rapport d'activité

2015

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

PROTÉGER LES DONNÉES PERSONNELLES, ACCOMPAGNER L'INNOVATION, PRÉSERVER LES LIBERTÉS INDIVIDUELLES

CNIL
Commission Nationale de l'Informatique et des Libertés

La documentation Française

rapport d'activité **2015**

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

PROTÉGER LES DONNÉES PERSONNELLES,
ACCOMPAGNER L'INNOVATION,
PRÉSERVER LES LIBERTÉS INDIVIDUELLES

Prévu par l'article 11 de loi du 6 janvier 1978,
modifiée par la loi du 6 août 2004

Les chiffres clés de 2015

Conseiller & réglementer

2 571
DÉCISIONS ET DÉLIBÉRATIONS
dont :
- 244 autorisations
- 122 demandes d'avis

1 076
AUTORISATIONS DE TRANSFERT

50 339
FORMALITÉS SIMPLIFIÉES

Informer

34 367
COURRIERS REÇUS

136 251
APPELS TÉLÉPHONIQUES

250 INTERVENTIONS LORS DE CONFÉRENCES, COLLOQUES, SALONS.

Accompagner la conformité

96 323
DOSSIERS DE FORMALITÉS

12 463
DÉCLARATIONS POUR DES SYSTÈMES DE VIDÉOSURVEILLANCE

6 852
DÉCLARATIONS POUR DES DISPOSITIFS DE GÉOLOCALISATION

359
AUTORISATIONS EN MATIÈRE DE BIOMÉTRIE

73
LABELS DÉLIVRÉS

16 406
ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT soit 4.321 CIL
Plus de 1000 participants aux 34 ateliers CIL

78
GROUPES ONT ADOPTÉ DES BCR

Contrôler & sanctionner

510 CONTRÔLES DONT :
- 155 contrôles en ligne
- 87 contrôles vidéo

93 MISES EN DEMEURE

10 SANCTIONS DONT :
- 3 sanctions financières
- 7 avertissements

Protéger

7 908 PLAINTES, dont 36 % concernent internet

450 PLAINTES suite à des refus de demandes de déréférencement auprès des moteurs de recherche

5 890
DEMANDES DE DROIT D'ACCÈS INDIRECT (fichiers de police, de gendarmerie, de renseignement, FICOBA, etc).

8 784
VÉRIFICATIONS RÉALISÉES

Ressources humaines

192 POSTES

ÂGE MOYEN : **40** ANS
- 64 % : Femmes
- 36 % : Hommes
- 48 % des agents travaillant à la CNIL sont arrivés il y a 5 ans
- 71 % des agents occupent un poste de catégorie A

UNE ANCIENNETÉ MOYENNE DE
9 ANS ENVIRON

RAPPORT D'ACTIVITÉ 2015

Commission Nationale de l'Informatique et des Libertés

INTRODUCTION

1 ANALYSES

AVANT-PROPOS DE LA PRÉSIDENTE

La liberté envers et contre tout !

Isabelle Falque-Pierrotin,
Présidente de la CNIL

2015, C'EST AVANT TOUT LE CHOC, LA SIDÉRATION

L'année 2015 a commencé et s'est terminée dans la violence des attentats qui ont endeuillé la France. Il y aura bien un avant et un après 2015. Chacun d'entre nous a été intimement meurtri par la violence physique de ces attaques qui visaient nos valeurs démocratiques, c'est-à-dire ce qui nous unit et nous réunit et ce qui constitue le socle de notre identité française et européenne. Ces valeurs humanistes ont un sens tout particulier à la CNIL, auprès des 200 agents et 17 membres du Collège.

> « La CNIL a maintenu son cap, à la recherche d'un équilibre délicat entre des impératifs divers mais pas forcément antagonistes. »

Depuis, le curseur entre impératifs de sécurité et défense des libertés fondamentales s'est incontestablement déplacé. Dans ce contexte particulier, sous-tendu par une intense émotion, la CNIL a maintenu son cap, à la recherche d'un équilibre délicat entre des impératifs divers mais pas forcément antagonistes. Au-delà de leurs impacts individuels et collectifs, ces événements ont eu des effets très directs sur l'activité de la CNIL. En effet, la Commission a eu à se prononcer sur 14 textes (décrets d'application, projets de loi) en lien avec la lutte contre le terrorisme ou le renseignement. Si certains d'entre eux étaient déjà prévus, il est évident que les attentats ont accéléré leur mise en œuvre.

Concernant la loi sur le renseignement, le texte final a tenu compte de différents points que la CNIL avait soulignés dans son avis. Pour autant, et comme j'ai pu être amenée à le dire publiquement, la CNIL a regretté que les fichiers de renseignement ne soient pas soumis à un contrôle effectif a posteriori de leur régularité du point de vue de la loi Informatique et Libertés. Or, ce contrôle constitue une exigence fondamentale afin d'asseoir la légitimité de ces fichiers dans le respect des droits et libertés des citoyens.

> « Le plan stratégique doit dessiner un projet pour la CNIL, dans une période « extraordinaire », synonyme d'opportunités et de défis. »

Dans un autre registre et toute proportion gardée bien sûr, je qualifierai aussi de choc la décision de la Cour de Justice de l'Union Européenne du 6 octobre qui a invalidé le *Safe Harbor*. Cette décision a constitué un vrai séisme en Europe et aux Etats-Unis, pour les entreprises, les gouvernements, la Commission Européenne mais aussi les autorités de protection des données.

Sur le fond, la CJUE a relevé que les autorités publiques américaines peuvent accéder de manière massive et indifférenciée aux données transférées dans le cadre de la décision de Safe Harbor de juillet 2000, sans assurer de protection juridique efficace aux personnes concernées. Constatant que la Commission n'a pas recherché si les Etats-Unis « assurent » effectivement une protection adéquate, la Cour a prononcé l'invalidation de la décision d'adéquation. **La question de la surveillance massive et indiscriminée est donc au cœur de l'invalidation du *Safe Harbor* par la CJUE**, ce qui rejoint la position du G29 qui avait considéré qu'une telle surveillance était incompatible avec le cadre juridique européen et que les outils de transferts ne pouvaient constituer une solution à ce problème.

Les autorités européennes, sous l'égide du G29, se sont immédiatement mises en ordre de marche pour tirer les conséquences opérationnelles de cette décision majeure pour la protection des données de citoyens européens. Le 16 octobre, elles ont demandé aux Etats membres et aux institutions européennes d'engager, dans un délai de trois mois, les discussions avec les autorités américaines afin de trouver des solutions politiques, juridiques et techniques permettant de transférer des données vers le territoire américain dans le respect des droits fondamentaux. Force est de constater que ce sont d'abord les enjeux commerciaux qui ont capté l'attention des négociateurs qui ont semblé minorer voire ignorer, au moins dans un premier temps, la problématique centrale de la surveillance. Ce n'est donc seulement qu'à quelques heures de la date butoir du 31 janvier que l'esquisse d'un nouvel accord intitulé Privacy Shield a été annoncée.

Le G29 analysera ce nouvel accord à la lumière des garanties européennes essentielles rappelées par la CJUE. Il a déjà prévu de se réunir en séance plénière extraordinaire en avril prochain.

Dans le cas du Safe Harbor, les autorités de protection européennes doivent défendre une position commune européenne à la fois ferme et pragmatique, dans un univers d'une extrême complexité avec des enjeux économiques et politiques considérables. Car, ce dont il est question finalement, c'est bien **l'élaboration d'un standard mondial permettant de garantir aux citoyens européens une protection en continu sur leurs données et leurs droits, y compris quand elles quittent l'Europe.**

ET MAINTENANT, QUE DIRE DE 2016 ?

2016 sera assurément une année délicate, où tout peut arriver. Dans ce contexte instable, il est essentiel de fixer un cap et de le maintenir car, comme 2015 en témoigne, la stabilité ne viendra pas de l'extérieur, loin s'en faut. Ce cap, c'est le plan stratégique 2016-2018 de la CNIL qui le fixera. Son élaboration a donné lieu à un processus collaboratif associant l'ensemble des agents afin d'alimenter la réflexion collective.

Ce plan stratégique triennal doit permettre à la CNIL, non seulement de poursuivre les évolutions déjà engagées mais aussi de dessiner un projet pour une période que l'on peut qualifier « d'extraordinaire », synonyme d'opportunités et de défis.

Le premier défi consiste à assurer la transition vers le règlement européen et l'européanisation de certaines activités de la CNIL. Le règlement européen tant attendu va être finalement voté au printemps. Son adoption en décembre 2015 constitue un aboutissement de quatre années de travail et de négociations intenses et marque un tournant majeur dans la régulation des données personnelles. En effet, nous passerons d'un cadre national à un cadre prioritairement européen. Il faudra donc que ▸▸▸

▸▸▸ la CNIL intègre, dans l'ensemble de son fonctionnement, la dimension européenne de la régulation.

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

> « La CNIL est prête à se réinventer pour être plus agile, plus pragmatique. »

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

En introduisant un pouvoir de décision conjointe des autorités de protection des données de toute l'Union européenne, le règlement implique de systématiser la coopération, le partage d'information avec nos homologues. Il implique également de coopérer en amont, au stade de la conformité, afin de pouvoir fournir aux acteurs européens des outils harmonisés dont ils sont demandeurs (référentiels, labels, packs de conformité, etc.).

Le deuxième défi que la CNIL doit relever consiste à ancrer son action dans l'accompagnement et la facilitation de la transition numérique des acteurs économiques et publics. Ce tournant, bien que déjà engagé ces dernières années, s'accentuera dans les trois ans à venir. La CNIL doit accompagner le développement de la confiance dans les services numériques dans une logique de conformité et de respect des droits des personnes. Pour ce faire, elle sera plus ouverte sur l'extérieur et plus proche des acteurs de terrain, elle développera une doctrine plus « mobile » ainsi que de nouveaux outils pratiques (outils d'auto-évaluation, nouveaux labels ou référentiels, etc.).

Enfin, le dernier défi c'est de faire de la CNIL, la référence pour le grand public en matière de numérique. L'une des forces de la CNIL réside dans sa capacité à s'adresser à une communauté de publics très divers et notamment au grand public. Les citoyens sont toujours plus nombreux à s'adresser à la CNIL qu'ils identifient comme le service public de référence sur le numérique et un interlocuteur de confiance comme en témoignent les 7 900 plaintes reçues en 2015 (soit un nombre record), les 136 000 appels, les 4 385 requêtes électroniques via le bouton Besoin d'aide dont les questions/réponses ont été consultées 122 000 fois.

Le projet de loi pour une République Numérique conforte le rôle de la CNIL et prévoit de lui confier le soin d'organiser la réflexion sur l'éthique du numérique. Cette mission doit permettre d'associer la société civile à des débats publics sur les questions de société nouvelles posées par le numérique, et ce, au-delà du strict cadre des données personnelles. Cette nouvelle mission de réflexion, la CNIL ne l'entend pas la porter seule mais au contraire jouer un rôle de catalyseur du débat citoyen et d'animateur de communauté.

Tous ces défis sont immenses. Ils illustrent la mutation considérable de notre société qui est en cours du fait du numérique. **La CNIL est prête à relever ces défis et elle ne le fera pas seule.** Dans un univers numérique complexe, foisonnant, multiple et évolutif, elle partagera la charge de la régulation avec d'autres, en France et en Europe, en développant de la corégulation et de l'interrégulation.

Mais les questions ne sont pas seulement techniques, juridiques ou économiques. Elles n'intéressent pas seulement les professionnels ou les experts. Ce qui est en cause est le plus souvent une vision de la société, un choix de valeurs.

À ce titre, je voudrais dire que la CNIL est résolument au service des libertés. Dans le contexte actuel, **l'ensemble des agents et membres de la CNIL souhaite travailler avec toutes les composantes de la société et participer avec audace et détermination à la mise en place d'une société numérique à visage humain.** ■

> « Faire de la CNIL un véritable régulateur tourné vers ses publics. »

MOT DU SECRÉTAIRE GÉNÉRAL

La CNIL en 2015 : pour une régulation performante et de qualité

Édouard Geffray,
Secrétaire général

La CNIL avait, en 2012, arrêté un plan d'orientations stratégiques et opérationnelles pour les années 2012-2015. L'année 2015, dont le présent rapport annuel reflète l'activité et une partie des réflexions de fond, a donc été marquée par l'aboutissement de nombreux projets conformes à ces orientations : faire de la CNIL un véritable régulateur tourné vers ses publics, qu'il s'agisse d'informer et de protéger les droits des personnes, ou d'accompagner la mise en conformité des entreprises, administrations ou associations qui traitent des données.

Ce plan ambitieux était en avance de phase sur le projet de règlement européen, qui a fait l'objet d'un accord politique en décembre 2015 et est en cours d'adoption définitive. Il s'est traduit par l'évolution des métiers de la CNIL, notamment vers l'accompagnement de la mise en conformité. Comme les années précédentes, il a été conduit dans un environnement lui-même en forte évolution, que ce soit sous l'effet du progrès technologique, des bouleversements sociétaux induits par le numérique ou des nouvelles législations. Enfin, les évolutions et projets menés l'ont été dans un contexte marqué par la poursuite de la croissance de l'activité de l'institution. A titre indicatif, les plaintes reçues par la CNIL ont bondi de 36 % en un an, tandis que les autorisations adoptées ont, elles, augmenté de plus de 9 %. La Commission a pu, pour cela, s'appuyer sur la détermination et l'engagement des quelques 200 femmes et hommes qui composent ses services, et qui, animés de la conviction que protection des données personnelles et innovation vont de pair dans un Etat de droit, se sont attachés à rendre un service public performant et de qualité.

Pour le grand public, tout d'abord, la CNIL a mené à bien, au cours de l'année 2015, trois projets fondamentaux. Le premier est celui de la refonte du site internet : désormais adapté à tous les supports de consultations (smartphones, tablettes ou ordinateurs), il a été conçu pour répondre aux besoins spécifiques, soit des particuliers, soit des professionnels. Son lancement a été précédé par l'amélioration du téléservice des « plaintes ▸▸▸

en ligne » en avril 2015. Désormais, les personnes qui saisissent la CNIL sont accompagnées pour mieux comprendre leurs droits et mieux formuler leurs demandes. Enfin, la CNIL a développé un nouveau service, intitulé « Besoin d'aide », qui permet à tout internaute d'interroger une base de connaissances en langage naturel et d'obtenir ainsi les réponses aux questions les plus proches. En l'absence de réponse satisfaisante, il peut saisir la CNIL par courriel. Ce service a été interrogé, entre son lancement le 1er juillet et le 31 décembre 2015, plus de 122 000 fois, 4 385 personnes ayant sollicité des informations complémentaires par courriel. La base de questions-réponses est constamment enrichie pour apporter des réponses au plus près des besoins des personnes. Ces trois projets ont ainsi permis d'améliorer significativement le service aux publics.

La CNIL est en effet de plus en plus sollicitée par les particuliers, et est amenée à traiter de sujets de plus en plus complexes, qu'il s'agisse d'articuler protection de la vie privée et droit du public à l'information, comme en matière de déréférencement ou d'enjeux techniques complexes (comme en matière de cybersécurité).

Pour les acteurs du traitement des données, 2015 a également été l'année de la maturité des nouveaux outils de conformité de la CNIL, ce qui est essentiel dans la perspective du règlement européen. C'est ainsi que les labels ont confirmé leur ancrage dans les outils de conformité, avec les premiers renouvellements de ceux délivrés en 2012, mais aussi les premiers labels « gouvernance des données personnelles », qui valorisent les entités, publiques ou privées, qui optent pour une organisation interne vertueuse pour la protection des données. De la même manière, les CIL ont fêté leurs 10 ans, et passé, cette même année, la barre des 15 000 organismes pour atteindre 16 500 entités dotées de cette fonction.

Or, recourir à un CIL est aujourd'hui le meilleur moyen pour une entreprise ou une administration de se préparer au règlement européen sur la protection des données personnelles à venir. Le CIL est en effet le « chef d'orchestre » interne de la conformité à la loi informatique et libertés, et sera rendu obligatoire dans de nombreux cas en 2018, dans le cadre du règlement européen. Entreprises et administrations ont donc intérêt à se doter dès maintenant de CIL pour monter en puissance en vue du règlement européen, et bénéficier ainsi de l'accompagnement de la CNIL.

Enfin, les packs de conformité sont également ancrés dans le paysage de la conformité, et deux nouveaux packs sont envisagés en 2016 pour accompagner l'ouverture des données publiques et le développement des véhicules connectés dans le respect du droit à la protection des données.

S'agissant enfin des pouvoirs publics, la CNIL a été particulièrement sollicitée, dans le contexte de l'adoption de textes relatifs à la lutte contre le terrorisme. **Elle a ainsi reçu 122 demandes d'avis ou d'autorisations de la part d'administrations centrales de l'Etat**, et en dépit d'une forte hausse (+39 %), a réussi à diminuer les délais de traitements de plus de 10 %.

Le présent rapport annuel retrace l'ensemble de ces évolutions, non seulement quantitatives, mais également qualitatives. La CNIL se veut résolument tournée vers ses publics, dans un souci de qualité technique et juridique, et de performance. ■

> « 2015 a été l'année de la maturité des nouveaux outils de conformité de la CNIL. »

1

ANALYSES

Lutte contre le terrorisme et données personnelles : quelles garanties pour le citoyen ?

La série d'attentats tragiques qui a marqué l'année 2015 a naturellement conduit les pouvoirs publics à s'interroger sur les moyens et l'efficacité des services de renseignement. Le Gouvernement a ainsi pris plusieurs mesures visant à renforcer les moyens d'actions des services de renseignement, dont certaines intéressent directement la vie privée et la protection des données personnelles.

La CNIL a donc été particulièrement sollicitée durant cette année sur ces questions et sur les modalités d'articulation entre les impératifs de sécurité et de liberté qu'elles soulèvent. Dans ce cadre, son rôle est, au-delà d'une dichotomie réductrice entre sécurité et libertés, de s'assurer que des garanties, réelles et effectives, seules à même de garantir l'équilibre nécessaire au pacte républicain, accompagnent le renforcement des moyens mis à la disposition des services anti-terroristes et évitent toute atteinte disproportionnée au droit fondamental au respect de la vie privée.

LUTTE CONTRE LE TERRORISME ET PROTECTION DES DONNÉES PERSONNELLES : UNE LONGUE HISTOIRE

La lutte contre le terrorisme nécessite la collecte et l'analyse des informations pertinentes et, par conséquent, de données à caractère personnel. Le législateur est dès lors intervenu à de nombreuses reprises en cette matière, tant sur le volet judiciaire que sur le volet administratif de la lutte anti-terroriste, afin de prévoir les garanties légales propres à assurer une conciliation équilibrée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et le droit au respect de la vie privée. Ainsi, depuis les années 80 et jusqu'à l'adoption de la loi du 24 juillet 2015 relative au renseignement, **près d'une vingtaine de lois sont intervenues en la matière.** Parmi les plus substantielles, on peut citer la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, qui a notamment créé le dispositif des interceptions de sécurité (« écoutes administratives »), la loi du 23 janvier 2006 relative à la lutte contre le terrorisme (« LAT »), ou encore la loi du 18 décembre 2013 relative à la programmation militaire (« LPM »).

La LAT a en effet doté les services de renseignement de nombreux pouvoirs en posant les premiers jalons du cadre juri-

dique applicable aux réquisitions administratives des données de connexion, en permettant la mise en œuvre de dispositifs vidéo dans les lieux publics aux fins de prévention d'acte de terrorisme ou encore en autorisant la surveillance des déplacements des personnes susceptibles de participer à une action terroriste, aussi bien au niveau national (dispositifs de lecture automatisée des plaques d'immatriculation ou LAPI) qu'au niveau international, en autorisant la mise en œuvre de traitements de données recueillies à l'occasion de déplacements internationaux aériens.

La LPM a également permis un renforcement des moyens dont disposent les services de la « *communauté du renseignement* » en leur permettant d'accéder à certains traitements administratifs et judiciaires, en modifiant substantiellement le régime juridique applicable aux réquisitions administratives de données de connexion et en permettant, par exemple, la géolocalisation des terminaux mobiles des personnes en temps réel. Elle a en outre autorisé la mise en œuvre, à titre expérimental, du système « API-PNR France », qui permet la collecte des données relatives aux passagers aériens et leur utilisation par les agents de la police et de la gendarmerie nationales, des douanes, ainsi que des services de renseignement spécialisés, notamment à des fins de lutte anti-terroriste.

La CNIL s'est prononcée sur la plupart de ces dispositions législatives, ainsi que sur leurs textes réglementaires d'application. Elle a ainsi pu examiner la proportionnalité de ces différents dispositifs au regard du droit à la protection des données et faire état de ses analyses aux pouvoirs publics. Si ces observations n'ont pas toutes été suivies d'effets, un cadre juridique a été progressivement défini quant à l'utilisation des différents traitements de données à caractère personnel auxquels ont recours les services de renseignement. Ses évolutions témoignent en outre de l'accroissement des moyens de surveillance mis à disposition du renseignement ces dernières années.

RETOUR SUR L'ANNÉE 2015

L'année 2015 se caractérise par le nombre substantiel de mesures législatives et réglementaires adoptées concernant le traitement de données personnelles à des fins de lutte anti-terroriste, au premier rang desquelles figurent les nombreuses dispositions de la loi du 24 juillet 2015 relative au renseignement.

En outre, des dispositifs d'une nouvelle ampleur, en termes de volume de données traitées comme de modalités de collecte, ont été légalisés.

Du point de vue de la collecte et du traitement de données à caractère personnel, **trois tendances peuvent ainsi être observées :**

- la création de nouveaux fichiers ayant pour objet la lutte anti-terroriste, ou la modification de certains fichiers existants utilisés en la matière ;
- la surveillance et le contrôle des communications électroniques, y compris par l'utilisation de nouvelles techniques d'enquête et de recueil de données ;
- l'évolution du renseignement, avec la possibilité de collecter un volume important de données aux fins d'identifier les personnes à surveiller. La loi relative au renseignement contient en elle-même ces trois tendances.

> **En 2015, la CNIL s'est prononcée sur 14 projets de dispositions législatives ou réglementaires directement relatives au traitement de données à des fins de renseignement ou de lutte contre le terrorisme.**

La création de nouveaux fichiers et la modification de fichiers existants

À la suite des attentats de janvier 2015, le Gouvernement avait annoncé la création d'un nouveau fichier de suivi des personnes mises en cause ou condamnées pour des infractions liées au terrorisme. La CNIL s'est prononcée, le 7 avril 2015, sur un projet de dispositions législatives visant à créer un **fichier national des auteurs d'infractions terroristes (FIJAIT),** intégrées par voie d'amendement au projet de loi relatif au renseignement. Cet avis a été rendu public par le Gouvernement.

Les conditions de mise en œuvre de ce traitement sont très proches de celles du fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV), sur lequel la Commission s'est prononcée à plusieurs reprises et qui a fait l'objet d'un examen tant par le Conseil Constitutionnel que par la Cour européenne des droits de l'homme. L'objectif est en effet de disposer d'un fichier d'adresses des auteurs d'infractions liées au terrorisme, afin d'assurer un suivi de ces personnes au travers de différentes obligations (justification d'adresses, des déplacements à l'étranger, etc.).

Dans la mesure où des garanties identiques au FIJAISV ont été prévues pour le FIJAIT, la Commission a considéré que celles-ci étaient *a priori* de nature à assurer un équilibre entre le respect de la vie privée et la sauvegarde de l'ordre public. Elle a toutefois formulé plusieurs observations afin de limiter au strict nécessaire les atteintes aux droits et libertés fondamentaux.

▸▸▸

Ainsi, la CNIL a rappelé que la conservation d'adresses non mises à jour n'apparait pas utile au regard de la finalité de suivi des personnes concernées, ce qui est le cas des adresses conservées au-delà de la date de fin des obligations qui pèsent sur ces personnes, de même que la conservation, au-delà de cette date, de données qui pourraient déjà figurer dans d'autres fichiers judiciaires (TAJ et casier judiciaire, par exemple) ou de renseignement (tel CRISTINA). Sur les destinataires de ces informations, elle a estimé que les autorités judiciaires et les services spécialisés de renseignement ne devaient pouvoir accéder au FIJAIT que dans le seul cadre de leurs missions de lutte contre le terrorisme et que, s'agissant des préfets et administrations de l'État, le périmètre des enquêtes leur permettant de recevoir communication des données devait être précisé et restreint à certaines activités ou professions en lien avec les infractions pouvant donner lieu à une inscription dans le fichier.

DERNIÈRE MINUTE

Le FIJAIT créé par décret du 29 décembre 2015

Le 3 décembre 2015, la CNIL a été amenée à se prononcer sur le projet de décret d'application des dispositions législatives finalement adoptées relatives au FIJAIT. Elle a ainsi pu relever une diminution substantielle tant des durées de conservation des données que des durées des obligations incombant aux personnes inscrites dans le FIJAIT, tout en soulignant que, pour certaines des infractions concernées, les durées de conservation des données n'étaient pas similaires aux durées pendant lesquelles les personnes inscrites au FIJAIT sont soumises à ces obligations. La CNIL a ainsi pu rappeler qu'il appartenait au ministère concerné de prendre toutes mesures utiles pour que les données inexactes ou incomplètes soient rectifiées ou effacées, conformément à l'article 6-4° de la loi « Informatique et Libertés ». Le nouveau fichier national des auteurs d'infractions terroristes a finalement été créé par décret du 29 décembre 2015. La gestion de ce traitement est confiée au service du casier judiciaire national, sous l'autorité du ministre de la Justice et sous le contrôle d'un magistrat.

En avril 2015, la CNIL a également examiné un traitement, mis en œuvre par l'administration pénitentiaire, relatif *« au suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité publique »,* **dénommé « CAR »**. L'avis de la CNIL sur le projet de décret en portant création n'a pas été rendu public, car le ministère de la justice a entendu se prévaloir de plusieurs dérogations dont peuvent bénéficier les traitements intéressant la sécurité publique et la sûreté de l'Etat prévues par la loi du 6 janvier 1978 modifiée, et en particulier de l'absence de publication dudit décret et de l'avis de la CNIL correspondant. Néanmoins, il n'a pas exclu ce traitement du contrôle de la Commission. Ce traitement, finalement créé par décret du 10 novembre 2015 et qui est donc pleinement soumis à ses pouvoirs de contrôle, a bénéficié d'un avis « favorable avec réserve » de la CNIL.

En parallèle de la création de ces nouveaux traitements, plusieurs fichiers ont été modifiés en 2015.

Dans le cadre des débats parlementaires relatifs à la loi sur le renseignement, le Gouvernement a ainsi déposé un projet d'amendement visant à permettre aux services de renseignement de police et de gendarmerie d'accéder **au traitement des antécédents judiciaires (TAJ),** que la CNIL a déjà examiné à de nombreuses reprises. Pour rappel, le TAJ est le fichier d'antécédents commun à la police et à la gendarmerie nationales, qui s'est substitué aux fichiers STIC et JUDEX définitivement supprimés.

La CNIL s'est prononcée sur les dispositions législatives projetées, le 7 mai 2015, puis sur le décret d'application prévu par la loi relative au renseignement, le 10 décembre. Le cadre juridique de l'accès au TAJ par les services de renseignement spécialisés ainsi que par les services concourant à la mission de renseignement a ainsi été substantiellement modifié : pour la protection des intérêts fondamentaux de la Nation, ces services peuvent dorénavant prendre connaissance des données relatives à l'ensemble des procédures judiciaires donnant lieu à enregistrement dans le TAJ, y compris aux procédures en cours et aux procédures ayant donné lieu à une mention, à l'exclusion toutefois des données relatives aux victimes.

Le traitement **dénommé « FSPRT »** a également fait l'objet de modifications. Tout comme le traitement CAR, les décrets relatifs à ce fichier ne font pas l'objet d'une publication mais le pouvoir de contrôle de sa mise en œuvre par la CNIL n'a pas été écarté par le Gouvernement. Si les caractéristiques du traitement initial lui avaient permis de rendre un avis « favorable » fin 2014, la CNIL s'est montrée plus réservée sur les modifications qui lui ont été présentées, ce qui l'a conduit à rendre un avis « favorable avec réserve » à ces modifications, actées par décret du 30 octobre 2015.

Enfin, les conditions de mise en œuvre de quatre autres fichiers ont été modifiées cette année dans le cadre de l'application de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

Cette loi a en effet créé les dispositifs d'interdiction de sortie du territoire et d'interdiction administrative du territoire. L'adoption de ces nouvelles mesures a nécessité la modification du **fichier des personnes recherchées (FPR), du traitement automatisé de données à caractère personnel relatif aux passeports (TES), du traitement relatif aux cartes nationales d'identité sécurisées (FNG) ainsi que du fichier des objets et des véhicules signalés (FOVeS).**

La CNIL a ainsi été saisie d'un projet de décret portant amélioration des échanges d'informations entre services dans le cadre de la lutte contre le terrorisme. Celui-ci visait à tenir compte du dispositif d'interdiction de sortie du territoire, qui emporte, dès son prononcé et à titre conservatoire, l'invalidation du passeport et de la carte nationale d'identité, en permettant la transmission aux autorités policières des Etats européens la transmission des informations relatives à ces titres. Ce décret visait également à permettre l'inscription au FPR des personnes faisant l'objet d'une interdiction de sortie du territoire et des étrangers faisant l'objet d'une interdiction administrative du territoire. La CNIL s'est prononcée sur ce décret, publié le 15 février 2015, par délibération du 29 janvier 2015.

Le FOVeS a également été modifié, par arrêté du 18 février 2015 pris après avis de la CNIL, afin de permettre l'enregistrement des décisions d'invalidation de documents prononcées par les autorités administratives. Tout comme pour les trois autres fichiers concernés (FPR, TES et FNG), la Commission a notamment rappelé l'importance de s'assurer de la mise à jour des données figurant dans ce traitement afin de prendre en compte, dans les meilleurs délais, tout changement dans la situation des personnes ou des objets inscrits ou signalés dans ces fichiers. La mise à jour rapide et effective des quatre fichiers concernés est en effet nécessaire afin de limiter les conséquences défavorables qui résulteraient du maintien, dans ces fichiers, de personnes ne remplissant plus les conditions pour y être enregistrées.

La surveillance d'Internet et des communications électroniques

L'utilisation croissante, par les citoyens, des moyens de communication électroniques, et tout particulièrement d'Internet, a conduit le législateur à adopter plusieurs dispositions ces dernières années en matière de contrôle et de surveillance de ces moyens par les services en charge de la lutte contre le terrorisme.

La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a ainsi autorisé le **blocage et le déréférencement administratifs des sites Internet provoquant à des actes de terrorisme ou en faisant l'apologie,** renforçant un arsenal législatif important en matière de lutte contre ce phénomène, régulièrement complété et sur lequel la Commission a pu se prononcer à plusieurs reprises.

De manière générale, ces mesures administratives, précisées par deux décrets du 5 février et du 4 mars 2015 pris après avis de la CNIL, permettent d'associer directement les prestataires techniques dans la lutte contre le terrorisme et de bloquer ou déréférencer des sites ne faisant pas l'objet d'investigations judiciaires. Afin de garantir le respect des libertés individuelles, la loi prévoit qu'une personnalité qualifiée, désignée par la CNIL en son sein, s'assure de la régularité de ces différentes demandes et des conditions d'établissement, de mise à jour, de transmission et d'utilisation de la liste des sites faisant l'objet d'une mesure de blocage.

INFO +

Monsieur Alexandre Linden, commissaire au sein de la CNIL, a été désigné le 29 janvier comme personnalité qualifiée chargée du contrôle de la mise en œuvre de ce nouveau dispositif. La loi pour la confiance dans l'économie numérique, modifiée par la loi précitée du 13 décembre 2014, prévoit que cette personnalité doit rendre chaque année un rapport public d'activité, distinct du rapport annuel de la CNIL, sur les conditions d'exercice et les résultats de son activité, remis au Gouvernement et au Parlement.

Un an auparavant, la LPM avait été l'occasion de modifier le régime juridique applicable aux accès administratifs aux données de connexion, afin d'élargir les modalités d'accès à ces données par les services anti-terroristes.

La loi relative au renseignement a néanmoins constitué un tournant s'agissant de la surveillance des communications électroniques. En effet, son principal objet, du point de vue de la protection des données personnelles, a été d'autoriser ou de légaliser de **nouvelles modalités de collecte, pour certaines déjà utilisées par les services de renseignement, des données transitant sur les réseaux électroniques.**

La création de plusieurs « techniques de recueil du renseignement », dorénavant encadrées par les dispositions du code de la sécurité intérieure (CSI), a ainsi consacré l'importance majeure des outils de surveillance de ces réseaux dans le cadre de la lutte contre le terrorisme. Comme l'a rappelé la CNIL dans son avis du 5 mars 2015 sur le projet de loi, rendu public à la demande du Président de la Commission des Lois de l'Assemblée Nationale, ces dispositions ont en outre permis la mise en œuvre de mesures de surveillance beaucoup plus larges que celles autorisées ces dernières années.

Les conditions de **réquisition « classique » des données de connexion** ont ainsi été modifiées, en allongeant substantiellement leur durée de conservation par les services de renseignement : initialement conservées pendant un an, puis trois ans avec la LPM, elles peuvent dorénavant être conservées cinq ans par ces services. Les **interceptions de sécurité,** c'est-à-dire les écoutes administratives des contenus des conversations électroniques (téléphone, mail, chat, etc.), ont été étendues aux personnes appartenant à l'entourage des personnes surveillées.

La loi relative au renseignement a en outre étendu aux services de renseignement l'emploi de moyens déjà autorisés dans la cadre de la police judiciaire et ▸▸▸

autorisé l'usage de nouvelles techniques.

Par exemple, elle a prévu la possibilité de **nouveaux dispositifs techniques permettant d'accéder à des données informatiques** stockées dans un système informatique, qui s'affichent sur l'écran d'un utilisateur, que celui-ci introduit par saisie de caractères ou encore qui sont reçues et émises par des périphériques audiovisuels. Ces « key-loggers », que peuvent utiliser dans certaines procédures les autorités judiciaires, permettent ainsi de collecter toutes les données informatiques produites ou reçues par une personne sur son terminal électronique.

Les dispositions du CSI autorisent la pose de **« sondes »** qui permettent de recueillir les informations traitées par les opérateurs relatives à une personne préalablement identifiée comme présentant une menace. Ce recueil s'effectuera en temps réel et directement sur sollicitation du réseau des opérateurs de communications électroniques.

Elles permettent en outre l'installation, chez les opérateurs, de dispositifs permettant de détecter, par surveillance du trafic, des connexions susceptibles de révéler une menace terroriste. Ces **« boîtes noires » ou « traitements algorithmiques »** visent ainsi à détecter des signaux dits faibles de préparation d'un acte de terrorisme à partir de critères préétablis.

Des appareils permettant de capter à distance les données de connexion comme les correspondances échangées pourront également être utilisés par les services de renseignement. Ces **« IMSI-catchers »** constituent en pratique de fausses antennes relais, installées à proximité (de l'ordre d'une centaine de mètres, dans l'état actuel des techniques) de la personne dont on souhaite intercepter les échanges électroniques, afin de capter l'ensemble des données transmises entre le périphérique électronique et la véritable antenne relais.

Dans son avis sur le projet de loi, la Commission a observé que, parmi ces techniques, certaines sont susceptibles de conduire à une surveillance massive et indifférenciée des personnes.

