Ariane MOLE

RGPD : une révolution dans la continuité

La protection des données à caractère personnel existe depuis plus de 40 ans. Mais il a fallu l'évolution des usages et surtout le RGPD pour que les personnes sachent que ce droit existe et que les organisations commencent à sérieusement l'appliquer. Pour beaucoup, la mise en conformité n'est pas simplement un pas supplémentaire à accomplir pour se mettre au niveau des exigences du RGPD mais un véritable chantier à entreprendre à sa base. Ariane Mole, avocate pionnière de la pratique de la loi Informatique et libertés, nous expose les forces et les difficultés de mise en œuvre du RGPD que ce soit en France ou dans un contexte international, à l'aune de sa longue expérience de la matière.

Sylvie Rozenfeld : Vous avez travaillé sept ans à la Cnil auprès de la direction juridique et vous avez été la première à créer une activité d'avocat entièrement dédiée à la protection des données personnelles. Cela fait une quinzaine d'années que vous avez rejoint le cabinet Bird & Bird pour co-diriger l'activité mondiale en matière de données personnelles.
Vous avez donc été témoin d'une énorme transformation. A la fin du XXème siècle, la protection des données personnelles était un sujet d'initiés, pas toujours très pris au sérieux, vu la faiblesse du risque de sanctions. Aujourd'hui, les traitements sont omniprésents et le risque potentiel est énorme. Que vous inspire cette évolution ?

Ariane Mole : Le RGPD a opéré un vrai changement dans les organismes : avant rares étaient ceux qui avaient une organisation en matière de protection des données personnelles et qui recensaient leurs traitements. Je pense qu'il y a une évolution incroyable par rapport à la situation d'il y a deux ou trois ans, soit avant l'entrée en application du RGPD. Ce ne sont plus les mêmes enjeux, les mêmes problèmes. De façon générale, on constate une grande différence entre les PME et les grands groupes internationaux, et parmi ces derniers, une grande différence entre ce qui est mis en place au niveau du groupe et au niveau des filiales, mais aussi parfois de grandes différences entre les filiales elles-mêmes.
Avant, on me demandait rarement un audit Informatique et libertés et c'était moi qui devait attirer l'attention des entreprises sur sa nécessité. Aujourd'hui, les entreprises viennent vers nous avec de nouvelles demandes, pas seulement liées à la mise mise en place d'un registre des traitements, mais aussi pour des procédures, des process, des conseils sur la manière de mettre en œuvre un projet au regard des différentes actions de conformité, une étude d'impact, etc. Au début de ma pratique, il fallait convaincre de la nécessité de se préoccuper de la protection des données personnelles. C'est beaucoup moins vrai aujourd'hui.

Après un an et demi d'application du RGPD, qu'est-ce qui vous a le plus surprise ? Qu'est-ce qui a semblé complexe à intégrer ?
D'abord, le RGPD est une révolution, avec l'introduction du principe d'accountability, l'importance des sanctions, etc. Si ce texte reprend beaucoup d'éléments qui existaient déjà, il comporte aussi beaucoup de nouveautés. Mais il faut admettre que beaucoup d'organisations, une majorité d'entre elles, n'étaient pas du tout conformes avec les règles préexistantes. Au lieu d'avoir à accomplir le delta entre ce qui existait déjà et le RGPD, elles ont dû faire tout le chemin depuis le début pour se conformer à la législation du 6 janvier 1978, ce qui a donc ajouté à la difficulté de l'application du RGPD. Rares sont celles qui étaient conscientes de cette difficulté et de l'importance du chantier.
Un autre point surprenant a été de constater que les personnes concernées ont découvert des droits, vieux de plus de 40 ans. Quand le RGPD est devenu applicable, elles ont par exemple été nombreuses à mettre en œuvre leur droit d'accès, alors que ce droit existe en France depuis 1978. On a assisté à un déferlement de demandes, ce qui a posé des problèmes d'organisation pour les entreprises et les administrations. Cela n'est pas simple de répondre à une telle demande. Notre travail a aussi consisté, du fait du RGPD, à assister les organisations dans le contenu des réponses à apporter et dans la mise en place de procédures pour s'organiser afin de pouvoir répondre à de telles demandes.

