Protection des données en Europe

« *Un changement de culture* »

INTERVIEW

ISABELLE FALQUE-PIERROTIN

Présidente de la CNIL et du G29

La présidente de la CNIL, qui assure également depuis 2014 la présidence du G29, explique les changements induits par le règlement européen pour les autorités de protection des données et les missions du nouveau Comité européen de la protection des données (*European data protection board*).

■ **Quels sont les changements issus du Règlement général sur la protection des données (RGPD) concernant les autorités de contrôle des données ?**

Le règlement européen ouvre une nouvelle époque pour les autorités de protection des données, non seulement parce qu'elles auront à faire respecter une législation qui reconnaît des droits nouveaux aux personnes, mais aussi parce qu'elles vont devoir renforcer leur fonctionnement collectif, travailler de façon beaucoup plus intégrée avec leurs homologues européens, qu'il s'agisse de prendre des sanctions communes, ou de développer une jurisprudence et une doctrine communes sur un certain nombre de sujets. C'est un changement de culture important. En outre, elles devront s'approprier de nouveaux outils, comme les études d'impact de la vie privée, de nouveaux concepts comme le *privacy by design*, qu'il leur faudra décliner de façon opérationnelle.

■ **Quelles premières actions mener dans ce sens ?**

Le règlement européen est un texte extrêmement complexe qui résulte de divers compromis : c'est au G29 d'en tirer des obligations précises pour les acteurs. L'objectif principal du Règlement européen est l'harmonisation de la loi européenne et le G29 a donc souhaité identifier, dans ses plans d'action pour 2016 et 2017, les points principaux sur lesquels il est essentiel que l'harmonisation ne soit pas rompue par des interprétations divergentes entre les autorités nationales. Sur ces principaux points, le G29 va émettre des lignes directrices (*guidelines*) pour que toutes les autorités puissent avoir la même interprétation. En 2016, le G29 a ainsi publié des lignes directrices sur le droit à la portabilité, le rôle du DPO (*Data Protection Officer*), la notion d'autorité chef de file qui est essentielle pour éviter le forum *shopping*. Il en émettra d'autres au cours de l'année 2017.

C'est un travail considérable, surtout dans la période actuelle où l'Europe est malmenée, car cela rétroagit aussi sur la détermination des uns et des autres à développer des interprétations communes. En outre, certains éléments sont par nature liés au règlement mais relèvent du droit national, par exemple concernant les procédures de sanction : le règlement ouvre la possibilité d'une sanction collective, mais les procédures ne sont pas traitées par le règlement européen, et relèvent des lois nationales. Le règlement réserve également des exceptions qui sont renvoyées au droit national,

par exemple, dans le domaine de la santé ou du journalisme. Enfin, il prévoit des domaines dans lesquels la loi nationale peut ajouter aux conditions du règlement. Le puzzle est donc très complexe à assembler.

Pour y parvenir, nous privilégions un processus de concertation avec les acteurs. Dans cette perspective, le G29 organise des « *Fablab* », qui sont des ateliers de co-construction de ces règles d'interprétation du règlement européen en fonction des réalités du terrain. Ces ateliers réunissent les représentants des entreprises à travers leurs fédérations professionnelles, mais aussi des représentants de la société civile (Bureau européen des unions de consommateurs – BEUC). Nous encourageons aussi les autorités nationales à organiser à leur niveau des concertations préalables aux *Fablab* européens, comme le fait régulièrement la CNIL. Le prochain *Fablab* aura lieu en avril à Bruxelles sur les questions du profilage, du consentement et des notifications de failles de sécurité. Nous espérons que cette co-construction permettra à l'écosystème numérique européen de se rassembler de façon unanime à travers ces interprétations du règlement européen.

■ Comment mettre en œuvre le principe de sanctions communes ?

Le règlement offre en effet la possibilité pour les autorités de protection de prendre collectivement une sanction vis-à-vis d'un acteur qui aurait des traitements à destination de plusieurs pays européens (traitements transnationaux). Celle-ci peut atteindre 4 % du chiffre d'affaires mondial de l'acteur concerné, ce qui représente un niveau élevé et donc très dissuasif. Elle sera prise par l'autorité chef de file mais au nom et pour le compte des 28 autorités nationales. Ce principe est intéressant parce qu'il donne la pleine mesure de la capacité de l'Union européenne à dialoguer d'une seule voix vis-à-vis des grands acteurs mondiaux. C'est une avancée considérable pour la protection des données mais elle nécessite une coopération totalement inédite entre les autorités nationales.

■ Comment les nouveaux outils seront-ils déclinés au niveau national ?

Le règlement européen importe des outils d'inspiration anglo-saxonne, comme la certification, les labels ou encore les codes de conduite, qui doivent compléter les procédures plus classiques d'autorisations ou d'avis donnés par les autorités nationales. À la CNIL, nous connaissons bien ces outils parce que nous les développons depuis de nombreuses années à travers une approche de co-régulation. Notre postulat est que, face au numérique, il est illusoire d'encadrer les pratiques par des autorisations ponctuelles, liées à un traitement spécifique ; il faut en réalité mettre en place une sorte de continuum de conformité vis-à-vis des pratiques d'un secteur. Pour cela il faut établir une relation nouvelle entre le régulateur et les acteurs : ainsi la CNIL a lancé en France les packs de conformité. Ceux-ci sont construits sur la base des négociations menées avec un secteur économique donné : il s'agit de mettre à plat ses usages, présents et futurs, et de rechercher en concer-

