AFRIQUE ADVISORS

PROTECTION DES DONNÉES DE SANTÉ AU MAROC EN TEMPS DE PANDÉMIE DE COVID-19

En cette période de crise sanitaire mondiale, de nombreuses mesures envisagées par les pouvoirs publics ou par des organismes privés pour permettre d'endiguer la propagation du virus Covid-19 au Maroc voient le jour.

Parmi ces mesures figurent notamment l'annonce du déploiement national d'une application mobile de traçage des contaminations ainsi que diverses actions envisagées par les employeurs pour assurer la sécurité et la santé au travail, dans le contexte de multiplication récente des foyers de contaminations dans le secteur industriel.

Dans la mesure où elles impliqueront la collecte et le traitement de données personnelles, notamment de données de santé, et qu'elles font émerger un risque accru d'atteinte à la protection de ces données et au respect de la vie privée, ces deux types de mesures suscitent de nombreux débats et interrogations pour lesquels quelques éclairages sont proposés dans le cadre de la présente étude.

Laila Slassi

Amélia Marques

#SpecialAdvisoryUnit
Cybersecurity & Data Protection
Avril 2020

SOMMAIRE

En raison de leur appartenance à une catégorie particulière de données personnelles, les données relatives à la santé bénéficient d'une protection accrue. Leur collecte et traitement doivent être réalisés en conformité avec des principes généraux de nature constitutionnelle et légale.

La Commission Nationale de Contrôle de la protection des Données à caractère Personnel (« CNDP ») a eu l'occasion de se prononcer sur les principes essentiels à respecter par la future application marocaine de traçage des contaminations afin de concilier crise sanitaire, protection des données personnelles et confiance numérique. Elle a également attesté de la conformité de l'application de traçage des déplacements des automobilistes déployée par la Direction Générale de la Sûreté Nationale (« DGSN ») et a clarifié les modalités à respecter pour la prise de température, en vue de l'accès au lieu de travail, pendant la durée de l'état d'urgence sanitaire. Ces prises de positions rapellent l'importance des enjeux soulevés par ces technologies et pratiques nouvelles et la nécessité d'une conformité accrue avec le cadre réglementaire existant.

En raison de l'impact potentiel des différentes mesures envisagées au niveau national sur la protection des données personnelles et le respect de la vie privée, une analyse approfondie de leur compatibilité juridique avec la législation en vigueur en matière de protection des données personnelles s'avère opportune.

A l'occasion de cette étude, certaines recommandations en vue de trouver le juste équilibre entre gestion de crise, impératifs sanitaires et protection du respect de la vie privée et des données personnelles seront formulées.

1. Principes généraux applicables aux données de santé

La protection des données de santé est régie par des principes généraux de nature constitutionnelle et législative.

Celle-ci est également renforcée par des sanctions pénales.

1.1. Protection de nature constitutionnelle

Les données relatives à la santé relèvent de la sphère de la vie privée de chaque individu et sont, de ce fait, protégées au titre du droit au respect de la vie privée, consacré par l'article 24 de la Constitution du Royaume selon lequel : « Toute personne a droit à la protection de sa vie privée ». L'atteinte à ce droit est sanctionnée notamment par l'article 447-2 du Code pénal marocain.

1.2. Protection renforcée des données de santé

Par principe, toute information relative à la santé physique ou mentale d'une personne (ex : information sur l'état de santé, résultats d'examens médicaux, antécédents médicaux, traitements, dossier médical, motifs d'un arrêt maladie, etc.) constitue une donnée à caractère personnel dite « sensible », soumise principalement aux dispositions du Dahir n°1-09-15 du 22 Safar 1430 portant promulgation de la Loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (« Loi n°09-08 ») et du Décret n°2-09-165 du 25 Joumada I 1430 pris pour l'application de la Loi n°09-08 (« Décret n°2-09-165 »).

Une fois la qualification de données de santé retenue, un régime juridique particulier justifié par la sensibilité des données en cause s'applique. Ainsi, en principe, le traitement des données sensibles est soumis au consentement de la personne concernée et à l'autorisation préalable de la CNDP.

D'une part, selon l'article 4 de la Loi n°09-08, le traitement des données personnelles est subordonné au consentement non équivoque, c'est-à-dire libre, spécifique et informé, de la personne concernée pour le traitement envisagé. Le responsable est donc tenu d'attendre que la personne concernée ait consentie avant de procéder au traitement des données. Le consentement est donc le garant du respect de la vie privée.

" Les données relatives à la santé relèvent de la sphère de la vie privée de chaque individu et sont, de ce fait, protégées au titre du droit au respect de la vie privée, consacré par l'article 24 de la Constitution "

“ En principe, le traitement des données sensibles est soumis au consentement de la personne concernée et à l’autorisation préalable de la CNDP ”

Le consentement n’est toutefois pas exigé si le traitement est nécessaire notamment :

- « au respect d’une obligation légale à laquelle est soumis(e) la personne concernée ou le responsable du traitement » ;

- « à la sauvegarde d’intérêts vitaux de la personne concernée, si elle est physiquement ou juridiquement dans l’incapacité de donner son consentement » ;

- « à l’exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées » ;

- « à la réalisation de l’intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l’intérêt ou les droits et libertés fondamentaux de la personne concernée ».

Il est intéressant de noter qu’en février 2020, le Tribunal administratif de Rabat, statuant en référé, dans une affaire concernant la mention de données de santé sur l’attestation de travail d’une fonctionnaire, destinée à être communiquée à un tiers, a jugé qu’une telle mention, sans le consentement de la personne concernée, constituait une atteinte à ses données sensibles et donc une violation de la Loi n°09-08.