« Au lieu d'avoir à accomplir le delta entre ce qui existait déjà et le RGPD, les organisations ont dû faire tout le chemin depuis le début pour se conformer à la législation du 6 janvier 1978, ce qui a donc ajouté à la difficulté de l'application du RGPD. »

Quelles nouveautés du RGPD vous ont semblé difficiles à intégrer ?
Les organismes, et même les autorités de contrôle parfois, ne savent pas comment mettre en œuvre certains droits, comme le droit à la portabilité des données ou à la limitation des traitements. Les contours de ces nouveaux droits ne sont pas toujours clairs alors que cela représente autant d'obligations pour les organismes. Il en va de même du droit pour la personne de donner des instructions sur le sort de ses données après sa mort, qui figure dans la loi Informatique et libertés. Ces droits sont écrits mais ils n'ont pas été explicités. Il y a également l'étude d'impact, qui est une obligation nouvelle. La Cnil a publié la liste blanche et la liste noire des traitements soumis ou non à cette obligation. Néanmoins, entre la liste blanche et la liste noire, il existe une zone grise où chaque responsable de traitement doit se faire son opinion et déterminer si le traitement est soumis à cette obligation. Le sujet des études d'impact a été très précisé par les textes, par les publications des autorités de contrôle, avec la mise à disposition par la Cnil d'un logiciel d'aide à la réalisation d'étude d'impact qui est très utilisé, y compris à l'étranger. Malgré ces éclairages, cette obligation reste complexe pour les organismes. Il faut d'abord déterminer si le traitement entre

dans le champ de l'obligation, les risques si on s'abstient de faire une analyse d'impact, etc. Tout cela nécessite un travail et une participation de plusieurs directions. Et c'est aussi une des difficultés du RGPD qui semble tenir pour acquis que tout le monde se parle dans un organisme, la direction de la conformité qui dialogue avec la direction juridique, qui s'entend très bien avec la direction des ressources humaines ou du marketing, la DSI, etc. Dans le monde du RGPD, on est solidaire, on communique et on se comprend pour faire de belles études d'impact, des registres des traitements bien exhaustifs, etc. Or, nous ne vivons pas dans ce monde idéal ou tout le monde travaille naturellement ensemble. Cela implique de s'adapter et de s'organiser en conséquence.

D'où l'intérêt d'avoir un DPO.
Effectivement mais à condition qu'il fasse consensus sur sa fonction, ce qui n'est pas évident.

Justement, comment est perçu le DPO dans les organisations ? Est-il pris vraiment au sérieux ? A-t-il de vrais moyens ?
Cela dépend des organisations, de leur politique, de leurs moyens.

Mais le DPO a beaucoup plus d'assise que le CIL.
Oui, il n'y a pas de comparaisons. Le CIL a été une création de la loi de 2004. D'abord sa nomination était toujours facultative et pour certains organismes elle était seulement motivée par la dispense de déclarations des traitements à la Cnil. Certaines organisations, plus rares, étaient sérieusement motivées et nommaient un CIL pour que la loi soit bien appliquée. Aujourd'hui, la présence d'un DPO est obligatoire pour tout le secteur public ou pour les entreprises qui traitent des données sensibles à grande échelle ou qui procèdent à un suivi des personnes à grande échelle. Les autres sont encouragées à en désigner un. Je n'ai pas de réponse toute faite sur l'opportunité de se doter d'un DPO. Cela dépend de la structure de l'organisme, des risques, etc. On peut respecter le RGPD sans disposer d'un DPO. Mais le fait d'en désigner un envoie un signal qui témoigne d'une volonté de respecter la protection des données personnelles, notamment à l'égard des clients, qu'on soit responsable de traitement ou sous-traitant. En interne, une telle désignation envoie également un signal fort. Cela a plus de poids que de charger quelqu'un de veiller au respect du RGPD. Beaucoup d'organismes ont désigné un DPO en raison des enjeux liés au règlement. Quand le risque équivaut à 4% du chiffre d'affaires, vous considérez la question avec une attention particulière. En cas de contrôle de la Cnil, la première question posée porte sur l'organisation interne et la gouvernance en termes de données personnelles. Comme il est désormais obligatoire, en tous cas, d'avoir une organisation en protection des données personnelles, beaucoup d'organismes ont fait le choix de nommer aussi un DPO au sein de cette organisation, même s'ils n'y sont pas obligés juridiquement. C'est un bon choix, à condition d'avoir les moyens de le faire et de le faire de manière sérieuse, à savoir que le DPO soit formé, soutenu et accepté. Dans certains organismes, l'intégration du DPO peut être difficile car il faut faire la part des choses entre les fonctions d'audit et de supervision du DPO et les fonctions d'audit ou de conformité qui existent déjà. Il y a des réglages à opérer.

