

## **7<sup>ème</sup> Conférence annuelle de l'AFAPDP**

**Les 21 et 22 novembre 2013**

**Marrakech**

*Discours prononcé à l'occasion de la séance inaugurale*

### **Isabelle FALQUE-PIERROTIN**

*Secrétaire générale de l'AFAPDP*

*Présidente de la CNIL*

Monsieur le ministre, Mesdames, Messieurs les présidents d'autorités, Madame, Monsieur, Chers participants,

Je voudrais à mon tour remercier les hôtes de la manifestation d'aujourd'hui, le gouvernement marocain et la CNDP qui nous accueillent, remercier également tous les participants, membres de l'AFAPDP ou extérieurs.

Il me revient à la fois de clore ces interventions inaugurales mais aussi d'introduire les sujets de discussion d'aujourd'hui et demain.

Cette année, il nous a semblé que l'actualité internationale était un bon « fil rouge » et qu'elle mettait en lumière beaucoup de questions stratégiques mais aussi des questions qui nous sont quotidiennes.

Cette année est sur le plan international marquée, selon moi, par deux tendances ou événements majeurs.

#### **La concurrence normative**

Cette nouvelle forme de concurrence est celle qui se fait jour entre les systèmes normatifs qui se développent aux Etats-Unis, en Asie, en Europe

En Europe, le projet de règlement qui rénove le cadre juridique de la directive de 1995 est au centre des préoccupations et des lobbys. Avec plus de 4 000 amendements déposés sur ce texte, le Parlement européen a enregistré un record qui témoigne de son importance.

En Asie de même, les réunions sur l'encadrement des flux transfrontières se sont multipliées ...

Sans parler bien sûr de la révision de la convention 108 dont Jean-Philippe Walter vous parlera plus longuement.

Chaque espace géographique se bat donc pour faire prévaloir sa vision de la protection des données personnelles dans le but, notamment, d'attirer la croissance numérique de demain.

#### **L'affaire Snowden ou PRISM**

Avec PRISM nous avons découvert un système de collecte et d'analyse massif, systématique et automatisé de données de citoyens européens opéré par la NSA au nom de la lutte contre le terrorisme. Un système qui s'affranchit du cryptage et qui ne paraît pas s'inscrire facilement dans les cadres juridiques existants.

PRISM c'est également l'existence d'une coopération ou pis d'une alliance entre les géants de l'internet. Une alliance entre les collecteurs de nos données et les autorités publiques américaines ; sans que l'on sache exactement qui dirige qui.

PRISM c'est enfin la révélation du fait que notre vie quotidienne en ligne est entièrement entre les mains d'opérateurs économiques étrangers et qu'elle est l'objet d'une surveillance qui concerne tout le monde ; de la masse des citoyens « anonymes » aux dirigeants étrangers (Brésil).

Les chiffres donnent qui décrivent ce système donnent le vertige. Les données collectées par PRISM ont alimenté 77000 rapports du renseignement américain depuis 2007. L'importance de PRISM pour le renseignement américain est avérée par le fait que dans 15% des rapports de la NSA figurent des données issues de PRISM. Le vertige vient encore du fait que le budget de ce seul programme équivaut presque à celui que la France consacre à la CNIL....

Si nous ne connaissons pas le volume de données concernées par PRISM nous savons cependant que les neuf plus grandes sociétés de l'internet sont impliquées. Pour stocker et traiter ces données la NSA construit un centre de traitement en Utah dont la capacité des bases de données se compte en Yottabits ( $10^{24}$  bits). A ce stade là nous comptons par milliards de milliards de pages de texte !

### **Que montrent ces deux évènements ?**

D'abord que la place des données personnelles est désormais centrale et qu'en 2013 les données ont acquis un pouvoir sur nos vies quotidiennes mais aussi sur l'économie.

On parle de « big data » et d'ouverture des données. On parle de ressource essentielle et de pétrole de l'économie numérique. Ce que nous vivons tous et que vous vivez aussi avec le développement du téléphone mobile c'est la possibilité, malgré un pourcentage d'utilisateurs de l'internet mobile encore très faible, d'un saut « *quantique* » direct dans le numérique. D'un mode de vie tout analogique vers un mode de vie numérique.

Ces téléphones offrent de multiples services comme les communications audio et vidéo, le micro-paiement, le guidage et géolocalisation et tout un écosystème d'applications qui vont du programme télé jusqu'à du suivi médical.

La révolution numérique centrée sur les données est à l'œuvre sur tous les continents.

Ensuite, ces évènements montrent aussi que tout ceci n'est pas un paysage tranquille, que les données sont des armes de conquête (*comme le fut en son temps le cinéma et l'américain way of life*). Un instrument de pouvoir pour les Etats et les entreprises, chacun voulant imposer sa vision et sa dominance. Ce qui frappe c'est que le passage n'est pas si difficile entre les bienfaits de ces services et une vision beaucoup plus noire faite de ciblage, d'espionnage et de surveillance.

