Excellence, M. le Président de la République,

Honorables invités,

Chers collègues,

LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'identification de l'individu a toujours constitué une préoccupation essentielle des sociétés humaines. Ainsi, en Afrique, certaines ethnies comme les yombes du Congo, les mursis d'Ethiopie et les haalpulaars du Sénégal, portaient des scarifications sur leurs membres comme signe distinctif de l'appartenance ethnique.

L'organisation sociétale et les besoins de singularisation, de différenciation et d'identification de la personne commandent, désormais, de collecter ses nom et prénom (s), sa date de naissance, sa filiation, …

Cette collecte des données élémentaires, liées à l'état civil de la personne, connaît une véritable mutation avec le développement des technologies de l'information et de la communication, tant sur les moyens, les finalités que sur la quantité prodigieuse des données collectées.

Titre d'exemple, Google traite, tous les jours, pas moins de 24 millions de milliards d'octets de données et on estime à près de 100 milliards le nombre d'objets connectés d'ici 2020.

Ces technologies, basées sur l'utilisation massive des données, configurent une nouvelle ère de « l'économie guidée par les données ». Aussi, apparaissent de nouvelles activités au modèle économique axé sur l'exploitation des données personnelles, notamment à des fins publicitaires, économiques et politiques.

D'après une étude du CIGREF, Réseau de grandes entreprises en France, le marché européen des données représentera, d'ici 2020, une valeur économique de 1000 milliards d'euro.

Pour optimiser la récolte des données personnelles, dénommées or noir du numérique, il n'y a pas un instant de nos journées ou de nos nuits qui ne soit

scruté, traqué et repéré par les algorithmes d'intelligence artificielle des Gafam (Google, Apple, Facebook, Amazon et Microsoft).

En outre, les pouvoirs publics ne sont pas en reste puisque l'efficience de leurs politiques commande la dématérialisation de plus en plus de l'administration avec corollaire la mise en œuvre de techniques de collecte et de traitement des données des usagers.

Pour exemple, le système du parrainage intégral, instauré par la loi du 11 mai 2018 dans l'architecture constitutionnelle sénégalaise, entraîne une abondante collecte des données des citoyens de la part des candidats aux élections.

De même, la mise en ligne du fichier électoral, par souci d'efficacité et surtout de transparence, implique une utilisation à profusion des données personnelles des citoyens.

Ce phénomène de collecte exponentielle et de valorisation des données personnelles s'accentue avec l'émergence de techniques inédites (logiciels mouchards, métadonnées, intelligence artificielle, etc) de profilage, de prédiction et de manipulation de l'internaute rendu pratiquement transparent notamment dans son identité physique, physiologique, psychique, génétique, économique, sociale et culturelle.

Ces technologies sont, certes, sources de progrès. Toutefois, elles charrient des risques majeurs d'atteinte à la vie privée et aux libertés individuelles compte tenu de leur caractère intrusif et invasif.

L'actualité récente, dans le domaine des réseaux sociaux, met en exergue ces atteintes contre la vie privée d'hommes et de femmes voués aux gémonies suite à la diffusion de leurs images intimes.

Ces atteintes peuvent être aussi le fait de structures organisées, qu'elles soient étatiques ou privées.

En témoignent les révélations d'Edouard Snowden sur l'existence de plusieurs programmes de surveillance de masse américains et britanniques et le scandale

des données personnelles de près de 88 millions d'utilisateurs de Facebook collectées et analysées à leur insu par la société Cambridge Analytica.

Ces intrusions, outre qu'elles portent atteinte à la sphère privée, tendent à nier les valeurs de démocratie et de liberté des sociétés modernes par la manipulation de données des citoyens.

Notre analyse se propose d'aborder la problématique des données à caractère personnel sous l'angle de la protection de la vie privée et des libertés individuelles, excluant de son champ les atteintes à la souveraineté de l'Etat commises par le biais des TIC.

Face à la récurrence des atteintes à l'intimité de la vie privée, le droit intervient pour redonner à l'homme son pouvoir d'autodétermination informationnelle, c'est-à-dire le droit de chacun de décider des conditions d'utilisation de ses données ou du moins d'avoir connaissance de l'usage qui en est fait.

C'est tout le sens du droit à la protection des données personnelles.

Seulement, l'œuvre de protection doit réaliser un équilibre kafkaïen entre d'une part, le besoin d'assurer le développement de l'économie numérique, vecteur de progrès, et d'autre part, l'impératif de préserver les données à caractère personnel contre les atteintes préjudiciables à la vie privée et aux libertés liées à l'utilisation des TIC.

Les anglophones parlent de privacy paradox.

C'est là toute la problématique de la protection des données à caractère personnel. Avant d'en envisager l'étude, il importe d'éclairer quelques concepts fondamentaux.

Par opposition aux informations à caractère économique ou industriel, les données personnelles renvoient à une information ou un ensemble d'informations

concernant une personne physique identifiée ou identifiable par le croisement d'éléments intrinsèquement liés à sa personnalité.

Ainsi, les données peuvent être sériées en deux catégories:

La première catégorie regroupe les données personnelles identifiantes, rattachées directement soit à l'identité d'une personne (nom, prénom, adresse, filiation, situation familiale,…) soit à un numéro d'identification ou à une adresse (n° de pièce d'identité, n° téléphone, n° d'immatriculation véhicule, n° compte bancaire ou de permis de conduire), soit à des éléments propres à chaque être humain (voix, image, photo, ADN, empreintes digitales).

