Elie Koné, Associé

Traitement des données personnelles :

Etude comparative droit communautaire UEMOA - RGPD.

Par Elie Koné, Avocat à la Cour d'appel d'Abidjan, Côte D'Ivoire et M'Bia Hortense De-Yolande, PhD. Droit International, Enseignante-chercheure (Université Virtuelle de Côte D'Ivoire).

Introduction

Le 16 février 2010, la Communauté Economique Des Etats de l'Afrique de l'Ouest (CEDEAO) prenait l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel ; lequel acte, est également applicable aux Etats membres de l'UEMOA[1]. A ce jour, plus de la moitié des Etats signataires se sont inspirés de cet Acte pour asseoir une législation nationale de protection des données à caractère personnel (DCP)[2].

Le Règlement Général sur la Protection des Données numéro 2016/679 du 27 avril 2016 (RGPD), en application depuis 2018 dans les Etats membres de l'Union Européenne, semble avoir fait le tour de la question sur la protection des données personnelles et apparaît plus adapté, selon les observateurs, aux défis actuels dictés par l'usage quotidien de l'outil numérique.

La présente étude se propose de faire un comparatif de ces deux textes juridiques appelés à garantir, chacun de son côté, la protection des données personnelles dans des espaces communautaires différents, mais combien liés par des enjeux économiques importants.

---

[1] Les huit pays membres de l'Union Economique et Monétaire Ouest-Africain en abrégé UEMOA, que sont la Côte d'Ivoire, le Mali, le Burkina Faso, la Guinéee Bissau, le Sénégal, le Niger, le Togo et le Benin, sont tous membres de la CEDEAO.

[2] Six (6) Etats sur un total de huit (8) se sont dotés d'une loi sur la protection des données personnelles. Seule la Guinéee Bissau n'a pas suivi le mouvement- https://www.africadataprotection.com/liste-des-pays.html.

Nous reviendrons sur les grands principes dégagés par ces deux textes tenant au traitement, aux obligations du responsable du traitement et sa responsabilité, pour terminer sur la nécessaire opération de mise en conformité sous le regard vigilant des autorités de régulation.

A ce propos, une attention particulière sera accordée à l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire (ARTCI) et la Commission Nationale Informatique et Libertés (CNIL) en France.

I) Les grands principes du traitement

La notion de grands principes fait référence aux règles qui gouvernent le traitement des données à caractère personnel. A chaque traitement est assigné un but, un objectif, à ne pas outrepasser, au risque de tomber dans l'illégalité ou l'illégitimité par rapport au RGPD et à l'Acte Additionnel. Ces deux textes s'accordent pour définir le traitement, lequel doit être licite, c'est à dire être fait dans le cadre d'une activité professionnelle.

Les informations collectées par une entreprise auprès de sa clientèle en vue d'effectuer par exemple une livraison, éditer une facture ou proposer une carte de fidélité, constituent dans leur ensemble, un traitement des données personnelles ayant pour objectif la gestion de sa clientèle.

Le traitement de données à caractère personnel au regard du RGPD fait appel à plusieurs grands principes[3], notamment ceux de transparence, loyauté, limité dans la durée et les finalités, etc.
Les impacts sont de deux ordres :

Sur le plan interne, les organismes devront pour certains :

- désigner un délégué à la protection des données[4], chargé de contrôler la conformité de l'entreprise à la règlementation sur la protection des données personnelles,
- pour les entreprises de plus de deux cent cinquante employés ou qui réalisent certains types de traitements, elles devront constituer et tenir à jour un registre des activités de traitement[5].
- et dans tous les cas, mettre en place des procédures internes permettant d'assurer la « protection des données dès la conception » des traitements (Privacy by design)6 et mener des analyses d'impact, préalables à la mise en œuvre de certains traitements.

