus adaptées aux besoins et questions que se posent les startups seront bientôt proposés sur le site de la CNIL. Design Factory, une plateforme développée par la CNIL sera bientôt disponible. Elle permettra aux professionnels du design d'échanger sur leurs pratiques, de partager leur approche des enjeux de protection des données et de co-construire un design éthique de la protection des données.

L'élaboration de nouveaux cadres de référence

La CNIL proposera de nouveaux cadres de référence aux professionnels en poursuivant et développant ce qu'elle a initié depuis mai en matière de lignes directrices, référentiels (ressources humaines, vigilance sanitaire, gestion de la relation client, etc.), règlements type (sur le modèle de celui dédié au contrôle d'accès biométrique sur les lieux de travail), listes de traitements non soumis à une analyse d'impact obligatoire, etc.

2. Un dialogue étroit avec les professionnels

Un dialogue étroit entre le régulateur et les secteurs régulés est nécessaire. En effet, il n'y a pas toujours de solution « passe-partout » pour protéger les données personnelles : il existe pour chaque secteur d'activité, pour chaque métier, des enjeux spécifiques qui appellent des réponses adaptées (commerce en ligne, gestion des ressources humaines à l'heure du big data, objets connectés, etc.).

Par ailleurs, tout ne saurait reposer sur l'action du seul régulateur : il faut au contraire que la culture « informatique et libertés » se diffuse au plus près des professionnels, et que chacun des acteurs – fédérations professionnelles, entreprises, parties prenantes - se l'approprie. C'est ainsi que le niveau de conformité « informatique et libertés » s'élèvera le plus efficacement.

La CNIL avait entamé depuis plusieurs années cette approche sectorielle, au travers de packs de conformité (véhicule connecté, économie des séniors, logement social, etc.). A l'heure du RGPD, elle entend la renforcer, par plusieurs canaux. La CNIL mise tout d'abord sur une stratégie de **sensibilisation des « têtes de réseau »** (groupements, fédérations professionnelles et interprofessionnelles, communautés de délégués, etc.) pour favoriser leur montée en compétence – et à travers eux la montée en maturité « informatique et libertés » de tous –, susciter **des codes de conduite**, et plus largement pour démultiplier son action. Ce dialogue nourrira également les outils de droit souple élaborés par la CNIL (référentiels, contenus du site, etc.). **L'appui maintenu aux délégués à la protection des données**, dans la continuité des actions menées de longue date auprès des correspondants informatiques et libertés, sera un autre canal de dialogue précieux. Enfin, la poursuite de la montée en puissance de la **démarche de certification** – l'une des nouveautés du RGPD – sera l'une des clés de cette diffusion des outils de la conformité dans l'ensemble du tissu économique.

3. Une activité répressive : contrepartie naturelle d'une responsabilisation accrue des acteurs

Cette amplification des actions d'accompagnement s'opérera en parallèle d'un contrôle exigeant et, dans les cas qui le nécessitent une sanction ferme car la crédibilité du RGPD repose aussi sur **une politique de contrôles et de sanctions efficace**. C'est la contrepartie naturelle de la responsabilisation accrue des acteurs et de leur capacité à apporter la preuve de leur conformité par une approche dynamique et continue.

S'agissant de la doctrine « répressive » de la CNIL, l'année 2018 a constitué une année de transition destinée à permettre aux responsables de traitement de comprendre et assimiler les exigences du RGPD adopté en 2016.

L'année 2019 marque l'achèvement de cette phase de transition entre l'ancienne législation et le RGPD.

La CNIL **vérifiera ainsi pleinement le respect des nouvelles obligations et nouveaux droits issus du cadre européen (analyse d'impact, portabilité des données, tenue d'un registre des traitements et des violations**). Lorsqu'elle constatera des manquements, elle en tira les conséquences qui s'imposent, jusqu'à la sanction si nécessaire.

