DONNÉES PERSONNELLES : L'APPROCHE DE LA CNIL

PAR MONSIEUR LAURENT LIM

JURISTE, CHARGÉ DE MISSION AU SERVICE DES AFFAIRES EUROPÉENNES ET INTERNATIONALES DE LA CNIL

Merci beaucoup, Monsieur le Président, pour votre invitation. Deux précisions, immédiatement. La première étant que ma parole sera, aujourd'hui, à titre personnel. Je ne serai pas un représentant officiel de la CNIL, mais je vais quand même tâcher de vous donner quelques informations intéressantes. Deuxième précision, je ne suis pas forcément le spécialiste des réseaux sociaux à la CNIL, puisque je travaille au service des affaires internationales. Mais, il doit y avoir des points de convergence qui peuvent être tout à fait intéressants. Je vais essayer de donner un éclairage sur ce qui ce passe au niveau international, et à mesure cela peut toucher aussi les grands acteurs comme Facebook, Google, etc. Alors, je vais vous épargner une présentation fastidieuse de l'institution que vous connaissez tous. Vous vous rappeler qu'il s'agit d'une autorité administrative indépendante avec des missions de conseil, de contrôle, de sanction ; une mission a priori, une mission a posteriori. Je n'ai pas les derniers chiffres d'activité, mais en 2010, on a reçu environ 70 000 déclarations dans l'année. On a fait près de 300 contrôles sur place, une centaine de mise en demeure, quelques avertissements et quelques dizaines de sanctions financières.

Concernant les sanctions financières et les 150 000 € infligés à Google, il s'agit du montant maximum prévu par la loi française. Mais, pour relativiser et remettre cela dans un contexte davantage international, on peut prendre le cas de l'Espagne. L'autorité espagnole a sanctionné Google à hauteur de 900 000 €. Et par ailleurs, le fisc français poursuit Google pour un redressement fiscal de l'ordre du milliard d'euros. Il y a quelques semaines, le Commissaire européen à la concurrence a abandonné ses poursuites contre Google pour les infractions qui lui étaient reprochées en matière de non-respect du droit de la concurrence. Et là, les enjeux étaient de plusieurs milliards d'euros. Donc effectivement, cette mise en perspective milite pour que soit renforcé notre pouvoir de sanction financière.

Je rappelle rapidement que la CNIL est une commission collégiale de dix-sept commissaires : deux députés, deux sénateurs, deux conseillers à la Cour de cassation, deux conseillers au Conseil d'État, deux conseillers à la Cour des comptes et sept personnalités qualifiées. Notre Présidente vient d'être très récemment réélue et la CNIL va quelque peu

reconfigurer ses directions, notamment pour se mettre en ordre de bataille en vue de l'adoption du règlement européen. Donc, on aura une direction de la conformité et des affaires juridiques. On voit bien qu'on va davantage aller vers les outils de conformité. Et c'est un peu l'angle d'approche qui a été celui de la CNIL par rapport aux réseaux sociaux : des recommandations techniques. C'est plutôt un travail de prise de conscience des risques. Puis, on a aussi le sujet de l'éducation au numérique qui est important, il s'agit d'un travail d'éducation qui s'adresse aux jeunes.

Je propose de revenir rapidement sur le droit à l'oubli en essayant de contextualiser quand j'en aurai l'occasion. Permettre une prise de conscience, on l'a dit, c'est le travail de la CNIL. On a récemment travaillé sur la réputation numérique à l'occasion du *Safer internet day 2014*. On a publié une petite plaquette sur ce sujet-là, avec un certain nombre de recommandations. Par exemple, pour prendre la mesure de l'importance des plaintes qui concernent les réseaux sociaux, simplement pour Facebook, en 2008 on avait environ 300 plaintes, et en 2010 on en était à 1000 plaintes. Donc, en deux ans, on a eu une progression de 42%. On voit bien que les gens ont de plus en plus recours aux services de la CNIL lorsqu'ils sont confrontés à une problématique de suppression de données. Alors, le droit à l'oubli n'est pas une notion si neuve que ça. Finalement, il s'agit de la combinaison de l'obligation de répondre aux demandes d'opposition, lorsqu'elles sont faîtes, et du principe de limitation de la durée de conservation des données. J'ouvre ici une parenthèse sur les discussions au niveau international, le principe de limitation de la durée de conservation des données – qui va être cœurs des obligations qu'on va demander aux réseaux sociaux, aux opérateurs sociaux de respecter – ne se retrouve pas dans l'ensemble des textes internationaux. Cela peut être un enjeu dans les négociations. Par exemple, les lignes directrices de l'OCDE, qui n'ont pas de force contraignante, ne comportent pas de principes de limitation de la durée de conservation. Il faut aussi dire que l'OCDE est un cénacle au sein duquel les États-Unis sont très influent. Le droit d'opposition est un objet d'enjeu important dans les négociations internationales. On voit que le projet de règlement essaie de renverser la charge de la preuve en matière de droit d'opposition, et qu'au niveau du Conseil de l'Europe, la Convention 108 actuellement en cours de renégociation va aller dans le même sens en reprenant la même idée. Ce sera au responsable du traitement de démontrer qu'il est absolument nécessaire pour lui de conserver les données alors qu'il est confronté à une demande d'opposition. Sur ce sujet-là, un certain nombre de pistes de solutions a été proposées par la Commission et a été soumis à consultation publique. L'une des idées serait d'élaborer un référentiel standard des durées de

