CONFERENCE DE PRESSE

27 mars 2017

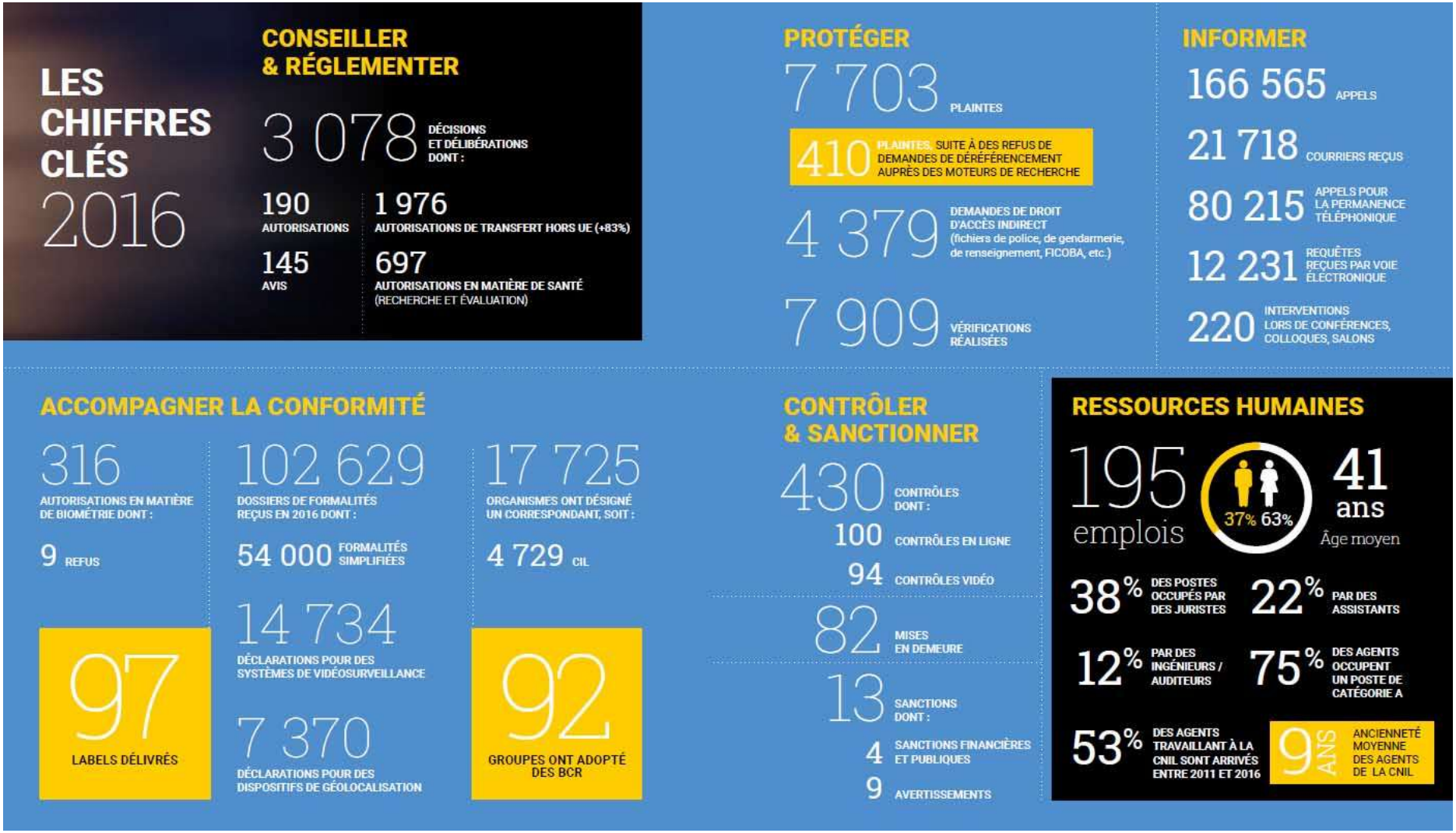
Présentation du 37ème

Rapport d'activité 2016

et des enjeux 2017

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Chiffres clés de l'année 2016