Elle a rappelé que de telles atteintes au droit au respect de la vie privée, et notamment de la protection des données à caractère personnel, peuvent être justifiées au regard de la légitimité des objectifs poursuivis et des intérêts en cause et que les outils nécessaires à l'exercice des missions des services de renseignement doivent être adaptés aux nouvelles formes d'actions des personnes et organismes menaçant ces principes fondamentaux.

Néanmoins, elle a rappelé que les atteintes portées au respect de la vie privée doivent être limitées au strict nécessaire. Elles doivent être adéquates et proportionnées au but poursuivi et des garanties suffisantes doivent être prévues pour en encadrer et contrôler la mise en œuvre.

À cet égard, si la CNIL a pu relever plusieurs garanties dans le projet qui lui a été soumis, elle a formulé de nombreuses observations complémentaires, en particulier concernant les mesures de surveillance des communications électroniques, afin que ces dernières soient davantage encadrées. De fait, plusieurs de ses propositions ont été prises en compte et intégrées dans la loi finalement adoptée, sensiblement différente du projet de loi qui lui avait été soumis.

D'une surveillance individuelle ciblée à l'identification de personnes considérées comme « à surveiller » : un changement d'échelle en matière de renseignement

Au-delà des mesures concrètes adoptées en 2015 par le législateur ou le pouvoir réglementaire, la Commission a constaté, dans sa délibération sur la loi relative au renseignement, que les mesures de surveillance ne portent plus uniquement sur des personnes identifiées comme présentant une menace terroriste : elles peuvent également reposer sur la collecte généralisée et indifférenciée d'un volume important de données, parmi lesquelles les services de renseignement devront ensuite identifier les données utiles à l'accomplissement de leur mission.

À titre d'exemple, si les conditions exactes de mise en œuvre des « boîtes noires » ne sont pas encore connues, ces dispositifs reposent sur un postulat : **identifier les personnes présentant une menace nécessite de collecter et traiter les données d'un groupe plus large, en l'espèce des utilisateurs des réseaux de communications électroniques.**

En effet, ces traitements de détection des connexions obligeront les opérateurs, non plus seulement à conserver les données qui transitent par leurs réseaux aux fins de leur éventuelle mise à disposition des autorités, mais à exploiter les informations relatives à toutes les communications répondant aux paramètres établis par les services de renseignement. De nombreuses données, principalement relatives à des personnes ne présentant aucune menace pour la sûreté de l'Etat, seront donc concernées par ces dispositifs.

Il est donc nécessaire que ces évolutions soient encadrées par des garanties permettant d'assurer une réelle protection des données.

QUELLES GARANTIES POUR LES CITOYENS ?

Des garanties substantielles contenues dans la loi relative au renseignement

La CNIL avait souligné, dans son avis du 5 mars 2015, certaines mesures de nature à limiter les atteintes disproportionnées à la vie privée des citoyens, au premier rang desquelles figurent la délimitation du périmètre des activités des services de renseignement, la définition de leurs missions, des techniques qu'ils peuvent mettre en œuvre et des conditions de contrôle *a priori* et *a posteriori* de ces mesures. Des garanties supplémentaires ont ensuite été prévues dans le cadre des travaux parlementaires, reprenant pour partie les recommandations de la CNIL.

Le projet de loi finalement adopté a été examiné par le Conseil constitutionnel, qui a estimé que, à l'exception des mesures de surveillance internationale et des procédures dites « d'urgence opérationnelle », les dispositions relatives aux techniques de recueil du renseignement prévoient des moyens d'encadrement suffisants au regard des principes constitutionnellement garantis (droit au respect de la vie privée, liberté de communication et droit à un recours juridictionnel effectif) et ne portent dès lors pas d'atteinte disproportionnée à ces droits fondamentaux.

Ces dispositions ont donc été déclarées conformes à la Constitution, notamment au regard des garanties principales suivantes :

- les finalités précises pour lesquelles chacune de ces techniques peut être mise en œuvre, les techniques les plus intrusives ne pouvant être mises en œuvre que pour certaines de ces finalités ;
- le respect du principe de subsidiarité pour la mise en œuvre de ces techniques, certaines n'étant autorisées que lorsque les renseignements ne peuvent être recueillis par un autre moyen ;
- les modulations de leurs conditions exactes de mise en œuvre, permettant d'assurer la proportionnalité des mesures : en ce qui concerne leurs modalités et leurs durées d'autorisation de mise en œuvre, les durées d'exploitation et de conservation des informations recueillies, les lieux dans lesquels les dispositifs techniques peuvent être installés ou encore les catégories de personnes faisant l'objet de telles mesures (avocats, parlementaires, etc.) ;
- la possibilité de mettre en œuvre de telles techniques réservée aux seuls agents individuellement désignés et spécialement habilités ;
- le contrôle hiérarchique sur les autorisations de mise en œuvre de ces techniques, qui relèvent du Premier ministre ;
- le contrôle exercé par une nouvelle autorité administrative indépendante, la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR), notamment chargée d'examiner préalablement toute demande d'autorisation d'une telle technique et de contrôler la mise en œuvre de cette dernière ;
- l'indépendance de la CNCTR et l'effectivité de son contrôle ;
- la possibilité pour toute personne de saisir la CNCTR et le Conseil d'Etat aux fins de vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard.

Ainsi, le législateur a soumis les techniques de renseignement à **deux types de contrôle,** le premier exercé par la CNCTR et le second par le Conseil d'État. La nouvelle autorité administrative indépendante est ainsi chargée d'examiner les motifs de la demande des services de renseignement, sa finalité ainsi que la proportionnalité du recours à la technique invoquée. Le Conseil d'État est quant à lui chargé d'examiner les recours contentieux dans le cadre du recours illégal à l'une des techniques de recueil du renseignement et peut donc exercer un contrôle juridictionnel sur ces activités.

Concrètement, le citoyen peut ainsi saisir d'une réclamation la CNCTR lorsqu'il souhaite vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard. Cette commission doit alors procéder au contrôle de la ou des techniques invoquées, en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du cadre juridique, et peut adresser des recommandations aux autorités compétentes dans le cas contraire.

À l'issue de cette procédure, le citoyen peut en outre saisir le Conseil d'Etat aux fins d'obtenir l'annulation de l'autorisation de mise en œuvre d'une technique de recueil du renseignement, la destruction des renseignements irrégulièrement collectés et l'indemnisation du préjudice subi.

Ces garanties s'ajoutent ainsi à celles que contient la loi « Informatique et Libertés ». En effet, les informations collectées par l'intermédiaire de ces techniques de recueil du renseignement ont vocation à alimenter les fichiers utilisés par les services en charge de la lutte anti-terroriste.

La création et la modification de ces fichiers sont soumises à l'examen préalable de la Commission, qui dispose en outre d'un pouvoir de contrôle des conditions de mise en œuvre de la plupart de ces traitements. Toute personne peut en outre saisir la CNIL d'une demande d'exercice de ses droits d'accès et de rectification aux données qui la concernent. Depuis la loi relative au renseignement, le Conseil d'Etat est compétent pour connaître des requêtes concernant la mise en œuvre du droit d'accès à ces fichiers.

Enfin et de manière plus générale, l'ensemble des dispositions de la loi devra également faire l'objet d'une évaluation par le Parlement, dans un délai maximal de cinq ans à l'issue de l'entrée en vigueur de cette loi.

Cette « clause de rendez-vous » permettra donc au législateur de réexaminer les dispositifs qu'il a créés, à l'aune de leurs conséquences concrètes pour les citoyens. Il s'agit d'un point fondamental, au vu du caractère particulièrement intrusif de certaines techniques et des prémices de l'avènement d'une nouvelle logique d'action des services de renseignements, basée sur la collecte et l'exploitation indifférenciées de données à caractère personnel.

Par ailleurs, dans son champ de compétence, la CNIL s'assurera du respect des garanties posées par la loi informatique et libertés. ■

Les caméras-piétons utilisées par les forces de l'ordre

Depuis quelques années se multiplient de nouveaux usages en matière de caméras utilisées par des personnes pour des besoins de plus en plus variés, dans des lieux nouveaux et en recourant à des technologies de plus en plus avancées. Par exemple, les dispositifs de caméras embarquées (sur des véhicules ou des personnes) se développent aujourd'hui à grande échelle et, en particulier, les caméras dites « boutonnières » dont se dotent notamment des agents de sécurité privée, de police municipale ou encore de police et de gendarmerie nationales.

En ce qui concerne les « caméras-piétons » utilisées par les forces de l'ordre, des expérimentations souhaitées par le ministère de l'intérieur ont été mises en œuvre dans plusieurs zones de sécurités prioritaires (ZSP). Des initiatives locales ont également donné lieu à l'équipement de personnels. Depuis 2013, plusieurs centaines de caméras ont ainsi été affectées dans des services de police et unités de gendarmerie.

Ce développement imposait que la CNIL examine plus précisément les conditions de mise en œuvre de ces dispositifs et fasse connaître son analyse en la matière.

QUELS ENJEUX DU POINT DE VUE DE LA PROTECTION DE LA VIE PRIVÉE ?

De manière générale, l'installation de caméras sur la voie publique ou dans des lieux ouverts au public soulève de nombreuses questions en matière de respect des libertés individuelles. C'est pourquoi le Législateur a précisément encadré la mise en œuvre de ces dispositifs, notamment afin de limiter les atteintes à la vie privée qu'ils peuvent occasionner.

Ainsi, le code de la sécurité intérieure (CSI) prévoit notamment :

- les finalités pouvant justifier l'installation de caméras de vidéoprotection (prévention des atteintes à la sécurité des personnes et des biens, prévention d'actes de terrorisme, mais également secours aux personnes et défense contre l'incendie, régulation des flux de transport, etc.) ;
- les lieux que ces caméras peuvent filmer (la voie publique et les lieux et établissements ouverts au public lorsqu'ils sont particulièrement exposés à des risques d'agression ou de vol, à l'exclusion de l'intérieur des immeubles d'habitation et de leurs entrées) ;
- une durée maximale de conservation des enregistrements, fixée à un mois ;
- des droits pour les personnes concernées par ces enregistrements (d'être informées « *de manière claire et permanente de l'existence du système de vidéoprotection et de l'autorité ou de la personne responsable* », d'accéder aux enregistrements qui les concernent et d'en vérifier la destruction dans le délai prévu) ;

Le Législateur a encadré l'installation de caméras sur la voie publique ou dans des lieux ouverts au public car celle-ci soulève de nombreuses questions de respect des libertés individuelles.

▸ des modalités de contrôle de ces dispositifs, préalablement à leur installation (autorisation préfectorale prise après avis d'une commission départementale de vidéoprotection) et durant leur mise en œuvre (contrôle de la CNIL).

Or, certaines de ces garanties sont difficilement applicables aux caméras embarquées. En effet, ces caméras sont, par définition, susceptibles de filmer la voie publique, des lieux et établissements ouverts au public, des lieux non accessibles au public, ainsi que des lieux privés, le tout dans le cadre d'une même opération, en fonction des circonstances de l'intervention présidant à l'utilisation de ces dispositifs. En outre, ces caméras sont susceptibles, par définition, de filmer indifféremment tout ce qui se trouve dans leur champ de vision, alors que l'orientation des caméras fixes est strictement délimitée.

La possibilité de filmer des zones privées, et en particulier des domiciles privés, soulève d'importantes questions : elle est susceptible de porter atteinte à l'intimité de la vie privée des personnes concernées. Une telle ingérence de l'autorité publique nécessite dès lors que des garanties substantielles soient prévues afin d'assurer la proportionnalité du dispositif.

L'obligation d'information prévue pour les caméras de vidéoprotection peut également poser des difficultés s'agissant des caméras-piétons. Il faut en effet s'assurer par un dispositif adapté que les personnes filmées sont pleinement conscientes de l'enregistrement dont elles font l'objet et, par conséquent, de leur possibilité d'exercer un droit d'accès aux enregistrements qui les concernent, puisqu'il s'agit de garanties essentielles du point de vue du respect des droits des personnes concernées.

Les caméras-piétons utilisées par les forces de l'ordre sont en outre fréquemment **dotées de microphones permettant d'enregistrer les paroles prononcées par les personnes filmées.** La collecte de telles informations n'est pas prévue explicitement par les dispositions précitées du CSI.

À RETENIR

Des questions similaires se posent pour l'ensemble des caméras mobiles utilisées par les autorités publiques, qu'il s'agisse de caméras embarquées sur des véhicules par exemple ou encore de drones. Pour des raisons diverses, l'ensemble des garanties prévues par le législateur s'agissant des caméras filmant la voie publique semble difficilement applicable à de tels dispositifs. Leur utilisation croissante soulève dès lors des enjeux importants en matière de vie privée qu'il importe de mieux prendre en compte.

QUEL ENCADREMENT PRÉVOIR POUR LES CAMÉRAS EMBARQUÉES ?

Dans ce contexte, la CNIL estime qu'un encadrement légal, spécifique et adapté à de tels dispositifs, est nécessaire. Un tel encadrement doit être de nature législative : seule la loi peut en effet fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés, au titre desquelles figure le droit au respect de la vie privée. L'intervention du législateur semble donc nécessaire, à l'instar de ce qui a été fait au milieu des années 90 dans le cadre du développement des caméras de vidéosurveillance, afin de concilier, sous le contrôle du Conseil constitutionnel, le respect de la vie privée et la sauvegarde de l'ordre public et la recherche des auteurs d'infractions.

Un encadrement qui doit être de nature législative

Ce cadre juridique devrait en premier lieu **préciser les finalités exactes de ces dispositifs.** En effet, les caméras-piétons, à la différence des caméras de vidéoprotection classiques, ne sont pas utilisées comme des instruments de surveillance continue. Ils visent à prévenir les incidents susceptibles de survenir au cours des interventions des agents de la police et de la gendarmerie nationales, par leur effet modérateur, et à déterminer les circonstances de tels incidents, en permettant l'utilisation des enregistrements à des fins probatoires dans le cadre de procédures engagées à l'encontre de ces agents ▸▸▸

ou de la personne filmée. Le déploiement de ces dispositifs entend donc principalement répondre à un besoin de sécurisation physique et juridique des interventions des agents de la police et de la gendarmerie nationales.

Ces objectifs, qui se distinguent de ceux prévus par le code de la sécurité intérieure, devraient donc être clairement établis dans la loi, de même que toute autre finalité envisagée pour les caméras-piétons, comme par exemple leur utilisation à des fins pédagogiques et de formation. En conséquence, ce cadre juridique devrait également **définir les catégories de personnes pouvant utiliser ces dispositifs.**

En deuxième lieu, le cadre juridique devrait **préciser les lieux dans lesquels ces enregistrements pourraient intervenir,** le cadre juridique permettant ces enregistrements ainsi que les catégories de données susceptibles d'être collectées.

Ainsi, **la possibilité de procéder à des enregistrements audio,** non prévue par le CSI mais qui peut être nécessaire au vu des objectifs poursuivis, **devrait être expressément prévue.** Elle impose néanmoins, du fait de son caractère davantage intrusif que le seul enregistrement visuel, des mesures de confidentialité stricte des enregistrements.

Le périmètre exact de mise en œuvre des dispositifs de caméras individuelles devrait également être précisé, et notamment la détermination des lieux dans lesquels les interventions des agents de la police et de la gendarmerie nationales pourraient permettre de tels enregistrements. S'il est envisageable, au vu des finalités assignées à ces caméras, que toute intervention soit concernée, sans distinction du caractère public ou privé du lieu en cause, un tel champ d'application exigerait la mise en œuvre de fortes garanties, juridiques et techniques, afin d'assurer la proportionnalité du dispositif, tout particulièrement si cette captation de données est autorisée au sein de domiciles privés dans le cadre d'interventions des forces de sécurité.

C'est pourquoi l'encadrement juridique de ces dispositifs devrait prévoir, en troisième lieu, des mesures permettant de s'assurer d'une utilisation strictement conforme à ces caractéristiques. Ainsi, **ces caméras ne devraient pas procéder à des enregistrements permanents mais devraient uniquement pouvoir être activées dans certaines circonstances.** Les agents du ministère de l'intérieur devraient en outre disposer de lignes directrices claires, dans le cadre d'une doctrine d'emploi, par exemple, dont le respect devra être strictement contrôlé, quant aux circonstances permettant l'activation de leurs caméras. Ces règles devraient réserver un sort particulier aux enregistrements réalisés au sein des domiciles privés, que seules certaines circonstances impérieuses devraient autoriser.

Dans la mesure où les enregistrements doivent uniquement permettre de disposer de preuves en cas d'infraction ou de manquement, **seule l'ouverture d'une procédure judiciaire, administrative ou disciplinaire nécessitant de consulter ces enregistrements devrait permettre l'exploitation de ces vidéos.**

De même, l'utilisation des enregistrements à des fins de formation des agents commande la suppression de tout élément permettant l'identification directe ou indirecte des personnes filmées, qui

n'apparaît pas nécessaire dans ce cadre. Des procédés de floutage des visages et de déformation du son devraient dès lors être mis en œuvre.

Les droits des personnes doivent également faire l'objet d'une attention toute particulière. Tout comme pour les caméras de vidéoprotection, **le principe de transparence à l'égard du public doit être la règle,** et ce d'autant plus que l'utilisation des caméras-piétons a notamment pour objet de prévenir tout incident en apaisant les tensions qui peuvent survenir à l'occasion de certaines interventions.

Plusieurs mesures pourraient être prévues pour assurer cette transparence. L'information des personnes concernées sur l'enregistrement dont elles font l'objet doit ainsi être obligatoire. Le recours à des signaux visuels spécifiques, permettant à la personne filmée de prendre conscience qu'elle est effectivement enregistrée, devrait également être privilégié. En outre, le public devrait pouvoir accéder directement aux enregistrements qui le concernent, dans les mêmes conditions que celles qui prévalent pour les caméras de vidéoprotection.

Des mesures de sécurité devraient également garantir l'absence de visualisation des enregistrements avant l'ouverture de toute procédure, la traçabilité totale des consultations de ces enregistrements, ainsi que l'intégrité de ces derniers, de l'activation de la caméra à l'exploitation des images collectées.

Enfin, **des mesures de contrôle de l'ensemble de ces dispositions devraient être prévues.** Dans la mesure où seront collectées par l'intermédiaire de ces dispositifs de nombreuses données personnelles, dont certaines touchant à l'intimité de la vie privée, il semble naturel que leur mise en œuvre soit soumise au contrôle a posteriori de la Commission, qui dispose déjà de telles prérogatives pour les caméras de vidéoprotection comme pout tout traitement de données à caractère personnel.

QUEL AVENIR POUR LES CAMÉRAS-PIÉTONS ?

Ces analyses de la CNIL concernant les caméras-piétons utilisées par les agents de police et de gendarmerie ont été transmises au ministère de l'intérieur à l'été 2015. Le ministère a suivi le raisonnement de la Commission s'agissant de la nécessité d'un cadre législatif ad hoc pour encadrer la mise en œuvre de ces dispositifs et s'est engagé à prévoir plusieurs des garanties identifiées par la Commission.

Cet encadrement législatif est essentiel. En effet, la préservation du droit fondamental à la protection des données personnelles constitue non seulement une obligation juridique, mais également une condition d'acceptabilité, par les citoyens, de ces nouvelles caméras. Il importe dès lors que le cadre juridique applicable à ces dispositifs concilie efficacement les différents intérêts en cause.

La Commission aura en tout état de cause l'occasion de préciser ses analyses dans le cadre de son avis sur le projet de décret d'application de ces dispositions législatives. Elle aura en outre la possibilité de contrôler et de sanctionner tout manquement à ce cadre. ■

DERNIÈRE MINUTE

Le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale

Ce projet de loi, déposé le 3 février 2016, contient des dispositions spécifiques relatives aux caméras-piétons (article 32 du projet de loi), qui reprennent plusieurs des garanties demandées par la CNIL. Par exemple, l'absence d'enregistrement permanent des interventions, l'information des personnes filmées et l'impossibilité, pour les personnels dotés de ces caméras individuelles, d'accéder directement aux enregistrements sont expressément prévus dans le projet de loi. Celui-ci prévoit en outre que les modalités d'application de ces dispositions sont fixées par décret en Conseil d'Etat pris après de la Commission.

> La préservation du droit fondamental à la protection des données personnelles constitue une condition d'acceptabilité, par les citoyens, de ces nouvelles caméras.

Comment concilier protection de la vie privée et liberté de la presse ?

L'application de la loi Informatique et Libertés aux traitements journalistiques résulte de l'informatisation de l'ensemble de la chaîne de production de l'information, de la rédaction d'un article à sa diffusion. Elle résulte aussi de la volonté expresse du législateur qui, tout en aménageant un régime dérogatoire propre, n'a pas souhaité exclure complètement cette activité du champ de la loi. Il convient ainsi de trouver un juste équilibre entre liberté de la presse et protection des données.

DES LIENS ANCIENS

La question de l'articulation entre la protection des données et l'activité des organes de presse a été abordée dès les travaux parlementaires relatifs à la future loi Informatique et Libertés. Interrogé lors de la séance publique du 5 octobre 1977, le rapporteur du projet de loi a en effet souligné qu'il n'y avait pas d'oubli sur ce point : *« C'est une question délicate sur laquelle le Gouvernement estime que nul n'est mieux placé que vous-mêmes pour se prononcer. Nous avons donc décidé de nous en remettre sur ce point à la sagesse du Parlement. Vous représentez, mesdames, messieurs les députés, toutes les nuances des opinions politiques françaises. C'est à vous qu'il appartient légitimement de trancher cette question. ».*

Aujourd'hui pour l'informatique, comme hier pour la presse, les choses vont vite. De même que le droit sur la liberté de la presse ne se présentait plus du tout dans les mêmes conditions après l'invention des rotatives en 1867 que sous la Révolution française, de même, aujourd'hui, le droit de l'informatique doit tenir compte de l'évolution de la technique depuis une trentaine d'années.

Jean FOYER,
rapporteur du projet de loi relatif à l'informatique et aux libertés devant l'Assemblée Nationale
5 octobre 1977

UNE APPLICATION ADAPTÉE DÈS L'ORIGINE

Le législateur a donc décidé d'appliquer la loi du 6 janvier 1978 à la presse écrite et audiovisuelle, tout en prévoyant les nécessaires aménagements dictés par la spécificité du secteur.

Il a ainsi adopté une position médiane en Europe, à mi-chemin des pays ayant choisi de ne pas appliquer leur loi de protection des données aux organes de presse et ceux qui, à l'inverse, avaient fait le choix de la leur appliquer intégralement.

Les organes de presse installés en France n'ont donc pas été soumis, et ce dès l'origine, à :

- l'interdiction de traiter informatiquement les données dites sensibles (origines raciales ou ethniques, opinions politiques, philosophiques et religieuses, appartenances syndicales, mœurs) ;
- la limitation du traitement des infractions, condamnations et mesures de sûreté ;
- l'encadrement des transferts de données d'un pays vers l'autre.

Cependant, l'obligation d'information préalable à la mise en œuvre d'un traitement, l'obligation de choisir et de respecter une durée de conservation des données traitées et la possibilité d'exercer les droits d'opposition, d'accès, de rectification et de suppression n'ont pas été écartés.

Par ailleurs, le législateur de 1978 a subordonné l'application du régime d'exception à deux conditions : que les données considérées soient traitées par les organes de presse « *dans le cadre des lois qui les régissent* » et dans les seuls cas « *où leur application aurait pour effet de limiter l'exercice de la liberté d'expression* ».

DES AMÉNAGEMENTS COMPLÉMENTAIRES PROMUS PAR LA CNIL

C'est à l'issue d'une mission d'information menée en 1994 dans les locaux du Figaro que la CNIL a pris conscience des difficultés que pouvait poser l'application de la loi à la presse et, notamment, que l'exercice des droits reconnus aux personnes par la loi avant publication pouvait conduire à une forme de censure.

La Commission a donc engagé de sa propre initiative des travaux pour fixer des lignes directrices conciliant protection des données et liberté de la presse.

À l'issue d'une série d'auditions et de visites sur place dans l'ensemble de l'Hexagone, **la Commission a adopté le 24 janvier 1995 une recommandation relative « *aux traitements journalistiques et rédactionnels des données personnelles par les organismes de la presse écrite ou audiovisuelle* ».**

La CNIL y mettait en avant trois préconisations :

- l'adoption de mesures techniques particulières destinées à préserver la sécurité des données traitées ;
- la mise en place systématique d'un lien informatique entre l'article faisant l'objet d'une rectification, d'un droit de réponse ou d'une décision judiciaire définitive et les précisions apportées ;[1]
- la désignation d'un correspondant de la CNIL, chargé de l'application de la recommandation au sein de chaque organe de presse.

Cette première initiative a été complétée, en 2001, par une seconde recommandation concernant plus spécifiquement les chroniques judiciaires diffusées en ligne. La CNIL émettait notamment le souhait qu'une réflexion déontologique « *puisse être entamée ou se poursuivre, à l'initiative des organes de presse et en concertation avec la CNIL, dans le souci de ménager la vie privée et la réputation des personnes concernées lorsque, en tout cas, la liberté d'information ne paraît pas nécessiter qu'elles soient citées nominativement* ».

1 **Cette préconisation a d'ailleurs été imposée le 25 juin 2009 par le tribunal de grande instance de Paris qui, dans une ordonnance de référé, a ordonné à l'éditeur d'un site web de prendre toute mesure propre à assurer que la consultation en ligne d'un article depuis son fonds d'archives « s'accompagne d'un texte joint qui devra être immédiatement accessible par lien hypertexte, depuis la page consultée », au titre du « droit de suite ».**

UN RENFORCEMENT DU RÉGIME DÉROGATOIRE EN 2004

L'article 67 de la loi Informatique et Libertés, créé par la loi du 6 août 2004 à la suite de la transposition de la directive européenne du 24 octobre 1995 sur la protection des données, a élargi le nombre de dispositions de la loi ne s'appliquant pas aux traitements journalistiques.

Aux trois exceptions déjà prévues en 1978 se sont effet ajoutées :

- la possibilité de traiter les données sans limitation de durée ;
- l'absence d'obligation d'information des intéressés ;
- l'exclusion des droits d'accès, de rectification et de suppression.

En dépit de ces dispositions explicites, l'application à la presse de la loi Informatique et Libertés et, notamment, du droit d'opposition aux organes de presse a pu être contestée au motif que les éventuelles atteintes à la liberté de la presse, constitutionnellement protégée, doivent nécessairement bénéficier des garanties instituées par la loi du 29 juillet 1881 (formalisme des demandes et des actes de procédure, délais de rigueur, prescriptions courtes, etc.). Toutefois, les ▸▸▸

organes de presse ne sont pas soumis à cette seule loi, mais également à des dispositions diverses, telles que l'article 9 du code civil, certaines dispositions du code pénal, ou encore l'article 6 de la loi pour la confiance dans l'économie numérique. L'article 67 de la loi Informatique et Libertés se borne à rappeler que le droit d'opposition pour motifs légitimes est un outil juridique parmi d'autres.[3]

Enfin, il convient de rappeler à ce stade que, **lorsque la CNIL intervient à l'appui d'une demande d'opposition, ce n'est pas pour obtenir le retrait de l'article concerné, mais pour s'assurer que la demande sera bien examinée et qu'elle fera l'objet d'une réponse motivée,** ainsi que le prévoit les textes applicables.

À RETENIR

En définitive, et depuis la modification de la loi Informatique et Libertés en août 2004, restent seulement applicables aux organes de presse :
- **l'obligation de mise à jour, prévue par l'article 6 de la loi ;[2]**
- **le respect du droit d'opposition pour motifs légitimes, prévu par l'article 38 de la loi ;**
- **l'obligation de déclaration des fichiers informatisés, sauf si l'organe de presse désigne un correspondant « informatique et libertés ».**

2 Rejoignant par là l'article 13 de la loi du 29 juillet 1881 modifiée qui offre une possibilité particulière de « mise à jour » à la personne mise hors de cause dans une procédure pénale, la charte européenne des devoirs et des droits des journalistes, qui rappelle l'obligation de « rectifier toute information publiée qui se révèle inexacte » et la charte d'éthique professionnelle des journalistes adoptée par le Syndicat National des Journalistes, qui indique qu'un journaliste digne de ce nom « dispose d'un droit de suite, qui est aussi un devoir, sur les informations qu'il diffuse et fait en sorte de rectifier rapidement toute information diffusée qui se révèlerait inexacte. ».

3 Selon l'exposé des motifs du projet de loi modifiant la loi du 6 janvier 1978 présenté par Madame Marylise LEBRANCHU, Garde des sceaux, ministre de la Justice, cette disposition rappelle que les dérogations à la loi du 6 janvier 1978 applicables aux traitements journalistiques « ne font pas obstacle à l'application des dispositions civiles et pénales ayant pour objet la protection de la vie privée, ainsi que la protection des personnes contre les atteintes à leur réputation ».

L'EXERCICE DU DROIT D'OPPOSITION

Une personne citée dans un article de presse en ligne peut donc s'opposer, pour des motifs légitimes, à la diffusion des données le concernant (en pratique, son identité complète). Elle ne peut en revanche demander la rectification ou la suppression de l'article en se fondant sur la loi Informatique et Libertés, qui exclut cette possibilité depuis 2004.

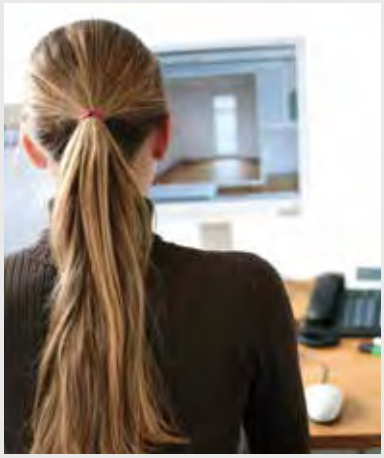
Cette demande d'opposition doit être accompagnée d'un justificatif d'identité et être motivée au regard, par exemple, du temps écoulé depuis la première diffusion de l'article (notion d'actualité), des conséquences de cette diffusion sur le demandeur (réinsertion, recherche d'emploi, sécurité personnelle…), etc.

L'organe de presse saisi doit répondre, positivement ou négativement, dans un délai de deux mois.

Si la demande d'opposition est incomplète (adresse, justificatif d'identité…) ou imprécise (article concerné, motifs de la demande…), l'organe saisi doit inviter le demandeur à les lui fournir en précisant en quoi ces éléments complémentaires sont nécessaire au traitement de sa demande.

Si l'organe de presse, considérant les motifs invoqués comme légitimes, choisit de faire droit à une demande d'opposition, il peut, en pratique, **anonymiser l'article concerné, désindexer volontairement la page web correspondante[4] ou le supprimer de son site web ou de ses archives en ligne.** Il n'appartient pas à la CNIL d'imposer l'une de ces solutions, mais à l'organe de presse de recourir à celle qui lui semble la plus adaptée eu égard à la situation.

L'anonymisation d'un article implique de signaler aux moteurs de recherche (signalement d'un lien « périmé ») la modification effectuée afin que l'identité complète du demandeur, disparue de l'article, n'apparaisse plus dans les résultats d'une interrogation au moyen d'un moteur de recherche.



Un organisme qui refuse de faire droit à une demande d'opposition doit motiver sa décision au regard des raisons invoquées par le demandeur à l'appui de sa demande. En effet, tant la demande d'opposition de la personne que l'éventuel refus de l'organe de presse ne peuvent reposer sur des motifs généraux (atteinte à la réputation, à la vie privée ou « droit à l'oubli » sans plus de détail pour les personnes / liberté de la presse, respect du travail accompli pour les organes de presse).

4 La désindexation volontaire d'une page web par le responsable du site web considéré n'a pas les mêmes effets que le déréférencement d'un résultat de recherche par un moteur de recherche. Dans le premier cas, c'est l'ensemble des informations diffusées par l'intermédiaire de la page web en question ; dans le second, seul un résultat apparaissant sur des critères définis ne figurera plus dans les résultats d'une recherche utilisant ces critères (imaginons, par exemple, que M. Roger Cuniculi, éleveur de lapins à Rambouillet, obtienne le déréférencement du résultat apparaissant sur interrogation de son identité ; l'information reste néanmoins accessible si l'on utilise d'autres critères de recherche – notamment ici « éleveur » + « lapin » + « Rambouillet ». Dans l'hypothèse d'une désindexation volontaire de la page web correspondante, il ne serait pas possible d'accéder à l'information, quels que soient les critères de recherche utilisés.).

LES DIFFICULTÉS RENCONTRÉES

Alors que les plaintes concernant les organes de presse sont en augmentation constante depuis quelques années (cf. encadré), la CNIL est parfois confrontée à des difficultés, de nature diverse, dans leur instruction :

- **l'absence de réponse :** si le silence de l'organe de presse pendant deux mois est constitutif d'un refus à la demande d'opposition la Commission préconise d'indiquer, a minima, au demandeur les motifs de ce refus.

Dans tous les cas, les organes de presse ne sont pas dispensés de répondre à la Commission lorsqu'elle intervient à l'appui d'une demande d'opposition.

Il en est de même des réponses qui se contentent d'indiquer aux plaignants que leur demande ne peut être examinée car elle n'est pas conforme aux conditions posées par les textes en vigueur (cf. plus haut).

Comme on l'a vu, c'est à l'organe de presse saisi d'inviter le demandeur à compléter sa requête.

- **les refus mal fondés :** certains organes de presse considèrent qu'ils relèvent exclusivement du droit de la presse et refusent de faire droit aux demandes d'opposition dont ils sont saisis en arguant, par exemple, que la loi « informatique et libertés » ne leur est pas applicable, qu'un site web n'est pas un traitement ou que la loi prévoit un régime dérogatoire pour les archives de presse.

Or, comme rappelé plus haut, c'est volontairement que le législateur n'a pas écarté l'application du droit d'opposition pour motifs légitimes aux traitements journalistiques.

Certains organes de presse refusent aussi de faire droit aux demandes dont ils sont saisis par un simple courrier stéréotypé, sans examen au fond des motifs invoqués. Or, leur refus doit être motivé dès lors que la demande n'est pas abusive. La CNIL a ainsi dû adopter une mise en demeure à l'égard d'un organe de presse qui adressait la même lettre-type de refus à tous les demandeurs.

- **la lourdeur de démarches :** dans certains cas, des articles anonymisés restent référencés de façon nominative par les moteurs de recherche. Une recherche effectuée sur la base de l'identité du plaignant renvoie donc toujours vers l'article en cause.

Une demande d'opposition acceptée par un organe de presse ne peut produire tous ses effets que si l'article anonymisé ou supprimé fait l'objet d'un signalement volontaire aux moteurs de recherche afin que la page web correspondante soit indexée dans sa version modifiée.

Ainsi, un journal qui fait droit à la demande d'une personne doit s'assurer qu'aucune recherche sur la base de son identité ne permette de renvoyer vers l'article anonymisé ou désindexé.

Si le nombre de plaintes a augmenté, la CNIL relève toutefois que la multiplication des contacts avec les organes de presse a permis une très sensible amélioration du traitement des demandes d'opposition formulées par des personnes auprès des organes de presse.

L'INSTAURATION DU DROIT AU DÉRÉFÉRENCEMENT ET SES CONSÉQUENCES

La reconnaissance, en mai 2014, du droit au déréférencement a modifié l'équilibre et provoqué une certaine confusion dans l'utilisation des outils juridiques disponibles.

