



**HAL**  
open science

# NOUVEAUX RISQUES DES NTIC : QUEL CADRE JURIDIQUE POUR LE BIG DATA AU MAROC ?

Mhammed Bouzit, Abdelkrim Ghali

► **To cite this version:**

Mhammed Bouzit, Abdelkrim Ghali. NOUVEAUX RISQUES DES NTIC : QUEL CADRE JURIDIQUE POUR LE BIG DATA AU MAROC ?. International journal of advanced research, 2018, 6 (4), pp.317 - 323. 10.21474/IJAR01/6860 . hal-01829704

**HAL Id: hal-01829704**

**<https://hal.science/hal-01829704>**

Submitted on 4 Jul 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Journal Homepage: -[www.journalijar.com](http://www.journalijar.com)  
**INTERNATIONAL JOURNAL OF  
 ADVANCED RESEARCH (IJAR)**

Article DOI:10.21474/IJAR01/6860  
 DOI URL: <http://dx.doi.org/10.21474/IJAR01/6860>



### RESEARCH ARTICLE

#### NOUVEAUX RISQUES DES NTIC : QUEL CADRE JURIDIQUE POUR LE BIG DATA AU MAROC ?

Bouzit Mhammed<sup>1</sup> and Ghali Abdelkrim<sup>2</sup>.

1. Doctorant en droit privé, Faculté des Sciences Juridiques, Economiques et Sociales Souissi. Université Mohammed V de Rabat. Maroc.
2. Professeur, Docteur en droit privé, Faculté des Sciences Juridiques, Economiques et Sociales Souissi. Université Mohammed v de Rabat. Maroc.

#### Manuscript Info

##### Manuscript History

Received: 06 February 2018  
 Final Accepted: 08 March 2018  
 Published: April 2018

#### Abstract

Les données personnelles ou données nominatives sont en principe protégées par la loi, cependant d'autres données qui peuvent le devenir, par leur recueil à travers divers sources, posent problème. Il s'agit du Big Data.

A la suite de la révolution numérique et le développement rapide de la technologique qui en résulte, il est apparu au cours des dernières années, le concept de Big Data qu'à met en cause les gouvernements, les institutions universitaires et commerciales, ce phénomène a contribué à la croissance du volume des données et de la diversité.

Au Maroc, la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel vise à protéger les citoyens contre l'utilisation excessive et irresponsable de leurs données par des organismes privés ou publics. Dans ce document on essaye de confronter le phénomène "Big Data" avec la législation relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, et soulever par la suite les enjeux juridiques qui en résultent.

*Copy Right, IJAR, 2018.. All rights reserved.*

#### Introduction:-

Les données personnelles ou données nominatives sont en principe protégées par la loi<sup>1</sup>, cependant d'autres données qui peuvent le devenir, par leur recueil à travers divers sources, posent problème. Il s'agit du Big Data<sup>2</sup>.

Au milieu des années 1990, une commission d'un groupe d'assurances américain décidait de publier les données médicales anonymisées d'employés de l'État du Massachusetts.

<sup>1</sup> En France : La loi de 1978 est encore modifiée par la loi du 6 août 2004 afin de transposer en droit français les dispositions de la directive 95/46/CE sur la protection des données personnelles. La loi de 1978 modifiée et complétée par son décret d'application n°2005-1309 en date du 20 octobre 2005. Cette transposition modifie de manière substantielle le texte de 1978, en élargissant le domaine des données qualifiées de personnelle.

Au Maroc : Le législateur marocain a dans ce contexte adopté la loi relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel : la loi 09-08.

<sup>2</sup> La protection juridique des données à caractère personnel au Maroc. Abdelkrim Ghali, REMALD N° 87-88. 2009.

**Corresponding Author:- Bouzit Mhammed.**

Address:- Doctorant en droit privé, faculté des sciences juridiques, économiques et sociales Souissi. Université Mohammed V de Rabat. Maroc.

Une étudiante en informatique, Latanya Sweeney, en demanda une copie et travailla à leur « réidentification ». Le gouverneur du Massachusetts assurant que l'organisme d'assurances avait protégé chaque patient en effaçant tous les identifiants nominatifs, Sweeney utilisa les listes des votants de la ville où le gouverneur habitait et commença à croiser les bases de données. Dans cette ville, six personnes seulement partageaient les mêmes dates de naissance, trois étaient des hommes et une seule avait le même code postal... L'informaticienne envoya au gouverneur tout son dossier médical. Quelques années plus tard, Latanya Sweeney démontrait que 87 % des Américains pouvaient être identifiés uniquement à partir de trois informations : le code postal, la date de naissance et le sexe. Ainsi des informations apparemment anonymes peuvent devenir personnelles quand elles se combinent avec suffisamment d'autres données<sup>3</sup>.