Temps forts 2016

Février

09/02
Mise en demeure publique à l'encontre de Facebook pour sa politique de confidentialité

Avril

08/04
Publication de la position de la CNIL en matière de chiffrement

Juin

15/06
Lancement de la consultation sur le règlement européen

Août

01/08
Entrée en vigueur du Privacy Shield

Octobre

08/10
La loi pour une république numérique est publiée au Journal Officiel

14/10
GOSSIP, les potins anonymes, mise en demeure pour atteintes graves à la vie privée

19/10
CDISCOUNT : avertissement et mise en demeure pour de nombreux manquements

27/10
Avertissement public pour le parti socialiste en raison de failles de données sensibles en ligne

28/10
L'avis de la CNIL sur le fichier TES est publié

Mars

24/03
Sanction de 100 000 € à l'encontre de Google qui ne procède pas au déréférencement sur l'intégralité des extensions du nom de domaine de son moteur de recherche

Mai

04/05
Parution au journal officiel de l'Union européenne du règlement européen sur la protection des données personnelles

Juillet

20/07
Mise en demeure à l'encontre de MICROSOFT concernant Windows 10

27/07
Les contrôles sur les cookies s'étendent au-delà des éditeurs de sites

29/07
Le G29 publie sa position sur le Privacy shield

Septembre

26/09
Le premier label coffre-fort numérique est délivré

27/09
Un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail

Novembre

08/11
La CNIL précise les règles que doivent respecter les candidats et partis quand ils utilisent des données issues des réseaux sociaux

Décembre

27/12
Publication des avis de la CNIL sur les décrets relatifs à l'utilisation des caméras piétons par les forces de l'ordre

29/12
Deux sites de rencontre sanctionnés pour défaut de consentement exprès

Bilan 2016 : une année d'activité intense marquée par l'adoption de deux textes majeurs pour les droits des personnes

L'année 2016 s'est traduite, une fois encore, par une activité intense et diversifiée, dans un contexte d'évolutions majeures en matière réglementaire qui impactent de façon considérable son fonctionnement ou ses missions. La CNIL doit ainsi faire face à l'afflux des demandes des particuliers et des professionnels, tout en préparant l'entrée en application du règlement européen le 25 mai 2018.

BILAN D'ACTIVITE 2016

1. La CNIL au service des citoyens

L'e-réputation et la prospection par courrier électronique : premiers motifs de plaintes

En 2016, la CNIL a reçu 7 703 plaintes, ce qui demeure un nombre élevé, dans des proportions presque semblables à l'année 2015, qui avait enregistré un record de plaintes (7900 en 2015).

- **33% 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 exercer son droit au déréférencement auprès du moteur de recherche. 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.

- **33% 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.

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

  - les ressources humaines (vidéosurveillance excessive, refus de communication du dossier professionnel) ;
  - la banque et le crédit (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 (difficultés à accéder au dossier médical ou social, création de dossiers pharmaceutiques sans consentement).

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

- **les objets connectés soulèvent des enjeux croissants** : jouets connectés (poupée connectée), voitures connectées (nature des données collectées, destinataires de ces données, absence d'information), compteurs communicants (15 plaintes, notamment de mairies, qui pointent un manque d'information sur l'installation des compteurs, les données collectées, leurs destinataires).
- **Le wifi tracking est de plus en plus utilisé pour suivre les personnes** : analyse de la fréquentation d'un lieu ; capteurs installés dans des commerces d'un centre-ville, capteurs au sein de magasins dans un centre commercial, de gare, aéroport pour analyser le parcours des usagers, la fréquentation d'un lieu, l'audience des dispositifs publicitaires.
- **La vidéosurveillance au travail :** les employeurs visualisent à distance via leur smartphone/tablettes leurs salariés pour diriger l'activité, surveiller voire critiquer les pratiques.
- **Les télé services d'inscription aux lycées et aux établissements d'enseignement supérieur (AFFELNET et APB)** suscitent des plaintes ou saisines de la CNIL sur l'opacité sur les critères de sélection des candidats et sur le fonctionnement de l'algorithme.