La seconde catégorie, toute nouvelle, vise les données dites comportementales, désignant l'ensemble des comportements d'un individu collectés grâce notamment au suivi de ses navigations (utiliser un site d'achat, mots clés saisis sur un moteur de recherche).

Pour être protégées, ces données doivent faire l'objet d'un traitement défini comme un ensemble d'opérations tels que la collecte, l'enregistrement, la diffusion, l'interconnexion effectuée en totalité ou en partie à l'aide de procédés automatisés ou non automatisés.

Ainsi, le traitement des données personnelles est une notion transversale qui innerve presque toutes les activités humaines.

Ce statut particulier des données à caractère personnel explique qu'elles soient l'objet d'une protection à trois niveaux.

Au niveau international, les prémisses d'un droit à la protection des données personnelles revêtent les parures d'un principe universel inscrit dans la Déclaration universelle des droits de l'homme de 1948 (article 12), les Principes directeurs pour la règlementation des fichiers informatisés contenant des données personnelles (ONU-Résolution 49/45 du 14 décembre 1994), la Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Au niveau régional et sous-régional, la protection des données à caractère personnel est prise en charge par la Convention de Malabo du 27 juin 2014 et l'Acte additionnel de la CEDEAO du 16 février 2010.

S'inspirant de ce bouclier protecteur, le Sénégal a aménagé un cadre juridique et institutionnel applicable au traitement des données personnelles.

A ce titre, la loi 2008-12 du 25 janvier 2008 constitue le texte de référence. Cette loi soumet au respect de ces dispositions tous les traitements automatisés ou non automatisés, de données à caractère personnel à l'exception de ceux mis en œuvre à des fins exclusivement personnelles ou familiales, sans aucune communication à des tiers ou diffusion des données.

Elle régit tout traitement de données personnelles dont le responsable dispose d'un établissement sur le territoire sénégalais ou fait recours à des moyens de traitement situés sur ledit territoire.

La glose de ces dispositions révèle que la préservation des données personnelles demeure une option cardinale réalisée par l'alliage d'un dispositif légal et institutionnel protecteur **(I)** avec une architecture de sanctions judiciaires appropriées, garante de l'effectivité de la protection **(II)**.

Cependant, au regard de l'universalité, de la technicité et et l'accélération constante des technologies de l'information et de la communication génératrices de nouvelles formes d'atteintes plus insidieuses et plus pernicieuses, la réadaptation de notre arsenal législatif est souhaitable par la mise à jour du dispositif de protection. Ce qui fera l'objet de quelques recommandations phares à titre conclusif.

I- LA MISE EN PLACE D'UN DISPOSITIF LEGAL ET INSTITUTIONNEL PROTECTEUR DES DONNEES PERSONNELLES

Pour préserver les données à caractère personnel, la loi du 25 janvier 2008 a posé des principes essentiels applicables à tout traitement (A) et a institué une autorité administrative indépendante, chargée d'en assurer le contrôle (B).

A – La détermination des principes de base de la protection des données personnelles

La mise en œuvre d'un traitement de données personnelles est une étape, à la fois pratique et juridique qui impose un ensemble de principes de base, stricts et cumulatifs, applicables aux opérations de traitement et aux acteurs.

Ces principes irriguent tout le processus de collecte des données et fixent les conditions de licéité des traitements (article 34 de la loi).

1-Les principes applicables au traitement

Le responsable de traitement est assujetti à deux obligations essentielles : une obligation de transparence et une obligation de sécurité.

a -L'obligation de transparence

L'exigence de transparence (art 37 loi 25 janvier 2008) implique, pour le responsable de traitement, avant toute collecte des données, de préciser la finalité de traitement, de fournir des informations précises et détaillées sur ledit traitement et enfin de recueillir le consentement préalable de la personne concernée.

- La finalité

Préciser la finalité, c'est indiquer la raison pour laquelle le traitement est créé. La protection des données repose essentiellement sur le respect de la finalité du traitement déclarée auprès de l'autorité de protection des données à caractère personnel.

Pour être licites, le traitement de données doit obéir à **des finalités déterminées, explicites et légitimes** correspondant aux missions du responsable de traitement (art 34 loi 25 janvier 2008).

Aussi, les données traitées doivent être **adéquates**, **pertinentes** et **non excessives** au regard de la finalité poursuivie.

Cette prescription traduit le principe de proportionnalité qui limite la collecte de données à celles nécessaires pour réaliser l'objectif poursuivi.

Pour exemple, lorsqu'une personne souhaite souscrire un abonnement téléphonique auprès d'un opérateur, il n'est pas nécessaire que celui-ci demande au futur client sa situation matrimoniale. Une telle demande serait, évidemment, excessive.

C'est en application de ce principe que la Commission Nationale de l'Informatique et des Libertés a instauré une règle de sectorisation qui limite l'accès des données aux secteurs concernés. Ainsi, pour la CNIL, l'accès d'un fichier recensant les locataires mauvais payeurs doit être limité aux professionnels du secteur de l'immobilier. La mise à disposition des informations collectées à tous secteurs confondus constituerait une atteinte disproportionnée à la vie privée.

Cette règle de sectorisation n'a pas été respectée lors de l'élaboration de la loi sur les Bureaux d'information sur le crédit, lesquels collectent les données de tous les facturiers publics et privés du pays.

Le principe de finalité est utilement complété par l'obligation d'information mise à la charge du responsable du traitement.

- L'information

Le responsable de traitement doit, avant toute collecte, fournir à la personne concernée des informations détaillées portant notamment sur son identité, sur la nature des données collectées, sur leur finalité et sur le transfert des données à destination de l'étranger.

