5.
CONTRÔLER ET SANCTIONNER

La notification des violations de données à caractère personnel, une nouvelle mission

Les contrôles

Les sanctions

LA NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL, UNE NOUVELLE MISSION

À l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées. Cette obligation a été transposée en droit français à l'article 34 bis de la loi « Informatique et Libertés » par l'ordonnance du 24 août 2011.
Le législateur a donc confié à la CNIL d'une nouvelle mission : elle doit apprécier le niveau de sécurité des systèmes des fournisseurs de services de communications électroniques, mais surtout les accompagner dans la mise en œuvre de mesures de protection efficaces contre toute violation de données. Elle peut enfin, en fonction de la gravité de cette violation, imposer aux fournisseurs l'information des personnes concernées.

15
NOTIFICATIONS REÇUES

LE PRINCIPE : UNE OBLIGATION DE NOTIFICATION

Actuellement, l'obligation de notification des violations s'impose uniquement aux fournisseurs de services de communications électroniques devant être déclarés auprès de l'ARCEP (fournisseurs d'accès à internet, de téléphonie fixe ou mobile), et lorsque la violation intervient dans le cadre de leur activité de fourniture de services de communications électroniques. À titre d'illustration, l'intrusion dans la base clients d'un FAI devra être considérée comme une violation de données soumise à notification, mais pas le piratage du fichier des ressources humaines de ce même FAI.

Dès qu'il constate une violation de données, **le responsable de traitement doit sans délai en informer la CNIL**. Il doit également informer les personnes dont les données ont fait l'objet de la violation, sauf s'il a mis en œuvre en amont des mesures techniques qui rendent les données incompréhensibles à toute personne

INFOS +

Qu'est-ce qu'une violation de données à caractère personnel ?

Toute destruction, perte, altération, divulgation ou accès non autorisé à des données à caractère personnel est une violation de données à caractère personnel.
Une violation peut résulter d'un acte malveillant (par exemple, en cas de piratage informatique) ou se produire à la suite d'une erreur matérielle (par exemple, lorsqu'un salarié détruit ou divulgue le fichier clients de sa société du fait d'une fausse manipulation).

non autorisée à y avoir accès. La CNIL peut cependant, si elle estime que la gravité de la violation le justifie, mettre en demeure le fournisseur d'informer les intéressés.

Le défaut de notification à la CNIL et aux personnes concernées est sanctionné à l'article 226-17-1 du Code pénal (cinq ans d'emprisonnement et 300 000 euros d'amende).

FOCUS

ATTENTION Le projet de règlement européen relatif à la protection des données prévoit, à ce stade, la généralisation de cette obligation de notification à l'ensemble des responsables de traitement. Actuellement, les responsables de traitement qui n'entrent pas dans le champ de l'article 34 bis de la loi « Informatique et Libertés » restent tout de même soumis à une obligation générale de sécurité et de confidentialité des données.

L'ACTION DE LA CNIL

En 2012, la CNIL a reçu une quinzaine de notifications de violation de données personnelles. Ce faible nombre de notifications s'explique par le fait que les modalités de mise en œuvre de cette nouvelle obligation n'ont été que récemment fixées. En effet, au niveau national, un décret d'application a été publié en mars 2012. Le règlement européen visant à harmoniser les procédures de notification des violations aux autorités de protection des données personnelles a quant à lui été adopté en janvier 2013.

Ce règlement prend largement en compte l'avis rendu par le G29 et auquel la CNIL a contribué. Il définit notamment le contenu et les délais de notification aux autorités de protection des données et impose à ces dernières de mettre à disposition des déclarants un moyen électronique sécurisé de notification.

Dans les mois et les années à venir, cette nouvelle mission aura des conséquences sensibles sur l'activité de la CNIL qui devra non seulement traiter les notifications des fournisseurs de services de communications électroniques, mais également accompagner ces derniers dans l'appréciation et la mise en œuvre de mesures de protection efficaces. À cet égard, la CNIL participe aux travaux menés par le G29 pour aider les responsables de traitement à évaluer le niveau de gravité des violations subies.

De manière plus générale, ces nouvelles obligations s'inscrivent dans un processus de responsabilisation accrue des acteurs en charge des données personnelles. Il ne s'agit plus d'attendre que les victimes déposent plainte ou que la CNIL contrôle et sanctionne. Le responsable du traitement doit assumer pleinement la responsabilité des erreurs commises en amont, afin d'éviter toute conséquence pour les personnes concernées. Cette obligation permettra donc à la CNIL d'avoir une meilleure vision du niveau de sécurité mis en œuvre, mais également d'offrir un meilleur accompagnement. ■

> Ces nouvelles obligations s'inscrivent dans un processus de responsabilisation accrue des acteurs

LES CONTRÔLES

L'année 2012 a confirmé la tendance amorcée depuis plusieurs années, qui consiste à faire des contrôles sur place un moyen d'action privilégié de la Commission. Ainsi, le nombre de contrôles réalisés a encore notablement augmenté, qu'ils portent sur les fichiers soumis à la loi « Informatique et Libertés » ou sur les dispositifs de vidéoprotection relevant de la loi du 21 janvier 1995.

458
CONTRÔLES EN 2012

DONT 285
PORTANT SUR DES DISPOSITIFS RELEVANT DE LA LOI « INFORMATIQUE ET LIBERTÉS »

ET 173
PORTANT SUR DES DISPOSITIFS DE VIDÉOPROTECTION/ VIDÉOSURVEILLANCE

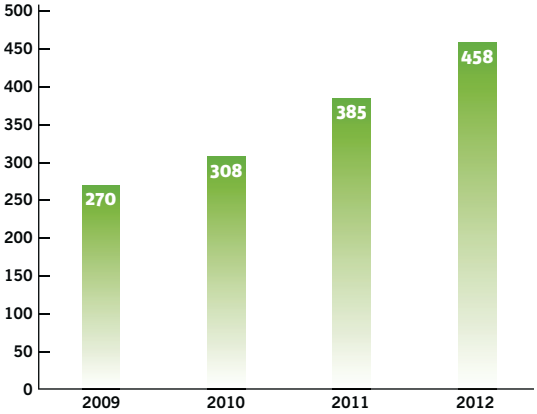
UNE AUGMENTATION DE 19 %
PAR RAPPORT À 2011

La CNIL a effectué **458 contrôles au cours de l'année 2012, ce qui représente une augmentation de 19 % par rapport à l'année précédente**. Cette augmentation illustre une nouvelle fois la volonté de la Commission de vérifier, par ses contrôles sur place, le respect des textes dont elle est chargée d'assurer l'application.

L'activité de contrôle de la CNIL se répartit comme suit : 285 contrôles portant sur des dispositifs relevant de la loi « Informatique et Libertés » et 173 contrôles portant sur des dispositifs de vidéoprotection/vidéosurveillance.

Dans le premier cas, 23 % des contrôles ont été effectués dans le cadre de l'instruction de plaintes, 11 % dans le cadre de la procédure de sanction (par exemple, afin de vérifier le respect des engagements pris par un responsable de traitement mis en demeure par la Présidente de la CNIL) et 26 % au regard de l'actualité.

Évolution du nombre de contrôles depuis 2009



40 % des contrôles réalisés se sont inscrits dans les thématiques issues du programme annuel décidé par la Commission.

Ces contrôles ont donné lieu à l'adoption d'une vingtaine de mises en demeure par la Présidente de la CNIL et 4 avertissements par la formation restreinte. Pour autant, on doit constater que les courriers adressés à la suite de ces contrôles ont conduit, dans la quasi-totalité des cas, à ce que les organismes adoptent une démarche de mise en conformité vis-à-vis de la loi du 6 janvier 1978 modifiée, y compris parfois en désignant des correspondants à la protection des données.

Ce programme annuel était structuré autour des thèmes suivants :

- **« La sécurité des données de santé »** : une vingtaine de contrôles ont été réalisés dans ce cadre ; ils ont porté sur les conditions de traitement des données par des organismes aussi divers que les hébergeurs agréés, les centres d'étude et de conservation des œufs et du sperme humains (CECOS), les pharmacies (dossier pharmaceutique), un groupe hospitalier d'importance nationale, des laboratoires d'analyse médicale et des prestataires développant des logiciels ou produits destinés à traiter des données de santé.
- **« Les failles de sécurité »** : de nombreux contrôles ont porté sur les conditions de sécurité de traitement des données à caractère personnel. Ces contrôles ont pu être réalisés dans le cadre d'alertes adressées à la CNIL ou dans le cadre de notification de violations de données à caractère personnel (article 34 bis de la loi voir pages 52-53).
- **« Sport et vie privée »** : une vingtaine de contrôles ont également été menés auprès

d'acteurs de toute taille du secteur sportif, qui traitent pour certains d'entre eux des dizaines de milliers de données concernant leurs adhérents. Des contrôles ont ainsi été réalisés auprès de fédérations sportives ou auprès de clubs de sport. L'objet de ces contrôles visait essentiellement à apprécier la proportionnalité des données collectées, l'information des personnes et les mesures de sécurité mises en place.

▸ **« Les données à caractère personnel et la vie quotidienne »** : des contrôles de grande ampleur ont été effectués auprès des principaux fournisseurs de gaz, d'électricité ou de services de communications électroniques. Ces contrôles ont notamment porté sur l'analyse des zones dites « commentaires » afin de s'assurer que les données collectées sur les clients de ces opérateurs étaient conformes à la loi. Enfin, une série de contrôles a été opérée auprès de sociétés d'autoroute afin, notamment, d'apprécier la conformité de certains de leurs dispositifs innovants (lecture de plaque d'immatriculation, péage sans contact, etc.).

▸ **« La délivrance des visas »** : la Commission a également procédé à des contrôles afin de vérifier les conditions de recueil et de traitement des données biométriques des demandeurs de visas. Ces contrôles ont été effectués auprès des services centraux situés en France mais également auprès de consulats français situés à l'étranger et auprès de certains des prestataires privés auxquels il est fait appel dans ce cadre.

> Dans la quasi-totalité des cas, les organismes se mettent en conformité après un contrôle

LE CONTRÔLE DES DISPOSITIFS DE VIDÉOPROTECTION/ VIDÉOSURVEILLANCE

Les dispositifs dits « de vidéoprotection », qui filment la voie publique et les lieux ouverts au public sont soumis aux dispositions du code de la sécurité intérieure. Les dispositifs dits de « vidéosurveillance » qui concernent des lieux non ouverts au public (locaux professionnels non ouverts au public comme les bureaux ou les réserves des magasins) sont soumis aux dispositions de la loi « Informatique et Libertés ».

Dans les faits, on constate qu'il est rare de trouver un dispositif relevant d'une seule législation : les dispositifs comprennent généralement une partie des caméras filmant des zones ouvertes au public (les espaces de vente par exemple) et une partie filmant des zones non ouvertes au public.

C'est dans le cadre de sa mission de contrôle de l'ensemble de ces dispositifs que la CNIL a effectué 173 contrôles au cours de l'année 2012. Ce chiffre représente une augmentation de 14,5 % par rapport à l'année précédente et témoigne de la volonté de la CNIL de se saisir pleinement des pouvoirs qui lui ont été confiés par le législateur en 2011. On doit également relever que les contrôles ont porté sur des structures du secteur public et privé, de toute taille. Ces contrôles ont permis à la CNIL d'alimenter sa réflexion sur les conditions de mise en œuvre des systèmes de vidéoprotection/ vidéosurveillance.

De manière générale, ces contrôles ont conduit la CNIL à adopter 12 mises en demeure, une sanction pécuniaire et un avertissement. ■

FOCUS

Le contrôle STIC

En 2009, la CNIL a formulé 11 propositions d'amélioration du fichier STIC. En 2012, plus d'une vingtaine de contrôles ont été effectués afin de vérifier si des améliorations ont été apportées au fonctionnement de ce fichier. Les investigations ont été menées auprès de l'ensemble des acteurs chargés de garantir le bon fonctionnement et la bonne utilisation du fichier : services de police, tribunaux et préfectures notamment. Le bilan de ces constats fera l'objet d'une communication globale au premier semestre 2013.

- **23 contrôles sur place dans 9 départements ;**
- **61 contrôles sur pièces (concernant 27 préfectures et 34 tribunaux de grande instance) ;**
- **200 interlocuteurs entendus ;**
- **300 pièces papiers et numériques copiées.**

LES SANCTIONS

En 2012, la Présidente de la CNIL a adopté 43 mises en demeure dont 2 ont été rendues publiques. 13 sanctions ont été prononcées par la formation restreinte dont 4 sanctions pécuniaires, 9 avertissements et 1 injonction de cesser le traitement (certaines de ces sanctions pouvant se cumuler).

43
MISES EN DEMEURE

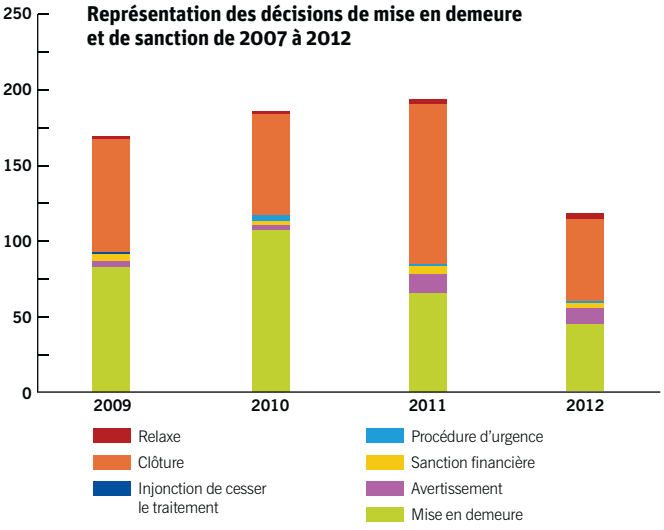
13
SANCTIONS DONT 8 SANCTIONS PUBLIQUES

9
AVERTISSEMENTS

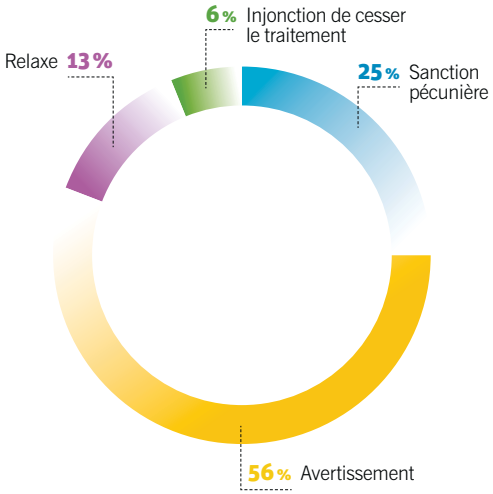
Le bilan de l'année 2012 est marqué par l'augmentation du nombre de sanctions rendues publiques par la formation restreinte. En effet, 8 des 13 décisions ont été rendues publiques, soit environ 60 % des sanctions, alors qu'en 2011, seules 21 % des sanctions ont été publiées.

L'année 2012 s'est également singularisée par l'adoption des premières mises en demeure publiques. Depuis la réforme introduite par la loi du 29 mars 2011 relative au Défenseur des droits, la Présidente de la CNIL peut demander au bureau de la CNIL (composé de la Présidente et des deux vice-présidents) de rendre publiques les mises en demeure qu'elle adopte (article 46 de la loi du 6 janvier modifiée). Les critères retenus pour justifier une telle publicité sont notamment la nature et la gravité des manquements et le nombre de personnes concernées. Pour respecter les droits des organismes faisant l'objet d'une telle décision, la clôture des mises en demeure est également rendue publique. En pratique, les mises en demeure puis les courriers de clôture sont diffusés sur le site internet de la CNIL.