Gros plan sur le droit au déréférencement : un droit qui a fait ses preuves !

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.

Près de trois ans après la décision de la CJUE de mai 2014, le droit au déréférencement rencontre un vif engouement auprès des Français pour lesquels contrôler leur réputation sur internet constitue une préoccupation grandissante. En effet, sur les 700 000 demandes reçues par Google depuis cette date, 225 000 concernent la France, soit 32%. **Dans 43% des cas, Google supprime les URLs concernées**.

En 2016, la CNIL a reçu plus de 400 plaintes de personnes physiques qui se sont vu opposer un refus à une demande de déréférencement effectuée auprès d'un moteur de recherche. Les personnes demandent principalement la suppression de liens (URLs) diffusés sur des annuaires, des blogs, pages web perso, des annuaires, des sites marchands, des sites de presse et des réseaux sociaux. Au total, **plus de 1000 plaintes ont été reçues par la CNIL depuis juin 2014**.

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). Quand les plaintes sont recevables, la CNIL les analyse sur la base des critères communs élaborés par le G29 (groupe des CNIL européennes).

Elle est intervenue auprès des moteurs de recherche pour leur demander un déréférencement pour 30% des dossiers traités. Ces demandes ont été suivies d'effets dans 75% des cas. Le solde est soit encore en cours de traitement, soit donne lieu à de nouveaux échanges entre la CNIL et les moteurs de recherche.

Une augmentation des demandes d'accès au fichier TAJ (Traitement des antécédents judiciaires)

En 2016, la CNIL a reçu **4 379 demandes de droit d'accès indirect**. Ces demandes reçues représentent un total de 8101 vérifications à mener concernant par ordre d'importance : le fichier TAJ des antécédents judicaires de la police et de la gendarmerie, le fichier FICOBA de l'administration fiscale, et les fichiers de renseignement.

54 % des demandes reçues ont porté sur le fichier TAJ (2167 demandes), ce qui représente une augmentation de 34% par rapport à 2015. Cette évolution est liée au contexte de l'état d'urgence (perquisitions administratives, assignations à résidence, retrait de badges aéroportuaires ou de cartes professionnelles). Le renforcement des effectifs au sein des forces de sécurité depuis les attentats de 2015 (création annoncée de 8 500 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.

La croissance s'explique aussi par la réception en 2016 de 400 demandes de ressortissants français souhaitant travailler sur le territoire suisse dans le domaine de la sécurité. En effet, les autorités de cet Etat ont imposé à ces personnes d'exercer leur droit d'accès indirect auprès de la CNIL pour obtenir les données issues du fichier TAJ dans le cadre d'une enquête préalable de moralité. Cette situation a été régularisée à la fin de l'année 2016 par une modification de l'article R. 40-29 du code de procédure pénale, pris après avis de la CNIL, qui permet désormais aux 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.

2. La CNIL conseille les pouvoirs publics

En 2016, la CNIL a rendu 3078 décisions et délibérations dont **145 avis** portant notamment sur différents champs d'activité :

- **La régulation du numérique** : 6 décrets d'application de la loi pour une République numérique ;
- **La santé** : le dossier médical partagé, les conditions d'échange et de partage d'informations entre professionnels de santé et professionnels des champs social et médico-social, le dossier médical partagé, la mise en œuvre du système national d'information interrégimes de l'assurance maladie (SNIIRAM), la création du système national des données de santé (SNDS) ;
- **La sécurité** : la vidéoprotection de cellules de détention, la lutte contre le financement du terrorisme, le traitement (TES) relatif aux passeports et aux cartes nationales d'identité, les caméras piéton utilisées par les forces de l'ordre et la police municipale ;
- **L'emploi** : le « Système d'information du Compte personnel d'activité » (SI-CPA), la dématérialisation des bulletins de paie ;
- **Divers** : le chèque énergie, la création du fichier des contrats de capitalisation et d'assurance vie dénommé « FICOVIE », le téléservice Bloctel pour la gestion de la liste d'opposition au démarchage téléphonique…

La CNIL a également participé à une trentaine d'auditions parlementaires.

