

CONTRIBUTION CITOYENNE

# 10 ARTICLES

SUR LES TECHNOLOGIES NUMERIQUES

ASSANE SY

CYBERJURISTE-CONSULTANT |  
SPECIALISTE EN DROIT NUMERIQUE

## SOMMAIRE

# 1

Les services financiers numeriques: nouvelle  
cible des cyberattaques au senegal

# 2

Comment protéger la propriété intellectuelle  
des actifs lies au technologie de  
l'information

# 3

Jeunesse et internet : quand les reseaux  
sociaux participent a la degradations des  
moeurs au senegal

# 4

La protection des mineurs en ligne: un enjeu  
important pour les parents

# 5

Internet et vie privee : comment devons nous  
comporter dans le monde virtuel

## SOMMAIRE

### 6

tentatives de piratage à l'ère de la pandémie :  
attention aux hameçonnages sur les réseaux  
sociaux

### 7

Pour une réforme du cadre juridique de la  
protection des données personnelles au  
Sénégal

### 8

l'usage abusif des réseaux sociaux au Sénégal :  
la recrudescence du nombre de victimes chez  
les jeunes inquiète la population

### 9

Les services financiers numériques : socle de  
l'inclusion financière en Afrique de l'Ouest

### 10

Internet et mode de vie : 10 bonnes pratiques  
à adopter dans le cyberspace

ARTICLE 1

# Les services financiers numériques: nouvelles cibles des cyberattaques au Sénégal

ASSANE SY





Les services financiers numériques sont de plus en plus victimes d'actes cybercriminels. Les Cyber délits dans ce secteur vont sans aucun doute s'accroître. L'actualité dans notre pays et même dans le continent vient conforter ces propos.

Ces derniers temps, le Sénégal est devenu la cible de malfaiteurs qui utilisent les nouvelles technologies comme support pour perpétrer leurs infractions. L'actualité de cette semaine concernant le démantèlement d'un réseau de cybercriminels qui tentaient de s'introduire dans le système informatique du célèbre opérateur de télécommunications vient mettre en lumière un phénomène en progression au Sénégal. Aujourd'hui et de plus en plus, des personnes malintentionnées s'introduisent où tentent de s'introduire dans les systèmes informatiques de nos organisations publiques comme privées.

Le développement de ce fléau est inquiétant. L'Etat, les entreprises et la population peuvent tous être de potentielles victimes de ces infractions. Cependant, le secteur privilégié des cybercriminels reste celui des services financiers numériques.

L'utilisation des technologies de l'information dans les activités des services financiers numériques attire de nouveaux prédateurs animés par l'appât du gain. Profitant de failles techniques ou humaines, les cybercriminels utilisent des techniques variées pour tenter d'accéder au SI de ces structures. Ce qui peut parfois avoir de lourdes conséquences pour la structure victime. En guise d'exemple, l'opérateur Orange, à travers la filiale ORANGE FINANCE MOBILE SENEGAL (OFMS) a été victime récemment d'une cyberattaque orchestrée par un groupe de jeunes Nigériens qui logeaient à Ouakam. Cette action leur a permis de soutirer un montant de presque 1 milliard de FCFA via le service de mobile Money[1] (Orange Money). Finalement, ces cybers délinquants ont été arrêtés par la brigade de recherche de la gendarmerie nationale (section ouakam).

## ARTICLE 1

Cette situation de plus en plus récurrente dans notre pays alarme les services financiers numériques. Il devient donc urgent pour ces derniers de renforcer leurs dispositifs de sécurité pour préserver l'intégrité et la fiabilité de leurs systèmes.

Au Sénégal, les structures n'ont pas toujours l'expertise pour faire face aux cyberattaques. Dans mes prochains articles, je présenterai les dispositifs techniques, organisationnels et juridiques pour réagir et limiter les impacts des attaques informatiques.



ARTICLE 2

Comment protéger la  
propriété intellectuelle  
des actifs liés aux  
technologies de  
l'information ?

ASSANE SY

L'ère dans laquelle nous vivons, également appelée l'ère des technologies de l'information, de la révolution digitale, ou de l'industrie 4.0, a entraîné de profondes transformations dans nos sociétés. Grâce aux avancées dans le domaine des technologies de l'information, les technologies numériques sont de plus en plus utilisées par les particuliers, dans les administrations et dans les entreprises du monde entier. Cette situation a entraîné une forte hausse des demandes de solutions informatiques au niveau mondial. Des entreprises (entreprises de services du numérique, startups, éditeurs de logiciels, etc..) ont su profiter de cette forte demande pour proposer des solutions technologiques, numériques toujours plus innovantes pour répondre aux besoins des utilisateurs. Nous assistons à une véritable bataille d'innovations technologiques. Cependant, la question qui préoccupe bon nombre de ces entreprises et qui nous est souvent posée par nos clients dans le domaine des TI est la suivante : **Comment pouvons-nous protéger la propriété intellectuelle de nos solutions (actifs) informatiques ?**

Dans ce papier, nous apportons quelques précisions sur les différents moyens de protection de la propriété intellectuelle à la disposition des entrepreneurs du numérique.

### **La genèse de la propriété intellectuelle :**

La protection de la propriété intellectuelle a toujours préoccupé les innovateurs et créateurs. A titre de rappel, les œuvres humaines (créations) faisaient souvent l'objet de polémiques, de controverses. Parfois même, l'identification des auteurs de certaines œuvres humaines était assez difficile. La création ou l'innovation était alors une affaire ouverte, appartenant à tous. Cette situation plus ou moins anarchique était due à l'absence de mécanismes de protection juridique visant à protéger les œuvres humaines. Durant la révolution industrielle et avec l'avènement de nouveaux produits et innovations, il a été jugé nécessaire de mettre en place des mécanismes de protection des différentes inventions de l'Homme. C'est dans ce contexte qu'est apparue la notion de propriété intellectuelle.

Cette expression regroupe l'ensemble des créations issues de l'esprit humain (grâce à son intelligence et sa faculté d'imagination). Elle touche plusieurs domaines : œuvres littéraires, œuvres artistiques, marques, inventions, etc. La propriété intellectuelle comporte deux branches : La propriété littéraire et artistique et la propriété industrielle. Il est important de distinguer la propriété littéraire et artistique (les droits d'auteurs et droits connexes) de la propriété industrielle (marques, brevets, licences, etc.). L'objectif de la propriété intellectuelle est de protéger légalement les productions humaines, tout en conférant un droit d'exclusivité aux titulaires de ces œuvres.

### **Pourquoi est-il important de protéger la propriété intellectuelle des actifs informatiques ?**

Dans cet environnement marqué par la révolution numérique, l'objectif premier de la propriété intellectuelle semble menacé. Avec l'essor du numérique favorisant le développement du partage de l'information, l'accès aux œuvres numériques a été grandement facilité. Il devient dès lors simple de modifier, réutiliser ou encore copier un produit (une solution informatique) de manière illégale.

L'importance de la protection de la propriété intellectuelle des actifs informatiques est qu'elle permet aux entreprises numériques de réduire leur manque à gagner. En effet, l'utilisation frauduleuse de solutions informatiques occasionne d'importantes pertes financières pour les entreprises numériques. De plus, la protection de la propriété intellectuelle des actifs informatiques donne à ces entreprises les moyens de pouvoir s'imposer en toute légitimité sur le marché national et international. La protection de la propriété intellectuelle des actifs informatiques permet d'encadrer d'une certaine manière la concurrence. Elle permet aussi aux entreprises numériques d'être plus productives et favorise une augmentation des investissements liés à l'innovation technologique.

Compte tenu de l'importance de la protection de la propriété intellectuelle des actifs informatiques, les acteurs (juristes, chefs d'entreprises, etc.) s'intéressent de plus en plus à comment assurer efficacement cette protection ?

### **Comment protéger la propriété intellectuelle des actifs informatiques ?**

La propriété intellectuelle des actifs informatiques touche principalement aux produits ou solutions informatiques déployés par les entreprises. Ces actifs informatiques peuvent être constitués de logiciels, d'applications, de sites internet et de toutes autres innovations technologiques.

### **Quels sont les moyens disponibles pour protéger les actifs informatiques ?**

#### **La protection par brevet logiciel :**

Les logiciels conçus sur la base d'un ensemble de programmes (de code informatique) constituent des œuvres humaines nécessaires au fonctionnement des ordinateurs. A titre de rappel, la convention de Berne de 1886 sur la protection des œuvres littéraires et des droits d'auteur a défini l'œuvre (littéraire et artistique) comme toute production du domaine littéraire, scientifique ou artistique quel qu'en soit le mode ou la forme d'expression (article 2 de la convention). Dès lors cette définition globale de l'œuvre humaine concerne aussi le logiciel. Cet actif informatique est aujourd'hui protégé par un brevet qui n'est rien d'autre qu'un droit exclusif conféré sur une invention. Ce droit permet de protéger l'invention technique du logiciel, mais à certaines conditions :

Le logiciel doit être destiné à une utilisation industrielle

Le logiciel doit être nouveau et ne doit faire l'objet d'aucune publication antérieure

Le logiciel doit impliquer une activité inventive.

Le regroupement de ces trois conditions permet à un logiciel d'être brevetable. Aujourd'hui, nonobstant l'importance des brevets dans la protection des logiciels, la question de la territorialité pose quelques soucis aux acteurs car le brevet est un droit territorial et n'est applicable qu'au pays qui l'a délivré.

