L'IMPACT DU RÈGLEMENT GÉNÉRAL ENCADRANT LA PROTECTION DES DONNÉES PERSONNELLES SUR LES ENTREPRISES AFRICAINES

Les données personnelles [1] sont omniprésentes et désormais au cœur de la chaîne de création de valeur des entreprises. Bien gérées et sécurisées, elles permettent de gagner en efficacité et en compétitivité, de personnaliser et de conforter la relation avec les clients, de conquérir de nouveaux marchés, d'améliorer les produits et services et de faciliter la collaboration et la mobilité. Pour s'adapter aux enjeux du numérique et garantir une meilleure maîtrise des données personnelles, une nouvelle régulation européenne, le Règlement Général sur la Protection des Données («RGPD»), est entrée en vigueur le 25 mai 2018.

Ainsi, le nouveau règlement vise, non seulement à harmoniser le cadre juridique fragmenté de la protection des données dans l'Espace Économique Européen («EEE»), mais aussi à garantir les droits fondamentaux des individus dans l'économie digitale d'aujourd'hui [2].

Pour le législateur Européen, le renforcement de ce cadre juridique est appelé à réduire les coûts de mise en conformité des entreprises, mais également à asseoir la confiance des consommateurs dans la sécurité de l'économie numérique mondiale. C'est en considération de cet objectif que l'application du RGPD n'entend pas s'enfermer dans les limites géographiques de l'Union européenne («UE»). Cet expansionnisme législatif affirmé, soulève inévitablement la question de l'extraterritorialité du RGPD.

En effet, afin de réduire considérablement l'inégalité découlant de la soumission exclusive des entreprises territorialement localisées dans l'UE –laquelle inégalité les désavantageait dans les rapports concurrentiels–, le RGPD s'est attelé à imposer les mêmes obligations aux entreprises établies hors de l'UE, parmi lesquelles les entreprises africaines, dès lors que ces dernières proposent des produits ou services aux résidents européens.

La formalisation de la portée mondiale du RGPD ne devrait plus surprendre aucune entreprise internationale puisque dès les premières phases de son élaboration, la portée extraterritoriale avait été affichée.

En tant que figure juridique originale défiant le principe ancien de la territorialité de la loi, l'extraterritorialité assumée du RGPD appelle une réflexion sur son impact inévitable, sur les entreprises africaines qui recueillent et/ou traitent des informations personnelles des résidents européens.

L'analyse de son contenu et de son application révèle qu'elle met à la charge des entreprises africaines une obligation de mise en conformité (1), dont le non-respect est susceptible de sanctions (2).

1. Obligation de mise en conformité des entreprises africaines traitant des informations personnelles des résidents européens

L'étude de cette obligation ne peut s'effectuer (1.1) qu'au travers de l'analyse de son fondement et (1.2) des actions à entreprendre pour la mise en conformité.

1.1. Fondement

Une norme est extraterritoriale lorsque la compétence normative d'un Etat *« régit des rapports de droit situés en dehors du territoire de cet Etat »* [3]. Par conséquent, la norme extraterritoriale « tend à développer certains effets au-delà du territoire de l'Etat qui l'a émise » [4]. L'extraterritorialité va ainsi à l'encontre du principe de territorialité des lois selon lequel, un Etat souverain exerce ses compétences législatives dans les limites de son territoire, de façon à ne pas heurter la souveraineté d'Etats voisins.

La vocation extraterritoriale d'une loi nationale n'est admise en droit international, qu'à la condition que la loi envisagée se borne à saisir des situations juridiques constituées à l'extérieur de son territoire, mais possédant un lien objectif étroit avec l'Etat d'origine de la norme. En effet, selon le professeur Brigitte Stern, un Etat peut appliquer une loi à l'étranger non seulement si un critère de rattachement est présent, mais également si ce dernier est raisonnablement rattaché aux faits [5]. C'est sous le droit international privé qu'est étudiée cette matière.

