TEMPS 2

Etablir la confiance dans une société connectée

Le cadre législatif de la confiance

1

Sophie Nerbonne, Directrice de la Direction de la conformité
de la Commission nationale de l'informatique et des libertés (CNIL)

La CNIL a été créée il y a plus de 30 ans par la loi du 6 janvier 1978 dite « loi informatique et libertés » dont les principes de base se sont avérés tout à la fois robustes et flexibles alors que le contexte technologique a été bouleversé et que nous sommes entrés dans une nouvelle ère imposant de multiples changements.

La CNIL s'adapte à ce nouvel environnement tant dans son organisation que ses méthodes de travail. Elle entend être partie prenante de l'écosystème de notre société numérique. Ainsi, elle s'est notamment dotée d'un service de l'expertise informatique qui est un des plus importants parmi les CNIL européennes, d'un laboratoire pour y tester des produits innovants, d'une équipe de prospectivistes et d'une direction de la conformité. Cette direction de la conformité est tournée vers les publics professionnels, tant du secteur public que privé, administrations et entreprises qui mettent en œuvre des traitements de données à caractère personnel afin de mieux les accompagner dans le développement de leurs projets. Pour une conformité à la loi qui soit opérationnelle et non pas seulement administrative, nous déployons de nombreux services et outils.

La présente communication va être structurée selon quatre grandes thématiques :

- le rappel du cadre juridique actuel de la protection des données personnelles,
- les outils de conformité permettant d'assurer sécurité et prévisibilité juridique indispensable pour un système juridique efficace,
- le projet de règlement européen qui dessine le paysage du XXIe siècle en matière de pro-

tection des données personnelles ; ce texte est dans sa dernière ligne droite, puisque le trilogue vient de s'ouvrir entre Parlement européen, Conseil et Commission européenne pour une adoption envisagée à la fin de l'année,

- Enfin, la protection des données qui génère la confiance peut également être un élément de compétitivité, contrairement à l'idée reçue selon laquelle « la réglementation freine l'innovation technologique ».

La protection des données personnelles en cinq règles d'or

Le cadre juridique actuel remonte à 1978, année de naissance de la loi informatique et libertés en France. A l'origine de cette loi, on retrouve le numéro d'identification au registre de l'Insee qui parle à chacun d'entre vous. Cette loi a été votée en réaction à un projet de l'administration malencontreusement baptisé SAFARI et reposant sur l'interconnexion de tous les fichiers publics sur la base du numéro de sécurité sociale ou NIR. Depuis lors, ce ne sont pas seulement les administrations, mais aussi les grands acteurs privés qui sont en mesure d'avoir une connaissance approfondie de notre vie privée. Nous sommes désormais dans un monde de « traçabilité généralisée » des personnes, à la fois dans le temps et dans l'espace. Pour préserver la vie privée et le respect des droits et libertés individuelles et publiques, permettre à chacun d'entre nous de garder la maîtrise de nos données, le législateur a défini un cadre reposant sur cinq principes, cinq règles d'or qui se sont avérées singulièrement robustes, certainement du fait de leur flexibilité.

Avant de passer en revue ces cinq règles d'or de la protection des données, précisons que ce qui existe au niveau français existe aussi au niveau européen : la protection des données personnelles est consacrée par la charte des droits fondamentaux de l'Union européenne. Ce sont des droits personnels, à l'instar de la liberté de penser, la liberté d'opinion, la liberté d'aller et venir. Par rapport au débat sur la patrimonialité de ces données, l'ensemble des autorités de protection des données européennes a pris position sur le fait que ce ne sont pas des droits patrimoniaux. Quand bien même les données auraient été cédées, même soi-disant gratuitement en échange d'un service, l'individu continue à pouvoir exercer ses droits (modification, opposition,…). Il garde la maîtrise et le droit de demander à s'opposer à figurer dans le traitement, à ce que les informations soient supprimées, dans les conditions définies par la loi. Ce sont des droits liés à la personne qui ne peuvent être aliénés.

