Questions actuelles sur la commercialisation des données à caractère personnel

Dany Cohen

Cahiers de droit de l'entreprise n° 3, Mai 2012, entretien 3

Questions actuelles sur la commercialisation des données à caractère personnel

Entretien avec Dany Cohen
Professeur des universités à sciences po, avocat au barreau de Paris,

et Romain Perray
Avocat au barreau de Paris - Cabinet ANDCO Avocats,

et Judith Rochfeld
Professeur à l'École de droit de la Sorbonne, université paris I,

et Ambroise Soreau
Avocat au sein du cabinet Henri Leclerc & associés

Sommaire

La question de la commercialisation des données personnelles se pose à partir des pratiques observées et des tentatives d'encadrement menées jusqu'ici. Alors que la Commission européenne a présenté une vaste réforme du cadre juridique européen relatif à la protection des données à caractère personnel, qui est maintenant devant le Parlement et le Conseil, la question de changer ou non le concept de données personnelles s'est posée.

Aussi cette table ronde, animée par Dany Cohen, qui réunit Romain Perray, Judith Rochfeld et Ambroise Soreau, revient-elle sur la qualification existante des données à caractère personnel et sur la question de savoir s'il conviendrait (ou non) de modifier ou d'étendre la qualification de données à caractère personnel pour en assurer une meilleure protection.

Sera également abordée la question de savoir si l'exigence d'un accord préalable ou d'un consentement aux traitements est toujours pertinente et suffisante, cela en gardant à l'esprit qu'il semble que, dans leur immense majorité, les gens sont loin d'imaginer la quantité impressionnante d'informations précises récoltées à leur sujet. Enfin les débats reviendront sur les liens entre vie privée et protection des données à caractère personnel.

1. Faut-il changer ou étendre la qualification de données à caractère personnel pour en assurer une meilleure protection ?

La question de la commercialisation des données personnelles se pose à partir des pratiques observées et des tentatives d'encadrement menées jusqu'ici. Nous pourrions commencer par discuter de la qualification existante des données à caractère personnel et nous demander s'il conviendrait (ou non) de modifier ou d'étendre la qualification de données à caractère personnel pour en assurer une meilleure protection.

Une toute petite réserve venant de la part du praticien. Pour les juristes qui s'intéressent aux données personnelles, le concept est très clair. Néanmoins, en ce qui concerne les clients, il leur est délicat d'appréhender ce qu'est une donnée personnelle et la qualification l'est donc moins. Par exemple, un client m'a demandé de rédiger un contrat dont une clause comprenait les aspects informatique et libertés. Il m'a assuré que son traitement ne comprenait aucune donnée à caractère personnel. En réalité, il était question d'adresses IP qui sont des données à caractère indirectement personnel au sens de la loi *Informatique et Libertés*. Dès qu'on passe à des données techniques, notamment dans l'informatique, la notion est difficile à appréhender pour des non spécialistes.

Bio Express :

▲ Dany COHEN

Professeur des universités à Sciences Po et directeur du master Carrières judiciaires et juridiques et de la spécialité Contentieux économique et arbitrage du master Droit économique, avocat au barreau de Paris.

Pour élargir le débat, je pense qu'il faudrait prendre en considération les traçages de toutes sortes, que l'on peut peiner à faire entrer dans la qualification traditionnelle. Certes, l'Union européenne et la CNIL française sont plutôt en faveur d'un élargissement de la notion de donnée à caractère personnel à ces derniers ; elles soumettent des données à caractère technique ou d'autres données indirectement identifiantes à la protection accordée aux données à caractère personnel. Mais je voudrais néanmoins insister sur la spécificité des données tracées et le fait de devoir les prendre en considération, qu'elles soient traitées par *cookies* de connexion, par puces RFID ou par géolocalisation : ces traçages portent sur des données relatives à la personnalité, plutôt qu'à l'identité. En pratique, au côté de la collecte du nom ou des coordonnées bancaires, les traitements portent également sur la personnalité de chacun et ses comportements. On le constate dans les utilisations qu'implique la publicité ciblée par exemple : il y a commercialisation massive de données qui ne sont pas rattachées à l'identité ou à l'identification d'une personne, telles qu'on les connaissait traditionnellement ; il s'agit plutôt de données rattachées à la personnalité, au comportement des personnes. Les autorités de contrôle élargissent aujourd'hui la notion de donnée à caractère personnel pour y faire rentrer tous ces traçages de la personnalité, au sein desquels l'identité n'est pas centrale. Je pense donc qu'il faut considérer aujourd'hui, derrière la protection des données à caractère personnel *stricto sensu*, celle de la « présence numérique » de chacun. Cela ne requiert pas forcément de changer la qualification mais au moins d'accepter de l'élargir à des données de personnalité.

Ne pourrait-on dire que le traçage est relié à la personnalité, dans la mesure où les moyens électroniques actuels permettent de faire le lien entre une adresse électronique et un numéro de carte bancaire pour ne prendre que cet exemple ?

L'impression que j'ai par rapport à la définition qui existe actuellement de la donnée à caractère personnel, son caractère direct ou indirect et notamment les moyens qui sont à la disposition du responsable de traitement ou de toute autre personne, et le fait que cette définition soit extrêmement large, à mon sens, permet déjà d'inclure de manière marginale cette question de la personnalité.

Nous sommes bien d'accord. C'est pour cela que la décision de la Commission européenne de ne pas changer la qualification, mais d'y faire entrer des éléments qui auparavant étaient exclus me paraît bonne.

Pour revenir sur ce qui a été dit tout à l'heure, il est vrai qu'en tant que praticiens, nous avons beaucoup de mal à faire comprendre aux clients la notion de donnée à caractère personnel et qu'en la matière, l'adresse IP est un bon exemple.