« Et c'est aussi une des difficultés du RGPD qui semble tenir pour acquis que tout le monde se parle dans un organisme, la direction de la conformité qui dialogue avec la direction juridique, qui s'entend très bien avec la direction des ressources humaines ou du marketing, la DSI, etc. »

Marie-Anne Frison-Roche, professeure agrégée de droit, estime que l'UE est allée trop loin en imposant la compliance à toutes les entreprises alors que ce sont des obligations très lourdes pour des PME. Qu'en pensez-vous ?
Je suis d'accord avec ce point de vue. La mise en conformité au RGPD coûte cher. Je suis une grande passionnée de la protection des données personnelles et je suis depuis toujours convaincue de sa nécessité. Mais je pense qu'il est très difficile d'être en conformité et que la préservation des droits des personnes ne nécessitait pas forcément l'introduction de toutes ces nouvelles obligations. De la même manière qu'auparavant, je ne trouvais pas justifié que tant de traitements soient soumis à autorisation de la Cnil. Aujourd'hui,il me semble parfois exagéré de devoir faire des études d'impact trop complexes, de produire de la documentation pour tout, et le principe d' « *accountability* » oblige surtout à se protéger en cas de litige afin de pouvoir prouver que tout a été fait pour être conforme au RGPD. Mais c'est ne pas faire de distinction entre les différents types d'activité, entre une PME et les GAFA.

Le RGPD est très focus sur l'internet, n'aurait-il pas fallu adopter deux législations, l'une pour internet et l'autre pour les entreprises qui n'ont pas à transférer en masse des données ?
Je ne sais pas s'il aurait fallu adopter deux textes, mais il aurait été souhaitable de faire des distinctions ou des exceptions suivant les cas. Finalement, on se retrouve avec un texte qui ne prévoit pas d'exception. La seule exception

concerne les organisations de moins de 250 salariés qui n'ont pas à tenir de registre mais qui ont néanmoins l'obligation de recenser leurs traitements, d'avoir une organisation en protection des données personnelles, ce qui revient un peu au même. Par ailleurs, la Cnil a une interprétation très restrictive de cette exception puisqu'elle considère que presque rien ne doit échapper au registre. Cette seule exception ne bénéficie donc pas à grand monde.

Le RGPD a été davantage conçu en considération des grands groupes internationaux mais il s'applique à tous et comporte beaucoup d'obligations complexes à mettre en œuvre. Dans une réunion publique de l'EBDP (European Board for Data Protection) du 4 novembre 2019 sur l'exercice des droits, beaucoup d'entreprises ont souligné la difficulté de répondre aux demandes d'exercice droit d'accès. Si une personne demande un droit d'accès à toutes les données qu'une organisation détient sur elle y compris les logs et les traces, cela peut en effet demander un effort considérable. Comment fait-on quand on est une petite entreprise ? Dans les cas les plus complexes, nous proposons chez Bird & Bird un système d'analyse avec de l'intelligence artificielle pour arriver à trier et à trouver dans l'ensemble du système d'information les données relatives à la personne qui exerce son droit d'accès. Dans certains cas, on s'aperçoit que le RGPD est instrumentalisé, c'est-à-dire que la personne « *va à la pêche aux informations* » dans la perspective d'un contentieux alors que la finalité du droit d'accès est fondamentalement de permettre à la personne concernée d'assurer la protection de ses données personnelles en vérifiant que celles-ci sont traitées conformément à la législation.