L'extraterritorialité du RGPD trouve son fondement à l'article 3, alinéa 2 qui prévoit son application à tout responsable

de traitement ou sous-traitant qui, tout en étant établi hors de l'UE, traite des données personnelles de personnes concernées situées au sein de l'UE. Il s'agit là d'une volonté réelle du législateur européen, de rendre effective la protection des données personnelles, en fermant aux entreprises assujetties, toute possibilité de soustraction à l'empire du RGPD, au moyen d'une délocalisation hors de l'UE.
Le critère de rattachement étant lié au territoire national, tous les organismes privés ou publics, de grande ou de petite taille, établis ou non au sein de l'UE, devront appliquer les exigences issues du RGPD, dès lors que leurs activités se rapportent au traitement des données personnelles de personnes se trouvant dans l'UE. Les entreprises africaines n'y échappent pas.
Par ailleurs, il n'est pas nécessaire, pour faire naitre l'obligation de mise en conformité, que les activités principales de ces entreprises soient en rapport avec l'utilisation, le stockage ou la collecte de données personnelles. Il suffit qu'un procédé ou un système de l'entreprise utilise des données personnelles à une certaine étape du processus de l'activité, pour que les dispositions du RGPD soient applicables. Il peut s'agir, à titre illustratif, des entreprises du secteur bancaire ou encore des télécommunications.

1.2. Procédure

La mise en conformité au RGPD des entreprises traitant des données personnelles de personnes situées au sein de l'UE peut se résumer en 4 étapes [6].

1.2.1. Recensement des fichiers

L'entreprise doit procéder à une «cartographie» de l'ensemble des traitements de données inhérents à son activité. Elle doit à cet effet, tenir un registre des divers traitements de données personnelles, permettant ainsi de cerner ses besoins pratiques [7].
Le registre est placé sous la responsabilité du dirigeant de l'entreprise et devra contenir des fiches créées pour chaque activité recensée, en précisant :
- l'objectif poursuivi ;
- les catégories de données utilisées ;
- les personnes ayant accès aux données ;
- la durée de conservation de ces données.

La constitution du registre permettra d'avoir une vision d'ensemble sur le traitement des données effectué par l'entreprise.

1.2.2. Tri dans les données

Pour chaque fiche créée, l'entreprise doit nécessairement vérifier que :
- les données traitées sont nécessaires à ses activités ;
- les données traitées ne sont pas des données dites «sensibles» ou, le cas échéant, qu'elle est autorisée à le faire ;
- les personnes habilitées ont accès aux données dont elles ont besoin ;
- les données ne sont pas conservées au-delà du temps nécessaire.

Cette étape permet à l'entreprise d'améliorer ses pratiques en : - minimisant la collecte de données ; - éliminant de ses formulaires de collecte et de ses bases de données toutes les informations inutiles ; - redéfinissant les personnes habilitées à avoir accès aux données ; - créant des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans les applications utilisées [8].

1.2.3. Respect des droits des personnes

Le RGPD a renforcé l'obligation d'information et de transparence à l'égard des personnes dont les données sont traitées. Celles-ci doivent être informées sur la nature des données collectées et doivent également avoir les moyens d'exercer facilement leurs droits.

1.2.3.1. Le droit à l'information

Pour être loyale et licite, la collecte de données personnelles doit s'accompagner d'une information claire et précise des personnes sur :
- l'identité du responsable du fichier ;
- la finalité du fichier ;
- le caractère obligatoire ou facultatif des réponses et les conséquences d'un défaut de réponse ;
- l'autorisation à traiter ces données ;
- les personnes ayant accès aux données ;
- la durée de la conservation de ces données ;
- les modalités d'exercices des droits des personnes dont les données sont collectées ;
- les éventuels transferts de données [9].

A l'issue de cette étape, l'entreprise aura répondu à son obligation de transparence.

1.2.3.2. Faciliter les moyens d'exercice des droits des personnes sur leurs données

Les personnes dont les informations sont traitées ont des droits sur leurs données notamment : un droit d'accès, de rectification, d'opposition, d'effacement, de portabilité et de limitation du traitement.