Car finalement, ce qu'illustre PRISM c'est qu'il est possible de mettre *a priori* sous surveillance des populations entières dans les actes les plus banals de leur vie quotidienne (SMS, réseaux sociaux, mails,...) et qu'en quelque sorte s'inverse le paradigme de la surveillance.

Tous surveillés par défaut, même sans menace spécifique et probablement avec une conservation sans limite ; de tout ; sur tout le monde. Le nouveau concept est donc la « *surveillance by default* » !

Compte tenu de cette actualité, il me semble que nous sommes arrivés à la croisée des chemins. Les technologies et les usages sont là. Le numérique peut nous apporter des bénéfices considérables mais aussi un risque majeur de surveillance généralisé, il est temps de fixer des balises.

On affirme ici et là que la protection des données est un frein à la lutte contre le terrorisme ou la cybercriminalité, que c'est un frein à l'innovation et pour l'économie

Si le choix est entre le terrorisme et le totalitarisme, entre une concurrence sans règles et l'absence d'innovation alors il va falloir se montrer déterminé pour ouvrir une troisième voie et la francophonie a un mot à dire sur cela. La francophonie, cela a été dit, ce n'est pas seulement une langue donnée en partage, c'est aussi une vision commune.

Cette troisième voie, c'est celle, étroite, d'un développement de la société du numérique respectueuse du droit de personnes où chacun pourra profiter des bienfaits du numérique sans craindre ce que l'avenir ou la perversion du système pourrait entraîner. Comment alors pouvons-nous ouvrir cette troisième voie ?

### **La nécessité d'une régulation effective et transparente**

La première exigence que nous devons avoir vis-à-vis de nous même, mais aussi des autorités de nos pays respectifs, c'est la nécessité d'obtenir une reconnaissance légale de la protection des données et des autorités indépendantes.

Le développement des lois de protection des données et de des autorités est une des missions centrales de l'AFAPDP. Aujourd'hui, notre bilan sur ce point est encore insuffisant.

Peut-être par ce que nos autorités, nos lois ont souvent été vues comme des « gadgets », souvent mal comprises des citoyens et des gouvernements. Je crois qu'avec les développements de l'année 2013, nous pouvons aussi faire entendre que la protection des données personnelles n'est pas un accessoire des autres grandes libertés mais qu'elle en est au contraire le socle à l'heure du numérique.

Il ne s'agit plus seulement de vie privée mais désormais aussi de sécurité, de liberté d'expression, de liberté d'aller et de venir, de liberté d'entreprendre, d'autodétermination même de la personne.

Qui peut se dire tranquille quand toutes ses conversations peuvent être écoutées et qu'il peut être géolocalisé à quelques centimètres.

Qui peut se dire qu'il s'appartient pleinement quand nos données font l'objet de transactions inspirées de mécanismes boursiers pour savoir à quel moment et à quelles personnes délivrer la meilleure publicité en fonction de ses échanges de mails, de sa

navigation internet, de sa localisation spatiale et de données de santé collectées à la volée ?

Mais aussi, qui peut véritablement offrir un pacte de confiance à ses clients, à ses investisseurs, s'il ne s'appuie pas sur un cadre juridique clair qui garantit la sécurité des données et les conditions de leur utilisation.

Il ne s'agit pas d'être alarmiste mais au contraire, de faire valoir que, tant pour la défense des libertés que pour l'innovation et la croissance, nous devons donc continuer à développer, au sein du monde francophone, les lois de protection et les autorités indépendantes qui en assurent le respect ; à ce titre, la situation actuelle de l'AFAPDP n'est pas satisfaisante et nous devons maintenir nos efforts.

### **Des autorités au service de la transparence**

Le cas Snowden, après WikiLeaks et d'autres, conforte une dimension que nous apporte le numérique, celle de la transparence. Dans ce cas, il s'agit d'une transparence brutalement imposée mais le message est clair : « sans transparence, pas de confiance des citoyens ».

Je crois que, à ce titre, les autorités peuvent jouer un rôle majeur et aider à la mise en place de la transparence, dans un Etat de droit.

Une Résolution a été adoptée à Varsovie sur la transparence, elle invite les organisations et les gouvernements à plus de transparence sur l'usage des données personnelles.

Les entreprises elles-mêmes essaient de s'inscrire dans cette démarche de transparence comme par exemple Apple qui a publié son premier rapport de transparence en novembre 2013 et demande plus de transparence aux services de renseignement.

Sans naïveté ou angélisme nous devons constater que c'est bien la pression publique qui entraîne la réaction des opérateurs économiques qui craignent la perte de confiance et donc de profit...

Dans un tel environnement, nous avons donc une clef : refuser et exiger ... collectivement !

Une partie de cette clef c'est la proposition de Résolution francophone sur le thème de la transparence qui sera discutée pour adoption vendredi.

### **La voie de l'éducation au numérique**

Une autre partie tient dans le fait que seules autorités ne peuvent prendre en charge la régulation des données. C'est aussi aux individus de se responsabiliser dans leurs utilisations du numérique. Seule une société civile, des individus « éveillés » pourront maîtriser les usages et surtout, être capables de profiter de toutes les potentialités du numérique.