D’autre part, selon l’article 21 de la Loi n°09-08, le traitement des données sensibles est subordonné à l’obtention d’une autorisation préalable. Elle peut être prévue par la loi ou, à défaut, être accordée par la CNDP notamment dans les cas suivants :

- en cas de consentement exprès de la personne concernée ou lorsque le traitement des données est indispensable à l’exercice des fonctions légales ou statutaires du responsable du traitement ;

- lorsque le traitement est nécessaire à la défense d’intérêts vitaux de la personne concernée et si elle se trouve dans l’incapacité physique ou juridique de donner son consentement.

Par dérogation, l’article 22 de la Loi n°09-08 dispose que le traitement des données de santé est subordonné à une simple déclaration à la CNDP lorsqu’il a notamment pour seule finalité : « la médecine préventive, les diagnostics médicaux, l’administration de soins ou de traitements ou la gestion

des services de santé et qu'il est effectué par un praticien de la santé soumis au secret professionnel ou par toute autre personne également soumise à une obligation de secret ».

En somme, si le traitement est mis en œuvre par des professionnels de santé, tenus au secret professionnel, aux fins médicales précitées, une simple déclaration auprès de la CNDP suffit.

1.3. Opération de traitement encadrée

La notion de « traitement » est largement définie par la Loi n°09-08 et couvre plusieurs types d'opérations. Il s'agit de toute opération effectuée ou non à l'aide de procédés automatisés et appliquée à des données à caractère personnel, telles que : 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 toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction[1].

En vertu de l'article 3 de la Loi n°09-08, les principes suivants s'appliquent au traitement de toute donnée personnelle : le principe de finalité du traitement (déterminée, explicite et légitime), le principe de proportionnalité et de pertinence du traitement, le principe de traitement loyal et licite des données, le principe de durée limitée de conservation des données.

Ensuite, selon l'article 5 de la Loi n°09-08, toute personne sollicitée directement, en vue d'une collecte de ses données personnelles, doit être préalablement informée de manière expresse, précise et non équivoque, sauf si elle en a déjà eu connaissance, des éléments suivants : identité du responsable du traitement, finalités du traitement, destinataires des données, caractère facultatif ou obligatoire des réponses aux questions, existence d'un droit d'accès et de rectification des données la concernant, caractéristiques du récépissé de la déclaration ou de l'autorisation délivrée par la CNDP.

La mise en œuvre d'un traitement des données de santé en lien avec la crise sanitaire liée au virus Covid-19 devra donc également tenir compte de ces principes généraux.

« Les principes suivants s'appliquent au traitement de toute donnée personnelle : le principe de finalité du traitement, le principe de proportionnalité et de pertinence du traitement, le principe de traitement loyal et licite des données et le principe de durée limitée de conservation des données »

1 Article 1er §2 de la Loi n°09-08

1.4. Protection renforcée par des sanctions pénales

Tout d'abord, en application de l'article 57 de la Loi n°09-08, le fait pour quiconque de procéder sans le consentement exprès des personnes intéressées, au traitement des données à caractère personnel relatives notamment à la santé, est puni d'une peine d'emprisonnement de six mois à deux ans et d'une amende allant de 50.000 à 300.000 dirhams ou de l'une de ces deux peines seulement.

Par ailleurs, selon l'article 52 de la Loi n°09-08, sans préjudice d'une action en responsabilité civile à l'égard des personnes ayant subi des dommages, la mise en œuvre d'un fichier de données à caractère personnel sans déclaration ou autorisation est sanctionnée d'une amende allant de 10.000 à 100.000 dirhams. Ces sanctions peuvent être portées au double en cas de récidive. Lorsque l'auteur est une personne morale, et sans préjudice des peines pouvant être appliquées à ses dirigeants, les peines d'amende sont doublées. Les biens de la personne morale peuvent également être confisqués et ses établissements fermés.

Ensuite, les informations de santé font également l'objet d'une protection au titre du secret médical. Le secret médical, composante du secret professionnel, est consacré légalement et déontologiquement. Ainsi, tout professionnel de santé est tenu de ne pas révéler les informations sur la santé de ses patients.

La violation du secret professionnel est pénalement sanctionnée par l'article 446 du Code pénal. Selon cet article : « les médecins, chirurgiens ou officiers de santé, ainsi que les pharmaciens, les sages-femmes ou toutes autres personnes dépositaires, par état ou profession ou par fonctions permanentes ou temporaires, des secrets qu'on leur confie, qui, hors le cas où la loi les oblige ou les autorise à se porter dénonciateurs, ont révélé ces secrets, sont punis de l'emprisonnement d'un mois à six mois et d'une amende de 1.200 à 20.000 dirhams ».

" Le fait pour quiconque de procéder sans le consentement exprès des personnes intéressées, au traitement des données à caractère personnel relatives notamment à la santé, est puni d'une peine d'emprisonnement de six mois à deux ans et d'une amende allant de 50.000 à 300.000 dirhams ou de l'une de ces deux peines seulement "

2. Applications pratiques en temps de pandémie de Covid-19

La multiplication des initiatives destinées à endiguer la propagation du Covid-19, à l'instar par exemple du déploiement d'une application marocaine de traçage des contaminations ou des mesures envisagées par l'employeur pour assurer la santé et la sécurité au travail soulèvent de nombreuses interrogations concernant la conciliation entre lutte contre la propagation du virus, protection des données de santé et respect de la vie privée.