A la suite de la révolution numérique et le développement rapide de la technologique qui en résulte, il est apparu au cours des dernières années, le concept de Big Data qu'à met en cause les gouvernements, les institutions universitaires et commerciales, ce phénomène a contribué à la croissance du volume des données et de la diversité, comme l'émergence des téléphones intelligents et des technologies de réseautage social qui produisent et envoient une quantité énorme de données de façon continue, ce qui permet à tous les appareils d'entrer en communication entre eux. La production de nouvelles données, en plus de la puissance du cloud computing et la réduction des coûts de stockage ont permis l'exploitation dans plusieurs domaines telles que la génétique, la recherche biologique et environnementale, la météorologie.

Du point de vue législatif, le traitement des données personnelles a pris une importance primordiale au niveau international, et c'est ce que présente l'article 12 de la déclaration universelle des droits de l'homme, qui stipule que "Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.". L'ONU a adopté en 1989 un guide d'informatisation et de traitement des données personnelles. L'UE a produit aussi un guide général depuis 1995<sup>4</sup>.

En 1989, l'Assemblée générale des Nations Unies (ONU) a adopté des "Directives sur l'utilisation des données personnelles informatisées"<sup>5</sup>.

Le 14 décembre 1990, l'Assemblée générale a adopté les «Lignes directrices pour la réglementation des données à caractère personnel informatisées» dans leur version révisée<sup>6</sup>. «Les principes contiennent des principes similaires aux principes directeurs de l'OCDE et à la Convention du Conseil de l'Europe. Elles constituent des recommandations non contraignantes aux États membres et contiennent des principes concernant l'exactitude, la spécification des objectifs, les droits d'accès, la non-discrimination et la sécurité<sup>7</sup>.

Au Maroc, la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel vise à protéger les citoyens contre l'utilisation excessive et irresponsable de leurs données par des organismes privés ou publics<sup>8</sup>.

Une commission nationale du contrôle et de la protection des données personnels a été créée afin d'œuvrer au respect de la loi précitée.

La question qui se pose est de savoir dans quelle mesure le législateur marocain par la législation relative à la protection des données à caractère personnel pourrait il garantir réellement la protection des données personnelles à l'ère des Big Data?

---

<sup>3</sup> Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12.

<sup>4</sup> UN General Assembly Official Records 45th Session 1990, Supplement No. 49 (A/45/95).

<sup>5</sup> UN, Guidelines on the Use of Computerised Personal Data Flow, Resolution 44/132, adopted in December 1989, approved on 4 December 1990, UN Doc. E/CN.4/Sub.2/1988/22.

<sup>6</sup> UN General Assembly Official Records 45th Session 1990, Supplement No. 49 (A/45/95).

<sup>7</sup> UN Doc. E/CN.4/Sub.2/1988/22, p. 10 Annex I; UN Doc. E/CN.4/1990/72 of 20 February 1990.

<sup>8</sup> Un décret d'application de cette loi a été publié au Bulletin Officiel du 18 juin 2009.

En d'autre terme, y-a-il des limites à cette loi ? (I) ou y-a-il une alternative en l'occurrence l'instauration d'une législation spécifique ? (II)

### **Limites à l'égard de la protection de la vie privée:-**

Il y a lieu de confronter les deux phénomènes traités, et, soulever par la suite les enjeux juridiques qui en résultent.

#### **1) Confrontation entre Big Data et données personnelles:-**

Etre responsable du traitement des Big Data est plus large que la résolution des problèmes de confidentialité. Dans un domaine émergent avec autant de possibilités et où les limites technologiques ont évolué d'une façon spectaculaire, et les conséquences de l'utilisation ne sont pas toujours prévisibles. Un débat sur ce qui est principalement juste et faux est nécessaire.

