



HAL
open science

L'évolution de la question de protection des données personnelles au Bénin.

Cherif Allade

► **To cite this version:**

Cherif Allade. L'évolution de la question de protection des données personnelles au Bénin.. 2022.
hal-03652527

HAL Id: hal-03652527

<https://hal.science/hal-03652527>

Preprint submitted on 26 Apr 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**Sujet : L'évolution de la question de protection des données personnelles au
Bénin**

ALLADE CHERIF RAIMI

Doctorant au *Centre d'Études sur la Sécurité internationale et la Coopération Européenne (CESICE)* à l'université de Grenoble-Alpes

Introduction

I-Régulation des données à caractère personnel au Bénin

- A- La portée de la loi N°2009-09 portant protection des données à caractère personnel
- B- La loi N°2009-09 portant protection des données à caractère personnel reformée.

II- Analyse comparée de l'évolution des différentes législations pour la protection des données personnelles béninoises

- A-Évolution du champ d'application du traitement des données à caractère personnel
- B-Mécanismes d'encadrement actuel du transfert des données personnelles

Introduction

L'impact d'internet de nos jours dans les sociétés africaines revêt une révolution tant économique et sociale. Cette révolution est la conséquence directe de la production en masse des données quotidiennes des utilisateurs numériques. Cette forte production de données dans le continent devient une autre ressource précieuse pour le développement en dehors des autres ressources minières traditionnelles que comporte l'Afrique. Au Bénin, le fort taux de pénétration d'internet est estimé à 3,5 millions de population dont 28,4%¹. Une nette croissance au regard du taux de pénétration estimé à 18,2% en 2020. Ce boom de pénétration d'internet généralisé dans le continent ses dernières années met en défi les acteurs numériques composants cet écosystème à relever les défis de sécurité et de protection des données des utilisateurs. Dans l'une de ses sorties, le Président ivoirien en 2014, alerte le continent sur la nécessité de participer à la dernière révolution industrielle : « *L'Afrique a raté la seconde révolution industrielle, elle n'a pas le droit de rater la troisième*² ». Cet appel à la responsabilité souligne l'état de nécessité des normes juridiques, techniques et organisationnelles permettant de renforcer la souveraineté numérique des États. La souveraineté numérique des États passe ainsi par la capacité à protéger et à sécuriser les systèmes d'information et l'information générée par les usagers : la mise en vigueur des différentes lois et textes réglementaires sur la protection des données à caractère personnel. Le Bénin n'étant pas épargné des exigences en matière de la révolution numérique, l'objet de cet article est de faire une analyse juridique de l'approche du législateur béninois sur la protection des données personnelles des utilisateurs béninois.

L'adoption de la loi N°2009-09 relative à la protection des données à caractère personnel en république du Bénin³ fait du pays l'un des premiers pays de l'Afrique de l'Ouest à l'instar du Burkina-Faso⁴ et le Sénégal⁵ à se doter d'un cadre législatif règlementant la collecte, le stockage, le traitement et l'usage des données à caractère personnel tout en situant la responsabilité des acteurs intervenant dans leurs différentes fonctions. Le but de cette loi est la protection et la promotion dans un espace numérique, des libertés publiques, collectives ou

¹ Digital Report 2021 of We Are Social and Hootsuite

² Sophonie KOUDE, « Le continent doit faire sa révolution numérique », Tribune Technologie, jeuneafrique, 05 juin 21

³ La Loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin

⁴ Loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel au Burkina-Faso.

⁵ Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel au Sénégal.

individuelles, le droit à la vie privée et aux droits de l'homme ⁶. Subséquemment, le Bénin s'est doté du code numérique ⁷ présenté en cinq chapitres à savoir : les outils électroniques ; les services de confiance en l'économie numérique ; le commerce électronique ; la protection des données à caractère personnel en enfin la cybercriminalité et la cybersécurité ⁸. Le présent code a pour objet de renforcer les différentes activités dans son cyberspace. Ainsi, ce dernier a modifié l'ancienne loi sur la protection des données à caractère personnel en vigueur dans ce pays.