[3]-La Licéité, la loyauté et la transparence du traitement
-La limitation des finalités
-La minimisation des données
-L'exactitude des données
-La limitation de la conservation
-L'intégrité et la confidentialité des données https://www.cnil.fr
[4] RGPD, articles 37 à 39
[5] RGPD, article 30
[6] RGPD, article 25

Sur le plan externe, les organisations concernées devront prendre des mesures :

- à l'égard des personnes concernées, en mettant à jour les mentions d'information[7] ainsi que les modalités de recueil du consentement[8],
- à l'égard de l'autorité de contrôle, mettre en place un dispositif permettant de lui notifier la survenance d'une violation des données engendrant *« un risque pour les droits et libertés des personnes physiques »*, notification qui devra être étendue à l'ensemble de ces personnes physiques, si ce risque est *« élevé »*[9].
- à l'égard des autres acteurs non institutionnels du traitement, établir des contrats écrits non seulement avec les sous-traitants, mais aussi avec les responsables conjoints de traitement, en énumérant et répartissant précisément les rôles et responsabilités de chacun.

Tous ces principes ont pour objectif de garantir les droits de l'individu sur son *« or noir »*[10] et de mener les organisations à plus de responsabilité et de confidentialité dans le traitement des DCP.
Même si les principes mis en avant dans l'Acte Additionnel, à savoir les principes de consentement, légitimité, licéité, loyauté, finalité, pertinence, conservation, exactitude, transparence, confidentialité, de sécurité et du choix du sous-traitant sont édictés[11], l'on peut relever que le RGPD a englobé des notions non prises en compte dans l'Acte Additionnel, notamment celle de la protection des données dès leur conception. Ultimement, ces grands principes servent à mesurer l'ampleur des obligations qui pèsent sur le responsable du traitement.

II) Les obligations du responsable du traitement

Le RGPD définit le responsable de traitement comme toute personne, entreprise, organisme, autorité publique *« qui détermine les finalités et les moyens d'un traitement de données »*.

Dans la pratique, le responsable de traitement est la personne morale (entreprise, collectivité, association, etc.) incarnée par son représentant légal (président, gérant, maire…) qui est à l'origine et qui réalise le traitement. Le traitement tel que défini dans les deux textes,[12] consiste en diverses opérations. L'on pourrait citer à titre d'exemples :

- - la collecte d'informations de clients pour l'achat et/ou la livraison de biens ou pour la confection de cartes de fidélité
- - la conservation d'informations d'identification sur les salariés par les ressources humaines
- - la mise en place d'un système de vidéosurveillance, etc.

[7] RGPD, articles 13 et 14
[8] Pour les traitements soumis à consentement ; RGPD, article 7.
[9] RGPD, articles 33 et 34
[10] Matthieu Bourgeois ; Droit de la donnée, Principes théoriques et approche pratique, page XVII
[11] Acte Additionnel, Articles 23 à 29
[12] L'article 1 de l'ACTE ADDITIONNEL définit le traitement comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel ». A sa suite, l'article 4(2) du RGPD considère le traitement, comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte : l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Sur cette base, plus de la moitié de la population mondiale a eu une fois au moins ses données traitées, sans toutefois savoir que ce traitement obéissait à des principes, et que son consentement était nécessaire avant tout traitement.
Tout compte fait, le responsable de traitement est soumis à des obligations générales dont l'inobservation ou le défaut de conformité, est susceptible d'engager sa responsabilité.

A) Les obligations générales du responsable du traitement

Le responsable du traitement est soumis à diverses obligations, au nombre desquelles[13] :

- obligation de licéité du traitement : le responsable de traitement doit traiter les données en conformité avec le RGPD de manière loyale, licite, transparente. Par exemple, si le traitement repose sur le consentement d'une personne, le responsable de traitement doit être en mesure de rapporter la preuve de ce consentement.
- obligation d'information : pour la réalisation d'un traitement, le responsable de traitement a l'obligation d'informer les personnes concernées de la catégorie de traitement des données, leurs utilisations, les finalités du traitement, etc.
- obligation de sécurité : le responsable de traitement a l'obligation de mettre en place des dispositions permettant de sécuriser les données traitées. Et, en cas de violation des dispositions de protection des données, il est tenu d'en informer la CNIL et, dans les cas les plus graves, les personnes concernées.
- obligation de prise en compte des droits des personnes : le responsable de traitement doit faciliter l'exercice de leurs droits pour les personnes concernées et prendre en compte les demandes liées à l'exercice de ces droits.