Les risques majeurs qui en résultent mettent en évidence ce que les organisations doivent prendre en considération pour protéger leurs affiliés et eux-mêmes contre l'impact des Big Data. Il s'agit notamment de :

#### **a) L'anonymisation des données pourraient être impossibles:-**

Les grands ensembles de données sont souvent soumis à un processus d'anonymisation pour permettre l'utilisation des données à des fins de marketing ou de recherche scientifique sans risque de fuite d'informations sur les individus et sans être en contradiction avec l'article premier de la loi n° 09-08<sup>9</sup>. Cependant, aucune base de données utile ne peut jamais être parfaitement anonyme.

En outre, depuis plusieurs décennies, la communauté de la recherche en sécurité de l'information a reconnu que les corps de données de faible sensibilité, lorsqu'ils peuvent être corrélés, peuvent souvent donner lieu à un ensemble de données beaucoup plus significatives que les ensembles de données originaux. Lorsqu'il est fait avec une intention malveillante, cela est appelé une attaque d'inférence, ou légèrement le terme plus neutre «réidentification»<sup>10</sup>.

Le «triple identificateur» de l'anniversaire, du sexe et du code postal est tout ce dont une personne a besoin pour identifier de manière unique au moins 87% des citoyens américains dans des bases de données accessibles au public<sup>11</sup>.

#### **b) La négligence et l'inconscience des consommateurs:-**

Tout le monde ne se soucie assez de leur propre vie privée. De nombreux consommateurs utilisent négligemment les médias sociaux ou les services Internet, ce qui permet à d'autres d'utiliser l'information de manière inattendue. Considérez les exemples suivants :

1. La publicité sur Twitter que vous êtes en vacances ou "vérifié" quelque part avec toute la famille montre que vous n'êtes pas à la maison.
2. Les consommateurs ne lisent presque jamais les termes et conditions.
3. Pour recevoir une promotion, les consommateurs doivent souvent fournir des informations personnelles.

<sup>9</sup> Article 1er de la loi n° 09-08 : L'informatique est au service du citoyen et évolue dans le cadre de la coopération internationale. Elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme. Elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens.

Pour l'application de la présente loi, on entend par :

9- « consentement de la personne concernée » : toute manifestation de volonté, libre, spécifique et informée, par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement ;

10- « cession ou communication » : toute divulgation ou information d'une donnée portée à la connaissance d'une personne autre que la personne concernée ;

11- « interconnexion de données » : forme de traitement qui consiste à établir un rapport entre les données d'un fichier et les données d'un fichier ou plusieurs fichiers tenus par un autre ou par d'autres responsables, ou tenus par le même responsable mais dans un autre but.

<sup>10</sup> Coulibaly Ibrahim, La protection des données à caractère personnel dans le domaine de la recherche scientifique, Thèse de doctorat en droit privé, Université de Grenoble, 25 novembre 2011. Accessible à l'adresse : <http://tel.archives-ouvertes.fr/tel-00798112>.

<sup>11</sup> Voir le cas de l'étudiante en informatique, Latanya Sweeney, dans l'introduction.

Même si on s'attend à ce que les gens sachent ce qu'ils font et qu'il n'y ait pas de problèmes juridiques après que les consommateurs ont consenti à fournir de l'information, les entreprises ont un risque de réputation si les consommateurs croient que leur confiance a été rompue. Ce que les consommateurs vous font confiance (ou ne le font pas) ne correspond pas nécessairement à ce qui est légalement autorisé à faire.

**c) L'étendu de la vidéosurveillance:-**

Les caméras de vidéosurveillance sont installées partout sur le domaine public et privé. Avec l'avènement de nouveaux phénomènes tel le terrorisme et le sentiment d'insécurité qu'il engendre, ces caméras contribuent au rassurement d'une population qui, dans l'ensemble les aperçoit avec toute bienveillance. Cependant ce système de surveillance est controversé et va à l'encontre de la loi.

On craint toujours des atteintes à la protection de la personne qui feraient que chacun de nos actes et gestes serait espionné

La loi est claire, "Toute personne sollicitée directement, en vue d'une collecte de ses données personnelles, doit être préalablement informée de manière expresse, précise et non équivoque, elle a aussi le droit d'accès à ses propres images<sup>12</sup>. Cependant, ce droit reste théorique. Qu'en est-il dans l'espace public et privé? La loi sur la protection des données personnelles reste silencieuse vis à vis cette question. Somme-nous passés de l'état de droit à l'état de surveillance ?<sup>13</sup>

**d) La révélation des paiements:-**

Les transactions financières, sont des données que détiennent les établissements financiers qui nous connaissent mieux que nous-mêmes. Mais que font-ils de ce flux important de données et qu'a une grande valeur ajoutée? De toute façon pas de choses importantes en dehors de leurs bureaux, mais à l'intérieur, certaines s'en servent pour nous envoyer des offres, des annonces publicitaires, d'autres pour développer des produits adaptées à vos avoirs.