L'on pourrait s'interroger sur la modification et la pertinence des dispositions concernant la protection des données à caractère personnel présente dans le code numérique depuis son entrée en vigueur. En réalité, deux explications pourraient être apportées à cette interrogation. Il s'agit, tout premièrement, du renforcement des droits des personnes détaillés et explicites eu égard à leurs données personnelles. Deuxièmement, cette reprise s'inscrit dans le cadre d'une politique d'harmonisation des dispositions nationales avec le droit communautaire portant sur la protection des données à caractère personnel dans l'espace CEDEAO en 2010⁹ et aussi la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel adoptée en 2014¹⁰. Cette harmonisation, suscitée avec le droit communautaire, se traduit par l'acte additionnel de la CEDEAO en son article 2 soulignant la nécessité pour chaque pays membre de disposer un cadre légal de protection des données de la vie privée¹¹. Cette recommandation fut rappelée en son article 8.1 de la convention de Malabo de 2014¹².

⁶ Article 2 de la Loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin

⁷ Loi N°2017-20 DU 20 Avril 2018 portant code du numérique en République du Bénin.

⁸ Article 2 idem.

⁹ Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 Février 2010.

¹⁰ Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 Juin 2014.

¹¹ Article 2 de l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 Février 2010 : « *chaque État membre met en place un cadre légal de protection de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel sous réserve de la protection de l'ordre public.* »

¹² Article 8.1 de la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 Juin 2014 : *chaque État partie s'engage à mettre en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel.*»

Toutefois, la matérialisation de ces différentes dispositions à l'échelle régionale et continentale par le Bénin portant sur la protection des données à caractère personnel semblerait relative. Il est à noter que le Bénin, jusqu'aujourd'hui n'a pas encore ratifié la convention de Malabo malgré le respect des grandes lignes de ladite convention. Il s'agit par exemple de la mise en place d'une autorité indépendante chargée de la protection des données à caractère personnel, des obligations du responsable de traitement et les droits des personnes dont les données font l'objet d'un traitement. La non-ratification de cette convention pourrait être pour des raisons politiques qui ne sembleraient pas importantes d'évoquer dans le présent article.

Par ailleurs, la régulation des données personnelles visant à responsabiliser les acteurs intervenant dans cet environnement numérique quant à la collecte, le traitement, le stockage et l'usage des données à caractère personnel se heurtent à d'autres enjeux peu prévisibles. A titre illustratif, la condition défavorable à laquelle sont confrontées ces différentes lois est l'absence de culture numérique pour la population majoritairement analphabète.

Bien que la gouvernance numérique entende situer les responsabilités de chaque acteur intervenant dans le domaine numérique, elle a pour but d'encadrer la transformation numérique de la société. Au regard du contexte africain actuel, le nouvel environnement semble obscur et favorise les multinationales (GAFAM, BATX etc.) dans la collecte illégale des données des pays africains. Cette collecte de données opérée, consiste à renforcer la pratique de la commercialisation des données africaines au détriment des utilisateurs des services de ces multinationales¹³. Même si, n'ayant pas cette culture numérique, les utilisateurs africains notamment les béninois favorisent cette pratique jugeant selon eux, comme une contrepartie des services gratuitement proposés par ces multinationales. Une situation qui illustre bien les propos de A. Lewis soulignant : « *Si vous ne payez pas un service sur le Net, c'est que vous n'êtes pas un consommateur, vous êtes le produit vendu*¹⁴ ». On peut citer par exemple, la politique de Facebook '*Free Basics*' qui permet l'accès gratuitement au réseau social Facebook et autres services aux utilisateurs béninois¹⁵. Une pratique trompeuse qui laisse croire qu'il s'agit d'un favoritisme à la connectivité Internet.

¹³ Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haïdara, « Droit des activités numériques », 1^{re} éditions, Dalloz, 2014

¹⁴ Propos de A. Lewis, cité par J.-E. Ray, « Actualité des TIC », Dr.soc.2011, N°9-10, P933

¹⁵ Jean-Philippe Louis, « Free Basics : Facebook étend son service Internet pour les plus démunis en Afrique », Les Échos, 2016

Les récents progrès au Bénin en matière de gouvernance numérique laissent croire à une prise de conscience de la nécessité d'encadrement de cet environnement numérique. C'est le cas des différents textes législatifs en vigueur dans le pays encadrant la protection des données à caractère personnel. L'objet de cet article est d'exposer l'évolution et les insuffisances perceptibles des différents textes réglementaires à la protection des données personnelles au Bénin. Ainsi, il sera question de présenter les différents textes juridiques applicables à la protection des données personnelles (I) et d'analyser les différents apports de ces textes pour un régime efficace de protection de ces données (II).