Dans l'Acte additionnel[14], il faut retenir, au titre des obligations du responsable de traitement :

- obligations de confidentialité : le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et sur ses seules instructions.
- obligations de sécurité : le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et notamment, pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.
- obligations de conservation : les données à caractère personnel doivent être conservées pendant une durée fixée par un texte réglementaire et uniquement pour les fins en vue desquelles elles ont été recueillies.
- obligations de pérennité : le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

Le RGPD a une vocation extraterritoriale, puisqu'il impose des obligations aux responsables de traitement et aux sous-traitants établis hors de l'Union Européenne. Et par voie de conséquence, s'applique également en Afrique, dès lors que ces responsables traitent des données de personnes physiques résidentes européennes ou encore, lorsque le responsable de traitement est une filiale ou

[13] Informations disponibles sur le site de la CNIL --https://www.cnil.fr
[14] Article 42 à 45-Acte Additionnel A/SA.1/01/10 CEDEAO/UEMOA

une entité d'une personne morale de droit européen ou lorsque les données traitées concernent des personnes morales de droit européen.

L'impact de cette réglementation est significatif, puisqu'avec le RGPD, le sous-traitant même situé hors UE est pleinement responsable en cas de manquement aux obligations du RGPD.

Plusieurs personnes peuvent être responsables de traitement : le RGPD contrairement à l'Acte additionnel prévoit les cas de co-responsabilité. Dans un tel cas, un accord doit définir précisément les obligations et le partage de responsabilités de chacune d'elles.
Quel que soit le texte, le responsable de traitement engage sa responsabilité en cas de non-respect de ses obligations.

B) La responsabilité du responsable du traitement

Le responsable de traitement est tenu d'assurer la conformité du traitement qu'il réalise. Cela implique la prise de toutes les mesures nécessaires pour assurer cette conformité et d'être en mesure de démontrer la conformité du traitement au RGPD. C'est la consécration du principe général d'accountability. Le responsable de traitement, en fonction du traitement envisagé, doit donc évaluer les risques potentiels qui peuvent survenir et prendre toutes les mesures adéquates. Par exemple, pour certains traitements, notamment les données à caractère sensibles, des mesures supplémentaires devront être prises, comme la réalisation d'une étude d'impact ou un hébergement spécifique de ces données.[15]

Par ailleurs, si le responsable du traitement recourt à des sous-traitants, il devra s'assurer de ce que ces derniers opèrent en conformité avec le Règlement, sous peine de voir sa responsabilité engagée personnellement.

Les sanctions prévues à l'encontre du responsable, essentiellement administratives peuvent aller jusqu'à une amende de vingt millions (20 000 000) d'euros ou, pour les entreprises, jusqu'à 4% du chiffre d'affaires mondial.

L'Acte additionnel fait référence à une sanction sous forme d'amende, sans en préciser le montant[16] . Outre cette amende, des sanctions administratives peuvent être prononcées, telles que le retrait provisoire de l'autorisation de traitement accordée. Le retrait définitif peut également être prononcé par l'Autorité de protection.

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci a grand intérêt à choisir un sous-traitant offrant des garanties suffisantes de capacité et de compétence. Il incombera au responsable du traitement et à son sous-traitant de veiller au respect des mesures de sécurité définies par l'Acte additionnel.

Le traitement des données appelle donc à une extrême vigilance pour le responsable de traitement, au regard de ses implications et sanctions, en cas de violation.

[15] RGDP, article 30
[16] Article 20

III. L'autorité de régulation et la mise en conformité

Il ressort d'un état des lieux de la protection des données en date du 22 janvier 2022[17], qu'une autorité de protection des données à caractère personnel existe dans six (6) Etats [18]de l'UEMOA sur un total de huit (8).