3. La CNIL accompagne les entreprises

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, 18 000 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.

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. Aujourd'hui 6 packs de conformité ont été lancés : compteurs communicants, assurance, secteur social, banque, véhicule connecté et *Open data*.

Les labels
97 labels ont été délivrés depuis 2012.
En 2016, la CNIL a attribué son premier label « coffre-fort numérique » et a reçu les premières demandes de renouvellement pour les labels « audit » et « formation ».

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

Les contrôles

La CNIL a réalisé **430 contrôles** en 2016, dont **:**

- **300 contrôles sur place (dont 94 contrôles portant sur des dispositifs vidéo)**.
- **100 contrôles en ligne**
- **30 contrôles sur pièces et sur convocation**, adaptés notamment aux organismes établis hors de France

La combinaison de différents modes d'intervention a été mise en œuvre avec succès dans de nombreuses missions relatives à des **problèmes de sécurité de données** (failles de sécurité ou fuites de données). Après un contrôle en ligne figeant la preuve de manquements, des agents habilités se déplacent auprès de l'organisme concerné pour procéder à des constatations complémentaires. Une vingtaine d'opérations de ce type ont pu être menées en 2016, et ont d'ores et déjà donné lieu à 4 avertissements, dont un public.

Les contrôles ont été réalisés sur de nombreuses thématiques :

- le paiement sans contact ;
- les risques psychosociaux en entreprise ;
- le système national des permis de conduire ;
- le SNIIRAM (système national d'information inter-régimes de l'assurance maladie) ;
- les data brokers (courtiers en données).

Les irrégularités récurrentes en matière de vidéoprotection portent sur :

- l'autorisation préfectorale (défaut d'autorisation ou autorisation expirée) ;
- l'information du public (panneaux absents, peu lisibles ou incomplets) ;
- la sécurité (accès aux images et aux enregistrements insuffisamment protégé).

Au programme 2017

- **La confidentialité des données de santé traitées par les sociétés d'assurance** : les sociétés d'assurance recueillent des données relatives à l'état de santé de leurs clients, dans le cadre de nombreux contrats. Ces données constituent un élément essentiel d'évaluation du risque qui conditionne l'engagement de l'assureur. Elles sont également recueillies lorsqu'un assuré demande l'indemnisation d'un sinistre relatif à son état de santé. Cette thématique permettra de s'assurer de la conformité des sociétés d'assurance aux règles de confidentialité des données de santé et au respect du secret médical, deux ans après l'adoption du pack de conformité assurance.
- **Les fichiers de renseignement** : plusieurs fichiers intéressant la sûreté de l'Etat, la défense ou la sécurité publique feront l'objet de vérifications de la CNIL. Il s'agit notamment des fichiers de prévention des atteintes à la sécurité publique autorisés par décret et mis en œuvre par les services du ministère de l'Intérieur, dans lesquels ont été versés les anciens dossiers des renseignements généraux: **PASP** (Prévention des Atteintes à la Sécurité Publique), **GIPASP** (Gestion de l'Information et Prévention des Atteintes à la Sécurité Publique) et **EASP** (Enquêtes Administratives liées à la Sécurité Publique). Des vérifications porteront également sur le fichier **STARTRAC**, lui-aussi autorisé par décret et comprenant les déclarations de soupçons de blanchiment d'argent transmises au service à compétence nationale TRACFIN.
- **Les télévisions connectées (« Smart TV »)** : la télévision connectée offre de nouveaux services aux téléspectateurs, comme la télévision de rattrapage, la vidéo à la demande ou l'accès aux plateformes de vidéos en ligne. Elle permet à l'usager d'interagir au moyen de nombreux supports sur les réseaux sociaux. Certains modèles dotés de technologies de reconnaissance vocale permettent d'analyser la voix de l'utilisateur afin d'exécuter ses instructions. Les informations recueillies sont susceptibles de révéler de nombreux aspects de la vie privée des utilisateurs, en particulier leurs habitudes de vie. Les contrôles prévus porteront sur les traitements de données collectées par les télévisions connectées, en particulier la pertinence des informations recueillies, la finalité des traitements effectués ainsi que les mesures de sécurité et de confidentialité mises en œuvre.

