LIVRE BLANC

LE NUMÉRIQUE À L'ÉPREUVE DE L'ÉTAT D'URGENCE SANITAIRE COVID19 AU SÉNÉGAL : ENTRE INNOVATION (S) ET NÉCESSAIRE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Approuver un régime d'état d'urgence sanitaire pour lutter contre la pandémie actuelle n'est pas synonyme de blanc-seing donné au pouvoir politique et aux autres décideurs publics. Toutefois, les considérations d'efficacité fonctionnelle ont supplanté la prise en compte de la garantie des droits et libertés fondamentales. C'est ainsi que le droit positif sénégalais, la législation sur la protection des données offre des processus permettant à minima de définir un équilibre entre l'action publique et la protection des droits des personnes. Par conséquent, dans un communiqué du 24 avril 2020, l'autorité de régulation, à savoir la Commission de Protection des Données Personnelles[1] (CDP) a précisé le régime dérogatoire prévu par les textes, car il s'agit concrètement de mettre en œuvre un traitement de données personnelles sensibles, en vue :

- de sauvegarder des intérêts vitaux des personnes ;
- de répondre à un motif d'intérêt public;
- de promouvoir le dépistage. et protéger la santé publique ;

Dans ce contexte exceptionnel, l'autorité a tenu à rappeler in fine que les traitements des données des citoyens doivent être encadrés en tenant compte notamment de certaines mesures (confidentialité et sécurité) et principe (la minimisation des données).
Le numérique est aujourd'hui partout et déploie ses applications et solutions dans tous les domaines. Qu'il s'agisse de générer de l'interactivité entre les personnes, de permettre aux chaînes d'approvisionnement de maintenir une activité essentielle ou encore d'optimiser la gestion opérationnelle de la crise sanitaire.

Les données personnelles en tant que matière première sont évidemment au cœur de cette activité digitale et mettent en évidence la question de la conformité de leur traitement. Pour rappel, cet encadrement juridique a pour vocation de mieux accompagner les missions des différents exploitants de la donnée et sans pour autant freiner l'innovation pendant cette période inédite. En revanche, la gestion prioritaire de l'état d'urgence et des conséquences de la crise sanitaire ne doit pas générer la mise en production de traitements et applications dits « abusifs » et « anarchiques » de la part des acteurs.

L'enjeu est ici de confronter les usages en période de risque sanitaire et de survie économique au regard de la Doctrine Informatique et Libertés. Comment appliquer la réglementation sur les données en pleine crise, mais également pour la période post Covid19 ? Quels enseignements en tirer en termes de points de vigilance par rapport aux nouvelles exigences internationales et aux évolutions à venir des réglementations sénégalaises.Ce livre blanc contribue ainsi à évaluer plusieurs innovations portées par la digitalisation au travers de services, d'applications et traitements. Il démontre qu'il est impératif de concilier l'objectif de sécurité sanitaire et la protection de la vie privée.

[1] HTTPS://WWW.CDP.SN/CONTENT/COVID-19-COMMUNIQU%C3%A9-DE-LA-CDP-SUR-LE-TRA%C3%A7AGE-NUM%C3%A9RIQUE

L’idée est de sortir de cette crise multidimensionnelle en étant mieux organisé et proactif afin de sauvegarder notre souveraineté numérique. De fait, la sécurité numérique et la protection des droits et libertés des citoyens peuvent être considérées comme de nouveaux enjeux de conquête démocratique et de développement. D’autant plus qu'avec la transformation numérique, les systèmes d’information de santé et les applications dédiées abritant de plus en plus de données personnelles sensibles sont mis à rude épreuve.
Le pouvoir régalien et les acteurs économiques sont généralement les plus grands collecteurs et utilisateurs de données de toutes sortes. Il s’agit des décideurs pour des raisons organisationnelles voire politiques, et des entreprises pour des raisons économiques. Au Sénégal, nous avons noté au tout début de la pandémie un sursaut national d’engagement de tous bords pour maîtriser aussi rapidement que possible cette maladie à coronavirus. C’est ainsi que des initiatives recourant aux technologies du XXIe siècle ont été noté ça et là (cf. livrable édité par Socialnetlink).

Face à ce risque, Quel est le dispositif de régulation adéquat pour protéger à minima les citoyens ? Certainement, il convient plus que jamais de libérer le potentiel des technologies exploitant de la donnée personnelle pour contribuer à endiguer la crise sanitaire de la Covid-19. Il urge, au préalable, que l’on s’interroge sur la prise de conscience par ces acteurs de l’impact du traitement des données personnelles sur la vie privée et les libertés individuelles ? Pour ceux qui en ont conscience, quelles garanties suffisantes de sécurité offrent-ils pour minimiser les risques ?

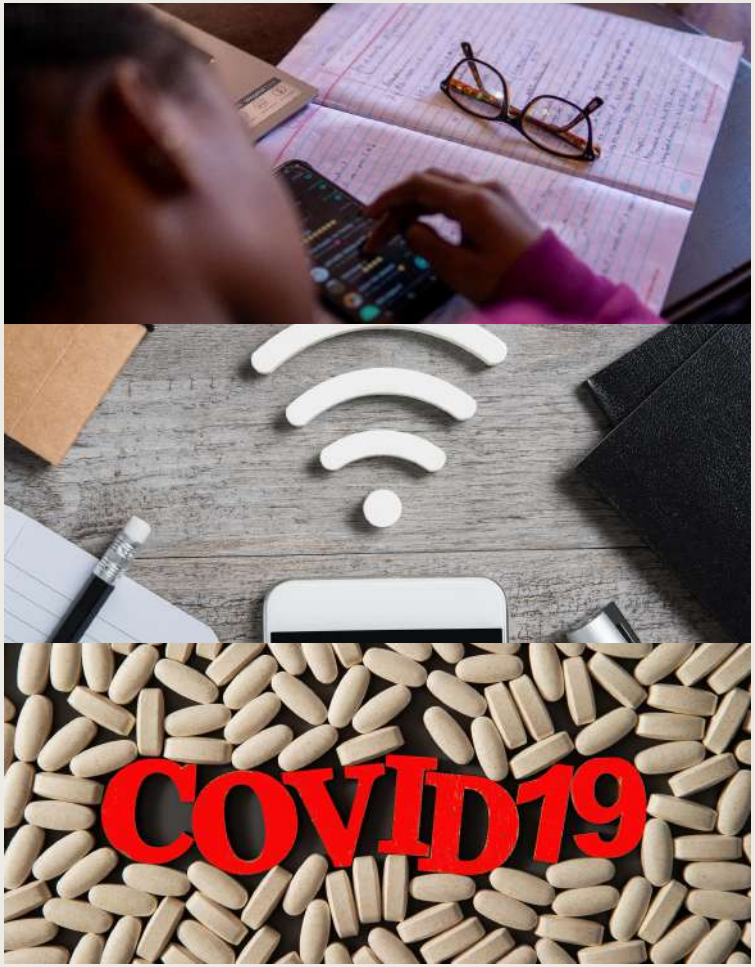
Comment, dans ce contexte de pandémie, respecter la confidentialité et la vie privée dans le traitement et la collecte de ces données à caractère personnel ? Quid des droits des personnes dans pareille situation ?

[2] HTTPS://WWW.SOCIALNETLINK.ORG/2020/04/COVID-19-DIGITAL-SOCIALNETLINK-LANCE-UN-RECUEIL-GRATUIT-SUR-LES-INITIATIVES-SENEGALAISES/

Emmanuel Maurice DIOKH
Responsable Internet Sans Frontière Sénégal
Africtiviste, membre du réseau des blogueurs du Sénégal
Juriste en Droit du numérique - Data Protection Officer (DPO)
Il accompagne depuis plusieurs années des Startup dans le conseil, la mise en conformité des innovations sous le prisme de la protection des données personnelles.

Pape Fodé DRAME
Juriste Droit du numérique et Expert RGPD
Diplômé en droit à la Sorbonne et ancien juriste à la direction de la Conformité de la CNIL.
Il accompagne depuis plusieurs années des organisations dans le conseil et l'accompagnement juridique et notamment dans la protection des données personnelles.Fort d'une expérience accrue en matière de Droit du numérique et en audit I&L, vous accompagne également dans les projets de transformation numérique et la Conduite du changement.

PRÉFACE DE MONSIEUR EL HADJ ABDOULAYE SECK



La pandémie de la Covid-19, bien qu'ayant démontré la fragilité de notre système de gouvernance, nous offre l'opportunité de réorienter nos priorités en positionnant ainsi les droits humains et la technologie comme des piliers dans l'architecture du monde moderne.

La technologie peut et doit jouer un rôle important dans la lutte contre la pandémie de la Covid19 pour sauver des vies en diffusant notamment aux populations des informations cruciales sur les moyens de prévention et de prise en charge de la maladie. C'est ainsi que beaucoup de solutions e-santé ont été déployées ou continuent à l'être dans plusieurs pays au monde.

Si ces mesures prises le sont au nom de la préservation de la vie des personnes, elles ne doivent pas être dévoyées et ainsi constituer de sérieuses menaces à l'atteinte au droit à la vie privée notamment. Il se trouve cependant que la technologie telle qu'elle est utilisée par les gouvernements aujourd'hui renforce leur pouvoir en matière de surveillance.

Si dans le discours officiel, nombre d'application de traçage ont été déployés pour suivre des contacts de la Covid19 et assurer leur prise en charge, la réalité est toute autre dans beaucoup de cas.

Le Security Lab d'Amnesty International a procédé à l'analyse technique de 11 applications utilisées en Algérie, à Bahreïn, aux Emirats arabes unies, en France, en Islande, en Israël, au Koweït, au Liban, en Norvège, au Qatar et en Tunisie. Certaines de ces applications sont des outils de surveillance de masse les plus dangereuses que l'ONG de droits humains a examiné puisqu'ils procèdent tous activement à la localisation (quasiment) en direct des utilisateurs en envoyant fréquemment des coordonnées GPS à des serveurs.

Nous sommes tous d'accord que le monde traverse une période inédite qui demande l'intervention des gouvernements pour garantir le droit à la vie. Cet impératif ne doit cependant pas faire oublier l'obligation qu'ont les Etats de ne pas minimiser ou ignorer le droit à la vie privée, à la liberté d'expression et à la non-discrimination, au nom de la gestion de la crise sanitaire. Au contraire, protéger les droits humains permet aussi de promouvoir la santé publique.