**La protection des innovations technologiques : applications, sites web, base de données, etc.**

Le développement des technologies numériques a occasionné une multiplication des applications mobiles et web. Ces applications reposent sur des codes sources et disposent d'interfaces graphiques (qui nécessitent d'être protégés). Concernant la protection du « code source » de l'application, le propriétaire de la solution peut utiliser un brevet d'invention reconnu par les normes internationales de la propriété intellectuelle. En ce sens, l'obtention de ce brevet lui permettra d'avoir l'exclusivité sur l'application. Il pourra ainsi vendre, utiliser ou encore mettre à la disposition du public ces innovations technologiques. La protection par un brevet peut être utilisée aussi dans le cadre de l'interface graphique de l'application. Pour ce faire, cette interface doit revêtir d'un caractère original et spécifique à l'entreprise. Par exemple, les interfaces graphiques de SAMSUNG ou de Microsoft permettent d'identifier directement ces entreprises. Ainsi, la protection que ces entreprises vont bénéficier empêche toute reproduction de leurs interfaces graphiques

L'entreprise qui crée une solution informatique (application mobile ou web) peut aussi revendiquer un droit d'auteur. Cette protection confère à l'auteur de la solution des droits patrimoniaux et légitimes sur l'application.

La protection des actifs informatiques peut aussi porter sur les bases de données des entreprises. Ainsi, l'architecture de la base de données peut être protégée par droit d'auteur conféré au propriétaire de la base. Pour ce faire, le propriétaire doit justifier l'originalité de cette base. Pour protéger le contenu de la base de données, les entreprises informatiques peuvent aussi faire appel au droit sui generis.



**La protection des marques informatiques de commerce :**

Les entreprises informatiques proposent de plus en plus des solutions technologiques généralement associées à une marque qui doit être impérativement protégée. En principe, la marque est un signe spécifique qui indique que tel produit ou service est fourni par telle personne ou telle entreprise. Elle permet aux entreprises de bénéficier de visibilité sur le marché tout en tirant profit du produit. Généralement, la marque est protégée par un enregistrement, symbolisé par le sigle ®. Ce symbole qui signifie « Registered » en anglais justifie que la marque a été enregistrée au niveau de l'organe compétent en la matière.

Les moyens disponibles pour protéger la propriété intellectuelle des actifs informatiques sont nombreux. Nous avons délibérément décidé de nous concentrer sur les mécanismes présentés plus haut puisqu'ils apportent un bon niveau de protection.

Compte tenu du nombre important d'entreprises au Sénégal qui développent et commercialisent des solutions informatiques, notre prochain article portera sur les démarches à suivre au niveau du Sénégal pour protéger les actifs informatiques en application de la législation en matière de propriété intellectuelle.





ARTICLE 3

Jeunesse et Internet :  
quand les réseaux sociaux  
participent à la  
dégradation des mœurs au  
Sénégal

ASSANE SY

L'utilisation tendancieuse des réseaux sociaux chez les jeunes au Sénégal inquiète de plus en plus la population. Avec cette explosion significative des médias sociaux, les jeunes considèrent souvent ces plateformes comme un lieu public pour divulguer des contenus indésirables, voire même obscènes. Ainsi, cet espace virtuel est devenu l'agora de cette couche sociale addictive aux innovations technologiques. Cette situation très accablante participe à la dégradation des mœurs et incite les jeunes à promouvoir la médiocrité dans les réseaux sociaux. Alors, qui sont les responsables de cette situation ? Quelles sont les raisons qui expliquent cette situation ? Comment les réseaux sociaux participent-ils à la dégradation des bonnes mœurs au Sénégal ? À travers cet article, nous essayerons de répondre à ces questions qui inquiètent de plus en plus les sénégalais

Le développement des nouvelles technologies de l'information et de la communication continue d'impacter tous les secteurs de la vie. L'utilisation de l'internet devient de plus en plus incontournable pour la société. Ainsi, depuis quelque temps, nous constatons que le nombre d'internautes dans le monde a connu une évolution significative. Au Sénégal, cette évolution se justifie par des chiffres plus ou moins alarmants. Sur une population de 16.52 millions d'habitants, 10 millions sont des internautes et 3.5 millions sont actifs sur les réseaux sociaux .

### **Quelles sont les raisons qui expliquent cette situation ?**

Cette situation qui devient de plus en plus inquiétante pour la société est d'une part due à l'utilisation des réseaux sociaux. Cet espace virtuel de communication est devenu le point de convergence de milliers de Sénégalais, particulièrement des jeunes. Depuis l'explosion des plateformes de médias sociaux dans le monde, surtout avec la libération de Facebook en 2004, l'utilisation des réseaux sociaux est devenue de plus en plus de la mode chez les jeunes. La multiplication incessante des médias sociaux occasionne des choix divers et variés pour les utilisateurs. S'il en existe des dizaines de réseaux sociaux dans le monde, les plateformes les plus utilisés au Sénégal sont entre autres Facebook, Whatsapp, Snapchat, LinkedIn, Twitter et récemment Tik Tok. ainsi, si chacun d'entre eux présente sa particularité, leur point commun réside sur le fait que l'utilisateur du réseau fournit ses données personnelles de manière volontaire ou involontaire.

Dès lors, le fonctionnement des réseaux engendre des conséquences désastreuses particulièrement chez les jeunes qui sont devenus de plus en plus addictifs. Parmi les multiples impacts que peuvent occasionner ces réseaux sociaux, la déperdition des valeurs sociales est la plus illustrative au Sénégal.

### **Comment ces réseaux sociaux participent-ils à la dégradation des bonnes mœurs au Sénégal ?**

Tous les jours, des contenus obscènes, choquants ou contraires aux bonnes mœurs transitent sur les différents réseaux sociaux précités. Les jeunes exposent quotidiennement leur vie privée sur les réseaux sociaux à travers la publication de photos, vidéos ou encore des messages sous format audio. Si certains d'entre eux ignorent les conséquences qui peuvent en découler de cette situation, d'autres en vont plus loin, jusqu'à même faire des médias sociaux un outil de concurrence de la mode ou encore de promotion de la médiocrité au Sénégal.

À ce titre s'ajoute le phénomène du « Buzz » que convoitent certains jeunes ou encore la recherche de profit sur les rémunérations que proposent certains réseaux sociaux tels que Snapchat ou Tik Tok, en échange des données personnelles des utilisateurs. L'analyse des comportements, les émoticônes et le principe des "stories" proposé par ces réseaux leur permettent de maîtriser sur toute la ligne la vie privée des utilisateurs. Ainsi, l'absence de culture numérique, le faible niveau d'alphabétisation et le niveau d'inconscience notée chez les jeunes participent de plus en plus à la dégradation de cette couche sociale. Toutefois, malgré le nombre fabuleux de victimes observé ces temps si dans le cyberspace, ces jeunes continuent de prêter une oreille sourde aux dérives qui sont présentes sur les réseaux sociaux. Ils développent ainsi des comportements désastreux et abominables pour la société, et font intervenir plusieurs responsabilités.

### **Alors, qui sont les responsables de cette situation ?**

Aujourd'hui, nonobstant le contrôle et la veille parentale sur les jeunes, cette couche sociale utilise des techniques qui leur permettent d'exploiter les réseaux sociaux, même en présence de leur entourage. Cette situation très bouleversante se justifie du fait que les jeunes sont devenus de plus en plus familiers avec les réseaux sociaux et s'adaptent plus rapidement à ces innovations technologiques. Ce conflit de génération dans le domaine du numérique a fait que la majeure partie des parents sont dépassés par cette évolution technologique. De même, les concepteurs de ces réseaux sociaux facilitent l'utilisation des plateformes à toutes les couches sociales et ne s'intéressent pas souvent sur l'âge de l'utilisateur, ce qui est déplorable.

Alors face à ce phénomène très alarmant, les gens s'intéressent très souvent sur l'avenir de la jeunesse sur les réseaux sociaux. Si certains d'entre eux avancent la question de la protection de la vie privée sur les réseaux sociaux, d'autres soulèvent la responsabilité des différents acteurs de l'écosystème. Ainsi, compte tenu de la situation attendrissante des jeunes sur la toile au Sénégal, nous développerons dans nos prochains articles les bonnes pratiques (techniques, juridiques, habitudes) à adopter sur internet en général et sur les réseaux sociaux en particulier.



A young girl with dark braids is looking down at a tablet computer she is holding. She is wearing a white sweater with yellow star patterns. In the background, another child is blurred, suggesting a classroom or school setting.

ARTICLE 4

La protection des mineurs  
en ligne: un enjeu  
important pour les  
parents

ASSANE SY

**L'utilisation des nouvelles technologies par les mineurs devient de plus en plus inquiétante pour la société. Avec les multiples risques qui sont présents dans le cyberspace, cette couche sociale très vulnérable est souvent exposée à des dangers qu'ils ne maîtrisent pas assez. Avec ce nombre pléthorique de plateformes de médias sociaux et de la facilité d'utilisation d'internet, nous constatons une montée exponentielle de la présence des mineurs en ligne. En ce sens, divers facteurs peuvent expliquer cette situation qui est souvent considéré comme un inconvénient majeur pour la société.**

L'utilisation des nouvelles technologies devient de plus en plus inéluctable pour la société. Considéré comme la révolution la plus importante pour l'humanité, le numérique en général et l'internet en particulier reste à ce jour un village planétaire qui regroupe des milliers de personnes d'origines différentes.