Représentation des décisions de mise en demeure et de sanction de 2007 à 2012



Les sanctions prononcées en 2012

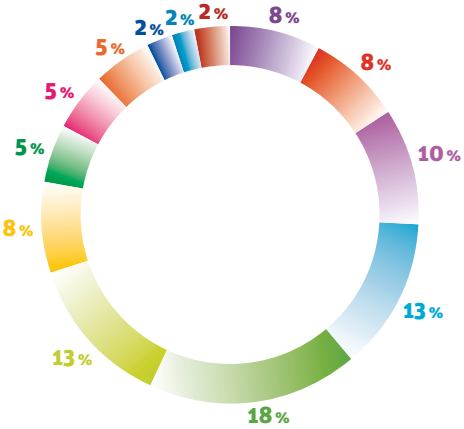


FOCUS

L'arrêt ACADOMIA du Conseil d'État du 27 juillet 2012

Dans un arrêt rendu le 27 juillet 2012, le Conseil d'État a confirmé l'avertissement public prononcé par la CNIL à l'encontre de la société AIS2 (enseigne ACADOMIA) le 28 mai 2010. Cette décision, apporte un éclairage intéressant sur différents aspects de la procédure mise en œuvre par la CNIL.
Dans cette décision, le Conseil d'État a estimé que la nouvelle procédure de contrôle mise en œuvre par la CNIL était conforme à la Convention européenne des droits de l'Homme (CEDH). En effet, la CNIL informe désormais expressément les organismes contrôlés de leur faculté de s'opposer à une mission de contrôle par la remise, en début de contrôle, d'un document spécifique leur rappelant leurs droits. Plus encore, le Conseil d'État a confirmé que la formation restreinte n'était pas tenue de développer une argumentation spécifique pour justifier de la publicité de ses décisions. Cette publicité, qui est une sanction complémentaire, peut être motivée par référence à la motivation d'ensemble de la sanction principale qu'elle complète. Enfin, la Haute juridiction a validé le fait de prononcer un avertissement à l'encontre d'un organisme et, concomitamment, de lui notifier une mise en demeure dès lors que celle-ci porte sur des faits postérieurs à l'avertissement et sont distincts de ceux-ci.

Les manquements proposés dans les rapports de sanction en 2012



Liste des sanctions prononcées en 2012

Date	Nom ou type d'organisme	Décision adoptée	Manquements proposés	Thème
26/01/2012	Union régionale des syndicats CGT des établissements de l'enseignement supérieur	Sanction pécuniaire publique (5 000 euros)	Collecte déloyale, non respect du droit d'opposition, défaut de réponse à la CNIL	Prospection syndicale
16/02/2012	Commune	Avertissement non public	Défaut de formalités préalables, défaut de sécurité et confidentialité	Collectivité
08/03/2012	SYMEV	Avertissement public	Défaut de formalités préalables, collecte déloyale, défaut d'information, durée de conservation excessive	Fichier d'exclusion
08/03/2012	Organisme de ventes aux enchères publiques judiciaires	Avertissement non public	Défaut de formalités préalables, défaut d'information, défaut de sécurité	Fichier d'exclusion
08/03/2012	Organisme de ventes aux enchères publiques judiciaires	Avertissement non public	Défaut de formalités préalables, défaut d'information, défaut de sécurité, défaut de mise à jour des données et non définition d'une durée de conservation	Fichier d'exclusion
15/03/2012	Groupe scolaire	Sanction pécuniaire non publique (1 000 euros)	Caractère excessif des données, défaut d'information	Vidéosurveillance
29/03/2012	EURO INFORMATION	Avertissement public	Défaut de sécurité et de confidentialité des données	Travail
12/04/2012	Société de transport	Avertissement non public	Défaut de caractère pertinent et non excessif des données au regard de la finalité, défaut d'information	Vidéosurveillance
03/05/2012	YATEDO France	Avertissement public	Défaut de mise à jour des données, non respect du droit d'opposition, défaut de coopération avec la CNIL	Réseau social - internet
24/05/2012	Établissement Équipements Nord Picardie	Sanction pécuniaire publique (10 000 euros)	Non respect du droit d'accès, défaut de réponse à la CNIL	Travail
24/05/2012	Commune de Montreuil	Avertissement public	Traitement illicite, défaut de sécurité	Liste électorale
21/06/2012	FNAC DIRECT	Avertissement public	Défaut du recueil du consentement des personnes, non respect d'une durée de conservation, défaut de sécurité et de confidentialité des données	Données bancaires
13/09/2012	Établissement public	Relaxe	Défaut de formalités préalables, défaut de collecte loyale, défaut d'information, défaut de sécurité	Cybersurveillance
18/10/2012	Société	Relaxe	Non respect du droit d'accès	Travail/accès au dossier personnel
08/11/2012	Syndicat des copropriétaires "ARCADES CHAMPS ÉLYSÉES"	Sanction pécuniaire publique assortie d'une injonction de cesser le traitement	Non respect de proportionnalité du dispositif	Vidéosurveillance

6. CONTRIBUER À LA RÉGULATION INTERNATIONALE

Instances de régulation internationale et codes de bonne conduite

Rassembler les autorités de protection des données autour des valeurs de la francophonie

Quel cadre européen des données personnelles ?

GROS PLAN

Audit des règles de confidentialité Google : une première dans la coopération des autorités européennes

INSTANCES DE RÉGULATION INTERNATIONALE ET CODES DE BONNE CONDUITE

LE G29, GROUPE DES 27 « CNIL » EUROPÉENNES

INFOS +

Le groupe des autorités nationales de contrôle des États membres de l'UE, nommé en référence à l'article 29 de la directive de 1995 qui l'a institué.
Le G29 en 2012, c'est :
40 documents adoptés,
8 groupes de travail,
40 réunions, 5 plénières regroupant les 27 autorités de protection.

Au cours de l'année 2012, les activités du G29 ont été aussi diverses que nombreuses.

Le sous-groupe « Technologies » a vu ses travaux s'intensifier. Ont ainsi été adoptés des avis sur le *cloud computing*, la reconnaissance faciale, la biométrie, les exceptions au recueil du consentement pour les cookies. Le sous groupe s'est également attaché à analyser le projet de règlement envisagé par la Commission Européenne sur la notification des violations de données à caractère personnel. L'analyse des nouvelles règles de confidentialité de Google ainsi que le rapport d'audit de Facebook ont également fait l'objet de nombreuses discussions et d'une importante collaboration entre les membres du G29.

Le sous-groupe « e-government » s'est quant à lui penché sur le traitement des données personnelles qui peut être fait par les CERTS (Computer Emergency Response Teams), organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents, sur la proposition de directive concernant la réutilisation des informations du secteur public et sur la proposition de règlement sur l'identification électronique et les services de confiance pour les transactions électroniques.

Le G29 s'est également attaché à poursuivre ses travaux sur l'encadrement des **transferts internationaux**. Dans ce cadre, un modèle de règles d'entreprises contraignantes pour les sous-traitants élaboré par le sous groupe « Transferts » a été adopté, ainsi qu'un avis sur la demande d'adéquation de Monaco. Par ailleurs, des discussions ont été menées avec le groupe de travail « Vie privée » de l'APEC sur la possibilité de relier le système BCR et le système dénommé *Cross-Border Privacy Rules* (« CBPR ») existant dans la zone Asie – Pacifique.

Le sous-groupe « Questions financières » a poursuivi ses analyses sur le Foreign Account Tax Compliance Act **(FACTA)** qui vise à lutter contre la fraude fiscale, et sur la directive anti blanchiment.

Le sous-groupe « Frontières, voyage et activités répressives » a formulé des remarques à la Commission européenne concernant le programme Smart Borders et le projet de règlement Eurosur (système européen de surveillance des frontières). Il a également analysé le nouveau projet de dispositif d'inspection-filtrage des passagers aériens initié par **IATA** (association internationale des transporteurs aériens) ainsi que les informations sur les données passagers (API). Il a aussi suivi les questions relatives aux échanges de données **PNR** avec les pays tiers.

Le sous-groupe en charge d'analyser des problématiques transversales, a quant à lui étudié les dispositions de la directive 95/46 concernant la réutilisation des données pour un traitement ultérieur.

Enfin, **le sous-groupe « Futur de la vie privée »**, après avoir adopté un premier avis général sur le projet de réforme européen, a poursuivi ses travaux sur des sujets plus spécifiques, notamment l'expression du consentement, la définition de données personnelles, le recours aux actes délégués et d'exécution.

LE CONSEIL DE L'EUROPE ET L'OCDE

Le processus de modernisation de la Convention n° 108 du Conseil de l'Europe

Le Conseil de l'Europe a été une organisation internationale phare de la protection des données personnelles avec l'adoption du **premier instrument juridique européen contraignant en matière de protection des données en 1981** : la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite « Convention 108 »), complétée par un Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données.

Sur une initiative du Comité des ministres du Conseil de l'Europe de mars 2010, les travaux de révision de la Convention 108 ont débuté en 2011 avec pour objectif l'adaptation de ses dispositions aux réalités actuelles.

Les principales propositions d'évolution du texte sont notamment : l'insertion d'une référence au droit de chaque individu de « contrôler ses propres données » ; l'insertion d'un principe de minimisation des données ; l'inversion de la logique du droit d'opposition (le responsable de traitement devant justifier de l'existence de motifs légitimes prépondérants pour refuser de faire droit à la demande) ; la notification des failles de sécurité aux autorités de contrôle ; l'ajout des principes d'*accountability* et « de protection de la vie privée dès la conception » et la préservation de l'acquis communautaire en matière de transferts internationaux.

Le projet de modernisation de la convention 108 a été adopté par la plénière du comité consultatif dit « Comité T-PD » le 30 novembre 2012.

Il doit ensuite, après une étape de discussion au sein d'un comité intergouvernemental ad hoc (dont la première réunion est prévue pour le mois de juin 2013), être soumis au Comité des ministres du Conseil de l'Europe.

La révision des lignes directrices de l'OCDE

L'Organisation de coopération et de développement économiques (OCDE), fondée en 1960 et vouée au développement mondial, compte aujourd'hui 34 pays membres à travers le monde. Le 23 septembre 1980, l'OCDE a adopté des « *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel* », sous la forme d'une recommandation.

En 2010, à l'occasion du 30e anniversaire des lignes directrices, l'OCDE a engagé des travaux en vue de leur révision. Les principales modifications envisagées concernent notamment : l'insertion du principe *d'accountability* pour les responsables de traitements et l'obligation de notification des failles de sécurité (aux autorités compétentes et aux individus concernés).

INFOS +

L'OCDE compte 34 pays membres à travers le monde, de l'Amérique du Nord et du Sud à l'Europe, en passant par la région Asie-Pacifique et LE CONSEIL DE L'EUROPE, 47 pays membres dont la quasi-totalité des États du continent européen.

Les lignes directrices modifiées devraient être adoptées par le Conseil de l'OCDE à la fin du premier semestre 2013.

Certaines modifications impliquant de véritables changements de fond par rapport à l'approche initiale, la CNIL demeure **vigilante sur le maintien d'un niveau élevé de protection ainsi que de l'acquis communautaire, notamment en matière de règles applicables aux transferts internationaux de données personnelles**. La CNIL soutient également l'insertion d'un principe de limitation de la durée maximale de conservation des données au nombre des « principes fondamentaux » des lignes directrices.

LES RÈGLES INTERNES D'ENTREPRISE (« BCR »)

Les Binding Corporate Rules (BCR) constituent un code de conduite interne définissant la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne. Ces règles doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous les salariés de ces entités. Les BCR permettent alors d'assurer un niveau de protection suffisant aux données transférées hors de l'Union européenne au sein d'un même groupe.

Fin 2012, 40 groupes ont déjà adopté des BCR, dont **35 % ont choisi la CNIL comme autorité chef de file** pour mener ▸▸▸

40

GROUPES ONT DÉJÀ ADOPTÉ DES BCR

DONT 35 % ONT CHOISI LA CNIL COMME AUTORITÉ CHEF DE FILE

FOCUS

Le lancement des BCR sous-traitants

À compter du 1er janvier 2013, il sera également possible d'adopter des BCR « sous-traitants », destinés à encadrer les transferts intra-groupes de données traitées par un sous-traitant selon les instructions et pour le compte de ses clients responsables de traitement. Particulièrement adaptés aux évolutions technologiques telles que le Cloud computing, ces BCR créent une sphère de sécurité pour les transferts effectués par des sous-traitants, apportant alors des garanties suffisantes aux transferts pour les responsables de traitement.

les BCR, laboratoire pour la rédaction de l'*accountability* dans le projet de règlement

la procédure de coopération entre les autorités européennes de protection des données. Un guide sur les transferts, disponible sur le site de la CNIL, fournit davantage d'informations sur la procédure de coopération européenne pour les BCR.

Les BCR rencontrent de plus en plus de succès car ils constituent un outil d'encadrement des transferts, mais également parce qu'ils permettent de mettre en œuvre des mesures proactives et concrètes dites d'*accountability* (formations, audits, délégués à la protection des données, etc.). La Commission européenne a d'ailleurs récemment déclaré que les BCR avaient été « *un laboratoire pour la rédaction de l'accountability dans le projet de règlement* »[1], ce qui est confirmé par de nombreuses multinationales ayant adopté des BCR car elles les envisagent plus comme un **programme mondial de conformité** que comme un simple outil d'encadrement des transferts.

VERS UNE ARTICULATION DE L'ENCADREMENT DES FLUX ENTRE L'EUROPE (BCR) ET LA ZONE ASIE PACIFIQUE (CBPR) ?

La Coopération économique pour l'Asie-Pacifique (APEC) a récemment développé un système de règles transfrontalières de protection de la vie privée, les « Cross-Border Privacy Rules » (CBPR), afin d'apporter des garanties aux transferts de données et d'obtenir leur certification par des tiers certificateurs externes eux-mêmes agréés par l'APEC.

Partant du constat que les systèmes BCR et CBPR sont basés sur des approches similaires (codes de conduite sur les transferts internationaux développés par des entreprises et revus *a priori* par des autorités de protection des données ou par des tiers agréés), le G29 a étudié les CBPR afin d'identifier leurs similarités et leurs différences avec les BCR. Sur la base de cette comparaison, le G29 a lancé une réflexion pour développer des outils pratiques qui permettraient aux organisations d'adopter des politiques internes respectueuses des deux systèmes, et ce en vue d'obtenir **une « double certification BCR-CBPR »** dans le respect des procédures d'approbation propres à chaque zone.

En janvier 2013, des représentants d'autorités européennes de protection des données dont la CNIL, le Contrôleur européen, l'autorité allemande se sont réunis pour la première fois avec le Comité BCR/CBPR de l'APEC afin d'échanger leurs vues sur ce projet. ■

[1] *Déclaration de Marie-Hélène BOULANGER, chef de l'unité Protection des données de la Commission européenne dans le cadre du panel "A Great Ascent: How to Summit from BCR Basecamp to Accountability and Global Interoperability", organisé le 14/11 lors de la Conférence IAPP du 13-14 novembre 2012, Bruxelles*

RASSEMBLER LES AUTORITÉS DE PROTECTION DES DONNÉES AUTOUR DES VALEURS DE LA FRANCOPHONIE

Les autorités de protection des données personnelles membres de l'Association francophone des autorités de protection des données personnelles (AFAPDP) affichent une volonté de travailler ensemble. Ces autorités partagent non seulement une langue, des valeurs et traditions juridiques communes, mais également une vision de la protection des données personnelles : une vision humaniste, qui place l'individu au centre des préoccupations mais qui veut aussi offrir des solutions pragmatiques. Cette approche de la Francophonie a été réaffirmée dans la Déclaration de Monaco en 2012.

C'est également un argument retenu par les pays africains en construction ou consolidation démocratique. Au Maroc, par exemple, les responsables politiques ont compris les enjeux économiques mais également politiques de la protection des données personnelles. La protection des données personnelles est un marqueur de démocratie : l'adoption d'une législation, l'installation d'une autorité indépendante chargée de garantir l'application de la loi, est un message fort envoyé à la population marocaine en attente du renforcement des droits individuels, et aux partenaires internationaux en attente de garanties démocratiques et économiques.

La CNIL a renforcé son soutien à l'AFAPDP avec la signature d'une convention d'objectifs pluriannuelle pour 2011-2013. La CNIL affirme de cette façon son intérêt à renforcer ce réseau francophone autour de ses valeurs et de sa vision pour enrichir le débat international sur

▸▸▸

FOCUS

La Déclaration de Monaco, adoptée par l'Assemblée générale le 23 novembre 2012 à Monaco, réaffirme les principes défendus par l'association, dans le contexte de la concurrence internationale entre les conceptions de la protection des données personnelles. L'AFAPDP s'engage notamment à promouvoir l'adoption de standards internationaux de protection des données personnelles et à renforcer la coopération avec les institutions et autres réseaux concernés par la protection des données.