« Désigner un DPO est un bon choix, à condition d'avoir les moyens de le faire et de le faire de manière sérieuse, à savoir que le DPO soit formé, soutenu et accepté. »

Dans d'autres cas, les personnes exercent un droit d'opposition sans préciser lequel ou un droit de suppression de l'ensemble de leurs données, alors qu'elles veulent en fait s'opposer à la prospection commerciale ou à un traitement particulier. Il faut alors revenir vers les personnes pour faire un travail d'explication. Par ailleurs, le délai de réponse d'un mois dans le RGPD est très court. Toutes les entreprises ne sont pas organisées pour répondre correctement à ces demandes.

Le RGPD est l'un des premiers instruments juridiques européens qui utilise la compliance comme mode de régulation, obligeant les entreprises à mettre en œuvre en interne les moyens pour se conformer au droit. Ce concept est-il bien intégré, bien compris par les entreprises ? Est-il efficace ?

Le client cherche à être en conformité mais nous devons adapter notre réponse, notre assistance, nos conseils à la taille de l'organisme, aux risques, et déterminer où se trouvent les enjeux les plus importants pour lui, compte tenu de son secteur d'activité, du nombre de salariés, des pays dans lesquels il intervient. Il faut donc différencier le cas de la PME ou de la start up des grands groupes qui ont besoin d'une conformité beaucoup plus documentée, car les risques et les enjeux sont plus importants. Cela nécessite d'adapter notre offre et nos prestations en prenant aussi en considération la difficulté de mettre en place toutes ces actions au regard de la taille de l'entreprise et de son activité.

Le RGPD a accompli une révolution. Un an et demi après son application, est-on encore au stade de rodage ? La transition est censée s'achever, la Cnil sera-t-elle encore compréhensive ?

La présidente de la Cnil, Marie-Laure Denis, a indiqué à plusieurs reprises que la période de clémence était terminée. La Cnil a pu montrer de l'indulgence pour les nouveautés introduites par le règlement, mais pas pour les obligations qui préexistaient au RGPD. Pour les contrôles qu'elle a effectués ou les sanctions qu'elle a prises, elle a été particulièrement rigoureuse sur les obligations qui préexistaient au RGPD : l'information des personnes, la durée de conservation, etc.

La Commission européenne a opté pour un règlement afin d'établir une réglementation homogène dans l'UE. Or, avec toutes les marges de manœuvres possibles, les législations sont différentes d'un Etat membre à l'autre. Vous qui exercez à l'international, considérez-vous que l'objectif a quand même été atteint ?

On a voulu créer un socle commun, une seule loi au lieu de vingt-huit. Au moment de la gestation du RGPD, la Commission européenne avait argué de la nécessité d'un règlement pour supprimer les divergences entre les législations, considérées comme trop complexes à gérer pour les entreprises multinationales. On a très vite vu qu'il allait y avoir des exceptions, des dérogations, des marges de manœuvres laissées aux Etats membres, comme sur les données sensibles, la presse, etc. Il y a eu beaucoup de lobbying. On avait par exemple promis aux multinationales qu'avec le RGPD elles pourraient disposer d'une seule autorité de contrôle en tant qu'interlocuteur

unique. Mais les autorités de contrôle ont fait valoir que ce n'était pas possible. La Cnil notamment a expliqué combien ça allait être compliqué pour les personnes si elles devaient s'adresser pour l'exercice de leurs droits à une autorité susceptible de ne pas être dans leur pays. Ces arguments légitimes ont été bien entendus. Désormais, les multinationales ont une autorité chef de file mais assortie d'un processus complexe de consultation des autres autorités concernées. En outre, en pratique, l'harmonisation est relative car on est bien obligé de tenir compte de l'interprétation du règlement par chaque autorité de contrôle. Nous avons bien un texte homogène, mais qui n'est pas interprété de la même manière par les autorités de contrôle et par les juges. S'ajoutent à cette complexité les législations locales, en application du RGPD qui prévoit des marges de manœuvres. Plusieurs Etats membres en ont profité pour rajouter du droit local, comme la France.