La protection des données peut se résumer à cinq grands principes portant sur les modalités de collecte et de traitement des données qui permettent d'identifier, directement ou indirectement des individus. Ces principes sont bien sûr bousculés par l'environnement technologique qui est actuellement complètement différent de celui de 1978, et même de 2004, époque à laquelle la loi a été sensiblement remaniée. Cependant le règlement européen, sur le point d'être adopté reprend ces principes, qu'il est donc important de bien d'avoir en tête.

Le premier d'entre eux est le principe de finalité : à quoi va servir la collecte des données, quelle est la finalité poursuivie par le traitement ? sachant qu'elle doit être explicite, légitime, et déterminée. Prenons en illustration la première demande d'autorisation reçue par la CNIL en matière de « *pay as you drive* », ces dispositifs que les assureurs utilisent en vue de modifier le montant de votre prime d'assurance en fonction de la façon dont vous conduisez.

Au passage, cela montre que la réflexion sur les objets connectés ne date pas d'hier. Nous nous étions interrogés dès 2005 sur ce sujet. Il s'agissait de baisser la prime des jeunes assurés automobile en échange de l'installation d'une boîte noire permettant de savoir que le jeune assuré ne conduirait pas le samedi soir, période de forte sinistralité, qu'il ne dépassait pas les vitesses légales autorisées et s'arrêtait toutes les deux heures. Or, un assureur qui contrôle si les vitesses légales sont dépassées n'est plus un assureur mais un gendarme. Cela ne relève pas de sa sphère de compétences. Quand bien même l'objectif poursuivi, à savoir limiter les accidents est légitime, la collecte de données relatives à des infractions routières n'est pas autorisée par la loi et c'est à ce titre que la CNIL avait alors refusé la mise en place de ce dispositif.

Le deuxième principe repose sur la pertinence des informations collectées, plus précisément la **pertinence, l'adéquation et le caractère non disproportionné des données au regard de la finalité poursuivie**. Ce principe trouve une déclinaison pratique en fonction de chaque cas d'espèce, de même que celui sur la **durée de conservation des données qui soit limitée en raison là encore de**

la finalité du traitement, ce qui n'empêche pas une utilisation à des fins statistiques dès lors que les données sont anonymisées. Un dialogue se noue avec la CNIL afin de justifier de cette pertinence de la donnée ou de sa conservation. On peut citer par exemple, dans les grilles d'analyse de *credit scoring* des établissements de crédit, les critères utilisés ; parmi eux, la CNIL, dans le cadre de son pouvoir d'autorisation, avait refusé la prise en compte du critère relatif à la différence d'âge entre les co-emprunteurs ou de la possession d'un téléphone portable, variables dont la pertinence et le caractère proportionné au regard de la finalité d'octroi d'un crédit à la consommation n'avaient pas été démontrés par l'organisme de crédit.

Le quatrième principe est tout aussi essentiel**. Il concerne la sécurité des données**. A l'heure actuelle, avec des traitements ouverts du fait du recours à internet, au cloud, les questions de faille de sécurité sont de plus en plus cruciales. Comment préserver la sécurité des données, éviter que des tiers non autorisés ne puissent y accéder ?

Enfin – et j'aurais pu commencer par ce principe fondamental –, **le responsable de traitement doit respecter les droits des personnes** : un droit à l'information sur ce qui est fait avec les données collectées, un droit d'accès à ces informations, complétés par la capacité de s'opposer ou de consentir à leur collecte en fonction des cas, d'en demander la rectification également. Néanmoins, il faut bien reconnaître que ces droits sont très peu exercés à l'heure actuelle. Ils le sont surtout dans un contexte contentieux, que ce soit avec son employeur, son opérateur télécom ou sa banque, ou dans le contexte particulier d'un cas pratique donné à des étudiants en droit dans le cadre de leur cours sur la protection des données personnelles.

Pour mettre en œuvre ces 5 règles d'or, la CNIL a conçu des outils de conformité adaptés au secteur professionnel concerné. Par ailleurs, les correspondants « informatique et libertés » désignés par les responsables de traitement soit en leur sein, soit de façon mutualisée pour de petits organismes, constituent des acteurs précieux dans la mise en œuvre effective de la loi.