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.** 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.

82 mises en demeure ont été adoptées en 2016 dont plusieurs portaient sur les cookies, sites de vente en ligne ou d'annonces d'emploi, associations caritatives. 70 mises en demeure relevaient **des manquements à la sécurité.**
La mise en demeure publique pour atteinte grave à la vie privée à l'encontre de l'application Gossip qui s'est doublée d'une dénonciation au Parquet, s'est finalement clôturée du fait de la fermeture de l'application, qui n'est plus utilisable.
13 sanctions ont été prononcées par la formation restreinte, dont 4 sanctions pécuniaires. 9 sanctions concernaient **des manquements à la sécurité**.

Le montant maximum des sanctions a été porté de 150 000 euros à 3 millions d'euros par la loi pour une République numérique du 7 octobre 2016. Ce montant ne peut concerner que les manquements constatés après cette date.

Le règlement fixe quant à lui un montant pouvant aller jusqu'à 4% du chiffre d'affaires mondial pour les entreprises ou 20 millions d'euros.

L'ADOPTION DE DEUX TEXTES MAJEURS QUI RENFORCENT LES DROITS DES PERSONNES A L'ERE NUMERIQUE

1. La loi pour une République numérique

La loi pour une République numérique du 7 octobre 2016 constitue une réelle avancée pour la protection des droits des personnes. Elle complète l'article 1er de la loi Informatique et Libertés et prévoit que :

« Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

En inscrivant ce droit à « l'autodétermination informationnelle », la loi réaffirme qu'à l'ère numérique, la personne est le centre de gravité de la législation sur la protection des données et renforce la maîtrise par celle-ci de ses données.

En effet, la loi reconnait aux personnes :

- la possibilité d'organiser le sort de ses données après la mort ;
- un droit à l'oubli renforcé pour les mineurs ;
- plus d'information et de transparence sur le traitement des données ;
- la possibilité d'exercer ses droits par voie électronique.

2. Le règlement européen

Le règlement européen sur la protection des données personnelles est paru le 27 avril 2016 et entrera en application le 25 mai 2018. Il conforte lui aussi le caractère central de la personne et renforce la maîtrise par l'individu de ses données. Il s'appliquera dès lors qu'un résident européen sera substantiellement affecté par un traitement de données. Les acteurs mondiaux seront donc soumis au droit européen dès lors qu'ils offrent un produit ou un service à un citoyen européen, même à distance. **Ce critère, dit du « ciblage »**, constitue une évolution profonde : désormais, la territorialité du droit européen de la protection des données se construit autour de la personne, et non plus seulement autour du territoire d'implantation des entreprises.

De plus, le règlement reconnait aux personnes :

- une information plus claire et accessible ;
- une protection des enfants renforcée avec un recueil du consentement auprès des parents ;
- un nouveau droit à la portabilité qui permet de récupérer ses données sous une forme aisément réutilisable et de le transférer ensuite à un tiers ;
- le droit à réparation d'un dommage matériel ou moral, notamment dans le cadre d'actions collectives.