Oui, l'adresse IP, ne serait-ce que parce qu'elle est parfois collectée par défaut dans des journaux de « log », les clients n'ont pas conscience qu'ils ont mis en oeuvre un traitement de donnée au sens de la loi.

Ce n'est pas tant le caractère technique de l'adresse IP qui pose problème, les clients savent pour d'autres données techniques immédiatement qu'elles sont à caractère personnel. Les clients sont en effet conscients que les données GPS sont très traçantes par exemple, il s'agit pourtant de données techniques. Dans le cas de l'adresse IP, le fait de collecter la donnée est courant, parce que la collecte existe dans le paramétrage par défaut des serveurs. De ce fait il n'a pas conscience d'effectuer une collecte de données et de mettre en oeuvre un traitement au sens de la loi.

2. L'exigence d'un accord préalable ou d'un consentement aux traitements

L'exigence d'un accord préalable ou d'un consentement aux traitements est-elle toujours pertinente et suffisante ?

Le véritable enjeu de la commercialisation des données à caractère personnel est surtout, à mon sens, l'information de la personne concernée par le traitement, qu'il porte sur les *cookies* ou sur l'adresse IP. Or, à cet égard, le véritable problème, en pratique, tient aux systèmes de cession de fichiers successifs qui amènent un internaute à être prospecté par une personne avec laquelle il n'a jamais eu de contact. Sur ce plan là, je vois l'intérêt de la proposition de règlement européen qui contient un mécanisme d'obligation de moyen un peu renforcé relativement à l'oubli numérique et à l'effacement. Le cadre me semble cependant parfois un peu général, notamment quant à l'exercice du droit d'opposition et son éventuelle conséquence directe ou non sur l'effacement. À mon sens, la difficulté qui existe à l'issue de la directive européenne, c'est toute la question des traitements ultérieurs.

Ne faut-il pas prendre en compte une autre dimension ? Le problème de consentement que vous venez d'évoquer ne se double-t-il pas d'une asymétrie d'informations ?

Je m'explique : la majorité des internautes n'a qu'une très faible idée de ce qui est collecté sur son compte. La quantité d'information – ce qui me semble central par rapport à ce que vous appeliez loyauté – est collectée sans que les gens le sachent. Les internautes ignorent quelles informations ils ont semées. Un exemple, ayant enseigné à Turin, lorsque je consultais mes emails à partir d'un ordinateur de l'université, s'affichaient à l'écran des publicités en français sur des commerces turinois, preuve qu'on avait identifié ma localisation et ma langue.

Bio Express :

▲ Romain PERRAY

Avocat au barreau de Paris – Cabinet ANDCO Avocats. Auteur du Juris-Classeur Administratif « Traitement de données à caractère personnel », chargé d'enseignement au sein du Master II Professionnel – Droit du Commerce Électronique et de l'Économie Numérique de Paris I.

J'ai une question pour nos professionnels, non pas sur le projet européen mais sur l'ancien « Paquet télécom » de 2009. Nous venons de transposer, par l'ordonnance du 24 août 2011, l'obligation d'information relativement à la pose de *cookies*. Il semblerait pourtant que nos professionnels français, pour l'heure, ne se mettent pas dans la meilleure des dispositions pour appliquer l'obligation. Est-ce que vos clients vous interrogent sur le consentement préalable et avez-vous déjà mis en place, avec eux, une procédure d'information et de consentement ?

Assez peu de clients, essentiellement des sociétés de B2C (on distingue dans le jargon des acteurs du web, le B2C, abréviation de « *Business to consumer* », qui désigne les relations des firmes avec les consommateurs, du B2B, abréviation de « *Business to business* », qui désigne les relations entre professionnel), m'ont interrogé sur ces problématiques. S'agissant des *cookies*, et en ce qui concerne les dispositions européennes, il est fait état d'un « accord préalable ». Je ne partage pas forcément l'analyse de la CNIL sur le fait qu'il faille un consentement préalable, même si la version anglaise de la directive utilise le terme de consentement, car la version française ne l'utilise pas. Elle renvoie en effet uniquement à la notion d'un « accord préalable » qui est, à mon sens, distinct du consentement à proprement parler qui, lui, fait justement l'objet d'une définition précise.

La réforme de la directive de 2009, qui modifie la directive de 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, a pour objectif de changer les dispositions qui existaient initialement concernant l'obligation de recueillir l'accord préalable à l'installation de *cookies*. Les dérogations prévues à l'époque étaient dans l'ensemble assez souples. Elles prévoyaient en effet la possibilité de ne pas obtenir l'accord préalable dès lors que l'installation du *cookie* sur le terminal était strictement nécessaire au service ou facilitait tout simplement la communication par voie électronique. À cet égard, je ne crois pas que le principal problème porte sur l'interprétation des nouvelles dispositions européennes en ce qu'elles tendent vers une application plus stricte des dérogations à l'accord préalable et les limitent à ce qui est « strictement nécessaire ». La principale difficulté réside plus, selon moi, dans la transposition de la directive de 2009 dans la loi *Informatique et Libertés*, et notamment le fait que les dérogations au principe de l'accord préalable n'aient pas été limitées au caractère strictement nécessaire, mais ont conservé une possibilité de dérogation lorsque l'installation de *cookies* a pour but de faciliter la communication. Pour l'instant, tant qu'il n'y a pas de décision, du type de celle qu'a rendue la CJUE à propos de la réglementation espagnole en matière de données personnelles (*CJUE, 3e ch., 24 nov. 2011, aff. C-468/10 et C-469/10*) sanctionnant cette transposition inexacte de la directive de 2009 par l'ordonnance du 24 août 2011, on se trouve, à mon sens, dans une situation

d'insécurité juridique, même si je reste convaincu que les nouvelles dispositions de la directive de 2009 laissent encore des marges de manoeuvre.