I- La régulation des données à caractère personnel au Bénin

Comme évoquée ci-dessus, la loi portant sur la protection des données personnelles a vu le jour en 2009. Cette loi référentielle¹⁶ s'est améliorée au fil des années pour être codifiée dans le code numérique¹⁷ qui, par la suite, fut modifié dans la loi N° 2020-35 portant modification du code du numérique aux termes des articles 121, 125 et 464¹⁸. Dans cette partie, la nouvelle loi portant modification du code numérique en vigueur ne sera pas abordée au regard de son apport sur le fonctionnement de l'Autorité Indépendante aux termes des différents articles évoqués ci-dessus. Ainsi, l'analyse juridique de l'environnement numérique béninois consiste à étudier les particularités des deux premières législations en matière de protection des données à caractère personnel : *la loi N°2009-09 portant protection des données à caractère personnel (A) et la Loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin (B)*.

¹⁶ La Loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin

¹⁷ La Loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin.

¹⁸ Les articles 121, 125 et 464 de la loi n° 2020-35 du 06 janvier 2021 portant modification du Code du numérique en République du Bénin portent sur l'organisation de l'Autorité de régulation de la communication électronique et de la poste et l'Autorité de protection des données à caractère personnel.

A- Loi N°2009-09 portant protection des données à caractère personnel

La question de la protection des données à caractère personnel a vu le jour au Bénin à travers la loi N°2009-09 et serait le premier cadre juridique réglementant les données à caractère personnel. En effet, cette loi définit les données à caractère personnel, au sens de l'article 4 alinéa 1, comme étant : « *Toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. [...]*¹⁹ ». Il résulte de cette disposition que le législateur béninois a exclu toutes les données relatives aux personnes morales. Loin de devenir une réglementation unique, l'instauration du cadre juridique sur la protection des données par le législateur trouve son fondement dans la loi informatique et libertés de 1978²⁰. Ainsi, il est important de noter que la loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel s'est inscrite dans les directives énoncées par la loi informatique et Libertés pour la liberté individuelle et publique lors du traitement automatisé des données personnelles.

Concernant le traitement des données à caractère personnel des personnes physiques, l'article 4 alinéa 7 le définit comme : « *Toute opération ou tout ensemble d'opérations portant sur de telles données quel que soit le procédé utilisé et notamment la collecte, l'enregistrement, l'organisation, la consécration, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission ou diffusion de tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction*²¹ ». Aux termes de l'article 1 de ladite loi, elle s'applique uniquement aux traitements automatisés des données à caractère personnel, contenues ou devant figurer dans des fichiers numérisés, en tout ou en partie, ou manuels²². Au sens de ladite loi, les traitements automatisés concernent l'ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et, d'une façon générale, leur exploitation²³.

¹⁹ Article 4 alinéa 1 de la loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin

²⁰ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; modifiées en 2004 pour une application nationale française.

²¹ Article 4 alinéa 7 ibid.

²² Article 1 ibid

²³ Article 4 Alinéa 6 ibid.

Subséquentement, il existe certaines données relatives à la personne physique dont le traitement est interdit au regard de cette loi. Ainsi, il s'agit des données dites sensibles énumérées à l'article 6 à condition d'un consentement exprès de la personne concernée²⁴ ou pour des motifs d'intérêt public²⁵ et de recherche dans le domaine de la santé²⁶. On peut citer comme données sensibles, les données précisant les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale des personnes ou des données relatives à la santé et à la vie sexuelle de ces personnes²⁷.

Ainsi, sont exclus également, les traitements non automatisés des données à caractère personnel, contenues ou devant figurer dans des fichiers numérisés, en tout ou en partie, ou manuels. Par ailleurs, cette loi n'a aucunement précisé le champ d'application territorial (champ d'application *ratione loci*) des traitements des données à caractère personnel effectués par les responsables de traitements et les sous-traitements. Cette absence du champ d'application territorial constituerait un obstacle pour l'applicabilité de cette loi au regard du caractère transfrontalier des données numériques.

Eu égard à cette loi, le champ d'application reste limitatif quant aux traitements des données à caractère personnel. Malgré ces insuffisances, cette loi serait un grand pas dans la normalisation des règles juridiques applicables aux données personnelles. L'adoption du code numérique peu d'années plus tard, a suscité une révolution législative dans l'environnement numérique dans l'espace béninois.

²⁴ Article 6 alinéa 1 *ibid.*

²⁵ Article 6 alinéa 3 *ibid.*

²⁶ Article 7-e-f *ibid.*

²⁷ Article 6 alinéa 1 *ibid.*

B- La Loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin.