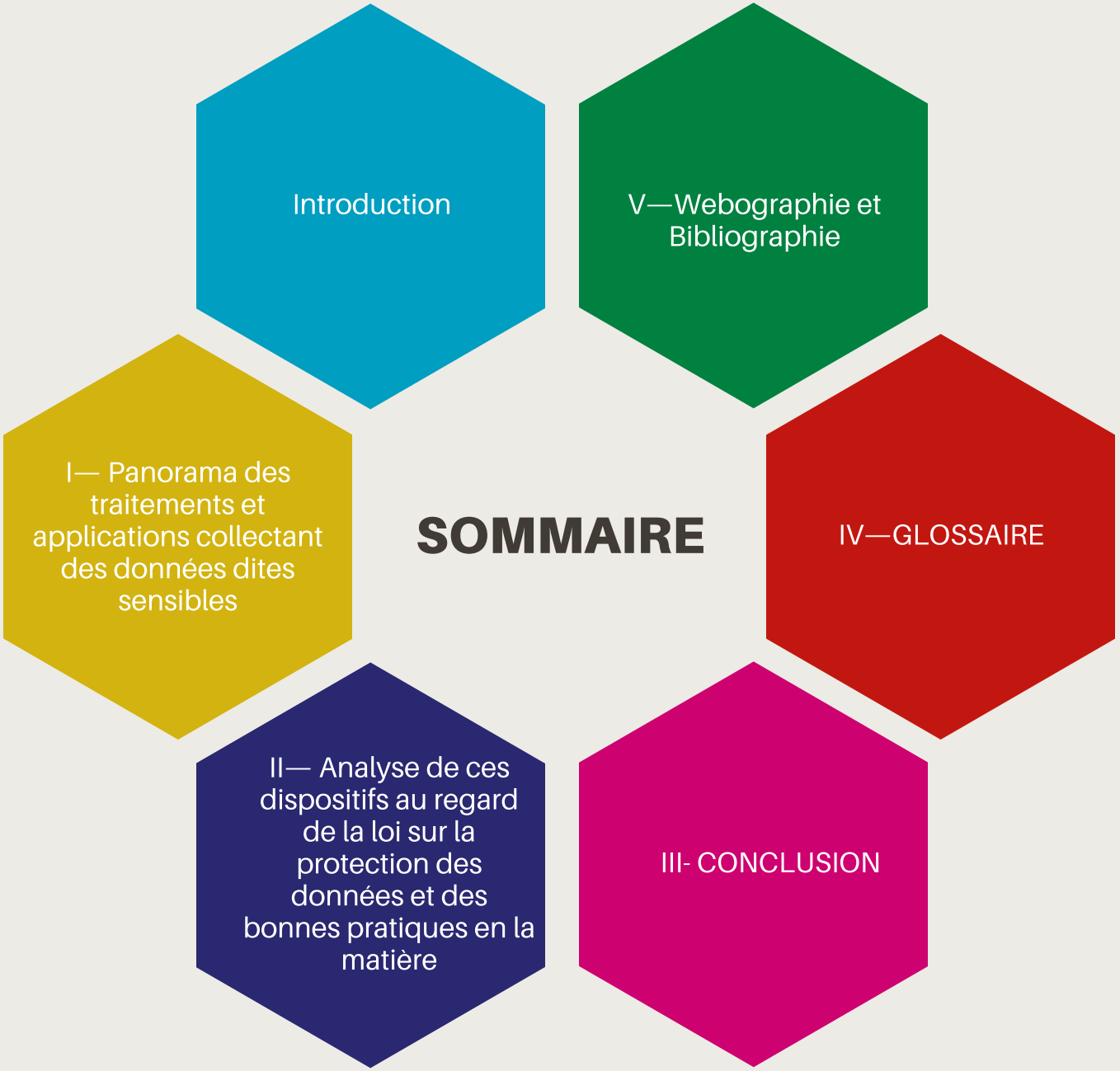
Ayant fini de se faire une place partout, le numérique doit être à notre service et non un outil utilisé au détriment de nos droits humains fondamentaux. C'est une demande forte qui doit être fortement exprimée par chacun-e, une « demande sociale » selon l'expression consacrée chez nous.

Il est donc impératif que les gouvernements accordent une attention accrue à l'information des citoyens afin que le consentement donné à la collecte et à l'usage de ces outils soit libre et éclairé. Les Etats doivent également rendre compte de l'utilisation qu'ils font de ces outils et faire peser ces mêmes obligations sur les entreprises et particuliers impliqués dans ces opérations.

Ce livre blanc sur le numérique à l'épreuve de l'état d'urgence sanitaire du Covid19 au Sénégal offre une belle perspective dans la prise en charge de ces questions. Il est d'autant plus pertinent que la problématique doit être au cœur de notre quotidien et de nos aspirations à vivre dans un environnement moins intrusif.

EL HADJ ABDOULAYE SECK

SOMMAIRE


Introduction
V—Webographie et Bibliographie
I— Panorama des traitements et applications collectant des données dites sensibles
IV—GLOSSAIRE
II— Analyse de ces dispositifs au regard de la loi sur la protection des données et des bonnes pratiques en la matière
III- CONCLUSION

INTRODUCTION GÉNÉRALE : QU'EST-CE QUE LA PROTECTION DES DONNÉES ET QUELLE EST SON UTILITÉ DANS L'ÉCOSYSTÈME NUMÉRIQUE ?

Protéger les données personnelles revient à protéger la personne physique elle-même contre les éventuelles atteintes à sa vie privée mais aussi à ses libertés fondamentales. Il s'agit donc d'un bouclier qui permet de préserver les libertés individuelles des citoyens se traduisant par des droits. Pour les entreprises, les données personnelles constituent un bien précieux dans la mesure où elles leur accordent un grand intérêt économique. En recourant à de vastes banques de données aussi détaillées que possible, les entreprises peuvent déterminer très précisément le comportement d'achat de divers types de consommateurs, ce qui leur permet par exemple de cibler et de mettre en œuvre leur stratégie publicitaire.[3]

Pour le pouvoir régalien, grand collecteur de données personnelles des citoyens, il est inconcevable de ne pas avoir un contrôle minimal sur l'utilisation des données concernant sa population. Dans le même temps, pour toute société démocratique fondée sur le respect du droit et de la personne humaine, l'Etat est tenu de collecter que les données nécessaires à l'atteinte de finalités visées

En somme, quelle que soit l'entité en face, chacun doit en principe, pouvoir déterminer lui-même, dans la mesure du possible, quelles informations personnelles peuvent être transmises, à qui elles peuvent l'être, à quel moment et dans quel contexte.

La catégorie particulière des données sensibles

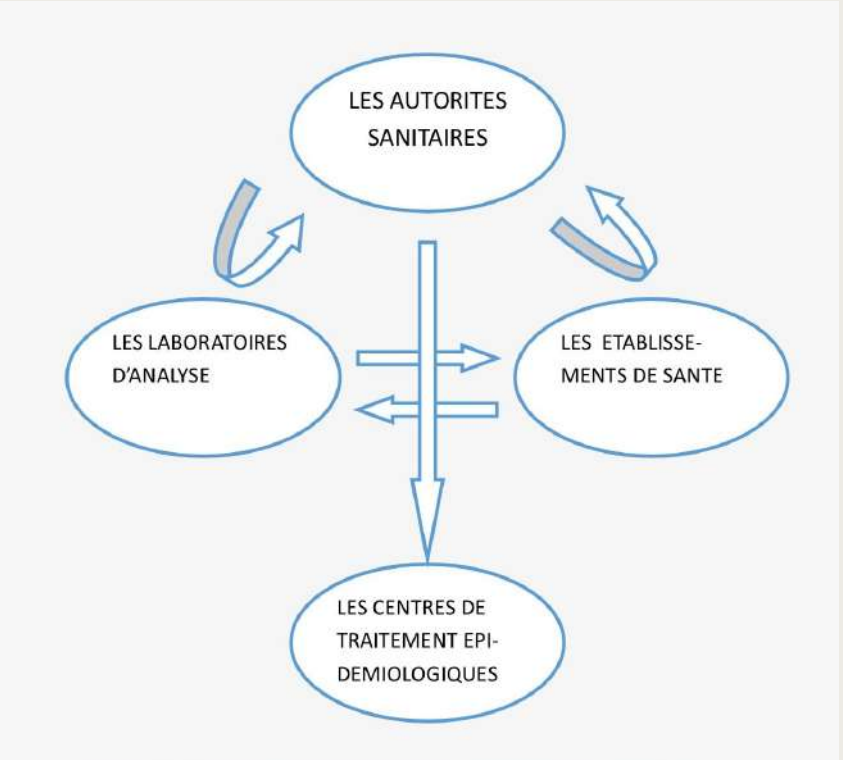
En principe, il existe une interdiction (art 40 loi 2008) de collecter ou de traiter des données dites sensibles. Il s'agit principalement de la catégorie de données touchant à l'intimité de la personne, notamment les données de santé[4]. La définition large de cette notion permet d'englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne.

[4] Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

Dans un contexte de gestion de la pandémie, les informations obtenues lors d'un test ou d'un examen de même que les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de soins de santé[5] sont en soi des données de santé. Les services de l'État et les autorités sanitaires dans le cadre de la stratégie nationale de lutte contre la maladie, testent, retracent les contacts et le cas échéant les isolent. De même, les professionnels de la santé peuvent légitimement mettre en œuvre de tels traitements dans la limite de leurs attributions. Autant de données de santé traitées et conservées en fonction du contexte bien déterminé. Au regard de la loi, en tant que responsable de traitement, si les professionnels de santé disposent d'un intérêt légitime pour les opérations de traitement de données de santé, les autorités sanitaires quant à elles disposent d'une mission d'intérêt public pour traiter des données de santé et autres données sensibles personnelles sans recueillir le consentement des personnes exposées. Toutefois, des obligations demeurent les mêmes en termes de confidentialité, de sécurité et de droits au profit des personnes.

Enfin, la collecte et le traitement des données de santé étant résolument sensibles, ces dernières bénéficient d'une protection accrue imposant aux seuls professionnels de santé de mettre en œuvre leurs traitements. Ce qui se justifie dans la mesure où une mauvaise manipulation d'une donnée de santé peut conduire à une erreur de diagnostic et avoir des conséquences néfastes sur la santé du patient. Aujourd'hui, les technologies avancées permettent la collecte et une meilleure gestion de l'information médicale. La démocratisation d'internet a permis le développement des applications mobiles et des objets connectés, le secteur de la santé a connu des changements dans la manière de diagnostiquer les patients. Le Quantified self "mesure de soi-même" est l'exemple le plus parlant, il s'appuie sur l'utilisation d'applications et d'objets connectés afin de mesurer divers éléments, dont la température du corps, le rythme cardiaque, le sommeil, le nombre de pas journalier, la mesure de la glycémie etc. Donc autant d'innovations qui reposent sur des données de santé.

Le schéma suivant met en évidence la nécessité du partage de l'information médicale s'appuyant sur une diffusion numérique pour une prise en charge rapide des personnes à risques. Toutefois, au vu des nombreux acteurs et à priori destinataires ou générateurs de la donnée de santé, les obligations en termes de sécurité et de confidentialité doivent être renforcées. Une étude d'impact doit être menée pour s'assurer que les traitements dits à risque (traitement de masse, données sensibles, profilage etc.) respectent bien les droits fondamentaux des personnes et minimisent les risques aux violations des obligations légales.



Parcours de la donnée de santé et gestion épidémiologique des personnes condamnées à la Covid-19

[5] HTTPS://WWW.INTERNET-JURIDIQUE.COM/DONNEES-DE-SANTE/

I- PANORAMA DES TRAITEMENTS ET APPLICATIONS COLLECTANT DES DONNEES DITES SENSIBLES

Il s'agit pour chaque traitement / application de renseigner les éléments fournis (matrice des principes fondamentaux : finalité, données collectées, destinataires) pour ensuite en faire une analyse au regard des exigences en matière de protection des données personnelles.

Pour circonscrire l'épidémie à coronavirus, beaucoup d'ingénieurs télécoms, de développeurs, informaticiens, acteurs du digital et évidemment les autorités sanitaires ont mis en place des solutions numériques. La finalité est d'aider les décideurs à lutter contre l'épidémie en donnant la bonne information pour lutter contre les infox (fausses informations) ou retracer et procéder à la prise en charge des cas avérés.

1-Les traitements de services digitaux

a-1) LAfrica Mobile

LAfrica Mobile via le #2121# qui devrait passer au #2930# avec comme responsable le Ministère de la Santé, est une structure spécialisée dans la fourniture de services mobiles innovants

L'objectif de la solution est de donner la bonne information via un code USSD[6] qui paraît moins intrusif. Au regard du cœur de métier de l'entreprise (les services mobiles), le respect de la finalité du traitement permettrait que les numéros ne soient pas utilisés à des fins de prospection.