Dire que le règlement a simplifié la tâche des multinationales est excessif dans la mesure où il a considérablement augmenté leurs obligations. Nous avons toujours vingt-huit lois locales même si leurs particularités sont moins importantes qu'avant. Et certains secteurs d'activité sont plus impactés que d'autres par le droit local. Prenons par exemple le secteur de la santé : en France, les dispositions de la loi Informatique et libertés sur la recherche ont un champ d'application territorial différent de celui du RGPD puisque les dispositions de la loi Informatique et libertés modifiée sur la recherche en santé s'appliquent dès lors qu'il y a un patient concerné en France. Donc, avec la loi française, n'importe quel organisme où qu'il soit en France, dans l'Union européenne ou ailleurs dans le monde, à partir du moment où il effectue un essai clinique sur des patients en France, va devoir appliquer la loi française qui prévoit une autorisation de la Cnil ou une déclaration de conformité aux méthodologies de référence alors que le RGPD a aboli toutes les demandes d'autorisation et les déclarations.

« Il faut faire très attention à la qualification de ses partenaires, prestataires, fournisseurs, car cette qualification – responsable de traitement, co-responsable de traitement ou sous-traitant – est lourde de conséquences juridiques. »

L'Allemagne a prévu, quant à elle, d'autres dispositions spécifiques sur la santé. Voilà un exemple de secteur d'activité où le RGPD n'a pas harmonisé les règles. Autre exemple, les durées de conservation des données ne sont pas harmonisées d'un Etat membre à l'autre car les durées de prescriptions dépendent du droit national ;de plus les préconisations de chaque autorité nationale de protection des données ne sont pas les mêmes.

Or, une difficulté pour les entreprises réside dans le fait qu'elles ne peuvent pas mettre un drapeau sur toutes les données. Il faut donc les aider à trouver des lignes de force, des dénominateurs communs à tous les pays, par exemple en matière d'information des personnes. Concernant les salariés, il faut tenir compte du droit du travail car il est très interpénétré avec la protection des données personnelles et il varie selon les pays. Quand on met en place un dispositif d'alerte, une charte d'utilisation des systèmes d'information ou un contrôle des emails, on est confronté à beaucoup de différences d'un pays à l'autre. Nos clients nous demandent souvent de leur apporter une réponse globale « *one size fits all* », expression difficile à traduire en français : une approche unique, une même charte éthique ou une même privacy policy pour l'ensemble de l'UE. On ne peut pas toujours y parvenir complètement mais on essaie de s'en approcher.

Le brexit représente-t-il une difficulté ?

Certainement. Au regard des données personnelles, nous sommes dans l'expectative. Nous attendons l'adoption de l'accord de retrait de l'UE car le projet d'accord comporte des dispositions sur les données personnelles. Il y aura ensuite d'autres négociations. Le Royaume-Uni deviendra un pays tiers, hors UE et donc tous les flux de données à destination du Royaume-Uni devront respecter les garanties spécifiques prévues par le RGPD pour les transferts de données hors UE. S'agissant des organismes internationaux établis à titre principal en Grande-Bretagne, ils doivent pour certains reconsidérer leur organisation s'ils veulent continuer à bénéficier d'une autorité chef de file au sens du RGPD, car lorsqu'un organisme est établi à titre principal hors de l'UE il n'a plus droit à une autorité chef de file.

Nous venons d'obtenir pour un groupe international établi au Royaume-Uni les premières BCR (Binding Corporate Rules) adoptées en vertu de l'article 64 du RGPD, après avis de l'EDPB au niveau européen. Ce groupe a dû adapter ses BCR et les soumettre à l'EBDB. Il a dû également changer d'autorité chef de file, c'est-à-dire trouver une autre autorité principale dans l'Union européenne que l'ICO - l'autorité britannique. Nous l'avons accompagné dans toutes les actions nécessaires à l'obtention des BCR dans la perspective du Brexit.