L'avancée majeure de ce code numérique est la vaste prise en compte des données ainsi que leurs traitements. Le cadre juridique de la protection des données à caractère personnel se trouve au chapitre 5 de ce code numérique. L'objectif des différentes dispositions prévues dans ce chapitre est la protection de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel²⁸.

En effet, aux termes de l'article 1 du code numérique, on entend par donnée à caractère personnel : « *Toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée* ²⁹ ». Et ajoute, est réputée identifiable, « *une personne qui peut être identifié, directement ou indirectement notamment par référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs des éléments spécifiques propres à son identité physique, psychologique, génétique, psychique, culturelle, sociale ou économique* ³⁰ ». Au regard de cette définition, le législateur n'a pas apporté de changement majeur quant à la définition des données à caractère personnel prévue dans l'ancienne loi. Par conséquent, les données de type morales sont exclues du champ d'application de ce code numérique. En outre, le code exclut tout traitement de données opérées par une personne physique dans le cadre exclusif de ses propres activités personnelles ou domestiques et dont le but n'est pas de les communiquer à des tiers ou de les diffuser à l'exception des règles applicables en procédure pénale³¹.

Ils existent d'autres données personnelles soumises aux régimes particuliers. Il s'agit des données sensibles³², des données à caractère personnel relatives aux condamnations pénales et aux mesures de sûreté connexes³³, des données à caractère personnel à des fins historiques, statistiques ou scientifiques³⁴ et des données à caractère personnel aux fins de journalisme, de

²⁸ Article 379 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin.

²⁹ Article 1 *ibid.*

³⁰ *Ibid.*

³¹ Article 382 *ibid.*

³² Article 394 *ibid.*

³³ Article 396 *ibid.*

³⁴ *Ibid.*

recherche, d'expression artistique ou littéraire³⁵, le législateur conclut à une interdiction relative de leur traitement. Cette interdiction relative s'explique par une autorisation sous certaines conditions de ses différentes données personnelles.

D'abord, l'autorisation du traitement des données sensibles s'applique lorsque le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ; le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public; le traitement est effectué en exécution de lois relatives à la statistique publique ; le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; etc.³⁶.

Ensuite, l'autorisation du traitement des données à caractère personnel relative aux condamnations pénales et aux mesures de sûreté connexes s'applique lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis, ou à l'exécution d'une mission effectuée pour des motifs importants d'intérêt général, dans la mesure où ce traitement est autorisé par le droit des États membres de la CEDEAO ou par la législation d'un État membre prévoyant des garanties adéquates³⁷.

En outre, l'autorisation du traitement des données à caractère personnel à des fins historiques, statistiques ou scientifiques s'applique lorsque ces données sont anonymes et ne permettant pas d'identifier les personnes concernées dans le cas d'un éventuel traitement³⁸. Enfin, l'autorisation du traitement des données à caractère personnel aux fins de journalisme, de recherche, d'expression artistique ou littéraire s'applique lorsqu'il poursuit des objectifs à titre professionnel en matière d'expression littéraire et artistique dans le cadre de leurs professions³⁹.

³⁵ Article 397 *ibid.*

³⁶ Article 394 *ibid.*

³⁷ Article 395 *ibid.*

³⁸ Article 396 *ibid.*

³⁹ Article 397 *ibid.*

II- Analyse comparée de l'évolution des différentes législations pour la protection des données personnelles béninoises

L'avancée majeure du code numérique concerne la prise en compte des recommandations de l'acte additionnel de 2010 relative à la protection des données à caractère personnel dans l'espace de la CEDEAO, particulièrement les traitements des données à caractère personnel. Des recommandations dues à l'avancée majeure des questions de la protection des données à caractère personnel face à la menace cyber qui est devenue de plus en plus préoccupante face à la transformation numérique de la société. La prise de conscience dans l'usage quotidien des technologies et de la communication devient un enjeu majeur inhérent à la vie privée et professionnelle des utilisateurs. Ainsi, il convient d'analyser l'évolution législative observée dans les traitements des données personnelles au Bénin ainsi que les modalités du transfert de ces données.

A- Évolution du champ d'application du traitement des données à caractère personnel

Au regard de ces différentes lois, la révolution législative qu'il serait important de dégager dans le cadre juridique du traitement des données est l'inclusion dans le code numérique des traitements non automatisés des données à caractère personnel, contenues ou devant figurer dans des fichiers numérisés, en tout ou en partie, ou manuels. Une avancée majeure à l'actif du pays dans le cadre du processus d'harmonisation **des lois nationales** des pays membres de la CEDEAO pour la protection des données à caractère personnel.