Ainsi, pour la mise en œuvre du traitement, des données personnelles comme le numéro de téléphone sont collectées pour fournir les infos sur la Covid19. Il faut signaler que pour le #2121# la solution a été consultée par plus de 1.000.000 de sénégalais selon les responsables.

Heureusement, pour exercer votre droit d'accès, vérifier si vous figurez dans les bases de données, le cas échéant, demander la suppression des informations personnelles vous concernant cette adresse **contact@lafricamobile.com** a été communiquée.

a-2) L'application SunuCity

SunuCity est une application dont l'objectif est de faciliter le travail du ministère de la santé en permettant aux populations de recevoir et d'envoyer des informations en cas d'incidents, de risque sanitaire avec la possibilité de se faire géolocaliser à l'aide de coordonnées GPS. Ainsi, il est possible de recevoir des informations ciblées en fonction du lieu de résidence de l'utilisateur.

Pour ce faire, les données suivantes sont collectées: numéro de téléphone, données de localisation GPS et photos matérialisant l'incident à signaler.

Par contre, à la date du 07 juillet il n'y avait toujours pas de mentions légales sur le site afin d'informer sur les droits des personnes et les destinataires des données.

[6]UNSTRUCTURED SUPPLEMENTARY SERVICE DATA, CE QU'ON PEUT TRADUIRE PAR « SERVICE SUPPLÉMENTAIRE POUR DONNÉES NON STRUCTURÉES ». ON LES APPELLE PLUS SOUVENT LES CODES SECRETS (MÊME SI CEUX-CI SE TROUVENT FACILEMENT SUR INTERNET !). L'IDÉE CONSISTE À POUVOIR DÉCLENCHER DES ACTIONS SUR VOTRE MOBILE À DISTANCE, EN ENVOYANT DES DEMANDES ET INFORMATIONS VIA LES RÉSEAUX GSM, 3G OU 4G.

a-3): Le centre d'appel 800 00 50 50 et le #2930#

Il s'agit du centre d'appel du ministère de la Santé et de l'Action sociale qui a pour objectif de recevoir les signalements de cas suspect afin de procéder au prélèvement pour réaliser les tests. Pour le #2930# l'information est fournie via le code Ussd par un message push.

Pour assister l'État du Sénégal dans la lutte et la prévention contre la #COVID19, l'opérateur FREE avait proposé de mettre à sa disposition le matériel technique et toutes ses plateformes pour une bonne diffusion des messages de sensibilisation.

Pour atteindre cette finalité, les données ci-après sont collectées: nom, prénom, localité, numéro de téléphone, commentaires dans l'application de gestion d'appel.

2-La généralisation de l'usage du numérique dans l'éducation et la formation

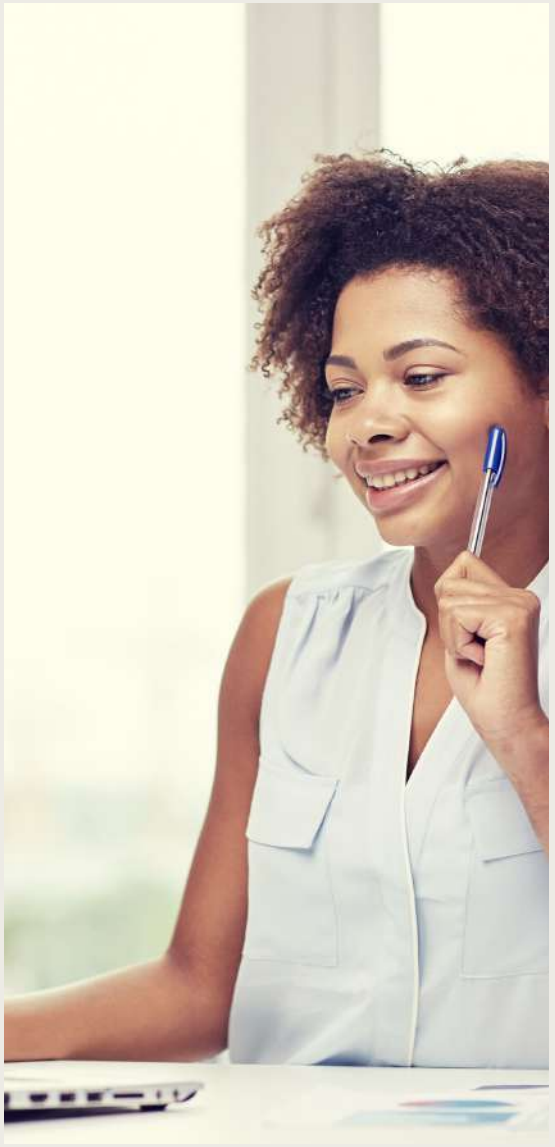
Afin d'assurer la continuité pédagogique le Ministre de l'enseignement supérieur de la recherche et de l'innovation avait proposé le recours aux TICE. C'est ainsi que les Assemblées délibérantes avaient retenu :

- de poursuivre en ligne les activités pédagogiques ;
- d'accompagner les enseignants dans la mise en ligne des contenus pédagogiques :
- de mettre en ligne des milliers de cours via les plateformes des instituts de formations ouvertes à distance (IFOAD) ;
- d'envoyer à distance les exercices aux étudiants ;

Une rencontre entre le MESRI et la Coordination des Organisations Privées d'Enseignement Supérieur (CUDOPES) avait permis de noter que des établissements utilisaient déjà l'enseignement à distance et d'autres prévoyaient de le faire en attendant les bonnes conditions d'une reprise en présentiel. (Source discours MERS, du 26-05-2020).

2-1): Les applications de Formation à distance.

Au regard de ce qui précède, nous convenons que certains établissements d'enseignement supérieur utilisent des plateformes pour assurer les cours à distance. En dehors de ceux qui ont développé des plateformes en interne, la plupart utilise des plateformes dont les responsables de traitement se trouvent au Sénégal et à l'étranger.



La finalité du dispositif est d'assurer la continuité de l'enseignement avec une collecte de données suivantes: les données d'identification des élèves, données des enseignants, images, données d'appréciation et commentaires libres, données sur le parcours de formation des apprenants et notations. Sont également collectées pour certains, des informations sur les tuteurs Père ou Mère, tuteur légal, nom et numéro de téléphone du conjoint.
Concernant les plateformes consultées, il n'y a pas de communication sur les droits des étudiants et apprenants en général. En outre, les données sont transférées hors du pays (logiciel en SaaS).

3—Les bases de données dans le cadre de la gestion du transport en période de Covid

Il est établi un traitement de données personnelles à travers un manifeste de transport selon les termes de l'arrêté du 05 Juin 2020 n°10333 fixant les règles d'exploitation des gares routières interurbaines
.La finalité est de suivre le parcours des voyageurs dès leur embarquement afin de retracer un éventuel cas suspect ou de pouvoir circonscrire la contamination par rapport à un cas avéré.
Pour y arriver, les données ci-après sont collectées : Nom et prénoms des passagers, numéro d'identification nationale, numéro de téléphone, adresse et destination. Prénoms et noms, adresse et numéro de téléphone de la personne à contacter en cas de besoin pour chaque passager. Par ailleurs, avant l'assouplissement des mesures restrictives, des données comme l'e-mail et le numéro de téléphone faisaient l'objet de collecte pour les demandes d'autorisation de circuler.

Concernant cette plateforme du ministère du transport avant la levée des mesures de restriction, il était possible, à l'aide du scan du QR [7] code de l'autorisation par un tiers, d'avoir accès aux informations personnelles du voyageur.

Deux problèmes majeurs sont à soulever sur cette collecte de données :

- la confidentialité et de l'obligation de sécurité ;
- la sécurité pour les fiches de renseignements entre les mains des chauffeurs et apprentis.

[7]CE CODE QUICK RESPONSE CODE, CE CODE VISUEL EN DEUX DIMENSIONS PEUT ÊTRE LU PAR DIFFÉRENTS TERMINAUX, EN PARTICULIER LES DISPOSITIFS MOBILES. CETTE LECTURE DÉCLENCHE DIFFÉRENTES ACTIONS (AJOUTER UNE CARTE DE VISITE VIRTUELLE, NAVIGUER SUR UN SITE INTERNET, VISIONNER UNE VIDÉO, ETC.)

4—Le développement de l'e-santé et des solutions d'hébergement des données de santé : L'œil de l'expert

E-santé et enjeux du traitement des données de santé

Au Sénégal, l'ambition est claire depuis quelques années : intégrer les technologies de l'information et de la communication au domaine de la santé. Le développement de la télémédecine, définie comme une forme de pratique médicale à distance utilisant ces technologies, répond en effet à des impératifs : réduire les coûts, faciliter l'accès aux soins, améliorer la prise en charge des patients et le suivi des maladies chroniques. Pour cela, la numérisation des données de santé des patients est un préalable, ce qui pose la question de l'encadrement spécifique de ces données dont la conservation peut s'avérer pertinente dans certaines situations.

Depuis 2018, le Ministère de la Santé et de l'Action Sociale à mis en place le «Plan stratégique Santé Digitale 2018-2023», une réflexion lancée depuis deux ans. Un agenda bouleversé par l'épidémie de la Covid-19 ou plutôt qui a trouvé en elle une aubaine pour redorer l'image de la santé par le digital.

Cette crise a encore renforcé la pertinence du développement de la télémédecine afin de pallier à l'insuffisance de professionnels de santé dans les zones rurales. Les technologies numériques sont de plus en plus utilisées pour la prise en charge des malades. Mais avec quels risques pour la sécurité numérique des données des patients ?

« Un nom plus une pathologie, c'est déjà une donnée médicale ; envoyer un mail non crypté, c'est la chose à ne pas faire », explique Jérôme Soistier, dans Jeune Afrique[8] il dirige la société française C3Medical, créée en 2011 pour organiser et optimiser les parcours de soin, et dont 70 % de l'activité est sur le continent.

[8] HTTPS://WWW.JEUNEAFRIQUE.COM/1011492/ECONOMIE/EN-AFRIQUE-AUSSI-LA-GUERRE-DES-DONNEES-MEDICALES-AURA-BIEN-LIEU/

L'hébergement des données de santé, un secteur d'activités insuffisamment encadré

En Europe particulièrement en France pour les applications de gestion de parcours de soin, les données sont rassemblées chez un hébergeur agréé données de santé (HADS), qui les stocke en locale. Depuis deux ans, tous les grands hébergeurs ont développé ce type de service.

Avec la récupération de données individuelles il est possible de voir où émerge un foyer de pandémie. Mais il faut que ces données restent anonymes, pour qu'elles ne soient pas utilisées à d'autres fins que l'amélioration des politiques de santé publique , comme le fait savoir le dirigeant de C3Medical. Par contre, nous savons qu'en 2001, Latanya Sweeney alors doctorante au sein du MIT (Massachussetts Institute of Technology) avait prouvé que garantir l'anonymisation des données de santé n'est pas chose aisée.
En croisant une liste électorale avec une base de données médicales pseudonymisées, c'est-à-dire purgées de tous ses éléments directement identifiants mais contenant des codes postaux, dates de naissance et sexe, elle parvint à ré-identifier 90% des individus et à prendre connaissance des données médicales du Gouverneur de l'Etat du Massachussetts de l'époque. Avec la puissance de calcul des machines et l'intelligence des algorithmes, le respect des principes de protection des données personnelles est gage de sécurité. Mieux, il faut veiller à leur respect depuis la conception.

Au Sénégal, il n'existe pas pour l'instant de règlementation spécifique applicable à l'hébergement de données de santé permettant des dispositions garantissant la protection juridique et technique, tant au niveau des échanges que du partage des données de santé.