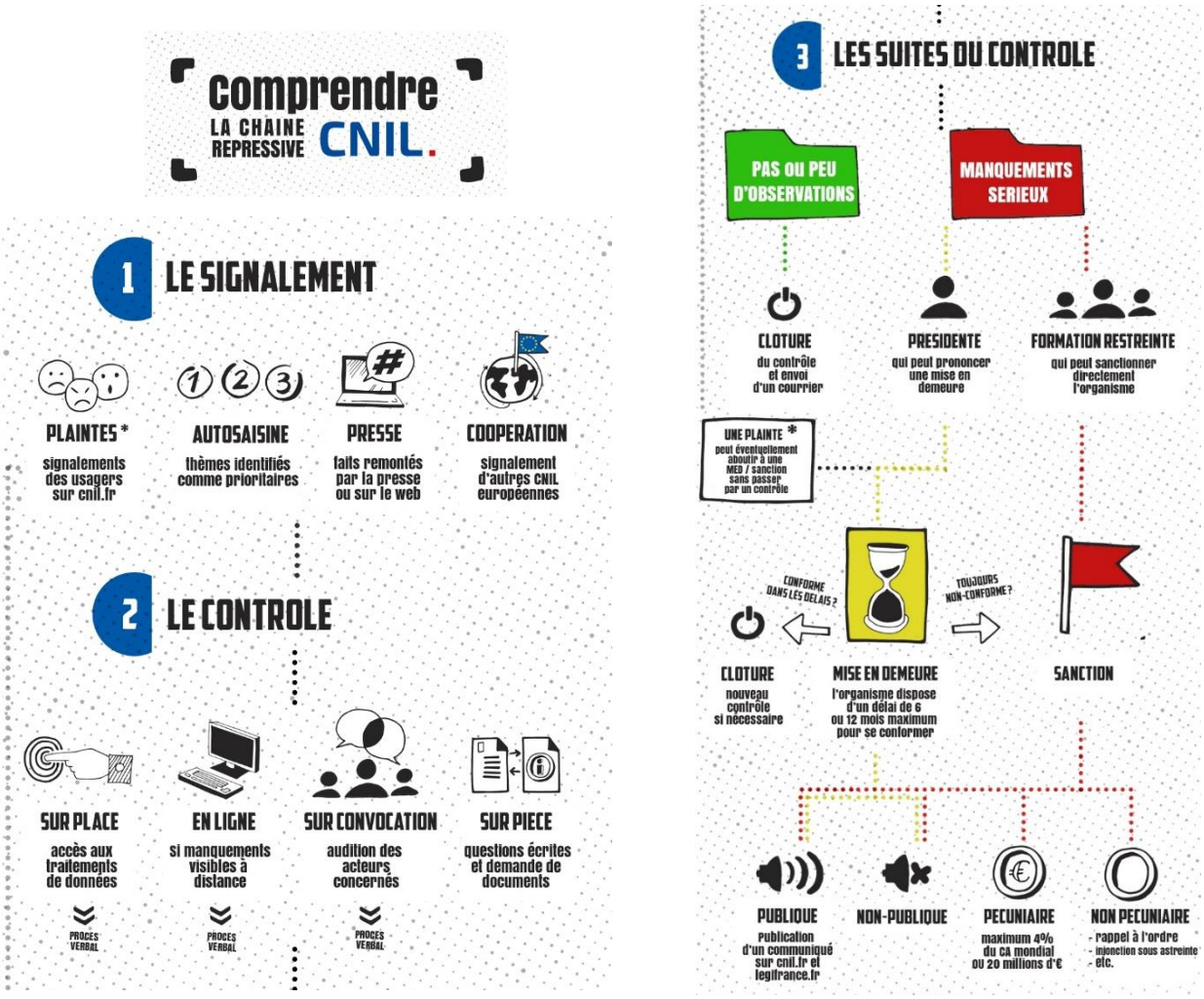
Mais comme par le passé, la CNIL fera preuve de **discernement** dans le choix des mesures correctrices. Les textes prévoient toute une palette de réponses : clôture avec observations, mise en demeure, rappel à l'ordre, injonction sous astreinte, sanction pécuniaire. Pour choisir la réponse appropriée, la CNIL tiendra ainsi compte de la gravité des manquements, de l'activité et de la taille de l'organisme concerné, de sa coopération et de sa bonne foi.