Aux termes de l'article 383 du code numérique, le législateur béninois fixe les conditions générales de licéité des traitements de données à caractère personnel. Considérant les différentes conditions, le législateur impose, que les données à caractère personnel soient traitées de façon licite, transparente et collectées pour des finalités déterminées. Ces dernières doivent être explicites, légitimes, adéquates, pertinentes et limitées à ses finalités. Enfin, elles doivent être exactes, tenues à jour et conservées de façon temporaire et sécurisée⁴⁰. L'approche du législateur béninois est sans équivoque et homogène sur les

⁴⁰ Article 383 *ibid.*

conditions de traitement des données à caractère personnel depuis l'avènement de l'ancienne loi.

Cette homogénéité s'observe dans la définition des responsables de traitement et des sous-traitants tant au niveau de l'ancienne loi ⁴¹ et du code numérique⁴². Les termes employés dans l'ancienne loi par le législateur restent flous mais sont élucidés et détaillés dans le code numérique. Selon le code numérique, les responsables de traitements peuvent être une personne physique, l'État, les collectivités territoriales, les personnes morales de droit public ou de droit privé⁴³.

Contrairement à l'ancienne loi, la prise en considération du champ d'application territorial pour le traitement des données à caractère personnel des personnes concernées se trouvant au Bénin est une avancée majeure de la protection des données à caractère personnel. Ainsi, aux termes de l'article 381 du code numérique, les dispositions relatives à la protection des données à caractère personnel présent dans le code numérique s'appliquent d'abord, à tout traitement effectué par un responsable de traitement ou d'un sous-traitant sur le territoire du Bénin quel que soit le lieu de traitement des données⁴⁴. Ensuite, sous certaines conditions, elles s'appliquent au traitement relatif à des personnes concernées qui se trouvent sur le territoire béninois quel qu'en soit le lieu d'établissement du responsable de traitement ou du sous-traitant lorsque le traitement concerne les données relatives à l'offre de biens ou de services des personnes concernées au Bénin ; des données relatives des personnes concernées pour le suivi de leur comportement ayant lieu au Bénin et le traitement mis en œuvre sur le territoire d'un État membre de la CEDEAO⁴⁵. L'approche du législateur béninois vise à appliquer les dispositions nationales sur la protection des données à caractère personnel quand le traitement de ses données concerne les béninois ou quand le responsable de traitement ou sous-traitant se trouve sur le territoire béninois.

Enfin, selon le même article, les dispositions relatives à la protection des données à caractère personnel présent dans le code numérique s'appliquent au traitement effectué dans un autre État

⁴¹ Article 4 alinéa 4 de la loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin

⁴² Article 380 alinéa 1 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin.

⁴³ Ibid.

⁴⁴ Article 381 alinéa 1 ibid.

⁴⁵ Article 381 alinéa 2 ibid.

ou le droit de la République du Bénin s'applique en vertu du droit international⁴⁶. En somme, l'approche sur la compétence territoriale sur le traitement des données à caractère personnel des personnes concernées se trouvant au Bénin s'est inspiré du Règlement Général de la protection des données (RGPD) du modèle européen⁴⁷.

B- Mécanismes d'encadrement actuel du transfert des données personnelles

Bien que l'ancienne loi sur la protection des données à caractère personnel ait consacré une disposition sur le transfert des données à caractère personnel vers un État étranger⁴⁸, elle demeure floue quant à la condition posée par le législateur pour ledit transfert. Selon le législateur, il faudrait que cet État garantisse un niveau de protection suffisant pour garantir cet éventuel transfert. Bien que le législateur ait utilisé terme '*niveau de protection suffisant*', les termes référentiels sont assez larges pour une bonne compréhension. Il s'agit par exemple, des dispositions de protection en vigueur dans cet État, des mesures de sécurité⁴⁹. Il faut attendre le code numérique pour avoir plus de précision sur la condition nécessaire pour un éventuel transfert vers d'autres pays étrangers des données à caractère personnel. L'article 391 du présent code numérique apporte une clarté sur le contenu du terme '*Niveau de protection équivalent et suffisant*'⁵⁰. Le niveau de protection équivalent et suffisant revêt la prise de considération dans l'État étranger, de l'État de droit, le respect des droits de l'homme et libertés fondamentale, les législations dans les domaines de sécurité publiques, de la défense et de la sécurité nationale, les règles applicables en matière de protection des données, les droits reconnus aux personnes concernées, analyse de l'autorité compétente et indépendante en matière de protection des données et ses missions, ses engagements internationaux et sa participation dans les systèmes multilatéraux pour la protection des données à caractère personnel.