Ce souci de protection de l'anonymat est constaté chez les jeunes start-up Sénégalais qui proposent des logiciels de parcours de soin pour les hôpitaux et les cliniques. Cependant, le fait que le piratage de données soit plus courant à l'étranger que chez nous ne signifie pas que nous sommes à l'abri. Au contraire, c'est un élément suffisant pour miser sur la sécurité des plateformes. L'Afrique est un terreau fertile pour les data brokers et les données de santé ont de la valeur.
Ce n'est pas parce que des données sont hébergées en Belgique ou que les exploitants des données sont en conformité avec le RGPD qu'il n'y a pas de risque de piratage.
Il faut que nous arrivions à un niveau où les données sont stockées localement par des hébergeurs de données de santé agréés par l'Etat du Sénégal. Dans le même temps, la mise en conformité doit être de mise au regard de la législation de nos pays. Pour s'en convaincre, il suffit d'apprécier le dossier pendant devant la CNIL concernant l'éventuelle vente de données de santé par Doctissimo.[9]

[9] https://www.lemonde.fr/pixels/article/2020/07/01/donnees-personnelles-doctissimo-vise-par-une-plainte-aupres-de-la-cnil_6044829_4408996.html

Des initiatives sous régionales prometteuses

Le Réseau d'Afrique francophone pour la télémédecine (RAFT) mis sur pied avec les Hôpitaux universitaires de Genève réfléchit à la protection des données des patients depuis ses débuts. Lancée en 2003, d'abord au Mali puis en Mauritanie, la plateforme offre des cours accessibles en ligne, mais permet aussi et surtout des échanges entre praticiens sur les diagnostics et traitements dans une vingtaine de pays. Développée par un ingénieur malien, dont le pays compte 0,1 médecin pour 1000 habitants, l'application Bogou (web et mobile) a été conçue spécialement pour le réseau.

Pour reprendre les termes du professeur Antoine Geissbuhler, médecin-chef du service de cybersanté et télémédecine des Hôpitaux Universitaires de Genève à Jeune Afrique :

« La protection des données personnelles est un enjeu important et les outils du RAFT y font particulièrement attention. Concernant les activités de télé-expertise, notre outil utilise une infrastructure à clés publiques (PKI) qui garantit que seuls les destinataires explicites du message seront capables de le décrypter »,

Le gestionnaire de chaque centre de consultation est seul habilité à accueillir de nouveaux participants pour la télé-expertise, et est chargé de vérifier l'identité et la qualité de chaque nouveau membre du cercle de collaboration. « À ce jour, à l'issue de milliers de consultations de télé-expertise, aucun problème de sécurité concernant ces données sensibles n'a été identifié », assure le professeur.

Les hébergeurs des données sont pour le moment le plus souvent à l'étranger, mais la donne va changer.

« *Que ce soit pour l'Agence de l'informatique de l'État ou pour les opérateurs télécoms, l'installation d'hébergeurs au Sénégal va devenir inéluctable* » estime Henri Ousmane Gueye, d'Eyone.

L'épidémie de Covid-19 a mis en lumière l'absolue nécessité pour le continent de posséder des infrastructures fiables, des outils efficaces, pour faire remonter l'information le plus vite possible, s'organiser, et aider le personnel médical à soigner. **À Dakar, par exemple, sur instruction des autorités, les données concernant l'épidémie sont hébergées en locale.**

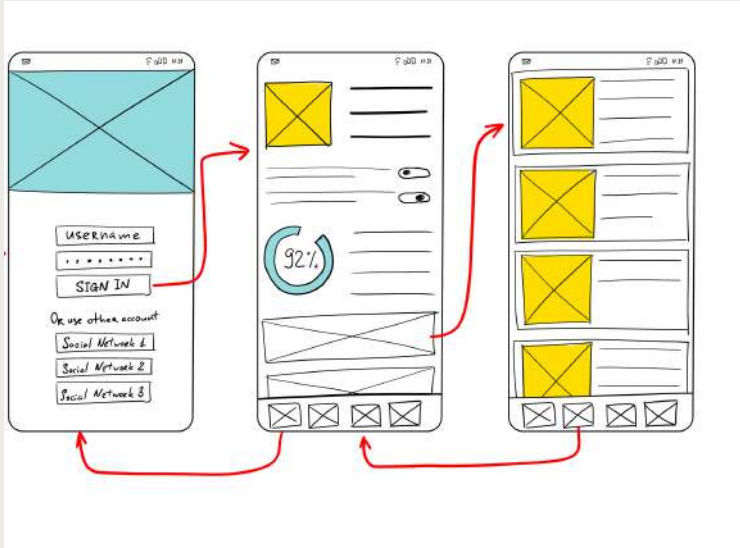
Le *leapfrog* risque de ne pas être possible dans certains pays d'Afrique avec le faible taux d'alphabétisation et les problèmes liés à l'accès à internet la santé digitale risque d'être un luxe pour certains alors qu'elle devrait être inclusive.

Dans l'attente d'encadrement spécifique, les industriels du secteur doivent veiller à se conformer aux principaux objectifs poursuivis par la réglementation relative aux données de santé et issus de la loi sur la protection des données de 2008, et donc, en particulier, à assurer la sécurité, la confidentialité et la disponibilité des données, et à respecter la volonté des personnes concernées.

5—Les bases de données et applications de dépistage, de prévention et de gestion de la pandémie mises en œuvre par le Ministère de la santé et de l'action sociale

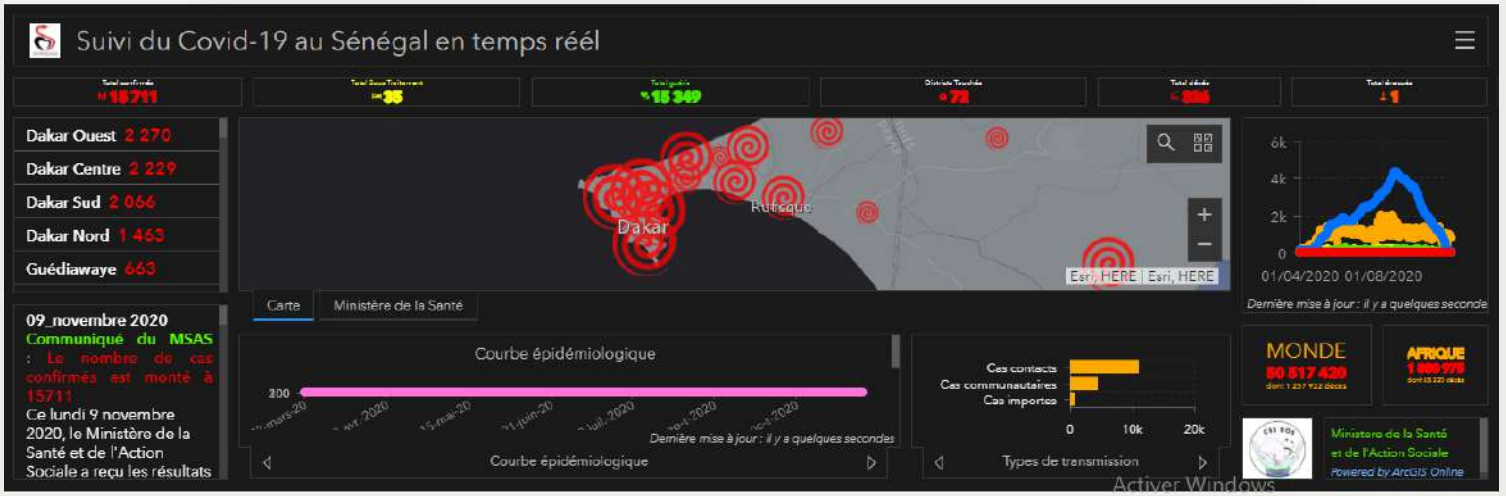
Le système d'information sanitaire DSHI2 et les applications associées

Le système d'information de santé DSHI2 permet de remonter systématiquement les données sanitaires depuis les niveaux décentralisés. Quant au module tracker, il permet de gérer et de collecter des informations nécessaires à la détermination des personnes ayant été en contact avec les personnes diagnostiquées porteuses du SARS-CoV-2 ou présentant des symptômes avérés. Sont collectées, les données d'identification (nom, prénoms, date de naissance, sexe) de la personne, le numéro d'identification nationale, l'adresse de la personne, le numéro de téléphone de la personne à contacter, les données permettant de déterminer que la personne est infectée (caractère positif du test, date des prélèvements et les résultats). Nous avons également les informations d'identification des personnes présentant un risque d'infection avec la collecte des informations relatives aux contacts des personnes infectées et, le cas échéant, la réalisation d'enquêtes sanitaires, en présence notamment de cas groupés. Ces données permettent également d'alimenter l'Application de Gestion du Dossier Médical des malades de la COVID avec les éventuelles pathologies anciennes du patient ou comorbidité.



Les données sont échangées entre les autorités sanitaires, les centres de traitement et les laboratoires d'analyse.

La gestion de l'information sanitaire est une déterminante de la performance des cases, postes, centres de santé et hôpitaux. Bref, de la politique sanitaire d'une manière plus large



6—Les bases de données mises en œuvre dans le cadre de la gestion de l'aide alimentaire en période de Covid

La crise sanitaire se prolonge en une crise économique et sociale, le ciblage des populations pouvant bénéficier de l'aide, est un outil permettant de collecter une masse de données sensibles sur les personnes cibles.

La mairie de Dakar plateau à pour son compte, mit en ligne un formulaire de collecte de données. La collecte a eu lieu à l'adresse suivante https://dakarplateau.sec.gouv.sn/formulaire .

Les données collectées sont : le nom, Prénoms, date et lieu de naissance, genre, adresse, numéro de téléphone, numéro carte nationale d'identité, numéro de la CNI CEDEAO, lieu de vote quartier de résidence, Copie CNI en recto verso (à envoyer).
Les droits des personnes ne sont pas expliqués au niveau du footer (bas de page).

6-1) le dispositif national de ciblage et d'identification des bénéficiaires du programme d'appui de résilience des ménages du Ministre du Développement Communautaire et de l'Equité Sociale et Territoriale

Il s'agit d'un dispositif permettant d'apprécier les difficultés sociales des ménages les plus vulnérables du Registre National Unique[10] (RNU) et par extension aux ménages impactés par la crise sanitaire[11] pouvant bénéficier de l'aide d'urgence.

Figurent parmi les données collectées : les données d'identification des personnes figurant dans la base nationale du RNU. A cela s'ajoute, les données de personnes retenues par les comités de sélection dans le cadre de la confection des listes d'extension des ménages en vertu des critères retenus.
En somme, des informations nécessaires pour décider de l'attribution à l'aide d'urgence.

Pour les destinataires : les comités régionaux et communaux, le Maire et les services en charge d'acheminer les aides, l'ANSD.

[10]http://www.sante.gouv.sn/sites/default/files/PROGRAMME%20D%E2%80%99APPUI%20A%20LA%20RESILIENCE%20DES%20MENAGES%20POUR%20FAIRE%20FACE%20AUX%20CONSEQUENCES%20SOCIO-ECONOMIQUES%20DU%20COVID%2019%20.pdf

[11] 1. Les ménages ne figurant pas dans le RNU (Registre national Unique) dont la liste est remise ; 2. Les ménages non bénéficiaires du PNBSF (Programme National de Bourses de Sécurité Familiale) ; 3. Les ménages sans revenu salarié fixe et/ou régulier ; 4. Les ménages dont le niveau de consommation alimentaire, les moyens d'existence et la situation nutritionnelle sont fortement affectés par les conséquences de la pandémie de Covid19.

7—Le dispositif de collecte et de traitement des données personnelles de géolocalisation à des fins de santé publique

Des dispositifs permettent le repérage des patients contaminés, des contacts, des cas communautaires et de leurs accompagnateurs dans le cadre de la gestion de l'afflux des malades du coronavirus.