INFOS +

Créée en 2007, l'Association francophone des autorités de protection des données personnelles (AFAPDP) rassemble les autorités de protection des données personnelles (16 membres adhérents) et les pays de l'espace francophone qui n'ont pas encore adopté de loi dans ce domaine (membres associés de l'AFAPDP).
L'AFAPDP est un réseau de promotion du droit à la protection des données personnelles et d'échange de bonnes pratiques. Ses actions concourent à l'adoption de lois de protection des données personnelles et à la mise en place d'autorités de contrôle indépendantes.
La CNIL assure le secrétariat général de l'AFAPDP depuis 2007. Le Bureau de l'association est composé par ailleurs des représentants des autorités du Québec (présidence), du Burkina Faso et de Suisse (vice-présidences).

La voix singulière de la Francophonie est de nature à pondérer un débat mondial largement monopolisé par une approche anglo-saxonne

la protection des données personnelles. Dans le contexte d'une concurrence internationale forte entre les conceptions de la protection des données personnelles, la voix singulière de la Francophonie est de nature à pondérer un débat mondial largement monopolisé par une approche anglo-saxonne.

En outre, l'AFAPDP s'est rapprochée du Réseau ibéro américain des autorités de protection des données personnelles (www.redipd.org), puisque les deux réseaux partagent la même démarche (rassemblement autour d'une langue) et les mêmes valeurs humanistes. L'ambition des réseaux est de constituer une communauté internationale capable de proposer une vision originale et diversifiée de la protection des données personnelles.

Renforcement des compétences des autorités et de leurs outils

Depuis 2012, la CNIL participe aux travaux des groupes de travail sur l'encadrement des transferts de données dans l'espace francophone (BCR francophones) ainsi que sur la consolidation des fichiers d'état civil et des listes électorales, en partenariat avec le Réseau des compétences électorales francophones (RECEF). La CNIL accueille également tout au long de l'année les délégations des jeunes autorités francophones.

Soutien aux États qui souhaitent adopter une loi de protection des données personnelles

La présidente de la CNIL s'est rendue à Tunis en juin 2012 pour soutenir le projet de réforme de l'autorité nationale de protection des données personnelles devant les hauts responsables tunisiens. Ce type de mission de sensibilisation est réalisé en partenariat avec les réseaux institutionnels : institutions locales, Organisation internationale de la Francophonie, réseaux diplomatiques nationaux, réseaux institutionnels francophones.

Promotion de la diversité culturelle

Au sein de l'AFAPDP, la CNIL encourage l'interprétation en français lors des Conférences internationales des commissaires à la protection des données personnelles et à la vie privée. ■

QUEL CADRE EUROPÉEN DES DONNÉES PERSONNELLES ?

Suite aux consultations menées en 2011, la Commission européenne a proposé le 25 janvier 2012 une réforme de la directive de 1995 sur la protection des données personnelles, en deux volets : une proposition de règlement définissant un cadre général et une proposition de directive relative aux données traitées à des fins de police et de justice.

La réforme vise à doter l'Union de règles uniformes adaptées aux défis d'un environnement technologique en rapide évolution et d'une économie mondialisée. La directive de 1995 sur la protection des données à caractère personnel (95/46/CE) sera abrogée et remplacée par le nouveau règlement, d'application directe et qui devra être mis en œuvre dans les deux ans suivant sa publication. La nouvelle directive remplacera notamment la décision-cadre 2008/977 du Conseil du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

DES AVANCÉES SALUÉES PAR LA CNIL

Tout en réaffirmant les principes généraux relatifs aux traitements des données à caractère personnel, la proposition contient des avancées notables en ce qui concerne **les droits du citoyen**, notamment :

- le consentement des personnes au traitement de leurs données personnelles doit être explicite ;
- un « droit à l'oubli numérique » est créé – la CNIL souhaite d'ailleurs qu'il se prolonge d'un droit au déréférencement auprès des moteurs de recherche ;
- le droit à la portabilité des données est reconnu ;
- les obligations générales d'information et de transparence sont renforcées ;
- le sous-traitant se voit attribuer un statut légal à part entière.

Les formalités administratives (déclarations, consultations préalables) sont allégées au profit d'une plus grande **responsabilisation des organismes**. Ces derniers sont tenus de mettre en œuvre des mécanismes et des procédures internes afin de veiller au respect des règles contenues dans le règlement : analyse d'impact des traitements à risque, désignation d'un délégué à la protection des données pour les entreprises comptant plus de 250 employés, documentation, règles d'entreprise contraignantes, codes de bonne conduite et certification, etc.

Les autorités de contrôle voient leurs compétences et pouvoirs harmonisés (avec notamment des sanctions financières renforcées) et leur indépendance réaffirmée. Par ailleurs, une coopération renforcée entre autorités des différents États membres est mise en place, avec un rôle accru pour le G29 (rebaptisé Comité européen pour la protection des données).

> La CNIL préconise de retenir également le critère du ciblage, c'est-à-dire le lieu de résidence du citoyen concerné

DES MOTIFS DE PRÉOCCUPATION

Parmi les motifs de préoccupation identifiés par la CNIL, on retiendra principalement les suivants :

Lorsque l'entreprise a des établissements dans plusieurs États membres, l'autorité du pays de l'établissement principal de l'entreprise aurait, selon le projet initial, une compétence exclusive. La CNIL y voit une source d'insécurité juridique compte tenu de la difficulté d'identifier l'établissement principal. Elle craint également une incitation au « forum-shopping » et un facteur d'éloignement de la protection du citoyen. De plus, elle met en garde contre la possibilité de recours croisés entre autorités qui seraient contraires à l'esprit de la construction européenne.

- **La CNIL préconise de retenir, à côté de l'établissement principal du responsable de traitement ou du sous-traitant, le critère du ciblage, c'est-à-dire le lieu**

▸▸▸

de résidence du citoyen concerné. Une autorité chef de file disposant de compétence non exclusive serait désignée et agirait pour le compte des autres autorités concernées selon un système de codécision.

La possibilité est ouverte aux entreprises d'encadrer les transferts de données hors UE grâce à des instruments juridiques non contraignants ou résultant d'une autoévaluation des risques par le responsable de traitement.

La CNIL considère qu'il est essentiel de maintenir un contrôle *a priori* sur les transferts, sur la base de règles clairement définies, et d'écarter la possibilité de recours à des instruments sans valeur juridique pour encadrer ces transferts.

Le pouvoir est donné à la Commission européenne d'adopter des actes délégués et d'exécution dans un nombre important de domaines.

La CNIL souhaite une meilleure ventilation des compétences entre la Commission, le nouveau Comité européen et les autorités de contrôle nationales.

> L'intention est de parvenir à une adoption du règlement à la fin de l'année 2013, pour mise en œuvre dès 2016

LES AVIS DU G29

La CNIL a participé activement aux travaux du sous-groupe « Futur de la vie privée » du G29. Soucieuse que le citoyen reste au cœur du projet, elle s'est montrée particulièrement active sur la problématique de la compétence, multipliant les contacts avec ses homologues, la présidence du G29 et le Contrôleur européen de la protection des données.

Un **premier avis**, adopté le 23 mars 2012, reprenant sensiblement la position de la CNIL, démontre un partage des préoccupations eu égard à la proposition de règlement entre les autorités de protection des données membres du G29. Cet avis aborde d'autres questions, telles que le seuil pour l'application de certaines règles aux entreprises, la proportionnalité et la modulation des sanctions en fonction des mécanismes mis en place par les entreprises, les exemptions applicables aux autorités publiques ou la désignation d'un représentant du responsable de traitement qui n'est pas établi dans l'Union européenne. Le G29 a par ailleurs souligné la nécessité d'assurer la complémentarité et la cohérence des deux instruments proposés – règlement et directive.

Après la publication de ce premier avis général, le G29 a poursuivi ses travaux sur des problématiques plus spécifiques de la proposition de règlement, qui ont abouti à un **second avis** du 5 octobre 2012. Dans cet avis, le G29 défend le caractère nécessairement explicite du consentement, l'inclusion des adresses IP dans la définition des données personnelles et un recours limité aux actes délégués pour la mise en œuvre du règlement.

LE PROCESSUS DÉCISIONNEL

La CNIL a poursuivi ses échanges avec ses interlocuteurs à la direction générale de la justice, des droits fondamentaux et de la citoyenneté de la Commission européenne, afin d'exposer ses préoccupations. Toutefois, en 2012, les discussions se sont déplacées au Parlement européen et au Conseil de l'Union européenne. L'intention déclarée par la Commission européenne, le rapporteur au Parlement européen et la présidence irlandaise de l'Union est de parvenir à une adoption du règlement à la fin de l'année 2013, pour mise en œuvre dès 2016.

La CNIL a aussi sensibilisé la commission des affaires étrangères de l'Assemblée nationale et la commission des affaires européennes du Sénat. Respectivement en février et en mars, **les deux assemblées ont exprimé dans une résolution européenne des réserves sur la proposition de règlement en ce qui concerne les règles de compétence, rejoignant en cela la position exprimée par la CNIL**. Le 8 février 2012, à l'occasion d'un débat organisé en séance publique au Sénat sur la question de la protection de la vie privée, le Ministre de la Justice, garde des Sceaux, s'était prononcé très clairement contre le critère de l'établissement principal.

Les discussions avec le gouvernement français se sont poursuivies tout au long de l'année 2012 et devraient continuer en 2013. ■

GROS PLAN

AUDIT DES RÈGLES DE CONFIDENTIALITÉ GOOGLE : UNE PREMIÈRE DANS LA COOPÉRATION DES AUTORITÉS EUROPÉENNES

“Les autorités européennes demandent à Google de s’engager publiquement sur le respect des principes de protection des données”

Le 24 janvier 2012, Google annonçait l’entrée en vigueur de nouvelles règles de confidentialité et de nouvelles conditions d’utilisation applicables à la quasi-totalité de ses services à partir du 1er mars 2012. Face aux nombreuses questions soulevées par ces changements, la CNIL a été mandatée par le groupe des CNIL européennes (G29) pour conduire une enquête sur les nouvelles règles.

Dans le cadre de cette mission, la CNIL a envoyé un premier questionnaire à Google le 16 mars 2012. Un certain nombre des réponses fournies par Google s’étant avérées incomplètes ou approximatives, un questionnaire complémentaire a été envoyé le 22 mai 2012. En particulier, Google n’avait pas fourni de réponses satisfaisantes sur des points essentiels comme la description de tous les traitements de données personnelles qu’il opère ou la liste précise des plus de 60 politiques de confidentialité qui ont été fusionnées dans les nouvelles règles.

> 60 politiques de confidentialité ont été fusionnées dans les nouvelles règles

Sur la base de l’analyse des réponses fournies par Google et suite à l’examen, par les experts de la CNIL, de nombreux documents et mécanismes techniques, les autorités européennes ont tiré leurs conclusions et formulé des recommandations sous la forme d’un courrier adressé à Google le 16 octobre 2012 et signé par 27 autorités européennes de protection des données.

Cette initiative constitue une première et une avancée considérable dans la mobilisation et la coopération des autorités européennes. ▸▸▸

LES PRINCIPALES CONCLUSIONS ET RECOMMANDATIONS

L'analyse menée ne permet pas de s'assurer que Google respecte les principes essentiels de la Directive sur la protection des données personnelles que sont la limitation de finalité, la qualité et la minimisation des données, la proportionnalité et le droit d'opposition. En effet, les nouvelles règles de confidentialité suggèrent l'absence de toute limite concernant le périmètre de la collecte et les usages potentiels des données personnelles.

Google fournit des informations incomplètes ou approximatives sur les finalités et les catégories des données collectées

Avec les règles actuelles, l'utilisateur d'un service Google est incapable de déterminer quelles sont les données personnelles utilisées pour ce service et les finalités exactes pour lesquelles ces données sont traitées. Il arrive même que les utilisateurs ne reçoivent aucune information quant aux données qui sont traitées. Tel est le cas des utilisateurs passifs, c'est-à-dire de ceux qui n'interagissent avec Google qu'au travers des plateformes publicitaires tierces ou des boutons " +1 ".

Les autorités européennes ont donc demandé à Google de fournir une information plus claire et plus complète sur les données collectées et les finalités de chacun de ces traitements de données personnelles. Par exemple, les autorités européennes ont recommandé la mise en place d'une présentation avec trois niveaux de détails qui assurera une information conforme aux exigences de la Directive sans dégrader l'expérience des utilisateurs. L'ergonomie de la lecture des règles pourrait également être améliorée grâce à des présentations interactives.

Google ne permet pas le contrôle par les utilisateurs de la combinaison de données entre ses nombreux services

La **combinaison de données entre services** a été généralisée avec les nouvelles règles de confidentialité : concrètement toute activité en ligne liée à Google (l'utilisation de ses services, de son système Android ou la consultation de sites tiers utilisant des services Google) peut être rassemblée et combinée.

Les CNIL européennes relèvent que cette combinaison poursuit des finalités différentes. Il s'agit :

- de la fourniture de services où l'utilisateur demande la combinaison des données,
- de la fourniture de services demandés par l'utilisateur et où la combinaison s'opère sans que l'utilisateur en soit directement informé,
- de la finalité de sécurité,
- du développement de produits et d'innovation marketing,
- de la mise à disposition du Compte Google,
- de la publicité,
- de l'analyse de fréquentation,
- de recherche universitaire.

La législation européenne prévoit un cadre précis pour les traitements de données personnelles et exige notamment que le responsable de traitement dispose d'une base légale et que la collecte soit proportionnée aux finalités poursuivies. Or, pour certaines de ces finalités, notamment la publicité, Google ne peut s'appuyer ni sur le consentement de la personne, ni sur son intérêt légitime, ni sur l'exécution d'un contrat.

▸ Google doit donc modifier ses pratiques et notamment : renforcer le consentement des personnes pour la combinaison des données pour certaines finalités, offrir un meilleur contrôle des utilisateurs sur la combinaison de données en centralisant et simplifiant le droit d'opposition (opt-out) et en leur permettant de choisir pour quels services leurs données sont combinées, et enfin adapter ses outils afin de limiter cette combinaison aux finalités autorisées.

Google ne précise pas les durées de conservation des données récoltées

Enfin, en dépit des questions précises et réitérées soumises par les CNIL européennes, Google n'a pas été en mesure de fournir une durée maximale ou habituelle de conservation des données personnelles traitées.

▸ Les CNIL européennes ont donc demandé à Google de respecter le principe d'une durée de conservation strictement limitée au regard des finalités.

La CNIL et les autorités européennes accueillent favorablement l'initiative de Google de réduire et de simplifier ses règles de confidentialité. Toutefois, cette évolution ne doit pas se faire au prix d'une information moins transparente et moins complète. Google dispose de quatre mois à compter du 16 octobre 2012 pour se mettre en conformité sur les différents points évoqués. ■

7. ANTICIPER ET INNOVER

GROS PLAN

Vie privée a l'horizon 2020 : quelles transformations, quels enjeux et quelle régulation ?

Accompagner l'innovation : une activité centrale pour la CNIL

GROS PLAN

VIE PRIVÉE À L'HORIZON 2020 :

QUELLES TRANSFORMATIONS, QUELS ENJEUX ET QUELLE RÉGULATION ?

« À l'heure du « tous connectés », la protection des données personnelles au centre d'enjeux technologiques, économiques, juridiques, sociaux et éthiques »

L'environnement a totalement changé depuis une dizaine d'années. L'informatique des grands fichiers publics qui prévalait en 1978 a, peu à peu, fait place à un « univers numérique », celui de la dématérialisation des activités, des professions et des usages. Des changements des pratiques sociales et des modèles économiques en ont résulté et sont toujours en cours.