Le programme des contrôles 2019

Dans le cadre de son programme annuel des contrôles qui représente environ ¼ de ses investigations, la CNIL souhaite concentrer cette année son action sur les plaintes et trois grandes thématiques, directement issues de l'entrée en application du RGPD.

- Une stratégie de contrôles centrée sur les plaintes reçues (collectives ou individuelles) pour rester en prise directe avec les attentes des citoyens. Les contrôles porteront notamment sur l'exercice pratique des droits, ce qui représente 73,8% des plaintes reçues en 2018.

- Des contrôles sur des grandes thématiques qui concernent tous les secteurs plutôt que sur des traitements : la répartition des responsabilités entre les sous-traitants et les donneurs d'ordre, les données des mineurs (publication de photos, biométrie et vidéosurveillances dans les écoles, recueil du consentement des parents pour les moins de 15 ans).



Les enjeux de 2019 (2) : une CNIL experte sur les infrastructures et plateformes numériques

Afin de continuer à être un régulateur du numérique efficace et pragmatique, la CNIL doit constamment se réinventer pour être en mesure de toujours maîtriser des sujets supposant une expertise technologique pointue. Dans un contexte d'innovation permanente, il s'agit d'un enjeu majeur pour la CNIL.

Dans l'économie numérique, dans les politiques publiques, dans notre vie personnelle et professionnelle, les enjeux de protection des données personnelles sont omniprésents. Régulateur de la donnée personnelle, la CNIL se trouve donc au cœur des grands équilibres d'un monde numérique toujours plus complexe.

Dans ce contexte, l'efficacité de sa régulation suppose, en premier lieu, **une capacité d'expertise toujours en pointe et ouverte à toutes les disciplines** (technologiques, juridiques, éthiques, sciences humaines, etc.) qui permettent de saisir l'ensemble de ces enjeux.

Depuis plusieurs années, la CNIL a ainsi développé des compétences nouvelles d'expertise technologique au sein de la direction des technologies et de l'innovation. Cela lui permet de comprendre en profondeur les nouvelles technologies, anticiper leurs impacts et maitriser les questions de cybersécurité. Les contacts avec l'écosystème du numérique se sont également multipliés dans le cadre des activités d'innovation et de prospective, aussi bien à travers les activités du LINC (Laboratoire d'innovation numérique de la CNIL) que de la déclinaison de la stratégie startups. A l'avenir, ces tendances sont amenées à s'amplifier ; elles devront notamment davantage irriguer les activités de contrôle, dans lesquelles la CNIL sera amenée à renforcer ses capacités en matière d'investigation numérique.

En complément de son approche juridique et technologique, la CNIL approfondira en 2019 ses réflexions sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques. Elle l'a fait, dès 2017, sur le thème de l'intelligence artificielle et des algorithmes, qui a donné lieu à des évènements publics et un rapport. La CNIL poursuivra cette mission sous une autre forme en 2019, notamment en intégrant une dimension éthique, dès leur conception, à ses travaux sur les principaux sujets de société (civic tech, partage de données, etc.).

L'efficacité de la régulation exige, en deuxième lieu, **une coopération approfondie avec les autres régulateurs** intervenant dans ces mêmes équilibres, afin d'apporter aux citoyens et aux opérateurs une réponse publique cohérente et efficace. Cette **interrégulation** méritera aussi d'être renforcée dès 2019, à un double titre. D'une part, parce que la question des données dépasse le simple cadre de leur protection : on pense, ici, à leur valeur dans une logique concurrentielle. D'autre part, parce que la protection des données peut être une partie d'une régulation plus globale – par exemple, les réflexions liées à la régulation des plateformes numériques. Dès lors, la CNIL entend renforcer ses liens avec les autres régulateurs concernés (Autorité de la concurrence, CSA, ARCEP, ACPR, etc.). Cette expertise technique lui permet de dialoguer avec les grands acteurs de l'internet ou les startups mais aussi de rendre plus visibles aux yeux du grand public des écosystèmes complexes.