Selon les sources du MSAS, il existe un système d'information général (SIG), donnant une vue instantanée de la maladie par localité. De ce fait, plusieurs données sensibles sont collectées et traitées. Il est fort probable qu'il y ait une interconnexion voire un rapprochement ou une mise en relation automatisée ou non avec d'autres applications du MSAS pour retracer les chaînes de contamination. En tout état de cause, les données de localisation, de GPS, de bornage avec un traitement du numéro de téléphone et des activités de communications électroniques et connexion internet sont susceptibles d'être collectées.

Les services du ministère de la santé, ceux du Ministère de l'intérieur (renseignement), du Ministère des Transport et les opérateurs de téléphonie peuvent travailler ensemble pour le partage des données de géolocalisation des cas en contexte de crise sanitaire.

8—Médias: la gestion de l'information en période de crise sanitaire et la lutte contre la désinformation et des fake news sans oublier les informations impactant la vie privée des citoyens.

Les plateformes numériques, bien qu'elles soient l'outil par excellence pour propager les fakenews et la désinformation, ont néanmoins prouvé qu'elles peuvent être en mesure de contrer ces infox. Facebook a essayé de limiter le nombre de partages sur WhatsApp, émetteur majeur de fakenews pendant la crise sanitaire.

Au Sénégal, dans les articles de presse en ligne, nous constatons un certain nombre de traitements des données personnelles dans la gestion de l'information avec comme finalité de satisfaire aux exigences du droit à l'information. Au tout début, concernant les premiers cas de décès, la presse en ligne n'hésitait pas à mettre à disposition du public un certain nombre d'informations sur l'identité de la défunte personne et ses antécédents médicaux. Cette presse se fait parfois aider par les proches des victimes qui, sous le choc, essaient de trouver consolation dans les réseaux sociaux en fournissant les détails du décès.

Ainsi, le grand public était informé des pathologies, éléments de comorbidité dont souffrait un patient identifié. Ce qui constitue non seulement une violation du secret médical mais aussi du droit au respect de la dignité humaine.

Pour destinataires, concernant ces données, nous devrions avoir que le ministère de la santé, le centre des opérations d'urgence sanitaire et les médecins traitants. S'agissant du droit à l'information, en application du principe de collecte minimum, il fallait juste dire à la presse que ces personnes souffraient de comorbidité. L'intérêt d'une telle démarche trouve sa justification dans la volonté de préserver aux familles de défunts d'une stigmatisation ou encore, de la connaissance par le grand public de maladies héréditaires les concernant. Ils ont encore le droit de souscrire à des assurances maladie auprès des compagnies d'assurance. Et, nous le savons, avec le Big data, la police d'assurance risque de changer.

9-La surveillance et les outils de travail à distance (administration et secteur privé).

L'alternative qu'offre le travail à distance en période de Covid19 doit être pris en compte avec comme objectif de trouver l'équilibre entre sécurité des données de l'entreprise et protection des données des salariés. Il est loisible pour les employeurs de traiter des données personnelles dans la mesure où ce traitement vise le respect des obligations légales. Ainsi, beaucoup d'entreprises ont mis en œuvre le télétravail durant cette période de la Covid 19 afin d'assurer la continuité de l'activité de manière à honorer certains engagements.

Pour ceux qui continuent le travail en présentiel, il est inconcevable que l'employeur mette en place un traitement visant à collecter des informations sur certaines pathologies (les comorbidités) susceptibles de constituer des causes aggravantes en cas d'infection au Covid19. Nous pensons à cette mesure du ministre de l'éducation nationale dispensant certains enseignants de la reprise des activités. Comment vont-ils prouver cela ? À quel niveau de la hiérarchie ces données seront collectées ? Il s'agit là des enseignants ayant des pathologies qui pourraient aggraver leur situation en cas d'infection.

Dans le cadre du télétravail[12], les données ci-après peuvent faire l'objet de traitement. Il s'agit : des logs de connexion, identifiants, l'accès aux données de connexion de l'opérateur du salarié en télétravail, le contrôle à distance de l'activité du salarié et des outils informatiques. Mettons aussi sur la balance l'épineuse question de l'activation des vidéos durant les réunions. Est-ce que l'employeur est à même d'exiger de son employé son activation ?

[12]Non prévu par le droit du travail sénégalais, il est tout de même défini par l''article L1222-9 du Code du travail français comme "Toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication". Cf. Article de Mbaye SENE : « un virus peut en cacher un autre »

Autant de questions auxquelles les salariés au Sénégal ne sont pas préparés, nombreux sont ceux qui ne demandent pas de compte en la matière. Même en entreprise, salariés, vous disposez du droit au respect de votre vie privée[13] a fortiori quand vous travaillez à domicile.

Nous avons aussi la question des habilitations, des différents niveaux d'accès pour éviter que des informations atterrissent sur l'écran d'un collaborateur non habilité. C'est ici que nous sentons l'utilité d'une charte informatique en entreprise, elle protège aussi bien le salarié que l'employeur.

Nous avons là une occasion de faire évoluer la législation du travail concernant l'usage des technologies de l'information et de la communication comme par exemple le télétravail qui doit s'accommoder avec le droit au respect de la vie privée du salarié en entreprise, ce que beaucoup de dirigeants ignorent actuellement.

[13] https://www.dakaractu.com/Un-virus-peut-en-cacher-un-autre_a186352.html https://juristicom.blogspot.com/2016/01/les-rh-lepreuve-des-tic.html

10—Focus sur les applications de traçage numérique mobile

L'utilisation des technologies d'identification en matière épidémiologique est au cœur des solutions visant à répondre au défi sanitaire de la Covid 19.

Bornage téléphonique, GPS, Bluetooth, toutes ces technologies de surveillance mobilisées pour gérer l'épidémie ont en commun de s'appuyer sur les données des téléphones mobiles pour identifier des sujets « contact » (backtracking ou contact tracing) afin :

- de retracer le parcours récent des personnes testées positives ;
- d'informer la population des zones à risque ;
- de relever directement les contacts récents entre les individus testés positifs et des personnes tierces[14]

En France, cela s'est matérialisé par le déploiement d'une application mobile dénommée STOPCOVID téléchargeable sur Apple et Android munie d'une architecture centralisée mise en œuvre dans le cadre d'une mission d'intérêt public. Le traitement de données à caractère personnel repose sur le volontariat avec le recours à la technologie Bluetooth plus le protocole ROBERT[15] reconnu comme le moins intrusif.

[14] https://blog.lefigaro.fr/bensoussan/

[15]Ce Protocole de communication partagé par sept pays européens, jusqu'à présent, s'appelle ROBERT pour Robust and privacy-preserving proximity Tracing protocol permet de garantir l'anonymat et en aucun cas utilise les données de bornage GSM ni de géolocalisation.Cf, « Contact tracing » : Bruno Sportisse

En réalité, dans tous les pays où le traçage mobile a été rendu obligatoire, cela a permis d'éviter des nouveaux cas de contamination lors des rencontres. A Singapour, l'application TRACETOGETHER a fini par montrer ses failles[16] et puis à dégénérer en une surveillance massive[17]. En Corée du Sud, les personnes testées positives et les personnes confinées – à leur domicile ou dans des centres mis en place par le gouvernement – doivent télécharger une application mobile officielle permettant aux autorités de contrôler leurs déplacements en temps réel.[18]

La crise sanitaire a montré que le numérique peut contribuer efficacement à freiner la propagation du virus toutefois, l'usage non encadré ou non maitrisée peut conduire à une surveillance généralisée où les honnêtes citoyens peuvent être tracés au moindre déplacement.

Par ailleurs, dans la délibération[19] de la CNIL, l'autorité française de protection des données personnelles sur le projet STOPCOVID avait rappelé en substance qu'au travers de cette application, il y avait un besoin de trouver un équilibre entre deux principes à valeur constitutionnelle (la vie privée et la santé publique) et selon elle, **l'analyse de la proportionnalité des données collectées en vertu du RGPD était liée à la notion d'utilité du traitement projeté dans le cadre de la stratégie de déconfinement**.
Or, en l'état actuel, au 10 juin, les autorités en charge annoncent que sur les 1,4 millions de personnes ayant téléchargé l'application[20] seulement 2% ont activé l'application avec le bluetooth et les notifications de cas positifs sont au nombre de 14.

Finalement, l'autorité française de régulation des données personnelles, a fini par mettre en demeure le Ministère de la Santé suite à de nombreuses irrégularités notées dans le cadre d'un contrôle en ligne de l'application.
Ce n'est que récemment que la CNIL a levé cette mise en demeure en considérant que l'application était désormais conforme au RGPD. Néanmoins du fait de la méfiance des Français à l'égard de l'application, conséquence du faible nombre d'activations, le gouvernement français prévoit une nouvelle version de l'application tout en rebaptisant;

[16] https://www.numerama.com/tech/622089-apres-lechec-du-stopcovid-local-singapour-passe-a-une-solution-beaucoup-plus-radicale.html
[17] https://www.letemps.ch/economie/singapour-tracage-app-degenere-surveillance-masse
[18]https://www.frenchweb.fr/coronavirus-ou-en-sont-les-applications-mobiles-de-tracage-dans-le-monde/399341#gsc.tab=0
[19]https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf
[20]https://www.lemonde.fr/pixels/article/2020/06/10/l-application-stopcovid-connait-des-debuts-decevants_6042404_4408996.html

Au Sénégal, aucune application de traçage mobile n'a vu le jour pour le moment dans le cadre de la stratégie de riposte et de semi confinement. Tout porte à croire que c'est le système de bornage et/ou de géolocalisation qui a été utilisé pour retracer des contacts « à risque » comme l'a relaté E-médias[21] le 19 avril 2020 et confirmé par les propos du ministre de la santé. Un encadrement juridique était donc requis avec le support d'un avis motivé de la Commission des Données Personnelles.

Du coté du secteur privé, dans le cadre de notre veille juridique, il nous a été communiqué que des entreprises ont développé en interne des applications de traçage mobile à destination de leurs salariés avec des directives tendant à activer le bluetooth en dehors de tout encadrement légal.

La surveillance généralisée est incompatible avec la démocratie, et le solutionnisme technologique est à relativiser pour éradiquer un fléau de ce type. Il faut donc plus de transparence dans l'utilisation des données et à fortiori de données dites sensibles pour une acceptabilité sociale générale de la part des citoyens.

[21]http://www.emedia.sn/VIDEO-LES-PARCOURS-DES-CAS-COMMUNAUTAIRES-SERONT-TRACES.html?var_mode=calcul

II- Analyse de ces dispositifs au regard de la loi sur la protection des données et des bonnes pratiques en matière d'exploitation des données personnelles.

Cette étude a été réalisée sur la base d'interviews des personnes désignées et d'observations visuelles sans aucune intervention physique sur les systèmes d'informations ou applications. Elle ne peut pas être assimilée à un audit *informatique et libertés* détaillé. Nous exploitons les informations fournies par les autorités sanitaires, les interviews, l'autorité de régulation, la presse, des informations rendues publiques par les responsables de traitements et les acteurs de l'écosystème numérique.

L'étude s'inscrit dans un cadre d'analyse délibérément international mais aussi national au travers des normes et standards de référence en la matière.

En vertu de loi 2008-12 portant protection des données à caractère personnel précité les applications, traitements énumérés comme sensibles et collectant des données personnelles reposent majoritairement sur la mission d'intérêt public des autorités sanitaires en tant que base légale et par conséquent doivent respecter les principes et obligations réglementaires de collecte et de traitement des données (minimisation, confidentialité, sécurité, anonymisation, durée de conservation limitée et respect du droit des personnes).