Face aux défis pour la protection des données personnelles que sont le *cloud computing*, le *big data*, l'*Open data*, le développement des réseaux sociaux, l'internet mobile et la banalisation de la géolocalisation, il est nécessaire de bâtir le cadre juridique et éthique de l'univers numérique de demain. Or, la CNIL ne peut, ni ne doit intervenir de façon isolée. Il lui est indispensable d'être à l'écoute de la société civile, de dialoguer avec elle et de solliciter le plus grand nombre possible de points de vue, afin de mieux saisir l'environnement complexe et mouvant dans lequel elle intervient. Cela lui permet également de mieux anticiper les évolutions technologiques, les usages innovants, les risques émergents et les nouvelles attentes en termes de régulation des données personnelles, et d'apporter des réponses adaptées.

C'est dans ce contexte que la direction des études, de l'innovation et de la prospective de la CNIL a lancé, à l'automne 2011, un chantier prospectif. Il l'a conduit à rencontrer jusqu'au printemps 2012 une quarantaine d'experts d'horizons variés : sociologues, économistes, philosophes, juristes, historiens, chercheurs en sciences

de la communication et en sciences de l'ingénieur en informatique, représentants du monde de l'entreprise et d'associations intervenant dans les domaines du numérique et/ou de la défense des droits des personnes, etc.

Ces experts ont été interrogés sur :

- Les incidences des principales évolutions technologiques, économiques et sociétales dans le champ de la vie privée, des libertés et des données personnelles ;
- Les transformations, en cours ou à venir, dans la relation des individus et de la société à la vie privée et aux données personnelles ;
- Leur vision des formes de régulation de demain, leurs attentes à propos des autorités de protection des données ;
- Leurs projets et orientations dans le champ concerné.

Ces entretiens ont donné lieu à une synthèse qui a été publiée dans le premier numéro des *Cahiers IP - Innovation & Prospective* - sous la forme d'une étude sur les défis de la protection des données à l'horizon 2020.

La CNIL a aussi pris une deuxième initiative destinée à associer la communauté intellectuelle à ses réflexions, en organisant le 30 novembre 2012 une journée d'étude « *Vie privée 2020* » dans les locaux du Monde. Elle a ainsi souhaité apporter son concours à la constitution d'une communauté de recherche en matière de protection des données, qui réunirait des spécialistes de tous horizons.

Quatre tables rondes, symbolisant les principaux enjeux de la protection des données personnelles pour aujourd'hui et pour demain, se sont succédées, avec la participation des sociologues Dominique Cardon, Antonio Casilli, Dominique Boullier et Emmanuel Kessous, du directeur de recherche de l'INRIA Daniel Le Métayer, des avocats Olivier Iteanu et Alain Bensoussan, des économistes Fabrice Rochelandet et Alain Rallet, de la philosophe du droit Antoinette Rouvroy, de la spécialiste des sciences de gestion Caroline Lancelot-Miltgen, du juriste Jean Frayssinet, des acteurs du numérique Daniel Kaplan, Christine Balagué et Philippe Lemoine, du journaliste Jean-Marc Manach, ainsi que de la présidente d'IRIS, Meryem Marzouki.

JOURNÉE D'ÉTUDES VIE PRIVÉE 2020 : QUELQUES RÉFLEXIONS CLÉS DES EXPERTS

1/ La révolution du web social

La révolution du web social permet l'apparition d'une nouvelle forme d'expressivité, qui est ouverte à tous. Chacun peut dorénavant exprimer sa singularité au travers de manifestations de soi, de ses activités conversationnelles et de ses centres d'intérêt, et ainsi devenir une « *personne publique* ». L'individu peut s'exprimer dans un espace qui n'est pas exactement public, mais qui se situe entre le privé et le public. La tendance à la « *théâtralisation de soi* » qui s'en suit fait bouger le curseur entre vie privée et vie publique et l'individualise : chaque individu peut déplacer ce curseur pour ce qui le concerne. La vie privée devient une revendication des personnes dans un mouvement d'autonomie individuelle. Ce modèle n'en suscite pas moins des interrogations sur la réalité de la maîtrise sur sa vie privée et sur ses données personnelles.

Par ailleurs, ce qui est dit sur les réseaux sociaux est toujours lié à un contexte. Dès lors, la légitimité des regards extérieurs, par opposition à ceux des destinataires initiaux, est très incertaine. Or, on a, jusqu'à présent, surtout mis l'accent sur la personne qui s'expose sur les réseaux sociaux, en lui demandant d'être consciente des risques qu'elle prend. Ne faudrait-il pas également s'interroger sur l'attitude de celui qui regarde, hors contexte, des éléments qui ne le concernent pas ?

2/ Sommes-nous entrés dans la dictature du calcul des algorithmes ?

Le *big data* et le *cloud computing* banalisent les traitements de masse et offrent, grâce à des analyses algorithmiques toujours plus poussées, de nouvelles modalités de valorisation des données, des profilages de plus en plus individualisés et des analyses censées

▸▸▸

Les idées exprimées reflètent les avis formulés par les experts invités par la CNIL

JOURNÉE D'ÉTUDES VIE PRIVÉE 2020 : QUELQUES RÉFLEXIONS CLÉS DES EXPERTS suite

prédire les comportements. Avec le *big data*, l'extraction de connaissances nécessite l'utilisation de techniques d'intelligence artificielle, d'apprentissage informatique et de réseaux neuroniques. Ainsi apparaît une nouvelle manière de gouverner qui ne s'appuie que sur du pur calcul : il suffit de mettre en place des ensembles de données brutes et de leur appliquer des algorithmes qui fabriqueront automatiquement des modèles de comportements.

On assiste ainsi, avec les applications de *data mining* et de profilage, à une « *objectivation à distance des comportements* ». Les individus sont de plus en plus catégorisés, non pas au travers de catégories préexistantes, mais dans le cadre d'un « *nouveau régime d'intelligibilité du réel* » qui dispense de toute normativité préétablie. Dès lors, la personnalisation se passe de tout rapport à une norme commune. Ces dispositifs informatiques sont à l'origine d'une nouvelle manière d'interpréter le réel et le monde : ils font parler nos données à notre place. À la rationalité déductive succède une rationalité inductive qui, de plus, se veut prédictive.

Mais souhaitons-nous vivre dans une société dans laquelle toutes nos interactions et transactions pourraient être gouvernées par nos comportements passés ?

Ces évolutions sont également à l'origine d'autres questionnements : la personnalisation qui en résulte est paradoxale, puisque ce travail s'effectue sans jamais demander l'avis de l'individu sur ses désirs et ses intentions. Or, comment peut-on devenir des sujets si nos désirs nous précèdent, si l'on est de fait réduit à nos activités passées ? Comment, par ailleurs, garantir un espace public de délibération si l'on s'en remet à des systèmes algorithmiques pour évaluer le réel ?

3/ La donnée au cœur des modèles d'affaires

La donnée personnelle étant placée au cœur des modèles d'affaires du numérique, il n'est pas surprenant que l'on entende de plus en plus parler de monétisation des données personnelles. Mais peut-on croire à un « *marché* » des données personnelles ? Le droit à la souveraineté sur sa vie virtuelle passe-t-il par la reconnaissance d'un droit de propriété sur ses données ? La protection des données peut-elle être aussi source d'activités économiques ?

Au plan économique, la promesse du *big data* correspond à un monde totalement personnalisé dans lequel le calcul domine au détriment des autres formes de rationalités économiques. Dans ce monde, le système concurrentiel ne porte plus sur le rapport qualité-prix mais sur les mécanismes de singularisation du service. Le marché passe des « *biens* » au « *lien* », grâce aux traces d'usage. La vision collective de l'humanité ne risque-t-elle pas d'être ainsi mise à mal ?

4/ Quelles nouvelles formes de régulation pour demain ?

Depuis 1978, les frontières entre vie publique et vie privée sur lesquelles était initialement fondée la loi « Informatique et Libertés », se sont déformées. De nouvelles frontières sont apparues, entre économie de marché et logique d'émancipation des personnes. Ces changements sont essentiels, dans la mesure où de plus en plus de *business models* sont fondés sur la captation des données. À l'inverse, des mouvements visent à développer un internet citoyen.

Pour certains, une régulation purement procédurale devrait se substituer à l'actuelle régulation substantielle. Le consentement de l'individu devrait en être la clé, conduisant ainsi à faire de l'individu un personnage souverain. Mais celui-ci sera-t-il toujours en mesure de faire ses arbitrages ? Est-il souhaitable d'ailleurs de lui demander de s'installer dans une logique de marché ? Par ailleurs, le concept de *privacy* prend une place croissante dans les réflexions européennes.

Sur toutes ces questions, il est nécessaire de gagner la bataille conceptuelle et idéologique, car des modèles s'affrontent dans un contexte de concurrence internationale. Seul le plus attractif sera promu. Les Européens devront être capables de proposer des concepts nouveaux et de compléter ceux qui existent, par exemple en reconnaissant de nouveaux droits. Certains craignent que parler de régulation constitue une régression. Pourtant, au-delà des querelles de mots, il apparaît que la simple contrainte législative et réglementaire ne saurait suffire. La régulation est à comprendre comme un « *art de saltimbanque* », l'art de régir les rapports entre individus. Elle ne peut qu'être constituée par l'ensemble des outils qui sont utiles pour administrer le système. Ce qui comprend notamment la réglementation.

ACCOMPAGNER L'INNOVATION : UNE ACTIVITÉ CENTRALE POUR LA CNIL

Afin de renforcer sa mission de veille et de réflexion prospective, la CNIL a créé en mai 2012 un Comité de la Prospective faisant appel à des experts extérieurs. Ouverture, démarche pluridisciplinaire, confrontation d'idées, innovation dans son mode de gouvernance… tels sont les mots clés de cette initiative.

LA CRÉATION D'UN COMITÉ DE LA PROSPECTIVE : DE NOUVEAUX HORIZONS POUR LA CNIL

La Commission estime indispensable de développer sa compréhension des évolutions du numérique et d'innover dans son mode de gouvernance.

Ce comité se veut en premier lieu un comité d'orientation scientifique des études conduites par la CNIL. Il a donc un rôle de conseil notamment dans le cadre de l'élaboration du programme annuel d'études et dans l'exploration de nouveaux champs d'études (par exemple dans le domaine des neurosciences). Les premières réunions du comité ont d'ailleurs été l'occasion de définir plus précisément les sujets d'études pour les deux années à venir (cf. ci-après).

Véritable « Boîte à idées », le comité peut également jouer un rôle moteur dans le développement d'un espace d'échanges et de réflexion sur les problématiques « Informatique et Libertés ». Il peut par exemple initier ou animer des tables rondes avec d'autres experts et favoriser ainsi le débat public sur les enjeux « Informatique et Libertés ». Le comité a ainsi contribué à la préparation de la journée d'études « vie privée 2020 » organisée le 30 novembre 2012.

Enfin, il s'agit aussi de renforcer l'expertise de la CNIL, notamment dans les domaines économiques et sociologiques, pour mieux identifier, comprendre et anticiper les transformations technologiques présentes et à venir et en évaluer les enjeux éthiques.

INFOS +

Placé sous la présidence de la Présidente de la CNIL, le comité se compose de :

- **M. Pierre-Jean Benghozi, directeur de recherche au CNRS, professeur à l'École Polytechnique (directeur du pôle de Recherche en Économie et Gestion). Il est en charge de la Chaire d'enseignement et de recherche « Innovation et Régulation des services numériques »**
- **Mme Stefana Broadbent, psychologue, professeur d'Anthropologie à l'*University College* de Londres (UCL) où elle enseigne l'anthropologie numérique. Elle dirige le Master en Anthropologie du numérique dans le département d'Anthropologie de UCL et elle participe aux recherches du Center for Digital Anthropology de UCL**
- **M. Dominique Cardon, sociologue au Laboratoire des usages SENSE d'Orange Labs, chercheur associé au Centre d'étude des mouvements sociaux de l'École des Hautes Études en Sciences sociales (CEMS/EHESS)**
- **M. Olivier Oullier, professeur à Aix-Marseille Université, chercheur au laboratoire de psychologie cognitive (UMR CNRS 7290) et au Center for Complex Systems and Brain Sciences, conseiller scientifique au Département Questions sociales du Centre d'analyse stratégique et Young Global Leader du Forum Économique Mondial**
- **Mme Antoinette Rouvroy, chercheur qualifié du FRS-FNRS en philosophie du droit, associée au Centre de Recherche en Information, Droit et Société (CRIDS), chargée de cours à l'Université de Namur et maître de conférences à l'Université Libre de Bruxelles**
- **M. Henri Verdier, directeur d'Etalab, dirigeant d'entreprise, membre du conseil scientifique de l'institut Mines-Télécom**
- **M. Didier Gasse, conseiller maître honoraire à la Cour des comptes, membre de la CNIL en charge du secteur télécommunications et internet – sécurité - vote électronique**
- **M. Gaëtan Gorce, sénateur de la Nièvre, membre de la CNIL en charge du secteur libertés publiques et e-administration**

LE PROGRAMME D'ÉTUDES 2012-2013

Construit avec l'aide du **Comité de la Prospective** et approuvé par la Commission en juillet 2012, ce programme définit les principaux axes du programme d'études de la CNIL dans les domaines de l'innovation et de la prospective pour 2012 et 2013. Ces axes de travail sont les suivants.

Un travail autour des usages des photos et de la perception de la reconnaissance faciale

300 millions de photos sont publiées chaque jour sur Facebook. Chaque géant du web a acquis une entreprise développant une technologie de reconnaissance faciale. Les utilisateurs de smartphones et de réseaux sociaux sont confrontés quotidiennement à la question de cette place des images et photos dans leur « patrimoine numérique personnel ». Il apparaît nécessaire d'avoir une vision plus complète des comportements et usages réels des utilisateurs : appliquent-ils des règles particulières aux choix des photos publiées, à leur accessibilité, au tag de personnes,… et ce pour les différents types de photos : les photos de profil, les photos personnelles, les photos taguées ou non… comment conçoivent-ils le respect de l'intimité de leurs proches et amis, de quelle façon assurent-ils les droits des tiers ?

Pour répondre à ces questions un sondage a été réalisé fin 2012. Par ailleurs la CNIL élabore une feuille de route technologique comportant une analyse des technologies existantes et en émergence, complétée de démonstrations et d'expérimentations au sein du laboratoire de la CNIL.

Une étude prospective de la biométrie dans la vie quotidienne à l'horizon 2020

Les technologies biométriques sont de plus en plus nombreuses, et elles peuvent s'employer dans des contextes de plus en plus variés. Cependant, la biométrie reste une technologie qui semble encore peu utilisée dans la vie quotidienne, en dehors des usages de souverainetés – police… Les produits grand public qui ont été développés (verrouillage d'ordinateurs portables…) ont pour le moment eu un succès limité pour diverses raisons. Quel est l'état réel du marché des différents types de biométries en France et à l'étranger ? Quelle place pour la biométrie dans la vie quotidienne (Internet des objets,

enjeux de cybersécurité et d'identification, paiement mobile…) ? En lançant cette étude, il s'agit pour la CNIL de tenter d'anticiper sur d'éventuels champs d'applications nouveaux de la biométrie, de dresser un panorama comparatif des usages et technologies biométriques dans d'autres pays (Europe, Asie, Amérique du nord) et de contribuer aux travaux de réflexion engagés par la CNIL quant à l'évaluation de ses positions sur le sujet.

Deux chantiers exploratoires sont également engagés par la DEIP :

Le premier **autour de la question de la santé et du bien-être dans le monde numérique**, que bouleverse l'apparition de nombreux services nouveaux se trouvant souvent à la frontière entre le monde médical et la question du bien-être au quotidien : applications mobiles de santé sur smartphones, parfois avec des capteurs dédiés, services de réseaux sociaux centrés sur des communautés de patients, suivi et aide des malades de maladies chroniques, apparition de communautés pratiquant l'auto-mesure (*Quantified Self*). Il est, du point de vue prospectif, intéressant d'analyser le faisceau convergent de ces nouveaux usages et besoins de services de santé et d'en évaluer les enjeux éthiques et en particulier de protection des données personnelles.