conservation. Cela permettrait d'avoir un étalon de référence et de fixer ces durées maximales de conservation une fois pour toute. L'idée aussi de mettre l'utilisateur en position de pouvoir mieux maitriser ses données en lui donnant des outils adaptés. On veut par exemple limiter la diffusion d'une information dans sa durée en faisant en sorte que l'utilisateur puisse lui-même fixer la date de péremption de la publication de son information. Autre piste : élargir les possibilités d'agir pour l'utilisateur auprès des hébergeurs, parce qu'il est parfois difficile d'identifier le responsable du traitement, soit parce qu'il se dissimule, soit parce qu'il a changé de coordonnées. Une solution plus simple pour le retrouver serait de donner la possibilité à l'utilisateur de s'adresser à l'hébergeur pour pouvoir obtenir la suppression des données, et ce en l'absence de réponse du responsable de traitement. Puis, afin de permettre une meilleure efficacité de la mise en œuvre de ce droit à l'oubli, tout cela pourrait aller de pair avec une obligation juridique de déréférencement dans les moteurs de recherche. Ce sont là des idées, des pistes de solutions qui ont été soumises à consultation publique en 2013. J'ai, rapidement, quelques chiffres à vous donner. Par exemple, cette consultation de près de 3300 internautes nous apprend que 86% d'entre eux vérifient s'il y a des informations qui les concernent sur internet. Donc, ils se « googlelisent » eux-mêmes. Et 47% constatent qu'il y a des informations diffusées sans leur accord. Enfin, 17% considèrent que la diffusion de ces données a eu une influence négative sur leurs vies professionnelles.

Tout cela est soumis à discussion, et le point de vue des professionnels a été recueilli : ils sont plutôt en faveur du droit à l'effacement que du droit à l'oubli. Effectivement, ils ne sont pas forcément d'accord sur l'idée d'élaborer un référentiel des données maximales de conservation. Et sur la possibilité d'agir directement auprès de l'hébergeur, il y a aussi des réserves parce que la plupart des professionnels interrogés considéraient qu'il revient plutôt aux tribunaux, et non aux hébergeurs, de se prononcer sur la publication et la diffusion d'une information. Quant au thème de l'éducation au numérique, il n'a pas été retenu comme grande cause nationale 2014 comme nous le souhaitions.

Pour en terminer, très rapidement, je voudrais rebondir sur certains aspects qui ont été évoqués ce matin, en particulier l'enjeu économique. Il y a, derrière cela, la commercialisation des données par les réseaux sociaux. Ces enjeux économiques sont énormes ; on le voit bien dans le contexte de l'actualité de 2013, avec les révélations dans la presse de l'affaire Snowden et avec l'implication supposée d'un certain nombre de gros acteurs dans des mécanismes comme les procédures de programme de surveillance électronique de masse. Effectivement, il y a une perte confiance, ce qui fait que pas mal d'utilisateurs-entreprises se

demandent s'il ne faudrait pas se tourner vers un *cloud* européen plutôt que d'envoyer toutes nos données aux États-Unis. A la CNIL, un groupe de travail s'est penché sur cette question de l'accès par les autorités administratives étrangères aux données personnelles de citoyens français et européens. A cette occasion, on a pu essayer de décortiquer la loi américaine, le Patriot Act, la Loi FISA qui autorisent les agences de renseignement à collecter des données de renseignement sur n'importe quelle personne, à l'étranger, en dehors des États-Unis. On a pu voir que lorsque une agence américaine demande la communication d'informations à une société qui se trouve sur le territoire américain, cette société est tenue par le secret. Elle a l'obligation de garder le secret, de ne pas dire qu'elle a reçu ces demandes. Effectivement, la perte de confiance suite aux révélations des mécanismes est énorme. Cela se traduit par un manque à gagner important pour l'économie numérique américaine. Cela se chiffre en milliards. Du coup, on prend davantage en compte les enjeux de *lobbying* qu'il y a actuellement dans les processus de réforme des textes au niveau européen, puisque le projet de règlement a reçu 4000 amendements, du jamais vu. Il faut bien avoir conscience de l'importance de ces enjeux financiers ; on le voit même en dehors de la réforme des textes en matière de protection des mails puisque vous avez peut-être entendu parler, actuellement, d'une négociation qui concerne un partenariat transatlantique sur le commerce et l'investissement. Peut-être l'un des plus gros accords commerciaux entre l'Union européenne et les États-Unis ; il y a de gros débats pour savoir si la question de la protection des données doit être incluse, s'il doit y avoir des dispositions dans ce traité ou pas. Nous y sommes fortement opposé car l'inclusion de disposition dans ce traité serait supérieure au droit dérivé européen et donc, du coup, s'imposerait aux règlements. De ce fait, on voit bien tous les enjeux qui peuvent y avoir derrière.

Dans la présentation a été évoqué l'*accountability*. C'est une notion qu'on retrouve non seulement dans le projet de règlement mais aussi dans l'OCDE et au Conseil de l'Europe. On voit donc bien que les textes européens et internationaux convergent vers l'intégration de cette notion-là. Il y a donc une nécessité de faire des études d'impact, de mettre en place des contrôles internes de conformité. Puis, il y a le *privacy by design*. Nous, ce qui nous fait un petit peu peur, c'est l'analyse de risque : jusqu'où va-t-on dans l'analyse de risque ? Effectivement, on peut moduler les outils, la charge administrative, en fonction de l'analyse du risque qu'on peut faire, mais il ne faut pas que cela affecte les principes même. Merci.