Ainsi, compte tenu des réalités sociales et de l'importance qu'occupe ce réseau dans notre quotidien, il paraît difficile voire même impossible de se désintéresser à cette révolution digitale. Son utilisation peut être différente et dépend le plus souvent des objectifs visés par l'utilisateur. En effet, si certaines personnes exploitent l'internet à des fins purement professionnelles, d'autres internautes profitent du contenu social, éducatif ou même divertissant. Alors, ce monde virtuel s'agrandit de jour en jour et enregistre des nouveaux entrants continuellement.

### **Une explosion du nombre d'internautes dans le monde ;**

Selon le rapport de We are social de 2019, les chiffres relatifs à l'utilisation d'internet en général et des médias sociaux en particulier sont devenus alarmants. Sur les 7.676 Milliards de personnes dans le monde, 4.388 milliards d'entre eux de sexes et d'âges différents sont des internautes et 3.484 milliards sont actifs sur les médias sociaux.

Au Sénégal, le nombre d'internautes continue d'évoluer exponentiellement. Sur une population de 16.52 Millions d'habitants, 9.75 Millions utilisent ce réseau et 3.50 Millions d'entre eux sont actifs sur les médias sociaux. Parmi cet important nombre d'utilisateurs figure une couche sociale sensible et très vulnérable aux risques présents sur la toile. Cette catégorie de personnes dite mineur dans le jargon juridique a été bien définie en droit sénégalais. Ainsi, selon l'article 276 du code de la famille, sont mineures les personnes de l'un ou de l'autre sexe qui n'ont pas encore l'âge de 18 ans accomplis. Leur présence en ligne suscitent des débats et poussent beaucoup de pays à s'intéresser davantage sur la question de leur protection.

### **Les causes de la présence des mineurs en ligne sont nombreuses ;**

Nonobstant l'ouverture de la toile à toutes les couches sociales, la présence des mineurs en ligne n'est guère enthousiasmante au Sénégal. Cette situation assommante est souvent due à plusieurs raisons. Toutefois, si une partie de la population fustige l'accessibilité et la facilité d'utiliser internet et les réseaux sociaux, d'autres préfèrent soulever la question de la pluralité des plateformes de médias sociaux qui ne cessent de s'accroître. Face à ses multiples motifs qui gravitent autour de la situation, les parents continuent de démontrer leurs incapacités à veiller et à contrôler les activités de leurs enfants en ligne. Cette absence de contrôle parental peut être justifiée d'une part par un manque de culture numérique observé chez certains parents. D'autre part les contraintes de temps occasionnées par les activités professionnelles fait que certains d'entre eux s'intéressent rarement sur la présence de ces mineurs en ligne.



**Les conséquences qui peuvent découler de cette situation sont énormes ;**

Cette situation qui est pour la plus part aggravante peut avoir des conséquences majeures sur le mineur. Avec les risques énormes qui sont présents sur la toile, cette couche sociale peut souvent être exposée à des dangers exorbitants tels que le cyber harcèlement (menaces et chantages), les images à caractère sensible ou sexuel (pédopornographie) ou encore le détournement de leurs données personnelles à des fins commerciales sans le moindre consentement. À ce titre, s'ajoute l'absence de mécanisme consistant à filtrer l'âge des usagers sur la majeure partie des médias sociaux. Les responsables de traitement de ces plateformes collectent en masse les données des personnes qui utilisent leurs services, y compris celles des mineurs.

Au Sénégal, les efforts consentis par le législateur national en matière de protection des mineurs en ligne ne sont pas assez fabuleux. **La loi n° 2008-12 du 25 janvier 2008** sur la protection des données à caractère personnel réserve un traitement plus ou moins faible pour cette catégorie sociale. Les dispositifs normatifs ne sont pas à la hauteur des attentes, surtout dans un contexte marqué par l'addiction des mineurs à ces innovations technologiques. Ainsi, sur la base de ce constat, des solutions devront être préconisées pour pallier les risques que guettent les mineurs sur leur présence en ligne

**Quelques recommandations visant à remédier à ce fléau ; Pour faire face à cette situation, plusieurs mécanismes peuvent être engagés par les différents acteurs de l'écosystème :**

· D'abord, la sensibilisation semble être la clé de voute pour amoindrir les dangers qui ne cessent de se multiplier dans le cyberespace. Toutes les parties prenantes de l'écosystème doivent unir leurs forces pour fomentier et assister les mineurs à être beaucoup plus prudents sur la toile. Ainsi, l'insertion de programmes de sensibilisation dans les écoles pourrait considérablement réduire la propagation de ce fléau.

· Du côté des parents, ils doivent renforcer leurs responsabilités pour assurer la mission de contrôle parentale sur leurs enfants mineurs. À cet effet, les mécanismes techniques (filtrage de certains sites, limité les heures de connexions) pourraient être des solutions adaptées pour remédier à ce phénomène.

Enfin, le cadre juridique de protection des mineurs sur internet doit être renforcé afin de garantir un niveau de sécurité beaucoup plus élevé à ces derniers. Pour ce faire, le législateur national devra dorénavant introduire de nouvelles dispositions dans le corpus juridique interne, comme à l'image de l'Europe avec le nouveau règlement (RGPD) qui oblige une protection spécifique des mineurs. Dès lors, compte tenu de son état d'imaturité et de ses incapacités intellectuelles et physiques, le mineur doit nécessairement bénéficier d'une protection optimale contre les différentes menaces qui pourraient impacter négativement sa vie. En ce sens, les risques fréquents présents dans le cyberespace ne sont pas laissés en rade, vu que les enfants sont devenus de plus en plus addictifs aux nouvelles technologies.



ARTICLE 5

Internet et vie privée :  
comment devons nous  
comporter dans le monde  
virtuel

ASSANE SY

Chaque jour, nous interagissons avec pas mal de personnes dans un monde totalement virtuel. Considéré comme un moyen de communication pour échanger des données entre utilisateurs, Internet constitue un village planétaire ouvert et accessible à toutes les couches sociales. Ainsi, faisant partie intégrante de notre vie quotidienne, ce vaste réseau présente des enjeux multidimensionnels et occasionne un nouveau conflit d'intérêts partout à travers le monde. Dès lors, notre présence en ligne n'est pas dépourvue de risques dans la mesure où nous fournissons quotidiennement des informations relatives à notre vie privée. Cette situation très favorable aux dangers présente dans le cyberspace nécessite l'adoption de nouvelles habitudes pour minimiser les atteintes relatives à notre vie privée. Ces bonnes pratiques à embrasser peuvent être ressenties sur plusieurs niveaux :

**Du point de vue technique, nous devons dorénavant être beaucoup plus prudents :**

Aujourd'hui, il faut admettre que certaines entreprises sont en perpétuelle quête de données personnelles. Les informations relatives à notre vie privée ont une valeur commerciale, voire même politique. Ainsi, dans le cadre de l'exercice de nos activités, nous utilisons des plateformes de recherches (navigateurs) ou encore des plateformes de médias sociaux (Réseaux sociaux) pour faciliter notre communication. Dès lors, même si en théorie nous sommes seuls devant un écran, il faut en priori se détromper de la conception qu'internet est un monde virtuel. Toutes nos répercussions sur la toile ont un rapport direct avec notre vie privée. Ces nuages d'informations que nous fournissons en ligne sont souvent exploités par des géants du net, ou encore par des personnes mal intentionnées.

À cet effet, il semble être une nécessité pour tous utilisateurs d'adopter de bonnes pratiques en ligne pour amoindrir les risques omniprésents dans le cyberspace. Du point de vue technique, les utilisateurs devront dorénavant être beaucoup diligents sur les applications qu'ils installent directement sur leurs appareils. Certaines applications peuvent être conçues par des personnes mal intentionnées pour usurper vos données personnelles. Pour la plupart des cas, les cybercriminels utilisent techniques de « clown » pour produire des applications similaires à celles authentiques. Ils introduisent des programmes malveillants (virus) pour récupérer vos données, avoir le contrôle de vos appareils ou même modifier vos données. À cet effet, l'utilisateur doit vérifier la source et l'authentification des applications. Par exemple, il est fortement recommandé d'installer des applications via Play store pour le système « Android » ou encore Apple Store pour ceux qui utilisent le système « IOS ».

Parfois, notre présence en ligne occasionne la réception de mails malveillants ou encore de liens qui peuvent nous rediriger vers d'autres sites suspects. Toutefois, le simple fait de cliquer sur des liens dont nous ignorons la provenance peut nous induire à des erreurs irréparables. Les cybercriminels se cachent souvent derrière ces techniques pour porter atteintes à la vie privée des utilisateurs, d'où l'importance de bien vérifier les sources. La création d'un mot de passe très solide et le facteur de la double authentification ainsi que l'utilisation des navigateurs légalement reconnus permet aussi de réduire considérablement les risques qui nous guettent sur la toile.

## Quels doivent être nos agissements en ligne ?

Internet est un monde à part entier, ouvert et accessible à toutes les couches sociales. Ainsi, il est important de comprendre que pour la majeure partie des cyberattaques, l'individu a toujours été la cible des malfaiteurs. Les cybercriminels analysent continuellement notre comportement en ligne pour pouvoir définir leur plan d'attaque. Compte tenu de cette situation, nous devons toujours nous comporter en « bon père de famille » dans le monde numérique pour minimiser les risques. Les sites que nous visitons ainsi que notre historique sur la toile peut en dire trop sur notre identité, raison pour laquelle nous devons avoir un objectif bien déterminé lorsque nous sommes en ligne. Il est préférable pour tous utilisateurs de définir son plan de navigation ainsi que ses heures de connexion. En effet, toujours dans ce même sillage, la logique voudrait à ce que nous soyons plus vigilants, prudents et avisés, surtout concernant le contenu que nous visualisons en ligne. Aujourd'hui, ce que beaucoup d'entre nous ignore est que nonobstant l'anonymisation ou le pseudo que nous utilisons en ligne, le monde numérique est le reflet du monde réel.