La gouvernance des données est aujourd'hui un enjeu stratégique pour les organisations. Il faut limiter les risques cyber et les sanctions administratives. A la base, certains systèmes d'informations composés de données et de traitements sensibles à grande échelle de la population, présentent de facto des risques en termes de sécurité et de violations des obligations légales.

Les bases de données et applications de dépistage, de prévention et de gestion mises en œuvre par le Ministère de la Santé et de l'Action Sociale.

Critères de conformité	Constats	Points d'attention
Minimisation des données	Données adéquates et pertinentes Pas de durée de conservation déterminée	Les données à caractère personnel doivent être conservées uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte. Seules les données présentant un intérêt historique, scientifique ou statistique peuvent être conservées sans limitation de durée.
Respect des droits des personnes	Pas de référence au droit des personnes.	Mettre en place une politique globale de protection des données. Prévoir une charte d'habilitation en fonction du besoin d'en connaître des professionnels de santé
Obligation de sécurité et évaluation des risques sur les droits et libertés	Niveau de sécurité : données de santé pas bien cloisonnées et absence règles d'habilitation	1- les bases de données du SI santé doivent être chiffrées ou données pseudonymisées. 2- l'accès aux données doit être tracé. 3- les transmissions (papier et électronique) doivent être sécurisées. 4- les destinataires des informations doivent être formellement identifiés. 5- le seul responsable de l'accès aux données est le médecin responsable de l'information médicale.

https://blog.lefigaro.fr/bensoussan/

Le dispositif de ciblage et d'identification des bénéficiaires du programme d'appui de résilience des ménages du ministre du Développement communautaire et de l'équité sociale et territoriale.

Critères de conformité	Risques encourus	Points d'attention
Minimisation des données	Beaucoup de données sensibles collectées avec surement par aspiration des données contenues dans d'autres bases de données (RNU), Bourse familiale CMU...	Compte tenu du contexte et de la portée du traitement, une analyse d'impacts est nécessaire en raison de la nature des données hautement sensibles. Risque de détournement de finalités et d'interconnexion de fichiers pas assez encadrée.
Respect des droits des personnes	Pas d'information délivrée dans le cadre de ce traitement.	Prévoir des engagements de confidentialité et limiter le nombre de personnes ayant accès aux données.
Obligation de sécurité et évaluation des risques sur les droits et libertés	Formulaire papier pas assez bien conservé.	Prévoir si possible une pseudonymisation.

https://blog.lefigaro.fr/bensoussan/

L'application mobile SunuCity en Développement.

Critères de conformité	Risques encourus	Points d'attention
Minimisation des données	Données de géolocalisation et pas d'information sur les partages avec des destinataires inconnus, pas de transparence sur la durée de conservation Absence de Privacy by design	Il est de la responsabilité exclusive des pouvoirs publics de collecter un certain nombre de données dont la géolocalisation
Respect des droits des personnes	Pas de rubrique informant sur les droits des personnes.	Prendre des mesures pour ne pas traiter des données incluant celles d'autres personnes sans leur consentement géolocalisation (photos)
Obligation de sécurité et évaluation des risques sur les droits et libertés	Ils sont en train de démarcher le ministère de la santé pour transférer la responsabilité de gestion. Néanmoins, pas de cloisonnement des données de santé avec les autres données dans la base. Niveau de sécurité insuffisant	Préciser les éventuels destinataires. Faire des professionnels de la santé les responsables de traitement. Toutefois, prévoir une clause de réversibilité et la purge des données déjà collectées et conservées

https://blog.lefigaro.fr/bensoussan/

Les dispositifs de télétravail

Critères de conformité	Risques encourus	Points d'attention
Minimisation des données	Enregistrement des réunions dont voix et images.	Informer les salariés pour avoir leur consentement et éviter d'exiger l'activation continue de la vidéo. L'employeur ne peut traiter que des données à caractère personnel strictement nécessaires à la satisfaction de ses obligations en matière de droit du travail ou encore de protection sociale.
Respect des droits des personnes	Pas de communication sur les droits du salarié en télétravail. Les plateformes utilisées ne garantissent pas l'effacement des données	Mettre en place une charte informatique pour clarifier les limites et possibilités pour chaque partie.
Obligation de sécurité et évaluation des risques sur les droits et libertés	Risque de transfert des données dans le Bigdata par exemple Prise de contrôle à distance et fuite de données	Ne pas outrepasser les pouvoirs de direction Fixer avec l'employeur un planning pour les activités à mener

L'œil de l'expert cybersecurité Mbaye SENE

CYBER CRIMINALITÉ ET COVID 19 : LE TÉLÉTRAVAIL ET LA PROTECTION DES DONNÉES DE SANTÉ

En l'absence d'une agence nationale de la sécurité des systèmes d'information chargée de coordonner la stratégie de cyber sécurité, d'autres entités peuvent être pour le moment sollicitées.

- **L'École nationale en cyber sécurité à vocation régionale (ENVR)** : dont le but est d'augmenter les capacités locales des États africains à lutter contre la délinquance, le terrorisme ou la radicalisation et à développer des moyens d'investigation numérique contre les cybercriminels[22].
- **La Division cyber sécurité de la police judiciaire sénégalaise** : Chargée du traitement de la cybercriminalité « classique », elle a également pour autre objectif majeur de participer à la lutte contre le terrorisme[23].

- **La Commission de Protection des données Personnelles (CDP-Sénégal)[24] : Ses missions sont, entre autres,**
  - Le contrôle et l'investigation :
    - Informe sans délai le procureur de la République des infractions dont elle a connaissance ;
    - Peut prononcer une sanction à l'égard d'un responsable de traitement pour insuffisance des mesures de sécurité.

[22] https://www.france24.com/fr/20181107-afrique-senegal-dakar-le-drian-kaba-envr-ecole-renforcer-lutte-cybercriminalite
[23] https://www.jeuneafrique.com/449560/politique/senegal-police-emploie-grands-moyens-cybersecurite/
[24] https://www.cdp.sn/content/cadre-institutionnel

Dans un contexte de Covid 19, comment assurer la continuité d'activité d'une économie de plus en plus numérisée tout en garantissant la disponibilité, l'intégrité et la confidentialité des données qui en sont le principal gisement de valeur ?

Face à la numérisation des données de santé liées à l'épidémie, comment garantir une stricte confidentialité de ces données proportionnellement à leur sensibilité, quelles règles de sécurité établir et quelle réflexion éthique mener pour accompagner cette mutation ?
Comment pourrait-on renforcer la participation des instances nationales précitées dans un contexte de Covid 19 ?

En traitant de manière complémentaire les innovations technologiques sous le prisme de la cybersécurité, cette présente contribution, par une approche globale et intégrée, permet d'appréhender tous les enjeux de sécurisation et de contrôle de l'information véhiculée par les systèmes d'information et formule des recommandations pour la période post Covid.

1.Télétravail

Le confinement avec son lot de loisirs numériques, la dématérialisation de l'administration, l'éducation à domicile et le télétravail ont amplifié nos interactions avec nos appareils connectés d'une manière exponentielle. Le 10 Mars 2020, DE-CIX, le plus gros point d'échange Internet mondial, situé à Francfort a enregistré un pic de consommation de bande passante à 9,1 térabits par seconde, record mondial enregistré avec un trafic de 12 % supérieur au précédent pic du même point d'échange[25]. Dans le même sillage, Akamai dont le réseau internet mondial est composé de plus de 100 000 serveurs a mesuré une hausse du trafic de l'ordre de 30 % lors du confinement.

Cette amplification de nos interactions avec nos appareils connectés est allée jusqu'à susciter des questionnements sur la résistance du réseau en cas de fortes sollicitations (ce qui n'est pas le sujet dans cette partie) ; mais pose également la question sur les comportements de sécurité à adopter pour éviter que nos données soient exposées, volées ou divulguées.
Le croisement des données de localisation de notre téléphone ou de notre ordinateur, de l'historique de notre circulation sur le net, de nos contacts, des écrits dans notre messagerie et sur les réseaux sociaux (Facebook, Instagram, WhatsApp, Twitter...) et les détails de nos transferts financiers donne une image complète sur qui nous sommes[26].

Donc si on est d'accord avec Nicolas Apargian que les services numériques qu'on utilise au quotidien sont des mémoires exhaustives des faits et gestes de notre vie personnelle et professionnelle; on comprend facilement que le télétravail n'est pas la potion magique du druide panoramix mais doit concomitamment être accompagné de mesures techniques et organisationnelles de sécurité.

[25] https://www.lesnumeriques.com/vie-du-net/coronavirus-internet-la-consommation-de-bande-passante-explose-nouveau-record-atteint-n148403.html
[26] Nicolas Arpagian, Que sais-je ? La Cyber sécurité, p6

Qu’est-ce que le télétravail ?

Le télétravail renvoie à toute forme de travail à distance s'effectuant notamment via une connexion internet permettant à chaque collaborateur d’accéder régulièrement et via plusieurs types de supports possibles (Pc, smartphone, tablette…) aux informations sensibles, stratégiques et confidentielles d’une entreprise, d’un état ou d’une institution administrative et hospitalière, d’une organisation, selon les cas.

Nous avons notamment vu le Président de la République tenir son conseil des ministres en vidéoconférence lors de la période de confinement. Pourtant nous voyons aussi la complexité que cela peut engendrer : plusieurs protocoles de communications, avec autant de vulnérabilités potentielles et de risques à gérer, **plusieurs types de périphériques avec des moyens d’authentification variés et pas toujours d’un niveau de sécurité équivalent.**

Selon Bleeping computer, l’application de vidéo conférence Zoom, un des leaders du domaine, qui a connu un succès fulgurant en mars en raison de la généralisation du télétravail et du respect de la distanciation sociale, connait une énorme faille de sécurité : en convertissant une adresse en un lien cliquable destiné aux autres participants, Zoom envoie aussi votre nom d’utilisateur et votre mot de passe,
qui peuvent être piratés en quelques secondes à l’aide d’un logiciel gratuit comme Hascat[27].

[27] https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

Un hacker aurait donc tout loisir d'intercepter vos identifiants et pirater votre compte. La faille touche toutes les versions de Windows, qu'il s'agisse de Windows 10, Windows 8.1, Windows 7.

Depuis, la société a résolu le problème et publié un correctif vendredi 10 juillet, avec les notes de version 5.1.3 (28656.0709) indiquant que le correctif « corrige un problème de sécurité affectant les utilisateurs exécutant certaines versions de Windows ».

Aussi, selon Jérôme Notin, Directeur Général du site cybermalveillance.gouv.fr *«les tentatives malveillantes ont été multipliées par 10 avec le télétravail..., avec plus de 400% d'augmentation de tentatives d'hameçonnage constatées* ».

Il y a cinq fois plus de cyberattaques que d'habitude, selon l'éditeur de logiciels antivirus Bitdefender, et trois fois plus d'arnaques par email utilisant les mots "covid-19" et "coronavirus" au cours de la dernière semaine de mars, selon la société Sophos[28].

En réalité, le télétravail, même s'il permet de gagner en efficacité et en productivité et de nous adapter à ce contexte de confinement, augmente le risque qui nous expose à des menaces différentes sur la sécurité de nos données.

Des facteurs tels que l'hétérogénéité des supports informatiques et des périphériques, le manque de culture en cybersécurité de certains collaborateurs et l'anxiété liée au contexte, augmentent considérablement les vecteurs d'attaque (ransomware, social engineering, phishing etc.).