Pour compléter sur cette question du *cookie*, quand un professionnel va placer un *cookie* dès la page d'accueil pour suivre la navigation et permettre une navigation personnalisée sur le site, il est peu disposé à cette idée de recueillir l'accord préalable. Le professionnel trouve cela disproportionné de demander un accord explicite et considère que, dès lors qu'il a indiqué dans ses conditions générales d'utilisation (CGU) qu'il y avait un *cookie* placé, il a été suffisamment informatif. Je comprends bien, évidemment, la finalité qu'il peut y avoir en ce qui concerne la protection des données à caractère personnel, mais je pense que la règle sous-estime les aspects pratiques.

Pour synthétiser, soit pour Romain Perray la règle française va au-delà du « Paquet télécom » et de ce qui était exigé, soit, pour Ambroise Soreau, quand bien même on l'aurait bien transposé, c'est disproportionné en pratique.

Peut-être cela paraît-il excessif mais ne serait-il pas possible, au lieu d'une liste de conditions dont on sait qu'elles ne seront pas lues et presque destinées à ne pas l'être, d'envisager qu'une question s'affiche à l'écran ?

C'est la question du bandeau.

Un accord préalable à travers un clic systématique peut nuire à une certaine fluidité de navigation. La question, d'un point de vue pratique, revient à savoir si les CGU suffisent. Elle aurait peut-être mérité une meilleure évaluation.

Puisque le consentement doit être donné de manière éclairée, les gens ne devraient-ils pas savoir ce qui est relevé sur eux ? En pratique, ils l'ignorent.

Bio Express :

▲ Judith ROCHFELD

Professeur de droit privé à l'École de droit de la Sorbonne, université Paris 1, Panthéon-Sorbonne, où elle dirige le Master 2 de droit du commerce électronique et de l'économie numérique. Elle enseigne le droit civil, le droit européen, ainsi que le droit du numérique. Elle a publié divers ouvrages en droit des contrats, du commerce électronique et en droit privé européen, ainsi que de nombreux articles et chroniques en ces différentes matières. Le dernier ouvrage paru, en 2011, aux Presses Universitaires de France, s'intitule *Les grandes notions du droit privé*.

Certes, mais il demeure que les gens, dans l'immense majorité, ignorent ce qui est prélevé sur eux et sont loin d'imaginer la quantité impressionnante d'informations précises récoltées sur eux au passage.

3. *Digital Natives* et *Privacy paradox*

On évoque souvent une attitude différente de la génération née après l'arrivée de l'ordinateur individuel (ceux que l'on appelle les « *digital natives* »), qui se caractériserait par une certaine indifférence à la diffusion de leurs données personnelles. Qu'en est-il selon vous ?

Je pense que le vrai problème est de savoir si le fait que des informations soient prélevées sur eux les préoccupe.

Je pense que nous abordons là des questions cruciales. Il existe en effet ce que l'on appelle le « *Privacy Paradox* » : pour les *Digital Natives*, à savoir ceux qui ont toujours vécu avec Internet, la protection n'a pas la même importance. Ils ne raisonnent pas comme la génération qui n'est pas née avec Internet et n'ont pas la même compréhension de la vie privée.

C'est ce qu'on appelle le *Privacy Paradox*, c'est-à-dire que, pour eux, exister socialement c'est s'exposer, c'est « l'extimité », comme l'appelle le sociologue Serge Tisseron. Les réflexes que l'on peut avoir relativement à la protection de nos données, de la faire relever de notre vie privée, ne sont pas identiques. Par ailleurs, lorsque je discute avec mes étudiants – qui sont pour une bonne part conscients de ce qui se passe sur Internet, et qui ont une présence numérique très importante (dans leur grande majorité, ils participent aux réseaux sociaux, tiennent des blogs sur Internet, etc.), – cette préoccupation de protection n'existe pour ainsi dire pas. L'accès aux services leur paraît beaucoup plus important et l'exposition ne les dérange pas.

Cette évolution sociologique est à prendre en compte.

À cet égard, je me pose la question de savoir si la différence entre « eux » et « nous » ne tient pas, d'une part, à un effet d'âge qui nous conduit à nous inscrire dans une plus longue durée, mais d'autre part, au fait que nous réagissons en professionnels du droit ?

Sur le premier point, il me semble en effet qu'ils s'inscrivent dans une instantanéité et que l'idée du stockage, de la réutilisation est loin de leur vécu télématique : j'avais l'impression que mes étudiants prenaient cela pour de la donnée totalement fugace, alors qu'elle ne l'est pas. J'ajouterai que, lorsque l'on a étudié, avec des étudiants italiens, les trois poursuites qui sont engagées dans des *Landers* allemands contre Facebook (à cause de son logiciel de reconnaissance faciale, du non-effacement de certaines données et de l'« agglutination » de données sur des gens qui ne sont pas membres de Facebook, etc.) ainsi que le cas de cet étudiant autrichien Max Shrems, qui a demandé les données collectées sur lui sur trois ans, ces étudiants ont complètement changé d'idée sur la transparence d'Internet. Ils pensaient que les informations sur Internet n'étaient pas conservées.

Ne serions-nous pas là encore dans une situation d'asymétrie d'informations ?

4. Le droit à l'oubli numérique et les recours disponibles

Qu'en est-il du droit à l'oubli numérique et des recours possibles ?

Il y a un autre paradoxe. Finalement, jusqu'à récemment, en tous cas du point de vue de la jurisprudence française, il y avait peu d'intérêt relativement à l'utilisation des différents droits de la loi *Informatique et Libertés*, à l'exception de quelques très rares affaires dont la plus connue appelée « l'École de Laëtitia » : une jeune femme ayant effectué, dans sa jeunesse, un certain nombre de films pour adultes avait retrouvé des informations *via* Google qui la concernaient ; elle a engagé des actions en justice pour qu'il y ait un véritable effacement de ces données.