2.1. Application mobile de traçage des contaminations

Le Royaume du Maroc semble se diriger vers le développement d'une application mobile de traçage des contaminations (« Application mobile » ou « Application de Back tracking »). Celle-ci serait en cours de création et opérationnelle au mois de mai 2020.

Ce projet s'inscrit dans la direction retenue par plusieurs pays tels que la Corée du Sud, le Japon, la Chine, Singapour, Taiwan, Israël, ayant mis en place, de façon plus ou moins contraignante, des applications mobiles qui, selon l'objectif poursuivi, permettent de suivre le déplacement des personnes infectées pour comprendre les mécanismes de propagation du Covid-19, d'identifier les personnes ayant été en contact avec des individus porteurs ou encore de s'assurer du respect des mesures de confinement. Au sein de l'Union Européenne, plusieurs Etats ont annoncé le déploiement de technologies numériques plus ou moins similaires.

L'annonce du déploiement de cette application mobile incite, après une brève présentation de la technologie envisagée, à analyser sa compatibilité juridique avec la législation applicable en la matière et à formuler des recommandations sur le juste équilibre entre impératifs sanitaires, protection des données personnelles et respect de la vie privée.

2.1.1. Présentation des principales caractéristiques de l'application mobile

A ce stade, aucune présentation officielle des options techniques retenues et du fonctionnement de l'application mobile n'a été communiquée.

Toutefois, d'après les informations aujourd'hui rendues publiques,

« L'annonce du déploiement de cette application mobile incite, après une brève présentation de la technologie envisagée, à analyser sa compatibilité juridique avec la législation applicable en la matière et à formuler des recommandations sur le juste équilibre entre impératifs sanitaires, protection des données personnelles et respect de la vie privée »

“ L’application mobile, en permettant d’identifier et d’avertir les cas contacts en retraçant le parcours des utilisateurs déclarés positifs au Covid-19, impliquera la collecte et le traitement de données de santé, mais également, selon la technologie utilisée, de données de localisation et de données liées au terminal mobile ”

l’application mobile inclura, en priorité, les fonctionnalités suivantes :

- Back-tracking : traçage de l’historique de contact des cas confirmés sur les 14 à 21 derniers jours pour déterminer les personnes à risque, et notification aux Ministères de l’Intérieur et de la Santé ;

- Tableau de bord de pilotage en central pour permettre le suivi de la situation sanitaire des utilisateurs.

L’application devrait également offrir d’autres fonctionnalités telles que :

- la communication d’informations de source officielle à l’ensemble des utilisateurs (communiqués officiels, statistiques, fake-news, etc.) ;

- l’information des utilisateurs sur les zones à risque (foyers locaux, présence de cas de Covid-19) afin de les éviter lors des sorties autorisées ;

- la mise à la disposition d’autorisation numérique de sortie pendant le déconfinement (notamment un QR code, en fonction du profil/région de l’utilisateur) ; et

- l’auto diagnostic en ligne des symptômes du Covid-19 à travers un questionnaire et la possibilité d’enregistrement pour un test de dépistage.

Selon les informations disponibles à ce jour, un identifiant unique sera associé à chaque installation de l’application. Le traçage de l’utilisateur se fera soit par GPS (en enregistrant la localisation de l’utilisateur) soit par Bluetooth (en enregistrant les identifiants des téléphones proches), soit en utilisant les deux technologies.

Concrètement, le Back-tracking consiste à conserver un historique des contacts entre individus pour réussir à identifier toutes les personnes qui auraient pu être en contact/à proximité d’une personne déclarée porteuse du virus Covid-19, afin de pouvoir les informer et éventuellement les dépister.

Si l’on ne connait pas encore avec précision le fonctionnement de la technologie envisagée, on peut déduire des éléments précités que l’application mobile, en permettant par le biais des données de géolocalisation (GPS) et/ou de connexions Bluetooth d’identifier et d’avertir les cas contacts en retraçant le parcours des utilisateurs déclarés positifs au Covid-19, impliquera la collecte et le

traitement de données de santé[2], mais également, selon la technologie utilisée, de données de localisation et de données liées au terminal mobile.

2.1.2. Garanties attendues de l'application de Back-tracking

En principe, les données collectées par l'application mobile seront soumises aux dispositions de la Loi n°09-08. Pour assurer sa compatibilité avec la protection des données personnelles et le respect de la vie privée, il est aussi essentiel qu'elle tienne compte des recommandations de la CNDP.

Application de la Loi n°09-08 aux traitements envisagés par l'application mobile

Par principe, les dispositions de la Loi n°09-08 ne s'appliquent pas[3]:

- aux données à caractère personnel recueillies et traitées dans l'intérêt de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat ; et

- aux données à caractère personnel recueillies en application d'une législation particulière.

Etant précisé que les projets ou propositions de loi portant création de fichiers relatifs aux données précitées sont communiqués à la CNDP en indiquant :

- l'autorité responsable du fichier ;

- la ou les finalités du traitement ;

- la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant ;

- l'origine de ces données ; et

- les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement.

La déclaration de l'état d'urgence sanitaire pourrait implicitement conduire à assimiler la lutte contre la propagation de la pandémie de Covid-19 à une composante de l'intérêt

" La déclaration de l'état d'urgence sanitaire pourrait implicitement conduire à assimiler la lutte contre la propagation de la pandémie de Covid-19 à une composante de l'intérêt de défense nationale et de la sécurité intérieure ou extérieure de l'Etat "

2 Le fait de savoir qu'un utilisateur est porteur du virus Covid-19 constitue de facto une donnée de santé. Par ailleurs, l'application devrait permettre d'effectuer un suivi sanitaire des utilisateurs ou encore de permettre aux utilisateurs d'effectuer un auto-diagnostic et de s'inscrire pour un test de dépistage.