Le second chantier ouvert se concentre sur **l'influence des usages numériques dans les relations de travail**, l'atténuation de la frontière entre la vie privée et la vie professionnelle, notamment avec l'essor du « *Bring your own device* », c'est-à-dire l'utilisation, de plus en plus massive, des smartphones et tablettes personnels au travail. Il s'agit de dresser un état des lieux des usages numériques au travail et de leurs conséquences en matière de relations entre employés, dans le management et dans les relations hiérarchiques. Il s'agira en particulier d'analyser l'évolution des **techniques de suivi d'activité** (monitoring de performance, reporting…) voire de **surveillance au travail**.

Ces thèmes feront l'objet de travaux internes d'analyse et de veille, ils alimenteront la feuille de route du laboratoire d'innovation et serviront de base à des partenariats ou des études externes.

PARTENARIATS ET COOPÉRATION

Poursuivant sa démarche de coopération avec le monde académique, la CNIL a signé, à l'occasion de la journée d'études vie privée 2020, le 30 novembre 2012 une convention de partenariat avec l'institut mines-telecom. Celle-ci permettra notamment de sensibiliser encore plus la communauté scientifique à la protection des données et de la vie privée et de mener des travaux de recherche en commun. Première application pratique, la direction des études, de l'innovation et de la prospective était présente aux 7e entretiens de Télécom ParisTech, les 5 et 6 décembre 2012 sur le thème *big Data*, *big value*, et est intervenue lors d'une table ronde consacrée à la protection des données personnelles.

Enfin, la Commission participe activement à plusieurs groupes de travail, en France et à l'international, afin de développer des bonnes pratiques de sécurité protectrices de la vie privée.

Elle est ainsi présente notamment :

• à l'ISO (organisation de normalisation internationale), dans laquelle un de ses agents joue le rôle d'éditeur de la principale norme en sécurité, l'ISO/IEC 27001, relative au système de management de la sécurité de l'information, où la CNIL agit en tant que liaison avec le G29 pour coordonner les positions de ses homologues européens sur les projets de normes relatifs à la protection de la vie privée, et où elle participe au développement de nouvelles normes relatives au *cloud computing*, à la gestion des risques sur la vie privée, etc. ;

• au Club EBIOS (communauté d'experts en gestion des risques), que l'un de ses agents préside ;

• au CESIN (communauté de responsables de la sécurité des systèmes d'information).

Innover dans le débat « Informatique et Libertés » : le PrivacyCamp

Pour la première fois, la CNIL a organisé, en association avec des acteurs du numérique, un événement participatif et ouvert sous la forme – innovante pour la CNIL – d'un Barcamp, c'est-à-dire d'une non-conférence ouverte à tous ceux qui le souhaitent.

Le 30 mars 2012, à l'invitation de la CNIL, et en association avec Mozilla, Owni et Silicon Sentier, la communauté du numérique a ainsi pris possession de La Cantine, lieu d'échanges et espace de *coworking*, pour une demi-journée de

▸▸▸

FOCUS

Le prix de thèse « Informatique et Libertés »

Le Prix de thèse « Informatique et Libertés » incite au développement des recherches universitaires concernant la protection de la vie privée et des données personnelles.
Pour la 4e année consécutive, la CNIL a attribué le prix « Informatique et Libertés ». Le jury du Prix, présidé par M. Jean-Marie COTTERET, membre de la CNIL, a décidé de récompenser Mme Jessica EYNARD, docteur en droit privé (Université de Toulouse Capitole 1) et qualifiée aux fonctions de Maître de conférences par le Conseil National des Universités, pour son essai remarqué sur la donnée à caractère personnel. Son travail, particulièrement d'actualité, notamment dans le cadre de la révision de la législation européenne en la matière, fera l'objet d'une publication dans les mois à venir.

Le jury présidé par M. Jean-Marie COTTERET se compose de :
- **M. Daniel Le Metayer**, Directeur de recherches INRIA
- **Mme Nathalie Mallet-Poujol**, Directrice de recherches CNRS
- **M. Jean-Emmanuel Ray**, Professeur à l'Université Paris I – Panthéon – Sorbonne
- **M. Fabrice Rochelandet**, Maître de conférences à l'Université Paris Sud
- **M. Michel Riguidel**, Professeur émérite à Télécom ParisTech
- **Mme Sophie Vulliet-Tavernier**, Directrice des études, de l'innovation et de la prospective de la CNIL
- **M. Dominique Wolton**, Directeur de l'Institut des Sciences de la Communication du CNRS

rencontres et d'échanges autour de la question « comment contrôler ses données personnelles sur le web ? ».

Innovation dans la forme comme dans le fond pour la CNIL, cet événement a été un succès : une centaine de personnes se sont inscrites pour venir échanger autour des outils, des pratiques et des services permettant de maîtriser sa vie privée en ligne et de comprendre les flux et « fuites » de données personnelles en ligne.

Détecter les signaux faibles de l'innovation technologique

La Direction des études et de la prospective a aussi développé ses participations et interventions dans des événements autour de ses sujets de travail. Ainsi, elle était présente à la conférence LeWeb, conférence internationale qui se déroule à Paris tous les ans. Le thème central cette année était l'internet des objets. La tendance du *Quantified Self* était également à l'honneur.

Elle a également participé et est intervenue à la conférence annuelle de l'IDATE, le DiGiworld Summit qui avait pour thème cette année « *Game changers : mobile, cloud, big data* ».

Remise du prix de thèse 2012 à Madame Jessica EYNARD

LE LABORATOIRE D'INNOVATION

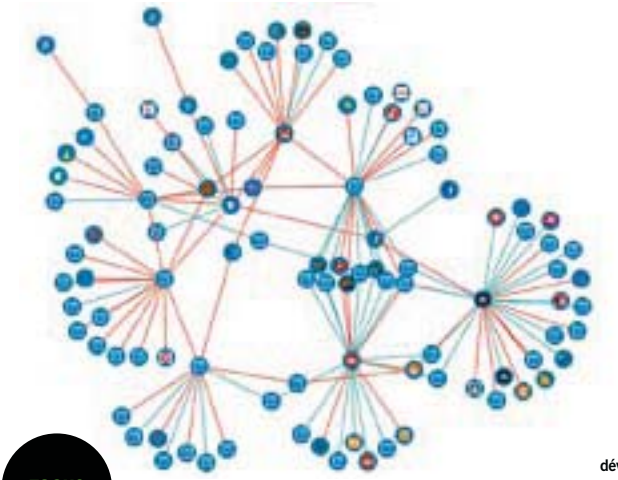
Ce laboratoire, créé en 2011, répond à la volonté de la CNIL de disposer en son sein de moyens informatiques dédiés permettant de tester et d'expérimenter, en réel, des produits et applications innovants. Il permet de disposer de nouveaux produits ou services afin d'en tester les fonctionnalités et d'en évaluer les impacts sur la protection de la vie privée.

Le laboratoire est donc pleinement opérationnel au plan technique depuis le début de l'année 2012 : une infrastructure associant des machines (serveurs, ordinateurs…) et un réseau informatique propre a été constitué et offre une plateforme technique sur laquelle de nombreux projets viennent s'appuyer. Tout au long de l'année, des tests sont donc réalisés grâce à ce matériel spécialement configuré : analyse des fuites de données sur des applications mobiles, étude sur les réseaux sociaux, tests de matériel biométrique…

De manière plus ambitieuse, le laboratoire porte des projets d'analyse et d'expérimentation qui sont en quelque sorte et toutes proportions gardées, à la CNIL ce que des projets de « Recherche & Développement » sont pour une entreprise. Ces projets prennent progressivement plus d'ampleur, et un premier projet lancé début 2012 montre l'ensemble des facettes de cette activité de laboratoire d'innovation.

Un autre projet a été lancé au second semestre 2012 et s'articule autour des « cookies » et de la traçabilité en ligne. Tout comme l'écosystème des smartphones, ce monde des cookies est marqué par une grande opacité : sauf à s'intéresser vraiment à la question, il est très difficile pour l'internaute de savoir quand et comment il est « tracé » par des programmes et outils aux finalités variées (analyses statistiques des visites, aide à l'achat en ligne, mais aussi et peut-être surtout ciblage publicitaire). La CNIL a donc décidé d'explorer ce monde au sein du laboratoire sous deux angles complémentaires : vu depuis la navigation de l'internaute, et vu depuis l'analyse macroscopique du web. Sous le premier angle, la CNIL dispose aujourd'hui d'un outil très pédagogique pour comprendre ce qu'est réellement un cookie et comment les cookies sont utilisés pour tracer les internautes. Cet outil, baptisé *CookieViz*, représente sur un graphe interactif et dynamique en temps réel au cours d'une navigation l'apparition de liens vers des sites tiers par des cookies ou autres codes. Il est pour le moment utilisé par les services lors de présentations publiques sur le thème des cookies et permet de faire mieux comprendre les recommandations du G29 et de la CNIL en la matière. Le laboratoire travaillera en 2013 sur une version web de cet outil pouvant éventuellement être mise à la disposition du public. Sous le second angle, un projet baptisé *CookieMiner* est en cours de développement depuis l'automne 2012 et vise à cartographier de la manière la plus exhaustive possible la présence de cookies et autres traqueurs dans le web français en « .fr ».

Progressivement, le laboratoire va donc élargir ses travaux pour aller vers plus d'expérimentations, d'essais et des développements d'outils. Le laboratoire pourra alors étendre son action pour porter les actions innovantes et expérimentales de la CNIL et cela en tout domaine : l'innovation doit pour la CNIL être technologique, mais aussi sociétale et juridique ! Le laboratoire sera un support essentiel dans la création d'une plateforme d'innovation ouverte au service de l'institution. ■



Outil « CookieMiner » développé par le laboratoire.

FOCUS

Mobilitics

Le laboratoire porte un projet de développement très concret lancé conjointement par la CNIL et l'INRIA dans le cadre de la convention de partenariat qui lie l'autorité à cet institut public de recherche, leader européen et mondial dans les recherches en informatique et sciences du numérique. Intitulé « *Mobilitics* », ce projet commun de recherche est tourné vers les smartphones et l'analyse de ce qui se passe à l'intérieur de ces « boîtes noires ». *Mobilitics* est ainsi une suite directe des travaux « smartphones et vie privée » pilotés en 2011 par la Direction des études, de l'Innovation et de la Prospective (voir rapport annuel 2011, pp : 23 à 27). Après un an de développement et d'échanges réguliers, une équipe de chercheurs INRIA[1] et la CNIL disposent à présent d'un outil qui permet de pousser très loin l'analyse du fonctionnement et des usages des smartphones et de la manière dont est géré l'accès aux données personnelles dans un téléphone (en particulier ce qui se passe lorsqu'une application cherche à accéder à un certain nombre de données personnelles : carnet d'adresses, localisation géographique, identifiant unique du téléphone, photographies…). À la fin de l'année 2012, le laboratoire a, pour la première fois, lancé une expérimentation *in vivo* avec l'aide de volontaires parmi les agents de la CNIL. Cette première expérimentation - qui consistait en l'utilisation, en condition réelle, de téléphones du laboratoire spécialement configurés - a permis de recueillir beaucoup de données qui sont en cours d'analyse et de valorisation. Certaines de ces analyses seront diffusées prochainement auprès des spécialistes par l'intermédiaire de publications dans des revues scientifiques ou techniques spécialisées. Cependant, l'ambition du laboratoire est plus large que de simplement valoriser des travaux auprès du monde de la recherche : il s'agit aussi d'explorer de nouvelles manières de diffuser une culture technologique et une pédagogie des usages en développant notamment des outils à destination du grand public. Le projet Mobilitics s'attachera en 2013 à se tourner ainsi vers l'extérieur, par exemple par la publication des enseignements tirés de l'analyse des données issues de l'expérimentation, mais aussi en explorant le prototypage de solutions techniques (par exemple permettant de tester la faisabilité de nouvelles solutions protectrices de la vie privée sur smartphones).

Ce projet Mobilitics est un bon prototype des futurs projets du laboratoire : ancrés dans un besoin d'approfondissement d'une thématique émergente et identifiée comme prioritaire par l'institution, ils devront se déployer à la fois vers le monde de la recherche, vers l'expérimentation réelle mais aussi vers la promotion d'outils concrets de maîtrise des données.

[1] *Équipe INRIA « Planete » http://planete.inria.fr/*

8.
LES SUJETS DE RÉFLEXION EN 2013

Big Data, tous calculés ?

Vers un droit à l'oubli numérique ?

La biométrie : une doctrine pragmatique et évolutive

BIG DATA, TOUS CALCULÉS ?

Jusqu'à récemment, les traitements massifs de données semblaient réservés à des acteurs disposant d'infrastructures informatiques importantes. La quantité exponentielle de données désormais disponibles et le cloud « démocratisent » aujourd'hui l'accès à ces traitements de masse et offrent des possibilités nouvelles de valorisation des données.

FOCUS

Les 3 V du Big Data

Le Volume : La masse de données informatiques et numériques produites en 2008 sur Internet représentait 480 milliards de gigagoctets. En 2010, ce furent 800 milliards soit l'équivalent de ce que l'humanité avait écrit, imprimé, gravé, ou enregistré jusqu'en 2003. 90 % des données ont ainsi été créées ces deux dernières années et on s'attend à une croissance annuelle de 40 % dans le monde entre 2011 et 2020[1].

La Variété : le volume et la variété sont intrinsèquement liés à l'évolution des usages : les utilisateurs partagent des données issues de tout une diversité de contenus (photos[2], vidéos, billets de blog, micro-conversations, objets et capteurs connectés);

La Vélocité : le traitement de grande masse de données est aujourd'hui simplifié. De nouvelles générations de technologies et d'algorithmes offrant toujours plus de puissance et d'analyse de calcul permettent de traiter de nouveaux types de données, en particulier non-structurées, et ont favorisé l'émergence d'une industrie qui pesait près de 700 milliards d'euros en 2012[3].

Le concept de Big Data est certainement l'un des thèmes les plus en vogue lorsque l'on s'intéresse aux évolutions technologiques pouvant avoir le plus d'impact dans les 10 prochaines années, aussi bien sur un plan économique que sociétal. Le Big Data est souvent caractérisé par la formule dite des « trois V » : volume et variété dans un premier temps, car on amasse des sommes de données de plus en plus considérables par des moyens variés ; vélocité dans un second temps, car la masse des données recueillies doit être traitée en temps réel.

Ainsi, l'avènement du Big Data va-t-il permettre l'émergence d'une nouvelle forme de science, sans hypothèse ? Une nouvelle manière de prendre des décisions qui ne s'appuierait que sur du pur calcul, autour de modèles de comportements ? Quels enjeux nouveaux pose-t-il en termes « Informatique et Libertés » ?

NOUVELLES DONNÉES, NOUVEAUX CHAMPS, LE BIG DATA S'INVITE PARTOUT...

Les opportunités offertes par le Big Data sont aujourd'hui majoritairement valorisées dans le domaine du marketing et de la publicité pour des usages d'analyse des données sur le comportement des consommateurs dans le but de mieux anticiper leurs attentes. La publicité en ligne constitue sans doute la meilleure illustration au travers du développement de techniques permettant d'affiner le ciblage publicitaire en fonction du profil avec des adaptations en temps réel[4] du message affiché, ou le recours à des techniques de « re-targeting » ou reciblage publicitaire pour améliorer l'efficacité d'une campagne.

Les applications sont nombreuses dans le domaine scientifique : géologie, météorologie, par l'intermédiaire de capteurs pour surveiller et prévoir le déclenchement de phénomènes naturels. De la même manière on retrouve des applications dans des domaines d'intérêts publics comme l'aide au diagnostic médical ou la veille sanitaire.

De grandes sociétés informatiques développent aussi des projets pour accompagner des villes avec la promesse de les rendre plus « intelligentes », en adaptant les ressources aux besoins au moyen d'algorithmes de prévision de trafic par exemple. Dans le domaine de la sécurité publique, il s'agit d'agréger et d'analyser un ensemble de données dans le but de détecter les comportements « anormaux » et d'anticiper les menaces criminelles.

À une période où le coût d'accès à des ressources sur le cloud ne cesse de baisser, les technologies du Big Data s'étendent à de nombreux secteurs de l'économie, fort consommateurs de données, et sont principalement mobilisées pour leurs vertus prédictives.

[1] McKinsey 2011 / [2] Cf. gros plan du chapitre 1 La place des photos dans la vie numérique / [3] Étude IDATE Cloud et Big Data, mai 2012 / [4] On parle de RTB Real Time Bidding pour décrire les enchères en temps réel offertes aux annonceurs, et rendues possibles par la vélocité des systèmes de traitement.

TOUS GOUVERNÉS PAR DES ALGORITHMES ?

La « gouvernementalité algorithmique » est la thèse développée par certains chercheurs[5et6] pour lesquels ces systèmes de détection, de classification et d'évaluation anticipative des comportements structurent *a priori* le champ d'action possible des individus. L'extrême diversité des données susceptibles d'être analysées, la puissance de calcul permise par les technologies du Big Data, combinées aux capacités de stockage offertes par le cloud conduisent ainsi à s'interroger sur l'effectivité des principes « Informatique et Libertés » appliqués au Big Data. Qu'il s'agisse des principes de finalité, de pertinence des données, de loyauté de la collecte ou encore du concept même de donnée personnelle.

C'est la raison pour laquelle la Commission a souhaité engager une réflexion sur cette problématique, qui a d'ailleurs été le sujet d'une des tables rondes organisées dans le cadre de la journée d'études vie privée 2020.

TOUTES LES DONNÉES DEVIENNENT-ELLES IDENTIFIANTES ?

La démocratisation de l'accès à cette puissance de calcul autorise de telles potentialités de croisement et de recoupement de données (pour beaucoup cependant anonymes au départ) qu'elles ouvrent bien évidemment des possibilités infinies de profilage voire de ré-identification des personnes. L'eldorado du Big Data est constitué par ces informations qui ne sont pas nominatives a priori mais qui, grâce au volume de traces ou d'informations en réseaux combinées à d'autres sources, permettent de créer de nouvelles données directement ou indirectement nominatives[7]. En ce sens les technologies du Big Data questionnent l'effectivité des techniques d'anonymisation.

> Serons-nous tous calculés par le Big Data ?

[5] Antoinette Rouvroy et Thomas Berns, Le nouveau pouvoir statistique / [6] Cf. p.18-20 sur « La dictature des algorithmes : demain, tous calculés ? » dans le premier numéro des cahiers IP / [7] Les recherches de Latanya Sweeney, directrice du Data Privacy Lab à l'Université d'Harvard, ont montré que 87 % des américains pouvaient être identifiés à partir de la seule combinaison de 3 informations : le code postal, la date de naissance et le genre.

TOUTES LES DONNÉES DU CLOUD SONT-ELLES UTILISABLES ?

C'est un véritable sujet de débat parmi les chercheurs comme pour la CNIL qui s'interrogent sur le statut à accorder à ces informations considérées comme « publiques », parce qu'elles sont accessibles au travers des réseaux sociaux et donc facilement « agrégeables » avec les technologies du Big Data. Peuvent-elles être simplement utilisées, sans en demander la permission ? Des traitements et analyses peuvent-ils se faire à l'insu des personnes ?

L'analyse de micro-conversations peut par exemple permettre d'avoir des informations assez fines sur les orientations politiques d'un individu.

L'architecture en *cloud* pose également des questions sur la manière dont les données circulent, sur leur stockage et leur analyse en continu. Comment les sécuriser ? Est-il possible, souhaitable de limiter les recoupements, l'interconnexion et la centralisation de toutes ces données potentiellement sensibles ?

90 %
DES DONNÉES CRÉÉES L'ONT ÉTÉ CES 2 DERNIÈRES ANNÉES

FINALEMENT, TOUS PRÉVISIBLES ?

Toutes ces données sont *in fine* traitées par des algorithmes pour les transformer en informations capables de déduire ou de prédire des comportements. C'est d'ailleurs ce qui inquiète certains dans ce passage du déductif à un inductif purement statistique, une forme de nouvelle science sans hypothèse. Laisser ainsi des systèmes automatisés définir ce qui est suspect et ce qui ne l'est pas ne va pas sans poser des questions sérieuses sur un plan éthique.

En particulier, est-il acceptable de vouloir définir et détecter des comportements « anormaux » sur une logique statistique ?

Se pose également la question de la légitimité de la prise de décision sur la base d'un traitement automatique dont les individus ne connaissent pas la logique. Dans la mesure où ces algorithmes sont de véritables boîtes noires, comment les informer sur les conditions d'exploitation de données au départ anonymes et dont on ne connaît pas a priori l'usage qui en sera fait ? Comment assurer le respect de leurs droits ? Comment pourraient-ils contester la logique qui sous tend une décision prise sur la base d'un tel traitement ? Ou, à l'inverse les individus sont-ils susceptibles d'adopter certains comportements en anticipant des traitements de ce type ?

Au final, comment appliquer le principe de proportionnalité et de pertinence des données dans un contexte où il est de l'essence même du Big Data de recueillir toujours plus de données ?

Alors que les Big Data commencent à émerger en tant que champ de recherche et que ces technologies se diffusent à l'ensemble de l'économie, beaucoup de questions restent en suspens quant aux implications éthiques de leurs usages. L'intérêt pour ces questions a été appuyé par les experts rencontrés pour le premier numéro des Cahiers IP et lors de la journée d'études « vie privée 2020 ». Elles sont à l'ordre du jour du programme d'études de la CNIL en 2013. ■

Big Data : une nouvelle science sans hypothèse ?

VERS UN DROIT À L'OUBLI NUMÉRIQUE ?

Le droit à l'oubli numérique est la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie privée ou publique mise en ligne. Nécessité humaine et sociétale, ce droit ne doit, cependant, pas être interprété comme un impératif absolu d'effacement des données. Il est, en effet, nécessaire de trouver un équilibre entre le droit à l'oubli, d'une part et la nécessité de se ménager des preuves, le devoir de mémoire et la liberté d'expression, d'autre part.

LE DROIT À L'OUBLI SOUS L'ANGLE « INFORMATIQUE ET LIBERTÉS »

Le droit à l'oubli n'est pas en lui-même un concept juridique reconnu par le législateur, mais il résulte de l'application combinée de plusieurs principes issus de la loi « Informatique et Libertés » dans sa rédaction initiale comme dans celle résultant de la transposition de la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles, ainsi que dans la convention 108 du Conseil de l'Europe du 28 janvier 1981. Au-delà des principes de finalité, de loyauté, d'exactitude et de mise à jour des données, la Commission a ainsi toujours veillé à l'obligation de définir et de respecter des durées de conservation conformes à la finalité poursuivie et de prendre en compte les demandes de droit d'opposition en résultant.

La circulation d'informations personnelles concernant une personne peut en effet avoir de graves conséquences sur sa vie privée et professionnelle. Les plaintes adressées à la CNIL illustrent parfaitement ce risque d'atteinte à la vie privée des particuliers. **Celles liées aux problématiques de droit à l'oubli sur Internet (suppression de textes, photographies ou vidéos en ligne) sont en constante augmentation depuis plusieurs années.**

> Nécessité humaine et sociétale, le droit à l'oubli ne doit pas être interprété comme un impératif absolu d'effacement des données

LA NÉCESSITÉ DE SE DOTER DE SOLUTIONS JURIDIQUES ET TECHNIQUES INNOVANTES PERMETTANT D'ASSURER L'EFFECTIVITÉ DU DROIT À L'OUBLI

À la veille de l'adoption d'un nouveau règlement européen consacrant le droit à l'oubli, il est nécessaire de s'interroger collectivement sur l'effectivité réelle de ce droit à propos duquel s'exprime une demande sociale importante. Il s'agit d'examiner les solutions juridiques et techniques innovantes permettant d'assurer un meilleur respect de ce nouveau droit et offrant aux individus les moyens réels de maîtriser la diffusion de leurs données à caractère personnel.

Il serait par exemple possible d'offrir aux utilisateurs des fonctionnalités leur permettant de définir une date de « péremption » de leurs publications ou de gérer leurs propres publications en leur offrant directement la possibilité de les modifier ou de les supprimer.

Par ailleurs, l'effectivité du droit à l'oubli doit être complétée par une obligation juridique de déréférencement à la charge des moteurs de recherche. Ces derniers sont, en effet, devenus les principales clés d'entrée pour la recherche et la diffusion des données à caractère personnel sur Internet. Cette obligation s'avère utile, notamment, en cas de reproduction multiple d'une publication, en cas d'inaction du responsable de traitement initial (par exemple : l'éditeur du site internet) ou en cas d'impossibilité de contacter le responsable de traitement à la suite de son décès. Le droit au déréférencement, corollaire du droit à l'oubli, pourrait ainsi être consacré dans le règlement européen.

> Le droit au déréférencement, corollaire du droit à l'oubli, pourrait être consacré dans le règlement européen

La CNIL se félicite enfin que le projet de règlement prévoit un droit à la portabilité. Ce droit permet d'obtenir auprès du responsable du traitement une copie de ses données, dans un format électronique structuré couramment utilisé et permettant leur réutilisation. Le droit à la portabilité concourt donc au droit à l'oubli en autorisant les individus à récupérer leurs données et en leur évitant d'être captifs d'un service particulier.

Le développement des réseaux sociaux se manifeste, notamment, par une propension croissante des individus à exposer leur vie privée. Le caractère transnational du réseau Internet accentue la difficulté de maîtriser les informations publiées. Il apparaît alors essentiel que les autorités de protection des données, en concertation avec les professionnels, les acteurs de la société civile et les citoyens, agissent ensemble pour que le droit à l'oubli numérique puisse être effectif. ■

LA BIOMÉTRIE : UNE DOCTRINE PRAGMATIQUE ET ÉVOLUTIVE

Six ans après l'adoption des premières délibérations de la CNIL sur les dispositifs biométriques, la CNIL a constaté que l'évolution des technologies et des usages imposait une modernisation de sa doctrine en matière de biométrie.

UNE RÉFLEXION INSCRITE DANS LE PRINCIPE DE RÉALITÉ

À la suite de plus d'une dizaine d'auditions, notamment avec les syndicats de salariés ou patronaux, un consensus s'est clairement exprimé pour considérer comme disproportionnée l'utilisation de la biométrie aux fins de contrôle des horaires. Dès lors, en octobre 2012, la Commission a décidé de modifier l'AU-007 qui autorisait l'utilisation du contour de la main aux fins de gestion des horaires.

Fin 2012, la Commission a soulevé plusieurs questions de fond sur les usages de la biométrie pour accéder à des activités sportives ou de loisirs relevant de l'exercice d'une mission de service public. Au cours de ce travail, la Commission a constaté la nécessité d'approfondir sa réflexion.

En 2013, la CNIL souhaite mesurer l'impact de l'évolution des technologies biométriques et de leurs usages et favoriser une approche réaliste de nouveaux enjeux technologiques, économiques ou sociaux. La Commission a donc initié cette réflexion en auditionnant des experts du secteur, le 7 février 2013.

Ces experts représentaient la **communauté scientifique**, les **industriels du secteur** et la **société civile**.

Les discussions ont notamment porté sur :

- la relation entre le traitement de données biométriques (corporelles, irrévocables) et la protection du corps humain, sur la signification du critère de « proportionnalité »,
- un encadrement des finalités lors d'un stockage centralisé des empreintes digitales,
- la distinction des finalités de sécurité et de confort et sur la notion de « consentement préalable » des personnes concernées.

Aujourd'hui, la mise en œuvre de dispositifs biométriques à des fins de « souveraineté » (contrôle d'identité pour le compte de l'État) ne constitue plus qu'un des nombreux « marchés » de la biométrie. Les enjeux de cette technologie ne sont donc plus seulement sécuritaires mais deviennent également sociaux et ludiques (reconnaissance faciale en ligne par exemple). Dans ces conditions, la CNIL doit tenir compte d'un contexte économique et social en permanente évolution.

> La CNIL consulte la communauté scientifique, tient compte des propositions des fabricants et des représentants de la société civile

QUEL ENCADREMENT DE LA BIOMÉTRIE ?

Au-delà des aspects techniques et juridiques pris en considération par les délibérations de la CNIL, la Commission souhaite aujourd'hui s'interroger sur :

- **la perception par les utilisateurs de ces dispositifs biométriques** : entre, d'une part, le légitime besoin de sécurité ou l'utilité pratique et, d'autre part, le spectre de « Big brother » : quel est le ressenti réel de la société face à ces nouveaux instruments ?
- **le rôle de la CNIL face à l'essor de ces dispositifs** : la CNIL devrait-elle imposer une frontière claire entre les usages pertinents de la biométrie et ceux qui ne sont pas considérés comme acceptables car présentant trop de risques pour la vie privée eu égard à leur finalité ? Devrait-elle davantage développer une compétence pédagogique afin de sensibiliser chacun de nous aux risques relatifs à la vie privée, et nous permettre ainsi des choix plus éclairés ?
- **les instruments proposés par la CNIL à disposition des responsables de traitement** : la CNIL devrait-elle mettre à disposition des déclarants des outils leur permettant d'analyser la pertinence du dispositif biométrique envisagé au regard des critères de finalité, de proportionnalité, de sécurité et d'information des personnes en référence au modèle anglo-saxon et à la notion d'« *analyse d'impact relative à la protection des données* » (PIA en anglais) inscrite à l'article 33 du projet de règlement communautaire du 25 janvier 2012 ?
- modèles de supports d'information à diffuser auprès de tout éventuel client ?

La CNIL envisage de moderniser ses instruments d'aide à la décision sur l'usage des solutions biométriques, afin qu'ils soient utiles et fonctionnels pour l'ensemble des responsables de traitement, des utilisateurs et des industriels du secteur. ■

ANNEXES

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 élue présidente de la CNIL le 21 septembre 2011.

Vice-président délégué

Emmanuel de GIVRY, conseiller honoraire à la Cour de cassation
Secteur : Ressources humaines
Emmanuel de Givry est membre de la CNIL depuis février 2004, puis vice-président délégué depuis février 2009.

Vice-président

Jean-Paul AMOUDRY, sénateur de la Haute-Savoie
Secteur : Banques et crédit
Jean-Paul Amoudry est membre de la CNIL depuis janvier 2009, et vice-président depuis octobre 2011.

LES MEMBRES (COMMISSAIRES)

Jean-François CARREZ, président de chambre honoraire à la Cour des comptes
Secteur : Transports, élections
Jean-François Carrez est membre de la CNIL depuis janvier 2009.
Il est membre élu de la formation restreinte.

Dominique CASTERA, membre du Conseil économique, social et environnemental
Secteurs : Coopération policière internationale – Vie associative
Dominique Castera est membre de la CNIL depuis octobre 2010.

Jean-Marie COTTERET, professeur émérite des universités
Secteur : Police nationale et sûreté de l'État
Jean-Marie Cotteret est membre de la CNIL depuis janvier 2004.
Il est vice-président de la formation restreinte.

Claire DAVAL, avocate
Secteur : Justice
Claire Daval est membre de la CNIL depuis janvier 2009.
Elle a été élue Présidente de la formation restreinte.

Claude DOMEIZEL,
sénateur des Alpes-de-Haute-Provence
Secteur : Développement durable, énergie et logement
Claude Domeizel est membre de la CNIL depuis décembre 2008.
Il est membre élu de la formation restreinte.

Laurence DUMONT,
députée du Calvados
Secteur : Questions sociales et fiscales
Laurence Dumont est membre de la CNIL depuis octobre 2012.

Didier GASSE, conseiller maître honoraire à la Cour des comptes
Secteurs : Télécommunications et internet – sécurité – vote électronique
Didier Gasse est membre de la CNIL depuis janvier 1999.

Gaëtan GORCE, sénateur de la Nièvre
Secteur : Libertés publiques et e-administration
Gaëtan Gorce est membre de la CNIL depuis décembre 2011.

Sébastien HUYGHE, député du Nord
Secteur : Identité, défense et affaires étrangères
Sébastien Huyghe est membre de la CNIL depuis juillet 2007.

Jean MASSOT, président de section honoraire au Conseil d'État
Secteurs : Santé et assurance maladie – archives et données publiques
Jean Massot est membre de la CNIL depuis avril 2005.

Marie-Hélène MITJAVILE, conseiller d'État
Secteur : Recherche et statistiques
Marie-Hélène Mitjavile est membre de la CNIL depuis janvier 2009. Elle est membre élue de la formation restreinte.