Les sous-traitants sont devenus co-responsables. La relation contractuelle entre responsable de traitement et sous-traitant

doit être réaménagée, qu'est-ce qui pose le plus difficulté ?
Lors de l'application du RGPD, et encore aujourd'hui, beaucoup d'attention a été portée aux avenants aux contrats existants, ou aux nouveaux contrats, pour qu'ils soient conformes au règlement. Avant, le sous-traitant n'était pas responsable, vis-à-vis de la Cnil ou du juge, de sa non-conformité à la législation sur la protection des données personnelles et n'était redevable que de ses obligations contractuelles.

Désormais, le sous-traitant est également responsable : il doit nommer un DPO dans certains cas, avoir un registre des traitements, participer aux études d'impact, etc. Si le contrat n'est pas conforme au RGPD, le responsable du traitement et le sous-traitant sont tous les deux responsables et ils encourent tous les deux un risque de sanction. Il s'agit là également d'un des changements apportés par le RGPD. Les sous-traitants n'en ont pas toujours complètement pris la mesure. Pourtant, on voit de plus en plus que dans les appels d'offre des secteurs public et privé, il est demandé dans le cahier des charges que la prestation du sous-traitant soit conforme au RGPD.

On constate par ailleurs qu'il y a beaucoup d'incompréhensions sur ce qu'est un sous-traitant. Lors de l'entrée en application du règlement, certains ont cru bon d'envoyer à tous leurs partenaires, à qui ils communiquaient des données, des contrats incluant les clauses de l'article 28 du RGPD, considérant qu'ils étaient leurs sous-traitants. Or, ce n'est pas parce qu'on communique des données personnelles à un partenaire qu'il est sous-traitant. Le sous-traitant est celui qui effectue une prestation sur les données personnelles. Une agence de voyage, une agence de recrutement, un avocat ne sont pas des sous-traitants. Moi-même, comme d'autres confrères, j'ai reçu des contrats à signer en tant que sous-traitant au 25 mai 2018 ! Il faut faire très attention à la qualification de ses partenaires, prestataires, fournisseurs, car cette qualification – responsable de traitement, co-responsable de traitement ou sous-traitant – est lourde de conséquences juridiques. Quand ce n'est pas évident, il convient de se poser les bonnes questions : avantages, inconvénients, analyse des critères et de leurs conséquences.

« Nous avons toujours vingt-huit lois locales même si leurs particularités sont moins importantes qu'avant. Et certains secteurs d'activité sont plus impactés que d'autres par le droit local. »

En matière de contrats informatiques, on a assisté à la négociation des plafonds de responsabilité en cas de manquement par l'une des parties à ses obligations en matière de traitement des données à caractère personnel. Est-ce une question épineuse entre client et prestataire ?
C'est une question de rapport de force, comme dans beaucoup de relations contractuelles. Elle est surtout épineuse, compte tenu de l'importance des sanctions potentielles. Et puis, quand on intervient dans plusieurs pays, on se retrouve à nouveau confronté aux différences de législation suivant les pays. Le droit des contrats n'est pas le même en France, en Angleterre, en Allemagne ou dans un autre pays du monde.
On ne peut pas s'exonérer de sa responsabilité de la même manière dans un pays ou dans un autre. Je travaille beaucoup avec mes associés en droit des contrats ou en IT en France et dans nos autres bureaux dans le monde car la protection des données personnelles est une question complètement transverse.

