



**AUDIENCE SOLENNELLE
DE RENTRÉE DES COURS ET TRIBUNAUX
*Mardi 08 janvier 2019***

-----∞-∞-∞-∞-∞-∞-----

-----∞-∞-∞-∞-----

-----∞-∞-----

THÈME :

La protection des données personnelles

ALLOCUTION

DE

**MONSIEUR CHEIKH AHMED TIDIANE COULIBALY
PROCUREUR GÉNÉRAL
PRES LA COUR SUPRÊME**

ANNÉE JUDICIAIRE 2018 - 2019

***Monsieur le Président de la République,
Président du Conseil supérieur de la Magistrature,
Garant de l'indépendance de la justice,***

Notre loi fondamentale vous confie une responsabilité éminente et emblématique, celle de garantir l'indépendance du pouvoir judiciaire, assisté du conseil supérieur

de la magistrature. En acceptant, ce matin, comme vous le faites depuis votre accession à la magistrature suprême, de présider l'audience solennelle de rentrée des cours et tribunaux, vous faites honneur à la cour et à la justice et symbolisez de manière forte le rôle particulier du Chef de l'Etat à l'égard du pouvoir judiciaire.

Monsieur le Président de la République, notre attente et notre espoir sont grands de vous voir réaliser les projets attendus pour notre justice. Acceptez alors l'expression de notre profonde gratitude.

Monsieur le Garde des Sceaux, nous vous accueillons pour la deuxième fois dans nos locaux, à l'occasion de l'audience solennelle de rentrée. Nous savons que vous vous investissez totalement dans les fonctions difficiles mais exaltantes qui vous sont confiées et portez un intérêt tout particulier à l'institution judiciaire et nous saluons la qualité de l'approche que vous avez des défis qui nous interpellent. Vous pourrez toujours compter sur l'écoute attentive et la disponibilité des magistrats.

***Monsieur le Président de l'Assemblée nationale,
Monsieur le Premier Ministre,
Monsieur le Président du Haut Conseil des Collectivités territoriales (HCCT),
Madame la Présidente du Conseil Économique, Social et Environnemental,
Mesdames, Messieurs les Ministres,
Mesdames, Messieurs les députés,
Monsieur le Président du Conseil constitutionnel,
Monsieur le Premier président de la Cour suprême,
Monsieur le Premier président de la Cour des comptes,
Monsieur le Procureur général près ladite Cour,***

Mesdames, Messieurs les chefs d'institutions juridiques et autorités administratives autonomes,
Mesdames, Messieurs les Ambassadeurs et Chefs de Missions diplomatiques,
Messieurs les Officiers généraux,
Messieurs les Recteurs, Messieurs les Doyens et Professeurs représentant la communauté universitaire,
Messieurs les Dignitaires religieux et coutumiers,
Monsieur le Bâtonnier du Conseil de l'Ordre des Avocats,
Mesdames, Messieurs les anciens Chefs ou membres de la juridiction suprême,
Mesdames, Messieurs les Magistrats et chers collègues,
Mesdames, Messieurs les Avocats,
Mesdames, Messieurs les Officiers ministériels et Auxiliaires de justice,
Mesdames, Messieurs,
Honorables invités,

Je voudrais vous remercier de votre fidélité à cette cérémonie annuelle de rentrée solennelle des cours et tribunaux et vous souhaiter une bonne et heureuse année 2019.

Au cours de l'année qui s'achève la Cour suprême a reçu 500 requêtes et rendu 554 arrêts et ordonnances toutes chambres confondues, compte tenu du stock précédent. Les inspections des cours et tribunaux et des parquets ont rendu visite à la Cour d'appel de Kaolack, aux tribunaux de grande instance et d'instance de la même localité et de Nioro du Rip. Des rapports ont été établis sur les difficultés réelles de fonctionnement de ces juridictions qui sont d'ordre matériel, d'équipement et de personnel.