**e) Les données de localisation détenues par les opérateurs:-**

Les Smartphones sont connectés de façon continue aux antennes relais de téléphonie mobile. Les données concernant nos déplacements peuvent être collectées pour servir à résoudre des problèmes d'urbanisation et des flux dans les routes. Swisscom propose un projet de ville intelligente "Smart City" qui illustre la rentabilité du traitement massif de donnée (big data).

Ainsi se posent des questions d'ordre juridique. Ces big data sont-elles anonymes? Est ce qu'on a en tant que propriétaire de ces données le droit d'accès ? S'agit-il vraiment des données personnelles ?

La loi sur les télécommunications invoque des dispositions telles que le secret des télécommunications<sup>14</sup>, or ce dernier ne peut pas être opposé à la personne concernée.

**2) Nouveaux enjeux socio-juridiques:-**

En effet le Big Data se trouve au croisement de trois volontés opposées :

- L'entreprise qui veut accéder au maximum de données personnelles pour les valoriser en améliorant son offre de produits et services.
- L'État, ou le régulateur, qui entend conserver ses prérogatives en matière de libertés publiques et de sûreté publique en encadrant l'utilisation de ces données.
- L'utilisateur final/consommateur qui veut bénéficier de services plus pertinents tout en gardant le contrôle de ses «données à caractère personnel<sup>15</sup> ».

<sup>12</sup> Article 5 de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

<sup>13</sup> Loi antiterroriste : « Nous sommes passés de l'Etat de droit à l'Etat de surveillance ». LE MONDE IDEES | 11.10.2017. Propos recueillis par Anne Chemin et Jean-Baptiste Jacquin.

En savoir plus sur : [http://www.lemonde.fr/idees/article/2017/10/11/mireille-delmas-marty-nous-sommes-passees-de-l-etat-de-droit-a-l-etat-de-surveillance\\_5199594\\_3232.html#qWfWiHW8fMUo7kp9.99](http://www.lemonde.fr/idees/article/2017/10/11/mireille-delmas-marty-nous-sommes-passees-de-l-etat-de-droit-a-l-etat-de-surveillance_5199594_3232.html#qWfWiHW8fMUo7kp9.99)

<sup>14</sup> Article 26 de la loi n°24-96 consolidée relative à la poste et aux télécommunications, telle qu'elle a été modifiée et complétée.

L'usage du Big Data paraît strictement encadré juridiquement. Au Maroc, les opérateurs intervenant dans la collecte et l'analyse des données sont soumis à la surveillance de la Commission Nationale de Contrôle de Protection des Données à Caractère Personnel (CNDP). L'usage de ces données nominatives est réglementé par la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Le législateur marocain précise que les données personnelles doivent être collectées et traitées avec un objectif précis : seules les données pertinentes pour un usage défini peuvent être collectées. D'autant plus que la loi reconnaît le droit à toute personne d'être informée de la collecte et de l'utilisation de ses données personnelles. En effet, chaque personne peut décider elle-même de l'utilisation des données la concernant.

Le Big Data obéit en principe aux exigences de la Commission Nationale de Contrôle de Protection des Données à Caractère Personnel et ses usages directement concernés par le cadre législatif en vigueur.

Cependant, si on résume les enjeux juridiques possibles du Big Data on trouve la corrélation des informations que l'on ne cherchait pas a priori, la possibilité d'identifier des personnes à partir de données que l'on avait pourtant fait exprès de les rendre non identifiantes, la possibilité que ces données traitées soient erronées, ces manœuvres ne touchent pas forcément la qualité générale du traitement (voire cela peut les rendre plus riches dans certains cas) et finalement la possibilité d'entrevoir le futur.