Les *Digital Natives* n'ont peut-être pas encore conscience que leurs données sont conservées et que leurs futurs recruteurs pourront les trouver dix ans plus tard. La notion d'oubli numérique, telle qu'elle apparaît d'ailleurs dans le règlement européen, est assez intéressante.

Il y a, certes, le fait qu'on n'a peut-être pas assez d'informations, mais, à l'inverse, il faut avoir conscience que les informations peuvent être stockées. Il suffit pour cela de taper son nom dans Google pour constater qu'il y a parfois tout un ensemble de pages que nous n'avons pas sollicité. Il y a des moyens d'actions, le problème étant, pour les mettre en oeuvre, qu'il est difficile de les opposer à une trentaine de sites différents.

La réforme est assez intéressante de ce point de vue puisque, à l'avenir, le responsable de traitement devra effacer et interdire la diffusion et qu'il devra le faire à l'égard des tiers à qui il a transmis les données.

Le système en chaîne qui est envisagé est très intéressant en ce qu'il impose à chaque responsable de traitement de s'assurer que les responsables de traitement ultérieur suivront bien les mêmes instructions que lui.

5. Responsabilisation des professionnels et mise en place d'outils de gestion des données

***Quid* de la responsabilisation des professionnels et de la mise en place d'outils de gestion de ses données ?**

Il me semble que la proposition de règlement valorise aussi, auprès des professionnels, la mise en place de tableaux de bord (sorte d'outil mis à disposition des internautes afin qu'ils puissent connaître toutes les données qu'un professionnel détient sur eux et puissent les gérer).

Non seulement cela, mais ces évolutions alimentent une construction qui me paraît intéressante et qui tient en l'émergence de l'auto-détermination informationnelle. Cela consiste à reconnaître à chacun la possibilité, à partir de l'information, du consentement, et de moyens techniques mis à sa disposition (les tableaux de bord par exemple), de contrôler et de gérer les données que détiennent les professionnels avec qui il est en contact. Je voulais demander à nos praticiens s'ils avaient, parmi leurs clients, des entreprises qui se dirigeaient vers ce type d'outils de mise à disposition.

Bio Express :

▲ Ambroise SOREAU

Avocat au sein du cabinet Henri Leclerc & Associés, en charge du droit des nouvelles technologies et propriété intellectuelle, docteur en droit.

Non, parce que cela pose des problèmes de coûts pour les entreprises. Cela suppose, à chaque fois qu'on délivre un tableau de bord, une extraction des données, de la puissance de traitement, etc. Tout cela génère probablement des coûts assez importants, sans compter les problèmes de sécurité. En effet, il s'agit de s'assurer que le profil va être délivré à la bonne personne. Par ailleurs, je voudrais rebondir sur ce qui a été dit au préalable : ceux qui sont nés dans un environnement numérique s'exposent beaucoup plus que les anciennes générations ; dans le même temps, ils sont aussi très habiles pour mettre en place des stratégies. Par exemple, ils ne s'enregistrent pas sous leur vrai nom sur Facebook, ils utilisent différents profils, différentes adresses électroniques, selon leurs besoins.

Certes, mais si on regarde les dernières versions de Google Chrome, elles contraignent plus ou moins les gens à demeurer dans leur véritable identité, ce à travers un rattachement de toutes les données à l'adresse IP.

Pour Google, le point de rattachement est l'adresse email. À partir de là, on crée un compte qui va servir pour Google+, plus généralement pour tous les services Google. Certains savent le faire et il est possible de créer plusieurs profils. Toutefois, dans ce cas, il est vrai que tout n'est plus interconnecté et que l'utilisateur perd une partie des avantages des services agrégés par Google.

Une enquête menée il y a un an ou deux auprès des recruteurs américains a établi que 80 % d'entre eux admettaient avoir refusé des candidatures après avoir effectué des recherches sur Internet sur les candidats.

J'ai l'impression que la culture américaine et la culture européenne sur la protection des données à caractère personnel sont extrêmement différentes. Il y a un autre aspect : en France, il y a une culture de la crainte du fichage. La loi *Informatique et Libertés* est née de cette problématique. En France, en 1978, se manifeste la crainte du fichage public. On l'a encore senti quand le Gouvernement a essayé de mettre en place le fichier Edvige. Cela a provoqué un raz-de-marée de réactions.

Le croisement des portefeuilles de données peut être une crainte, en effet.

6. Quels sont les liens de la vie privée et de la protection des données à caractère personnel ?

Comment concilier ce qui vient d'être dit quant aux recherches auxquelles se livrent certains employeurs sur l'Internet avec l'insouciance et la placidité des jeunes évoquées par Judith Rochfeld ? Est-ce un problème de comportement des internautes ou de comportement des entreprises ?

Si la Cour de cassation a été obligée d'anonymiser ce qu'on trouve sur Légifrance, c'est d'abord à cause des employeurs qui cherchaient si le salarié n'avait pas eu un divorce un peu délicat ou n'avait pas eu de problèmes avec son propriétaire... Ce type de recherches ne dépend absolument pas des internautes ; les gens ne sont pas allés sur le web ; ils avaient, d'une manière ou d'une autre, eu affaire à la justice et c'est l'employeur qui a cherché des indications. Je repensais aussi au cas – qui a fait un certain bruit aux États-Unis – d'une jeune doctorante à qui l'université a refusé la délivrance de son doctorat à cause d'une photo où elle était un peu éméchée, un peu déguisée dans une soirée banale. Le danger ne vient-il pas plutôt de l'utilisation qui est faite des données, à travers des recherches ciblées ?