• Le droit d'opposition

Les personnes doivent pouvoir s'opposer à la réutilisation par le responsable du fichier, de leurs coordonnées à des fins de sollicitations, notamment commerciales, lors d'une commande ou de la signature d'un contrat.
Une case à cocher, non cochée par défaut, doit leur permettre d'exprimer leur choix directement sur le formulaire ou le bon de commande à remplir. La simple mention de l'existence de ce droit dans les conditions générales n'est pas suffisante.

• Les droits d'accès

Toute personne doit : accéder à l'ensemble des informations la concernant ; connaître l'origine des informations le concernant ; accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision le concernant ; en obtenir la copie (des frais n'excédant pas le coût de la reproduction peuvent être demandés) [10].

• Le droit de rectification

Toute personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données inexactes à caractère personnel la concernant. Compte tenu des finalités du traitement, la personne concernée a également le droit d'obtenir que ces données soient complétées, y compris en fournissant une déclaration complémentaire [11].

• Le droit à l'effacement

Le droit à l'effacement, ou encore droit à l'oubli, permet à tout citoyen résidant dans un pays membre de l'Union européenne de demander à un organisme d'effacer les données personnelles le concernant.
Cette notion de droit à l'oubli peut être définie par sa finalité, en écartant les éventuels risques qu'un individu soit atteint de manière durable par l'utilisation des données qui le concerne à son insu, que celles-ci soient présentes en ligne par sa propre initiative, ou par celle d'une tierce personne.
En plus d'obtenir du responsable du traitement l'effacement des données ayant un caractère personnel, le droit à l'oubli numérique prévoit également d'effacer la diffusion de ces données personnelles, et en particulier quand la personne concernée n'accorde plus son consentement pour leur utilisation [12].

• Droit à la limitation du traitement

Le droit à la limitation du traitement s'entend comme le droit au marquage des données personnelles conservées, afin de limiter leur traitement dans le futur. En d'autres termes, ce droit indique à l'organisation concernée d'arrêter de traiter les données personnelles d'un individu sur sa demande. Concrètement, le droit à la limitation du traitement prévoit un «gel» des données pendant une durée bien définie [13].

• Droit à la portabilité des données

Le droit à la portabilité offre aux personnes la possibilité d'obtenir et de réutiliser leurs données personnelles pour répondre à leurs propres besoins, à travers différents services. A cet effet, elles peuvent désormais :
- récupérer les données les concernant traitées par un organisme, pour leurs usages personnels, et les stocker ;
- transférer leurs données personnelles d'un organisme à un autre.

Le droit à la portabilité renforce la maitrise des personnes sur leurs données personnelles. Il crée également de nouvelles opportunités de développement et d'innovation, en facilitant le partage des données personnelles de manière sécurisée et sous le contrôle de la personne concernée [14].

1.2.4. Sécurisation des données

L'entreprise doit garantir l'intégrité de son patrimoine de données en minimisant les risques de pertes de données ou de piratage.
Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que l'entreprise traite et des risques qui pèsent sur les personnes en cas d'incident [15].
Différentes actions peuvent alors être mises en place, notamment :
- des mises à jour des antivirus et logiciels des entreprises ;
- des changements réguliers des mots de passe et utilisation de mots de passe complexes ; ou
- du chiffrement des données de l'entreprise dans certaines situations.

A l'issue de cette étape, l'entreprise sera en capacité d'assurer une protection des données personnelles en continu et de faire face aux éventuels incidents.
En définitive, l'Europe, à travers le RGPD, diffuse dans le monde ses valeurs en matière de protection de la vie privée. Elle protège ainsi ses résidents contre l'usage abusif de leurs données personnelles. L'évolution de ce cadre européen de référence en la matière doit amener les acteurs du digital à faire preuve de responsabilité à l'égard des citoyens. Du côté des entreprises, le RGPD doit inciter à mettre en avant leur conformité à la réglementation comme un atout concurrentiel, tout en développant de nouveaux modèles économiques, dans leurs stratégies de gestion des données personnelles.
Les données des clients doivent être considérées parmi les «biens» les plus précieux de l'Entreprise. A ce titre, elles doivent être protégées et bénéficier d'un niveau de sécurité maximum. Des audits et/ou des certifications d'entreprises sur des normes internationales devront permettre de démontrer que le niveau adéquat de protection est bien appliqué aux données des clients (informations personnelles, informations bancaires, informations médicales par exemple), y compris lorsqu'elles transitent ou sont manipulées au sein d'une entreprise africaine, partenaire d'affaires, client ou fournisseur d'une entreprise européenne.
Le non-respect de ses nombreuses obligations réglementées dans le RGPD, est susceptible d'engendrer des sanctions lourdes de conséquences pour l'entreprise ou l'organisme fautif.