La violation de l'obligation d'information rend illicite et déloyale le traitement mis en œuvre. La mise à disposition d'une information complète sur le traitement devrait permettre à la personne concernée de donner un consentement éclairé.

- Le consentement

Le consentement préalable de la personne concernée est une condition de licéité de tout traitement de données personnelles. Il s'analyse en une manifestation de **volonté libre**, **spécifique** et **informée**, par laquelle la personne concernée accepte le traitement envisagé.

Le consentement écrit de la personne concernée est obligatoire s'agissant de traitement de données sensibles portant notamment sur l'origine raciale, les convictions religieuses, les données de santé.

L'obligation de consentement pose avec acuité la problématique des contrats d'adhésion des GAFAM. L'internaute qui veut bénéficier des services proposés est obligé d'accepter leurs conditions générales d'utilisation qui intègrent la collecte et le traitement des données personnelles, généralement à des fins publicitaires.

Seulement, il demeure obligatoire pour ces entreprises de décliner de manière complète et compréhensible leurs conditions d'utilisation et de fournir, à leurs clients, des informations détaillées sur le traitement des données personnelles.

Il importe, évidemment, de prendre le temps de bien lire et comprendre les contrats d'adhésion des applications comme Facebook ou Tweeter et ne pas valider « tête baissée » l'option « j'accepte », enjôlé par les services supposés gratuits. Car comme le dit l'adage « sur la toile, quand c'est gratuit, et même parfois quand c'est payant, c'est vous le produit !».

Une autre problématique tient au fait que ces CGU prévoient presque toujours une clause attributive de juridiction qui donne compétence aux tribunaux américains pour connaître de tout litige résultant de leur exécution.

Pour la Cour d'appel de Paris (arrêt du 12 février 2016, Pôle 2 Chambre 2), une telle clause est inopposable aux utilisateurs de Facebook en France. Pour un

contrat de consommation, l'utilisateur doit avoir le choix de saisir le tribunal de son domicile situé à Paris.

Les juridictions sénégalaises n'ont pas encore eu l'occasion de se prononcer sur une telle question.

Seulement, nous pouvons avancer que certes notre droit positif permet de déroger aux règles de compétence territoriale (art 114-2 CPC), exception faite pour les règles d'ordre public organisant notamment les voies de recours. Il reste que le déséquilibre contractuel amène le consommateur sénégalais à adhérer aux conditions générales d'utilisation des géants du numérique, sans aucune possibilité d'en discuter les termes.

La faiblesse du consommateur face à ces professionnels ne devrait pas être accentuée par l'admission d'une clause attributive de juridiction dont le caractère abusif est manifeste puisqu'ayant pour effet de priver le consommateur de son droit à un procès. Dès lors, une telle clause devrait être déclarée inopposable au consommateur. Ne dit-on pas qu'entre « le fort et le faible, c'est la liberté qui opprime mais c'est la loi qui libère » ?

Par ailleurs, le consentement préalable n'est pas requis lorsque notamment le traitement est nécessaire au respect d'une obligation légale, pour la sauvegarde de la vie de la personne concernée ou dans le cadre d'une mission de service public

Ces dérogations, formulées en des termes généraux, devraient être interprétées de façon stricte, dans la mesure où elles sont susceptibles de réduire de façon significative le régime de protection applicable aux données personnelles.

b- <u>L'obligation de sécurité</u>

Le responsable de traitement doit prendre toutes mesures utiles pour assurer la qualité et la conservation des données.

- La qualité des données

Garantir la qualité des données, c'est prendre toutes les mesures de sécurité physique et technique pour empêcher que les données soient déformées ou endommagées.

Le sous-traitant est aussi assujetti à cette exigence de sécurité et agit sous la responsabilité du maître de traitement.

- La conservation des données

Le responsable de traitement précise la durée de conservation des données compte tenu de la finalité poursuivie. A défaut, l'autorité de régulation doit indiquer la durée.
Au-delà, les données ne peuvent être conservées que pour une utilisation à des fins historiques, statistiques ou scientifiques.
Toujours dans un souci de protection des données, la loi a prévu un catalogue de principes applicable aux sujets du traitement.

2-Les principes applicables aux sujets

Les personnes dont les données font l'objet de traitement jouissent d'un ensemble de droits qui constituent autant d'obligations à la charge du responsable de traitement.

a-Les droits des personnes concernées

Il s'agit du droit d'accès et du droit d'opposition qui confèrent un véritable pouvoir de contrôle à postériori à la personne concernée qui conserve un droit de regard sur l'utilisation de ses données. Ces droits constituent, ainsi, une muraille de protection au profit des personnes dont les données sont collectées.

• L'accès (rectification, suppression)

En vertu du droit d'accès, toute personne (héritier, tuteur justifiant de son identité) peut s'adresser au responsable de traitement pour savoir si ses données font l'objet de traitement et recevoir le cas échéant des informations sur ledit traitement et communication de ses données sous une forme intelligible.

Munie de ces informations, la personne concernée peut, au besoin, demander au responsable de corriger, modifier ou supprimer les données si elles s'avèrent inexactes, erronées ou obsolètes ou si elles sont traitées en violation de la loi sur les données personnelles.

La réponse du responsable de traitement à ladite demande n'est enfermée dans aucun délai. C'est peut-être là une lacune de la loi qu'il faudrait corriger par l'instauration d'un délai raisonnable.

S'il s'avère qu'il y a violation de la loi sur les données personnelles ou même défaut de réponse, la personne conserve le droit de saisir l'autorité de régulation de toute violation de la loi ou même en cas défaut de réponse.