Il vient des deux. Votre profil Facebook, par exemple : vous avez des marges de manoeuvre sur l'utilisation qui en est faite. On peut par exemple se référer à l'analyse du conseil des prud'hommes de Boulogne : en disant « Voilà, vous n'avez pas fermé l'accès à tant de personnes », il a induit une volonté de rendre publiques les données. Le fait d'être une personnalité publique compte également : il y a beaucoup de gens que leurs données intéressent, stimulent ; on en trouve un bon exemple avec la télé-réalité. C'est la perception de ce qu'est l'intimité qui évolue. Je pense que les deux s'alimentent : si chacun laisse cours à ses informations et en permet l'accès, effectivement les employeurs s'en emparent...

L'évolution de la jurisprudence française montre cependant que de plus en plus de gens vont avoir le réflexe d'engager des actions judiciaires pour préserver une partie de leurs droits, particulièrement en matière de droit du travail.

Dispose-t-on des chiffres quant au contentieux ?

Je n'ai pas de chiffres de contentieux, mais si vous prenez le JCP Social, par exemple, vous voyez qu'il y a de plus en plus de décisions. Il y a ainsi de plus en plus régulièrement des jurisprudences sur l'importance de la charte informatique, ses conséquences : est-ce qu'il en existe une ou pas ? Quelles conséquences cela a pour les employés ? Pourrez-vous être licencié ou pas, avec quelles conséquences financières ? Il va y avoir de plus en plus de réactions par rapport à ces aspects là.

De façon encore plus générale, je pense que, dans la lignée de la Charte des droits fondamentaux de l'Union européenne, il faudrait qu'on aille, pour sortir d'une législation spéciale conçue en 1978, vers la reconnaissance d'un « droit à la protection des données personnelles » qui puisse être brandi par chacun, à l'instar du droit au respect de la vie privée. Il faudrait toutefois, à mon sens, le séparer du droit au respect de la vie privée parce que, je le répète, il ne me semble pas que le droit au respect de la vie privée et le droit à la protection des données se superposent exactement. Je pense que le choix qu'a opéré la Charte des droits fondamentaux de l'Union européenne est le bon, c'est-à-dire d'avoir séparé les deux, contrairement à la jurisprudence de la Cour européenne des droits de l'homme. Je me demande donc si nos professionnels seraient horrifiés de lire un nouvel article du Code civil (9-2 par exemple) portant ce droit au respect des données personnelles, subjectif et permettant d'introduire un contentieux... Est-ce que, pour vous, intégrer ce droit subjectif et général, hors le cadre de spécialisation connue jusqu'à présent, représenterait beaucoup de changements ?

C'est une question sur laquelle j'avais réfléchi, puisque j'ai fait ma thèse doctorale sur le droit au respect de la vie privée. Je pense cependant que la protection des données à caractère personnel poursuit la même finalité que le droit au respect de la vie privée. C'est la capacité à gérer, à préserver sa singularité, à décider des rapports avec autrui ; c'est un droit à l'autodétermination. Cela peut être utile, mais

je ne pense pas que cela soit absolument nécessaire. Je pense que l'article 9 du Code civil est général ; le danger qu'il peut y avoir à une trop grande spécialisation, c'est de ne pas arriver à une bonne rédaction. Est-ce que l'article 9 ne suffit pas en lui-même ?

Il me semble que ces articles ne traiteraient pas exactement de la même question. Pour moi, il y a des éléments qui ne relèvent pas de la vie privée dans le traçage, ou le traitement de la présence numérique plus généralement. C'est d'ailleurs pour cela que la Charte des droits fondamentaux de l'Union européenne a pris le parti de séparer les deux notions (articles 7 et 8). D'une part, il existe des traitements de données publiques : c'est parce qu'elles sont croisées, organisées en portefeuille, traitées d'une certaine façon, que les problèmes surgissent. Mais, on ne recoupe pas ici la vie privée. D'autre part, dans les traçages (*cookies* et autres), les traitements peuvent ne pas concerner des données que nous placerions traditionnellement dans la vie privée. Je reviens à mon idée que c'est la personnalité, la « présence numérique », des comportements, qui sont tracés. Ce ne sont pas forcément des éléments qui seraient qualifiés de vie privée devant un juge.

Ça se discute...

Je donne juste un autre exemple, très parlant à mon sens. Lors des auditions pour l'élaboration du rapport parlementaire sur les évolutions de la vie privée à l'heure du numérique, les parlementaires ont interrogé le directeur juridique de Yahoo ! France. Qu'a-t-il dit à propos des *cookies* ? Je trouve ça vraiment exemplaire. Il a dit : « Nous ne traitons pas la vie privée ; je ne me préoccupe pas de l'identité des personnes sur le disque dur desquelles je mets un *cookie*. Ce qui m'intéresse n'est pas leur identité – il l'a dit clairement – c'est leur personnalité. C'est leur comportement qui m'intéresse ». Le traçage comportemental, pour un juge ordinaire en tout cas, ne rentrera pas dans la vie privée.

Ce que dit Judith Rochfeld est intéressant. Ceci dit, de mon point de vue de praticien, je n'en perçois pas du tout l'utilité.

Selon vous, le dispositif actuel permet à toute personne, comme Max Shrems, d'aller devant un juge français et de dire : « On n'a pas respecté mes données » ?

Complètement. Là où je vous rejoins, c'est qu'il y aurait, dans l'introduction d'un article dédié, une forme d'autonomie. Il y a la vie privée, d'un côté. De l'autre, on peut parler de traçabilité, mais en disant que cela ne rejoint pas la vie privée, on ne se réfère qu'au sens que donne le Code civil.

Tout à fait, je parle d'une introduction dans le Code civil.

Pour moi, la protection des données à caractère personnel est un élément du droit au respect de la vie privée. C'est l'un de ses aspects assez spécifiques, notamment au travers du traitement automatisé ou non.