Derrière chaque identifiant se cache une personne physique d'où l'importance de développer en soi de bonnes pratiques. Toujours dans cette optique, il y est d'un grand intérêt pour les internautes de restreindre leur cercle d'amis, surtout ceux qui utilisent les médias sociaux, dans le but d'avoir une maîtrise des personnes avec qui l'on communique en ligne. Cette restriction du périmètre des « amis virtuels » pourrait être aussi ressentie au niveau des publications (textes, audio, photos, etc.) à un point que des contenus indésirables qui pourraient nuire votre réputation ne transitent pas dans les réseaux. Si actuellement certaines personnes se sentent menacé ou gêné par des publications obscènes, c'est parce qu'elles n'avaient pas pu mesurer les conséquences qui peuvent découler d'une mauvaise utilisation des outils technologiques. Toutefois, compte tenu des nombreuses victimes observées ces derniers temps si dans la toile, nous devons ainsi utiliser le numérique en bon escient et contrôler avec assiduité notre présence en ligne.

**Enfin, nous devons nous familiariser avec le cadre juridique existant:**

La virtualité de l'Internet ne signifie pas que ce monde est dépourvu de réglementation. En effet, il existe un ensemble de dispositifs juridique composé d'un cadre normatif et institutionnel visant à assurer cette réglementation sur la toile. Depuis 2008, notre pays s'est doté d'un arsenal juridique de taille. Il s'agit bien évidemment de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données personnelle. Dans son article premier, l'objet de cette loi s'affiche clair et net. Elle a pour vocation de mettre en place un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel. Sur cette même lancée, cette loi veille à ce que les Technologies de l'Information et de la Communication (TIC) ne portent pas atteintes aux libertés individuelles ou publiques, notamment à la vie privée ». (cf. article 1 de la loi de 2008-12 du 25 janvier 2008).

Fort de ce constat, il n'est plus à prouver l'existence du cadre juridique de la protection des vies privées au Sénégal. Ainsi, les internautes ne doivent pas ignorer l'importance d'une telle disposition juridique qui vise à garantir notre sécurité face aux nouvelles formes d'attaques. En plus de cette loi, nous avons la commission de protection des données personnelles (CDP) au Sénégal. Cette autorité administrative indépendante a pour mission d'assister la population sur la protection de leurs données personnelles. Elle veille à ce que les traitements de données personnelles soient conformes avec la législation en vigueur. Elle collabore étroitement avec la population et accompagne toute personne qui manifeste une menace sur la confidentialité, l'intégrité, ou la disponibilité de ses données personnelles. En ce sens, nous devons ainsi avoir le réflexe de saisir cette commission lorsque notre vie privée semble être menacée. Cette collaboration permettra de réduire considérablement les risques qui pèsent sur notre vie privée lors de notre interaction avec monde virtuel.

Néanmoins, nous savons tous que le risque zéro n'existe pas dans le monde virtuel du fait que le facteur humain sera toujours impliqué dans ce sphère, mais l'adoption de certaines bonnes pratique en ligne pourra réduire les atteintes relatives à notre privée. Ainsi, chacun doit prendre sa sécurité à main, surtout dans un contexte marqué par une évolution exponentielle de la technologie et de l'immersion de nouvelles plateformes de communication virtuelles.



ARTICLE 6

Tentatives de piratage à  
l'ère de la pandémie :  
attention aux  
hameçonnages sur les  
réseaux sociaux

**À l'heure de cette pandémie du Covid-19, des personnes malveillantes profitent de la situation pour porter atteinte à la vie privée des internautes. Des tentatives de Phishing sont devenues de plus en plus recrudescences, surtout avec la diffusion ou le partage de messages indésirables via les réseaux sociaux. Pour rappel, cette criminalité informatique n'est guère une pratique nouvelle mais la réapparition de ce fléau est devenue trop inquiétante, d'où la nécessité d'adopter de nouveaux comportements.**

**Quelle méthode utilisent les hackers pour procéder aux hameçonnages via les réseaux sociaux ?**

Ces derniers temps, les réseaux sociaux sont devenus la cible préférée des hackers pour procéder à des cyberattaques. Ainsi, avec le phénomène du coronavirus, ces personnes malveillantes ont multiplié les tentatives de piratage à travers des messages qui transitent sur les plateformes de communication électronique.

Par des vagues de fausses informations faisant allusion à une promotion ou offre de crédit gratuit, les cybercriminels introduisent des liens malveillants sur les messages qui circulent sur la toile. Plus loin, d'autres cyberattaquants semblent être plus formels en proposant de la connexion gratuite à travers des messages que les utilisateurs partagent via WhatsApp par exemple, sous prétexte que la contrepartie fictive (volume de giga) pourra leur permettre de rester chez eux, surtout en cette période de pandémie, ce qui est contraire à la réalité. Cette pratique, communément appelée « hameçonnage » ou « phishing » dans le jargon de la cybercriminalité permet aux hackers d'effectuer une usurpation d'identité afin d'obtenir des informations confidentielles pour en faire un usage criminel. Pour la plupart, les cybercriminels se font passer pour des entreprises publiques, des banques ou même des opérateurs de téléphonie pour proposer de fausses offres qui visent à attirer les utilisateurs.

Dans le cadre des réseaux sociaux, le pirate procède à la diffusion de faux message contenant un programme malveillant ou malicieux et invite les utilisateurs à cliquer sur le lien ou à transférer le message. Ainsi, l'ouverture de ces liens frauduleux permet aux cybercriminels d'avoir à leur disposition des informations personnelles (données personnelles, mot de passe, identifiants, données bancaires etc.) qu'ils pourront utiliser à leur guise. Ce fléau dans le domaine numérique continue de s'élargir et facilite le développement des cyberattaques en ligne.

**Comment réagir face à une tentative d'hameçonnage sur les réseaux sociaux ?**

Les bons comportements en ligne permettent de réduire considérablement les risques qui sont omniprésents dans le cyberspace. Pour éviter d'être une proie des hackers, il est impératif pour tout utilisateur des médias sociaux d'être plus vigilant et prudent que possible.

Ainsi, si vous êtes par hasard le destinataire de ce type de message via les réseaux sociaux, le premier réflexe que vous devez avoir c'est de ne pas cliquer sur le lien qui se trouve sur le texte (le lien est souvent écrit en bleu). Le simple fait d'ouvrir le lien peut permettre au cybercriminel de réussir son opération de pêche car l'utilisateur est automatiquement redirigé vers un site frauduleux. A cet effet, il est fortement recommandé de supprimer le message pour ne pas faciliter au pirate la réussite de son action. Des fois, toujours dans cette mouvance de piratage, le cybercriminel peut solliciter le partage en masse (avec vos contacts) du message pour pouvoir élargir ses cibles et avoir le maximum de proie possible.

Cependant, pour ne pas participer à la réalisation de cette pratique cybercriminelle, l'utilisateur doit éviter de faire passer le message reçu avec ses contacts ou dans les groupes de discussion.

La majeure partie des gens qui utilisent les médias sociaux n'ont pas une culture numérique solide et n'hésiteront pas à cliquer sur n'importe quel message, ce qui peut être fatal dans certains cas de figure. Aussi, le fait de ne pas fournir ses informations personnelles sur les plateformes ou onglets qui s'ouvrent lors d'un clic sur un lien frauduleux fait partie des bons réflexes à adopter lors d'un piratage par hameçonnage. Toutefois, si par accident vous avez mordu à l'hameçon du hacker, pensez automatiquement à déconnecter votre appareil ainsi que tous les comptes qui s'y trouvent et changer les identifiants et les mots de passe. De plus, l'utilisateur doit scanner son appareil pour pouvoir s'assurer de la sécurité. Bref, le phishing est une pratique assez courante qui touche pas mal de personnes, surtout dans le contexte actuel. À ce titre, il est important de maîtriser les méthodes qu'utilisent les cybercriminels pour pouvoir s'en prémunir et agir de manière responsable.



ARTICLE 7

Pour une réforme du  
cadre juridique de la  
protection des données  
personnelles au Sénégal

ASSANE SY



La révolution numérique a impacté tous les secteurs de la vie. Chaque jour, nos agissements, dans ce monde hyperconnecté facilitent et favorisent le traitement des informations associées à notre identité. Les données personnelles permettant d'identifier directement ou indirectement une personne physique sont aujourd'hui très convoitées par plusieurs acteurs. Donc, compte tenu de l'importance de ces informations, la notion de protection des données personnelles devient alors une obligation. Ainsi, c'est dans ce contexte que s'inscrit l'article 12 de la Déclaration universelle des droits de l'homme de 1948 qui dispose 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. »

### Etat des lieux du cadre juridique de la protection des données personnelles au Sénégal.

Actuellement, dans un souci de mieux protéger la vie privée des citoyens surtout dans un contexte marqué par le traitement en masse de données personnelles, tous les états au monde ont élaboré des mécanismes juridiques relatifs à la protection des données personnelle. Au niveau du continent africain, des pays comme le Sénégal ont bien saisi l'importance de la mise en place d'un tel dispositif de protection. D'ailleurs, c'est dans ce contexte que le législateur national a initié depuis 2008 un cadre juridique visant à assurer la protection des données des personnes. Il s'agit d'une part de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel. Cette disposition juridique a pour objectif de lutter contre les atteintes à la vie privée des personnes. En effet, ces atteintes peuvent être réalisées lors de la collecte, le traitement, la transmission, le stockage et l'utilisation des données personnelles (cf. art premier de la loi).