3 Article 2§4 de la Loi n°09-08

de défense nationale et de la sécurité intérieure ou extérieure de l'Etat.

Toutefois, dans la mesure où, d'une part, la lutte contre les épidémies/pandémies et leur propagation n'a pas été officiellement et expressément qualifiée de composante de l'intérêt de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat et, d'autre part, que les données traitées par l'application mobile ne le sont pas en application d'une législation particulière adoptée dans le contexte de crise sanitaire[4] , il convient de déduire que les traitements envisagés seront soumis à la Loi n°09-08.

Nécessité d'un fondement spécifique pour autoriser le traitement des données en dehors de tout consentement

Le cadre juridique actuel permet de traiter des données personnelles sous réserve de l'existence, selon la nature des données traitées et du traitement envisagé, d'une déclaration préalable à la CNDP, d'une autorisation légale ou d'une autorisation préalable octroyée par la CNDP et du consentement préalable, libre et éclairé, des personnes concernées. Il est à noter que la nécessité de fournir une information la plus complète et compréhensible possible découle de l'exigence d'obtenir un consentement libre et éclairé.

Ce même cadre juridique permet de déroger limitativement à l'exigence de consentement dans les hypothèses où le traitement est nécessaire notamment (i) au respect d'une obligation légale à laquelle est soumise la personne concernée ou le responsable du traitement ; (ii) à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou encore (iii) à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée[5].

Ces différentes bases légales peuvent se cumuler pour fonder un traitement des données personnelles hors consentement.

" Le cadre juridique actuel permet de traiter des données personnelles sous réserve de l'existence, selon la nature des données traitées et du traitement envisagé, d'une déclaration préalable à la CNDP, d'une autorisation légale ou d'une autorisation préalable octroyée par la CNDP et du consentement préalable, libre et éclairé, des personnes concernées"

4 Si une législation particulière intervenait, le projet ou proposition de loi portant création de fichiers relatifs aux données personnelles devra en principe être communiqué à la CNDP.

5 Article 4 de la Loi n°09-08

A ce jour, aucune disposition légale spécifique, adoptée dans le cadre de l'état d'urgence sanitaire, ne prévoit qu'il est possible de déroger à l'obligation de consentement des personnes concernées dans le cadre d'un traitement de données personnelles en lien avec la gestion de la crise sanitaire. Toutefois, la lutte contre la propagation de la pandémie de Covid-19 pourrait constituer, implicitement, une mission d'intérêt public[6] ou un intérêt légitime, en vertu de la déclaration de l'état d'urgence sanitaire.

A titre d'exemple, dans un communiqué officiel en date du 22 avril 2020, la CNDP a considéré que l'application mobile de traçage des déplacements des automobilistes déployée par la DGSN auprès des agents de sûreté de terrain pour s'assurer du respect des mesures de confinement était conforme à la Loi n°09-08 dans la mesure où notamment la licéité de la collecte et du traitement repose sur l'exécution d'une mission d'intérêt public.

Il est donc possible que la collecte et le traitement de données envisagés par l'application mobile puissent ultérieurement être considérés comme relevant de l'exécution d'une mission d'intérêt public. Néanmoins, en l'absence de déclaration officielle en ce sens, il n'est pas possible, à ce jour, de considérer qu'il existe un fondement légal autorisant l'application mobile à traiter les données personnelles, indépendamment de tout consentement.

A droit constant, il parait donc nécessaire de recueillir le consentement préalable des citoyens pour que l'application mobile ne soit pas en contradiction avec la Loi n°09-08. Dès lors, le traçage des contaminations prévu par l'application mobile doit être basé sur le volontariat.

Dans son communiqué officiel du 16 avril 2020, la CNDP, après avoir rappelé le caractère louable d'une telle application, « *insiste sur la nécessité de conforter la confiance, en particulier la confiance numérique : Si*

" A ce jour, aucune disposition légale spécifique, adoptée dans le cadre de l'état d'urgence sanitaire, ne prévoit qu'il est possible de déroger à l'obligation de consentement des personnes concernées dans le cadre d'un traitement de données personnelles en lien avec la gestion de la crise sanitaire "

6 A titre de comparaison, le considérant de principe n°46 du Règlement (UE) 2016/679 du 27 avril 2016, dit « RGPD », dispose que : « […] Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine ».

celle-ci n'est pas assurée, le nécessaire large usage de l'application s'en trouvera affecté et les résultats escomptés altérés. » Par ailleurs, elle recommande « *que l'usage de ce type d'application soit déployé sur la base d'une confiance volontariste et non sur la base d'une obligation difficile à mettre en œuvre ».*

Afin de concilier la compatibilité de l'application de Back-tracking avec la règlementation en vigueur, et dans l'hypothèse où l'utilisation de l'application aurait vocation à être obligatoire sans consentement des personnes concernées, deux choix s'offrent donc au législateur : soit le vote d'une loi autorisant l'Etat à collecter et traiter, via l'application mobile, les données des individus, dans le contexte de lutte contre le Covid-19, soit la qualification de la collecte et du traitement prévus par l'application mobile en tant que « mission d'intérêt public ».