Données personnelles et campagnes électorales

L'activité politique, notamment pour les campagnes électorales, n'échappe pas à la numérisation : prospection ciblée, réseaux sociaux, risques de failles de sécurité sur internet. Les partis et candidats politiques doivent donc intégrer la protection des données dans leurs obligations vis-à-vis des citoyens.

La CNIL a créé dès 2012 un « **observatoire des élections** ». Cette petite structure interne, réactivée pour chaque campagne électorale, a pour mission :

- d'informer les candidats et partis de leurs obligations, et de les accompagner dans leur mise en conformité ;
- d'informer les électeurs de leurs droits « Informatique et Libertés » ;
- de recueillir les signalements des électeurs pour réagir rapidement en cas de manquement à la loi « Informatique et Libertés ».

A l'issue des élections présidentielles et législatives, la CNIL dressera le bilan de cette activité pour, le cas échéant, proposer des pistes d'amélioration aux pouvoirs publics s'agissant du cadre juridique existant en matière de protection des données personnelles traitées à des fins de communication politique.

Accompagner les partis et candidats

Afin d'expliciter les règles applicables, la CNIL a, dès 2012, adopté **une recommandation** relative à la communication politique, après consultation des principales formations politiques. Elle a également publié un **guide pratique**, constitué de fiches pratiques qui peuvent guider les partis et candidats dans la mise en place d'outils conforme à la loi « Informatique et Libertés ».

Plus récemment, afin de faciliter l'accès aux règles en matière de communication politique, la CNIL a élaboré **un guide commun avec le Conseil supérieur de l'audiovisuel (CSA)**.

Enfin, elle a explicité **les principes applicables à l'utilisation de logiciels de prospection politique, et au recours aux données issues des réseaux sociaux**. Ce travail est l'aboutissement d'une réflexion amorcée au premier semestre 2015 avec l'audition des principaux concepteurs de logiciels de prospection politique.

Le suivi de la campagne pour les élections présidentielles et législatives

Outre le suivi des primaires, qui a notamment permis à la CNIL de s'assurer de la destruction des listes des votants, la CNIL a adressé un courrier de sensibilisation à tous les candidats figurant sur la liste officielle arrêtée par le Conseil constitutionnel, notamment sur les questions relatives à la sécurité des données. Elle répond aux demandes de conseils qui lui sont adressées par ceux-ci.

Les enjeux pour 2017 (1) : sécuriser le passage au règlement pour les professionnels

Le règlement européen sur la protection des données, qui entrera en vigueur le 25 mai 2018, renouvelle profondément le cadre juridique applicable en matière de protection des données. Les organismes publics et privés doivent donc se préparer à ce nouveau cadre juridique. La CNIL leur propose un accompagnement pour leur permettre de comprendre ce que change le règlement mais aussi pour conduire la transition en interne de manière méthodique.

Une évolution substantielle du cadre juridique

La protection des données est actuellement régie par la directive 95/46/CE du 24 octobre 1995 et la loi du 6 janvier 1978. Si cette législation a fait la preuve de la solidité et de la pertinence de ses principes (principe de finalité, proportionnalité, légitimité du traitement, droits des personnes), elle nécessitait plusieurs adaptations à l'univers numérique. C'est le sens du règlement européen adopté en 2016.

Ce 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. Ceux-ci doivent donc s'adapter avant le 25 mai 2018, date d'entrée en application de ce nouveau cadre.

Le règlement traduit un renforcement des droits des personnes à l'ère numérique.
Il conforte la place de l'individu au cœur du système juridique, technique et éthique de la protection des données en Europe et lui offre de nouveaux droits ou garanties :

- l'expression du consentement est renforcée, de même que l'information ;
- la protection des enfants est renforcée, le consentement des parents étant nécessaire dans de nombreux cas ;
- les personnes peuvent récupérer leurs données sous un format aisément réutilisable : c'est le **droit à la portabilité des données.**

L'ensemble de ces éléments concourt à un même objectif : donner à la personne les moyens de mieux maîtriser le devenir de ses données.