Quand je vois une juridiction judiciaire, dans une affaire relative à une prétendue liaison d'un homme, et que le président du tribunal de grande instance de Paris exclut justement l'application de la loi *Informatique et Libertés*, en disant qu'il ne peut pas y avoir de cumul entre cette législation et l'article 9 du Code civil, je ne suis pas d'accord.

Je pense qu'il y a une véritable autonomie de la protection des données à caractère personnel et qu'elle n'a pas besoin d'être réintégrée au Code civil. C'est une réglementation propre, avec un champ d'application très large tout à fait susceptible de s'appliquer de manière générale.

C'est là où nous divergeons.

Une reconnaissance d'un droit propre de la protection des données à caractère personnel me semble d'autant moins utile que le Conseil constitutionnel l'a déjà rattachée au droit au respect de la vie privée. Il l'a donc mis en avant, au niveau d'un droit fondamental...

La proposition ne serait pas forcément de la reconnaître comme un droit fondamental de suite, mais au moins d'un droit subjectif, présent dans le Code civil.

C'est un droit de la personnalité...

Ce que je trouve extrêmement intéressant, c'est que la protection de la vie privée, au travers du Code civil, me semble effectivement plus difficile à mettre en oeuvre, alors que l'exercice des droits qui résulte de la loi *Informatique et Libertés*est simple : il y a des conditions et l'on vérifie si elles sont remplies. Si c'est le cas, on se borne alors à en faire application. À mon avis, la protection existe complètement aujourd'hui.

Et vous trouvez ces droits suffisamment sanctionnés par les juges ordinaires pour ne pas proposer un article plus général, du point de vue judiciaire ?

Tout à fait. À mon sens, dans l'ensemble des jurisprudences que je consulte, il existe une protection. Il est vrai que souvent, dans l'analyse qui est faite par le juge judiciaire, on peut considérer qu'il n'y a pas une intégration complète de l'enjeu de la protection des données personnelles.

C'est-à-dire que le juge judiciaire passe à côté de la protection...

Exactement.

Je suis assez d'accord avec vous. La loi de 1978 reste une loi spéciale, en dehors du droit commun de la personne.

Oui, mais cela pourrait être encore plus le cas pour le juge administratif. Or, le juge administratif n'a aucun problème à appliquer les règles. Quand je vois la jurisprudence du Conseil d'État, en train de se préciser de plus en plus, je trouve qu'effectivement, c'est assez intéressant.

À mon sens, il est vrai que c'est une réglementation spécifique, mais qui touche tellement, aujourd'hui, le quotidien, toutes les activités économiques, particulièrement avec la commercialisation des données à caractère personnel, que l'on ne peut pas l'ignorer...

C'est ce décalage qui est regrettable, entre une utilisation qui est quotidienne et qui fait partie d'attaques « quotidiennes » que peuvent vivre les individus, et le fait que la protection ne soit pas rentrée, en tant que droit tout à fait ordinaire et général, à l'instar d'autres droits subjectifs de la personnalité, dans le droit commun. Ce décalage me paraît, à notre époque, paradoxal.

Pour moi, c'est un problème d'interprétation de la loi *Informatique et Libertés* : quand je vois l'arrêt de la chambre criminelle de la Cour de cassation sur les traitements des données à caractère personnel qui, à aucun moment, ne parvient à la conclusion que le fait d'aller sur Internet, de prendre un crayon et de lister les adresses IP, permet l'identification des individus je suis sceptique...

Sur l'adresse IP, le caractère indirect...

Exactement. Comment, à la lecture des définitions de traitement et de donnée à caractère personnel, la Cour de cassation a-t-elle pu parvenir à dire qu'il n'y a pas de traitement de données à caractère personnel ? À la limite aurait-elle pu dire qu'il y avait seulement un traitement non automatisé. Mais, cette circonstance n'aurait en l'espèce pas pu jouer puisque les dispositions de l'article 25 de la loi *Informatique et Libertés* prévoient justement un régime d'autorisation préalable pour tout traitement, automatisé ou non, portant sur des infractions. Mais la Cour de cassation ne s'est pas intéressée à cela, ce qui relève, selon moi, d'une mauvaise lecture des dispositions qui existent.

Pour aller dans le sens de ce que disait Judith Rochfeld n'y a-t-il pas un problème de délimitation de ce qui relève de la vie privée, notamment relativement aux données comportementales des individus ? N'y a-t-il pas une instabilité de la nature juridique de ces dernières ? Des données apparemment banales, recueillies (pour la plupart à l'insu de l'internaute) à l'occasion d'une navigation tout aussi banale sur l'Internet (par exemple l'achat en ligne d'un livre) ne semblent pas de prime abord présenter un caractère personnel ; mais si, lors d'une, deux ou trois navigations sur ce site là, ce sont plusieurs dizaines voire plus de cent données qui ont ainsi été collectées sur ce même individu, n'est-on pas, par la précision et l'abondance de l'information prélevée, entré dans la vie privée de celui-ci ? En d'autres termes, des données, banales lorsqu'elles sont considérées isolément, ne deviennent-elles pas personnelles par effet d'accumulation et d'hyper-précision ?

On peut s'interroger sur la qualification que leur apposerait le juge judiciaire. Il n'est pas certain qu'il opte pour celle de vie privée. Il s'agit davantage de personnalité et de « présence numérique », qui peut apparaître comme autre chose que ce que le juge judiciaire approche sous le couvert de la vie privée. C'est pour ça que je voudrais l'aider en lui donnant un article qui l'incite à réfléchir autrement. La question s'était justement posée dans les affaires de segmentation bancaire, dont le Conseil d'État s'était emparé. C'était une très belle question : est-ce que la connaissance et le traitement des comportements des individus – qui permettaient aux banques d'anticiper les risques des prêts accordés – constituaient des traitements sur des données à caractère personnel ? Est-ce que cette segmentation comportementale était identifiante ? De façon assez innovante, le Conseil d'État a fait entrer cette segmentation comportementale dans la qualification de données à caractère personnel. Que ce soit « purement » identitaire n'était pas le fond du problème. Pour nous, juristes de droit privé, ces éléments ne seraient pas entrés facilement dans la vie privée ; ils n'étaient pas, à proprement parler, identifiants. La réponse du Conseil d'État n'était donc pas acquise d'avance. Ce que je voudrais, quant à moi, c'est que tout justiciable puisse aller devant le tribunal, comme il peut le faire pour défendre sa vie privée, et qu'il puisse dire, comme Max Shrems : « j'ai un droit au respect de mes données personnelles », « je demande une indemnisation pour la violation de ce droit subjectif, ce sans démonstration d'un préjudice... ». Il y aurait évidemment à repenser une articulation avec le rôle de la CNIL.