- L'opposition

Elle permet à toute personne de s'opposer, pour des motifs légitimes, à ce que ses données fassent l'objet de traitement. Toutefois, ce droit d'opposition ne s'applique pas lorsque le traitement répond à une obligation légale.

La personne concernée peut refuser, sans avoir à se justifier, que ses données soient communiquées à des tiers ou fassent l'objet de prospection commerciale.

Par ailleurs, le responsable du traitement est assujetti à des obligations de responsabilité et de confidentialité.

b- <u>Les obligations du responsable du traitement</u>

Le responsable de traitement est celui qui, seul, ou avec d'autres, prend la décision de collecter des données à caractère personnel et en détermine les moyens et la finalité. Il doit assurer la confidentialité et la pérennité des données.

• Les obligations de pérennité

Cette obligation engage le maître du traitement de prendre toutes les dispositions nécessaires pour que les données traitées puissent être exploitables

quel que soit le support technique utilisé. L'évolution technologique ne doit pas constituer un obstacle à l'exploitation ultérieure des données.

• La confidentialité

Le responsable de traitement doit observer la confidentialité dans la mise en œuvre de la collecte des données (article 38 de la loi du 25 janvier 2008). Aussi, des mesures de précaution sont nécessaires pour éviter que les données ne tombent entre les mains de tiers non autorisés.

Une autorité administrative indépendante est garante du respect de ces principes.

B- <u>la création d'une autorité de protection des données</u>

Au Sénégal, la Commission des données personnelles (CDP), autorité administrative indépendante, est garante du respect de la vie privée et des libertés individuelles ou publiques dans le traitement des données personnelles. Elle veille au respect du dispositif de protection par l'ensemble des acteurs, étatiques ou privées.

Pour ce faire, elle procède à un contrôle à priori et à posteriori sur tout traitement de données personnelles.

<u>1- La protection à priori exercée par la Commission des données personnelles: les régimes de protection</u>

Préalablement à la mise en œuvre d'un traitement de données personnelles, le responsable doit accomplir des formalités auprès de l'autorité de régulation. Ces formalités obéissent à un régime juridique déterminé en fonction en fonction de la finalité de traitement et de la nature des données collectées.

Il existe trois types de régime.

a-<u>le régime de déclaration</u>

C'est le régime de droit commun. Il s'applique aux traitements usuels tels ceux mis en œuvre par les organismes publics et privés pour la gestion de leur

personnel ou ceux réalisés à partir des systèmes d'information notamment la vidéosurveillance, les cartes magnétiques, ou systèmes de géolocalisation.

Pour être licites, ces traitements doivent faire l'objet de déclaration auprès de la CDP qui dispose d'un délai d'un mois pour procéder à un contrôle formel du projet avant de délivrer récépissé, document obligatoire avant toute mise en œuvre du traitement envisagé.

Dans sa délibération du 19/02/2016, la CDP a opposé un refus de délivrer récépissé à l'entreprise « W » et l'a sommée d'interrompre le traitement de données entrepris en violation des formalités déclaratives.

Aussi, doit être proscrite la tendance notée chez certains particuliers de procéder à des installations de vidéosurveillance (lieux de travail, domicile) sans aucune déclaration auprès de la CDP. De telles pratiques sont illicites et pénalement réprimées par les dispositions de l'article 431-14 CP.

b-Le régime de demande d'autorisation

Ce régime est de rigueur pour les traitements de données personnelles comportant **des risques élevés d'atteinte à la vie privée et aux libertés individuelles**. Il s'agit des traitements concernant les données sensibles, notamment les données biométriques, de santé et celles faisant l'objet d'un transfert vers d'autres pays.

Pour ce type de données, la CDP procède à un contrôle plus poussé avant de rendre une décision motivée.

c- Le régime de l'avis

Ce régime oblige de recueillir l'avis de la CDP préalablement à la mise en œuvre de traitements réalisés pour le compte des pouvoirs publics (Etat, collectivités territoriales, établissements publics).

Pour permettre à la CDP de mieux jouer son rôle d'avant-garde, les projets de loi et de décret portant sur le traitement de données personnelles devraient lui être soumis pour avis.

Néanmoins, la CDP peut accorder des dispenses ou édicter des normes simplifiées pour les traitements ne présentant pas de risques avérés ou potentiels pour la vie privée des individus

Ces formalités obligatoires permettent à l'autorité de régulation de procéder au contrôle du projet de traitement. Elle peut, alors, s'opposer à la mise en œuvre du traitement par décision motivée.

Ce contrôle formel placé en amont du traitement se complète d'une vérification de fond axée sur les opérations de traitement proprement dites.

2-La protection a posteriori

Elle vise à contrôler le traitement des données personnelles afin d'en vérifier la conformité au dispositif légal de protection. En cas de manquement constaté, la CDP est en droit d'infliger des sanctions administratives ou pécuniaires au responsable du traitement.

a-Les missions de contrôle

La CDP est dépositaire, outre des missions de veille et de contrôle, d'un pouvoir d'investigation pour vérifier la régularité du traitement des données. Elle peut, ainsi, accéder aux systèmes d'information du responsable de traitement et exiger communication de tout document ou information utile à l'accomplissement de sa mission de contrôle.

La Commission peut recueillir l'appui d'autorités étrangères de régulation lorsque les vérifications doivent être étendues sur le territoire d'autres Etats. Après les vérifications, elle dresse, de manière contradictoire, un procès-verbal des opérations de contrôle.