Le règlement impose une adaptation rapide des organismes qui traitent des données

Le nouveau cadre applicable 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 *ab initio* une protection optimale des données et une minimisation de la collecte.

Les entités 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**, ces délégués étant les interlocuteurs de référence de la CNIL.

- **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 vie privée (EIVP) pour les traitements à risque,** sous le contrôle du régulateur ;

- **notifier les failles** de sécurité à la CNIL et, le cas échéant, aux personnes concernées.

Une adaptation accompagnée par la CNIL

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.

Afin d'aider les entreprises établies en France, qu'elles soient nationales ou transnationales, la CNIL met donc en place un dispositif d'accompagnement :

- supports d'information permettant de s'approprier plus facilement la nouvelle législation ;
- méthode pour se préparer à ce nouvel environnement en 6 étapes ;
- outils dédiés (notamment pour les études d'impact sur la vie privée) ;
- permanence juridique dédiée pour les CIL.

Au-delà, la CNIL va élaborer des référentiels qui permettront aux entreprises de connaître leurs obligations par secteur ou type d'activité, et ainsi de mettre en œuvre leurs traitements en toute sécurité. Ces référentiels seront portés par la CNIL au niveau européen pour que les entreprises installées en France puissent bénéficier d'un niveau exigence uniforme sur tout le territoire de l'Union.

Les enjeux de 2017 (2) : disposer impérativement d'une nouvelle loi Informatique et Libertés avant mai 2018

Le règlement européen comporte de très nombreux renvois au droit national. Par ailleurs, il n'est pas applicable à certains traitements de données, notamment les fichiers relatifs à la sécurité publique. Le Parlement devra donc adopter une nouvelle loi « informatique et libertés » pour tenir compte de ce nouvel environnement européen qui devra être impérativement adoptée avant le 25 mai 2018, sous peine de rendre très largement inapplicable le nouveau cadre de protection en France.

Le règlement européen comporte 57 mentions ou renvois au droit des Etats membres, donc au droit national. En outre, parallèlement au règlement, a été adoptée une directive applicable aux fichiers en matière de sécurité publique et de recherche et répression des infractions pénales (dite « police-justice »). Il est donc indispensable que le Législateur, en France, procède à une adaptation profonde de la loi « informatique et libertés » pour tenir compte de cette évolution et parachever l'environnement réglementaire, et transposer la directive « police-justice »

Concrètement, la loi devra comporter **plusieurs types de dispositions.**

- La loi devra tout d'abord **abroger une série d'articles** dont la substance est reprise par le règlement ou qui ne peuvent pas coexister avec celui-ci. Tel est notamment le cas de la plupart des articles relatifs aux définitions, règles et principes en matière de protection des données, ainsi que de la plupart des dispositions relatives aux droits des personnes et aux obligations des entreprises ;
- La loi devra ensuite **redéfinir les procédures applicables à la CNIL impactées par le règlement, notamment en matière répressive, afin de prévoir l'européanisation des procédures ;**
- **Le Législateur se prononcera également sur les règles applicables dans les matières pour lesquelles le règlement renvoie au droit des Etats membres.**

Le règlement fixe le cadre général applicable à l'ensemble des traitements de données à caractère personnel. Toutefois, compte tenu des spécificités de certaines données, ou de l'imbrication entre le droit de la protection des données et d'autres pans du droit (santé, etc.), le règlement européen renvoie, dans plusieurs hypothèses, au droit national.

Les renvois du règlement au droit national sont assez divers, rendant complexe une présentation synoptique. Le chapitre IX a pour objet d'énumérer des champs d'intervention dans lesquels les Etats membres peuvent préciser ou déroger au règlement : traitements journalistiques, traitements et accès du public aux documents officiels, traitement du NIR, traitement des données au travail, traitement des données à des fins de recherche historique, scientifique ou statistique, obligations de secret. Mais il existe aussi des dispositions disséminées, qui renvoie le soin aux Etats membres de fixer les mesures et garanties appropriées ou de compléter les règles existantes.

