



QUELLE PROTECTION DES DONNÉES PERSONNELLES AU MAROC ?

A l'heure du big data et de l'omniprésence des systèmes d'information, la question de la protection des données à caractère personnel est devenue incontournable pour les entreprises. Au Maroc, la loi 09-08 et le CNDP imposent un cadre strict au traitement de ces données. Mais pour de nombreuses PME, il faut également tenir compte du RGPD européen pour continuer son activité. Explications.

Le traitement des données de personnes physiques par les entreprises concerne un très grand nombre d'opérations : gestion des ressources humaines, facturation, contrôle des accès, vidéosurveillance, campagnes marketing, utilisation de sites web ou d'applications mobiles, etc. A travers elles, de nombreuses données personnelles peuvent être enregistrées, telles que le nom des personnes, leurs coordonnées, numéro de carte d'identité nationale, photo, et toutes les informations utiles à l'activité de l'entreprise.

Respecter la loi marocaine

Si ces opérations sont bien souvent indispensables au travail de chaque société, elles ne doivent pas porter atteinte à la vie privée et aux droits des personnes concernées. C'est dans ce sens que la loi 09-08 a été adoptée au Maroc et que la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) a été créée. Ainsi, selon cette commission, " tous les traitements dont les responsables ou les moyens de traitement sont situés sur le territoire marocain, qu'ils soient propriété d'un organisme marocain ou d'un donneur d'ordre étranger - sous-traitance, délocalisation, etc. - sont tenus de se conformer à la loi 09-08 du 18 février 2009 (BO n°5714 du 05-03-2009) ".

Exigences de la loi 09-08

D'après cette loi, les entreprises doivent informer la CNDP avant de mettre en œuvre un traitement de données personnelles et, le cas échéant, obtenir certaines autorisations. Dans ce cadre, elles doivent s'assurer que ces données sont collectées et traitées d'une façon loyale, légitime et transparente, en veillant à leur exactitude et mise à jour. De plus, celles-ci doivent être nécessaires, proportionnelles et non excessives au regard de la finalité du traitement envisagé. Cette finalité doit d'ailleurs être précise et légitime, et communiquée aux personnes concernées lors de la collecte des informations et à la CNDP lors de la notification du traitement. En outre, "les données personnelles permettant l'identification des personnes concernées doivent être conservées pour une durée limitée, n'excédant pas la durée nécessaire à l'accomplissement de la finalité du traitement pour laquelle elles ont été collectées. A l'expiration de cette durée, les données doivent être détruites". Si l'entreprise souhaite les conserver davantage elle doit demander une autorisation expresse à la CNDP.

La CNDP

La Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) a été créée par la loi n°09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Elle est chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'homme. Elle offre de nombreux services en ligne et indique aux entreprises les démarches à suivre : <https://www.cndp.ma>

LE RGPD

Le Règlement Général sur la Protection des Données (RGPD) est le texte de référence en matière de protection des données à caractère personnel au sein de l'Union Européenne. Entré en vigueur le 25 mai 2018, il remplace la directive sur la protection des données personnelles (95/46/CE) adoptée en 1995.

Pour en savoir plus et se conformer, consulter le site de l'Union Européenne (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_fr) ou le site de la CNIL en France (<https://www.cnil.fr/fr/comprendre-le-rgpd>)



L'ŒIL DE L'EXPERTE

MAÎTRE LINA FASSI-FIHRI, ASSOCIÉE GÉRANTE LPA-CGR À CASABLANCA, AVOCATE AU BARREAU DE PARIS

“La mise en conformité au RGPD commence nécessairement par une phase d'audit. On répond à des questions simples : qui a les données, où elles sont, pourquoi on les collecte, conserve, transfère et à qui ? Combien de temps on les conserve ?

Les réponses à ces questions, vont permettre de cartographier les données personnelles. A l'issue de cet audit, on va mesurer l'écart entre ce que demande la réglementation et ce qui est vraiment en place dans l'entreprise. C'est à ce stade notamment que l'accompagnement d'un expert est utile car le texte est ardu et il faut aussi savoir prioriser en fonction des risques légaux quelles actions doivent être mises en place.

Ce qui amène à la deuxième phase, le plan d'implémentation des actions identifiées qui seront : rédiger la documentation, créer un registre des traitements, mettre en place un data protection officer, renforcer le volet IT, faire des formations... Tout ce dispositif prend généralement plusieurs mois.”

Jusqu'à présent, trop peu de dirigeants d'entreprise au Maroc se sont inquiétés de leur mise en conformité. Pourtant, il faudrait y voir un outil capable de dynamiser son activité, de faire de la smart compliance, et surtout le moyen de ne pas perdre de parts de marché si ses donneurs d'ordres sont européens.

Droit des personnes

La loi 09-08 prévoit un certain nombre de droits pour les personnes dont les données sont collectées, et il incombe à l'entreprise de tout mettre en œuvre pour les garantir et permettre leur exercice. Le responsable du traitement doit également « prendre toutes les précautions utiles pour garantir l'intégrité et la confidentialité des données personnelles en sa possession en vue de les protéger contre la destruction ou la perte accidentelle et contre toute forme de traitement illicite ». Il doit donc veiller à ce que ses sous-traitants et les tiers qui ont accès aux informations, respectent toutes les dispositions de la loi 09-08. Aussi, il est fortement recommandé aux entreprises de consulter la CNDP pour vérifier qu'elles respectent parfaitement le cadre législatif.

Respect du RGPD pour de nombreuses PME

Au-delà de la loi marocaine, qui devrait prochainement évoluer pour se rapprocher des réglementations internationales, de nombreuses PME sont également concernées par le règlement de l'Union Européenne (UE). En effet, le Règlement Général sur la Protection des Données (RGPD), entré en vigueur en mai 2018, s'applique aussi en dehors de l'UE lorsque cela concerne des données personnelles de résidents européens.

De ce fait, beaucoup d'entreprises marocaines sont concernées dans les secteurs de l'offshoring (centres d'appels et autres sous-traitants), du tourisme (hôtels), des télécoms ou des banques notamment. Plus encore, les sites web visités par des Marocains Résidents à l'Etranger (MRE) ou tout ressortissant européen, doivent se conformer au RGPD.

En cas de non respect, les sanctions financières peuvent être lourdes : jusqu'à 20 millions d'Euros ou jusqu'à 4% du chiffre d'affaires mondial (le montant le plus élevé étant retenu). De plus, le risque est grand pour les PME marocaines de perdre des clients européens si elles ne respectent pas cette réglementation.

CONSEILS POUR SE CONFORMER

- **Diagnostiquer la situation** : s'informer sur la ou les réglementations (locales et internationales) qui s'applique(nt) à l'entreprise, puis auditer les processus pour étudier leur conformité.
- **Mettre en place un plan de conformité** : sensibiliser les salariés et revoir l'ensemble des procédures et contrats pour les rendre conformes à la réglementation. Suivre le plan dans la durée pour veiller à ce que les nouveaux projets correspondent bien aux attentes.
- **Désigner un Délégué à la Protection des Données (DPO)** : rendu obligatoire par le RGPD dans certains cas, le DPO est chargé de mettre en œuvre la conformité au règlement européen. Il peut s'agir d'un salarié formé pour la fonction ou d'un prestataire externe qui suivra l'ensemble des projets.