2. Sanctions en cas de non mise en conformité

L'article 51 du RGPD prévoit la mise sur pied, par chaque État membre de l'Union, d'une ou plusieurs autorités publiques indépendantes chargées de surveiller la mise en conformité des entreprises au règlement RGPD (ci-après l'«autorité de contrôle»), afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union.
L'intervention de l'autorité de contrôle est graduelle et varie en fonction de la gravité des violations relevées.
En effet, avant de parvenir aux pénalités les plus élevées, l'autorité de contrôle peut commencer par : des avertissements ou mise en demeure de l'entreprise fautive avec rappel du devoir de mise en conformité des traitements de données sensibles au RGPD ; des injonctions de cesser les violations ; et, dans certains cas, des limitations ou suspensions temporaires des traitements de données.
Si malgré ces diverses mises en garde l'autorité de contrôle constate la persistance des violations, elle pourra recourir, à l'égard de l'entreprise coupable de violations, à des (2.1) sanctions pouvant entrainer des (2.2) conséquences.

2.1. Sanctions

Il peut s'agir de sanctions administratives ou pénales.

2.1.1. Sanctions administratives

Les sanctions administratives sont celles qui sont prononcées par l'autorité de contrôle. Elles sont réparties en deux paliers, en fonction de la durée, de la nature et de la gravité de la violation du RGPD [16].
Lorsqu'il s'agit d'un manquement aux obligations incombant (i) au responsable du traitement et au sous-traitant, (ii) à l'organisme de certification ou (iii) à l'organisme chargé du suivi des codes de conduite, une amende d'un montant égal à 2% du chiffre d'affaires annuel de l'entreprise fautive ou de dix millions (10 000 000) d'euros peut être appliqué.
Dans le cas d'infractions plus graves liées à (i) l'obligation de consentement de la personne concernée avant collecte, traitement ou stockage des données personnelles, (ii) aux autres droits des personnes concernées, (iii) aux transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale, (iv) à toutes les obligations découlant du droit des Etats membres ou encore (iv) au non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle, une amende correspondant au montant de 4% du chiffre d'affaires annuel de l'entreprise fautive ou de vingt millions (20 000 000) d'euros peut être prononcée.
En considération des coûts élevés de ces amendes, les entreprises assujetties seront moins enclines à s'exposer volontairement à de telles sanctions en traitant/sous-traitant avec un partenaire d'affaires ou un fournisseur qui ne serait pas aligné sur les exigences de cette réglementation.

2.1.2. Sanctions pénales

Les sanctions administratives ne se substituent pas aux sanctions pénales. Une entreprise qui manque à ses obligations peut également être poursuivie en justice par des victimes ou toute personne concernée par ces violations.
Les sanctions pénales peuvent être édictées par les États membres de l'Union Européenne pour les cas de violations non prévus par le RGPD [17].
En France par exemple, ces sanctions sont décrites dans les articles 226-16 à 226-24 du Code pénal sous le chapitre relatif aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.
En fonction de la gravité des infractions, les peines prononcées peuvent aller jusqu'à cinq (05) ans d'emprisonnement et trois cent mille (300.000) euros d'amende.
Ces sanctions, susceptibles d'être rendues publiques, peuvent avoir un très mauvais effet sur l'image et la renommée des entreprises coupables de violation.

