Lexis Maroc
En partenariat avec Ikone Juris

Protection des données personnelles en entreprise en période de crise sanitaire

Lina Fassi-Fihri

Associée gérante LPA-CGR à Casablanca, Avocate au Barreau de Paris

1 . - APERÇU RAPIDE

1.1. - Éléments clés

Les mesures prises par les dirigeants de sociétés depuis le début de la crise du Covid-19 les conduisent à traiter des données personnelles de leurs salariés.

Or la crise du Covid-19 n'a pas fait disparaître les obligations liées à la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

1.2. - Textes

- L. n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel : BORM n° 5714, 7 rabii I 1430 (5 mars 2009)
- CNDP, Délibération n° D-107-EUS/2020 du 23 avril 2020 régissant le télétravail dans le secteur de la Relation Client en situation d'état d'urgence sanitaire- Covid-19
- CNDP, 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
- Code du travail

1.3. - Bibliothèque LexisNexis

- Synthèse n° 320, « Protection des données personnelles », par Mehdi Kettani : Lexis Maroc, rubrique « Encyclopédie »
- Fiche pratique n° 4389, « Quelles sont les obligations des entreprises sous-traitantes marocaines au regard de la règlementation RGPD ? », par Sonia Mavouna, Kelly Hazan et Julie Schwartz : Lexis Maroc, rubrique « Contenus pratiques »

2 . - PREPARATION

2.1. - Informations préalables

Comment protéger les flux de données personnelles de mes salariés et en particulier les données de santé ?

Comment concilier les obligations de l'employeur (relatives à la sécurité de ses employés et aux demandes des autorités locales) et la conformité à la loi n° 09-08 ?

Comment assurer la sécurité de mon système d'information lorsque mes salariés sont en télétravail ?

Auditer ma conformité à la protection des données personnelles (relation avec mes prestataires externes, autorisation et/ou déclaration à la CNDP) et gérer mes audits avec mes donneurs d'ordre européens soumis au RGPD qui répercutent les obligations qui en découlent à leurs sous-traitants.

2.2. - Inventaire des solutions et éléments de décisions

Les premières interrogations ont émané des employeurs qui ont été confrontés en quelques jours à une situation inédite : d'une part, assurer la sécurité et la protection de ceux de leurs employés demeurés sur le site et d'autre part, poursuivre l'activité et la communication avec certains de leurs employés en télétravail.

3 . - MISE EN ŒUVRE

3.1. - L'obligation de sécurité de l'employeur au cœur du débat

De manière générale, l'obligation de sécurité issue de l'article 24 du Code du travail incombant à l'employeur a dicté les choix des dernières semaines, mais cette obligation est renforcée et constante lorsqu'il s'est agi de protéger les employés travaillant sur site.

Il a donc fallu prendre des mesures préventives dont certaines ont pu heurter les principes de la protection des données à caractère personnel.

3.1.1. - Le principe de proportionnalité doit dicter les actions des managers

Dans l'objectif de prévenir une contagion, certains employeurs ont souhaité conditionner l'accès de leur site à un relevé de température corporelle ou bien à l'analyse des réponses à des questionnaires sur la santé de leurs employés.

Il convient de rappeler que les données de santé sont des données dites sensibles selon l'article 1 de la loi n° 09-08 (la Loi) et leur collecte est soumise à une autorisation préalable de la CNDP dans les conditions prévues par les articles 12 et 21 de la Loi.

En France, de telles pratiques sont interdites, l'Autorité de contrôle, la CNIL, ayant décidé qu'elles étaient disproportionnées par rapport à l'objectif recherché.

Au Maroc, l'article 3 de la Loi rappelle que la collecte de données à caractère personnel doit être adéquate, pertinente et non excessive, au regard des finalités pour lesquelles elles sont collectées, et pour lesquelles elles sont traitées ultérieurement.

Le principe de proportionnalité, essentiel à la protection des données personnelles, doit guider le manager qui doit tenter de trouver l'alternative la moins intrusive pour ses salariés.

Sur ces points, la CNDP vient de donner son avis dans une délibération n° D-106-EUS/2020 du 23 avril 2020 et a encadré un tel traitement de la manière suivante :

- ce traitement est légal de manière exceptionnelle en ce contexte d'état d'urgence sanitaire ;
- la finalité de ce traitement est « *le contrôle d'accès à des fins de sécurité sanitaire* » ;
- la base légale de ce traitement est l'intérêt légitime de l'employeur ;
- la CNDP recommande l'information des personnes concernées par le 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* » ;
- la mise en œuvre de ce dispositif doit être faite sous le contrôle du service de médecine du travail, incluant la possibilité de conserver les données pour faire une courbe historique ;
- pour les entreprises qui dépendent d'une structure étrangère, seul le représentant établi au Maroc est habilité à traiter les données relatives à la prise de température dans le respect des termes édictés par ladite délibération.