En cas de manquements dûment constatés, la CDP dispose d'une panoplie de sanctions pour contraindre le responsable de traitement à se conformer aux prescriptions légales.

b-Les sanctions

Il s'agit de sanctions graduelles allant de l'avertissement à la mise en demeure qui tendent à amener le responsable à se conformer aux prescriptions légales.

Si le maître de traitement ne se soumet pas aux instructions reçues, la CDP peut prononcer un retrait provisoire à définitif de l'autorisation de traitement ou une amende pécuniaire d'un (1) million à cent (100) millions de Frs CFA.

Pour exemple, dans sa décision du 06 novembre 2015, la CDP a adressé une mise en demeure à une société pour méconnaissance des principes de licéité, de loyauté et de proportionnalité et aussi violation de l'obligation d'information et de consentement préalable de la personne concernée.

En l'espèce, il s'agit d'un employeur qui avait adressé une demande d'explication à une salariée sur l'usage *« des réseaux sociaux pendant les heures de travail »*. Par la suite, il a procédé à son licenciement pour *« utilisation de l'ordinateur de travail à des fins étrangères à l'activité de la société »*.

L'employeur avait procédé à la collecte de plus de 100 messages purement privés de la salariée par le biais d'un logiciel d'espionnage installé, de manière indue, dans son ordinateur de travail.

La Commission des données personnelles rappelle, très justement, « que le salarié a droit, même au temps et au lieu de travail, au respect de son intimité et de la vie privée ».

Il est évident que l'employeur a fait preuve d'amalgame entre cyber sécurité et cyber surveillance des salariés. Il importe, en effet, de ne pas confondre la sécurité des systèmes d'information avec la surveillance systématique des salariés par le biais de dispositifs (vidéosurveillance ou logiciels) intrusifs installés dans leur environnement de travail.

Au surplus, en raison du principe de loyauté exigé en matière probatoire (Ass. Plénière C. cass. 07 janvier 2011), les sms collectés, en violation de la vie privée et de façon déloyale, ne sauraient servir de fondement audit licenciement.

En cas de découverte de faits délictuels, la CDP les dénonce immédiatement au procureur de la République. C'est la voie ouverte aux sanctions judiciaires.

II-LA MISE EN ŒUVRE JUDICIAIRE DU DISPOSITIF DE PROTECTION DES DONNEES PERSONNELLES

L'application du dispositif de protection peut générer deux types de contentieux. Il s'agit d'un contentieux extra pénal d'une part et d'un contentieux pénal d'autre part.

A-La protection extra pénale des données à caractère personnel

La loi du 25 janvier 2008 aménage une voie de recours, au profit du maître de traitement, contre les décisions de la CDP. C'est un contentieux administratif dévolu à la Chambre administrative de la Cour suprême (art 1er de la loi organique du 17 janvier 2017). Par ailleurs, la responsabilité du maître de traitement peut être engagée lorsque les opérations causent un dommage à autrui. C'est le contentieux civil.

1- La protection du juge administratif (les recours contre les décisions de la CDP)

Le recours contre les décisions de la CDP doit être formé dans un délai de deux mois à compter de la publication ou de la signification de la décision. Le contrôle de la Haute juridiction s'exerce aussi bien sur les décisions concernant les opérations de traitements que sur celles portant sur les formalités préalables.

a- Le contrôle de la Chambre administrative sur les décisions de la CDP concernant les formalités préalables

Le contrôle porte sur les décisions de la CDP relatives aux régimes de déclaration et d'autorisation.

Pour ce qui est du régime déclaratif, l'autorité de régulation délivre récépissé dès que le responsable respecte les prescriptions légales par le dépôt d'un dossier complet.

Le conseil d'Etat français rappelle d'ailleurs ce principe dans son arrêt du 06 janvier 1997 suite au recours pour excès de pouvoir intenté par la Caisse d'épargne Rhône Alpes Lyon qui est restée plus de neuf mois sans obtenir de réponse de la CNIL sur sa déclaration préalable de traitement.

La Haute juridiction considère que la CNIL ne peut refuser de délivrer récépissé du dépôt de déclaration dès lors que le dossier est complet, c'est-à-dire qu'il comporte l'engagement du responsable que le traitement est conforme et que la déclaration comprend toutes les informations requises.

b- Le contrôle de la Chambre administrative sur les décisions de la CDP concernant les opérations de traitement

D'abord, il faut souligner que le responsable du traitement, tout comme la personne concernée d'ailleurs, est autorisé à contester la décision de la CDP par la voie du référé administratif en application des dispositions de l'article 83 de la loi organique n°2017-09 du 17 janvier 2017 sur la Cour suprême.

Deux procédures semblent les mieux adaptés aux contentieux contre les décisions de la CDP.

Le référé suspension dont les conditions et les effets procèdent de l'article 84 de la loi précitée permet de demander au juge des référés de suspendre l'exécution de la décision administrative en cause ou de suspendre certains de ses effets dans l'attente d'une décision au fond.

Le référé liberté, prévu par l'article 85 de la même loi, permet d'obtenir, sous 48 heures, toute mesure nécessaire à la sauvegarde d'une liberté fondamentale à laquelle l'autorité a porté une atteinte grave et manifestement illégale.

Ensuite, pour ce qui est des manquements liés aux opérations de traitement, les décisions de la CDP n'ont pas encore fait l'objet de recours contentieux devant la Chambre administrative.

La jurisprudence du Conseil d'Etat français nous offre des exemples de décisions de censure de responsables de traitement ayant méconnus la loi du 06 janvier 1978 en matière de protection des données personnelles.