En effet, la désindexation de la page web concernée était souvent utilisée, plutôt que la suppression ou l'anonymisation de l'article. Cette solution permettait de ne pas modifier l'article, qui était toujours diffusé sur le site web de l'organe de presse ; elle satisfaisait le plaignant, l'article ne figurant plus dans les résultats d'une recherche effectuée sur son identité complète.

Or, la reconnaissance du droit au déréférencement a pu donner l'impression que cette nouvelle procédure se substituait à l'exercice du droit d'opposition auprès des organes de presse.

Pourtant, cette voie juridique nouvelle n'a aucune incidence sur la possibilité pour le plaignant d'exercer son droit d'opposition ou sur la qualité de responsable de traitement des organes de presse. La Cour de justice de l'Union européenne a en effet explicitement jugé que ces deux voies d'action étaient ouvertes parallèlement. En effet, si les personnes sont désormais en mesure de solliciter le déréférencement des pages contenant des informations les concernant directement auprès des moteurs de recherche, cela n'exonère cependant pas les organes de presse, en tant que responsable de traitement, de donner suite aux demandes qui leurs sont adressées sur le fondement de l'article 38 de la loi Informatique et Libertés.

Ainsi, sur les 132 plaintes concernant des articles de presse adressées en 2015 à la CNIL, 75 % portaient sur des difficultés dans l'exercice du droit d'opposition, 8 % portaient sur des demandes de déréférencement[5] et 16 % portaient sur ces deux aspects.[6]

En outre, si le droit d'opposition et le droit au déréférencement se ressemblent, leurs effets sont différents : le premier permet d'obtenir **la suppression à la source** d'une information diffusée en ligne et l'autre permet uniquement d'obtenir **la suppression d'un résultat d'une recherche** effectuée sur l'identité d'une personne.

132

PLAINTES REÇUES EN 2015 CONCERNANT DES ARTICLES DE PRESSE

5 Le dernier pour cent concerne une interrogation générale sur droit d'opposition et droit au déréférencement.
6 Certains plaignants justifient leur demande de déréférencement par l'ignorance que leurs propos ou leur photographe seraient diffusés en ligne ou diffusés de façon nominative.

LE BILAN DES AUDITIONS MENÉES EN 2015

La CNIL a organisé, au printemps 2015, l'audition de différents représentants d'hebdomadaires, de quotidiens régionaux et nationaux, qu'ils soient sur divers supports ou « tout en ligne ».

Ces rencontres visaient à mieux connaître les pratiques des organes de presse en matière de gestion des demandes d'opposition et leur présenter les critères d'analyse des demandes de déréférencement dégagés par le G 29 (autorités européennes de protection des données).

Les professionnels invités ont ainsi pu dresser un état des demandes dont ils sont saisis et faire part de leurs difficultés et inquiétudes. Ils ont notamment souligné qu'ils :

- reçoivent de plus en plus de demandes d'opposition, qui concernent des contenus de plus en plus variés (articles, mais également résultats du baccalauréat ou d'élection, voire diffusion de photographies) ;
- souffrent d'un manque de moyens matériels et humains qui ne leur permet pas un traitement satisfaisant de ces demandes qui ne font, par ailleurs, l'objet d'aucune procédure ou de critères prédéfinis ;
- souhaiteraient être mieux informés des déréférencements opérés par les moteurs de recherche afin de pouvoir, le cas échéant, les contester ;
- craignent que ce droit limite la visibilité de leurs contenus et ne soit utilisé comme un moyen de contourner le formalisme et les délais courts de la loi sur la liberté de la presse (l'action en diffamation est enfermée dans un délai de trois mois, par exemple - cf. plus haut).

LES INITIATIVES ENVISAGÉES

À l'issue de ces auditions, la Commission a décidé de poursuivre ses efforts de conciliation de la liberté de la presse et de la protection des données, en concertation avec les professionnels du secteur.

Dans ce but, la Commission s'apprête à communiquer sur **le bilan des auditions** menées en 2015 et à diffuser **deux fiches pratiques** « Comment exercer son droit d'opposition » et « Comment répondre à une demande d'opposition » à destination du grand public et des organes de presse.

De même, elle organisera, à destination des organes de presse, **une journée d'information et d'échanges sur les modalités de traitement des demandes d'opposition** (forme des demandes, possibilités de réponse, rôle de la CNIL, conséquence d'une réponse positive, etc.) et le droit au déréférencement (acteurs, effets, critères, etc.).

Enfin, elle proposera aux organes de presse un accompagnement juridique dans le traitement des demandes d'opposition qui leur sont adressées directement et envisage **une mise à jour de la recommandation du 21 janvier 1995.** ■

INFO +

Des plaintes en augmentation

Depuis le 7 janvier 1978, la CNIL a reçu 785 plaintes concernant la presse.

Près de 90 % d'entre elles lui ont été adressées dans les cinq dernières années et elle en a reçu 356 (soit plus de 45 % de l'ensemble) au cours des deux dernières années.

Le nombre de plaintes concernant des organes de presse et, tout particulièrement, les articles diffusés par l'intermédiaire de leur site web connaît ainsi une augmentation quasi constante depuis quelques années : 35 en 2010, 55 en 2011, 98 en 2012, 149 en 2013, 224 en 2014 et 132 en 2015. La diminution en 2015 doit être rapprochée de l'augmentation du nombre de demandes de déréférencement, mais pourrait aussi s'expliquer par une plus grande habitude des organes de presse de traiter les demandes d'opposition qui leur parviennent.

Ces chiffres ne sont pas importants au regard du nombre total de plaintes reçues annuellement par la CNIL (7900 en 2015), mais ils mettent en lumière un recours croissant au droit d'opposition pour motifs légitimes et au droit au déréférencement (cf. ci-dessous) à l'égard des articles de presse diffusés en ligne. Compte tenu de l'importance de la conciliation entre protection de la vie privée et droit de la presse, ils justifient une action d'accompagnement particulière de la CNIL

Typologie des plaintes : objet de l'article concerné

Les 132 plaintes reçues en 2015 se répartissent de la façon suivante :

OBJET DE L'ARTICLE	PLAINTES	PROPORTION
Chroniques judiciaires (procès, condamnations, etc.)	55	42 %
Mise en cause judiciaire (rumeur, enquête, témoin, instruction, etc.)	19	14 %
Faits divers	10	8 %
Prise de position publique (grève de la faim, appel au boycott, critique du gouvernement, défense d'un homme politique, etc.)	8	6 %
Événement de la vie (mariage, décès, etc.)	7	5 %
Vie professionnelle (évolution, changement de métier, cumul, etc.)	6	5 %
Élections (résultats, photo et âge de candidats)	5	4 %
Actualité sociale et syndicale (élection, procès, manifestation, etc.)	5	4 %
Actualité économique (liquidation, interview, etc.)	4	3 %
Information factuelle (activité d'un centre de loisirs, etc.)	4	3 %
Faits de société (garde parentale, mal logés, mammectomie, etc.)	4	3 %
Parcours scolaire ou universitaire	3	2 %
Photographie jugée peu valorisante	1	1 %
Total	132	100 %

Cette typologie rejoint celle des organes de presse auditionnés au début de l'année 2015. On constatera que les trois premières catégories (« chroniques judiciaires », « mise en cause judiciaire » et « faits divers ») rassemblent presque 64 % des motifs de saisines concernant la presse. On soulignera aussi que certaines plaintes portent sur des articles pouvant entrer dans plusieurs des catégories ci-dessus (portrait évoquant à la fois le parcours professionnel et la vie privée, candidat à une élection prenant une position publique, etc.).

Histoires vécues

Un ancien médiateur pénal est mis en cause, en 2001, dans une affaire pénale ; un quotidien régional relate ses déboires et se fait l'écho de ses protestations d'innocence.
En 2013, deux articles de 2001 et 2002 sont toujours diffusés en ligne. Le plaignant exerce alors son droit d'opposition auprès du quotidien, en mettant en avant l'ancienneté des faits et l'atteinte à son honneur du fait d'une décision en sa faveur rendue en appel. Le quotidien lui répond que sa demande n'est pas conforme aux textes en vigueur et lui demande une copie de l'arrêt d'appel. Les articles étant toujours en ligne en 2015 malgré l'envoi de l'arrêt, l'intéressé saisit la CNIL, qui intervient auprès du quotidien. Ce dernier a procédé au retrait et au déréférencement des deux articles.

Une personne, présente dans le véhicule d'un membre d'une famille royale européenne, est à l'origine d'un incident avec les nombreux journalistes suivant l'événement.
L'incident est évidemment relayé par de nombreux médias. La personne demande le déréférencement des liens hypertextes pointant vers les divers articles, mais essuie un refus. Il saisit alors la CNIL d'une plainte. Après instruction, la Commission a refusé d'intervenir à l'appui de sa demande aux motifs que « cet incident récent est intervenu dans l'espace public, s'inscrivant dans le contexte de votre relation avec une personne jouant un rôle dans la vie publique. En outre, le récit de cet incident a été effectué à des fins journalistiques. ».

La protection des données personnelles au cœur de la cybersécurité

Cybersécurité et protection de la vie privée ne sont plus dissociables. Pour améliorer la confiance dans l'écosystème numérique, le rôle de la CNIL est désormais autant d'accompagner directement les responsables de traitements et le grand public dans l'amélioration de la sécurité des systèmes et réseaux, que de promouvoir les bonnes pratiques de sécurité en France et à l'international.

LA CYBERSÉCURITÉ AU CŒUR DE L'ACTION DE LA CNIL

L'année 2015 fut marquée par de nombreux changements dans l'écosystème du numérique et de la cybersécurité : le cloud computing, les objets connectés et le big data ont pris de l'ampleur ; le paysage légal a évolué avec la loi de programmation militaire et la loi relative au renseignement ; le nombre de cyberattaques a encore progressé ; les violations de données se sont multipliées (Uber, Anthem, Ashley Madison…) et le nombre de données concernées se sont souvent comptées en dizaine de millions.

Comment, dans ce contexte, instaurer la confiance des partenaires et des internautes pour accompagner l'innovation numérique ? Les efforts en matière de sécurité devront être non seulement poursuivis, mais aussi adaptés.

Le besoin d'intégrer la cybersécurité et la protection de la vie privée

Le respect de la vie privée est au cœur du développement du numérique. Il en est de même de la prise en compte de la sécurité des systèmes d'information, permettant d'assurer notamment la résilience des infrastructures.

Les notions de sécurité et de protection de la vie privée sont aujourd'hui indissociables. De même qu'il n'est plus envisageable aujourd'hui de développer un service sans prendre en compte la dimension sécurité, la confiance dans le monde du numérique passe notamment, comme l'a rappelé le Premier Ministre lors de la présentation de la stratégie nationale pour la sécurité du numérique, par la prise en compte et le respect des notions de vie privée et de protection des données à caractère personnel.

> Les notions de sécurité et de protection de la vie privée sont aujourd'hui indissociables.

INFO +

Les règles de base de sécurité

- la mise en œuvre de solutions de sécurisation des flux et des données stockées,
- le cloisonnement des environnements en fonction de leur sensibilité et des données qui y sont traitées(le réseau WiFi ouvert aux clients ne doit par exemple pas être connecté au réseau bureautique ou de production de l'entreprise),
- la gestion des habilitations permettant de limiter l'accès des données aux seules personnes autorisées, la contractualisation de la sécurité dans la relation avec les tiers.

De nombreuses violations de données à caractère personnel continuent d'avoir lieu. Or, leur occurrence aurait pu être évitée ou, à tout le moins, leurs conséquences auraient pu être réduites, par la **mise en œuvre et le respect de règles simples de sécurité.** Si tout le monde s'accorde sur le fait qu'il est illusoire d'espérer atteindre un niveau absolu de sécurisation, il paraît inconcevable que ce premier niveau de sécurité ne soit pas respecté.

Les objets qui nous entourent deviennent de plus en plus autonomes, intelligents et traitent toujours plus de données. Dans ce contexte, la cybercriminalité se développe, ne ciblant plus uniquement les grandes entreprises, mais visant désormais les petites structures ou les individus eux-mêmes. L'omniprésence du phénomène cybercriminel sur Internet nécessite la mise en œuvre de solutions de sécurité toujours plus poussées, dans le respect de la protection de la vie privée, afin de déceler les fraudes ou les attaques. **La détection devient un élément fondamental de la protection des entreprises,** des institutions et des utilisateurs en général.

En conséquence, dans l'intérêt de l'écosystème du numérique et des personnes qui le composent, **des règles de transparence et d'information doivent être instaurées, s'appuyant sur ces nouvelles solutions de sécurité.** Ces dernières doivent être mises en œuvre pour garantir la protection des individus derrière les données.

Le rôle de la CNIL en matière de cybersécurité

La CNIL aide à construire la confiance dans l'environnement numérique. Elle est chargée, en vertu de l'article 34 de la loi Informatique et Libertés, de s'assurer que les entités qui traitent des données personnelles le font dans des conditions de sécurité optimale. **À ce titre, elle mène plusieurs actions :** À travers ses missions (conseil, formalités, contrôles, sanctions) la CNIL veille au niveau de sécurité mis en place par les organismes dans les systèmes et réseaux. Elle accompagne également l'évolution du cadre juridique (participation au débat sur le règlement protection des données, règlement eIDAS sur l'identité électronique, loi pour une République Numérique). Elle participe activement à plusieurs groupes de travail spécialisés en sécurité de l'information réunissant des experts issus d'horizons multiples (Club EBIOS, Club des experts de la sécurité de l'information et du numérique). Elle est enfin très active dans le domaine de la sensibilisation, notamment à travers son action dans le domaine de l'éducation au numérique.

La CNIL propose des solutions techniques aux responsables de traitements et au grand public. En matière de sécurité, elle publie notamment des guides, fiches pratiques et recommandations pour aider les entreprises et les citoyens à adopter les bonnes pratiques et ainsi à se protéger des risques. Elle se prononce sur les mesures de sécurité mises en œuvre par les responsables de traitement, les accompagne dans leurs choix et les conseille. Elle développe aussi la labellisation de procédures ou de produits (ex : coffre-fort électronique, label gouvernance).

La CNIL apporte une assistance aux victimes d'actes de cybermalveillance. D'une part, elle reçoit des plaintes, dans tous les domaines liés aux nouvelles technologies et apporte une assistance aux victimes par exemple en les réorientant vers les services compétents (police, parquet). D'autre part, elle reçoit les notifications de violations de données à caractère personnel, permettant ainsi aux personnes concernées d'être prévenues et de prendre les mesures appropriées. Elle est également partenaire de Signal spam et peut notamment être amenée à contrôler des entreprises identifiées par Signal spam.

La CNIL porte les valeurs de la France au sein du G29 et d'autres instances internationales qui travaillent sur la sécurité et les nouvelles technologies (OCDE, ISO, groupe de Berlin, Conférence internationale des commissaires). Elle a ainsi édité la principale norme en sécurité de l'information à l'ISO (ISO/IEC 27001), a contribué aux travaux européens pour définir les mesures de sécurité pour les smart grids, a représenté le G29 dans l'un des groupes permanents conseillant l'ENISA (l'agence européenne de sécurité), et a fourni des recommandations techniques, au niveau national ou européen, dans différents domaines liés aux nouvelles technologies (cloud computing, internet des objets, etc.) Elle réalise aussi des actions de régulation visant les grands acteurs de l'internet, promouvant ainsi les valeurs européennes.

> La prise en compte de la sécurité doit être au centre de nos préoccupations pour protéger les citoyens, les clients, les sociétés, et l'écosystème du numérique dans son ensemble.

Vers le Privacy by design

La mise en œuvre de la sécurité doit passer par une prise en compte dès l'élaboration du projet et doit suivre tout le cycle de vie de la donnée. Il en va de même pour la protection de cette dernière au sens de la vie privée.

Cela passe par la mise en œuvre d'un dialogue entre les métiers et la direction des systèmes d'information, et par la compréhension mutuelle des enjeux associés à ces développements.

Idéalement, cette réflexion sera menée le plus tôt possible, dès la conception des projets (notion de « *privacy by design* »).

L'ÉTUDE D'IMPACT SUR LA VIE PRIVÉE : UN NOUVEL OUTIL POUR BÂTIR ET DÉMONTRER SA CONFORMITÉ

Pour aider les TPE et PME à « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données* » (article 34 de la loi informatique et libertés), la CNIL a publié en 2010 un premier guide intitulé « La sécurité des données personnelle ». Celui-ci présente les précautions élémentaires à mettre en place pour s'assurer de la sécurité d'un traitement.

En juin 2012, la CNIL a mis en ligne un guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Ce dernier a pour but d'aider les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Ce guide a été révisé depuis afin d'être plus en phase avec le projet de règlement européen sur la protection des données, et avec les réflexions du G29 sur l'approche par les risques pour déterminer les mesures de sécurité. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs. Enfin, il marque explicitement le passage d'une simple application de bonnes pratiques de sécurité à une véritable mise en conformité globale à la loi Informatique et Libertés.

C'est ainsi que depuis juillet 2015, la Commission communique sur sa méthode pour mener des études d'impacts sur la vie privée (EIVP), plus communément appelée PIA *(Privacy Impact Assessment)* ou encore, dans le projet de Règlement européen sur la protection des données, DPIA *(Data Protection Impact Assessment).*

Problématiques liées à la gestion des risques et aux PIA

La conformité dans le domaine de la protection de la vie privée repose principalement sur des exigences légales. **Le principe de sécurité relève quant à lui de la gestion des risques.**

L'article 17 de la Directive 95/46/CE dispose ainsi que « *le responsable du traitement doit mettre en œuvre [des] mesures [assurant]* ***un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger ».***

En outre, l'article 34 de la loi Informatique et Libertés dispose que ***« le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement,*** *pour préserver la sécurité des données».*

Par ailleurs, l'article 33 de la proposition de règlement européen sur la protection des données impose de réaliser une étude des risques dès lors qu'un traitement expose les personnes concernées à des risques sur leur vie privée, avant la mise en œuvre du traitement.

La conformité relative à la sécurité repose sur une réflexion des risques sur la vie privée (de qui ou de quoi ?), et non pas sur la seule comparaison avec de bonnes pratiques ou sur l'application seule de la doctrine (quelle doctrine ?).

En revanche, les outils, mesures et documentations requises (produites selon le principe d'*accountability*) peuvent varier selon les risques auxquels le traitement est exposé.

Ainsi, le fait même de mener un PIA, de consulter préalablement l'autorité de protection des données ou de mettre en place telle ou telle mesure pour traiter les risques de sécurité des données, dépend du niveau de risque qui pèse sur le traitement.

Qu'est-ce qu'un PIA ?

En avance de phase par rapport au projet de règlement européen sur la protection des données, **la CNIL a publié sa méthode pour mener des études d'impact sur la vie privée (également appelée PIA - *Privacy Impact Assessment*).**

L'article 33 du règlement européen sur la protection des données décrit le DPIA de la manière suivante :

« *L'analyse contient au moins* ***une description générale des traitements envisagés, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face aux risques,*** *les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le présent règlement, en tenant compte des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées* ».

En quoi consistent les guides PIA ?

Les guides PIA sont des guides méthodologiques. La méthode de la CNIL a été conçue conformément au projet de Règlement européen sur la protection des données et aux normes internationales. Elle se compose de trois guides :

- le guide PIA 1 : **la démarche méthodologique ;**
- le guide PIA 2 : **l'outillage ;**
- le guide PIA 3 : **le catalogue de bonnes pratiques.**

Cette méthode repose sur deux piliers :

- **les principes et droits fondamentaux,** « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;
- **la gestion des risques sur la vie privée des personnes concernées,** qui permet de déterminer les mesures (techniques et d'organisation) appropriées pour protéger les données personnelles.

La démarche (guide PIA 1) comprend 4 étapes :

- **étude du contexte :** délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- **étude des mesures :** identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;

- **étude des risques :** apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- **validation :** valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, au regard des enjeux identifiés dans l'étape 1, ou bien refaire une itération des étapes précédentes.

L'outillage (guide PIA 2) contient des exemples et des modèles, destinés à aider ceux qui mènent un PIA à réaliser leur étude et à formaliser leur rapport :

- les exemples permettent de disposer de bases de connaissances relatives à tous les éléments utiles pour mener un PIA (sources de risques, impacts sur la vie privée, menaces et vulnérabilités exploitables…) ;
- il contient également des modèles de tableaux et de textes, permettant de présenter les résultats de l'ensemble des étapes de la méthode.

Enfin, **le catalogue de bonnes pratiques (guide PIA 3) propose des exemples de mesures à mettre en œuvre,** d'une part pour respecter les exigences légales, et d'autre part pour traiter les risques identifiés en utilisant la méthode. ■

INFO +

Le PIA

Le PIA est une étude comprenant une réflexion sur le traitement de données à caractère personnel, l'appréciation des risques sur la vie privée, et la description de leur traitement. Il correspond à la mise en œuvre du processus de gestion des risques sur la vie privée aux fins d'en tirer les conséquences sur les mesures de sécurité à mettre en œuvre.
Pour tous les cas non couverts par des packs de conformité, des formalités simplifiées ou des guides sectoriels, et en compléments de ceux-ci, le PIA aide à la mise en conformité, notamment pour les traitements complexes, jugés à risque ou à forts enjeux d'un point de vue informatique et libertés.

L'invalidation du Safe Harbor : le travail coordonné de la CNIL et du G29 pour prendre en compte les conséquences de l'arrêt « SCHREMS »

Les révélations d'Edward Snowden faites en juin 2013 ont suscité un débat sur l'échelle des activités de surveillance menées par les services de renseignement, tant aux États-Unis qu'au sein de l'Union européenne. Ce débat a notamment porté sur les conséquences d'une surveillance de masse sur les droits au respect de la vie privée et à la protection des données.

M. Maximillian Schrems, citoyen autrichien, utilise Facebook depuis 2008. Comme pour les autres abonnés résidant dans l'Union, les données fournies par M. Schrems à Facebook sont transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles font l'objet d'un traitement.

M. Schrems a déposé une plainte auprès de l'autorité irlandaise de protection des données, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des États-Unis (en particulier la *National Security Agency* ou NSA), le droit et les pratiques des États-Unis n'offrent pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays.

L'autorité irlandaise a rejeté la plainte, au motif notamment que, dans sa décision du 26 juillet 2002, la Commission a considéré que, dans le cadre du régime dit de la « sphère de sécurité » ou *Safe Harbor,* les États-Unis assurent un niveau adéquat de protection aux données à caractère personnel transférées.

Saisie de l'affaire, la Haute Cour de justice irlandaise *(High Court of Ireland)* a souhaité savoir si cette décision de la Commission avait pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat et, le cas échéant, de suspendre le transfert de données contesté.

La question de la surveillance massive et indiscriminée est au cœur de la décision de la CJUE.

L'ARRÊT RENDU PAR LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

L'arrêt[1] rendu par la Cour de Justice de l'Union européenne (ci-après « CJUE ») dans l'affaire Schrems est **majeur pour la protection des données** à plusieurs égards.

Tout d'abord, la Cour a répondu à la Haute Cour de justice irlandaise que ***« l'existence d'une décision de la Commission*** *constatant qu'un pays tiers assure un niveau de protection adéquat aux données à caractère personnel transférées* ***ne saurait annihiler ni même réduire les pouvoirs dont disposent les autorités nationales de contrôle*** *en vertu de la Charte des droits fondamentaux de l'Union européenne et de la directive ».*

Elle a ajouté que, **même en présence d'une décision de la Commission, les autorités nationales de contrôle,** saisies d'une demande, **doivent pouvoir examiner en toute indépendance si le transfert des données d'une personne vers un pays tiers respecte les exigences posées par la directive.** Elle a donc consacré l'indépendance des autorités de protection des données vis-à-vis de la Commission européenne.

> La CJUE a consacré l'indépendance des autorités de protection des données vis-à-vis de la Commission européenne.

Toutefois, il revient à la seule Cour de décider si une décision de la Commission est valide ou non. A ce titre, elle a, par l'arrêt Schrems, invalidé la décision par laquelle la Commission européenne avait constaté que les principes du Safe Harbor assuraient un niveau de protection suffisant des données à caractère personnel européennes transférées [2].

La Cour a notamment relevé que la Commission n'avait pas suffisamment détaillé dans sa décision les mesures par lesquelles les Etats-Unis assuraient un niveau de protection des données suffisant à raison de leur législation nationale ou de leurs engagements internationaux [3].

En effet, « *la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, EU:C:2014:238, point 52 et jurisprudence citée)* »[4].

L'exigence de proportionnalité

Ainsi, « n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant

> La Commission n'avait pas suffisamment détaillé dans sa décision les mesures par lesquelles les États-Unis assuraient un niveau de protection des données suffisant.

l'accès que l'utilisation de ces données [voir en ce sens, en ce qui concerne la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54), arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, EU:C:2014:238, points 57 à 61].[5] »

L'atteinte au droit fondamental au respect de la vie privée constituée par un accès généralisé par les autorités publiques

« En particulier, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu ▸▸▸

1 Arrêt de la Cour (grande chambre), 6 octobre 2015, dans l'affaire C 362/14, ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par la High Court (Haute Cour de justice, Irlande), par décision du 17 juillet 2014, parvenue à la Cour le 25 juillet 2014, dans la procédure Maximillian Schrems contre Data Protection Commissioner, en présence de: Digital Rights Ireland Ltd).
2 2000/520/CE: Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique [notifiée sous le numéro C(2000) 2441] (Texte présentant de l'intérêt pour l'EEE.)
3 Voir notamment le paragraphe 83 de l'arrêt : La décision 2000/520 «concerne uniquement le caractère adéquat de la protection fournie aux États-Unis par les principes [de la sphère de sécurité] mis en œuvre conformément aux FAQ en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive [95/46]», sans pour autant contenir les constatations suffisantes quant aux mesures par lesquelles les États-Unis d'Amérique assurent un niveau de protection adéquat, au sens de l'article 25, paragraphe 6, de cette directive, en raison de leur législation interne ou de leurs engagements internationaux. »
4 Paragraphe 92 de l'arrêt SCHREMS
5 Paragraphe 93 de l'arrêt SCHREMS

de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte (voir, en ce sens, arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, EU:C:2014:238, point 39)[6].

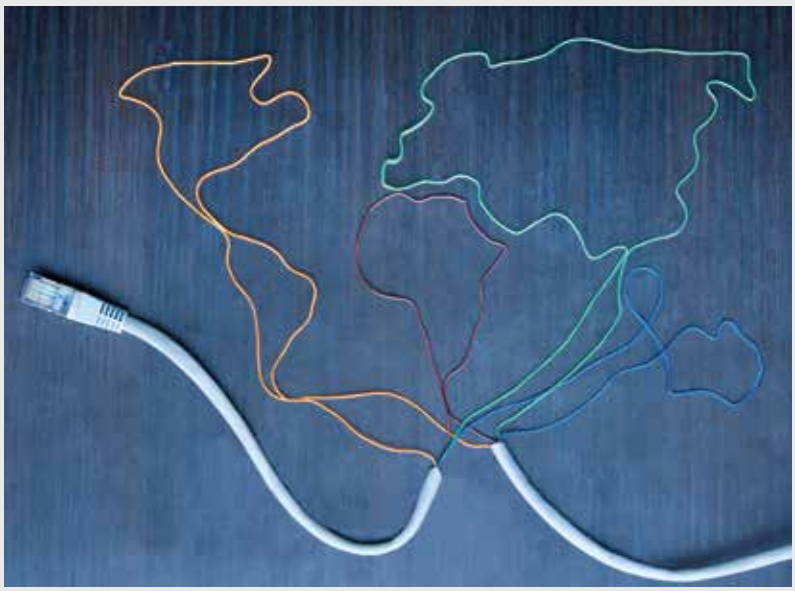
La nécessité d'un recours effectif pour le justiciable

« *De même, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne, dont les droits et libertés garantis par le droit de l'Union ont été violés, ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article. À cet égard, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit (voir, en ce sens, arrêts Les Verts/Parlement, 294/83, EU:C:1986:166, point 23; Johnston, 222/84, EU:C:1986:206, points 18 et 19; Heylens e.a., 222/86, EU:C:1987:442, point 14, ainsi que UGT Rioja e.a., C 428/06 à C 434/06, EU:C:2008:488, point 80).* »

Or, la Commission a elle-même constaté que « les autorités américaines pouvaient accéder aux données à caractère personnel transférées à partir des États membres vers les États-Unis et traiter celles-ci d'une manière incompatible, notamment, avec les finalités de leur transfert, que dans la mesure où cet accès est strictement nécessaire et proportionné à la protection de la sécurité nationale. De même, la Commission a constaté qu'il n'existait pas, pour les personnes concernées, de voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression.[7] »

6 Paragraphe 95 de l'arrêt SCHEMS
7 Voir paragraphe 90 de l'arrêt.

LES ACTIONS DU G29



La CNIL et ses homologues européens se sont réunis le 15 octobre pour élaborer un plan d'action commun permettant aux acteurs de s'adapter au nouveau contexte juridique.

Dès le 16 octobre 2015, le G29 a publié un communiqué soulignant l'importance d'une gestion commune des conséquences de l'arrêt. Il a également constaté que la surveillance de masse est un élément déterminant du raisonnement de la cour. A ce titre, il a rappelé sa doctrine constante aux termes de laquelle la surveillance de masse est incompatible avec le droit européen et les instruments de transferts de données ne sauraient être détournés à cette fin.

Aussi, il a appelé les institutions européennes à engager des discussions avec les autorités américaines afin de trouver des solutions légales et techniques permettant de garantir que les transferts de données vers les Etats-Unis respectent les droits fondamentaux.

À cet égard, il a considéré que la négociation d'un accord international prévoyant des garanties plus importantes pour les personnes concernées pourrait faire partie de la solution, tout comme les discussions sur la réforme du *Safe Harbor* et **fixé le 31 janvier 2016 comme date butoir.**

Le G29 a constaté que les transferts intervenant sur la base du *Safe Harbor* étaient, de fait, illégaux. Il s'est ensuite engagé à étudier les conséquences de l'arrêt sur les autres outils de transfert dans l'intervalle de temps nécessaire à ces discussions. Il a précisé que les clauses contractuelles et les règles contraignantes d'entreprises demeuraient utilisables durant cette période et que les autorités se réservaient la possibilité d'instruire des dossiers particuliers, par exemple en cas de plaintes, et d'exercer leurs pouvoirs afin de protéger les droits des individus. De plus, le G29 a indiqué qu'à l'issue du délai, il pourrait, le cas échéant, engager des poursuites, si nécessaire coordonnées.

Il a par ailleurs annoncé des actions de sensibilisation auprès des acteurs concernés et les a invités à envisager les risques pris du fait du transfert de données et à réfléchir aux solutions légales et techniques permettant de les réduire.

L'ANALYSE RÉALISÉE PAR LE G29

Dès la mi-octobre 2015, le G29 a entrepris d'analyser l'impact de l'arrêt SCHREMS et des principes rappelés par la Cour sur les autres instruments de transferts de données vers des pays tiers, tels que les clauses contractuelles et les règles contraignantes d'entreprise.

À cette fin, il a identifié les garanties essentielles applicables aux activités des services de renseignement aux termes du cadre légal et de la jurisprudence européenne.

Il a ensuite analysé le cadre légal des activités des services de renseignement fédéraux des Etats-Unis ainsi que leurs pratiques à la lumière de ces garanties avec pour objectif de vérifier si les conditions dans lesquelles des ingérences dans le droit à la vie privée et au respect de la protection des données sont permises, respectent ces garanties.

Afin de vérifier l'exactitude de ses constats, le G29 a organisé des auditions et consultations d'universitaires, représentants du secteur privé/entreprises, des représentants du gouvernement américain et de la société civile, tant européenne qu'américaine.

L'identification des garanties essentielles applicables aux activités des services de renseignement aux termes du cadre légal et de la jurisprudence européenne

Partant des constats de la CJUE dans l'arrêt SCHREMS, le G29 a analysé les autres arrêts de la Cour de Luxembourg portant sur les activités de surveillance étatique ainsi que les arrêts de la Cour européenne de sauvegarde des libertés fondamentales (ci-après « CEDH ») ainsi que le droit primaire et secondaire applicable à la matière.

Les résultats de cette analyse ont été discutés lors d'une réunion plénière du G29 les 2 et 3 février 2016.

Quatre garanties essentielles s'appliquent à ces activités :

- Le traitement doit être fondé sur des règles claires, précises et accessibles : cela signifie que quiconque qui est raisonnablement informé devrait être en mesure de prévoir les règles qui s'appliqueraient à ses données si elles étaient transférées.
- L'Etat doit être en mesure de démontrer la nécessité et la proportionnalité de ses activités de renseignement et notamment des traitements de données personnelles qui en résultent au regard de l'objectif légitime poursuivi : un équilibre doit être trouvé entre l'objectif pour lequel les données sont collectées et traitées (en général, la sécurité nationale) et les droits des individus.
- Un système de supervision/contrôle indépendant doit exister, qui soit à la fois effectif et impartial : il peut être le fait d'un juge ou de tout organe indépendant dès lors qu'il bénéficie d'une capacité à mener les contrôles nécessaires.
- Les individus doivent pouvoir se prévaloir de recours effectifs : toute personne devrait avoir le droit de faire valoir ses droits devant un organe indépendant.

Le G29 a souligné que ces quatre garanties devraient être respectées dès lors que des données personnelles sont transférées depuis l'Union européenne vers les Etats-Unis et en direction d'autres Etats tiers ainsi que par tout Etat membre.

L'analyse du cadre légal et de la pratique américaine à la lumière de ces garanties essentielles

Le G29 a étudié les principaux textes règlementant les activités des services de renseignement fédéraux américains et sollicité les acteurs précités pour en connaître la pratique. Il résulte de cette analyse et des contributions des acteurs concernés que des efforts importants ont été menés par les Etats-Unis en 2014 et 2015 afin d'améliorer la protection des données personnelles des non-américains dans ce contexte. Toutefois, le G29 demeure préoccupé par le cadre légal actuellement applicable au regard des quatre garanties précitées, plus particulièrement au regard du champ d'application et des recours accessibles aux personnes concernées par le transfert de leurs données personnelles depuis le territoire de l'Union européenne.

> **Le G29 a souligné que 4 garanties devraient être respectées dès lors que les services de renseignement américains accèdent à des données de citoyens européens.**

LES ACTIONS MENÉES PAR LA CNIL

La décision de la CJUE ayant invalidé le mécanisme d'adéquation Safe Habor permettant le transfert de données vers les entreprises adhérentes aux Etats-Unis, il n'a plus été possible, dès cette date, de réaliser un tel transfert sur la base du Safe Harbor.

Formellement, cela impliquait que les entreprises concernées adressent une demande de modification de leur déclaration initiale à la CNIL afin de notifier, selon le cas, la cessation des transferts en question ou le recours à un autre outil d'encadrement des transferts.

La CNIL a donc pris les mesures afin d'en informer les entreprises concernées et de leur indiquer les alternatives à leur disposition et les procédures à suivre pour s'y conformer. Elle a notamment procédé à un envoi de courriels aux entreprises identifiées comme concernées et publié sur son site les questions/réponses.

Dans l'hypothèse où le transfert s'avérait nécessaire, le G29 ayant considéré que les autres mécanismes juridiques de transfert pouvaient être utilisés par les entreprises jusqu'au 31 janvier, la CNIL a informé les entreprises de la possibilité de recourir aux (BCR)[8] et aux clauses contractuelles type[9] adoptées par la Commission européenne (clauses de responsable de traitement à responsable de traitement et clauses de responsable de traitement à sous-traitant). ■

DERNIÈRE MINUTE

Annonce d'un nouvel accord Privacy Shield

Les Etats-Unis et la Commission Européenne ont annoncé le 1er février 2016 la conclusion d'un nouvel accord appelé EU-U.S. *Privacy Shield*. Cet accord publié le 29 février 2016 doit désormais être analysé par le G29 afin d'en connaître précisément le contenu et d'évaluer s'il répond aux préoccupations importantes relatives aux transferts internationaux de données soulevées par la décision de la CJUE. Une séance plénière du G29 est prévue en avril 2016.