Ainsi, les principes qui fondent notre système légal et de prévoir la protection des informations nominatives rentrent en opposition frontale avec ces composants, comme on le démontre à travers ces remarques :

D'après l'article 3<sup>16</sup>, les données à caractère personnel doivent être :

- traitées loyalement et licitement ;
- collectées pour des finalités déterminées explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec finalités ;
- les données doivent être « exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées » ;
- un traitement permettant de prendre des décisions sur un éventuel comportement futur pourrait rentrer en contradiction avec l'article 11.<sup>17</sup>

Cependant, la réglementation en question ne s'applique pas à des données nominatives qui ont été anonymisées telles que les données statistiques. Mais si ces dernières redeviennent tout de même identifiantes, la réglementation s'impose, et doit s'appliquer et notamment l'information préalable des individus dont les informations sont recueillies, voire leur consonance dans certains cas, en l'occurrence ;

### **Tendance vers un droit adéquat au Big Data**

Le système juridique du traitement des données personnelles actuel est amplement fondé sur le principe de formalités préalables à réaliser guidant le cadre exact du traitement effectué. Cette orientation est-elle en harmonie avec l'évolution du phénomène du Big Data ?

Tout est dit pour le Big Data ? Le croire serait négliger un apport important du règlement européen sur la protection des données personnelles actuellement en discussion au niveau européen destiné à remplacer les lois locales

<sup>15</sup> BIG DATA – ENTRE RISQUE ET OPPORTUNITÉ ? Groupe de veille et d'analyse – 19e Session nationale spécialisée 2015-2016 « Protection des entreprises et intelligence économique ».

<sup>16</sup> Article 3 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

<sup>17</sup> Article 11 de la loi 09-08 «Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

existantes : celui-ci opère une révolution copernicienne en remplaçant le principe de formalités préalables par l'exigence de conformité du traitement aux règles posées<sup>18</sup>.

Devant cette réalité on ne peut rester dans l'insouciance vis à vis de cette innovation juridique européenne. Surtout que la réglementation de la protection des données personnelles ne pourrait parvenir à couvrir ces nouveaux enjeux.

### 1) **Appréciation de la réglementation de la protection des données:-**

Après près de cinq ans de travail intensif, accompagné de discussions politiques et un large écho sociétal sur les données de l'Union européenne (UE), la réforme de la protection est enfin devenue une réalité. Le nouveau cadre consiste d'un règlement général sur la protection des données (GDPR)<sup>19</sup>, qui remplacera la directive actuelle sur la protection des données<sup>20</sup>.

Il est important de souligner que le droit à la vie privée est un concept important dans le droit de l'UE et a reçu une place significative qui reflète ses valeurs. S'appuyant sur les recommandations du Conseil de l'Europe et la convention européenne des droits de l'homme, qui protège le droit au respect de la vie privée et familiale dans son article 8. La charte des droits fondamentaux de l'Union européenne distingue entre le droit au respect pour la vie privée et familiale à l'article 7<sup>21</sup> et le droit à la protection des données, qui sont explicitement consacrées à l'article 8<sup>22</sup>.

### 2) **Nécessité d'une nouvelle législation pour les Big Data?:-**

Dans la plupart des pays, les initiatives Big Data sont traitées dans le cadre de la législation existante sur des questions telles que la protection de la vie privée et des données personnelles. De plus, les lois de protection des données sont convenues que les principes actuels de protection des données doivent être maintenus.

À notre avis, de nouveaux concepts et paradigmes, tels que le cloud-computing ou le Big Data, ne devraient pas abaisser ni saper les niveaux actuels de protection des données en tant que droit humain fondamental. Les principes centraux existants en matière de protection des données, tels que la légalité, l'équité, la proportionnalité, les droits des personnes concernées et la finalité ne devraient pas être remis en cause par l'avènement du Big Data.

Les droits des individus à l'autodétermination informationnelle devraient être la pierre angulaire de la société de l'information moderne, protégée par un cadre moderne de protection des données, offrant une protection efficace des données à l'individu tout en permettant à des intérêts légitimes. D'autant plus que la plupart des législateurs en la matière sont conscients de l'affrontement fondamental entre les Big Data et les principes de protection des données, comme discuté précédemment.

Il est remarquable d'après un sondage<sup>23</sup> que seulement certaines nouvelles mesures législatives qui sont en cours d'élaboration pourraient répondre spécifiquement aux nouveaux dangers posés par les mégadonnées. Certaines lois

<sup>18</sup> Protection des données personnelles et Big Data : inconciliables, vraiment ?

Par François Coupez, Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies. Disponible sur :

<https://www.silicon.fr/protection-donnees-personnelles-big-data-inconciliables-114312.html>

<sup>19</sup> Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

<sup>20</sup> Directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

<sup>21</sup> "Respect de la vie privée et familiale : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications."

<sup>22</sup> Article 8 de la loi 09-08 : Protection des données à caractère personnel.