En temps normal, la collecte de données sensibles est soumise à l'autorisation de la CNDP qui vérifie notamment si le consentement préalable a été recueilli. Cette délibération assouplit semble-t-il ces conditions puisque seule l'information de la personne concernée est requise, et une procédure simplifiée de notification de demande d'autorisation unique a été mise en place.

La CNDP recommande de détruire toutes les données à caractère personnel collectées dans ce contexte « *dès lors*

que la finalité déclarée ou autorisée est atteinte ». Sur ce point, on peut s'interroger sur le point de savoir quand cette finalité sera effectivement atteinte, lorsque l'état d'urgence sanitaire sera levé ou bien lorsque la menace d'un nouvel épisode de pandémie due au Covid-19 sera définitivement éloignée ?

Une autre disposition mérite réflexion : celle par laquelle la CNDP donne la « *possibilité à l'employeur de refuser l'accès à ses locaux à toute personne refusant cette prise de température, à condition toutefois de ne point constituer une mesure discriminatoire à l'égard de la personne concernée, mais visant à préserver la santé de la collectivité* ».

D'une part, se pose la question de savoir si ce refus de l'employé peut être considéré comme légitime compte tenu des droits des personnes concernées et comment il peut véritablement avoir lieu en pratique lorsqu'il existe un rapport hiérarchique et la crainte d'être sanctionné, particulièrement en cette période de fragilité de maintien des emplois.

D'autre part, et surtout, on peut s'interroger sur le traitement en droit du travail de ce refus par l'employeur d'accéder au site à un salarié (est-ce un cas de suspension de son contrat ? une faute ?) et pourquoi une autorité de contrôle relative à la protection des données personnelles peut se positionner sur une telle question.

Parallèlement à cette nécessaire mise en conformité au regard des lignes directrices récemment promulguées par la CNDP, il est possible de faire appliquer des bonnes pratiques dans son entreprise et responsabiliser ses employés en les incitant à remonter de manière volontaire les informations les concernant et qui peuvent mettre en danger leurs collègues.

Dans cette perspective, l'employeur doit donner des consignes et instructions claires relatives aux situations dans lesquelles les employés se doivent de remonter les informations les concernant ou leur entourage et aménager un canal de communication dédié.

3.1.2. - Encadrer la communication des données à caractère personnel de ses employés à des tiers

La poursuite ou la reprise proche de l'activité, notamment de grandes entreprises, peut impliquer le transfert de données personnelles à des tiers.

En effet, parmi les mesures de sécurité à prendre, celle de la prise en charge du transport du personnel via des prestataires privés peut se révéler utile pour éviter les transports publics.

Dans certains cas, des entreprises ont également choisi de communiquer régulièrement des données personnelles de leurs employés aux autorités locales à des fins de recoupement d'information et de prévention de la propagation de l'épidémie.

S'agissant des nouveaux prestataires, il convient d'encadrer juridiquement dans les contrats les conditions de sécurité et de confidentialité attendues pour le traitement des données personnelles des salariés, et ce conformément aux alinéa 2 et 3 de l'article 23 de la Loi.

S'agissant des autorités, il est possible de communiquer des données personnelles pour la réalisation de missions, directement liées aux fonctions du tiers et sous réserve du consentement préalable de la personne concernée ou sans ce consentement dans des cas limités prévus à l'article 4 de la Loi.

Dans le contexte précité, il serait possible de déroger à cette obligation si l'on considère que le traitement est nécessaire :

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

Cette mesure peut être prise par l'entreprise pour respecter son obligation légale de sécurité vis-à-vis de ses employés et dans un intérêt légitime de protection de ses

salariés et de son activité. Il faut s'assurer cependant que les données personnelles transmises soient limitées à ce qui sera utile aux prestataires et aux autorités publiques pour la finalité de chaque traitement, préalablement identifiée.

3.2. - La sécurité des données, un principe essentiel pouvant être malmené par le télétravail

Dans le cas du télétravail, qui pour rappel n'est encadré par aucun texte à tout le moins concernant le secteur privé, les problématiques sont plus particulièrement liées aux mesures de sécurité des données.