8 Les Binding Corporate Rules (BCR) constituent un code de conduite, définissant la politique d'une entreprise en matière de transferts de données. Les BCR permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe.

9 Il s'agit de modèles de clauses contractuelles adoptées par la Commission européenne qui permettent d'encadrer les transferts de données personnelles hors de l'Union européenne. Elles ont pour but de faciliter la tâche des responsables de traitement dans la mise en œuvre de contrats de transfert. On distingue les transferts de responsable de traitement à responsable de traitement et les transferts de responsable de traitement à sous-traitant. Il existe donc deux types de clauses afin d'encadrer chacun de ces transferts.

2

BILAN D'ACTIVITÉ

Informer le grand public et les professionnels

Conseiller et réglementer

Accompagner la conformité

Protéger les citoyens

Contrôler et sanctionner

Anticiper et innover

**La régulation internationale,
un élément indispensable de la protection
des données à l'ère numérique**

Informer le grand public et les professionnels

La CNIL est investie d'une mission générale d'information des personnes sur les droits et les obligations que leur reconnaît la loi Informatique et Libertés. Elle répond au public, qu'il s'agisse des professionnels ou des particuliers, mène des actions de communication et s'investit particulièrement en matière d'éducation au numérique. Elle est présente dans la presse, sur internet, sur les réseaux sociaux où elle met à disposition des outils pédagogiques. Directement sollicitée par de nombreux organismes, sociétés ou institutions pour conduire des actions de formation et de sensibilisation, la CNIL participe aussi à des colloques, des salons ou des conférences pour informer et s'informer.

LA CNIL VOUS INFORME AU QUOTIDIEN

Un site internet refondu pour mieux répondre aux demandes

Depuis sa création en 1998, le site de la CNIL s'est constamment enrichi de contenus et de services afin de répondre aux attentes d'un public de plus en plus varié : particuliers, membres de la communauté éducative, professionnels, associations, CIL, homologues internationaux.

L'année 2015 a été particulièrement marquée par la mise en ligne de plusieurs services à destination des usagers de la CNIL :

- **« Besoin d'aide »** offre un service de réponses de premier niveau aux usagers particuliers et professionnels. En outre, il permet de contacter la CNIL dans le cas où la réponse ne se trouverait pas parmi les réponses proposées.
- Le service **« Plainte en ligne »** a été repensé et élargi afin d'offrir aux usagers de nouvelles possibilités de saisir la CNIL en ligne. Dans le cas où la plainte à la CNIL requiert des démarches préalables, la CNIL accompagne davantage l'usager dans ces démarches.
- **L'offre éditoriale** à destination des enseignants et des acteurs de l'éducation numérique s'est enrichie avec la mise en ligne de tutoriels, actualités et de conseils à destination des jeunes et de leurs formateurs sur le site dédié educnum.fr

DERNIÈRE MINUTE

Un nouveau site pour la CNIL

Le 16 février 2016, La CNIL a mis en ligne une nouvelle version de son site internet. Plus clair, plus pédagogique, mieux adapté à la consultation sur mobile et tablette. Le nouveau site de la CNIL a pour ambition de mieux répondre aux préoccupations des citoyens. Il propose également de nouveaux contenus pour les internautes qui souhaitent contrôler l'exposition de leur vie privée en ligne ou gérer un problème d'e-réputation.
Il dispose d'un espace entièrement dédié aux professionnels débutants ou experts et les accompagne pour mettre en œuvre une politique de protection des données personnelles efficace.
Pensé pour respecter la vie privée des internautes, Cnil.fr propose un mécanisme de consentement aux cookies permettant à l'internaute de choisir les fonctionnalités sociales qu'il souhaite activer ou désactiver.

▸ Le mini site élections a été relancé à l'occasion des **élections régionales**.
▸ La mise en ligne d'une page **Open CNIL** dédiée à la présentation des jeux de données mis à disposition sur Etalab.

Parallèlement, l'année 2015 a été également consacrée à un projet de refonte globale du site. Pour fêter ses 18 ans, cnil.fr a fait peau neuve début 2016 avec un nouveau site.

Les réseaux sociaux, enjeu et vecteur de protection de la vie privée pour la CNIL

La CNIL est principalement présente sur 5 plateformes sociales (Dailymotion, Facebook, Google+, LinkedIn, Twitter). Citoyens, relais d'influence, professionnels : la CNIL sensibilise des publics très différents à la question des données personnelles et instaure un dialogue constant avec ses communautés, quel que soit leur niveau de connaissance de la Loi Informatique et Libertés.

Selon la plateforme TalkWalker/auraMundi*

Le cap des 50.000 followers sera bientôt atteint par le compte Twitter de la @CNIL qui enregistre une année record pour les conversations sociales citant la CNIL. Son action internationale, ses actualités contentieuses et ses infos pédagogiques ont été largement commentées dans plus de 110.000 tweets* !

Chaque année, des centaines d'internautes utilisent les réseaux sociaux pour exercer leurs droits informatiques et libertés auprès des responsables de traitement ou simplement pour demander une information à la CNIL. En 2016, la

CNIL augmentera le nombre de formats pédagogiques publiés sur Twitter, LinkedIn - pour l'information des entreprises - et sur sa page Facebook relayée par plus de 22.000 ambassadeurs de la vie privée en ligne.

La CNIL du point de vue des citoyens

Depuis 2004, la CNIL mesure sa notoriété. L'enquête IFOP a été menée auprès d'un échantillon de 1 005 personnes, représentatif de la population française âgée de 18 ans et plus. Les interviews ont eu lieu par téléphone du 4 au 5 décembre 2015.

64 %
DES PERSONNES CONNAISSENT LA CNIL

LES RÉPONSES AU PUBLIC

> BESOIN D'AIDE

Le service des relations avec les publics (SRP) répond, par différents canaux, aux demandes d'information et d'orientation émanant des particuliers comme des professionnels.
En plus de la gestion du standard téléphonique de la CNIL, le service assure une permanence de renseignement juridique par téléphone du lundi au vendredi. Cette permanence renseigne les usagers et les oriente dans leurs démarches avec la CNIL. Un nouveau service d'assistance en ligne, « Besoin d'aide ? », est disponible depuis juillet 2015 sur cnil.fr : il propose des questions/réponses très pratiques, rédigées afin d'être accessibles à tous ; il offre la possibilité aux usagers, lorsqu'ils n'ont pas trouvé de réponse à leur question, d'adresser des requêtes par voie électronique. Le nombre de consultations des questions/réponses effectuées entre le 1er juillet et le 31 décembre 2015 (122 603) et celui des requêtes reçues attestent de ce que le service répond à un véritable besoin des usagers.

▸ **34 367 courriers**
▸ **136 251 appels au 01.53.73.22.22 (+2,3 % par rapport à 2014)**
▸ **75 860 appels pour la permanence juridique (+6,1 % par rapport à 2014)**
▸ **10 646 requêtes par voie postale et électronique (+17,7 % par rapport à 2014)**

INFO +

Besoin d'aide ?

- 400 Questions/ Réponses diffusées sur www.cnil.fr
- 4 648 requêtes électroniques reçues
- Top 5 des Questions les plus consultées en 2015

- Faut-il déclarer un site web à la CNIL ?
- «Article 31» : comment obtenir la liste des déclarations faites à la CNIL par un organisme public ou privé ?
- Comment faire une déclaration à la CNIL ?
- Windows 10 : quelles précautions élémentaires prendre ?
- Déclarer à la CNIL, c'est gratuit ?

L'ÉDUCATION AU NUMÉRIQUE, UNE MISSION STRATÉGIQUE POUR LA CNIL

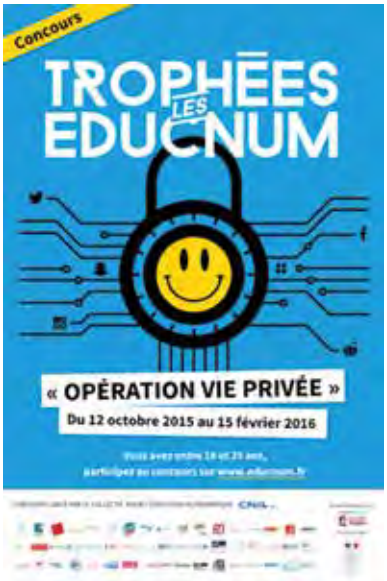
Durant l'année 2015, la CNIL a poursuivi l'animation du Collectif « éducation au numérique » et le pilotage des actions estampillées « Collectif educnum ». Le Collectif a accueilli de nouvelles structures en son sein (Association de la fondation étudiante pour la ville, Conférence des Présidents d'Universités, fondation SNCF, fondation Simplon) afin de renforcer ses actions d'éducation au numérique vers les publics jeunes. Elle a fortement développé ses relations avec le ministère de l'éducation nationale et multiplié les visites de terrain.

Un nouveau site pour le Collectif EDUCNUM

Un nouveau site www.educnum.fr, piloté par la CNIL, permet aux membres du Collectif de communiquer plus largement sur leurs actions. Des actualités sur des thématiques ou des évènements liés à l'éducation au numérique sont publiées régulièrement. Les ressources pédagogiques « vie privée » du site Jeunes de la CNIL ont été mises à jour et progressivement transférées sur le site Educnum. Le site s'est par ailleurs enrichi de nouveaux contenus et outils pédagogiques sur le thème de la protection de la vie privée : atelier sur « les jeunes et les réseaux sociaux », vidéos, fiches pédagogiques à l'attention des enseignants, des animateurs et des parents, etc.

Les suites des Trophées EDUCNUM

Compte tenu du succès de la 1ère édition des Trophées EDUCNUM, la CNIL et le Collectif ont lancé la 2ème édition en octobre 2015. Ce concours, qui a pour objet de susciter et récompenser des projets innovants pour sensibiliser les plus jeunes aux bons usages du web, est désormais ouvert à tous les jeunes de 18 à 25 ans. Il a bénéficié du soutien des ministères de l'éducation nationale et de la Jeunesse et Sports. Une campagne radio diffusée par Skyrock a permis de toucher une cible plus large de candidats au concours. La CNIL a mené des ateliers dans des écoles, des universités et des lieux de coworking, à Paris et en région, pour accompagner les jeunes dans la construction de leurs projets. Les lauréats du Prix Spécial du Jury « Data fiction, le site dont vous êtes le héros » étaient également présents en soutien. Les lauréats du Grand Prix du jury pour le web documentaire « Les aventures croustillantes de Prince chip » ont écrit les scénarios de trois nouveaux épisodes, sur les thèmes de l'arnaque, les cookies et l'usurpation d'identité, pour une mise en production début 2016. Dans le prolongement des Trophées EDUCNUM, le Collectif était une nouvelle fois au rendez-vous de Futur en Seine, le 11 juin 2015, sous forme d'un atelier sur le thème « Comment sensibiliser les plus jeunes aux bons usages du web ? ». De plus, le ministère de l'éducation nationale et la CNIL ont décidé d'agir ensemble en lançant, en décembre 2015, un concours national vers les écoles élémentaires, afin de développer une éducation aux usages responsables d'Internet.).



Sensibiliser, encore et toujours

La CNIL a poursuivi ses actions de formation des formateurs afin de démultiplier les messages d'éducation citoyenne au numérique, en direction de différents publics relais : Jeunes Ambassadeurs des Droits de l'Enfant, community managers des clubs de football, étudiants…

Au plan international, l'éducation au numérique en actions

L'éducation au numérique s'est aussi fortement développée au plan international, avec la mise en œuvre du plan d'action 2014-2015 adopté par le groupe de travail piloté par la CNIL, composé de plus de 40 autorités de protection des données.

Ce plan d'action comprend :

- La création d'une plateforme web de mutualisation des ressources pédagogiques dans le domaine de la protection des données ouverte à toutes les autorités de protection des données ;
- L'élaboration d'un kit tutoriel destiné à la formation des formateurs sur le thème de la protection des données qui se poursuivra en 2016 ;
- La conception d'un guide pratique pour la conduite de concours par les autorités.

Enfin, un atelier a été organisé par la CNIL en marge de la 37ème conférence internationale des commissaires à la protection des données et à la vie privée. ■

Conseiller et réglementer

L'activité de conseil et de réglementation de la CNIL est variée : avis sur des projets de texte d'origine gouvernementale concernant la protection des données personnelles ou créant de nouveaux fichiers, élaboration de cadres juridiques simplifiant l'accomplissement des formalités préalables, autorisations, recommandations, conseils. Dans toute cette gamme d'activités, la CNIL veille à la recherche permanente d'un juste équilibre, au service du citoyen, entre la protection des libertés publiques et la mise en œuvre d'outils opérationnels des administrations et organismes publics et privés.

LA SIMPLIFICATION DES FORMALITÉS ADMINISTRATIVES : UNE PRIORITÉ POUR LA CNIL

50 339
FORMALITÉS SIMPLIFIÉES

21
AUTORISATIONS UNIQUES ADOPTÉES

1
NORME SIMPLIFIÉE

5
ACTES RÉGLEMENTAIRES UNIQUES

La CNIL est engagée depuis plusieurs années dans un processus de simplification administrative auprès des organismes publics et privés. Elle peut adopter des dispenses de déclaration, des normes simplifiées pour les traitements soumis à régime déclaratif, des autorisations uniques pour les traitements soumis à régime d'autorisation et des méthodologies de référence pour les recherches les plus courantes en matière de santé. Pour les traitements du secteur public, la Commission rend des avis sur des projets d'actes réglementaires uniques dont la création reste cependant à l'initiative des administrations concernées.

Les normes de simplification adoptées par la CNIL permettent d'alléger considérablement les formalités, tout en homogénéisant les pratiques et en promouvant les plus vertueuses. En effet, les organismes n'ont qu'à faire un engagement de conformité à la norme concernée préalablement à la mise en œuvre de leur traitement. Cet engagement peut être accompli en ligne sur le site de la CNIL en quelques minutes.

En 2015, les effets de la simplification des formalités ont été particulièrement sensibles, notamment dans le champ des autorisations uniques (plus de 6 500 engagements de conformité reçus). Elaborés après concertation avec les acteurs d'un secteur, ces cadres demandent un investissement ponctuel important, mais se traduisent par la simplification de dizaines de milliers de démarches (plus de 50 000 dossiers pour 2015).

2 571
DÉCISIONS ADOPTÉES

456
DÉLIBÉRATIONS ADOPTÉES EN SÉANCE PLÉNIÈRE

1 076
AUTORISATIONS DE TRANSFERTS DE DONNÉES HORS UE

▸▸▸ Nombre d'engagements de conformité à une norme de simplification reçus par la CNIL depuis 2010

Type de normes de simplification	2010	2011	2012	2013	2014	2015	Total
Autorisations uniques	4 263	4 242	**4 734**	**4 366**	**4 623**	**6 582**	28 810
Méthodologies de référence	243	278	**256**	**293**	**365**	**609**	2 044
Normes simplifiées	38 983	41 306	**41 156**	**43 985**	**42 640**	**40 526**	248 596
Actes réglementaires uniques	1 378	1 475	**2 258**	**2 216**	**2 019**	**2 622**	11 968
Total général	**44 867**	**47 301**	**48 404**	**50 860**	**49 647**	**50 339**	291 418

FOCUS

La simplification des formalités CNIL dans le secteur de la santé

La CNIL a adopté en 2015 une autorisation unique et une méthodologie de référence dans le domaine de la santé afin de mettre à la disposition des acteurs concernés des outils de conformité adaptés à leurs pratiques, dans des conditions respectueuses de la protection des données personnelles :

- Autorisation unique AU-043 relative au dépistage organisé du cancer du sein et du cancer colorectal,
- Méthodologie de référence MR-002 relative aux études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro.

Les travaux de simplification en matière de recherche dans le domaine de la santé se poursuivent en 2016, afin de faciliter les démarches et de favoriser la mise en œuvre des projets dans des délais garantissant la compétitivité de la France dans ce secteur.

Deux projets ont été soumis à la concertation auprès d'organismes publics et privés représentatifs en octobre 2015 et devraient aboutir en 2016 :

- l'évolution de la méthodologie de référence 001 relative aux traitements de données à caractère personnel dans le cadre des recherches biomédicales,
- l'élaboration d'une nouvelle méthodologie de référence, portant sur les recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement écrit des personnes concernées.

754
AUTORISATIONS DE RECHERCHE EN MATIÈRE DE SANTÉ

142
AUTORISATIONS D'ÉVALUATION DES PRATIQUES DE SOINS

LES AVIS ET AUTORISATIONS

Lors des 32 séances plénières tenues en 2015, la Commission a examiné les demandes d'avis et les demandes d'autorisations qui sont de plus en plus nombreuses.

L'avis de la CNIL sur le projet de loi pour une République numérique

La CNIL s'est prononcée, lors de la séance plénière du 19 novembre 2015, sur l'avant projet de loi pour une « République numérique », dans sa version alors envisagée par le Gouvernement. Le projet de texte adopté en première lecture à l'Assemblée nationale comporte de nombreuses modifications, qui tiennent notamment compte de l'avis de la CNIL.

Une nécessaire cohérence avec les autres textes en préparation

Ce projet de loi intervient alors que le projet de règlement du Parlement européen et du Conseil relatif à la protection des données personnelles et à la libre circulation de ces données, est en cours de finalisation. Ce texte, d'application directe, doit assurer l'unification du droit européen et apporter un standard élevé de protection pour les citoyens européens avec notamment un renforcement de leurs droits. Le projet de loi pour une République numérique devra donc s'y conformer, ce qui impliquera de l'adapter en cours de procédure.

La CNIL a rappelé l'importance de veiller à la cohérence des dispositions adoptées en matière de diffusion de données publiques (open data), plusieurs lois récentes ou projets de loi, notamment le projet de loi relatif à la santé et la loi du 7 août 2015 portant nouvelle organisation territoriale de la République (« NOTRe »), comportant des dispositions spéciales en la matière.

Des droits renforcés, à harmoniser avec le droit européen

De manière générale, la Commission a salué le renforcement des droits des citoyens. Ainsi, la consécration du droit à la libre disposition de ses données, c'est-à-dire le droit de l'individu de décider de la communication et l'usage de ses données personnelles, va dans le sens d'une meilleure maîtrise par les individus de leurs données. Cette consécration est une continuité des droits déjà reconnus par la loi Informatique et Libertés tels que le droit d'accès, le droit d'opposition ou le droit de suppression.

La CNIL a également souligné l'intérêt de légiférer sur le devenir des données personnelles des personnes décédées et le renforcement de l'information des personnes, ainsi que sur la loyauté des plateformes.

Dans la mesure où le projet de règlement européen prévoit des dispositions spécifiques sur les mineurs et introduit un droit à la portabilité, le projet de loi devra être conforme, sur ces deux points, au texte européen. À cet égard, le « droit à la portabilité » introduit par le projet de loi a un périmètre et un champ d'application différent de celui du projet de règlement, qui porte exclusivement sur les données personnelles.

L'action de la CNIL confortée

Le projet de loi tend également à renforcer les pouvoirs de la CNIL et à conforter ainsi son engagement dans la régulation du numérique et son activité d'accompagnement des particuliers, des entreprises et des administrations. La question de la révision du montant des sanctions susceptibles d'être prononcées par la CNIL, actuellement de 150 000 euros, est actuellement en débat devant le Parlement.

244
AUTORISATIONS

9
REFUS D'AUTORISATION

122
DEMANDES D'AVIS (ADMINISTRATIONS CENTRALES)

À SUIVRE

La CNIL, animatrice du débat public sur l'éthique du numérique

Le projet de loi prévoit de confier à la CNIL la mission de conduire une réflexion sur les débats éthiques et les questions de société soulevés par l'évolution des technologies numériques. Régulateur des données personnelles, situé pour cela au cœur du numérique, la CNIL n'en a certes jamais ignoré les enjeux éthiques.
L'article 1er de la loi Informatique et Libertés établissait ainsi que « l'informatique doit être au service de chaque citoyen ». La CNIL n'entend cependant nullement monopoliser le débat public sur l'éthique du numérique. Son rôle sera plutôt celui d'animatrice et de facilitatrice de ce débat, impliquant tous les acteurs concernés (chercheurs, entrepreneurs, administration, société civile).
La CNIL compte tout particulièrement faire en sorte que cette réflexion puisse être l'occasion d'une appropriation par les citoyens des débats liés aux enjeux éthiques du numérique.

Ouverture des données et respect de la vie privée

Le projet de loi vise à développer l'open data, en prévoyant une large publication des données administratives et en posant le principe de libre réutilisation des données publiques mises en ligne.

La CNIL s'est engagée depuis plusieurs années dans l'accompagnement de l'open data, afin que l'ouverture des données publiques soit respectueuse des droits des personnes et de la vie privée. A cet égard, plusieurs garanties ont été apportées par le projet de loi, notamment à la suite de l'avis de la CNIL :

- Les conditions de communicabilité des documents administratifs, qui visent notamment à protéger la vie privée, ne sont pas modifiées.
- La publication de documents comportant des données à caractère personnel ne pourra intervenir qu'après anonymisation des données, sauf si une disposition législative ou réglementaire autorise une diffusion sans anonymisation préalable ou si la personne intéressée y a consenti.
- La réutilisation des données reste subordonnée au respect de la loi Informatique et Libertés, ce qui implique notamment qu'une base de données anonymisée ne puisse pas servir à ré-identifier des personnes.
- Enfin, la CNIL pourra certifier la conformité à la loi de méthodologies d'anonymisation, ce qui renforcera la sécurité juridique pour les administrations concernées.

Dans son avis, la Commission a estimé que ces dispositions ne remettaient pas en cause l'équilibre nécessaire entre transparence administrative, d'une part, et protection de la vie privée et des données personnelles, d'autre part. La conciliation de ces deux intérêts constitue en effet une condition essentielle à la mise en œuvre de toute politique d'ouverture des données.

La Commission a dès lors formulé plusieurs observations concernant les modalités effectives de respect de cet équilibre. En particulier, elle a rappelé que la vérification préalable des processus d'anonymisation, sous le contrôle de la CNIL, constitue un impératif majeur pour une ouverture des données respectueuse des droits des personnes.

Une simplification des procédures pour la statistique et la recherche publique, dans le prolongement des propositions de la CNIL

Le projet de loi comporte enfin des dispositions relatives à la recherche publique, en matière statistique ou scientifique. Il vise ainsi à simplifier les formalités préalables aux recherches publiques utilisant le NIR. La CNIL s'est montrée favorable à cette simplification, qu'elle avait proposée depuis plusieurs années, dès lors, d'une part, que le NIR fait l'objet d'un cryptage robuste et, d'autre part, que les recherches publiques à des fins scientifiques conduites sur ce fondement devront être autorisées par la Commission.

> La CNIL pourra certifier la conformité à la loi de méthodologies d'anonymisation renforçant la sécurité juridique pour les administrations.

FOCUS

Loi sur la modernisation de notre système de santé

Au titre de ses missions consultatives, la CNIL a été sollicitée sur le projet de loi de modernisation de notre système de santé. Elle a notamment participé à de nombreuses auditions et été sollicitée pour avis.

La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé est désormais promulguée. Elle modifie le régime d'autorisation des traitements de données à caractère personnel ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou activités de soins ou de prévention.

Afin d'unifier le régime d'autorisation de ces traitements qui relevaient respectivement des chapitres IX et X de la loi Informatique et Libertés, la loi a fusionné ces deux chapitres en un nouveau chapitre IX qui soumet ces traitements de données à une autorisation préalable de la CNIL, après avis, selon les études, soit d'un comité d'expertise soit d'un comité de protection des personnes. L'Institut national des données de santé (INDS), créé par cette même loi, pourra également éclairer la décision de la CNIL sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation envisagée.

La CNIL conserve le pouvoir d'homologuer et de publier des méthodologies de référence destinées à simplifier la procédure d'examen concernant les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Celles-ci seront établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés.

L'effectivité de la nouvelle procédure d'autorisation reste cependant soumise à la publication de plusieurs textes d'application, prévus par la loi, après avis de la CNIL. Dans l'attente de la publication de ces textes d'application, les procédures actuellement en vigueur en vertu des chapitres IX et X de la loi Informatique et Libertés restent applicables.

LES RELATIONS AVEC LE PARLEMENT

Au cours de l'année 2015, la CNIL a participé à une vingtaine d'auditions parlementaires et répondu aux nombreuses sollicitations juridiques et techniques liées à la fois à la protection des données personnelles mais, plus largement, aux évolutions du monde numérique.

Travaux législatifs : projets et propositions de loi

La CNIL a répondu aux invitations des rapporteurs des commissions permanentes dans les deux assemblées, qui ont eu à connaître trois projets de loi pour lesquels la CNIL avait été saisie pour avis par le gouvernement : le projet de loi de modernisation de notre système de santé, le projet de loi relatif au Renseignement et le projet de loi pour une République numérique. S'agissant de ces deux derniers textes, les avis de la CNIL ont été rendus publics à la demande du président de la commission des lois de l'Assemblée nationale.

Les parlementaires ont également recours de plus en plus fréquemment à l'expertise de la CNIL à l'occasion de la discussion des propositions de loi inscrites à l'agenda des assemblées. La CNIL a ainsi été entendue sur les propositions de loi portant sur la dématérialisation du Journal officiel de la République française et relative à la prévention et à la lutte contre les atteintes graves à la sécurité publique, contre le terrorisme et contre la fraude dans les transports publics de voyageurs.

Missions parlementaires de réflexion, de prospective et de contrôle

La CNIL a participé aux travaux de missions d'information mises en place en 2015, notamment l'usage de la biométrie en France et en Europe, le droit pénal à l'heure d'internet. Elle s'est également associée, comme elle le fait régulièrement, aux travaux de prospective de l'Office parlementaire d'évaluation des choix scientifiques et technologiques consacrés aux « enjeux éthiques et sociétaux de l'épigénétique » ou encore « aux robots et la loi ».

Elle a également répondu à la demande des sénateurs dans le cadre de deux commissions d'enquête : l'une consacrée à l'organisation et les moyens de lutte contre les réseaux djihadistes en France et en Europe ; l'autre relative au bilan et au contrôle de la création, de l'organisation, de l'activité et de la gestion des autorités administratives indépendantes. ■

Accompagner la conformité

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

LE CIL, UN EXPERT AU CŒUR DE LA CONFORMITÉ

En gérant les données personnelles qui leur sont confiées dans le respect des règles, les collectivités territoriales, les entreprises publiques ou privées ainsi que les associations, réduisent leur exposition aux risques et optimisent leurs investissements. Le CIL est un véritable acteur interne de la conformité, qui veille à la sécurité juridique et informatique de son organisme. Plus de 16.300 organismes ont déjà fait le choix de désigner un CIL pour piloter ces sujets. En 2015, le correspondant Informatique et Libertés (CIL) a fêté son 10ème anniversaire à l'aube de l'entrée en vigueur du règlement européen de l'UE sur la protection des données personnelles, qui le place au cœur de la gouvernance des nouveaux outils de conformité. Les actions menées cette année par la CNIL pour accompagner les CIL peuvent se résumer en deux mots clés : fédérer et préparer l'avenir.

Fédérer

Réguler les données personnelles implique de connaître précisément les spécificités métier des différents acteurs, pour pouvoir prendre rapidement position sur les sujets émergents ou diffuser des bonnes pratiques à partager. Consciente du rôle tenu par la communauté des CIL dans ce contexte, la CNIL a souhaité, à l'occasion des 10 ans de ce métier, orga-

> **Désigner un CIL dès aujourd'hui, c'est anticiper sur les nouvelles exigences posées.**

niser une Convention qui s'est tenue à la chambre de Commerce de Paris-Ile de France le 13 octobre 2015. Cet évènement a réuni au total 1 300 CIL qui ont pu suivre ces travaux : environ un millier à distance grâce à une retransmission en direct et une application participative et plus de 300 présents dans la salle.

Le bilan de la décennie a été dressé et a fait apparaitre en particulier le niveau d'expertise attendu auprès de la CNIL en raison de la complexification des demandes de conseil des CIL issus d'organismes en pleine transition numérique.

Cette journée a aussi été l'occasion d'évoquer la prochaine évolution de la profession telle qu'elle est envisagée par le règlement européen et la façon dont les CIL peuvent d'ores et déjà s'y préparer. Une enquête en ligne a été réalisée à cet effet pour affiner la connaissance de ce métier et faire ressortir ses besoins.

Les divers ateliers et table ronde ont permis de partager des bonnes pratiques et de bénéficier des retours terrains nécessaires à une bonne co-régulation et à la construction d'outils pratiques. Ainsi, des sujets riches et variés ont pu être abordés librement tels que « Comment se préparer à l'évolution européenne de la protection des données », « Sécurité et vie privée à l'heure du tout connecté », « Comment valoriser la conformité ou comment convaincre », « Le CIL dans la mise en œuvre du principe d'*accountability* » ou « Pratiques contractuelles, comment bien encadrer les relations avec vos partenaires ? ».

Le succès rencontré par cet évènement est un signal clair pour la CNIL, qui dans ses conclusions a réaffirmé tout l'intérêt qui s'attache à ce nouveau métier, avec en perspective une campagne de communication auprès des organismes qui ont désigné un CIL afin de les sensibiliser aux évolutions prévues par le règlement européen. Par ailleurs, la CNIL va renforcer ses actions pour une collaboration à la fois plus ciblée (par secteur d'activité) et plus en profondeur (sur les sujets abordés). Enfin, elle veut aider au déploiement de nouveaux réseaux, prenant appui et exemple sur les bons résultats obtenus avec les réseaux existants, tels que SUPCIL (réseau de CIL des établissements d'enseignement supérieur et de recherche).

INFO +

Résultats enquête IFOP sur le métier de CIL

Afin de connaitre plus finement la population des CIL en pleine évolution et de pouvoir adapter ses procédures et outils, la CNIL a mené une étude en ligne pendant 3 semaines (fin juin à mi-juillet 2015) auprès d'un échantillon de 1308 CIL. Les résultats, présentés lors de la Convention des 10 ans des CIL en octobre 2015, font apparaitre des informations intéressantes :

- **53% des CIL viennent d'organismes privés et 47% sont issus de la sphère publique ;**
- **95% des CIL sont désignés en interne de leur organisme et font donc peu appel à des prestataires pour exercer ce métier (des limitations juridiques existent actuellement dans la loi mais vont disparaitre dans le règlement européen) ;**
- **si la plupart des CIL sont issus d'un cursus technique, les profils sont assez diversifiés (47% sont issus du secteur des TIC/SI, 29% occupent ou ont occupé des fonctions juridiques, 10% des fonctions administratives et 10% environ occupent des fonctions d'audit ou de conformité).**
- **73% sont favorables à la mise en place d'une évaluation des compétences lors de leur entrée en fonction**

On découvre également que plus de 57% des CIL exercent leur fonction moins de 2 jours par mois et que 50% n'ont mis aucune procédure en place, que ce soit pour traiter les réclamations ou pour organiser les équipes en cas de contrôle de la CNIL. Enfin, plus de 80% des CIL actuels n'ont engagé aucune réflexion sur l'évolution de leur fonction et attendent les préconisations de la CNIL ou du G29 (56%). Alors que le CIL sera rendu obligatoire dans de nombreux cas dès 2018, du fait de l'entrée en application du règlement européen, la diffusion d'informations et de bonnes pratiques est donc une priorité stratégique de la CNIL.

Préparer l'avenir

Alors que la désignation d'un CIL est actuellement optionnelle, le futur délégué à la protection des données sera au cœur du modèle proposé par le règlement européen qui prévoit en particulier l'obligation de mettre en œuvre des mesures dynamiques de protection des données personnelles et d'être en mesure de les démontrer (souvent connue sous le terme anglais d'*accountability*).

En effet, bientôt obligatoire pour de nombreux organismes, son rôle de pilote de la conformité est consacré au travers d'un renforcement de ses missions et moyens.

Il devient un véritable « chef d'orchestre » en la matière, chargé notamment d'informer, de conseiller le responsable et les employés sur leurs obligations et, en ce qui concerne l'analyse d'impact sur la vie privée, de surveiller son exécution. Il sera également le point de contact de l'autorité de régulation avec laquelle il coopère. En tant que pilote de la conformité, il s'assurera de la bonne tenue de la documentation relative aux traitements de données personnelles.

À cet effet, le futur délégué devra être associé d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données, et détenir les ressources nécessaires à ▸▸▸

l'exécution de ses missions (notamment pour accéder aux données et aux traitements) ainsi qu'au maintien de ses connaissances.

Fort de ces nouveaux éléments, désigner un CIL dès à présent permet d'organiser au plus tôt la conformité interne aux nouvelles règles de la protection des données personnelles.

Dans ce contexte, la CNIL, qui a fait le choix depuis plusieurs années de mettre en place un service dédié aux CIL, continuera à développer ses actions de communication auprès des CIL et de leurs responsables, tout en poursuivant l'adaptation des outils nécessaires au changement d'échelle prévu par le règlement européen (accompagnement dans la mutualisation des délégués à la protection des données, élaboration de référentiels et de guides de bonnes pratiques, e-learning, etc.).

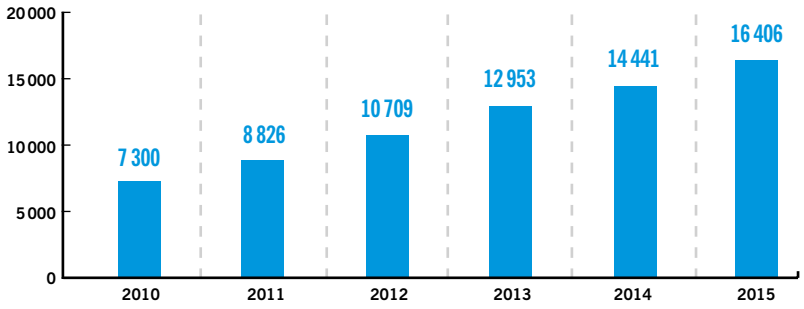
Le CIL devient un véritable « chef d'orchestre » de la conformité

16 406
ORGANISMES ONT DÉSIGNÉ UN CIL, SOIT 4321 CIL

1 163
PERSONNES ACCUEILLIES LORS DE 34 ATELIERS CIL

2 100
DEMANDES DE CONSEIL JURIDIQUE TRAITÉES

Nombre d'organismes ayant désigné un CIL entre 2010 et 2015



LES PACKS DE CONFORMITÉ

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

À SUIVRE

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

Les packs dans le secteur économique : développer et accompagner dans la durée

Le lancement du Pack de conformité banque

Le secteur banque regroupe l'ensemble des établissements bancaires et organismes financiers qui offrent leurs services aux particuliers notamment. Il s'agit d'un secteur fortement réglementé, soumis à de nombreuses contraintes qui concernent à la fois les modalités de gestion de la relation client mais aussi, et de plus en plus, la mise en œuvre de traitements destinés à s'assurer de la légalité des transactions.