En effet, il convient de noter que l'ancienne loi n'offre qu'une seule possibilité en matière de transfert des données à caractère personnel vers un État étranger : la garantie d'un niveau de

⁴⁶ Article 381 alinéa 3 *ibid.*

⁴⁷ Article 3 du Règlement Général de la protection des données (RGPD)

⁴⁸ Article 9 de la loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin

⁴⁹ Article 43-h *ibid.*

⁵⁰ Article 391 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin

protection suffisant. Exclue, contrairement au code numérique, toute organisation internationale susceptible de respecter cette unique condition. Ainsi, le code numérique pose deux possibilités pour évoquer le transfert des données à caractère personnel : d'abord, il s'agit des États tiers ou organisation internationale assurant un niveau de protection équivalent et suffisant pour le transfert des données à caractère personnel et ensuite, les États tiers ou organisation internationale n'assurant pas un niveau de protection adéquat pour un transfert des données à caractère personnel⁵¹.

A défaut de ce niveau suffisant de protection, le législateur béninois a énuméré six (06) conditions dans lesquelles ce transfert peut être effectué⁵². Sans préjudice à ses six (06) conditions pour les États étrangers ou organisation internationale, le législateur offre une possibilité de dérogation permettant d'effectuer le transfert des données à caractère personnel. Il s'agit de la prise d'un décret autorisant le transfert en Conseil des Ministres après consultation de l'autorité indépendante. Ce décret intervient lorsque le responsable de traitement provenant des États tiers ou organisation internationale présente des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants⁵³.

La normalisation de la seule possibilité du transfert des données à caractère personnel, sous l'égide de l'ancienne loi, dépendrait de l'avis de la Commission Nationale de l'Informatique et des Libertés du Bénin (CNIL Bénin)⁵⁴. Seule une autorisation de cette dernière facilitait la mise en œuvre dudit transfert⁵⁵. La même disposition fut observée avec le code numérique qui contraint les responsables de traitement à une obligation de déclaration auprès de l'Autorité⁵⁶. Malgré le changement d'institution assurant et régulant la protection des données à caractère personnel dans le code numérique, le législateur n'a pas changé de directive quant aux formalités auprès de l'Autorité Indépendante. La directive permet à l'Autorité, à l'instar de l'ancienne loi, d'émettre une autorisation préalable dans le cas du transfert des données à

⁵¹ Article 392 *ibid.*

⁵² *Ibid.*

⁵³ *Ibid.*

⁵⁴ Article 41 de la loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en République du Bénin a institué la création de la Commission Nationale de l'Informatique et de Libertés du Bénin (CNIL Bénin)

⁵⁵ Article 43-h *ibid.*

⁵⁶ Article 405 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin a institué la création de l'Autorité de Protection des Données à Caractère personnel (APDP)

caractère personnel à destination d'un État tiers. On conclut qu'en cas de transfert des données à caractère personnel des béninois, l'Autorité indépendante doit, après être informée, donner son avis sur l'opération. Elle veille à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte à l'identité humaine, aux droits de l'Homme, à la vie privée, aux libertés individuelles ou publiques.

Selon le législateur béninois, la violation du responsable de traitement des conditions préalables pour un transfert des données vers un tiers ou autres est considérée comme un *manquement grave*⁵⁷. Une approche de sanction adoptée par le législateur béninois depuis l'ancienne loi sur la protection des données personnelles⁵⁸. S'agissant de ce manquement grave, l'Autorité peut prononcer un avertissement à l'encontre du responsable du traitement et/ou procéder à une mise en demeure de cessation du manquement dans un délai de huit (08) jours. En cas de non-conformité à la mise en demeure prononcée par l'Autorité, le responsable du traitement peut se voir infliger des sanctions telles que : des sanctions pécuniaires selon l'intime conviction de l'Autorité en rapport à la taille de l'entreprise, son domaine d'intervention et à la nature du manquement⁵⁹, une injonction de cessation dudit traitement⁶⁰, le verrouillage de certaines données personnelles, un retrait temporaire ou définitif d'autorisation à son exercice⁶¹: il s'agit des sanctions administratives. Une approche de sanction adoptée et prévue par le législateur béninois en conformité à l'acte additionnel de la CEDEAO⁶². Le responsable de traitement n'est pas exempté des sanctions pénales conformément aux dispositions du code numérique⁶³. Il encourt une peine de six (06) à dix (10) ans d'emprisonnement et/ou d'une amende de dix millions (10 000 000) à cinquante millions (50 000 000)⁶⁴. Il convient de souligner toutefois que le législateur béninois punit aussi toute tentative ainsi que tous complices des violations