Conforter la confiance numérique

De manière générale, dans ses recommandations en date du 16 avril 2020, la CNDP rappelle plusieurs principes et garanties essentielles à respecter pour le développement de l'application mobile et pour conforter la confiance numérique.

A titre d'information, la confiance numérique peut être définie comme la nécessité de créer une confiance chez les internautes dans l'usage d'Internet et des outils numériques. Elle permet de mesurer à quel point les internautes font confiance à la vie numérique.

Le renforcement de la confiance numérique passe notamment par la protection des données personnelles, la transparence et l'information claire et complète des citoyens notamment en cas de collecte et traitement de leurs données, la protection des citoyens notamment lors d'actes d'e-commerce, la sécurité des utilisateurs et des infrastructures numériques et la lutte contre les cyberattaques.

Enfin, en plus des recommandations de la CNDP, et pour renforcer davantage la confiance des citoyens dans l'utilisation de la future application mobile, il est également souhaitable que :

- l'application privilégie les technologies les moins intrusives possibles. Sur ce point, de nombreux experts ont indiqué que contrairement aux données

---

" Dans l'hypothèse où l'utilisation de l'application aurait vocation à être obligatoire, deux choix s'offrent au législateur : le vote d'une loi autorisant l'Etat à collecter et traiter les données des individus, ou la qualification de la collecte et du traitement prévus par l'application en tant que mission d'intérêt public "

de géolocalisation et aux données GPS, la technologie Bluetooth serait plus protectrice de la vie privée et des données à caractère personnel en raison du fait qu'elle n'implique pas le traitement des données de localisation ou de déplacements des utilisateurs[7] mais un recours aux données de proximité, ce qui serait moins intrusif ;

- l'application garantisse l'anonymat des porteurs du virus déclarés et des cas contacts supposés et la confidentialité des données ;

- les données ne puissent en aucun cas être transmises et partagées avec le secteur privé (ex : assurances, employeurs, etc.) à l'insu ou sans le consentement libre et éclairé des personnes concernées ;

- une telle application soit régulièrement évaluée et qu'elle n'ait qu'un caractère temporaire.

Pour conclure, l'efficacité et le succès d'une application mobile de traçage dans la lutte contre la propagation du virus Covid-19 supposent qu'elle soit utilisée par le plus grand nombre de citoyens. Pour cela, il est essentiel qu'elle soit mise en œuvre dans un cadre respectueux de la vie privée et de la législation relative à la protection des données personnelles, afin d'entourer son usage de garanties suffisantes pour créer les conditions d'une confiance et d'une acceptabilité citoyenne.

Empêcher les risques de discrimination

Il est nécessaire de souligner que l'utilisation d'une telle application mobile, même sur la base du volontariat, peut être source de dérives susceptibles de conduire à des discriminations sociales ou économiques.

L'application et son utilisation doivent être entourées de garanties suffisantes permettant de s'assurer qu'elle ne puisse contribuer à faire émerger un risque de discrimination, voire de stigmatisation, envers les personnes signalées comme porteuses ou susceptibles d'être porteuses du coronavirus, celles qui ne l'utiliseraient pas ou encore celles qui auraient des difficultés à la faire fonctionner.

" L'efficacité et le succès d'une application mobile de traçage supposent qu'elle soit mise en œuvre dans un cadre respectueux de la vie privée et de la législation relative à la protection des données personnelles, afin d'entourer son usage de garanties suffisantes pour créer les conditions d'une confiance et d'une acceptabilité citoyenne "

7 On peut noter par exemple qu'en Israël ou en Corée du Sud, le choix de technologie a été porté sur les données de géolocalisation (GPS), tandis qu'à Singapour, l'application TraceTogether utilise la technologie Bluetooth.

“ Il existe un risque de dévoiement, par les organismes publics ou privés, de l’utilisation de l’application mobile de traçage des contaminations susceptible de conduire à des discriminations ”

A titre d’exemple, on peut imaginer l’hypothèse où un employeur conditionnerait une offre d’emploi ou la conclusion d’un contrat de travail au partage préalable des données de santé et résultats contenus dans l’application mobile, ou celle où une compagnie d’assurance ou un établissement bancaire subordonneraient la signature d’un contrat d’assurance ou l’octroi d’un prêt à ce partage préalable de l’information ou à l’utilisation d’une telle application. Sans compter les cas éventuels où des restaurants, cinémas, supermarchés pourraient conditionner l’accès à un service ou à un bien au partage préalable des données contenues dans l’application mobile des utilisateurs.

Il existe donc un risque de dévoiement, par les organismes publics ou privés, de l’utilisation de l’application mobile de traçage des contaminations susceptible de conduire à des discriminations.

Or, à titre de comparaison, on peut noter qu’aux termes de l’article 431-1 du Code pénal, « constitue une discrimination toute distinction opérée entre les personnes physiques [ou entre les personnes morales] à raison de l’origine nationale ou sociale, de la couleur, du sexe, de la situation de famille, de l’état de santé, du handicap, de l’opinion politique, de l’appartenance syndicale, de l’appartenance ou de la non appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée ». La discrimination est punie d’une peine d’emprisonnement variant d’un mois à deux ans et d’une amende de 1.200 à 50.000 dirhams lorsqu’elle consiste :

- à refuser la fourniture d’un bien ou d’un service ;

- à entraver l’exercice normal d’une activité économique quelconque ;

- à refuser d’embaucher, à sanctionner ou à licencier une personne ;

- à subordonner la fourniture d’un bien ou d’un service ou l’offre d’un emploi à une condition fondée sur l’un des éléments précités.