Antoinette Rouvroy, chercheuse au Crids de Namur dit que *« le concept de données personnelles n'a pas vraiment de sens dans un contexte de données massives et il risque même de nous induire en erreur. Ce qui confère une utilité, une valeur aux données, ce sont les corrélations qu'elles permettent de faire apparaître entre des éléments infrapersonnels, donc des fragments insignifiants, de purs signaux. (...) C'est pourquoi la critique de la technologie me semble mal adressée. Elle reste emprisonnée dans une vision dépassée du monde, selon laquelle nous serions des sujets espionnés par un pouvoir centralisé. La situation est presque plus inquiétante. Dans notre monde, les sujets ont disparu. Il n'y a plus personne... Non seulement Big Brother n'existe pas, mais nous n'avons jamais été si peu considérés et regardés qu'aujourd'hui ».*

Que pensez –vous de sa réflexion ?
Cette réflexion me fait penser à l'interprétation de la notion de données personnelles et à son évolution. La définition de cette notion n'a pas ou a peu évolué en droit. A l'origine, nous avions la définition de l'information nominative dans la loi Informatique et libertés de 1978, qui a été peu ou prou reprise par la directive de 1995, seul le nom a changé puisqu'elle a été renommée donnée personnelle. On retrouve cette définition dans le RGPD, avec des illustrations en plus, telle que la référence à l'identité psychique, physiologique, etc., pour souligner l'ampleur du champ d'application Mais quand on regarde

l'interprétation de la Cnil suivie par le Conseil d'Etat, on voit bien que la notion de données personnelles va au-delà de sa définition. Je pense à une délibération de la Cnil en 2015 suivie par un arrêt du Conseil d'Etat en 2017 sur l'affaire JC Decaux relative aux panneaux publicitaires intelligents, qui est une illustration très intéressante de la question de ce qu'est une donnée personnelle. Il n'y avait aucun nom enregistré mais l'adresse MAC des portables captée par Wi-Fi. JC Decaux avait proposé de tronquer l'adresse MAC pour éviter la qualification de donnée personnelle. Mais la Cnil a considéré qu'il s'agissait toujours d'une donnée à caractère personnel, peu importe qu'on ne sache pas qui est derrière les octets. Ce qui compte, c'est qu'un signal permet d'isoler un individu dans un ensemble et de relier entre elles ses données. On ne sait pas quelle est la personne qui passe devant le panneau publicitaire mais on peut mesurer combien de fois la même adresse MAC, même tronquée, passe devant le panneau publicitaire ou si cette adresse MAC passe ensuite devant un autre panneau publicitaire. Cela reste des données individualisées et qui peuvent être reliées entre elles, même si on ne sait pas à qui elles correspondent.

Par conséquent, même si nous avons toujours une définition selon laquelle la personne doit être identifiée ou identifiable, supposant qu'on peut remonter jusqu'à l'identité de l'individu, l'interprétation qui a été faite va davantage dans le sens d'une application des règles de protection des données personnelles si les données sont reliables entre elles. De même, à l'heure actuelle sur internet, ce qui prime est de connaître votre comportement par exemple pour vous adresser des messages publicitaires ou politiques, peu importe comment vous vous appelez. C'est pourquoi, on est allé au-delà de la définition théorique de la donnée personnelle pour prendre en compte la possibilité de corréler des enregistrements pour en déduire des informations.

« Nous venons d'obtenir pour un groupe international établi au Royaume-Uni les premières BCR (Binding Corporate Rules) adoptées en vertu de l'article 64 du RGPD, après avis de l'EDPB au niveau européen. »

Je voudrais aussi rappeler que la loi française a depuis l'origine un article premier et qui n'est pas dans le RGPD selon lequel l'informatique est au service du citoyen et ne doit porter atteinte ni aux droits de l'homme ni à la vie privée ni aux libertés individuelles ou publiques, ni à l'identité humaine. J'ai toujours été sensible à cet article qui donne le ton. Je pense que cette notion d'identité humaine vient signifier que la donnée à caractère personnel n'est pas seulement une donnée qui permet d'identifier la personne et qu'elle répond à la réflexion d'Antoinette Rouvroy : aujourd'hui il n'y a plus personne. Car cette notion d'identité humaine fait référence au fait que malgré les corrélations et entre les signaux, la personne ne doit pas disparaître.

C'est beaucoup plus fort que la seule notion de données personnelles.

Propos recueillis par
Sylvie ROZENFELD