Cette loi symbolisant une partie du cadre normatif permet d'encadrer les activités liées au traitement de données personnelles. C'est dans cette logique qu'elle impose aux responsables de traitement (structures publiques comme privées qui traitent des données personnelles) des obligations telles que la confidentialité des données (art 70), la sécurité des données collectées (art 71), la conservation des données (art 72) et enfin l'obligation de pérennité des données (art 74). De même, les personnes faisant l'objet de traitement de donnée personnelle ont des droits garantis par cette même loi. Il s'agit d'abord du droit à l'information (art 58), obligeant au responsable de fournir un certain nombre d'édifications à la personne faisant l'objet de traitement. Tout de même, la personne, objet d'un traitement de donnée personnelle peut manifester un droit d'accès à ses données par écrit ou quel que support que ce soit si cette dernière justifie son identité (art 62). Ainsi, elle peut aussi s'opposer à un quelconque traitement relatif à ses propres données pour des motifs légitimes (art 68).

Enfin, le cadre juridique de la protection des données personnelles garantit aux personnes faisant l'objet de traitement la possibilité de demander au responsable de traitement de rectifier ou de supprimer ses données.

Cependant, hormis l'existence d'un cadre normatif, l'environnement de la protection des données personnelles est aussi caractérisé par un cadre institutionnel qui est assuré par un organe de régulation. Créée depuis le 25 janvier 2008, la commission de protection des données personnelles (CDP) est une autorité administrative indépendante qui a pour mission d'assurer à ce que le traitement des données personnelles soit aux dispositions de la loi. Elle devient ainsi l'autorité compétente en matière de protection des données personnelles au Sénégal. Toutefois, malgré l'encadrement juridique du traitement des données personnelles, nous constatons néanmoins des manquements dans la régulation de ce secteur.

Pour cette raison, il est important de mettre en place de nouveaux mécanismes allant dans le sens de l'actualisation du cadre juridique de la protection des données personnelles au Sénégal.

**L'actualisation du cadre juridique de la protection des données personnelles : une nécessité pour le législateur national.**

Actuellement, la révolution numérique à créer de nouveaux prédateurs de données personnelles partout dans le monde. Des géants du web connu sous l'acronyme du GAFAM (Google, Amazon, Facebook, Apple, Microsoft) considèrent nos données comme une niche d'or a exploité. Cette situation irrépressible constitue ainsi une nouvelle source de menace pour l'atteinte à notre vie privée. À ce titre s'ajoute une évolution exponentielle de la technologie, occasionnant ainsi l'avènement de nouvelles innovations dans le cyberspace qui n'ont pas été pris en compte par la loi de 2008. Par exemple l'intelligence artificielle, l'Internet des objets, ou le big data, pour ne citer que ces nouvelles technologies exploiter par les entreprises à l'absence d'une réglementation spécifique.

Face à cette situation, il semble important voire même cruciale pour le législateur national de procéder à un mis à jour du cadre juridique de la protection des données personnelles. Pour ce faire, de nouvelles dispositions devront être prises pour une adaptation de l'arsenal juridique face l'écosystème numérique. D'une part, la révision du cadre normatif au niveau interne doit nécessairement s'effectuer. Elle permettra au législateur national de constater clairement les insuffisances persistantes dans le corpus juridique national. Tout de même, il pourra introduire de nouvelles dispositions juridiques permettant à l'arsenal juridique de répondre aux réalités du terrain. Ainsi, le renforcement des obligations des responsables de traitements permettra de réduire considérablement les atteintes relatives à la vie privée des personnes. En plus, la consolidation des droits des personnes faisant l'objet d'un traitement de donnée personnelle constitue à ce jour une obligation pour le législateur car elle permet d'instaurer un climat de confiance entre les acteurs concernés.



Au niveau communautaire, l'harmonisation des dispositions juridiques relatives à la protection des données personnelles permettra aussi de réduire la fracture juridique entre les pays de la sous-région. À l'image de l'union européenne avec le RGPD, il serait important de mettre en place une disposition communautaire visant à faciliter la gestion de la question des données personnelles.

D'autre part, l'amélioration du cadre institutionnel de protection des données personnelles doit aussi interpeller le législateur national. Elle peut s'effectuer d'abord par une migration de la commission en Autorité nationale de régulation. Ce changement de statut permettra de renforcer les pouvoirs politiques et financiers de l'organe de régulation. Compte tenu de l'enjeu mondial de la protection des données personnelles, cette initiative participera ainsi à une consolidation de ce cadre institutionnel. L'Autorité de régulation pourra bénéficier aussi d'un pouvoir de sanction, ce qui obligera en toute plénitude aux responsables de traitement de respecter la vie privée des personnes.

En ce moment, au-delà des efforts considérables menés par l'État du Sénégal en matière de protection des données personnelles, des améliorations pourront toujours être avantageuses. Ainsi, nonobstant les ressources parcimonieuses dont dispose la CDP, cette commission continue tant bien que mal d'assurer la mission de régulation en matière de protection des données personnelles en s'appuyant sur les bases de la loi de 2008. Toutefois, même si des axes d'optimisation ont été identifiés sur le cadre juridique, le Sénégal reste quand même une référence en Afrique dans le domaine de la protection des données personnelles. En effet, il fait partie des pays africain signataires de la convention de Malabo de 2014 et est le deuxième pays du continent ayant ratifié la convention 108 depuis 2016.

ARTICLE 8

L'usage abusif des réseaux sociaux au Sénégal : la recrudescence du nombre de victimes chez les jeunes inquiète la population.

L'utilisation des nouvelles technologies au Sénégal et un peu partout dans le monde commence à déceler ses tares dans la société. Ces derniers temps-ci, le nombre de victimes dans le cyberspace a connu une augmentation très inquiétante pour l'opinion publique. L'internet en général et les plateformes de communications électroniques en particulier constituent les principaux supports de commission d'infractions cybercriminelles. Considéré comme une zone de non limite, la toile constitue ainsi un monde virtuel où passe une interconnexion entre plusieurs milliards d'individus. Cette situation présente des risques pour les cyberconsommateurs, notamment les jeunes qui sont devenus très habitués aux technologies numériques.

Au Sénégal, la diffusion de certains contenus inappropriés aux réalités sociales est devenue virale ces derniers moments, suscitant des débats dans toutes les instances. Comment est-on arrivé à ce stade? Pourquoi la jeunesse est la principale victime des dérives sur le cyberspace? Quelles sont les conséquences qui peuvent en découler d'une telle situation? Des solutions sont-elles envisageables pour éradiquer ce fléau? Telles sont les questions qui méritent d'être élucidées au profit de la population pour une meilleure compréhension de la situation.

### **L'explosion des médias sociaux : l'un des facteurs aggravants de la situation.**

La facilité d'utilisation d'internet et l'émergence significative des médias sociaux lors de cette dernière décennie a occasionné des impacts négatifs dans la société. Pour rappel, les plateformes de communications électroniques ne datent pas d'aujourd'hui et ne sont guère nouvelles dans l'écosystème numérique. En effet, depuis les prémices de Facebook en 2004, les médias sociaux ne cessent de s'accroître de manière exponentielle. Aujourd'hui, on en compte plus d'une vingtaine d'applications diverses et variées selon les contenus proposés et la révolution numérique continue de suivre son épilogue. Cette situation a favorisé la multiplication du nombre d'internautes dans le monde. La courbe des cyberconsommateurs suit une logique ascendante faisant ainsi le Web un village planétaire. Ainsi, avec le contexte sanitaire mondial marqué par cette pandémie de covid-19, le nombre d'internautes et d'utilisateurs des médias sociaux a connu une hausse dans le monde et cette situation n'épargne pas le Sénégal.

Compte tenu des mesures édictées par l'Etat dans la lutte contre la propagation du virus en occurrence l'état d'urgence et le couvre-feu, l'usage des médias sociaux était devenu le passe-temps favori de certains Sénégalais. À l'en croire, certains d'entre eux pouvaient passer plus de 6 h de temps avec leurs smartphones pour combler le vide occasionné par la pandémie. Ainsi, cette situation a contribué à la multiplication des dérives sur la toile. Toutefois, même si que les dangers du monde virtuel ne laissent en rade aucun internaute, la jeunesse, cette couche sociale très vulnérable est souvent victime d'une mauvaise utilisation des médias sociaux.

**La jeunesse : principale victime des dérives dans le cyberspace.**

La révolution numérique continue de se disséminer partout dans le monde. Avec le développement des nouvelles technologies, la planète a connu un bouleversement spectaculaire sur tous les plans, permettant ainsi à la population mondiale de revoir leur façon de penser, de faire et de vivre. Les grandes firmes qui s'activent dans le domaine technologique produisent en masse des outils de communication électroniques pour répondre aux besoins de la population. Au bout de quelques décennies, le monde a assisté à un développement pharamineux du nombre de plateforme numérique ouvert et accessible à toutes les couches sociales et évoluant de génération en génération. Sous le coup de l'innovation, cette nouvelle génération, en occurrence la jeunesse est tombée sur des outils de communication électronique très sophistiquées et modernes. La révolution des téléphones mobiles classiques en smartphone a ouvert une nouvelle brèche dans l'écosystème numérique. Ainsi, cette situation a instauré un conflit de génération digitale. Les jeunes sont devenus beaucoup plus familiers avec ces plateformes, ce qui constitue sans doute un risque majeur pour cette couche sociale.