Ensuite, le préambule du Code du travail rapelle que « toute personne a droit à un emploi adapté à son état de santé, à ses qualifications et à ses aptitudes » et qu’est « également interdite à l’encontre des salariés, toute discrimination fondée sur la race, la couleur, le sexe, le handicap, la

situation conjugale, la religion, l'opinion politique, l'affiliation syndicale, l'ascendance nationale ou l'origine sociale, ayant pour effet de violer ou d'altérer le principe d'égalité des chances ou de traitement sur un pied d'égalité en matière d'emploi ou d'exercice d'une profession, notamment, en ce qui concerne l'embauchage, la conduite et la répartition du travail, la formation professionnelle, le salaire, l'avancement, l'octroi des avantages sociaux, les mesures disciplinaires et le licenciement ».

En pratique, au regard des éléments précités, il semble capital que l'utilisation, même sur la base du volontariat, de l'application de traçage des contaminations soit accompagnée d'un certain nombre de garanties empêchant l'essor d'éventuelles discriminations et stigmatisations et soit même éventuellement assortie de sanctions à l'égard de tout opérateur privé ou public qui conditionnerait ou menacerait de conditionner l'octroi d'un bien, d'un service ou d'un emploi au partage préalable des données ou statuts divulgués par l'application mobile ou à l'utilisation préalable de l'application.

Sur ce point, il est intéressant de noter qu'au Royaume-Uni, un projet de loi intitulé « The Coronavirus (Safeguards) Bill 2020 », proposant plusieurs garanties destinées à protéger les citoyens contre les potentiels effets discriminants découlant de l'utilisation d'une application de Back-tracking, a récemment été déposée. Parmi ces garanties, on dénombre notamment l'importance qu'aucune discrimination liée à l'utilisation ou au défaut d'utilisation d'une application mobile de Back-tracking ne puisse émerger et qu'aucune sanction de nature civile, pénale ou administrative (amende ou peine d'emprisonnement) ne puisse être prévue pour absence d'installation, d'utilisation, mauvaise utilisation ou suppression de l'application. Enfin, le projet de loi insiste sur le fait qu'aucune personne, sauf certaines personnes compétentes et limitativement identifiées (ex : un agent de police, un fonctionnaire, etc.) ne puisse exiger de manière générale la présentation d'un « certificat d'immunité » délivré sur l'application comme condition préalable pour quitter son domicile, entrer dans les espaces publics, utiliser les transports en commun, etc.

« Au Royaume-Uni, un projet de loi intitulé Coronavirus (Safeguards) Bill 2020, propose plusieurs garanties destinées à protéger les citoyens contre les potentiels effets discriminants découlant de l'utilisation d'une application de Back-tracking »

2.2. Collecte des données de santé par l'employeur

Dans un contexte de multiplication des foyers de contaminations dans le secteur industriel, certaines mesures envisagées par l'employeur pour lutter contre la propagation du virus, à l'instar de la prise de température ou de la diffusion de questionnaires de santé, invitent à s'interroger sur la conciliation entre obligation d'hygiène et de sécurité de l'employeur et le respect des données de santé et de la vie privé des employés.

Dans la délibération n°D-106-EUS/2020 du 23 avril 2020 portant sur la prise de température, en vue de l'accès au lieu de travail, pendant la durée de l'état d'urgence sanitaire, la CNDP a en partie clarifié les mesures pouvant être mises en place au sein des entreprises pour limiter la propagation du virus. Néanmoins, d'autres mesures envisagées par les entreprises, à l'instar de la diffusion de questionnaires de santé, n'ont pas été évoquées.

2.2.1. Prise de température et installation de caméras thermiques

Dès lors que les emplois ne sont pas éligibles au télétravail, certaines entreprises peuvent envisager de soumettre leurs employés à une prise de température ou d'installer des caméras thermiques, sur le fondement de l'obligation générale de préserver la sécurité et la santé des employés au travail[8].

Concernant la prise de température, le Ministère du Travail et de l'Insertion Professionnelle a indiqué, dans son Guide à l'attention des employeurs et des salariés dans le contexte du Covid-19, qu'au vu des mesures exceptionnelles de prévention entreprises par les services de la santé, l'employeur est en droit de mesurer la température du salarié avant que ce dernier n'accède à son lieu de travail.

Deux situations paraissent toutefois devoir être distinguées : (i) lorsque la température est prise uniquement avant l'entrée sur le lieu de travail, sans faire l'objet d'aucun enregistrement/traitement, de quelque nature et sous quelque forme que ce soit, par l'employeur et (ii) lorsqu'elle est relevée et conservée/enregistrée pour permettre par exemple d'établir une sorte de suivi de l'évolution de la santé

" Le Ministère du Travail et de l'Insertion Professionnelle a indiqué, dans son Guide à l'attention des employeurs et des salariés dans le contexte du Covid-19, que l'employeur est en droit de mesurer la température du salarié avant que ce dernier n'accède à son lieu de travail "

8 Article 24 du Code du travail

des employés (ex : établir une courbe de température, etc.).

A priori, si la prise de température a pour seule finalité de permettre à l'employeur de décider si un employé peut ou non entrer sur le lieu de travail, sans faire l'objet d'aucun enregistrement et traitement, elle n'est pas soumise à la Loi n°09-08. Par ailleurs, compte tenu de l'obligation de l'employeur de garantir la sécurité des employés, et sous réserve de s'appuyer sur les services médicaux du travail ou les médecins du travail, une telle mesure paraît proportionnée et justifiée au titre de la prévention de la crise sanitaire et de la gestion de la propagation du virus au sein de l'entreprise.