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

<sup>23</sup> Working Paper no. 20: International and comparative legal study on Big Data, 2016.

se réfèrent à la réglementation générale sur la protection des données à venir et indiquent qu'elles espèrent que ces règles les aideront à maîtriser adéquatement les dangers du Big Data.

Par exemple, la loi de protection des données britannique suggère «que les propositions pour le nouveau règlement général sur la protection des données de l'UE intègrent certaines mesures que nous avons identifiées comme étant importantes pour assurer la conformité dans le Big Data, par ex. des avis de confidentialité plus clairs, des évaluations de l'impact sur la vie privée et la confidentialité dès la conception<sup>24</sup>.

On se réjouit du fait que ces mesures soient mises en avant, bien que l'on craint qu'elles ne soient considérées comme un simple exercice bureaucratique. De plus, le parlement estonien discute d'une nouvelle législation sur les Open-Data (y compris les Big Data). En outre, d'autres pays font référence à la corégulation et à l'autorégulation comme solution possible.

En effet, la réglementation actuelle est principalement fondée sur l'individu et ses intérêts - cela vaut pour les droits de l'homme tels que la vie privée et la protection des données, qui repose sur le concept de «données personnelles» qui permet d'identifier ou d'individualiser une personne physique. Cependant, les processus Big Data ne concernent pas uniquement le stockage et le traitement des données à un niveau individuel, mais plutôt la tendance à travailler de plus en plus avec des données agrégées, des profils généraux et des profils de groupe. Par conséquent, on peut se demander si l'accent mis sur l'individu, sur les données personnelles, peut encore être maintenu à l'ère du Big Data. Les corrélations statistiques et les profils de groupe ne qualifient pas les données personnelles, mais peuvent être utilisés, entre autres, pour altérer, façonner ou influencer dans une large mesure le milieu de vie des personnes. De plus, la tendance à l'utilisation des Big Data est également liée à ce problème, car on ne sait pas dans quelle mesure les Big Data seront toujours qualifiées de données personnelles.

### **Conclusion:-**

Par conséquent, pour répondre à la question de savoir s'il est souhaitable de formuler de nouvelles règles pour les processus de Big Data, trois facteurs déterminants en la matière :

1. Tout d'abord, la quasi-totalité des pays et des APD reconnaissent que les mégadonnées posent de nouveaux risques relativement fondamentaux au cadre réglementaire actuel, et en particulier aux principes sous-jacents.
2. Deuxièmement, le cadre réglementaire actuel est perçu comme (trop) restrictif par rapport au déploiement des nouvelles technologies et de l'innovation technologique, en particulier dans le secteur privé.
3. Troisièmement, de nombreuses parties prenantes ne sont pas certaines de la manière dont le cadre réglementaire actuel devrait être appliqué et interprété en ce qui concerne les mégadonnées.

Cependant, deux dangers pourraient en découler: d'une part, les parties prenantes, de peur d'enfreindre la loi, pourraient renoncer à de nombreuses innovations technologiques et à des utilisations de données qui seraient en fait légitimes. D'autre part, les parties pourraient utiliser -ou plutôt abuser- la zone grise existante pour déployer certaines technologies qui ne seraient pas conformes au cadre réglementaire actuel. La question de savoir si et comment un nouveau cadre réglementaire peut apporter une solution à ces problèmes doit être soigneusement évaluée par les régulateurs.

En définitive, quelques soient les contraintes et les visions, on assistera tôt ou tard à l'émergence d'une législation spécifique, ou au moins à des dispositions propres en la matière. Il ne s'agit pas seulement d'une idée, qualifiée bonne ou mauvaise que l'on propose<sup>25</sup>

---

<sup>24</sup> Ceci avant de prendre en considération les conséquences du Brexit en terme de protection des données personnelles.

<sup>25</sup> LE MONDE 05.02.2018, par Serge Abiteboul et Gilles Dowek (Chercheurs à l'Inria (Institut National de Recherche en Informatique)). Disponible sur : [http://www.lemonde.fr/idees/article/2018/02/05/la-propriete-des-donnees-personnelles-est-une-fausse-bonne-idee\\_5252158\\_3232.html#p0fxM6J3Jbdh4E6x.99](http://www.lemonde.fr/idees/article/2018/02/05/la-propriete-des-donnees-personnelles-est-une-fausse-bonne-idee_5252158_3232.html#p0fxM6J3Jbdh4E6x.99)