Le Togo dispose d'une loi dédiée à la protection des données et est sur le point de se doter d'une autorité de régulation.

La Guinée-Bissau pour sa part ne dispose d'aucune législation ni d'une autorité de protection des données à caractère personnel. Il faut espérer que les enjeux économiques liés à la protection des données personnelles décideront les autorités compétentes de ce pays à se doter d'un cadre normatif de protection des données.

A) L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire

L'Acte additionnel de la CEDEAO applicable dans l'espace UEMOA recommande que chaque Etat membre mette en place une Autorité de protection des données à caractère personnel[19].

En Côte d'Ivoire, l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) a été créée par l'ordonnance numéro 2012-293 du 21 mars 2012 à l'issue de la fusion du Conseil des Télécommunications de Côte d'Ivoire (CTCI) et de l'Agence des Télécommunications de Côte d'Ivoire (ATCI).

C'est une autorité administrative indépendante qui a pour mission, en autres[20], la protection des données personnelles. Elle exerce trois types d'attribution :

- informer et sensibiliser les populations et les responsables de traitement sur leurs droits et obligations,
- réceptionner les demandes et l'octroi des récépissés de déclaration et la délivrance des autorisations pour le traitement des données à caractère personnel,
- elle exerce un contrôle proactif du respect des dispositions légales en matière de protection des données à caractère personnel, la réception des réclamations et des plaintes des personnes concernées et la sanction le cas échéant, de la violation de la loi.

L'ARTCI exerce en la matière cinq (5) types de contrôle[21].

[17]AFRICA DATA PROTECTION https://www.africadataprotection.com/liste-des-pays.html (consulté le samedi 04 juin 2022) ;
[18] Benin, Burkina Faso, Mali, Sénégal, Niger, Côte d'Ivoire
[19] Acte Additionnel, article 14
[20] Confère Articles 46 et 47 de la loi en ce qui concerne les missions de l'Autorité de protection des données à caractère personnel
[21] Confère article 4 de la Décision n°2021-0676 du 4août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel

De Janvier 2019 à Décembre 2019[22], plus de cent cinquante (150) organismes ont saisi l'Autorité, soit par appels téléphoniques, courriels, lettres physiques, en vue d'obtenir des renseignements ou de se mettre en conformité avec la législation en vigueur. Cela dénote de l'intérêt croissant pour la problématique relative à la protection des données à caractère personnel. Plusieurs entreprises ont également été auditées[23] dans le cadre de leur procédure de mise en conformité[24]. La loi du 19 juin 2013 relative à la protection des données à caractère personnel donne le cadre général des formalités à accomplir pour les entreprises engagées dans le traitement des DCP et informe sur le régime des autorisations[25].

B) La Commission Nationale de l'Informatique et des Libertés

La CNIL a été créée en 1978 par la loi Informatique et libertés. Cette loi et ses textes modificatifs, fixe sa composition, son organisation et son fonctionnement. La CNIL a une triple mission d'information, de consultation et de régulation[26]. Elle accompagne les professionnels dans leur procédure de mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

Sur trois-cent (300) contrôles réalisés en 2019 par la CNIL, trente-cinq (35) ont été effectués en ligne et quarante-cinq (45) sur pièces.[27] Quarante-deux (42) mises en demeures et huit (8) sanctions pour un montant totalisant plus de cinquante et un millions (51 000 000) d'euros d'amende ont été prises. L'objectif du contrôle étant de vérifier que les traitements mis en œuvre par l'organisme sont conformes aux dispositions de la loi du 6 janvier 1978 modifiée et au RGPD. Dans l'exercice de cette mission de contrôle, la CNIL dispose des pouvoirs pour contrôler les fichiers d'enregistrement des données personnelles. Elle exerce trois types de contrôle[28]: sur place (dans les locaux du responsable du fichier), sur convocation (dans les locaux de la CNIL) ou sur pièces (demande de documents) ; et, depuis 2014, ces contrôles peuvent être faits en ligne (contrôle de sites internet).