Au titre de l'activité consultative, la Cour a reçu neuf (09) projets de loi et de décrets et émis huit (08) avis favorables.

Je voudrais aussi, relever, pour m'en réjouir, que la commission d'indemnisation d'une personne ayant fait l'objet d'une détention provisoire au cours d'une procédure

terminée à son égard, par une décision de non-lieu, de relaxe ou d'acquiescement devenue définitive, lorsque cette détention lui a causé un préjudice manifestement anormal et d'une particulière gravité, prévue par la loi organique sur la Cour suprême, est enfin opérationnelle et a reçu pendant l'année 2018 sept (07) requêtes.

Les réflexions de ce matin portent sur la protection des données à caractère personnel.

Elles ont été brillamment introduites par Ousmane Guèye conseiller à la Cour d'appel de Kaolack. Permettez-moi de le féliciter pour sa remarquable prestation.

Les données à caractère personnel sont, toute information relative à une personne physique, qui l'identifie ou est susceptible de l'identifier directement ou indirectement ; qu'il s'agisse du nom patronymique, de la signature, de l'image, des empreintes génétiques ou biométriques, d'un numéro de téléphone, d'une adresse IP, d'un numéro de NINEA ou de RCCM etc.

Pour des raisons évidentes d'ordre public et de responsabilité, de sécurisation des relations juridiques des particuliers entre eux ou avec l'Etat, aussi, nul n'a le droit incompressible de demeurer dans l'anonymat au sein d'une société organisée.

Les individus doivent être identifiés en tant que de besoin dans leur vie personnelle tout comme professionnelle y compris pour les besoins de l'exercice de leurs droits civiques, mais dans des proportions strictement nécessaires aux finalités poursuivies et dans le respect de leurs libertés et droits fondamentaux.

La question du traitement des données à caractère personnel n'est donc pas nouvelle, au vu de la place essentielle que la connaissance de celles-ci occupe dans le bon fonctionnement d'un Etat ; mais avec le développement de l'informatique, les possibilités et les capacités à collecter, stocker, interconnecter et traiter ces données, ont atteint un tel niveau de facilité et de simplicité, qu'un encadrement strict et approprié de toute action sur ces données, est devenu une priorité dans nos sociétés contemporaines. En effet, « les progrès de l'informatique sont porteurs d'autant de bienfaits

que

de dangers, notamment à l'égard du droit à la vie privée ». Aujourd'hui, il s'agit de protéger les individus contre les menaces que font peser les nouvelles technologies sur les libertés, d'éviter que l'utilisation des moyens technologiques n'entraîne, un recul des libertés individuelles même si le principe de la liberté de circulation des données personnelles doit être préservé.

Si au niveau international dès le début des années 90 la question a été prise en compte par les Nations Unies, au plan communautaire africain ce n'est qu'en 2010, avec l'acte additionnel relatif à la protection des données personnelles dans l'espace CEDEAO, que l'encadrement juridique s'est amorcé.

Pour sa part, le Sénégal a saisi les enjeux liés au traitement des données personnelles un peu plutôt, avec l'adoption en 2008 de la loi sur les données à caractère personnel.

Tenant compte de la particularité de l'écosystème du traitement des données personnelles, où le citoyen est entre le marteau des acteurs économiques et l'enclume des gouvernants, l'option de la régulation a été prise, par l'institution d'une autorité administrative indépendante, la CDP (Commission des Données Personnelles), en l'occurrence, chargée de traiter et de contrôler les différents régimes de liberté, de déclaration, d'autorisation et d'avis, applicables en fonction de l'auteur, des objectifs et des risques du traitement de données souhaité.

Parallèlement la protection des données à caractère personnel s'appuie sur la loi 2008-11 du 15 janvier 2008 portant sur la cybercriminalité, modifiée par la loi 2016-29 du 08 novembre 2016 portant modification du code pénal, qui a prévu des infractions pénales spécifiques adaptées à la répression de la délinquance informatique notamment les atteintes aux droits de la personne au regard du traitement des données à caractère personnel.