Comme beaucoup de secteurs économiques, le secteur banque connaît une évolution sous l'influence du numérique tant dans ses fonctions traditionnelles que sur le segment du paiement à distance. Pour la CNIL, le secteur bancaire est particulièrement important au regard de la place qu'occupent ces organismes dans la vie quotidienne de leurs clients. À ce titre, la CNIL souhaite faciliter la mise en conformité et accompagner ces professions dans leur mutation numérique par l'adoption d'un pack dédié.

Ce pack concrétise une volonté partagée d'aborder les traitements mis en œuvre par la profession dans leur globalité et de fournir des outils encore mieux adaptés aux besoins actuels. Outre un travail de reprise de l'existant et notamment des normes les plus

anciennes, le travail commun doit permettre d'aborder des questions nouvelles ou particulièrement sensibles tant pour la profession, les particuliers ou l'Etat.

C'est ainsi que le premier cycle de discussion a abouti en juillet 2015 à la production d'**une première autorisation unique consacrée à la gestion des comptes bancaires et coffres forts inactifs** (autorisation unique n°45). L'année 2016 verra la finalisation de **l'autorisation unique en matière de lutte contre la fraude et la révision des normes métiers liées à la gestion des crédits ou des prêts.**

Poursuivre la relation de confiance avec le suivi des packs existants

À l'issue des travaux des années 2013 et 2014, le secteur de l'assurance a pu bénéficier d'un pack complet entièrement dimensionné pour assurer aux sociétés, mutuelles d'assurance, institutions de prévoyance et intermédiaires une conformité à la loi Informatique et Libertés.

À ce titre, la CNIL a enregistré près de **1 300 engagements de conformité pour les normes simplifiées liées à la gestion des contrats d'assurance et à la gestion commerciale des clients.** Plus encore l'adhésion du secteur de l'assurance s'est traduit par l'adoption rapide par les compagnies des autorisations uniques du second volet du pack conformité qui permettent le traitement du NIR, de données d'infractions ou encore la lutte contre la fraude dans le respect de la législation.

En parallèle, les services de la Commission sont présents lors de manifestations organisées par les assureurs tant pour expliquer le pack que pour dialoguer autour de thèmes comme le Big data dans l'actuariat ou la relation client.

Avec plus de recul encore, l'expertise de la CNIL acquise dans le secteur de l'énergie est sollicitée par l'ensemble de la filière pour assurer la mise en application de la loi transition énergétique et croissance verte comme pour accompagner le déploiement du compteur Linky.

Forte d'une recommandation sur les réseaux de distribution électrique intelligents (2012) ou d'un **pack compteur communicant** (2014) la CNIL mobilise ses forces pour faciliter l'émergence de solutions respectueuses de la vie privée des consommateurs et répondant aux attentes de professionnels notamment en ce qui concerne l'ouverture des données.

Les modalités de déploiement des compteurs Linky sur la période 2015-2021, qui vont concerner 35 millions de foyers, reflète un équilibre acquis au terme de nombreux échanges avec les fournisseurs d'énergie, les gestionnaires de réseaux, le ministère de l'écologie et le médiateur de l'énergie.

?

DÉFINITION

Club de conformité assurance

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

Les packs de conformité de la sphère sociale et médico-sociale

Le lancement du pack dans le secteur social et médico-social

Il s'agit d'un secteur hétérogène, tant du point de vue des publics accompagnés (personnes âgées, personnes handicapées, familles en difficultés sociales, etc.) que des modes d'intervention (accompagnement administratif, judiciaire et social, logement et cadre de vie, insertion sociale et professionnelle, santé, accompagnement à la scolarité, animation socio-éducative).

De nombreux échanges avec les acteurs, représentants des travailleurs sociaux et organismes œuvrant dans le champ de l'action sociale et médico-sociale, sont intervenus tout au long de l'année 2015. Ils ont permis à la CNIL de mieux appréhender les particularités du secteur, tenant en particulier à la gestion de nombreuses données sensibles, et les difficultés rencontrées dans l'application de la loi Informatiques et Libertés.

Le *pack* de conformité qui résulte de ces travaux sera adopté au premier trimestre 2016 par la CNIL. Il se compose d' outils de simplification, de fiches explicatives et d'un guide opérationnel

▸ **Les trois outils de simplification des formalités au travers de référentiels thématiques :**

- une autorisation unique portant sur les traitements mis en œuvre dans le cadre de l'accueil et l'accompagnement des personnes handicapées et des personnes âgées,
- une autorisation unique relative aux traitements mis en œuvre dans le cadre de l'accueil, l'orientation et l'accompagnement social des personnes
- une autorisation unique relative aux traitements mis en œuvre dans le cadre de la prévention et la protection de l'Enfance.

▸ **Les fiches explicatives** rappelant les grands enjeux dans ce secteur (données sensibles, partage des informations, sécurité…). Elles sont destinées à accompagner les acteurs dans l'appropriation des règles relatives à la protection des données personnelles grâce à des informations pratiques (recommandations de la CNIL, bonnes pratiques, etc.)

▸ **Le guide opérationnel** consistant à accompagner les acteurs dans leur démarche de mise en conformité en leur proposant un recueil des actions concrètes à mener.

Le suivi du pack sur le logement social et les travaux menés sur la « silver économie »

Les packs de conformité s'accompagnent d'actions de sensibilisation des différents acteurs concernés (responsables de fichiers et chargés de la mise en œuvre). La CNIL est ainsi régulièrement associée à des manifestations organisées par les organismes du secteur social et médico-social pour développer sa mission de pédagogie auprès des professionnels et notamment dans le secteur du logement social. ■

À SUIVRE

Dans le prolongement des travaux menés pour l'élaboration du pack social, et dans le cadre du partenariat entre la CNIL et la FIEEC, un groupe de travail a été créé pour élaborer « une seconde brique » au pack sur les compteurs communicants. Elle est consacrée aux conditions de collecte et de traitement des données personnelles par les appareillages de domotique et de dispositifs d'assistance destinés à préserver l'autonomie des séniors.

DÉFINITION

Le label

Le Label atteste de la conformité d'un produit ou d'une procédure aux exigences des référentiels de la CNIL.

Il permet :
- De disposer d'un avantage concurrentiel
- D'afficher un indicateur de confiance,
- D'augmenter sa crédibilité,
- De prouver son attitude éthique et responsable,
- D'anticiper le futur règlement européen.

LE LABEL : UN AVANTAGE CONCURRENTIEL

Créé il y a un an, le label « Gouvernance » répond aux attentes des organismes tant privés que publics, de petites et de grandes tailles, soucieux de mettre en avant leur gestion des données personnelles de manière générale.

Le premier organisme bénéficiaire de ce label est le Département des Alpes Maritimes. Cet exemple ouvre désormais la voie aux 650 collectivités territoriales et Établissements Publics de Coopération Intercommunale qui disposent déjà d'un CIL et qui peuvent donc potentiellement prétendre à l'obtention de ce label. Depuis, d'autres demandes de label gouvernance ont été examinées et pourraient donner lieu à des obtentions en 2016.

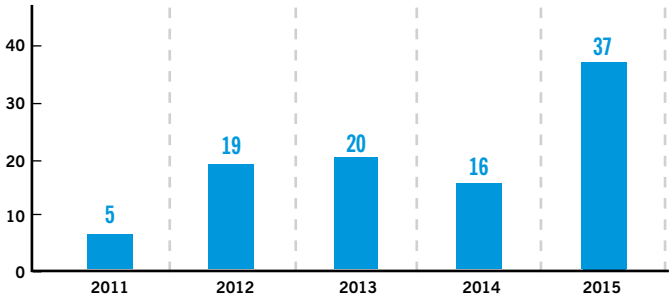
À la fois gage de sécurité juridique et informatique et instrument de valorisation, le label CNIL « gouvernance » est la démonstration de l'engagement éthique et citoyen de l'organisme.

Il est donc l'une des principales applications du principe d'*accountability* (principe de responsabilité) prévu par le projet de règlement européen. Ce texte encourage d'ailleurs, de façon très explicite, la création et le développement des labels, certifications, et marques de protection des données, notamment à l'échelle de l'Union Européenne.

Les premiers renouvellements des labels délivrés en 2012

Délivrés pour la première fois en juin 2012, les labels « Formation » et « Audit de traitements » font l'objet, en 2015, des premières demandes de renouvellement. En effet, six mois avant échéance de la durée de validité de 3 ans, les labels CNIL doivent faire l'objet d'une demande de reconduction afin d'être prolongés. Cette demande peut prendre plusieurs formes : du simple courrier en indiquant si des éléments constitutifs de l'objet du label ont changé au dépôt d'un nouveau formulaire. Dans tous les cas, ces demandes font l'objet d'une instruction de la part de la Commission qui a décidé, pour le moment, de reconduire l'intégralité des 14 demandes qui lui ont été adressées. ■

Nombre de demandes reçues



4
RÉFÉRENTIELS

97
DEMANDES DE LABELS REÇUES

73
LABELS DÉLIVRÉS

6
MOIS DE DÉLAI MOYEN DE DÉLIVRANCE

LES RÈGLES D'ENTREPRISE CONTRAIGNANTES OU BCR (BINDING CORPORATE RULES)

Simplification des transferts encadrés par des BCR

Les BCR sont des codes de conduite définissant la politique d'un groupe d'entreprises en matière de transferts de données personnelles effectués en dehors de l'Espace économique européen.

Grâce à la mise en œuvre de mesures proactives – dites d'*accountability* (responsabilisation) en sus des principes de la directive 95/46/CE, les BCR sont de véritables programmes de mise en conformité et de gouvernance, puisqu'elles permettent de définir les grandes valeurs du groupe en matière de protection des données à l'échelle mondiale, mais aussi les mécanismes internes qui permettront d'assurer concrètement leur respect (audit, formation, réseau de délégués à la protection des données, etc.). ■

INFO +

Les autorisations uniques BCR

Reconnaissant que l'adoption de BCR témoigne de l'engagement d'un groupe multinational à protéger les données personnelles lorsqu'elles sont transférées entre ses entités, la CNIL délivre depuis 2015 une autorisation unique par groupe ayant adopté des BCR. Cela permet aux responsables de traitement soumis au respect des obligations de la loi Informatique et Libertés d'effectuer un engagement de conformité à l'autorisation unique BCR de leur groupe (ou du groupe de son sous-traitant en présence de BCR « sous-traitant ») via le formulaire de déclaration simplifiée. Une fois cet engagement effectué, les responsables de traitement doivent tenir à disposition des services de la CNIL une liste détaillée et à jour de chaque transfert. Ainsi, il n'est plus nécessaire de demander à la CNIL une autorisation par finalité de transfert.
En 2015, la CNIL a délivré 17 autorisations uniques BCR.

Répartition par secteur d'activité des 78 groupes ayant officiellement adopté des BCR au 31 décembre 2015

BANQUE-ASSURANCE	
BCR « responsable de traitement »	ABN AMRO, AXA*, Citigroup, ING Bank, JP Morgan Chase & Co., Rabobank, Société Générale*
INDUSTRIE	
BCR « responsable de traitement »	Aker Solutions, Airbus Group*, AkzoNobel, ArcelorMittal, BakerCorp, BMW, BP, Cargill, Continental, Corning*, D.E. Master Blenders 1753 (ex Sara Lee), DSM, Engie* (ex GDF SUEZ), Fluor, General Electric*, Johnson Controls, Michelin*, Osram, Safran*, Schlumberger, Schneider Electric*, Shell, Siemens, Total*
LUXE	
BCR « responsable de traitement »	Hermès*, LVMH*
NOUVELLES TECHNOLOGIES	
BCR « responsable de traitement »	Atmel, CA Plc, Flextronics, HP Enterprise*, HP Inc.*, Intel, Motorola Mobility, Motorola Solutions, NetApp, OVH*,
BCR « sous-traitant »	Salesforce*
BCR « responsable de traitement » et « sous-traitant »	Atos*, BMC Software*, Linkbynet*, Philips Electronics
SANTÉ	
BCR « responsable de traitement »	AstraZeneca, Bristol Myers Squibb*, Cardinal Health, CareFusion, GlaxoSmithKline, IMS Health, Novartis*, Novo Nordisk, Sanofi*, UCB
BCR « responsable de traitement » et « sous-traitant »	Align Technology
SERVICES	
BCR « responsable de traitement »	Accenture, Akastor, American Express, Ardian* (ex AXA Private Equity), CMA-CGM*, Deutsche Post DHL, Deutsche Telekom, eBay, EY (ex Ernst & Young), Hyatt, International SOS*, LeasePlan, Legrand*, Linklaters, Simon-Kucher & Partners, Spencer Stuart,
BCR « responsable de traitement » et « sous-traitant »	First Data, Sopra HR Software* (ex HR Access), TMF Group

*** groupes ayant désigné la CNIL comme autorité chef de file**

Protéger les citoyens

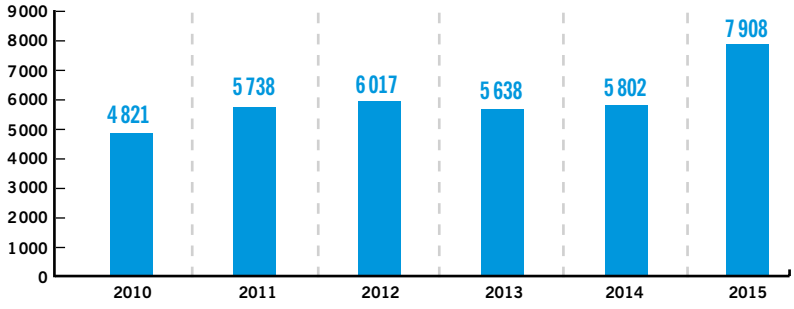
FORTE AUGMENTATION DU NOMBRE DE PLAINTES : 7 908 PLAINTES REÇUES EN 2015

Depuis quatre ans le nombre de plaintes était assez stable, grâce notamment à l'amélioration continue de l'information et de l'orientation des plaignants, mais l'année 2015 rompt avec cette tendance et affiche un nombre record de **7 908 plaintes reçues**. Cette augmentation s'explique en grande partie par l'amélioration du service de plainte en ligne qui permet désormais de saisir la CNIL sur un plus grand nombre de sujets.

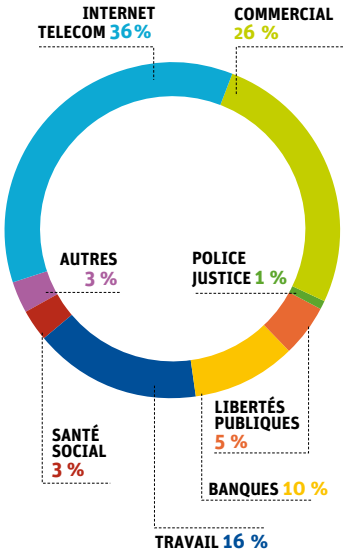
Comme les années précédentes, les plaintes concernent principalement les secteurs internet/téléphonie (36 %) et commerce (26 %) qui représentent à eux deux 62 % des plaintes.

La CNIL a reçu 7 908 plaintes dont plus de 65 % via le nouveau service de plaintes en ligne disponible sur son site. C'est 2000 de plus qu'en 2014.

Nombre de plaintes depuis 2010



Répartition des plaintes par secteur



INFO +

De manière générale, ces plaintes montrent que les citoyens souhaitent avoir une plus grande confiance dans l'économie numérique en ayant plus de sécurité au travers de l'utilisation des services en ligne.

Ils souhaitent également préserver leur vie privée, gérer leur e-réputation, connaître leurs droits et l'utilisation qui est faite de leurs données par les responsables de traitement.

Internet/télécom (36 % des plaintes reçues)

La majorité des personnes qui s'adressent à la CNIL s'opposent à la diffusion de leurs données personnelles (nom, coordonnées, commentaires, photos…) sur un annuaire, un site marchand, un site de rencontres, un réseau social, un blog ou un forum etc. Un nombre important de plaintes concerne également des problèmes de sécurisation des données.

Commerce/marketing (26 % des plaintes reçues)

Ces plaintes sont principalement relatives à de la prospection par courriel (spam) et à des demandes de radiation de fichiers publicitaires.

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

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

Banque/crédit (10 % des plaintes reçues).

▸ Le principal motif de saisine de la CNIL est l'absence de levée de l'inscription au fichier des incidents de crédit et de paiement (FICP) ou au fichier central des chèques et cartes après régularisation (FCC). Ces levées d'inscription tardives des fichiers gérés par la Banque de France, obtenues après l'intervention de la CNIL, et bien que les personnes ont régularisé leur situation, entraînent des préjudices importants. Ainsi, une inscription au FICP ne permet souvent pas aux personnes de se voir attribuer des moyens de paiement (chéquier, carte bancaire) et l'inscription au FCC entraîne les mêmes désagréments.

▸ La CNIL a également été saisie de plaintes relatives aux cartes bancaires sans contact (NFC).

Ces plaintes ont montré :

- que les clients n'étaient pas informés de manière satisfaisante de la mise en place de ce dispositif,
- les difficultés rencontrées pour obtenir une carte dépourvue de la fonction NFC.

Les établissements financiers, dans l'ensemble, se sont cependant conformés en 2015 aux recommandations de la CNIL en la matière.

Ressources humaines (16 % des plaintes reçues)

Le nombre de plaintes est en légère augmentation (+2%). Ces plaintes concernent pour la moitié des dispositifs de vidéo filmant les salariés sur leur lieu de travail, souvent de manière disproportionnée.

▸ Plus généralement, sont mis en cause des dispositifs de surveillance accrue des salariés : géolocalisation des véhicules ou des smartphones, accès à la messagerie, prise de contrôle à distance des postes de travail etc. Les employés sont souvent sommairement informés des dispositifs mis en place par leur employeur. L'intervention de la CNIL est également régulièrement sollicitée lorsque l'employeur refuse de communiquer au salarié les informations en lien avec son dossier professionnel.

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

Libertés publiques (5 % des plaintes reçues)

Ces plaintes concernent principalement des demandes d'anonymisation ou d'opposition à la diffusion en ligne d'articles de presse (voir Partie I Analyses sur vie privée et liberté de la presse).

▸ En raison des élections régionales qui se sont déroulées en2015, la CNIL a reçu de nombreuses plaintes relatives à des campagnes d'e-mailing politique ou des appels effectués par des automates. Plusieurs dysfonctionnements sont évoqués : non respect du droit d'opposition par les candidats ou les partis politiques, non respect du droit d'accès en particulier en ce qui concerne l'origine des données, détournements de fichiers (utilisation de fichiers d'associations ou de la collectivité pour de l'emailing politique), collecte déloyale.

Un étudiant a saisi la CNIL pour dénoncer l'installation de caméras dans les salles de classe. Ces caméras plaçaient sous surveillance constante les professeurs et les élèves. Elles étaient utilisées par la direction de l'établissement pour leur adresser des remarques sur leur comportement alors que ce dispositif avait pour vocation d'assurer la sécurisé des biens et des personnes. A la suite de l'intervention de la CNIL, l'établissement a retiré les caméras installées dans les salles de classe.

FOCUS

La e-réputation

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. Ces derniers ont à leur disposition deux démarches aux effets différents :
- 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. Si le site répond favorablement à la demande, il pourra supprimer le contenu qui ne sera plus accessible sur internet ou procéder à son anonymisation (par exemple, s'il s'agit d'un article ou d'un commentaire sur un forum, les références à l'identité de la personne seront supprimées mais pas le reste du contenu) ;
- soit effectuer une demande de déréférencement, c'est à dire demander la suppression de certains liens de la liste des résultats affichés par le moteur de recherche (ce droit a été reconnu par une décision de la cour de justice de l'union européenne - CJUE - du 13 mai 2014). En 2015, la CNIL a reçu près de 450 plaintes de personnes physiques qui se sont vu opposer un refus à une demande de déréférencement effectuée auprès d'un moteur de recherche.
Les usagers demandent principalement la suppression de liens (URLs) diffusés sur des annuaires, des blogs, pages web perso, des sites marchands, des sites de presse et des réseaux sociaux.
La CNIL est intervenue auprès des moteurs de recherche pour leur demander un déréférencement dans 30 % des dossiers traités. Elle a reçu de leur part 76 % de réponses favorables.
À signaler toutefois que de nombreuses demandes de déréférencement adressées à la CNIL n'entrent pas dans le cadre de la décision de la CJUE (par exemples : les données concernent des personnes morales et non des personnes physiques, ou la demande porte sur le respect des droits d'auteur).

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

En conséquence, l'inclusion de ces informations dans les résultats du moteur de recherche Google n'est pas pertinente au regard de l'intérêt du public à en connaître.

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

Succès du déploiement de la nouvelle version de la plainte en ligne

La CNIL a mis en ligne une nouvelle version de son service de plaintes en ligne en mars 2015 afin de mieux répondre aux besoins des internautes en les accompagnant davantage dans leurs démarches ou en les orientant vers les bons interlocuteurs.

Ainsi, une information détaillée est délivrée au travers d'une cinquantaine de scénarios qui comportent :

- des informations sur les démarches préalables à accomplir avant de déposer une plainte à la CNIL ;
- des modèles de courriers pour permettre à l'usager d'exercer ses droits d'accès, rectification et opposition ;
- des liens vers d'autres organismes compétents, notamment lorsque la saisine ne relève pas de la loi Informatique et Libertés (escroquerie, litige commercial, etc).

Cette nouvelle version du service de plaintes en ligne a rencontré un vif succès auprès des internautes. Depuis son ouverture, la CNIL a reçu 32 % de plaintes supplémentaires par rapport à la même période en 2014.

Cette nouvelle version propose à l'internaute 5 thématiques : internet, commerce, travail, téléphonie, banque et crédit. Les principaux motifs de plaintes concernent la suppression d'informations sur internet et les sollicitations commerciales par courrier électronique.

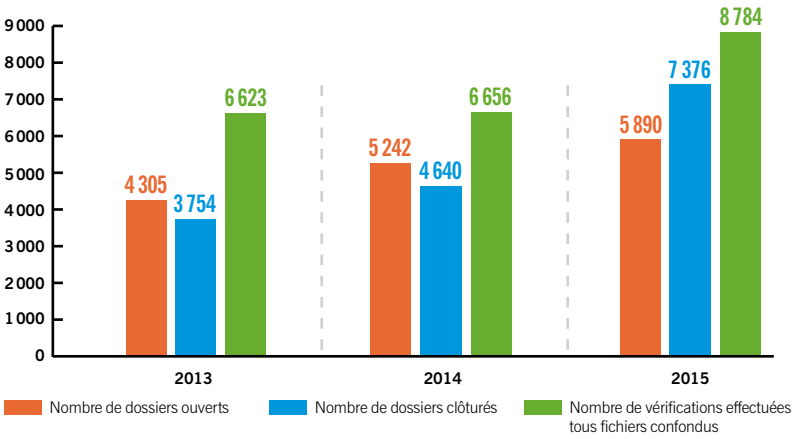
LE DROIT D'ACCÈS AUX FICHIERS DE POLICE, GENDARMERIE, RENSEIGNEMENT, FICOBA : UNE PROGRESSION CONSTANTE DES DEMANDES

En application des articles 41 et 42 de la loi du 6 janvier 1978 modifiée, les personnes qui souhaitent vérifier les données les concernant susceptibles d'être enregistrées dans les fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique (fichiers de renseignement, Système d'Information Schengen, etc.) ou qui ont pour mission de prévenir, rechercher ou constater des infractions (traitement d'antécédents judiciaires....) peuvent en effectuer la demande par écrit auprès de la CNIL.

5 890 personnes se sont adressées à la CNIL en 2015 pour exercer leur droit d'accès indirect, ce qui représente **une augmentation de 12 % par rapport à l'année précédente.** Le nombre de demandes a ainsi progressé de 37 % en l'espace de deux années sous l'effet principalement de l'afflux de demandes relatives au fichier FICOBA de l'administration fiscale pour le règlement des successions pour lequel les conditions d'accès sont légalement modifiées pour les héritiers et notaires à compter du 1er janvier 2016.

5 890
DEMANDES DE DROIT D'ACCÈS INDIRECT
soit + 12 % par rapport à 2014

Évolution des demandes de droit d'accès indirect 2013/2015

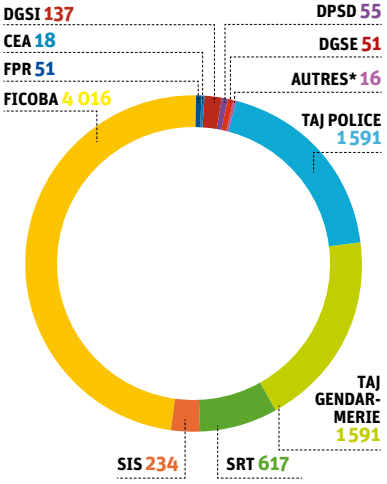


INFO +

Le Droit d'Accès Indirect, comment ça marche ?

À réception de la demande accompagnée d'une copie d'un titre d'identité, un magistrat de la CNIL appartenant ou ayant appartenu au Conseil d'État, à la Cour de Cassation ou à la Cour des Comptes est désigné pour mener les investigations utiles et faire procéder, le cas échéant, aux modifications nécessaires. Les données peuvent ensuite être portées à la connaissance de la personne concernée si, en accord avec l'administration gestionnaire, cette communication n'est pas de nature à nuire à la finalité du fichier, la sûreté de l'État, la défense ou la sécurité publique.

Demandes de droit d'accès indirect 2015 : répartition par fichiers des vérifications à effectuer



Afin de répondre à l'ensemble des attentes de la personne concernée, chaque demande implique généralement qu'il soit procédé à des vérifications dans plusieurs fichiers. Les 5 890 demandes reçues au cours de l'année 2015 représentent ainsi un total de 8 377 vérifications à mener qui concernent principalement le fichier FICOBA et le Traitement d'Antécédents Judiciaires (TAJ).

Au cours de l'année 2015, 8 784 vérifications ont été menées (soit + 32 % par rapport à l'année précédente) dont 38 % ont porté sur le Traitement d'Antécédents Judiciaires (TAJ) qui a succédé, au 1er janvier 2014, aux fichiers STIC et JUDEX.

L'ensemble des vérifications menées en 2015 pour les procédures établies par la police nationale s'est traduit par :

- la suppression de 16 % des enregistrements examinés,
- la mise à jour par mention des suites judiciaires favorables intervenues dans 16% des cas ayant pour effet de rendre les personnes « inconnues » de ce fichier sous son profil de consultation administrative (enquêtes pour l'obtention d'un agrément ou d'une habilitation pour l'exercice d'un emploi, d'un titre de séjour, d'une distinction honorifique). Le pourcentage de personnes bénéficiant de l'effet de telles mises à jour s'avère plus important pour la gendarmerie nationale (42 %) dans la mesure où, à titre général, moins d'affaires leur sont associées.

8 784

VÉRIFICATIONS ONT ÉTÉ MENÉES AU COURS DE L'ANNÉE

soit + 32 % par rapport à 2014

** FICOBA : Fichier des Comptes Bancaires et Assimilés - TAJ police : Traitement d'Antécédents Judiciaires (procédures police) - TAJ gendarmerie : Traitement d'Antécédents Judiciaires (procédure gendarmerie) - SRT : services de renseignement territorial - SIS : Système d'Information Schengen - FPR : Fichier des Personnes Recherchées - CEA : Direction Centrale de la Sécurité du Commissariat à l'Energie Atomique - DGSI : Direction Générale de la Sécurité Intérieure - DGSE : Direction Générale de la Sécurité Extérieure - DPSD : Direction de la Protection de la Sécurité de la Défense - Autres : Fichier des Courses et Jeux (FICOJ), Fichier des Interdits de Stades (FNIS), fichier relatif à la gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS), Europol…*

Résultats des vérifications concernant le Traitement d'Antécédents Judiciaires (TAJ)

	TAJ (procédures établies par la police nationale)	TAJ (procédures établies par la gendarmerie nationale)
Nombre de vérifications individuelles effectuées	1740	1562
Nombre de personnes inconnues	319	1069
Nombre de personnes enregistrées uniquement en tant que victimes	348	139
Nombre de fiches de personnes « mises en cause » vérifiées	1073	354
- dont pourcentage de fiches supprimées	16%	15%
- dont pourcentage de fiches mises à jour par mention de la décision judiciaire favorable intervenue (acquittement, relaxe, non lieu, classement sans suite) rendant la personne inconnue du fichier sous le profil de consultation administrative (enquêtes administratives)	16%	42%
- dont pourcentage de fiches rectifiées ayant eu pour effet de réduire le délai global de conservation de l'enregistrement	1%	<1%
-dont pourcentage de fiches examinées avec maintien de l'enregistrement de la personne (fiches exactes, rectifications mineures sans incidence sur la durée de conservation, défaut de réponse des procureurs de la République sur les suites judiciaires intervenues)	67%	42 %

À RETENIR

Le droit d'accès au fichier FICOBA : modification des modalités d'accès des héritiers et notaires dans le cadre des successions

À compter du 1er janvier 2016, date d'entrée en vigueur de la loi n°2014-617 du 13 juin 2014 relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence, les héritiers et notaires vont pouvoir obtenir directement auprès de l'administration fiscale, les données issues du fichier FICOBA relative à une personne décédée aux fins de règlement des successions (article L.151 B. du livre des procédures fiscales).

Ces derniers ne devront donc plus s'adresser à la CNIL pour accéder aux données de ce fichier. Elle demeurera uniquement compétente pour les demandes formulées par les personnes, ou le mandataire qu'elles auront désigné, pour l'accès aux données d'identification de leurs propres comptes bancaires (exemples les plus fréquents : double détention de livret A, usurpation d'identité....).

Le contentieux en matière de droit d'accès indirect : la compétence du Conseil d'État en premier et dernier ressort pour « certains traitements ou partie de traitements intéressant la sûreté de l'État »

La CNIL est régulièrement appelée, par les juridictions administratives, à présenter ses observations dans le cadre de requêtes introduites par les personnes contestant, au terme de la procédure de droit d'accès indirect, le refus de communication des données les concernant enregistrées dans les fichiers relevant des articles 41 et 42 de la loi Informatique et Libertés. 38 recours ont ainsi été engagés pour la seule année 2015, dont la plupart portant sur les fichiers des services de renseignement des ministères de l'intérieur et de la défense.

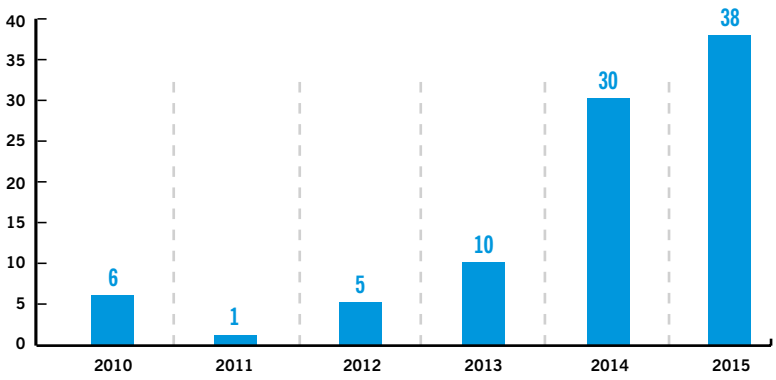
L'exercice du droit d'accès indirect n'emporte pas, en effet, pour la personne un droit à communication des données enregistrées dans les fichiers vérifiés par l'un des magistrats de la CNIL.

Les données ne peuvent être ainsi communiquées que si ce dernier, en accord avec le service gestionnaire, estime que cette communication n'est pas de nature à nuire à la « finalité du fichier, la sûreté de l'Etat, la défense et la sécurité publique ». Toute opposition du service gestionnaire fait obstacle à la moindre communication de la CNIL qui peut uniquement assurer la personne de la réalisation des vérifications sollicitées et lui indiquer les voies et délais de recours qui lui sont ouvertes pour contester le refus de communication.

Ces contentieux relèvent, en premier ressort, de la compétence du Tribunal Administratif et doivent être dirigés contre le ministère gestionnaire de fichier et non contre la CNIL dans la mesure où, comme l'a rappelé à plusieurs reprises le Conseil d'Etat, la lettre de notification qu'elle adresse à la personne ne fait que révéler la décision sous-jacente de refus de communication de ce dernier.

Toutefois la loi n°2015-912 du 24 juillet 2015 relative au renseignement attribue désormais compétence au Conseil d'Etat pour connaître, en premier et dernier ressort, des requêtes relatives à la mise en œuvre du droit d'accès indirect pour « certains traitements ou partie de traitements intéressant la sûreté de l'Etat » (article L.331-4-1 du code de justice administrative). Ces requêtes seront traitées par la formation spécialisée instituée, par cette même loi, pour connaître du contentieux relatif à la mise en œuvre des techniques de renseignement (articles L.773-1 et L 773-8 du code de justice administrative).

Nombre de contentieux relatifs au droit d'accès indirect (2010-2015)



Le décret n°2015-1808 du 28 décembre 2015 définit les traitements concernés par ces nouvelles dispositions (article R.841-2 du code de la sécurité intérieure). Sont notamment concernés : les fichiers de la Direction Générale de la Sécurité Intérieure (DGSI) du ministère de l'intérieur, les fichiers de la Direction Générale de la Sécurité Extérieure (DGSE), de la Direction de la Protection de la Sécurité de la Défense (DPSD) et de la Direction du Renseignement Militaire (DRM) du ministère de la défense.

Mise en demeure des ministères de l'intérieur et de la justice : délai de traitement des demandes relatives au Traitement d'Antécédents Judiciaires (TAJ)

La Présidente de la CNIL a adopté le 2 février 2015 une mise en demeure publique à l'encontre du ministère de l'intérieur et du ministère de la justice pour non respect des délais légaux dans le traitement des demandes de droit d'accès indirect au Traitement d'Antécédents Judiciaires (TAJ).