Ce doit être à l'occasion de cimenter les peuples autour d'une aspiration commune à la liberté de communiquer et au respect de valeurs fondamentales. C'est aussi répondre aux besoins des individus en les dotant de moyens de participer à la défense de leur propre vie privée et à tirer le meilleur des changements du monde.

Je ne crois pas qu'il revienne aux autorités d'éduquer au numérique, de dire ce qui est bon ou mauvais, ce qu'il convient de faire ou de ne pas faire. Notre rôle en matière d'éducation au numérique est malheureusement plus compliqué. Il nous incombe, parce que nous sommes indépendants, parce que nous disposons d'une certaine légitimité, d'impulser et d'accompagner le mouvement d'éducation au numérique.

C'est avec le tissu associatif mais aussi avec le soutien des entrepreneurs du numérique que nous devons construire des programmes, mutualiser des ressources, former des formateurs pour finalement donner à tous les publics la possibilité de trouver les outils de sa propre formation.

Pour l'impulser, la 35ème conférence des Commissaires à la vie privée et à la protection des données a adopté à Varsovie une Résolution sur l'éducation au numérique pour tous et a décidé du lancement d'un groupe de travail sur les bonnes pratiques.

Il faut se féliciter de cette résolution mais surtout de son contenu qui vise à faire de chaque utilisateur, un individu averti, doté des connaissances nécessaires pour exercer son esprit critique et ses choix éclairés

A Marrakech, nous pouvons nous aussi poursuivre dans cette voie et adopter une nouvelle résolution qui je le souhaite nous permettra de partager nos expériences en la matière et nos productions nationales.

### **La voie de la coopération**

Le temps où nous pensions que nos frontières étaient des frontières pour les données est révolu. Les données sont partout dans le monde et elles y circulent. Nous devons nous aussi nous montrer capables de prendre en compte ces évolutions.

La coopération est importante pour dresser des palissades, « faire bloc » et nous en avons besoin. Mais elle est également et principalement utile pour faire tomber des barrières.

Cette coopération est en marche et elle se concrétise par l'adoption de grands principes de protection des données notamment par les Standards de Madrid en 2009.

Désormais reconnus par tous au niveau international c'est principes constituent l'ébauche d'un socle commun de nature contraignante. Ces principes recoupent ceux de la Convention 108 du conseil de l'Europe.

Progressivement on dépasse l'affirmation du principe du respect de la vie privée (charte ONU) et les pétitions de principe sur la nécessité d'obtenir un instrument international (Jérusalem). Désormais nous avançons sur la voie d'un droit international de la protection des données. Il prendra du temps mais il est essentiel à notre 21<sup>ème</sup> siècle numérique.

La voie francophone est attendue au niveau de ces principes, notre participation s'est renforcée au sein de la conférence mondiale comme à Varsovie. Nous devons faire valoir que nous avons une identité spécifique qui concilie humanisme et logique économique.

Au-delà de l'affirmation et de la promotion de principes, notre coopération se développe sur un plan opérationnel. Qu'il s'agisse des groupes de travail de l'OCDE, du GPEN, de l'APEC, de la Conférence internationale, du G29, du réseau ibéro américain, du réseau francophone, tous les participants partagent le même constat de l'internationalisation et

de la nécessité d'apporter une réponse pratique qui puisse ne pas être et la même ambition.

Toutes ces initiatives visent à mieux appliquer concrètement les principes partagés dans un monde désormais mondialisé dans la circulation des données et à fournir des solutions globales aux acteurs.

Le monde francophone doit participer à ces échanges, sur les bonnes pratiques, sur les instruments juridiques internationaux, il doit être des actions concertées et concrètes.

A cet égard, ce que nous avons initié depuis plusieurs mois autour des BCR francophones va dans ce sens, dans le sens de l'interopérabilité. Il faut se féliciter de cela car dans le même sens des BCR ont été développés en Europe et nous travaillons avec l'APEC à rendre ces BCR compatibles avec les CBPR. Ce travail de rapprochement opéré avec la zone Asie pacifique est à notre portée ici Et demain nous pourrions envisager un espace de compatibilité plus vaste pour toutes ces BCR.

Le projet de résolution collectif sera soumis au vote des membres de l'AFAPDP vendredi

## **Conclusion**

Monsieur le ministre, Mesdames, Messieurs les présidents d'autorités, Madame, Monsieur, Chers participants, voilà les quelques réflexions que voulait partager avec vous le secrétaire général de l'AFAPDP

Nous avons tous au cours de l'année observés ces grands sujets internationaux, ils seront je pense utiles à nos débats et devons, aussi en raison des changements qui s'opèrent, nous guider pour réfléchir à la place et au rôle que nous voulons pour la Francophonie dans le monde de la protection des données.

Il nous reste à rejoindre nos conférences et ateliers pour engager les discussions et nous positionner collectivement dans le débat mondial avec notre sensibilité commune et nos identités propres.

Je vous remercie.