Ainsi ce cadre juridique et institutionnel organise la protection des données à caractère personnel depuis une dizaine d'années. Quel bilan faut-il en tirer ? Quel niveau de pertinence et d'efficacité présente-t-il ? Quelles perspectives envisager ? Autant de questions dignes d'intérêt auxquelles le discours d'usage a su

répondre

avec une éloquence remarquable.

Notre pays, il est vrai, a initié un dispositif juridique qui globalement correspond aux normes internationales ; malgré tout, les atteintes à la vie privée qui alimentent inlassablement les faits divers dans l'espace public, sont devenues si ordinaires et répétées, qu'elles exigent beaucoup plus d'attention dans l'optique d'une meilleure protection des données à caractère personnel.

Toutefois, il faut remarquer que les défaillances du secteur sont mondialement partagées parce que le développement ultrasonique du cyberspace a rendu énormément complexe toute entreprise de protection des données à caractère personnel.

L'informatique a profondément intégré nos sociétés contemporaines et contribue largement à faciliter nos actions du quotidien et nos relations interpersonnelles ou interprofessionnelles ; de même qu'elle offre d'immenses possibilités aux pouvoirs publics dans l'exercice de leurs missions régaliennes particulièrement celles de garantir la sécurité publique.

Ainsi le monde est dans une sorte de transition informatique, confronté à des interrogations essentielles qui touchent aux fondements de l'Etat de droit et de la démocratie.

Le traitement des données à caractère personnel est, en effet, au confluent de plusieurs droits fondamentaux qui s'entrechoquent, se contredisent et s'opposent.

Ce n'est plus une simple catégorie de droits de la personnalité caractérisée par leur extra-patrimonialité. L'utilisation massive et croissante des moyens de communication notamment des TIC (technologies de l'information et de la communication) a fait que les données à caractère personnel ont acquis une dimension socio-économique infinie qui en fait un objet de grande convoitise de sorte qu'il devient primordial, plus que partout ailleurs, de concilier dans le cyberspace, le respect de la vie privée avec la liberté d'entreprendre, la liberté d'information et d'expression

tout comme de trouver un équilibre entre les impératifs de l'ordre public et de la justice avec les droits fondamentaux et l'exercice des libertés publiques.

Ces préoccupations ne sont pas absentes de la loi sur les données personnelles qui précise dans son exposé des motifs que « Leur traitement doit se dérouler dans le respect des droits, des libertés fondamentales, de la dignité des personnes physiques. ».

Et dispose en son article premier qu'« elle prend également en compte les prérogatives de l'Etat, les droits des collectivités locales, les intérêts des entreprises et de la société civile.

...Veille à ce que les Technologies de l'Information et de la Communication (TIC) ne portent pas atteinte aux libertés individuelles ou publiques, notamment à la vie privée. ».

Pour ma part, je voudrais réfléchir sur les défis auxquels se heurte la régulation des données personnelles, notamment dans notre pays, au regard des difficultés à garantir le respect de la vie privée dans un monde où l'utilisation des TIC a intégré la banalité

du quotidien mais aussi où, la sécurité publique est plus que jamais au centre des préoccupations, particulièrement en raison de la persistance de la menace terroriste.

En effet, l'on ne peut rester indifférent aux interrogations sur la protection des données personnelles, suite à la valeur économique qu'elles ont acquise, à l'information en ligne, aux conséquences de leur extra-territorialisation ou encore au regard de la crise sécuritaire sans précédent que traverse le monde.

Protection des données personnelles et valeur socio-économique des données

A l'ère du numérique, la difficulté est telle que d'aucuns, sans doute résignés, décrètent « la mort de la vie privée », tandis que d'autres, certainement les plus prudents, parlent de « recul de la vie privée ». Le moins que l'on puisse dire, c'est qu'utiliser

les moyens de communication, sans renoncer à rester anonyme, relève du paradoxe.