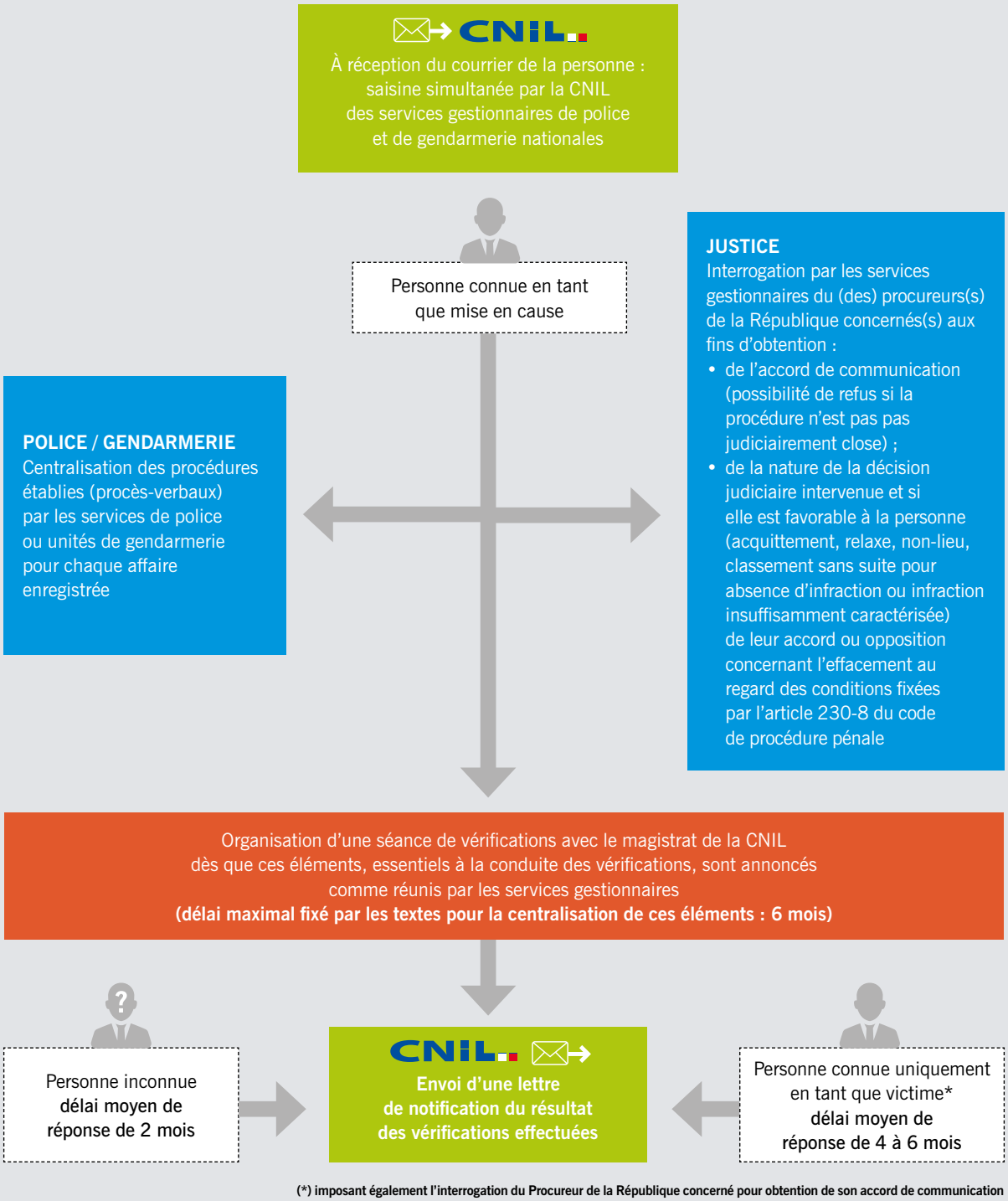
Cette mise en demeure est intervenue en raison des retards importants pris dans le traitement de ces demandes par les services de la police nationale et par les procureurs de la République, saisis dans ce cadre. Ces délais ont pour effet de priver les personnes d'un droit d'accès et de rectification efficaces aux données les concernant enregistrées dans ce fichier consulté notamment à des fins d'enquêtes administratives pour l'accès à certains emplois publics ou privés.

Les ministères concernés ont pris un certain nombre de mesures afin d'y remédier, en particulier :

- Le 31 juillet 2015, le ministère de la justice a rappelé par dépêche aux procureurs de la République leur rôle et les délais applicables en matière de droit d'accès indirect ;
- Le ministère de l'intérieur a procédé à un renforcement des effectifs de la police nationale dédiés au traitement des demandes de droit d'accès indirect et à une redéfinition des procédures internes de traitement et de suivi de ces demandes.

Si les effets de ces mesures ne peuvent être appréciés que dans la durée, le nombre de vérifications menées par les magistrats en charge du droit d'accès indirect pour la police nationale a d'ores et déjà sensiblement progressé (+ 7 % par rapport à 2014).

Procédure de droit d'accès indirect au traitement d'antécédents judiciaires (TAJ)



(*) imposant également l'interrogation du Procureur de la République concerné pour obtention de son accord de communication

À SUIVRE

Conditions d'effacement du Traitement des Antécédents Judiciaires (TAJ) : perspectives d'évolution de la législation nationale

Les conditions d'effacement du fichier TAJ pour les personnes mises en cause dans des infractions sont strictement définies par l'article 230-8 du code de procédure pénale. Seule l'obtention de certaines suites judiciaires favorables (jugement d'acquittement ou de relaxe, ordonnance de non-lieu ou décision de classement sans suite pour absence d'infraction ou insuffisances de charges) peut, sous réserve de l'accord du procureur de la République, permettre d'obtenir l'effacement des faits avant le terme du délai de conservation. A la suite de la première condamnation de la France par la Cour Européenne des Droits de l'Homme (CEDH) le 18 septembre 2014 (Affaire Brunet contre France), concernant au cas d'espèce une personne ayant obtenu une décision de classement sans suite pour un motif (médiation pénale) n'ouvrant pas légalement une telle possibilité d'effacement, des modifications législatives sont annoncées par le gouvernement afin de tirer les conséquences de cette jurisprudence.

... HISTOIRES VÉCUES

Effacement des enregistrements

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

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

Monsieur B., 30 ans, a souhaité qu'il soit procédé à des vérifications en raison des difficultés rencontrées pour la conduite de son projet professionnel dans le domaine de la sécurité privée en raison de sa condamnation à une amende pour conduite d'un véhicule sans permis et pour des faits commis par son frère qui avait usurpé son identité. Au terme des vérifications de la Commission, l'affaire qui lui était imputable a été supprimée en raison de l'expiration du délai de conservation (5 ans) et 6 autres infractions qui, après comparaison d'empreintes, se sont effectivement avérées avoir été commises par son frère ont été supprimées.

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

Mise à jour du fichier par mention des décisions judiciaires favorables obtenues

▸ **Monsieur R.**, 37 ans, a vu sa demande de naturalisation ajournée en raison de son enregistrement dans le fichier TAJ. Au terme des vérifications, une affaire a été supprimée en raison du jugement de relaxe intervenu et les 6 autres subsistantes ont fait l'objet d'une mise à jour par mention des décisions de classement sans suite dont il a bénéficié. Monsieur R. est ainsi devenu inconnu de ce fichier sous son profil de consultation administrative. ■

Contrôler et sanctionner

La CNIL a réalisé **510 contrôles en 2015.** Cela représente **20 % d'augmentation par rapport à l'activité menée en 2014 (421 vérifications).** Ces chiffres traduisent la volonté de la CNIL de s'assurer de la conformité réelle des organismes avec les règles de protection des données personnelles, mais aussi d'étendre le périmètre de ses investigations.

Sur ce total, la Commission a procédé à 155 contrôles en ligne contre 58 en 2014, sachant que ces contrôles n'avaient commencé qu'en octobre 2014, cette faculté ayant été ouverte par la loi cette même année. Ces contrôles en ligne constituent aujourd'hui un outil d'investigation à part entière, et permettent à la CNIL d'adapter ses modalités de contrôle à l'univers numérique.

87 contrôles ont permis à la CNIL de s'assurer de la conformité des dispositifs de vidéoprotection et de vidéosurveillance, tant au regard de la finalité déclarée de ces dispositifs que de leur proportionnalité. Ces contrôles confirment que l'action pédagogique de la CNIL (fiches pratiques, diffusion de conseils aux collectivités territoriales) favorise la convergence des pratiques et leur conformité à la loi.

Les autres contrôles, sur place ou sur pièces, ont porté sur les autres types de traitements de données à caractère personnel.

En 2015, 70 % des missions de contrôle réalisées (sur place, en ligne, sur audition) concernaient le secteur privé, 30 % le secteur public. S'agissant des contrôles en ligne, ce sont 81 % des vérifications qui ont été menées dans le secteur privé.

501
CONTRÔLES
dont 155 contrôles en ligne
87 contrôles vidéo

INFO +

L'origine des contrôles

- **41 % sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;**
- **35 % résultent du programme annuel décidé par la Commission ;**
- **15 % s'inscrivent dans le cadre de l'instruction de plaintes ;**
- **5 % sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction ;**
- **4 % font suite à un courrier d'observation adressé après un premier contrôle.**

PREMIERS BILANS

Le fonctionnement du Fichier des Incidents de remboursement des Crédits aux Particuliers (FICP)

Des contrôles sur place ont été effectués en 2015 auprès de la Banque de France, gestionnaire du Fichier des Incidents de remboursement des Crédits aux Particuliers (FICP), ainsi que des contrôles sur pièces auprès de 14 établissements bancaires (établissements nationaux, régionaux et banques en ligne).

Les résultats de ces contrôles se sont révélés disparates : si la gestion du fichier central par la Banque de France apparaît globalement satisfaisante, a contrario, les contrôles réalisés auprès des établissements monétaires et financiers ont montré qu'il n'existait pas de pratique homogène concernant l'utilisation de ce fichier. Ainsi, les modalités de consultation, les durées de conservation et l'information des personnes sur les conséquences d'un fichage au FICP ne respectent pas toujours les dispositions légales. La CNIL, qui a déjà adopté des mesures répressives en la matière, a rappelé à l'ensemble des acteurs concernés la nécessité de respecter scrupuleusement les textes encadrant le fonctionnement de ce fichier.

Le Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV)

Créé en 2004, le Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV) a pour objet de prévenir le renouvellement des infractions de nature sexuelle ou particulièrement violentes et de faciliter l'identification de leurs auteurs. Toute personne inscrite se voit contrainte de justifier périodiquement de son adresse auprès des forces de police. Le FIJAISV est également utilisé par les autorités compétentes afin de contrôler les conditions d'encadrement de certaines activités ou professions impliquant un contact avec des mineurs.

La CNIL a procédé à 24 contrôles auprès de l'ensemble des acteurs institutionnels exploitant le FIJAISV. Les 14 contrôles sur place et 10 contrôles sur pièces ont été menés auprès des ministères et services impliqués dans la gestion et l'exploitation du fichier : service du casier judiciaire, juridictions judiciaires, établissement pénitentiaire, protection judiciaire de la jeunesse, forces de police et de gendarmerie ainsi que ministères concernés (Education nationale, Jeunesse et sports). Ils ont notamment permis de vérifier la régularité des inscriptions, les modalités de conservation des données et la sécurisation de l'accès au fichier.

PREMIERS ÉLÉMENTS - BILANS PRÉVUS EN 2016

Le paiement sans contact

La CNIL a lancé une série de contrôles sur pièces auprès des principales banques françaises, concernant les cartes de paiement qui disposent d'une fonction de paiement sans contact. Ces contrôles visaient à déterminer la nature des données lisibles au moyen de la fonction de lecture sans contact, leurs modalités de sécurisation, ainsi que les modalités de désactivation de la fonction de paiement sans contact. La CNIL s'est également attachée à vérifier dans quelle mesure les porteurs de ces cartes de paiement sont informés de leurs droits. L'analyse des réponses des organismes contrôlés se poursuivra en 2016.

Les risques psychosociaux en entreprise (RPS)

Les enquêtes menées par les entreprises auprès de leurs salariés afin de mieux évaluer et lutter contre le stress au travail se sont multipliées. Ces enquêtes de prévention des risques psychosociaux conduisent à recueillir auprès des salariés des informations sur leurs sentiments, leurs perceptions et leurs expériences, suscitant des inquiétudes chez certains d'entre eux ainsi que chez des représentants du personnel. La CNIL a ainsi été saisie de plaintes qui ont provoqué des contrôles auprès d'organismes du secteur public et du secteur privé, ainsi qu'auprès de prestataires à qui sont confiées ces enquêtes. Les premières constatations ont mis en évidence l'utilisation de questionnaires accessibles sur internet, et la CNIL a porté une attention particulière à l'information des salariés sur le caractère facultatif des enquêtes, ainsi qu'au respect de l'anonymat des personnes interrogées.

Le Système national des permis de conduire (SNPC)

Le Système national des permis de conduire (SNPC) a fait l'objet d'une série de contrôles, visant les acteurs institutionnels chargés d'en assurer le fonctionnement et de l'exploiter. Près de 10 contrôles ont été réalisés afin de vérifier la régularité des procédures d'inscription des personnes et d'élaboration des titres (jusqu'à la réalisation physique du permis). Les contrôles ont également porté sur les modalités de gestion, de consultation et de mise à jour des données traitées au sein du SNPC, s'agissant en particulier de l'inscription des infractions et du retrait de points du permis de conduire. Ils permettront par ailleurs de vérifier la régularité des évolutions liées à la mise en place du nouveau permis de conduire européen (SI- FAETON).

FOCUS

Les traitements mis en œuvre au titre de la gestion de l'impôt sur le revenu

La CNIL a inscrit à son programme annuel de contrôle les traitements de gestion de l'impôt sur le revenu, auquel plus de 17,6 millions de contribuables ont été assujettis en 2014. Entre fin 2014 et début 2015, ce sont ainsi 12 contrôles sur place qui ont été réalisés sur l'ensemble du territoire national, auprès de directions et de services à compétence nationale comme de services déconcentrés de la direction générale des finances publiques (DGFiP). Des investigations ont été diligentées auprès de deux services des impôts des particuliers, cinq établissements de services informatiques, la direction nationale des enquêtes fiscales et une brigade de contrôle et de recherches. Ces investigations avaient pour objet d'analyser les principales étapes du dossier d'un contribuable, incluant son identification, sa déclaration de revenus, le règlement des sommes dues et la vérification des données déclarées.

C'est ainsi que près d'une dizaine de traitements mis en œuvre au titre de la gestion de l'impôt sur le revenu ont fait l'objet de contrôles :

- ILLIAD, traitement de gestion des dossiers du contribuable par les services des impôts des particuliers ;
- ADONIS, qui offre une vue synthétique du compte fiscal d'un particulier aux agents de la DGFiP ;
- SIR et PERS, traitements d'identification des contribuables ;
- Télé-IR, traitement de déclaration de revenus en ligne par le contribuable ;
- SATELIT, traitement de vérification de la taxation et de paiement de l'impôt en ligne ;
- SVAIR, téléservice permettant à des organismes tiers de vérifier l'authenticité de l'avis ou du justificatif d'impôt sur le revenu présenté par un contribuable ;
- les traitements relatifs à l'édition des déclarations de revenus pré-remplies et des avis d'imposition.

Au terme de ces investigations, il est apparu que les conditions de mises en œuvre des traitements contrôlés sont globalement satisfaisantes. Des mesures de sécurité appropriées ont été constatées (sécurité physique forte, gestion fine des habilitations, audits internes réguliers), de même qu'une collecte légitime et proportionnée des données.

Néanmoins, des axes d'améliorations ont été identifiés, s'agissant notamment des durées de conservation de certaines données. L'information des personnes quant aux droits garantis par la loi Informatique et Libertés s'est quant à elle avérée incomplète, voire absente de certains formulaires de collecte d'information.

Ces conclusions ont été portées à la connaissance du ministre des Finances et des comptes publics.

BILAN DES ACTIONS COORDONNÉES AU NIVEAU EUROPÉEN ET INTERNATIONAL

La CNIL a poursuivi en 2015 des actions d'audit en collaboration avec ses homologues européens et internationaux. Cette collaboration s'est traduite par la participation à un nouveau « Sweep Day », ainsi que par des contrôles réalisés en concertation avec ses homologues européens.

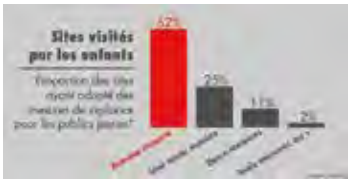
Sweep Day, quelle protection des données personnelles sur les sites pour les jeunes ?

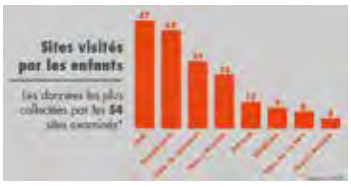
Pour la troisième année consécutive, la CNIL s'est associée aux 29 autorités membres du GPEN *(Global Privacy Enforcement Network* - réseau international d'autorités en charge de la protection de la vie privée) pour participer à une opération conjointe dite Sweep Day.

En 2015, l'opération a porté sur les sites internet consultés par les enfants et adolescents. La CNIL a examiné en mai une cinquantaine de sites et analysé le niveau de protection de la vie privée du jeune public visé (données collectées, qualité de l'information, mesures de vigilance, etc.).

Elle a mis en évidence l'insuffisance des mesures de protection des données sur ces sites, et ce, qu'il s'agisse de réseaux sociaux ou de sites de jeux, liés à des chaînes de télévision, éducatifs, d'actualités, ou encore de soutien scolaire. Or, ces sites collectent massivement des données personnelles, en imposant la création d'un compte utilisateur pour accéder à leurs fonctionnalités. De même, l'information n'est que rarement adaptée au public visé et la plupart des sites ne mettent en œuvre aucune mesure de vigilance ou de contrôle parental.

Au-delà de l'action de coopération internationale, cette action coordonnée a permis de sensibiliser les parents aux questions de protection de la vie privée et de promouvoir des bonnes pratiques auprès des responsables de ces sites.





EURODAC

Exploité par 32 Etats membres de l'Union européenne et partenaires, le traitement EURODAC a pour finalité de déterminer l'État responsable de l'examen d'une demande d'asile. Il comprend un système automatisé de reconnaissance d'empreintes digitales et inclut près de 2,7 millions de profils de demandeurs d'asile et de personnes ayant franchi une frontière extérieure de l'Union européenne de manière irrégulière. Depuis 2015, le traitement peut être consulté par les autorités de poursuite pénale lorsqu'elles recherchent les auteurs d'infractions pénales graves ou d'actes de terrorisme.

La CNIL fait partie de l'organe indépendant de contrôle d'EURODAC, aux côtés de ses homologues européens ainsi que du Contrôleur européen de la protection des données (CEPD). A ce titre, elle a vérifié en 2015 le respect de la procédure de droit d'accès dont bénéficie chaque personne inscrite ainsi que les modalités d'inscription et de mise à jour de la base pour les personnes ayant demandé une protection internationale sur le sol français.

Le système d'information Schengen II (SIS II)

Le fichier SIS II a pour objet de permettre aux pays de l'espace Schengen de mettre en place une politique commune de contrôle des entrées dans l'espace Schengen et ainsi faciliter la libre circulation de leurs ressortissants tout en préservant l'ordre et la sécurité publics. Alimenté quotidiennement par l'ensemble des Etats membres de l'espace Schengen, il rassemble notamment les données relatives aux étrangers signalés aux fins de non admission sur le territoire européen. Il est exploité par les services des ministères régaliens (Intérieur et Affaires Etrangères) lorsqu'ils mettent en œuvre la politique de visas, s'agissant des demandes d'entrée adressées à la France. Dans le but d'assurer une approche coordonnée, le Contrôleur européen de la protection des données (CEPD) et les autorités nationales de protection des données se réunissent à intervalles réguliers afin d'examiner les problèmes communs que pose le fonctionnement du SIS II et de recommander des solutions communes. En 2015, les investigations de la CNIL ont particulièrement porté sur l'instruction des demandes de droit d'accès indirect (accès à la demande d'une personne par l'intermédiaire de la CNIL) et sur l'exactitude et la mise à jour des données exploitées par les services administratifs dans le cadre des admissions sur le territoire français.

Les règles de confidentialité de Facebook

En coopération avec les autorités de protection des données personnelles de Belgique, des Pays-Bas, d'Espagne et du Land allemand de Hambourg, la Commission a mené en 2015 des investigations relatives aux règles de confidentialité applicables aux services du réseau social Facebook.

Les investigations ont pris la forme de contrôles sur place, sur pièces et en ligne. Les autorités nationales de protection des données personnelles ont échangé des informations afin de veiller à la cohérence de leurs actions et la CNIL examine les suites éventuelles à donner à ses constatations.

DERNIÈRE MINUTE

Dernière minute...

Le 9 février 2016, la Présidente de la CNIL a mis publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi Informatique et Libertés. Elle lui demande notamment de collecter loyalement les données de navigation des internautes ne disposant pas de comptes FACEBOOK et que les membres puissent s'opposer à la combinaison de l'ensemble de leurs données à des fins publicitaires.

Une année de contrôles en ligne

De nombreuses thématiques ont été abordées, telles que les sites de tirage d'albums photo, de conseil de santé en ligne, de crédit en ligne, d'adhésion à des partis politiques, de demande d'actes d'état civil ou encore de participation volontaire à des études cliniques.
Les vérifications ont porté sur la pertinence des informations collectées, la sécurité des traitements de données, l'information des utilisateurs ainsi que la conformité à la réglementation relative aux cookies.
Le pouvoir de contrôle en ligne a considérablement renforcé les capacités de réaction de la CNIL lorsqu'elle constate des failles de sécurité accessibles via internet, dont certaines ont pu conduire à l'adoption de mises en demeure ou de sanctions, voire à l'information du procureur de la République.

155 CONTRÔLES EN LIGNE ONT ÉTÉ RÉALISÉS EN 2015.

28 contrôles en ligne réalisés en 2015 ont conduit à la notification d'une mise en demeure en 2015 ; deux procédures de sanction ont été engagées mais sont toujours en cours en février 2016

ACTIVITÉ RÉPRESSIVE : DES MISES EN DEMEURE EN FORTE AUGMENTATION

L'année 2015 se caractérise par une forte hausse du nombre de mises en demeure adoptées par la Présidente de la CNIL.

En effet, 93 mises en demeure ont été adoptées (soit une augmentation de 50 % par rapport à 2014). Cette hausse s'explique notamment par la réalisation de contrôles s'inscrivant dans des thématiques ayant révélé de nombreux manquements : **cookies** (40 mises en demeure à l'encontre d'organismes disposant de sites internet), **sites de rencontre** (8 mises en demeure publiques) ou encore **services dématérialisés d'actes d'état civil** (20 mises en demeure à l'encontre de communes).

La grande majorité des mises en demeure fait suite à des missions de contrôle (92 % des décisions) dont certaines consécutives à des plaintes reçues.

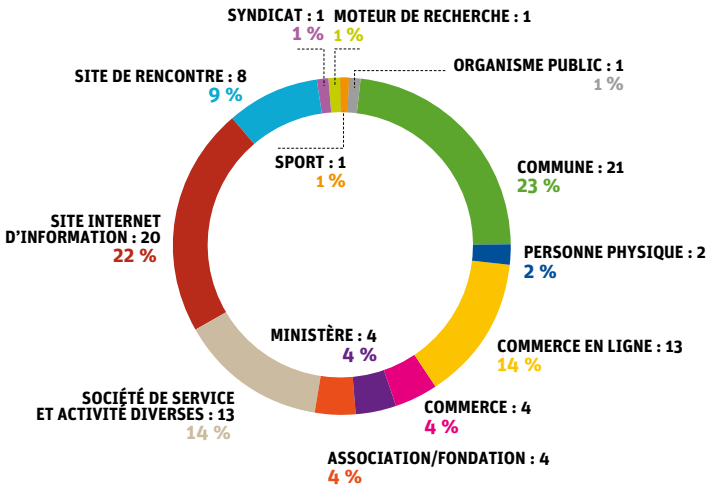
93
MISES EN DEMEURE
dont 12 publiques

10
RAPPORTS DE SANCTIONS

3
SANCTIONS FINANCIÈRES
dont 2 publiques

7
AVERTISSEMENTS
dont 2 publics

Répartition des mises en demeure par secteur



> Le recours à une mise en demeure conduit dans la grande majorité des cas à une mise en conformité et donc à une clôture du dossier

INFO +

La mise en demeure

La présidente de la CNIL peut mettre en demeure un responsable de traitement qui ne respecte pas les obligations découlant de la loi Informatique et Libertés de faire cesser le manquement constaté. Elle fixe un délai pour cette mise en conformité. Une mise en demeure n'est pas une sanction. Aucune suite n'est donnée à cette procédure si la société se conforme à la loi dans le délai imparti.
Dans la très grande majorité des cas, les mises en demeure donnent lieu à une mise en conformité et donc à une clôture de la procédure. Dans le cas contraire, la formation restreinte peut prononcer des sanctions.
La présidente de la CNIL peut demander au bureau (composé de lui-même et des deux vice-président) de rendre publique la mise en demeure, notamment en raison de la gravité des manquements ou du nombre important de personnes concernées. La clôture fait l'objet de la même mesure de publicité que celle de la mise en demeure.

FOCUS

Mise en demeure à l'encontre de la société GOOGLE INC

Par décision du 13 mai 2014, la Cour de justice de l'Union européenne a jugé que tout moteur de recherche est tenu de respecter les droits de rectification, d'effacement, de mise à jour et d'opposition des personnes en procédant au « déréférencement » de certains liens.
Pour un moteur de recherche, procéder à un déréférencement revient à retirer de la liste des résultats affichés à la suite d'une recherche associée au nom d'une personne, des liens renvoyant vers des pages web et contenant des informations relatives à cette personne. Il convient de rappeler que les pages web à l'origine de la diffusion restent en ligne dans leur forme d'origine et qu'elles sont accessibles par d'autres mots clés que le nom de la personne ayant obtenu le déréférencement.
La Cour de justice a précisé que le refus du responsable de traitement de procéder au déréférencement sollicité pouvait être contesté auprès de l'autorité de contrôle de protection des données (en France, la CNIL) ou de l'autorité judiciaire compétente au sein de chaque Etat membre.
La CNIL a ainsi été saisie par de nombreux particuliers s'étant vus refuser le déréférencement de liens Internet (ou adresses URL) par Google. Pour certains d'entre eux, elle a demandé à cette société de procéder au déréférencement des liens évoqués. A cette occasion, la Commission a précisé que le déréférencement devait se faire sur toutes les extensions géographiques du moteur de recherche et pas uniquement sur les extensions européennes comme Google le faisait.
En effet, la CNIL a considéré que le droit au déréférencement s'exerce auprès d'un responsable de traitement (Google), concernant l'intégralité d'un traitement (le moteur de recherche). Le droit reconnu aux personnes est de ne plus figurer dans certains résultats du moteur de recherche, et non de voir leur « exposition » varier selon les modalités d'interrogation du moteur en question. Dans le cas contraire en effet, cela signifierait que la portée d'un droit fondamental varie en fonction des tiers, et en fonction du mode d'interrogation du traitement.
Le déréférencement sur toutes les extensions apparaît ainsi comme le seul moyen de garantir l'effectivité du droit des ressortissants français.
La législation en matière de protection des données et la nécessité de garantir l'effectivité du droit des personnes conduisent ainsi à considérer que le déréférencement doit intervenir sur l'ensemble des extensions du moteur de recherche.
Devant le refus de Google de procéder ainsi, la Présidente de la CNIL a mis en demeure la société le 21 mai 2015 de procéder au déréférencement sur l'ensemble des extensions du moteur de recherche avant le 31 juillet 2015. Les suites à donner à ce dossier sont actuellement en cours d'instruction par la CNIL.

LES RECOURS DEVANT LE CONSEIL D'ÉTAT

Obligation de notification d'une violation de données personnelles et auto incrimination

Un prestataire de service de la société Orange a été victime d'une intrusion informatique ayant généré la fuite des données à caractère personnel de plus d'un million de clients de l'opérateur. Conformément à la loi Informatique et Libertés (article 34 bis), cet opérateur a notifié cette violation de données personnelles à la CNIL. Les contrôles effectués par la CNIL auprès de la société et de ses sous-traitants par la suite, ont révélé que toutes les précautions utiles n'avaient pas été prises pour garantir la sécurité et la confidentialité des données. Considérant que la société n'avait pas satisfait à son obligation d'empêcher la communication des données à des tiers non autorisés (article 34 de la loi « Informatique et Libertés »), la formation restreinte de la CNIL a prononcé un avertissement public à son encontre.

La société a contesté cette décision devant le Conseil d'État en invoquant que la décision de la formation restreinte de la CNIL violait l'article 6-1° de la Convention Européenne des Droits de l'Homme (CEDH). Elle estimait en effet avoir contribué à sa propre incrimination dans la mesure où la sanction adoptée reposait sur les faits qu'elle avait elle-même notifiés. Le Conseil d'État a indiqué, dans sa décision du 30 décembre 2015, que la loi Informatique et Libertés prévoyait **deux obligations distinctes, autonomes l'une de l'autre :** l'article 34 impose de prendre toutes précautions utiles pour préserver la sécurité et la confidentialité des données alors que l'article 34 bis met à la charge des responsables de traitements fournissant un service de communications électroniques, une obligation spécifique de notification des violations de données à caractère personnel.

En l'espèce, le Conseil d'État a confirmé la sanction prononcée. Il a ainsi considéré qu'elle était fondée sur des manquements à l'obligation de sécurité constatés à l'occasion des contrôles et non sur des éléments obtenus par le biais de la procédure de notification.

▸▸▸

Vidéosurveillance au travail : confirmation de l'interprétation de la CNIL

Dans une décision rendue le 18 novembre 2015, le Conseil d'État a confirmé la sanction pécuniaire publique infligée à la société PS CONSULTING, un prestataire de services informatique dont le dispositif de vidéosurveillance ne respectait pas la loi Informatique et Libertés. Le Conseil d'État a retenu que la surveillance constante de salariés par le biais de caméras orientées vers certains postes de travail était disproportionnée. Il a ainsi relevé l'absence d'impératif de sécurité avéré, l'accès aux locaux étant en outre déjà sécurisé. Selon le Conseil d'État, la finalité avancée par la société de lutter contre les vols commis par ses propres salariés ne permettait pas, en l'espèce, de justifier du bienfondé du dispositif. Il a enfin confirmé que l'information à destination des salariés et la politique de sécurité des outils informatiques étaient insuffisantes.

À RETENIR

À l'occasion de cette décision le Conseil d'État a précisé certains aspects de la procédure de contrôle de la CNIL.

Une même décision de contrôle peut valablement servir de fondement à plusieurs missions de vérifications sur place auprès d'un même responsable de traitement.

Sauf exception, le droit de garder le silence et de se faire assister d'un avocat s'applique uniquement à la procédure de sanction de la CNIL et non à la procédure de contrôle.

Éclairage sur l'étendue du droit d'accès

Par décision rendue le 15 octobre 2015, le Conseil d'État a rejeté le recours formé par un plaignant à l'encontre de la décision de clôture de sa plainte par la Présidente de la CNIL. Le plaignant invoquait le non-respect de son droit d'accès aux données le concernant auprès de son ancien employeur. Cette personne soutenait que le refus de la CNIL d'exiger la communication des justificatifs accompagnant ses notes de frais était constitutif d'une atteinte à son droit d'accès tel que garanti par l'article 39 de la loi Informatiques et Libertés . Le Conseil d'État a rejeté sa requête au motif que le droit d'accès n'a pas pour objet d'imposer la communication de documents mais seulement d'informations.

La CNIL avait ainsi satisfait à ses obligations dans la mesure où elle avait obtenu, lors de l'instruction de la plainte, la communication des données à caractère personnel relatives aux notes de frais concernant le plaignant. ■

À RETENIR

À l'occasion de cette décision le Conseil d'État a précisé certains aspects de la procédure de contrôle de la CNIL.

Une même décision de contrôle peut valablement servir de fondement à plusieurs missions de vérifications sur place auprès d'un même responsable de traitement.

Sauf exception, le droit de garder le silence et de se faire assister d'un avocat s'applique uniquement à la procédure de sanction de la CNIL et non à la procédure de contrôle.

La liste complète des organismes contrôlés en 2015 est disponible sur le site de la CNIL.
La liste complète des mises en demeure et des sanctions prononcées en 2015 est disponible en annexe.

Anticiper et innover

Dans le cadre de ses activités d'innovation et de prospective, la CNIL souhaite anticiper de nouveaux usages, tendances ou technologies émergents pour alimenter les débats de société sur l'éthique des données. Cette approche s'est en particulier incarnée en 2015 dans le troisième Cahier Innovation & Prospective « Les données, muses et frontières de la création », ainsi que dans l'animation des travaux du Comité de la Prospective élargi, autour du thème des « données dans la société et l'économie du partage ».

LIRE, ÉCOUTER, REGARDER ET JOUER À L'HEURE DE LA PERSONNALISATION

Le monde des contenus culturels et créatifs a connu une transformation numérique précoce. Aujourd'hui, des millions de Français produisent et consomment des contenus vidéo, musicaux, vidéoludiques ou écrits par l'intermédiaire de services numériques. Ces usages sont massifs, et les revenus associés deviennent incontournables pour les acteurs économiques. Ainsi, le streaming musical rapporte déjà en France un revenu équivalent à celui du téléchargement de musique.

Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) laissent ici symboliquement place aux ASNS : Amazon pour les livres, Spotify et Deezer pour la musique, Netflix pour la vidéo à la demande et Steam pour les jeux vidéos. Ils symbolisent une nouvelle approche de la distribution et de la consommation de contenus culturels, dans laquelle les données jouent un rôle majeur.

Émergence de nouveaux modèles économiques

La transformation précoce des marchés culturels constitue un formidable laboratoire des modèles d'affaires, et vient interroger l'affirmation faisant des données « le pétrole de l'économie numérique ». Les données personnelles des utilisateurs, mobilisées comme monnaie d'échange, ont pour fonction première de contribuer à la personnalisation de l'expérience au bénéfice de l'utilisateur. Elles peuvent ▸▸▸

> **Les contenus dématérialisés représentent aujourd'hui environ 40% des revenus de l'industrie culturelle - contre seulement 17% en 2010 ; ils devraient atteindre 63% de ces revenus en 2018 (IDATE).**

INFO +

Cahier IP n°3 : Les données, muses et frontières de la création

Dans un contexte où nos consommations de contenus culturels dématérialisés deviennent massivement productrices de données, le troisième Cahier Innovation et Prospective explore les industries créatives (musique, vidéo, livre numérique et jeux vidéos) et contribue à alimenter le débat sur la place des algorithmes et sur les manières de redonner du contrôle aux utilisateurs. Il succède à un numéro dédié aux nouvelles pratiques de santé et bien-être connectés (« Le corps, nouvel objet connecté », 2014) et au panorama prospectif du premier cahier (« La vie privée à l'horizon 2020 », 2012)

▸▸▸ également être utilisées pour remplir des objectifs bien différents. Certaines données sont nécessaires pour rendre le service quand d'autres vont permettre de construire une connaissance qui pourra bénéficier au fournisseur de services comme à des tiers.

Ces formes de participation des utilisateurs à la création de richesse des acteurs économiques s'apparentent à ce que certains chercheurs appellent le digital labor. À l'adage « *si c'est gratuit, c'est vous le produit* », on pourrait désormais ajouter, comme le propose Antonio Casilli, « *si vous ne payez pas, c'est que vous êtes le travailleur* ».

Des données culturelles personnelles… et intimes

Les données personnelles collectées et traitées dans le contexte des contenus culturels et créatifs ont des particularités liées au caractère très intime de la relation entre une personne et les œuvres qu'elle choisit, constitutives de sa personnalité et de son identité. Les *data-scientists* exploitent ainsi la valeur de données d'apparence très anodines : profils, descriptions des contenus, popularité, enrichissement, goûts et contexte. Ceci est facilité par le fait que peu d'individus mettent en place des stratégies d'obfuscation (consistant à publier en quantité des informations pour tenter de rendre moins visibles les informations existantes que l'on souhaite cacher) dans leurs consommations de culture, contrairement à d'autres domaines comme les réseaux sociaux, où l'on observe des comportements plus tactiques.

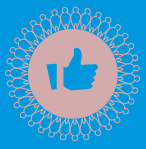
Ainsi, **le contexte sera très important dans le domaine musical** (musique au travail ? pendant le sport ? pendant une fête ? dans les transports ?). **Dans le domaine du livre, en revanche, il sera plus crucial d'analyser les interactions entre la personne et le contenu** (vitesse de lecture, phrases soulignées) pour comprendre les moteurs de son intérêt. **Pour la vidéo à la demande, il s'agira de comprendre la structure du foyer** et donc deviner qui est devant les écrans à quel moment. Les données collectées dans le jeu vidéo auront trait à l'usage et aux actions des utilisateurs, elles permettront d'évaluer leurs préférences, leurs choix ou leurs comportements.

INFO +

Typologie des données

Des données personnelles au sens le plus classique : données d'identité, de contact et de **PROFIL** sociodémographique, qui sont finalement les données d'un fichier client et de gestion de la relation client traditionnel.