Il s'agit à nouveau d'un principe essentiel de la règlementation relative à la protection des données, rappelé à l'article 23 de la Loi, qui dispose que : « *Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé (…). Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger* ».

Le Règlement Européen relatif à la Protection des Données Personnelles (RGPD) fait de ce principe un fil conducteur qui doit guider les actions du responsable de traitement, dès leur conception et par défaut (notions de *privacy by design* et *by default*).

Or, depuis le début de la crise, la cybersécurité est un enjeu majeur car les attaques notamment par hameçonnage se sont multipliées, par le biais d'envoi de messages émanant de fausses adresses d'autorités publiques.

En pratique, deux aspects sont à prendre en considération.

En premier lieu, les équipements utilisés. Il convient de choisir et de s'adapter en fonction de l'audit réalisé, de déterminer si ses employés utiliseront leurs propres ordinateurs ou si l'entreprise est en mesure de fournir des équipements incluant l'installation d'un pare-feu, d'un antivirus et d'un outil de blocage d'accès à des sites malveillants, ainsi que l'installation d'un VPN.

En deuxième lieu, il est également nécessaire d'informer et de (re)sensibiliser les employés aux problématiques de données personnelles et de rappeler les mesures de sécurité relatives à la confidentialité des codes d'accès, les précautions à prendre lors de la réception de courriels provenant de sources inconnues et contenant des pièces jointes. Il faut également être vigilant dans le choix des outils de visioconférence et encadrer leur bonne utilisation et celle des messageries.

Sur ce volet également, des bonnes pratiques existent : d'abord, demander conseil à son *data protection officer* s'il en a été nommé un, qui saura apporter ses conseils pour paramétrer les mesures de sécurité et apprécier le principe de proportionnalité pour chaque traitement. Aussi, il est utile de rédiger une charte de télétravail incluant les attentes en matière de sécurité et rappelant les obligations des employés. C'est également ce que recommande la CNDP dans sa délibération n° D-107-EUS/2020 du 23 avril 2020 régissant le télétravail dans le secteur de la Relation Client précisément, qui dispose que « *l'élaboration d'une charte de télétravail qui peut être un avenant à la charte informatique semble indispensable pour poser les bases d'un régime unifié du télétravail au sein de l'entreprise tout en définissant les droits et obligations des parties prenantes* ».

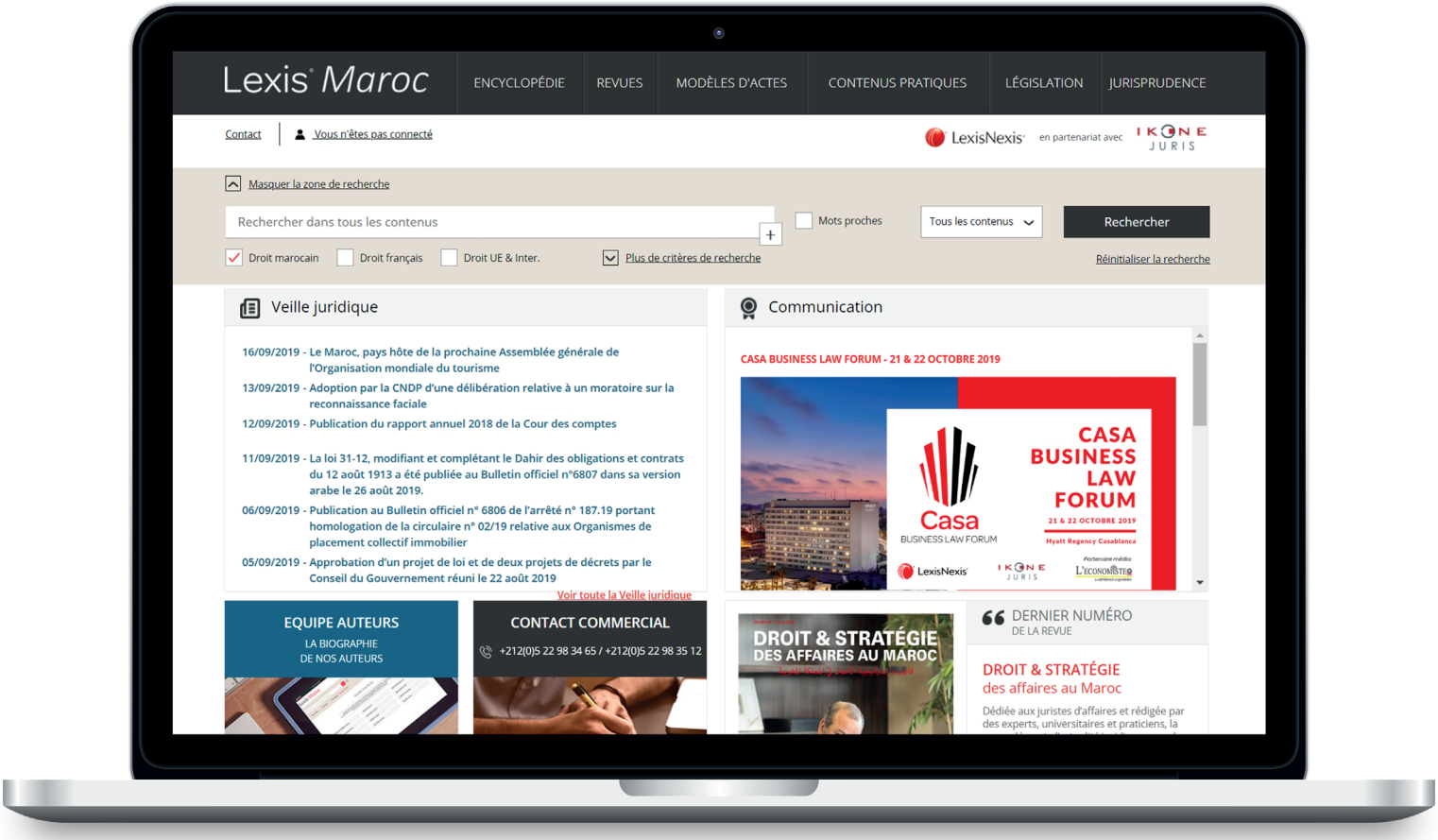
En conclusion, il faut essayer de trouver, dans la mesure du possible, des moyens de rendre cette période de crise positive pour son activité et sa reprise.