L'informatique, il faut le reconnaître, à force d'investir tous les rouages de la société, est devenue un phénomène social, un instrument dont on ne peut plus se passer. Un auteur a dit que « l'informatique constitue aujourd'hui, un nouvel impérialisme. Elle est partout, envahit tout, la vie personnelle comme

la vie professionnelle sous forme de matériel, de logiciels et de services » (A. Lucas, I. Deveze et Frayssinet).

Le progrès technologique dit-on ne connaît pas de retour en arrière, mais l'informatique, pour paraphraser MALLET-POUJOL, est un puissant vecteur de collecte et de diffusion de données à caractère personnel. Et ce, plus que jamais, avec l'explosion des réseaux sociaux. Nous sommes dans une société de l'information, où l'individu tire sa fierté et sa satisfaction, mesure sa réussite, au nombre de regards qu'il attire, en exposant sa vie au public.

L'hégémonie de l'informatique et l'attrait inconsidéré de l'homme moderne pour les réseaux sociaux, aiguissent des appétences de toutes sortes notamment pour les employeurs et les sociétés commerciales.

Les premiers s'en servent pour contrôler l'activité de leurs salariés, tandis que les secondes y trouvent un outil inestimable de profilage et de fichage aux fins de marketing, leur permettant de brasser un nombre incalculable d'informations auprès des utilisateurs du réseau internet, parfois même à leur insu.

Bien entendu cette collecte de données personnelles est soumise à la loi sur les données personnelles notamment à une obligation de loyauté ; autrement dit le consentement de la personne concernée doit être recueilli préalablement ; l'on parle ainsi de données déclaratives.

Mais nous savons tous, que cette soupape est fragile dès lors que ce consentement est souvent indispensable pour continuer à naviguer utilement, au point que,

l'internaute pour ne pas être pénalisé, n'a d'autre choix que de cocher la case acceptation, sans avoir la certitude que les données sollicitées sont pertinentes au regard de la finalité du traitement et seront conservées dans des conditions de sécurité lui garantissant la confidentialité indispensable au respect de sa vie privée ; il donne ainsi son consentement sans aucune assurance que les données collectées ne seront pas détournées de leur finalité ou revendues.

De toute façon nonobstant tout consentement, l'avancée technologique a affiné les méthodes de traçage par l'utilisation et l'exploitation de « cookies » ou témoins

de connexion, des données de connexion informatique, métadonnées, objets connectés etc. qui ont permis de développer le captage de données dites perceptibles, c'est-à-dire de données collectées à l'insu des utilisateurs.

De sorte que, les entreprises privées peuvent constituer des « méga-bases de données » ou « big data » qui leur donnent « la possibilité d'établir de manière automatique et systématique un profil économique, psychologique, sociologique et culturel, de déterminer des probabilités fortes d'opinions, de conviction et de comportements... » (Claude BOURGEOS). Autrement dit, nos habitudes intimes de consommation et même de vie ne leur sont plus étrangères. La profondeur de cette intrusion est effrayante !

Aujourd'hui il n'échappe à aucun observateur averti, que les principes qui gouvernent le traitement des données personnelles sont souvent ignorés par les responsables de traitement. Les dérives ont atteint un tel niveau que l'on parle de surveillance de personnes privées par d'autres personnes privées à des fins économiques.

Les citoyens doivent pouvoir en saisir les enjeux et faire montre de plus de prudence, car bien que leur inquiétude soit grandissante, leur utilisation des TIC, ne faiblit pas.

La garantie du respect de la vie privée doit passer nécessairement par une plus grande sensibilisation des sénégalais aux techniques de navigation sécurisées et la vulgarisation des droits qu'ils tiennent de la loi. En raison des enjeux des données personnelles, une protection efficace passe nécessairement par une CDP beaucoup plus entreprenante et proactive.