Au Sénégal, l'addiction des jeunes aux médias sociaux se justifie par plusieurs arguments. Par exemple sur un smartphone, les utilisateurs ont souvent tendance à installer plusieurs applications proposant les mêmes contenus ou des contenus différents, ce qui favorise la publication en masse de leurs données personnelles. Cette circonstance qui est le plus souvent adossée un quantum horaire signifiant d'utilisation des médias sociaux contribue d'une part à la multiplication des dérives dans le cyberspace. D'autre part, la question des amis virtuels pose souvent d'énormes problèmes. Dans ce monde virtuel, la confiance numérique constitue un élément très important, ce que beaucoup d'internautes ignorent à ce jour.

### **Mauvais usage des médias sociaux : une situation très déconcertante avec des conséquences déplorables.**

L'utilisation tendancieuse des médias sociaux au Sénégal participe à une dégradation massive des bonnes mœurs surtout chez les jeunes. Depuis quelque temps, on constate que des contenus obscènes ou contraires aux réalités sociales transitent au niveau des plateformes de communication. Les internautes en général et la jeunesse en particulier s'adonnent à des pratiques malencontreuses. Ainsi, le nombre de scandale devient très vite pléthorique et le monde virtuel se présente comme une zone de danger. Pour rappel, Jean Foyer, le rapporteur de la loi informatique et liberté de 1978 avait alerté sur la situation avec l'interrogation suivante : « La civilisation de l'informatique ne va-t-elle pas devenir celle de l'indiscrétion et de l'implacabilité, celle qui n'oublie, ni ne pardonne, qui enfonce le mur de l'intimité, enfonce la règle du secret de la vie privée, déshabille les individus ? ». Aujourd'hui, le temps lui a donné raison. À l'espace de deux mois, des photos et vidéos à caractère pornographique tourné par des adultes sont devenus viraux, poussant ainsi les acteurs judiciaires à saisir et traiter le dossier.

D'ailleurs ce n'est pas tout, fréquemment des publications à caractère injurieux, racial ou confrérique font la une des plateformes de communications électroniques. De l'autre côté, des personnes malintentionnées préfèrent le dénigrement, la diffamation ou encore l'usurpation d'identité pour des raisons diverses et variées. Toutefois, si certains sont victimes d'une culture numérique insuffisante, d'autres sont souvent trahis par des personnes de mauvaise foi, ce qui rejoint en principe la question de la confiance numérique dans le cyberspace. A cela s'ajoute le phénomène du «partage» sur la toile qui participe grandement à la chaîne de victimisation des internautes. Cependant, il ne faut pas perdre de vue que l'utilisation sans modération des médias sociaux participe à la déperdition des valeurs sociales. Pire encore, certains contenus peuvent déstabiliser la cohésion sociale et être la source de conflit, ce qui n'est pas souhaité. Pour ce qui de la vie privée, l'e-réputation des acteurs de telles publications est souvent remis en cause car le problème du droit à l'oubli s'impose généralement sur la toile.

Actuellement, les conséquences de cette situation sont énormes et parfois même elles dépassent l'opinion publique. La question de la vie privée sur internet a ainsi fait couler beaucoup d'encre et de salive. Si d'un côté certains s'intéressent sur la protection des données personnelles sur internet, de l'autre côté d'autre préfèrent s'aventurer sur les comportements et la responsabilité des internautes. Alors face à cette montée exponentielle du nombre de victimes dans le monde virtuel, il semble important voire même urgent de mettre en place des solutions pour extirper un tel fléau très néfaste pour la société.

**Malgré cette situation désastreuse, des solutions pourront toujours être utiles pour l'éradication de ce phénomène.**

Les problèmes liés à l'usage abusif des médias sociaux sont d'ordre planétaire. Aujourd'hui, il est très difficile d'échapper aux tentatives d'atteintes à la vie privée sur internet étant donné que le risque zéro n'existe nullement pas dans le cyberspace. Néanmoins, des solutions aléatoires peuvent toujours aider à anéantir les dangers omniprésents sur la toile. Toutefois, même si quelque la sensibilisation fait défaut au Sénégal, elle reste à ce jour la clé de voûte pour assurer une meilleure protection des internautes. Pourvue que la majeure partie des usagers des plateformes de communication électroniques s'aventurent dans un monde parfaitement incompris, l'éveil de leur conscience sur les cyber risques peut aider à réduire considérablement les atteintes à leurs données personnelles .

A travers cette sensibilisation, les acteurs concernés pourront insister sur l'existence d'un cadre institutionnel et normatif relatif aux activités en ligne et que certaines pratiques sont prévues et punies par la législation sénégalaise.

A ce titre, il est important de rappeler aussi que l'usage des réseaux sociaux est une question à responsabilité partagée. L'adoption de bons comportement en ligne doit être l'affaire de tout un chacun d'entre nous, surtout dans ce contexte marqué par une multiplication incessante des dérives. Tout de même, l'alourdissement des sanctions pour les cybercriminels n'est pas laissé en rade en guise de solution. D'une part, si certaines personnes insistent sur l'actualisation du cadre juridique de la protection des données personnelles au Sénégal d'autre préfèrent soulever la question du pouvoir de sanction que doit avoir l'autorité de régulation en occurrence la CDP pour mieux assurer l'organisation et le fonctionnement des activités numériques au Sénégal.



ARTICLE 9

Les services financiers  
numériques: socle de  
l'inclusion financière en  
Afrique de l'ouest.



Il y'a de cela deux décennies, personne n'aurait imaginé qu'il était possible d'avoir de l'argent sur son téléphone portable, payer ses factures d'eau ou d'électricité , ou encore régler une facture d'achat avec son cellulaire. Ceci constituait un véritable mythe pour la population et certaines l'imaginaient quasiment impossible. Aujourd'hui, les technologies numériques ont rendu possible cette donne, ce qui a permis à toute l'humanité de se plonger dans une ère digitale. Toutes nos interactions passent désormais par des canaux virtuels, ce qui modifie considérablement nos activités. Pas mal de domaines ont subi l'implication des nouvelles technologies ce qui fait que le secteur financier n'est pas laissé en rade. Dans un passé très récent, on a tous vu naître une nouvelle activité dans l'atmosphère financière : il s'agit des services financiers numériques.

Pour son fonctionnement, cette nouvelle tendance dans ce secteur traditionnel (secteur bancaire et financier) s'appuie sur des supports technologiques ainsi que sur la monnaie électronique.

Ainsi, dans un rapport du Groupe Consultatif d'assistance aux Pauvres (GCAP) sur la régulation des services financiers digitaux rédigé entre février et juillet 2016, il a été mentionné que la notion de services financiers numériques n'a pas de définition commune et largement reconnue. Mais, dans plusieurs cas de figure, le concept sert à désigner la prestation de services financiers par voie de communication numérique (habituellement par la téléphonie mobile, cartes ou internet), avec un usage limité de l'infrastructure bancaire traditionnelle. Dès lors, on peut appréhender que ces services consistent à offrir à travers l'utilisation de supports numériques, des possibilités de transactions bancaires à des personnes qui n'ont généralement pas accès aux opérations des banques et établissements financiers, ce qui constitue sans doute un enjeu pharamineux pour l'humanité. L'Afrique de l'ouest a si tôt saisi l'importance d'une telle innovation dans le cadre de l'inclusion financière. C'est ainsi que les acteurs de cet écosystème ont pris très au sérieux cette activité depuis le début, même si des défis importants restent à relever.

### **L'Afrique : le berceau des services financiers numériques...**

Dans un contexte fortement marqué par les technologies numériques, une mutation multisectorielle sévit un partout dans le monde. La transformation digitale constitue ainsi la nouvelle tendance des domaines d'activités, y compris celui de la finance. Compte tenu des réalités actuelles et d'une forte demande sociale issue de la clientèle, les acteurs traditionnels du secteur bancaire et financier commencent à améliorer leurs activités en proposant de nouvelles offres et services adaptés aux besoins de la population. En ce sens, de nouveaux mécanismes de digitalisation des services financiers voient le jour. C'est l'exemple du Mobile Money, une innovation née bien de chez nous.

Face à une population à faible niveau de revenus, sous bancarisée ou mal desservie, une nouvelle opportunité s'est présentée en Afrique : le Mobile Money. Il s'agit d'un partenariat entre les banques et les opérateurs de téléphonies mobiles où le client ne dispose pas de compte bancaire mais plutôt un compte de monnaie électronique.

Pour rappel, cette innovation a été lancée pour la première fois en 2007 au Kenya. Il était l'œuvre de l'opérateur Safaricom, une filiale du groupe britannique de télécommunication Vodafone. Ce partenariat a généré le M-Pesa, premier service financier numérique en Afrique.

A l'origine, ce service était destiné à faciliter le remboursement de microcrédits de Faulu Kenya, une institution de microfinance. Les bénéficiaires devraient s'appuyer sur les services de l'opérateur Safaricom pour s'acquitter de leur engagement vis-à-vis de l'institution. Ainsi, compte tenu d'un franc succès de ce partenariat, les clients ont vite saisi les opportunités de cette innovation en effectuant des opérations qui n'ont pas été prévues au départ tel que le paiement des biens et services ou encore l'envoi et le retrait d'argent. Ce succès spectaculaire du Kenya a vite inspiré les autres états africains, ce qui fait que le modèle s'est vite reproduit un peu partout dans le continent, notamment en Afrique de l'ouest.