⁵⁷ Article 453-2 *ibid.*

⁵⁸ Article 60 de la loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin a institué la création de la Commission Nationale de l'Informatique et de Libertés du Bénin (CNIL Bénin)

⁵⁹ Article 454 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin a institué la création de l'Autorité de Protection des Données à Caractère personnel (APDP)

⁶⁰ Article 456 *ibid.*

⁶¹ Article 455 *ibid.*

⁶² Voir l'article 20 de l'Acte additionnel.

⁶³ Article 460-8 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin a institué la création de l'Autorité de Protection des Données à Caractère personnel (APDP)

⁶⁴ Article 461 *ibid.*

des dispositions du code numérique, plus précisément des dispositions en cas de transfert des données à caractère personnel⁶⁵.

Par ailleurs, l'application des législations en matière de protection des données à caractère personnel dans le monde crée une autre bataille juridique entre les États. C'est le cas des différentes conditions imposées par le législateur béninois en cas de transfert des données à caractère personnel qui semblent se confronter à d'autres législations étrangères. Ainsi, l'approche béninoise en matière de protection des données à caractère personnel se conforme et s'harmonise avec le Règlement Général sur la Protection des Données (RGPD)⁶⁶. Du point de vue formel, existe une parfaite harmonisation de la protection des données personnelles entre les deux législations. En revanche, l'application de la législation en matière de protection des données personnelles dans l'espace béninoise se heurte aux législations américaines plus précisément le Patriot Act et le Cloud Act. Ces différentes législations ayant une logique d'extra-territorialité de la justice américaine, ont un caractère très offensif dans la quête des données. En effet, le Patriot Act⁶⁷ voté par le Congrès américain au lendemain des attentats du 11 septembre 2001, vise à renforcer les pouvoirs des agences gouvernementales américaines (FBI, NSA, CIA et l'armée américaine) dans la lutte contre le terrorisme. Pour cela, sans informer la personne concernée eu égard à la sensibilité de l'enquête, le Patriot Act permet d'obtenir des informations ou données auprès de toutes les entreprises ou autres sans autorisation préalable.

Le Cloud Act⁶⁸ quant à lui, vise à permettre aux autorités américaines d'obtenir des informations ou données, après une autorisation judiciaire, auprès de toute entreprise ou autres relevant du droit américain. L'objet de cette législation est la demande directe opérée par les autorités américaines auprès des fournisseurs de service relevant du droit américain. L'élément le plus important pour l'application de cette loi est la nationalité de l'entreprise. Il s'agit d'une loi alternative permettant d'obtenir rapidement des données au lieu de recourir à des demandes

⁶⁵ Ibid

⁶⁶ Rectificatif au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal Officiel de l'Union Européenne L1272 du 23/05/2018

⁶⁷ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 : loi de 2001 visant à unir et renforcer les États-Unis en fournissant les outils appropriés nécessaires pour intercepter et empêcher le terrorisme

⁶⁸ Clarifying Lawful Overseas Use of Data Act of 2018 (CLOUD ACT), Public Law 115-141.

d'entraide judiciaire internationale communément appelées MLAT (mutuel legal assistance treaties) jugées trop longue.

Il résulte de ces différentes législations que la protection des données personnelles des béninois ne serait pas effective lorsque la demande provient des autorités américaines et ou sans autorisation judiciaire dans le cadre d'une enquête judiciaire. Un grand risque que court les béninois face aux incontournables entreprises américaines dans le monde de télécommunication. L'effectivité de cette protection s'opérerait lorsque des données sont stockées sur le territoire béninois par une structure relevant du droit béninois et détenue par une société béninoise. Une appréciation juridique jugée peu idéaliste au regard des capacités et l'inculture des entreprises béninoises dans l'urgence et l'utilité des données personnelles.

L'urgence d'un nouveau paradigme dans le traitement des données personnelles pourrait être une solution. Une solution consistant à repenser la valeur des données personnelles des béninois et les moyens dont disposent ces derniers pour exercer leur droit dans le traitement de leurs données personnelles.