Il faut aussi accorder davantage d'attention à la collecte des données personnelles des mineurs ou par les mineurs et, redoubler de vigilance concernant le traitement des données sensibles, telles les données de santé, à des fins commerciales, qui peut avoir de fâcheuses répercussions, au point que certains spécialistes plaident l'interdiction nonobstant le consentement des intéressés.

Il est vrai que l'utilisation dans les pays technologiquement très avancés des données comportementales à des fins de prospection n'est pas pour le moment

comparable à la situation des pays en développement mais, il faut dans une démarche prospective, mettre l'accent sur le contrôle à posteriori agrémenté de moyens techniques adéquats, parce que le droit à l'anonymat et à la vie privée doit prévaloir sur les intérêts économiques et sur la liberté d'entreprendre.

De toute manière si le sentiment d'insécurité perdure, nos pays auront du mal à profiter pleinement du commerce numérique. La confiance des citoyens envers l'administration et les entreprises privées qui collectent les données personnelles,

est fonction, en effet, du respect de la législation en matière de protection des données personnelles.

Mesdames, Messieurs, l'information en ligne mérite davantage de vigilance.

Les informations à caractère personnel, mises en ligne par la presse électronique, portent par comparaison à la presse papier, une atteinte sans commune mesure aux droits fondamentaux, notamment au droit au respect de la vie privée et à la présomption d'innocence.

La presse en ligne offre des possibilités de duplication et d'archivage qui ont tendance à donner aux informations publiées un caractère permanent, par la consultation facile et à tout moment via un simple clic sur les moteurs de recherche qu'elle permet.

Certes au nom de la liberté fondamentale d'information, toute référence aux affaires judiciaires en cours ne peut être interdite mais au regard des opportunités de diffusion et de pérennisation des données publiées sur internet, le respect de la vie privée et de la présomption d'innocence, recommande plus de prudence relativement aux données personnelles qui sont publiées.

Il n'est pas rare, bien après une décision de relaxe, que des informations attentatoires à la présomption d'innocence soient toujours accessibles par les moteurs de recherche, en violation de ce droit fondamental ; ou que par la magie du WEB des publications de condamnations pénales puissent être consultées, longtemps après que les concernés eurent purgé leur peine. Ce référencement perpétuel ne paraît pas compatible avec le respect de la vie privée.

Il faudrait donc veiller à l'anonymisation des publications en matière pénale pour assurer la protection de la vie privée et de la présomption d'innocence.

Surtout, il faudra enrichir notre cadre juridique d'un droit à l'oubli et au déferencement. Il ne s'agit pas de comprimer la liberté d'information mais de la concilier avec les droits fondamentaux de la personne, par la suppression de tous liens associés aux données personnelles d'un individu si la conservation de celles-ci est illégitime.

Au-delà de la responsabilité des cybercriminels, le déferencement constitue une mesure de réparation efficace contre les textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne, publiés illicitement et qui portent atteinte

à la réputation des individus sur internet.

D'ailleurs, la problématique du contenu sur internet avec le développement du WEB2.0, interpelle à plus d'un titre. Lors de son audition devant le congrès Américain, le Président Directeur général de Facebook a admis « ne pas avoir suffisamment réfléchi à la manière d'éviter les abus dans l'utilisation des données personnelles de ses 2,23 milliards d'utilisateurs actifs ».

Quoiqu'il en soit il faut agir ; mais le faire avec circonspection car il ne s'agit pas d'entraver la liberté d'expression, mais de sanctionner les dérives ou autres abus car « ce qui était hier inadmissible sur support papier demeure inacceptable, à l'heure d'Internet sous forme de fichier électronique ».

Cependant le caractère international du réseau internet, qui permet une circulation transfrontière des données, constitue actuellement un défi majeur de la protection des données personnelles.