Le télétravail soulève également plusieurs questions de sécurité tant pour les équipements appartenant à tout type d'organisation (État, institutions administratives et hospitalières, entreprises) que pour les **BYOD (Bring Your Own Device :équipement personnel de communication)** :

[28] https://www.francetvinfo.fr/replay-radio/nouveau-monde/nouveau-monde-les-cyber-escrocs-surfent-sur-la-vague-du-coronavirus_3869203.html

- Quel pourrait être le contrôle sur un périphérique n'appartenant pas à l'organisation mais qui contiendrait des données de l'organisation ?

- Quel pourrait être le contrôle de l'organisation sur un équipement qui ne suivra pas les standards de sécurité de l'entreprise mais qui utilisera les protocoles de connexions et d'authentification en accord avec la politique de l'organisation ? *tentatives d'hameçonnage constatées* ».

- Quel pourrait être le contrôle de l'organisation sur le vol de ce type d'équipement qui contient un mot de passe pour l'accès à des services stratégiques ?

- L'utilisateur pensera-t-il déclarer le vol d'un objet qui lui appartient pour que des mesures de fermeture de son compte d'accès soient prises immédiatement ?

- Comment gérer les mises à jour des équipements à distance, l'installation de logiciel par les utilisateurs, la sécurité physique de l'environnement de télétravail, la sécurité du point d'accès wifi utilisé et le patch si une nouvelle vulnérabilité est publiée ?

- Répondre à ces questions suppose dès lors de prendre au préalable des mesures concrètes et des solutions techniques de sécurité avant toute mise en place d'un dispositif de télétravail[29]:

- **Former et sensibiliser les collaborateurs** à l'hygiène informatique et aux risques liés au télétravail, afin de limiter les attaques et leurs impacts pour chaque support PC, tablette et smartphones, professionnels ou personnels et selon chaque type d'attaque (virus, malware, hameçonnage, rançon, Cheval de Troie, brute force…)

[29]https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

- Intégrer le télétravail dans votre politique d'organisation (PSSI, PLS…)
- **Réaliser l'inventaire des activités des utilisateurs compatibles** avec le télétravail
- **Catégoriser les télétravailleurs** selon les principes du moindre privilège et du besoin d'en connaitre (qui a accès à quoi ? quel est son métier ? quel est son statut (admin,user) ? pour quel besoin ?
- **Maitriser la gestion des télétravailleurs** (révocation des comptes et des droits d'accès au SI, changement de catégorie de l'utilisateur nomade ; la gestion des équipements mobiles et des logiciels qu'on peut y installer)
- **Mettre en œuvre des moyens de protection physique des équipements de télétravail** (filtre écran de confidentialité, des scellés pour identifier une éventuelle compromission matérielle ; des verrous de ports USB et RJ45 si nécessaire ; éventuellement un câble antivol à la maison).
- **Renforcer la sécurité des supports informatiques** (mise à jour régulière des antivirus, des OS, des applications, des backups, gestion "durcie" des identifiants et mots de passe : MFA, gestionnaire de mot de passe), limiter l'usage de périphériques externes pour échanger des données (clés USB, disques durs, fichiers partagés, port FTP…)
- **Dissocier et protéger les appareils : attribuer au télétravailleur un PC à usage strictement professionnel ou exclure certaines applications bureau (ex. messagerie, compta) sur les PC maison.**

2 LA SECURITE DES DONNEES DE SANTE DANS UN CONTEXTE COVID

La pandémie Covid19 a renforcé au Sénégal et partout dans le monde l'utilisation et l'émergence d'applications connectées, de dossiers médicaux partagés et dématérialisés et de dispositifs médicaux connectés en vue d'aider les acteurs publiques et médicaux à mieux cartographier et circonscrire l'épidémie.

Par exemple, en France, l'application Stop Covid permet de prévenir les personnes qui ont été à proximité d'une personne testée positive, afin que celles-ci puissent être prises en charge le plus tôt possible.

Sunu city au Sénégal permet d'envoyer et de recevoir des informations sur les incidents Covid, les risques sanitaires avec une possibilité de géolocalisation.

Toutefois, dans un article intitulé « les données de santé, le nouveau continent de valeur [30]» ,Le Big four Ernest Young souligne que les données de santé constitue « le nouveaux gisement » de valeur avec un fourmillement d'intérêt sans précèdent des grandes entreprises tel que **Google** par sa filiale Verily (traitement des patients et médecine de précision) , Amazone (l'assurance santé) , Microsoft (Machine Learning pour vaincre le cancer) , Alibaba (identification des médicaments contrefaits).

Ce regain d'intérêt pour les données de santé n'est pas l'apanage des grandes firmes internationales. La tendance actuelle du Dark Web est la vente d'informations de santé protégées ou PHI en anglais (Protected Healh Information). Il s'agit de données extraites illégalement d'hôpitaux, de cliniques et d'autres établissements de soins de santé par des pirates informatiques qui profitent des faiblesses de leur cyber sécurité[31].
Les PHI en vente sont généralement constitués de numéros de sécurité sociale, des dates de naissance, des diagnostics, des prescriptions de médicaments, des procédures médicales et les résultats médicaux, et dans certains cas des informations financières ou des données de personnes décédées...

[30]https://questionsdetransformation.ey.com/dossiers/les-donnees-de-sante-nouveau-continent-de-valeur_f-60.html
[31]https://www.infohightech.com/les-tendances-sur-le-piratage-des-donnees-medicales-dans-le-dark-web/

Selon Znet, les données de santé se vendent à des prix d'or sur le Dark Web. Par exemple, un pirate qui se fait appeler "thedarkoverlord" a mis en vente d'énormes bases de données d'adhérents américains à des assurances médicales pour un million de dollars de Bitcoin[32]. Le prix des données de santé dans le Dark web a considérablement augmenté depuis et fait des établissements public de santé, l'une des cibles privilégiées par les pirates informatiques.

Les données de santé sont particulièrement sensibles en ce qu'elles permettent d'identifier une personne sur des éléments précis et privés. La sécurisation des données de santé est d'autant plus importante qu'il ne s'agit pas que d'assurer uniquement la confidentialité, mais également la santé des patients. Une intrusion, qui induirait une modification de données médicales, peut, par effet de circonstances, mettre en danger la vie d'un patient.[33]

La sensibilité des données de santé les expose à des risques cyber nombreux et variés qu'il convient de prendre conscience avant toute collecte d'information et en cas de stockage et de traitement de ces informations des patients du Covid.

[32] https://www.zdnet.com/article/hacker-advertising-huge-health-insurance-database/
[33] https://healthcare.orange.com/fr/dossiers/securite-des-donnees-de-sante/

Parmi ces risques on peut citer :

- L'accès non autorisé ou une modification non désirée des données du patient Covid (avec ses effets sur le traitement du patient : modification de la dose à administrer, modification des parties symptomatiques du corps à soigner, administration de médicaments allergiques pouvant aller jusqu'à la mort du patient etc…)
- La divulgation des données personnelles de santé (les symptômes et la maladie dont souffre la personne avec son lot de stigmatisations et ses effets sur le morale du patient
- La vente des données personnelles de santé et l'exploitation de ces données (profiling, publicité ciblée…)

Les recommandations en termes de bonnes pratiques cyber sont, entre autres, les suivantes :

- La sensibilisation des médecins et tous les intervenants de la chaine de traitement sur la sensibilité des données de santé et les risques de sécurité encourus.
- La séparation des données par le cloisonnement logique ;
- Le contrôle strict des accès aux données avec les principes du « *need to know*», MFA, IAM
- Le principe du « Data minimization » est également applicable lors du recueil des données des patients ;
- Réaliser régulièrement une revue des comptes ;
- **Stocker les données de santé dans des serveurs à sécurité renforcée (hardenning) ou chez un provider certifié HDS ;**
- -Mettre en place un plan de conformité aux recommandations des standards tel que HDS, ISO 27001 et du RGPD sur les données de santé, la PGSSI-S.

3.Rôle des instances nationales de cyber sécurité dans un contexte Covid

Le Sénégal a franchi un cap dans la transformation numérique des
pans entiers de secteurs d'activités vitales à l'économie du pays.
Cette mutation des secteurs d'activités tels que la santé vers « **le tout numérique** » n'est pas sans risque et doit se faire concomitamment à **l'implémentation des mesures de cyber sécurité à chaque étape du processus.**
Plusieurs instances chargées d'intervenir sur des sujets sporadiques en lien avec la sécurité informatique existent (CDP...), **mais il n'existe pas un cadre global d'harmonisation de lutte contre les menaces cyber.**
La première recommandation serait de fluidifier la communication entre les différentes instances de décision et de standardiser et d'harmoniser leurs rôles et missions dans la gestion du Covid 19

quelles recommandations de sécurité font-elles sur le télétravail ? Quelles sont les rôles de chacune des instances et quel est leur niveau d'intervention et d'habilitation en cas de fuite de données personnelles de santé ? Comment se transmettent les informations sanitaires ? Comment et qui sensibilise les médecins et les autres acteurs des risques numériques ? Où sont stockées des données de santé Covid et quelles sont les mesures renforcées de protection mises en place ? Pour quelles durées sont stockées les informations sanitaires et comment elles sont éliminées?). Toutes ces questions doivent être posées et résolues.
L'érection d'une instance chargée d'accompagner et de
sécuriser le développement numérique serait vitale pour renforcer la résilience du pays aux cyber menaces.

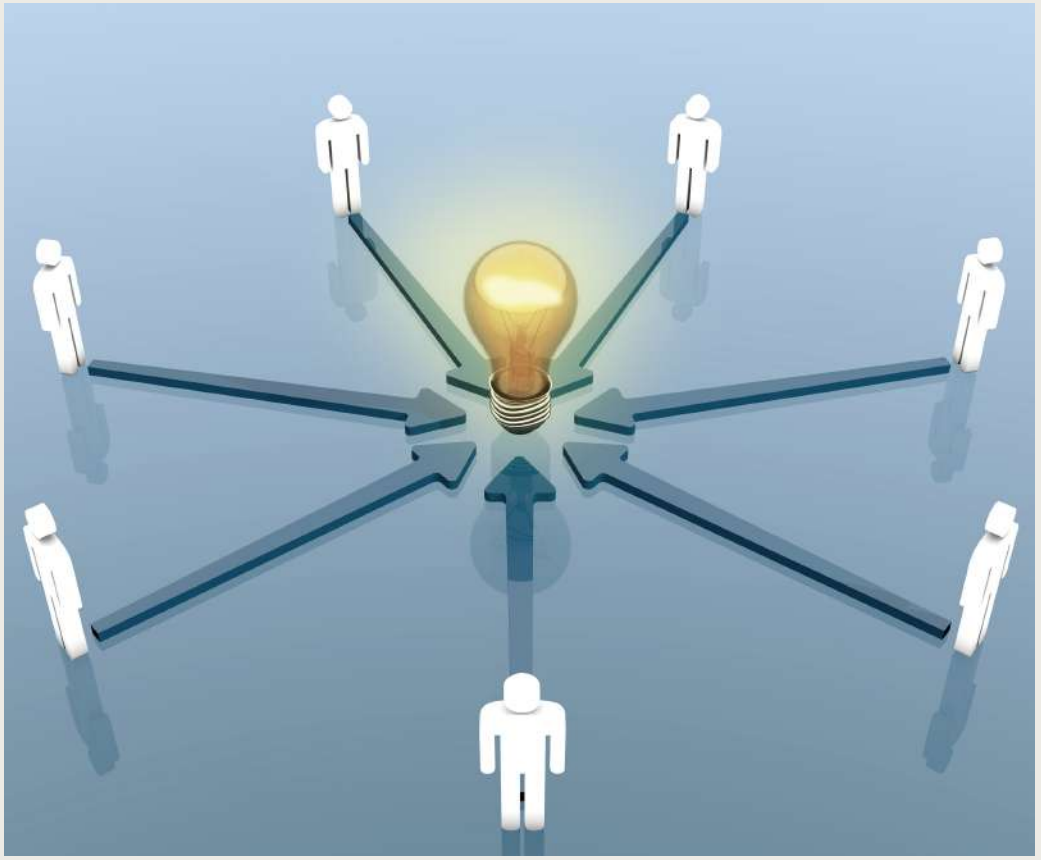
[31]https://www.infohightech.com/les-tendances-sur-le-piratage-des-donnees-medicales-dans-le-dark-web/

Cette instance pourrait venir en support à l'Agence de l'Informatique de l'Etat dans sa mission de digitalisation des secteurs d'activité de l'économie du Sénégal. Elle pourra avoir, entre autres, comme mission, d'apporter une expertise et une assistance technique aux administrations publiques et aux entreprises du Sénégal dans la sécurisation de leurs systèmes d'informations. **Elle permettra également de cartographier les secteurs d'activités d'importance vitale en vue d'un renforcement de la sécurité des systèmes d'information critiques du Sénégal avec des mesures de sécurité spécifiques et renforcées.**

Cette instance pourra aussi mener une réflexion sur la souveraineté numérique du Sénégal et de l'Afrique de manière globale ainsi que du déploiement de la Convention de Malabo et des différentes directives et règlements étatiques au niveau des administrations publiques.