Pour exemple, dans son arrêt du 30 dec.2015, Le CE a confirmé une décision de la CNIL ayant prononcé un avertissement public contre la société Orange pour méconnaissance de l'obligation de sécurité. En l'espèce, il s'agissait d'une intrusion illicite sur le serveur d'une société sous-traitante d'un prestataire d'Orange permettant d'accéder aux données d'un million de clients et prospects de l'opérateur.

La Haute juridiction a rappelé l'obligation du responsable de prendre toutes les mesures appropriées de sécurité du traitement des données confiées à un sous-traitant.

La responsabilité du maître de traitement peut aussi être engagée sur le fondement de la responsabilité civile.

2-La protection assurée par le juge civil

En premier lieu, le juge civil peut être amené à se prononcer en dehors de tout contentieux. C'est le cas lorsque le responsable de traitement refuse l'accès des locaux aux membres de la CDP. Dans ce cas, la visite des locaux et le contrôle des installations ne peuvent se faire que sur autorisation du président du TGI territorialement compétent, par la voie de la procédure de référé injonction (art. 249 Code de procédure civile). La décision est susceptible d'appel devant le Premier Président de la Cour d'appel du ressort.

L'office du juge civil peut aussi être requis dans des situations d'urgence pour prendre toute mesure de sécurité nécessaire, notamment séquestre, saisie et autres décisions propres à empêcher ou faire cesser les atteintes aux données personnelles.

Ici, l'intervention du juge statuant à bref délai est requise, en dehors de toute procédure, afin qu'il ordonne au fournisseur d'accès de bloquer les contenus manifestement illicites.

C'est, notamment, le cas lorsqu'un blog recèle des contenus portant atteinte à la personnalité.

Cette obligation de retrait de contenu illicite à la charge de l'hébergeur, l'ayant eu en connaissance, prévue aussi à l'article 3 de la loi sur les transactions électroniques, devrait être renforcée par une nouvelle incrimination tendant à contraindre les responsables de sites, de forum ou de blog à assurer leur modération afin de mettre fin aux injures et autres appels à la haine.

Ensuite, les opérations de traitement peuvent causer des dommages qui justifient les victimes à saisir le juge civil afin d'obtenir réparation du préjudice subi. C'est la mise en œuvre de la responsabilité civile qui suppose l'existence d'une faute, d'un préjudice et d'un lien de causalité.

Les fautes susceptibles d'engager la responsabilité civile de l'auteur du traitement se résument généralement en des atteintes au respect de la vie privée ou du droit à l'image.

Le droit à l'image est concrètement le droit pour toute personne de s'opposer à la fois à la capture de son image et à la diffusion de celle-ci, sans son consentement préalable et expresse.

C'est sur le fondement du respect du droit à l'image que la cour suprême a, par arrêt du 200414 octobre 2011, confirmé l'arrêt de la Cour d'appel de Dakar du 17 novembre qui a déclaré fautive la publication d'un dépliant touristique exposant, avec un commentaire peu élogieux, l'image de deux dames photographiées à leur insu et leur a alloué des dommages-intérêt à titre de réparation.

Aussi, par arrêt du 19 janvier 2017, la Cour d'appel de Dakar a confirmé la condamnation d'un employeur qui avait adressé un courrier électronique à ses partenaires les informant du licenciement de trois de ses salariés. Le message était accompagné de la photo de chacun des ex salariés dont s'agit.

Dans sa motivation, la Cour a convoqué les dispositions de l'article 11 du Code de la famille pour soutenir que l'utilisation et la publication d'une photo sans autorisation de la personne concernée étaient constitutives d'une violation du droit à l'image. En conséquence, la Cour a retenu la responsabilité de l'auteur de la diffusion qu'elle a condamné au paiement de dommages-intérêts.

La juridiction d'appel a retenu, à juste titre, que le droit à l'image n'est paralysé par le droit à l'information que lorsque celle-ci porte sur des évènements historiques ou d'actualités. Et encore faudrait-il que l'image publiée respecte la dignité de la personne humaine sous peine de sanctions civiles ou pénales. Ainsi, la diffusion d'images de victimes d'accident, de crime ou même de personnes poursuivies en justice est punissable.

Par ailleurs, les atteintes aux données personnelles peuvent être constitutives d'infraction à la loi pénale.

B- <u>La protection pénale des données à caractère personnel</u>

La préservation des données personnelles commande de réprimer certains actes attentatoires à la vie privée et au dispositif légal de protection. A ce titre, les sanctions pénales apparaissent comme une arme dissuasive tendant à lutter efficacement contre les manipulations illicites de données personnelles.

La loi du 8 novembre 2016 modifiant le code pénal prévoit une série d'infractions qui se présentent d'une part en des violations du dispositif légal de protection des données personnelles et d'autre part en des atteintes spécifiques à la vie privée.

Le dispositif répressif intègre aussi la création de plusieurs unités spécialisées de lutte contre la cybercriminalité à la Direction de la police judiciaire et au niveau de la gendarmerie nationale. Ces unités ont une compétence nationale et sont dotées de moyens techniques leur permettant de mener des investigations en ligne.

1-<u>Les infractions attachées au respect de la loi du 25 janvier 2008</u>

Il s'agit, notamment, du délit de traitement en violation des formalités déclaratives (art 431-14), de détournement de finalité (art. 431-26 CP), de traitement de données en violation des mesures de sécurité (art.431-18 CP), d'entrave à l'action de la CDP (art 431-28).