Profitons par conséquent de la baisse d'activité pour avancer sur les problématiques de conformité à la règlementation sur les données personnelles, et ce sur plusieurs volets : le référentiel de sécurité à savoir les mesures de sécurité mises en œuvre (archivage, gestion des sous-traitants,…), les procédures permettant de traiter les droits des personnes, les registres ou la cartographie de ses données, et enfin, la formation et la sensibilisation de son personnel.

4 . - OUTILS

4.1. - Check-list

- ☐ Les données de santé sont des données sensibles dont la collecte est soumise à une procédure simplifiée pour autorisation de la CNDP ;
- ☐ Les mesures d'accès à son site visant à vérifier l'état de santé de ses salariés doivent être proportionnées à la finalité du traitement ;
- ☐ Préférer responsabiliser ses salariés afin qu'ils remontent de manière volontaire les informations incluant des données à caractère personnel les concernant ;
- ☐ Encadrer juridiquement les contrats avec les nouveaux prestataires sur les problématiques de sécurité des données personnelles communiquées ;
- ☐ L'obligation de sécurité et l'intérêt légitime de l'employeur issus du droit du travail sont des bases légales à un traitement de données personnelles de ses employés ;
- ☐ Il faut veiller à la sécurité des données personnelles en cas de télétravail : par des outils IT et par la sensibilisation de ses salariés ;
- ☐ Une délibération de la CNDP encadre le télétravail dans le secteur de la Relation Client ;
- ☐ Encadrement des obligations des salariés par une charte de télétravail.



LexisMaroc, La solution qui simplifie votre quotidien

Conçu en étroite relation avec des praticiens et plus de 100 auteurs, LexisMaroc est un portail dédié aux professionnels du droit : avocats, magistrats, notaires, juristes, experts-comptables, universitaires…

Le fonds documentaire sans équivalent de LexisMaroc est composé de sources officielles (jurisprudence et législation) et de contenus éditoriaux pour accroitre votre productivité :

- Synthèses
- Modèles d'actes
- Fiches et guides pratiques
- Droit de l'OHADA
- Revue Droit et Stratégies des Affaires au Maroc
- Revue Marocaine d'Administration Locale et de Développement (REMALD)

Plus de 22 000 documents originaux nécessaires à votre activité

Un accès à l'information adapté aux contenus et à votre pratique quotidienne

Une équipe d'auteurs universitaires et praticiens spécialisés hautement qualifiés

Réservez une démo sur
Lexismaroc.ma/Maroc/contactus

LexisNexis®