2.2. Conséquences

L'autorité de contrôle peut obliger les entreprises à communiquer sur les sanctions prononcées à leur encontre, aux personnes impactées par leur non-conformité.
Ça a été le cas le 21 janvier 2019, lorsque la formation restreinte de la Commission nationale de l'informatique et des libertés «CNIL», autorité de contrôle en France, a prononcé une sanction à hauteur de cinquante millions (50 000 000) d'euros contre Google LLC en application du RGPD pour défaut de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité [18].
Une sanction de l'autorité de contrôle rendue publique peut avoir un très mauvais effet en termes d'image. En Copyright Lexbase p. 6/8 effet, l'autorité de contrôle diffuse généralement un communiqué officiel reprenant les détails du manquement, ce qui a pour conséquence des répercussions médiatiques entrainant une perte de confiance du public .
L'impact est encore plus grand pour les entreprises cotées en Bourse, en raison d'un éventuel repli des investisseurs car, à une époque où les individus portent une attention particulière au respect de leurs droits et données personnelles, une entreprise faisant preuve de négligence peut sérieusement écorner sa notoriété.
Les conséquences de la non-conformité au RGPD étant importantes, il est nécessaire pour les entreprises africaines souhaitant continuer à traiter ou sous-traiter avec les entreprises européennes, de s'adapter à la nouvelle réglementation. A défaut, elles s'exposeraient à des sanctions sévères.
Le temps presse car cette réglementation est entrée en vigueur le 25 mai 2018. Inutile d'envisager de rediriger les

marchés vers l'Asie ou l'Amérique du Nord. Des réglementations similaires, tout aussi contraignantes, y sont déjà appliquées ou en voie de l'être. Il faut donc transformer, dans un délai de 18 mois, les entreprises pour les rendre conformes aux obligations réglementaires.

Le nouveau Règlement vise, non seulement à harmoniser le cadre juridique fragmenté de la protection des données dans l'Espace économique européen, mais aussi à garantir les droits fondamentaux des individus dans l'économie digitale d'aujourd'hui. C'est en considération de cet objectif que l'application du RGPD n'entend pas s'enfermer dans les limites géographiques de l'Union Européenne, mais à s'étendre aussi aux entreprises établies hors de l'UE, parmi lesquelles les entreprises africaines, dès lors que ces dernières proposent des produits ou services aux résidents européens. L'on peut retenir synthétiquement qu'il :

-renforce les droits des personnes physiques résidentes de l'UE ; -resserre les obligations de consentement ;
-durcit la responsabilité conjointe des sous-traitants et responsables du traitement ;
-impose la traçabilité des activités de traitement des données personnelles ;
-construit un sévère régime de sanction en cas de non-conformité.

Les conséquences de la non-conformité au RGPD étant importantes, il est nécessaire pour les entreprises africaines, notamment du secteur bancaire ou encore des télécommunications, souhaitant continuer à traiter ou sous-traiter avec les entreprises européennes, de s'adapter à la nouvelle réglementation. Celle-ci étant entrée en vigueur le 25 Mai 2018, Il faut transformer, dans un délai de 18 mois, ces entreprises pour les rendre conformes aux obligations réglementaires.

Sarada Nya et Khadidja Benazir Moussa
Avocate aux barreaux du Cameroun et de Paris,
Associée du cabinet Chazai & Partners
et Juriste collaboratrice au sein du cabinet Chazai & Partners

[1] Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Le traitement de données personnelles, quant à lui, est un ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement) .
[2] Préambule, RGPD.
[3] J. Salmon, Dictionnaire de droit international public, Bruylant, 2001, p. 491.
[4] J.-M. Jacquet, La norme juridique extraterritoriale dans le commerce international, Journal du droit international, 1985, p. 347.
[5] B. Stem, Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit, AFDI, XXXII, 1986. p. 10.
[6] Guide pratique de la sensibilisation au RGPD pour les petites et moyennes entreprises, Bpifrance, le Lab, CNIL, avril 2018, p.31.
[7] RGPD, art. 30.
[8] Ibidem.
[9] RGPD, art. 12.
[10] RGPD, art. 15.
[11] RGPD, art. 16.
[12] RGPD, art. 17.
[13] RGPD, art. 18.
[14] RGPD, art. 20.
[15] Bpifrance, le Lab, CNIL, op. cit., p. 38 .
[16] RGPD, art. 83.
[17] RGPD, art. 84.
[18] Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC..