Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE

MINISTÈRE DE LA COHÉSION DES TERRITOIRES ET DES RELATIONS AVEC LES COLLECTIVITÉS TERRITORIALES

CONCOURS PROFESSIONNEL

SECRÉTAIRES D'ADMINISTRATION ET DE CONTRÔLE DU DÉVELOPPEMENT DURABLE

CLASSE EXCEPTIONNELLE

Spécialités administration générale et contrôle des transports terrestres

SESSION 2020

Épreuve n°1 : rédaction d'une note de synthèse sur un sujet d'ordre général à partir d'un ou plusieurs documents (durée : trois heures ; coefficient 3). Cette épreuve est destinée à mesurer les connaissances du candidat et à évaluer les compétences suivantes : compréhension, analyse et synthèse.

SUJET : LES DONNÉES PERSONNELLES

A l'aide du dossier documentaire joint, vous rédigerez une note exposant à la fois les enjeux liés à l'utilisation des données à caractère personnel et le cadre réglementaire applicable au plan national.

Le dossier documentaire comprend 23 pages.

Dossier documentaire :

TOTAL : 23 pages

Document 1

Commission Nationale de l'Informatique et des Libertés

Définitions

Donnée personnelle

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.
Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association) :

Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.

A noter : pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.
Attention : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

Traitement de données à caractère personnel

[Un traitement de données à caractère personnel est une] opération portant sur des données personnelles, quel que soit le procédé utilisé. Par exemple, enregistrer, organiser, conserver, modifier, rapprocher avec d'autres données, transmettre, etc. des données personnelles.

<u>Des fichiers mais pas seulement :</u>
Un traitement n'est donc pas uniquement un fichier, une base de données ou un tableau Excel. Il peut s'agir aussi d'une installation de vidéosurveillance, d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc. ;
Des traitements apparaissent et évoluent selon les innovations technologiques.

<u>Informatisés mais pas uniquement :</u>
Un traitement de données à caractère personnel peut être informatisé ou non ; Un fichier papier organisé selon un plan de classement, des formulaires papiers nominatifs ou des dossiers de candidatures classés par ordre alphabétique ou chronologique sont aussi des traitements de données personnelles.

Document 2

Le Monde (24/05/2018)

Protection des données : ce que le RGPD change pour les entreprises

----

Le règlement général sur la protection des données (RGPD) entre en vigueur le 25 mai dans toute l'Europe. Il constituera désormais le cadre dans lequel les sociétés pourront exploiter les données personnelles en leur possession, qu'il s'agisse de celles de leurs employés, de leurs clients ou de leurs fournisseurs.

Une information claire et transparente

Premier changement introduit par le RGPD : il crée un cadre réglementaire unifié au niveau européen, là où chaque pays, précédemment, avait sa propre législation nationale sur le traitement des données personnelles. Ce projet participe de la volonté de créer un marché numérique unique au sein de l'Union, dont la Commission estime qu'il pourrait générer 415 milliards d'euros par an et créer des centaines de milliers d'emplois. Or les industries du numérique s'appuient de plus en plus sur les données pour créer de la richesse. En unifiant les pratiques dans chaque pays, la Commission souhaite permettre aux acteurs du numérique européen d'accéder plus facilement à ce marché de 500 millions de clients potentiels, et ainsi faciliter l'émergence de géants continentaux.

Mais ce coup de pouce va de pair avec une demande de plus de responsabilités. Afin de gagner la confiance des citoyens, pour qu'ils acceptent plus facilement de partager leurs données, le RGPD demande que tous les responsables de traitements garantissent aux utilisateurs un certain nombre de droits : une information claire sur l'utilisation qui va être faite de leurs données, une possibilité pour eux de consulter les données utilisées, de les modifier ou de les supprimer, etc. Même si beaucoup de ces droits existaient déjà, leur exercice par les utilisateurs était jusque-là fastidieux.

Enfin le RGPD vise également à rééquilibrer la concurrence avec les acteurs extraeuropéens, GAFA (Google, Apple, Facebook, Amazon) en tête, puisque ceux-ci seront soumis aux mêmes contraintes dès lors qu'ils voudront manipuler les données des citoyens européens.

Les entreprises responsabilisées

En matière de traitement des données personnelles, les entreprises françaises étaient soumises, jusque-là, à la loi Informatique et liberté de 1978, modifiée en 2004 pour intégrer des dispositions d'une directive européenne de 1995. Pour les entreprises, il s'agissait déjà de démontrer qu'elles ne procédaient pas à une utilisation disproportionnée des données personnelles. La loi imposait une déclaration préalable de ces traitements auprès de la Commission nationale de l'informatique et des libertés (CNIL), voire une autorisation préalable pour les cas les plus sensibles. Pour faciliter les démarches, elle prévoyait la possibilité de recourir aux services d'un correspondant informatique et libertés (CIL), chargé de vérifier la bonne application de la loi au sein de l'entreprise.

Avec le RGPD, ce fonctionnement disparaît. Plus de déclarations préalables : les entreprises sont censées être responsables. En cas de visite de la CNIL, elles doivent pouvoir démontrer qu'elles appliquent les bonnes politiques de gestion des données personnelles.

Pour ce faire elles doivent tenir à jour un registre expliquant toutes les données personnelles qu'elles exploitent, pouvoir prouver que celles-ci ont été obtenues avec le consentement éclairé des utilisateurs (en les informant précisément de la finalité pour laquelle les données sont exploitées), et démontrer qu'elles ont adopté les mesures de sécurité appropriées en fonction du caractère sensible des données, tout particulièrement contre les cyberattaques. Ces obligations s'appliquent aussi aux sous-traitants de l'entreprise impliqués dans le traitement des données (hébergeurs, etc.).

Les CIL eux aussi disparaissent, laissant la place à des délégués à la protection des données (data privacy officers, DPO), chargés de s'assurer de la bonne conformité de l'entreprise avec le règlement. Le DPO peut être un salarié de l'entreprise. Pour les plus petites structures, il peut être externalisé ou mutualisé, par exemple entre différents membres d'une même profession (comme les notaires). Le DPO n'est obligatoire que pour les entreprises se livrant à « un suivi régulier et systématique des personnes à grande échelle » (un réseau social, par exemple) ou manipulant à grande échelle des données dites « sensibles » (données de santé, données biométriques, etc..).

Des sanctions renforcées

L'innovation la plus frappante introduite par le nouveau règlement est le niveau inédit des amendes encourues pour les contrevenants. Jusqu'en 2016, la CNIL ne pouvait pas infliger d'amendes supérieures à 150 000 euros. Depuis la loi pour la république numérique, ce plafond a été relevé à 3 millions d'euros. Avec le RGPD, le pouvoir de sanction de la CNIL est très largement renforcé puisqu'il pourra s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial.

Le niveau de l'amende est en rapport avec la gravité de l'infraction. Faute de jurisprudence, difficile de dire aujourd'hui quand la peine maximale pourra être appliquée.

De nouveaux recours pour les utilisateurs

Le RGPD donne désormais la possibilité à plusieurs particuliers d'intenter des actions de groupe pour obtenir réparation à la suite d'un préjudice dont se serait rendue responsable une entreprise traitant vos données personnelles. Jusque-là les actions de groupe n'étaient possibles que pour faire cesser le trouble (le partage non consenti des données avec une entreprise tierce, par exemple). Désormais, les plaignants pourront réclamer une indemnisation financière.

Document 3

Vie-publique.fr

L’essentiel de la loi du 20 juin 2018 sur la protection des données personnelles

---

La loi relative à la protection des données personnelles a été promulguée le 20 juin 2018. Elle adapte la loi "Informatique et libertés" du 6 janvier 1978 au "paquet européen de protection des données".

Ce paquet européen comprend le règlement général sur la protection des données (RGPD), un règlement du 27 avril 2016 directement applicable dans tous les pays européens au 25 mai 2018 ainsi qu’une directive datée du même jour sur les fichiers en matière pénale, dite directive "police".

La loi fondatrice du 6 janvier 1978 est modifiée sur plusieurs points pour la mettre en conformité avec le RGPD (missions et pouvoirs de la CNIL, élargissement des données sensibles) ou tirer parti des marges de manœuvre qu’il permet (majorité numérique, etc.).

L’adaptation du rôle de la CNIL et de ses pouvoirs de contrôle et de sanction

La composition, les missions et les pouvoirs de la Commission nationale de l’informatique et des libertés (CNIL) sont modifiés.

L’évolution des missions de la CNIL

Les missions de la CNIL évoluent afin de les adapter à la nouvelle logique de responsabilisation et d’accompagnement des acteurs traitant des données (entreprises, administrations, etc.) instaurée par le RGPD. Les formalités préalables auprès de la CNIL sont quasiment toutes supprimées. En complément des missions qu’elle exerce déjà, la CNIL est désormais chargée :

- d’établir et de publier des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements et à procéder à l’évaluation préalable des risques par les responsables de traitement et leurs sous-traitants ;
- d’encourager l’élaboration de codes de conduite par les acteurs traitant des données ;
- de produire et de publier des règlements types afin d’assurer la sécurité des systèmes de traitement et de régir les traitements de données biométriques, génétiques et de santé ;
- de certifier des personnes, des produits, des systèmes de données ou des procédures ;
- de lister les fichiers pénaux pouvant présenter un risque élevé pour les droits et libertés des personnes.

Dans l’exercice de ses missions, la CNIL doit prendre en compte les besoins propres des collectivités locales, dont beaucoup se sont inquiétées des nouvelles règles européennes. Pour les aider, la CNIL a publié sur son site internet plusieurs pages qui leur sont dédiées. La loi prévoit que les petites et moyennes entreprises (TPE-PME) doivent également faire l’objet d’un accompagnement personnalisé. C'est pourquoi la CNIL, en partenariat avec Bpifrance, a mis à leur disposition un guide pratique les sensibilisant au RGPD.

Toujours au titre de ses missions, la CNIL peut dorénavant être consultée sur toute proposition de loi portant sur la protection des données personnelles par les présidents ou les commissions compétentes de l’Assemblée nationale ou du Sénat et par les présidents des groupes parlementaires.

Le renforcement des pouvoirs de contrôle et de sanction de la CNIL

Les pouvoirs de contrôle de la CNIL sont précisés et étendus. La nature des locaux que ses agents peuvent visiter et les conditions dans lesquelles le secret professionnel, notamment médical, peut

leur être opposé sont redéfinies. De plus, pour les contrôles en ligne, les agents peuvent désormais recourir à une identité d'emprunt.

Plusieurs articles de la loi sont également consacrés à la procédure de coopération entre la CNIL et les autres autorités de protection européennes en cas de traitements transnationaux (touchant des personnes de plusieurs pays européens). Le RGPD pose, en effet, de nouvelles règles en la matière. L'objectif est d'apporter une réponse unique en cas d'atteinte au droit à la vie privée des citoyens de plusieurs pays européens (atteinte illustrée par exemple par l'affaire Cambridge Analytica-Facebook).

Les pouvoirs de sanction de la CNIL sont par ailleurs adaptés. De nouvelles sanctions, comme le prononcé d'une astreinte ou le retrait d'une certification ou d'un agrément, sont prévues en cas de violation des règles sur la protection des données. En outre, le montant des amendes administratives est fortement augmenté. Ces astreintes et amendes concernent autant les entreprises que les collectivités locales et les associations, qu'elles soient responsables d'un traitement ou sous-traitant. Seul l'État en est dispensé.

Lors de la discussion du projet de loi, le Sénat voulait exempter les collectivités locales de ces sanctions financières. Il souhaitait également que leur produit serve à financer l'accompagnement par l'État des responsables de traitement et de leurs sous-traitants. Il a, de plus, proposé la création d'une dotation communale et intercommunale afin d'aider les collectivités à se mettre en conformité avec le RGPD. Cette mise en conformité va, en effet, avoir un coût budgétaire pour les petites collectivités. Toutefois, ces amendements ont été rejetés. Néanmoins, à la demande des sénateurs, la mutualisation des services numériques entre les collectivités et leurs groupements est facilitée. Les communes peuvent, en particulier, se doter d'un délégué à la protection des données commun.

L'élargissement des données sensibles

Conformément au RGPD, le champ des données sensibles (sur l'origine raciale, les opinions politiques, etc.) est étendu aux données génétiques et biométriques ainsi qu'aux données relatives à l'orientation sexuelle d'une personne. En principe, ces données ne peuvent pas faire l'objet d'un traitement en raison de leur nature même.

Des dérogations à cette interdiction sont toutefois prévues par le droit européen (si la personne a expressément consenti au traitement de ses données ou si elle les a rendues publiques, en matière de sécurité sociale, etc.). La loi du 20 juin 2018 ajoute d'autres dérogations. Sont notamment permis les traitements de données biométriques (empreintes digitales, etc.) strictement nécessaires aux contrôles d'accès sur les lieux de travail, aux ordinateurs et aux applications utilisés au travail. Sont de même autorisés les traitements portant sur la réutilisation d'informations figurant dans les décisions de justice diffusées dans le cadre de l'open data.

Les marges de manœuvre permises par le RGPD

Le RGPD, bien que d'application directe, contient plus d'une cinquantaine de marges de manœuvre, qui autorisent les États membres à préciser certaines dispositions. La plupart de ces marges de manœuvre ont permis de conserver des dispositions qui existaient déjà dans la loi CNIL de 1978. La loi du 20 juin 2018 n'aménage que quelques points, afin notamment de répondre aux évolutions technologiques et sociétales.

Des formalités préalables maintenues pour certains traitements

Les formalités préalables (autorisations ou déclarations) auprès de la CNIL sont quasiment toutes supprimées. Comme l'autorise le RGPD, la loi en maintient certaines pour :

- les traitements comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR), sauf exceptions ;

- les traitements de données génétiques ou biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes mis en œuvre pour le compte de l'État ;
- les traitements qui intéressent la sûreté de l'État, la défense, la sécurité publique ou qui ont pour objet la prévention et la répression des infractions pénales ;
- les traitements de données de santé justifiés par une finalité d'intérêt public (sécurité des médicaments, etc.).

Catégories particulières de traitement

Plusieurs dispositions de la loi sont consacrées à des catégories particulières de traitements. Sont notamment visés les traitements de données de santé, qui font l'objet d'un régime spécifique.

Sont aussi concernés les traitements de données sur les infractions, condamnations ou mesures de sûreté connexes (hors champ de la directive c'est-à-dire à d'autres fins que la prévention et la répression des infractions). Ces traitements peuvent à présent être effectués par une liste élargie de personnes : par exemple des associations d'aide aux victimes ou de réinsertion ou des personnes mises en cause ou victimes dans une procédure pénale. En revanche, le Conseil constitutionnel, saisi par des sénateurs Les Républicains, a déclaré anticonstitutionnel l'élargissement de la mise en œuvre des tels traitements "sous le contrôle de l'autorité publique" (comme l'hébergement des données sur un serveur). Cette rédaction, qui recopie le RGPD, a été jugée insuffisamment précise.

Droits des personnes

Sur ce point encore, la loi utilise les marges de souplesse permises par le RGPD.

Elle fixe à 15 ans la majorité numérique, c'est-à-dire l'âge à partir duquel un enfant peut consentir seul au traitement de ses données, typiquement sur les réseaux sociaux. Le gouvernement et les sénateurs souhaitaient retenir le seuil de 16 ans, l'âge du consentement fixé par défaut par le RGPD. Le texte a toutefois laissé aux États la possibilité de l'abaisser jusqu'à 13 ans. C'est dans ce cadre que les députés ont voté l'âge de la majorité numérique à 15 ans.

La loi ouvre, par ailleurs, plus largement la possibilité pour l'administration de recourir à des décisions individuelles automatisées. Les décisions fondées exclusivement sur un algorithme ne sont plus interdites. Néanmoins, de nouvelles garanties sont données aux administrés : droits à l'information et à l'explication (déjà consacrés par la loi pour une République numérique de 2016), droit à recours avec une intervention humaine a posteriori, obligation pour l'administration de maîtriser l'algorithme et ses évolutions (prohibition des algorithmes auto-apprenants), interdiction d'utiliser des données sensibles.

Sur ce point les deux chambres étaient à nouveau en désaccord. Les sénateurs souhaitaient encadrer plus strictement l'usage des algorithmes par l'administration. Ils demandaient aussi la transparence des algorithmes utilisés par les universités dans le cadre de Parcoursup (transparence exclue par la loi "orientation et réussite des étudiants" du 8 mars 2018). Les propositions du Sénat ont été rejetées mais, sur amendement du gouvernement, le fonctionnement de Parcoursup va faire l'objet chaque année d'un rapport au Parlement. Le 1er rapport du Comité éthique et scientifique de Parcoursup a été présenté en janvier 2019.

Dans sa décision du 12 juin 2018, le Conseil constitutionnel a jugé conforme à la Constitution les nouvelles règles régissant l'emploi des algorithmes par l'administration. Il considère que "le législateur a défini des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme".

La loi oblige aussi les écoles, collèges et lycées publics à rendre public, à partir de la rentrée 2018, le registre de leurs traitements de données scolaires. Il s'agit entre autres de permettre aux parents d'élèves de savoir comment les données de leurs enfants sont traitées. En vue de sensibiliser les

acteurs de l'Éducation nationale à la protection des données, le ministère de l’Éducation nationale et la CNIL ont signé en décembre 2018 une convention.

Actions de groupe

Les actions de groupe, déjà autorisées depuis fin 2016 pour faire cesser en justice un manquement par un responsable de traitement ou un sous-traitant, sont étendues à la réparation des préjudices matériels et moraux subis en cas de violation des données personnelles.

En vertu du RGPD, les citoyens peuvent aussi se faire représenter par les associations ou organismes actifs dans le domaine de la protection des données pour exercer en leur nom une réclamation auprès de la CNIL, un recours juridictionnel contre la CNIL ou contre le responsable du traitement ou sous-traitant.

C'est ainsi qu'en mai 2018 l’association La Quadrature du Net a déposé une plainte collective auprès de la CNIL contre les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) estimant que ces derniers ne respectent pas le RGPD sur le consentement "libre et éclairé" des internautes. L'association None Of Your Business a également déposé plainte. C'est sur la base de ces plaintes que la CNIL a prononcé le 21 janvier 2019 une amende de 50 millions d'euros contre Google LLC.

Plus récemment, l'association UFC-Que choisir a lancé une action de groupe contre Google, devant le tribunal de grande instance de Paris. Selon le communiqué de l'association du 26 juin 2019, "L’objectif de cette action est de mettre fin à l’exploitation insidieuse des données personnelles" des utilisateurs de Google, "particulièrement ceux détenant un équipement Android avec un compte Google, et de les indemniser à hauteur de 1 000 €".

Le libre choix de ses applications sur smartphone

Cette disposition est issue de l’amendement "Bothorel", du nom du député qui l’a porté. Aujourd’hui, la quasi-totalité des smartphones vendus en France et en Europe sont équipés d’un système d’exploitation mobile iOS ou Android qui impose par défaut, donc sans consentement véritable, le même moteur de recherche à leurs utilisateurs (comme Google). La loi oblige les fabricants ou distributeurs de smartphones à proposer aux consommateurs plus de choix dans les applications. L’objectif est de faire un peu plus de place aux navigateurs web et moteurs de recherche "alternatifs", parfois plus respectueux de la protection des données personnelles de leurs utilisateurs (tel Qwant en France)

La transposition de la directive "police"

La loi du 20 juin 2018 transpose enfin la directive du 27 avril 2016 qui harmonise le régime des traitements à finalité pénale (fichiers de police et de justice comme le fichier national des empreintes génétiques, à l’exclusion des fichiers de renseignement).

Un droit à l’information est en particulier créé pour les personnes fichées en matière pénale. Ces dernières peuvent aussi désormais exercer de façon directe leur droit d’accès auprès du responsable du traitement (sauf exceptions). Elles peuvent ensuite demander la rectification des données les concernant, voire leur effacement.

Les autorités publiques doivent, par ailleurs, respecter un certain nombre d’obligations (production d’une analyse d’impact pour les données sensibles, tenue d’un registre des activités du traitement et d’un journal pour certaines opérations de traitement, désignation d’un délégué à la protection des données, communication de toute violation de données à la CNIL et à la personne concernée, etc.).

De nouvelles règles sur les transferts de données personnelles vers les autorités judiciaires et les forces de l’ordre des pays hors Union européenne sont également posées.

Pour assurer la bonne application du RGPD, la CNIL compte 200 collaborateurs fin 2018, un chiffre qui la place, comparé à la population, dans les autorités de protection les moins bien loties en Europe. L'augmentation des effectifs de la CNIL reste un enjeu important, selon sa nouvelle présidente, Marie-Laure Denis.

Document 4

CNIL

Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » (CNIL)

La Commission nationale de l'informatique et des libertés,

Saisie par le secrétaire d'Etat chargé du numérique d'une demande d'avis concernant les conditions et modalités de l'éventuelle mise en œuvre de l'application « StopCovid » au regard des règles françaises et européennes de protection des données à caractère personnel ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I- 2°e) ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; [...]

Emet l'avis suivant :

La Commission a été saisie par le Secrétaire d'Etat chargé du numérique, le 20 avril 2020, d'une demande d'avis relative aux conditions et modalités de l'éventuelle mise en œuvre de l'application « StopCovid » au regard des règles françaises et européennes de protection des données à caractère personnel [...].

Cette saisine intervient dans le contexte de l'état d'urgence sanitaire liée à l'épidémie de COVID-19, et plus particulièrement de la stratégie dite de « déconfinement ». Dans ce cadre, le Gouvernement envisage de développer et de proposer une application, dénommée « StopCovid », disponible sur ordiphones (smartphones) et autres équipements mobiles. Cette application permettrait d'informer les personnes l'ayant téléchargée du fait qu'elles ont été à proximité, dans un passé proche, de personnes diagnostiquées positives au COVID-19 et disposant de la même application, cette proximité induisant un risque de transmission du virus.

Il s'agirait d'une application de « suivi de contacts » (ou «contact tracing»), et non de suivi des personnes exposées ou diagnostiquées positives au virus, qui reposerait notamment sur l'utilisation de la technologie de communication de proximité « Bluetooth » pour évaluer la proximité entre deux ordiphones, sans recourir à une technologie de géolocalisation. Elle serait utilisée uniquement sur la base du volontariat et ses modalités de mise en œuvre viseraient à minimiser toute identification directe ou indirecte des personnes qui y auraient recours. [...]

Dans ce contexte et sur la base de ces informations, le Gouvernement interroge la Commission sur l'existence ou non, dans le cadre de l'hypothèse de la mise en œuvre d'une telle application, d'un traitement de données à caractère personnel au sens du règlement (UE) 2016/679 du 27 avril 2016 susvisé (ci-après, le « RGPD ») et de la loi « Informatique et Libertés »,

sur l'identification de la base légale d'un tel traitement, au sens des mêmes dispositions, sur la conformité d'un tel dispositif aux règles de protection des données personnelles et, le cas échéant, sur les garanties supplémentaires qu'il conviendrait de prévoir.

Le présent avis de la Commission vise à apporter ces éléments de réponse et à éclairer le Gouvernement sur l'analyse d'une telle application du point de vue du droit de la protection des données à caractère personnel, étant précisé que le déploiement de cette application comme ses modalités exactes de mise en œuvre, sur les plans juridique, technique et pratique, ne sont pas encore arrêtés à ce stade. La Commission demande, après la tenue du débat au Parlement et s'il était décidé de recourir à un tel instrument, qu'elle soit à nouveau saisie pour se prononcer sur les modalités définitives de mise en œuvre du dispositif.

A titre liminaire, la Commission souligne qu'elle a pleinement conscience de la gravité de la situation sanitaire liée à l'épidémie de COVID-19 [...]. Le projet du gouvernement [...] traduit le souhait de ne laisser de côté aucun outil permettant d'endiguer la maladie [...]. En outre, la conception de l'application StopCovid témoigne du souci de protéger la vie privée des personnes, notamment en évitant que soit centralisée dans un serveur une liste des personnes qui se déclarent malades.

Pour autant, il est également du devoir de la Commission de souligner que ce projet pose des questions inédites en termes de protection de la vie privée. Certes, il ne consiste pas à suivre tous les mouvements géographiques des personnes : il ne s'agit pas de tracer les individus de façon continue. Néanmoins, il s'agit d'établir, par la collecte de traces pseudonymes, la liste des personnes dont chaque porteur de l'application a été physiquement proche, pendant une durée circonscrite, parmi tous les porteurs de l'application. Une telle collecte, qui a vocation à s'appliquer à la plus grande partie de la population possible, doit être envisagée avec une grande prudence.

La protection de la vie privée est garantie par la Constitution et d'autres sources de droit ; le fait de collecter les listes de personnes que les individus ont fréquentées y porte une atteinte forte, qui ne peut, le cas échéant, être justifiée que par la nécessité de répondre à un autre principe constitutionnel, à savoir la protection de la santé, qui découle [...] de la Constitution de 1946. Le recours à des formes inédites de traitement de données peut en outre créer dans la population un phénomène d'accoutumance propre à dégrader le niveau de protection de la vie privée et doit donc être réservé à certaines situations exceptionnelles [...].

L'existence de traitements de données à caractère personnel et notamment de données de santé

Le dispositif envisagé à ce jour se compose, d'une part, d'une application mobile qui sera mise à disposition sur les équipements mobiles (notamment ordiphones et tablettes) [...] et, d'autre part, d'un serveur central qui assurera le stockage et la transmission d'un certain nombre de données nécessaires au fonctionnement global du dispositif. Le gouvernement s'interroge sur l'existence de données à caractère personnel traitées dans le cadre du dispositif dès lors, d'une part, que le téléchargement et l'utilisation de l'application ne requerraient pas la fourniture de données directement identifiantes (telles que nom, numéro de téléphone, adresse électronique, etc.) et, d'autre part, que l'application téléchargée, et donc son utilisateur, ne serait identifiée par le serveur central que par un pseudonyme, c'est-à-dire une donnée non identifiante par elle-même. Le protocole décrit dans la saisine repose ainsi sur un système associant à chaque application téléchargée un identifiant aléatoire permanent (ci-après, le pseudonyme permanent) permettant ensuite de créer plusieurs identifiants aléatoires temporaires (ci-après, les pseudonymes temporaires).

En premier lieu, il faut souligner qu'afin de pouvoir informer un utilisateur d'une exposition possible au virus, le serveur central doit vérifier s'il existe une concordance entre les pseudonymes

attribués, lors de son installation, à l'application de cet utilisateur et ceux ayant été transmis au serveur central par l'application d'une autre personne reconnue comme positive. Il en résulte que demeure un lien entre les pseudonymes et les applications téléchargées, chaque application étant elle-même installée sur un terminal, qui correspond généralement à une personne physique déterminée. Du fait de ce lien, la Commission estime que le dispositif traitera des données à caractère personnel au sens du RGPD. En outre, la collecte des pseudonymes temporaires des personnes avec lesquelles l'utilisateur a été en contact pourrait permettre de reconstituer l'ensemble des relations qu'il a eues avec d'autres utilisateurs de l'application. Au regard de ces éléments, la Commission estime que le dispositif projeté est soumis aux règles de protection des données à caractère personnel [...].

En deuxième lieu, le serveur central disposerait de l'information selon laquelle un utilisateur aura ou non reçu une notification lui indiquant qu'il a été exposé au virus. La Commission relève que toute l'architecture du dispositif envisagée tend à ne faire remonter au serveur central que les pseudonymes générés par les applications associées aux personnes avec lesquelles un individu infecté a été en contact, et non le pseudonyme de ce dernier. Elle souligne que ce procédé minimise le risque de réidentification de la personne infectée à l'origine d'une alerte, dans le plein respect des principes de protection des données personnelles.

En troisième lieu, la Commission observe que des données concernant la santé seront traitées par le dispositif. [...]. [L'information] selon laquelle une personne présente un risque suffisamment élevé d'avoir contracté une maladie [...] est, selon l'analyse de la Commission, une donnée concernant la santé et [bénéficie] du régime de protection spécifique de ces données sensibles prévu par le RGPD [...]. Cette information sera présente dans le serveur central. En outre, si des précautions techniques sont prises pour minimiser la possibilité de réidentification de la personne infectée par les personnes qu'elle a côtoyées et qui ont reçu l'alerte, ce risque [...] peut subsister et est à prendre en compte.

Néanmoins, la Commission rappelle que la présence de données à caractère personnel ne fait pas obstacle, par principe, à la mise en œuvre du dispositif. Elle impose cependant de prévoir des garanties adaptées d'autant plus fortes que les technologies sont intrusives, garanties au titre desquelles l'atténuation des possibilités de ré-identification constitue une mesure essentielle.

Un dispositif fondé sur le volontariat

Une finalité limitée à l'alerte de personnes exposées au risque de contamination

La Commission rappelle que le principe de limitation des finalités, consacré par l'article 5(1) (b) du RGPD, est un principe cardinal de la protection des données à caractère personnel : celles-ci ne doivent être utilisées que pour un objectif précis et déterminé à l'avance. Toute autre utilisation des données est en principe interdite.

En l'espèce, ainsi qu'il a été dit, l'objectif de «suivi de contacts» [...] consiste à pouvoir informer un utilisateur de l'application que son téléphone [...] s'est trouvé à proximité, au cours des jours précédents, de celui d'une personne [...] diagnostiquée positive au COVID-19, de sorte qu'il existe un risque qu'il ait été contaminé à son tour. [...]

Une application fondée sur le volontariat des utilisateurs

La Commission prend acte de ce que le projet du gouvernement consiste à mettre à disposition de la population résidant sur le territoire national l'application StopCovid, dont le téléchargement et l'utilisation reposeraient sur une démarche volontaire. Elle considère à ce titre que le caractère volontaire de l'usage, conjugué à une transparence renforcée quant au mode de fonctionnement et aux finalités de traitement, est un élément déterminant pour assurer la

confiance dans le dispositif et favoriser son adoption par une partie significative de la population.

A cet égard, il convient de souligner que le volontariat ne doit pas uniquement se traduire par le choix, pour l'utilisateur, de télécharger puis de mettre en œuvre l'application (installation de l'application, activation de la communication par Bluetooth, voire fait de se déclarer positif au COVID-19 dans l'application) ou la faculté de la désinstaller. Le volontariat signifie aussi qu'aucune conséquence négative n'est attachée à l'absence de téléchargement ou d'utilisation de l'application. Ainsi, l'accès aux tests et aux soins ne saurait en aucun cas être conditionné à l'installation de l'application. L'utilisation d'une application sur la base du volontariat ne devrait pas conditionner ni la possibilité de se déplacer, [...], ni l'accès à certains services, tels que par exemple les transports en commun. [...]

La base légale de l'application StopCovid

L'article 6 du RGPD et l'article 5 de la loi « Informatique et Libertés » prévoient que le traitement de données à caractère personnel n'est possible que dans certaines hypothèses et pour certains motifs limitativement énumérés, qui constituent les « bases légales » possibles du traitement. En l'espèce, le gouvernement s'interroge sur la possibilité de fonder l'application StopCovid sur la base légale du consentement de ses utilisateurs ou, à défaut, sur l'existence d'une mission d'intérêt public de lutte contre l'épidémie de COVID-19.

[La Commission] rappelle que le droit de la protection des données à caractère personnel n'établit aucune hiérarchie entre les différentes bases légales et que la base légale appropriée doit être déterminée uniquement au cas par cas, de manière adaptée à la situation et au type de traitement. Chaque base légale obéit en effet à des conditions spécifiques et emporte des conséquences juridiques particulières pour l'organisme mettant en œuvre le traitement comme pour les personnes concernées par celui-ci. [...]

La Commission relève que la lutte contre l'épidémie de COVID-19 constitue une mission d'intérêt général dont la poursuite incombe en premier lieu aux autorités publiques. [...]

L'admissibilité de l'atteinte à la vie privée par un dispositif de suivi de contacts

La Commission rappelle qu'en vertu de la protection constitutionnelle de la vie privée [...], le gouvernement doit veiller à ce que l'atteinte portée à la vie privée demeure proportionnée à l'objectif poursuivi. Comme il a été indiqué, la protection de la santé constitue également un objectif à valeur constitutionnelle.

D'une part, le respect du principe de proportionnalité se traduira notamment par une collecte et une conservation des données limitées à ce qui est strictement nécessaire, afin de minimiser l'atteinte portée à la vie privée des personnes [...].

D'autre part, il apparaît à la Commission que l'atteinte portée à la vie privée ne sera en l'espèce admissible que si [...] le gouvernement peut s'appuyer sur des éléments suffisants pour avoir l'assurance raisonnable qu'un tel dispositif sera utile à la gestion de la crise [...]. Or, si ce type de dispositif peut potentiellement aider les autorités publiques à surveiller et à contenir la pandémie de COVID-19, en complétant les méthodes traditionnelles de recherche de contacts utilisées pour contenir la propagation des épidémies, il n'en possède pas moins des limites [...].

La Présidente

Marie-Laure DENIS

Document 5

Légifrance

Décision n°MED-2019-036 du 31 décembre 2019 mettant en demeure la société ENGIE

La Présidente de la Commission nationale de l'informatique et des libertés,

[...]

Sur les compteurs communicants LINKY

Le compteur communicant LINKY permet de relever à distance des données de consommation d'électricité plus fines que les compteurs traditionnels, telles que les consommations quotidiennes et à la demi-heure.

Les compteurs LINKY sont actuellement en cours de déploiement par ENEDIS, le gestionnaire du réseau de distribution. ENEDIS prévoit d'installer 35 millions de compteurs communicants d'ici 2021.

Sur la collecte des données de consommation issues des compteurs communicants LINKY

Lors du contrôle effectué le 21 février 2019, la délégation a été informée et a constaté que la société ENGIE recueille le consentement des usagers à la collecte de leurs données de consommation fines par le biais d'une case à cocher.

Plus précisément, l'usager se voit proposer d'activer la collecte de ses données quotidiennes et à la demi-heure via une seule case à cocher autoriser, rédigée ainsi : *Afin d'avoir accès au suivi de consommation détaillée, j'autorise le distributeur d'électricité à collecter et à transmettre à ENGIE les informations de mesure de consommation détaillées, notamment la courbe de charge, passées et à venir du point de livraison.*

En complément, en cliquant sur un lien en savoir plus sur les données collectées , il est précisé Quelles sont les données collectées ? À quoi servent-elles ?

- *Votre consommation et vos index quotidiens en kWh nous permettent d'afficher votre consommation quotidienne en kWh et en euros*
- *La puissance maximale quotidienne nous permettra de vous apporter des conseils tarifaires sur la puissance souscrite*
- *La courbe de charge nous permettra de vous présenter une répartition par usage personnalisé* .

La délégation a été informée que la société ENGIE recueille ce consentement en vue d'afficher dans l'espace client les consommations quotidiennes et à la demi-heure.

Sur les durées de conservation

La délégation a été informée, qu'à l'issue de la résiliation du contrat, la société ENGIE conserve en base active les coordonnées du client (nom, prénom, adresse), ainsi que les données nécessaires à l'exécution du contrat (pièces comptables, factures, les consommations mensuelles, contrat).

La délégation a été informée que ces données sont conservées pendant trois ans en base active puis sont archivées pendant huit ans en archivage intermédiaire.

<u>Les manquements au regard des dispositions du RGPD</u>

Un manquement à l'obligation de disposer d'une base légale pour les traitements mis en œuvre
Selon la granularité de la donnée (données journalières ou données de consommation fines à l'heure ou à la demi-heure) et le rôle du responsable de traitement dans la chaîne énergétique (gestionnaire du réseau de distribution ou fournisseur), la collecte des données de consommation peut nécessiter de recueillir le consentement du client.

Ainsi, le gestionnaire du réseau de distribution (ENEDIS) collecte par défaut les consommations journalières pour permettre à l'usager de consulter gratuitement l'historique de ses consommations, conformément au code de l'énergie. En revanche, il ne collecte pas les données de consommation fines (horaires et/ou à la demi-heure) de manière automatique. En effet, ces données ne peuvent être collectées par le gestionnaire du réseau de distribution qu'avec l'accord de l'usager ou, de manière ponctuelle, lorsqu'elles sont nécessaires à l'accomplissement des missions de service public assignées au gestionnaire du réseau par le code de l'énergie (par exemple, pour l'entretien et la maintenance du réseau ou l'intégration des énergies renouvelables).
En ce qui concerne les fournisseurs d'énergie tels que la société ENGIE, ces derniers ne peuvent collecter les consommations quotidiennes et horaires et/ou à la demi-heure qu'avec le consentement de l'abonné.
Pour être valable, le consentement doit être *libre, spécifique, éclairé et univoque* , en application de l'article 4, paragraphe 11, du RGPD. [...]
S'agissant du caractère spécifique du consentement, il résulte du RGPD que la personne concernée doit être en mesure de donner son consentement de façon indépendante et distincte pour chaque finalité poursuivie. Ainsi, le considérant 43 prévoit que *le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce* […]

S'agissant du caractère éclairé du consentement, il ressort des lignes directrices du G 29 sur le consentement que *pour que le consentement soit éclairé, il est nécessaire d'informer la personne concernée de certains éléments cruciaux pour opérer un choix, [tels que] (…) (ii) la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité, (iii) les (types de) données collectées et utilisées* (p. 15).

En l'espèce, la délégation a été informée et a constaté que la société ENGIE recueille le consentement des usagers à la collecte de leurs données de consommation quotidiennes et à la demi-heure par le biais d'une seule case à cocher, et ce pour deux opérations de traitement distinctes, à savoir l'affichage dans l'espace client des consommations quotidiennes et l'affichage dans l'espace client des consommations à la demi-heure.

Ainsi, le consentement pour le traitement des données quotidiennes emporte automatiquement consentement pour le traitement des données à la demi-heure. Pourtant, les opérations de traitement évoquées ci-dessus sont distinctes et indépendantes les unes des autres : ainsi, un usager peut souhaiter consulter l'historique de ses consommations journalières, sans nécessairement souhaiter accéder à ses données à la demi-heure.

En conséquence, le traitement des données à des fins d'affichage des index journaliers et celui plus complet et détaillé des données à la demi-heure constituent des opérations de traitement distinctes, de sorte que l'usager devrait pouvoir donner un consentement pour chacune d'entre elles et activer

la collecte des index journaliers, sans nécessairement devoir accepter d'activer de manière corrélée celle de la courbe de charge.

Il résulte de l'ensemble de ces éléments que le consentement des utilisateurs n'est ni spécifique ni suffisamment éclairé, de sorte que les modalités de son recueil ne sont pas conformes [au RGPD].

Un manquement à l'obligation de définir une durée de conservation proportionnée à la finalité du traitement

En application de l'article 5, paragraphe 1, e) du RGPD, *les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* .
En l'espèce, la société ENGIE a informé la délégation, qu'à l'issue de la résiliation du contrat, elle conserve en base active les coordonnées du client (nom, prénom, adresse), ainsi que les données nécessaires à l'exécution du contrat (pièces comptables, factures, les consommations mensuelles, contrat). Ces données sont conservées pendant trois ans en base active puis sont placées pendant huit ans en archivage intermédiaire.

Or, si les coordonnées du client peuvent être conservées en base active pendant trois ans à l'issue de la résiliation du contrat à des fins de prospection commerciale, les données de consommation mensuelles ne sont pas nécessaires à cette finalité, de sorte que leur conservation est excessive.

Dès lors, la conservation en base active des consommations mensuelles pendant trois ans à l'issue de la résiliation du contrat est excessive au sens de l'article 5, paragraphe 1, e) du RGPD.

En conséquence, la société ENGIE, sise 1 place Samuel de Champlain à Courbevoie (92400), est mise en demeure sous un délai de trois (3) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :
- recueillir un consentement libre, spécifique, éclairé et univoque préalablement à la collecte des données de consommation quotidiennes et à la demi-heure de ses clients, y compris de ceux dont les données sont déjà enregistrées, par exemple, en mettant en place une case à cocher pour chaque opération de traitement et, à défaut, supprimer lesdites données collectées, conformément aux articles 4, paragraphe 11, et 6, paragraphe 1, a) du RGPD ;
- définir et mettre en œuvre une politique de durée de conservation des données qui n'excède pas la durée nécessaire aux finalités pour lesquelles ces données sont collectées et, au besoin, purger les données non conformes à cette politique de durée de conservation, conformément aux dispositions de l'article 5, paragraphe 1, e) du RGPD ;
- justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.
À l'issue de ce délai, si la société ENGIE s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la société ENGIE ne s'est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des sanctions prévues par l'article 20 de la loi du 6 janvier 1978 modifiée.

La Présidente

Marie-Laure DENIS

Document 6

Village de la Justice – Octobre 2017

Données personnelles : anonymisation ou pseudonymisation ?

L'anonymisation permet d'échapper à la réglementation sur les données personnelles. Néanmoins les techniques existantes, examinées par le G29 dès 2014 (avis 05/2014) sont complexes et rarement efficaces à 100%

A l'heure où la collecte et le traitement des données personnelles deviennent des incontournables de la vie des affaires, l'anonymisation, comme moyen d'échapper à la réglementation sur les données personnelles, est de plus en plus envisagée.

L'anonymisation est une technique appliquée aux données à caractère personnel afin d'empêcher leur identification de façon irréversible. En l'absence d'irréversibilité, les techniques mises en place relèvent essentiellement de la pseudonymisation, laquelle, en réduisant simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée, ne permet pas de se soustraire à la réglementation relative aux données personnelles.

I. L'anonymisation

1.1. Approche générale de la notion d'anonymisation

L'anonymisation offre une double garantie : celle de la sécurisation de l'exploitation des données personnelles et celle du respect des droits fondamentaux des personnes dont les données personnelles sont traitées.
L'appréciation du caractère irréversible de l'anonymisation, lequel offre la possibilité ou non d'identifier une personne, dépend « des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le RT, soit par une autre personne ».
Dans le cas où un responsable de traitement transfère certaines données non identifiantes mais n'efface pas les données personnelles de ses systèmes, il doit être considéré que les données transmises constituent encore des données à caractère personnel, et ce même si les identifiants directs ont été supprimés.
Dans ce type de cas, seule la transformation des données en données statistiques agrégées à un niveau supérieur assure une réelle anonymisation, par exemple « le samedi, dans la boutique Y, le nombre de visiteurs est supérieur de 350 % à celui du lundi ».

Au regard de la Loi Informatique et Libertés, l'anonymisation a vocation à être utilisée à deux stades différents :
- **l'anonymisation à bref délai** : dans ce cas, le processus d'anonymisation suit immédiatement la collecte des données (quelques minutes). Toutefois, du fait de l'existence d'un temps, bien que bref, entre la collecte des données et leur anonymisation réelle, la CNIL reste compétente pour autoriser la mise en place du procédé d'anonymisation. Dans la mesure où l'anonymisation à bref délai permet à l'entreprise de se voir exemptée d'appliquer certaines règles de la loi de 1978 (notamment en matière d'information préalable des personnes), la CNIL appréciera l'efficacité du procédé envisagé afin de garantir la sécurité des personnes dont les données personnelles sont traitées.
- **l'anonymisation « ultérieure »**, en tant que second traitement des données : le processus d'anonymisation se fera un certain temps après la collecte, imposant dès lors à l'entreprise le respect de toutes les exigences légales et règlementaires en matière de données personnelles, jusqu'à ce qu'elles soient effectivement anonymisées.

[...]

1.3. Degré d'efficacité des techniques d'anonymisation

Rendre impossible l'identification d'une personne ne consiste pas en la seule suppression des éléments directement identifiants la concernant. Il existe en effet une série de procédés permettant d'exploiter un ensemble de données afin d'identifier un ou des individus.
L'appréciation du degré d'efficacité d'une technique d'anonymisation s'apprécie en imaginant qu'une personne malveillante pourrait procéder à des recoupements relevant de ces trois situations :
- **L'individualisation** : correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données ;
- **La corrélation** : consiste dans la capacité de relier entre eux, au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes).
Si une attaque permet d'établir (par exemple, au moyen d'une analyse de corrélation) que deux enregistrements correspondent à un même groupe d'individus, mais ne permet pas d'isoler des individus au sein de ce groupe, la technique résiste à l'« individualisation », mais non à la corrélation ;
- **L'inférence** : est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs.

Une solution résistant à ces trois risques offrirait par conséquent une protection fiable contre les tentatives de réidentification, même si aucune technique n'est infaillible.

II. La pseudonymisation

L'article 4 du RGPD définit la pseudonymisation de la manière suivante : « (…) on entend par pseudonymisation : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. »

2.1. Approche de la notion de pseudonymisation

La pseudonymisation permet toujours d'identifier un individu grâce à ses données personnelles car elle consiste simplement à remplacer un attribut par un autre au sein d'un enregistrement. En effet, le considérant 26 du RGPD rappelle que « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».

Le Règlement communautaire qui entrera en vigueur le 25 mai 2018 évoque beaucoup la notion de pseudonymisation comme technique de respect du principe du Privacy By Design et de la minimisation des données (article 25 du RGPD notamment). [...]

Les sanctions prévues par le RGPD (20 millions d'euros d'amende ou 4% du chiffre d'affaires mondial) vont sans nul doute inciter de nombreuses sociétés à recourir à l'anonymisation dès qu'elles le pourront.

Document 7

Le Monde (28/05/2017)

Des données personnelles très convoitées

Le business des données personnelles sur Internet est en plein boom, mais les GAFA[1] trustent 95 % du marché. Est-il encore possible de réguler le secteur pour protéger la vie privée des citoyens ?

Tous surveillés. Les traces que l'on laisse derrière soi sur le Net – préférences idéologiques, culinaires ou sportives, achats, peines de cœur, soucis de santé… – sont devenues une industrie extrêmement lucrative. Selon le cabinet IDC, le marché des données des citoyens de l'Europe des Vingt-Huit s'élevait à 60 milliards d'euros en 2016, et devrait atteindre 80 milliards en 2020.

Et ce n'est que la partie émergée de l'iceberg. Indirectement, c'est-à-dire en tenant compte du chiffre d'affaires supplémentaire et des emplois générés par les utilisateurs de ces informations, la valeur de « l'économie européenne des données » s'élèverait à quelque 300 milliards d'euros en 2016, et pourrait atteindre 430 milliards en 2020. C'est le pétrole du XXIe siècle, assurent les plus enthousiastes. Mais un pétrole qui connaît ses premières marées noires.

Quelques condamnations viennent de rappeler la part d'ombre des données : celle de WhatsApp pour avoir tenté de forcer ses utilisateurs à partager leurs données avec sa maison mère, Facebook. Dans la foulée, celle de Facebook pour avoir juré à la Commission européenne, en 2014, que ce partage de données serait techniquement impossible. Et le 17 mai, c'est la Commission nationale de l'informatique et des libertés (CNIL) qui condamne Facebook pour atteinte à la vie privée, à travers six manquements graves à la loi informatique et libertés, dont « la combinaison potentiellement illimitée de toutes les données des utilisateurs… sans qu'ils puissent mettre fin au suivi massif dont ils sont l'objet ».

Collecte massive

Les mises en cause des géants du Net ne sont certes pas nouvelles, et les sanctions bien modestes. Mais elles se multiplient, et touchent aujourd'hui au cœur du système : la collecte de ces informations sensibles et leur traitement.

Les risques que Google, Apple, Facebook ou Amazon (ou GAFA) font courir à notre société sont jugés tels qu'ils suscitent une volonté de remise à plat musclée des règles par les autorités. Avec pour objectif de redonner aux individus la maîtrise de leurs données personnelles, afin qu'ils sachent enfin ce qui en est fait et qu'ils puissent donner, ou non, leur accord de manière libre et éclairée.

Cette révision met en émoi tous les acteurs qui vivent de cette collecte massive, souvent à l'insu des individus, et qui suivent à la trace leur moindre requête, like et autres partages, pour réaliser un profilage commercial de plus en plus fin, dans le but de personnaliser les messages qui leur sont adressés par tous les commerçants et fournisseurs de services pullulant sur la Toile. A commencer

1 L'acronyme GAFA désigne les cinq entreprises géantes du numérique que sont Google, Apple, Facebook et Amazon

par les acteurs de la publicité en ligne, le plus gros consommateur de données personnelles à ce jour.
Dans un an, le nouveau règlement général européen sur la protection de la vie privée, RGDP, entre en vigueur. Il impose une application beaucoup plus stricte des droits existants, avec des sanctions très lourdes, jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires.

Inquiétude des acteurs

« Voilà qui commence à être dissuasif et va contraindre chacun à respecter des règles qui ne l'étaient que rarement », reconnaît Me Alain Bensoussan, spécialiste du droit des technologies.
Et le texte apporte quelques changements majeurs : la notion de « donnée personnelle » est élargie à « tout ce qui permet d'identifier directement ou indirectement les personnes », y compris l'adresse IP de l'ordinateur et les cookies, ces petits fichiers posés par les collecteurs de données sur le navigateur des internautes pour enregistrer leur activité. Et ces données ne pourront plus être collectées qu'avec le consentement « libre, éclairé, explicite et univoque » des individus.

Et le texte apporte quelques changements majeurs : la notion de « donnée personnelle » est élargie à « tout ce qui permet d'identifier directement ou indirectement les personnes », y compris l'adresse IP de l'ordinateur et les cookies, ces petits fichiers posés par les collecteurs de données sur le navigateur des internautes pour enregistrer leur activité. Et ces données ne pourront plus être collectées qu'avec le consentement « libre, éclairé, explicite et univoque » des individus.

En clair, la collecte massive opérée en douce avec un accord donné une fois pour toutes par une case précochée, dite d'« opt-out », et pour des finalités très générales, c'est fini ! Désormais, l'accord devra être acquis par une case « à cocher », dite d'« opt-in », pour des finalités précises et claires, y compris quand les données sont combinées avec d'autres. Il devra être révocable d'un clic, et à tout instant. Et si l'internaute n'y consent pas, l'accès au service ne pourra pas lui être refusé.

L'inquiétude des acteurs est d'autant plus forte que ces obligations s'imposeront désormais à toute la chaîne : du collecteur à l'annonceur, en passant par tous ceux qui manipulent des données personnelles pour « toucher le bon consommateur au bon moment », dans une chaîne ultracomplexe qui comprend aussi des e-mailers, des acheteurs d'espace automatisés, des éditeurs de logiciels de CRM (gestion de la relation client), etc.

Un profilage de plus en plus comportemental
[...]
Les data brokers[2] sont déjà dans le viseur de la CNIL, qui a mené 50 contrôles en 2016. D'abord parce que les internautes ne savent souvent rien des données utilisées par les entreprises et de l'usage qui en sera fait. Ils ignorent qu'ils font en réalité l'objet d'un profilage qui n'est plus seulement sociologique, mais de plus en plus comportemental – distinguer par exemple les bons et les mauvais payeurs –, et qui peut être à l'origine d'une discrimination invisible.

[...]

2 Courtiers en données qui agrègent des fichiers et bases disparates pour vendre des profils à des sociétés

Document 8

Next Inpact (29/08/2018)

« Alerte attentat » : après l'application, voilà le traitement de données personnelles SAIP

Au Journal officiel, l'Intérieur a publié un arrêté pour autoriser la création d'un traitement automatisé d'alerte des populations. Ce système préfigure l'arrivée d'un nouveau SAIP, abandonné en mai dernier. Contactée, la Cnil refuse de nous communiquer son avis motivé, qui n'a pas été publié malgré une obligation légale.

Lancée à l'occasion de l'Euro 2016, l'application SAIP (système d'alerte et d'information des populations) a finalement été délaissée deux ans plus tard par l'exécutif.