Les principales dispositions figurent :

- à l'article 9, relatif aux données sensibles : « Les Etats membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé » ;
- à l'article 10, relatif aux données relatives aux infractions ou condamnations pénales ;
- à l'article 36, sur les pouvoirs des autorités de contrôles sur les fichiers d'intérêt public ;

La loi devra enfin conserver un chapitre relatif à la composition, au fonctionnement et aux missions de la CNIL, qui vont d'ailleurs au-delà du champ du règlement européen.

Les enjeux de 2017 (3) : algorithmes, intelligence artificielle et éthique

La loi pour une République numérique du 7 octobre 2016 a confié à la CNIL la mission de conduire une réflexion sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques. Elle a choisi de consacrer les premières réflexions au thème des algorithmes et de l'intelligence artificielle en initiant un cycle national de débats publics, ateliers ou rencontres, dans une démarche associant de très nombreux partenaires.

Les algorithmes : de nombreuses questions éthiques pour des outils au cœur de nos vies

Résultats de requêtes sur un moteur de recherche, ordres financiers passés par des robots sur les marchés, diagnostics médicaux automatiques, affectation des étudiants à l'Université : dans tous ces domaines, des algorithmes sont à l'œuvre. Pourtant, la mise en œuvre de tels dispositifs pose de nombreuses questions éthiques, notamment en termes d'autonomie de l'individu, qu'il soit l'auteur d'une décision « aidée » par un algorithme ou qu'il en fasse l'objet.

Les Français en ont d'ailleurs une représentation inégale. Si **83 %** d'entre eux ont déjà entendu parler des algorithmes, ils sont plus de la moitié à ne pas savoir précisément de quoi il s'agit (**52%**). Leur présence est déjà jugée massive dans la vie de tous les jours par **80%** des Français qui considèrent, à **65%,** que cette dynamique va encore s'accentuer dans les années qui viennent. Concernant l'opinion sur les algorithmes, une courte majorité (**53%**) estime qu'ils sont plutôt sources d'erreur contre **47 %** qui pensent qu'ils sont fiables.

Les algorithmes, à l'heure de l'intelligence artificielle, suscitent donc **des questions complexes** :

- Sont-ils les « nouveaux décideurs » ?
- Faut-il repenser, face aux progrès de l'intelligence artificielle, la responsabilité des acteurs publics et privés qui y ont recours ?
- Les algorithmes ont-ils pour effet de nous enfermer dans une bulle informationnelle, mettant en danger ouverture culturelle et pluralisme démocratique ? Ou sont-ils au contraire un moyen d'accéder à des idées, contenus, données ou personnes inaccessibles ou invisibles jusqu'alors ?
- En un mot, quelle autonomie de l'individu dans un monde « algorithmé » ?

Faire des algorithmes l'objet d'un vaste débat public pour faire progresser la connaissance et la réflexion par la société civile s'impose donc comme une nécessité.

Un débat public décentralisé, initié par la CNIL

La CNIL a décidé d'initier un vaste processus de discussion collectif que feront vivre tous ceux – institutions publiques, société civile, entreprises – qui souhaitent y prendre part en organisant des débats et manifestations multiformes. Près d'une trentaine de partenaires ont ainsi décidé d'organiser des évènements divers (colloques, séminaires, ateliers), afin soit de sensibiliser le grand public, soit d'approfondir les questions éthiques soulevées par les algorithmes dans divers secteurs d'activité (santé, justice prédictive, éducation, etc.).

À l'automne 2017, la CNIL rendra publique la synthèse des échanges et des contributions. L'objectif est d'établir un panorama des défis et enjeux. Des pistes ou propositions pour accompagner le développement des algorithmes dans un cadre éthique pourront être présentées aux pouvoirs publics.