Dans ce contexte de digitalisation des données de santé, la création d'une instance numérique de gestion et de protection des données santé en vue de créer les conditions du développement et de la régulation du numérique en santé, de promouvoir la sécurité au profit des professionnels et des usagers et d'assister les pouvoirs publics dans la conduite de projets numériques pourrait être utile. Nous avons l'exemple de l'agence numérique de la santé anciennement appelé l'ASIP Santé en France. Cette instance pourra également avoir comme mission **de mettre en place des référentiels régaliens nécessaires à la digitalisation du secteur de la santé telle qu'une politique nationale de sécurité des systèmes d'informations de santé. Elle pourra accompagner les établissements hospitaliers du pays dans leur transformation numérique.**

III- CONCLUSION



En définitive, ce livre blanc est un début d'analyse réalisé sur la base d'informations mises à la disposition du public. Il a permis opportunément de faire une réelle **analyse de l'impact des traitements des données personnelles sur les libertés individuelles et particulièrement sur la vie privée.** La période Post Covid19 sera jalonnée de défis à relever et des disruptions nécessaires qui devront prendre en compte la question de la maîtrise de nos données personnelles. Cette maitrise ne se fera pas sans une prise de conscience citoyenne des enjeux du numérique.

Le rôle de la Commission de Protection des données personnelles (CDP) sera d'aider à mettre fin aux traitements qui avaient pour finalité la gestion de la Covid et l'accompagnement des structures sanitaires qui, au-delà de cette crise sanitaire, sont naturellement des coresponsables des traitements des données de santé dites sensibles. Elle aura la lourde responsabilité de sauvegarder voire **rétablir l'équilibre entre le droit à la santé et le respect de la vie privée sous le prisme des technologies** dans un contexte où le gouvernement à travers le ministère de la santé compte moderniser son secteur avec le Plan Stratégique Santé Digitale 2018-2023. L'encadrement du numérique dans le secteur de la santé va permettre entres autres de rendre plus effective la télémédecine sous le support des dossiers médicaux électroniques avec un système d'agrément des hébergeurs de données de santé.

Le contrôle citoyen dans la gouvernance globale du numérique s'avère donc nécessaire afin de stimuler les réflexions des gouvernements confrontés à des configurations sans cesse renouvelées.

De manière plus générale, le dispositif de protection des données personnelles ne permet pas assez de protéger la vie privée des sénégalais face aux nouveaux usages du numérique. Dans les autres pays francophones, bon nombre de lois ont été inspirées de celle de la France datant de 1978, laquelle a été modifiée voire amendée à plusieurs reprises jusqu'après même l'entrée en application du Règlement Général sur la Protection des Données (RGPD). Les interrogations sur la pertinence du cadre juridique actuel ont pour toile de fond un environnement technologique, économique et social dans lequel la circulation des données personnelles s'est généralisée sans que les individus puissent la maîtriser[34]...

Tout de même, afin d'éviter le piège qui consiste à vouloir légiférer à chaque innovation, et comme rappelé par certains auteurs[35], des concepts axés sur la méthodologie comme le Privacy by design, by default ainsi que l'analyse de risque permettent, a minima, d'anticiper les nouveaux usages du numérique en termes de sécurité et de confidentialité.

[35] http://www.osiris.sn/Rokhaya-Sarr-Pape-Fode-Drame.html reprenant in extenso l'article de MaitreRokhaya Sarr & Pape Fodé Dramé. (Source : Revue africaine de sciences politiques,UGB n° 26, mars 2020, p. 167-176)

[34] La loi Informatique et libertés est-elle dépassée ? RFDA, 2015 p. 99 Laurent Cytermann, Maître des requêtes au Conseil d'État.

GLOSSAIRE

Par données à caractère personnel, il convient d’entendre : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d’identification ou à un ou plusieurs éléments qui lui sont propres. Autrement dit : données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Pour déterminer si une personne est identifiable, il convient de considérer l’ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable de traitement ou tout autre personne.

Par traitement de données à caractère personnel, il convient par ailleurs d’ entendre : « toute opération ou tout ensemble d’opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l’enregistrement, l’organisation, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l’interconnexion, ainsi que le verrouillage, l’effacement ou la destruction. En d’autres termes, par traitement, il faut entendre comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Le responsable de traitement : est sauf désignation expresse par les dispositions légales ou réglementaires relatives à ce traitement la personne, l'autorité publique ou privée, le service ou l'organisme qui détermine ses finalités et ses moyens.
L**es données biométriques :** sont les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Par traitement de données biométriques, il s'agit des traitements automatisés comportant des données biométriques nécessaire au contrôle de l'identité des personnes. Il peut s'agir, des dispositifs de contrôle d'accès physique ou logique qui reposent sur la collecte de l'empreinte digitale ou des réseaux veineux du doigt.

Le responsable de traitement : est sauf désignation expresse par les dispositions légales ou réglementaires relatives à ce traitement la personne, l'autorité publique ou privée, le service ou l'organisme qui détermine ses finalités et ses moyens.

Le sous –traitant : est un prestataire de services qui agit pour le compte du responsable de traitement et est tenu à une obligation d'assurer la sécurité et la confidentialité des données personnelles qui lui sont confiées par son donneur d'ordres.

L**a Pseudonymisation :** est le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.
Des données sont anonymisées: si tous les éléments identifiants ont été supprimés d'un ensemble de données à caractère personnel. Les informations ne doivent plus contenir aucun élément qui soit susceptible, au moyen d'un effort raisonnable, de servir à réidentifier la ou les personnes concernées. Lorsque des données ont été correctement anonymisées, elles ne sont plus des données à caractère personnel.

Le profilage : est toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Le fichier : est tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Le tiers : est une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

Le consentement de la personne concernée : est toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

La violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Par données génétiques, on entend par les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Le Cloud Computing ou nuage informatique : est une technologie permettant de délocaliser des données n’importe où dans le monde et de bénéficier des services ou applications informatiques en ligne.

Le Big data : est un ensemble de données volumineux traitées et analysées à des fins le souvent prédictives.

La vidéosurveillance : est un système composé d’une ou de plusieurs caméras installées à l’intérieur et ou à l’extérieur d’un local, dans un espace public ou privé, pour surveiller en vue de capter des images et ou des sons.

La géolocalisation : est un système permettant de collecter des informations sur une personne ou sur un objet à l’aide de leurs coordonnées géographiques.

Les réseaux sociaux : sont des technologies qui permettent de mettre en relation des personnes en fonction de leur centre d’intérêt commun ou dans le cadre professionnel.

L’internet des objets : désigne la connexion desdits objets au réseau internet en vue de récupérer, stocker, transférer et traiter des données collectées auprès des utilisateurs ou de leur environnement.

L'algorithme: est une suite d’instructions exécutées par une machine en vue d’un résultat donné. C’est une formalisation de la solution à un problème à l’aide d’une suite d'opérations élémentaires (lecture, écriture, itération, schémas conditionnels).

L’e-santé (ou santé numérique) fait référence à « l’application des technologies de l’information et de la communication (TIC) à l’ensemble des activités en rapport avec la santé ».

Un « PIA » (Privacy Impact Assement) est un outil de gestion de risque à disposition du responsable de traitement ou du correspondant « Informatique et Libertés » dont l’objectif est d’analyser l’impact en termes de protection de la vie privée des personnes concernées d’un nouveau projet informatique.

La violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

IV—ANNEXE

La loi sénégalaise sur la protection des données à caractère personnel du 25 janvier 2008 ;

L'acte additionnel de la CEDEAO du 16 février 2010 relatif à la protection des données à caractère personnel, qui est d'application directe dans les Etats membres de la communauté ;

La Convention de Malabo du 27 juin 2014 sur la cyber sécurité et la protection des données à caractère personnel

La convention N° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dont le Sénégal est parti ;

Le Règlement européen sur la Protection des Données 2016/679 du 27 avril 2016

V—Webographie et Bibliographie

www.cdp.sn
www.jo.gouv.sn
https://www.cndp.ma/fr/
www.cnil.frhttps://ico.org.uk/
https://www.privacy.org.nz/
https://www.ge.ch/ppdt/bureau/presentation.asp
www.socialnetlink.orgwww.jeune-afrique.com
www.ephata.sn
www.asutic.org
www.seneplus.com
www.osiris.snhttps://juristicom.blogspot.com/
www.emedia.sn
https://public.flourish.studio/visualisation/2241702/ (l'outil du MIT pour surveiller les applications de traçage numérique.)
BRULET (V.), Règlement européen sur la protection des données, textes, commentaires et orientations pratiques, 2e éd., 2018, Larcier.
FERAL-SCHUHL (C.), Le droit à l'épreuve d'internet, 7 éd., 2018-2019, Dalloz.
TOURE (A.), L'influence des nouvelles technologies dans l'administration de la justice pénale, 2017, Dalloz.
ARPAGIA, (N), La cyber sécurité, collection « que sais-je ?», Puf, Paris 2010.
DESGENS-PASANAU (G): La loi informatique et liberté, édition LexisNexis 22/08/2012, 294 pages
QUEMENER, (M), Le droit face à la disruption numériques, Gualino, 2018, 360 pages

THESES CONSULTEES

SARR Rokhaya, avocate à la Cour d'Appel de Paris, Auteure d'une thèse sur l'impact du RGPD sur la pratique des entreprises établies en France et au Sénégal soutenue en 2019 à l'UCAD

DIOUF Jean Baptiste, Docteur en droit et auteur d'une thèse intitulée : La protection des données a caractère personnel : un nouveau défi de sécurité juridique soutenue en Dec 2019 à l'UCAD.

REMERCIEMENTS

El hadj Abdoulaye SECK
Emmanuel SAMBOU
Iphigénie NDIAYE
Mohamed DIOP
Alioune TINE
Val Samuel Hodonou
Manou Emma
Bernadette Coly
Jean Michel Niane
Michel Sarr
(WA MBED MI) (EPHATA) APAC (Association Panafricaine pour la Cybersécurité) (FAGARU NGUIR MUCC CI COVID)

Mbaye SENE
Maître Rokhaya Sarr
Balla CISSE
Dr Boubacar DIAME
Charif ASSADILAH
Abdou FLEUR
Momoya SYLLA
Aboubacry WADE
Kaoussou Thierry BASSENE
Basile NIANE et l'équipe de SocialNetlink
Mouhamed Ndiaye BOCOUM

conception réalisation

DIALOB VISION
www.diamoral.com/dialobvision