L'extra-territorialité des données

Lorsque les données traitées sont hébergées sur le « cloud computing », par l'utilisation de plusieurs serveurs disséminés à travers la planète, il devient pratiquement impossible de déterminer le droit applicable ou d'identifier le juge

compétent et de qualifier les obligations qui pèsent sur chaque responsable du traitement.

C'est le cas également pour le transfert international des données.

Dans nos pays, le transfert des données vers des entreprises basées hors de nos frontières, rend difficile voire impossible, la protection des informations. En effet, les données stockées à l'étranger sont soumises à la législation du pays d'accueil. Et ce transfert n'est pas sans conséquence puisque les données stockées pourraient être détournées de leur finalité.

Ancienne membre de la CNIL, Madame Marie Georges, soutenait à ce propos que « ce sont des activités contraires aux droits de l'homme qui nécessitent l'adoption d'un instrument international sous l'égide de l'organisation des Nations-Unies ».

La solution à ces difficultés c'est d'arriver donc à mettre en œuvre un cadre de coopération internationale. Notre pays a élaboré une stratégie nationale pour la transformation numérique et se trouve être avec l'Ile Maurice, seul pays Africain membre de la convention de Budapest sur la cybercriminalité et dont l'article 32 postule l'accès transfrontalier aux données personnelles.

L'Afrique devra travailler à assurer un niveau de protection adéquat des données à caractère personnel par l'adoption d'une législation conforme aux standards internationaux et à la mise en place d'une autorité de protection véritablement opérationnelle susceptible de donner confiance aux investisseurs, aux particuliers ainsi qu'aux professionnels des secteurs des TIC.

Mesdames messieurs, ces dernières années nous avons été habitués à ce que les infractions les plus insidieuses portant notamment sur le traitement illicite de données personnelles soient révélées par des fuites de données communément appelées « Leaks » savamment organisée par ceux qu'il est convenu d'appeler les lanceurs d'alerte.

Ces dénonciateurs citoyens sont devenus les sentinelles de nos démocraties de sorte que certaines législations, à l'instar de la France, qui ont saisi leur utilité, s'organisent pour leur conférer un statut.

Au Sénégal, notre législation, ne laisse aucune place aux lanceurs d'alerte, le procédé, étant du reste pénalement réprimé, mais il me semble que cet activisme civique mérite d'être protégé et encadré, d'autant plus que notre charte fondamentale dispose en son article 25-3 alinéa 2 que « Tout citoyen a le devoir de défendre la patrie contre toute agression et de contribuer à la lutte contre la corruption et la concussion ».

Protection des données à caractère personnel et crise sécuritaire

Parce que la sécurité est pour eux un bien beaucoup plus précieux que la liberté, les hommes acceptent, pour une vie paisible, de renoncer au profit de l'Etat à une parcelle de leur liberté.

Mais dans un Etat de droit, les contraintes que peut supporter l'exercice des libertés, doivent être nécessaires et proportionnées aux objectifs poursuivis ; il ne saurait en être autrement car « Toute Société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des Pouvoirs déterminée n'a, point de Constitution. ».

Concilier les impératifs de liberté et sécurité, de liberté et justice, de sécurité et justice, est donc une exigence absolue de nos démocraties.

Mais aujourd'hui, avec les réactions toujours plus intrusives des gouvernants face à la recrudescence des actes terroristes, cet équilibre est plus que jamais fragilisé au détriment des libertés et droits fondamentaux.

Dans ce contexte, la protection des données personnelles, se trouve au centre de toutes les attentions, particulièrement depuis qu'un célèbre lanceur d'alerte (Edouard SNOWDEN pour ne pas le nommer) a révélé au grand jour, la surveillance massive et généralisée de l'ensemble de la population par des acteurs privés, pour le compte d'acteurs publics.

Le secret des communications électroniques, le droit d'aller et de venir, ont été, en effet, chahutés par les velléités de surveillance systématique. Ce qui a mis à rude épreuve nos démocraties qui se trouvent confrontées à des interrogations essentielles.