CONCLUSION

La question de la protection des données à caractère personnel a connu une évolution significative ces dernières décennies. Une avancée majeure dans la prise en compte de l'importance des données personnelles dans un contexte particulièrement difficile dans la sous-région. Même si la question d'efficacité de ces différentes dispositions reste toujours un sujet à débat, le cadre formel de cette question n'en est point. Les citoyens béninois demeurent toujours insensibles à cette question. Une situation qui constitue un vrai paradoxe. Les autorités prennent des dispositions légales pour l'établissement de la vie sociétale, mais les ayant droits sont toujours dans le déni. Il n'est plus à démontrer que les données personnelles sont les carburants de l'économie numérique. N'ayant pas été sensibilisés, les citoyens ne mesurent pas l'importance de cette matière première qu'ils génèrent quotidiennement. Les données personnelles font l'objet de notre vie privée que l'on cherche absolument à protéger. Une

protection loin d'être effective quand l'on sait la valeur marchande de cette dernière dans la transformation de la société moderne et numérique de nos jours. Une situation qui illustre bien les propos de Gildas Avoine et Marc-Olivier Killijian : « (...) ; *elles ne cessent d'être divulguées, de circuler entre des mains différentes et de faire l'objet d'une exploitation marchande*⁶⁹ ». Pour remédier à cette situation, plusieurs pistes sont à étudier, mais ce qui paraît approprié, c'est la valorisation de la personne concernée dans tout le processus allant de la collecte et au gain de ces données générées. Ainsi, il est évident que lors de la collecte et le traitement des données personnelles, sauf dérogation prévue par la loi, la question de la protection des données personnelles ne se limite plus à un simple consentement de la personne concernée. Il convient toutefois de l'étendre vers la marchandisation de ces données personnelles⁷⁰. Une approche qui met la personne concernée dans un élan proactif quand il s'agit de ces données personnelles. Ces différentes actions ne seraient effectives si la sensibilisation ne fait pas l'objet d'une attention particulière.

Par ailleurs, la question des droits des personnes concernées sur leurs données personnelles reste toujours dubitative. Dans un contexte d'ignorance observé dans le cas du Bénin, la question des moyens directs dont disposent les citoyens béninois à l'encontre de ces entreprises de collecte ou autres constituent une vraie gageure. Comment les citoyens béninois peuvent-ils s'assurer de l'application effective du droit d'effacement et d'opposition de leurs propres données lorsque la demande est faite expressément ? Une question des moyens d'action et de vérification est un vrai enjeu pour lequel les autorités béninoises doivent penser pour garantir l'application effective des droits de la personne concernée. La mission de contrôle et de régulation reconnue à l'Autorité indépendante⁷¹ est limitative dans la mesure où la personne concernée de l'abus du pouvoir exercé par le responsable de traitement est inculte et/ou n'est pas au courant de cette violation.

⁶⁹ Gildas Avoine et Marc-Olivier Killijian, « *13 défis de la cybersécurité* », CNRS Editions, 2020

⁷⁰ Ibid.

⁷¹ Article 483 de la loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin a institué la création de l'Autorité de Protection des Données à Caractère personnel (APDP)

Bibliographies

Gildas Avoine et Marc-Olivier Killijian, « *13 défis de la cybersécurité* », CNRS Editions, 2020

Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haidara, « *Droit des activités numériques* », 1^{re} éditions, Dalloz, 2014

Documents officiels

Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 Février 2010.

Clarifying Lawful Overseas Use of Data Act of 2018 (CLOUD ACT), Public Law 115-141.

Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 Juin 2014.

Digital Report 2021 of We Are Social and Hootsuite

Loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel au Burkina-Faso.

Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel au Sénégal.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; modifiées en 2004 pour une application nationale française.

Loi N°2009-09 du 22 Mai 2009 relative à la protection des données à caractère personnel en république du Bénin a institué la création de la Commission Nationale de l'Informatique et de Libertés du Bénin (CNIL Bénin)

Loi N°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin a institué la création de l'Autorité de Protection des Données à Caractère personnel (APDP)

Rectificatif au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal Officiel de l'Union Européenne L1272 du 23/05/2018

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 : loi de 2001 visant à unir et renforcer les États-Unis en fournissant les outils appropriés nécessaires pour intercepter et empêcher le terrorisme

Presse et articles scientifiques

A. Lewis, cité par j.-E. Ray, « Actualité des TIC », Dr.soc.2011, N°9-10, P933

Jean-Philippe Louis, « Free Basics : Facebook étend son service Internet pour les plus démunis en Afrique », Les Échos, 2016

Sophonie KOBOUDE, « Le continent doit faire sa révolution numérique », Tribune Technologie, jeuneafrique, 05 juin 21