A l'inverse, l'enregistrement et le traitement des températures relevées quotidiennement pour effectuer un suivi de la santé de chaque salarié afin d'identifier d'éventuels symptômes caractérisent un traitement de données de santé soumis aux dispositions de la Loi n°09-08 et donc subordonné à l'obtention d'une autorisation de la CNDP.

S'agissant de l'installation de caméras thermiques pour dépister des employés potentiellement malades, les informations collectées par ces caméras (température corporelle d'une personne identifiée) constituent également un traitement de données de santé.

Dans sa délibération n°D-106-EUS/2020 du 23 avril 2020, la CNDP, après avoir indiqué qu'il était possible d'utiliser des outils de prise de température des employés, sous-traitants et visiteurs, personne par personne, précise les modalités et conditions dans lesquelles une telle mesure peut être mise en œuvre au sein de l'entreprise pendant la durée de l'état d'urgence sanitaire. Elle indique notamment que :

- « le responsable de traitement est tenu d'informer les personnes concernées, au moyen d'une affiche ou d'un pictogramme placés à l'entrée des lieux du travail, du recours à la prise de température pour le contrôle d'accès et des caractéristiques du traitement mis en œuvre" ;

- l'accès aux locaux peut être refusé à toute personne refusant la prise de température, à condition de ne pas constituer une mesure discriminatoire à l'égard de la personne concernée mais visant à préserver la santé de la collectivité ;

" A priori, si la prise de température a pour seule finalité de permettre à l'employeur de décider si un employé peut ou non entrer sur le lieu de travail, sans faire l'objet d'aucun enregistrement et traitement, elle n'est pas soumise à la Loi n°09-08 "

“ La CNDP rappelle que les principes de minimalité, de proportionnalité et de non détournement de finalités s’appliquent aux traitements ”

- il est possible d’utiliser « sous le contrôle de la médecine du travail et selon les recommandations des autorités sanitaires, les moyens technologiques adéquats permettant la collecte de la température du corps de façon individuelle » ;

- il est possible « d’établir, sous le contrôle de la médecine du travail, et pendant la durée recommandée par les autorités sanitaires, des courbes d’historique de température avec pour seule finalité la détection des situations nécessitant une intervention préventive pour l’intérêt de la santé des individus et de la collectivité ».

Les traitements évoqués ci-dessus doivent être notifiés par le responsable de traitement auprès de la CNDP. Une procédure simplifiée de notification par demande d’autorisation unique a été mise en place à cet effet.

La CNDP rappelle également que « les principes de minimalité, de proportionnalité et de non détournement de finalités s’appliquent aux traitements ».

Concrètement, comme tout traitement de données, le responsable du traitement devra ne collecter que des données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées (en l’espèce, la gestion des cas de suspicions de contamination au Covid-19 au sein de l’entreprise), ne transmettre les données de santé qu’aux autorités compétentes, prévoir une durée limitée de conservation des données (les données devront être détruites dès lors que la finalité déclarée ou autorisée sera atteinte). Par ailleurs, comme le rappelle la CNDP, il est essentiel que la collecte et le traitement de ce type de données dans le cadre d’une entreprise soient confiés aux médecins du travail ou aux services médicaux de l’entreprise, seuls garants du secret médical.

Il est à noter que la CNDP précise que seul les représentants établis au Maroc sont habilités à traiter les données relatives à la prise de température.

En tout état de cause, il est souhaitable que les entreprises optent pour les solutions les plus adéquates et proportionnées pour permettre de concilier protection des données de santé, respect de la vie privée des employés et prévention des risques de contamination au sein de

l'entreprise. A titre d'exemple, il serait disproportionné que les caméras thermiques effectuent des enregistrements vidéo des employés.

A titre de comparaison, en France, la Commission Nationale de l'Informatique et des Libertés (« CNIL ») a indiqué que les relevés obligatoires des températures de chaque employé à adresser quotidiennement à la hiérarchie ne sont pas autorisés.

2.2.2. Diffusion de questionnaires de santé

La diffusion de questionnaires de santé auprès des employés pour déterminer s'ils présentent des symptômes du Covid-19 est une réponse envisagée par certains employeurs pour prévenir la santé et la sécurité au travail. La question se pose de savoir si l'employeur peut exiger de ses employés de le tenir informé régulièrement de leur état de santé via, par exemple, un questionnaire à remplir.

En premier lieu, la mise en place d'une telle mesure constituerait un traitement de données sensibles impliquant de respecter les conditions préalables prévues par la Loi n°09-08.

En second lieu, il est essentiel que les modalités de mise en œuvre de tels questionnaires, leur contenu, leur suivi et le traitement des informations de santé communiquées par les employés incombent aux services médicaux du travail ou au médecin du travail, tenus au secret professionnel, et non à l'employeur ou aux ressources humaines. Les informations relatives à la santé des salariés, protégées par le secret médical, n'ont pas vocation à être portées à la connaissance d'un employeur.