Des outils de conformité collant à la réalité des besoins des professionnels

La CNIL entend bâtir ses outils de conformité à partir des besoins des professionnels. Dans la

perspective d'une mise en œuvre effective des principes susmentionnés, elle élabore ainsi depuis deux ans des « packs de conformité » qui sont tout à la fois une méthode de travail et un nouvel outil de régulation.

S'agissant tout d'abord de la méthode de travail, il s'agit d'interagir avec les professionnels, mais aussi avec les pouvoirs publics, les autorités de régulation sectorielle éventuellement concernées et les associations d'usagers, secteur d'activité par secteur d'activité. En 2014, nous avons pu avancer dans trois secteurs, représentatifs des différentes situations où des professionnels se sont rendu compte qu'il leur était nécessaire de se mettre en conformité.

Le premier de ces trois cas concerne le secteur des assurances. Secteur très réglementé et pour lequel la conformité fait partie de son ADN. Les associations professionnelles représentant l'ensemble des branches d'activité ont posé sur la table l'ensemble des difficultés rencontrées dans l'application de la loi, pour que nous puissions bâtir des outils juridiques répondant à ces questions. Nous avons utilisé les vecteurs juridiques qui sont à notre disposition, normes simplifiées et autorisations uniques et le travail d'écriture s'est fait en concertation étroite avec les professionnels concernés. Ce travail de corégulation s'est avéré essentiel pour permettre l'appropriation par les professionnels de ces règles. Ils parlent désormais de « leur » pack de conformité et le déclinent dans l'ensemble de leur réseau. Les bonnes pratiques et recommandations sur

ce que l'on peut collecter et traiter en tant qu'assureur ont ainsi été clarifiées. Par ailleurs, deux réunions par an permettent de mettre à jour ce corpus de règles.

Le deuxième cas concerne le logement social : à la suite de plaintes, de contrôles et de sanctions prises par la CNIL, le secteur a eu la volonté de se mettre à hauteur en termes de respect de la loi et cette démarche de régularisation a débouché sur un pack de conformité dans le logement social pour rappeler là encore quelles sont les règles de collecte et de traitement des données.

Le troisième exemple est celui des compteurs communicants et plus précisément des services déployés en aval des compteurs dits « intelligents » dont le déploiement débute, et qui enregistrent toute la consommation électrique dans un domicile – rien de plus personnel que ce qui se passe au sein du foyer. Les industriels de la fédération des industries électriques, électroniques et de communication (FIEEC) ont travaillé avec la CNIL sur les garanties offertes par les produits domotiques en mode « *privacy by design* », c'est-à-dire en intégrant le plus en amont possible dans la technologie, les éléments relatifs à la protection des données. La FIEEC a considéré que la valeur ajoutée de ce travail commun consistait dans le facteur de confiance en résultant, ce qui constitue un atout concurrentiel très intéressant pour ses membres. Bien évidemment, la FIEEC a souhaité que ce travail soit capitalisé au niveau européen, ce que représente la dimension la plus adaptée à ces travaux.

Par ailleurs, il faudrait également parler des labels délivrés par la CNIL et aussi de la mise en place de « règles internes d'entreprises » en matière de transferts de données hors de l'Union européenne, dites « BCR » qui sont des outils de conformité très utiles. Ces outils sont repris largement dans le projet de règlement européen ainsi d'ailleurs que les correspondants « informatique et libertés ».

Une dimension européenne incontournable

Pour la CNIL, l'adoption du règlement européen envisagé depuis 2012, apparait essentiel pour créer un cadre unique en matière de protection des données pour tous les pays d'Europe. Ce n'est en effet pas encore le cas à l'heure actuelle puisque des différences, tant en termes de pouvoirs et missions des différentes autorités nationales que des doctrines établies, découlent des transpositions nationales qui ont été faites de la directive européenne de 1995. Le règlement européen doit constituer un cadre juridique efficace porteur de sécurité et de prévisibilité juridique. Ce cadre unique va aussi permettre de rétablir l'équilibre vis-à-vis des grands acteurs, notamment américains, qui ont pris une longueur d'avance dans le déploiement de modèles économiques faisant fi de la protection des données personnelles. Certains considèrent, et à juste titre je pense, que nous arrivons à la fin d'une première période, qui a été en quelque sorte le Far West du numérique, période au cours de laquelle chacun a amoncelé des informations de façon massive. Il est temps de « civiliser » ces modes de collecte et de traitement des données non respectueuses des droits des personnes et de donner à celles-ci plus de maîtrise et de contrôle de l'usage de leurs données.