A quel prix faut-il adapter notre arsenal juridique de prévention et de répression du terrorisme ? Quel compromis trouver ? Où placer le curseur entre la sécurité et la liberté dans la lutte contre le terrorisme ?

Celle-ci a justifié de nouvelles lois toujours plus répressives et restrictives des droits fondamentaux mais les garanties de la démocratie et de l'Etat de droit ne sauraient être sacrifiées sur l'autel de la lutte contre le terrorisme ; au risque de perdre d'avance le combat parce que justement, c'est l'Etat de droit que, combattent les terroristes.

Aussi impérieuse qu'elle soit, la lutte contre le terrorisme ne saurait valoir caution pour que les gouvernants usent et abusent de leurs ressources et de leurs prérogatives pour justifier des atteintes hors de proportion à la vie privée notamment.

Elle appelle au contraire, des réponses légales et judiciaires efficaces mais respectueuses de l'Etat de droit. Les cours suprêmes du Sahel membres de l'Association des Hautes Juridictions de Cassation des pays ayant en partage l'usage du Français (AHJUCAF) ont du reste, manifesté leur attachement à cet équilibre dans les lignes directrices qu'elles ont adoptées à Dakar le 2 mars 2018 dans le cadre de la lutte contre le terrorisme.

Il ne faut pas s'y tromper, la technologie offre aux pouvoirs publics la possibilité d'actions toujours plus intrusives, vidéosurveillance, géolocalisation, biométrie etc. ; le véritable enjeu a trait aux moyens de contrôle efficaces et effectifs qui les accompagnent pour garantir le respect des droits fondamentaux du citoyen.

Notre pays, a fait le choix fort, que les investigations informatiques en matière d'infraction relative au terrorisme, ne soient pas dérogatoires au droit commun. Ainsi l'interception de correspondances téléphoniques ou émises par voie électronique ou l'utilisation d'un logiciel à distance pour recueillir des éléments de preuve utiles à l'enquête se font sous la direction et le contrôle d'un magistrat quand bien il s'agisse de terrorisme.

A cet égard, le rôle du juge judiciaire, protecteur des libertés fondamentales est primordial. Ainsi par exemple, la loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant code de procédure pénale, à son article 90-13, permet grâce au mécanisme du référé électronique, au président du tribunal de grande instance statuant à bref délai, de prendre toute mesure permettant d'empêcher la

diffusion d'images ou de représentation de mineurs à caractère pornographique ou de contenus manifestement illicites.

Le juge administratif et le juge constitutionnel également, doivent veiller particulièrement à ce que toute restriction législative des droits fondamentaux soit nécessaire et proportionnée. A cet effet, ils ne doivent jamais perdre de vue que, la surveillance secrète, massive et indiscriminée est inacceptable, au même titre que l'accès à des données personnelles aux fins de sécurité dans une société démocratique, dès lors qu'il est massif et sans condition.

Somme toute, il est devenu extrêmement difficile de protéger les données personnelles, surtout quand elles transitent par internet, ce d'autant plus, lorsque la sécurité nationale est en cause.

C'est le lieu de rappeler l'importance du mécanisme du référé administratif, institué par la nouvelle loi organique sur la Cour suprême. En effet par le référé mesures utiles ou le référé libertés fondamentales, le Président de la Cour suprême statuant en urgence peut jouer un rôle fondamental dans la protection des données personnelles mises en péril.

En conclusion, retenons avec Pape Assane Touré, magistrat, expert en cyber droit, que « les transformations digitales d'aujourd'hui, sans précédent (cloud computing,

Big Data, Open Data, internet des objets) font que « l'Afrique se trouve à la croisée des chemins et doit prendre en main son cyber destin » pour que selon vos propos, **Monsieur le Président de la République**, après avoir raté la révolution industrielle, elle réussisse la révolution numérique.

Je vous remercie.