Des données **DESCRIPTIVES DES CONTENUS** : données de catalogage (artiste, auteur, interprète), de caractérisation (durée, genre, sous-genre) mais aussi données techniques (format, compression, échantillonnage) et données juridiques (concernant exemple).



Des données générales de consommation, c'est-à-dire renseignant sur les goûts collectifs comme la **POPULARITÉ** d'une chanson, le nombre total d'écoutes, les commentaires et citations sur les services de réseaux sociaux, etc ...

Des données d'**ENRICHISSEMENT** : photos ou biographie des artistes, critiques, notes et évaluations, liens de téléchargement, prix, paroles de chansons.
Ces données peuvent être fournies par des professionnels (par exemple les critiques) ou générales par les utilisateurs.

Des données concernant l'usage, les comportements et les **GOÛTS** de chaque utilisateur: ces données peuvent être très générales (type, quantité, durée, rythme d'achat/de consultation, playlist créées ...) mais aussi très fines (les passages surlignés d'un livre, la vitesse de lecture ...).

Des données de **CONTEXTE** comme l'horodatage, la localisation ou toutes les données issues de capteurs (les mouvements, les émotions, l'état physiologique, l'humeur, etc.).

La recommandation au cœur des stratégies

Recommander permet aux diffuseurs de contenus culturels d'attirer de nouveaux clients, de les fidéliser et d'optimiser leurs revenus. La recommandation est peu transparente et compréhensible pour l'utilisateur du fait qu'elle peut techniquement combiner des outils et approches très différentes : analyse d'experts (par recommandation humaine), analyse automatique des contenus (par les métadonnées), analyse du profil de l'utilisateur et de son réseau, « filtrage collaboratif ».

Si les utilisateurs acceptent la collecte de leurs données et sont prêts à payer pour des services efficaces et « sans couture » de recommandation, ils souhaitent à la fois garder le contrôle et s'exposer parfois à des frictions, c'est-à-dire des moments où ils choisissent de découvrir des contenus culturels en dehors de leur « bulle de filtres » (selon l'expression d'Eli Pariser). Cette volonté de transparence des utilisateurs amène certains industriels comme Netflix à expliciter leurs critères de recommandations. ▸▸▸

> **La prescription n'étant pas incarnée, le consommateur n'a en retour aucune possibilité de la recontextualiser et se contente trop souvent de la subir. La traçabilité fonctionne à sens unique.**
>
> Olivier Ertzscheid,
> *maître de conférences en sciences de l'information à l'université de Nantes*

Vers la personnalisation de l'expérience

Dans ce nouveau paysage, la personnalisation de l'expérience devient plus intime, l'intrication entre l'œuvre et l'expérience d'utilisation plus grande, la frontière entre création par l'auteur et contenus générés par et pour l'utilisateur plus floue.

Certaines tendances lourdes, transversales aux différents secteurs, dessinent les contours de ce qui pourrait advenir dans les prochaines années.

La prise en compte des caractéristiques du contexte *(context awareness)* permettra d'adapter le contenu des œuvres aux utilisateurs, de manière invisible. La recommandation passera probablement par l'analyse en temps réel des sentiments de l'utilisateur via les objets connectés. Les technologies immersives et les nouvelles interfaces homme-machine rendront possibles des nouvelles formes de narration et d'œuvres, plus interactives.

En outre, la combinaison de la donnée et du matériel *(hardware)* bouleverse la chaîne de valeur de secteurs traditionnels et fait émerger de nouveaux modèles économiques. La collecte devient déjà multi-source et les services s'hypercontextualisent, ce qui pose naturellement la question de la neutralité, de la pertinence des algorithmes et du contrôle de l'utilisateur sur l'utilisation de ses données.

INFO +

Que nous apprend l'enquête Médiamétrie* réalisée pour la CNIL sur les usages des services de streaming et de SVOD (octobre 2015) ?

- 1 tiers des utilisateurs souscrivent à un abonnement payant de musique en streaming.
- 60 % des utilisateurs écoutent les recommandations musicales (74 % des abonnés payants) / 68 % regardent les recommandations de films ou de séries.
- 2/3 des utilisateurs apprécient ces recommandations personnalisées.
- 1 utilisateur sur 2 s'est déjà demandé comment fonctionnent les systèmes de recommandation.
- 25 % des utilisateurs ont déjà été influencés dans leurs choix d'écoute ou de partage, sachant que leurs écoutes pouvaient être vues par leurs contacts ou leurs amis.

(*) Enquête réalisée du 21 au 29 septembre 2015 sur 503 internautes de 15 ans et plus, utilisateurs d'un service de musique en streaming (Deezer ou Spotify) ou de vidéo à la demande (Netflix ou Canalplay).

LE COMITÉ DE LA PROSPECTIVE

2015 a aussi été l'occasion pour la CNIL de renouveler la composition et le format de son Comité de la prospective. Désormais élargi à 15 membres, il a vocation à enrichir la réflexion de l'institution sur les enjeux sociétaux et éthique du numérique afin de mieux cerner leurs impacts sur les droits et libertés.

En réunissant des expertises et des expériences plurielles, le comité constitue un espace privilégié d'échanges et de réflexion. En 2016, il étudiera notamment la place des données personnelles dans la société et l'économie du partage.

Il est placé sous la présidence d'Isabelle FALQUE-PIERROTIN. ■

EXPERTS EXTÉRIEURS

Laurent Alexandre, chirurgien-urologue, chef d'entreprise : créateur du site Doctissimo, PDG de DNA Vision. Chroniqueur au Huffington Post et au journal Le Monde.

Pierre-Jean Benghozi, membre du Collège de l'ARCEP et professeur à l'Ecole polytechnique.

Stefana Broadbent, psychologue, professeur d'Anthropologie honoraire à l'University College de Londres où elle enseigne l'anthropologie numérique.

Dominique Cardon, sociologue au Laboratoire des usages SENSE d'Orange Labs, professeur associé à l'Université de Marne la vallée (LATTS).

Milad Doueihi, philosophe, historien des religions et titulaire de la chaire d'humanisme numérique à l'université de Paris-Sorbonne (Paris IV), co-titulaire de la chaire du Collège des Bernardins sur l'humain au défi du numérique.

Claude Kirchner, directeur de recherche Inria, président du comité opérationnel d'évaluation des risques légaux et éthiques (COERLE) d'Inria, conseiller du Président d'Inria.

Cécile Méadel, Sociologue, professeure de l'Université Panthéon-Assas, responsable du master Communication et multimédia. Chercheuse au CARISM, chercheuse associée au Centre de sociologie de l'innovation (Mines-CNRS).

Tristan Nitot, entrepreneur, auteur et conférencier sur le thème des libertés numériques, a fondé et présidé Mozilla Europe. Directeur de produit (Chief Product Officer) chez Cozy Cloud (logiciel de Cloud personnel). Membre du Conseil National du Numérique (CNNum).

Bruno Patino, journaliste et spécialiste des medias numériques. Directeur de l'École de journalisme de Sciences-Po.

Antoinette Rouvroy, juriste,chercheuse FNRS au Centre de Recherche Information, Droit et Société (CRIDS) de Namur.

Henri Verdier, directeur interministériel du numérique et du système d'information et de communication de l'État (DINSIC).

Célia Zolynski, professeur de droit à l'Université de Versailles Saint-Quentin.

MEMBRE DE LA CNIL

Joëlle Farchy, professeure de sciences de l'information et de la communication à l'Université Paris I et chercheure au Centre d'économie de la Sorbonne.

Eric Pérès, membre du Conseil économique, social et environnemental.

La régulation internationale, un élément indispensable de la protection des données à l'ère numérique

2015, ANNÉE PAPILLON

Le rapport annuel de la CNIL qualifiait l'année 2014, s'agissant du projet de règlement européen, de chrysalide, l'année 2015 est sans aucun doute celle du papillon. En effet, la réforme sur la protection des données a été adoptée au mois de décembre, permettant d'adapter le droit européen, de manière harmonisée, à l'univers numérique.

Cet aboutissement a été le fruit d'un travail intense mené par les trois institutions de l'Union (la Commission, le Parlement et le Conseil de l'UE) tout au long de l'année 2015. Un accord a été conclu sur le règlement en juin, puis en parallèle du trilogue sur le règlement, un autre accord a été trouvé en octobre sur le projet de Directive Police Justice. Le second semestre a abouti, dans des délais contraints, à un accord global et commun aux trois institutions des deux textes, scellant ainsi le nouveau cadre juridique de la protection des données de l'Union.

Cette réforme va bien au-delà de la Directive actuelle puisque les deux textes adoptés couvrent non seulement les traitements du secteur privé, ceux du secteur public mais également les traitements mis en œuvre dans le cadre de la coopération policière et judicaire.

Il reste désormais une dernière étape formelle à franchir : celle de **l'adoption en plénière du Parlement européen et en Conseil des ministres de ce paquet protection des données prévu pour le printemps 2016.**

La CNIL et l'ensemble des autorités nationales de protection des données ont régulièrement contribué à la finalisation de ce projet par la publication de leurs positions à divers moments des négociations. De nombreuses rencontres ont également été organisées afin de les présenter aux institutions.

Ce changement de cap majeur représente un progrès pour les droits de l'individu, une approche de la conformité plus efficace pour les entreprises et un nouveau modèle de gouvernance pour les autorités.

L'enjeu est désormais de transformer ce texte en réalité opérationnelle, à la fois pour les responsables de traitements et les citoyens. C'est pourquoi le G29 a, dès l'annonce de l'adoption du texte, arrêté un plan d'action ambitieux pour la mise en œuvre de ce règlement et sa propre « mutation » en comité européen de la protection des données.

Le second temps fort de l'activité internationale de la CNIL en 2015 a résulté de l'arrêt de la Cour Européenne de Justice du 6 octobre 2015 invalidant le Safe Harbor. Le G29 a convoqué une plénière extraordinaire dès le 16 octobre, au cours de laquelle il a lancé un appel aux institutions et gouvernements européens et américains afin de trouver d'ici la fin janvier 2016 une solution pour que les transferts vers les Etats Unis soient opérés dans le respect des droits fondamentaux européens. Le G29 a par ailleurs ouvert un vaste chantier d'évaluation de l'impact

de ce jugement sur les autres outils de transferts que sont les BCR et les Clauses Contractuelles Types.

L'année 2016 s'annonce riche en développements tant sur le plan européen qu'international. Un nouveau monde s'ouvre pour l'Europe et il est à construire collectivement avec les acteurs de la société civile, les représentants de l'industrie, les institutions et les autorités. La mise en œuvre de cet arrêt de principe mais également de ce nouveau règlement européen est un défi pour tous et l'Europe n'aura de crédibilité et de poids dans la défense de ses valeurs que si elle avance unie et coordonnée. C'est cet objectif que la CNIL, qui préside à nouveau le G29 pour deux ans, et ses homologues européens, se sont fixés.

> **L'Europe n'aura de crédibilité et de poids dans la défense de ses valeurs que si elle avance unie et coordonnée.**

LE SUIVI ET LA FINALISATION DU RÈGLEMENT EUROPÉEN

Le Règlement

Après plus de quatre ans de négociations, l'année 2015 a été marquée par un double accord politique : d'une part, celui obtenu au Conseil de l'UE en juin 2015 qui a permis d'ouvrir la phase de négociations ou « trilogue » entre les trois institutions européennes (la Commission, le Parlement et le Conseil de l'UE) et d'autre part, l'aboutissement de ces négociations avec un accord sur le texte en décembre 2015.

Si ce dernier doit encore être formellement adopté par les institutions européennes, cette approbation représente une étape essentielle et attendue par tous les acteurs. En effet, le texte tel qu'adopté en décembre, prévoit, notamment:

▸ **Pour le citoyen,** un renforcement des droits existants, notamment en lui permettant de disposer d'informations complémentaires sur le traitement de ses données mais également de les obtenir sous une forme claire, accessible et compréhensible. Le droit à l'oubli est conforté et un nouveau droit, le droit à la portabilité, est prévu, rendant ainsi plus effective la maîtrise de ses données par la personne. Les mineurs font également l'objet d'une protection particulière.

▸ **Pour les entreprises,** une simplification des formalités, la possibilité d'un interlocuteur unique pour toutes les autorités de protection des données européennes et d'une mise à disposition d'une boîte à outils de conformité dont certains seront nouveaux (ex : code de conduite, certification). Ces outils pourront être modulés en fonction du risque sur les droits et libertés des personnes. (ex : tenue d'un registre, consultation des autorités de protection, notification des failles de sécurité…).

▸ **Pour les autorités de protection,** une affirmation de leurs compétences dès lors qu'il existe un établissement sur leur territoire ou que leurs citoyens sont affectés par le traitement mais également un renforcement de leurs pouvoirs notamment répressifs avec la possibilité de prononcer des sanctions administratives pouvant aller jusqu'à 4% du chiffre d'affaire mondial de l'entreprise concernée. Surtout, les « CNIL » européennes pourront désormais prononcer des décisions conjointes, aussi bien pour constater la conformité d'un organisme que pour prononcer une sanction. Cette intégration européenne renforcera ainsi la protection des personnes et la sécurité juridique pour les entreprises.

▸ **Une nouvelle architecture de coopération entre les autorités de protection avec un nouvel organe européen :** le Comité Européen de la Protection des Données (CEPD) en charge d'arbitrer les différends entre les autorités et également d'élaborer une doctrine « européenne »

Le G29 a suivi de près ces avancées en apportant son expertise notamment par des prises de position régulières et communes et des rencontres organisées avec les institutions communautaires.

Ainsi, **dans le cadre du trilogue,** le G29 a indiqué, en juin 2015, les points sur lesquels il convenait de porter une attention particulière et notamment :

- L'assurance que le nouveau cadre réglementaire **n'abaissera pas le niveau de protection actuel,** ni ne remettra en cause les principes et droits fondamentaux actuellement prévus dans la directive 95/46/CE.
- **L'interprétation large qu'il convenait de faire de la définition de données personnelles.** Ainsi les adresses IP et autres identifiants en ligne doivent, en règle générale, être considérées comme des données personnelles.
- **Le recours à la pseudonymisation** comme technique pouvant limiter les risques pour les personnes concernées. Les données pseudonymes ou pseudonymisées ne doivent pas être définies comme une nouvelle catégorie de données permettant de déroger à certaines obligations définies par le règlement. La pseudonymisation constitue uniquement une mesure de sécurité.
- **Le nécessaire respect des principes fondateurs que sont les principes de finalité et compatibilité des traitements,** en particulier dans le contexte du big data.
- **Une protection efficace des droits des personnes concernées,** notamment par un droit à la portabilité effective et des autorités de protection dotés de pouvoirs coercitifs appropriés et de ressources suffisantes.
- **Un nouveau modèle de gouvernance européenne efficace et équilibrée** pour les autorités de protection, fondé sur la proximité avec les citoyens et une coopération entre autorités intensifiée.

Le G29 s'est également exprimé en septembre 2015 sur la future structure interne du CEPD considérant les éléments suivants comme composantes nécessaires du nouveau modèle européen :

- **un CEPD fort et indépendant, agissant comme organe incontournable de décision.** Il est composé d'un président, des 28 commissaires des autorités de protection de chaque État membre et du contrôleur européen de la protection des données (chargé de contrôler la conformité des traitements des institutions communautaires). Il s'appuie sur des groupes de travail composés d'experts.
- **un Président, mandaté par le CEPD** qui exprime la voix des autorités de protection. Elu parmi ses membres, la durée de son mandat doit être suffisante afin de lui permettre de mener à bien ses misions. Ainsi, un exercice à plein temps de ses missions lui permettrait de remplir cette exigence. Le Président, en tant responsable du CEPD, devrait également disposer d'un contrôle s'agissant de son budget et de son personnel.
- **un comité exécutif dont la mission première serait d'assurer l'effectivité des missions du CEPD**. Composé du Président et de deux vices présidents, il devrait, en autre, aider et assister le Président dans ses relations avec les autorités de protection.
- **un secrétariat, doté de ressources suffisantes et professionnelles.** Fourni par le contrôleur européen de la protection des données, il est placé sous la responsabilité du président du CEPD.

Les étapes du règlement européen

LA DIRECTIVE

L'année 2015 a été marquée par l'aboutissement de la phase de négociations ou « trilogue »[1] entre les trois institutions européennes (la Commission, le Parlement et le Conseil de l'UE) en décembre 2015 sur le texte de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

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

1 **Pour rappel, le Parlement européen a adopté sa position en première lecture le 12 mars 2014. Le Conseil a, de son côté, dégagé une orientation générale le 8 octobre 15. Cinq trilogues ont ensuite eu lieu d'octobre au 15 décembre 2015. Ils ont abouti à l'adoption du texte du trilogue le 16 décembre 2015 par le Comité des représentants permanents des Etats membres au Conseil et au vote du texte par la Commission libertés civiles, justice et affaires intérieures du Parlement européen le 17 décembre 2015.**

Le respect relatif des préconisations du G29

Le G29 a écrit en décembre 2015 aux institutions européennes afin de souligner les points sur lesquels il convenait de porter une attention particulière.

Il a tout d'abord exprimé deux remarques générales. Il a ainsi regretté le principe même d'avoir deux instruments au lieu d'opter pour un règlement qui s'applique à tous les secteurs. De nombreuses administrations (fiscale, douanière, etc.), devront se conformer à des obligations distinctes selon que leurs activités sont régies par l'un ou l'autre texte. Il a également rappelé l'objectif de consacrer, au moyen de la réforme en cours, un haut niveau de protection des données et, par conséquent, insisté pour que les exceptions aux principes justifiées par les spécificités de la matière répressive, demeurent d'interprétation stricte. Il a également souhaité que les principes consacrés par les deux textes fassent l'objet d'une définition commune.

Il a ensuite exprimé un certain nombre de préoccupations spécifiques dont une grande partie a été résolue dans le texte de l'accord auquel sont parvenues les institutions.

Ainsi, conformément aux demandes du G29, **le texte de l'accord reprend les définitions des concepts clés** (données à caractère personnel, traitement, pseudonymisation, violation de données à caractère personnel, données génétiques, données biométriques, données de santé) consacrées par le règlement. De plus, **il distingue les niveaux d'implication et les rôles des personnes dont les données sont traitées dans une procédure pénale** (victime, suspect, auteur) et assure l'exactitude et la pertinence des données traitées ainsi que le respect des droits découlant de ces différents statuts.

Comme cela a été soutenu par le G29 dans ses réflexions sur la réforme de la protection des données, les traitements mis en œuvre à des fins répressives devront à l'avenir tenir compte du respect de la vie privée dès leur conception *(privacy-by-design)* et permettre ce respect « par défaut » *(privacy by default)*.

En termes de sécurité, les obligations des responsables de traitement et sous-traitants ont été renforcées conformément aux attentes du G29 : journalisation obligatoire des opérations de traitement, mise à disposition des autorités de contrôle avec laquelle ils doivent coopérer sur demande, réalisation d'une étude d'impact relative à la protection des données pour tout traitement susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques. Par ailleurs, les failles de sécurité affectant les données à caractère personnel traitées devront être notifiées à l'autorité de contrôle par principe, à moins qu'il soit peu probable que la violation en question engendre des risques pour les droits et libertés de d'une personne physique.

Par ailleurs, **la désignation d'un délégué à la protection des données est rendue obligatoire** sauf pour les tribunaux et autres autorités judiciaires indépendantes.

Le texte prévoit également la désignation d'une autorité de contrôle indépendante afin de surveiller la bonne application de la directive et la coopération des autorités entre elles. Le G29 avait souligné le rôle particulièrement important de ces autorités dans un contexte où les données traitées permettent de limiter les libertés fondamentales des personnes concernées au titre de la prévention, la répression ou la poursuite d'une infraction. Les pouvoirs des autorités de contrôle auraient toutefois gagné à être développés davantage, tout comme les sanctions applicables en cas de manquement.

Dans son adresse aux trois institutions, le G29 avait appelé à ce que les principes clefs de la protection des données ne soient pas vidés de leur substance par l'étendue des exceptions qui y seraient prévues. A cet égard, le texte de l'accord n'est toutefois pas entièrement satisfaisant. Ainsi, le traitement de catégories particulières de données à caractère personnel [2] est autorisé sous conditions plutôt qu'interdit sauf exceptions. De même, il est possible de prendre une décision fondée exclusivement sur un traitement automatisé, y compris par le biais du profilage, dès lors que le droit de l'union ou la loi nationale l'autorise alors que le G29 préconisait également une interdiction sujette à exceptions. Par ailleurs, la consultation de l'autorité de contrôle, préalablement à la mise en œuvre d'un traitement est limitée à certaines hypothèses de traitements considérés comme « à risque ». Quant aux droits des personnes (accès, rectification, suppression), ils sont largement calqués sur ceux prévus par le règlement mais les hypothèses dans lesquelles ils peuvent être limités ou exclus demeurent vagues et pourraient couvrir de nombreux scenarii.

La question des transferts vers des pays non adéquats suscite également certaines réserves. Comme l'avait souligné le G29, la question des finalités pour lesquelles elles pourraient ensuite être réutilisées demeure cruciale. La problématique de la surveillance de masse ne saurait être esquivée et les données ne devraient être transférées que lorsqu'elles sont strictement nécessaires à la réalisation d'une enquête ou à une procédure.

> **Le G29 a insisté pour que les exceptions aux principes justifiées par les spécificités répressives demeurent d'interprétation stricte.**

2 Termes désormais employés pour désigner les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques permettant d'identifier une personne de manière univoque ou des données concernant la santé ou la vie et l'orientation sexuelles.

LA PRÉSIDENCE DU G29 ET SES ACTIVITÉS

Le G29, présidé par la présidente de la CNIL depuis février 2014, a souhaité se positionner sur les sujets structurants que sont notamment la réforme du cadre européen (le Règlement et la Directive Police Justice), les activités de surveillance et le droit à l'oubli.

Par ailleurs, toujours marqué par une actualité européenne chargée, le G29 s'est prononcé sur plusieurs thématiques sectorielles et transversales.

À travers ses avis et déclarations, le G29 construit ainsi une véritable régulation européenne de la protection des données.

Sur les aspects de police-justice

À la suite des attentats à Paris le 7 et 8 janvier 2015, le G29 s'est exprimé sur le sujet du PNR (Passenger Name Record) européen. Il a rappelé que si la mise en place de mesures pour contrer les activités terroristes et la préparation d'activités terroristes est légitime, ces mesures doivent être mises en œuvre dans le respect des droits fondamentaux et du respect de la vie privée et de la protection des données. Ainsi le système de PNR Européen doit être respectueux des principes de nécessité et de proportionnalité.

Le G29 a poursuivi son analyse des accords PNR organisant la transmission des données de passagers européens voyageant vers des pays tiers, et en particulier vers les Etats-Unis et le Mexique. Dans ce cadre, l'absence de base légale permettant le transfert des données PNR des passagers européens aux autorités mexicaines a été souligné

Il s'est également penché sur les scénarii soumis par le comité Cybercrime du Conseil de l'Europe concernant l'accès transfrontière direct par des autorités répressives aux données stockées dans d'autres juridictions

Sur les aspects technologiques

Le G29 a élaboré un avis sur les drones ainsi que sur un code de conduite développé par l'industrie concernant le cloud computing. Il a également poursuivi son analyse des politiques de vie privée de certains grands acteurs de l'Internet (ex : Google, Facebook, …) ainsi que ses travaux sur les standards techniques (ex : ISO, Do Not Track).

Sur les aspects financiers et ceux concernant le secteur public

Le G29 a adopté des lignes directrices sur l'échange automatisé d'informations fiscales tel que développé par les standards CRS de l'OCDE et a poursuivi ses travaux sur les standards OCDE en matière financière. Il a également analysé le règlement européen sur l'identification électronique ainsi que la problématique de la publication des données des représentants officiels.

Sur les thématiques transversales

Suite à l'arrêt de la CJUE Google Espagne en 2014 relatif au déréférencement, qui a conclu que l'exploitant d'un moteur de recherche était un responsable de traitement soumis au droit européen dès lors que l'une de ses entités en Europe participait au traitement de données en question, par exemple en matière publicitaire, le G29 s'est penché sur l'actualisation de son avis de 2010 sur le droit applicable. Il a également assuré un travail de coordination s'agissant du traitement de plaintes liées au droit au déréférencement.

Enfin, afin de renforcer la cohérence de ses travaux sur des sujets transversaux, un nouveau groupe de travail en charge des aspects de coopération a été créé. Ce dernier travaille sur le développement d'outils communs de coopération (ex : formulaire unique de plainte, organisation d'ateliers thématiques, amélioration du site internet G29, etc.) et sur les aspects liés à la coopération internationale (GPEN, conférence de printemps, conférence internationale).

INFO +

En 2015, le G29, c'est : 41 documents adoptés, 8 groupes de travail, 6 plénières regroupant les 29 autorités de protection des données de l'Union Européenne.

LA COOPÉRATION INTERNATIONALE ET EUROPÉENNE

Le développement technologique et la mondialisation ancrent fermement les enjeux informatique et libertés sur la scène internationale.

C'est pourquoi la question de la coopération internationale et européenne apparait comme un sujet particulièrement stratégique et d'ampleur croissante, qui nécessite un investissement dans toutes les initiatives qui se développent.

Cette coopération s'effectue au sein de plusieurs forums dont la Conférence Internationale, la Conférence de Printemps, ou encore dans des forums plus spécifiques comme l'Association Francophone des Autorités de Protection des Données (AFAPDP).

La 37ème Conférence Internationale

En 2015, la 37ème Conférence internationale des commissaires à la protection des données et de la vie privée s'est tenue à Amsterdam aux Pays-Bas et a réuni plus de 100 autorités et commissaires. Lors de la session fermée, deux thèmes ont été débattus : les données génétiques et le contrôle des activités de surveillance.

Les données génétiques, quels défis pour l'avenir ?

Partant du constat que les données génétiques offrent de nombreuses et diverses informations scientifiques, médicales et personnelles sur les individus tout au long de leur vie, les autorités et commissaires à la protection des données et à la vie privée ont souhaité faire un certain nombre d'observations communes quant à la manière dont ces données doivent être traitées. Ainsi, il est apparu particulièrement important d'énoncer que les personnes concernées doivent pouvoir garder le contrôle de leurs données, recevoir des informations appropriées et voir leurs choix respectés. Cela peut être effectué grâce à divers moyens permettant d'assurer une gestion dynamique du consentement tout au long du cycle de vie des données, et complété par des garanties supplémentaires telles que : des comités de protection des personnes (CPP), des programmes de gestion de la vie privée, des évaluations d'impact de la vie privée, le *Privacy by design* et les certifications.

Par ailleurs, une volonté de rapprochement entre la communauté scientifique et celle de la protection des données et de la vie privée a été formulée. En effet, cela permettrait à ces communautés d'accroître leur compréhension mutuelle et de garantir que l'innovation continue à tirer les bénéfices des données génétiques tout en s'assurant que les droits fondamentaux et droits des consommateurs soient respectés.

Le contrôle des activités de surveillance, quel rôle pour les autorités de protection des données dans une société en mutation ?

L'ampleur du débat public sur les activités de renseignement à travers le monde, ainsi que la mutation de l'environnement de sécurité du fait de la potentialité d'activités terroristes dans tous les pays, ont soulevé des questions difficiles pour les autorités de protection des données. Ces dernières ont identifié plusieurs points sur lesquels leurs actions seraient importantes : la promotion des principes de proportionnalité et de légalité des activités de renseignement ; la coordination avec les organismes de surveillance nationaux et internationaux ; la promotion d'une meilleure transparence ; la promotion d'une utilisation plus large du chiffrement comme un moyen légitime pour protéger les données de consommation.

La prochaine Conférence internationale des commissaires à la protection des données et de la vie privée se déroulera à l'automne 2016 au Maroc.

L'AFAPDP

En 2015, 48 pays membres de la Francophonie sur 80 disposent d'une loi et d'une autorité de protection des données personnelles. La protection des données personnelles doit encore progresser dans de nombreux pays. Ceux-ci peuvent s'inspirer des textes nationaux et pratiques adoptés par les pays représentés au sein de l'AFAPDP, et des textes régionaux en vigueur en Afrique et en Europe. L'AFAPDP se félicite de la coopération mise en place avec les autorités de protection des données récemment installées en Côte d'Ivoire, au Kosovo et au Mali.

Les membres de l'AFAPDP, dont la CNIL, ont adopté lors de leur assemblée générale en 2015 deux résolutions : l'une, inspirée des déclarations canadienne et européenne, sur les principes fondamentaux pour éviter tout risque de surveillance de masse et contrôler les activités des services nationaux de renseignement ; l'autre sur la prise en compte des principes éthiques lors des traitements de données de santé et génétiques. Ces résolutions consolident les bases d'une doctrine francophone de la protection des données. Les membres de l'AFAPDP ont également mis à l'agenda de la prochaine Conférence internationale des commissaires à la protection des données l'adoption d'une résolution sur la protection des données dans le domaine de l'action humanitaire internationale. L'AFAPDP poursuit aussi le travail de mise en commun des méthodes de contrôle de l'application des lois commencé à l'automne 2015.

Au-delà de l'animation du réseau de ses membres, l'AFAPDP est ouverte à des partenariats ou coopérations multiples autour des droits fondamentaux. Elle a notamment travaillé cette année avec le réseau des Médiateurs et Ombudsmans francophones pour la sensibilisation des enfants à leurs droits. ■

INFO +

La Conférence internationale des commissaires à la protection des données et à la vie privée

Depuis 1979, les autorités et commissaires à la protection des données et à la vie privée de tous les continents se réunissent pour réfléchir ensemble aux défis majeurs qui se dressent en matière de respect de la vie privée, dans un contexte international marqué par de fortes évolutions technologiques, politiques, juridiques et économiques. La Conférence internationale des commissaires à la protection des données et de la vie privée se compose d'une session fermée regroupant l'ensemble des autorités et commissaires ainsi que d'une session ouverte à la société civile et aux entreprises.

3

LES SUJETS DE RÉFLEXION EN 2016

Data brokers, le pétrole et l'iceberg

**Véhicules connectés :
en route vers le pack de conformité**

**Des objets connectés aux objets autonomes :
quelles libertés dans un monde robotisé ?**

Data brokers : le pétrole et l'iceberg

Les courtiers de données ne constituent pas une catégorie juridique clairement identifiée mais au regard de l'importance qu'elle commence à revêtir, elle appelle l'attention de la CNIL. Par courtiers, on entend généralement des professionnels opérant sur un marché secondaire des données. Cette définition recouvre plusieurs activités qui toutes tendent à faciliter la circulation des données et leur enrichissement.

Dans un premier cas, le courtier assume un rôle de mise en relation entre détenteurs de données souhaitant monétiser ou acquérir des bases ; une seconde figure fait du courtier un concentrateur qui procède à l'agrégation et à l'enrichissement des données, provenant de partenaires, clients ou de registres publics, pour le compte de clients ou pour son propre compte. Dans cette dernière hypothèse, l'analyse des données lui permet d'offrir des services à valeur ajoutée (constitution, affinage du profil et segmentation client) à des sociétés souhaitant mieux cibler leurs offres de biens et de services..

Encore mal connue en Europe, cette activité est d'ores et déjà clairement identifiée outre-Atlantique où **elle suscite des questionnements notamment sur la transparence, le degré de contrôle des personnes sur leurs données et sur la sécurité.**

LE PÉTROLE

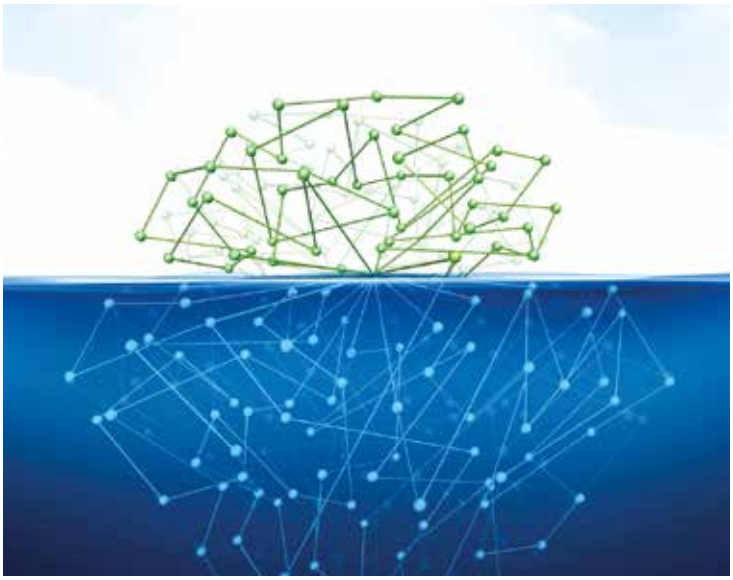
Depuis quelques années, les données font figure de « pétrole du numérique », alimentant le moteur de la nouvelle économie. Pour autant, le commerce des données n'est pas uniformément considéré et fait l'objet de courants d'opinion contradictoires. Cette opposition s'exprime clairement dans l'affrontement des tenants d'une propriété de la donnée et de ceux qui considèrent la donnée comme le support d'un droit personnel. Dans son étude annuelle de 2014, le Conseil d'Etat a mis en évidence cette opposition pour écarter la notion de « propriété » et conforter l'approche européenne en recommandant l'adoption d'un droit-liberté reconnu en Allemagne par la Cour constitutionnelle. **Ce droit à l'autodétermination informationnelle** se traduit par l'affirmation du droit de toute personne de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant. Repris

dans le projet de texte sur la République numérique, ce droit rejette la dimension propriétaire du droit sur la donnée.

Si le commerce des fichiers et leur valeur marchande sont reconnus (cf. à cet égard, la jurisprudence de la Cour de cassation, notamment par son arrêt du 25 juin 2013), ce sont donc sous condition de légalité et sans écarter les droits des personnes concernées par les données cédées.

L'enjeu du commerce des données réside donc dans la légalité du traitement, qui s'exprime par l'examen des caractéristiques du traitement opéré sur les données en termes de base légale, de finalité, de proportionnalité et de respect des droits des personnes concernées, outre le cas échéant, le régime de formalité applicable.

La loi Informatique et Libertés permet sans conteste la circulation des données entre destinataires et l'apparition de nouveaux responsables de traitements, eux-mêmes soumis en cascade à des obligations particulières ou communes avec le responsable initial. Le règlement sur la protection des données personnelles comporte également des dispositions qui concernent les courtiers, notamment par le fait que le courtage vise dans une large mesure à permettre la création de profils destinés à automatiser des actions.



L'ICEBERG

Le cadre juridique existant ne reflète cependant pas la réalité de la situation du courtage car ce hub des données revêt les caractères de l'iceberg ; sa partie émergée n'est pas la plus importante. Le courtage de données vise à l'agrégation des données puis à leur redistribution pour des finalités qui peuvent être variées, mais qui, pour l'heure, se concentrent sur le ciblage commercial (marketing direct, publicité, amélioration de l'expérience client), la vérification de caractéristiques (honorabilité, solvabilité, identité) des personnes et la lutte contre la fraude. Les données collectées le sont à partir de sources qui peuvent varier dans la pratique, notamment internationale, de l'exploitation de sources ouvertes à des transferts de données collectées par des responsables tiers.

En matière de marketing, le modèle conduit à l'agrégation de bases de données constituées pour la relation client dans les magasins avec des données issues de la navigation, des commandes sur internet ou de l'utilisation de services de la société de l'information. La clé de rapprochement, qu'il s'agisse de données nominatives, de cookies, d'adresse électronique, postales ou de tout autre donnée, est donc fondamentale pour la création du profil.