Dans la perspective de ce que vous venez de dire : les cartes de fidélité des magasins qui mémorisent les achats me semblent entrer, par endroits mais franchement, dans la vie privée de leur titulaire.

Cela ne relève pas exactement de la vie privée, mais davantage de la personnalité.

Si le client a acheté de la nourriture casher ou hallal, s'il a acheté des préservatifs, s'il a acheté des couches pour bébé, la mémorisation des achats permet d'engranger des données sur sa vie familiale, voire intime.

Pour le juge judiciaire, il faudrait que cela puisse être relié à un élément composant son identité...

En l'espèce, cela le serait puisque la carte est nominative.

Encore faut-il qu'il y ait une collecte.

Je trouve cette question de la création d'un droit subjectif extrêmement intéressante. Pour moi, dès lors qu'il y a une violation de la loi *Informatique et Libertés*, une loi spéciale, il y a nécessairement une violation de la vie privée. Je pense que l'un des problèmes vient de l'interprétation de l'article 9 du Code civil et de la définition de ce qu'est la vie privée. Déjà, la distinction entre l'intimité de la vie privée et la vie privée pose problèmes. D'un point de vue juridique, si on regarde toute la littérature, les manuels de droit, la doctrine, la définition de la vie privée est extrêmement difficile. Mais le terme lui-même, de par sa généralité, ne fait pas obstacle à affirmer que si l'on a violé la loi *Informatique et Libertés* parce qu'on a communiqué la liste de mes dix dernières commandes chez Amazon, on viole également nécessairement ma vie privée.

À cet égard, connaissez-vous beaucoup d'affaires où un justiciable est allé devant le tribunal en arguant d'une violation de son droit à la protection de la vie privée parce que des données avaient été collectées ?

Non, d'abord parce qu'il n'y a pas énormément de contentieux. Pour les gens, la divulgation de leurs données ne représente pas un préjudice énorme ; elle les agace énormément, mais il est difficile d'assumer 2 000 € de frais de justice pour défendre ses données. Mais cela ne me dérangerait absolument pas, en tant qu'avocat, de viser à la fois l'article 9 et les articles de la loi *Informatique et Libertés*.

Mais la loi de 1978 n'a pas été conçue comme intronisant un droit subjectif individuel. Donc cela ne vous choquerait pas et vous le défendriez ? Pensez-vous que, devant un juge judiciaire, vous aboutiriez ?

Je pense que, en expliquant bien ce qu'est l'article 9, quel intérêt il protège (à savoir le droit à l'autodétermination d'un individu dans ses rapports avec la société et autrui), j'arriverais à démontrer – du moins je l'espère – qu'en violant la loi *Informatique et Libertés*, on viole nécessairement la vie privée, c'est-à-dire un droit à l'autodétermination.

J'aimerais voir émerger un contentieux de cet ordre... L'idée d'un droit subjectif, que chacun pourrait brandir contre des violations ne me paraît cependant pas acquise aujourd'hui. Je souhaite cette reconnaissance, mais elle ne me paraît pas établie en l'état actuel des mentalités judiciaires et des textes. La superposition que vous opérez, entre la loi de 1978 et une violation d'un droit subjectif, qui pourrait

de suite tomber sous une sanction de l'article 9 n'est pas évidente de mon point de vue (outre les questions de définition de ce qui relève de la vie privée, sur lesquels nous avons déjà discuté).

Ma difficulté, en tant que praticien, ce serait peut-être de démontrer que j'ai un préjudice distinct entre la violation de la loi *Informatique et Libertés* et celle de l'article 9. Le juge me demanderait probablement en quoi, puisque c'est le même intérêt, j'ai légitimité à agir différemment. En visant à la fois l'article 9 et l'une des dispositions de la loi *Informatique et Libertés*, il faut que j'arrive à justifier de deux préjudices distincts, d'où l'intérêt de viser les deux textes.

Mais l'article 9 ne requiert pas le préjudice : la violation en soi d'un droit subjectif ne le requiert pas...

Mais à partir du moment où on engage une action, c'est pour obtenir des dommages et intérêts !

Si je vise l'article 9, c'est pour en retirer des dommages et intérêts, effectivement. La loi *Informatique et Libertés* permettrait simplement de faire retirer la donnée.

L'article 9 n'offre-t-il pas des outils intéressants ? Je puis me contenter de l'euro symbolique de dommages-intérêts, mais solliciter en outre des mesures très intéressantes comme la publication, la diffusion de la condamnation, coûteuses à maints égards pour le défendeur.