L'oraison funèbre a été nourrie en août 2017 par un rapport au Sénat qui jugeait cette app « imparfaite », avec des « bugs résiduels », issue d'un produit conçu « dans l'urgence » avec « des défaillances persistantes ». L'auteur du rapport, le sénateur Jean-Pierre Vogel, critiquait surtout la doctrine d'emploi, s'agissant d'alertes pas toujours déclenchées par les autorités.

À la place, l'exécutif a finalement prévu de privilégier les réseaux sociaux, en particulier Google, Facebook et Twitter. Sur ce dernier, le compte @Beauvau_Alerte a été calibré pour informer quiconque « d'un événement majeur de sécurité publique ou civile survenant en France ».

De même, a été envisagée la possibilité d'utiliser le Safety Check de Facebook, suite à un partenariat technologique. Sur Google, un bandeau d'alerte est censé mettre en avant les contenus diffusés par les autorités. Un système similaire doit être programmé sur France Télévisions, Radio France, la RATP et Vinci Autoroute, histoire d'informer les non-internautes. (le communiqué du ministère).

SAIP v2, en cas d'événements graves, imminents ou en cours de réalisation

Ce matin, au Journal officiel, un arrêté vient créer « un traitement de données à caractère personnel relatif au système d'alerte et d'information des populations ». Il laisse donc présager le déploiement effectif du nouveau système d'alerte.

Concrètement, il autorise le ministère de l'Intérieur et plus précisément la direction générale de la sécurité civile et de la gestion des crises, à mettre en œuvre un traitement dont la finalité est « de permettre la diffusion des mesures d'alerte et d'information à destination de la population, à la demande d'une autorité de police administrative, en cas d'événements graves, imminents ou en cours de réalisation, susceptibles de porter atteinte à l'intégrité physique des personnes ».

Le texte a été publié sur le fondement de l'article 26 de la loi de 1978 sur l'informatique et les libertés. Celui-ci autorise en effet ces traitements de données personnelles mis en œuvre pour le compte de l'État et qui intéressent la sûreté, la défense ou, comme ici, la sécurité publique.

Deux traitements de données personnelles, un large accès

Peu bavard sur le mode opératoire, le texte signé Gérard Collomb permet l’enregistrement des données des agents habilités à accéder aux données et informations du traitement (nom, prénom, qualité, adresse, etc.) Un deuxième fichier s’intéresse cette fois aux destinataires de ces mêmes flux, que ce soit des personnes physiques ou morales (nom, prénom, adresse).

Plusieurs entités se voient reconnaître un droit d’accès à ces informations : le premier ministre, le ministre de l'Intérieur, les préfets, les maires, des agents de la direction de la sécurité civile et de la gestion des crises, mais encore les agents des services d'incendie et de secours dans leur zone de compétence. L’arrêté prévoit classiquement une traçabilité dans chacune des opérations, que ce soit pour la création, la consultation, la mise à jour et les suppressions éventuelles.

Document 9

Commission Nationale de l'Informatique et des Libertés (23/05/2019)

1 an de RGPD : une prise de conscience inédite

Le RGPD, entré en application il y a un an, a créé une dynamique remarquable pour les particuliers et les professionnels. La CNIL a reçu un nombre record de plaintes et elle développe de nouveaux outils de conformité pour garantir à tous la protection des données personnelles.

Retour sur une année exceptionnelle

L'entrée en application du RGPD a marqué une forte prise de conscience des enjeux de protection des données, en France comme en Europe. Cela s'est traduit pour les particuliers, sur la période de mai 2018 à mai 2019, par :

- une augmentation considérable des plaintes adressées à la CNIL : plus de 11 900 plaintes en France (+ 30 %) et 144 376 plaintes au niveau européen ;
- une coopération européenne engagée et opérationnelle entre les CNIL européennes sur 1 013 procédures concernant plusieurs milliers de personnes, dont plus de 800 dans lesquelles la CNIL est impliquée.

70 % des Français se disent aujourd'hui plus sensibles aux problématiques de protection des données.
Sondage IFOP réalisé en avril 2019 sur un échantillon de 1 000 personnes, représentatif de la population française de 18 ans et plus, selon la méthode des quotas.

Cette prise de conscience se manifeste également chez les professionnels, qui s'approprient progressivement les nouveaux dispositifs du RGPD :

- 2 044 notifications de violation de données en France et 89 271 au niveau européen ;
- plus de 19 000 délégués à la protection des données (personnes physiques ou morales) ont été désignés par plus de 53 000 organismes ;
- un afflux de demandes d'information de la part des professionnels souhaitant s'approprier ce nouveau cadre qui ont identifié la CNIL comme une source d'information de référence.

Témoin de cette mobilisation croissante des professionnels et particuliers sur la protection des données, le site de la CNIL a cumulé plus de 8,1 millions de visites depuis un an.

RGPD, an II : réussir le RGPD, clé de voûte d'un numérique de confiance

L'année 2019 sera décisive pour crédibiliser le nouveau cadre juridique et transformer cet ambitieux pari européen en succès opérationnel. Les attentes de la société civile et des acteurs économiques sont très fortes et ce modèle suscite des intérêts à travers le monde entier.

L'année 2019 marque l'achèvement de la transition vers le RGPD. Il est essentiel que, désormais, les organismes appliquent complètement le nouveau texte. Dans l'instruction des plaintes et dans ses contrôles, la CNIL vérifiera donc pleinement le respect des nouvelles exigences. Elle en tirera au besoin toutes les conséquences, y compris en termes de sanction. Mais comme par le passé, elle fera preuve de discernement dans son action répressive, en tenant compte, notamment, de la bonne foi des organismes.

Pour soutenir les opérateurs dans leur dynamique de conformité et réussir la mise en œuvre du RGPD, la CNIL va amplifier ses actions d'accompagnement à destination des professionnels :

- la sensibilisation à destination des collectivités territoriales, via un plan d'accompagnement qui se matérialise par la diffusion d'un guide pratique de sensibilisation à destination des plus petites collectivités, de fiches thématiques (téléservices, sécurité, DPO et collectivités, etc.) et d'un module dédié dans sa formation en ligne ouverte à tous ;
- l'accompagnement des start-ups grâce à des contenus dédiés sur le site de la CNIL : des contenus pour faire du RGPD un atout ainsi qu'un kit développeur ont déjà été publiés ;
- l'élaboration de nouveaux cadres de référence sous la forme de référentiels (gestion des ressources humaines, gestion de la relation client, gestion des impayés, alertes professionnelles), règlements type ou listes de traitements non soumis à une analyse d'impact obligatoire ;
- un dialogue étroit avec les professionnels, avec la sensibilisation de « têtes de réseaux » pour favoriser la montée en compétences de tous les secteurs et l'appui maintenu aux délégués à la protection des données.

Les outils pratiques au service des particuliers et professionnels

La CNIL a élaboré ces derniers mois de nombreux outils pratiques d'aide à la conformité qui restent à disposition de tous sur son site, et qu'elle continuera à enrichir et compléter :

- pour les personnes souhaitant exercer leurs droits ou poser une question à un organisme qui gère leurs données : la CNIL leur permet de vérifier si cet organisme a désigné un délégué à la protection des données (DPO) et met à leur disposition ses coordonnées publiques via un moteur de recherche dédié ;
- une formation en ligne ouverte à tous (MOOC) sur le RGPD depuis mars 2019, déjà suivie par plus de 35 100 personnes dont 6 900 ayant obtenu une attestation de réussite ;
- un modèle de registre des activités de traitement, qui permet de recenser l'ensemble des traitements de données et de disposer d'une vue d'ensemble des actions autours des données personnelles ;
- un logiciel libre pour mener une analyse d'impact sur la protection des données (AIPD), obligatoire pour certains traitements.