L'analogie avec l'iceberg concerne donc à la fois le mode de production de ces profils (par stratification progressive de données éparses mais reliées ; puis par consolidation des données jusqu'à former un ensemble cohérent), mais aussi par le caractère invisible de l'ensemble ainsi formé.

La question est donc celle de la transparence nécessaire et du pouvoir reconnu à chacun de contrôler le sort d'une donnée collectée lors de l'achat d'un article en supermarché qui est utilisé pour adresser une publicité sur un téléphone mobile par une enseigne en ligne.

Encore peu visibles, les data brokers constituent l'un des sujets de réflexion de l'année 2016. ■

Véhicules connectés : en route vers le pack de conformité

Le véhicule connecté est un enjeu stratégique majeur pour les constructeurs automobiles mais il est également identifié par de nombreux autres professionnels comme une opportunité nouvelle de recueillir des informations ou d'entrer en relation avec les automobilistes par le bais de nouveaux services plus personnalisés et plus pertinents.

Le 7 janvier 2015, la CNIL a organisé la première rencontre de l'ensemble de l'écosystème français du véhicule connecté. Cette initiative, réalisée en partenariat avec les animateurs du plan « *Big data* » du programme « *Nouvelle France Industrielle* », a permis de mesurer la diversité des attentes et vérifier la nécessité d'offrir un cadre de régulation des données personnelles fondé sur la prise en compte de la protection de la vie privée dès la conception du produit (ou « *privacy by design* »).

Cette démarche a été complétée par de premiers travaux sur une étude de cas liée au véhicule connecté afin de vérifier la pertinence de la démarche par scénarii, telle qu'elle avait été conduite dans les précédents travaux sur les compteurs intelligents (ou *smart grids*) et l'exploitation des données énergétiques dans le foyer. Tout au long de l'année 2015, la CNIL a donc consolidé son expertise sur des sujets connexes comme le véhicule électrique, la mobilité urbaine, l'accidentologie, le *Pay how you Drive* afin d'offrir aux participants des travaux sur le pack de conformité un éventail de réflexions complet.

LES GRANDES QUESTIONS INFORMATIQUE ET LIBERTÉS

Les premiers échanges avec les constructeurs, équipementiers, assureurs, *startups,* et forces de l'ordre mettent en évidence deux questions particulièrement structurantes pour le véhicule connecté et qui serviront de fil rouge aux travaux sur le pack de conformité.

La première est évidemment liée à la sécurité. En effet, contrairement à des objets connectés « traditionnels », l'automobile est par définition en mouvement dans l'espace public. Il n'est pas besoin de rappeler les chiffres de la sécurité routière pour constater que **cet objet n'est pas comme les autres et que la question de la sécurité est nécessairement centrale**. La question de la sécurité et de la confidentialité des données à caractère personnel se double dans le cas de l'automobile connectée d'une dimension cybersécurité. On ne peut réduire le risque à celui d'une atteinte à la vie privée puisque la compromission des éléments de pilotage peut conduire à des conséquences importantes voire vitales pour les occupants et les tiers.

La seconde question est celle de l'accès aux données produites par le véhicule ou son utilisateur. Par la force de l'évidence, les données produites dans le véhicule vont constituer un enjeu majeur. Ces données, qu'elles soient des données techniques, des données environnementales ou comportementales, constituent un gisement important d'informations pour tous ceux qui à un titre ou à un autre ont un lien avec l'automobile et son conducteur. Que l'on songe à la maintenance, à la commercialisation de biens ou de services en lien avec l'auto ou encore aux villes intelligentes, la voiture connectée va devenir une plateforme de données incontournable.

UNE PLATEFORME MOBILE

L'adoption récente du règlement européen sur la protection des données personnelles marque pour beaucoup une étape de l'intégration européenne en matière de coopération entre autorités. Le véhicule connecté, par définition mobile sur tout le territoire de l'Union Européenne, doit bénéficier d'un traitement européen harmonisé pour tirer le plein potentiel de l'innovation. En matière de données personnelles, les autorités françaises et allemandes sont d'ores et déjà en contact pour assurer la coordination des travaux nationaux en prévision du portage des conclusions nationales au niveau européen. Les travaux du pack qui seront conduits en prenant en compte le règlement dont l'application est prévue pour 2018 permettront d'anticiper de nouveaux droits comme celui à la portabilité des données ou encore l'exigence de protection dès la conception.

> **Les travaux du pack prendront en compte le règlement européen dont l'adoption est prévue en 2018.**

QUESTION DE MÉTHODE

Entre enjeux industriels, d'innovation et de protection de la liberté d'aller et venir, le véhicule connecté doit bénéficier d'une approche partenariale sans laisser personne sur le bord de la route. Pour cette raison, la CNIL a proposé que le pack de conformité ne soit pas l'affaire de quelques-uns mais puisse s'ouvrir à tout l'écosystème du véhicule connecté afin de refléter les attentes, besoins et exigences de protection. Depuis la fin février 2016, les acteurs discutent afin de pouvoir présenter leurs premières réflexions au Mondial de l'Automobile à l'automne 2016. ■

Des objets connectés aux objets autonomes : quelles libertés dans un monde robotisé ?

Enfin, un futur avec des robots ? Depuis des décennies, la science-fiction nous prédit des robots omniprésents. Pourtant, notre vie quotidienne en paraît encore bien démunie. L'est-elle tant que cela ? Des robots industriels aux « robots logiciels », les signaux, tout comme les questions éthiques et juridiques, se multiplient. La CNIL a décidé d'inscrire ce sujet à son programme de réflexion afin de nourrir une exploration prospective des enjeux éthiques et juridiques de la robotique, par une analyse à la fois économique et sociétale.

Si les prédictions sur la taille future des marchés concernés sont sujettes à caution, les experts s'accordent sur l'évolution de la robotique en dehors du domaine industriel vers des services aux formes très diverses. **Dans une étude de 2015,** l'Institut Xerfi prévoit ainsi des opportunités à l'horizon 2020 pour les robots compagnons, les drones, les robots médicaux, les robots de transports de marchandises et de personnes, etc.

Les enjeux en termes de respect de la vie privée sont très forts. Les robots compagnons évolueront dans l'intimité du domicile des personnes, et les robots médicaux sont (déjà) utilisés dans un environnement par nature sensible. Dans le domaine de la sécurité comme dans ceux des transports ou de la logistique, les questions de surveillance seront inévitables. Enfin, les usages, certes encore très émergents, des robots dans le commerce, ouvrent de nouvelles possibilités pour le marketing, la relation commerciale, le ciblage et le suivi.

LES ROBOTS, DES OBJETS CONNECTÉS COMME LES AUTRES ?

Les ingrédients pour un robot : des capteurs, du calcul et des moyens d'agir

Smartphone, objets connectés pour la maison (thermostats, pèse-personnes, aspirateurs), objets mesurant des constantes du corps (bracelets, montres), drones, voitures, etc… les objets connectés ou communicants sont partout, avec une caractéristique commune : rendre « smart » ou intelligents des objets du quotidien. Que signifie « intelligent » ? Assez simplement, il s'agit de l'adjonction de trois capacités : **des capteurs, de la puissance de calcul et des communications réseau.**

La captation permanente de données dans notre environnement quotidien est une vraie nouveauté. Une telle intensité de captation crée une grande différence avec le monde des fichiers traditionnels, comme le montrait le deuxième Cahier IP **« Le corps, nouvel objet connecté »** de la CNIL. Au-delà des informations sensibles (présentes par exemple dans un dossier médical), on capte sur longue durée des

> La captation permanente de données dans notre environnement quotidien est une vraie nouveauté.

données d'apparence anodine (nombre de pas, CO2 dans une pièce, courbe de poids, cycle du sommeil, voire localisation). L'accumulation induit la sensibilité, en permettant d'inférer des informations sur la personne (par exemple, prédire statistiquement son état de santé futur).

Les capteurs sont connectés et deviennent ensuite communicants, soit directement (par des réseaux dédiés comme ceux de Sigfox ou Lora) soit par le smartphone, devenu le véritable centre de contrôle des objets connectés.

L'étape suivante de cette transformation numérique semble être de **« faire disparaître au maximum ces technologies »,** comme l'explique Rand Hindi de la start-up d'intelligence artificielle française Snips, car les sollicitations permanentes sont des perturbations que l'individu apprécie peu. Il faut donc ajouter une capacité à décider et à agir de manière automatique, grâce au machine *learning,* au *big data,* ou à l'intelligence artificielle.

Or, la conjonction de ces caractéristiques définit justement un robot, c'est-à-dire une machine réunissant des capacités de perception, de décision, d'action et d'interaction adaptées à son environnement et aux tâches pour lesquelles il est conçu. La robotique est donc un horizon pour l'internet des objets.

Plus une machine est « autonome », plus elle est en réalité dépendante… des données

Par rapport à des objets connectés traditionnels, les robots sont dotés d'un plus grand niveau d'autonomie. Or, l'autonomie implique la capacité à coopérer avec des humains dans un espace commun : les robots deviennent des *cobots* (robots collaboratifs), pouvant agir avec des humains et non pas à leur place ou loin d'eux.

Pour ce faire, ils doivent collecter beaucoup plus de données, ce qui révèle un paradoxe éthique fondamental dans le domaine de la protection des données : pour être plus autonome, une machine doit être en réalité plus dépendante aux données personnelles. Par exemple, une voiture autonome doit capter en permanence ce qui se passe autour d'elle (voir encadré), de même qu'un drone autonome (voir encadré). Un robot compagnon pour aider des personnes dépendantes isolées doit quant à lui collecter des données sur le logement, ne serait-ce que pour ne pas blesser la personne qu'il doit aider. Il doit aussi reconnaître les personnes présentes et donc, pourrait recourir à des technologies biométriques de reconnaissance faciale ou de la voix. ▸▸▸

FOCUS

Les drones, déjà presque des robots volants

Les drones font régulièrement les gros titres de la presse. Pourtant, des aéromodèles télépilotés existent depuis longtemps, même s'ils étaient difficiles à maîtriser et constituaient donc un loisir de passionnés. Aujourd'hui, les drones ressemblent à des smartphones volants et faciles à prendre en mains, puisque le vol en est déjà assisté. Les modèles récents peuvent décoller, se stabiliser, éviter des obstacles tout seuls (fonction dite sense and avoid). D'autres vont même pouvoir suivre automatiquement une personne, par exemple pour la filmer pendant une séance de vélo ou de ski (mode follow me). Ces prouesses techniques s'appuient sur toujours plus de capteurs, et toujours plus de données, en particulier concernant l'utilisateur et les personnes à proximité. Et bientôt, les drones seront vraiment des robots, accomplissant des tâches, parfois même en essaim, sous la supervision plus ou moins directe d'humains. L'effectivité de la nouvelle procédure d'autorisation reste cependant soumise à la publication de plusieurs textes d'application, prévus par la loi, après avis de la CNIL. Dans l'attente de la publication de ces textes d'application, les procédures actuellement en vigueur en vertu des chapitres IX et X de la loi Informatique et Libertés restent applicables.

Il est donc indispensable de penser globalement la gouvernance des données, en faisant du *privacy by design* (intégration de la protection de la vie privée dès la conception) un impératif pour la robotique. Dans son rapport **« éthique de la recherche en robotique »,** la Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene (CERNA) (Allistène, 2014) préconise ainsi : « s'il n'est pas possible de prémunir à sa conception un robot d'un usage inapproprié ou illégal des données qu'il capte, le chercheur doit néanmoins veiller à ce que le système robotique facilite le contrôle de l'usage des données. »

INFO +

Les voitures autonomes, des robots sur nos routes

La tendance est au développement de véhicules partiellement voire totalement autonomes sur les routes. Les prototypes de véhicules autonomes à l'essai intègrent de plus en plus de capteurs, par exemple des radars ou lidars (permettant un guidage laser). Certains chiffres concernant la collecte de données évoquent presque un Gigaoctet de données par seconde. Etant donnée la nature particulièrement complexe du trafic routier, l'autonomie de ces véhicules nécessite qu'ils soient en réseau et qu'ils puissent apprendre collectivement (par exemple pour faire face à des situations nouvelles). C'est la voie suivie par certains constructeurs de voitures électriques, qui échangent des données en temps réel.

VERS UNE RÉFLEXION ÉTHIQUE DU NUMÉRIQUE ET UNE CULTURE DE LA DONNÉE

Trois enjeux éthiques[1] se distinguent spécifiquement dans le domaine de la robotique, chacun d'eux faisant écho à des préoccupations concernant les données.

1 La réparation et l'augmentation de l'humain par la machine

Les questions éthiques liées au rapprochement entre la robotique et le corps même des individus sont fondamentales. Tout rapprochement entre les technologies et le corps créera un impératif éthique de respect de la dignité de la personne humaine, de son droit à l'autodétermination informationnelle et à faire des choix libres sans risquer la discrimination.

2 L'imitation du vivant et les interactions affectives et sociales : vers de véritables interactions humains-machines respectueuses des droits des personnes ?

Quelle confiance peut-on avoir dans les robots ? Comment rendre compte de leur comportement ? « *Le consentement devra être réinventé en environnement robotique, d'autant plus que les risques de manipulation émotionnelle de la personne sont importants* », comme l'a souligné le psychologue Serge Tisseron lors des auditions de l'Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques en décembre 2015. Les robots permettant des interactions humains-machines sophistiquées, ils doivent aussi permettre un dialogue contextuel et explicite, adaptée aux souhaits de la personne.

3 Autonomie et capacités décisionnelles : jusqu'à quel point les technologies doivent-elles prendre des décisions à notre place ?

La robotique pose enfin une question éthique générale à propos de la capacité à agir de l'utilisateur. Pour la CNIL, il n'est donc pas toujours utile de distinguer un robot mécanique d'un robot logiciel pour penser la régulation de l'autonomie décisionnelle. La question de la transparence des algorithmes ou au moins de leurs règles, celle de la capacité à comprendre comment des décisions qui affectent les personnes sont prises par des systèmes autonomes, sont des questions éthiques prospectives fondamentales. ■

1 Ces enjeux sont identifiés dans le rapport de la CERNA, déjà cité.
2 OPECST, « Les robots et la Loi », auditions publiques du 10 décembre 2015.

4

BILAN FINANCIER ET ORGANISATIONNEL

Les membres de la CNIL

Les ressources humaines et financières

Les membres de la CNIL

LE BUREAU

PRÉSIDENTE
Isabelle FALQUE-PIERROTIN,
conseiller d'État
Membre de la CNIL depuis 2004
et vice-présidente de 2009 à 2011,
Isabelle Falque-Pierrotin est présidente
de la CNIL depuis le 21 septembre 2011.

VICE-PRÉSIDENTE DÉLÉGUÉE
Marie-France MAZARS,
conseiller honoraire à la Cour de cassation
Secteur : *Ressources humaines, travail et biométrie*
Marie-France Mazars est membre
et vice-présidente déléguée de la CNIL
depuis février 2014.

VICE-PRÉSIDENT
Eric PERES,
membre du Conseil économique,
social et environnemental
Secteur : *industrie, transports, énergie, défense*
Eric Peres est membre de la CNIL
depuis décembre 2010, puis vice-président
depuis février 2014.

Les membres élus de la formation restreinte sont :
- **Jean-François CARREZ *(Président)***
- **Philippe GOSSELIN**
- **Dominique CASTERA**
- **Marie-Hélène MITJAVILE**
- **Alexandre LINDEN**
- **Maurice RONAI**

LES MEMBRES
(COMMISSAIRES)

Jean-François CARREZ,
président de chambre honoraire
à la Cour des comptes
Secteurs : *Police, immigration, coopération internationale*
Jean-François Carrez est membre
de la CNIL depuis janvier 2009.

Dominique CASTERA,
membre du Conseil économique,
social et environnemental
Secteurs : *Libertés individuelles, vie associative, vote électronique, élections.*
Dominique Castera est membre
de la CNIL depuis octobre 2010.

Nicolas COLIN,
inspecteur des finances, co-fondateur
et associé de la société de capital-risque
TheFamily
Secteur : *santé (assurance maladie/ recherche/ e-santé)*
Nicolas Colin était membre de la CNIL
de février 2014 à février 2016.

Loïc HERVE,
sénateur de la Haute-Savoie
Secteur : *santé*
Loic Hervé est membre de la CNIL
depuis septembre 2014.

Laurence DUMONT,
député du Calvados
Secteurs : *social et logement*
Laurence Dumont est membre
de la CNIL depuis octobre 2012.

Joëlle FARCHY,
professeure de sciences de l'information
et de la communication à l'Université
Paris I et chercheure au Centre d'économie
de la Sorbonne
Secteurs : *affaires culturelles, sportives, jeux, tourisme.*
Joëlle Farchy est membre de la CNIL
depuis février 2014.

Gaëtan GORCE,
sénateur de la Nièvre
Secteur : *justice, eurojust*
Gaëtan Gorce est membre de la CNIL
depuis décembre 2011.

Philippe GOSSELIN,
député de la Manche
Secteur : *collectivités territoriales, vidéoprotection et téléservices*
Philippe Gosselin est membre de la CNIL
depuis février 2015.

Philippe LEMOINE,
Président du Forum d'Action Modernités
et Président de la Fondation internet
nouvelle génération
Secteurs : *recherche, statistiques, archives et données publiques.*
Philippe Lemoine est membre de la CNIL
depuis février 2014.

Marie-Hélène MITJAVILE,
conseiller d'État
Secteur : *international*
Marie-Hélène Mitjavile est membre
de la CNIL depuis février 2009.

Alexandre LINDEN,
Conseiller honoraire à la Cour de cassation
Secteur : *santé (assurance maladie / recherche/ e-santé)*
Alexandre Linden est membre de la CNIL
depuis février 2014.

François PELLEGRINI,
professeur des universités à l'université
de Bordeaux
Secteurs : *distribution, commerce-marketing, lutte contre la fraude et impayés, international*
François Pellegrini est membre de la CNIL
depuis février 2014.

Maurice RONAI,
chercheur à l'École des Hautes Études
en Sciences Sociales (EHESS)
Secteurs : *NTIC, communications électroniques, innovation technologique.*
Maurice Ronai est membre de la CNIL
depuis février 2014.

Jean-Luc VIVET,
conseiller Maître à la Cour des comptes
Secteurs : *banque, crédit, assurance et fiscalité*
Jean-Luc Vivet est membre de la CNIL
depuis février 2014.

COMMISSAIRES DU GOUVERNEMENT
Jean-Alexandre SILVY,
Catherine POZZO DI BORGO, adjoint

Les ressources humaines et financières

LES RESSOURCES HUMAINES

Pour faire face à l'augmentation soutenue de ses missions traditionnelles et à l'accroissement de son périmètre d'intervention par l'entrée en vigueur de nouveaux textes législatifs (contrôles en ligne, contrôle du blocage administratif des sites), la CNIL a bénéficié, en 2015, d'une allocation complémentaire de 7 postes par le législateur. Ainsi, elle est passée de **185 postes à 192,** soit une progression de 3,8%.

Les nouveaux emplois ont permis de consolider les équipes dédiées aux activités principales de la CNIL (examen de formalités préalables obligatoires, instructions de plaintes, sanctions, contrôles) afin de répondre à une activité en forte croissance tout en améliorant la qualité du service rendu aux usagers. Ces moyens ont également permis de répondre aux nouvelles compétences confiées par le législateur (contrôles en ligne).

Dans la perspective d'évolution croissante de l'activité de la CNIL, les moyens en personnel vont continuer à progresser, **à raison d'une moyenne de 6 créations de postes en 2016 et 5 postes en 2017.**

S'agissant des compétences de ses agents, la CNIL a élaboré fin 2015 un plan stratégique qui guidera son action pour les trois ans à venir. L'adoption du projet de règlement européen sur la protection des données personnelles au cours du 1er semestre 2016 et le projet de loi pour une République numérique nécessiteront en effet d'accompagner l'évolution des compétences en interne, notamment dans la perspective d'une coopération accrue de la CNIL avec ses homologues européennes. L'enjeu est donc de poursuivre la formation des agents et la diversification de leur profil, tout en assurant une mobilité interne régulière.

PROFIL DES 192 AGENTS DE LA CNIL

- **Âge moyen : 40 ans**
- **36 % des postes occupés par des juristes, 20 % par des assistants, 14 % par des ingénieurs / auditeurs**
- **48 % des agents travaillant à la CNIL sont arrivés entre 2011 et 2015**
- **71 % des agents occupent un poste de catégorie A**
- **64 % de femmes / 36 % d'hommes**

L'ancienneté moyenne à la CNIL est de 9 ans environ

LES RESSOURCES FINANCIÈRES

En 2015, les crédits octroyés à la CNIL s'élèvent à 22 061 370 € en autorisation d'engagement et 18 298 779 € en crédits de paiement, répartis comme suit : 13 090 783 € pour le budget de personnel (titre 2) et 8 970 587 € en autorisation d'engagement et 5 207 996 € en crédits de paiement pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6 : soit le budget hors titre 2).

Ainsi, les crédits alloués au budget du personnel ont progressé de 6,13 % en raison des 7 créations de postes et le budget hors titre 2 (HT2) a augmenté de 1,2 % en crédits de paiement en raison de la refonte de son schéma directeur des systèmes d'information (SDSI) minoré par l'effort budgétaire demandé aux institutions publiques.

Toutefois, la CNIL a poursuivi l'effort de maîtrise rigoureuse des dépenses de fonctionnement, entrepris depuis 2012. Ainsi, le budget réellement consommé de la CNIL s'est élevé à 4,461 millions d'euros. Si ce solde s'explique en partie par la finalisation de projets informatiques structurants au terme de l'année budgétaire, il témoigne aussi des efforts très importants de réduction des dépenses. Pour la deuxième année consécutive, le budget consommé est ainsi inférieur à 4,9 millions d'euros, alors qu'il était encore de 5,6 millions d'euros en 2012, soit une baisse de plus de 10 % (20 % hors loyers).

En 2015, le schéma directeur des systèmes d'information (SDSI) de la CNIL a permis de :

- **Redéfinir** la réponse de premier niveau à nos publics en s'appuyant sur de nouveaux contenus en ligne et outils de questions / réponses ;
- **Améliorer** l'accompagnement des usagers dans leurs démarches de plaintes en ligne et permettre une saisine de la CNIL en ligne, quel qu'en soit le fondement, conformément aux obligations légales ;

▸▸▸

▸▸▸ ▸ **Disposer** d'outils métiers pleinement adaptés aux missions de la Commission ;

▸ **Poursuivre** la refonte du site internet cnil.fr, opérationnel en février 2016

▸ **Mettre en œuvre** le projet Open data.

La CNIL a poursuivi la mutualisation d'achats avec les services du Premier ministre et le service des achats de l'Etat (SAE) afin de pouvoir dégager des économies pour des dépenses de fonctionnement courant et de ré-allouer ces sommes à des projets métiers. ■

CRÉDITS 2015	AUTORISATIONS D'ENGAGEMENT	CRÉDITS DE PAIEMENT
Budget LFI	**22 907 204 €**	**18 817 431 €**
Titre 2	13 156 566 €	13 156 566 €
Hors Titre 2	9 750 638 €	5 660 865 €
Budget disponible	**22 061 370 €**	**18 298 779 €**
Titre 2	13 090 783 €	13 090 783 €
Hors Titre 2	8 970 587 €	5 207 996 €
Budget Consommé	**21 407 908 €**	**17 178 189 €**
Titre 2	12 716 435 €	12 716 435 €
Hors Titre 2	8 691 473 €	4 461 754 €

Organigramme des directions et services

Isabelle FALQUE-PIERROTIN
Présidente

EDOUARD GEFFRAY
Secrétaire général

Service des affaires européennes et internationales	Direction de la Conformité (DC)	Direction de la protection des droits et des sanctions (DPDS)	Direction des technologies et de l'innovation (DTI)	Direction des relations avec les publics et de la recherche (DRPR)	Direction administrative et financière (DAF)
Conseil juridique et Relations institutionnelles	Service du secteur régalien et des collectivités territoriales	Service des plaintes	Service de l'expertise technologique	Service de l'information et de la documentation	Service des ressources humaines
Service de la communication externe et interne	Service de la santé	Service des contrôles	Service de l'informatique interne	Service des relations avec les publics	Service des finances et marchés publics
Qualité performance et risques	Service du secteur économique	Service des sanctions	Pôle innovation, études et prospective	Pôle des publications scientifiques et partenariats avec le monde de la recherche	Service des moyens généraux
	Service des questions sociales & RH	Service droit d'accès indirect		Pôle éducation au numérique	
	Service des correspondants Informatique et Libertés				
	Pôle en charge de la gestion des formalités préalables				
	Pôle BCR				
	Pôle labels				

5

ANNEXES

Liste des sanctions prononcées en 2015

Liste des mises en demeure prononcées en 2015

Liste des sanctions prononcées en 2015

DATE	NOM OU TYPE D'ORGANISME	THÈME	MANQUEMENTS PRINCIPAUX	DÉCISION ADOPTÉE
12/02/2015	PERSONNE PHYSIQUE	Prospection politique	collecte et traitement illicite de données	Avertissement non public
12/02/2015	PERSONNE PHYSIQUE	Prospection politique	collecte et traitement illicite de données	Avertissement non public
12/02/2015	THÉÂTRE NATIONAL DE BRETAGNE*	Prospection politique	données incompatibles avec la finalité pour lesquelles elles ont été collectées	Avertissement public
09/04/2015	COMMUNE	Gestion des inscriptions scolaires	données inadéquates, non pertinentes et excessives, défaut d'information	Avertissement non public
18/05/2015	SOCIÉTÉ D'ANALYSE DES COMMANDES DES CONSOMMATEURS SUR SITE E-COMMERCE	Lutte contre la fraude à la carte bancaire	non respect des formalités préalables	Sanction pécuniaire non publique
01/06/2015	PRISMA MEDIA	Prospection	non respect des dispositions de l'article L.34-5 du Code des postes et des communications électroniques, défaut d'information, non respect d'une durée de conservation	Sanction pécuniaire publique de 15 000 euros
18/06/2015	SOCIÉTÉ VENTE D'ABONNEMENTS EN LIGNE	Faille de sécurité impactant les données des clients et des prospects	défaut de sécurité des données	Avertissement non public
05/11/2015	OPTICAL CENTER	Gestion des données des clients et des prospects	défaut de sécurité et de confidentialité des données, y compris celles gérées par un sous-traitant	Sanction pécuniaire publique de 50 000 euros
10/12/2015	BANQUE	Gestion des mots de passe des clients pour la consultation des comptes en ligne	défaut de sécurité et de confidentialité des données	Avertissement non public
21/12/2015	PROFILS SÉNIORS	Constitution d'une base de données/collecte déloyale	défaut de formalités préalables non respect des dispositions relatives aux transferts de données hors de l'Union européenne collecte déloyale défaut du consentement des personnes au traitement de leurs données par des tiers défaut de sécurité des données défaut de sécurité et de confidentialité des données gérées par un sous-traitant	Avertissement public

*** Recours pendant devant le Conseil d'Etat**

Liste des mises en demeure prononcées en 2015

ORGANISMES	THÉMATIQUES	MANQUEMENTS PRINCIPAUX	
LES MISES EN DEMEURE PUBLIQUES			
			Date de clôture
SASP PARIS SAINT GERMAIN FOOTBALL	Fichier d'exclusion	Non respect des autorisations délivrées	11/09/2015
MOTEUR DE RECHERCHE GOOGLE	Déréférencement	Non respect du droit d'opposition	Non clôturée
BOULANGER	Commentaires excessifs, cookies	Non adéquation, non pertinence et caractère excessif des données ; défaut d'information des personnes ; durée de conservation disproportionnée ou non définie ; défaut de sécurité et de confidentialité des données	06/11/2015
MINISTÈRE DE LA JUSTICE ET MINISTÈRE DE L'INTÉRIEUR	Demande d'accès à des fichiers de police et de justice	Non respect des délais prévus par la procédure de droit d'accès indirect des personnes	09/09/2015
8 SITES DE RENCONTRES : TOODATE, SAMADHI, NESS INETRACTIVE, GEB ADOPTAGUY, PHOENIX CORP, MEETIC, LT SERVICES, 2 L MULTIMEDIA	Réseaux sociaux de rencontres	Absence de formalités préalables/transferts hors UE ; défaut de consentement exprès de la personne ; défaut d'information des personnes ; non adéquation, non pertinence et caractère excessif des données ; durée de conservation disproportionnée ou non définie ; défaut d'information et d'accord préalable au dépôt de cookies ou à leur lecture ; non définition d'une finalité déterminée, explicite et légitime ; défaut de sécurité et de confidentialité des données ainsi que de celles gérées par un sous-traitant ; non respect du droit d'accès ; traitement déloyal	Non clôturées
LES MISES EN DEMEURE NON PUBLIQUES			
COMMUNES	Demandes d'état civil en ligne	Défaut d'information des personnes ; défaut de sécurité et de confidentialité des données	
COMMUNE	Dépôt de cookies	Défaut d'information et d'accord préalable des personnes	
PERSONNE PHYSIQUE DU MONDE POLITIQUE	Prospection politique	Absence de formalités préalables ; défaut de coopération avec les services de la CNIL	
PERSONNE PHYSIQUE RESPONSABLE D'UN BLOG	Droit d'opposition sur des informations figurant sur un blog	Non respect du droit d'opposition	

▸▸▸

▸▸▸ Liste des mises en demeure prononcées en 2015

ORGANISMES	THÉMATIQUES	MANQUEMENTS PRINCIPAUX
LES MISES EN DEMEURE NON PUBLIQUES		
SOCIÉTÉS PROPOSANT UN VASTE CHOIX DE SERVICES MARCHANDS EN LIGNE EN RELATION AVEC LA PHOTO NUMÉRIQUE	Service de photos en ligne	Défaut d'information des personnes ; défaut de sécurité et de confidentialité des données ; durée de conservation disproportionnée ou non définie
SOCIÉTÉS RÉALISANT DES ESSAIS CLINIQUES	Études cliniques	Défaut de mise à jour des formalités préalables ; défaut d'information et du recueil du consentement de la personne ; défaut de sécurité et de confidentialité des données ; non définition d'une durée de conservation des données ; défaut de sécurité et confidentialité des données gérées par un sous-traitant ; non adéquation, non pertinence et caractère excessif des données
SITES DE SUIVI DE GROSSESSE	Suivi de grossesse	Défaut d'information des personnes ; défaut de sécurité et de confidentialité des données ; durée de conservation disproportionnée ou non définie
MINISTÈRES	Fichier de l'Etat	Données collectées inexactes ; non respect de la durée de conservation des données ; défaut de sécurité des données
ÉTABLISSEMENT PUBLIC	Données inexactes dans un fichier d'un bénéficiaire géré par un organisme	Données inexactes, incomplètes et non mises à jour
SITES D'ACTUALITÉ	Cookies presse	Défaut d'information et d'accord préalable des personnes ; défaut de sécurité et de confidentialité des données ; non définition d'une finalité déterminée, explicite et légitime du traitement ; durée de conservation disproportionnée ou non définie; non respect des dispositions de l'article L34-5 du code des postes et des communications électroniques
SITES D'INFORMATIONS THÉMATIQUES DIVERSES	Cookies	Défaut d'information et d'accord préalable ; non définition d'une finalité déterminée, explicite et légitime ; durée de conservation disproportionnée ou non définie ; défaut de sécurité et de confidentialité des données
ASSOCIATIONS	Prospection, vidéosurveillance, commentaire de décisions de justice	Collecte déloyale de données ; défaut d'information des personnes ; durée de conservation disproportionnée ou non définie ; défaut d'adéquation, de pertinence et caractère excessif des données, défaut de sécurité des données ; non respect du droit d'opposition

Liste des mises en demeure prononcées en 2015

ORGANISMES	THÉMATIQUES	MANQUEMENTS PRINCIPAUX
LES MISES EN DEMEURE NON PUBLIQUES		
COMMERCES ET GRANDE DISTRIBUTION	Fichier d'exclusion, scannettes, vidéosurveillance, vidéoprotection, géolocalisation, surveillance permanente des salariés, enregistrement des conversations téléphoniques	Absence de formalités préalables/non respect de l'autorisation délivrée par la CNIL/ défaut d'autorisation préfectorale/non respect des finalités prévues par le code de sécurité intérieure ; défaut d'adéquation, de pertinence et caractère excessif des données ; durée de conservation disproportionnée ou non définie ; défaut d'information des personnes ; défaut de sécurité et de confidentialité des données ; collecte illicite ; défaut de mise en oeuvre d'un registre ; non respect des dispositions de l'article L34-5 du code des postes et communications
COMMERCES EN LIGNE	Fichier d'exclusion, prospection commerciale, cookies, données bancaires	Absence de formalités préalables/défaut de mise à jour des traitements déclarés/transfert hors UE ; défaut de coopération avec la CNIL ; non adéquation, non pertinence et caractère excessif des données ; défaut de recueil du consentement ; défaut d'information et d'accord préalable au dépôt des cookies ; durée de conservation disproportionnée ou non définie ; absence de définition d'une finalité déterminée, explicite et légitime ; défaut de sécurité et de confidentialité des données ; non respect des dispositions de l'article L34-5 du code des postes et des communications
ASSURANCES	Gestion des sinistres, données d'infractions, données de santé	Absence de formalités préalables ; collecte illicite de données ; non adéquation, non pertinence et caractère excessif des données ; défaut de recueil du consentement ; défaut d'information des personnes ; absence de définition d'une durée de conservation des données
SOCIÉTÉS DE RECOUVREMENT	Recouvrement de créance sécurité	Défaut d'information des personnes ; défaut de sécurité des données
SYNDICAT	NIR	Traitement illicite des données
PLATEFORME TÉLÉPHONIQUE D'APPELS	Suivi d'activité	Absence de définition d'une durée de conservation des données ; défaut d'information des personnes ; défaut de sécurité et de confidentialité des données
SOCIÉTÉ DE SÉCURITÉ	Droit d'accès d'un salarié	Absence de formalités préalables ; non respect du droit d'accès ; défaut de réponse à la CNIL
SOCIÉTÉS DE SERVICE	Site internet, cookies vidéosurveillance, et vidéoprotection, gestion des données clients et prospects	Absence de formalités préalables ; défaut d'accord préalable au dépôt des cookies ; non adéquation, non pertinence et caractère excessif des données ; défaut d'information des personnes ; défaut de sécurité et de confidentialité des données ; non respect du droit d'accès ; non respect des dispositions de l'arrêté préfectoral d'autorisation ; défaut de réponse aux demandes de la CNIL ; durée de conservation disproportionnée ou non définie ; non respect du droit d'opposition

Commission nationale de l'informatique et des libertés
8, rue Vivienne - 75083 Paris Cedex 02 / www.cnil.fr / Tél. 01 53 73 22 22 / Fax 01 53 73 22 00

Conception & réalisation graphique LINÉAL 03 20 41 40 76 / www.lineal.fr
Impression et diffusion Direction de l'information légale et administrative
Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr
Crédit photo CNIL, Fotolia, istockphoto

Commission nationale de l'informatique et des libertés
8, rue Vivienne
75083 Paris Cedex 02
Tél. 01 53 73 22 22
Fax 01 53 73 22 00

www.cnil.fr

Diffusion
Direction de l'information légale et administrative

La Documentation française
Tél. 01 40 15 70 10
www.ladocumentationfrançaise.fr

ISBN : 978-2-11-010351-2
DF : 5HC42290
Prix : 15 €

CNIL
Commission Nationale de l'Informatique et des Libertés