Si j'avais une action comme celle-là, j'invoquerais les deux textes. Ce qui me frappe dans notre conversation, c'est que, en réalité, à aucun moment je ne me pose cette question de la relation des deux textes, parce que, quand je travaille sur le champ d'application de la loi, je regarde les conditions d'application de la donnée à caractère personnel et, une fois que les conditions en sont remplies, les droits qui en découlent sont simples à appliquer. La véritable démonstration tient au fait de savoir s'il y a une donnée, un caractère personnel et s'il y a un traitement. Une fois qu'il y a une donnée et un caractère personnel, dans 99,99 % des cas, il y a un traitement. Je raisonne en termes d'application. Il y a des conditions : « Est-ce une information ? Oui », « Relative à une personne physique ? – Oui », « Identifiée ou qui peut être identifiable par des éléments propres ? ». Ensuite, l'article 2 de la loi dispose que « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification, dont dispose ou auxquels peut avoir accès le responsable du traitement ou tout autre personne* ». Je fais une application extrêmement stricte de ces dispositions dont les conditions sont larges ; c'est pour cela que je ne me pose pas la question de la vie privée.

C'est partir du principe que tout a été *a priori* bien fait. Pour ma part, je pars de la position du justiciable : je découvre, par exemple, qu'on ne m'a pas prévenue qu'il y aurait un *cookie* sur mon disque dur et un traçage comportemental alors que je ne le souhaite pas, pas plus que je ne souhaite faire l'objet d'une publicité ciblée. Puis-je attaquer le responsable du traitement, selon votre système, pour violation de mes données personnelles ?

Pour violation des données personnelles, oui, et j'irais même plus loin : si j'arrive à démontrer que j'ai eu un préjudice du fait que le professionnel a eu une information

très particulière sur moi – par exemple le fait d'avoir des enfants – je ne vois aucun problème pour viser en même temps l'article 9.

Mais pourra-t-on jamais démontrer le préjudice ?

En l'état actuel, que diriez-vous à un client qui voudrait, en France, mener la même action que celle que Max Shrems a mené en Autriche ?

Mon premier réflexe ne serait pas d'aller devant les juridictions. Mon premier réflexe, pour des raisons d'efficacité, serait d'aller devant la CNIL pour voir si elle ne peut pas faire avancer les choses plus rapidement.

Combien de temps prendra la réponse de la CNIL ?

Cela peut prendre un peu de temps, sauf si la violation est extrêmement grave. Si j'allais en justice pour un cas de violation, je ferais constater que l'on se trouve dans le champ d'application de la loi et ferais juger si les traitements sont conformes à la loi *Informatique et Libertés*. Il est facile de bousculer les choses. Cela reposerait sur la démonstration d'une faute, dans le sens où il y aurait la mise en oeuvre d'une opération constitutive d'une inégalité.

Suggérez-vous que la loi est ineffective ? Vous semblez penser que l'immense majorité des traitements opérés ne sont pas conformes à la réglementation.

Je pense que la loi est mal appliquée par certaines juridictions. Elle reste néanmoins très applicable.

Si on veut la respecter parfaitement, il est extrêmement difficile de décrire les traitements, les données collectées... dans un texte de conditions générales. Parfois les traitements sont extrêmement complexes à décrire.

7. Les préjudices indemnisables et les sanctions effectives

Qu'obtiendrait le client de La Redoute qui aurait fait l'objet d'une publicité ciblée, sans avoir donné son consentement à la pose de *cookies* ? Que viseriez-vous ?

Il obtiendrait peu de chose, car l'évaluation du préjudice serait difficile. C'est pour cela qu'il n'y a pas plus d'actions.

Il obtiendrait peut-être quelque chose de symbolique ; je viserais l'article 9 et la loi *Informatique et Libertés*, cumulativement.

Je ferais la même chose. Concernant le contentieux : dans l'arrêt *École de Laëtitia*, on a visé les deux ; dans l'arrêt concernant la prétendue liaison d'un homme politique, le juge judiciaire a déclaré que le droit des données personnelles n'a pas à être appliqué sur le fondement de l'article 9. Cela relève plus d'une bonne application de la réglementation ; il y a une évolution plutôt positive du côté des juridictions judiciaires. Par exemple, à la suite de l'arrêt de la Cour de cassation, il y a eu une ordonnance de référé du tribunal de grande instance dans l'affaire de

Jean-Yves Lafesse qui reconnaissait que, en réalité, il y avait une possibilité d'identification.

J'ai l'impression que devant le juge judiciaire, ce contentieux cache la forêt. On s'est focalisé sur la qualification de données à caractère personnel, et on a oublié toute l'importance que pourrait avoir ce droit à une protection générale.

Il n'y a pas plus de contentieux venant porter ces questions, mais je vois tout de même une évolution qui n'est pas si négative que cela. Dans le cas de l'adresse IP, seul le juge judiciaire a mis du temps à l'accepter. Le Conseil constitutionnel a très clairement dit, dès 2004, que l'adresse IP est une donnée à caractère personnel. Dans l'ensemble, la législation est bien appliquée.

Comment expliquer ce décalage, relativement au juge judiciaire, habituellement plus rapide et plus réactif sur les questions de droits de la personnalité ?

Il n'a peut-être pas été saisi de contentieux suffisamment rapidement.

Surtout, il faut prendre en compte la position de la chambre criminelle en matière notamment de procédures contre la contrefaçon : elles allaient tomber et, à mon sens, c'est plutôt un choix de politique jurisprudentielle qui a été fait.

La question de l'adresse IP est à corréler avec le débat qu'il y a eu sur la possibilité de prendre les adresses IP pour dresser des procès-verbaux d'infractions au Code de la propriété intellectuelle par les agents assermentés SACEM, etc.

Pour revenir aux évolutions de la jurisprudence, je relève que si le juge administratif est plus vigilant à l'application de la loi *Informatique et Libertés*, c'est peut-être surtout pour une raison historique, puisque le fichage public est à l'origine de cette loi. Et c'est sans doute grâce à la fréquence à laquelle il a eu à se prononcer sur ces sujets que le Conseil d'État commence à esquisser des analyses particulièrement intéressantes, notamment sur des notions aussi importantes que l'interconnexion par exemple.

Propos recueillis par Estelle Devisme et Aurore Marie, étudiantes de l'École de Droit de Sciences Po