Lorsque les constatations n'appellent pas d'observations particulières, la procédure de contrôle est clôturée par une simple lettre du Président de la CNIL. En revanche, si des manquements significatifs sont constatés, ils peuvent aboutir à une mise en demeure adressée au responsable du traitement, aux fins d'adopter des mesures correctives dans un délai imparti ou encore, elles peuvent donner lieu à la transmission du dossier à la formation restreinte de la CNIL, qui pourra prononcer les sanctions y relatives. En tout état de cause, l'absence de réponse à la mise en demeure ou le non-

[22] Rapport activités ARTCI 2019 (https://www.artci.ci/images/stories/pdf/rapport_activite/rapport_activites_artci_2019.pdf); Page 72

[23] L'audit dont il est question ici, est mis en œuvre par L'ARTCI en collaboration avec des cabinets d'avocats certifiés.

[24] Idem

[25] Articles 5 à 11.

[26] Le RGPD confirme ces missions aux articles 57 et 58

[27] https://www.mission-rgpd.com/comment-se-deroule-un-controle-cnil/ (consulté le 04 juin 2022).

[28] Les contrôles sont effectués sur la base d'un programme annuel, des plaintes reçues par la Cnil, ou encore des informations présentes dans les médias. Ils peuvent également faire suite à un précédent contrôle. A la suite du contrôle, la CNIL reprend le procès-verbal de contrôle et examine les documents dont une copie aura été effectuée pour apprécier les conditions de mise en œuvre des traitements de données à caractère personnel. https://www.mission-rgpd.com/comment-se-deroule-un-controle-cnil/ (consulté le 4 juin 2022).

respect des injonctions formulées par la CNIL, peuvent donner lieu à, la transmission du dossier à la formation restreinte de la CNIL, qui pourra prononcer des sanctions plus importantes[29].

Conclusion :

La problématique de la protection des données à caractère personnel, se pose avec plus d'acuité avec l'usage croissant de l'outil numérique, qui offre plus de souplesse et d'opportunités dans sa gestion quotidienne. Ces avantages qui comportent en eux leurs propres inconvénients, en raison de l'exposition de flux importants de données à un public indéterminé et inquantifiable, comporte des risques et enjeux importants que de nombreux textes sur divers continents, ont eu pour vocation de réduire ou juguler.

Ces textes, notamment l'Acte additionnel du 16 février 2010 et le RGPD du 27 avril 2016, ont l'avantage de répondre à ce besoin de sécurité des personnes dont les données personnelles sont au quotidien, l'objet de traitement, à des fins diverses. En cela, ils constituent une évolution qualitative.

Cet objectif fort louable peut se retrouver quelque peu distancé par la vitesse de transformation du vecteur de ces données que sont les télécommunications et les nouvelles technologies, devant donner lieu à une capacité d'adaptation permanente de la législation en la matière, voire à une législation prospective. Faute de quoi, les dispositions textuelles peuvent se trouver assez vite dépassées.
C'est déjà le cas pour l'Acte Additionnel de 2010, qui devra faire sa mue.

Conscients de ces faiblesses, la plupart des Etats membres de l'UEMOA ont adopté des législations récentes dont les dispositions pour certaines, dépassent le cadre du texte communautaire. C'est le cas en Côte d'Ivoire, avec la loi du 19 juin 2013 relative à la protection des données à caractère personnel. L'intelligence artificielle, qui est de plus en plus prégnante, ouvrira à n'en point douter de nouveaux enjeux quant au traitement des données personnelles.

Enfin, ces données, traitées, conservées et contrôlées, par les autorités de contrôle de différents espaces, notamment l'UEMOA et l'Europe, qu'en est-il des rapports entre ces différentes autorités ? Coopèrent-elles, dans quel cadre ?

Tel pourrait être l'enjeu d'une véritable protection des données à caractère personnel, dans un monde virtuel, sans frontières.

[29] https://www.mission-rgpd.com/comment-se-deroule-un-controle-cnil/