D'abord, toute mise en œuvre d'un traitement clandestin, c'est-à-dire sans accomplissement des formalités préalables, expose le contrevenant (personne physique ou morale) à une sanction pénale (peine 01 an à 5 ans et ou d'une amende 500.000 frs à 10.000.000 frs CFA) en application des dispositions de l'article 431-14 du Code pénal.

Ensuite, pour permettre à la CDP de mener efficacement sa mission de contrôle à posteriori des opérations de traitement, tout ace tendant à entraver ladite mission fait l'objet d'une sanction pénale sous la qualification du délit d'entrave à l'action de la CDP, prévue et punie par l'article 431-28 du code pénal (six mois

à sept ans et d'une amende 200.000 frs à 1.000.000 frs CFA, ou l'une de ces peines).

Tombe sous le coup de cette incrimination le fait soit : de s'opposer aux membres de la CDP procédant aux contrôles des établissements de traitement, de refuser de leur communiquer les documents et renseignements utiles ou de délivrer des informations erronées ou inexploitables.

Ainsi, le responsable d'une association religieuse a été jugé coupable du délit d'entrave à l'action de l'autorité de régulation pour avoir envoyé à cet organisme des informations inexactes dans le but d'éluder le contrôle envisagé.

Enfin, le délit de collecte déloyale de données à caractère personnel (art.431-19 CP) permet de réprimer la collecte de données faite à l'insu de la personne concernée.

Le Tribunal de grande instance de Dakar, dans son jugement du 12 juin 2018, a déclaré frauduleuse la collecte de données effectuée par un prévenu qui a accédé, de manière indue, à la messagerie électronique de son épouse. La déloyauté de la collecte résulte de la fraude ou de l'absence de consentement de la personne concernée.

Seulement, d'après les pénétrantes remarques de notre collègue Dr Papa Assane Touré formulées dans sa thèse de doctorat d'état intitulé « le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal » publié dans les Editions de l'Harmatan, le simple accès indu à la messagerie électronique d'un tiers ne constitue pas une collecte déloyale de données personnelles en dehors de toute utilisation des dites données ; Ce comportement s'analyse plutôt en un accès frauduleux à un système informatique.

2-<u>Les infractions contre la vie privée et la représentation de la personne</u>

La tendance effrénée de divulgation, dans les réseaux sociaux, de données touchant à l'intimité des personnes, particulièrement dommageable, convainc le législateur d'opter pour une politique répressive contre la cyberdélinquance. C'est

le lieu, peut-être, de plaider pour plus de sévérité contre les auteurs de tels actes attentatoires à la vie privée.

Pour juguler ce phénomène criminogène, la loi du 08 novembre 2016 et celle du 25 janvier 2008 sur la cybercriminalité prévoient une série d'incriminations ayant pour objet la protection pénale de la vie privée et de l'image des personnes en général.

On peut citer le délit de divulgation illicite de données à caractère personnel (art. 431-27 du CP peine de six mois à cinq ans et/ou d'une amende de 300.000à 5.000.000 frs CFA).

Ce délit, assez récurrent, consiste à porter à la connaissance de tiers des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée.

Pour une application jurisprudentielle, le Tribunal de grande instance de Dakar, dans son arrêt n° 2114 du 03 mai 2013, considère que le fait de poster sur Facebook une vidéo montrant l'intimité d'un couple constitue une divulgation illicite de données à caractère personnel.

Aussi la captation ou diffusion des paroles d'une personne prononcées à titre privé sans son consentement est pénalement réprimée (art. 363 bis 1° CP).

La captation ou diffusion de l'image d'une personne se trouvant dans un lieu privé sans son consentement (art. 363 bis 2° CP) et la publication d'un montage réalisé avec l'image ou les paroles d'une personne sans son consentement (art. 363 bis alinéa 3 CP) sont aussi sévèrement sanctionnées d'une peine d'un an à cinq ans et d'une amende de 500.000 frs à 5.000.000 frs CFA.

Outre la répression, l'autorité judiciaire ou de police peut, par réquisition, faire retirer ou rendre inaccessibles des contenus attentatoires à la vie privée même hébergés à l'étranger (art. 90-14 CPP).

Aussi, le blocage judiciaire d'un site au contenu manifestement attentatoire à la vie privée peut être ordonné si nécessaire.

Il appartient au Juge d'instruction ou à l'Officier de police judiciaire sur autorisation du Procureur de la République de notifier au fournisseur d'accès internet les adresses des services de communication électronique qu'il doit bloquer sans délai (art. 90-13 CPP).

Toutefois, il existe des limites objectives à l'efficacité des moyens de lutte contre ces actes cybercriminels.

Le premier écueil résulte des techniques des techniques de contournement du dispositif de retrait et de blocage de contenus illicites à travers le recours à des procédés technologiques complexes (recours à un réseau privé virtuel, usurpation d'une adresse IP, navigation dans le dark web, web sombre ou clandestin assurant l'anonymat et par suite une certaine impunité aux cybercriminels, …).

En outre, avec la rapidité et les particularités de circulation des informations dans le cyberespace , les contenus préjudiciables à la vie privée finissent par se distiller dans les réseaux sociaux (Face book, Twitter, Linkedin, etc.) et les autres réseaux de communication (Imo, WhatsApp, Viber, You tube, etc.).

En effet, la publication instantanée en ligne est référencée par de multiples moteurs de recherche et mise à la disposition d'un public planétaire ; elle est ainsi susceptible d'être consultée indéfiniment et téléchargeable au gré d'une requête ou d'un lien hypertexte.

L'effectivité du retrait ou du blocage des informations transitant par ces plates-formes exige une coopération avec les acteurs globaux de l'internet, pour l'essentiel établis au pays de l'oncle Sam, qui considèrent souvent les données personnelles comme l'essence de leur modèle économique.

Enfin, l'espace territorial national paraît étroit pour combattre les atteintes à la vie privée et aux libertés résultant du traitement des données personnelles. C'est un phénomène transfrontalier au contenu mouvant et variable au-delà du pays des Diallobé, eu égard aux mœurs généralement différentes et aux intérêts antinomiques.

Toutes limites qui postulent finalement à la nécessaire réadaptation du dispositif de protection des données personnelles face aux nouvelles transformations du numérique.

Conclusion

Le dispositif légal et institutionnel de protection des données personnelles vient d'avoir 10 ans. Il est encore en phase d'incubation. Mais déjà, les transformations du numérique engendrées par les mutations à la fois techniques (méga données, intelligence artificielle, internet des objets, …), économiques (profilage des consommateurs), sociales et culturelles commandent la mise à jour dudit dispositif et l'adoption de nouvelles règles protectrices des données personnelles.

La Commission des données personnelles a déjà entrepris des travaux d'actualisation de la loi du 25 janvier 2008 et aussi d'éminents juristes comme le Professeur Mamoudou Niane et le docteur Mouhammadou Lô ont défriché la voie avec d'excellentes contributions.

Au regard de tous ses travaux et aussi de ce qui précède, la réadaptation de l'arsenal de protection devrait s'articuler autour du tryptique suivant : amélioration du cadre juridique actuel, renforcement les moyens de la Commission de protection des données et sensibilisation des acteurs par les politiques.

Pour améliorer le cadre juridique, il est souhaitable :

- d'alléger les formalités relatives aux traitements sans risque par une procédure de simplification à définir avec les acteurs ;

- d'amener les responsables de traitement (personnes morales) à désigner un Délégué à la protection des données personnelles, en contrepartie de l'allègement des obligations déclaratives ;

- de définir avec les acteurs le rôle des Délégués à la Protection des données en termes d'informations, de veille et d'audit ; A ce niveau, il urge de nommer des points focaux dans les ministères afin d'éviter que des traitements de données personnelles soient mis en œuvre sans avis préalable de la CDP. Comme ce fut le cas avec les permis numériques qui comportent des données très sensibles dont le groupe sanguin.

- d'encourager l'utilisation de technologies protectrices des données personnelles dès la conception de l'application ou du logiciel, c'est le « privacy by design » ou dans ses paramètres par défaut, il s'agit du « privacy by default » ;

- de consacrer le droit à l'oubli, la notification des violations des données personnelles, le droit au déférencement et la portabilité des données ;

- de fixer dans un texte la durée maximale de conservation des données ;

- d'adopter des règles pour l'anonymisation systématique des décisions de justice publiées ;

-d'interdire l'hébergement de certaines données hors du Sénégal (données de santé, biométriques, données des services de sécurité) ;

- de rendre obligatoire l'avis de la CDP avant tout traitement de données au profit des pouvoirs publics et pour les projets de lois et décrets concernant les données personnelles ;

-Inviter les pouvoirs publics à saisir la Chambre administrative de la Cour suprême en cas d'avis négatif.

- d'exclure le sursis pour les auteurs de cyberdélits portant sur la vie privée, la représentation des personnes, les injures et les appels à la haine ;

- d'élaborer et mettre en œuvre, en rapport avec l'Union africaine, un cadre africain de protection des données personnelles par la mise en place d'un cloud continental pour limiter la perte de la souveraineté numérique ;

Pourquoi ne pas envisager la création d'une instance africaine de protection des données personnelles ?

Pour être efficace, la protection des données personnelles doit nécessairement revêtir une dimension transnationale : à un phénomène globale doit correspondre une régulation globale.

L'Afrique ne saurait être considérée comme une « tabula rasa » en matière de réglementation du traitement des données personnelles. Une protection efficiente des dites données dépasse forcément le cadre étriqué de l'Etat-nation et devrait revêtir une dimension continentale.

Les pays occidentaux ajustent de plus en plus leur législation pour permettre aux autorités judiciaires d'accéder aux informations stockées dans les serveurs des prestataires.

Le cloud act des Etats-Unis d'Amérique et son pendant le projet européen E-evidence permettent aux autorités répressives de ces pays d'obtenir communication des preuves électroniques détenues par les fournisseurs de service internet et cloud, indépendamment de leurs lieux de localisation.

En ce qui concerne la CDP, à ce niveau, il y a de l'ouvrage mais peu d'ouvriers et de moyens, alors pour la renforcer, il faudrait commencer par :

- l'ériger en une Autorité des données à caractère personnel (harmoniser les textes et renforcer sa légitimité) ;

- lui fournir des moyens techniques et des ressources humaines conséquents ;

- prévoir d'autres sources de financement comme des redevances à payer pour ses services et prestations.

Pourquoi ne pas envisager la création d'un fonds de protection des données personnel alimenté par les responsables de traitement notamment ?

Enfin dans le cadre des politiques publiques de protection des données, il est impérieux d'engager un travail méthodique d'éducation et de sensibilisation de l'ensemble des acteurs, surtout les citoyens à la base pour que les TIC (surtout internet) ne soient pas sources de régression mais plutôt de progression par le respect absolu de la personne humaine, de sa vie privée et de sa dignité.

DAKAR, LE 08 JANVIER 2019