Éric PERES, membre du Conseil économique, social et environnemental
Secteur : Éducation et enseignement supérieur
Éric PERES est membre de la CNIL depuis décembre 2010.

Bernard PEYRAT, conseiller honoraire à la Cour de cassation
Secteur : Commerce et marketing
Bernard Peyrat est membre de la CNIL depuis février 2004.

Dominique RICHARD, consultant
Secteurs : Affaires culturelles et sportives – vidéoprotection
Dominique Richard est membre de la CNIL depuis janvier 2009.
Il est membre élu de la formation restreinte.

Commissaires du gouvernement

Jean-Alexandre SILVY
Catherine POZZO DI BORGO, adjointe

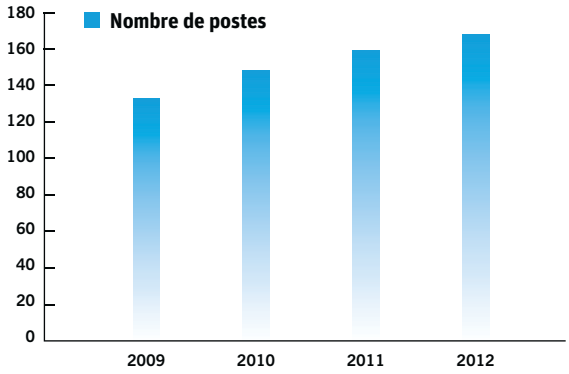
LES MOYENS DE LA CNIL

LE PERSONNEL

Afin de faire face à l'augmentation soutenue de ses missions traditionnelles ainsi qu'à l'extension de son périmètre d'intervention par l'entrée en vigueur de nouveaux textes législatifs, la CNIL connaît une croissance continue et significative de ses moyens humains.

Ainsi, en 2012, elle a été dotée de 12 postes supplémentaires, passant ainsi de 159 postes à 171, soit une augmentation de 7,5 % de ses effectifs.

Ces nouveaux emplois ont permis notamment le renforcement des moyens humains en matière d'expertise informatique et d'investigation



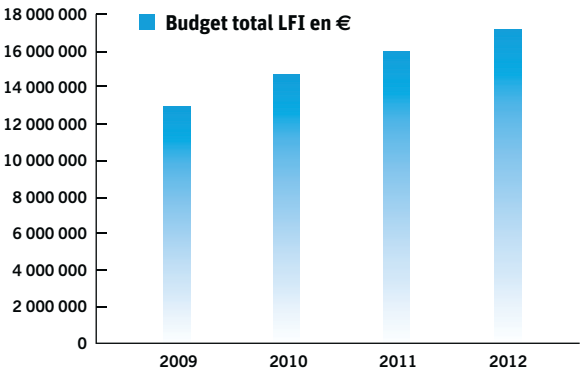
La croissance soutenue de l'activité des services de la Commission, tant dans ses missions premières de conseil, d'examen des formalités préalables obligatoires (demandes d'avis et d'autorisation), d'instruction des plaintes, de contrôles, de sanctions et d'animation du réseau des CIL, que dans les dernières confiées par le législateur (contrôle de la vidéoprotection - loi n°2011-267 du 14 mars 2011 dite LOPPSI 2 et enregistrement des notifications des failles de sécurité -, loi n°2011-302 du 22 mars 2011) conduit à maintenir cette phase de croissance des effectifs a minima tout au long du triennal 2013-2015. 7 créations de postes ont de ce fait été actées pour chacune des trois prochaines années.

LES CRÉDITS

En 2012, la CNIL a été dotée d'un budget total de 17,2 millions d'euros répartis à hauteur de 11,3 millions pour le personnel et 5,9 millions d'euros pour le fonctionnement. Le budget alloué au personnel croît ainsi d'un million d'euros entre 2011 et 2012. Cette augmentation de 10 % du budget est inhérente à l'accroissement du nombre de postes ouverts à la CNIL.

Le budget de fonctionnement augmente également mais dans une moindre mesure (+180 000 euros par rapport à 2011).

Dans ce contexte de maîtrise actuelle des finances publiques, le budget de fonctionnement fait donc l'objet d'une utilisation contrôlée et d'une optimisation des fonds mis à disposition. Les dépenses de fonctionnement courant sont donc particulièrement surveillées et maximisées afin de pourvoir à l'équipement des postes de travail des nouveaux arrivants sans augmenter significativement les budgets alloués par famille



d'achats. Dans cette optique, la CNIL recourt depuis 2012 à des dispositifs d'achats mutualisés, notamment les marchés passés par le Service d'Achats de l'État, en vue de réaliser des économies structurelles sur des dépenses de fonctionnement courant obligatoires telles que les fournitures de bureau, la papeterie, les achats de documentations ou d'abonnements. ■

ORGANIGRAMME DES DIRECTIONS ET SERVICES

Isabelle Falque-Pierrotin
Présidente

Édouard Geffray
Secrétaire général

Norbert Fort
Directeur adjoint, chargé de mission Qualité performance et risques

Clarisse Girot, Stéphane Grégoire et Geoffroy Sigrist
Conseil juridique et relations institutionnelles

Elsa Trochet-Macé
Service de la communication externe et interne

Sophie Vulliet-Tavernier
Direction des études, de l'innovation et de la prospective

Edmée Moreau
Service de l'information et de la documentation

Hervé Machi et Sophie Nerbonne (adjoint)
Direction des affaires juridiques internationales et de l'expertise

Paul Hebert
Service des affaires juridiques

Florence Raynal
Service des affaires européennes et internationales

Gwendal Le Grand
Service de l'expertise informatique

Florence Fourets Mathias Moulin (adjoint)
Direction des relations avec les usagers et du contrôle

Fatima Hamdi
Service d'orientation et de renseignements du public

Daniéla Parrot
Service des plaintes

Thomas Dautieu
Service des contrôles

Elise Wolton
Service de la gestion des sanctions

Albine Vincent
Service des correspondants

Maryline Abiven
Service du droit d'accès indirect

Isabelle Pheulpin
Direction des ressources humaines, financières, informatiques et logistiques

Olivier Tournut
Service des ressources humaines

Magali d'Elia
Service financier

Hervé Brassart
Service de l'informatique interne

Marcel Fanjeaux
Service logistique

LISTE DES ORGANISMES CONTRÔLÉS EN 2012

ASSURANCE

APRIL PARTENAIRES
MAIF
MUTEX

BANQUE

BANQUE TRAVELEX SA
CRCAM DES SAVOIE CREDIT AGRICOLE DES SAVOIE

COLLECTIVITES LOCALES

COMMUNAUTE D'AGGLOMERATION DE RENNES
COMMUNE DE CHELLES
COMMUNE DE CHOISY-LE-ROI
COMMUNAUTE DE COMMUNES DE RUFFEC
COMMUNE DE PARIS
COMMUNE DE RENNES
COMMUNE DE VILLERS-SUR-MER
CONSEIL GENERAL DE LA CHARENTE MARITIME
CONSEIL GENERAL DU VAL D'OISE
SERVICE DEPARTEMENTAL D'INCENDIE ET DE SECOURS DES BOUCHES DU RHONE

COMMERCE

ADIDAS CHAMPS ELYSEES
AMAZON.FR
APPLE FRANCE
ARNELLL
AUCHAN E-COMMERCE FRANCE
AUCHAN LA DEFENSE
BOULANGER
BOURSE IMMOBILIERE
BOUYGUES TELECOM
CANAL + FRANCE
CASINO CANNES BALNEAIRE PALM BEACH
CASINO DE PANTIN
CASINO DE TROUVILLE
CARREFOUR MARKET VERSAILLES
CASH CONVERTERS
CEE DIRECTE
CELIO FRANCE VINCENNES
CENTRE DE RESSOURCES INTERACTIF
CHAUSPORT REIMS
CHRISTIE'S FRANCE SAS
COGEMEX
COMMUNICATION DIRECTE EXTERNALISEE DE L'ENTREPRISE (C.DIRECTE)
CORA MONDELANGE
CORA
COURIR FRANCE
CRITEO
DALKIA FRANCE
DECATHLON MONTREUIL SOUS BOIS
DECATHLON SAINT DENIS
DIA NANTERRE
DROUOT MONTMARTRE HOLDING
EBSCO
EDF
EGEYS
EMAILVISION
EMB SERVICE
EOREZO
ERDF
ETAM CRETEIL
EURODIF
EURO PACTE
FIA-NET
FNAC DIRECT
FONEX
FRANCE TELECOM
FRANPRIX NEULLY SUR SEINE
GAP
GALERIES LAFAYETTE LILLE
GALERIES LAFAYETTE REIMS
GDF-SUEZ
GFK RETAIL AND TECHNOLOGY FRANCE
GO SPORT
GOOGLE Inc.
GRDF
GROUPE CONCOURSMANIA
GROUPE D.S.E. FRANCE
GUCCI FRANCE
HEMA FRANCE EVRY
HITEX
INTERMARCHE COMPIEGNE
INTRINSEC
JDC

▸▸▸

▸▸▸

JENNYFER CRETEIL
JIVE SQUAD
JUST AROUND US
LA FRANCAISE DES EAUX
LA HUTTE FRANCE SPORT REIMS
LEADER PRICE NANTERRE
LE FURET DU NORD
LEROY MERLIN
LIDL EVRY
LYONNAISE DES EAUX FRANCE
OBJECTIF TERRAIN
OMER TELECOM LIMITED
OPINION-WAY
PANDIS DISTRIBUTION PANTIN
PAYBOX SERVICES
P COMME PERFORMANCE
P2H INVESTISSEMENT
PIXMANIA
POWEO
PRISMA PRESSE
MARIONNAUD PARFUMERIE
MESSAGE BUSINESS
MEUBLES IKEA FRANCE SNC
MOBEO
MONOPRIX CONVENTION
MONOPRIX ROUEN
MONOPRIX TERNES
NANTAISE DES EAUX SERVICES
NOVEX
RUE DU COMMERCE
SHALISO
SENSEE
S.F.I.G.
SIMONPLAST
SMART & CO
SOCIETE FRANCAISE DE RADIOTELEPHONE (SFR)
SOGETI FRANCE
SOCIETE DE PROTECTION ELECTRONIQUE ET MECANIQUE
SOTHEBY'S FRANCE
SWATCH STORE
TMB
TRIDENT MEDIA GUARD
TOTAL RAFFINAGE MARKETING
TRAVELEX PARIS SAS
TUTO4PC.COM
UNITEAD
VEOLIA EAU – COMPAGNIE GENERALE DES EAUX
VERSAILLES VOYAGES
VENTE-PRIVEE.COM
VIA2S
ZONG SAS

CULTURE

CENTRE NATIONAL D'ART ET DE CULTURE GEORGES POMPIDOU
OPERA NATIONAL DE PARIS
THEATRE DU CAVEAU DE LA REPUBLIQUE

EDUCATION

CENTRE REGIONAL DE DOCUMENTATION PEDAGOGIQUE
COLLEGE HENRI BARBUSSE
COLLEGE GEORGES CLEMENCEAU
LYCEE HENRI IV
LYCEE MARCELIN BERTHELOT

IMMOBILIER

AGENCE NATIONALE POUR LA RENOVATION URBAINE (ANRU)
EIFFAGE IMMOBILIER ATLANTIQUE
FRANCE HABITATION
GREEN POINT (BE PREM'S)
IMMOBILIERE 3 F
OFFICE PUBLIC DE L'HABITAT DU TERRITOIRE DE BELFORT
OPH-PARIS HABITAT

POLICE - JUSTICE

AGENCE NATIONALE DES TITRES SECURISES (ANTS)
CONSEIL NATIONAL DES ACTIVITES PRIVEES DE SECURITE (CNAPS)

MINISTERE DE L'INTERIEUR :

EURODAC
CIRCONSCRIPTION DE SECURITE PUBLIQUE DE COMPIEGNE
CIRCONSCRIPTION DE SECURITE PUBLIQUE DE STRASBOURG
DIRECTION DEPARTEMENTALE DE LA SECURITE PUBLIQUE DE LYON
SERVICE CENTRAL DE DOCUMENTATION CRIMINELLE
PREFECTURE DU BAS–RHIN
PREFECTURE DE GIRONDE
PREFECTURE DE L'OISE
PREFECTURE DU RHONE
PREFET DELEGUE CHARGE DE LA SECURITE ET DE LA SURETE DES PLATEFORMES AEROPORTUAIRES DE ROISSY ET DU BOURGET
SERVICE DEPARTEMENTAL D'INFORMATION GENERALE DE BORDEAUX

MINISTERE DE LA JUSTICE :

MAISON D'ARRET DE CHALONS-EN-CHAMPAGNE
TRIBUNAL DE GRANDE INSTANCE DE BOBIGNY
TRIBUNAL DE GRANDE INSTANCE DE BORDEAUX
TRIBUNAL DE GRANDE INSTANCE DE LYON
TRIBUNAL DE GRANDE INSTANCE DE SENLIS
TRIBUNAL DE GRANDE INSTANCE DE STRASBOURG

MINISTERE DES AFFAIRES ETRANGERES :
MISSION POUR LA POLITIQUE DES VISAS
DIRECTION DES SYSTEMES D'INFORMATION
CONSULAT GENERAL DE FRANCE D'ISTANBUL
CONSULAT GENERAL DE FRANCE DE LONDRES
CONSULAT GENERAL DE FRANCE DE MOSCOU

SANTE - SOCIAL

AIMSU
AMBULANCE LA MALOUINE
AMEDIM
BEBE VIEW
BIOSYNERGIE
CAISSE NATIONALE D'ALLOCATIONS FAMILIALES
CAISSE PRIMAIRE D'ASSURANCE MALADIE DE TOULOUSE
CENTRE COMMUNAL D'ACTION SOCIALE DE RENNES
CENTRE HOSPITALIER COCHIN (CECOS)
CENTRE MEDICO CHIRURGICAL DE READAPTATION DES MASSUES
CEGEDIM
CLINIQUE GERIATRIQUE CHATEAU GOMBERT
CONSEIL GENERAL DE L'HERAULT
ECHOGRAFILM
FONDATION DES APPRENTIS D'AUTEUIL
FONDATION HOSPITALIERE SAINTE-MARIE
FRANCE TELECOM – ORANGE BUSINESS SERVICES
GRANDE PHARMACIE BAILLY
GRANDE PHARMACIE BROCHANT
GROUPE HOSPITALIER JEAN-VERDIER (CECOS)
HOPITAL PRIVE GERIATRIQUE LES MAGNOLIAS
HOSPICES CIVILS DE LYON
I-DISPO
INSERM
LABORATOIRE ALPHA
LABORATOIRE BEAUHAIRE ET BIENVENU
LABORATOIRE CENTRAL 92
LABORATOIRE DUBREUIL
LABORATOIRE DU VAL-AKNOUCHE
LABORATOIRE GENDRAULT-TALLOBRE MANCY
LA PHARMACIE BLEUE
LINK CARE SERVICES
MAISON D'ENFANTS A CARACTERE SOCIAL MAISON JEAN XXIII
MEGABUS INTERNATIONAL
NCS NORD DE FRANCE
OVH
PHARMACIE ALIMI SOFIYAT
PHARMACIE COULAND REGINE ISABELLE
PHARMACIE D'ALBRET
PHARMACIE DE LA REPUBLIQUE
PHARMACIE DE L'HOTEL DE VILLE ET DE ST ANDRE
PHARMACIE DES GRANDS HOMMES
PHARMACIE DU CHATEAU
PHARMACIE DU FOUR-BONAPARTE
PHARMACIE EDGAR QUINET
PHARMACIE MONTPARNASSE
REGISTRE FINISTERIEN DES TUMEURS DIGESTIVES
REGIME SOCIAL INDEPENDANTS AQUITAINE
RESEAU DE CANCEROLOGIE ONCOBOURGOGNE
RESIDENCE LA GUILBOURDERIE
SEDAD
SIAO 67
S.M.A.I.O