La régulation du numérique, portée par la CNIL, appelle, enfin, **un travail de fond prioritaire sur les sujets les plus structurants et impactants.** Outre les plateformes, qui occupent de longue date les équipes de la CNIL, deux axes de travail seront plus particulièrement mis en lumière en 2019 : **le *cloud computing* et les assistants personnels.**

1. Le cloud computing

La CNIL travaille sur le sujet depuis le début des années 2010, en collaboration avec les autres autorités européennes de protection des données. Après une large consultation, en juin 2012, la CNIL a publié ses premières recommandations en matière de cloud computing, suivies par le G29.

Depuis, le recours au cloud n'a fait que s'intensifier : Gartner estimait récemment ce marché atteindrait 300 milliards de dollars en 2021. Dans le même temps, Eurostat indiquait que 55% des entreprises ont recours au cloud pour des fonctions critiques (finances, comptabilité, CRM ou applications métiers).

À l'heure du RGPD, qui modernise les obligations applicables aux responsables de traitements comme aux sous-traitants, un état des lieux s'impose sur l'utilisation du cloud dans les organisations. Les recommandations de 2012 ont-elles été intégrées ? La protection des données personnelles est-elle maitrisée lors d'une migration vers le cloud ?

La CNIL souhaite tout d'abord approfondir les aspects techniques pour mieux comprendre le détail des infrastructures des principaux fournisseurs de services de *cloud* et plus généralement de cet écosystème. Dans un second temps, elle analysera les contraintes et les risques auxquels les entreprises clientes sont réellement confrontées aujourd'hui. Enfin, ces travaux lui permettront d'actualiser ses recommandations et d'identifier de nouveaux leviers de régulation de ce secteur à mobiliser.

2. Les assistants personnels

La thématique des assistants vocaux a été identifiée comme axe de travail par la CNIL dès 2017. Celle-ci est entrée rapidement en contact avec différents parties prenantes afin d'avoir une parfaite compréhension des systèmes déployés. Elle a mené d'importantes réflexions au sein du laboratoire d'innovation numérique de la CNIL (LINC), sa structure dédiée à l'expérimentation et à l'étude des tendances émergentes d'usage du numérique. Un dossier thématique composé d'articles et d'entretiens avec des professionnels a ainsi été publié sur son site.

Aujourd'hui, les fabricants mènent de nombreux travaux afin d'améliorer les capacités des assistants vocaux et leur sécurité. Si certains souhaitent ainsi supprimer de plus en plus le recours au mot clé pour le réveil de l'assistant, d'autres travaillent à mettre en œuvre des traitements de séparation des sources sonores afin d'améliorer la capacité d'écoute des systèmes, par exemple pour atténuer le son de la télévision, séparer la parole d'une personne de celle d'une autre, *etc.* Enfin, les professionnels investiguent de nouveaux lieux d'usage, comme le parc hôtelier ou les espaces de travail, renouvelant de ce fait les questions autour des usages effectifs des données.

En 2019, la CNIL prévoit de prolonger ces travaux, à la fois en continuant d'échanger avec les industriels et les académiques dont c'est l'objet d'étude, mais également en poursuivant des tests sur ces appareils. Il s'agira en particulier d'évaluer comment garantir que les utilisateurs sont bien informés des données collectées, des usages qui en sont faits et des moyens à leur disposition pour exercer leurs droits d'accès, modification, suppression et portabilité, ainsi que d'étudier la sécurité des données traitées et la manière dont est réalisé l'apprentissage des algorithmes d'intelligence artificielle inhérents à ces appareils.