**Les services financiers numériques : un pilier fondamental pour lutter contre l'exclusion financière...**

Depuis très longtemps, le circuit bancaire n'était réservé qu'à une couche sociale bien déterminée de la population. L'accès aux opérations bancaires était inaccessible, voire même impossible pour certaines populations. Cette situation avait fini par instaurer une fracture numérique et financière entre les personnes non bancarisées et celles qui avaient intégralement accès aux services financiers. Pour certains, la banque était un luxe spécialement dédié aux personnes à revenu élevé, ce qui fait qu'elles étaient dans une situation d'exclusion financière. Par exemple, le monde rural a longtemps été écarté des infrastructures bancaires, occasionnant ainsi une marginalisation de sa population. Il en était de même pour les personnes pauvres, les personnes mal desservies ou encore les femmes qui éprouvaient d'énormes difficultés pour accéder aux services financiers. Aujourd'hui, avec le développement exponentiel des technologies numériques adossé à un taux de pénétration significatif de la téléphonie mobile, cette tendance s'est vite inversée, constituant alors un vieux souvenir pour la population. Ainsi, la technologie a joué un rôle crucial dans ce processus d'inclusion financière.

Avec l'importation massive de supports électroniques (téléphones, TPE, applications), l'Afrique est devenue un véritable hub du digital. Selon André Grissonnanche, expert de la Sécurité des Systèmes d'information, des transactions électroniques sécurisées et des systèmes électroniques de paiement, « l'Afrique a connu un incroyable développement du téléphone mobile au cours des dernières années. On compte aujourd'hui 850 millions de téléphones mobiles en Afrique, soit un taux de pénétration de 50% de la population. Le nombre de téléphones mobiles peut même parfois être supérieur à celui de la population. À titre d'exemple, il y a au Sénégal 1,2 téléphone mobile par habitant ».

Toutefois, si l'Afrique de l'ouest a réussi le pari de digitalisation des services financiers, elle le doit en grande partie à la téléphonie mobile. Ce support qui ne se limitait qu'à un usage très restreint (émettre et recevoir des appels) est vite devenu un outil multifonctionnel, surtout dans les activités financières.

Les services financiers numériques ont permis ainsi aux personnes jusque-là non bancarisées d'accéder aux services financiers formels grâce à l'utilisation de canaux numériques. Avec une très grande accessibilité et une facilité d'utilisation, les nouvelles plateformes de services financiers proposent au public un large choix de gamme de produits et d'offres à distance en s'appuyant sur les technologies déjà existantes, ce qui reste toujours bénéfique pour toutes les couches sociales. L'avantage de cette finance digitale est qu'elle offre à la population financièrement exclus des solutions alternatives aux opérations bancaires à moindre cout.

Ainsi, dans son allocution d'ouverture lors du forum de haut niveau sur les innovations technologiques au service de l'inclusion financière tenu à Dakar le 27 Novembre 2018, M. Tiémoko Meyliet Koné soutenait que « le développement accéléré des produits de la finance digitale favorisé par la révolution du numérique intervenue au cours des derniers années, a généré des retombées significatives dans les pays en développement tout en consolidant la dynamique d'inclusion financière. Les innovations, en particulier l'adoption de la téléphonie mobile et des smartphones ont facilité l'élargissement de l'accès aux services financiers aux entreprises et aux populations jusque-là difficiles à atteindre ». Ces propos peuvent être soutenus par plusieurs exemples de réussite des services financiers numériques dans le cadre de l'inclusion financière, surtout en Afrique de l'ouest car les avantages de ses services sont très vastes, et parfois même incommensurables.

Aujourd'hui, avec les services financiers digitaux, les utilisateurs parviennent en un temps record de stocker ou encore de transférer des fonds via la téléphonie mobile, ce qui permet à ces derniers d'améliorer le potentiel de leurs revenus et de lutter contre la pauvreté et l'exclusion financière. Ils permettent aussi d'anticiper sur les risques financiers en facilitant la collecte d'argent auprès des amis, proches ou parents, à un coût très réduit, ce qui constitue un avantage majeur pour l'inclusion financière. D'ailleurs, l'Afrique de l'ouest a réalisé des exploits significatifs dans la stratégie d'inclusion financière car se fiant aux propos de Gisèle Ndoye lors de la deuxième semaine dédiée à cette activité en novembre 2019, la zone UEMOA a dépassé le taux de 57%, ce qui est rassurant du fait que la courbe est ascendante.

**Toutefois, des défis restent à relever dans le secteur des services financiers digitaux...**

L'importance des services financiers numériques dans la consolidation de l'inclusion financière n'est plus à démontrer. Partout à travers le monde, ces services ont permis à toutes les couches sociales de retrouver une place importante dans le circuit financier longtemps réservé à une catégorie de personne bien déterminée. En Afrique de l'ouest, l'implication des technologies numériques dans le secteur de la finance a réduit considérablement la pauvreté, surtout dans certaines zones où l'accès aux infrastructures bancaires étaient difficile. Toutefois, nonobstant l'importance de ce secteur à l'heure actuelle, des défis majeurs restent à relever. En effet, parmi tous les acteurs de l'écosystème des services financiers numériques, le consommateur reste le plus important du fait qu'il représente le destinataire final. Compte tenu de sa position, beaucoup de risques peuvent peser sur lui et sur ses données personnelles. En ce sens, le renforcement des mécanismes juridiques et techniques de protection du consommateur devient une urgence.

Pour rappel, pour la majeure partie des transactions qu'il effectue, le client est appelé à fournir certaines informations qui peuvent être dès fois confidentielles. Même si cela entre dans un cadre bien précis (la lutte contre le blanchiment de capitaux et le financement du terrorisme), il s'avère nécessaire de renforcer la vigilance sur les données collectées, surtout le respect du principe de la finalité. Dans des activités aussi stratégiques que les services financiers numériques, la notion de confiance joue un rôle crucial du fait qu'elle permet de retenir la clientèle. Dans cette activité, la confidentialité des données personnelles et la protection des consommateurs est tout temps remise en cause. Cette situation s'explique du fait que la majeure partie des données sont collectées et traitées de manière passive et automatique, c'est-à-dire sans que le consommateur ne s'en rende compte. Les données peuvent ainsi transiter entre prestataires sans une autorisation préalable de la personne concernée.

Ces actions sont illégales et peuvent amoindrir la confiance entre les prestataires de services financiers et les consommateurs, surtout lorsque certaines opérations sont suspectes ou encore certaines irrégularités s'opèrent sur le compte du client sans que ce dernier effectue une quelconque transaction. Ainsi, ces entraves peuvent souvent être source d'échec ou d'anéantissement, surtout dans un secteur qui est appelé à évoluer perpétuellement. L'autre défi important à relever dans ce secteur reste, entre autres, l'interopérabilité des plateformes de service financier numérique.

Aujourd'hui, si le développement de ces services connaît un ralentissement dans certaines zones, c'est parce qu'il est difficile de rendre interopérables certaines plateformes. Pour la plupart des cas, on observe dans ces zones la présence de peux de services, ce qui peut être une source de blocage des activités.

Actuellement, il est clair que l'exclusion financière de certaines populations est occasionnée par cette absence d'interopérabilité des services financiers numériques. A titre de définition, l'interopérabilité peut être appréhendée comme « la capacité de l'utilisateur d'un compte ou d'un portefeuille géré par un prestataire, de recevoir ou d'effectuer des transferts vers le compte ou portefeuille d'un utilisateur géré par un autre prestataire. On peut aussi décrire l'interopérabilité au niveau de l'agent, quand un client d'un prestataire peut effectuer des transactions auprès de l'agent d'un autre prestataire[1] ». Ce mécanisme permet ainsi de soutenir un écosystème de paiement inclusif car l'utilisateur pourra effectuer des opérations avec le prestataire de son choix ou entre prestataires.

Ainsi, le problème d'interopérabilité entre les systèmes de paiements, les cartes ou encore les portes monnaies électroniques constitue une contrainte de taille pour l'inclusion financière. Même si que des projets importants allant dans ce sens sont en cours dans l'espace communautaire, l'atmosphère des services financiers numériques n'a pas encore connu l'effectivité de l'interopérabilité des plateformes. Toutefois, des efforts considérables sont en train d'être menés par des Fintechs telles que Paydunya ou encore Touch. Dans une démarche participative, ces agrégateurs dans le secteur financier ont aussi eu l'idée de promouvoir l'interopérabilité, ce qui constitue d'ailleurs un pas important dans la promotion de l'inclusion financière en Afrique de l'ouest



ARTICLE 10

# Internet et mode de vie : 10 bonnes pratiques à adopter dans le cyberespace

ASSANE SY



**Aujourd'hui, il est indéniable que les technologies numériques font partie intégrante de notre quotidien. Ainsi, elles s'avèrent être un besoin nécessaire pour l'humain dans le cadre de l'usage personnel comme professionnel. Toutefois, il faut comprendre que ce monde virtuel est souvent synonyme de risques qui peuvent être fatales pour notre vie privée. Au-delà du fait que les utilisateurs constituent les premiers boucliers de sécurité, ils sont aussi ce maillon sur lequel s'appuient les cybercriminels pour commettre des infractions. Nos comportements peuvent être des failles que ces derniers exploitent continuellement, c'est pourquoi nous mettons à votre disposition une série de 10 recommandations pouvant participer amplement à votre sécurité en ligne.**

**Avant de partager une information dans le monde virtuel, ayez l'habitude de la vérifier pour s'assurer de son authenticité et de sa véracité.**

La vitesse exponentielle adossée à la viralité de l'internet fait que les informations sont partagées de façon instantanée. Au bout d'un seul clic, elles peuvent faire le tour de la toile et atteindre une cible très large. Et pourtant, rares sont d'entre nous qui prennent le temps de vérifier l'information. Si certains le font par méconnaissance, d'autres préfèrent s'accaparer de « l'exclusivité » ou encore de convoiter le phénomène du « buzz ». On est véritablement à l'ère de l'infobésité, de la désinformation et des fakes news. C'est pourquoi il est très important de procéder à la vérification préalable de l'information que nous devons partager car quelque part, on pourrait engager notre responsabilité.