SECURITE PRIVEE – RECOUVREMENT DE CREANCES

ASSISTANCE RISQUE CLIENT (ARCA CONSEIL)
BUREAU EUROPEEN D'INFORMATIONS COMMERCIALES –BEIC
CRISTAL RISK MANAGEMENT
GENERALE D'EDITION ELECTRONIQUE
MES CONSEILS
OFFICE JURIDIQUE NATIONAL DE RECOUVREMENT (OJNR)

SPORT

CONSORTIUM STADE DE FRANCE
FEDERATION FRANCAISE D'ATHLETISME
FEDERATION FRANCAISE DE FOOTBALL
FEDERATION FRANCAISE DE TENNIS
FEDERATION FRANCAISE DE WUSHU ARTS ENERGETIQUES ET MARTIAUX CHINOIS
GOLF INTERNATIONAL DE GRENOBLE
LIGUE DE FOOTBALL PROFESSIONNEL
LIGUE REGIONALE DE TIR DE LA COTE D'AZUR
PARIS SAINT-GERMAIN FOOTBALL
PISCINE SAINT-CHARLES

TRAVAIL - RECRUTEMENT

AFPA RENNES
PROFESSIONAL SERVICE CONSULTING
ROLESCO
START PEOPLE

TRANSPORT

KEOLIS BORDEAUX
SANEF
SOCIETE DES AUTOROUTES ESTEREL, COTE D'AZUR, PROVENCE, ALPES (ESCOTA)
VEOLIA TRANSPORT MONT-SAINT-MICHEL
VINCI PARK

LISTE DES ORGANISMES CONTRÔLÉS EN 2012 DISPOSITIFS DE VIDÉOPROTECTION/VIDÉOSURVEILLANCE

ASSOCIATION

AUTOMOBILE CLUB DE FRANCE

BANQUE

BANQUE DE FRANCE
BARCLAYS BANK
CAISSE REGIONALE DE CREDIT AGRICOLE MUTUEL DE NORMANDIE
CREDIT MUTUEL BRESSAN
SOCIETE GENERALE

COLLECTIVITES LOCALES

COMMUNAUTE URBAINE DE STRASBOURG
COMMUNE D'ALLONNE
COMMUNE D'ARGENTEUIL
COMMUNE DE BRY-SUR-MARNE
COMMUNE DE CAGNES-SUR-MER
COMMUNE DE CHELLES
COMMUNE DE LYON
COMMUNE DE MORANCE
COMMUNE DE NOGENT-SUR-MARNE
COMMUNE DE PANTIN
COMMUNE DE ROUEN
COMMUNE DE SAINT-GERMAIN-EN-LAYE
COMMUNE DE SAINT-MANDE
COMMUNE DE TOULOUSE
COMMUNE DE VILLENEUVE-LA-GARENNE

COMMERCE

ALKERN NORD
ANASUN
AOCT
BATI DOLE
BIJOUTERIE LEPAGE
BOUCHERON
MAGASINS BOULANGER
BOUTIQUE BODY'MINUTE
CABINET DOUCET-KORHEL
CARLTON'S HOTEL
CENTRES E. LECLERC
CHOCOLATERIE DE BEUSSENT LACHELLE
DALLOYAU
GARAGE BOURBON GENLIS
GENTILE MOTO SPORT
GRANDE PHARMACIE DU MARCHE
GROUPE MARIE-CLAIRE
GUESS
HANDINAMYC
HERMINE DE PASHMINA
HOTEL BRIGHTON
HOTEL CRILLON
HOTEL DE FRANCE
HOTEL FROCHOT
HOTEL GALANT
HOTEL IBIS GRENOBLE GARE
HOTEL LE BRISTOL
HOTEL MERCURE
HOTEL MERCURE PARIS AUSTERLITZ
HOTEL PELETIER OPERA
HOTELS & SPA SAINT-JAMES & ALBANY
INCOGNITO
INSTITUT KARITE
MAGASINS INTERSPORT
JLC OPTICIEN LUNETIER
KEEP COOL
LA FERME DU LAC
LA MODE EST A VOUS
AGENCES LA POSTE
LE MATELY'S
LE PANETON
M'SPORTS
MADE IN V
MAN DIESEL SAS
MAGASINS CARREFOUR
MAGASINS CONFORAMA
MAGASINS DARTY
MAGASINS DECATHLON
MAGASINS GO SPORT
MAGASINS FNAC
MAGASINS JULES
MAGASINS KIABI
MAGASINS LA CHAISE LONGUE
MAGASINS YVES ROCHER
MAP
MARQUES VICTOR
MAUBOUSSIN
MONTRES SUISSES SA
NCT - NOUVELLE COMMUNICATION TELEPHONIQUE
NETTO
NOVOTEL
OPTIQUE CALAS
ORGAPHARM

PATHE GRENOBLE-CHAVANT
PEAU D'ANE
PHARMACIE DE LA GARE
PHARMACIE DU HOHBERG
PHARMACIE HASSAN
PLESSIS GRAND HOTEL
PROLIVAL
PROMOCASH
PRONUPTIA
PROVIDIS LOGISTIQUE SA
RESTAURANTS MC DONALD'S
RESTAURANTS SUBWAY
ROGER CDB
SALMA STORE
SEPHORA
SERGE BLANCO
STARBUCKS COFFEE
SOCIETE D'EXPLOITATION DE LA TOUR EIFFEL
SOCIETE D'AMENAGEMENT TOURISTIQUE ET D'EXPLOITATION LA CLUSAZ (SATELC)
SOCIETE COMMERCIALE DES HOTELS ECONOMIQUES
SOCIETE HOTELIERE MANAGEMENT
SOGIDUN
SUPERMARCHES FRANPRIX
TABAC LE PRESSE BOOK
TABAC LOTO BERTHO
TABAC MERLICO
UGC CINE CITE
UGC GEORGE V
VCASH
VAN CLEEF ET ARPELS

CULTURE

LA MAISON DU LIMOUSIN
MUSEE D'ANGOULEME
MUSEE DE LA MARINE
MUSEE DES ABATTOIRS DE TOULOUSE
MUSEE DES BEAUX ARTS DE DIJON
MUSEE DU LOUVRE
MUSEE JULES VERNE DE NANTES
MUSEE MUNICIPAL D'ORANGE
MUSEE NATIONAL DE LA VOITURE ET DU TOURISME DE COMPIEGNE
THEATRE DU NORD-EST DE THIONVILLE

EDUCATION

ASSSOCIATION DE GESTION « LA DOCTRINE CHRETIENNE »
ECOLE ELEMENTAIRE SERMET
ENSEN (ECOLE SUP. DE L'EDUCATION NATIONALE)

IMMOBILIER

CITYA SAINT-HONORE CANNES
SYNDICAT DES COPROPRIETAIRES ARCADES DES CHAMPS-ELYSEES

POLICE - JUSTICE

DIRECTION DEPARTEMENTALE DES FINANCES PUBLIQUES DES HAUTS DE SEINE
PREFECTURE DE POLICE DE PARIS

SANTE/SOCIAL

CENTRE CARDIOLOGIQUE DU NORD
CLINIQUE LA PERGOLA
EHPAD ORPEA
HOPITAL EUROPEEN DE PARIS GVM CARE & RESEARCH
RESIDENCE ORPEA « LES MARINIERS »

SPORT

FITNESS PARK
PISCINE LEO LAGRANGE (TOULOUSE)

TRANSPORT

RATP
VEOLIA TRANSPORT

LEXIQUE

AFAPDP
L'Association francophone des autorités de protection des données personnelles (AFAPDP) a été créée en 2007, à Montréal, à l'initiative d'une trentaine de représentants d'autorités de contrôle et représentants d'États francophones.
Elle a pour objectif de :
• **Promouvoir le droit à la protection des données personnelles**, dans les États non encore dotés d'une législation (la majorité des États dans le monde), et également au niveau international (pour encourager l'établissement d'un instrument juridique international contraignant) ;
• **Développer et valoriser l'expertise francophone** en matière de protection des données personnelles.

ACCOUNTABILITY
L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

BCR
BCRs signifie « Binding Corporates Rules » ou règles d'entreprise contraignantes. Ces règles internes applicables à l'ensemble des entités du groupe contiennent les principes clés permettant d'encadrer les transferts de données personnelles, de salariés ou de clients et prospects, hors de l'Union européenne.
Ces BCRs sont une alternative au Safe Harbor (qui ne vise que les transferts vers les États-Unis) ou aux Clauses Contractuelles Types adoptées par la Commission européenne.
Elles garantissent qu'une protection équivalente à celle octroyée par la directive européenne de 1995 s'applique aux données personnelles transférées hors de l'Union européenne.

Big data
On parle depuis quelques années du phénomène de « Big Data », que l'on traduit souvent par « données massives ». Avec le développement des nouvelles technologies, d'internet et des réseaux sociaux ces vingt dernières années, la production de données numériques a été de plus en plus nombreuse : textes, photos, vidéos, etc. Le gigantesque volume de données numériques produites combiné aux capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiquées offre aujourd'hui des possibilités inégalées d'exploitation des informations.

Biométrie
La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales…).

Bring your own device (BYOD)
Pratique qui consiste à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel

CASSIOPEE (Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants)
Le traitement CASSIOPEE, mis en œuvre dans les tribunaux de grande instance, permet l'enregistrement d'informations relatives aux plaintes et dénonciations reçues par les magistrats, dans le cadre de procédures judiciaires, afin d'améliorer le délai de traitement des procédures, et d'assurer l'information des victimes.

Cloud Computing
Le Cloud Computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (Cloud) composé de nombreux serveurs distants interconnectés.

CNIL
Autorité administrative indépendante, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers, 4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1), par le Président du Sénat (1), par le conseil des ministres (3). Le mandat de ses membres est de 5 ans.

Conférence mondiale des Commissaires à la protection des données et à la vie privée
Cette conférence se tient chaque année à l'automne. Elle réunit l'ensemble des 81 autorités et commissaires à la protection des données et à la vie privée de tous les continents. Elle est ouverte aux intervenants et participants du monde économique, des autorités publiques, et de la société civile. Une partie de la Conférence est réservée aux représentants des autorités accréditées par la Conférence, durant laquelle sont adoptées les résolutions et déclarations.

Correspondant « Informatique et Libertés »
La principale mission du correspondant est de s'assurer que l'organisme qui l'a désigné auprès de la CNIL, respecte bien les obligations issues de la loi Informatique et Libertés. Il a un rôle de conseil et de diffusion de la culture Informatique et Libertés auprès de ses collaborateurs, supérieurs hiérarchiques et collègues. À ce titre, le correspondant

est devenu l'acteur incontournable pour toute entité soucieuse de sa responsabilité sociale, de ses valeurs et respectueuse des droits et libertés des usagers, clients et salariés.

Donnée personnelle
Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale…).

Donnée sensible
Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Droit à l'oubli numérique
Le droit à l'oubli numérique est la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie privée ou publique mise en ligne. Nécessité humaine et sociétale, ce droit ne doit, cependant, pas être interprété comme un impératif absolu d'effacement des données. Il est, en effet, nécessaire de trouver un équilibre entre le droit à l'oubli, d'une part et la nécessité de se ménager des preuves, le devoir de mémoire et la liberté d'expression, d'autre part.

Droit d'accès direct
Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'accès indirect
Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.

Droit d'opposition
Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

Droit de rectification
Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

FICOBA (Fichier national des comptes bancaires et assimilés)
FICOBA sert à recenser les comptes de toute nature (bancaires, postaux, d'épargne…), et à fournir aux personnes habilitées des informations sur les comptes détenus par une personne ou une société.

Formation restreinte
Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi « Informatique et Libertés », la CNIL siège dans une formation spécifique, composée de six membres appelée « formation restreinte ». À l'issue d'une procédure contradictoire, cette formation peut notamment décider de prononcer des sanctions pécuniaires pouvant atteindre 300 000 euros.

G29
L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationale. Cette organisation réunissant l'ensemble des CNIL européennes a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G 29 se réunit à Bruxelles en séance plénière tous les deux mois environ.

IaaS / PaaS
IaaS (« Infrastructure as a Service ») désigne la fourniture d'infrastructures de calcul et de stockage en ligne.
PaaS (« Platform as a Service ») désigne la fourniture d'une plateforme de développement d'applications en ligne

NIR
Le Numéro d'Inscription au Répertoire ou numéro de sécurité sociale est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.

Open data
L'Open data désigne un mouvement, né en Grande-Bretagne et aux États-Unis, d'ouverture et de mise à disposition des données produites et collectées par les services publics (administrations, collectivités locales…).

PNR (« Passenger Name Record »)
Il s'agit des informations collectées auprès des passagers aériens au stade de la réservation commerciale. Elles permettent d'identifier, entre autres : l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que des préférences alimentaires spécifiques (végétarien, asiatique, cascher, etc.) ou des services liés à l'état de santé du passager. Des informations du

▸▸▸

▸▸▸

type « tarif pèlerin » « missionnaire » « clergé » telles qu'elles figurent dans les champs « libres » des rubriques « remarques générales ». Ces données étant susceptibles de faire apparaître indirectement une origine raciale ou ethnique supposée, des convictions religieuses ou philosophiques, ou l'état de santé des personnes, sont considérées par la directive européenne comme des données sensibles, à exclure ou à protéger.

Quantified self
Le Quantified Self désigne la pratique de la « mesure de soi » et fait référence à un mouvement né en Californie qui consiste à mieux se connaître en mesurant des données relatives à son corps et à ses activités

RFID (Radio Frequency Identification)
Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micro-puce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution, leur coût est d'environ 5 centimes d'euros.
D'autres puces communicantes, plus intelligentes ou plus petites font leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi-invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm^2, possèdent une capacité de stockage de 512 Ko (kilo octets) et échangent des données à 10 Mbps.(méga bits par seconde).

Séance plénière
C'est la formation qui réunit les 17 membres de la CNIL pour se prononcer sur des traitements ou des fichiers et examiner des projets de loi ou de décrets soumis pour avis par le Gouvernement.

SIS (Système d'information Schengen)
Le système d'information Schengen (SIS) est composé d'une base centrale située à Strasbourg et, dans chaque pays participant à l'espace Schengen, de bases nationales. Les informations concernent essentiellement des personnes :
- recherchées pour arrestation aux fins d'extradition ;
- étrangères, signalées aux fins de non-admission dans l'espace Schengen à la suite d'une décision administrative ou judiciaire ;
- signalées aux fins de surveillance discrète ou de contrôle spécifique.

Smart Grids
Le compteur communicant est une des composantes des réseaux de distribution d'énergie intelligents (également désignés sous les termes anglais de « smart grids »). Ces réseaux utilisent des moyens informatiques évolués afin d'optimiser la production et l'acheminement de l'électricité, notamment grâce à la télétransmission d'informations relatives à la consommation des personnes. Cette télétransmission aura notamment pour conséquence de supprimer la relève physique des compteurs.

STIC (Système de traitement des infractions constatées)
Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées. Il facilite la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il permet également d'élaborer des statistiques.

Traitement de données
Collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation de fichiers ou bases de données, notamment des interconnexions.

Transfert de données
Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Vidéoprotection
Les dispositifs dits « de vidéoprotection » filment la voie publique et les lieux ouverts au public sont soumis aux dispositions du code de la sécurité intérieure

Vidéosurveillance
Les dispositifs dits de « vidéosurveillance » concernent des lieux non ouverts au public (locaux professionnels non ouverts au public comme les bureaux ou les réserves des magasins) sont soumis aux dispositions de la loi « Informatique et Libertés ».

Violation de données à caractère personnel
Toute destruction, perte, altération, divulgation ou accès non autorisé à des données à caractère personnel est une violation de données à caractère personnel.
Une violation peut résulter d'un acte malveillant (par exemple, en cas de piratage informatique) ou se produire à la suite d'une erreur matérielle (par exemple, lorsqu'un salarié détruit ou divulgue le fichier clients de sa société du fait d'une fausse manipulation).

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 EFIL 02 47 47 03 20 / www.efil.fr
Impression La documentation Française / Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr, imprimé en France
Crédit photo Fotolia, istockphoto / **Diffusion** Direction de l'information légale et administrative

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 : 978-2-11-009349-3
DF : 5 HC33610
Prix : 15 €

CNIL.
Commission Nationale de l'Informatique et des Libertés