Le règlement européen prévoit ainsi de nouveaux droits pour les personnes, tels que le droit à la portabilité des données, qui vont au-delà de ceux qui ont été indiqués. Ces droits plus classiques se trouvent confortés, renforcés comme par exemple le droit de consentir. A l'heure actuelle, comment considérer que le consentement est éclairé et explicite lorsqu'on ne sait pas à quoi on consent, faute d'une information adaptée. Par ailleurs, lorsque cette information est faite, un travail de sensibilisation est nécessaire afin de ne pas accepter, au moment où nous téléchargeons une application sur notre téléphone portable par exemple, les conditions générales d'utilisation sans vérifier ce qui va être fait de nos données.

Ces droits fondamentaux qui existent au niveau européen se diffusent également dans le reste du monde. Il existe une association des autorités nationales francophones de protection des données, ce qui permet d'étendre et d'associer à la réflexion un certain nombre de pays notamment africains. La même structure existe pour les pays hispanophones en Amérique Latine. Aux Etats-Unis, la protection des consommateurs est prise en considération dans un cadre juridique établi non pas de façon globale mais sectorielle.

La réglementation « informatique et libertés », un facteur de confiance nécessaire pour une innovation durable

Le cadre juridique protégeant les données personnelles est critiqué par les partisans d'une déréglementation qui opposent réglementation et innovation. Or, la réglementation est non

seulement un gage de sécurité juridique et de limitation des risques mais elle permet aussi d'accroitre le capital de confiance vis-à-vis des personnes concernées. Elle constitue ainsi un facteur de compétitivité pour les entreprises qui peuvent se prévaloir de pratiques vertueuses et de mise en place d'outils ou d'acteurs tels que les correspondants Informatique et Libertés, les labels ou les règles internes d'entreprise qui témoignent de leur engagement pour un déploiement d'innovations prenant en compte la protection des données.

La CNIL considère que cette réglementation peut être un outil pour bâtir une innovation durable se déployant dans une société préservant les valeurs humanistes dont l'Europe a tout lieu de s'enorgueillir. Il est bien naturel que l'Europe ne se laisse pas dicter un modèle économique et qu'elle entende peser dans le débat mondial pour faire passer le message d'un choix de société dans laquelle nous voulons vivre et qui est en définitive le soubassement de cette législation.

Certes la réglementation n'est pas tout. Comme le disent les Américains, il n'y a pas de « *silver bullet* », pas une seule balle, pas une seule solution. En matière de protection des données, il y a tout à la fois matière à poursuivre l'éducation au numérique des citoyens, des dirigeants, à sensibiliser les professionnels, encourager le déploiement d'innovations technologiques permettant de préserver la vie privée et les libertés, que ce soit des mécanismes d'anonymisation, de limitation de la durée de conservation des données, de gestion par les individus des données qui les concernent… Il y a là aussi un champ infini d'explorations sur le plan technique. ■

La technologie au service de la confiance ?

2

Philippe Tassi (1972), Directeur général adjoint de Médiamétrie, Vice Président d'ENSAE Alumni

« C'est un joli mot : confiance » aurait pu chanter Jean Ferrat. Sur ce mot reposent beaucoup d'équilibres de notre société, dont celui de la société connectée actuelle et à venir.

Les données ou statistiques, détenues ou élaborées par des administrations ou des entreprises, ont en général été construites à partir d'informations individuelles, ce qui pose la question de la protection des sources, c'est-à-dire de la vie privée, compte tenu des progrès constants de la science et des processus de traitement.

Comment établir et maintenir la confiance du grand public, partie prenante numéro un, tout en respectant l'équilibre entre promesse de confidentialité et utilisation des données recueillies ?

L'établissement de la confiance s'appuie sur deux conditions nécessaires et fondamentales : l'une est réglementaire, et montre que beaucoup d'Etats ont pris conscience depuis longtemps de la nécessité d'établir des garde-fous juridiques ; l'autre s'appuie sur la déontologie et l'éthique des acteurs.