**Ne publiez pas de contenus choquants, obscènes ou contraires aux réalités sociales : publiez juste ce qui est nécessaire et utile.**

Nos publications sur la toile reflètent très souvent notre comportement dans le monde réel. Ainsi, il y va de notre propre intérêt de bien revoir les contenus que nous véhiculons car ils peuvent en dire trop sur notre personne. Si les médias sociaux contribuent à la dégradation des bonnes mœurs, c'est par qu'en réalité on les utilise sans modération. Compte tenu de notre niveau parcimonieux de culture numérique, il serait beaucoup plus important pour chaque utilisateur de se focaliser sur l'utilité et laisser en rade la futilité.

**Ne faites jamais confiance à un ami virtuel car on ne sait pas qui se cache réellement derrière l'écran.**

Dans le monde virtuel, l'identité réelle de la personne n'est jamais connue. On ne sait véritablement qui est qui et qui fait quoi. Ainsi, la question de la confiance pose un véritable problème dans le monde du numérique. Avec les nombreuses techniques qu'utilisent les personnes malintentionnées (usurpation d'identité, contrôle de compte), on peut se faire piéger facilement et livrer des informations capitales relatives à notre vie privée. D'ailleurs, c'est pourquoi il est crucial de faire attention aux discussions que nous abordons en ligne.

**N'abordez pas de discours haineux, racistes, xénophobes ou sexistes en ligne : internet n'est pas une zone de non-droit.**

L'expression « tout ce que vous dites peut être retenu contre vous » est aussi valable dans le cyberspace. Nous sommes tous responsables des contenus que nous véhiculons sur les différentes plateformes de communication. Nonobstant la virtualité supposée, Internet constitue une zone encadrée par des lois et des règlements établis par les législateurs. Toutefois, il ne faut pas perdre de vue que les textes juridiques ont prévues de lourdes sanctions à l'endroit des personnes qui tiennent des discours déplacés (haineux, racistes, xénophobes). Les auteurs de telles infractions peuvent encourir une peine d'emprisonnement allant de six (6) mois à sept (7) ans de prison ferme et d'une amende de 500.000 à 10.000.000 de FCFA. (Art 431-41 et suivants de la loi n° 2016-29 du 08 Novembre 2016 portant code pénal).

**Ne partagez pas des informations qui peuvent nuire à la réputation d'une personne : même si vous n'êtes pas l'auteur principal du post, briguez la chaîne de viralité en s'abstenant de toute diffusion.**

Le phénomène du partage constitue une pratique très fréquente dans le cyberspace. Certaines d'entre nous s'empressent très souvent de partager à volonté des contenus sur la toile sans pour autant réfléchir sur le sort de cette action. D'ailleurs, c'est ce qui fait que certains contenus indésirables deviennent viraux, juste à la minute qui suit leur publication. Et pourtant, cette pratique nuit à la réputation de plusieurs personnes. Ainsi, dans un souci de mieux protéger l'humain dans le cyberspace, essayons toujours d'analyser les contenus que nous voulons partager avant leurs publications. Apprenons aussi à briguer la chaîne de transmission des contenus obscènes dans le but de consolider nos bonnes mœurs et nos réalités sociales.

**Ayez l'habitude de recueillir le consentement de la personne faisant l'objet d'une publication sur les médias sociaux, même si c'est un ami, proche ou parent.**

Le consentement d'une personne constitue une chose essentielle dans le monde virtuel, et pourtant il est très négligé par les internautes. Même si ça peut paraître insensé pour certains, recueillir l'autorisation de la personne faisant l'objet d'une publication sur les médias sociaux ou encore une personne faisant l'objet d'un traitement de donnée personnelle semble être crucial. Quelles que soient nos relations, cultivons en nous ce sens de responsabilité et recueillons l'aval de l'intéressé avant de procéder à quoi que ce soit dans le cyberspace. Cette habitude permettra ainsi d'éviter des différends dans le futur ou en cas de litige.

**N'envoyez pas de photos, vidéos ou messages contenant des scènes sexistes à qui que ce soit : apprenez à préserver votre vie privée en ligne.**

Ces derniers temps, beaucoup d'individus se sont fait piéger en ligne par des cybercriminels en envoyant leurs photos ou vidéos à caractère pornographique. Si certains d'entre eux se sont faits trahis par des amis, d'autres n'ont pas pu échapper au génie des technologies qu'utilisent des personnes malintentionnées. Très souvent, l'auteur des photos ou vidéos érotiques subit des chantages sous peine de voir ses contenus divulguer en ligne. En réalité, chacun d'entre nous peut échapper à ces pratiques indésirables en adoptant des comportements responsables en ligne. Nous savons tous que l'intimité est sacrée, raison pour laquelle elle ne doit pas être publiée ou exposée à la portée de tout le monde. Pour ce faire, évitons de filmer ou d'envoyer des contenus contraires à nos réalités sociales, quel que soit le motif évoqué par le destinataire.

**Internet est un couteau à double tranchant : Ayez l'habitude d'exploiter son côté positif et évitez d'en faire un usage futile.**

Internet constitue un levier fondamental pour booster les activités de l'Homme. Au-delà de l'aspect divertissant que nous procure la toile, le monde virtuel regorge d'énormes potentialités pouvant être bénéfiques pour l'humanité. Il ne nous donne que ce que nous lui demandons, alors ça serait bénéfique pour nous d'exploiter son côté positif, utile. Aujourd'hui, aucun secteur d'activité n'est épargné par les technologies numériques. Notre productivité peut être beaucoup plus significative si l'on se concentrait davantage sur les aspects importants d'Internet. Pour que cela se réalise, il nous faut impérativement une nouvelle lecture de la toile. Tout de même, l'acquis d'une bonne dose de culture numérique serait un atout pour tout un chacun d'entre nous.

**Ayez l'habitude de revoir les conditions d'utilisation, les paramètres d'accès et de préférences des applications que vous utilisez, modifiez les à votre guise si possible pour plus de sécurité à votre vie privée en ligne.**

Chaque jour, nous utilisons des applications sur nos différents supports (téléphones, ordinateurs, smart tv). Et pourtant, rares sont d'entre nous qui prennent le temps de lire intégralement les conditions d'utilisation. Très souvent, ce texte constitue le contrat d'adhésion qui nous lie avec la plateforme et il est mentionné la façon dont l'application traite nos données personnelles ainsi que notre vie privée. Au moment de l'installation aussi, certaines applications nous demandent des accès sur notre support. Toute autorisation d'accès peut donner la possibilité à l'application de contrôler certaines actions sur notre terminal.

Ce n'est pas tout, d'autres applications peuvent même aller plus loin, en demandant de suivre nos activités hors de la plateforme. Alors, il appartient à l'utilisateur de bien revoir en fond tous ces détails pour ne pas consentir à quelque chose dont il ne maîtrise pas. Limitons les accès et s'il le faut, désactivons le maximum possible les autorisations accordées aux applications et qui peuvent leur permettre d'avoir plus de détails sur notre vie privée.

**Enfin, ayez l'habitude de mettre à jour les appareils électroniques que vous utilisez dès que l'occasion se présente. Dans le monde virtuel, aucun détail n'est à négliger.**

Tous les moyens sont bons pour garantir sa sécurité en ligne. Dans le monde virtuel, il faut admettre qu'aucun détail n'est à négliger. Parfois, certains utilisateurs ignorent la mise à jour des appareils ou encore des applications qu'ils utilisent. Et pourtant, cette pratique peut quelque part améliorer la sécurité de l'appareil ou encore l'application avec des niveaux de correction beaucoup plus élevé. Toutefois, avant de procéder à une quelconque mise à jour, lisez intégralement les changements qu'elle va apporter à l'ancienne version.

Bien vrai que le risque zéro n'existe pas dans le monde virtuel mais nous devons sensibiliser davantage les internautes pour amoindrir le maximum possible les risques omniprésents sur la toile. Ce document s'inscrit dans cette logique et dans une dynamique de contribution citoyenne sur l'usage des technologies numériques.

## A propos de l'auteur



Assane sy est un cyberjuriste-consultant, spécialiste en droit du numérique. Il a fait ses études supérieures à l'Université Alioune Diop de Bambey où il a obtenu sa licence professionnelle en cybersécurité et commerce électronique et son Master en droit des affaires et cyberdroit. Il a intégré de grands cabinets comme SAYTU en tant que cyberjuriste-consultant, avant de rejoindre Bs Corp, devenu actuellement UnLine. Il a été responsable des formations de plusieurs initiatives de Meta au Sénégal, en occurrence Ma vie en ligne et Mon Univers digital Sénégal 1 &2. Il est aussi spécialiste en régulation du numérique après avoir fait un Master Professionnel en la matière à l'ESMT de Dakar. Il intervient également au niveau des médias nationaux et internationaux sur des questions liées au numérique, à la cybersécurité et la protection des données personnelles. Il est aussi auteur de plusieurs articles de presse et d'une quinzaine de certificats de formation délivrés par le GSMA.

mail : [sylassane2018@gmail.com](mailto:sylassane2018@gmail.com)      Tel : +221 77 862 08 21