La légitimité du médecin du travail comme interlocuteur privilégié des employés en cas de risque lié au virus Covid-19 et pour la collecte et le traitement des données de santé des employés peut notamment être déduite de l'article 318 du Code du travail, selon lequel « Le médecin du travail a un rôle préventif qui consiste à procéder sur les salariés aux examens médicaux nécessaires, notamment à l'examen médical d'aptitude lors de l'embauchage et à éviter toute altération de la santé des salariés du fait de leur travail, notamment en surveillant les conditions d'hygiène dans les lieux de travail, les risques de contamination et l'état de santé des salariés », ou encore de l'article 324 dudit code selon lequel « Le

" Il est essentiel que les modalités de mise en œuvre de tels questionnaires, leur contenu, leur suivi et le traitement des informations de santé communiquées par les employés incombent aux services médicaux du travail ou au médecin du travail, tenus au secret professionnel, et non à l'employeur ou aux ressources humaines "

médecin du travail est tenu de déclarer, dans les conditions prévues par la législation en vigueur, tous les cas de maladies professionnelles dont il aura connaissance ainsi que les symptômes ou maladies pouvant avoir un caractère professionnel ».

En tout état de cause, si une telle mesure semble envisageable au regard de la législation en vigueur, sous réserve du respect des conditions et des principes généraux applicables aux traitements des données, il est recommandé aux entreprises d'éviter de recourir à une telle mesure de manière généralisée et de privilégier des solutions alternatives moins intrusives permettant de prévenir la santé et la sécurité des employés. Pour éviter d'y recourir, l'employeur, après avoir rappelé aux employés qu'ils doivent veiller à respecter les gestes barrières, peut leur rappeler qu'ils doivent également préserver leur santé et sécurité ainsi que celles de leurs collègues et les inviter à se signaler auprès des services médicaux, du médecin du travail ou en dernier recours l'employeur, en cas de suspicion de contamination ou symptômes.

Dans l'hypothèse où une entreprise voudrait mettre en œuvre une telle mesure, et dans l'attente d'une éventuelle prise de position de la CNDP en la matière, il peut être utile aux entreprises de suivre les recommandations de la CNDP relatives à la prise de température.

En tout état de cause, de manière générale, le traitement des données en lien avec le virus Covid-19 par l'employeur doit être limité au strict minimum de ce qui est requis pour mettre en place des mesures de protection adéquates au sein de l'entreprise, gérer les cas de suspicions de contamination et informer les autorités compétentes (ex : date, identité de l'employé suspecté de contamination, mesure organisationnelle adoptée).

A titre de comparaison, la CNIL a indiqué que les employeurs doivent s'abstenir de collecter de manière systématique et généralisée, ou via des enquêtes et demandes individuelles, des informations relatives à la recherche d'éventuels symptômes présentés par un employé et ses proches. La collecte de questionnaires de santé auprès des employés n'est ainsi pas autorisée.

Ainsi, à ce jour, il n'est pas possible de considérer qu'au vu de l'urgence à endiguer et prévenir la propagation

du virus, le traitement des données de santé par les entreprises puisse intervenir en dehors des strictes règles de droit applicables. Dès lors, la CNDP devra être notifiée et les employés devront être informés et consentir au traitement de leurs données sauf si, d'ici là, une loi ou une autorité autorise ce type de traitements pendant la durée de l'urgence sanitaire.

La gestion de cette crise sanitaire ouvre ainsi la voie à une réflexion plus large, en termes de protection de la vie privée, sur l'opportunité de recourir ou non à des mesures et technologies diverses pour endiguer efficacement la pandémie.

La CNDP a précisé qu'elle adopterait une position spécifique en période de crise sanitaire en appréciant chaque situation « au regard de la balance entre le risque sanitaire et le risque impactant le respect de la vie privée » et que « la gestion du risque sanitaire, en période d'état d'urgence, sera, de toute évidence, systématiquement favorisée ».

Il appartient désormais à de nombreux autres acteurs d'enrichir ce débat ouvert afin de définir le meilleur équilibre entre la protection de la vie privée et la gestion du risque sanitaire, deux impératifs d'apparence contradictoires.

Epidémiologistes, développeurs d'applications mobiles, partenaires sociaux et pouvoirs publics devront dès lors déterminer précisément les bénéfices attendus des solutions envisagées pour permettre au régulateur de procéder aux arbitrages qui s'imposent et de les ajuster avec le temps.

CONTACTS
AFRIQUE ADVISORS – SPECIAL ADVISORY UNIT

Laila Slassi
Associée
lslassi@afriqueadvisors.com

Kenza Alaoui
Of Counsel - Juridique
kalaoui@afriqueadvisors.com

Maroua Alouaoui
Collaboratrice - Juridique
malouaoui@afriqueadvisors.com

Ismail Bekkaoui
Collaborateur - Stratégie & Finance
ibekkaoui@afriqueadvisors.com

Adil Hajoubi
Collaborateur - Stratégie
ahajoubi@afriqueadvisors.com

Amélia Marques
Collaboratrice - Juridique
amarques@afriqueadvisors.com

Talal Belrhiti
Associé
tbelrhiti@afriqueadvisors.com

Amine Amzazi
Of Counsel - Finance & Fiscalité
aamzazi@afriqueadvisors.com

Hajar Benyachou
Collaboratrice - Juridique
hbenyachou@afriqueadvisors.com

Salma El Jazouli
Collaboratrice - Juridique
seljazouli@afriqueadvisors.com

Meryem Lahlou
Collaboratrice - Juridique
mlahlou@afriqueadvisors.com

Contact Général
+212 661 57 07 29
specialadvisoryunit@afriqueadvisors.com

Afrique Advisors est un cabinet de conseil juridique, fiscal et stratégique basé à Casablanca, Maroc.

www.afriqueadvisors.com

10, rue Al Jihani, Casablanca, Maroc

AFRIQUE ADVISORS