tation avec ce secteur un cadre permettant d'abriter ces traitements. Les premiers packs de conformité ont porté sur les compteurs communicants avec le secteur énergétique, le logement social, l'assurance, ou encore le secteur social. La CNIL mène en outre des travaux avec le secteur automobile sur la voiture connectée. Avec l'entrée en vigueur du règlement, des mécanismes de certification, des codes de conduite, ou des labels, viendront se substituer à ces packs de conformité. L'objectif de la CNIL consiste à faire en sorte que les packs de conformité déjà existants puissent devenir des standards européens. En effet, même si aujourd'hui un pack de conformité ne contraint en principe que les parties prenantes de la fédération professionnelle avec laquelle il a été négocié, à terme, la commission européenne pourrait décider d'en étendre les obligations et les bénéfices à l'ensemble d'un secteur, sous forme d'un code de conduite. C'est une disposition qui existe déjà dans d'autres secteurs, comme le domaine social où des principes négociés par des partenaires sociaux ont ensuite été étendus de façon générale.

C'est un nouveau paysage de régulation qui est en train d'émerger. Demain, la régulation s'organisera sur deux jambes : d'une part, ces outils d'accompagnement souples, négociés avec les acteurs dans une approche sectorielle ; d'autre part, la sanction. Plus elle devient élevée, plus il est important pour un secteur de négocier avec le régulateur des conditions de développement d'usage et d'innovation conformes à la législation.

■ Que changera la mise en place du Comité européen de la protection des données (CEPD) en 2018 ?

Le CEPD remplacera en mai 2018 le G29 et aura deux principaux domaines d'action : le contentieux c'est-à-dire l'instance où se négocieront les sanctions communes pour les traitements transnationaux, et une activité normative d'harmonisation de la conformité à travers une doctrine et des référentiels sectoriels communs. Le CEPD sera une institution européenne (*european body*). Le G29, reste aujourd'hui encore un groupe informel, même s'il s'est affirmé sur le plan politique et opérationnel. Le renforcement institutionnel au travers de la création du CEPD permettra de dialoguer d'une façon plus équilibrée avec le reste du monde. Nous souhaitons que cette institution européenne ait une gouvernance à la fois plus intégrée, mais aussi distribuée. Nous voulons une institution européenne qui parvienne à parler d'une seule voix, mais avec une gouvernance collective portée par les autorités nationales de protection des données.

■ Comment y parvenir ?

Nous sommes en train de réfléchir à une organisation des pouvoirs entre les autorités nationales : pour couvrir tous les champs de la régulation, les autorités nationales vont devoir se spécialiser et en même temps mutualiser leurs efforts pour que leurs propositions convergent au final au sein du CEPD. Celui-ci devra mettre en musique l'ensemble de ces compétences en les traduisant par une voix unique. Certaines autorités nationales ont par exemple une bonne compétence sur les codes de conduite ; d'autres sont plus avancées sur le plan technologique. C'est un dispositif innovant, inspiré du fonctionnement de l'Internet avec un système en réseau. C'est aussi une gouvernance plus complexe, mais plus riche et au final plus solide.

Nous sommes déjà dans cette épure au sein du G29 : une dizaine de groupes de travail travaillent en parallèle sur différentes problématiques liées au règlement, au sein desquels participe une quinzaine d'autorités.

■ Comment s'organise la protection des données au niveau international ?

L'ensemble des autorités de protection des données se regroupe au sein de la Conférence mondiale. Cette instance, extrêmement active, est le théâtre d'une stratégie d'influence considérable entre les grandes parties du globe, parce que les enjeux économiques et ceux liés à une vision globale du numérique sont très importants. La présence francophone s'y exprime au travers de la CNIL, mais aussi à travers de l'Association francophone des autorités de protection des données personnelles (AFAPDP) dont la CNIL assure le secrétariat général et qui regroupe 17 autorités de pays francophones. Un de mes objectifs est de renforcer la participation francophone au sein de la Conférence mondiale pour faire entendre une autre voix que celle anglo-saxonne qui reste très majoritaire dans cette instance.

■ Peut-on imaginer aller vers des standards mondiaux de protection des données ?

Aller vers des standards mondiaux aujourd'hui consisterait probablement à s'aligner sur les moins-disants. Nous travaillons plutôt à l'heure actuelle sur des schémas d'interopérabilité : l'Europe doit être capable d'organiser des chemins de conformité entre les demandes du continent européen et celles du reste du monde. Par exemple, nous avons mené en 2014 une négociation avec la zone asiatique sur l'encadrement des flux transfrontières de données avec l'Europe. Nous avons bâti un référentiel qui permet d'organiser l'articulation entre les obligations liées au BCR[1] européens et les CBPR[2] établies par l'APEC[3]. L'Asie est en effet en plein essor sur le plan numérique. Par ailleurs, la CNIL a invité au mois de mai 2016 à Paris en marge d'une réunion de l'OCDE ses homologues asiatiques pour leur présenter le règlement européen, car celui-ci les concerne directement à compter de mai 2018 : en effet, un acteur qui effectue des traitements de données à destination de citoyens européens, même sans présence locale, se verra appliquer le droit européen.

■ Quels sont les moyens financiers et budgétaires à mettre en œuvre pour cette organisation européenne de la protection des données ?

Les autorités nationales expriment dans tous les pays un besoin de ressources supplémentaires pour honorer les obligations du règlement et nous envisageons de prendre une position publique sur ce sujet à la prochaine plénière du G29, début février. ■

Propos recueillis par Élisabeth Coulomb
le 30 janvier 2017.

1. *Binding Corporate Rules*.
2. *Cross-Border Privacy Rules*.
3. Coopération économique pour l'Asie-Pacifique.