Les enjeux de 2019 (3) : une diplomatie de la donnée personnelle, aux niveaux européen et international

La CNIL entend conserver un rôle moteur au niveau européen en défendant les positions françaises au sein du Comité européen de protection des données (CEPD) notamment dans le cadre des travaux prévus au programme de travail 2019-2020. Elle participera aux initiatives visant à développer une coopération opérationnelle avec ses homologues extra européens et une convergence des principes de protection des données au plan mondial.

1. Au plan européen

La CNIL sera activement impliquée en défendant les positions françaises au sein du Comité européen de protection des données (CEPD) dont les travaux se concentreront sur des problématiques ou technologies spécifiques inscrites à son programme de travail, telles que :

- le ciblage des utilisateurs de réseaux sociaux ;
- les nouveaux outils de transferts que sont la certification et les codes de conduite ;
- le champ d'application territorial du RGPD ;
- le Règlement e-Privacy ou encore l'interaction entre le RGPD et le flux de données non-personnelles.

Au-delà des sujets définis dans le cadre du programme de travail, la CNIL participera à :

- l'adoption d'avis au titre du mécanisme de contrôle de la cohérence ou de décisions pour arbitrer des litiges entre autorités ;
- l'évaluation du cadre juridique de protection des données dans le cadre de décisions d'adéquation de pays tiers.

Sur un thème plus régalien, le CEPD examinera :

- l'interaction entre les demandes de production de données émanant d'autorités étrangères adressées à des entreprises situés dans l'Union européenne et la législation américaine sur l'accès aux preuves électroniques détenues par les entreprises (le « Cloud Act »).

Ce sujet clé est également à relier au projet de cadre juridique en cours de préparation au niveau européen en matière d'accès par les autorités aux preuves électroniques (dit « e-evidence ») et la rédaction sur le même sujet d'un protocole additionnel à la Convention du Conseil de l'Europe sur la Cybercriminalité (Convention de Budapest). L'ensemble de ces initiatives réglementaires soulèvent des questions quant à un potentiel conflit entre les dispositions du RGPD et appellent à une vigilance quant aux garanties pour les droits des personnes dont les données pourraient être accédées dans un tel contexte.

2. Au plan international

Compte tenu de l'augmentation des échanges transfrontières de données personnelles en particulier en lien avec l'offre des services numériques, la protection des données s'inscrit naturellement dans une logique mondiale. Aussi, les entreprises quel que soit leur lieu d'implantation dans le monde se retrouvent confrontées à des problématiques de plus en plus similaires en la matière, ce qui appelle à une convergence des principes de protection des données personnelles.

A ce titre, la CNIL s'investit sur les travaux liés aux évolutions des principes de protection des données initiés récemment dans le cadre d'instances régionales mais plus généralement au niveau international, et notamment :

- les activités du Conseil de l'Europe relatifs à la Convention 108 sur la protection des données, qui est à ce jour le seul accord régional sur la protection des données ;
- les travaux de révision des lignes directrices sur la protection de la vie privée de l'OCDE.

Par ailleurs, elle entretient des contacts réguliers sur ces questions avec ses homologues au sein des Conférences européennes et internationales des autorités de protection des données notamment sur les éventuels outils de coopération internationale qui pourraient être développés pour faciliter les actions répressives et l'échange de bonnes pratiques. La CNIL ira d'ailleurs prochainement à la rencontre de ses homologues de l'Asie Pacifique

(APPA) pour échanger sur l'impact du RGPD dans cette région, réfléchir sur les perspectives de coopération et le partage d'expertise.

Enfin, la CNIL suit l'adoption des réglementations de protection des données dans le monde, comme, à titre d'exemple, aux Etats-Unis avec l'adoption par l'Etat de Californie en juin 2018 d'une loi sur la protection des données personnelles, et des initiatives en vue l'adoption d'une loi fédérale sur la protection de la vie privée, ou encore au Brésil qui a adopté en août 2018 une loi sur la protection des données personnelles qui s'inspire du RGPD.